Chapter 12

Broadband Network Management: WAN

Objectives

- Broadband WAN segment
  - IP (has been dealt with earlier)
  - ATM
  - MPLS
  - Optical and MAN feeder network
- ATM
  - Virtual path–virtual circuit (VP-VC) operation
  - Real-time and non-real-time function for broadband service
  - ATM as public and private switched networks
  - Emulated LAN configuration
  - ATM management: M1, M2, M3, and M4 interfaces
  - ATM digital exchange interface management
- MPLS
  - Possesses rich features of IP and good performance of ATM
  - Basic principles of label switching
  - Label switched path, LSP
  - Traffic engineering
  - MPLS OAM
  - Service level management
  - MPLS MIBs
  - MPLS TE MIBs
  - MPLS example
- Optical and MAN feeder network
  - SONET-based MAN
  - SONET transport hierarchy
  - SDH and (D)WDM network
  - SDH management
  - WDM management

Broadband Services

- Broadband Integrated Services Digital Network (BISDN) a.k.a broadband network
  - allow transfer of : Voice, video, and data services
  - define: Transport protocol and medium

- (Basic) Integrated Services Digital Network (ISDN) (The early form of ISDN a.k.a narrowband ISDN)

  - It consists of two basic channels: B-channels, 56-kilobaud rate each, combined with an 8-kilobaud signaling channel, D-channel. Together, they are referred to as 2B + D baud

bɔːd/

Noun COMPUTING, TELECOMMUNICATIONS

1.a unit of transmission speed equal to the number of times a signal changes state per second. For signals with only two possible states one baud is equivalent to one bit per second

2.B channel (bearer) is a telecommunications term which refers to the ISDN **channel** in which the primary data or voice communication is carried. It has a bit rate of 64 kbit/s in full duplex.

3.In the Integrated Services Digital Network (ISDN), the **D-channel** is the channel that carries control and signalling information. (The "D" stands for "delta" channel.) The B-channel ("B" for "bearer") carries the main data.

Broadband Services

- The broadband network and service have contributed significantly to advances:

  - WAN : In the WAN segment, protocols used in addition to IP are ATM (Asynchronous Transfer Mode) , SONET (the Synchronous Optical **Network-American standard**)/SDH (the Synchronous Digital Hierarchy – **international standard**) and MPLS (Multiprotocol Label Switching).

    - ATM Technology
    - *SONET/SDH WAN with data rate as an integral multiple of basic **OC-1 /STS** (Optical Carrier-1/Synchronous Transport Signal)*, which is 51.84 Mbps.

      – SDH (Synchronous Digital Hierarchy) is a standard technology for synchronous data **transmission on optical media**. It is the international equivalent of Synchronous Optical Network (SONet). Both technologies provide faster and less expensive network interconnection than some other traditional equipment

    - MPLS evolved as the broadband protocol and takes advantage of the high performance of ATM and the richness in features of IP and Ethernet.

  - LAN
  - Access Technology

Broadband Services

- The broadband network and service have contributed significantly to advances:
  - WAN
  - LAN

> Emulate =To imitate the function of (another system), as by modifications to hardware or software that allow the imitating system to accept the same data, execute the same programs, and achieve the same results as the imitated system.

- ATM LAN Emulation
  - The services provided by ATM differ from conventional LAN (**TCP/IP LAN**) in three ways. First, ATM is **connection oriented**. Second, ATM makes **one-to-one connection** between pairs of workstations in contrast to the broadcast and multicast mode in conventional LAN. Third, a LAN MAC address is dedicated to the **physical network interface card** and is independent of network topology. The **20-byte ATM address** is not.
  - In order to use ATM in the current LAN environment, it has to fit into the current TCP/IP LAN environment. Because of the basic differences ATM specifications has been developed for LAN emulation (LE or LANE) that emulate services of the current LAN network across an ATM network

- Access Technology
  - Cable modem used HFC (Hybrid fiber coax)
  - DSL (digital subscriber line)
  - Wireless

- A cable modem is a type of network bridge and modem that provides bi-directional data communication via radio frequency channels on a hybrid fibre-coaxial (HFC) and other insrastures

- A hybrid fiber coaxial (HFC) network is a telecommunication technology in which optical fiber cable and coaxial cable are used in different portions of a network to carry broadband content (such as video, data, and voice)

- DSL (Digital Subscriber Line) is a technology for bringing high- bandwidth information to homes and small businesses over ordinary copper telephone lines.

- **OC (Optical Carrier)** - the SONET physical standard that defines an optical signal capable of transmitting STS frames. As the name implies, it is the carrier at a specific data rate for the STS frames. OC-n is a carrier for the STS-n signal.

- **EC (Electrical Carrier)) - the SONET physical standard that defines an electrical signal capable of transmitting STS frames. As the name implies, it is the carrier at a specific data rate for the STS frames. EC-n is a carrier for the STS-n signal.**

- **STS (Synchronous Transport Signal) - the SONET logical standard that defines the framing, payload, and overhead (signaling) for data transmission over either an optical carrier (OC) or in rare cases, an electrical carrier (EC).**

Broadband Services Network

Figure 12.1 shows a broadband network

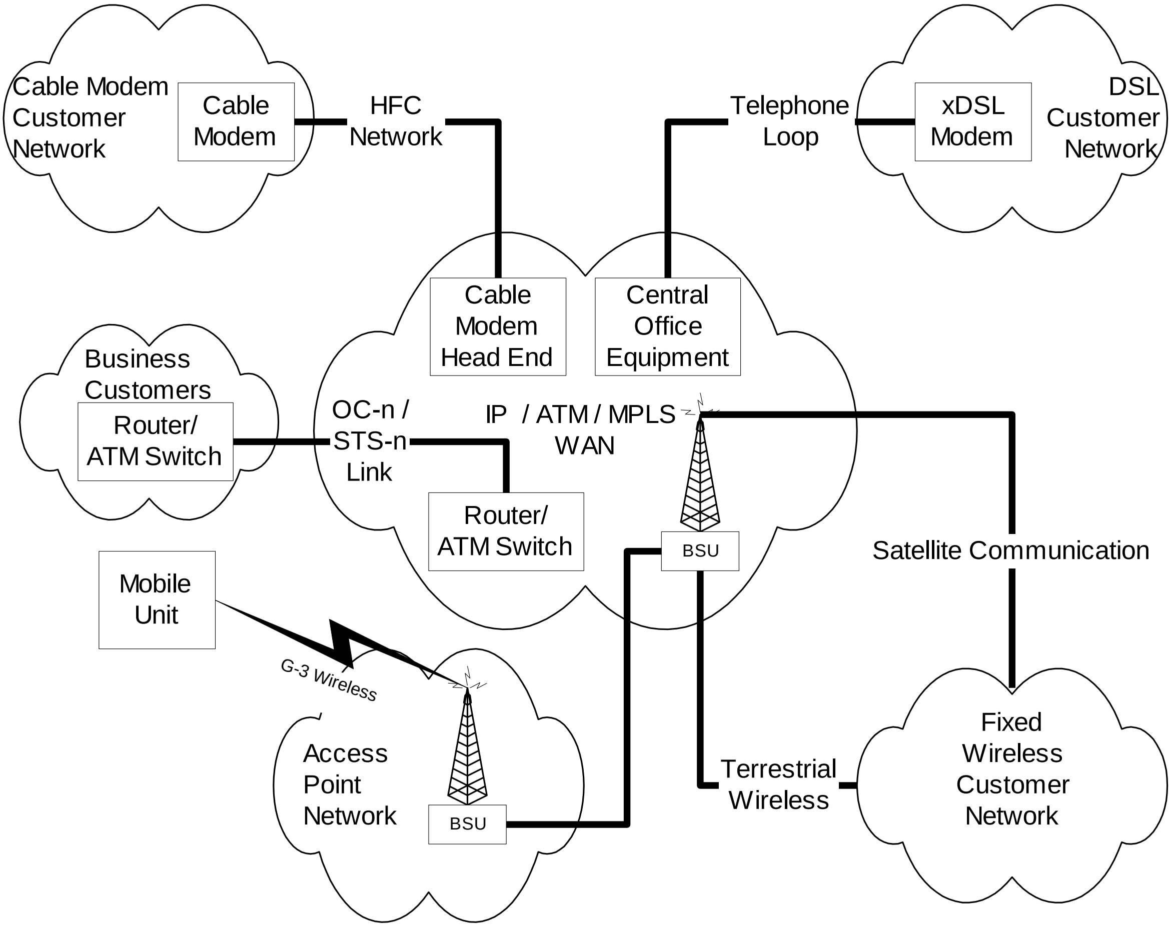


Figure 12.1 Broadband Service Networks

•The WAN is MPLS/IP/ATM. The WAN is linked to the customer premises using either optical links,
OC-n/STS ((Optical Carrier-n Synchronous Transport Signal), or a broadband link with emerging access technology (HFC, xDSL, or wireless).

•The customer network consists of two classes, residential customers and corporate customers with campus-like network. The residential customers are either residential homes or small corporations that use broadband services, but do not require the high-speed access network to WAN. Corporate customers need high-speed access and connect optical or synchronous links (like digital transmission formats E1 and T1) .

ATM Technology

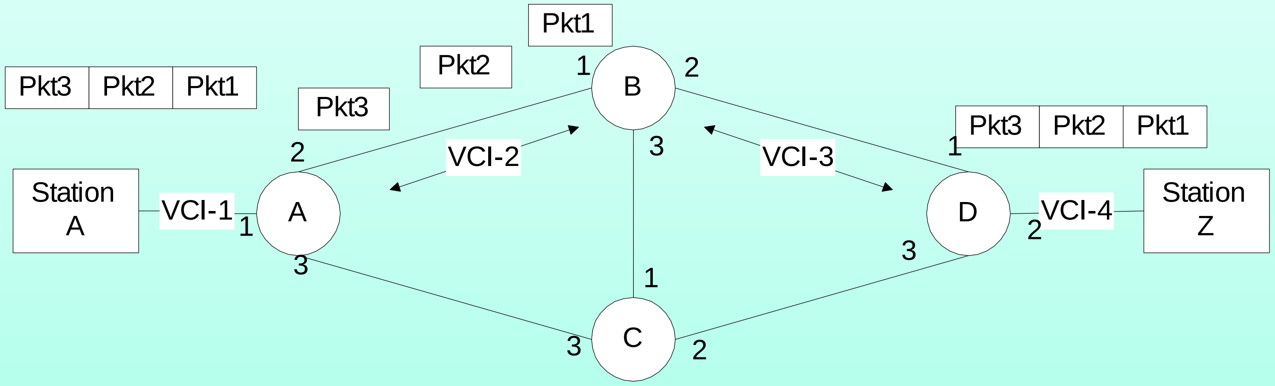
- ATM technology based on:

https://technet.microsoft.com/en-us/library/cc978149.aspx

  - VP (Virtual path)/ VC (Virtual circuit)
  - Fixed packet size or cell
  - Small packet size (53 bytes)
  - Statistical multiplexing
  - Integrated services
  - After initial set up, latency is reduced
  - Variable bit rate
  - Simultaneous real- and non-real time traffic

In telecommunications and computing, **bit rate** (sometimes written **bitrate** or as a variable R) is the number of **bits** that are conveyed or processed per unit of time.

VP - VC



VCI= Virtual Circuit Identifier

Figure 12.2 Virtual Circuit Configuration

Notes

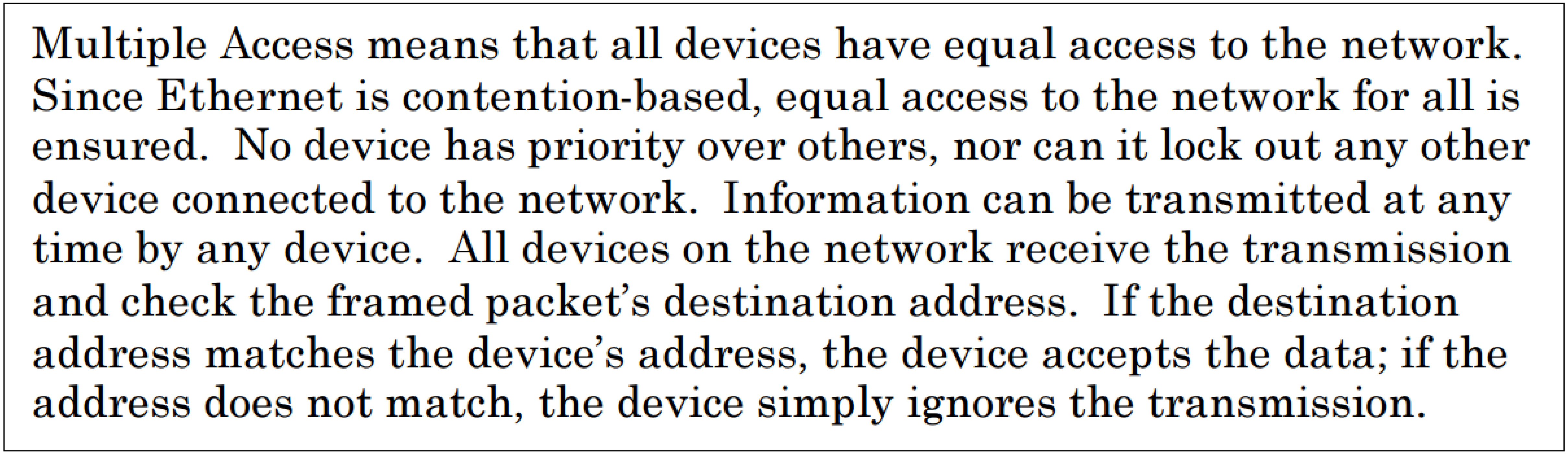
Table 12.2 A-Z Virtual Circuit –Routing Tables

Switch	Input VCI / Port	Output VCI / Port
A	VCI-1 / Port-1 VCI-2 / Port-2	VCI-2 / Port-2 VCI-1 / Port-1
B	VCI-2 / Port-1 VCI-3 / Port-2	VCI-3 / Port-2 VCI-2 / Port-1
D	VCI-3 / Port-1 VCI-4 / Port-2	VCI-4 / Port-2 VCI-3 / Port-1

- All packets take the same path and arrive in the same sequence in virtual circuit
- Packets in a session take the same path in VP/VC
- After initial set up, latency is reduced

ATM LAN Emulation (LANE)

- Difference between ATM and Ethernet
  - ATM is connection-oriented
  - ATM makes one-to-one connection
  - ATM 20-byte addressing scheme different from 6-byte Ethernet MAC address
- LANE emulates services of a traditional LAN



Multiple Access means that all devices have equal access to the network. Since Ethernet is contention-based, equal access to the network for all is ensured. No device has priority over others, nor can it lock out any other device connected to the network. Information can be transmitted at any time by any device. All devices on the network receive the transmission and check the framed packet's destination address. If the destination address matches the device's address, the device accepts the data; if the address does not match, the device simply ignores the transmission.

ATM WAN Reference Model

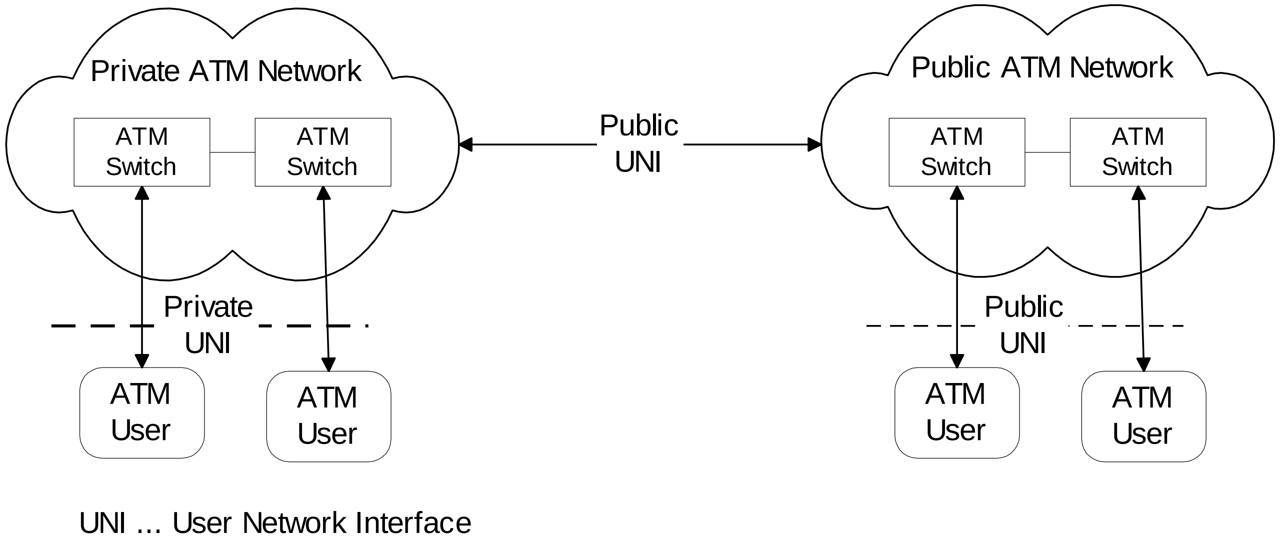


Figure 12.3 Private and Public ATM Network User Network Interfaces

Notes

- WAN service provided by public service providers
- Private networks use public WAN facilities
- Management functions (OAMP)
    - Operations
    - Administration
    - Maintenance
    - Provisioning
- Public and private User Network Interface (UNI) define user interfaces

ATM WAN Management

Figure 12.4 also shows interfaces between an ATM end user or device and an ATM network, as well as interfaces between ATM networks.

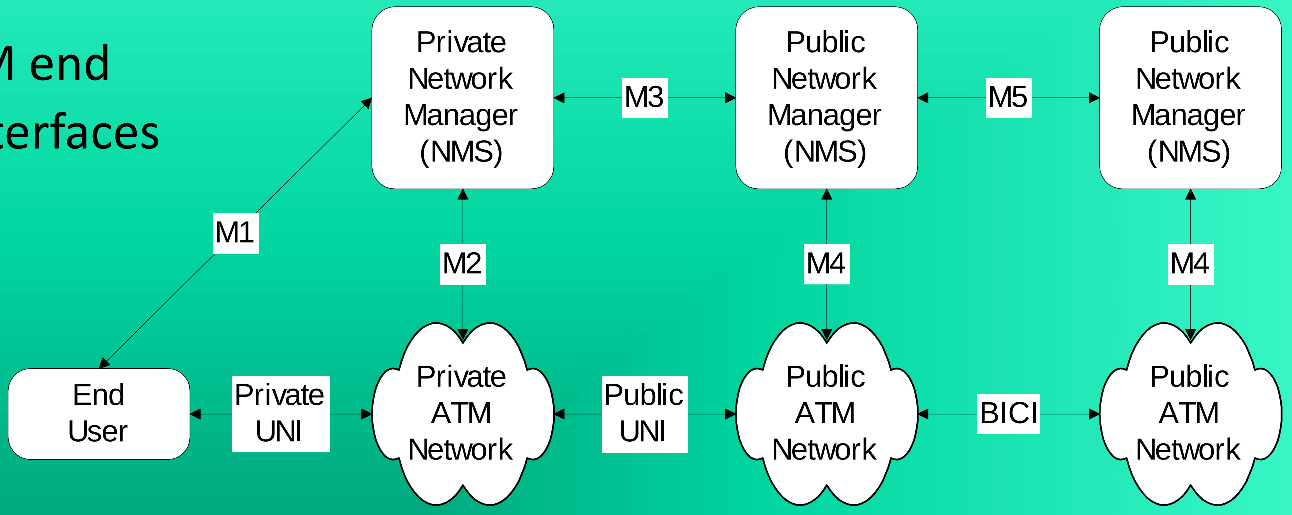
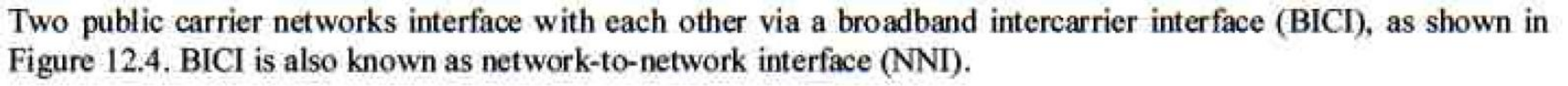


Figure 12.4 ATM Forum Management Interface Reference Architecture

Notes

- Management interface architecture defined by ATM Forum
- Public and private NMS responsible to manage respective domains
- OSI has defined five management interfaces:
  - M1 Interface between private NMS and end user
  - M2 Interface between private NMS and network
  - M3 Interface between private NMS and public NMS
  - M4 Interface between public NMS and network
  - M5 Interface between public NMSs



Two public carrier networks interface with each other via a broadband intercarrier interface (BICI), as shown in Figure 12.4. BICI is also known as network-to-network interface (NNI).

ATM MIB

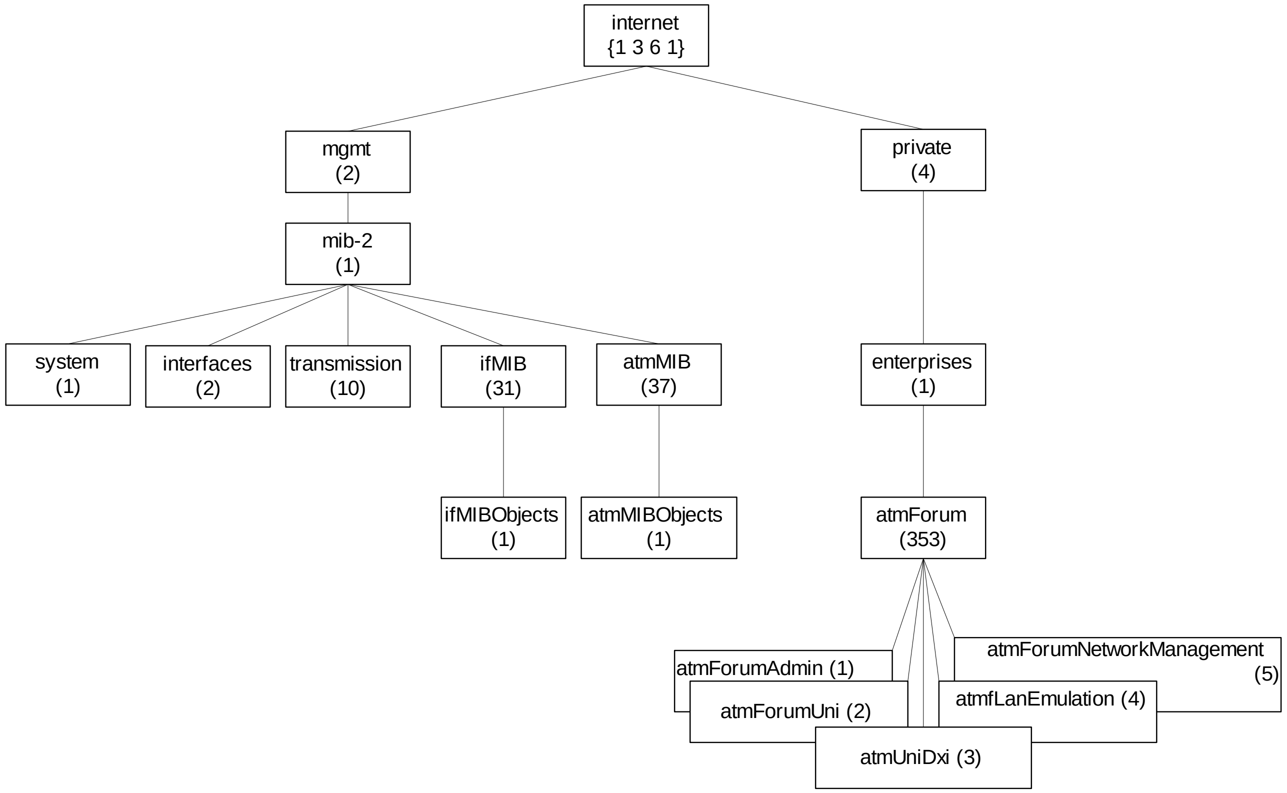


Figure 12.6 Internet ATM MIB

Notes

- MIBs defined in two sets of documents - IETF (5 nodes) & ATM Forum (1 node)
- ATM MIBs address ATM sublayer parameters only
- ifMIB contains additional objects not covered in interfaces MIB
- atmMIB contains ATM objects
- atmForum specifies interfaces, LANE, Mx, and ILMI
- atmRMON (experimental) address ATM remote monitoring (covered in Chapter 8)

SNMP ATM Management

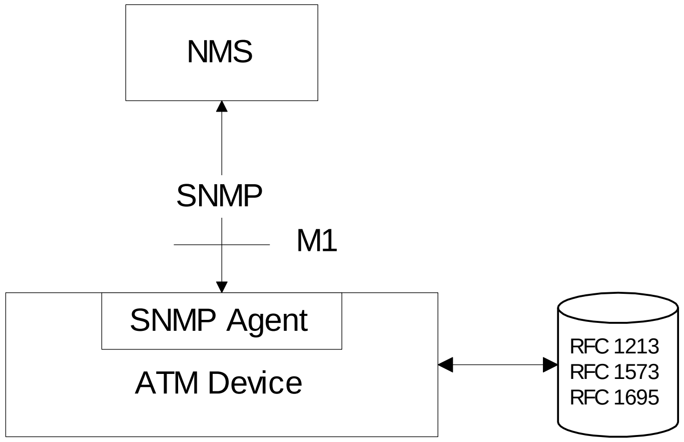


Figure 12.7 SNMP ATM Management (M1 Interface)

Notes

- ATM Management specifications available for both SNMP and OSI management implementations
- SNMP agent built in ATM device
- System, Interfaces, Interface types, transmission carrier groups (T1, T3, SONET), and ATM object groups are monitored

Simplified MPLS Network

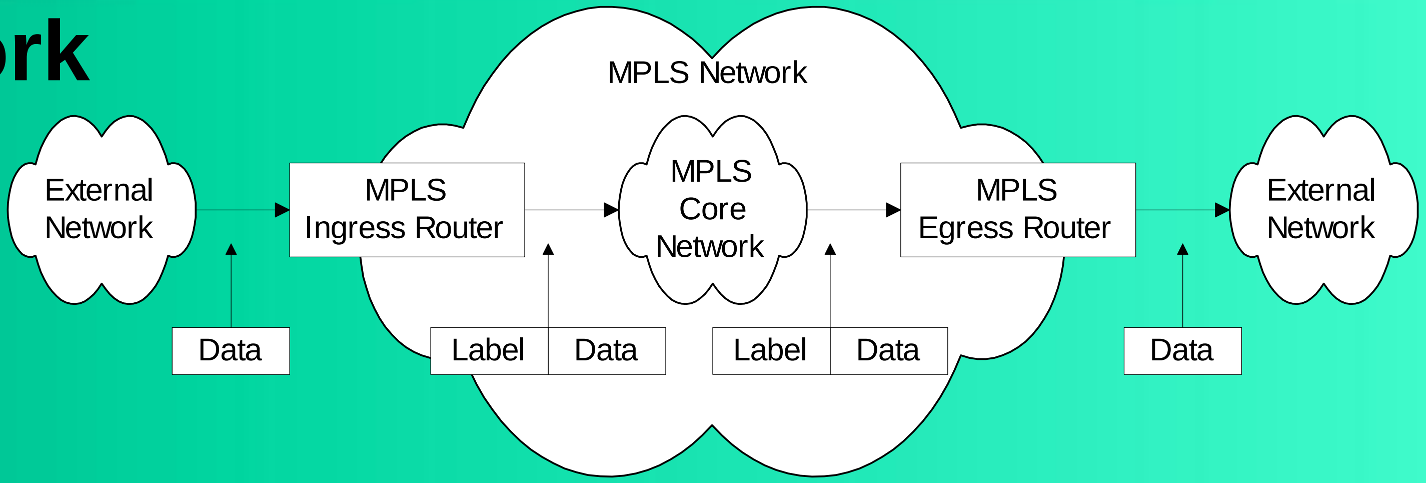


Figure 12.21 Simplified MPLS Network

- **MPLS … Multiprotocol Label Switching is a fast-emerging WAN technology that replaces pure IP and ATM networks. It combines**
  - **Richness of IP**
    - **An IP-based network is rich because of its extensive implementation and compatibility with Ethernet LAN. It routes packets intelligently. However, it is slow in performance as it has to open each packet at the layer 3 level to determine its next hop and its output port**
  - **Performance of ATM**
    - **the ATM protocol is a high-performance cell-based protocol switching cells at the layer 2 level. It is capable of handling real-time and non-real-time traffic simultaneously and thus is superior to the IP-based network. It has been deployed extensively in the WAN. However, its address incompatibility with the popular Ethernet LAN, along with difficult end-to-end circuit provisioning, has limited its usage at the customer premises network and hence related applications.**

- FEC (forward equivalent classes –for paquets-) assigned at the ingress router and encoded   in the label

- Label is removed at the egress router and original   protocol packet is sent out

Simplified MPLS Network

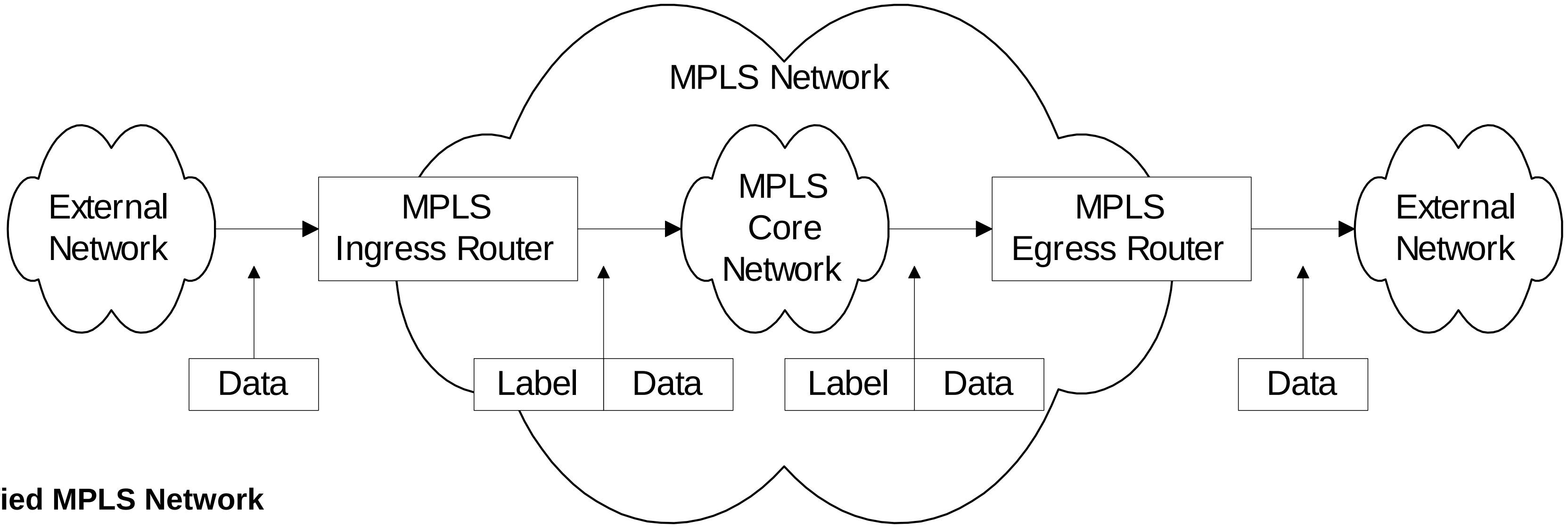


Figure 12.21 Simplified MPLS Network

- MPLS … combines
    - Richness of IP
    - Performance of ATM

- FEC (forward equivalent classes) assigned at the ingress router and encoded in the label

- Label is removed at the egress router and original protocol packet is sent out

The figure shows the MPLS header, named label, added to the packet/ATM cell delivered by the external network to the ingress router and removed by the egress router before delivering to its external router.

IP Network

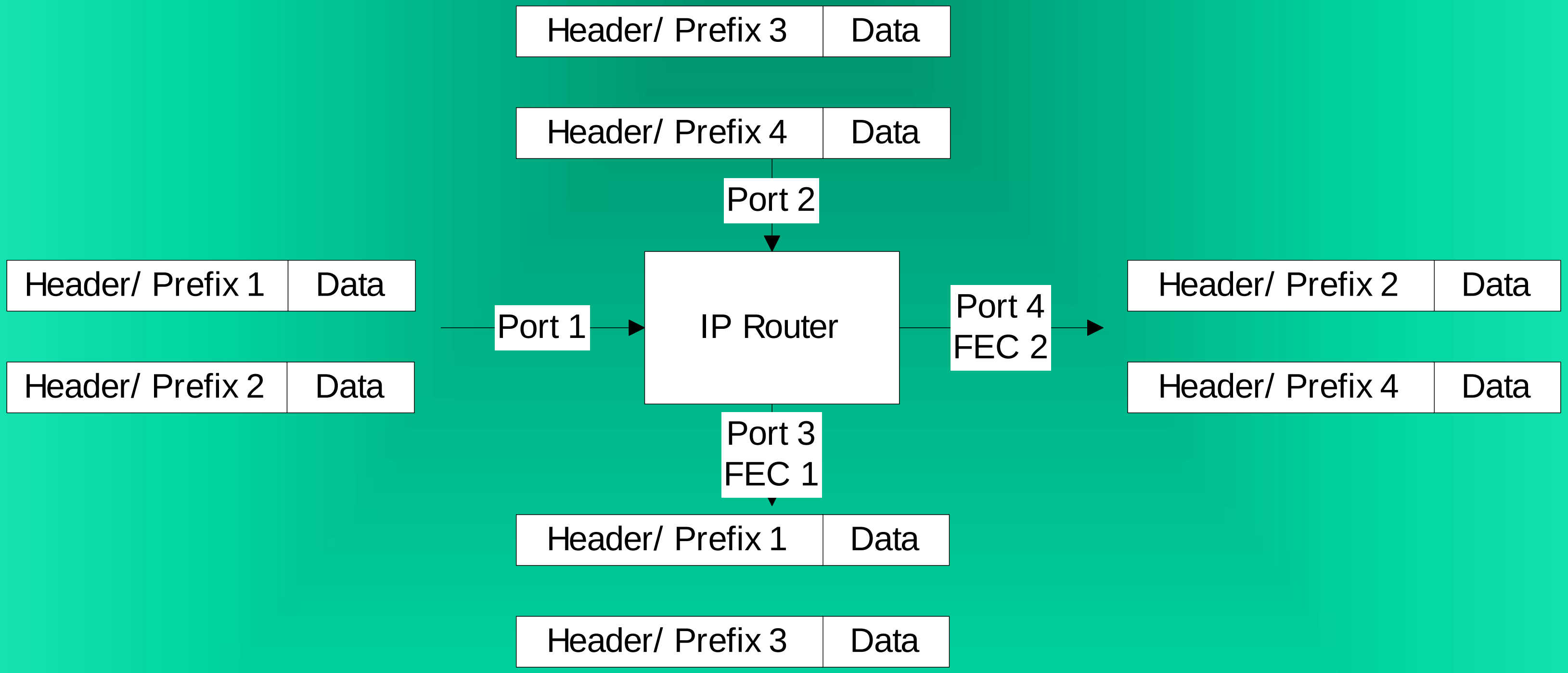


Figure 12.22(a) IP Packet Forwarding Based on the FEC Index Table

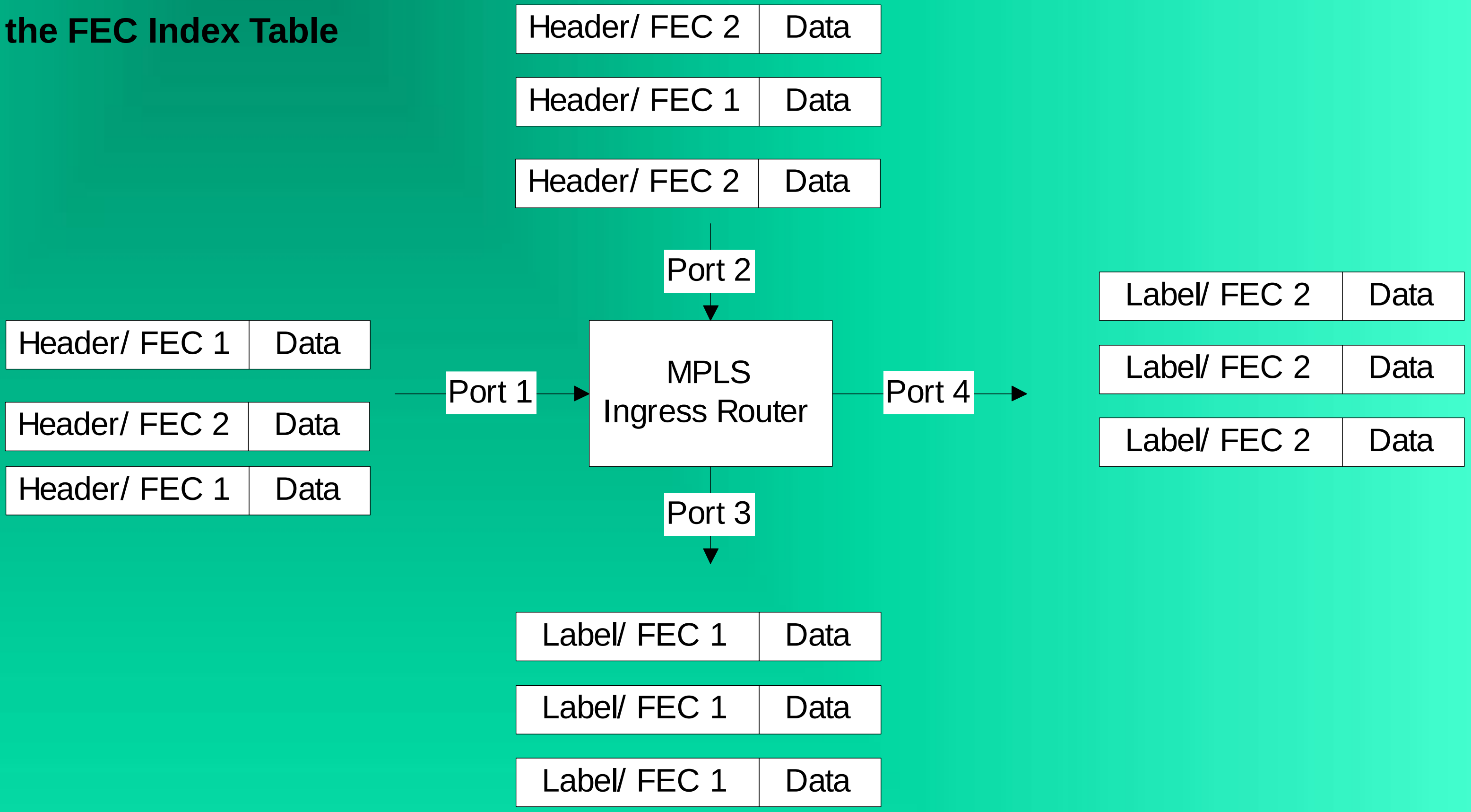
Notes

- FEC (Forward Equivalent Class) decides the port for the next hop
- Packets with the same FEC are indistinguishable and sent to the same port
- **FEC determination is complex and done at each node**
- This leads to low performance (compare with ATM VP-VC achieving high performance)

MPLS / IP Network

Figure 12.22(b) MPLS Packet Forwarding Based on the FEC Index Table

MPLS forwarding can be done by switches that are capable of doing label lookup and replacement



Notes

- **FEC assigned at the ingress router and encoded in the label**
- Label is removed at the egress router and original protocol packet is sent out
- Label is sent along with the packet
- Label is used as index to look up a table and forward the packet and a new label to the next hop
- **Packet not analyzed for FEC by downward routers**
- **Header in layer-3 ignored**

MPLS / ATM

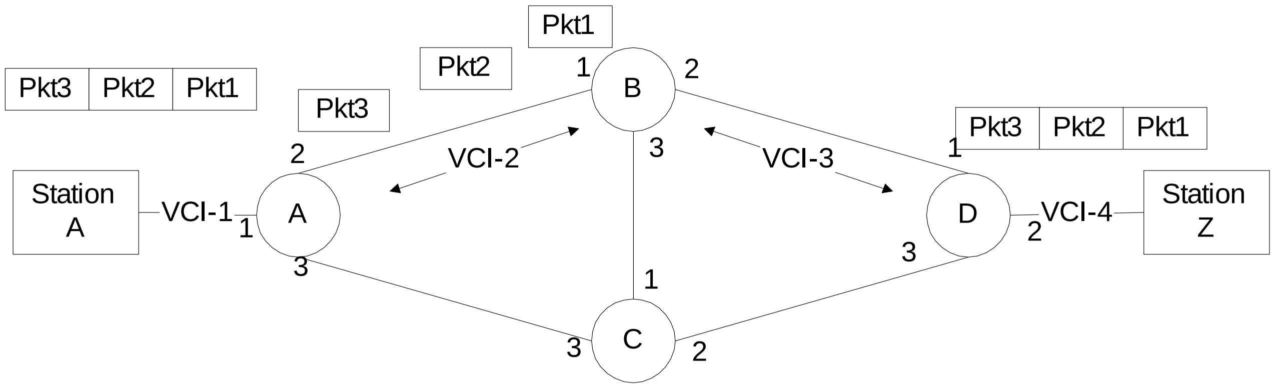


Figure 12.2 Virtual Circuit Configuration

How does MPLS preserves the efficiency of an ATM. In an ATM network, switching is done in layer 2. End-to-end path, “virtual path,” containing “virtual circuit” is determined by the VPI–VCI. This establishes a **virtual circuit-switched path** using “soft” switches. As mentioned earlier, **the MPLS router selects the next hop path using a table just as in the ATM switch and hence is efficient.**

--VPI=Virtual Path Identifier

Notes

Table 12.2 A-Z Virtual Circuit –Routing Tables

Switch	**Input VCI / Port**	**Output VCI / Port**
A	VCI-1 / Port-1 VCI-2 / Port-2	VCI-2 / Port-2 VCI-1 / Port-1
B	VCI-2 / Port-1 VCI-3 / Port-2	VCI-3 / Port-2 VCI-2 / Port-1
D	VCI-3 / Port-1 VCI-4 / Port-2	VCI-4 / Port-2 VCI-3 / Port-1

- All packets take the same path and arrive in the same sequence in virtual circuit
- Packets in a session take the same path in VP/VC
- After initial set up, latency is reduced
- Both real- and non-real time traffic handled simultaneously

MPLS Traffic Configuration

- In MPLS, packets with input labels are mapped to next hop with output labels. The header in layer 3 is ignored. **Once a packet is assigned an FEC, no further analysis is done by subsequent routers ; header in layer 3 ignored**

- **Packet routing configured for MPLS / IP with IGP with and without TE (traffic engineering) and tunneling**

Notes

- An interior gateway protocol (IGP) is **a type of protocol used for exchanging routing information between gateways** (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.
- **Network traffic engineering is a method of optimizing the performance of a telecommunications network by dynamically analyzing, predicting and regulating the behavior of data transmitted over that network.** Traffic engineering is also known as teletraffic engineering and traffic management. The techniques of traffic engineering can be applied to networks of all kinds, including the PSTN (public switched telephone network), LANs (local area networks), WANs (wide area networks), cellular telephone networks, proprietary business and the Internet.

MPLS / IP without Tunnel

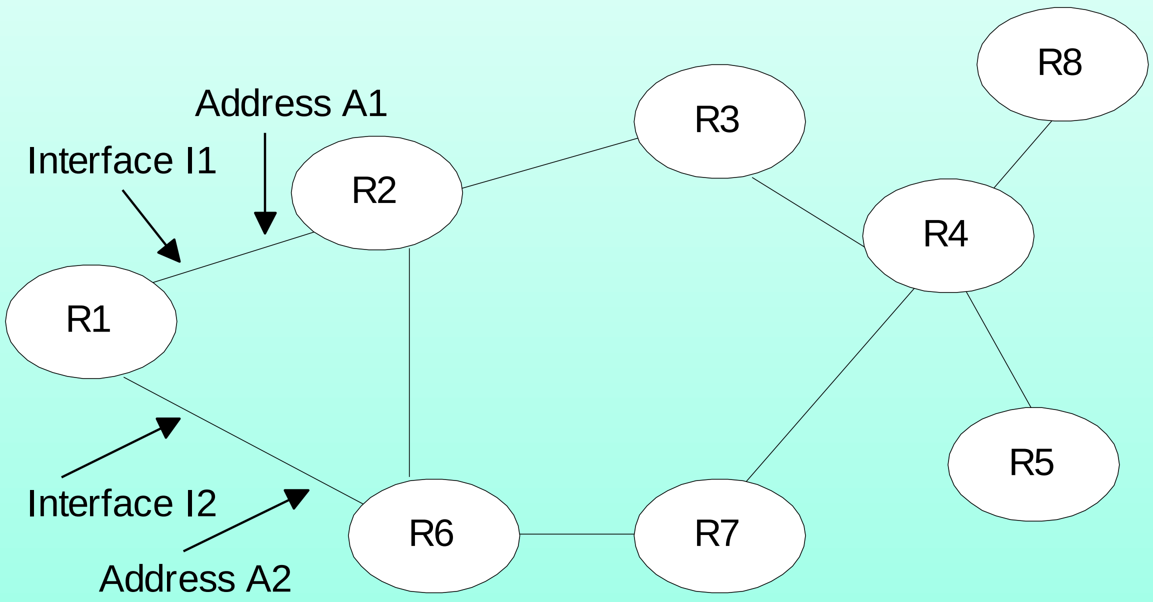


Figure 12.23 Topology without MPLS Tunnels

Notes

Table 12.12 R1 Routing Table without Tunnel

Dest	0utput Interface	Next Hop	Metric
2.2.2.2	I1	2.2.2.2	1
3.3.3.3	I1	2.2.2.2	2
4.4.4.4	I1 I2	2.2.2.2 6.6.6.6	3 3
5.5.5.5	I1 I2	2.2.2.2 6.6.6.6	4 4
6.6.6.6	I2	6.6.6.6	1
7.7.7.7	I2	6.6.6.6	2
8.8.8.8	I1 I2	2.2.2.2 6.6.6.6	4 4

- **Figure 12.23 illustrates IP routing with Interior Gateway Protocol (IGP) without traffic engineering (TE) and tunnels for router R1**

- For simplicity, the IP addresses of the routers are designated as i.i.i.i for each router Ri.

- Table 12.12, shows the output interface (logical port) and next hop for packets emanating from R1 to Ri. The last column in the table shows the metric of the number of hops from R1 to the destination router. **The paths are chosen using IGP. For example, there are two choices for the label-switched path (LSP) from R1 to R4, both of which are shown in Table 12.12. The two paths are R1–R2–R3–R4 and R1–R6–R7–R4. They both have the same metric of 3 hops. The former is transmitted via logical port I1 of R1 and the latter I2 of R2.**

- As can be observed, the router knows only its neighbor router in its routing table.

MPLS / IP with Tunnels

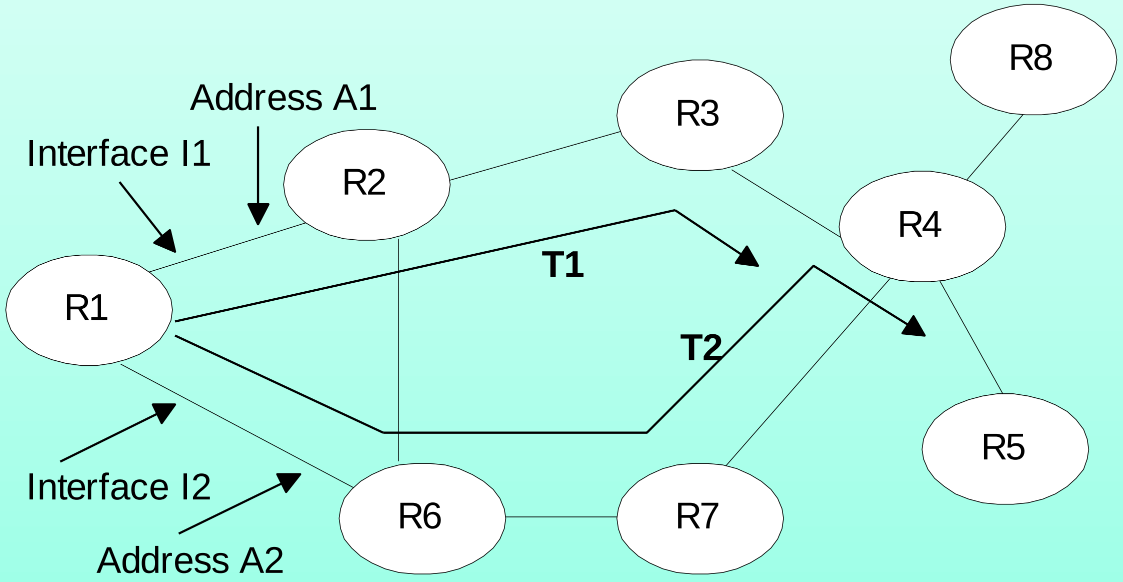


Figure 12.24 MPLS Topology with Tunnels

Notes

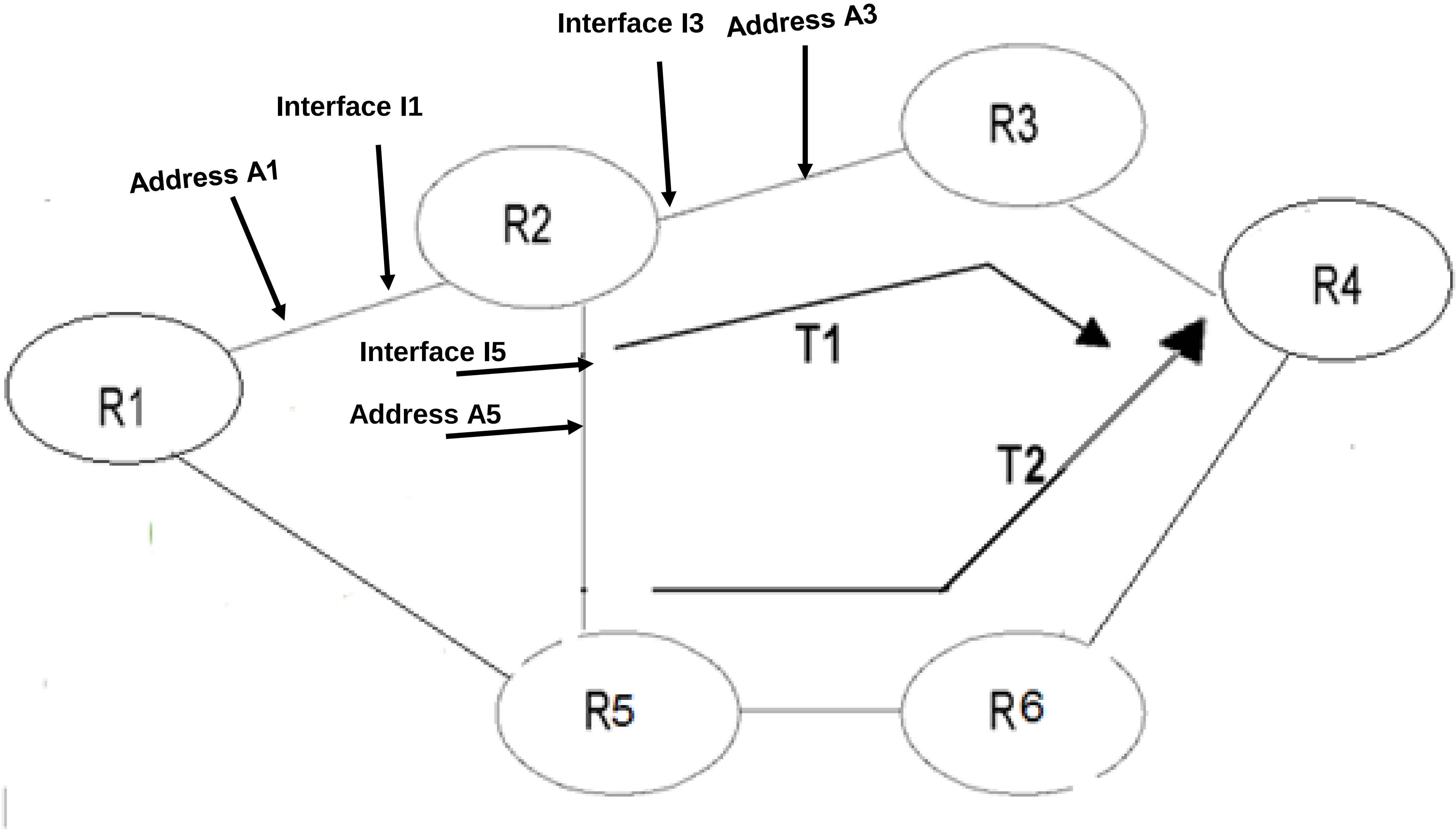
Table 12.13 R1 Routing Table with Tunnel

Dest	0 Intf	Next Hop	Metric
2.2.2.2	I1	2.2.2.2	1
3.3.3.3	I1	2.2.2.2	2
4.4.4.4	T1	4.4.4.4	3 /1
5.5.5.5	T2	5.5.5.5	4/1
6.6.6.6	I2	6.6.6.6	1
7.7.7.7	I2	6.6.6.6	2
8.8.8.8	T1	4.4.4.4	4/2

- LSPs (label-switched paths) for the same topology used in the MPLS protocol with MPLS-TE and tunnels are shown in Figure 12.24, and the routing table in the label-switching router (LSR) R1 is presented in Table 12.13.

- The LSRs (Label Switching Router) R4 and R5 are directly reached from R1 through tunneling. The transit time delay is low and the throughput is higher as the intermediate routers in the tunnel behave as pass through. The path from R1 to R4 now exits out of the logical port T1 and has the next hop as R4.

- There are two metrics shown for educational purpose. It is three if no absolute value for the tunnel path metric. If an absolute value, in our case chosen as 1, the value of the metric is 1. For the case of an LSP from R1 to R5, the corresponding metrics are 4 and 1.


Interface I3
Address A3
Interface I1
Address A1
R3
R2
R4
T1
Interface I5
Address A5
R1
T2
R5
R6

MPLS-TE

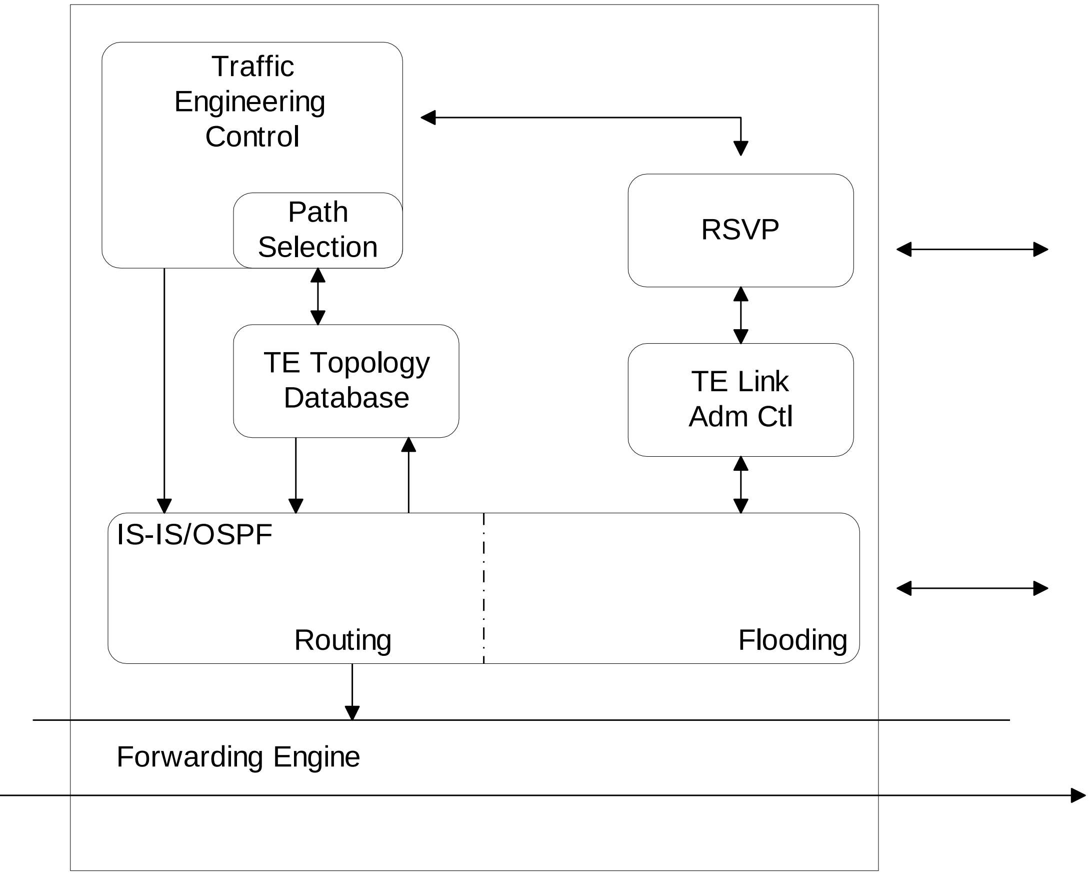


Figure 12.25 MPLS-TE System Block Diagram (Head-End Router)

Notes

•Traffic Engineering (TE): Optimization of performance

- Overlay over inadequate IGP
  - Constrained-base routing at VC level
  - VC paths
  - Path compression
  - Call admission control
  - Traffic shaping and policing
  - VC survivability

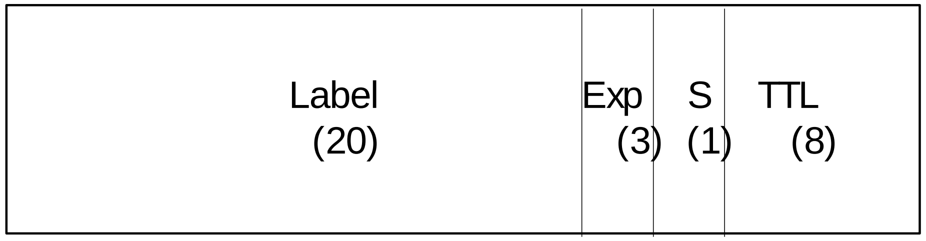
❑ In MPLS traffic engineering, all configurations are done on a specific network node called the headend or ingress node. Here is where all tunnels and constraints are created. **Tunnel destination address is also specified at the headend.**

Label Switching Router (LSR)

- MPLS router called Label Switching Rouer (LSR)
- End-to-end MPLS path called Label Switching Path (LSP)
- IGP extended to include MPLS-TE
- Route set up by RSVP-TE
- Control and data *planes* separated in MPLS
- VoIP handled using SIP (Session Initiation Protocol)

RSVP-TE: Resource Reservation Protocol - Traffic Engineering is an extension of the resource reservation protocol (RSVP). It supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. RSVP runs on both IPv4 and IPv6. **RSVP-TE generally allows the establishment of MPLS label switched paths (LSPs), taking into consideration network constraint parameters such as available bandwidth and explicit hops.**

MPLS Label



Label (20)	Exp (3)	S (1)	TTL (8)

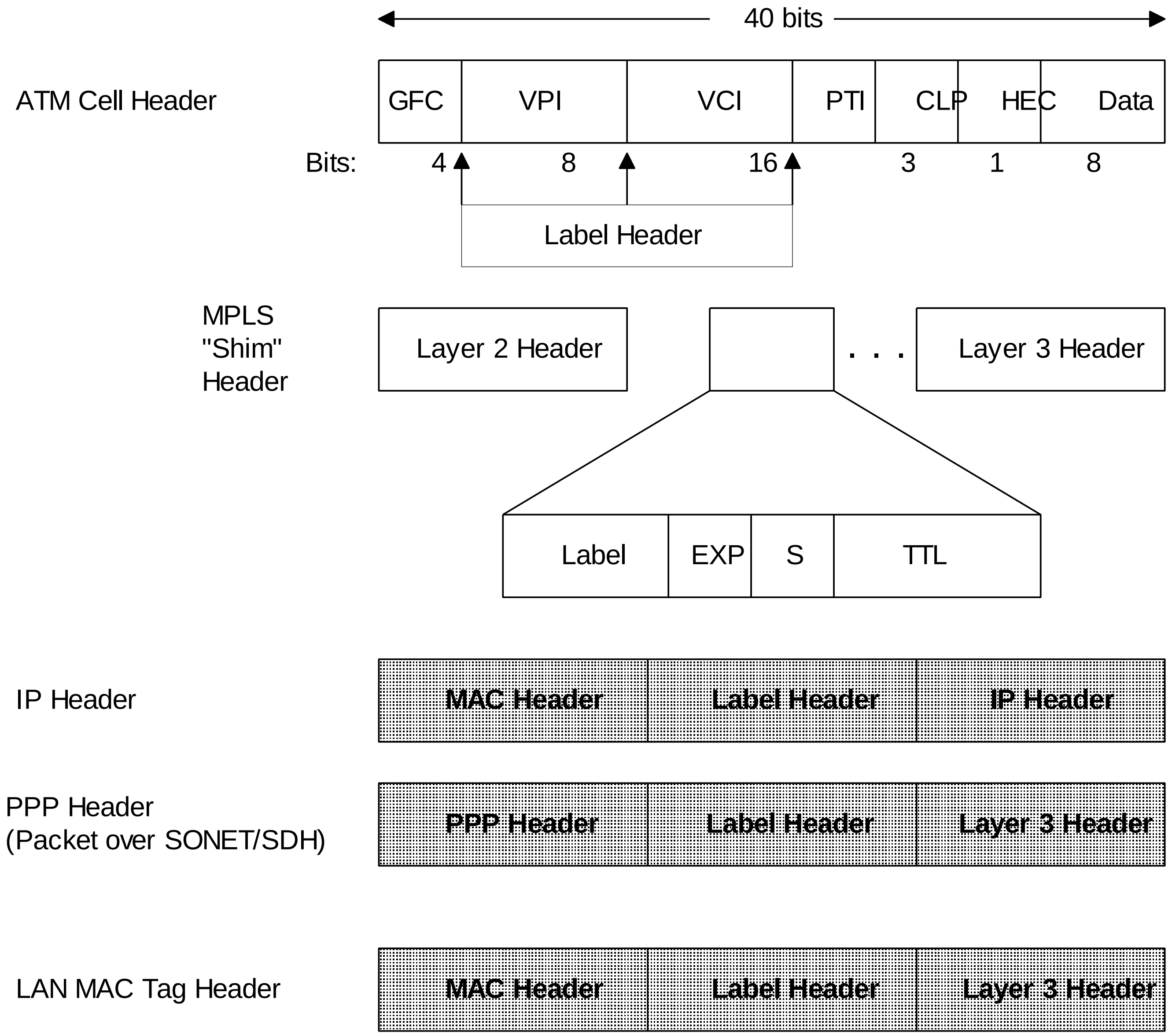
Figure 12.26 MPLS Shim Header

Exp…experimental
S…….stack indicator
TTL….time-to-live

Notes

- MPLS Label is
  - Short and fixed length – 32 bits
  - FEC locally significant identifier
- Label assigned by the downstream router
- Label is “shimmed” between layers 2 and 3 headers

MPLS Labeled Packets



40 bits

ATM Cell Header

GFC | VPI | VCI | PTI | CLP | HEC | Data

Bits: 4 8 16 3 1 8

Label Header

MPLS "Shim" Header

Layer 2 Header . . . Layer 3 Header

Label | EXP | S | TTL

IP Header: MAC Header | Label Header | IP Header

PPP Header (Packet over SONET/SDH): PPP Header | Label Header | Layer 3 Header

LAN MAC Tag Header: MAC Header | Label Header | Layer 3 Header

GFC	= 4-bit Generic Flow Header	VPI	= Virtual Path Identifier
VCI	= Virtual Circuit Identifier	PTI	= 3-bit Payload Type
CLP	= Congestion Priority	HEC	= Header Error Control
(CRC)			

Figure 12.27 Encapsulation of an MPLS-Labeled Packet

Label Generation

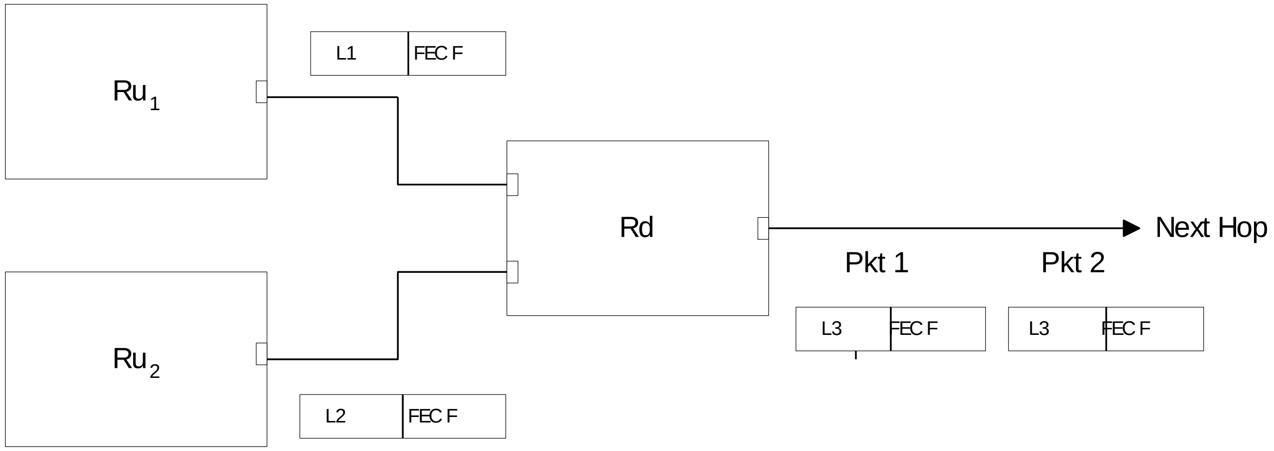


Figure 12.28 Label Generation

Notes

- Label generated by downstream LSR R_d
- Upstream LSR R_u and R_d together generate "label" between label Lx and FEC F
- R_d has incoming labels L1 and L2, and outgoing label L3 with FEC F
- Label L associated with FEC F is local to R_u and R_d
- R_u and R_d called "label binding pair"

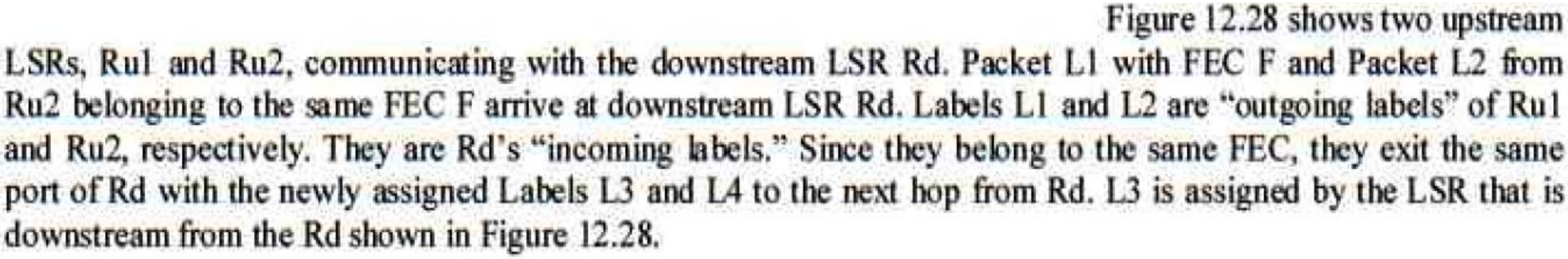


Figure 12.28 shows two upstream LSRs, Ru1 and Ru2, communicating with the downstream LSR Rd. Packet L1 with FEC F and Packet L2 from Ru2 belonging to the same FEC F arrive at downstream LSR Rd. Labels L1 and L2 are "outgoing labels" of Ru1 and Ru2, respectively. They are Rd's "incoming labels." Since they belong to the same FEC, they exit the same port of Rd with the newly assigned Labels L3 and L4 to the next hop from Rd. L3 is assigned by the LSR that is downstream from the Rd shown in Figure 12.28.

LSP, LSR, Label

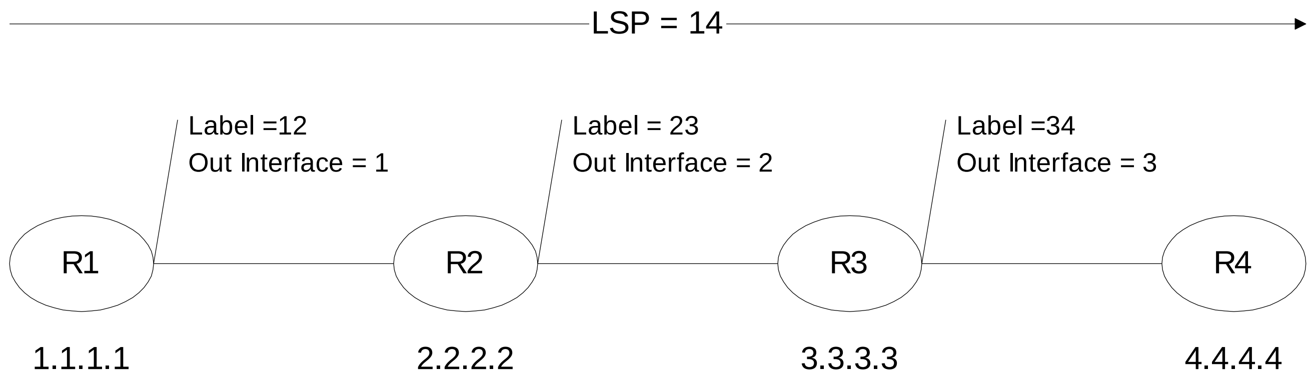


Figure 12.29(a) LSP, LSRs, and Labels without Tunnel

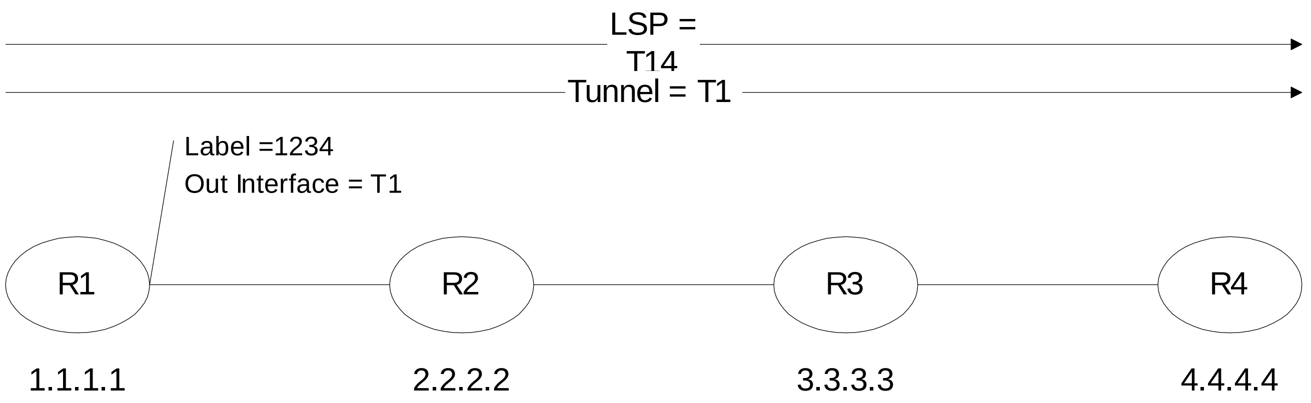


Figure 12.29(b) LSP, LSRs, and Labels with Tunnel

MPLS OAMP Management

- Data and control planes are separate in MPLS
- OAM packets travel the data path; OAM packets follow the data path (operations, administration, and maintenance)
- The MPLS layer can be visualized as the layer positioned between layers 2 and 3 and hence OAM of MPLS needs to address both networks, namely ATM/MPLS and IP/MPLS.

- Basic Tools
  - LSP connectivity verification (! End-to-end MPLS path called Label Switching Path)
  - LSP ping
  - LSP traceroute
- Fault management
- Configuration management
- Performance management

Data and control planes = Data and control channels

Fault Management of LSP

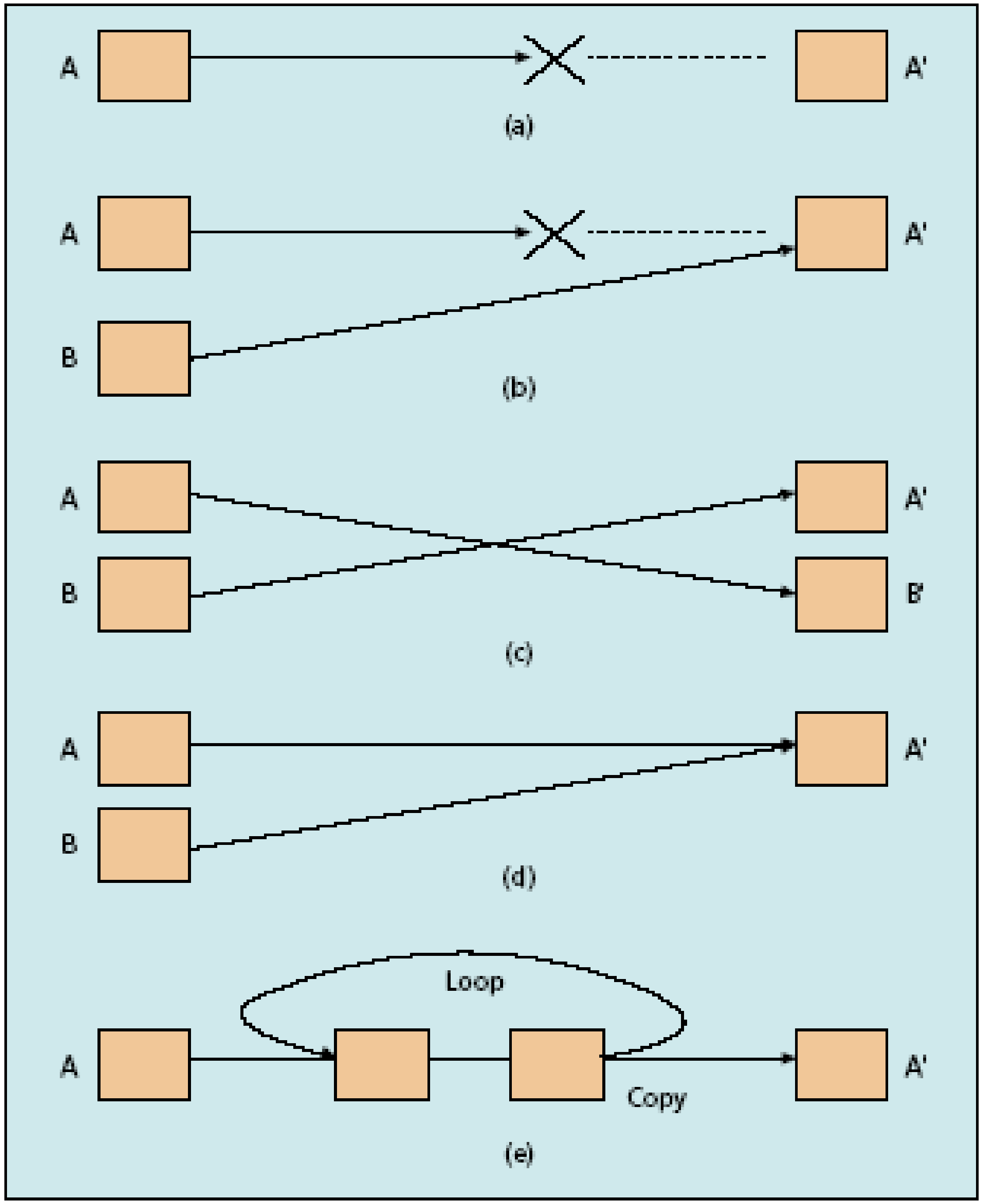


Figure 12.30 MPLS Fault Scenarios

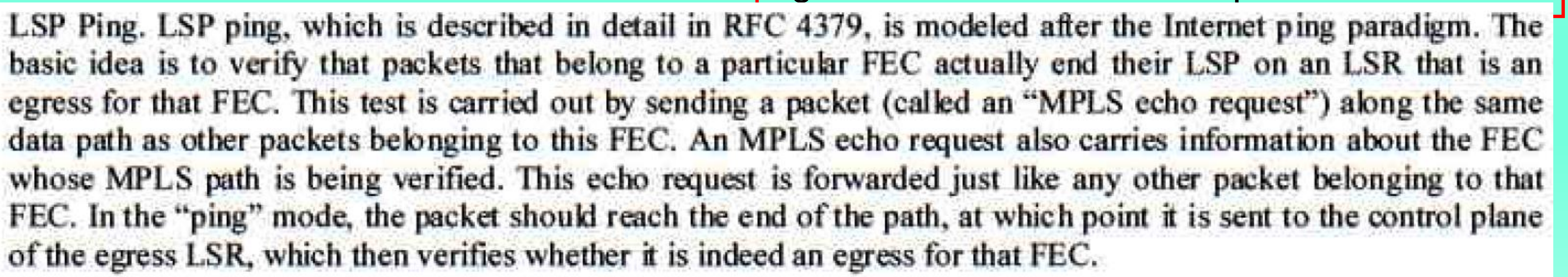
- When an LSP fails to deliver a packet to the egress LSR, the failure can be due to several reasons :
  - (a) Simple loss of connection
  - (b) Misconnection
  - (c) Swapped connection
  - (d) Mismerging
  - (e) Loop/unintended replication
- **Detection of LSP fault using**
  - **connectivity verification (CV) – ITU-T**
  - **Bidirectional forwarding detection (BFD) - IETF**

LSP Ping

Table 12.15 MPLS Echo Request Packet

Byte 1	Byte 2	Byte 3	Byte 4
Version Number		Global Flags	
Message Type	Reply Mode	Return Code	Return Subcode
Sender’s Handle			
Sequence Number			
TimeStamp Sent (seconds)			
TimeStamp Sent (microseconds)			
TimeStamp Received (seconds)			
TimeStamp Received (microseconds)			
TLV			

- **Modified Internet ping**
- **MPLS echo request from Ingress to egress LSR; response from egress LSR on connectivity and validation**
- Verify packets of specific FEC end their LSP on an LSR that is an egress for that FEC.
- Packet travels data path to egress LSR and transferred to control plan
- Control plane validates FEC belongs to the egress LSR and sends response



LSP Ping. LSP ping, which is described in detail in RFC 4379, is modeled after the Internet ping paradigm. The basic idea is to verify that packets that belong to a particular FEC actually end their LSP on an LSR that is an egress for that FEC. This test is carried out by sending a packet (called an “MPLS echo request”) along the same data path as other packets belonging to this FEC. An MPLS echo request also carries information about the FEC whose MPLS path is being verified. This echo request is forwarded just like any other packet belonging to that FEC. In the “ping” mode, the packet should reach the end of the path, at which point it is sent to the control plane of the egress LSR, which then verifies whether it is indeed an egress for that FEC.

LSP Traceroute

- Similar to IP traceroute
- Hop-by-hop fault localization as well as path tracing
- Packet sent to control plane of each transit LSR
- Transit LSR validates LSP
- Validates control plane against data plane of the LSR

Notes

Connectivity Verification

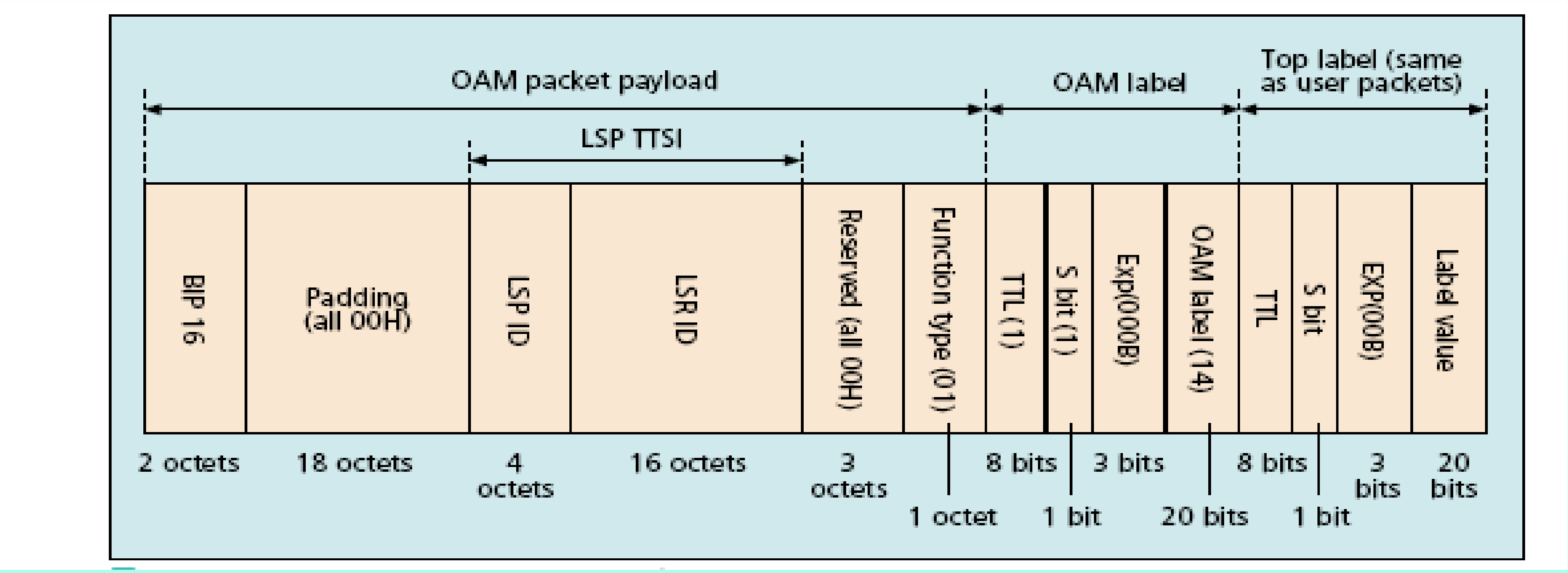


Figure 12.31 Connectivity Verification Packet

Notes

- Top label user packet label
- 2nd label OAM label with reserved value of 14
- Stack bit value 1 indicates bottom label
- **Ingress LSR sends CV packet with TTSI (trail termination source identifier) – LSP and LSR IDs**
- **CV packets sent asynchronously at regular intervals**
- **On consecutive loss of set number of packets (3) egress LSR declares loss of connectivity (dIOCV)**
- Other scenarios analyzed by egress LSR and notifications sent

BFD

- Bidirectional forwarding failure detection
- An IETF specification (CV is ITU-T spec); more versatile

- Uses LSP-ping MPLS echo - response to detect data plane failure in LSP

- Helpful to detect failures in the data plane when the control plane is functional and data plane is not

- Establishes session between ingress and egress LSRs

- Verification packet can be used at any protocol layer

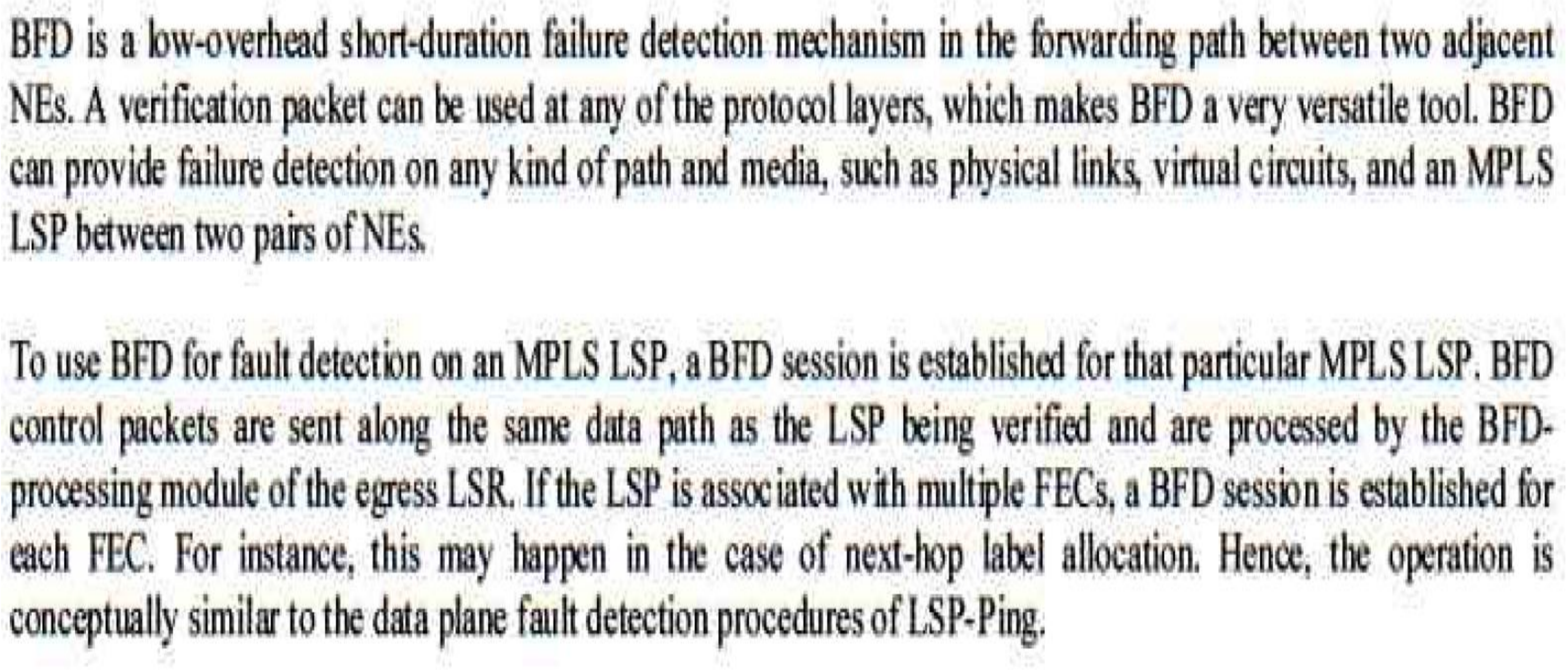
- Fast and low overhead detection between adjacent Nodes

- BFD fault detection interval should be longer than switching time in the fast-reroute LSP

- Separate session for multiple FECs in an LSP

- LSP traceroute used for data path check in alternate paths

BFD



BFD is a low-overhead short-duration failure detection mechanism in the forwarding path between two adjacent NEs. A verification packet can be used at any of the protocol layers, which makes BFD a very versatile tool. BFD can provide failure detection on any kind of path and media, such as physical links, virtual circuits, and an MPLS LSP between two pairs of NEs.

To use BFD for fault detection on an MPLS LSP, a BFD session is established for that particular MPLS LSP. BFD control packets are sent along the same data path as the LSP being verified and are processed by the BFD-processing module of the egress LSR. If the LSP is associated with multiple FECs, a BFD session is established for each FEC. For instance, this may happen in the case of next-hop label allocation. Hence, the operation is conceptually similar to the data plane fault detection procedures of LSP-Ping.

LSP Self-Test

- Used for fault localization of an LSP
- Uses 3 LSRs, ST (self test), LSR-U upstream, and LSR-D downstream
- LSR-ST sends special LSP-ping to LSR-U with TTL=3
- LSR-U forwards it via LSR-ST to LSR-D with TTL=2
- LSR-D sends reply to LSR-ST completing the test
- Fault localized for link and node failures and notification sent out

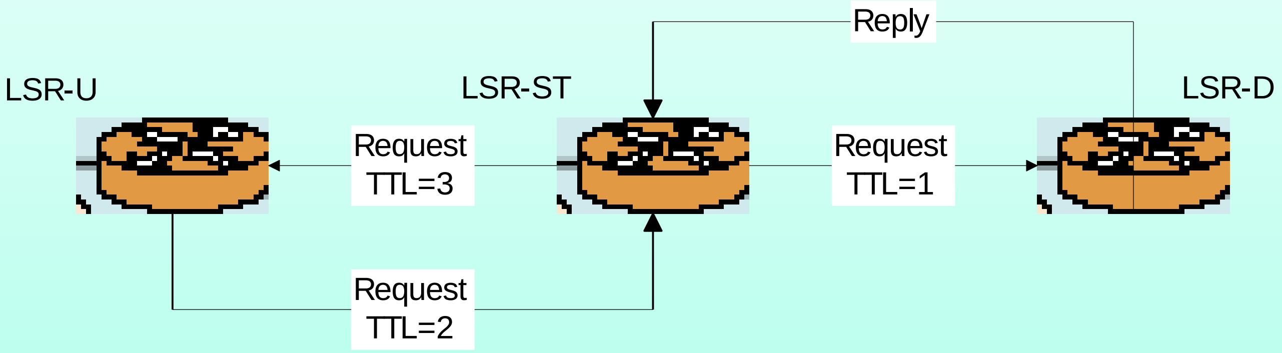
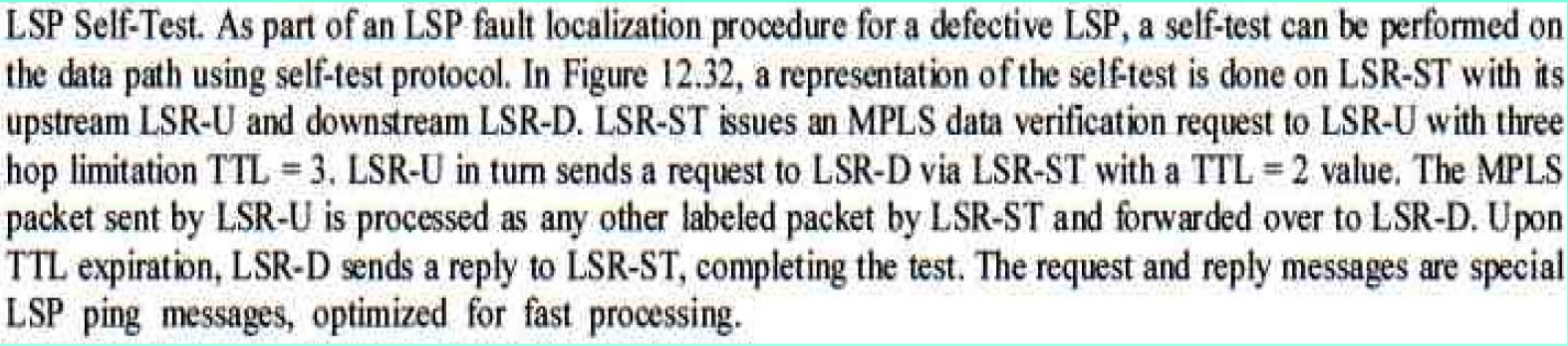


Figure 12.32 LSP Self-Test



LSP Self-Test. As part of an LSP fault localization procedure for a defective LSP, a self-test can be performed on the data path using self-test protocol. In Figure 12.32, a representation of the self-test is done on LSR-ST with its upstream LSR-U and downstream LSR-D. LSR-ST issues an MPLS data verification request to LSR-U with three hop limitation TTL = 3. LSR-U in turn sends a request to LSR-D via LSR-ST with a TTL = 2 value. The MPLS packet sent by LSR-U is processed as any other labeled packet by LSR-ST and forwarded over to LSR-D. Upon TTL expiration, LSR-D sends a reply to LSR-ST, completing the test. The request and reply messages are special LSP ping messages, optimized for fast processing.

MPLS Service Level Management

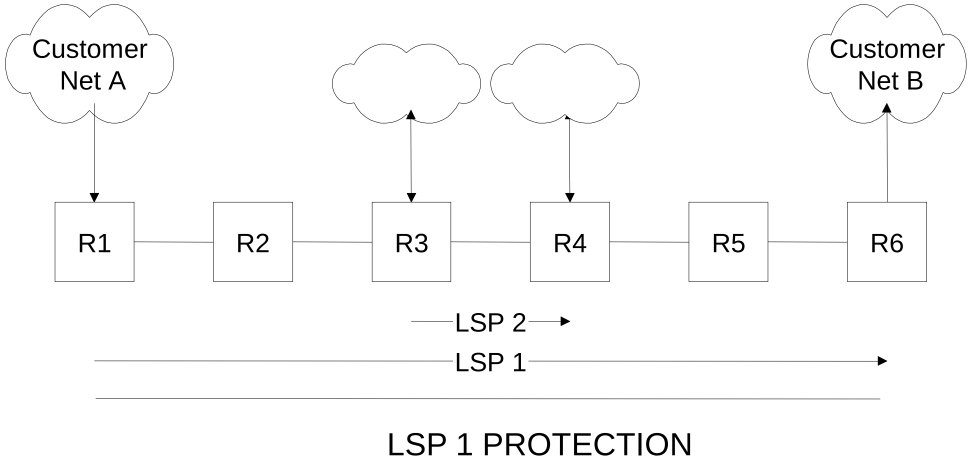


Figure 12.33 LSP Nesting and Fault Localization

Notes

- SLA between Service Provider and customer
- Multiple protection paths
- LSP1 PROTECTION global protection
- Nested path LSP 2 local protection path

MPLS MIB OID Tree

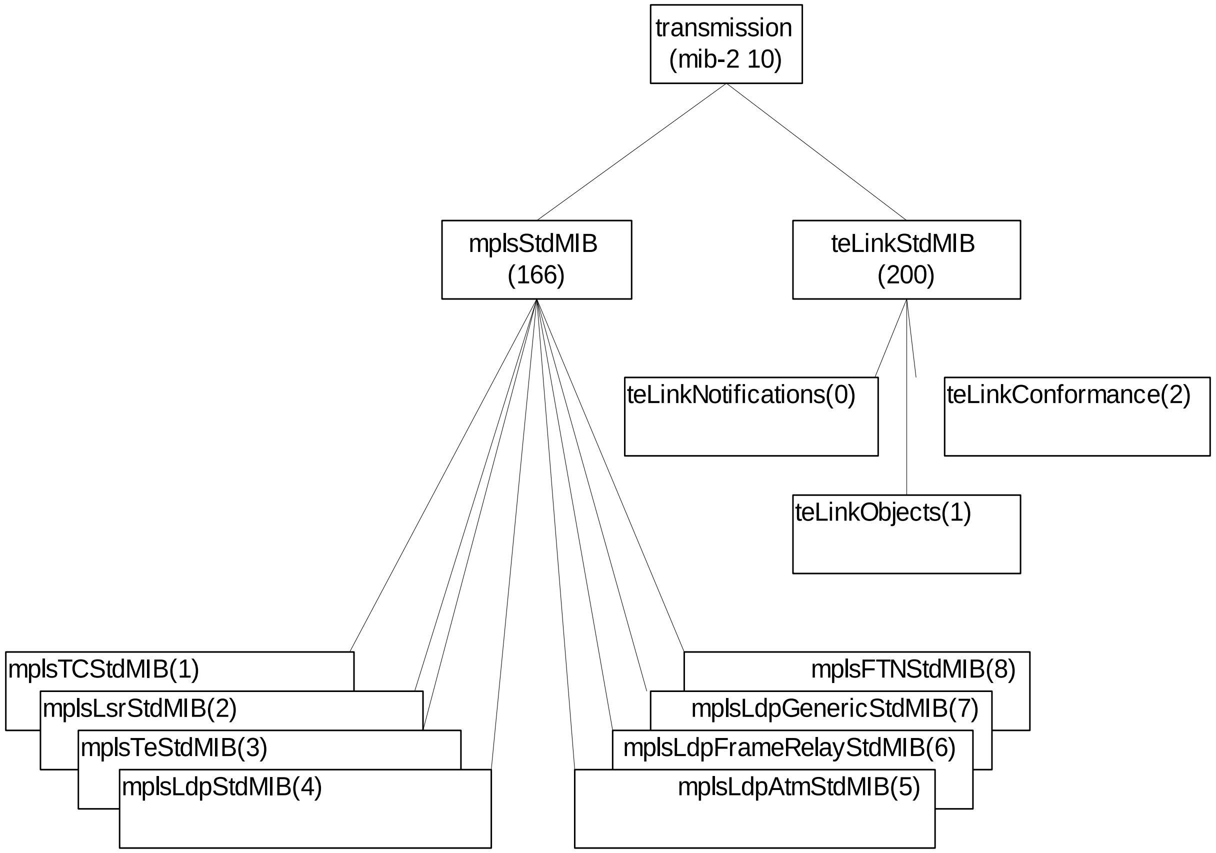


Figure 12.34 MPLS MIB OID Tree

Notes

- MPLS network has a range of MIB modules
- Complex and interdependent modules
- Two nodes under transmission (mib-2 10)
  - mplsstd MIB…MPLS OID group
  - teLinkstdMIB…MPLS Traffic engineered links

MPLS MIBs

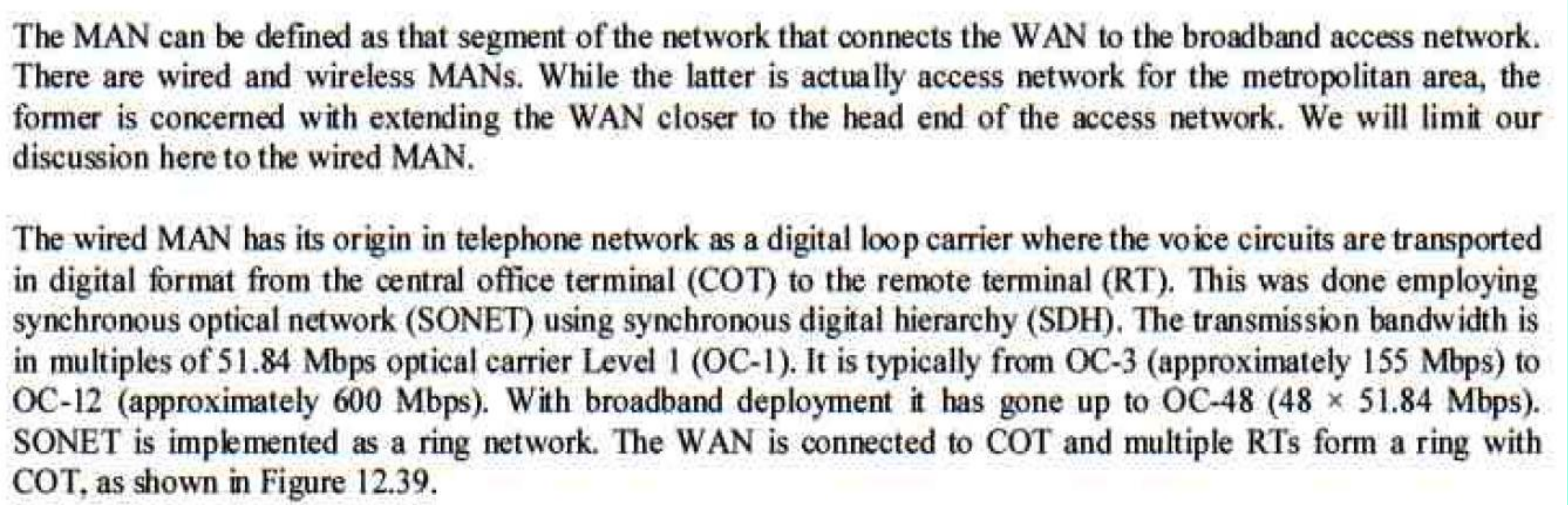
Table 12.16 MPLS Object Identifier (OID) MIB Group

Entity	**OID**	**Description (brief)**
mplsStdMIB	transmission (166)	MPLS OID Group
mplsTCStdMIB	mplsStdMIB (1)	Defines textual conventions
mplsLsrStdMIB	mplsStdMIB (2)	LSR Managed Objects (MO)
mplsTeStdMIB	mplsStdMIB (3)	Traffic Engineered Tunnel MO
mplsLdpStdMIB	mplsStdMIB (4)	Label Distribution Protocol (LDP) MO
mplsLdpAtmStdMIB	mplsStdMIB (5)	MO used with MPLS-LDP-STD-MIB for MPLS/ATM as layer 2
mplsLdpFrameRelayStdMIB	mplsStdMIB (6)	MO used with MPLS-LDP-STD-MIB for MPLS/Frame Relay as layer 2
mplsLdpGenericStdMIB	mplsStdMIB (7)	LDP Per Platform Label Space reserved for other platforms
mplsFTNStdMIB	mplsStdMIB (8)	FTN MO (FEC-to-NHLFE (Next Hop Label Forwarding Entry)

Notes

- MPLS-LSR-STD-MIB heart of the MPLS management architecture
- MPLS-LSR-STD-MIB describes managed objects for modeling MPLS LSR and comprises:
    - Label-forwarding info base (LFIB) -> View of LSP being switched by the LSR
    - Cross-connects and their properties referred in other MPLS MIBs

Optical Metropolitan Area Network (MAN)



The MAN can be defined as that segment of the network that connects the WAN to the broadband access network. There are wired and wireless MANs. While the latter is actually access network for the metropolitan area, the former is concerned with extending the WAN closer to the head end of the access network. We will limit our discussion here to the wired MAN.

The wired MAN has its origin in telephone network as a digital loop carrier where the voice circuits are transported in digital format from the central office terminal (COT) to the remote terminal (RT). This was done employing synchronous optical network (SONET) using synchronous digital hierarchy (SDH). The transmission bandwidth is in multiples of 51.84 Mbps optical carrier Level 1 (OC-1). It is typically from OC-3 (approximately 155 Mbps) to OC-12 (approximately 600 Mbps). With broadband deployment it has gone up to OC-48 (48 × 51.84 Mbps). SONET is implemented as a ring network. The WAN is connected to COT and multiple RTs form a ring with COT, as shown in Figure 12.39.

Notes

- MAN…segment that connects WAN to Access Network
- Wired (incl fiber) and wireless (WiMax) MAN
- Wired MAN evolved from digital loop carrier (DLC)
- Link SONET (synchronous optical network) ring using SDH (synchronous digital hierarchy)
- STM-1 (synchronous transport module level 1) @155.52 Mbps. STM-4 @ 622.08 Mbps (OC-3), etc.
- RT is add-drop multiplexer (ADM)
- Protocol is RPR (resilient packet ring)
- RTs connected to access networks

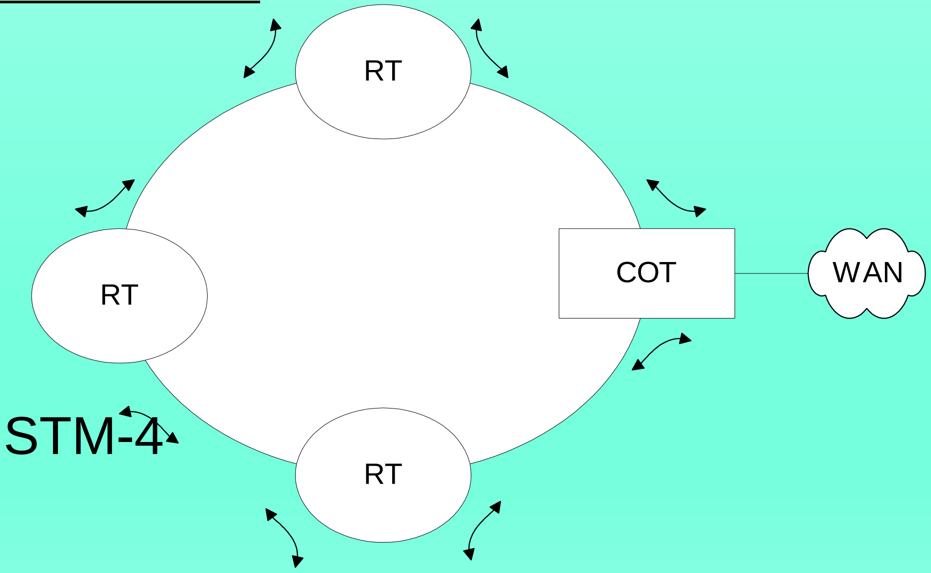
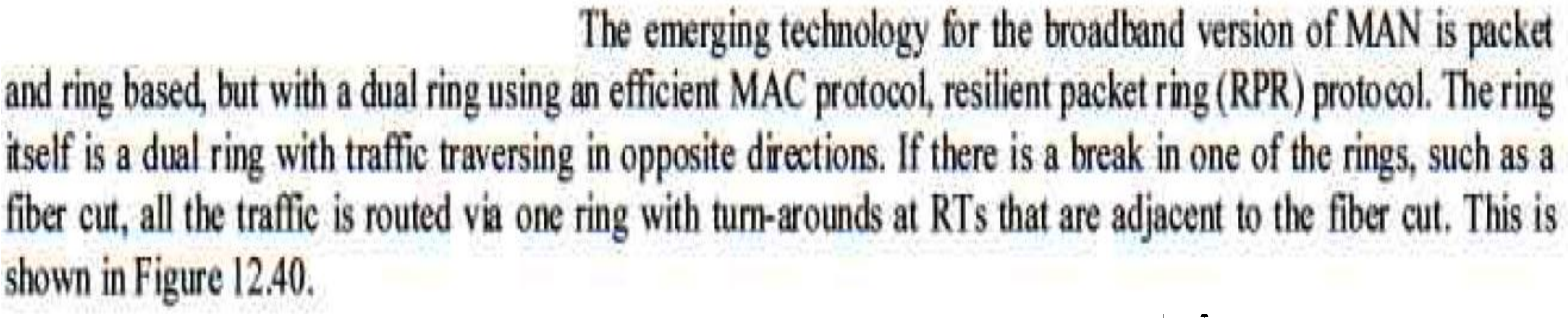


Figure 12.39 SONET-Based MAN

Dual Ring Configuration



The emerging technology for the broadband version of MAN is packet and ring based, but with a dual ring using an efficient MAC protocol, resilient packet ring (RPR) protocol. The ring itself is a dual ring with traffic traversing in opposite directions. If there is a break in one of the rings, such as a fiber cut, all the traffic is routed via one ring with turn-arounds at RTs that are adjacent to the fiber cut. This is shown in Figure 12.40.

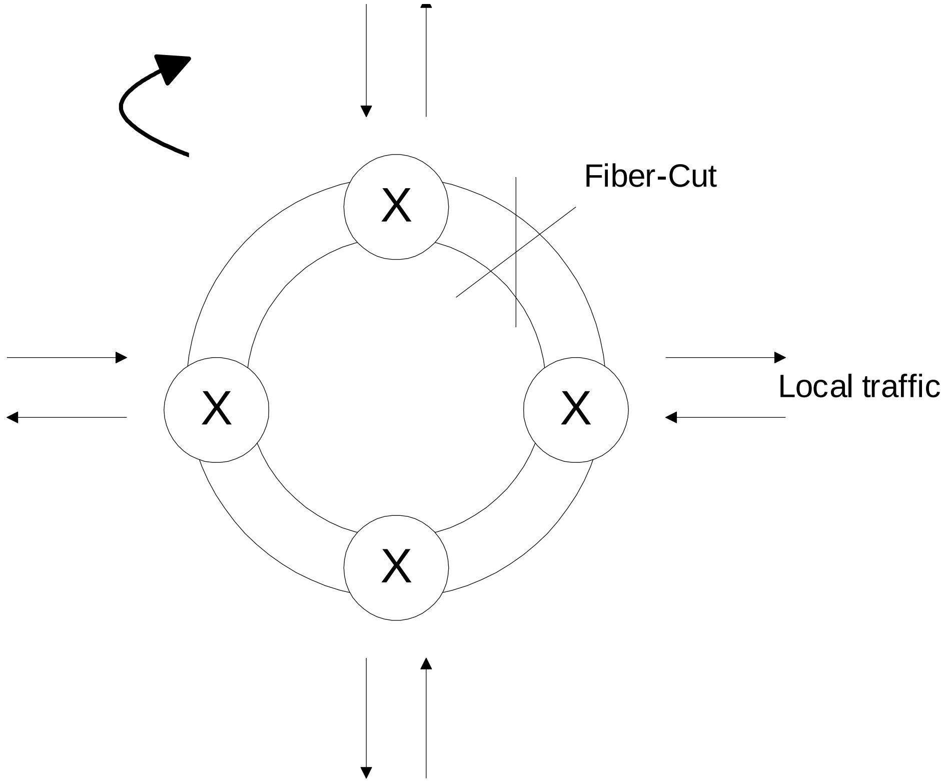


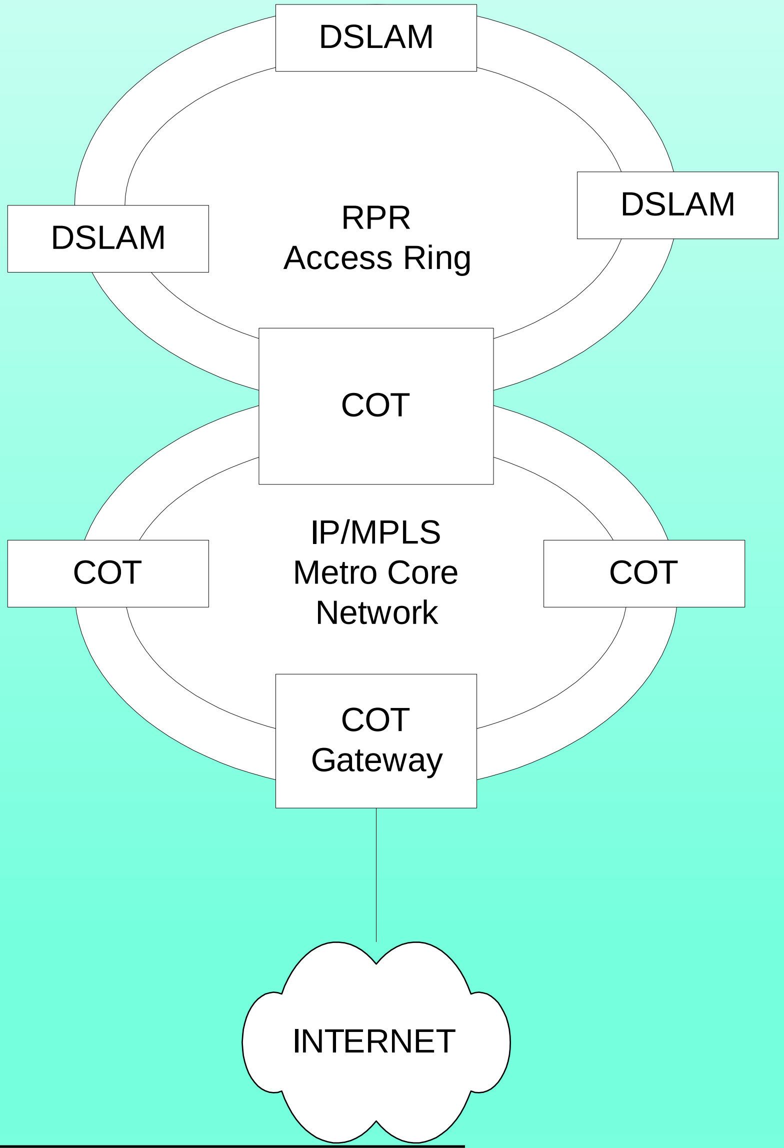
Figure 12.40 Dual Ring with Failure Recovery

Notes

- Failure recovery mode in dual ring configuration
- SONET/SDH OC-1 or STS (51.84 Mbps) signal multiplexed to higher level (e.g.,OC-3) and transmitted over optical carrier
- WDM (wavelength division multiplexer) strictly a physical layer (optical) system
- WDM directly interfaces with the switch
- DWDM (Dense WDM) higher density over fiber

Broadband MAN

In broadband implementation of RPR rings, the RTs house DSL access multiplexers (DSLAMs), and the local traffic shown in Figure 12.40 are DSL access networks carrying multimedia information. The architecture of a hierarchy of metro broadband network using RPR access rings and IP/MPLS metro core network connecting to the Internet via a gateway is shown in Figure 12.41.



Notes

Figure 12.41 Broadband Metro Network

SDH Management

- ITU-T G Series documentation
  - Transmission Systems and Media
  - Digital Systems and Networks
  - Digital Terminal Equipments
- G.774 SDH
  - Management Information Model
  - OAM
  - Data Communication Channels (DCCs)
- G.784 Element Management Functions (EMFs)
- G.831 Management capabilities of transport networks

Notes

SDH Data Communication Channels

- G.774 specifies 3 modes of management for DCCs
  - IP-only stack use PPP as data link
  - OSI-only use LAP-D as data link
  - Dual (IP + OSI) stack PPP or LAP-D with tunneling to communicate between stacks

Notes

SDH Element Management Functions

- G.784 specs equipment management functions (EMF)
    - Fault management
    - Performance management
    - Configuration management
- Two DCC channels
    - DCCM forwards over the multiplex sections: behaves as backbone network
    - DCCR (and LAN) forwards data to regenerators: interconnects backbone to equipment
    - DCCM and DCCR carry independent management applications

Notes

SDH Fault Management

- Alarm messages called ”defects”
- Error messages called “anomalies”
- Loss of signal (LOS) alarm triggers subsequent messages, alarm indication signals (AIS)
- Transmitter notified by return of an RDI (remote defect indicator) alarm

Notes

SDH Performance Management

- Performance parameters quantified in G.826
- Four commonly used parameters:
  - Errored seconds (ES)
    - # 1-second intervals containing at least 1 ES
  - Severely errored seconds (SES)
    - # 1-second intervals with > 30% block errors (or) one severely disturbed period
  - Background block error (BBE)
    - Errored block that is not SES
  - Unavailable seconds (UAS)
    - Circuit unavailable from the first of at least 10 consecutive SESs

Notes

SONET Hierarchy and IF Stack Layers

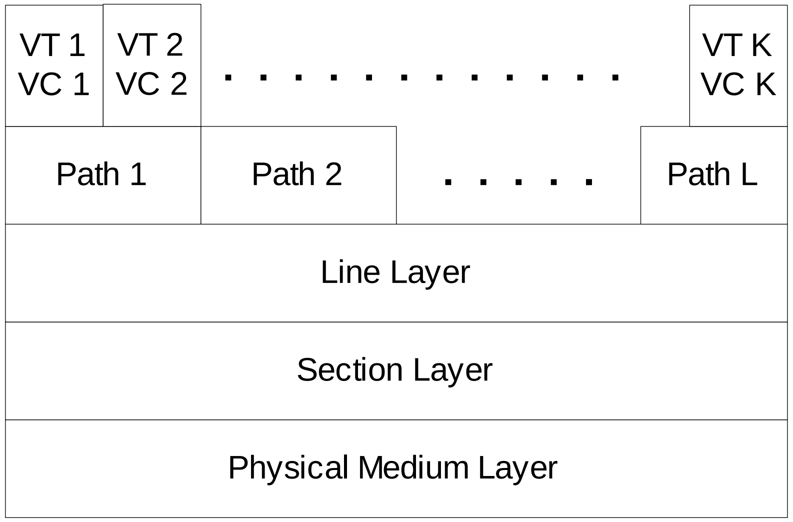


Figure 12.42 SONET / SDH Layers

VC-n …Virtual container (Europe)
VT-n … Virtual tributary (America & Japan)

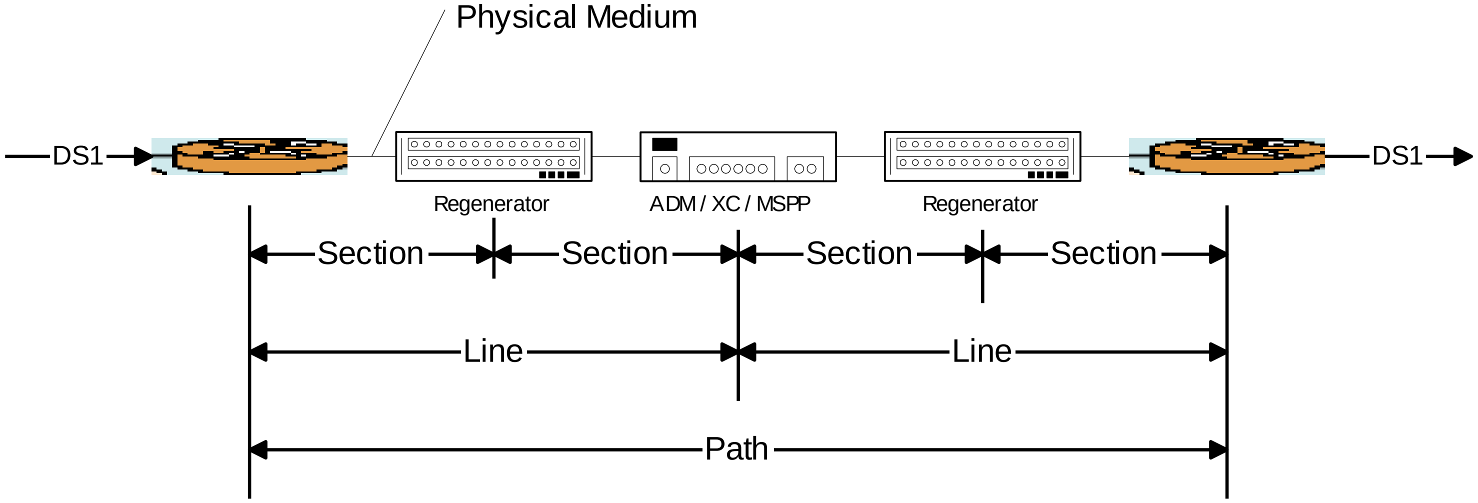


Figure 12.43 Topology of SONET / SDH Layers