INDEX

1 CSC AND VARIOUS SALES CHANNELS

1.1 LEARNING OBJECTIVES

At the end of this session, participants will be able to:

- Explain the CSC Categories.
- Operation and maintenance of BSNL CSCs.
- Role of BSNL sales team.
- Explain the Role of External sales channels.

1.2 CSC CATEGORIES

CSC refers to BSNL Customer Service Centre. The CSCs of the SSA has been broadly classified into three categories, namely Category-I / Category-II / Category-III CSCs, depending upon the monthly volume of business conducted.

1.3 OPERATION AND MAINTENANCE OF BSNL CSC

a) Sale of new SIMs-Normal and Bulk Booking/Vanity and fancy number Booking/Post paid to pre-paid and vice versa conversions.

b) Plan change/ISD/International roaming.

c) VAS Services.

d) Replacement of SIMs

e) Sale of post-paid mobile connections

f) Sale of Top-ups/STVs/PVs.

g) Sales Complaint redressal

h) Processing of MNP requests

i) Bill collection of Landline/Broadband/FTTH/ Postpaid Mobile.

j) New Phone booking and feasibility of land line / Broadband / FTTH / Wings / ASEEM, Vanity booking / ISDN / PRI / BRI

k) DND Activation/deactivation.

l) Handling of bill related queries and complaints.

m) Receiving and coordinating request for shift, name transfer, and closure of Connections.

n) All commercial and CSC Services which are presently being offered in CSCs (including services being provided free of charge) and all commercial and CSC services which may emerge in future.

1.4 TERMS AND CONDITIONS OF CSC

a) The CSCs are to be manned minimum from 8.00AM to 8.00 PM for all Category-I and from 9.00 AM to 6.30 PM for all Category-II & III CSCs on all days except National holidays.

b) Proper training and dress code for staff manning the counters should be ensured.

c) Sale of products and services of BSNL should be restricted only within CSCs.

d) Non BSNL products will not be allowed to sale any from the CSC,

e) The bidder will be paid for all sales as per franchise S&D Policy 2018 and related circulars on bill payments or as modified from time to time.

f) The bidder will get commission/facilitation charges as per franchisee policies of different products/services. All cash transactions in the CSC shall be done through the CBP/CTOPUP wallet and no cash transactions shall be done between BSNL and the bidder for collections done in CSC.

g) The bidder shall be paid Rs.2/- per transaction for items not defined in franchise S&D Policy 2018. There will be a capping of 150% for all non-commercial transactions e.g. issue of duplicate bills, DND activation / deactivation etc. based on average monthly volume of last six months, but it will be further restricted to ensure that it is not more than 10% of total charges/commission earned in a month.

h) For CM related sales, no FOS will be paid on SIM sale or Recharge sale, which is otherwise paid as per franchisee S&D Policy 2018.

i) All changes in Franchisee S & D policy will be implemented with reference to commission structure as and when BSNL does so.

1.5 CM SALES AND DISTRIBUTION POLICY - 2018

Provisions of the franchisee S&D Policy -2012 have been amended and integrated "CM Sales and Distribution Policy -2018" to be effective from 01.01.2018.
This Policy is divided in four parts:

1. **E-DISTRIBUTOR POLICY**

   Distributor will be responsible for selling of BSNL Products to customers through web-portal/ Kiosk/ ATMs/ POS (Retailers) and other electronic mode on Zonal/ PAN India basis.

2. **DSA POLICY**

   Direct Selling Agents (DSA) are individuals having direct agreement with BSNL. DSAs are responsible for selling all BSNL Products, as assigned to them, to the customers at their door steps.

3. RURAL DISTRIBUTOR POLICY

Rural Distributors are individuals having agreement directly with BSNL or through franchisee. Rural Distributors will be responsible for selling all BSNL Products in Rural BTS areas through retailers. Rural Distributor will be preferably served by concerned franchisee or by BSNL directly.

1.6 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 channels of RDs.

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

d) Appointment of Retailers

e) Franchisee must appoint sufficient numbers of retailers in the territory such that:
- Each Urban BTS areas & Rural BTS areas should have at least 8 retailers and 4 Retailers respectively.
- One retailer in urban commercial area at every 200 meter
- One retailer in urban residential area at every 500 meter
- At least one retailer in every Village
- Retailers in the rural areas will be appointed and served by RDs.
- Meeting all sales targets set by SSA/Circle for the franchisee territory. Franchisee is responsible for meeting these targets through all channel entities working under him.

f) CAF collection, documentation (physical documentation as well as electronic documentation) and timely submission of documents to BSNL as per regulatory guidelines and BSNL instructions. Once the CAF has been deposited by the Franchisee under receipt to BSNL, the responsibility of documents submitted in support of customer identity & address will be on Franchisee for a period of 90 days from the date of deposit of CAF. BSNL official will check the documents within 90 days and if anything is found wrong with respect to DOT/TERM guidelines then the form should be rejected/corrected and a token penalty of Rs 200/- shall be imposed per wrong CAF on franchisee.

g) 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. Franchisees will be responsible for the verifications done by all the channels i.e. Rural Distributors and retailers working within their network.

h) BSNL reserves the right for CAF entry/CAF collection/CAF submission through any third party on outsourced model. However verification of credentials as mentioned in para (g) above shall be the responsibility of franchisee.

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

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

k) Assist and cooperate 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.

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

m) All details and information (including but not limited to FoS details, secondary sales, etc.) as specified by BSNL from time to time in BSNL specified system e.g. Sancharsoft.

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 the Franchisee. Franchisee shall redress all possible complaints on the spot. If required, help from BSNL call centers may be taken. Remaining complaints can be forwarded to designated CSC/BSNL officials for further disposal.

p) Serving retailers and Rural Distributors at their doorsteps. Franchisee must ensure that BSNL products are available with rural distributors as well as retail networks in sufficient quantity on demand. Franchisee must ensure that no black-marketing or mal-treatment to customers is done through its network.

q) The margin/ discount/ incentives / commissions extended by BSNL to franchisee and eligible retailers in their chain/ network, which shall be deemed to be extended to the franchisee, with whom BSNL has entered into an agreement pursuant to this policy and statutory requirements shall be complied with, by the franchisee.

r) Receiving advertisement/ marketing material from BSNL, and displaying it at POS and distribution to Rural Distributors. Promotion of BSNL Products at franchisee‟s own cost.

s) 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.

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

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

v) 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.

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

x) 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 purposes

1.7 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. BSNL shall also appoint other members of the Sales & Marketing team at Circle and SSA level.

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. These quarterly/monthly sales targets will be communicated by BSNL in the last week of the previous quarter/month or in the first week of the quarter/month. The target will be given on each parameter defined in 'Performance Management System'. Any exceptions to this have to be approved directly by GM (Consumer Mobility)/ designated GM by HOC. Failure to achieve the minimum sales requirement may lead to review / termination of the contract.

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. SSA Sales Head must maintain a log of all complaints received and provide regular updates to SSA Head on action taken to resolve outstanding issues.

d. It will be the responsibility of the Account Officer to remit the collection from the franchisee to credit to the 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).The Account Officer shall maintain an account of inventory sold to the Franchisee and the defective goods received back from the Franchisee, and share the same periodically with BSNL"s accounts wing along with payment balance statement.

f. Franchisee manager / SSA Sales Head (Mobility) to ensure that all sales made by BSNL to franchisee are recorded in BSNL specified IT system. Further, the sales register/ books of accounts maintained by the Franchisee may be called for as and when required by BSNL, for examination and cross- verification of sales made by franchisees in respect of BSNL"s products.

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

h. Head of Circle / SSA will ensure that BSNL Product stocks are available in sufficient quantity with BSNL in required denominations well in advance. The SSA should maintain sufficient stock of inventory so that they can fulfill the demand for provisioning of the stock as required by the franchisees, Rural Distributors and other point of sales.

i. No refund requests of any defective or unused stock shall be entertained by BSNL. Defective stock (due to the default of BSNL) with the channel partners shall be replaced at the sole discretion of BSNL after due verification.

j. In order to manage returns of defective products, BSNL may, with prior approval of the Franchisee, inspect the stock at Franchisee's location to evaluate whether or not the products are maintained in proper condition.

k. 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.

l. In order to promptly receive CAFs, there should be at least one desk or 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. Details of in-charge and location of such CAF Desk should be intimated to all Franchisees/ DSAs.

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

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

o. 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:

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

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

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

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

v. Ensure alternate/standby media connectivity to Sanchar-Soft terminals working with franchisees.
Note: - Above facility shall be up-to the validity of agreement.
Trade discounts:-

vi. Attractive trade discounts / schemes shall be offered by BSNL to the franchisee from time to time as per prevalent market dynamics.

1.8 DSA POLICY 2018

I. Scope of the Work

The Direct Selling Agent shall market and sell all BSNL Products to customers at their door steps.

II. Selection of DSAs

1. Selection of DSAs will be done by SSA Head
2. The initial period of agreement shall be for 3 years.
3. Eligibility Criteria: Any person willing to serve customers/ prospects at their premises and fulfilling following criteria are eligible to apply.
   A. Turn over : No minimum turnover is required
   B. Age : 18 Yrs
   C. Local Resident : Residing in Area for more than 1 year.
4. Valid PAN No.
5. Valid Goods and Services Tax (GST) registration Certificate No. for respective state (if applicable)
6. Self-declaration along with the evidence that the bidder is not black listed by the GST authorities
7. In case the DSA 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
8. Security Deposit: Refundable Security Deposit of Rs.500/- (Rupees five Hundred only) (No security deposit from retired BSNL/DOT employee/ co-operative societies and spouse of BSNL/ DoT employee)

9. Area of Operation: within SSA.
10. DSAs will be given free C-TOPUP SIM with applicable concessional tariff and freebies.
11. Activation SIM: BSNL may give activation SIM to willing DSAs after taking additional security deposit of Rs.3000/- per SIM.
12. Verification of credentials of new customers.
    a. Verification of credentials of new customers – Verification of PIA (photo, identity and address) of new customer to be done as per the various guidelines issued by DoT and BSNL from time to time. DSA will be responsible for the verifications done by him.
    b. The DSA shall obtain from customers/subscribers such documents as prescribed from time to time by BSNL.
13. Discount: Franchisee discount / margin will be shared among DSAs
14. Minimum amount of sales to be made by DSAs shall be communicated by SSA on a monthly basis.
15. Termination: If not found active for six consecutive months, the DSA may be terminated after issue notice and seeking explanation.
16. Extension/Migration: SSA Head may extend / migrate agreement on year-to-year basis for a period of two years with the DSA on mutually agreed terms for the active DSAs. The decision of BSNL shall be final in regard to the grant of extension.
17. BSNL and DSA shall observe the official procedure in connection with purchase and sale of BSNL Products.

1.9 RURAL DISTRIBUTOR POLICY 2018

1.9.1 **Policy Framework Of Rural Distributors (RDs)**

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.

1.9.2 **Concept Of Rural Distributors:**

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

1.9.3 **Service To Rural Distributor (RDs)**

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

- If Territory Franchisee does not serve the RDs properly then RDs will be served by BSNL directly. SSA Head will make suitable arrangements for material delivery to RDs in such case at his doorstep.
- Territory Franchisee will collect all CAFs from RDs and will provide them SIM as well as Recharge Coupon/C-TOPUP.
- RDs will make payment at the time of delivery of stock. However, they should make the requisition to the territory franchisee in advance. Representative of Territory Franchisee will deliver the stock at their doorstep.
- Suitable unlimited Broadband plan will be given to willing RD free of cost.

1.9.4 **Eligibility For RD**

- Educational qualification: 8th passed
- Rural shop/distributor of any product preferably of FMCG products / electronic / mobile products etc.
- Resident of the same territory with proof of residence.
- PAN Number.
- Valid Goods and Services Tax (GST) registration Certificate No. for each state
- Interested party should provide a self-declaration along with the evidence that the bidder is not black listed by the GST authorities
- 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.

1.10 ROLE OF SALES TEAM MEMBERS

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

1.10.1 **Roles Of Circle Sales Team**

Circle sales team will consist of GM (Sales), DGM (Sales), AGMs (Sales), SDEs (Sales) and other supporting staff. Their roles and responsibilities will be as follows:-

- Monitoring of SSA / Franchisee wise sales and performance w.r.t. target.
- Appointment of franchisees.
- Ensuring the growth of sales channel network.
- Ensuring appointment of sales team in SSA.
- Monitoring the performance of FM/ RMC/ RM.
- Ensuring the action to be taken by the SSAs.
- Ensuring the smooth functioning of sales tools such as Sancharsoft, C-TOPUP, B&CCS terminals etc.
- Redressal of issues / queries reported by the SSAs/ Franchisees.
- Redressal of cross selling.
- Escalating the unresolved problems and suggestions to improve the sale to BSNL.

1.10.2 **Roles Of SSA Sales Team**

SSA sales team will consist of DGM (Sales), DE (sales), SDE (Sales) and other supporting staff.

- Fixing of target for franchisees.
- Monitoring the sales and performance of sales partner w.r.t. the target on daily / weekly basis.
- Growth of sales channel network.
- Appointment of required sales team of FM/ RMC/ RM.

- Monitoring the performance and visit of FM/ RMC/ RM.
- Set-up and smooth functioning of sales tools such as Sancharsoft, C-TOPUP, B&CCS terminals etc.
- Area demarcation and allotment of retailers.
- Consolidation of priority list of retailers.
- Support in ordering and delivering of material to sales channel.
- Ensuring the availability of BSNL products, tariff details, advertising material to all POS.
- Redressal of cross selling.
- Payment of allowances / KPA.
- Redressal of issues / queries reported by Sales partner/ sales channel team.
- Escalating the unresolved issues and suggestions to improve the sale to Circle office.

1.10.3 **Roles Of Ssa Franchisee Manager**

- Communicating target before beginning of month i.e. by 25th of previous month.
- Support in ordering and delivery of material to Franchisee doorstep.
- Communication /action raised by the RMCs / RMs.
- Collection of data from franchisee.
- Review of franchisee data with SSA sales team.
- Supply of POS material to franchisee.
- Ensure proper uses of Sancharsoft and data entry by Franchisee.
- Redressal of issues / queries of Franchisee.

1.10.4 **Roles Of Ssa Retail Manager Coordinator (RMC)**

- Plan RM visit to existing retailers and to potential area for appointment of new retailer.
- Daily review of RM performance.
- Appointment of new retailers in potential area.
- Verification of cross selling cases.
- Compilation of daily report submitted by the RM.
- Submission of retailer wise data regarding material availability, issues etc to FM with a copy to SSA Sales Head for action.
- Providing the information regarding BSNL product / schemes / trade schemes/ VAS etc to retailer manager for further publicity.
- Conduct validation visits with RMs and FMs.
- Entry of new C-TOPUP retailers' information in Sancharsoft.
- Organization of joint visit of RM and FOS to some distressed retailers.

1.10.5 **Roles Of Ssa Retail Manager (RM)**

- Auditing the no. of visits by the FOS to retailers.
- Auditing the incentives paid to retailers by the Franchisee.
- Providing the information regarding BSNL products / schemes / trade schemes/ VAS etc to retailers for further publicity.
- Feedback about replacement of damaged material by the franchisee.
- Feedback on supply of POS material such as Glow sign board etc.
- Assessment of potential area for appointment of new retailers.
- Combined visit with FOS and on spot issuing of C-TOPUP.

1.11 TELECOM INFRASTRUCTURE PROVIDERS (TIP)

1.11.1 **Scope Of TIP**

For providing FTTH, Broadband / voice services, Lease Circuits and value Added Services on Revenue Share Basis.

BSNL has provided unique opportunity to Builders, Resident Welfare Associations (RWAs), Telecom Infrastructure Providers, Hotel Owners, Hospitals, Trust, Franchisees, System Integrators, DIDs, Franchisees of BSNL, any registered company or society, Local Cable TV Operators, Telecom Service Providers, Local Shop Owners, BSNL Retailers, Direct Selling Agents, Unemployed Graduates, Local Youth having matriculation/degree or ITI, Start-ups or local entrepreneurs, , Spouses and Wards of BSNL/DOT employees or Retired BSNL/DOT employees etc. for registration as Telecom Infrastructure Providers BSNL (TIP) for providing BSNL Telecom Services in the existing and upcoming residential/commercial complexes and all other parts of rural and urban areas on revenue share basis.

1.11.2 **Advantages For Customers Through TIP**

For promotions of BSNL FTTH connections, BSNL has waived off the following charges for FTTH/BB Connections by TIPs

i. Installation charges
ii. Security deposit for landline/ voice connections.
iii. ONT Rentals
iv. One month additional free service on payment of advance annual bill.

1.11.3 **Additional Facilities Available To TIP**

1. One rent-free VPNOBB connection may be provided to TIPs for monitoring purpose who is having minimum Five OLTs or having less than Five OLTEs but has provided hundred FTTH connections.
2. One Free demo FTTH Connection in FTTH Plan of FMC Rs 675 may be provided for first month for demonstration in the targeted areas where new OLTs have been installed by TIPs which may be extended and same can be extended for one more month depending on expected demand in that area.
3. One Free Connection in FTTH Plan of FMC Rs 777 may be provided as an incentive to each TIP in his office who has provided 50 FTTH active connections.
4. Dedicated Nodal officers at each SSA level exclusively for coordination and support to TIP for FTTH related issues.
5. Dedicated Nodal officers are also available at Circle Office exclusively for TIP and FTTH related issues.
6. Dedicated Nodal officers at Circle Office have been deputed exclusively for settlement of revenue share of TIPs.
7. Total Technical guidance will be given by BSNL to TIPs through its highly experienced officers and staff.
8. Access to Franchisee Management System (FMS) Portal shall be provided to TIPs. All required update information can be obtained by TIP through FMS Portal.
9. Latest and updated information is also available on BSNL website

1.12 BSNL RED POLICY 2020

1.12.1 About BSNL RED Policy 2020

BSNL has recently launched VRS scheme 2019 for reducing aging employee, and approximately 75000 employees have opted for the scheme, and many of the VRS optees were working for Sales & Marketing units of the circles.

To address the shortage of direct selling agent / Sales persons and to make use of experienced BSNL VRS optees, BSNL introduced RED (RETIRED EMPLOYEE DISTRIBUTOR) Policy 2020 for utilization of best services of experienced people with attractive commission for each sale.

- BSNL Retailer CTOPUP Commission on Recharge, MNP, Bill Payment
- Know Your Nearest BSNL Retailer (KYR) Contact Details on SMS
- BSNL C Top Up Mobile Tariff with New Benefits for Retailer (POS)
- BSNL CTOPUP Registration for Retail Business (Prepaid/Postpaid)

In this new introduction, the RED (Retired Employee Distributor) shall market and sell the products like BSNL new prepaid SIM, CTop Up Recharge, Bill payment and other to customers at their door steps or through organizing Mela / Camp at various locations in the district or SSA / Business area, where the RED registered by earning huge commissions / discounts as defined subsequently under the BSNL RED policy.

1.12.2 BSNL RED Policy & Conditions, Requirements

- Refundable Security Deposit of Rs.500/- (Rupees five Hundred only) has to be paid in advance when allotted RED.
- The initial period of agreement shall be for 3 years and the selection of RED will be done by SSA Head
- Only retired employees of BSNL willing to serve customers/ prospects at their premises & through organizing Mela / Camp and shall be eligible to apply.
- Must have valid PAN Number
- Valid Goods and Services Tax (GST) registration Certificate Number for respective state (if applicable). If GST Certificates applicable, must submit along with application
- Self-declaration that the applicant is not black listed by the GST authorities.
- Self-declaration that the applicant is retired from BSNL.
- Security Deposit: Refundable Security Deposit of Rs.500/- (Rupees five Hundred only).
- Area of Operation: RED shall be allowed to operate within SSA where he/she is registered.
- BSNL RED will be given free C-TOPUP SIM with applicable concessional tariff and freebies.
- As per the BSNL Retired Employee Distributor Policy 2020, the RED can only do their sales within SSA where they are registered.
- RED can apply in any SSA, but can do business only within that registered SSA.

1.12.3 Targets For BSNL RED

There shall be a minimum monthly sales target of 50 no. SIM/FRC and C-top-up/recharge of Rs. 5000/- Sales targets assigned to RED shall be communicated by SSA on monthly basis. Targets will be reviewed every three months; if minimum monthly sales

targets are not achieved by the RED then they would not be continued further.

1.12.4 **Extension Of RED Agreement**

SSA Head may extend / migrate agreement on year-to-year basis for a period of two years with RED on same terms for the active RED. Decision of BSNL shall be final and binding in this regard.

1.12.5 **Termination For Inactive**

If not found active for six consecutive months, the RED may be terminated after issue of notice and seeking explanation. In case of any irregularity / violation of BSNL/ GoI rules, the RED registration may be terminated without any notice.

In case the RED 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 RED.

1.13 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 of sales channels like Franchisee, e-Distributor, DSA, Rural Distributor etc. to better serve its customers.

Note: Pl also check the latest circular of BSNL for any amendment /changes.

2 IP CONCEPTS

2.1 LEARNING OBJECTIVES

At the end of this chapter, participants will be able to understand:

- The concept of IP addressing fundamentals.
- The concept of IPv4 and IPv6 addressing scheme and its implementation.
- The concept of subnetting.
- Supernetting and VLSM.

2.2 INTRODUCTION

IP is a very important protocol in modern internetworking; you can't really comprehend modern networking without a good understanding of IP. Unfortunately, IP can be somewhat difficult to understand. This is probably because due to its importance, a large amount of complexity has become associated with the protocol over the years, to allow it to meet the many demands placed upon it.

Here basic concepts related to the Internet Protocol and how it works are mentioned. Since the task is more complex that is why the Internet architecture is of a layered design, which makes testing and future development of Internet protocols easy. To send data/information from one user to another user through a 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. 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 1

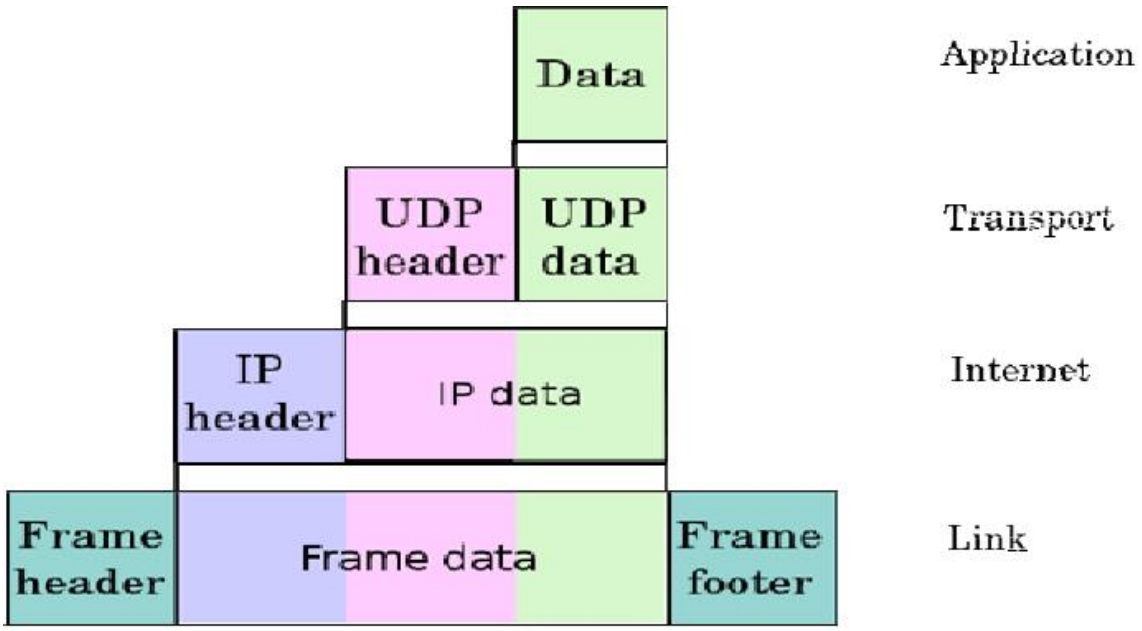


Figure 1: TCP layers and encapsulation method

2.3 FUNCTION OF LAYERS

2.3.1 The Application Layer:

The Application Layer refers to the higher-level protocols used by most applications for communication between/ among the hosts. Examples of application layer protocols are: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) etc. Data coded according to application layer protocols are then encapsulated into one or (occasionally) more transport layer protocols (such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)), which in turn use lower layer protocols to effect actual data transfer.

2.3.2 Transport Layer:

In computer networking, the Transport Layer is a group of methods and protocols within a layered architecture of network components which are responsible for encapsulating application data blocks into data units called datagrams or segments, suitable for transfer to the network infrastructure for transmission to the destination host.

2.3.3 Internet Protocol (IP)/ Internet Layer:

The Internet Layer is responsible for connecting 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. This layer also defines 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 important fields.

a) 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.

b) 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.

c) 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.

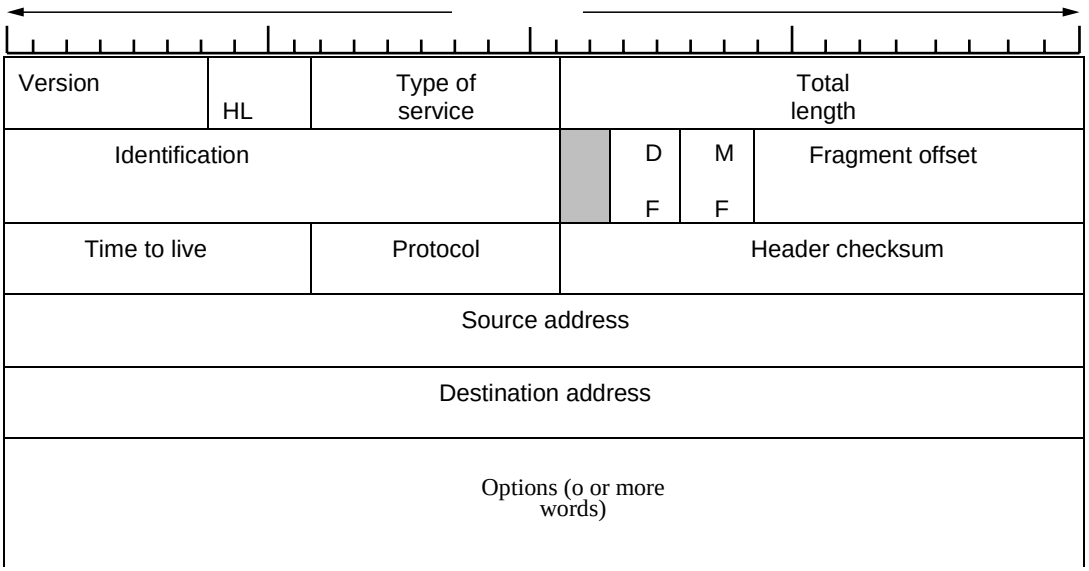


Figure 2: IP-datagram format

d) 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 a datagram decrements the TTL by one, the TTL can also represent a hop count.

e) 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.

f) 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) that changes a field in the IP header (e.g., time-to-live) must be recomputed the checksum before forwarding it.
Users of the IP must provide their own data integrity, since the IP checksum is only for the header.

g) Source Address – 32 Bit field

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

h) Destination Address – 32 Bit field

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

i) 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.

2.3.4 TCP/IP Transport Layer Protocols

The following section 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.

2.3.5 User Datagram Protocol (UDP)

The UDP provides application programs with a transaction oriented, single-shot datagram type service. The service is similar to the IP in that it is connectionless and unreliable. The UDP is simple, efficient and ideal for application programs such as TFTP and DNS.

The UDP operates at the transport layer and has a unique protocol number in the IP header (number 17). This enables the network layer IP software to pass the data portion of the IP datagram to the UDP software. The UDP uses the destination port number to direct the IP datagram (user datagram) to the appropriate process queue. The format of the UDP datagram is illustrated in Figure-3. Since there is no sequence number or flow control mechanism, the user of UDP must either not need reliability or self-service.

a) Source/Destination Port Numbers – 16 Bit field

The source and destination port numbers in conjunction with the IP addresses define the end points of the single-shot communication. The source port number may be equal to zero if not used. The destination port number is only meaningful within the context of a particular UDP datagram and IP address.

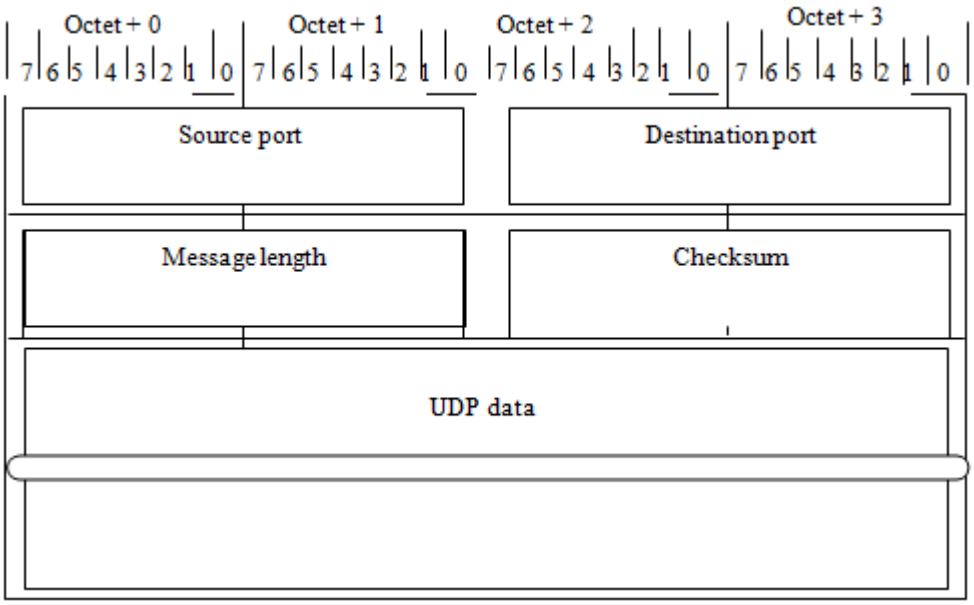


Figure 3: UDP datagram format

The source port number is a 16-bit field. The destination port number is also a 16-bit field.There are some fixed, pre-assigned port numbers used for services on the Internet – for example, number 7 is used for the UDP echo server and number 69 is used for trivial file transfer (TFTP). These fixed, pre-assigned port numbers are referred to as well-known ports and controlled by the IANA.

b) Length Field – 16 Bit field

The UDP message-length field is a 16-bit field that contains a count of the total number of octets in the user datagram, including the header. Hence, the minimum-size length field is 8.

c) Checksum – 16 Bit field

Usage of the UDP checksum is optional, however the field must be set to zero when not used. Since the IP layer does not include the data portion of the IP datagram in its checksum, UDP has its own checksum to provide data integrity. The UDP checksum is the 16-bit one's complement of the one's complement sum of the UDP header, UDP data, and some fields from the IP header.

2.3.6 Transmission Control Protocol (TCP)

TCP provides traditional circuit-oriented data communications service to programs. Unlike UDP, TCP is connection oriented. TCP provides a transport layer service in terms of the OSI reference model – it functions as layer 4.

a) 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-4. The following is a description of important fields in the TCP segment, and general characteristics of TCP associated with each field description.

b) Source/Destination Port Numbers

Each port number is an unsigned integer occupying 16 bits.

c) Sequence Numbers

The sequence number 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.

d) 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.

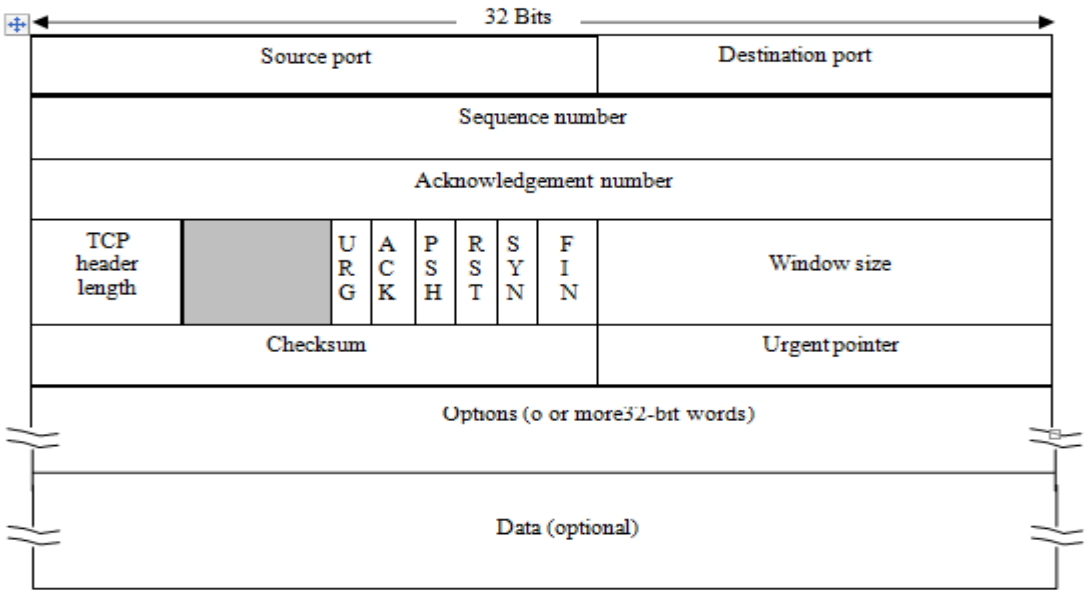


Figure 4: TCP format.

e) 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 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.

f) 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.
- 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.

g) 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.

h) 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.

2.3.7 Internet Control Message Protocol (ICMP)

The ICMP is used to report the error message back to the source. The ICMP message is encapsulated in an IP datagram. Error messages for different types of errors have different type field value. Below are some ICMP error messages with different type field.

Type	Field	ICMP Message Type
0		Echo reply
3		Destination unreachable
4		Source quench
5		Redirect (change route)
8		Echo request
11		Time exceeded for a datagram
12		Parameter problem on a datagram
13		Timestamp request
14		Timestamp response
17		Address mask request
18		Address mask response

Table 1. ICMP Type Codes

a) Flow Control

Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from outrunning a slow receiver.

b) Time-To-Live Exceeded

To prevent routing loops, the IP datagram contains a time-to-live that is set by the originator. As each gateway processes the datagram, it decrements by one. When zero is detected, the gateway sends an ICMP error message to the originator and discards the datagram.

2.3.8 Internet Group Management Protocol (IGMP)

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

2.4 IP ADDRESSING

2.4.1 IP Addressing – Introduction

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.

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.

Example 2:

10111100	00011010	00011110	00111100
156	26	30	60

We can use a dot as a separator. Now our IP address has the form 156.26.30.60

which is referred to as the dotted decimal notation.

2.4.2 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.

2.4.3 Address Classes

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

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

- Class D: Reserved for IP Multicasting.
- Class E: Reserved for future use. Addresses beginning with 1111 are reserved for future use.

2.4.4 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 your own system]
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

2.4.5 **Private Subnets**

There are three IP network addresses reserved for private networks. The addresses are:

- 10.0.0.0/8,
- 172.16.0.0/12,and
- 192.168.0.0/16

They can be used by anyone setting up internal IP networks, such as a lab or home.

Subnetting

Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media, preservation of address space, and security. The most common reason is to control network traffic.

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.

For example, 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/N Mask

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

Also, note that although subnet masks with non-contiguous mask bits are allowed, they are not recommended.

2.5 IP V6 ADDRESSING:

The rapid exhaustion of IPv4 addresses space and to fulfill the future need of IP addresses, the internet protocol is redesigned. This next generation of the Internet Protocol, aimed to replace IPv4 on the Internet, (IPv6) in 1995. The address size was increased from 32 to 128 bits or 16 octets. The new version (IP v6) is not designed to provide sufficient quantity of addresses alone, but it also allows efficient aggregation for routing.

The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. All modern desktop and enterprise server operating systems also support the IPv6 protocol, along with IPv4 but it is not yet widely deployed in other devices, such as home

networking routers, voice over Internet Protocol (VoIP) and multimedia equipment, and network peripherals.

Example of an IPv6 address: 2001:0df8:85a7:08d3:1319:8a2e:0370:7334

2.6 CONCLUSION

Internet Protocol (IP) has become a de-facto standard for developing and implementing data networks and internetworking. It is supported by all the manufacturers of all types of hardware and software from all developers. All the latest devices and applications presently in use like smart phones, smart and green building, smart city etc and various smart devices of future technologies like IOT, M2M will use IP. Hence, we need larger IP address space, which can be met by migration to IPv6.

3 ROUTER CONFIGURATION

3.1 LEARNING OBJECTIVES

This chapter covers the concept of router configuration fundamentals. After reading this chapter the participants will understand the concept of different types of router configuration and modes of routers.

The concept of static, dynamic and default routing will become clear after reading the chapter.

3.2 INTRODUCTION

In today's era of communication with the evolution of the 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.

3.3 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. Operators can 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 the processor.

3.4 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.

3.5 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.

3.6 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

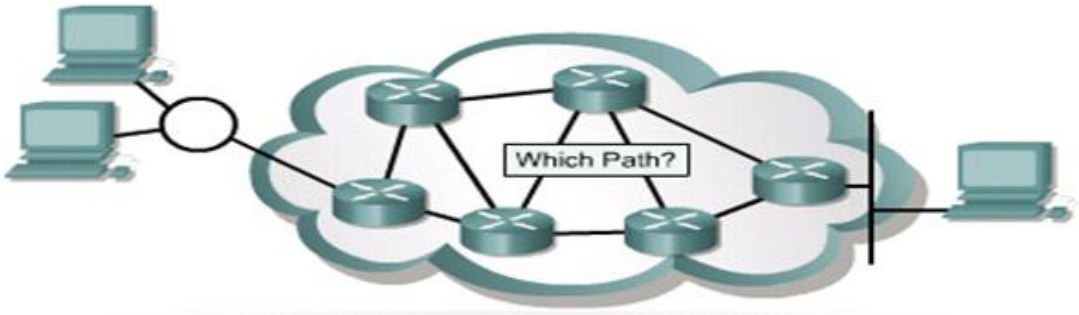


Figure 5: Layer 3 Functions to find the best path through the internetwork

3.7 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

3.8 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

3.9 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.

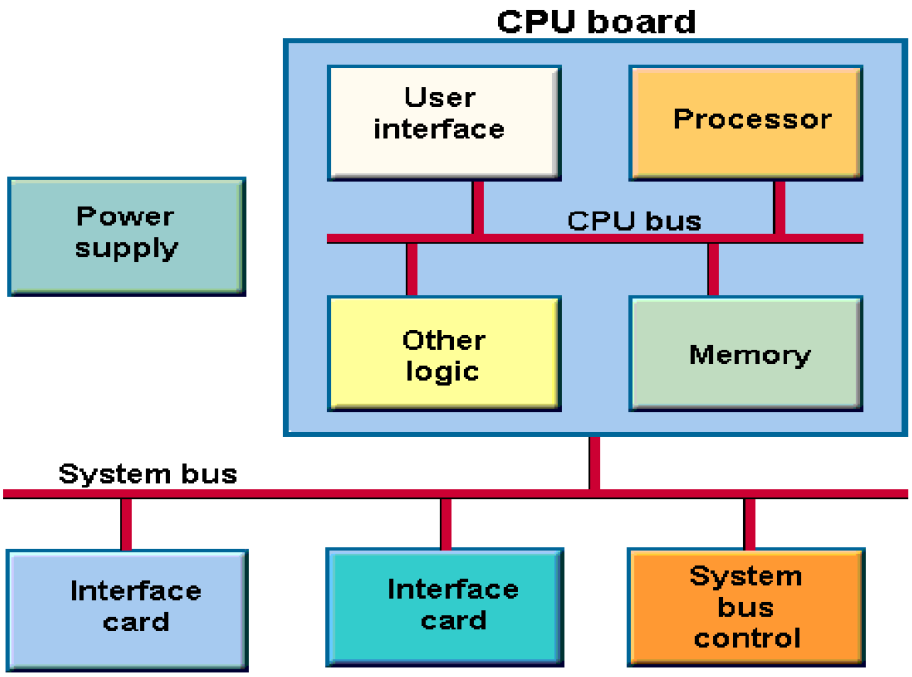


Figure 6: Router Components

3.10 INTERNAL COMPONENTS OF A ROUTER

3.10.1 **Boot ROM**

It stores the mini IOS (Internetwork 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

3.10.2 **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)

3.10.3 **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

3.10.4 NVRAM

It is a rewritable memory area that holds the router's configuration file. NVRAM retains the information whenever the 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

3.11 MEMORY ELEMENTS OF A ROUTER

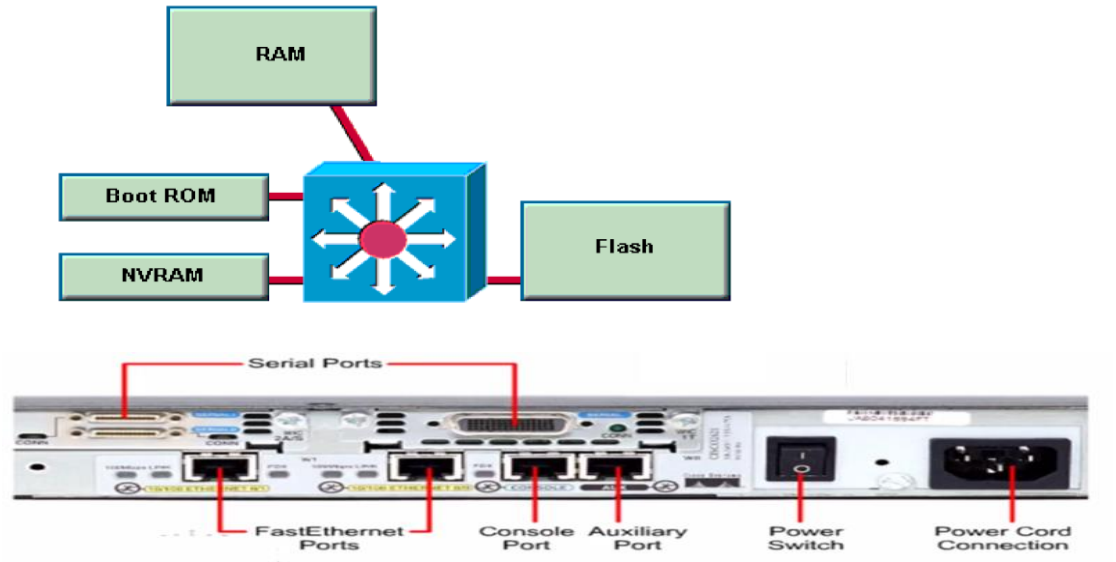


Figure 7: Memory Elements of Router

3.12 EXTERNAL COMPONENTS OF A ROUTER

3.12.1 Interfaces

- Connect routers to a network for packet entry and exit
- Can be on the motherboard or on a separate module

3.12.2 Type Of Interfaces

The three basic types of connections on a router are

- LAN interfaces,
- WAN interfaces,
- Management ports.

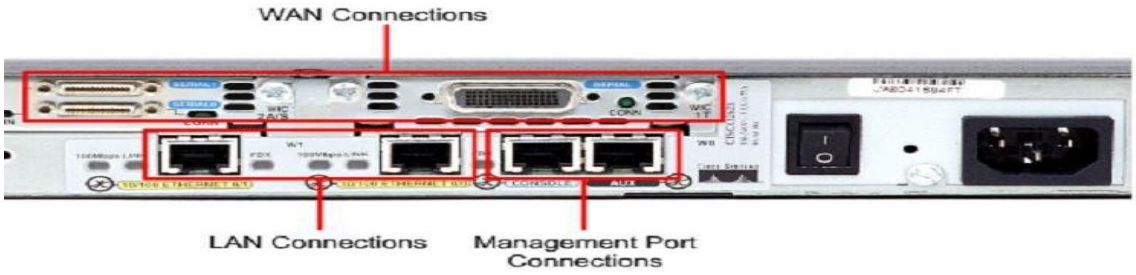


Figure 8: Interfaces

- 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.

3.13 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.

3.14 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.

3.15 IMPORTANT SHOW COMMANDS

#show access-lists	List access lists
#show arp	Arp table
#show cdp	CDP information
#show clock	Display the system clock
#show controllers	Interface controllers status
#show crypto	Encryption module

#show debugging	State of each debugging option
#show dhcp	Dynamic Host Configuration Protocol status
#show flash:	display information about flash: file system
#show frame-relay	Frame-Relay information
#show history	Display the session command history
#show hosts	IP domain-name, lookup style, name servers, and host table
#show interfaces	Interface status and configuration
#show ip	IP information
#show ospf	For OSPF debug only
#show ospfv3	For OSPFv3 debug only
#show processes	Active process statistics
#show protocols	Active network routing protocols
#show running-config	Current operating configuration
#show sessions	Information about Telnet connections
#show ssh	Status of SSH server connections
#show startup-config	Contents of startup configuration
#show tcp	Status of TCP connections
#show terminal	Display terminal configuration parameters
#show users	Display information about terminal lines
#show version	System hardware and software status

3.16 ROUTER BASIC CONFIGURATION

3.16.1 **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.

3.16.2 **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.

3.16.3 **Auxiliary Port Connection**

The Router Can Also Be Configured From A **Remote Location** By Dialing To A Modem Connected To The Auxiliary Port On The Router.

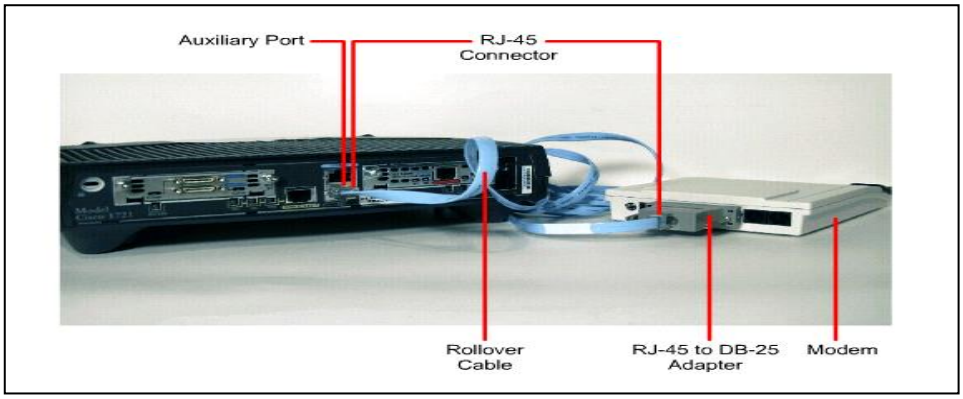


Figure 9: AuxiliaryPort

3.17 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)

3.18 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

3.19 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 software.

Find and apply the startup configuration file or enter the setup mode.
After the POST, the following occur as the router initializes:

- The generic bootstrap loader in ROM executes
  - The bootstrap loads instructions that cause other instructions to be loaded
- The operating system is loaded
  - The location is available in the boot field of the configuration register
- The operating system locates the hardware and software components and lists the results on the console terminal
- The configuration file saved in NVRAM is loaded into main memory and executed one line at a time
  - The commands start routing processes, supply addresses for interfaces, and define other operating characteristics of the router
- If no configuration file is found, the operating system enters setup mode

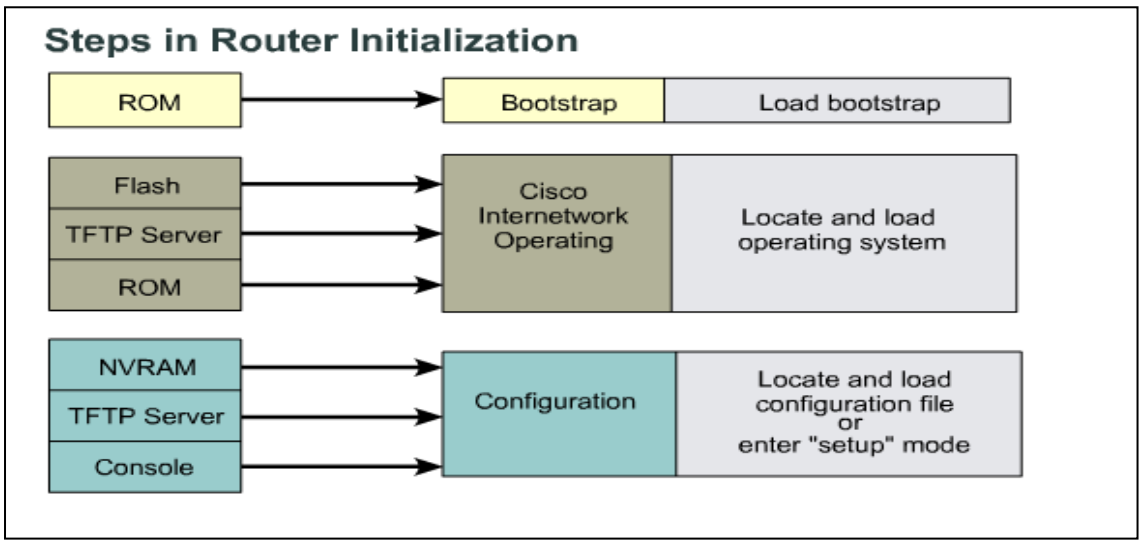


Figure 10: Router Configuration Steps

3.20 ROUTER USER INTERFACE MODES

The IOS provides a command interpreter service known as the command executive (EXEC). The EXEC validates and executes the command

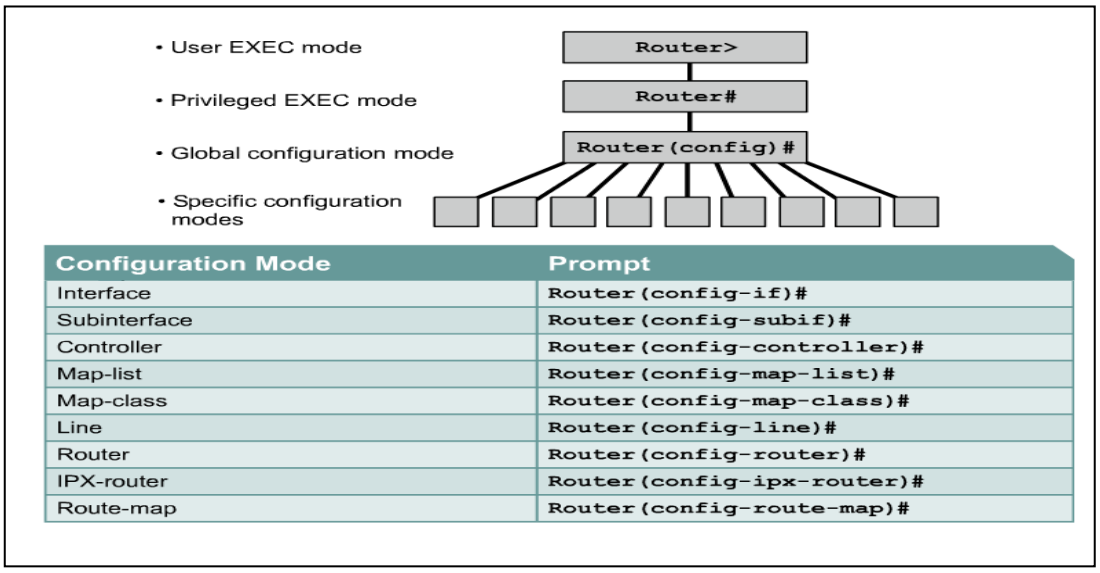
The EXEC session is separated in two 2 levels of access

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 11: Router interface modes

3.21 ROUTER CONFIGURATION

3.21.1 Configuring A Router Name

Router#config t
Router(config)#hostname BSNL
BSNL(config)#

3.21.2 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-confg]? RC
Writing running-config...!!
[OK - 497 bytes]

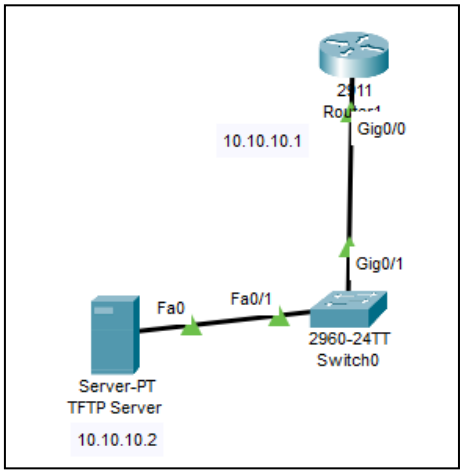


Figure 12: Example

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

3.22 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.

3.23 ROUTER CONFIGURATION WITH EXAMPLE

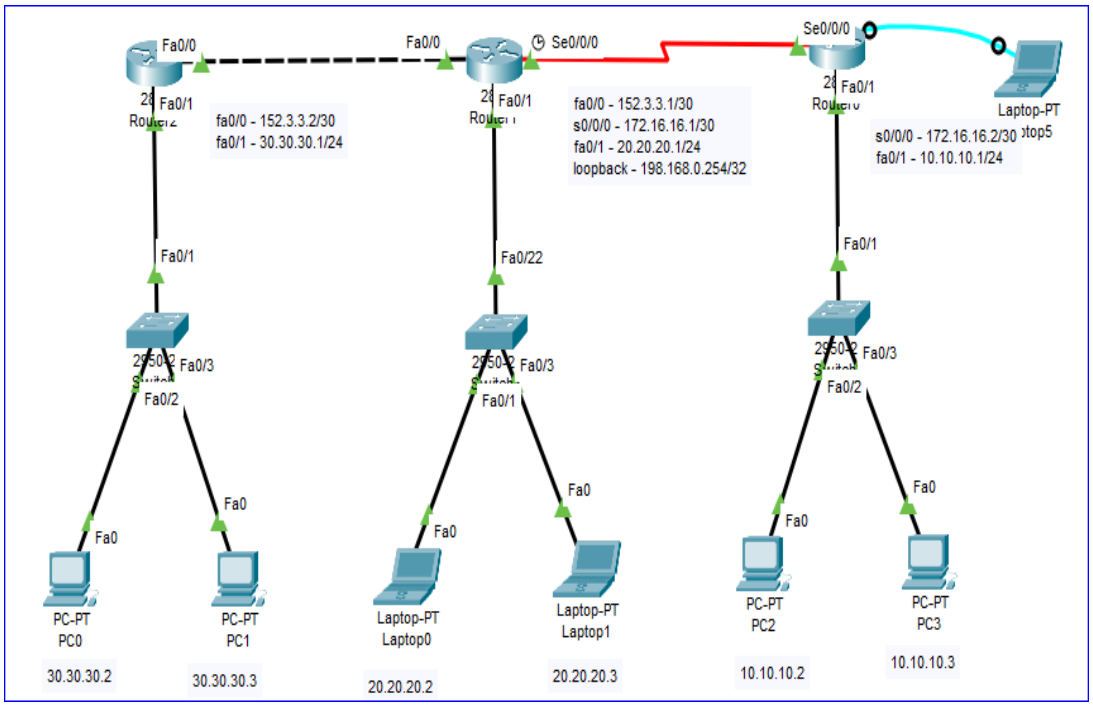


Figure 13: Router Configuration Example

3.24 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
```

3.25 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
```

3.26 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
```

3.27 STATIC ROUTING

3.27.1 **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

3.27.2 **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

3.27.3 **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

3.28 DEFAULT ROUTING

3.28.1 **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

3.28.2 **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

3.28.3 **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

3.29 DYNAMIC ROUTING

3.29.1 **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

3.29.2 **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
```

3.29.3 **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
```

3.30 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.

The router is the key network element works at layer no 3, all the IP packetmovement is done through this device, so, better understanding of routing fundamental and router configuration will make easy the handling of the network.

4 BROADBAND, MULTIPLAY AND MNG-PAN

4.1 LEARNING OBJECTIVES

This chapter covers the concept of NIB project and its architecture, broadband multiplay used in BSNL. After reading this chapter the participants will understand the concept of mutiplay broadband , its architecture, components and MNG-PAN.

4.2 NIB II PROJECT DETAIL

The turnkey implementation of "National Internet Backbone- Phase II" involved the following projects:

Table 2. NIB II Project Detail

Name of project	Description
Project 1	MPLS based IP Infrastructure
Project 2.1	Narrowband Access (Dialup Remote Access)
Project 2.2	Broadband Access (DSL Access)
Project 3	Messaging, Storage, Provisioning, Billing, Security, Order Management, Enterprise Management, AAA, Help Desk and Inventory Management.

NIB-II envisages four projects:-

- MPLS based IP Infrastructure in 100 cities (29 city STM-16 core).
- Access Gateway platform Narrow band (Augmentation of existing Dial up Internet capacity.
- Access Gateway Platform Broadband in 235 cities (Based on ADSL Technology)
- Services Platform consisting of messaging, Provisioning, billing, customer care, enterprise management system and Data centres.
- 71 location Managed IP & MPLS Network using MPLS enabled Routers
- Centralized NOC and DR site for NMS & PMS
- NOC site at Bangalore, DR site at Pune
- Integration with Narrowband and Broadband RAS Projects
- Test bed Setup - Proof of Concept Centre

4.3 OBJECTIVE OF NIB-II

- NIB-II is a mission to build world-class infrastructure that will help accelerate the Internet revolution in India.
- It provides a diversified range of Internet access services including support for VPN (Layer-2, Layer-3 and Dialup and Broadband services).

- It also offers SLA Reports including security, Qos and any to any connectivity.
- Offers fully managed services to customers.
- It offers services like bandwidth on demand etc. over the same network.
- The network is capable of on-line measurement and monitoring of network parameters such as latency, packet loss, jitter and availability so as to support SLAs with customers.
- The routers support value added services such as VPNs, Web and content hosting, Voice over IP, Multicast etc.
- Value Added Services like
    - Encryption Services
    - Firewall Services
    - Multicast Services
    - Network Address Translation (NAT) Service that will enable private users to access public networks
- Messaging Services
- Internet Data Centre Services at Bangalore, Delhi and Mumbai.
- Broad Band Services like
    - Broadcast TV using IP Multicasting service
    - Multicast video streaming services
    - Interactive Distant learning using IP multicasting Services
    - Video on demand
    - Interactive gaming service

4.4 NIB-II NETWORK ARCHITECTURE

- A1 – 5 Core cities:-
    - Bangalore, Chennai, Mumbai, Delhi (Noida), Kolkatta.
- A2/A3 – 9 next level core cities:-
    - Pune, Hyderabad, Ahmedabad, Ernakulam, Lucknow, Jaipur, Indore, Jullundur, Patna.
- A4 – 10 Major cities.

- B1, B2 – 47 other cities.
- A1 city core routers (Cisco 12416) are fully meshed between locations on STM-16.
- A2 core routers (Cisco 12410) dual home to Core A1 routers on STM-16.
- A3 core routers (Cisco 12410) are dual home to the nearest A1 or A2 routers on STM-16.
- A4 core routers (Juniper M40) are dual home to the nearest A1 or A2 or A3 routers on STM1 links.
- IGW – International Gateway Router – Connectivity to Internet is through this router.
- IXP – Internet Exchange Point – ISP's connect each other through this router.
- IDC – Internet Data Center – for connecting to BSNL Data Centers.
- IP-TAX – BSNL IP-TAX traffic enters to NIB2 through this router.
- RR – Router Reflector – For reflecting of BGP routes to the edge routers.
- B1 and B2 cities have only EDGE routers, which are dual homed to nearest A1/A2/A3/A4 core routers.
- All Core locations also have edge routers.
- 10 A4 locations have Juniper core routers with Cisco 7613 Edge routers.
- Some core locations have Cisco core router and Juniper edger router.

NIB2 Expansion and Year 2 Order Overview

- 29 locations added which makes the total to 100
- Core backbone is getting aligned to BSNL Transmission (DWDM) network
- 24 City core network increased to 29
- All 29 city core network links are STM-16 (ie STM1 connectivity of A4 cities will be upgraded to STM16)
- New 5 Cities are Belgaum, Dehradun, Rajkot, Jodhpur, Jabalpur

Metro Ethernet Project

- Providing Metro Ethernet Broadband connectivity at A1 and A2 locations of NIB2

- Total 12 routers ordered for Metro Ethernet Project
- 2 routers each at 6 locations for Metro Ethernet project
- Bangalore (A1) – 1*12416 and 1*12410
- Chennai (A1) – 1*12416 and 1*12410
- Kolkata (A1) – 1*12416 and 1*12410
- Ahmedabad (A2) – 2*12410
- Hyderabad (A2) – 2*12410
- Pune (A2) – 2*12410

4.5 COMPONENTS OF BROAD BAND ACCESS NETWORK

- Broad band Remote Access Server (BBRAS)
- Gigabit and Fast Ethernet Aggregation Switches (LAN Switches).
- Digital Subscriber Line Access Multiplexers (DSLAMs)
- SSSS/SSSC (Subscriber Service Selection System/ Centre)
- Servers for AAA, LDAP at NOC.
- Provisioning and configuration management at NOC.
- DSLCPEs
- The DSLAMs will in general be collocated with existing PSTN exchanges, which provide last mile access to customers over copper wire up to average span lengths of 3 KMs.
- All DSLAMs are aggregated through a FE interface except 480 port DSLAM, which are aggregated through Gigabit Ethernet Interface.
- The 240 ports DSLAM has two numbers of FE interface.
- The FX or GBIC module in DSLAM and LAN switch should be capable of driving up to 10KM on a single mode fibre.
- The SX or GBIC module in LAN Switch used for connecting Tier2 to Tier1 supports 40km.In bigger cities like A1, A2, A3 and A4, one BBRAS per city has been deployed initially.
- There are no BBRAS at B1 and B2 cities.

- The DSLAMs in B1.B2 and other lower hierarchical cities have been aggregated through Layer 2 switches, and are connected to the nearest BBRAS of A cities on Ethernet over SDH.
- The BRAS terminates the PPP sessions initiated by the customer and extends the connection further to MPLS VPN/ Internet as desired by the customer.

4.6 NIB II PROJECTS

Project 1 – IP / MPLS Core Backbone

- 100 location Managed IP & MPLS Network
- Awarded to HCL Infosystems Ltd.
- Network using Cisco (12410, 12416, 7613) and Juniper (M40e, M20) Router
- Common Backbone for all other projects of BSNL and integration with other projects of NIB-2 and other Data Projects of BSNL
- International Gateways connected for Internet access
- Provides MPLS-VPN Services and Internet Services, in certain cases

Project 2.1 – Narrowband Access Network

- Consists of Narrowband RAS (NRAS)
- Awarded to UTStarcom
- Network built using UTStarcom Total Control 1000
- Provides access to Dial-up Customers for Internet Access & Dial-VPN

Project 2.2 – Broadband Access Network

- Network for Providing Broadband Access
- Awarded to Huawei and UTStarcom (70 : 30 Split)
- Network built on Huawei Broadband RAS (BRAS), Huawei Tier-1 Switch, Huawei / 3Com Tier-2 Switch and Huawei / UTStarcom DSLAMs
- Provides Broadband Internet Access (DataOne) and VPN Services
- Broadband RAS (BRAS) working as PE Router for MPLS Core Network
- BRAS present at all ‘A’ Type Locations – 23 in No.
- Tier-1 Switch co-located with and connected to BRAS
- Layer 2 Network below is aggregated by Tier-1 Switch
- Tier-2 Switches connecting to Tier-1 Switches in Star Fashion

- DSLAMs connect to Tier-2 Switch

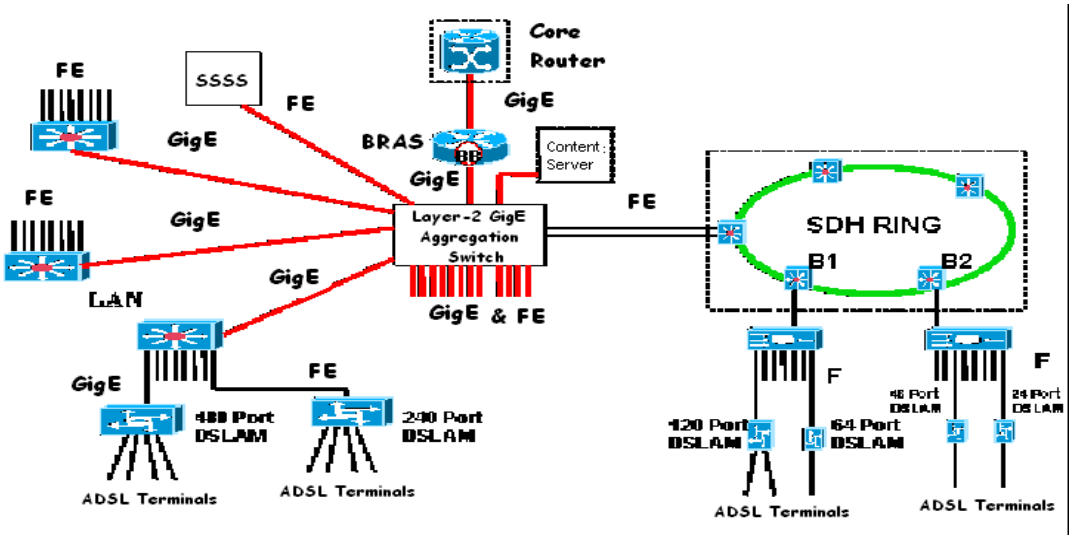


Figure 14: Broadband Project 2.2 Layout

Project 3 – Server / Application Infrastructure

- Consists of Data Centers in 4 locations – Bangalore, Pune, Mumbai & Noida
- Awarded to TCIL consortium with TCS and IBM
- IBM Servers, Nortel Network & Security equipment
- Provides Mail, DNS, Co-Hosting, Co-location, Billing etc.

4.7 BROADBAND MULTIPLAY NETWORK ARCHITECTURE

- A1 – 5 Core cities
- Bangalore, Chennai, Mumbai, Delhi (Noida), Kolkatta
- A2 – 3 Tier-2 cities
- Pune, Hyderabad, Ahmedabad,
- A3 – 6 next level core cities
- Ernakulam, Lucknow, Jaipur, Indore, Jullundur, Patna
- A4 – 10 Major cities; Chandiagrh, Ranchi, Mangalore, Nagpur, Bhubaneshwar, Guwahati, Vijaywada, Allahabad, Raipur, Coimbatore
- B1,B2 – 76 other cities

4.8 BROADBAND MULTIPLAY PROJECT COMPONENTS

- L3PE (MCR / PE Router of NIB-2 Project 1 – Supplied by HCL)

- BNG – Broadband Network Gateway
- Connects Multiplay Network to NIB2 Backbone (Project 1)
- RPR Tier-1 Switch
- Provides connectivity from BNG to Connects
- RPR Tier-2 Switch
- OC LAN Tier-2 Switch
- DSLAM
- DSL Tester
- Installation Related Material

Metro Core Routers

- Providing Access to the Broadband Multiplay NW at A1, A2 locations of NIB2
- Total 12 routers implemented as Metro Ethernet Project
- 2 routers each at 6 locations
- Bangalore (A1) – 1*12416 and 1*12410
- Chennai (A1) – 1*12416 and 1*12410
- Kolkata (A1) – 1*12416 and 1*12410
- Pune (A2) – 2*12410
- Hyderabad (A2) – 2*12410
- Ahmedabad (A2) – 2*12410

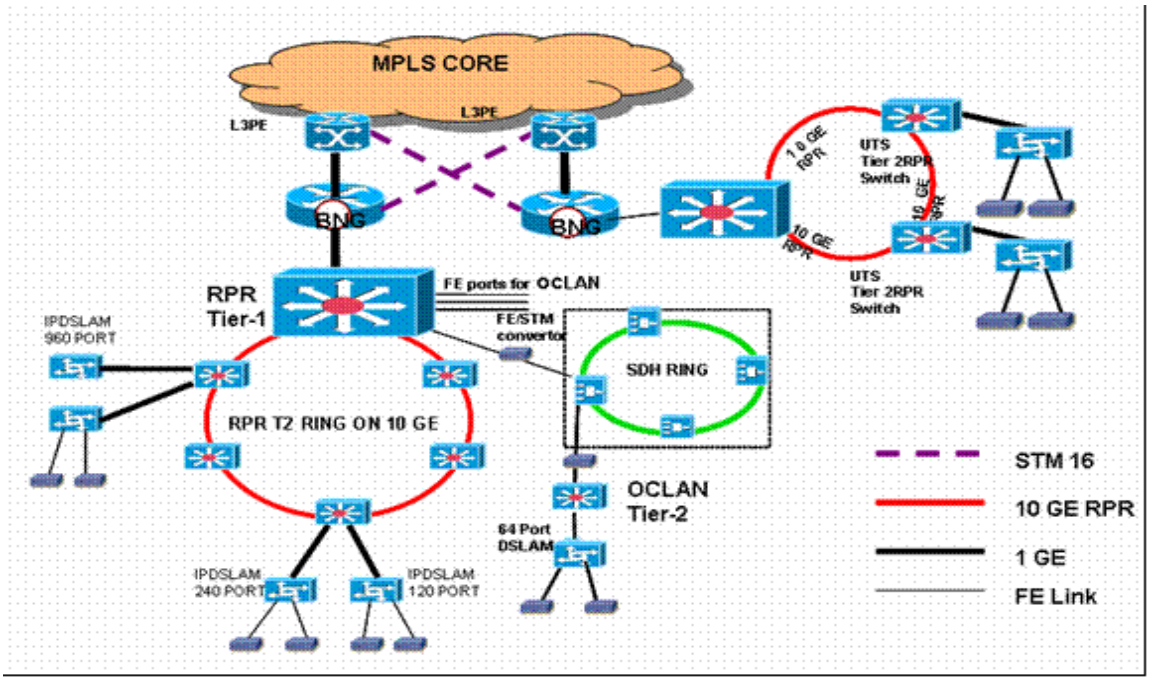


Figure 15: Broadband Multiplay Layout

4.9 SERVICES ON BB-MULTIPLAY

a. TVOIP

- **TVOIP** (also called as IPTV) delivers television programming to households via broadband connection using Internet protocols.
- Internet Protocol Television (IPTV) is expected to change the way people watch TV. As the name suggests, IPTV is television programs delivered to subscribers through the Internet
- It requires a subscription and IPTV set-top box **(STB)**.
- 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.
- **IPTV (Internet Protocol Television**) is a system where a digital television service is delivered by using Internet Protocol over a network.
- If you've ever watched a video clip on your computer, you've used an IPTV system in its broadest sense.
- For residential users, IPTV is provided with Video On Demand and may be bundled with Internet services such as Web access and VoIP.

- Microsoft is one of the many companies developing solutions to support the Internet Protocol TV (IPTV) market.
- IPTV is an emerging technology and will evolve into a completely interactive experience in the future!
- First things first: the Set-Top Box (STB), on its way out in the cable world, made a resurgence in IPTV systems.
- The box connects to the home DSL line and is responsible for reassembling the packets into a video stream and then decoding the contents.
- 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.)

b. 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 Internet as 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 over the Internet (VOI)

Benefits of VoIP

- Cost reduction
  - Toll by-pass
  - WAN Cost Reduction
- Operational Improvement
  - Common network infrastructure
- Simplification of Routing Administration Business Tool Integration
  - Voice mail, email and fax mail integration
  - Web + Call
  - Mobility using IP

VoIP Protocols

- **H.323:**
  - ITU-T standard, latest version v4

- Peer-to-peer protocol that supports terminals communicating over packet based networks

- **SIP:**
  - IETF standard, RFC 3261
  - Peer-to-peer protocol for initiation, modification termination of communication sessions between users
- **MGCP:**
  - ITU-T and IETF collaboration, RFC 3435
  - Master/slave protocol for media gateway controller to control media gateway.

4.10 MNG-PAN (MPLS BASED NEXT GENERATION PACKET AGGREGATION NETWORK)

The radical shift from traditional TDM based voice traffic to packet based data traffic, and growing demand for bandwidth from new services like 3G/4G, PTP, IPTV etc. presents a serious challenge to network operators in terms of capacity, supported services and related costs. Efficient, scalable and reliable aggregation network is a mandatory element of network infrastructure to address such business growth challenges in the era of explosive data traffic growth.

4.10.1 What Is MMG-PAN Network?

MNG-PAN: It is MPLS Based Next Generation Packet Aggregation Network which incorporates the MPLS-TP (MPLS-Transport Profile) technology for Transport network of telecom services. MNG PAN is an advanced Packet Aggregation Network solution designed for efficient multi-service aggregate of voice, video and data traffic from various access technologies including MSAN, DSLAM, FTTx, Broadband Wireless Access, as well as 3/4G mobile network base stations. The products offer high-performance aggregation and a broad feature set, including network-wide time/clock synchronization, carrier class sub 50ms recovery resiliency, guaranteed QoS and SLA enforcement, end-to-end multi-layer OAM.

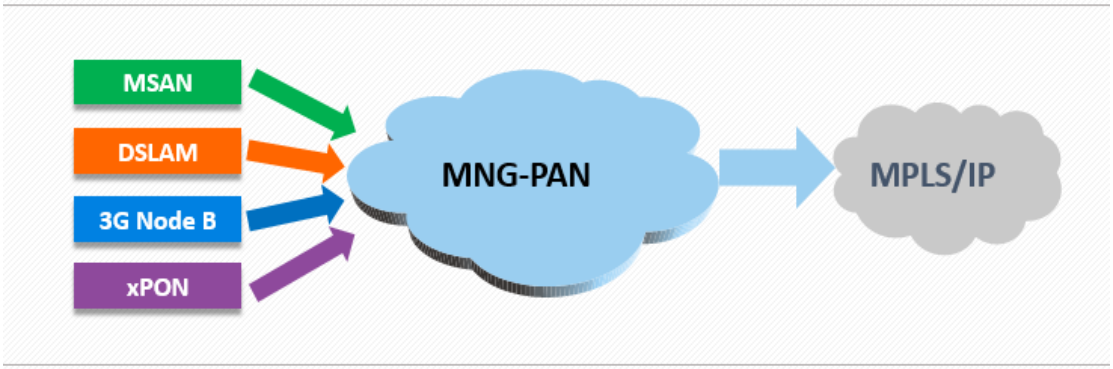


Figure 16: MNG-PAN

It is used for the aggregation of the traffic from various network elements being deployed in the BSNL Network

4.10.2 **What Is MPLS-TP**

MPLS-TP is designed for use as a network layer technology in transport networks. It will be a continuation of the work started by the transport network experts of the ITU-T, specifically SG15, as T-MPLS. Since 2008 the work is progressed in a co-operation between ITU-T and IETF. The required protocol extensions to MPLS being designed by the IETF based on requirements provided by service providers. It will be a connection-oriented packet-switched (CO-PS) application. It will offer a dedicated MPLS implementation by removing features that are not relevant to CO-PS applications and adding mechanisms that provide support for critical transport functionality.

4.10.3 **Difference Between MPLS-IP Technology And MPLS-TP**

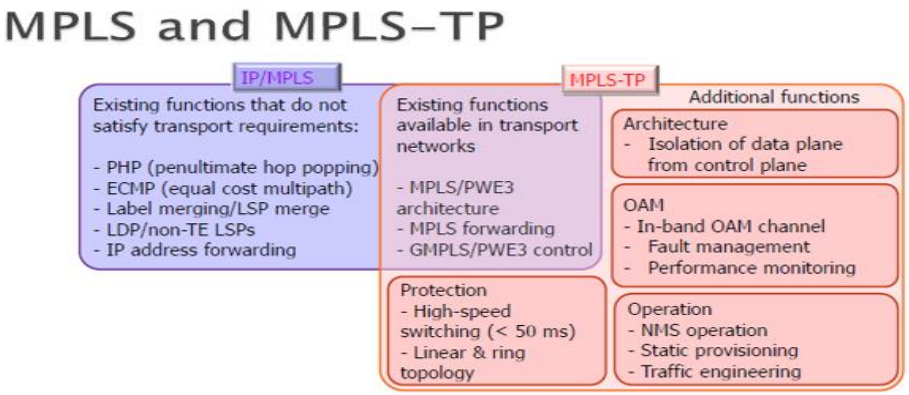


Figure 17: Difference between MPLS/IP Technology and MPLS-TP

MPLS-TP is to be based on the same architectural principles of layered networking that are used in longstanding transport network technologies like SDH, SONET and OTN. Service providers have already developed management processes and work procedures based on these principles.

MPLS-TP gives service providers a reliable packet-based technology that is based upon circuit-based transport networking, and thus is expected to align with current organizational processes and large-scale work procedures similar to other packet transport technologies.

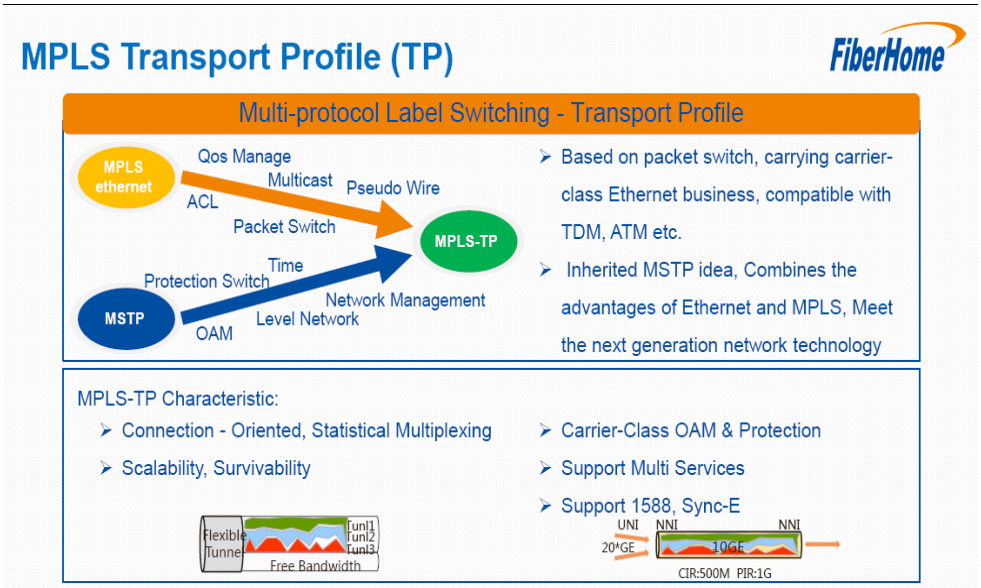


Figure 18: MPLS & MPLS-TP

4.10.4 Features Of MNG-PAN Network

1. The solution is based on Pseudo Wire over MPLS-TP technology that supports an efficient Ethernet aggregation.
2. The PAN platform offers wide range of protocols, standards and interfaces coupled with highest reliability
3. Carrier-class set of features, including the carrier class sub 50ms recovery resiliency,
4. Hard QoS/SLA guarantees,
5. End to end and multi-layer OAM, network-wide time/clock synchronization,
6. Efficient multicast data distribution.
7. Range of interfaces up to 10GE
8. Low power consumption
9. Centralized management

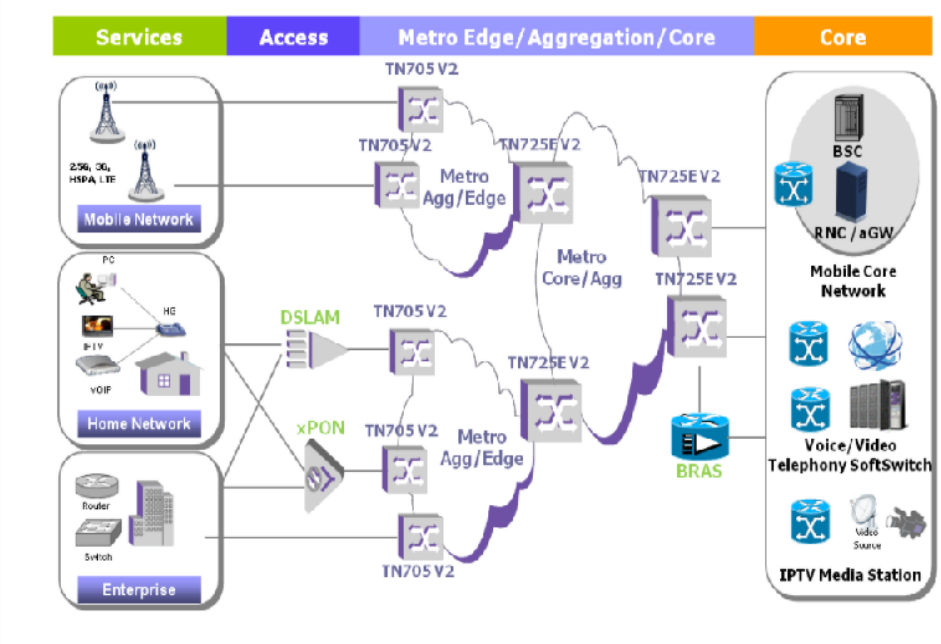


Figure 19: MNG-PAN Deployment in various network

4.10.5 Advantages Of MNG-PAN Transport Network

1. **Scalability**: Support of electrical and optical Ethernet interfaces from FE to 10GE. Large switching capacity.

2. **Reliability**: Carrier class reliability with fully redundant hardware architecture.

3. **Resilience**: Various protection schemes, sub-50ms failure recovery.

4. **Manageability**: Enhanced OAM capability with end-to-end service management. NMS-based operation.

5. **Inter-operability**: Compliant with ITU-T MPLS-TP standard. Easy integration with core IP/MPLS or OTN networks.

6. **Bandwidth Efficiency**: Packet nature of the network with flexible data-pipes enables users to request the service in smaller increments and provides better utilization at the aggregation level.

7. **Lower TCO**: Low power consumption; bandwidth efficiency due to optimized packet aggregation; fast fault isolation and simple management; smaller form factor.

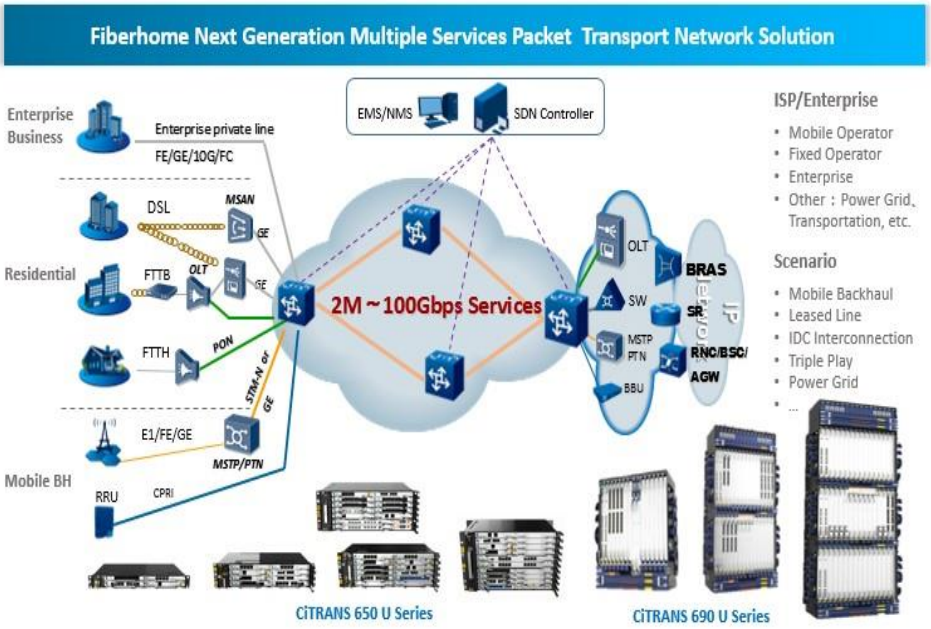


Figure 20: Fiber-home MNG PAN Network for BSNL Core network

4.11 CONCLUSION

With the help of NIB-II project, a pan-India, world-class IP based network is developed, which is supporting all types of services and has become a backbone for carrying all types of traffic e.g. Internet based services, NGN, CDR, ERP etc. It also supports VPN services such as L2 VPN, L3 VPN along with the support for online measurement of network parameters for supporting SLAs.

5 BROADBAND & MULTIPLAY LAB

5.1 LEARNING OBJECTIVES

- COMMANDS FOR ZTE DSLAM.
- COMMANDS FOR UTSTARCOM DSLAM.
- COMMANDS FOR NSN DSLAM.

5.2 ZTE DSLAM

- **To see the Subnet , IP Address & IP route of DSLAM**

show ip subnet

show ip route

- **To see the card statusof DSLAM**

show card

- **To Reset the Non-working card (which has ' Offline ' or ' Unknown ' status)**

Enter into Enable Mode by Command DSLAM >**Enable**

Enter the Password **: admin**

Give Command DSLAM # **reset card 3** (Where 3 is faulty card no.)

Wait for 4-5 minutes & then check the status of card again using **show card** command.

- **To Reset the particular port**

To Enter into configure mode give command **configure** (in Enable /# mode)

(config) # **interface adsl 2/9** (Where 2/9 is Slot no./ Port no.)

(cf dslam(cfg-if-adsl-2/9) # **shutdown**

(cf dslam(cfg-if-adsl-2/9) # **no shutdown**

Now check the admin status of port & confirm

- **To see the status of port of particular card (to see Admin status & Link status of all ports)**

show interface 2/1-64 port-status

(Here 2 is card no. & 1-64 is port list, if the card is of 64 port card)

- **To Check the status of Fan & Temperature in 120 port & higher ZTE DSLAM**

show fan

- **ToCheck status of Fan & Temperature in 64 Port ZTE DSLAM**

show temperature-check

If status of any fan is failed then first clean tha fan filter & check

If problem is not solved then replace the fan unit.

- **To Check SNR Margin, Attenuation & out power of all ports in particular slot**

(Note : Not applicable for 64 port DSLAM)

show interface 2/1-64 adsl-status

Here Divide the SNR Margin & Attenuation value by 10 e.g. Attenuation 208 becomes 20.8 dBm

- **To Check SNR & Attenuation level of up ports in 64 port DSLAM**

show adsl physical 2/10 (here 2/10 = slot no./Port no. & Port is UP)

Link status of the port must be UP, whose SNR & Attenuation is being checked

- **To find slot no./ Port no. in DSLAM from VLAN id**

show vlan 229 (here 229 is inner VLAN id)

- **To Check Uplink port Status & VLAN passed from uplink port of DSLAM**

show interface 9/1-6 port-status

show interface 9/1-6 vlan-config

- **To Check Uplink port Status & VLAN passed from uplink port of 64 Port DSLAM**

show interface 5/1-2 port-status

show interface 5/1-6 vlan-config

- **To Check MAC Address of all up ports in particular slot**

show mac-address-table slot 4(4 is slot no. - Not for 64 Port DSLAM)

- **ToCheck MAC address list of all up portsin 64 Port ZTE DSLAM**

show mac-address-table

5.3 UTSTARCOM DSLAM

- **To Check The All Card Status**

'**show slot'**

IPADSL8A is Line Cards &ICM3Gc is Controller card.

(A) is Active and (S) is Standby

- **To Check the Module Status & Temperature of Particular Slot**

Enter into particular Slot DSLAM # **slot 1** (here 1 is slot no.)

show module

show temperature

- **To Reset the Non-working Card (with Unknown Module status)**

 # reset 2 hard(here 2 is faulty slot no.)

Always use Hard Reset to RESET the Cards. AFTER Resetting the Card, To check the card Status **give** command **Show Slot** as above

- **To Check Status of all ports in particular card**

Go into Proper **SLOT** and into **Port** Mode

Each Card Contains the 48 DSL Port (1 to 48): According to this, calculate the right port.

 # slot 4 (here 4 is slot no.)

 # port (to enter in port mode)

 # show line dsl 1-48 (1-48 is port range for 48 port card)

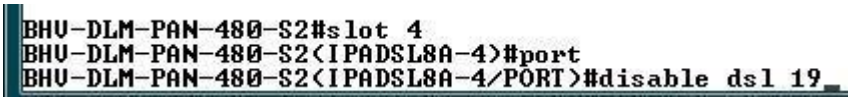
- **To Reset the particular Faulty Port (Use Disable or Enable the PORT)**

Enter into concern slot & then enter into port mode.

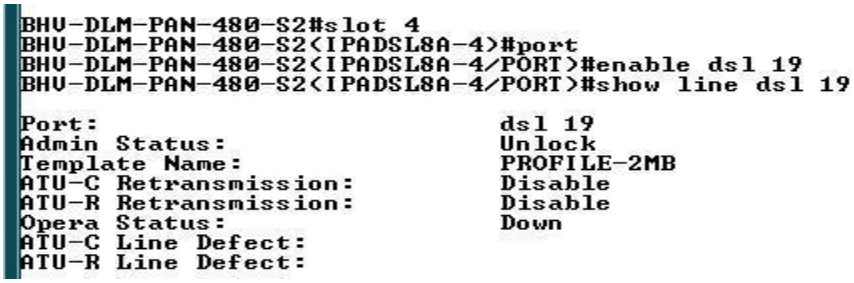
Give the Command:

IPADSL8A-4/PORT# **disable dsl 19**

IPADSL8A-4/PORT# **enable dsl 19**



When the port is disabled then the Port Admin Status becomes 'LOCK'



- **To Reset Series of Port**

Enter into concern slot & then in port mode & suppose port no. 1 to 8 are faulty

 # disable dsl 1-8 (here 1-8 shows series of dsl port 1 to 8)

 # enable dsl 1-8

 # show line dsl 1-8 (to check the admin status of ports)

- **To Check the Current MAC address on Up ports of particular slot**

 # slot icm (or enter slot1/2/3 to check mac in particular slot)

 # bridge

 # show fdb

- **To Check the IP route**

 # ip show route

```
AHD-VSN-UT-D9-M1#ip show route
Destination     Netmask         Gateway         Metric Interface
0.0.0.0         0.0.0.0         10.226.176.1    0      vlan124

AHD-VSN-UT-D9-M1#show system
System Information
System Description      :  IP-DSLAM
System Name             :  AHD-VSN-UT-D9
System Contact          :  +1(732)767-5200
System Location         :  33 Wood Ave. S, Iselin, NJ 08830
System UP Time          :  253 days 03:27:23
```

- **To Check the DSLAM System Up time**

 # show system

- **To Check the VLAN Configuration of ports in Particular Slot**

 # slot 3 (Enter into particular slot)

 # vlan

 # show(or enter show 226 to find particular port from vlan)

5.4 NOKIA SIEMENS DSLAM

- **To see the status of card**

show slot-overview

It shows the status of all equipped cards in module. Each card contains 72 ports. Here Control cards are equipped in slot no.5 and 6.

- **To Check the Status of Fan**

show status fan

- **To Check the configuration of each card separately**

show table shelf

- **To Check the Card temperature of all Equipped Cards**

show status temperature

- **To Check the Port Admin & Operation Status & xTUC & xTUR Line Rates**

show lre s1 xdsl phys-table linerates

(Here s1 indicates the slot no. 1, enter s3 for slot 3)

- **To find the Slot & Port no. from particular inner VLAN & to Check the MAC**

show mac vlan 137(here 137 is inner VLAN no.)

- **To Check the Attenuation & SNR Margin for particular UP port**

show lre 1/10 xdsl band-table(1/10 is slot no. / port no.)

- **To Reset the particular faulty card**

Enter into Enable Mode by using command > **enable**
Enter into Configuration Mode by using command **# configure terminal**
In configuration mode give command :
DSLAM(config)# reset card 2 (here 2 indicates the slot no.)
OR DSLAM(config # reset all (to reset all equipped cards)

- **To Reset the particular Port**

Enter into Enable Mode by using command > **enable**
Enter into Configuration Mode by using command **# configure terminal**
In configuration mode give command
DSLAM(config)**# bridge**
DSLAM(config) **# port lre 2/5 disable (here 2/5 is slot/port no.)**
DSLAM(config) **# port lre 2/5 enable**
DSLAM(config) **# show lre s2 xdsl phys-table linerates (check the port's admin status)**

- **To Reset the series of Port**

DSLAM(config **# port lre 2/1-15 disable** (here 2/1-15 is slot / series of port no.).
DSLAM(config) **# port lre 2/1-15 enable**

5.5 CONCLUSION

All the above commands of ZTE, UTStarcom and NSN DSLAM can help to understand operational and maintenance issues of these DSLAMs, thereby can help in maintenance of overall broadband network to whom they are a part of.

6 OVERVIEW OF SDH AND NGSDH

6.1 LEARNING OBJECTIVES

- Limitation of PDH signals.
- Concept of SDH.
- Multiplexing Structure of STM.

6.2 INTRODUCTION

With the introduction of PCM technology in the 1960s, communications networks were gradually converted to digital technology over the next few years. To cope with the demand for ever higher bit rates, a multiplex hierarchy called the Plesiochronous digital hierarchy (PDH) evolved. The bit rates start with the basic multiplex rate of 2 Mbit/s with further stages of 8, 34 and 140 Mbit/s. In North America and Japan, the primary rate is 1.5 Mbit/s. Hierarchy stages of 6 and 44 Mbit/s developed from this. Because of these very different developments, gateways between one network and another were very difficult and expensive to realize. PCM allows multiple use of a single line by means of digital time-domain multiplexing. The analog telephone signal is sampled at a bandwidth of 3.1 kHz, quantized and encoded and then transmitted at a bit rate of 64kbit/s. A transmission rate of 2048 kbit/s results, when 30 such coded channels are collected together into a frame along with the necessary signaling information. This so-called primary rate is used throughout the world. Only the USA, Canada and Japan use a primary rate of 1544 kbit/s, formed by combining 24 channels instead of 30. The growing demand for more bandwidth meant that more stages of multiplexing were needed throughout the world. A practically synchronous (or, to give it its proper name: plesiochronous) digital hierarchy is the result. Slight differences in timing signals mean that justification or stuffing is necessary when forming the multiplexed signals. Inserting or dropping an individual 64 kbit/s channel to or from a higher digital hierarchy requires a considerable amount of complex multiplexer equipment.

Traditionally, digital transmission systems and hierarchies have been based on multiplexing signals which are plesiochronous (running at almost the same speed). Also, various parts of the world use different hierarchies which lead to problems of international interworking; for example, between those countries using 1.544 Mbit/s systems (U.S.A. and Japan) and those using the 2.048 Mbit/s system. To recover a 64 kbit/s channel from a 140 Mbit/s PDH signal, it's necessary to demultiplex the signal all the way down to the 2 Mbit/s level before the location of the 64 kbit/s channel can be identified. PDH requires "steps" (140-34, 34-8, 8-2 demultiplex; 2-8, 8-34, 34-140 multiplex) to drop out or add an individual speech or data channel.

6.3 PLESIOCHRONOUS DIGITAL MULTIPLEXING

PDH technology (Plesiochronous Digital Hierarchy) is based on pulse code modulation (PCM). In pulse code modulation a multiple-shift usage of a transmission link is enabled by TDM (time division multiplexing). PDH technology enables with its hierarchical structures the implementation of networks with transmission capacities of up

to 140 Mbit/s. In applications with cross connecting on bit-level or with a demand of special interfaces, PDH system technology is in use even today.

Traditionally, transmission systems have been asynchronous, with each terminal in the network running on its own clock. In digital systems, clocking (timing) is one of the most important considerations. Timing means using a series of repetitive pulses to keep the bit rate of the data stream constant and to indicate where the ones and zeros are located in a data stream. Because these clocks are free running and not synchronized, large variations occur in the clock rate and thus the signal bit rate.

Asynchronous multiplexing uses multiple stages; lower-rate signals are multiplexed, and extra bits are added (bit-stuffing) to account for the variations of each individual stream and combined with other bits (framing bits) to form higher-level bit rates. Then bit-stuffing is used again to produce even higher bit rates. At the higher asynchronous rate, it is impossible to access these signals without multiplexing.

The Plesiochronous Digital Hierarchy (PDH) signals have the essential characteristics of time scales or signals such that their corresponding significant instants occur at nominally the same rate. The prefix plesio, which is of Greek origin, means "almost equal but not exactly," meaning that the higher levels in the CCITT (ITU today) hierarchy are not an exact multiple of the lower level. Any variation in rate is constrained within specified limits. The PDH systems belong to the first generation of digital terrestrial telecommunication systems in commercial use.

Before SDH transmission networks were based on the PDH hierarchy. 2 Mbit/s service signals are multiplexed to 140 Mbit/s for transmission over optical fiber or radio. Multiplexing of 2 Mbit/s to 140 Mbit/s requires two intermediate multiplexing stages of 8 Mbit/s and 34 Mbit/s. Multiplexing of 2 Mbit/s to 140 Mbit/s requires multiplex equipment known as 2nd, 3rd and 4th order multiplexer.

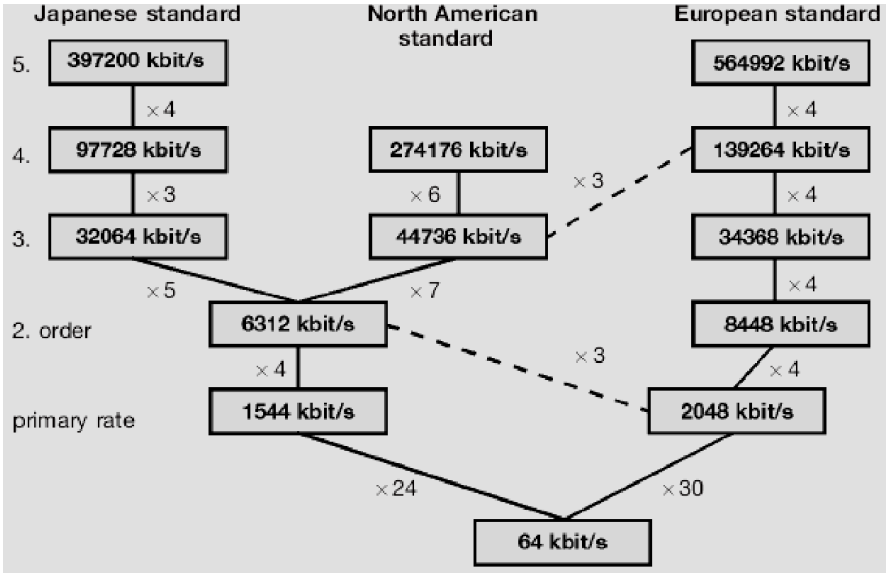


Figure 21: Plesiochronous Digital Hierarchies (PDH)

6.4 S.D.H. EVOLUTION

SDH evolution has become possible because of the following factors:

(i) **Fibre Optic Bandwidth:** The bandwidth in Optical Fibre can be increased and there is no limit for it. This gives a great advantage for using SDH.

(ii) **Technical Sophistication:** Although, SDH circuitry is highly complicated, it is possible to have such circuitry because of VLSI technique which is also very cost effective.

(iii) **Intelligence:** The availability of cheaper memory opens new possibilities.

(iv) **Customer Service Needs:** The requirement of the customer with respect to different bandwidth requirements could be easily met without much additional equipment. The different services it supports are:

1. Low/High speed data.
2. Voice
3. Interconnection of LAN
4. Computer links
5. Broadband ISDN transport (ATM transport)

6.5 ADVANTAGES OF SDH

SDH brings the following advantages to network providers:

6.5.1 **High Transmission Rates**

Transmission rates of up to 40 Gbit/s can be achieved in modern SDH systems. SDH is therefore the most suitable technology for backbones, which can be considered as being the super highways in today's telecommunications networks.

6.5.2 **Simplified Add & Drop Function**

Compared with the older PDH system, it is much easier to extract and insert low-bit rate channels from or into the high-speed bit streams in SDH. It is no longer necessary to demultiplex and then remultiplex the plesiochronous structure.

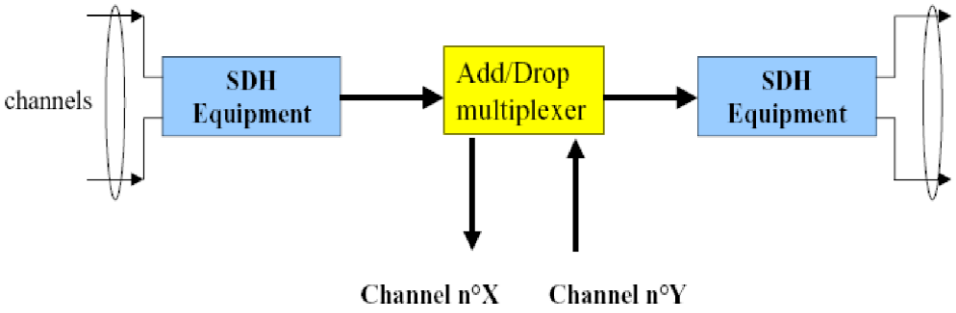


Figure 22: Simplified Add & Drop Function

6.6 HIGH AVAILABILITY AND CAPACITY MATCHING

With SDH, network providers can react quickly and easily to the requirements of their customers. For example, leased lines can be switched in a matter of minutes. The network provider can use standardized network elements that can be controlled and monitored from a central location by means of a telecommunications network management (TMN) system.

6.6.1 **Reliability**

Modern SDH networks include various automatic back-up and repair mechanisms to cope with system faults. Failure of a link or a network element does not lead to failure of the entire network which could be a financial disaster for the network provider. These back-up circuits are also monitored by a management system.

6.6.2 **Future-Proof Platform For New Services**

Right now, SDH is the ideal platform for services ranging from POTS, ISDN and mobile radio through to data communications (LAN, WAN, etc.), and it is able to handle the very latest services, such as video on demand and digital video broadcasting via ATM that are gradually becoming established.

6.6.3 **Interconnection**

SDH makes it much easier to set up gateways between different network providers and to SONET systems. The SDH interfaces are globally standardized, making it possible to combine network elements from different manufacturers into a network. The result is a reduction in equipment costs as compared with PDH.

6.6.4 **Support PDH Payloads**

SDH supports the transmission of existing PDH payloads, other than 8Mbit/s. Most importantly, because each type of payload is transmitted in containers synchronous with the STM-1 frame, selected payloads may be inserted or extracted from the STM-1 or STM-N aggregate without the need to fully hierarchically de-multiplex as with PDH systems.

6.7 SDH RATES

SDH is a transport hierarchy based on multiples of 155.52 Mbit/s. The basic unit of SDH is STM-1. Different SDH rates are given below:

STM-1 = 155.52 Mbit/s

STM-4 = 622.08 Mbit/s

STM-16 = 2588.32 Mbit/s

STM-64 = 9953.28 Mbit/s

Each rate is an exact multiple of the lower rate therefore the hierarchy is synchronous.

6.8 THE STM-1 FRAME FORMAT

The S.D.H. standards exploit one common characteristic of all PDH networks namely 125 micro seconds duration, i.e. sampling rate of audio signals (time for 1 byte in 64 k bit per second). This is the time for one frame of SDH. The frame structure of the SDH is represented using matrix of rows in byte units as shown. As the speed increases, the number of bits increases and the single line is insufficient to show the information on Frame structure. Therefore, this representation method is adopted. How the bits are transmitted on the line is indicated on the top of the figure.

The Frame structure contains 9 rows and number of columns depending upon synchronous transfer mode level (STM). In STM-1, there are 9 rows and 270 columns. The reason for 9 rows arranged in every 125 micro seconds is as follows:

For 1.544 Mbit PDH signal (North America and Japan Standard), there are 25 bytes in 125 micro second and for 2.048 Mbit per second signal, there are 32 bytes in 125 micro second. Taking some additional bytes for supervisory purposes, 27 bytes can be allotted for holding 1.544 Mbit per second signal, i.e. 9 rows x 3 columns. Similarly, for 2.048 Mbit per second signal, 36 bytes are allotted in 125 micro seconds, i.e. 9 rows x 4 columns. Therefore, it could be said 9 rows are matched to both hierarchies.

The standardized SDH transmission frames, called Synchronous Transport Modules of Nth hierarchical level (STM-N). The STM-1 frame is the basic transmission format for SDH. The frame lasts for 125 microseconds; therefore, there are 8000 frames per second.

A frame with a bit rate of 155.52 Mbit/s is defined in ITU-T Recommendation G.707. This frame is called the synchronous transport module (STM). Since the frame is the first level of the synchronous digital hierarchy, it is known as STM-1. Figure 4 shows the format of this frame. It is made up from a byte matrix of 9 rows and 270 columns. Transmission is row by row, starting with the byte in the upper left corner and ending with the byte in the lower right corner. The frame repetition rate is 125 ms., each byte in the payload represents a 64 kbit/s channel. The STM-1 frame is capable of transporting any PDH tributary signal.

The first 9 bytes in each of the 9 rows are called the overhead. G.707 makes a distinction between the regenerator section overhead (RSOH) and the multiplex section overhead (MSOH). The reason for this is to be able to couple the functions of certain overhead bytes to the network architecture. The table below describes the individual functions of the bytes.

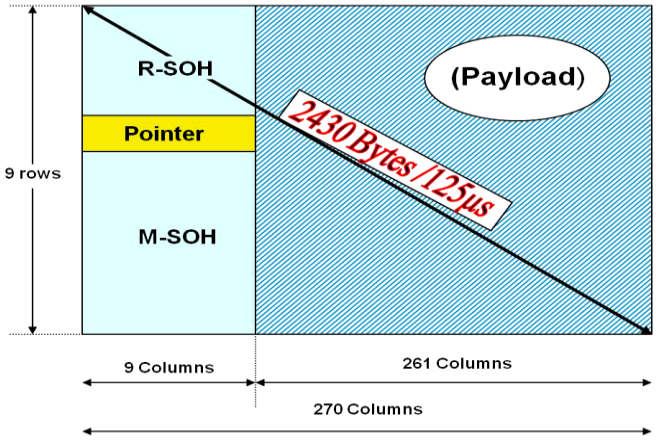


Figure 23: Schematic diagram of STM-1 frame

Calculation of Bit Rate of STM-1

- NO OF ROWS IN FRAME: 9
- NO OF COLUMNS: 270
- NO OF BYTES IN FRAME: 270*9
- NO OF BITS IN A FRAME: 270*9*8
- FRAME DURATION: 125us
- NO OF BITS TRANSMITTED IN ONE SECOND: 270*9*8*1/125 µs

=155.520Mb/S

6.8.1 Section Overhead (Soh) Area

The first 9 bytes in each of the 9 rows are called the overhead. SOH means the additional bytes in the STM-N frame structure needed for normal and flexible transmission of information payload and these bytes are mainly used for the running, management and maintenance of the network. In the 1~ 9 × N columns of the SDH frame, 1~3 rows and 5~9 rows are allocated to the SOH. SOH can be further categorized as RSOH (Regenerator Section Overhead) and MSOH (Multiplex Section Overhead). 1~3 rows are allocated to RSOH and 5~9 rows to MSOH. RSOH can be accessed either at the regenerator to at the terminal equipment. However, MSOH passes a regenerator transparently and is terminated at the terminal equipment. Fig. 3 shows distinction between the regenerator section overhead (RSOH) and the multiplex section overhead (MSOH).

STM-1 SOH

A1	A1	A1	A2	A2	A2	J0	X	X
B1	●	●	E1	●		F1	X	X
D1	●	●	D2	●		D3		
AU pointer								
B2	B2	B2	K1			K2		
D4			D5			D6		
D7			D8			D9		
D10			D11			D12		
S1					M1	E2		

X Reserved for national use

● Media-dependent use (radio-link, satellite)

Figure 24: Section Overhead

The table below describes the individual functions of the bytes.

Table 3. Overhead bytes and their functions

Overhead byte	Function
A1, A2	Frame alignment
B1, B2	Quality monitoring, parity bytes
D1 . . . D3	Q_{ECC} network management
D4 . . . D12	Q_{ECC} network management
E1, E2	Voice connection
F1	Maintenance
J0 (C1)	Trace identifier
K1, K2	Automatic protection switching (APS) control
S1	Clock quality indicator
M1	Transmission error acknowledgment

6.8.2 **Payload Area**

Information payload area is the place where information about various services is stored in the SDH frame structure. Horizontal columns 10 × N~270 × N, and vertical rows 1~9 belong to the information payload area. In it, there are still some Path Overhead (POH) bytes transmitted as part of the payload in a network and these bytes are mainly used for the monitor, management and control of the path performance.

6.8.3 **Administrative Unit Pointer (AU-PTR) Area**

AU PTR is a kind of indicator, mainly used to indicate the accurate position of the first byte of information payload in the STM-N frame, so that the information can be correctly decomposed at the receiving end. It is located at the fourth row of 1~9 × N columns in the STM-N frame structure. The adoption of the pointer mode is an innovation of SDH. It can perform multiplex synchronization and STM-N signal frame locating in the quasi-synchronization environment.

6.9 PATH OVERHEAD

Path Overhead (POH) bytes are mainly used for the monitor, management and control of the path performance. A distinction is made between two different POH types:

6.9.1 **Vc-11/12 POH**

The VC-11/12 POH is used for the low-order path. ATM signals and bit rates of 1.544 Mbit/s and 2.048 Mbit/s are transported within this path.

V5	Indication and error monitoring
J2	Path indication
N2	Tandem connection monitoring
K4	Automatic protection switching

6.9.2 **Vc-3/4 POH**

The VC-3/4 POH is the high-order path overhead. This path is for transporting 140 Mbit/s, 34 Mbit/s and ATM signals.

J1	Path indication
B3	Quality monitoring
C2	Container format
G1	Transmission error acknowledgment
F2	Maintenance
H4	Superframe indication
F3	Maintenance
K3	Automatic protection switching
N1	Tandem connection monitoring

6.10 NETWORK ELEMENTS OF SDH

Figure 25 is a schematic diagram of a SDH ring structure with various tributaries. The mixture of different applications is typical of the data transported by SDH. Synchronous networks must be able to transmit plesiochronous signals and at the same time be capable of handling future services such as ATM.

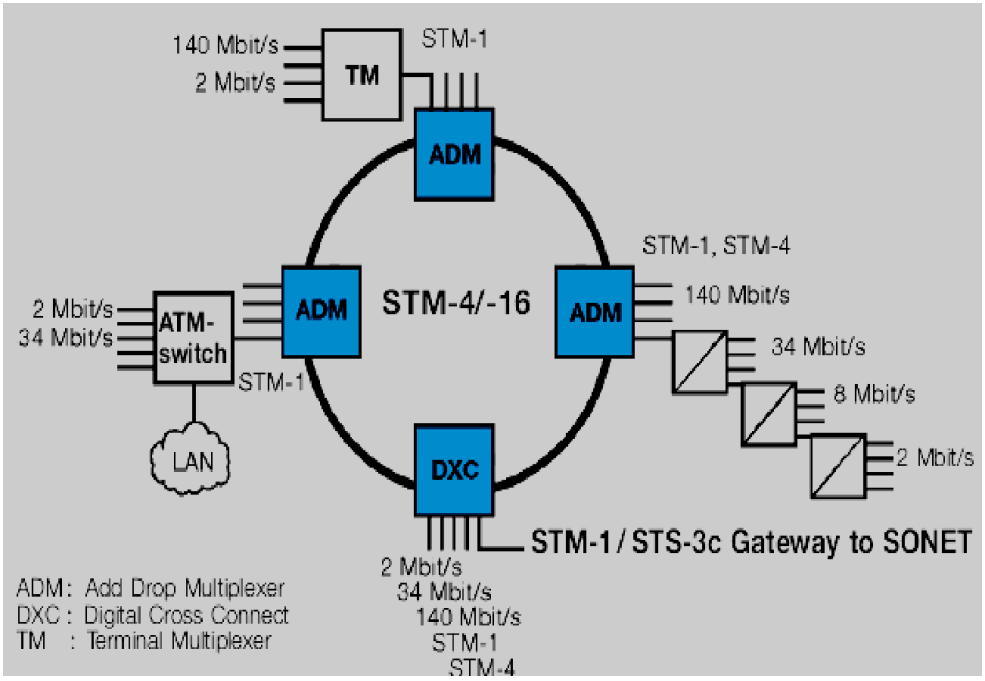


Figure 25: Schematic diagram of hybrid communications networks

Current SDH networks are basically made up from four different types of network element. The topology (i.e. ring or mesh structure) is governed by the requirements of the network provider.

6.10.1 Terminal Multiplexer (TM)

Terminal multiplexers are used to combine plesiochronous and synchronous input signals into higher bit rate STM–N signals as shown in Fig. 26 below. On the tributary side, all current plesiochronous bit rates can be accommodated. On the aggregate, or line side we have higher bit rate STM–N signals. Terminal multiplexers are used to combine plesiochronous and synchronous input signals into higher bit rate STM-N signals.

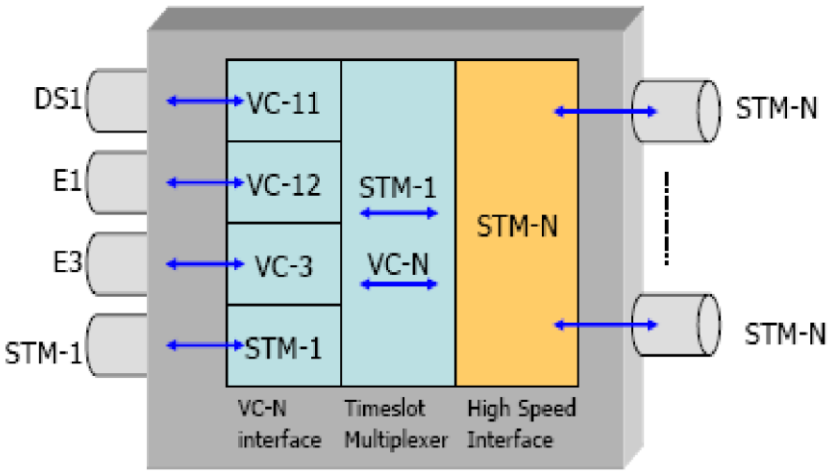


Figure 26: Terminal Multiplexer (TM)

6.10.2 **Add/Drop Multiplexers(ADM)**

Add/drop multiplexers (ADM**)** permits add and drop of lower order signals.Lower bit rate synchronous signals can be extracted from or inserted into high speed SDH bit streams by means of ADMs. This feature makes it possible to set up ring structures, which have the advantage that automatic back-up path switching is possible using elements in the ring in the event of a fault.

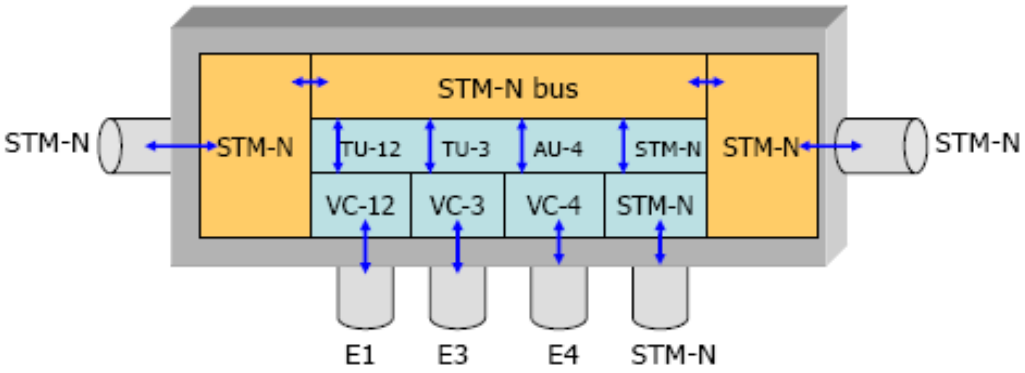


Figure 27: Add/Drop Multiplexers (ADM)

6.10.3 **Regenerators**

Regenerators as the name implies, have the job of regenerating the clock and amplitude relationships of the incoming data signals that have been attenuated and distorted by dispersion. They derive their clock signals from the incoming data stream. Messages are received by extracting various 64 kbit/s channels (e.g. service channels E1, F1) in the RSOH (regenerator section overhead). Messages can also be output using these channels.

Figure 28: Regenerator

6.10.4 **Digital Cross-Connect (DXC)**

This network element has the widest range of functions. It allows mapping of PDH tributary signals into virtual containers as well as switching of various containers up to and including VC-4.It permits switching of Transmission lines with different bit rates.

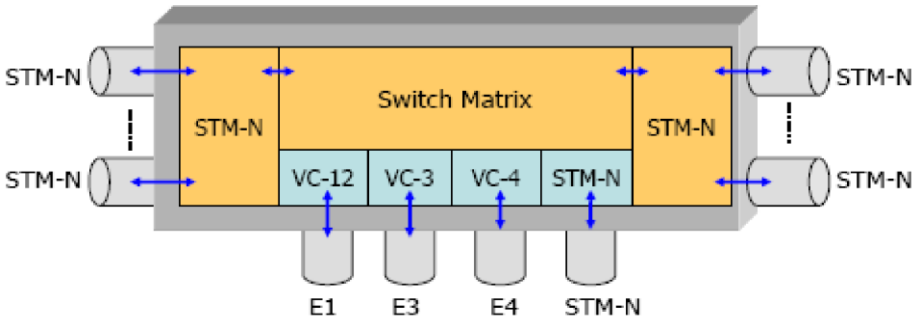


Figure 29: DXC

6.10.5 Network Element Manager

Telecommunications management network (TMN) is considered as a further element in the synchronous network. All the SDH network elements mentioned so far are software-controlled. This means that they can be monitored and remotely controlled, one of the most important features of SDH.

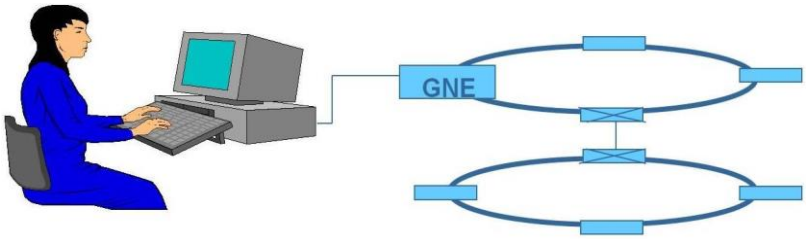


Figure 30: Network Element Manager

6.11 NEXT GENERATION SDH

Next Generation SDH enables operators to provide more data transport services while increasing the efficiency of installed SDH/SONET base, by adding just the new edge nodes, sometime known as Multi Service Provisioning Platforms (MSPP) / Multi Service Switching Platforms (MSSP), can offer a Combination of data interfaces such as Ethernet, 8B/10B, MPLS (Multi-Protocol Label Switching) or RPR(Resilient Packet Ring), without removing those for SDH/PDH. This means that it will not be necessary to install an overlap network or migrating all the nodes or fiber optics. This reduces the cost per bit delivered, and will attract new customers while keeping legacy services. In addition, in order to make data transport more efficient, SDH/SONET has adopted a new set of protocols that are being installed on the MSPP/MSPP nodes. These nodes can be interconnected with the old equipment that is still running.

6.11.1 What Is Next Generation SDH?

Following major issues that exist in the legacy SDH:

- Difficulty of mapping newer (Ethernet, ESCON, FICON, Fiber Channel etc) services to the existing SDH transport network.
- Inefficient use of the transport network in delivering data services.
- Inability to increase or decrease available bandwidth to meet the needs of data services without impacting traffic.

Three mature technologies—

- Generic Framing Procedure (GFP), ITU-T G.7041
- Link Capacity Adjustment Scheme (LCAS), ITU-T G.7042
- Virtual Concatenation (VCAT), ITU-T G.707

-together in Next generation SDH solved the above issues and adding three main features to traditional SDH:

- Integrated Data Transport i.e. Ethernet tributaries in addition to 2Mb, 140 Mb, STM-1,4,16 ----**GFP**
- Integrated non-blocking, wide-band cross connect (2Mb granularity) making the efficient use of the transport network in delivering data services ---**VCAT**

  Dynamic Bandwidth allocation, Intelligence for topology discovery, route computation and mesh based restoration------**LCAS**

Next Generation SDH is Packet Friendly and have IP router like capabilities. It does not matter if the client stream has constant or variable bit rates.

"VCAT provides more granularity, LCAS provides more flexibility and GFP efficiently transports asynchronous or variable bit rate data signals over a synchronous or constant bit rate".

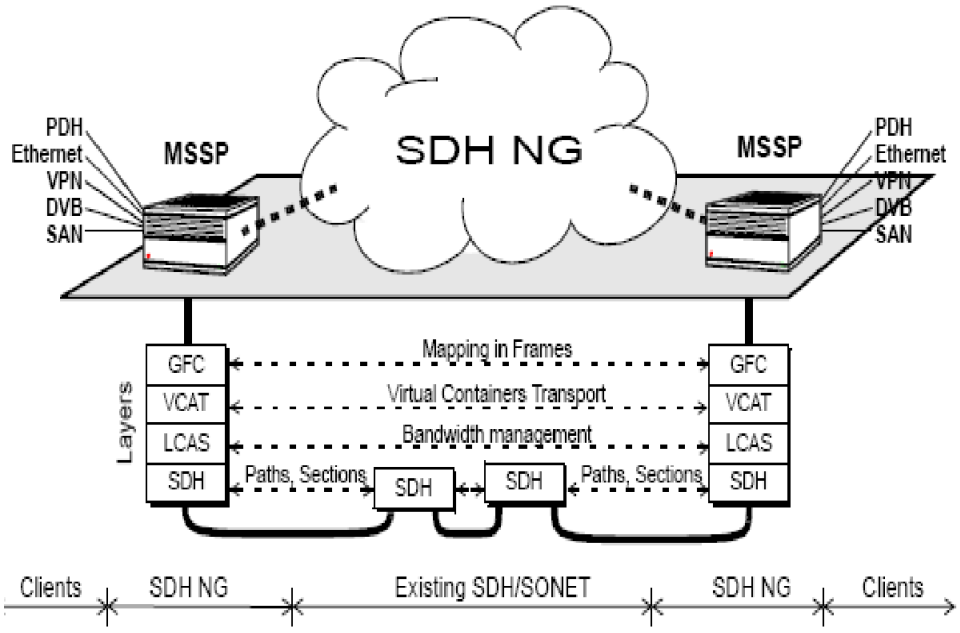


Figure 31: Block Diagram of NGSDH

Hence,

Next Generation SDH = Classic SDH + [GFP+VCAT+LCAS]

6.12 COMPONENTS OF NEXT GEN SDH

6.12.1 **Generic Framing Procedure (Gfp):**

Generic Framing Procedure (GFP), an all-purpose protocol for encapsulating packet over SONET (POS), ATM, and other Layer 2 traffic on to SONET/SDH networks. GFP is defined in ITU-T G.7041 along with virtual concatenation and link capacity adjustment scheme (LCAS) transforms legacy SDH networks to Next generation SDH networks.

GFP adds dynamism to legacy SDH. GFP is most economical way of adopting high speed services, constant bit rate and variable bit rate, in SDH networks and can provide basis for evolving RPR.

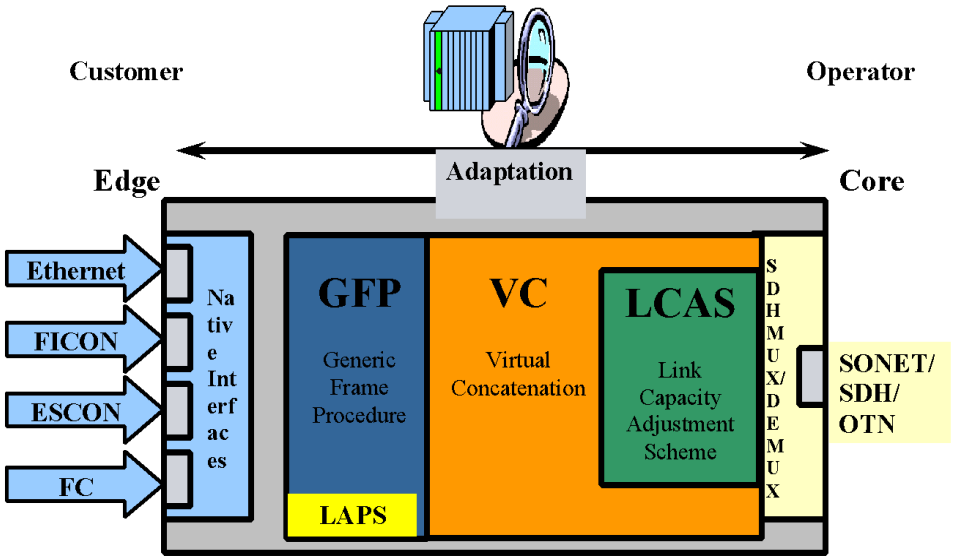


Figure 32: Functional Model of GFP

There are actually two types of GFP mechanisms ;-

1. PDU-oriented known as Frame mapped GFP (GFP-F)

2. Block-code-oriented known as Transparent GFP (GFP-T)

a) GFP-F: -

GFP-F(Framed) is a layer 2 encapsulation in variable sized frames. Optimised for data packet protocols such as DVD, PPP and Ethernet, MPLS etc Frame mode supports rate adaptation and multiplexing at the packet/frame level for traffic engineering. This mode maps entire client frame into one GFP frames of constant length but gaps are

discarded. The frame is stored first in buffer prior to encapsulation to determine its length. This introduces delay and latency.

b) GFP-T:

GFP-T is useful for delay sensitive services. GFP-T(Transparent) is a layer 1 encapsulation in constant sized frames. Optimized f or traffic based on 8B/10B codification such as VoIP,DVB-ASI,1000BASE-T, SAN, Fibre Channel, and ESCON.

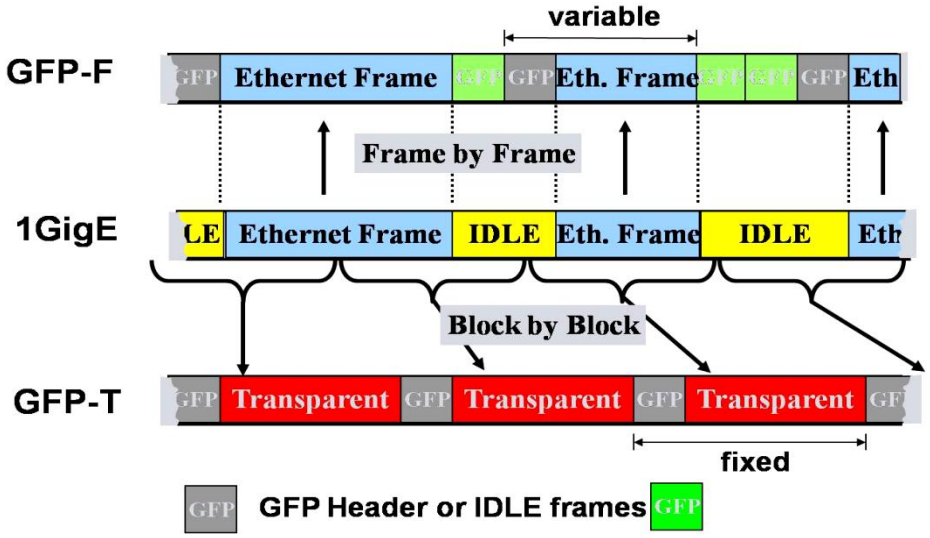


Figure 33: GFP-F & GFP-T

Transparent mode accepts native block mode data signals and uses SDH frame merely as a lightweight digital wrapper. GFP-T is very good for isocronic or delay sensitive protocols &SAN (ESCON). GFP-T is used for FC, Gigabit Ethernet etc.

6.12.2 **Concatenation (V-Cat & C-Cat) :**

SDH concatenation consists of linking more than one VCs to each other to obtain a rate that does not form part of standard rates. Concatenation is used to transport pay loads that do not fit efficiently into standard set of VCs.

Two concatenation schemes are:

1. Contiguous concatenation

2. Virtual concatenation

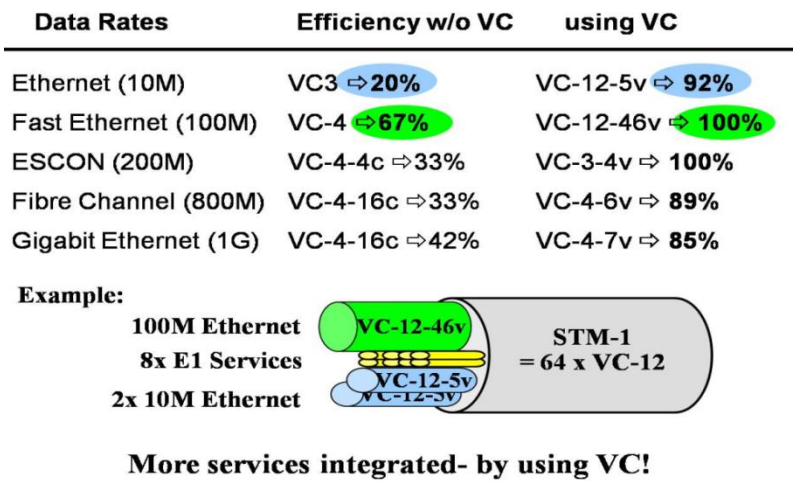


Figure 34: VCAT Efficiency

a) Contiguous concatenation:

The traditional method of concatenation is termed as contiguous. This means that adjacent containers are combined and transported across the SDH network as one container. Contiguous concatenation is a pointer based concatenation. It consists of linking N number of VCs to each other in a logical manner within the higher order entity i.e. VC4 and above. The concatenated VCs remain in phase at any point of network. The disadvantage is that it requires functionality at every N/E adding cost and complexity. Lower order VCs (VC-12, VC3) concatenation is not possible in contiguous concatenation as shown in Fig.

b) Virtual Concatenation:

Virtual concatenation maps individual containers in to a virtually concatenated link. Any number of containers can be grouped together, which provides better bandwidth granularity than using a contiguous method. It combines a number of lower/higher order VCs (VC-12, VC3 & VC4 payload) that form a larger concatenation Group, and each VC is treated as a member. 10 Mb Ethernet would be made up of five VC-12s, creating these finely tuned SDH pipes of variable capacities improve both, scalability and data handling/controlling ability as per SLA (service level agreement).

The transport capacity with or without VC is shown in Fig. 35

VCs are routed individually and may follow different paths, within the network, only the path originating and path terminating equipment need to recognize and process the virtually concatenated signal structure as shown in Fig. 35

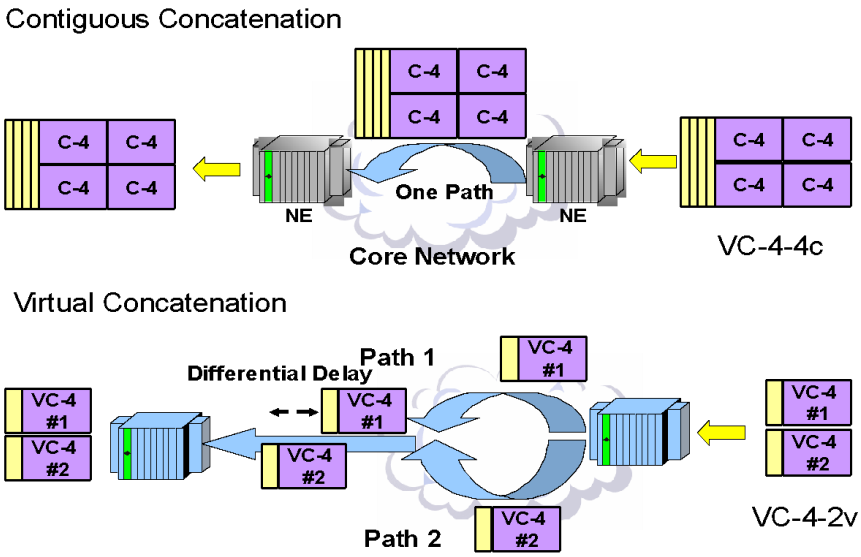


Figure 35: Virtual & Contiguous Concatenation

Virtual concatenation Benefits:

- Use the same core NEs, modify only edge NEs.
- Low investment and fast ROI (return on investment).
- Efficient & scalable i.e. fine granularity and multi-path capability.
- SDH gives best QoS, well engineered and reliable.

6.12.3 Link Capacity Adjustment Scheme(LCAS):

Link Capacity Adjustment Scheme (LCAS) is an emerging SONET/SDH standard and is defined in ITU-T G.7042 having capability to dynamically change the amount of bandwidth used in a virtually concatenated channel i.e. bandwidth management flexibility. LCAS is bi-directional signaling protocol exchanged over the overhead bytes, between Network Elements that continually monitors the link. LCAS can dynamically change VCAT path sizes, as well as automatically recover from path failures. LCAS is the key to provide "bandwidth on demand".

LCAS enables the payload size of VCG (group of VCs) to be adjusted in real time by adding or subtracting individual VCs, from VCG dynamically, without incurring hits to active traffic. In LCAS, signaling messages are exchanged between the two VCs end points to determine the number of concatenated payloads and synchronize the addition/removal of SDH channels using LCAS control packets.

6.12.4 Benefits Of LCAS :-

A . Call by call bandwidth (Bandwidth on demand)

Customer

⇨ rents a 6Mb Internet connection (VC-12-3v)

⇨ calls to get additional 2Mb

Operator

⇨ will provision additional VC-12 path

⇨.and will hitless add it to existing connection via LCAS!

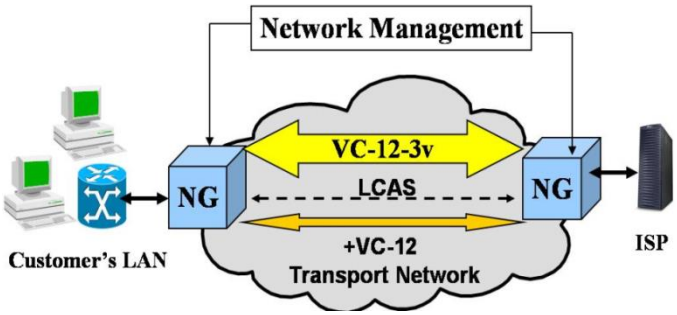


Figure 36: Bandwidth call by call

B. Bandwidth on Schedule

A customer is offered a fixed bandwidth of 100 Mb (VLAN) Ethernet, allotting 46 VC-12 (0ne VC12 = 2.176 Mb x 46 = 100.1 Mb). Every night for one hour additional 900 M ESCON service is provisioned by LCAS. New revenue opportunity at low traffic hours.

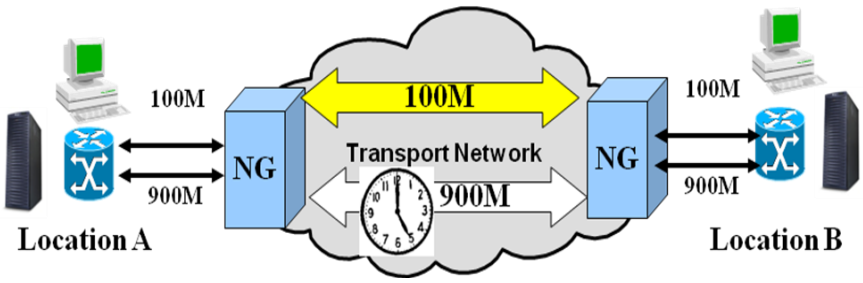


Figure 37: Bandwidth on scheduled Time

LCAS is not only used for dynamic bandwidth adjustment but also for survivability options for next generation SDH. LCAS is a tool to provide operators with greater flexibility in provisioning of VCAT groups, adjusting their bandwidth in service and provide flexible end-to-end protection options. LCAS is defined for all high and low order payloads of SDH.

6.13 CONCLUSION

SDH (Synchronous Digital Hierarchy) & NGSDH is a standard technology for synchronous data transmission on optical media. It is the international equivalent of Synchronous Optical Network. Both technologies provide faster and less expensive network interconnection than traditional PDH (Plesiochronous Digital Hierarchy) equipment. Now Next Generation SDH is capable to support packet data also.

7 FTTH TECHNOLOGY & INTRODUCTION TO BHARATNET

7.1 LEARNING OBJECTIVES

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

7.2 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.

7.3 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.

7.3.1 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.

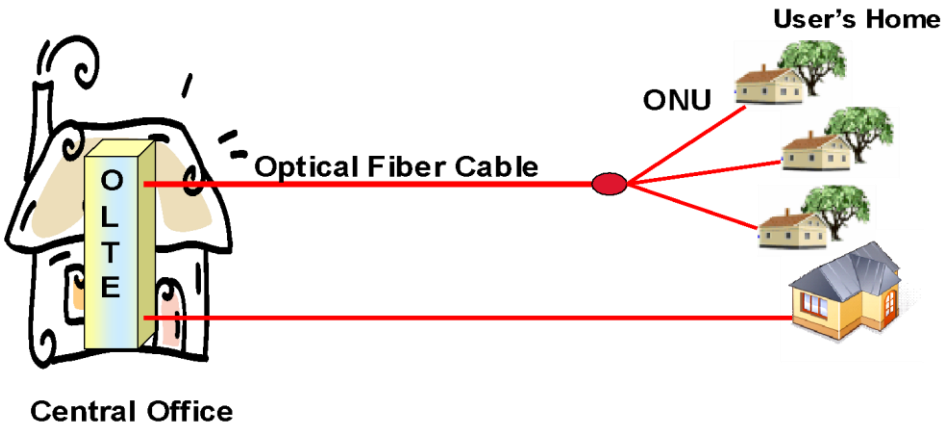


Figure 38: FTTH Configuration

7.3.2 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).

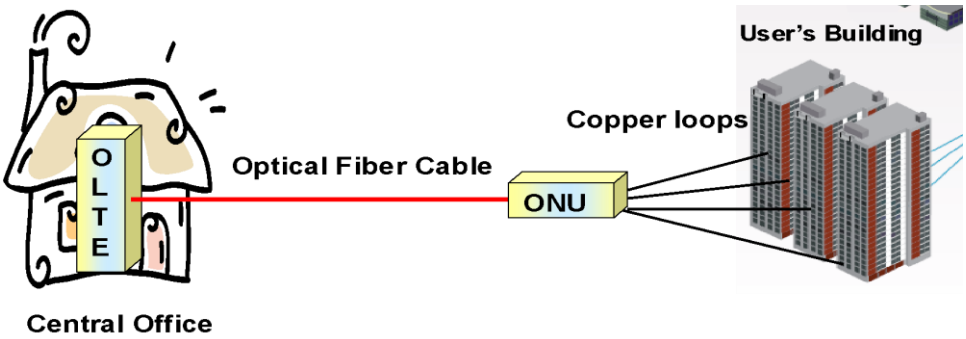


Figure 39: FTTB Configuration

7.3.3 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.

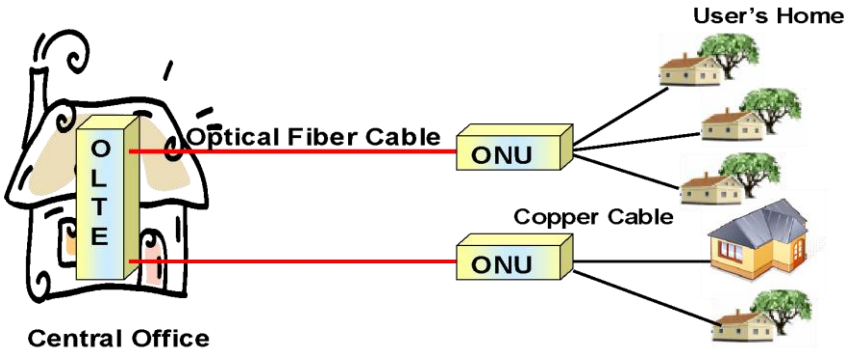


Figure 40: FTTC Configuration

7.4 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.

7.5 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)**.

7.5.1 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**".

a) 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.

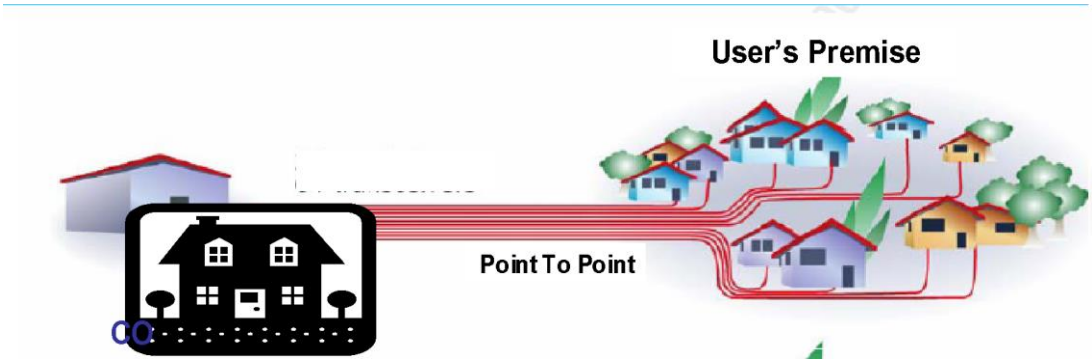


Figure 41: Home Run Fiber (Point-to-Point) architecture

b) Active Star Ethernet (Point-to-Multi Point) Architecture

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

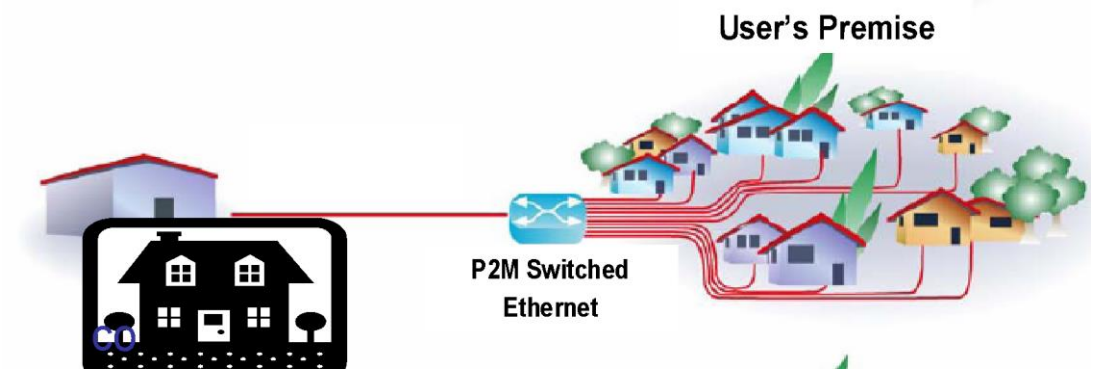


Figure 42: Active Star Ethernet (ASE) architecture

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.

7.6 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.

7.6.1 **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.

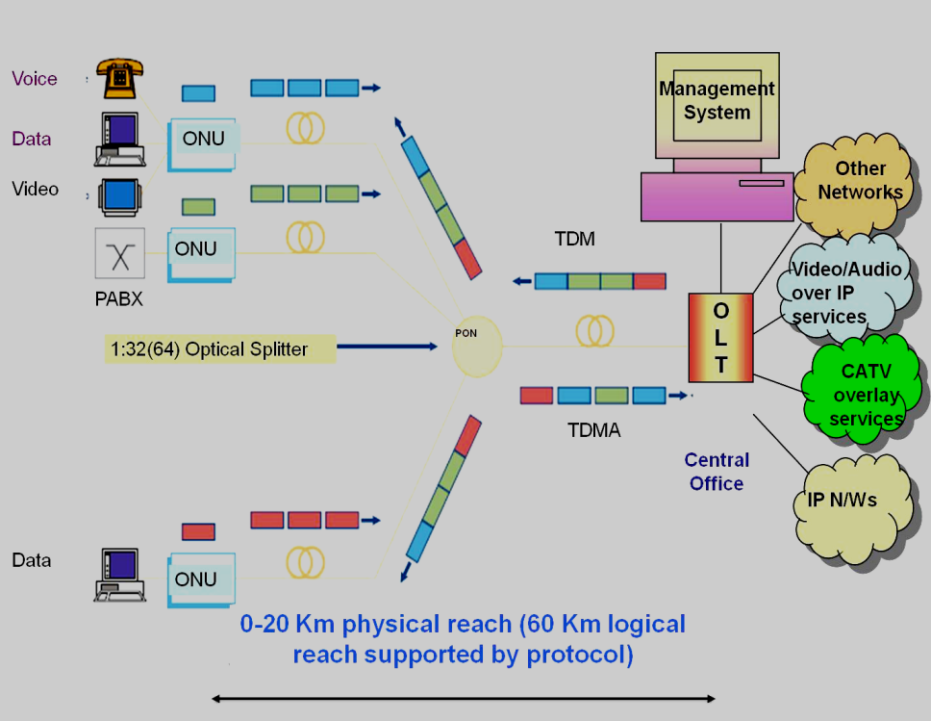


Figure 43: PON Architecture

7.6.2 ONU/ONT:

This provides access to the users i.e. an External Plant / Customer Premises equipment providing user interface for many/single customer. 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.

7.6.3 PON:

Distributed or single staged passive optical splitters/combiners provides 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 end to end basis. These are available in various options like 1:4, 1:8, 1:16, 1:32 and 1:64.

7.6.4 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.

7.7 SPLITTER CONFIGURATIONS

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

7.7.1 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'soptical network terminals (ONTs) at 32 homes are connected as shown in fig. 44.

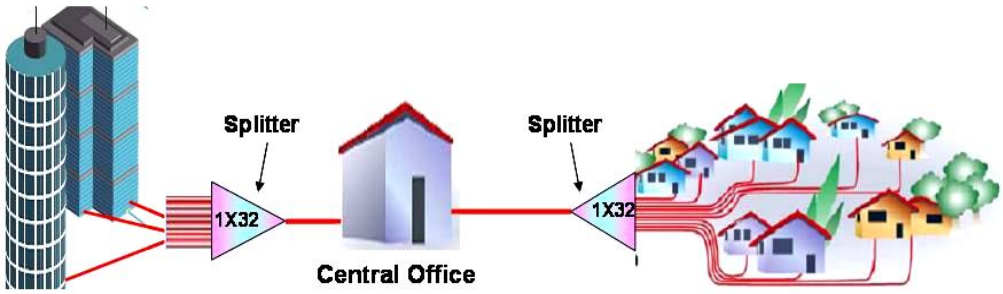


Figure 44: Centralized Splitter Approach

7.7.2 Cascaded Splitter Approach

A cascaded split configuration results in pushing splitters deeper into the network as shown in fig.45. 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.

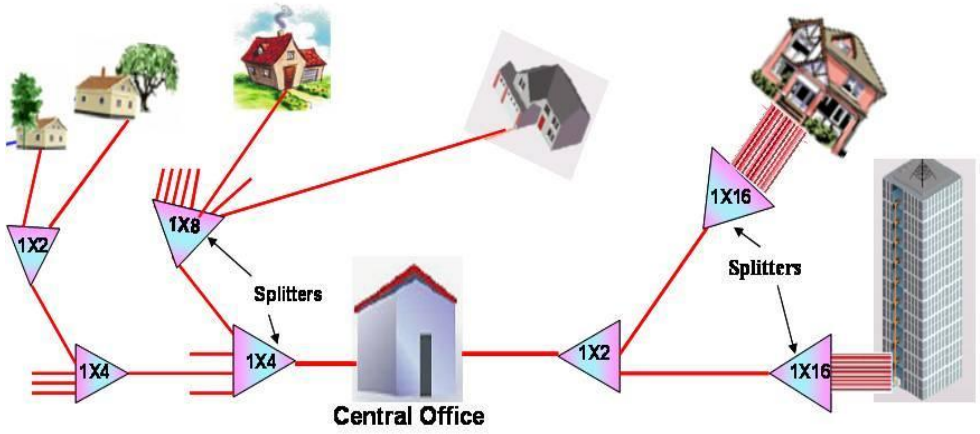


Figure 45: Cascaded Splitter Approach

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.

7.7.3 **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.

7.7.4 **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.

7.7.5 **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.

7.7.6 **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.

7.8 THE FEATURES OF DIFFERENT PON STANDARD

Table 4. 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	Support multiple	Support multiple	None

Switching	protection configuration	protection configuration	

7.9 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)

7.10 INTRODUCTION TO BHARATNET

BharatNet, also known as Bharat Broadband Network Limited, is a telecom infrastructure provider, set up by the Government of India under the Department of Telecommunications for the establishment, management, and operation of the National Optical Fibre Network to provide a minimum of 100 Mbit/s broadband connectivity to all 250,000 gram panchayats in the country, covering nearly 625,000 villages, to improve telecommunications in India and reach the campaign goal of Digital India. The last mile connectivity, with a total of 700,000 Wi-Fi hotspots to cover all 625,000 villages of India by adding 2 to 5 Wi-Fi hotspots per gram panchayat and a minimum of one Wi-Fi hotspot per village, have been created by connecting high-speed 4G base tower stations of commercial telecom operators to BharatNet, whereby commercially non-viable Wi-Fi hotspots will be subsidised by the union government grant to sustain the operation. The government has discounted the bulk BharatNet bandwidth rates to the commercial

telecom operators by 76% to enable them to offer the highly discounted, affordable, competitive, and commercially viable BharatNet-enabled wireless cellular 4G broadband deals to the rural customers. Theunion government share of funding will come from the Universal Services Obligation Fund of the Department of Telecommunications. It will be rolled out with the additional funding by state governments to connect all gram panchayats in India. BharatNet is the world's largest rural broadband connectivity program. It is built under the Make in India initiative with no involvement of foreign companies.

BharatNet will provide more employment opportunities, improved service delivery (online e-gram panchayat services, e-governance, e-education, e-health, e-medicine, e-grievances, e-agriculture, e-citizen, etc.), and an impetus to the Make in India, Digital India and Startup India initiatives. According to Morgan Stanley's research, of India's 33% internet penetration in November 2017 only 15% and 2% of total internet users use online shopping and retail shopping respectively, estimated to go up to 78% penetration, 62% online shoppers and 15% online retail shopper respectively by 2027. By the end of BharatNet Phase-II, the total current fibre optical network will grow by 100% to 10 million kilometres. This 100% increment in the fibre optic network would result in several hundred percent increment in the internet usage when in addition to 625,000 villages (each with minimum 100 Mbit/s), 2,500,000 government institutions and 5,000,000 households will also be connected to the BharatNet broadband by 2020, by adding several hundred million more broadband users to the current figures of 276.5 million wireless and wireline broadband connections out of total of 422.2 million internet users on 31 March 2017.

BharatNet Phase-I, connecting 100,000 village councils covering 300,000 villages, was completed by December 2017. BharatNet Phase-II was completed by 31 March 2019 to connect the remaining 150,000 village councils covering 325,000 villages. As of 31 December 2018, India had a population of 1.3 billion people, 1.23 billion Aadhaar digital biometric identities, 1.21 billion mobile phones, 446 million smartphones, 560 million internet users up from 481 million people (35% of the country's total population) in December 2017, and 51% growth in e-commerce.

It is both an enabler and a beneficiary of other key government schemes, such as Digital India, Make in India, the National e-Governance Plan, UMANG, Bharatmala, Sagarmala, the dedicated freight corridors, industrial corridors, and UDAN-RCS.

7.10.1 **History**

On 25 October 2011, the Government of India approved the National Optical Fibre Network (NOFN) initiative, later renamed as BharatNet, to connect all 250,000 gram panchayats in the country covering nearly 625,000 villages, by utilising the existing optical fibre network and extending it to the gram panchayats. To achieve this, Bharat Broadband Network was incorporated as a Special Purpose Vehicle(SPV) on 25 February 2012 under Companies Act of 1956. Between 2011 and 2014, project did not take off as planned, and only 350 km of optical fibre, out of 300,000 km optical fibre network needed for the Phase-I, was laid. Between 2014 and 2017, the original Phase-I target of laying 300,000 km of optical fibre was completed.

After renaming the project as the "BharatNet", several changes made to expedite the project, significantly enhanced the BharatNet funding to several billion dollars under the Digital India, set ambitious time-bound implementations deadlines, appointed government public sector units (BSNL, RailTel and PowerGrid Corp) for the swift implementation and monitoring, and to bypass the right of way issues for laying the optical fibre cable network the existing government-owned roads, rail lines and power lines were used. Bangalore based United Telecoms Limited won the bid, being almost 80% lower to the second lowest bidder ITI followed by Tejas, STL, etc. BharatNet collaborated with other government entities such as C-DOT, Telecommunications Consultants India Limited and National Informatics Centre for the design and rollout plan of BharatNet NOFN Project. BharatNet assigned the execution work of network roll out to several other Government of India Public Sector Units, namely BSNL, RailTel and Power Grid Corporation of India. Project was rolled out as a collaboration between the Union Government (to provide broadband connectivity at sub-district Block-level), state governments (optical fibre to gram panchayat level) and private sector companies (Wi-Fi hotspots in each village and connections to the individual homes). Union government total share is ₹450 billion (equivalent to ₹510 billion, US$7.1 billion or €6.6 billion in 2019), the rest will be funded by the respective state governments.

Once all the gram panchayats have been connected by the dedicated fibre optical network, the last mile connectivity to all villages will be provided by the commercial telecom operators by expanding the current national network of 38,000 Wi-Fi hotspots to 700,000 Wi-Fi hotspots to cover all 625,000 villages in India. ₹36 billion (equivalent to ₹41 billion, US$570 million or €520 million in 2019), union government subsidy support will be given to the telecom service operators for rolling out Wi-Fi hotspots in commercially non-vialble villages. BharatNet has offered the bulk broadband bandwidth at 75% discounted rates to the commercial telecom operators so that they can offer deeply discounted monetised competitive deals to the rural wireless broadband customers. Commercial operators Reliance Jio, Bharti Airtel, Idea Cellular and Vodafone have already connected their 4G-based-broadband base towers to BharatNet at various locations to provide the high speed last mile wireless broadband connectivity.

There are 36 states and union territories of India, including 28 states and 9 UTs. BSNL was awarded work for 18 of these, RailTel received work in 8 and Power Grid Corporation of India in 5. BSNL was awarded work for 18+ states and UTs, namely Andaman and Nicobar Islands, Assam, Bihar, Chandigarh, Chhattisgarh, Haryana, Jammu and Kashmir, Karnataka, Kerala, Lakshadweep, Madhya Pradesh, Maharashtra, Punjab, Rajasthan, Sikkim, Uttar Pradesh (divided into two projects, UP East and UP West), Uttarakhand and West Bengal. RailTel was awarded work for 8+ states and UTs, namely Arunachal Pradesh, Gujarat, Nagaland, Manipur, Mizoram, Meghalaya, Puducherry and Tripura.

Power Grid Corporation of India was awarded work for 5 states, namely Andhra Pradesh, Himachal Pradesh, Jharkhand, Odisha and Telangana. Delhi is included with Phase-I BSNL work for Haryana. Goa is also included with Phase-I BSNL work for Maharashtra. Dadra and Nagar Haveli and Daman and Diu are included with Phase-II work for RailTel. Tripura is likely included with Phase-II RailTel work for the Northeast India.

7.10.2 **Technology**

The components of the BharatNet architecture in the concept diagram are:

1. Gigabit passive optical network (GPON) technology at the national level.
2. Optical line terminal at subdistrict block level.
3. Optical fibre cable to each gram panchayat.
4. Beam splitters and combiners.
5. Optical network terminals at gram panchayat level.
6. Hotspot (Wi-Fi) at each village-level within the gram panchayat.
7. Connectivity to the individual homes.

7.10.3 **Implementation**

BharatNet Phase-I (Dec 2017):

BharatNet Phase-I, across 13 states and UTs was completed in December 2017 with the Phase-I union government funding share of ₹110 billion (equivalent to ₹120 billion, US$1.7 billion or €1.6 billion in 2019). It connected 100,000 gram panchayat, covering 300,000 villages by laying 300,000 km of optical fibre network. 13 states and UTs in this phase are: Andaman and Nicobar Islands, Chandigarh, Delhi, Goa, Haryana, Karnataka, Kerala, Lakshadweep, Manipur, Meghalaya, Puducherry, Sikkim and West Bengal. As of 31 December 2017, BSNL has laid 11,005 km optical fibre cable and completed the connection of out of all targeted 6,017 gram panchayats in Haryana.

BharatNet Phase-II (Dec 2018):

BharatNet Phase-II, to be completed by 31 March 2019 (unofficial target date 31 Dec 2018), will connect the remaining nearly 145,000 gram panchayats covering 325,000 villages through additional 1 million km of optical fibre. Phase-II commenced with the union government funding share of ₹340 billion (equivalent to ₹380 billion, US$5.4 billion or €5.0 billion in 2019), with the current 250 km per day pace of optical fibre network roll out which needs to be raised to 500 km per day to achieve the completion target of March 2019. Roll out will be expedited with November 2017 memorandum of understanding with seven more states, namely Andhra Pradesh, Chhattisgarh, Gujarat, Jharkhand, Tamil Nadu, Maharashtra and Telangana. Phase-II will double the total optical fibre network of the nation and will generate 100,000,000 mandays employment for the roll out.

DoT will invest ₹107.43 billion (US$1.5 billion) on BharatNet in Northeast India by December 2018, including erecting 6,673 towers to connect 8,621 villages at the cost of ₹533.6 billion (US$7.5 billion) and additional 4,240 gram panchayats by satellite broadband connectivity by December 2018.

7.11 CONCLUSION

From the BSNL network point of view GPON, being the TDM based technology, shall integrate into the existing switching network. While the VOIP feature in the GE-PON provides easy migration path to the **Next Generation Network (NGN)** of the BSNL. Since TDM switches and the NGN are to coexist for up to 2015 as per the NGN vision plan both GPON and GE-PON are the most suitable PON technologies for BSNL.

8 LMG ARCHITECTURE

8.1 LEARNING OBJECTIVES

- Hardware components of UTStarcom LMG.
- Functionality of different modules in LMG.
- Initial configuration of LMG's.

8.2 INTRODUCTION

B1205 is a cost effective & versatile Digital Loop Carrier (DLC) and Multi Service Access Node (MSAN) optimal solution from UTStarcom that provides a unique set of capabilities enabling service providers to deliver the most competitive triple play service offerings. It enables service providers to smoothly migrate to IP based next-generation applications while continuing to offer traditional TDM based services to customers.

The B1205 supports a range of technologies such as POTS, ADSL/ADSL2/ADSL2+, VDSL2, SHDSL(EFM) which allows the service providers to offer highly interactive and bandwidth intensive applications. B1205 Facts as a traditional TDM based DLC, IPDSLAM, Media Gateway platform rolled into one.

8.3 IAN B1205 OVERVIEW

Figure 46: IAN B1205

8.3.1 Physical Appearance-IAN B1205

Chassis Type	Height	Depth	Access	Splitters	Deployment
B1205	5U	270 mm	Front	External	Indoor

Port Density

Subscriber Interfaces	Capacity
ADSL2+	320 ports
FXS/VoIP	320 ports
Uplink	4 GE

Slot Assignment

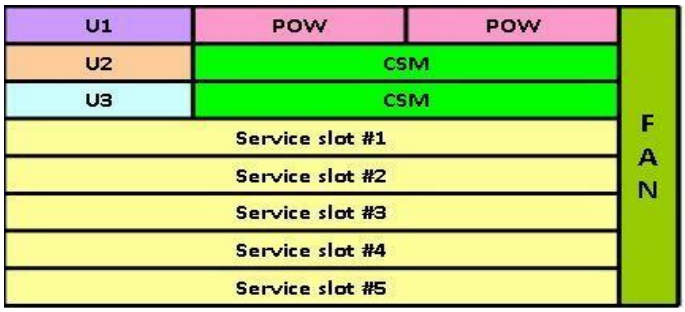


Figure 47: Physical Appearance-IAN B1205

8.3.2 Features

- Modular architecture: 64 to 320 pots per node
- 5RU ETSI Height Compliant chassis
- Versatile customer Interfaces - ADSL2+, VDSL2, POTS, E1, SHDSL(EFM)
- Transport/Trunk: GE, E1
- Supports combo subscriber port: IVD (Integrated ADSL2+ & POTS Module)
- Versatile solution for TDM/IP Based applications:
- Seamless migration from V5/AN to VoIP/AG
- Redundant Control, Switching & Power Modules with Hot redundancy. (All active calls are preserved)
- Over 28 Mbps capacity per DSL subscriber
- Inherits QoS and other functionality from proven iAN8K B1000

- Built-in loop test for voice-band and broadband
- ETSI 482.6mm width compliant
- CE, FCC,VCCI compliant

8.4 IAN B1205E OVERVIEW

Figure 48: IAN B1205E Overview

- 2x CSM slots full redundant control
- and switch modules
- 3 flexible U (Half) slots
- 10 universal slots for different modules
- 64 ports ADSL2+ card
- 64 ports FXS card
- 2x redundant –48VDC power supplies
- Built-in clock, ringer
- Metallic line testing
- Hot redundancy
- CLI and Telnet Management
- SNMP based Management
- External splitters

8.4.1 Physical Appearance-Ian B1205e

Chassis Type	Height	Depth	Access	Splitters	Deployment
B1205E	8 U	270 mm	Front	External	Indoor

	Port density	
	Subscriber Interfaces	**Capacity**
	ADSL2+	640 ports
	FXS/VoIP	640 ports
	Uplink	4 GE
	SLOT	Assignment

Slot Assignment

Figure 49: Physical Appearance-IAN B1205E

8.5 HARDWARE MODULE DESCRIPTION

A. Common module

1. CSM1A : The system control module controls the whole system operation which supports VoIP/AG services, AN services and DSLAM services.
2. POW1A : The power supply module with ring generator, converts -48V DC to +3.3V DC and +75V DC ring.
3. VPM1A : The voice process module provides up to 256 channels.
4. PCU1A : The Peripheral Control Unit provides the external signals access for the iAN B1205 system.

B. POTS user interface module

FXS1A : The remote user module provides 64 POTS subscriber connections and supports built-in line test (@1.8Kohm loop impedance).

C. ADSL user interface module

ASL1A : The ADSL user module provides 64 ADSL user connections

8.5.1 Csm1a–Control & Switching Module

Figure 50: CSM1A Card

VoIP protocols processing support SIP

L2 Switch with 20 GE ports (40 GE ports with Redundant CSM1A):

- 4xGE uplink interfaces with configurable SFP in front panel
- Uplink interfaces can be used for shelf cascading also.
- 2xGE interface to each of Slots 1 - 10
- 1xGE interface to each of Slots U1 and U3.
- 2xGE interface to slot U2.

  1+1 Hot Redundancy

- Manual switch
- Auto switch

DSLAM service processing

- System OAM features
- Download system and module firmware
- Stores system and module configuration data
- Detects, initialize and configure modules
- Communicates with PCU1A for external alarms

Management and Maintenance:

- GUI (SNMP) network management interface,
- CLI (Debug) interface
- Module self-test and diagnostic
- Support IPv6

POW1A- Power Supply Module

Supports DC/DC converter

- -48V DC current input, up to 20A
- -48V to +3.3V DC/DC converter
- -48VDC to +75VDC DC/DC converter

Supports 1+1 hot redundancy

- Surge protection
- EMC/EMI arrestor UTStarcom Confidential 14

Alarms

- Card absent alarm
- -48V power supply alarm
- +3.3V power supply alarm
- +75V ringing alarm

Integrated management by the CSM

8.5.2 **VPM1a- Voice Processing Module**

Figure 51: VPM1A Card

DSP Channel Capacity

- G.711: 256 channels ,
- G.729: 168 channels
- G.723.1: 128 channels
- G.726ADPCM : 256 channels

Voice Codec En-Coding & De-Coding

- G.711A/U Law, G.729AB ,G.723.1,G.726 ADPCM

Tone Detector and Tone Generator

- Voice Activity Detection (VAD)
- Comfortable Noise Generation (CNG)

  Line Echo Canceller

  DTMF/MF Relay, RFC2833

  Packet Loss Concealment & Recovery

  Fax Relay
- CED/CNG Tone Detection in Fax Mode
- V.21, V.27ter, V.29, V.17, V.33, V.34 HDX, V.34 Fax Forced Fallback
- T.38 over UDPTL, T.38 over RTP, T.38 Version 0/1/2/3

CallerID

- Bellcore , ETSI, NTT, Chinese and UK CID Generation & Detection

Performance Statistics

- RTCP (RFC3550/3551), RTCP-XR (RFC3611)

Management and Maintenance

- Debug interface on the faceplate
- Integrated management by the CSM1A

8.5.3 **PCU1a- Peripheral Control Module**

Figure 52: PCU1A Card

Collects external alarms

Buffer and distribute 2.048 MHz clock from central office to CSM

Provides one GE port for port mirroring function of CSM

Integrated management by the CSM

8.5.4 **FXS1a- Foreign Exchange Subscriber Module**

Figure 53: FXS1A Card

Provides 64 PSTN subscriber line interface ports

BORSCHT function

- Battery feeding
- Over-voltage and over-current protection
- Ringing control
- Supervision
- Codec
- Hybrid
- Test

Management and Maintenance

- Supports line test, self-test and diagnostics
- Debug interface
- Integrated management by the CSM1A

Special features:

- Configurable A-law and μ-law codec both
- Standard 1800 ohm loop length
- Balanced ringing signal for maximum 5 REN per port.
- Dial pulse with both 10 and 20 PPS.
- On-hook transmission for Calling Line Identity.
- Polarity reversal
- 16Khz and 12Khz tone generation
- Anti-lightning protection

8.5.5 **ASL1a-ADSL Subscriber Line Module**

Figure 54: ASL1A Card

Provides 64 ADSL ports for subscriber lines

Supports ADSL and ADSL2/2+ standards

- ANSI T1.413, G.992.2(G.lite),G.992.1(G.dmt) Annex-A, G.992.3(ADSL2), G.992.5(ADSL2+), G.992.3(ADSL2) Annex M, G.992.5(ADSL2+), G.992.3(ADSL2) (READSL) Annex L
- Up to 28 Mbps downstream.
- Up to 1 Mbps upstream for ADSL2+/Annex A,
- 3 Mbps upstream for Annex M standard.
- 8 PVCs per ADSL port

Supports Layer-2 switching

- 4K MAC address table
- MAC address limit per bridge port

Supports QoS

- 8 queues in DSL port
- 8 queues in WAN port

Supports multicast

- IGMP snooping v1/v2/v3
- Up to 256 multicast groups per module

Supports security

- MAC Flooding Control, MAC address spoofing, MAC filtering
- DHCP filter, DHCP Option82
- Gateway ARP spoofing, IP spoofing prevention
- Access Control List (ACL)

Management and Maintenance

- Supports SELT/DELT and diagnostics
- Debug interface
- Integrated management by the CSM

8.5.6 **Fan Tray**

Figure 55: FAN TRAY

Each fan tray contains four axial fans which are connected in parallel with 48 VDC power input.

The fan trays are hot-swappable and can be replaced without interrupting system operation.

Each fan tray transfers two fan alarms to PCU1A.

8.6 LMG DEPLOYMENT IN BSNL NETWORK

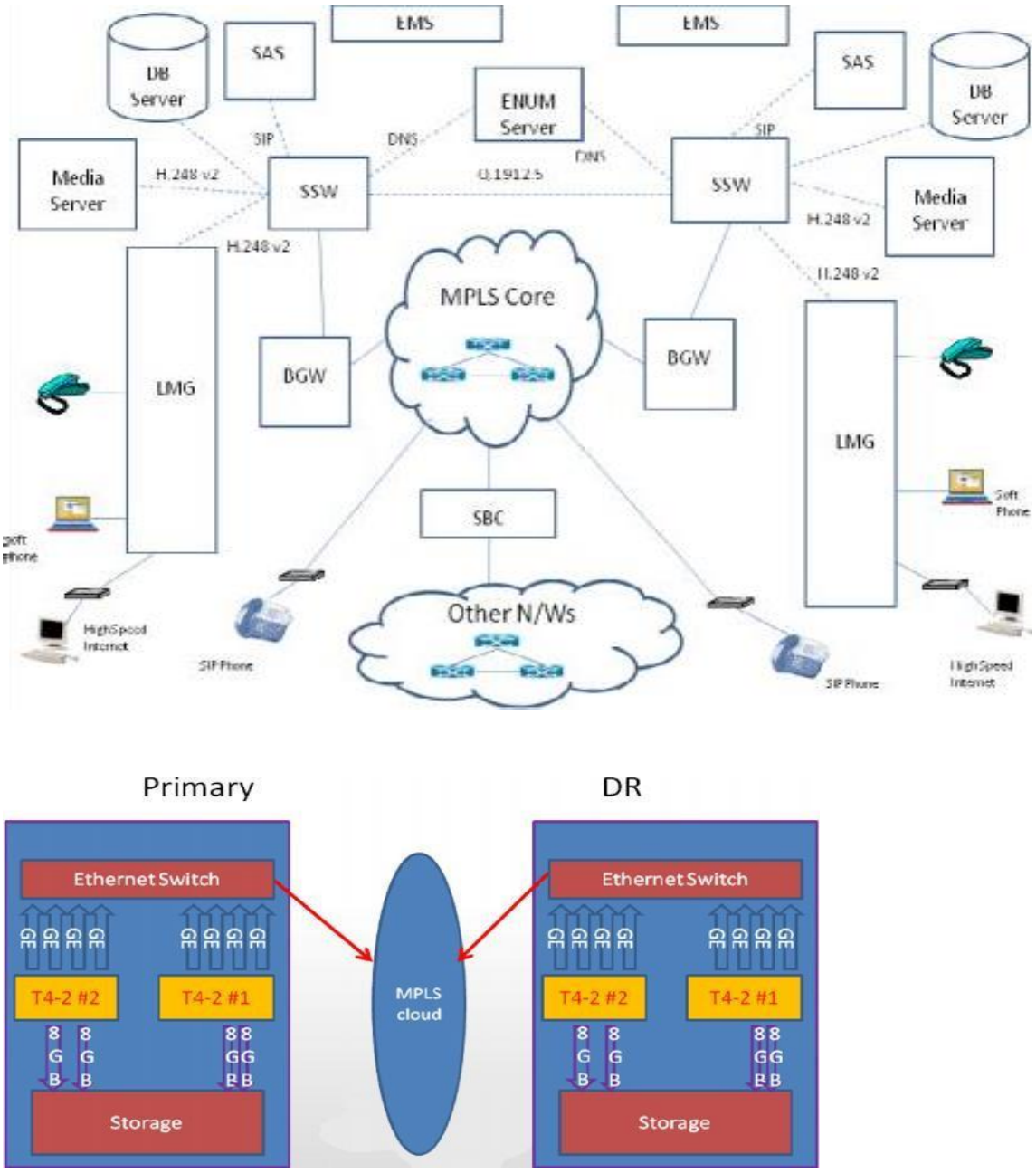


Figure 56: Primary and DR Configuration

Each T4-2 server will be divided to 2 Solaris Zones.

One zone (2 CPU Core) for Oracle Database and another zone (max of 14 CPU Core) for OMC-A application.

Two T4-2 server connect to Storage with HBA. For DR, the data copy is done via Ethernet interface of the server.

8.7 INITIAL CONFIGURATION OF LMGS

Console Port Connectivity

Connect the Debug Cable between the "COM" connector on the CSM faceplate and serial RS 232 connector on PC

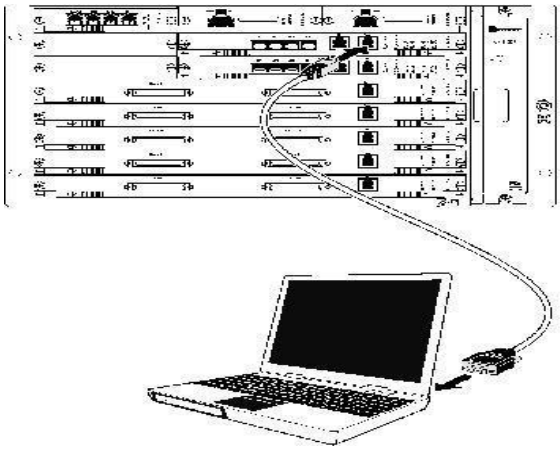


Figure 57: CONSOLE PORT Connectivity

Hyper Terminal Configuration

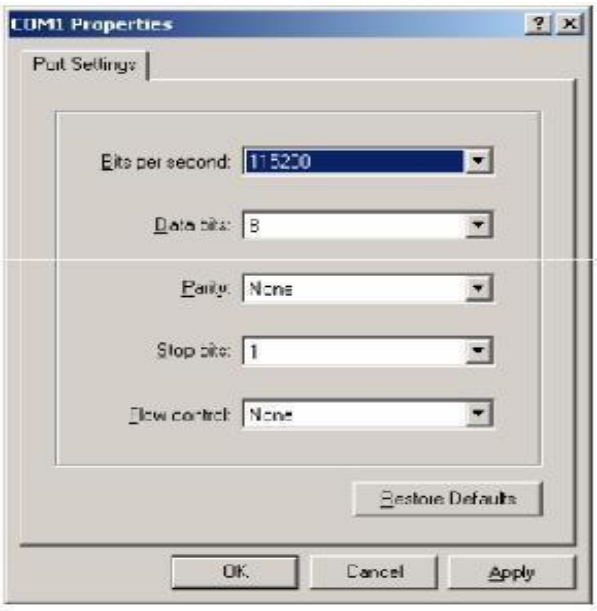


Figure 58: Hyper Terminal Configuration

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

8.8 NODE MANAGEMENT IP CONFIGURATION OF 256P & 500P LMG

The default username/password is admin/admin.

Log on to the CSM1A admin@10.230.7.4:

- ~#admin
- You are now in the Privileged Mode

Configure the IP address

- B1205#ip
- B1205(IP)#management address 10.230.7.5 netmask 255.255.255.0
- This command will change the IP address to 10.230.7.5.
- Execute anyway? (yes or no)
- Yes

Configure default route

- B1205(IP)#route 0.0.0.0 netmask 0.0.0.0 gateway 10.230.7.254

Check the IP address and default route setting

- B1205(IP)#show ip
- B1205(IP)#show route

Save Configuration

- B1205#save config bin

Now out band management port can be used to access CSM1A.

8.9 CONCLUSION

LMG's as an access equipment provides a simple solution to migrate from TDM based local exchanges to IP based equipment with less power and minimum maintenance. It also provides facilities for DSL services thereby eliminating the use of additional DSLAM. The compact build of LMG's provides an excellent choice for operators ready to migrate to an all IP based NGN network with reduced CAPEX and OPEX.

9 OCLAN

9.1 LEARNING OBJECTIVES

- Concept of OCLAN switch.
- Its architecture used in BSNL.
- OCLAN features and working principle.

9.2 INTRODUCTION

The OC LAN switch is deployed as Tier-2 Network Device in the BSNL MultiPlay connecting the Tier-1 RPR to DSLAM in other cities. ZXR10 T64G MPLS 10G Routing Switch is deployed as OC-LAN Switch in BSNL MultiPlay project. ZXR10 T64G is applicable to the core layer and convergence layer of the large-scale enterprise networks. The system features high reliability, high scalability, and powerful service capability. This product can be used to build the convergence layer and core layer of our network. Backplane bandwidth can reach 900 Gbps with switching capacity of 480 Gbps. It features with a packet-forwarding rate of 357 Mbps with L2/L3/L4 wire speed switching capability.

The ZXR10 T64G MPLS 10G Routing Switch adopts modular design and a parallel processing mechanism based on multiple processors. T64G adopts Crossbar architecture. The key module adopts 1:1 redundancy backup. It supports a wide variety of interfaces, such as 10GE; GE, FE, and POS and can provide multiple service functions such as MPLS, NAT, QoS, multicast and bandwidth control.

ZXR10 T160G/T64G is an Ethernet routing switch developed by ZTE Corporation which can be applicable to the backbone layer. ZXR10 T160G/T64G provides the interfaces including fast Ethernet, gigabit Ethernet. OCLAN can satisfy the increasing requirements for bandwidth. ZXR10 T160G/T64G also supports multiple Unicast and multicasting protocols.

9.3 WORKING PRINCIPLE

ZXR10 T64G is a large-capacity rack mountable Ethernet switch which implements wire-speed Layer2/3 switching via two-level hardware switching.

Level 1 switching is between ports of line interface cards;

Level 2 switching between line interface cards is implemented via control switching board.

9.4 FEATURES OF THE OCLAN SWITCH

1. high reliability
2. high scalability
3. Powerful service capability.

This can be used to build the convergence layer and core layer of our network. The Backplane bandwidth can reach 900 Gbps with switching capacity of 480 Gbps. These switches provide packet-forwarding rate of 357 Mbps with L2/L3/L4 wire speed switching capability. It supports a wide variety of interfaces, such as 10GE; GE, FE, and POS and can provide multiple service functions such as MPLS, NAT, QoS, multicast and bandwidth control.

9.5 HARDWARE STRUCTURE OF ZXR10 T64G

It adopts the structure of standard 19-inch plug-in box. ZXR10 T64G has 6 plug-in slots, one of which is slot for control and switching board, four of which are for line interface card, and the left one can serve as the slot for control and switching board or line interface card.

ZXR10 T64G includes the following four modules:

1. Control module
2. Switching module
3. Packet processing and interface module
4. Power supply module
5. Fan Module

9.5.1 **Control Module:**

Itis composed of main processor and some external functional chips, which implements processing to applications of the system. It provides various operational interfaces including serial interface and Ethernet interface to perform data operation and maintenance.

9.5.2 **Switching Module:**

It provides multiplex high-speed bi-directional serial interface to implement wire-speed data switch between line interface cards.

9.5.3 **Packet Processing And Interface Module:**

Interface module is the external interface of ZXR10/160G/T64G, providing one or multiple physical ports. Different line interface cards can implement access of different rates and types.

9.5.4 **Power Supply Module:**

It adopts 220V AC power supply or –48V DC power supply, providing power for other parts of the system.

9.6 CONFIGURATION OF LAPTOP FOR ACCESSING ZXR10 T64G VIA CONSOLE PORT:

1. Connect the PC’s serial port and OCLAN switch’s Console port in the Control
2. Switching module.
3. Go to
4. All Programs
5. Accessories

6. Communications
7. HyperTerminal
8. And set the following parameters as shown after selecting the appropriate COM port.
9. Bits per sec : 115200
10. Data bit : 8
11. Parity : none
12. Stop bit : **1**
13. Flow Control : **none**

SWITCH : ZXR10 T64G Chassis
OEM : ZTE Corporation

Figure 59: Unit/Component introduction

9.7 CONTROL SWITCHING BOARD

The Control Switching Board (MCS) is the core of ZXR10 T64G, implementing the functions of control module and switching module. It performs the function of master/slave switchover.

Interfaces Available

Console Interface

10/100 base TX Ethernet Interface.

Line Interface Cards

The Line Interface cards include Fast Ethernet Interface board, Gigabit Ethernet Interface board and 10giga bit Ethernet board.10 GB Ethernet is not being used in BSNL currently.

44 FE + 4 GE Interface Board

44 FE + 4GE Interface card board provides 44 Fast Ethernet Optical Interfaces and 4 gigabit Ethernet electrical Interfaces.

24 port Gigabit Ethernet Interface Board

This provides 4 gigabit Ethernet Electrical Interfaces and 20 Ethernet Optical Interfaces.

Line Interface Cards Used

1 * 44FE + 4GE Interface card

2 * 24 FE Interface Card

Ports Used in BSNL currently

GE Interfaces populated with SFPs : 17 Nos.

FE Interfaces populated with SFPs : 16 Nos.

9.8 ROLE OF OCLAN SWITCH

OCLAN Switch which becomes the Tier 2 component of the network resides in the Access layer. OCLAN switches aggregate the number of DSLAMs in every OC cities as required in the project.

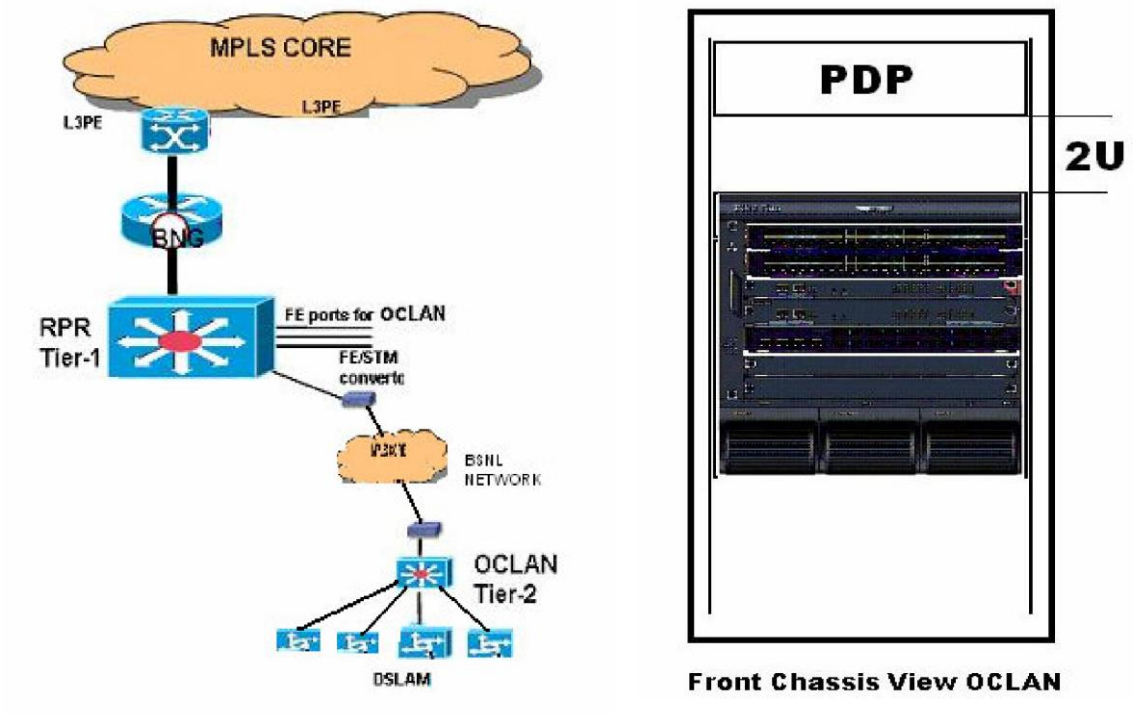


Figure 60: OCLAN Front View

OCLAN Switch which becomes the Tier 2 component of the network resides in the Access layer. OCLAN switches aggregate the number of DSLAMs in every OC cities as required in the project.

Note:

1. PDP should be fixed at the front side of Rack and should be at the TOP.
2. Between PDP and OCLAN Rack there should be 2U gap.

Power Cabling:

1. Power cable and Lugs for OCLAN is shipped along with the equipment and connect it accordingly and on PDP side crimp the –ve with point type lug and other two (+ve and ground) with round type.

9.9 CONTROL AND LINE INTERFACE CARD INSERTION RULE

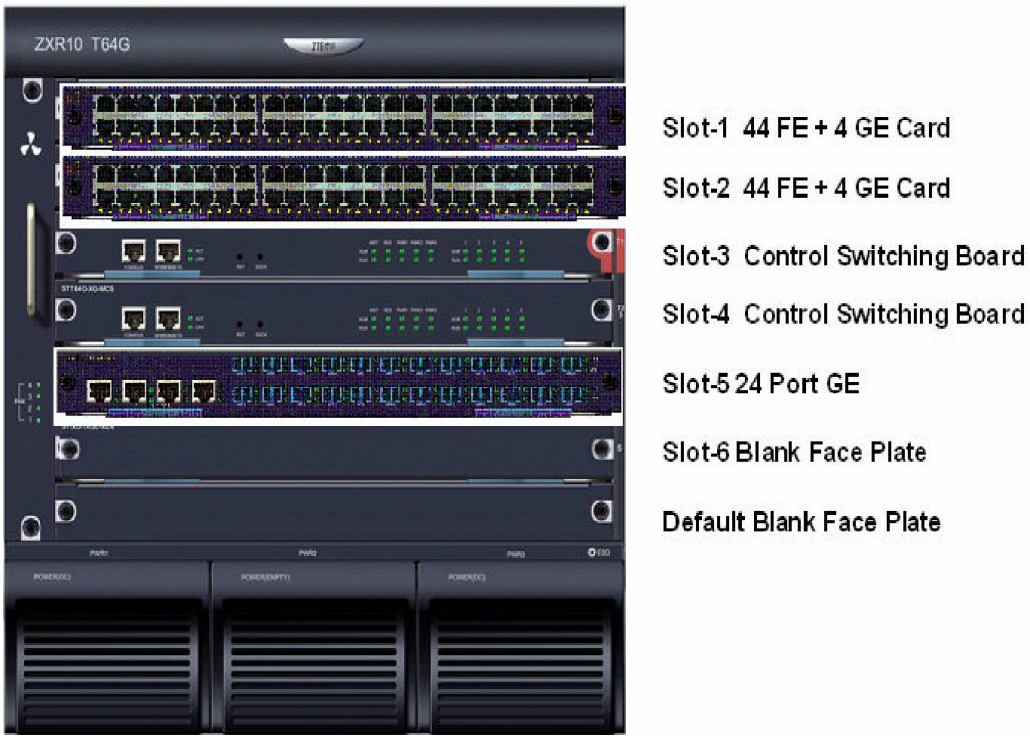


Figure 61: Control & Line Interface Cards of OCLAN

Note: Each Slot in the slot numbered from 1 to 6 from top of the switch has to be populated with appropriate cards as shown in the figure above.

SFP MODULE INSERTION RULE

As described in the above figure, slot 1 populated with 44 FE + 4 GE card will be inserted with the following SFP modules.

4 GE SFPs in port numbered 45, 46, 47 and 48

8 FE SFPs in port numbered 1, 2, 3, 4, 5, 6, 40 and 41

Port 40 to be configured for Uplink.

Port 41 is reserved for Uplink

All other ports mentioned above to be configured for connecting DSLAMs

Slot 5 populated with 24 GE card will be inserted with the following SFP modules.

9 GE SFPs in port numbered 5, 6, 7, 8, 9, 10, 11, 12 and 13

9.10 FIBER CABLING DETAILS

lot no	**Card Type**	**Port no**	**SFP/XFP Type**	**Fiber Cable Type**	**Connecting to**
	44 FE + 4 GE	**1** to 6	FE SFP	LC-FC Multimode	DSLAM via BSNL provided Converters
		40,41	FE SFP	LC-FC Multimode	T1 via UT Starcom supplied STM Converter
		45 to 48	GE SFP	LC-FC Singlemode	DSLAMs
	44 FE + 4 GE	1 to 6	FE SFP	LC-FC Multimode	DSLAM via BSNL provided Converters
		40,41	FE SFP	LC-FC Multimode	T1 via UT Starcom supplied STM Converter
		45 to 48	GE SFP	LC-FC Singlemode	DSLAMs
	24GE	5 to 13	GE SFP	LC-FC Singlemode	DSLAMs

Table 5. Fibre Cable Details

9.11 OPTICAL POWER RANGE FOR TRANSCEIVERS IN OCLAN SWITCH

Transceiver Type	**Fiber Type**	**Tx Optical Power Range in dBm**		**Rx Optical Power Range in dBm**	
		Min	**Max**	**Min**	**Max**
GE SFP	SMF	-5	2	-22	-3
FE SFP	MMF	-9.5	-3	-17	0

Table 6. Optical Power Range

Note:

Use 0 dB attenuators for GE Transceivers.

For FE Transceivers, use attenuators of appropriate dB so as to attain Optical Power within the given range, preferably towards the Rx Minimum value.

9.12 CONCLUSION

The OCLAN switch is very important component for O& M workflow, the proper understanding of features and functioning of OCLAN requires for uninterrupted services of the network .The guidelines for maintenance of Multiplay Broadband network and define the responsibilities of various node incharges to ensure uninterrupted service of Broadband and customer satisfaction.

10 CDR PROJECT

10.1 LEARNING OBJECTIVES

- Concept of CDR used in BSNL.
- implementation of CDR based convergent billing and customer care system.
- Customer care and billing for the Landline, Broadband and Leased Line Services.

10.2 INTRODUCTION

CDR based convergent billing and customer care system is Under Implementation stage in BSNL. This is the biggest project taken by any TSP (Telecom service provider) in India. This project has replaced all the previously existing systems of Commercial, TRA (Telecom Revenue Accounting), FRS (Fault Repair Service) and DQ (Directory Enquiry). The project covers the customer care and billing for the following services:

1. Landline
2. Broadband
3. CDMA
4. 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, it has implemented State-of-the-Art Customer Relationship Management (CRM) software. This software takes care of all types of requests from the customers and integrates with other systems such as Order Management and Billing systems. This software also provides a Web Self Care (WSC) module, which will enable customers to access the system through the Internet for placing any request, for making payments, or for general enquiry.

10.3 CONVERGENT BILLING AND ITS ADVANTAGES

i. This project implements a convergent billing system, which enables us to issue a single bill for a customer taking any type of service from BSNL.
ii. The electronic stapling software is implemented in all the four zones.
iii. A customer having presence only in a particular zone, spanning across SSAs and Circles, can have a single bill for all the services he takes from BSNL whether the bill for the particular service is prepared or not from this system.
iv. The electronic stapling software installed at Hyderabad, takes care of corporate customers having All India presence.
v. This system has interfaces with other zonal billing systems, GSM billing systems and the NIB billing system.
vi. With these interfaces, it is possible to issue a single bill to a corporate customer having All India presence.
vii. The system is also capable of taking the payments against this single bill and then distributing the payments back to the original billing systems of the different services taken by the customer for proper accounting. This is one of the biggest advantages of this project.
viii. The system also helps us introduce Combo Plans, offering flexible tariff plans to customers availing Landline, Broadband and GSM services.

10.4 ZONES FOR IMPLEMENTATION OF CDR PROJECT

CDR Project	Zone	Circles
Project-1	SOUTH	Andhra Pradesh, Chennai District, Tamilnadu, Karnataka, Kerala (Data Centre at Hyderabad)
	EAST	Kolkata Telecom District, West Bengal Circle, Orissa, Jharkhand, Bihar, Assam, North East-I, North East-II, Andaman & Nicobar (Data Centre at Kolkata)
Project-II	WEST	Maharashtra, Gujarat, Madhya Pradesh, Chattisgarh (Data Centre at Pune)
	NORTH	Punjab Circle, UP-East, UP-West, Haryana, Rajasthan, Himachal Pradesh, Uttarakhand, Jammu & Kashmir (Data Centre at Chandigarh)

Table 7. Zones For Implementation Of CDR Project

10.4.1 Implementation Data Centres For CDR Project

The entire project is implemented with four Data Centre, one each at:

1) **Hyderabad**
2) **Kolkata**
3) **Pune**
4) **Chandigarh**

These four Data Centers take care of all the activities of the Circles in the respective Zones. The South and East Zones are considered as one project & the North and West Zones are considered as the second project.

10.4.2 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 Centers. It is very important therefore to have a 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.

10.5 HARDWARE FOR CDR PROJECT

As far as hardware is concerned, we have procured Data Centre (DC) Class servers which are high-end servers having 64 cores/CPUs in each machine. These high-end machines shall be used for hosting the main applications such as Billing and CRM. We have procured low-end servers, which are two-CPU servers for small applications like Anti-virus, HTTP, Web servers, Authentication etc. They are mostly Windows or Linux based servers. In the Hyderabad Data Centre alone, we have 18 DC class servers and around 200 low-end servers.

10.6 NETWORK FOR CDR PROJECT

This project has implemented a countrywide Intranet. This network connects 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 has integrated all the networks and provides a countrywide IP network with MPLS as the backbone. This network is 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.

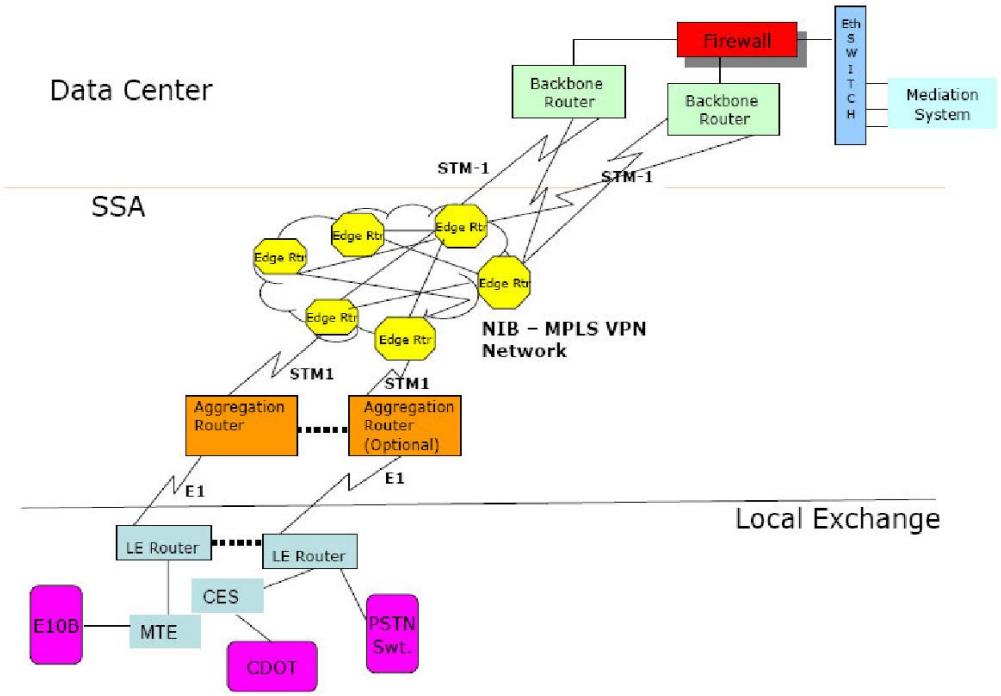


Figure 62: Network architecture of CDR

10.7 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, are connected using X.25 cards and Ethernet interface (wherever available).
- All CDOT exchanges are connected to the LE router using CES equipment supplied by CDOT through HCL.

- All E10B exchanges have been 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 is connected over STM-1 link to the nearest MPLS node.
- For redundancy purposes, the connectivity is 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 has been enhanced to 1 GBPS link, later.
- Thus, each exchange is connected to the Data Centre over E1 end links and through the MPLS network.

10.8 CDR PROJECT CONNECTIVITY TO TERMINALS

- The existing CSR network has been connected to the Aggregation Router.
- Thus, all the terminals of Commercial, TRA, FRS and Directory Enquiry which were connected to the local systems earlier, have been connected to the Data Centre through the Aggregation Router.
- The project envisages –

i. Establishment of new network for collection of CDR from the exchanges,
ii. Usage of existing CSR network, with addition of a few CSR, if necessary,
iii. And re-utilization of existing PCs in the network.

10.9 CDR PROJECT IVRS AND INTEGRATION WITH CALL CENTRES

This project has centralized IVRS (in each zone), CTI (Computer Telephony Interface), IP EPABX, etc.The core equipment required for Call Centre operations is installed at the Data Centres. The existing Call Centres, mostly one per each Circle, have been connected to the Data Centres. The 1500 calls and the 198 calls are being routed to this IVRS. Depending upon the Number or the CLI, the calls are being routed through the IP network to the respective Call Centres. IP phones are provided to each Circle as part of this project. The Call Centre Agents have one IP phone and a PC connected over an IP network to the Data Centre. The customer data is displayed on the screen of the computer and the IP phone provides the voice communications with the customer. This is how the existing Call Centres have been integrated with the Data Centres.

10.10 SOFTWARE COMPONENTS OF CDR PROJECT

i. CRM (including FRS)
ii. Billing
iii. Accounting
iv. Mediation
v. Provisioning
vi. Web Self Care (WSC)
vii. Bill formatter
viii. Revenue Assurance (RA)
ix. Inventory management, which takes care of customer inventory such as MDF

Particulars, Piller, DP particulars, etc.

x. Directory enquiry
xi. Inter Operator Billing and Accounting system (IOBAS)
xii. Fraud Management System (FMS)
xiii. Enterprise Management System (EMS)
xiv. Enterprise Application Interface (EAI)
xv. RDBMS

10.11 AFTER CDR PROJECT

- The introduction of this new project has eliminated the need of individual SSAs maintaining and operating TI systems for all the four functionalities, i.e. Commercial, TRA, FRS and DQ.
- The SSAs are now the end-users of the systems and have better tools and software at their disposal to provide better customer services.
- The database related jobs are now with the IT team at the Data Centres.

10.12 CHANGES IN BUSINESS PROCESSING DUE TO IMPLEMENTATION OF CDR PROJECT

Because of the introduction of new systems and to take advantage of the features of the system, some Business processes have been changed within BSNL for CDR project implementation

1) Revenue Accounting:
2) Surcharge/Late Fee
3) PCO Billing
4) Deposits
5) Billing Cycles
6) CDR based billing

10.12.1 **Revenue Accounting**

1) In the new system Balance brought forward accounting method is 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.
2) Every customer is identified by an Account Number, which is unique throughout the country.
3) Revenue booking is based on the Account even though the services under the account are scattered across the various SSAs.
4) The customers can pay any amount at any time and it shall be credited to the account and adjusted against the outstanding

10.12.2 **Surcharge/Late Fee**

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

10.12.3 **PCO Billing**

1) For PCO billing, the commission payable and the minimum guarantee is as per the billing cycle instead of on a monthly basis.
2) PCO operators are eligible for discounts instead of commission.
3) These changes have been done in the existing systems and are continued in the new system.

10.12.4 **Deposits**

1) Deposits are already made uniform and are common for all the Plans.
2) Offering any OYT or TATKAL deposits/schemes have been discontinued.
3) The existing OYT subscribers are continued to be billed till the completion of 20 years.
4) However, no new OYT connection is being provided after the introduction of CDR system.

10.12.5 **Billing Cycles**

1) The number of billing cycles in an SSA has increased. The new system has centralized billing process common for all the SSAs in a zone.
2) Therefore, the customers in the entire zone have been divided into different billing cycles to evenly distribute the process load on the servers.
3) The number of billing cycles have even gone up to 15 as the project has been rolled out in all the SSAs.

10.12.6 **Cdr Based Billing**

1) The previously existing tariff, which is based on MCUs and number of calls, has migrated to MOU (Minutes of Usage) based system.
2) The discounts can be given not in terms of Free Calls, but are in terms of Free Talk Time given as Minutes per month or Rupees per month.
3) Though the system offers a lot of flexibility in configuring different Plans, BSNL in turn is following certain discipline in offering various Plans to the customers.
4) Circle Office team has been authorized to configure the plans as per business requirements and SSAs may not be able to configure new Plans on their own but can get it done through the Circle Office team.
5) Each Plan is identified by a Plan Code in the system.
6) This discipline is helping the organization in monitoring the launch of tariff Plans across the country and it is helping BSNL to take correct business decisions.

10.12.7 **What The Ssas Have Done In Preparing & Migrating To The Cdr Project**

1) Provided connectivity of exchange routers to MPLS VPN.
2) Each exchange has been connected through one E1 link to the Aggregation Router.
3) A redundant (second) E1 link has been connected to the second Aggregation Router.
4) Connectivity of Aggregation Router of SSA has been done with two of the nearest MPLS nodes through STM-1 links
5) Connecting the previously existing CSR network has been done to the Aggregation Router of the SSA.
6) Have Provided Transmission media to all these connectivity in coordination with the Telecom Region to get channel allocation and connectivity to the MPLS node.

7) Coordination with NIB (Data network Circle) for allotment of STM-1 ports at all the MPLS nodes.
8) Have performed Cleaning and preparation of the data in the existing systems for data migration – to follow the guidelines given already by DDG (TRF).
9) Have performed Reconciliation of data between switches and the billing systems.
10) All the numbers found working in the telecom switch have been reconciled with those working in the billing system also.
11) The number of disconnected/closed connections, have also been reconciled between the switch and the billing system.
12) All connections, which are closed, have been settled and accounts finalized and are not to be transferred to the new system.
13) Thorough review of outstanding have been done and fictitious outstanding and other outstanding have been written off as per the Corporate Office guidelines.
14) Deposits data have been verified and corrected in the previously existing system before data migration is done.
15) All the facilities like CLIP, STD, ISD, Call forwarding, etc., have been gathered for all the customers and were kept ready before data migration.
16) All the accessories being charged to the customers in the previously existing billing system were thoroughly verified.
17) FRS data for all the customers regarding MDF, Pillar, and DP have been gathered and was kept ready before migration.
18) To start with, it was important to collect the information regarding Localities and Sub-localities, Pillars and DPs. Mapping of the External plant inventory to the Locality and the JTO Outdoor was very important. Instructions issued in this regard by CGM IT have been followed.
19) All the new technology switches, CDOT and E10 B exchanges have been kept ready for CDR generation for 100% of calls.
20) The requirements of X.25 interface cards and cables have been projected to the Corporate Office, keeping IT Circle informed.
21) The up-gradation and procurement of PCs have been done on top priority.
22) SSAs ensured the availability of Bar Code Scanners at all online counters and availability of A4 page scanners for scanning the application forms.
23) All the Circles have reviewed the previously existing network and project requirement of network elements for the Rollout phase of this project to the IT circle.
24) All the SSAs were requested to watch the CDR Project link provided in the BSNL Intranet Portal for regular updates and information on the progress of this project.

10.13 CONCLUSION

CDR project has set up an entirely up-to-date convergent billing system in place for Landline and Broadband services. It has facilitated the customers and BSNL staff with all the latest features and functions to fully fetch and utilize the services. It has opened new channels of revenue collection and handling the customer with the knowledge of their complete profile.

11 CYBER AND IT SECURITY

11.1 LEARNING OBJECTIVES

This chapter covers the concept of IT and cyber security so that the candidate can identify, analyze and remediate computer security breaches by learning and implementing the real-world scenarios in Cyber Investigations , Network Security and in Security and Penetration Testing.

11.2 INTRODUCTION

In the age of Information Revolution, the management of information and its security is the key concern for all organizations and nations. For sharing of information among the intended users, the systems have to be networked. With networking, the risk of unauthorized use and attack has taken major attention of managers. Networks and Information are subject to various types of attacks, various products are available in the market for securing the systems. But it needs the thorough understanding of the various issues involved and proper implementation

11.2.1 **Definition Of Information And Information Security By ISO**

- Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected' [BS ISO 27002:2005]
- Information can be created, stored, destroyed, processed, transmitted or used; whatever forms the information takes or means by which it is shared or stored, it should always be appropriately protected. [BS ISO 27002:2005]
- Information security means to make the shared information always available to authenticate users without loss and assuring confidentiality. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Information security is concerned with the CIA (Confidentiality, Integrity and Availability) of data regardless of the form the data may take: electronic, print, or other forms.
- Preservation of CIA of information; in addition, other properties such as authenticity, accountability, non-repudiation & reliability can also be involved. [ISO/IEC 17799:2005]

11.2.2 **Why Information Security Is Important?**

Regulatory Compliance –

• IT (Amendment) Act 2008 and IT Act 2000

Security Risk Management

• Reducing exposures to technology threats

• Preventing computer-related frauds

• Enforce policies and improve audit capability

Reducing Operational Costs

• Reducing cost of unexpected security events

• Reducing losses from frauds and security failures

Consequences

- Loss of competitive advantage
- Service interruption
- Embarrassing media coverage
- Legal penalties

11.2.3 What Does Information Security Ensure?

Information Security has three Components - C, I and A.

- Confidentiality - Preventing disclosure of information to unauthorized individuals or systems
- Integrity - Data shall not be modified without authorization.
- Availability - Information must be available when it is needed

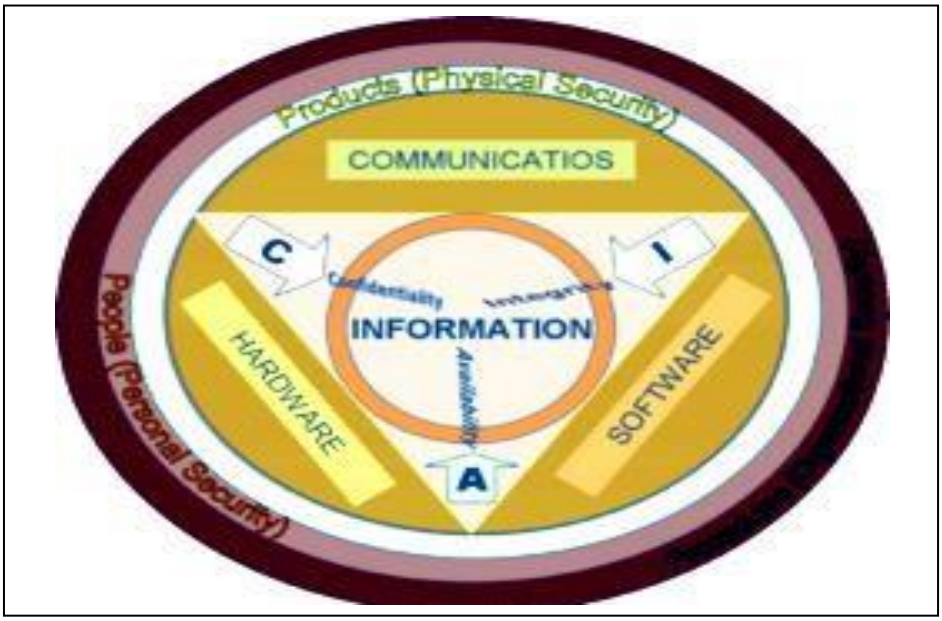


Figure 63: Information Security Areas

11.2.4 The Sources Of Information For Intruders

Intruder can hack your Information by using techniques such as:-

- Dumpster diving –Waste Baskets searching, Thrown papers, Scrapped Hard Disks
- Social Engineering- Talent hack, Help Desk persons ,Tech support persons Administrative support persons, Reception staff ,Retired Employees, Vendors Contractors, Partners etc may give out Information Knowingly or unknowingly.
- Information System- Electronically, Email Accounts (Default usernames and Passwords)
- Networked PC's (Using Virus activity) ,web pages(biodatas).

11.2.5 **What Are The Types Of Attacks On Information System?**

- Malicious Code Attacks
- Known Vulnerabilities
- Configuration Errors

11.2.6 **What Are The Indication Of Infections?**

- Poor System Performance
- Crashing of Applications
- Abnormal System Behavior
- Unknown Services are running
- Change in file extension or contents
- Automatic shutdown of System
- System Not Shutting Down
- Hard Disk is Busy.

11.2.7 **Why Systems Become Vulnerable To Attack?**

Information System Becomes Vulnerable to attack due to following reasons

- Use of Default User Accounts and Password
- Remote Access Not Disabled
- Logging and Audit Disabled
- No proper Access Controls on Files
- Non Availability of Updated Antivirus and Firewall
- Unnecessary Services running.

11.2.8 **How To Achieve Security By Monitoring?**

A lot can be observed by just watching & paying attention to what you can see & measure

- Monitor for any changes in Configuration of 'High risk' Devices
- Monitor Failed Login Attempts, Unusual Traffic, Changes to the Firewall, Access Grants to Firewall, Connection setups through Firewalls
- Monitor Server Logs.

11.3 AT WHICH LEVELS THE SECURITY NEEDS TO BE IMPLEMENTED?

OS/NOS LEVEL

- Keep OS Updated with Service packs (OS Release)

- Install Security Patches for OS
- Install up-to-date Antivirus Software
- Disable remote access
- Harden OS by turning off unnecessary Services and features.

11.3.1 **Application Levels**

- Keep Application Package Updated
- Install Security patches for Application Packages
- Do not Install Programs of unknown origin
- Take precautions while using emails
- Secure web Browsers.

11.3.2 **RDBMS Level**

- User Management
- Managing Allocation of Resources to Users
- Password Policy
- Backup and Recovery
- Auditing

11.3.3 **Network Level**

- Use of Firewalls to Monitor and control Network Traffic.
- Monitor for any changes in Configuration of 'High risk' Devices eg firewalls.
- Monitor Failed Login Attempts
- Monitor Server Logs

11.4 CYBER SECURITY

In the cyber world, the current state of the practice regarding the technical ability to track and trace Internet-based attacks is primitive at best. Sophisticated attacks can be almost impossible to trace to their true source using current practices. The anonymity enjoyed by today's cyber attackers poses a grave threat to the global information society, the progress of an information based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavor.

The domestic and international implication of an increasingly critical societal dependence on the Internet makes necessary the ability to deter, or otherwise minimize, the effects of cyber-attacks.

11.4.1 **What Is Cyberspace**

It is an electronic world created by interconnected networks of information technology and the information on those networks.

11.4.2 What Is Cyber Security

Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

11.4.3 Cyber Threats

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four: cyber espionage, cyber warfare, cyberterrorism, and cyber crime

1. **Cyber espionage:** Intelligence gathering and data theft. Examples of this are Titan Rain and Moonlight Maze.

2. **Cyber warfare:** It involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks.

3. **Cyber terrorism**: It is premeditated, politically motivated attack against information, computersystems, computer programs, and data which results in violence.

4. **Cybercrime:** It is any criminal activity that involves a computer, networked device or a network.

11.4.4 Information Technology Act, 2000

By understanding the growing demand and applications of Information Technology, the Government of India passed the bill of Information Technology in 2000, The Information Technology Act, 2000 or ITA, 2000 or IT Act, was notified on **October 17, 2000.** It is the law that deals with cybercrime and electronic commerce in India

The bill was **passed** in the budget session of 2000 and signed by President K. R. Narayanan on **9 June 2000.**

The original Act contained **94 sections**, divided into **13 chapters and 4 schedules**. The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law.

Amendments In Information Technology Act, 2000

A major amendment was made in **2008**. It introduced **Section 66A** which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".

Additionally, it introduced provisions addressing - **pornography, child porn, cyber terrorism and voyeurism**. The amendment was passed on **22 December 2008** without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on **5 February 2009**.

The major features of the act are:-

- It facilitates e-governance and e-commerce by providing equal legal treatment to

users.

- It made provision to accept electronic records and digital signature.
- It gave legal approval to electronic business transactions.
- The Act instructs banks to maintain electronic record and facilitate electronic fund transfer.
- It also sets up a Cyber Law Appellate Tribunal.

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to Rs.1,000,000

67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to Rs.1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to Rs.1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs.1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to Rs.100,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to Rs.100,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to Rs.100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to Rs.500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to Rs.100,000

74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to Rs.100,000

Table 8. List Of Offences And The Corresponding Penalties

11.4.5 Information Technology Rules, 2021

The Information Technology (**Intermediary Guidelines and Digital Media Ethics Code**) Rules, 2021 is secondary or subordinate legislation that suppresses India's Intermediary Guidelines Rules 2011. The 2021 rules have stemmed from section 87 of the Information Technology Act, 2000 and are a combination of the draft **Intermediaries Rules, 2018 and the OTT Regulation and Code of Ethics for Digital Media.**

The Central Government of India along with the Ministry of Electronics and Information Technology (MeitY) and the Ministry of Information and Broadcasting (MIB) have coordinated in the development of the rules.

Intermediaries had until 25 May 2021 to comply with the rules.

In the Monsoon session of the Parliament in 2018 a motion on "**Misuse of social media platforms and spreading of fake news**" was admitted. The Minister for Electronics and IT, accordingly made a detailed statement of the "**resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law**". MeitY then prepared the **draft Information Technology (Intermediary Guidelines) Rules 2018 to replace the 2011 rules**. The Information Technology Act, 2000 provided that intermediaries are protected liabilities in some cases.The draft 2018 Rules sought to elaborate the liabilities and responsibilities of the intermediaries in a better way. Further the draft Rules have been made "in order to prevent spreading of fake news, curb obscene information on the internet, prevent misuse of social-media platforms and to provide security to the users. The move followed a notice issued to WhatsApp in July 2018, warning it against helping to spread fake news and look on as a "**mute spectator**".

Structure of the Intermediary Rules

- Part I of the Intermediary Rules mainly lays down the definitions of terms.
- Part II deals with the regulation of intermediaries, including social media intermediaries. This part is administered by the Ministry of Electronics and Information Technology or MeitY.
- Part III deals with the regulation of digital news media (though there is a lack of clarity on exactly which news media these Rules apply to) and OTT platforms. Part III is administered by the Ministry of Information and Broadcasting.

11.4.6 Network Scenario

- LAN
- WAN
- INTERNET

- INTRANET
- Network Elements
- Communication Links
- Client – Server – Middleware, Workgroup, Cloud
- OS, Applications (Web based), Databases, Protocols
- Services

11.4.7 **Typical WAN Scenario**

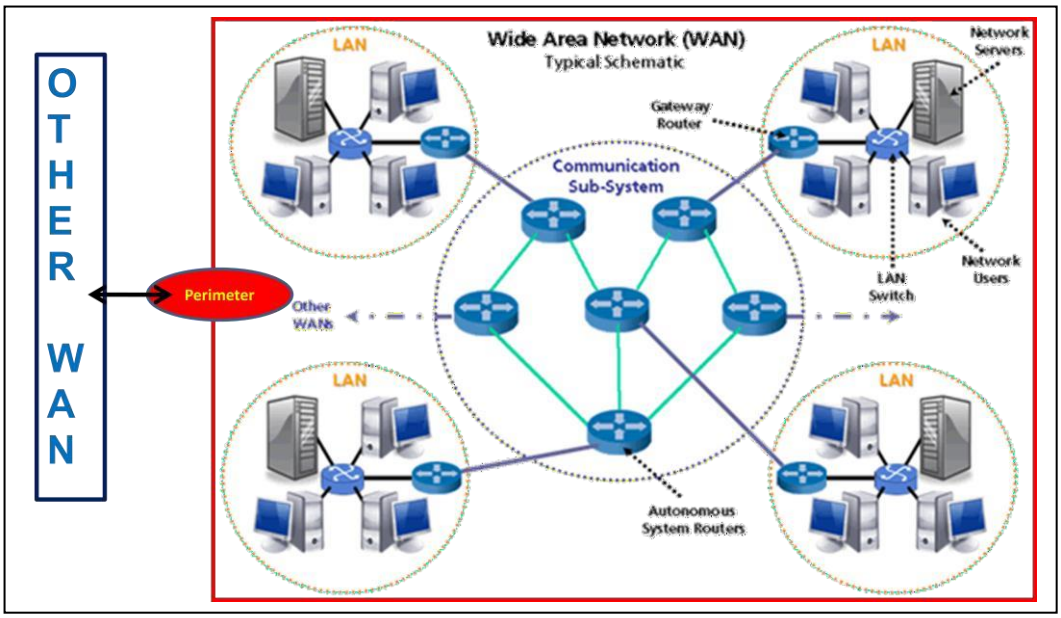


Figure 64: WAN Scenario

11.5 CYBER SECURITY

Cyber is a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. Anything related to the Internet also falls under the cyber category.

Cyber Security is defined as "the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the country, or that threatens public health or safety.

11.5.1 **Hacker**

- A hacker is a person able to exploit a system or gain unauthorized access through skill & tactics. There are black hat hacker, white hats (ethical hackers) & grey hats depending upon the capacity & goal of hacking involved.
- A hacker who breaks into your computer could

- Delete your files,
- Read your documents,
- View your passwords or crash your system.
- A hacker can do by using a Malware.

11.5.2 **Vulnerability**

- A vulnerability is weakness in Information Security system that could be exploited by a threat; that is a weakness in Network System components, Network security process & procedures. The common types of vulnerabilities errors in design, configuration of Network System components, Communication Links, OS, Applications (Web based), Databases, Protocols, Services etc.
- The widespread use of many COTS (commercial off-the-shelf) products means that once a vulnerability is discovered, it can be exploited by attackers who target many of the thousands or even millions of systems that have the vulnerable product installed.
- A lack of security expertise by most Internet users means that vendor security patches to remove the vulnerabilities will not be applied promptly.

11.5.3 **Various Security Threats**

High profile virus attacks in the recent past have forced a few businesses to shut down connections to the Internet. New viruses and malicious code are used to commit cybercrime and criminal acts. It pays to be aware of the various security threats.

- Viruses
- Worms
- Trojan Horses
- Spam

Location Of Defense

- Perimeter Defense
- Host Defense
- Application & Data Server Defense

11.5.4 **Internet Attacks**

- Figure shows that although the sophistication of Internet attacks has increased over time, the technical knowledge of the average attacker is declining, in the same manner that the technical knowledge of the average user has declined.
- Sophisticated attackers routinely build attack scripts and toolkits that the novice attacker can use with the click of mouse, with devastating effects.
- Hiding the tracks of the attacker and expunging or concealing any related evidence is an integral part of many attacker toolkits today.

11.5.5 **Security Process & Tools**

- Spoofing

- Phishing
- Denial of Services
- Spyware
- Keylogger
- Zombie computer
- Information Disclosure
- Elevation of Privilege

11.6 VIRUSES

What is Virus

A virus is a small piece of software (code) that piggybacks on real programs, O.S. or e-mails. Each time a program runs the virus gets Executed.

11.6.1 Type Of Viruses

- Executable Viruses
- Boot sector viruses
- E-mail viruses

How Virus works?

- **Executable Viruses**

Traditional Viruses

- pieces of code attached to a legitimate program
- run when the legitimate program gets executed
- loads itself into memory & looks around to see if it can find any other programs on disk

- **E-mail Viruses**

- Moves around in e-mail messages
- Replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book
- Example: Melissa virus etc.
- Some e-mail viruses don't even require a double-click, they launch when you view the infected message in the preview pane of your e-mail software

- **Macro Viruses**

- Infect programming environments rather than OS or files.
- Almost any application that has it's own macro programming environment
- MS Office (Word, Excel, Access…)
- Visual Basic
- Application loads a file containing macro and executes the macro upon loading or runs it based on some application based trigger.

- Melissa was really successful macro virus
- Usually spread as an e-mail attachment

- **Most Damaging Viruses**

- Melissa Virus
- Estimated financial damage-300 to 600 million dollars
- Affected 15-20% of all business PCs
- Spread via email

11.6.2 **Computer Worms**

Network Worms are self-replicating programs which spread all over the Internet at a very fast rate. They cause a huge bandwidth drain while propagating and sometimes bring even large networks down to their knees.

Worms are hated because:

- Bandwidth consumption
- Might crash computers they infect
- Infected computers may be used for other attacks such as DDoS, Phishing attacks etc

Difference between Worm & Virus

- They differ in the method of attachment; rather than attaching to a file like a virus a worm copies itself across the network without attachment.
- All copies have the same functionality and generally lack any sort of synchronization among themselves
- Infects the environment rather than specific objects
- Morris Worm, WANK, CHRISTMA EXEC

The life cycle of a simple worm

- Scanning for a victim (Scan IP)
- Exploiting the victim (a piece of code which provides ―access‖ by utilizing some flaw on the victim computer)
- Cloning itself onto the victim (copy of itself on the victim PC as FTP / HTTP server)
- Running the clone to further spread infection (Make it a service, Add a registry entry, Clone starts spreading infection further)
- Stealth techniques used to hide itself (Hide process / Files / activities / logs

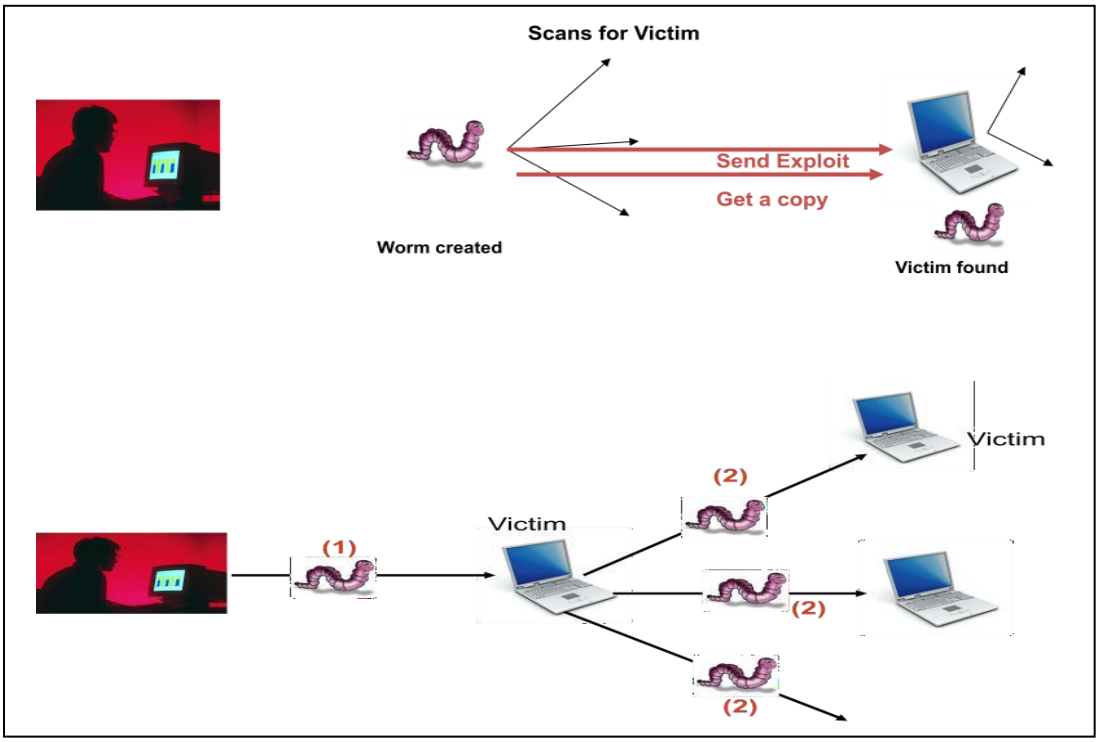


Figure 65: Life Cycle of a WORM

11.6.3 **Trojan Horses**

Trojan horses are dangerous programs that hide within other seemingly harmless programs.

- Once they're installed, the program will infect other files throughout your system and potentially wreak havoc on your computer.
- They can even send important information from your computer over the Internet to virus developer.
- The developer can control your computer, slowing your system's activity or causing your machine to crash.
- Used to remotely control windows
- Categorized as RAT(Remote Administration tool)
- Used for stealing credit card information
- Works on most of the operating systems
- Worms and Trojan horses are actually more common today than viruses.
- Antivirus programs offer protection against all viruses, worms, and Trojans Refer to all of these types of malware as viruses.

11.6.4 **Zombie Computer**

DENIAL OF SERVICE (DOS)

- Intruders launch a Denial of Service (DoS) attack to overload or halt network services such as web or file servers. Such attacks deny authorized access to resources and delay critical operations.
- Sometimes a cracker uses a network of zombie computers to sabotage a specific Web site or server. A cracker tells all the computers on his botnet to contact a specific server or Web site repeatedly. The sudden increase in traffic can cause the site to load very slowly for legitimate users. Sometimes the traffic is enough to shut the site down completely. We call this kind of an attack a Distributed Denial of Service (DDoS) attack.
- the cracker sends the command to initiate the attack to his zombie army. Each computer within the army sends an electronic connection request to an innocent computer called a reflector. When the reflector receives the request, it looks like it originates not from the zombies, but from the ultimate victim of the attack. The reflectors send information to the victim system and eventually the system's performance suffers or it shuts down completely as it is inundated with multiple unsolicited responses from several computers at once.
- From the perspective of the victim, it looks like the reflectors attacked the system. From the perspective of the reflectors, it seems like the victimized system requested the packets. The zombie computers remain hidden, and even more out of sight is the cracker himself.
- The list of DDoS attack victims includes some pretty major names. Microsoft suffered an attack from a DDoS called MyDoom. Crackers have targeted other major Internet players like Amazon, CNN, Yahoo and eBay.

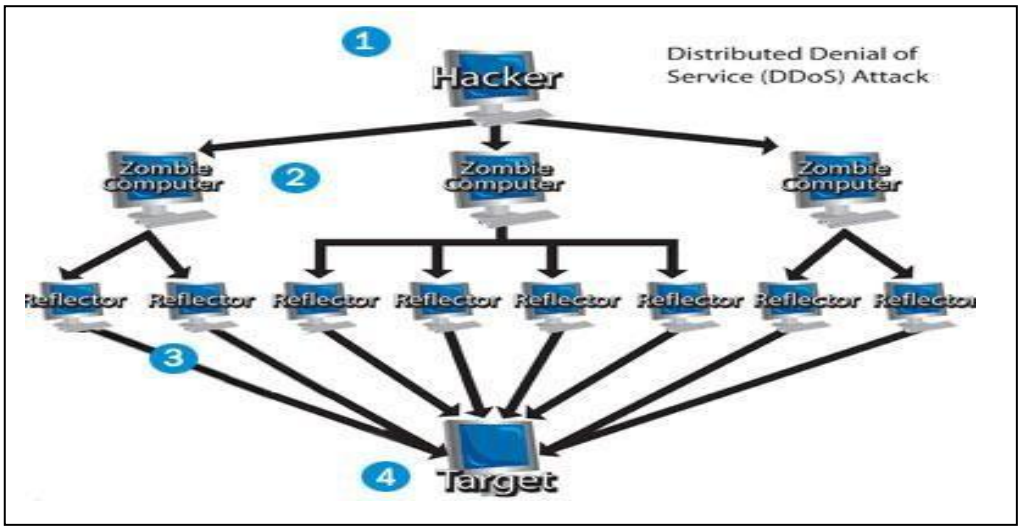


Figure 66: Denial of Service Attack

11.6.5 **Spams**

- Unsolicited bulk e-mail message that are commercial such as an advertisement or noncommercial such as chain letters or jokes, is called spam. Spam is usually a vehicle for virus.
- If you would like to send a lot of spam, then there are a number of companies set up to

send "bulk e-mail." The largest of these companies are able to send billions of spam e-mail messages a day.

11.6.6 **Spoofing**

- There are two main types of spoofing
- IP spoofing and
- e-mail spoofing.
- IP spoofing is largely a security exploit—here, the intruder sends data packets that display an IP address different than that of the intruder. Thus, if the packets appear to originate from a computer on the local network, the spoofed IP packet passes through the firewall security without any trouble. This technique is used primarily in one-way attacks such as Denial of Service (DoS) attacks.
- In e-mail spoofing, the e-mail message is forged so that the true address of the sender is not indicated. Hoax e-mails on security updates bearing a fake Microsoft e-mail address were sent to several e-mail users.
- Industry leaders, including Microsoft, have now co-developed a technology called the Sender ID Framework (SIDF) to counter e-mail spoofing and phishing. SIDF validates messages that originate from the mail servers they claim to come from

11.6.7 **Phishing**

- Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- Mostly carried over on email or IMs This technique, largely used by hackers, fraudulently acquires sensitive information posted on the Internet.
- Typically, an attacker sends an e-mail message that seems it has originated from a legitimate Internet address. On occasions, the message includes a hyperlink to websites that seemingly belong to legitimate enterprises. The content on such web pages then request you to verify your personal information or account details. For example, you may receive an e-mail from your bank requesting you to click a hyperlink in the e-mail and verify your online banking information.

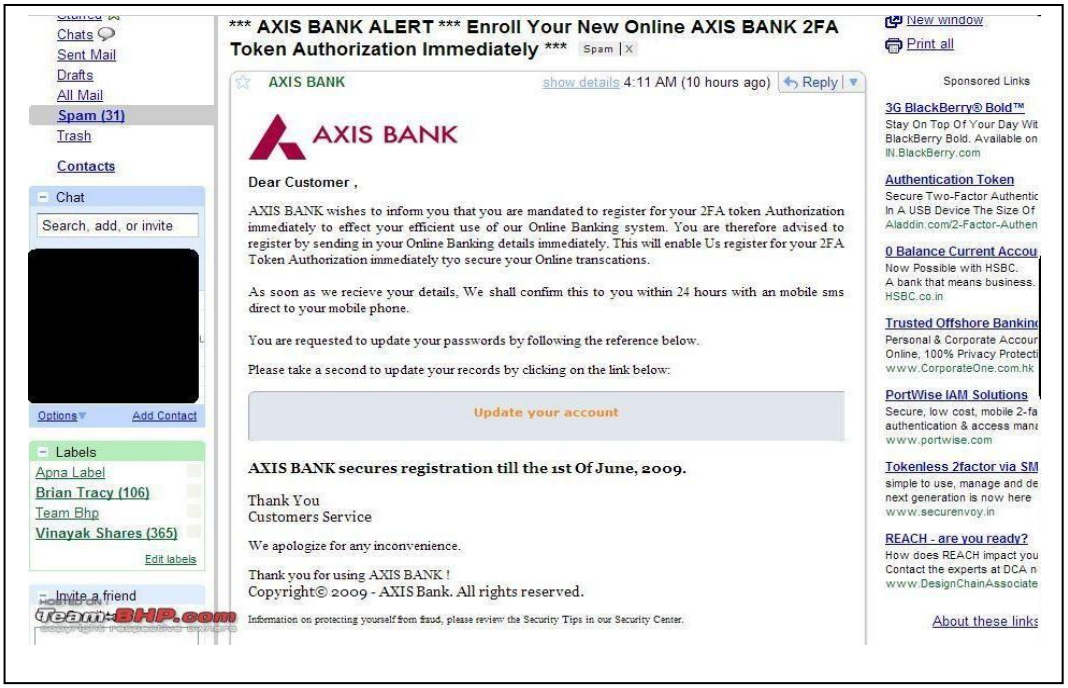


Figure 67: Phishing

11.6.8 **Spyware**

A program that covertly gathers information about your online activities without your knowledge, is called Spyware. Spyware usually enters the computer while downloading or installing a new program and allows intruders to monitor and access your computer.

Spyware differs from viruses and worms in that it does not usually self- replicate. However, spyware – by design – exploits infected computers for commercial gain. Typical tactics furthering this goal include:

- delivery of unsolicited pop-up advertisements;
- theft of personal information (including financial information such as credit card numbers);
- monitoring of Web-browsing activity for marketing purposes; or
- routing of HTTP requests to advertising sites.

11.6.9 **Key Logger**

Key logger surveillance software has the capability to record keystroke/captures Screen Shots and save it to a log file (usually encrypted) for future use. Captures every key pressed on the computer viewed by the unauthorized user. Key logger software can record instant messages, e-mail and any information you type at any time on your keyboard. The log file created by the key logger can then be saved to a specific location or mailed to the concerned person. The software will also record any e-mail address you use and Website URLs visited by you.

11.6.10 **Elevation Of Privilege**

Elevation of privilege is a process by which a user obtains a higher level of privilege than that for which he has been authorized. An intruder may mislead a system into granting unauthorized rights in order to compromise or destroy the system. For example, an attacker might use a guest account to log on to a network, detect a flaw in the software so that the guest privileges can be changed to administrative privileges.

"Elevation of privilege," then, is not a class of attack, as much as it is the process of any attack. Virtually all attacks attempt to do something the attacker is not privileged to do. The bad guy wants to somehow leverage whatever limited privilege he has, and turn it into higher ("elevated") privilege.

11.7 CONCLUSION

Securing our internet connection/access not only makes our valuable resources safe from unknown/unauthorized misuse, but also avoids social security related issues. Securing cyber space has a bearing on national security. Unsecured connections are liable to be misused by mischievous persons, anti-social elements and militants.

12 CPAN

12.1 LEARNING OBJECTIVES

After reading this unit, you should be able to understand:

- Limitation of circuit switched network signals.
- CPAN Technology.
- Network Architecture of CPAN.

12.2 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 interface for interconnection. Thus the volume of transport requirement for Ethernet Interfaces bas exponentially increased while requirement of TOM transport is rapidly vanishing. The network transportation requirement has clearly shifted from TOM with smaller portion of Packet to almost l00o/o Packet transport. As we move in the era of Packet transport, utilizing TDM network 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 transport layer for efficient delivery of services.

12.3 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 9. Packet Transport->Packet efficiency + Transport grade

12.4 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 the 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 these were not needed in Transport World and would simply the network. The features from MPLS that are not supported by MPLS-TP are:

a) MPLS Control Plane: MPLS-TP does not require LDP or any other control plane protocol to set up the circuits. Instead a user provisioned model is followed. The user can provision a circuit 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 of two 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 labels being used in the network. However it makes it impossible to

differentiate between traffic common from two different sources before the merging happened. To simplify things in transport networks, LSP merge was also disabled.

d) Equal Cost Multi Path: In traditional IP/MPLS networks different packets between a source-destination pair can take different paths. This is especially true when multiple equal cost paths exist. However this is in conflict with the concept of a circuit where all the traffic should follow the same path. Hence ECMP is disabled.

12.5 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.

12.6 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 Figure 1. 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 68, 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.

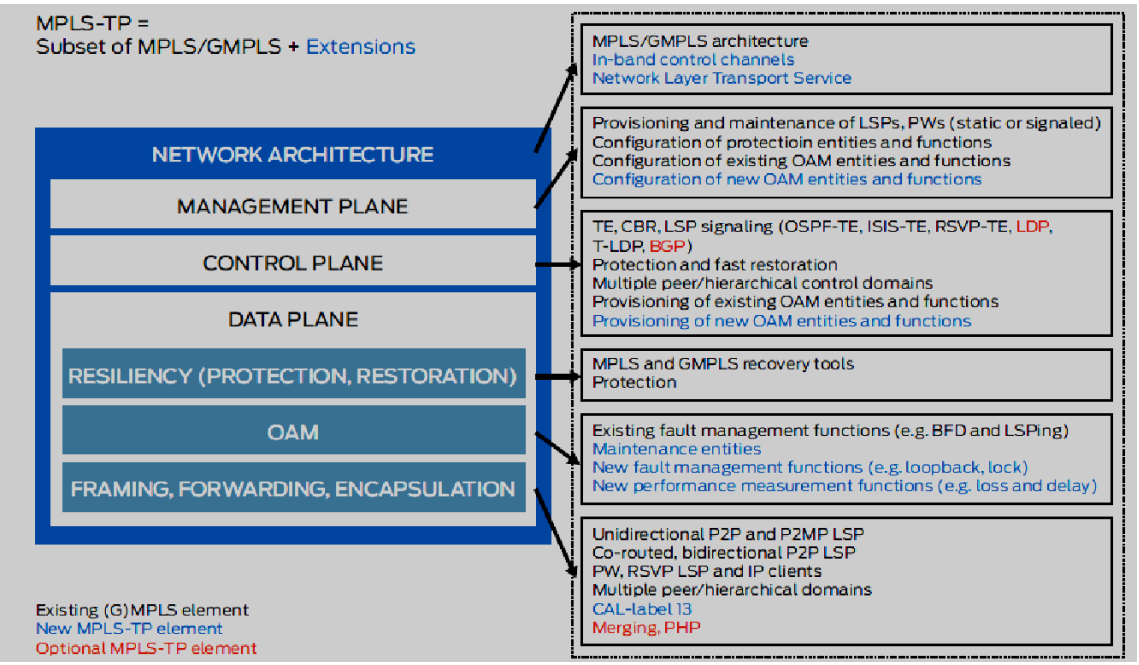


Figure 68: Components of MPLS and MPLS-TP

12.7 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 illustrates how IP/MPLS and MPLS-TP can be deployed together and are very complementary in nature.

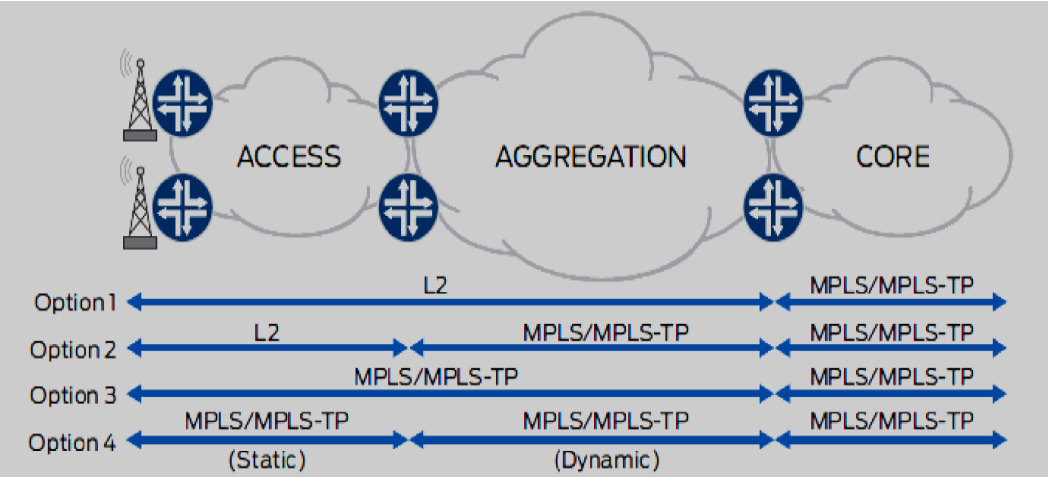


Figure 69: MPLS and MPLS-TP Deployment Options

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.

12.8 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) may be planned for transportation requirements in place of STM-1,16, 64 MADMs etc. wherever transport of packets is required. There is provision of carrying STM1 and E1 also in such devices.

12.8.1 **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.

12.8.2 **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)

12.8.3 **DISTANCE BETWEEN TWO NODES:-**

Type Al/A2 - 30 Km.

TypeBl/B2	-	50 Km.
Type C	-	50 Km.

12.8.4 **POWER SUPPLY:-**

Type Al /A2- AC Type or DC Type.

Type Bl /B2- DC Type.

Type C- DC Type.

12.9 TYPICAL NETWORK TOPOLOGY FOR MPLS-TP NODES

- Co-located network elements connected directly while the traffic between non co-located ones is transported through 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.

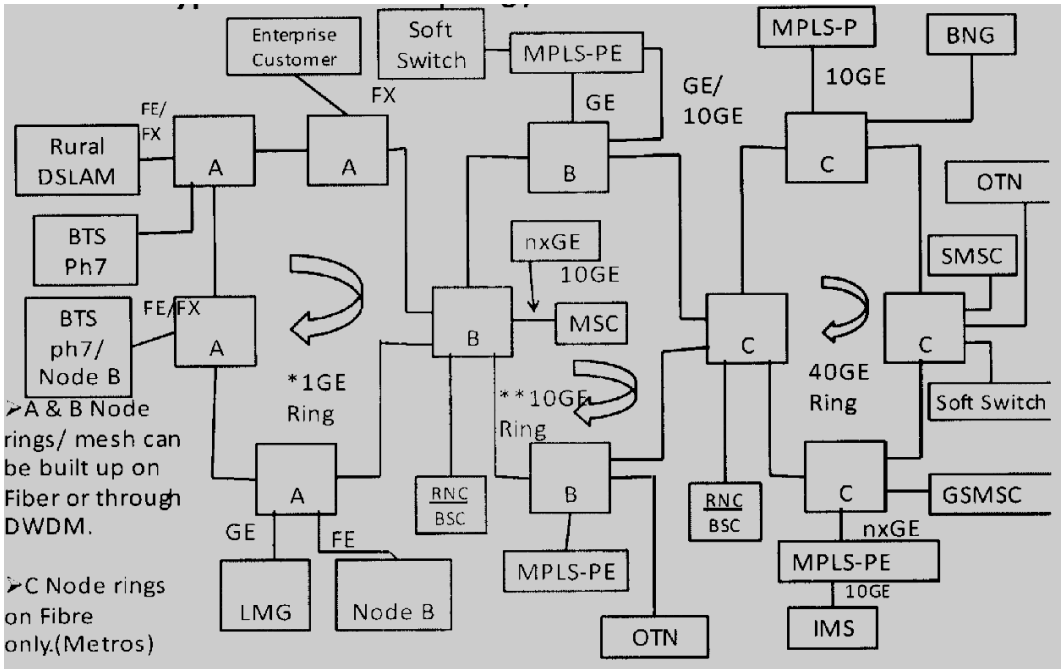


Figure 70: Typical Network Topology for MPLS-TP Nodes

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 the 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.

12.10 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.

13 SSTP ARCHITECTURE AND NETWORK

13.1 LEARNING OBJECTIVES

- Different nodes in signaling networks.
- Role of SSTP.
- Functions of SSTP.
- SSTP deployment in BSNL.

13.2 INTRODUCTION

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.

13.3 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.SS7 Common Channel Signaling Networks depicts the makeup and connectivity of SS7 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.

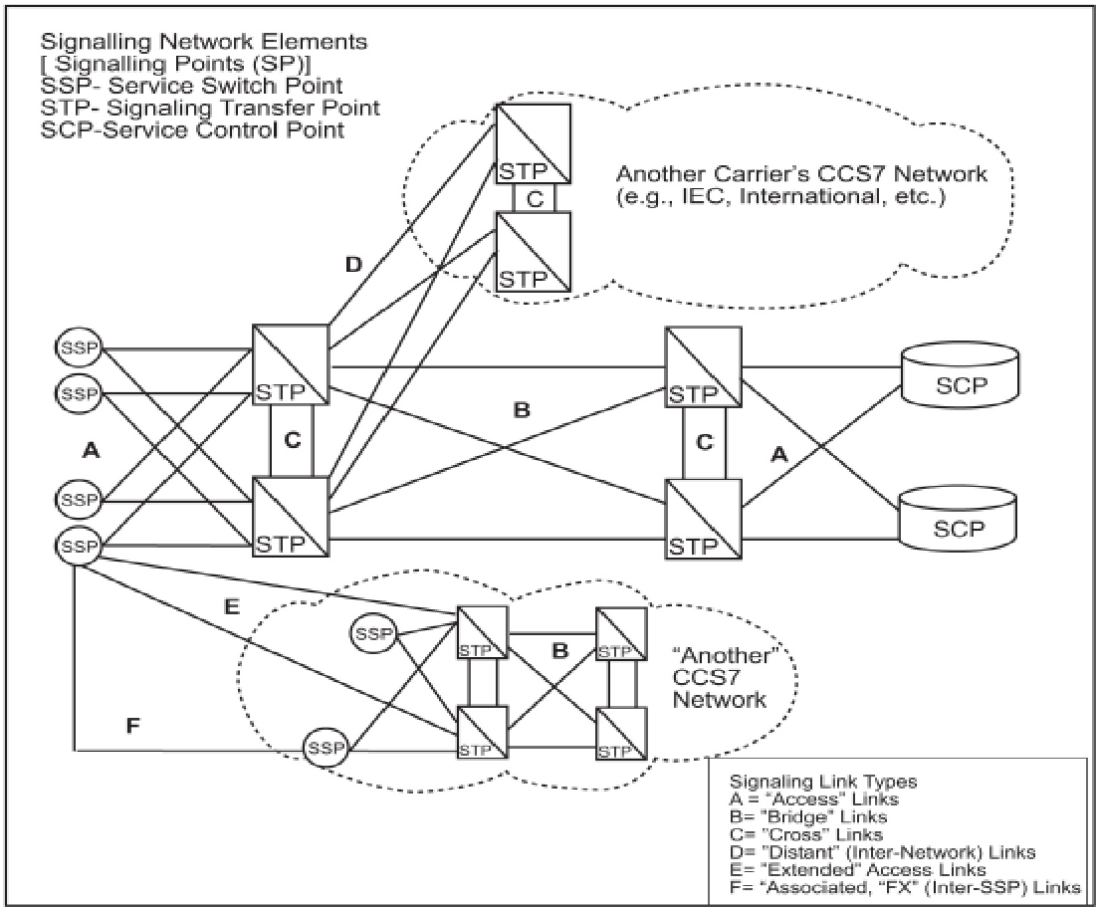


Figure 71: Common Channel Signaling Networks

13.3.1 **Service Switching Point (SSP)**

The SSPs are the legacy switches of the telecommunications network. SSPs are referred to as an "*End Office switch*", "*Central Officeswitch*", "Toll Tandem switch", etc. The central offices that house the SSP are identified by classes of ranging from a class 5-lowet, 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:

Call Processing function

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

Query Processing

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

SS7 Response Processing

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

Resource Interface

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

13.3.2 **Service Control Point (SCP)**

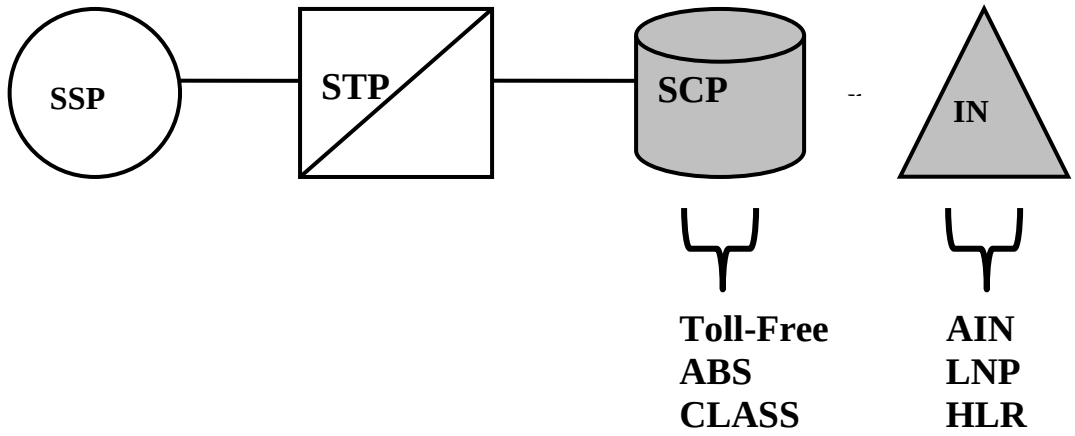


Figure 72: SCP Connectivity

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)

13.3.3 **Signaling Transfer Point (STP)**

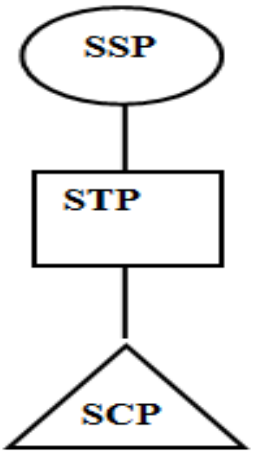


Figure 73: STP Connectivity

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.

STPs are generally deployed in pairs with mirrored databases. If one of the STPs are removed from service or signaling links fail, the mate can process all of the traffic that is typically shared by the mated pair. STP mated pairs are geographically separated , This helps ensure protection for message routing they perform if a natural disaster occur, etc.

STP two-level Architecture in CCS Network

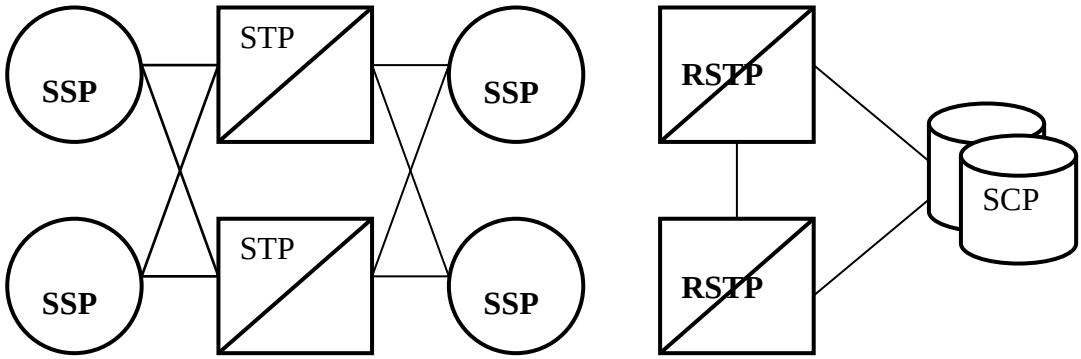


Figure 74: SSTP architecture

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.

13.4 SSTP FUNCTIONS

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

13.4.1 **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).

13.4.2 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 subsystem number SSN for delivery of the good database 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.

13.4.3 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.

13.4.4 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 functions: allow and block..

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

Objectives of SSTP's

Following were the main objectives:-

- Regulate, measure, and account for inter-network traffic including SMS messages from mobile networks including GSM and CDMA
- Achieve a flexibility and transparency in management of signalling for BSNL's wired and wireless networks.
- Optimal expansion of GSM & CDMA network of BSNL
- Introduction of new services.
- Offer CCS7 & IP Signaling Services to other Wire line & Wireless Network Operators.

13.5 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 PO no. 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 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.

13.6 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 consisting 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.

The chassis accommodate the same types of function boards that fall into the following six categories:

MPU Card (MPU1A):

This is the system main control board. It manages all hardware resources; provides a common, manageable and HA platform for the system. The MPU board in the chassis functions as a communication agent for the SNMS.

Line Card (PEM-S8):

It supports TDM-based MTP2 protocol and IP-based M2PA protocol; and implements reliable signaling link transmission between iSG6400 and SS7 devices. It also provides translation between SS7 common channel signaling and MTP3 messages.

CLOCK I/O board (PCU1A):

This provides the synchronization clock signal for E1/T1 trunks.

SPU (Signaling Processing Unit):

This is the signal processing equipment that provides SIGTRAN and SS7 signaling messages translation and distribution functionality. It supports MTP3, SCCP, and M3UA protocols.

Hardware Platform : X86 based Server

Both ISG6400 Chassis are active and active load sharing mode . Failure of any hardware module in one chassis does not impact any services. The LSL and HSL links from SSP are duplicated and to be connected to E1 ports on both chassis. LAN SW Pair works in Active –Active mode.

SPU (Signaling Processing Unit):

This software application runs are based on IBM servers. This is the signal processing equipment that provides SIGTRAN and SS7 signaling messages translation and distribution functionality. It supports MTP3, SCCP, and M3UA protocols.Two SPUs run on active – Active load sharing mode

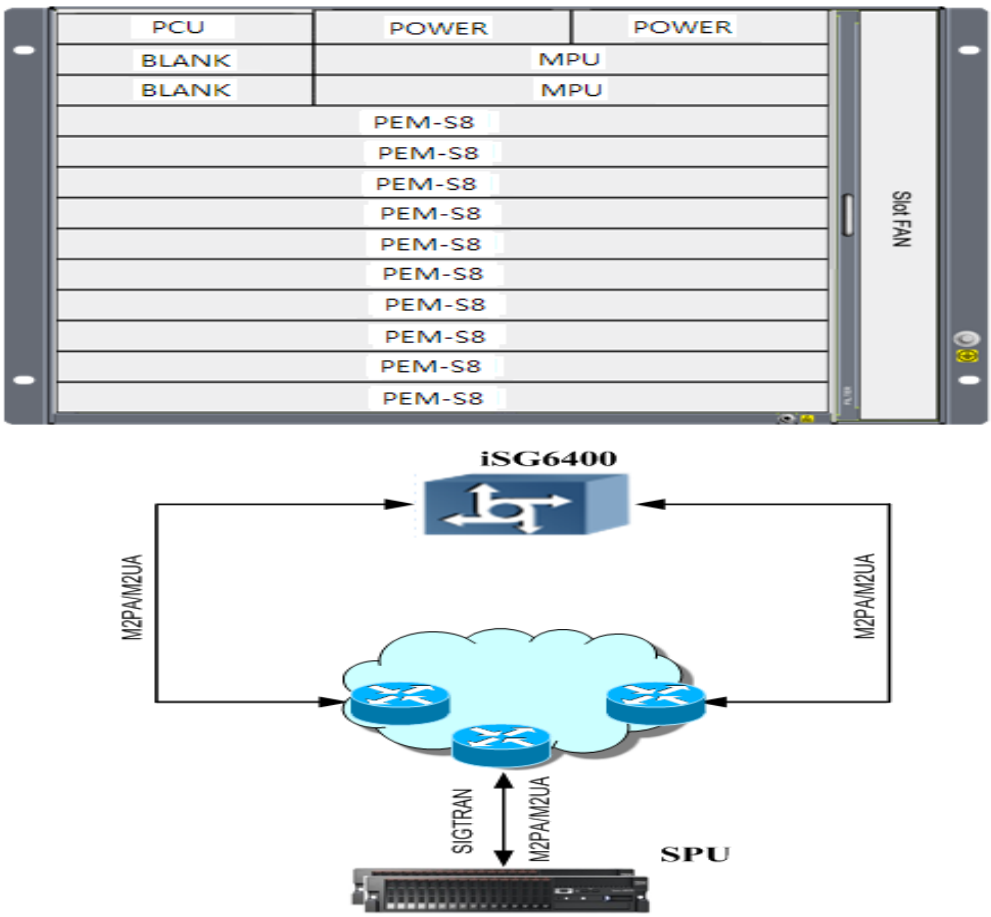


Figure 75: SSTP Hardware

Unique features of UTSTARCOM SSTP:

1. MNP capacity is 250M NP entries and can be further expanded
2. UT SSTP use 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 manage all the SSTP node which is 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.

13.7 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.

14 NGN ARCHITECTURE AND IMPLEMENTATION IN BSNL

14.1 LEARNING OBJECTIVES

- NGN – Vision and Definition.
- NGN Architecture.
- Protocols used in NGN.
- Migration from PSTN to NGN.
- NGN deployment in BSNL.

14.2 INTRODUCTION

Telecommunication industry is changing at a rapid pace. This change in the industry is basically driven by demand of new services from subscriber's side and urge to reduce CAPEX (Capital Expenditure) and OPEX (Operational Expenditure) from carrier side. Today All most all telecommunication giants are installing and maintaining at least three kinds of basic Network.

PSTN: Public Switch Telephone Network was basically developed and engineered for giving voice connectivity to the wire line subscribers. The network consists of Local exchange/RSU as a part of Access Network and TAXs as a part of core Network. Already huge amount of money has been invested in PSTN setup. Because of tough competition from Mobile & Voice over IP, it is becoming white elephant day by day for the operators. Another fact about PSTN is that most of its equipment are going to exhaust their lives in coming years.

PLMN: (Public Land Mobile Network): PLMN has been developed to provide voice services for wireless subscribers. Recent times SMS has emerged as killer application for mobile. PLMN includes BTS/BSC as access network and MSC as a core Network.

Data Network: This network was basically designed for accessing remote files and servers for defense people and universities but now a days nobody can think of living with data network services. The basic and most popular application of data networks is Internet. Other applications include E-commerce, online banking, online gaming, E- shopping, IPTV Video on demand and many more. Data network is an assembly of routers, which are responsible for forwarding information from one end to other.

The interesting fact about the current generation is that these networks have been developed during different time zones. That’s why they are separate network infrastructure. There is no sharing of infrastructure among them. However some gateways are available for inter network communication.

Another disadvantage of the current scenario is that all the three networks are having their own service platforms in other words services are tightly coupled with their networks because of that carrier or operators have to introduce service separately for separate networks. Because all the three networks are having separate access transport and switching network service provider has to invest in all the three networks separately.

Hence CAPEX increases on the other hand for maintenance of three different networks operational cost also increases. Manpower of the company has to have knowledge of multiple technologies.

14.3 NGN VISION

Next Generation Network is the framework where operator will have a common transport network based on Internet Protocol for providing all kinds of telecommunication services. Hence operators will have to install and maintain only a single network which will reduce its CAPEX and OPEX significantly. Moreover service provisioning will become easier because of the introduction of new and intelligent servers. NGN is able to provide Vendor independence because of the standard protocols it uses for interaction with network elements.

14.4 NGN DEFINITION

A Next Generation Network (NGN) is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.

14.4.1 **Generalized Mobility:**

At present subscribers are enjoying terminal mobility where network identification system is available in the form of SIM and the same is inserted in the terminal. If user is having that terminal he will be mobile with the identity of the SIM.

In NGN subscriber can have generalized mobility. Here, each individual will have its own network identity in the form of "SIPURL: xyz @ domain name.com". Users have to make registration from his devices against the given URL. Registrar servers of the company will maintain bindings with URL and physical location of registered devices. Users can register for more than one device at a time. With this subscribers need not to depend upon specific terminal. They can login with any device enabled with required protocols (SIP) and call will come to that device.

14.5 PSTN VERSUS NGN

- As shown in above figure PSTN Switch consists of interface, Switching and call control. All the functional entities are shown in one box that means they are interacting with each other using proprietary protocol. Where as in NGN model entities are interacting using standard protocols.
- In PSTN each node should have call control separately whereas NGN may have centralized call control.
- PSTN is dedicated network for providing voice services to the subscribers whereas NGN is developing with the idea of carrying all kind of traffic over it.
- PSTN is working on circuit switched principle whereas NGN is working on Packet switching.
- PSTN provides excellent quality of voice and it is tested in all conditions whereas NGN will provide good quality of voice and it is to be tested in adverse network conditions.

- In PSTN service integration is very difficult and because of vendor dependent. technologies, it is difficult to introduce services easily. Whereas NGN is able to provide separate service platform for introduction of services without depending upon underlying network related technologies.

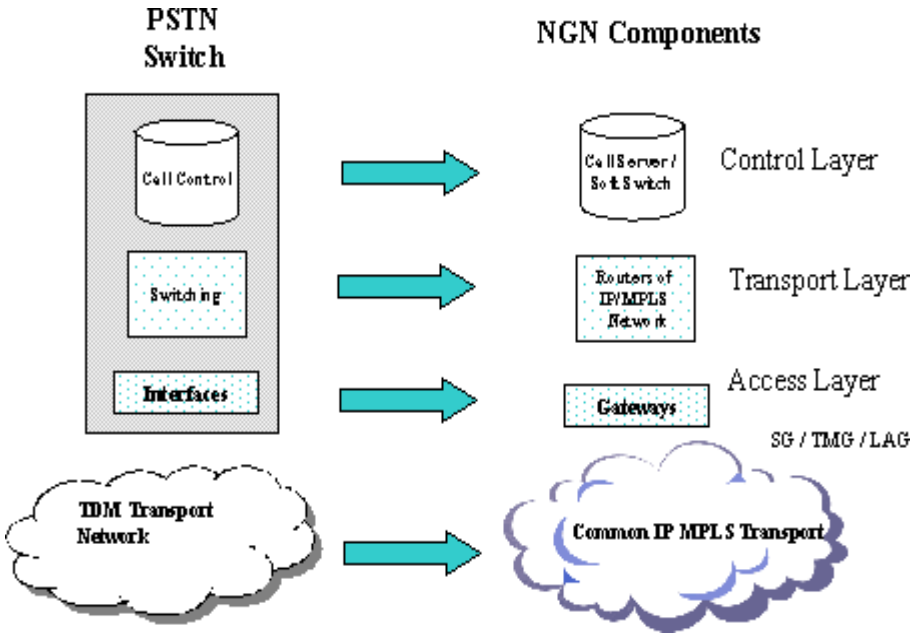


Figure 76: PSTN versus NGN

14.6 NGN ARCHITECTURE

NGN is a layered architecture consisting of transport, access, control and application layer. It is important to note that all the layers are independent from each other. Change in one layer should not affect other layers.

14.6.1 **Access Layer:**

Access Layers is responsible for direct subscriber attachment function. NGN can support all kind of existing access as well as upcoming access. NGN is capable of processing traffic originated from PSTN, GSM, CDMA, xDSL, WiMAX or any other access system. Depending upon the type of access, protocol conversion and/or media conversion may be required at the NGN Gateways.

Access Layer consists of Gateways. Example of getaways is Media Gateway, Access gateway. Signalling gateway etc. Media gateway terminates media, coming from PSTN/PLMN in E1 / STM. Here, it is responsible for packetisation of media under the instruction of control layer. After packetisation of information it throws packets to the transport Network. Access gateway is nearer to subscriber. Subscriber can directly be terminated in Access Gateway. All the required configuration of such subscribers should be done at control layer. Access Gateway and Media Gateways are responsible for carriage of Media whereas Signalling gateway is carrying signalling generated by PSTN and informs Control Layer about the signalling in required format.

14.6.2 **Transport Layer**

Transport Layer of NGN is based on IP (Internet Protocol). It can utilize the advantage of MPLS (Multi Protocol Label Switching). Transport Layer forms the core of the Network. It basically consists of Routers, which are responsible for carrying traffic originated by access layer. As the same core network is going to be used for all kinds of subscribers enjoying different kind of real time and non real time services, it should be able to make use of band width policies and Qos policies. Operator has to think of managed Network for its subscribers. It is basically an assembly of routers connected with optical network. Traffic coming from gateways is properly routed by those routers.

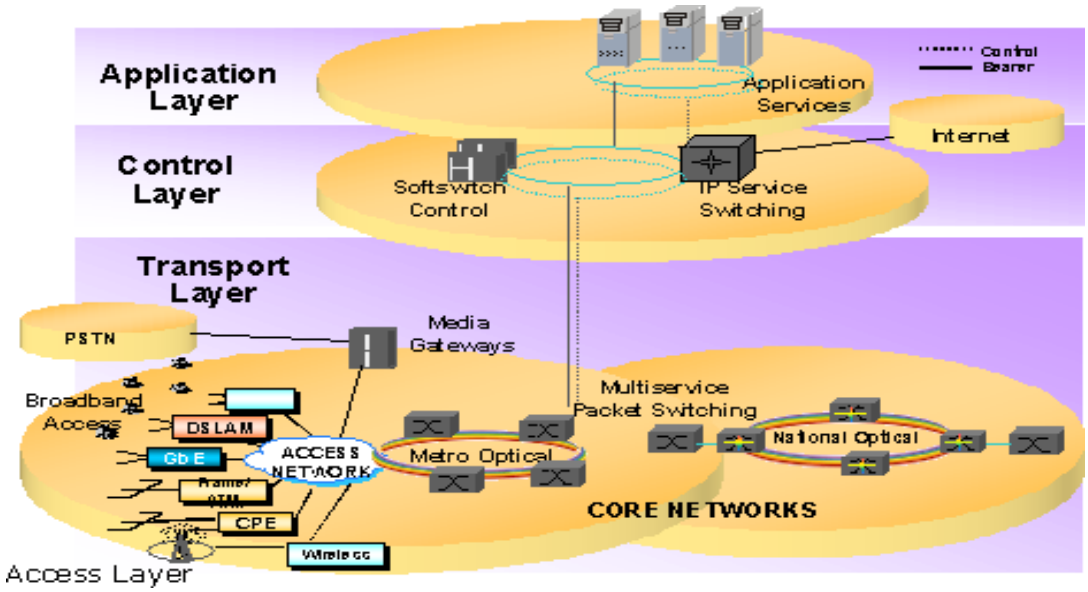


Figure 77: NGN Architecture

14.6.3 **Control Layer**

It is responsible of call setup, routing and charging policies and other controls in NGN environment. It consists of call servers where all information of the network resides. These call servers are responsible for setting up, modifying, charging and tear down of the calls. NGN may work on soft switch principle. It consists of MGC (Media Gateway Controller) as an overall controller and MGs(Media Gateway) for termination of traffic. MGC is basically a server and it is having all the necessary information of network MGC instructs MGs for establishing the call. Under the control of MGC, MG performs different call related tasks such as connection, modification and termination of media streams, packetisation of media etc.

14.6.4 **Application Layer**

It is responsible for OSS/BSS. Enhanced services to the subscribers will be provided with the help of application servers. It may include prepaid servers, announcement servers, Service servers etc. Hence NGN is making service separation from Network. Any service can be introduced with the help of server at any time without any modifications in the control, transport or access.

14.7 PROTOCOLS USED IN NGN NETWORK

The main feature of NGN architecture is separation of service, transport and control layers, which are interconnected by open interfaces and use standards protocols.

- **MEGACO**is a protocol which is sponsored from IETF and ITU. It is used inside one MGC (media gateway controller) for controlling media gateways (MG-s). This protocol allows the MGC to tell to the MG-s when to send and receive information towards/from different addresses. This protocol also is useful for sending all information to the MGC from MG-s regarding with detected events such is: on – hook, off hook etc. The equivalent protocol of MEGACO according to ITU is H248.

- **SIP**-Session Initiation protocol: is protocol that resides into application layer and is signaling protocol. SIP plays a very important role for session creation for audio/ videoconferences, interactive games and for call orientation towards IP network. SIP is IETF standard which supports traditional telephony services within IP domain such are: routing, identification, call establishment and other services.The job of SIP is limited to only the setup and control of sessions. SIP does not define the structure or content of message body. It is defined by other protocols like SDP(Session Description Protocol). The job of SIP is to carry that description upto destination.

- **SIGTRAN** Between Soft switch and Signalling gateway - sigtran suite of protocols :, shortened form of Signalling Transmission, is the standard for conversion, transport, and encapsulation of SS7 and ISDN over IP. It is one of the most important transition elements in moving from legacy TDM to **NGN** IP networks.

- **RTP**(Real Time Protocol) Between two media gateways for actual packet transfer-:It is a network protocol for delivering audio and video over IP networks. RTP is used in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications.

- **Real Time Control protocol (RTCP):** is a copy of RTP which offers control services. The main function of RTCP is identification of transport level for one RTP source.

14.8 MIGRATION FROM PSTN TO NGN

Migration from PSTN to NGN should be based on maximum possible reuse of existing equipment and replacement of components which are near the end-of-life.

Migration from PSTN to NGN involves:

- Replacement of TDM network elements in a phased manner
- Maximum reuse of existing resources
- Use of open and mature standards
- Convergence of access and backbone network
- Continuation of existing network capabilities and services with same or comparable QoS and security

- Interworking between different types of networks
- Addition of new services

It is true that NGN can provide operators, a better solution for their revenue models. But it is not possible for incumbent to replace their existing network overnight and install NGN. It will take time to migrate from PSTN to NGN. During that period of time both the networks will coexist. Operators have to follow some strategies to implement NGN in their network. Different phases for migration of PSTN to NGN are given below. However, the sequence of implementation depends on the business and strategic needs of a service provider. Different phases can be combined for implementation.

14.8.1 **Phase – I : Migration Of TAX**

In first phase of implementation operators can replace their transit network with softswitch architecture. Operators can make use of the SoftSwitch architecture for the National Long Distance calls.

In PSTN network Local Exchanges (LE) were connected with TAX for Long Distance Calls in turn TAX is connected with PSTN backbone which is carrying the traffic originated by subscribers of Local Exchanges. The setup of TAX and PSTN take care of signaling as well as voice media originated from LE subscribers.

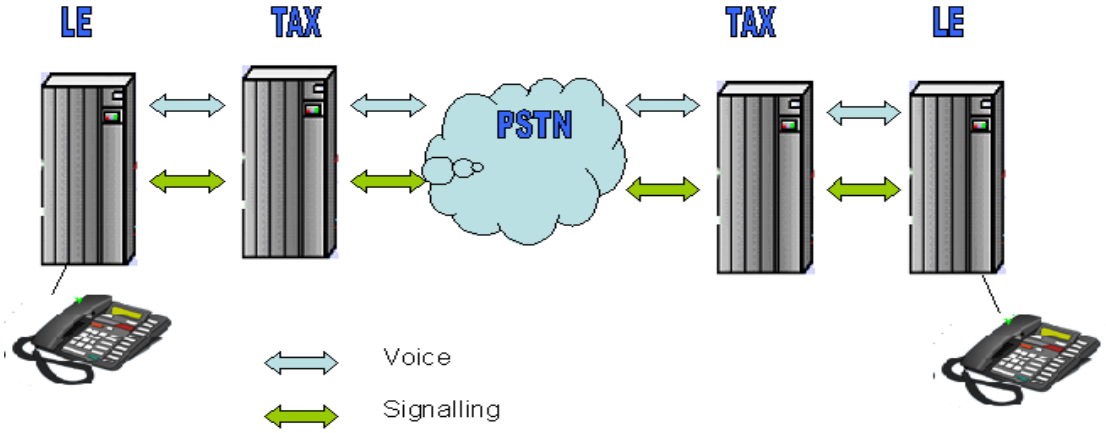


Figure 78: Setup of PSTN

In first phase of migration as discussed TAXs can be replaced by NGN components. This can be named as IPTAX in general. For that Local Exchanges have to be connected to Trunk Media Gateways for transportation of Media and will be connected to Signalling Gateway for signaling transport. Here Normal analog or ISDN subscriber dials the called party numberPSTN creates CCS#7 Signalling and sends it towards Signalling Gateway.Signalling Gateway converts CCS#7 messages to compatible SIGTRAN messages and sends it towards Media Gateway Controller or SoftSwitch.

After receiving signaling from SG, MGC instruct concerned originating and terminating media gateways to prepare connection for the desired call and at the same time through Signalling Gateway of destination PSTN side MGC / SS inform the destination

PSTN exchange about the call. When all the condition for the call is met, MGC instruct concerned originating and terminating media gateways for finally maturing the two communications. Both the MGs convert received TDM voice to packets using Real Time Protocol and vice versa. All the communication between MGC and MG is in H.248 protocol.The disconnection of the call is informed by the concerned SG to MGC/SS and then MGC/SS instructs both the MGs to disconnect the RTP link.

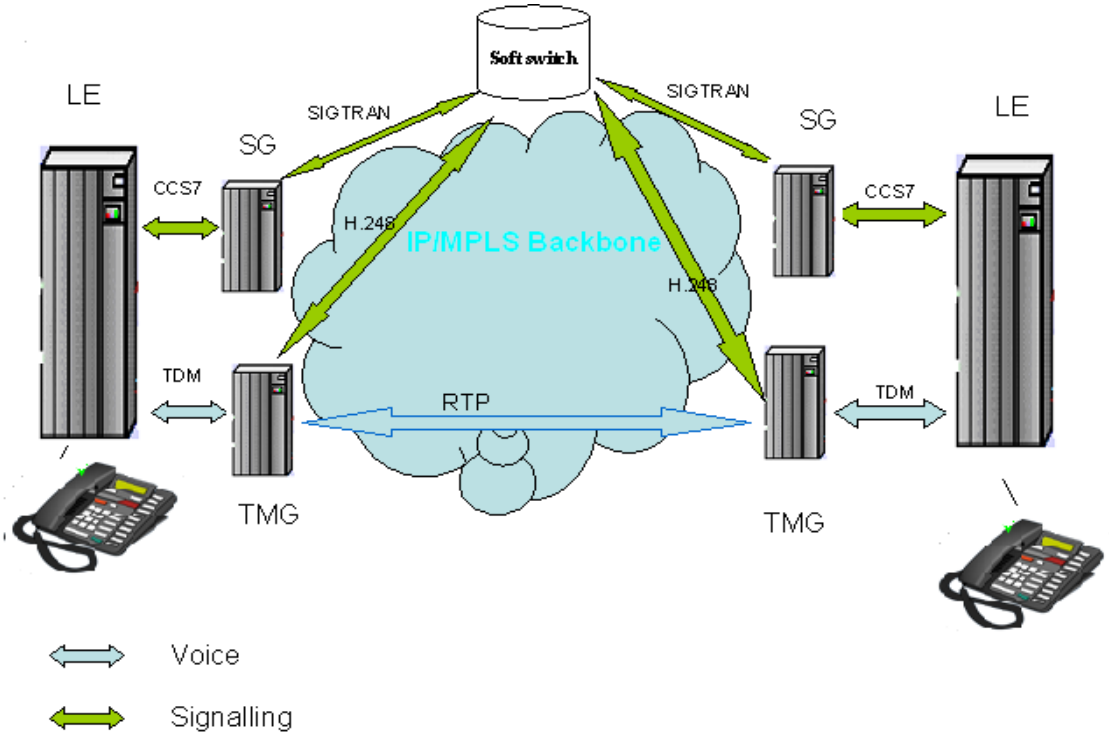


Figure 79: Phase I-Migration to NGN using TAX Replacement

14.8.2 **Phase II: Migration Of Local Exchanges**

In this phase Local Exchanges (LEs) are replaced by the Softswitch and Access Gateways (AGW) with same services. Softswitch with local features will be used as a common control element for class 5 applications. Access Gateways (AG) provide various types of access to the subscribers (e.g. PSTN, ISDN, V5.2, xDSL etc.) and connects them to IP core network. AGWs may be configured for various class 5 applications depending on end user topology, density, service requirements, etc. Depending upon the size of the network, a single softswitch with class 4 and class 5 applications may be planned.

In soft switch approach there are two types of NGN architecture: (i) Class -4 NGN Architecture (ii) Class -5 NGN Architecture.

The TAX exchanges are called class-4 switches and NGN based TAX is called Class-4 NGN Architecture. Similarly local exchange is called class-5 switch and NGN concept implemented in access network is called Class -5 NGN Architecture.

For migration the operators may first go for Class 4 NGN Architecture and then Class-5 NGN Architecture or some operators may follow reverse approach. BSNL has adopted the first approach and we have installed Class-4 NGN Architecture i.e. IPTAX.

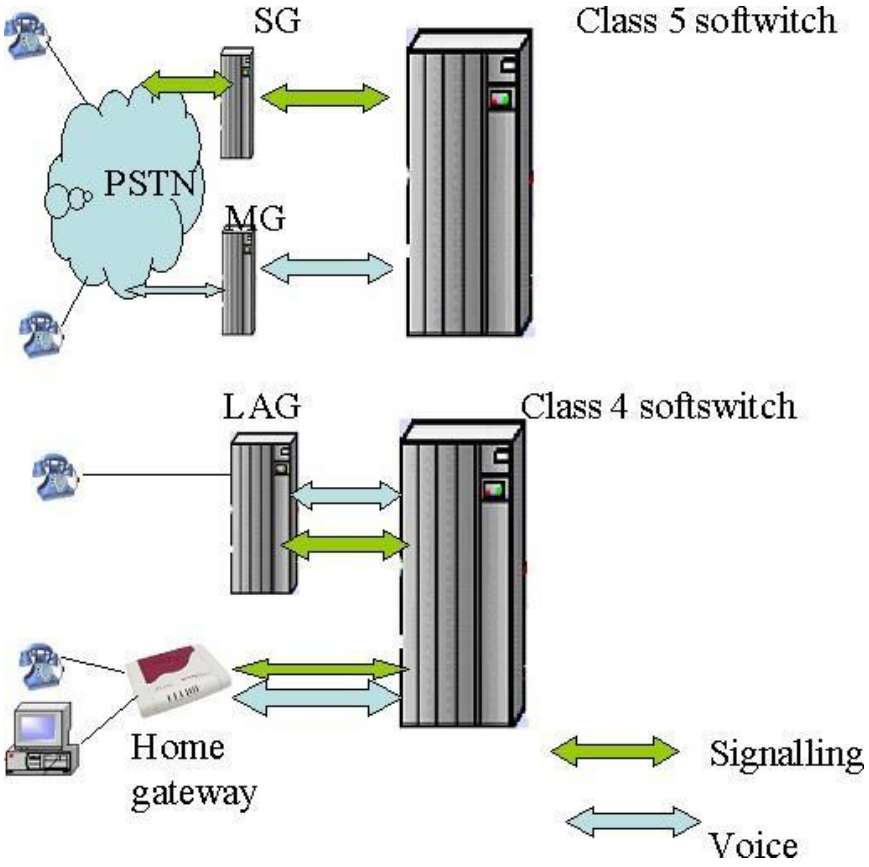


Figure 80: Phase II: Migration of Local Exchanges

14.8.3 **Phase – III Migration Of Services**

While migrating from PSTN to NGN, all PSTN services with same equipment, same look and feel should be provided. Two PSTN networks connected via NGN transit network should be able to provide transparency to all bearer services. The existing IN services are provided though SCP. The softswitch interacts with SCP through Signalling Gateways, using Intelligent Network Application Protocol (INAP). New IN and value- added services may be implemented using Application Servers (AS) which is accessed by softswitch via Session Initiation Protocol (SIP).

During the migration process new applications may be developed. These new applications along with existing IN services (including prepaid and number portability) is provided by Application Servers.

14.9 NGN DEPLOYMENT IN BSNL NETWORK

The strategy adopted by BSNL would be the overlay one as it has a huge base of circuit switched network that will coexist with packet switched network for a considerable period of time. The migration steps would be as follows :

- Introduce IP in Transit network at Level-1 TAX locations (IP TAX Project) - Class 4 NGN
- Extend IP network to Level-2 TAXs and large scale implementation in Access Network. – Class 5 NGN
- Develop MPLS core at Circle and LDCA Level.
- Offer Voice and Multimedia services to Broadband Subscribers using DSL, Optical Ethernet technologies.

IP Tax Project : 1st step towards NGN

The name given to this project has been IP Tax Project and is a class4 NGN implementation. The equipment for IP Tax is provided by M/s ZTE.

SCOPE OF IP TAX Project

This project was allocated to ZTE and as per the Solution provided by them, 3 types of sites are built according to different requirements of TMG capacity, and corresponding application scenarios, etc.

- Primary NOC Site
- Primary Site
- Secondary Site

These sites consist of the following products.

- ZTE Soft switch ZXSS10 SS1b,
- Trunk Media Gateways ZXSS10 MSG 9000(TMG)
- Announcement Server ZXSS10 MSG 9000

Soft switch Control: ZXSS10 SS1b

The Soft switch control device ZXSS10 SS1b mainly carries out the functions of call control, signaling process, resource management, accounting management, user management and protocol adaptation within its own domain, and uses 100M Ethernet interface to connect to the data network. Soft switch can support maximum load of traffic 2M BHCA/shelf without extension. When extension shelves (max.8) are present it can support Maximum traffic load of 16M BHCA . Billing records are stored at 3 levels. Maximum capacity of trunk is 200,000 DS0/shelf.

Trunk Media Gateway: ZXMSG 9000

The ZXMSG 9000(Trunk Media Gateway) is located on the core layer of the data MAN for connecting No.7 trunk users and PRI users. It connects the PSTN subscriber to the NGN to implement the conversion between voice/fax on the PSTN/ISDN trunk side and voice/fax on the IP network side. The ZXMSG 9000 can provide the functions of TG, SG and AG through different board and software configurations. When serving as TG, the ZXMSG 9000 is responsible to access PSTN to IP core network through trunk line and convert the voice/fax between PSTN/ISDN trunk side and IP network. It supports 5,600 E1 as Trunk Gateway.

Announcement Server: ZXMSG 9000

ZXMSG 9000 can be configured as announcement server, it is capable to provide sufficient announcement resources for all TMG under its control by interlocking with control device via ZXSS1b.

Network Management: ZXNMS

The softswitch integrated network management is developed independently by ZTE, which implement unified network management for softswitch product and relevant devices of ZTE. It can provide centralized management of facilities (Softswitch, TMG, SG, Data devices etc) with unified customer's interface, and can provide management interface for devices of other manufacturers. Every Site connects to MPLS/IP core packet network via a LAN Switch. Different types of sites consisting of the Soft switch control device, the service platform and network management system are constructed that is responsible for the call and service control and network management of the whole network.

Class 5 NGN Implementation:

For Class 5 implementation of Access equipment BSNL has adopted two different approaches:

1. Soft Switch based
2. IMS based

In Soft Switch based approach BSNL has given tender to M/s CDOT and for IMS based approach tender is given to M/s Huawei with additional capacity tender given to M/s UTSTARCOM.

SoftSwitch Based Class 5 Implementation.

The scope for the project to be executed by M/s CDOT includes equipment planning for CORE,ACCESS and NOC.

Zone Name	Primary Softswitch Site	DR Softswitch Site	Subscriber Ultimate Capacity (Main + DR)	NEBS Compliant Chassis/ Server
North Zone	Gurgaon	Chandigarh	33Lacs + 33Lacs	5 / 48
East Zone	Kolkata	Cuttack	16Lacs + 16Lacs	5 / 48
South Zone	Bangalore	Hyderabad	44Lacs + 44Lacs	5 / 48
West Zone	Pune	Bhopal	29Lacs + 29Lacs	5 / 48

Table 10. Core locations and capacity of CDOT sites

The table above summarizes the CORE locations divided zone wise with capacity of each zone. The zones were divided in Primary site and DR site for redundancy purpose.

IMS based Approach.

New Technology switches by IMS Class 5 NGN. These Provided by M/s Huawei and M/s UTStarcom. The IMS based project is implemented in two parts consisting of Package-1 IMS core elements and Package-2 Access Elements.

As is done in case of CDOT MAX NGN, IMS is also deployed in core and access parts with core located in four zones.
The Table below summarizes the location of CORE equipments and its capacity.

ZONE	PR Site	DR Site	Subscriber Capacity
NORTH	Chandigarh	Lucknow	800000
SOUTH	Hyderabad	Bengaluru	1500000
EAST	Bhubhaneshwar	Kolkatta	500000
WEST	Ahmedabad	Pune	1200000

Table 11. IMS Locations

An additional tender for 2.4 Mn lines is given to M/s UTStarcom, it has deployed core equipment with PR at Chandigarh and DR at Hyderabad site.

Package-2 Access Equipment are supplied by M/s Huawei, M/s ZTE and M/s UTStarcom. The Access equipment called as LMG or Line Media Gateway is a replacement to all the TDM based local exchanges. These LMG's are equipped with both voice and ADSL functionality thus eliminating the use of DSLAM's. The subscriber can avail voice as well as internet services from same equipment.

14.10 CONCLUSION

Migration to NGN and future networks brings many challenges to network and service providers, telecommunications and media regulators, equipment vendors, and other related business segments, but at the same it provides endless possibilities for rapid innovation of new networks, protocols and services.

15 SIP (SESSION INITIATION PROTOCOL)

15.1 LEARNING OBJECTIVES

- Explain the functions of SIP.
- Explain the components of SIP.
- Explain the relation among call, dialog, transaction & message.

15.2 INTRODUCTION

SIP (Session Initiation Protocol) is a signaling protocol used to create, manage and terminate sessions in an IP based network. . Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

SIP has been the choice for services related to Voice over IP in the recent past. It is a standard (RFC 3261) put forward by Internet Engineering Task Force (IETF). It SIP is still growing and being modified to take into account all relevant features as the technology expands and evolves. But it should be noted that the job of SIP is limited to only the setup and control of sessions. The details of the data exchange within a session e.g. the encoding or codec related to an audio/video media is not controlled by SIP and is taken care of by other protocols.

15.2.1 **A Brief History Of SIP**

Initially only the traditional switch-based telephone system was the main medium for transmitting messages. However with advent of the Internet, need was felt to fabricate a system, which connects people over the IP based network. Different communities put forward different solutions but the solution presented by IETF was finally accepted as most general one.

February 1996 Initial Internet drafts were produced in the form of - Session Invitation Protocol (SIP), Simple Conference Invitation Protocol (SCIP). SIP was originally intended to create a mechanism for inviting people to large-scale multipoint conferences on the Internet Multicast Backbone (Mbone). At this stage, IP telephony didn't really exist. The first draft was known as "draft-ietf-mmusic-sip-00". It included only one request type, which was a call setup request.

January 1999 The IETF published the draft called "draft-ietf-mmusic-sip-12". It contained the six requests that SIP has today.

March 1999 SIP published RFC 2543 as a standard. It was modified further to generate the more modern version of RFC 3261.

15.3 FUNCTIONS OF SIP

SIP is limited to only the setup, modification and termination of sessions. It serves four major purposes.

- SIP allows for the establishment of user location (i.e. translating from a user's name to their current network address).
- SIP provides for feature negotiation so that all of the participants in a session can agree on the features to be supported among them.

- SIP is a mechanism for call management - for example adding, dropping, or transferring participants.
- SIP allows for changing features of a session while it is in progress.

All of the other key functions are done with other protocols.

Yes! This does indeed mean that SIP is not a session description protocol, and that SIP does not do conference control. SIP is not a resource reservation protocol and it has nothing to do with quality of service (QoS). SIP can work in a framework with other protocols to make sure these roles are played out - but SIP does not do them. SIP can function with SOAP, HTTP, XML, VXML, WSDL, UDDI, SDP and others.

15.4 COMPONENTS OF SIP

Entities interacting in a SIP scenario are called User Agents (UA) User Agents may operate in two fashions –

- User Agent Client (UAC): It generates requests and sends those to servers.
- User Agent Server (UAS): It gets requests, processes those requests and generates responses.

Note: A single UA may function as both.

Clients: In general we associate the notion of clients to the end users i.e. the applications running on the systems used by people. It may be a soft-phone application running on your PC or a messaging device in your IP phone. It generates a request when you try to call another person over the network and sends the request to a server (generally a proxy server).

Servers: Servers are in general part of the network. They possess a predefined set of rules to handle the requests sent by clients. Servers can be of several types -
Proxy Server: These are the most common type of server in a SIP environment. When a request is generated, the exact address of the recipient is not know in advance. So the client sends the request to a proxy server. The server on behalf of the client (as if giving a proxy for it) forwards the request to another proxy server or the recipient itself.
RedirectServer: A redirect server redirects the request back to the client indicating that the client needs to try a different route to get to the recipient. It generally happens when a recipient has moved from its original position either temporarily or permanently.
Registrar: As you might have guessed already, one of the prime jobs of the servers is to detect the location of a user in a network. How do they know the location? If you are thinking that users have to register their locations to a Registrar server, you are absolutely right. Users from time to time refresh their locations by registering (sending a special type of message) to a Registrar server.
Location Server: The addresses registered to a Registrar are stored in a Location Server.

15.4.1 **Commands Of SIP**

Command	Meanings
INVITE	Invites a user to a call
ACK	Acknowledgement is used to facilitate reliable message exchange for INVITEs

BYE	Terminates a connection between users
CANCEL	Terminates a request, or search, for a user. It is used if a client sends an INVITE and then changes its decision to call the recipient.
OPTIONS	Solicits information about a server's capabilities.
REGISTER	Registers a user's current location
INFO	Used for mid-session signaling

Table 12. Commands of SIP & their Meaning

15.4.2 **A Typical Example Of SIP Session**

SIP signaling follows the server-client paradigm as used widely in the Internet by protocols like HTTP or SMTP. The following picture presents a typical exchange of requests and responses. Please note that it is only a typical case and doesn't include all possible cases.

Before understanding the methods, first you should understand the pictorial diagram. User 1 uses his soft-phone to reach the SIP phone of user2. Server1 and server2 help to setup the session on behalf of the users. This common arrangement of the proxies and the end-users is called "SIP Trapezoid" as depicted by the dotted line. The messages appear vertically in the order they appear i.e. the message on top (INVITE M1) comes first followed by others. The direction of arrows shows the sender and recipient of each message. Each message contains a 3-digit-number followed by a name and each one is labeled by 'M' and a serial number. The 3-digit-number is the numerical code of the associated message comprehended easily by machines. Human users use the name to identify the message.

The transaction starts with user1 making an INVITE request for user2. But user1 doesn't know the exact location of user2 in the IP network. So it passes the request to server1. Server1 on behalf of user1 forwards an INVITE request for user2 to server2. It sends a TRYING response to user1 informing that it is trying to reach user2. The response could have been different but we will discuss the other type of responses later.

Receiving INVITE M2 from server1, server2 works in a similar fashion as server1. It forwards an INVITE request to user2 (note: Here server2 knows the location of user2. If it didn't know the location, it would have forwarded it to another proxy server. So an INVITE request may travel through several proxies before reaching the recipient). After forwarding INVITE M3 server2 issues a TRYING response to server1.

The SIP phone, on receiving the INVITE request, starts ringing informing user2 that a call request has come. It sends a RINGING response back to server2 which reaches user1 through server1. So user1 gets feedback that user2 has received the INVITE request.

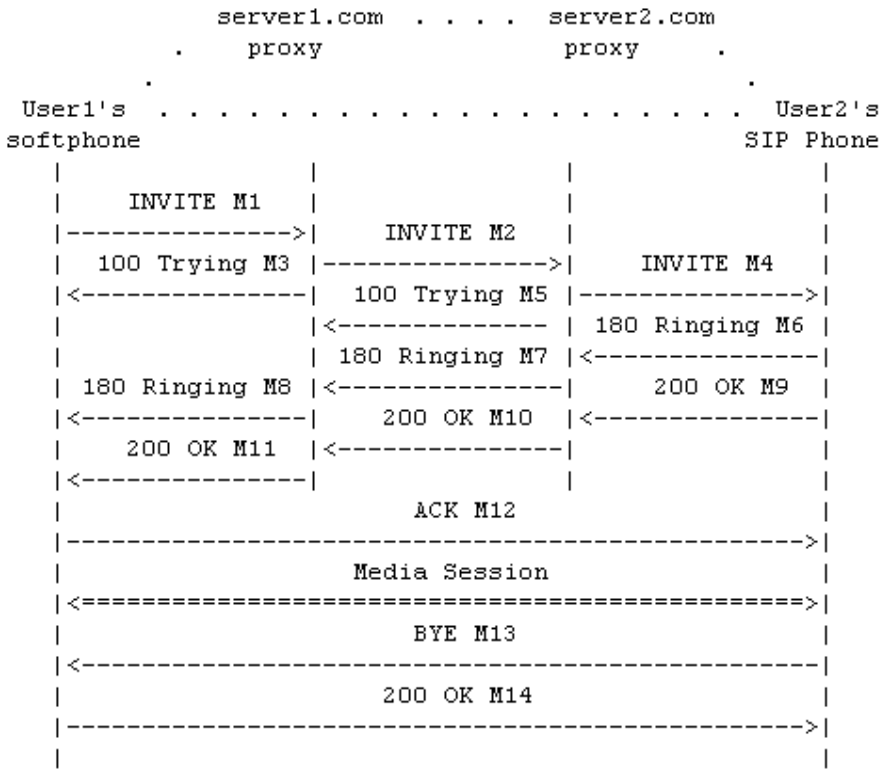


Figure 81: SIP session example with SIP trapezoid

User2 at this point has a choice to accept or decline the call. Let's assume that he decides to accept it. As soon as he accepts the call, a 200 OK response is sent by the phone to server2. Retracing the route of INVITE, it reaches user1. The soft-phone of user1 sends an ACK message to confirm the setup of the call. This 3-way-handshaking (INVITE+OK+ACK) is used for reliable call setup. Note that the ACK message is not using the proxies to reach user2 as by now user1 knows the exact location of user2.

Once the connection has been setup, media flows between the two endpoints. Media flow is controlled using protocols different from SIP e.g. RTP

When one party in the session decides to disconnect, it (user2 in this case) sends a BYE message to the other party. The other party sends a 200 OK message to confirm the termination of the session.

15.4.3 **Request Message Format Of SIP**

In the previous SIP session example it is seen that requests are sent by clients to servers. Now see what that request actually contains. The following is the format of INVITE request as sent by user1.

```
INVITE sip: user2@server2.com SIP/2.0
Via: SIP/2.0/UDP pc33.server1.com; branch=z9hG4bK776asdhds Max-Forwards: 70
To: user2 <sip: user2@server2.com>
From: user1 <sip:user1@server1.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.server1.com
CSeq: 314159 INVITE
Contact: <sip:user1@pc33.server1.com>
Content-Type: application/sdp
Content-Length: 142

---- User1 Message Body Not Shown ----
```

The first line of the text-encoded message is called Request-Line. It identifies that the message is a request.

15.4.4 Request-Line

Method SP Request-URI SP SIP-Version CRLF
[SP = single-space & CRLF=Carriage Return + Line Feed (i.e. the character inserted when you press the "Enter" or "Return" key of your computer)]
Here method is INVITE, request-uri is "user2@server2.com" and SIP version is 2. The following lines are a set of header fields.

- **Via**: *It contains the local address of user1 i.e. pc33.server1.com where it is expecting the responses to come*.
- **Max Forward**: *It is used to limit the number of hops that this request may take before reaching the recipient. It is decreased by one at each hop. It is necessary to prevent the request from traveling forever in case it is trapped in a loop.*
- **To**:*It contains a display name "user2" and a SIP or SIPS URI <user2@server2.com>*
- **From**: *It also contains a display name "user1" and a SIP or SIPS URI <user1@server1.com>. It also contains a tag which is a pseudo-random sequence inserted by the SIP application. It works as an identifier of the caller in the dialog.*
- **Call-ID**: *It is a globally unique identifier of the call generated as the combination of a pseudo-random string and the softphone's IP address*.
- **CSeq***: It contains an integer and a method name. When a transaction starts, the first message is given a random CSeq. After that it is incremented by one with each new message. It is used to detect non-delivery of a message or out-of-order delivery of messages*.
- **Contact**: *It contains a SIP or SIPS URI that is a direct route to user1. It contains a username and a fully qualified domain name (FQDN). It may also have an IP address.*

 Via field is used to send the response to the request. Contact field is used to send future requests. That is why the 200 OK responses from user2 go to user1 through proxies. But when user2 generates a BYE request (a new request and not a response to INVITE), it goes directly to user1 bypassing the proxies.

- Content-Type: ***It contains a description of the message body (not shown).***
- Content-Length: ***It is an octet (byte) count of the message body.***

The header may contain other header fields also. However those fields are optional. Please note that the body of the message is not shown here. The body is used to convey information about the media session written in Session Description protocol. You may continue your journey through SIP without worrying about SDP right now.

15.4.5 Response Message Format Of SIP

Here is what the SIP response of user2 will look like.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP site4.server2.com; branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP site3.server1.com;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
```

```
Via: SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776asdhds;received=192.0.2.1
To: user2 <sip:user2@server2.com>;tag=a6c85cf
From: user1 <sip:user1@server1.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.server1.com
CSeq: 314159 INVITE
Contact: <sip:user2@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

---- User2 Message Body Not Shown ----
```

Status Line

The first line in a response is called Status line.

SIP-Version SP Status-Code SP Reason-Phrase CRLF

[SP = single-space & CRLF=Carriage Return + Line Feed (i.e. the character inserted when you press the "Enter" or "Return" key of your computer)]

Here SIP version is 2, Status-Code is 200 and Reason Phrase is OK.

The header fields that follow the status line are similar to those in a request the differences are:

- **Via**: There is more than one via field. This is because each element through which the INVITE request has passed has added its identity in the via field. Three via fields are added by soft-phone of user1, server1 the first proxy and server2 the second proxy. The response retraces the path of INVITE using the via fields. On its way back, each element removes the corresponding via field before forwarding it back to the caller.
- **To**: Note that the to field now contains a tag. This tag is used to represent the called in a dialog.
- **Contact**: It contains the exact address of user2. So user1 doesn't need to use the proxy servers to find user2 in the future.

Response Types of SIP The first digit of a Status-Code defines the category of response. So any response between 100 and 199 is termed as a "1xx" response and so is done for any other type. SIP/2.0 allows six types of response.

1XX	Provisional	Request received, continuing to process the request.
2XX	Success	The action was successfully received, understood, and accepted.
3XX	Redirection	Further action needs to be taken in order to complete the request
4XX	Client Error	The request contains bad syntax or cannot be fulfilled at this server.
5XX	Server Error	The server failed to fulfill an apparently valid request.
6XX	Global Failure	The request cannot be fulfilled at any server.

If a response is received having a Status-Code of the form yxx, which is not understood by the receiving party, it treats the response as an y00 response i.e. if a client receives an unknown response 345, it treats that as a 300 response. An unknown 1xx is treated as 183 (Session in Progress). So each UA must know how to react to 100,183,200,300,400,500 and 600.

15.5 RELATION AMONG CALL, DIALOG, TRANSACTION & MESSAGE

Messages are the individual textual bodies exchanged between a server and a client. There can be two types of messages. (Requests and Responses).

Transaction occurs between a client and a server and comprises all messages from the first request sent from the client to the server up to a final (non-1xx) response sent from the server to the client. If the request is INVITE and the final response is a non-2xx, the transaction also includes an ACK to the response. The ACK for a 2xx response to an INVITE request is a separate transaction.

Dialog is a peer-to-peer SIP relationship between two UAs that persists for some time. A dialog is identified by a Call-ID, a local tag and a remote tag. A dialog used to be referred as a *'call leg'*.

Call of a called (Callee) comprises of all the dialogs. it is involved in. A Call is same as a Session.
A caller may have connections to a number of called at a time forming a number of dialogs. All these dialogs make a single call.
The following figure will make the relation clearer.

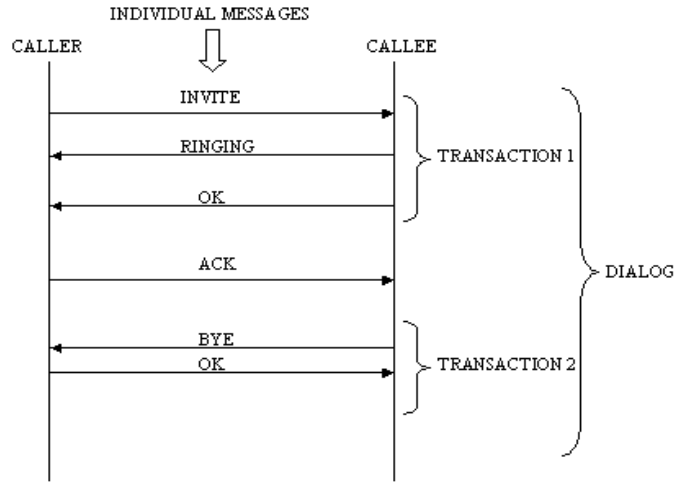


Figure 82: Relation among Call, Dialog, Transaction & Message

15.5.1 **Registration In SIP**

While going through a typical SIP version it is already seen that the caller doesn't know the address of the called initially. The proxy servers do the job of finding out the exact location of the recipient. What actually happens is that every user registers its current location to a REGISTRAR server? The application sends a message called REGISTER informing the server of its present location. The Registrar stores this binding (between the user and its present address) in a location server, which is used by other proxies to locate the user.

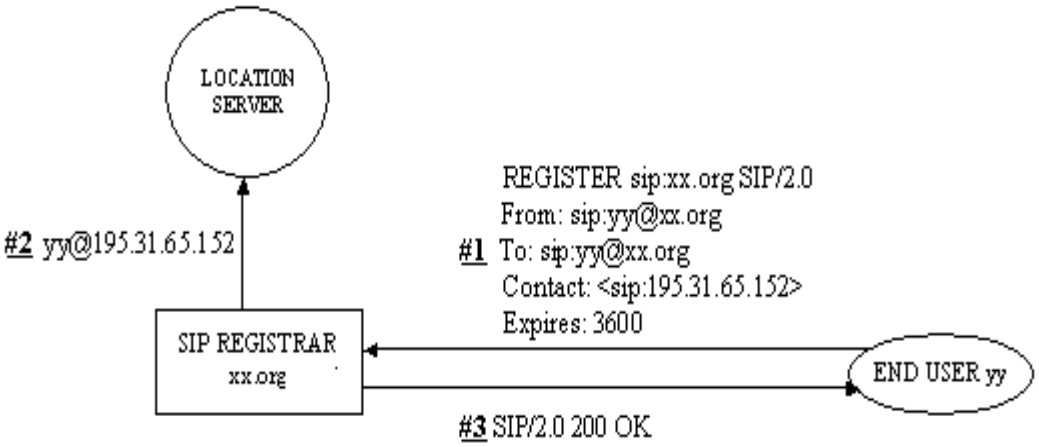


Figure 83: Registration in SIP

User YY uses the IP 195.31.65.152 as its current location and registers it with the server. This actually helps in user mobility. Say there is a messaging application. You can log in from different computers. As soon as you log in using your username, the application REGISTERS the username with the IP of that computer. The 'Expire' field reflects the duration for which this registration will be valid. So the user has to refresh its registration from time to time.

* Please note that the difference between a proxy server and a registration or a location server is often *only logical*. Physically they may be situated on the same machine.

15.6 CONCLUSION

SIP is one of the most common protocols used in VOIP technology. One should be able to recognize the major components in a SIP scenario and how different messages are exchanged to establish and terminate sessions.

16 ADVANCED MPLS NETWORK

16.1 LEARNING OBJECTIVES

This chapter covers the concept of MPLS. MPLS (Multi Protocol Label Switching) is a mechanism that switches traffic based on labels instead of routing traffic. MPLS VPN is a popular technique to build VPNs for customers over the MPLS provider network.

After reading the chapter the participants will be able to understand the concept of LSP, traffic engineering, loop detection and MPLS-BGP interaction.

16.2 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 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 class 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.

16.3 DRAWBACKS OF TRADITIONAL IP FORWARDING

- Routing protocols are used to distribute Layer 3 routing information and therefore every router may need full Internet routing information (more than 100,000 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.

16.4 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 link failures, 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

16.5 MPLS HEADER

16.5.1 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.

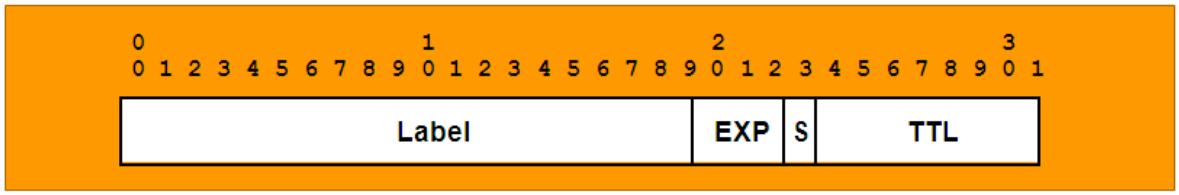


Figure 84: MPLS Header format

16.5.2 MPLS Label Stack

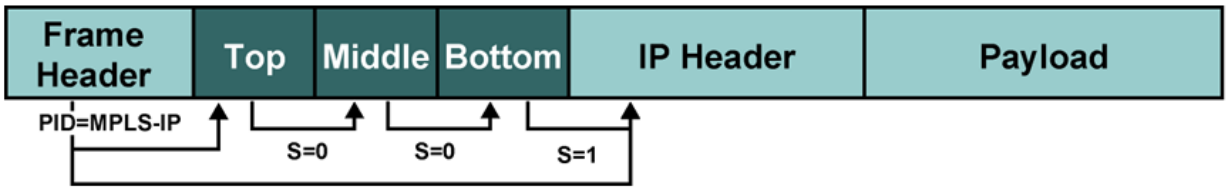


Figure 85: MPLS Label stack

- Protocol identifier in a Layer 2 header specifies that the payload starts with a label (labels) and is followed by 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 than one label:
    - •MPLS VPNs (two labels: The top label points to the egress router 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.)

16.6 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 Corerouters. 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.

16.7 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-stream type and Internet-access customer

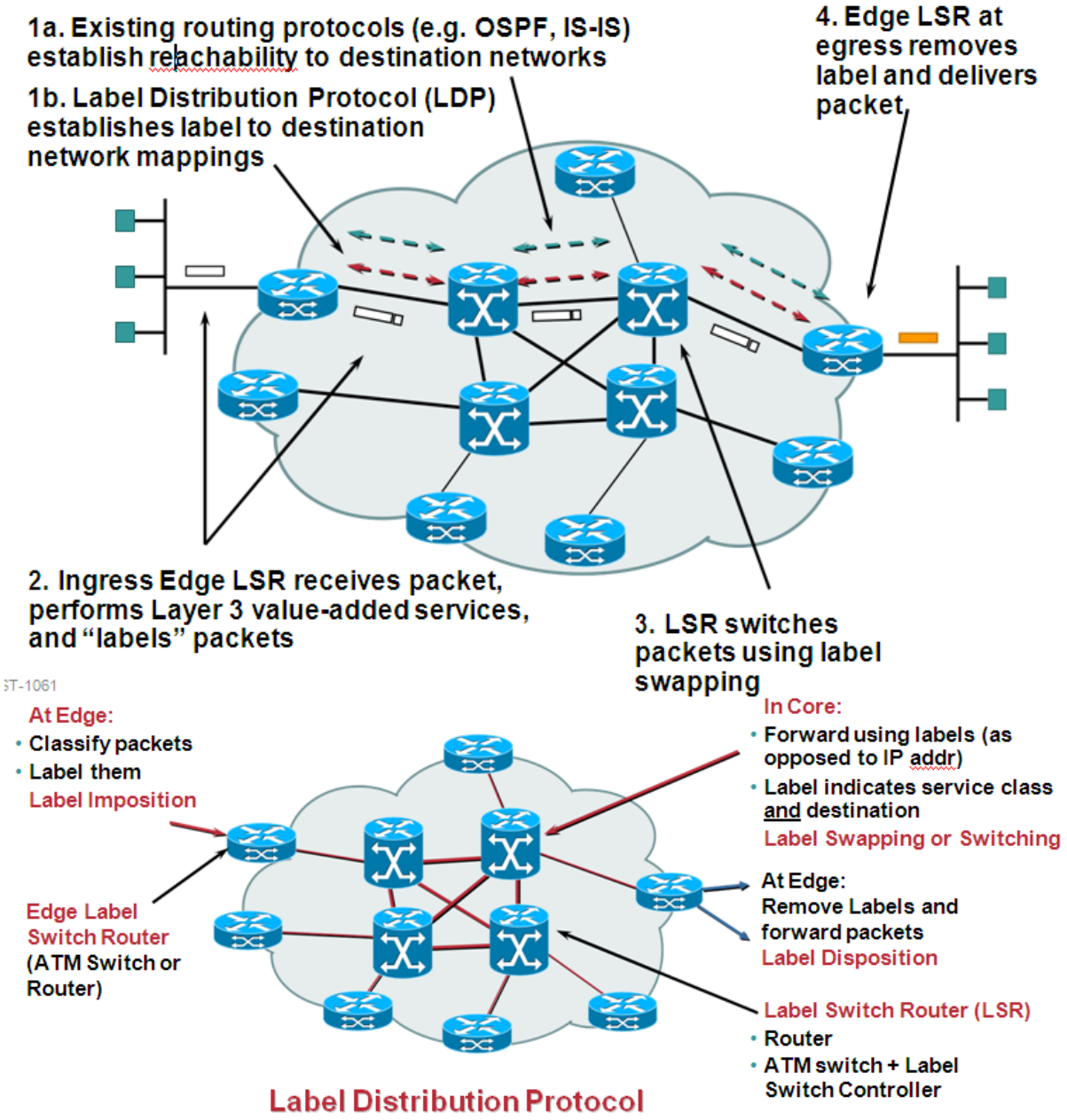


Figure 86: Forwarding of Packets in MPLS Network

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.

16.8 MPLS ROUTER FUNCTIONALITY

MPLS Router functionality is divided into two major parts

Control plane: Exchanges Layer 3 routing information 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.

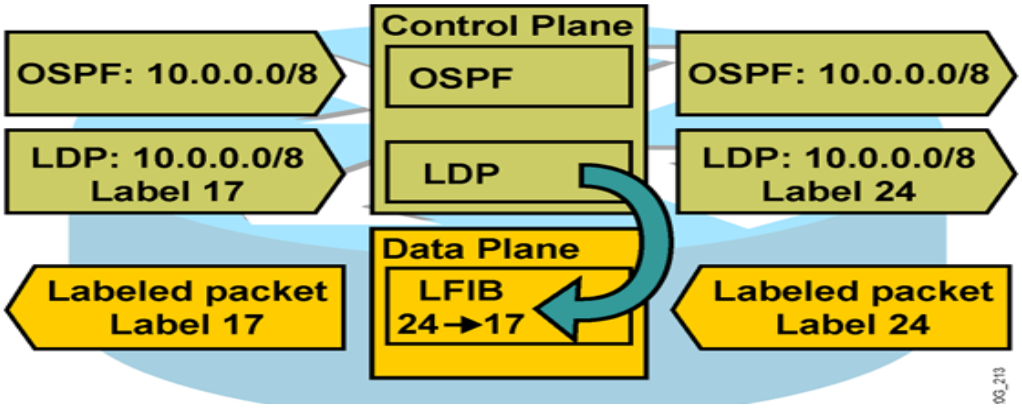


Figure 87: MPLS Control and Data Plane Functionality

Architecture of LER:

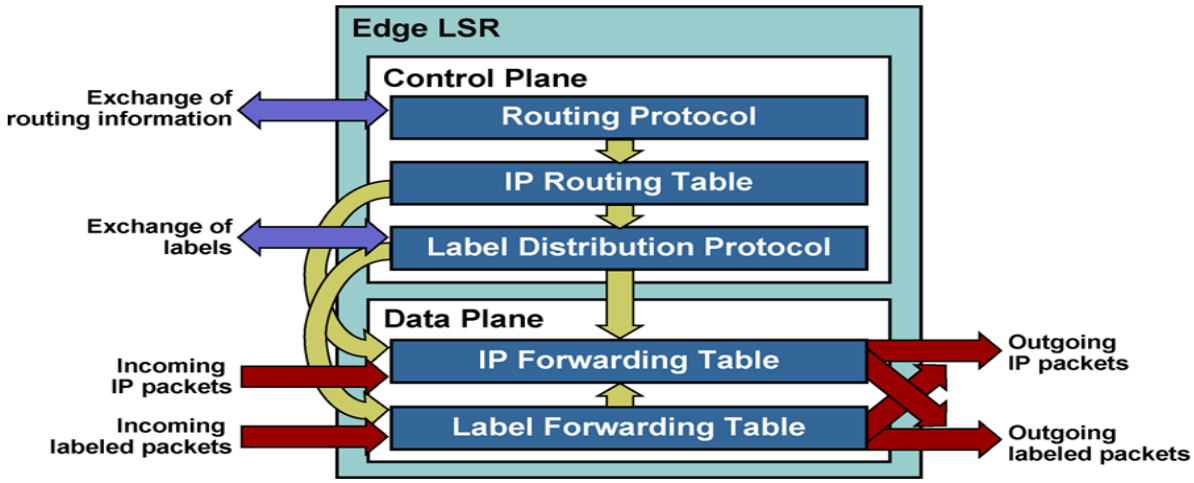


Figure 88: Architecture of LER

Architecture of LSR

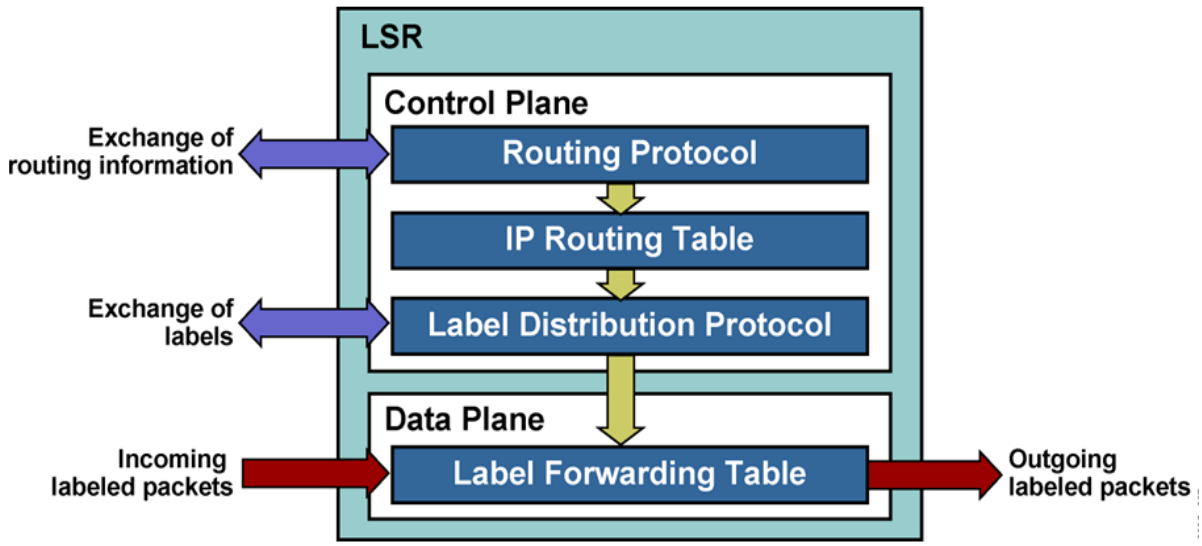


Figure 89: Architecture of LSR

16.9 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.

16.9.1 Router Example: Forwarding Packets

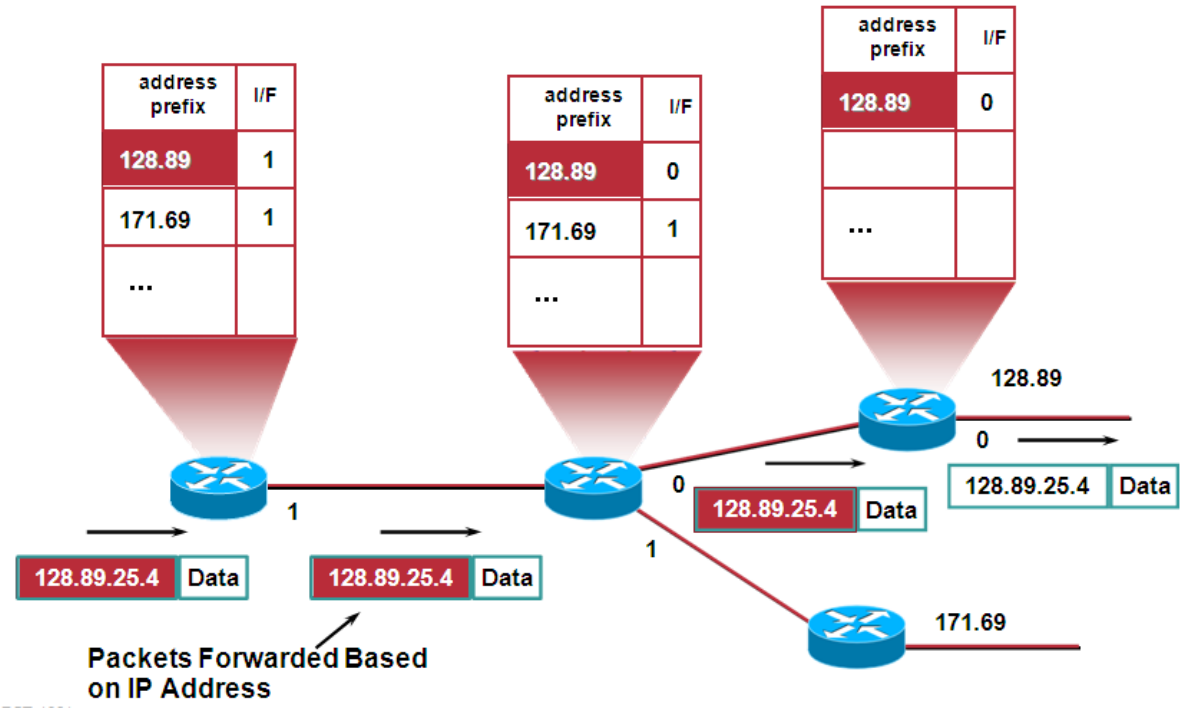


Figure 90: Routing example

16.9.2 MPLS Example: Routing Information

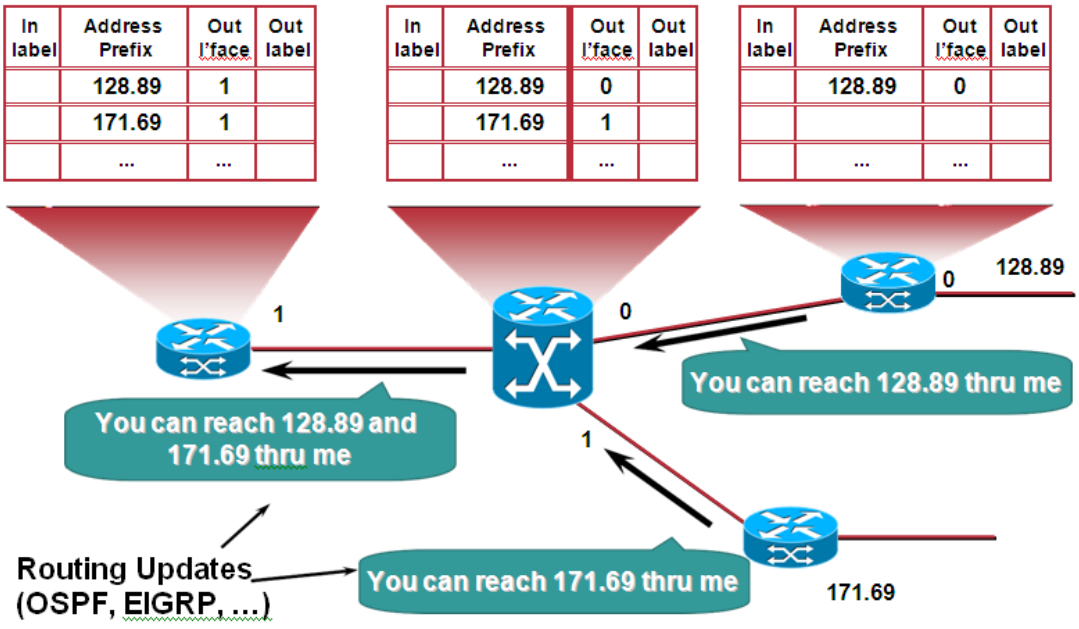


Figure 91: MPLS Example :Routing Information

16.9.3 MPLS Example: Assigning Labels

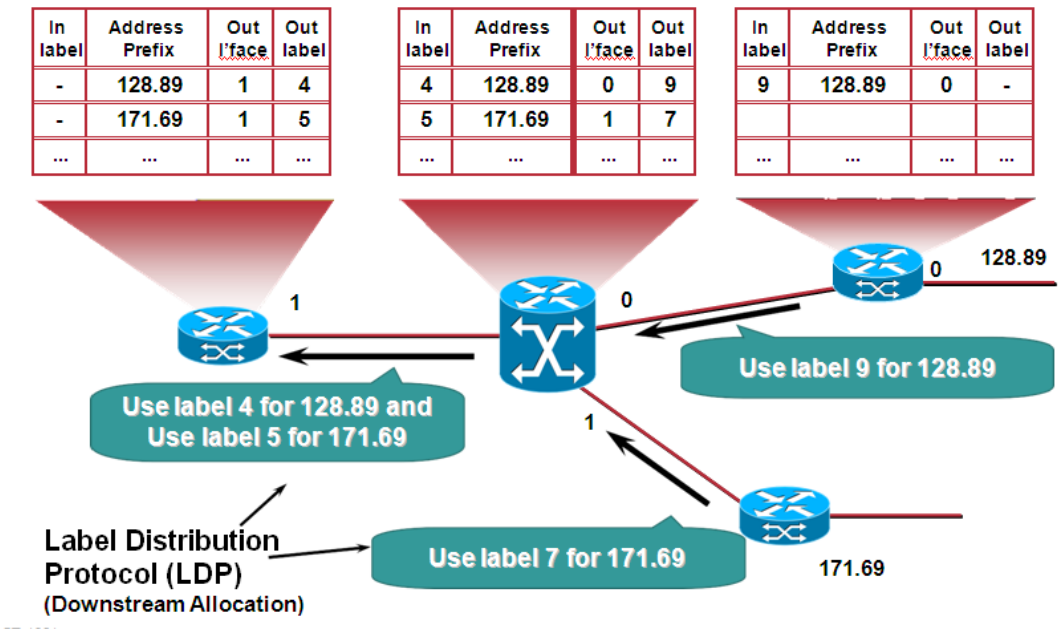


Figure 92: MPLS Example :Assigning Labels

16.9.4 MPLS Example: Forwarding Packets

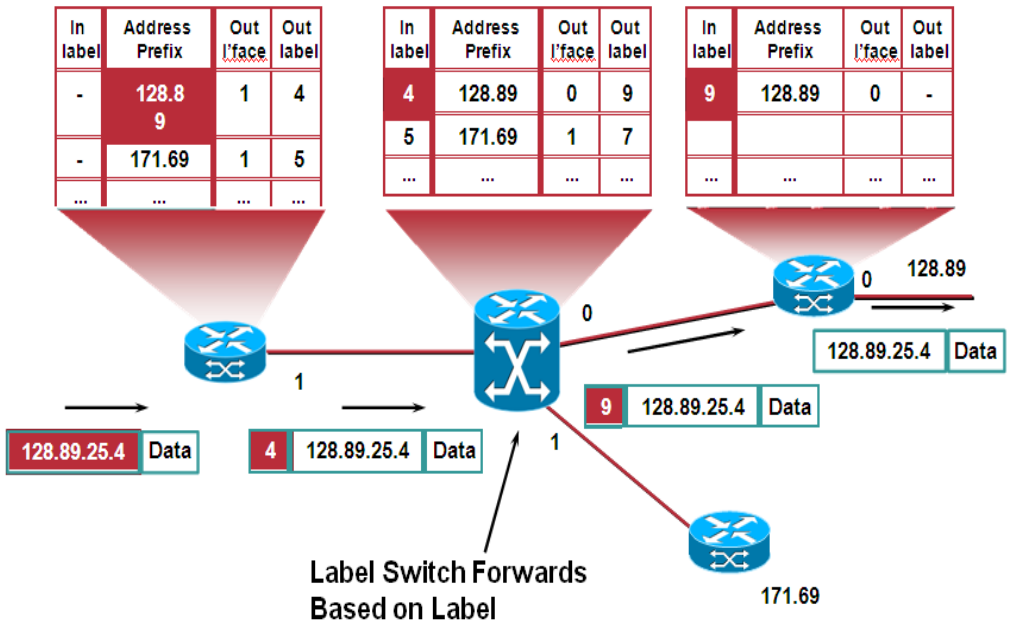


Figure 93: MPLS Example :Forwarding Packets

16.10 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 is as 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)

16.11 LDP (LABEL DISTRIBUTION PROTOCOL)

LDP Protocol has the following functions:

- Neighbor discovery

  Discover directly attached Neighbors—pt-to-pt links (including Ethernet)

  Establish a session

  Exchange prefix/FEC and label information

- Extended Neighbor Discovery

  Establish peer relationship with another router that is not a neighbor

  Exchange FEC and label information

  May be needed to exchange service labels

16.11.1 **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.

16.12 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

16.13 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., the LSR 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 the path, 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.

16.14 MPLS VPN

16.14.1 **What Is A VPN**

- VPN is a set of sites which are allowed to communicate 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 VPN Service 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 different organizations(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)

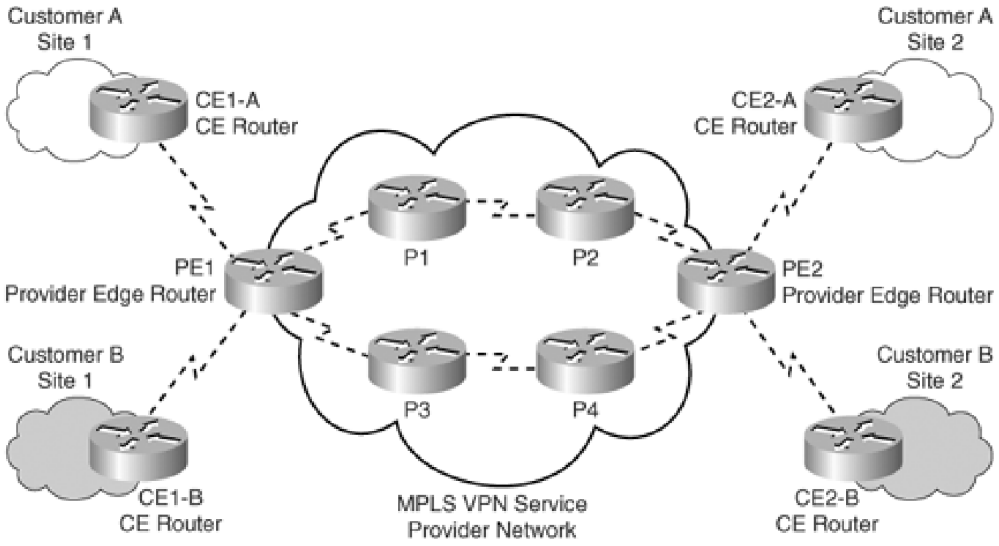


Figure 94: MPLS VPN Architecture

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.

16.14.2 **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

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.

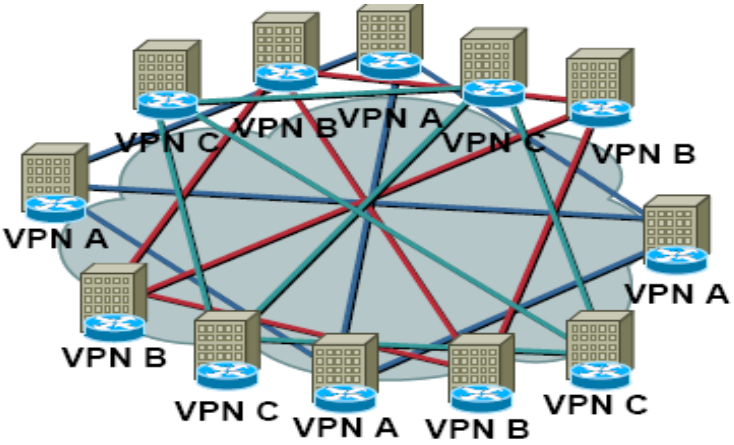


Figure 95: Overlay VPN

16.15 PEER-TO-PEER MODEL

The peer-to-peer modelwas 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.

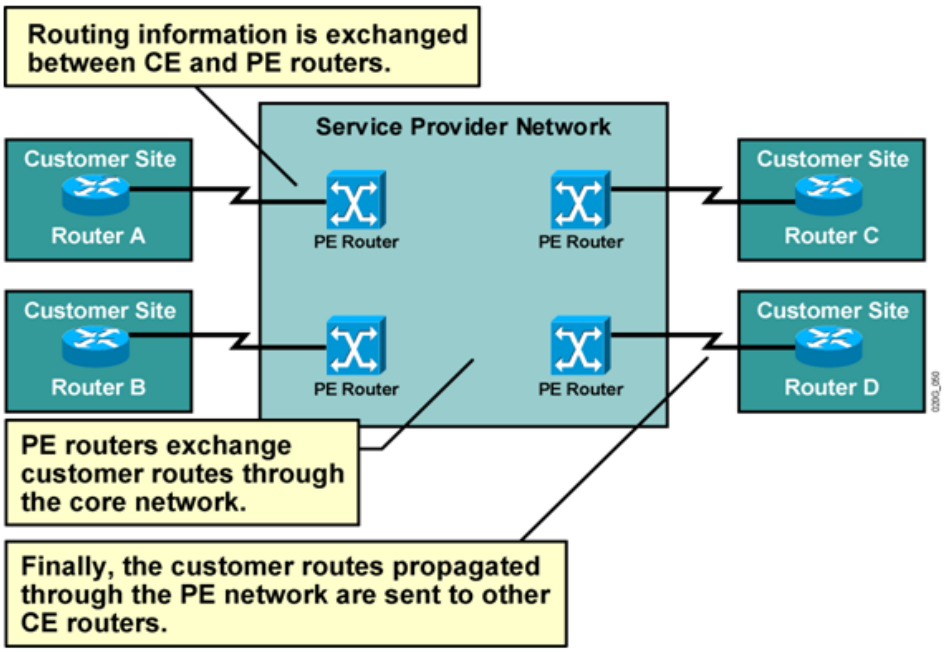


Figure 96: Peer – to – Peer VPN

16.16 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.

16.17 LAYER 2 AND LAYER 3 VPNS

- Layer 2 VPNs
  - Customer End points (CPE) connected via layer 2 such as Frame Relay 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 routers Single 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

16.18 MPLS VPN WORKING

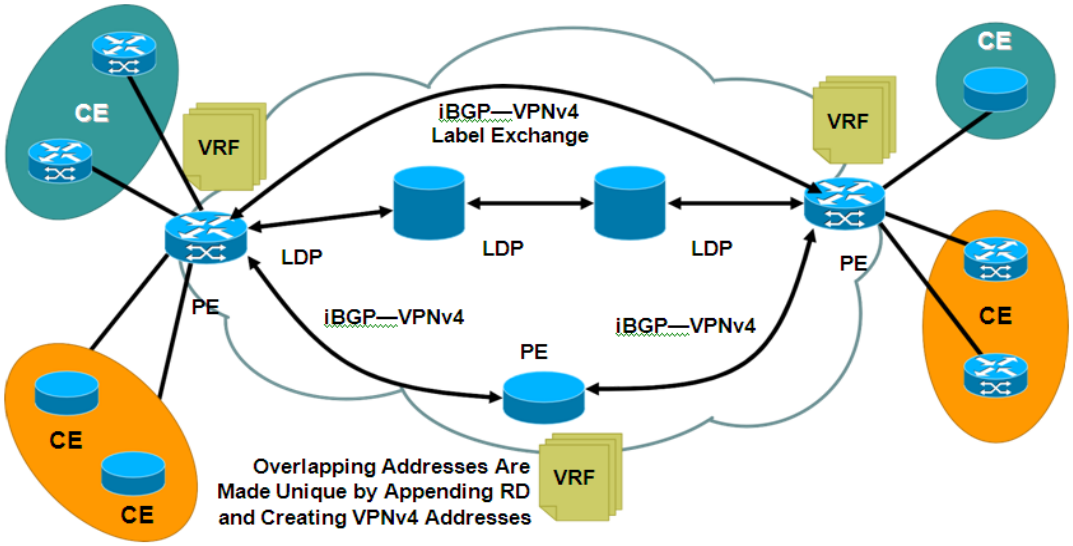


Figure 97: MPLS VPN Working

16.19 MPLS LER ARCHITECTURE

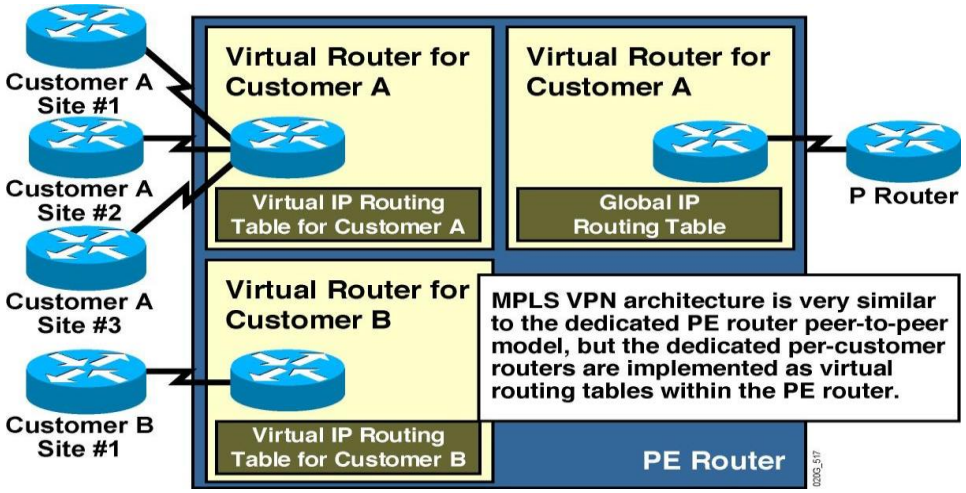


Figure 98: MPLS LER Architecture

16.19.1 MPLS Control Plane Path:

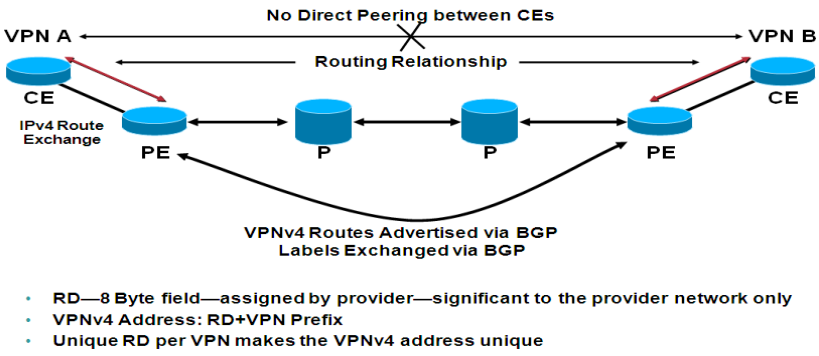
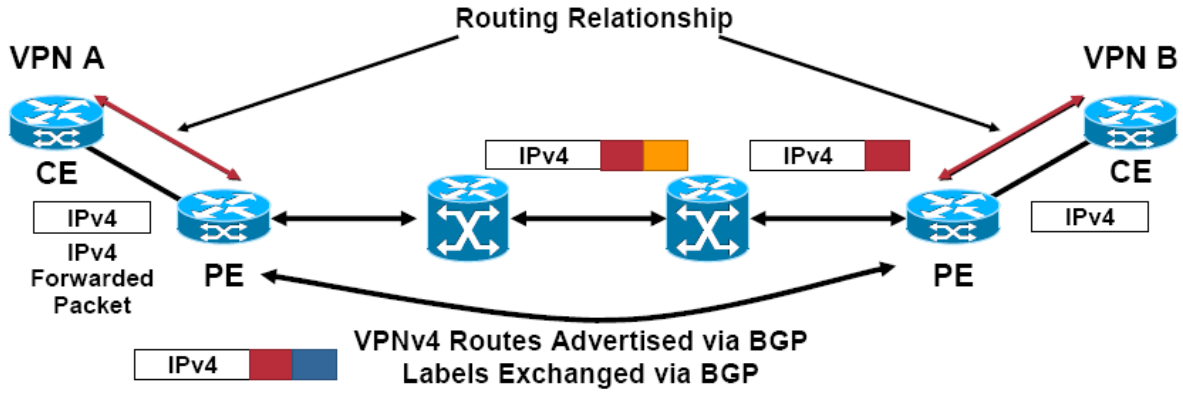


Figure 99: MPLS Control Plane Path

16.19.2 **MPLS Data Plane Path:**



- **Ingress PE is imposing 2 labels**

Figure 100: MPLS Data Plane Path

16.20 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.

16.21 CONCLUSION

MPLS VPN is a popular technique to build VPNs for customers over the MPLS provider network. The better understanding of MPLS – VPN facilitates the participants to better handle the O and M of MPLS network in real time scenario.

17 CONCEPT OF ONE NETWORK (CENTRALIZED NOC FOR CFA)

17.1 LEARNING OBJECTIVES

- Concept and requirement of One Network.
- The activities involved in one network concept.
- Implementation of one network program.
- The network and partner team management.

17.2 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)

17.3 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
- Monitoring and Management, Escalation of faults to maintenance in-charge
- Monitoring of Leased circuits (MLLN & Non-MLLN both), Monitoring ofWi-Fi Hotspots, intimation regarding faulty nodes to field maintenance teams
- Monitoring of BBNL OLTs

- Testing of OLTs of TIPs from BNG
- PING Test, Profile check, handling customer speed issues
- ILL testing of MPLS customers, CRC error testing
- Coordination with Transmission teams for fault and speed related issues
- BTS nodes (2G/3G/4G) - Periodic reporting of faulty BTS nodes to BTS maintenance teams
- TRE Combiner reset, partial fault reset of 2G/3G/4G BTS nodes
- Alarm Extension of unmanned BTS sites
- Clearance of all types of network faults and clearance of faults even in odd hours, thus facilitating network availability to the customer very high
-

(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 18005991001 (created by Bangalore Telecom District for partner management activities) shall be mapped with the telephone number at respective BA level CGPS.

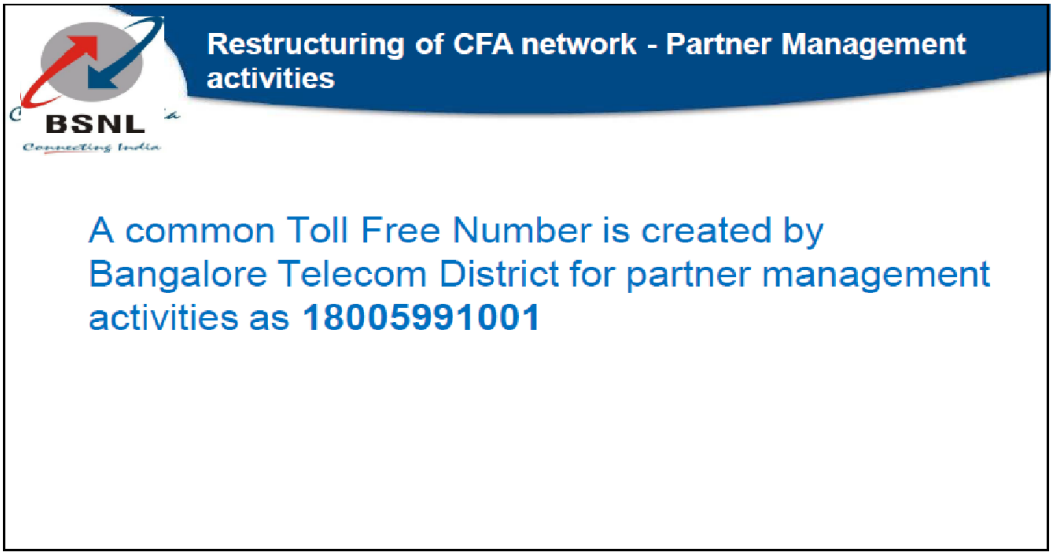


Figure 101: Common Toll Free Number for partner management

- 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.

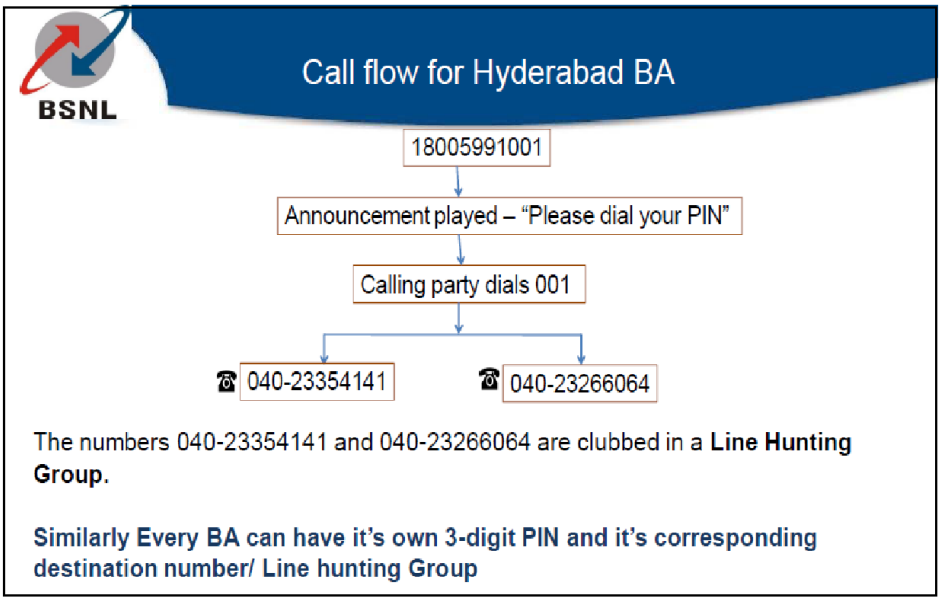


Figure 102: Call flow for BA

17.3.1 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.

17.3.2 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

17.3.3 **Ofc Route Patroller Monitoring**

- Patroller Monitoring and Reports.
- Updation of data for Patrollers and New OF route in Patroller Monitoring System.

17.4 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)

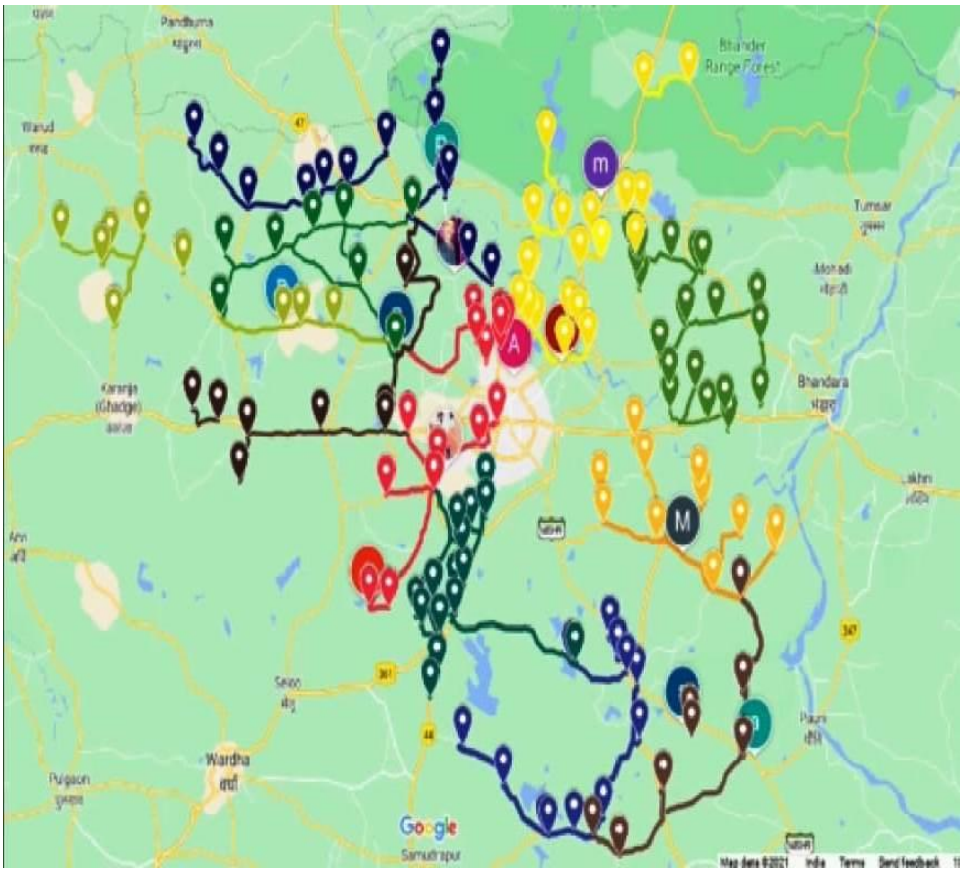


Figure 103: OFC Cable Route Mapping and Fault Localization by One Network

17.5 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	Mobile No.	E-mail ID

17.6 ONE NETWORK BA TEAM CASE STUDY OF MAHARASHTRA CIRCLE

One Network BA Team Case Study of Maharashtra Circle

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
	MH	Ahmednagar	Category-B	12	6
	MH	Amaravati	Category-C	8	4
	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	Nanded	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

17.7 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.

18 NOFN

18.1 LEARNING OBJECTIVES

- About NOFN Project Of India.
- NOFN Applications For Government.
- NOFN ROADMAP.
- NOFN Features.

18.2 INTRODUCTION

a. **NOFN** is a Countrywide National Fibre Optical Network project
b. **Objective:** Extend existing Optical Fiber Network to Panchayats by utilizing Universal Service Obligation Funds (USOF) and creating an institutional mechanism for management and operation of NOFN.
c. **Institutional Mechanism:** Bharat Broadband Network Limited (BBNL), a PSU has been registered under The Companies Act 1956 on Feb 25, 2012 for management and operation of NOFN
d. **Government Initiative**: - Government of India has approved on 25-10-2011 for the setting up of National Optical Fiber Network (NOFN) to provide connectivity to 2.5 lakh Gram Panchayats (Village Govt Office) of the country using optical fiber, which would ensure broadband connectivity with adequate bandwidth. This is to be achieved utilizing the existing optical fiber and extending it to the Gram Panchayats (Village Govt Office) i.e. by bridging the gap in the Aggregation Layer.
e. **Asset** :- NOFN is a National Asset
f. **Now NOFN will be called as BharatNET**
g. **BBNL** (Bharat Broadband Network Limited), is a Special Purpose Vehicle (SPV), set up by Govt of India incorporated as a Public Sector to implement and operate the NOFN project.
h. NOFN will provide Non-discriminatory access to all the Service Providers .This Telecom infrastructure which will bridge the gap (digital divide) in rural access. NOFN is being funded by the Universal Service Obligation Fund (USOF). Department of Telecom, Ministry of Communications & IT, Govt. of India provide secretariat service to project.
i. "The establishment of NOFN will open up new avenues for access service providers like mobile operators, cable TV operators etc. to launch next generation services and spur creation of local employment opportunities encompassing e-commerce and IT outsourcing, as well as e-banking, e-health and e-education".The project is being implemented by three central PSUs (CPSUs) namely BSNL, PGCIL and Railtel in the phase first.
j. The Government of India entity, Bharat Broad Band Nigam Limited (BBNL), will centrally manage the project through a high capacity Network Management System being developed by C-DOT. A key feature of the project is that the GPON equipment used in the project has been indigenously designed and developed by C-DOT and manufactured domestically.
k. The monitoring of the progress of the project will be done through Primavera Software(Oracle's Primavera Professional Project Management Software).In

the first phase NOFN shall be extended to cover 50,000 GPs, with the balance 2,00,000 GPs expected to be covered in a phased manner .

l. NOFN is part of the Digital India initiative of the Government of India. Digital India is an initiative of the Government of India to integrate the government departments and the people of India to ensure effective governance. It also aims at ensuring that the government services are made available to citizens electronically by reducing paperwork. The initiative also includes a plan to connect rural areas under high-speed internet networks.

The programme also aims at providing digital infrastructure as a utility to every citizen as well as high-speed internet as a core utility in all Gram Panchayats (Village Govt Office) through NOFN. On its completion, NOFN is expected to facilitate broadband connectivity to over 600 million rural citizens of the country.

18.3 WHY NOFN?

18.3.1 **The Bandwidth Requirements Of Applications Used In Indian Scenario**

Table below summarizes various applications in Indian scenario and bandwidth required to support such applications. From this, It is observed that tentative bandwidth requirements to run various applications ranges from 64 Kbps to 8 Mbps.

Table 13. The Bandwidth Requirements Of Applications Used In INDIAN Scenario

Application	Minimum bandwidth Required
Internet Surfing	Upto 256Kbps
E-Mail	64 Kbps
Voice Chatting	64 Kbps
Voice & Video Chatting	256-512 Kbps
Video Clips	256-512 Kbps
Tele-education	256-512 Kbps
Tele-Medicine	256 Kbps
Video Streaming	2 Mbps
Video Gamin	256-512-2Mbps
High Definition Videos	4-8 Mbps

a 256 Kbps - This speed is appropriate for viewing most websites, taking about 3 secs for the website to load.

b 512 Kbps - This is the most common speed used in homes and small businesses. It takes 1.6 secs for a website to load and about 1.5 mins to download a 5min music file at maximum speed. Suitable for video and music streaming.

c 1Mbps - This speed is also commonly used amongst homes and small businesses. It is appropriate for website viewing, streaming and online gaming. It takes 0.8 secs to load a web page and about 40 secs to download a 5 min music file at maximum speed.

d 2 Mbps - This and faster speeds are more suitable for people who play a lot of demanding online games. It is also suitable for people who share one Internet connection between many PC-s. It takes 0.4 seconds to load a website and about 20 seconds to download a 5 minute music file at maximum speed.

e 24 Mbps - Ultra fast broadband offered these high speed services are particularly good for watching real-time DVD quality film.

18.3.2 The Bandwidth Available On Various Technologies

Table 14. Bandwidth available via different BB Technologies

Connection Type	Megabytes per second	Connection Type	Megabytes per second
14.4 modem	0.014	ISDN	0.125
28.8 modem	0.028	Wireless local area network	0.127
V.92 Modem	0.055	Satellite	0.391
100 kbps	0.098	Broadband over power	0.488
Wireless Cellular	0.098	ADSL	0.625

18.4 THE SOLUTION – TECHNOLOGY USED - GPON

a The GPON (Gigabit Passive Optical Network) standard differs from other PON standards in that it achieves higher bandwidth and higher efficiency using larger, variable-length packets.

b A Passive Optical Network (PON) is a network architecture that brings fiber cabling and signals to the home using a point-to-multipoint scheme that enables a single optical fiber to serve multiple premises.

c GPON (Gigabit Passive Optical Network) will be used for NOFN Project. GPON is an open standard technology. C-DOT has developed this technology and the approval has been obtained for the same from TEC.(Telecommunication Engineering Center India)

d Encryption maintains data security in this shared environment. The architecture uses passive (unpowered) optical splitters, reducing the cost of equipment compared to point-to-point architectures.

e C-DOT has done the Transfer of Technology for GPON to manufacturers which include both CPSUs and private, to meet NOFN timely supply of equipments.

Need a countrywide National Fibre Optic Network to use GPON Technology

18.4.1 NOFN -Applications For Government

i **e-Monitoring and empowering of Various Govt Schemes like**

NREGS (National Rural Employment Guarantee Scheme) IAY (Indira Awas Yojna) NFSM (National Food Security Mission) RKVY (Rashtriya Krishi Vikas Yojna) BRGF (Backward Regions Grant Fund) RGGVY (Rajiv Gandhi Grameen Vidyutikaran Yojna) NRHM (National Rural Health Mission) SSA (Sarva Shiksha Abhiyan) MdM (Mid Day Meal) IWMP (Integrated Watershed Management Plan) PMGSY (Pradhan Mantri Gram Sadak Yojna) ICDS (Integrated Child Development Scheme) SGSY (Swaranjayanti Grameen Swarojgar Yojna) Scheme for Universal Access and Quality at Secondary Stage NHM (National Horticulture Mission) Macro Management of Agriculture Scheme Central Rural Sanitation Program NLRMP (National Land Records Management Program) TSC (Total Sanitation Campaign) APDRP (Accelerated Power Development and Reform Program) RMSA (Rashtriya Madhyamik Shiksha Abhiyan) ARWSP (Accelerated Rural Water Supply Program)

ii To meet Policy Aspiration for Broad Band

a Teledensity of the country is 73%, while broadband density is only 1.4%.
b Vision: BB on demand
c Increase rural teledensity from 35 to 60 by 2017 and 100 by 2020.
d Affordable and reliable broadband on demand by 2015.
e Achieve 175 Million Connection by 2017
f And 600 Million Connection by 2020 at minimum 2 mbps speed and higher speed upto 100 mbps on demand.
g Recognize Telecom and BB connectivity as a basic necessity like education and health and work towards, " Right to Broadband"
h Many Information and communication (ICT) application such as e-commerce, e-banking, e-governance, e- education and tele-medicine require high speed internet connectivity.

18.4.2 NOFN Applications In Panchayats

i **Panchayat Management:-**
- Gram sabha meetings, village records,
- updating of citizen databases,
- Effective performance monitoring of Panchayats.

ii **Community Participation :-**
- Intra-village, Intra-district sharing of practices and resources ,
- Communication with Block, and District

iii **Knowledge Dissemination :-**
- Sharing of Agricultural practices, productivity techniques ,
- Small enterprises, Vocational learning

iv Delivery of Citizen Services:-
- Delivery of services including Health, Education and Finance, etc ,
- Single point of Government to citizen interaction for Centrally sponsored/Central sector/ State sponsored schemes ,Grievance redressal**.**

v Developmental planning :-
- Road, transportation and power connectivity ,
- Knowledge connectivity in the form of good educational & training institutions ,
- Provision of drinking water and up-gradation of existing health facilities ,
- Market connectivity to enable farmers to get the best prices for their produce.

18.4.3 NOFN Statistics

- About 850 million population resides in 600,000 villages/ 250,000 Village Panchayats.
- Village Panchayat is the lowest level of governance in rural India Average population of 500 to 5,000.
- Panchayat are administered by 6,600 Blocks and 651 Districts.
- OFC POP reaches all Districts, Blocks and some major Panchayts of about 60,000.
- Government is implementing to connect 250,000 Village Panchayats on OFC within two years by laying 500,000 Route Km OFC over existing 1000,000 Km .

18.4.4 **NOFN Roadmap**

- Bridge the gap in Aggregation Layer by extending the existing networks
- 2.5 lakh Gram Panchayats (Village Govt Office) to be connected on Optical Fiber
- Approx 100 MB bandwidth at each Gram Panchayat
- Non discriminatory Access to all SPs
- Access Layer OFC to be provided through market dynamics
- CUG connectivity to be provided at Gram Panchayats (Village Govt Office) for G2C services
- Approx 5 lakh km new incremental OFC required
- Approx 4 to 5 lakh km of dark fiber from existing OFCs of BSNL/Railtel/Powergrid required on long term lease basis
- A High Level Committee (HLC) formed on 25-April-11 to guide the project

18.5 ROLE OF BBNL (BHARAT BROADBAND NETWORK LIMITED)

- BBNL is a The Special Purpose Vehicle (SPV) to implement and operate the project
- BBNL is a PSU set up under companies act by Govt of India under Rule 1956 has been registered on Feb 25, 2012 for management and Operation of NOFN.
- Constitution of BBNL Director Planning ,Director Operation , Director Finance working under CMD BBNL
- Vision of BBNL is **"To become the leading Telecom company to provide secure, reliable, affordable and high quality connectivity across India."**
- NOFN Phase I -Government of India has approved on 25-10-2011 for the setting up of National Optical Fiber Network (NOFN) to provide connectivity to 2.5 lakh Gram Panchayats (Village Govt Office) of the country using optical fiber, which would ensure broadband connectivity with adequate bandwidth. This is to be achieved utilizing the existing optical fiber and extending it to the Gram Panchayats (Village Govt Office) .
- NOFN Phase II - Bharat Broadband Network Ltd (BBNL) is in the process of building the National Optical Fiber Network (NOFN) that aims at providing broadband connectivity up to all 2,50,000 Gram Panchayats (Village Govt Office) across India.
- As part of this initiative, BBNL outsources the work of laying fiber initially connecting approximately 50,000 Gram Panchayats (Village Govt Office), that in turn laying an estimated 120,000 kilometres of optical fiber cable and connecting it to pre-determined end points. Survey has been completed for more than ninety percent of the Gram Panchayats (Village Govt Office). MoU for Right of Way has also been signed with most of the states and union territories

18.5.1 **Other Institutes And Agencies Involved For NOFN Project**

- DOT (Department of Telecommunications Govt of India) :- Secretariat service to the Project
- USOF: The Funding Agency via Ministry of Finance under Planned schemes.
- TAC(Technical Advisory Committee) under the chairmanship of Advisor to the Principal Advisor Scientific Advisor to PM, CDOT, BSNL, Railtel, Powergrid, USOF, NIC, TCIL.

- BSNL, Railtel, Powergrid: Executing Arm they will lay the OFC and lease the existing resources to NOFN/BBNL to optimally usage of resources .
- TCIL (Telecommunications Consultants India Ltd) :-Quality check and Project implementation scheme monitoring.
- C-DOT(Centre for Development of Telematics):-Technology provider and NMS (Network Management Service) Development.
- NIC (National Informatics Centre) :-GIS (geographic information system)Service provider and major user of the project

18.6 NOFN FEATURES

- GIS mapping of all BSNL OFC routes completed and validated once
- Detailed survey will be conducted by respective Circle through Nodal Unit created in each SSA of BSNL
- L-14 diagrams prepared for each OLT
- NMS by CDOT
- Estimate to be prepared by the SSA on the basis of detailed survey and plan
- Estimate will be sanctioned by BBNL
- NOFN shall be built using indigenous hardware e.g GPON (Gigabit Passive Optical Network) will be used for NOFN Project)
- NOFN shall have at least 1 Gbps capacity at the Panchayat level.
- NOFN shall provide at least 100 mbps at the panchayat level in exchange of right of way by states, with backhaul up to district level.
- NOFN shall be a 365x24 reliable, robust, scalable and available IP capable network to ensure continuous availability of services.
- NOFN Shall Lease Dark Fiber / Lambda (Launch Alien Lambda) / Bandwidth On Long term Lease (IRU) from BSNL, RailTel, PowerGrid and others as and when necessary on the existing and available fiber.
- NOFN shall have a national network operating center (NOC) using NMS with full visibility of the network, all activities observable in real time, and controllable from a central location at element level.

18.6.1 **Progress Of NOFN Project**

- Govt of India has approved the project of NOFN
- 2.5 Lac Panchayats with minimum 100 Mbps speed
- Aimed at providing various E-Gov applications,
- Support Telecom operators to roll out services in rural areas thereby enabling access of best technologies to the rural population.
- Amount of Rs 25,000 crores have already been sanctioned by the Govt for this project which will be funded through USOF (Universal service obligation fund).

18.6.2 **BSNL Infrastructure Provider For NOFN**

- Bandwidth Provider
- User of NOFN are access operators (TSPs/ISPs/Cable TV Operators)
- Enable them to launch various access services
- B2B, No retailing ;Operator of operators (Carrier of Carriers)

- Non-discriminatory access to all licensed operators
- Seeks to trigger Ecosystem opening up new Rural markets
- Detailed survey conducted by respective Circle through Nodal Unit created in each SSA of BSNL
- BSNL has been asked by the government to meet 70% of the countrywide cable laying, trenching and ducting work to take high-speed internet to 2.5 lakh village blocks.
- The total project involves laying 5 lakh route kms of optic fibre cables.

18.7 CONCLUSION

Government of India has approved on 25-10-2011 for the setting up of National Optical Fiber Network (NOFN) to provide connectivity to 2.5 lakh Gram Panchayats (Village Govt Office) of the country using optical fiber, which would ensure broadband connectivity with adequate bandwidth. This is to be achieved utilizing the existing optical fiber and extending it to the Gram Panchayats (Village Govt Office) i.e. by bridging the gap in the Aggregation Layer.