- E-Line also known as Virtual Private Wire Service (VPWS), Virtual Leased Line (VLL), Point-to-Point, or Ethernet Private Wire Service (EPVS).
- E-LAN also known as Virtual Private LAN Services (VPLS), Transparent LAN Services and MultiPoint-to-MultiPoint.
- E-TREE also known as Rooted-MultiPoint.

5. Core Network Technologies

5.1 Introduction

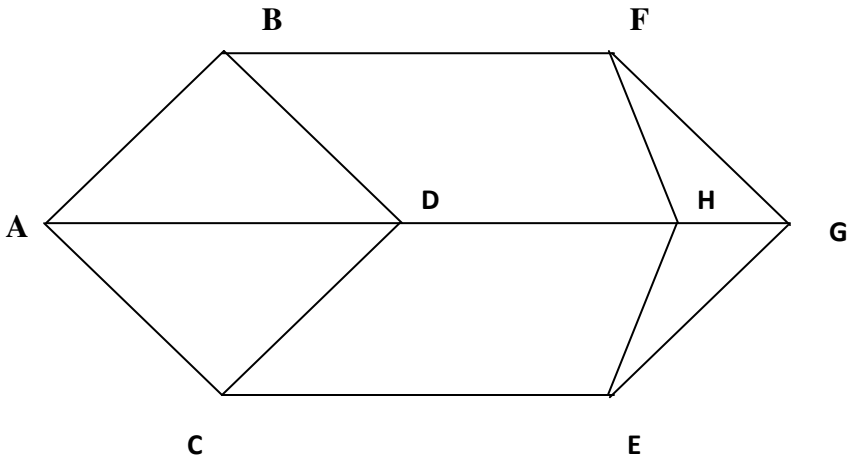
The core network is similar to highways of a road network. The highway network connects the major towns of the country by using highways which consists of wide roads. This road is shared by many vehicles.

The core network of a communication network is own and managed by the service providers. They look after the redundancy, reliability, availability etc. of the core network. If one route has a problem it will be switched to an alternative route. If one route to a particular destination has high traffic, another route also can be used to the same destination. Normally such things are managed by a protocol used in the network.

5.2 Transmission core network

In order to implement any core network, the physical core network is required and it can use any transmission media (Copper, fiber or radio) for the connectivity.

Consider the following physical core network.



The connectivity of difference links can be done on following manner.

DH - Radio

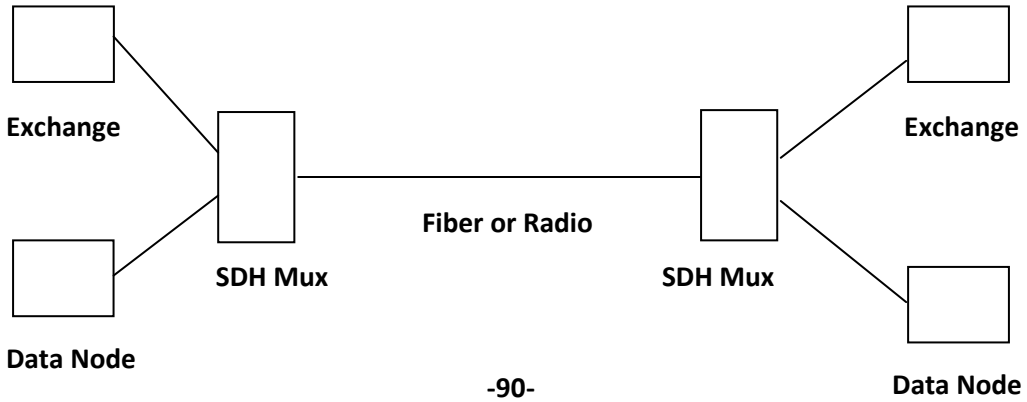
HC - Coaxial

HE - Radio

All other links - Fiber

Note: Nowadays coaxial is not used in the core network. Almost all links are fibers. If there is a Geographical constrain Radio link is used.

5.3 SDH Core Network

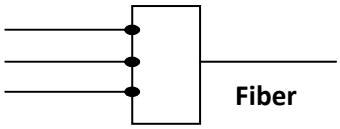


A Δ

Consider the SDH Mux shown in the figure. The SDH Muxes are connected by using a fiber or radio.
The radio can be STM-1

The fiber can be used for STM-1, 4, 16, 64, 256.

STM-1 – 155Mb/s
STM-4 –
STM-16 –
STM-64 –
STM-256 –
To be Filled



SDH Mux

The ports of the SDH Mux can be 1.5Mb/s, 2Mb/s, 6Mb/s, 24Mb/s, 45Mb/s or 140Mb/s, Also in some SDH Muxes 1Gb/s Ethernet interfaces are available.

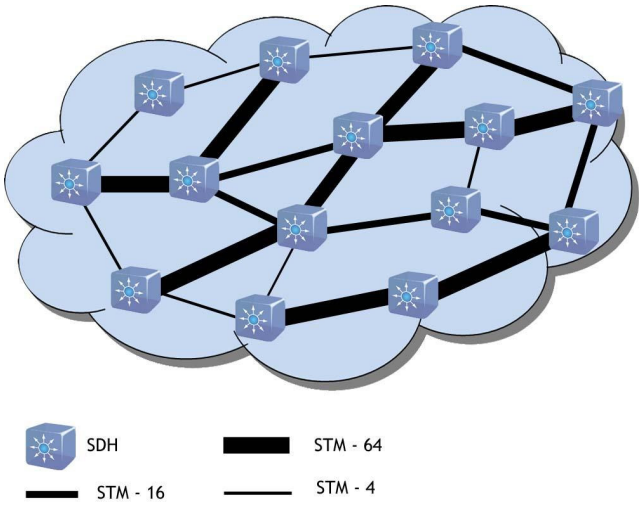
If there is a 96 core fiber between A and B , a pair of fiber is allocated to SDH Mux.

The SDH Mux can allocate any of the bit rate to different devices such as telephone exchanges. STM-1 can have usable 63 E1 s. For example, in the figure ……., several E1s allocate to telephone exchange. Several E1s can allocate to Date Node.

STM-4 Muxes can be down graded to STM-1 Muxes.

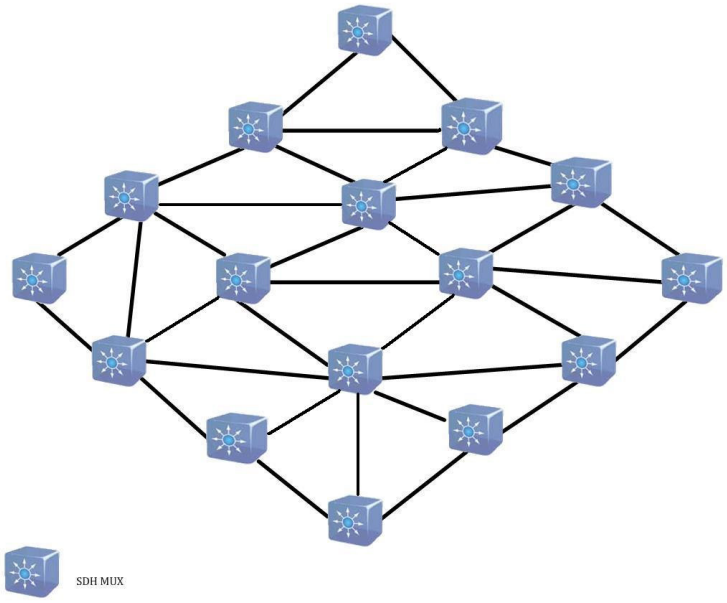
STM-16 Muxes can be down graded to STM-4 or STM-1 Muxes.
STM-64 Muxes can be down graded to STM-16 or STM-4 or STM-1 Muxes.

SDH Network



Physical SDH Network

SDH Over Fibre



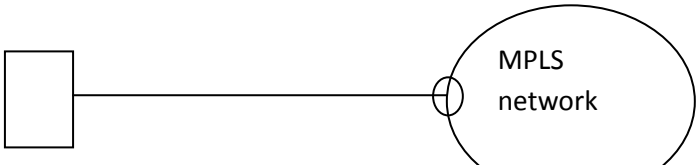
5.4 MPLS Core Network

MPLS stands for Multi Protocol Label Switching

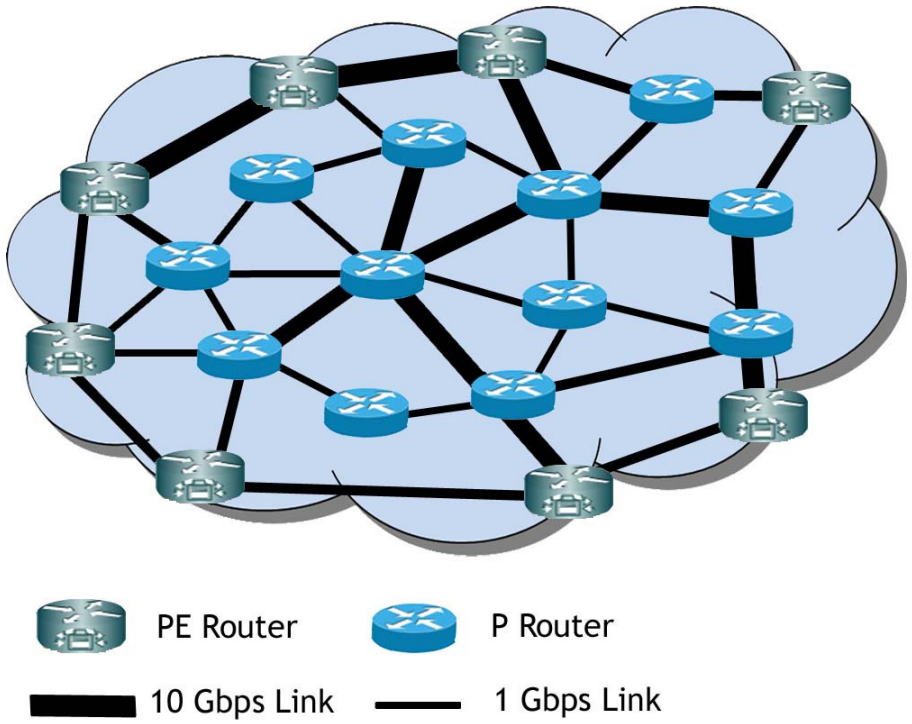
What is Label Switching?

MPLS Network has the Routers called Provider Router or P routers. Just like IP address in normal router. P router uses the label and its routing table has following fields.

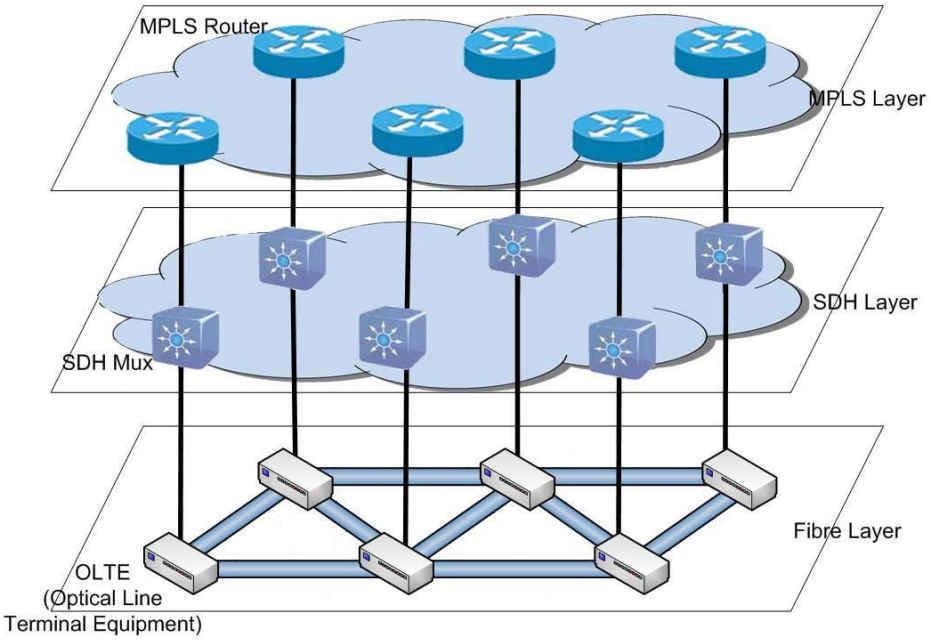
Input label	Output label
20	30
15	12



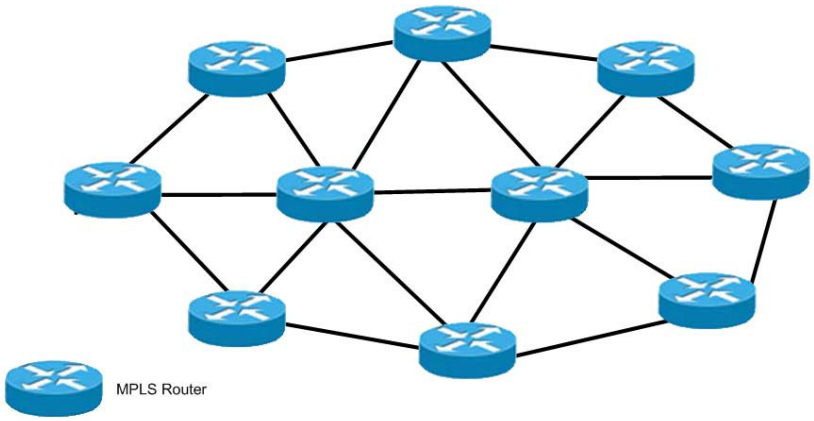
At the edge of the network the IP address is converted to label address and vise versa and such routers are called Provider Edge (PE) Routers.



The MPLS routers can be connected to Gigabit Ethernet interface of SDH Mux and it is called MPLS over SDH.



MPLS routers can be directly connected to fibres by the 1 Gigabit or 10 Gigabit Ethernets interface. It is called MPLS over fiber.



QoS of MPLS core nework

QoS can be applied in the core network Sri Lanka Telecom MPLS network provides Platinum, Gold, and Silver Services

Platinum

Gold

Silver

MPLS Applications

Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next with the help of labels. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular Data Link Layer technology, such as ATM, frame relay, SONET or Ethernet, and eliminate the need for multiple Layer 2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks.

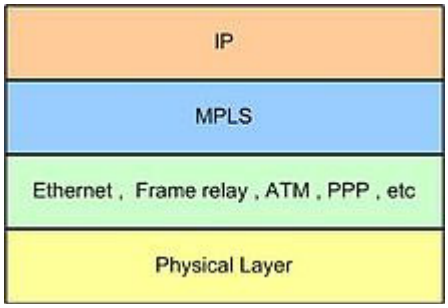
MPLS operates at an OSI Model layer that is generally considered to lie between traditional definitions of Layer 2 (Data Link Layer) and Layer 3 (Network Layer), and thus is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames.

A number of different technologies were previously deployed with essentially identical goals, such as frame relay and ATM. MPLS technologies have evolved with the strengths and weaknesses of ATM in mind. Many network engineers agree that ATM should be replaced with a protocol that requires less overhead, while providing connection-oriented services for variable-length frames. MPLS is currently replacing some of these technologies in the marketplace. It is highly possible that MPLS will completely replace these technologies in the future, thus aligning these technologies with current and future technology needs.

In particular, MPLS dispenses with the cell-switching and signaling-protocol baggage of ATM. MPLS recognizes that small ATM cells are not needed in the core of modern networks, since modern optical networks (as of 2008) are so fast (at 40 Gbit/s and beyond) that even full-length 1500 byte packets do not incur significant real-time queuing delays (the need to reduce such delays — *e.g.*, to support voice traffic — was the motivation for the cell nature of ATM).

At the same time, MPLS attempts to preserve the traffic engineering and out-of-band control that made frame relay and ATM attractive for deploying large-scale networks.

While the traffic management benefits of migrating to MPLS are quite valuable (better reliability, increased performance), there is a significant loss of visibility and access into the MPLS cloud for IT departments.



MPLS Layer

MPLS was originally proposed by a group of engineers from Epsilon Networks, but their "IP Switching" technology, which was defined only to work over ATM, did not achieve market dominance. Cisco Systems, Inc., introduced a related proposal, not restricted to ATM transmission, called "Tag Switching".[3] It was a Cisco proprietary proposal, and was renamed "Label Switching". It was handed over to the IETF for open standardization. The IETF work involved proposals from other vendors, and development of a consensus protocol that combined features from several vendors' work.

One original motivation was to allow the creation of simple high-speed switches, since for a significant length of time it was impossible to forward IP packets entirely in hardware. However, advances in VLSI have made such devices possible. Therefore the advantages of MPLS primarily revolve around the ability to support multiple service models and perform traffic management. MPLS also offers a robust recovery framework that goes beyond the simple protection rings of synchronous optical networking (SONET/SDH).

How MPLS works

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:

- A 20-bit label value.
- a 3-bit *Traffic Class* field for QoS (quality of service) priority (experimental) and ECN (Explicit Congestion Notification).
- a 1-bit *bottom of stack* flag. If this is set, it signifies that the current label is the last in the stack.
- an 8-bit TTL (time to live) field.

These MPLS-labeled packets are switched after a label lookup/switch instead of a lookup into the IP table. As mentioned above, when MPLS was conceived, label lookup and label switching were faster than a routing table or RIB (Routing Information Base) lookup because they could take place directly within the switched fabric and not the CPU.

The entry and exit points of an MPLS network are called label edge routers (LER), which, respectively, **push** an MPLS label onto an incoming packet and **pop** it off the outgoing packet. Routers that perform routing based only on the label are called label switching routers (LSR). In some applications, the packet presented to the LER already may have a label, so that the new LER pushes a second label onto the packet. For more information see penultimate hop popping.

Labels are distributed between LERs and LSRs using the “Label Distribution Protocol” (LDP).[5] Label Switch Routers in an MPLS network regularly exchange label and reachability information with each other using standardized procedures in order to build a complete picture of the network they can then use to forward packets. *Label Switch Paths (LSPs)* are established by the network operator for a variety of purposes, such as to create network-based IP virtual private networks or to route traffic along specified paths through the network. In many respects, LSPs are not

different from PVCs in ATM or Frame Relay networks, except that they are not dependent on a particular Layer 2 technology.

In the specific context of an MPLS-based virtual private network (VPN), LSRs that function as ingress and/or egress routers to the VPN are often called PE (Provider Edge) routers. Devices that function only as transit routers are similarly called P (Provider) routers. See RFC 4364.[6] The job of a P router is significantly easier than that of a PE router, so they can be less complex and may be more dependable because of this.

When an unlabeled packet enters the ingress router and needs to be passed on to an MPLS tunnel, the router first determines the forwarding equivalence class (FEC) the packet should be in, and then inserts one or more labels in the packet's newly-created MPLS header. The packet is then passed on to the next hop router for this tunnel.

When a labeled packet is received by an MPLS router, the topmost label is examined. Based on the contents of the label a *swap*, *push* (*impose*) or *pop* (*dispose*) operation can be performed on the packet's label stack. Routers can have prebuilt lookup tables that tell them which kind of operation to do based on the topmost label of the incoming packet so they can process the packet very quickly.

In a *swap* operation the label is swapped with a new label, and the packet is forwarded along the path associated with the new label.

In a *push* operation a new label is pushed on top of the existing label, effectively "encapsulating" the packet in another layer of MPLS. This allows hierarchical routing of MPLS packets. Notably, this is used by MPLS VPNs.

In a *pop* operation the label is removed from the packet, which may reveal an inner label below. This process is called "decapsulation". If the popped label was the last on the label stack, the packet "leaves" the MPLS tunnel. This is usually done by the egress router, but see Penultimate Hop Popping (PHP) below.

During these operations, the contents of the packet below the MPLS Label stack are not examined. Indeed transit routers typically need only to examine the topmost label on the stack. The forwarding of the packet is done based on the contents of the labels, which allows "protocol-independent packet forwarding" that does not need to look at a protocol-dependent routing table and avoids the expensive IP longest prefix match at each hop.

At the egress router, when the last label has been popped, only the payload remains. This can be an IP packet, or any of a number of other kinds of payload packet. The egress router must therefore have routing information for the packet's payload, since it must forward it without the help of label lookup tables. An MPLS transit router has no such requirement.

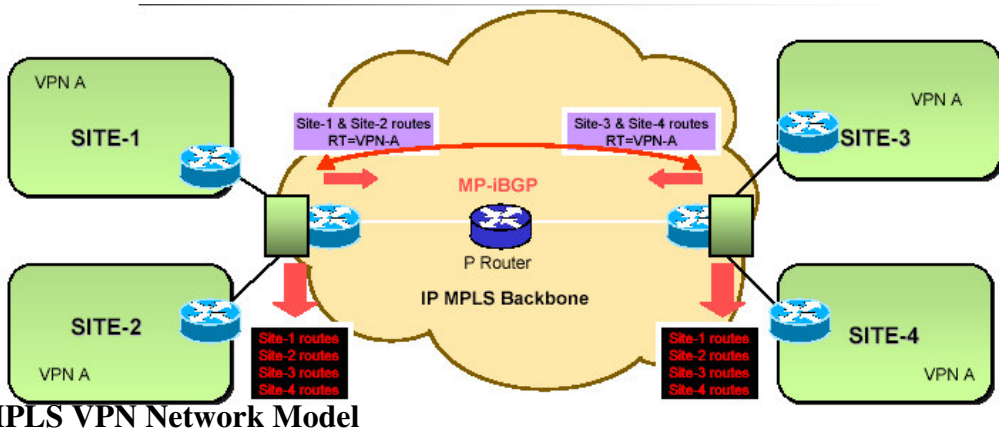
In some special cases, the last label can also be popped off at the penultimate hop (the hop before the egress router). This is called Penultimate Hop Popping (PHP). This may be interesting in cases where the egress router has lots of packets leaving MPLS tunnels, and thus spends

inordinate amounts of CPU time on this. By using PHP, transit routers connected directly to this egress router effectively offload it, by popping the last label themselves.

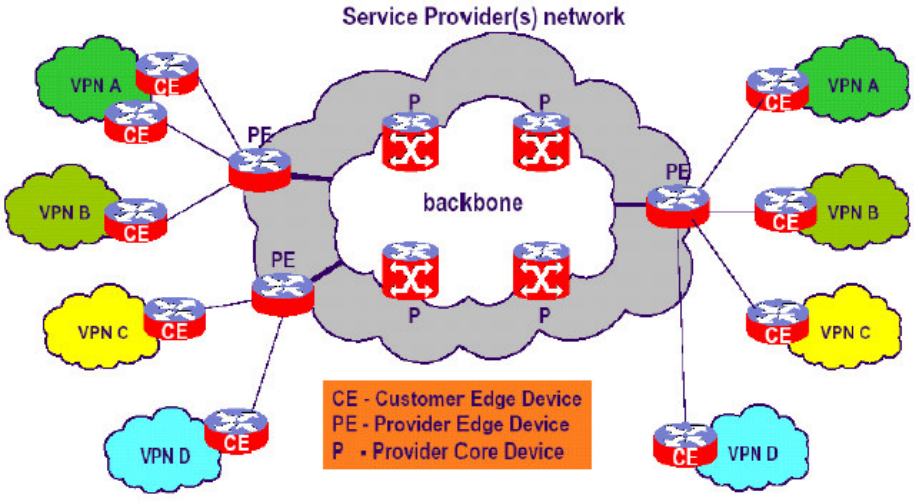
MPLS can make use of existing ATM network or frame relay infrastructure, as its labeled flows can be mapped to ATM or frame relay virtual circuit identifiers, and vice versa.

MPLS

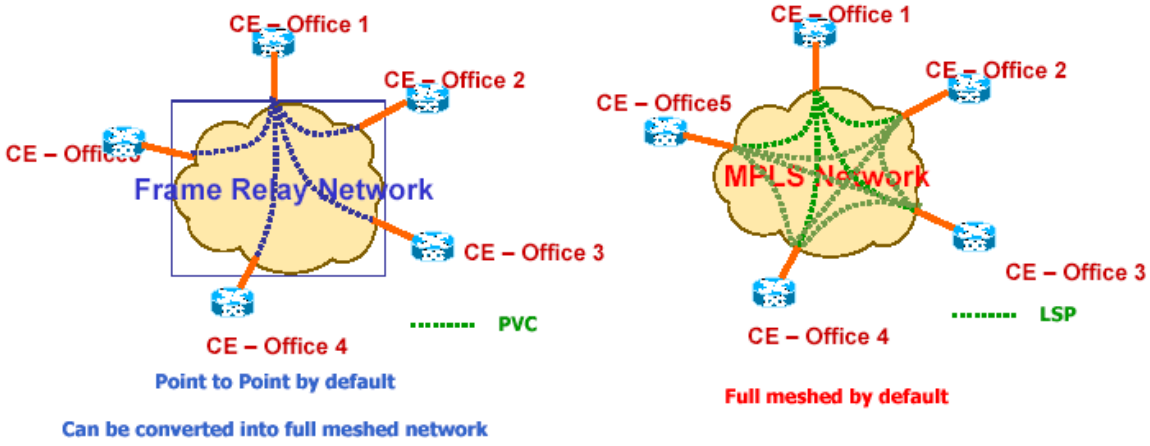
Basic Intranet Model Intranet Model



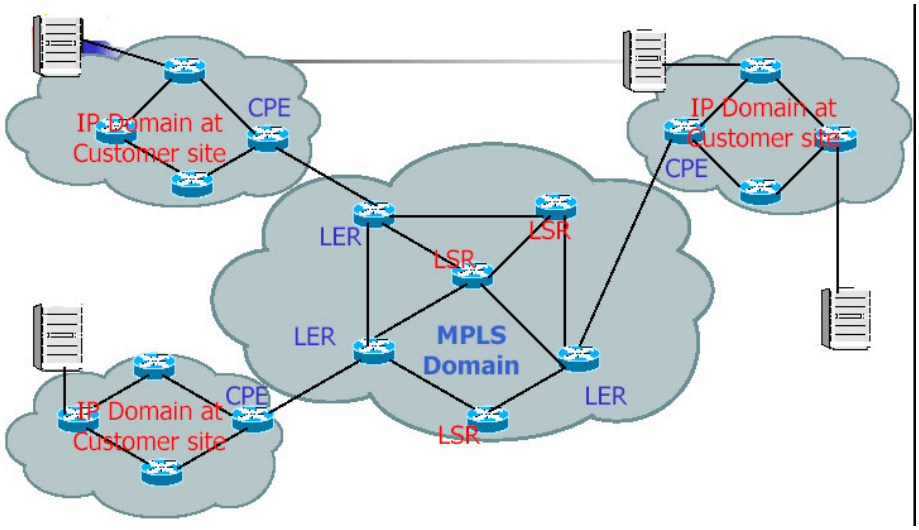
MPLS VPN Network Model



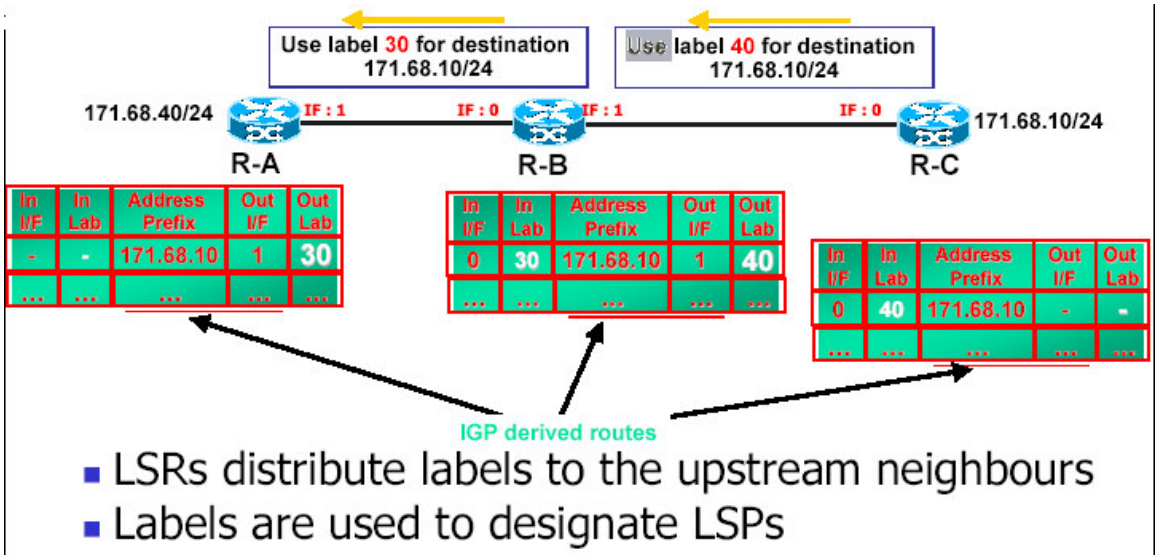
VPN Models



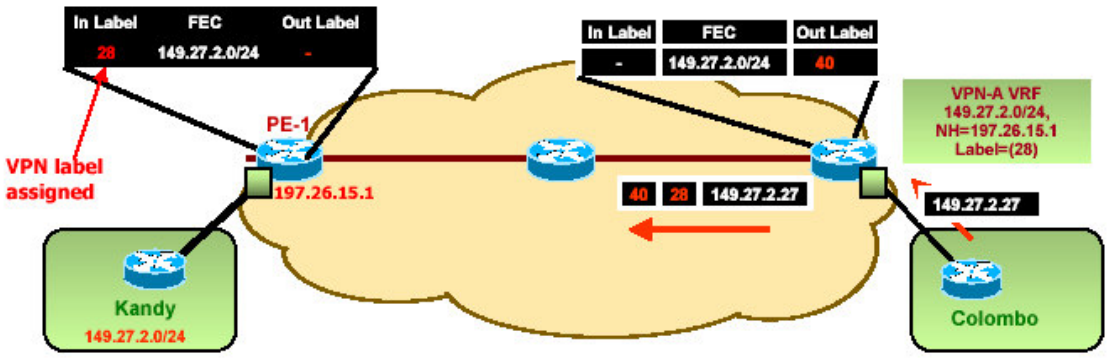
MPLS Domain And Components



Label Assignment and Distribution

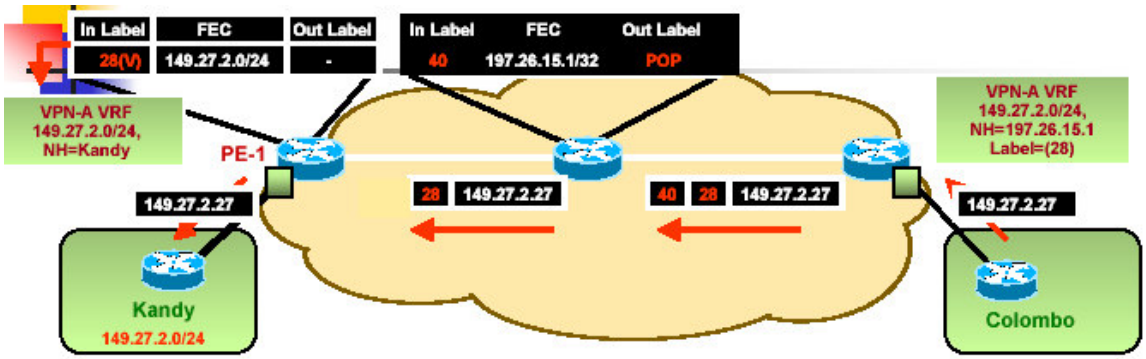


VPN Packet Forwarding VPN Packet Forwarding



• Ingress PE receives IP data packets

• PE router performs IP Best Match from VPN LFIB, finds iBGP next-hop and imposes a stack of labels <IGP, VPN>



Penultimate PE router removes the IGP label

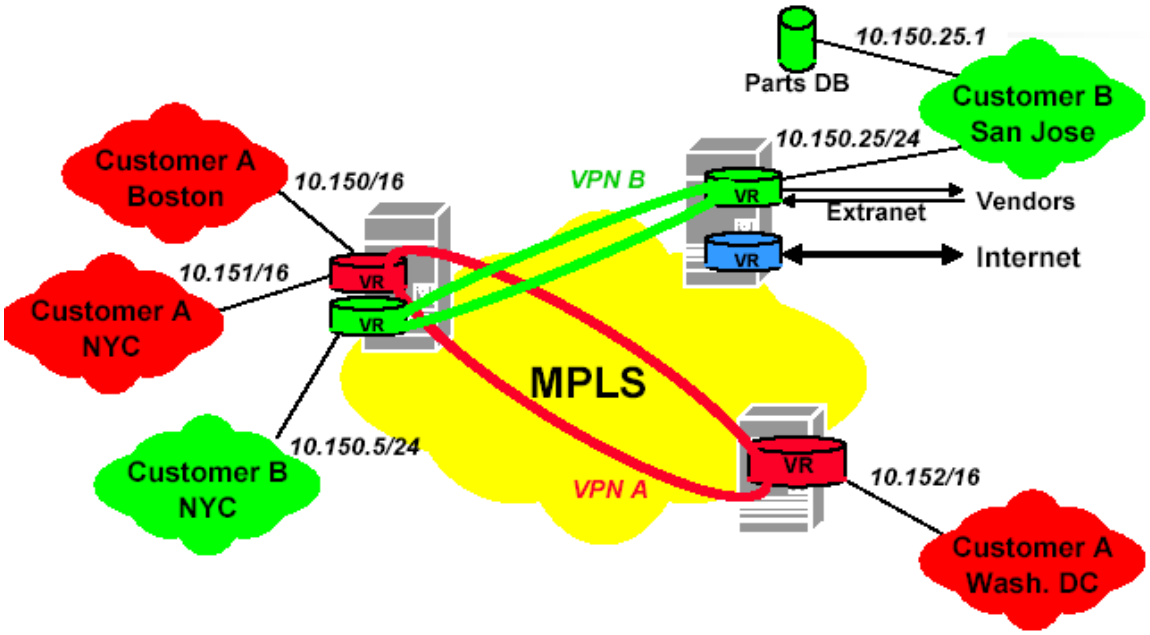
• **Penultimate Hop Popping procedures (implicit-null label)**

• Egress PE router uses the VPN label to select which VPN/CE to forward the packet to

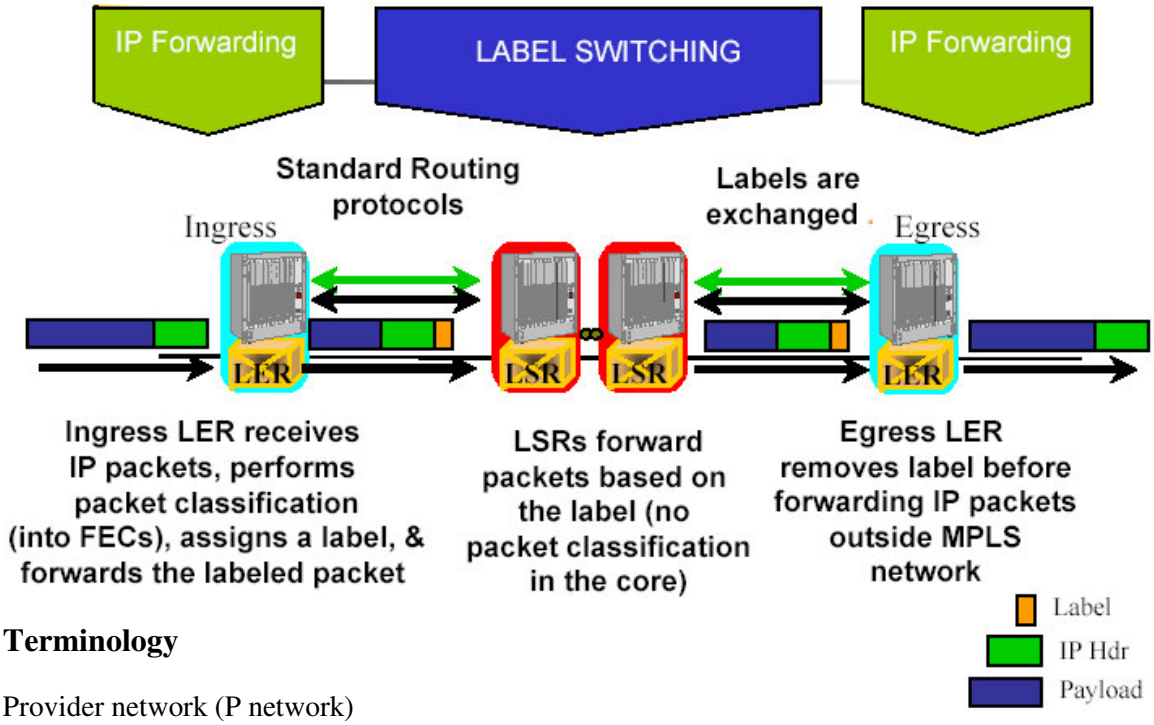
• VPN label is removed and the packet is routed toward the VPN site

Separate Routing - Private

Addressing



MPLS Operation



Terminology

Provider network (P network)
Provider edge router (PE/LER router) – physical connection to CE router and to core of network
Provider router (P/LSR router) - internal to P network and oblivious to existence of VPNs
Customer edge router (CE router) – physically connected to PE router
Customer router (C router) - internal to C network and invisible to PE router
PE-CE link

Label Edge Routers/Provider

LER Functions

1. Map IP Packets to labels

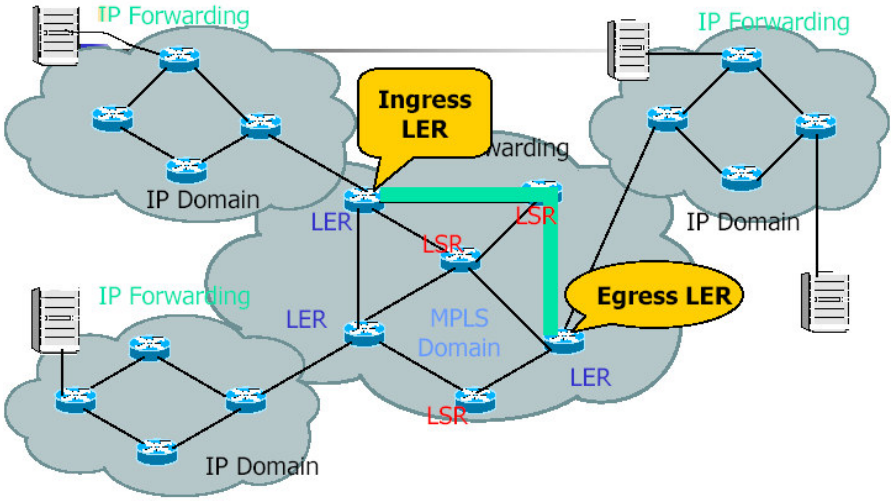
2. Push Labels on IP packets

3. Apply QoS Functions

4. Initiate LSP setup process

5. Traffic Engineering

Ingress and Egress LERs



Label Switched Routers/ Provider

Routers (LSR/P)

LSR Functions

1. Swap Labels
2. Apply QoS Functions
3. Participate in LSP setup process
4. Only knows routes within MPLS Domain

5.5 Layer 2 Core Network

Metro Ethernet

Metro Ethernet is a Metropolitan Area Network where Ethernet can be used to connect the computers (Networks) in several kilometers far away.

Layer 2 VPN

5.6 Frame Relay

Introduction

Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. The following two techniques are used in packet-switching technology:

- Variable-length packets
- Statistical multiplexing

Variable-length packets are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached.

Statistical multiplexing techniques control network access in a packet-switched network. The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today's popular LANs, such as Ethernet and Token Ring, are packet-switched networks.

Frame Relay often is described as a streamlined version of X.25, offering fewer of the robust capabilities, such as windowing and retransmission of last data that are offered in X.25. This is

because Frame Relay typically operates over WAN facilities that offer more reliable connection services and a higher degree of reliability than the facilities available during the late 1970s and early 1980s that served as the common platforms for X.25 WANs. As mentioned earlier, Frame Relay is strictly a Layer 2 protocol suite, whereas X.25 provides services at Layer 3 (the network layer) as well. This enables Frame Relay to offer higher performance and greater transmission efficiency than X.25, and makes Frame Relay suitable for current WAN applications, such as LAN interconnection.

Frame Relay Standardization

Initial proposals for the standardization of Frame Relay were presented to the Consultative Committee on International Telephone and Telegraph (CCITT) in 1984. Because of lack of interoperability and lack of complete standardization, however, Frame Relay did not experience significant deployment during the late 1980s.

A major development in Frame Relay's history occurred in 1990 when Cisco, Digital Equipment Corporation (DEC), Northern Telecom, and StrataCom formed a consortium to focus on Frame Relay technology development. This consortium developed a specification that conformed to the basic Frame Relay protocol that was being discussed in CCITT, but it extended the protocol with features that provide additional capabilities for complex internetworking environments. These Frame Relay extensions are referred to collectively as the Local Management Interface (LMI).

Since the consortium's specification was developed and published, many vendors have announced their support of this extended Frame Relay definition. ANSI and CCITT have subsequently standardized their own variations of the original LMI specification, and these standardized specifications now are more commonly used than the original version.

Internationally, Frame Relay was standardized by the International Telecommunication Union-Telecommunications Standards Section (ITU-T). In the United States, Frame Relay is an American National Standards Institute (ANSI) standard.

Frame Relay Devices

Devices attached to a Frame Relay WAN fall into the following two general categories:

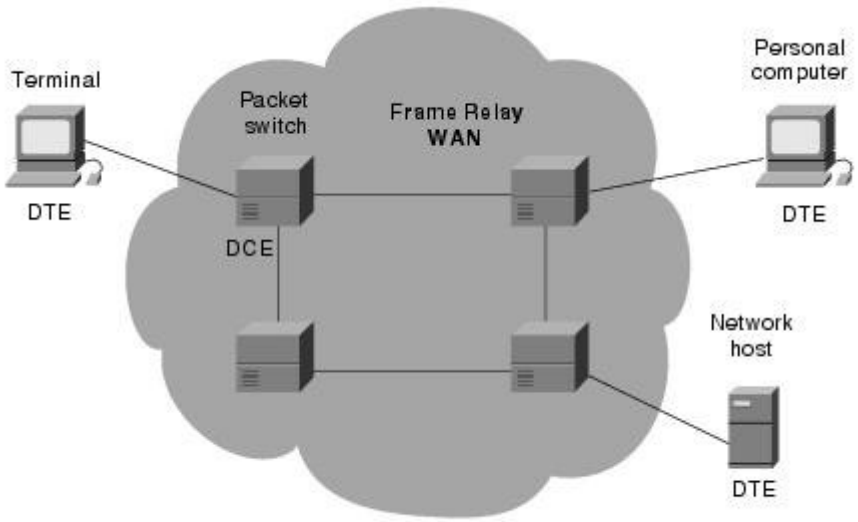
- Data terminal equipment (DTE)
- Data circuit-terminating equipment (DCE)

DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches.

Figure: DCEs Generally Reside Within Carrier-Operated WANs shows the relationship between the two categories of devices.

Figure: DCEs Generally Reside Within Carrier-Operated WANs



The connection between a DTE device and a DCE device consists of both a physical layer component and a link layer component. The physical component defines the mechanical, electrical, functional, and procedural specifications for the connection between the devices. One of the most commonly used physical layer interface specifications is the recommended standard (RS)-232 specification. The link layer component defines the protocol that establishes the connection between the DTE device, such as a router, and the DCE device, such as a switch. This article examines a commonly utilized protocol specification used in WAN networking: the Frame Relay protocol.

Frame Relay Virtual Circuits

Frame Relay provides connection-oriented data link layer communication. This means that a defined communication exists between each pair of devices and that these connections are associated with a connection identifier. This service is implemented by using a Frame Relay virtual circuit, which is a logical connection created between two data terminal equipment (DTE) devices across a Frame Relay packet-switched network (PSN).

Virtual circuits provide a bidirectional communication path from one DTE device to another and are uniquely identified by a data-link connection identifier (DLCI). A number of virtual circuits can be multiplexed into a single physical circuit for transmission across the network. This

capability often can reduce the equipment and network complexity required to connect multiple DTE devices.

A virtual circuit can pass through any number of intermediate DCE devices (switches) located within the Frame Relay PSN.

Frame Relay virtual circuits fall into two categories: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

Switched Virtual Circuits

Switched virtual circuits (SVCs) are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A communication session across an SVC consists of the following four operational states:

Call setup - The virtual circuit between two Frame Relay DTE devices is established.

Data transfer - Data is transmitted between the DTE devices over the virtual circuit.

Idle - The connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.

Call termination - The virtual circuit between DTE devices is terminated.

After the virtual circuit is terminated, the DTE devices must establish a new SVC if there is additional data to be exchanged. It is expected that SVCs will be established, maintained, and terminated using the same signaling protocols used in ISDN.

Few manufacturers of Frame Relay DCE equipment support switched virtual circuit connections. Therefore, their actual deployment is minimal in today's Frame Relay networks.

Previously not widely supported by Frame Relay equipment, SVCs are now the norm. Companies have found that SVCs save money in the end because the circuit is not open all the time.

Permanent Virtual Circuits

Permanent virtual circuits (PVCs) are permanently established connections that are used for frequent and consistent data transfers between DTE devices across the Frame Relay network. Communication across a PVC does not require the call setup and termination states that are used with SVCs. PVCs always operate in one of the following two operational states:

Data transfer - Data is transmitted between the DTE devices over the virtual circuit.

Idle - The connection between DTE devices is active, but no data is transferred. Unlike SVCs, PVCs will not be terminated under any circumstances when in an idle state.

DTE devices can begin transferring data whenever they are ready because the circuit is permanently established.

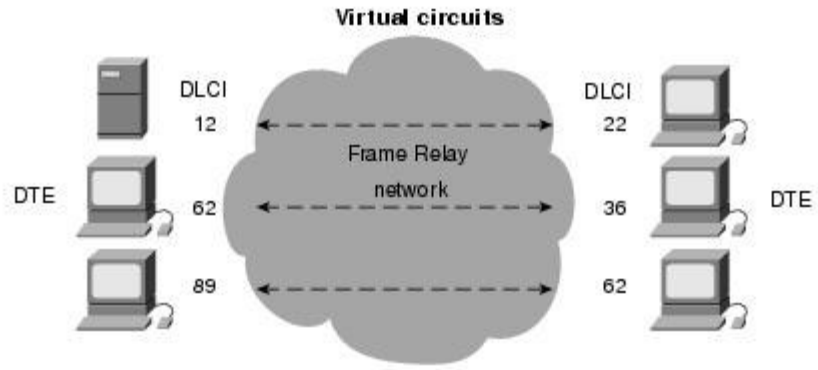
Data-Link Connection Identifier

Frame Relay virtual circuits are identified by data-link connection identifiers (DLCIs). DLCI values typically are assigned by the Frame Relay service provider (for example, the telephone company).

Frame Relay DLCIs have local significance, which means that their values are unique in the LAN, but not necessarily in the Frame Relay WAN.

Figure: A Single Frame Relay Virtual Circuit Can Be Assigned Different DLCIs on Each End of a VC illustrates how two different DTE devices can be assigned the same DLCI value within one Frame Relay WAN.

Figure: A Single Frame Relay Virtual Circuit Can Be Assigned Different DLCIs on Each End of a VC



Congestion-Control Mechanisms

Frame Relay reduces network overhead by implementing simple congestion-notification mechanisms rather than explicit, per-virtual-circuit flow control. Frame Relay typically is implemented on reliable network media, so data integrity is not sacrificed because flow control can be left to higher-layer protocols. Frame Relay implements two congestion-notification mechanisms:

Forward-explicit congestion notification (FECN)

Backward-explicit congestion notification (BECN)

FECN and BECN each is controlled by a single bit contained in the Frame Relay frame header. The Frame Relay frame header also contains a Discard Eligibility (DE) bit, which is used to identify less important traffic that can be dropped during periods of congestion.

The FECN bit is part of the Address field in the Frame Relay frame header. The FECN mechanism is initiated when a DTE device sends Frame Relay frames into the network. If the network is congested, DCE devices (switches) set the value of the frames' FECN bit to 1. When the frames reach the destination DTE device, the Address field (with the FECN bit set) indicates that the frame experienced congestion in the path from source to destination. The DTE device can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored.

The BECN bit is part of the Address field in the Frame Relay frame header. DCE devices set the value of the BECN bit to 1 in frames traveling in the opposite direction of frames with their FECN bit set. This informs the receiving DTE device that a particular path through the network is congested. The DTE device then can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow-control may be initiated, or the indication may be ignored.

Frame Relay Discard Eligibility

The Discard Eligibility (DE) bit is used to indicate that a frame has lower importance than other frames. The DE bit is part of the Address field in the Frame Relay frame header.

DTE devices can set the value of the DE bit of a frame to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices will discard frames with the DE bit set before discarding those that do not. This reduces the likelihood of critical data being dropped by Frame Relay DCE devices during periods of congestion.

Frame Relay Error Checking

Frame Relay uses a common error-checking mechanism known as the cyclic redundancy check (CRC). The CRC compares two calculated values to determine whether errors occurred during the transmission from source to destination. Frame Relay reduces network overhead by implementing error checking rather than error correction. Frame Relay typically is implemented on reliable network media, so data integrity is not sacrificed because error correction can be left to higher-layer protocols running on top of Frame Relay.

Frame Relay Local Management Interface

The Local Management Interface (LMI) is a set of enhancements to the basic Frame Relay specification. The LMI was developed in 1990 by Cisco Systems, StrataCom, Northern Telecom, and Digital Equipment Corporation. It offers a number of features (called extensions) for managing complex internetworks. Key Frame Relay LMI extensions include global addressing, virtual circuit status messages, and multicasting.

The LMI global addressing extension gives Frame Relay data-link connection identifier (DLCI) values global rather than local significance. DLCI values become DTE addresses that are unique in the Frame Relay WAN. The global addressing extension adds functionality and manageability

to Frame Relay internetworks. Individual network interfaces and the end nodes attached to them, for example, can be identified by using standard address-resolution and discovery techniques. In addition, the entire Frame Relay network appears to be a typical LAN to routers on its periphery.

LMI virtual circuit status messages provide communication and synchronization between Frame Relay DTE and DCE devices. These messages are used to periodically report on the status of PVCs, which prevents data from being sent into black holes (that is, over PVCs that no longer exist).

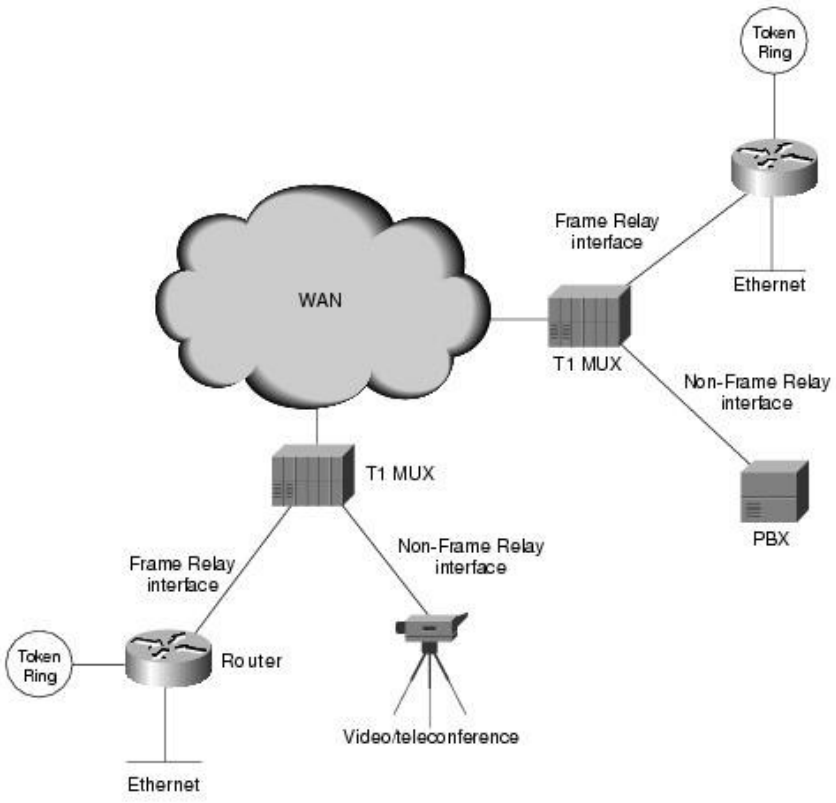
The LMI multicasting extension allows multicast groups to be assigned. Multicasting saves bandwidth by allowing routing updates and address-resolution messages to be sent only to specific groups of routers. The extension also transmits reports on the status of multicast groups in update messages.

Frame Relay Network Implementation

A common private Frame Relay network implementation is to equip a T1 multiplexer with both Frame Relay and non-Frame Relay interfaces. Frame Relay traffic is forwarded out the Frame Relay interface and onto the data network. Non-Frame Relay traffic is forwarded to the appropriate application or service, such as a private branch exchange (PBX) for telephone service or to a video-teleconferencing application.

A typical Frame Relay network consists of a number of DTE devices, such as routers, connected to remote ports on multiplexer equipment via traditional point-to-point services such as T1, fractional T1, or 56-Kb circuits. An example of a simple Frame Relay network is shown in Figure: A Simple Frame Relay Network Connects Various Devices to Different Services over a WAN.

Figure: A Simple Frame Relay Network Connects Various Devices to Different Services over a WAN



The majority of Frame Relay networks deployed today are provisioned by service providers that intend to offer transmission services to customers. This is often referred to as a public Frame Relay service. Frame Relay is implemented in both public carrier-provided networks and in private enterprise networks. The following section examines the two methodologies for deploying Frame Relay.

Public Carrier-Provided Networks

In public carrier-provided Frame Relay networks, the Frame Relay switching equipment is located in the central offices of a telecommunications carrier. Subscribers are charged based on their network use but are relieved from administering and maintaining the Frame Relay network equipment and service.

Generally, the DCE equipment also is owned by the telecommunications provider. DTE equipment either will be customer-owned or perhaps will be owned by the telecommunications provider as a service to the customer.

The majority of today's Frame Relay networks are public carrier-provided networks.

Private Enterprise Networks

More frequently, organizations worldwide are deploying private Frame Relay networks. In private Frame Relay networks, the administration and maintenance of the network are the responsibilities of the enterprise (a private company). All the equipment, including the switching equipment, is owned by the customer.

Frame Relay Frame Formats

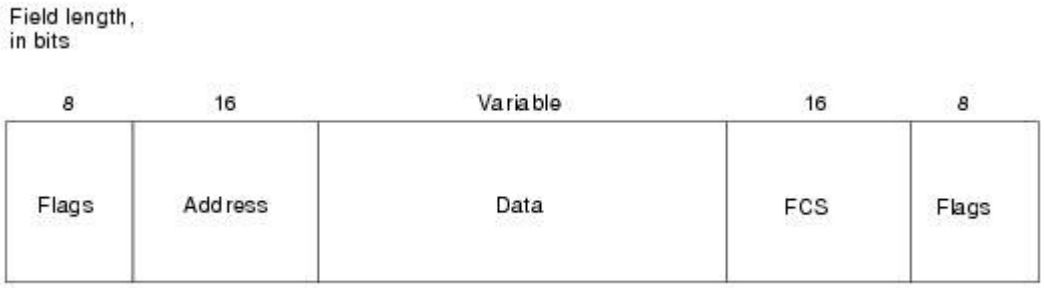
To understand much of the functionality of Frame Relay, it is helpful to understand the structure of the Frame Relay frame. Figure 10-4 depicts the basic format of the Frame Relay frame, and Figure 10-5 illustrates the LMI version of the Frame Relay frame.

Flags indicate the beginning and end of the frame. Three primary components make up the Frame Relay frame: the header and address area, the user-data portion, and the frame check sequence (FCS). The address area, which is 2 bytes in length, is comprised of 10 bits representing the actual circuit identifier and 6 bits of fields related to congestion management. This identifier commonly is referred to as the data-link connection identifier (DLCI). Each of these is discussed in the descriptions that follow.

Standard Frame Relay Frame

Standard Frame Relay frames consist of the fields illustrated in Figure: Five Fields Comprise the Frame Relay Frame.

Figure: Five Fields Comprise the Frame Relay Frame



The following descriptions summarize the basic Frame Relay frame fields illustrated in Figure 10-4.

Flags - Delimits the beginning and end of the frame. The value of this field is always the same and is represented either as the hexadecimal number 7E or as the binary number 01111110.

Address - Contains the following information:

DLCI - The 10-bit DLCI is the essence of the Frame Relay header. This value represents the virtual connection between the DTE device and the switch. Each virtual connection that is multiplexed onto the physical channel will be represented by a unique DLCI. The DLCI values have local significance only, which means that they are unique only to the physical channel on which they reside. Therefore, devices at opposite ends of a connection can use different DLCI values to refer to the same virtual connection.

Extended Address (EA) - The EA is used to indicate whether the byte in which the EA value is 1 is the last addressing field. If the value is 1, then the current byte is determined to be the last DLCI octet. Although current Frame Relay implementations all use a two-octet DLCI, this capability does allow longer DLCIs to be used in the future. The eighth bit of each byte of the Address field is used to indicate the EA.

C/R - The C/R is the bit that follows the most significant DLCI byte in the Address field. The C/R bit is not currently defined.

Congestion Control - This consists of the 3 bits that control the Frame Relay congestion-notification mechanisms. These are the FECN, BECN, and DE bits, which are the last 3 bits in the Address field.

Forward-explicit congestion notification (FECN) is a single-bit field that can be set to a value of 1 by a switch to indicate to an end DTE device, such as a router, that congestion was experienced in the direction of the frame transmission from source to destination. The primary benefit of the use of the FECN and BECN fields is the capability of higher-layer protocols to react intelligently to these congestion indicators. Today, DECnet and OSI are the only higher-layer protocols that implement these capabilities.

Backward-explicit congestion notification (BECN) is a single-bit field that, when set to a value of 1 by a switch, indicates that congestion was experienced in the network in the direction opposite of the frame transmission from source to destination.

Discard eligibility (DE) is set by the DTE device, such as a router, to indicate that the marked frame is of lesser importance relative to other frames being transmitted. Frames that are marked as "discard eligible" should be discarded before other frames in a congested network. This allows for a basic prioritization mechanism in Frame Relay networks.

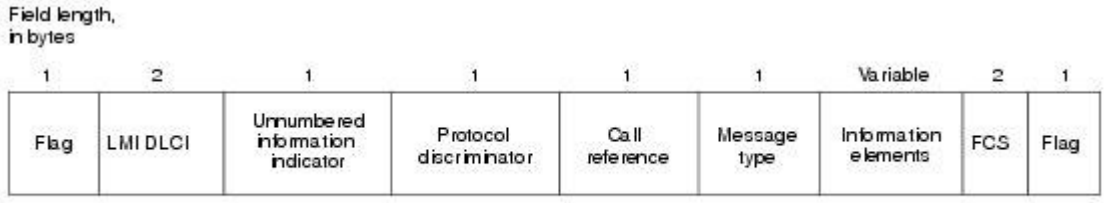
Data - Contains encapsulated upper-layer data. Each frame in this variable-length field includes a user data or payload field that will vary in length up to 16,000 octets. This field serves to transport the higher-layer protocol packet (PDU) through a Frame Relay network.

Frame Check Sequence - Ensures the integrity of transmitted data. This value is computed by the source device and verified by the receiver to ensure integrity of transmission.

LMI Frame Format

Frame Relay frames that conform to the LMI specifications consist of the fields illustrated in Figure: Nine Fields Comprise the Frame Relay That Conforms to the LMI Format.

Figure: Nine Fields Comprise the Frame Relay That Conforms to the LMI Format



The following descriptions summarize the fields illustrated in Figure 10-5.

Flag - Delimits the beginning and end of the frame.

LMI DLCI - Identifies the frame as an LMI frame instead of a basic Frame Relay frame. The LMI-specific DLCI value defined in the LMI consortium specification is DLCI = 1023.

Unnumbered Information Indicator - Sets the poll/final bit to zero.

Protocol Discriminator - Always contains a value indicating that the frame is an LMI frame.

Call Reference - Always contains zeros. This field currently is not used for any purpose.

Message Type - Labels the frame as one of the following message types:

Status-inquiry message - Allows a user device to inquire about the status of the network.

Status message - Responds to status-inquiry messages. Status messages include keepalives and PVC status messages.

Information Elements - Contains a variable number of individual information elements (IEs). IEs consist of the following fields:

IE Identifier - Uniquely identifies the IE.

IE Length - Indicates the length of the IE.

Data - Consists of 1 or more bytes containing encapsulated upper-layer data.

Frame Check Sequence (FCS) - Ensures the integrity of transmitted data.

Summary

Frame Relay is a networking protocol that works at the bottom two levels of the OSI reference model: the physical and data link layers. It is an example of packet-switching technology, which enables end stations to dynamically share network resources.

Frame Relay devices fall into the following two general categories:

Data terminal equipment (DTEs), which include terminals, personal computers, routers, and bridges

Data circuit-terminating equipment (DCEs), which transmit the data through the network and are often carrier-owned devices (although, increasingly, enterprises are buying their own DCEs and implementing them in their networks)

Frame Relay networks transfer data using one of the following two connection types:

Switched virtual circuits (SVCs), which are temporary connections that are created for each data transfer and then are terminated when the data transfer is complete (not a widely used connection)

Permanent virtual circuits (PVCs), which are permanent connections

The DLCI is a value assigned to each virtual circuit and DTE device connection point in the Frame Relay WAN. Two different connections can be assigned the same value within the same Frame Relay WAN-one on each side of the virtual connection.

In 1990, Cisco Systems, StrataCom, Northern Telecom, and Digital Equipment Corporation developed a set of Frame Relay enhancements called the Local Management Interface (LMI). The LMI enhancements offer a number of features (referred to as extensions) for managing complex internetworks, including the following:

Global addressing

Virtual circuit status messages

Multicasting

5.7 Asynchronous transfer mode (ATM)

This is a technology which can use as a Core Network Technology. However this technology can be used as an access network technology also.

ATM is another technique, which is used to provide layer 2 connectivity. It has the ability to provide different type of treatments for different services. The following are different type of Class B services.

Class A

Fixed bit rate (bandwidth), real time connection, connection oriented.

Eg: Voice

Class B

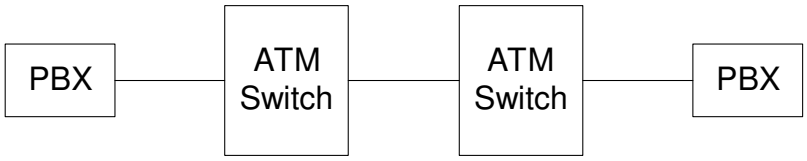
Variable bit rate, real time connection, connection oriented.

Eg: Compressed video

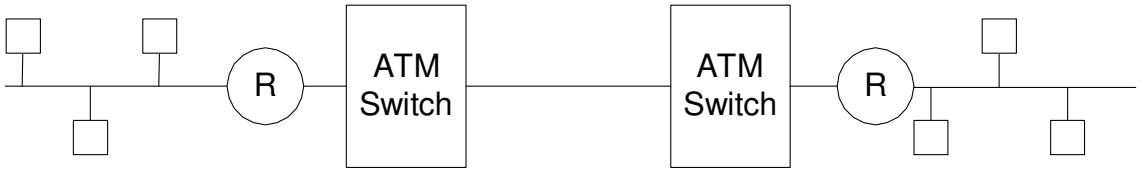
Class C/D/E

Variable bit rate, non-real time connection, connection less.

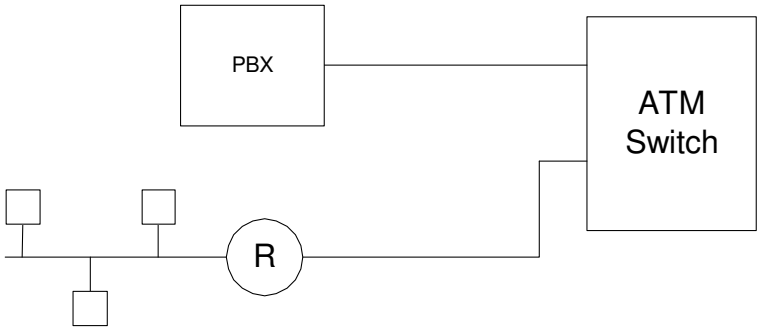
Eg: Transfer of data between two LANs through a router.



PBX provides voice services. Two PBX can be connected through ATM switch as shown in the figure.

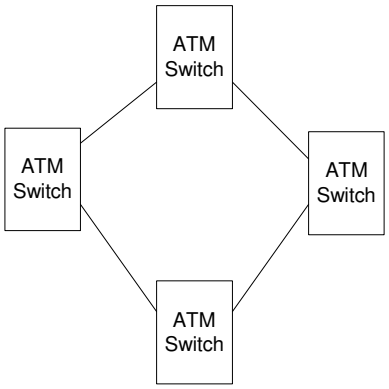


Two remote LANs can be connected using ATM switches as shown in the above figure.



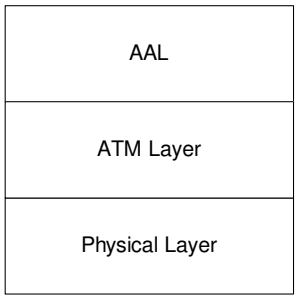
ATM switch has many ports. It can be connected to many services.

ATM Network



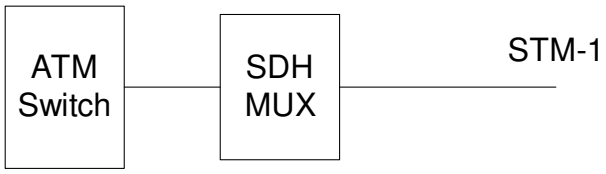
ATM network is made by connecting ATM switches. They connect by using transmission links. Normally they are fibres. The bit rates are 155 Mb/s, 620 Mb/s, 2.5 Gb/s etc.

ATM Protocol Architecture



Physical Layer

The physical layer defines the transmission medium, bit transmission, encoding and electrical to optical conversion.



The ATM switches can be connected to STM – n optical transmission system. The n can be 1, 4, 16, 64 etc.

STM – 1 = 155.52 Mb/s

STM – 4 = 622 Mb/s

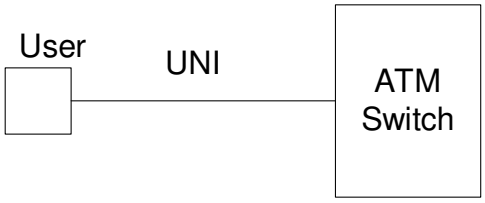
STM – 16 = 2.5 Gb/s

STM – 64 = 10 Gb/s

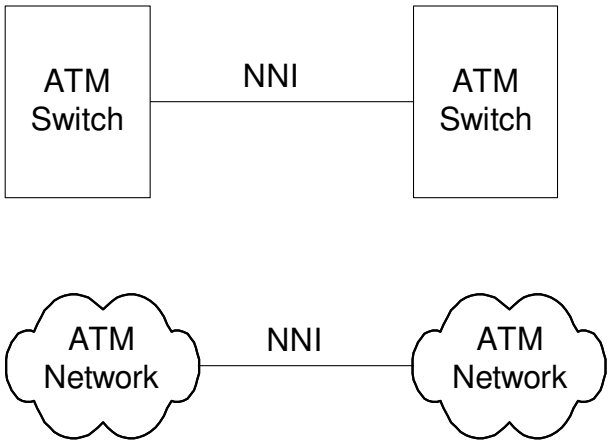
ATM Layer

The ATM uses a 48 byte data group collect a “Cell”. The ATM layer receives 48 byte cell payload (data) from ATM Adaptration Layer. The ATM layer adds 5 byte header to 48 byte payload. Then the ultimate size of a cell is 53 bytes.

There are two types of cell headers.

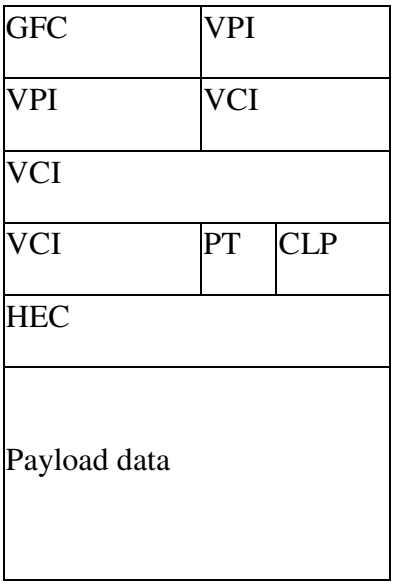


User Network Interface (UNI) header is uses between a user and ATM switch.

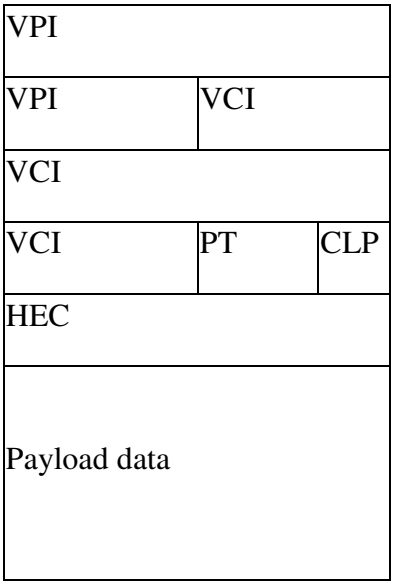


The network to Network header is used between two ATM switches or two ATM networks.

UNI Cell Format



NNI Cell Format



Generic Flow Control (GFC). This field provides flow control for the UNI cell.

VPI. VPI is an eight-bit field in a UNI cell and a 12-bit field in and NNI cell.

VCI. VCI is a 16-bit field in both cells.

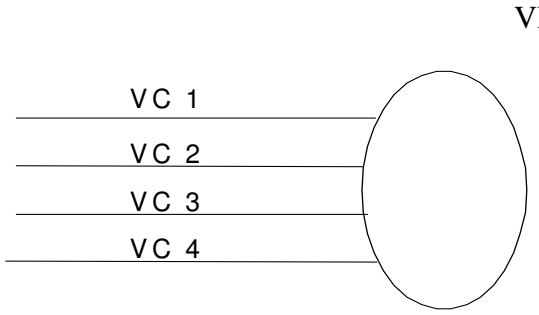
Payload type (PT). This defines the type of payload.

Cell Loss priority (CLP). This bit indicates to a switch which cell may be dropped and which must be retained.

Header error control (HEC). This is an eight- bit field to detect multiple–bit errors and correct single-bit errors in the header.

VPI & VCI

ATM is a connection oriented protocol. It established a permanent virtual channel between the source and destination. A group of virtual channels is called a virtual path. To identify virtual path, the virtual path Identifier (VPI) is used.



Is the above example VPI consists of 5 virtual channels. ie.VCI, VC2, VC3, VC4, VC5

The ATM switch direct the call to the out port by call switching. It can be switching to virtual channels, virtual paths or combination of both.

ATM Switch	Input		Output	
	VP I	VC I	VP I	VC I
1	10	51	20	48
2	20	48	15	37

This layer provides routing, traffic management, switching and multiplexing services.

ATM Adaptation Layer (AAL)

AAL has four Classes of services

AAL1 - Class A

AAL2 - Class B

AAL3/4 - Class C/D

AAL5 - Class E

Class A,B,C,D and E were explained earlier.

A part of ATM switch can be configured to one of the above services. The AAL layer segment the Application data to 47 bytes of segments and add 1 byte. The 48 bytes is sent to ATM layer. The 1 byte has the following format.

U U – User to user ID - 1 bit

T - 1 byte - 1 bit

L - Length - 2 bits

CRC - 4 bits

TCP/IP belongs to AAL 5 category.

5.8 Optical Transport Network

ITU-T defines **Optical Transport Network** (**OTN**) as a set of Optical Network Elements (3R) connected by optical fibre links, able to provide functionality of transport, multiplexing, switching, management, supervision and survivability of optical channels carrying client signals. [1]

ITU-T Recommendation G.709 is commonly called Optical Transport Network (OTN) (also called **digital wrapper technology** or **optical channel wrapper**). OTN is currently offered in the following line rates.

- **OTU1** has a line rate of approximately 2.66 Gbit/s and was designed to transport a SONET OC-48 or synchronous digital hierarchy (SDH) STM-16 signal.
- **OTU2** has a line rate of approximately 10.70 Gbit/s and was designed to transport an OC-192, STM-64 or WAN PHY (10GBASE-W).
- **OTU2e** has a line rate of approximately 11.09 Gbit/s and was designed to transport an 10 gigabit Ethernet LAN PHY coming from IP/Ethernet switches and routers at full line rate (10.3 Gbit/s). This is specified in G.Sup43.
- **OTU3** has a line rate of approximately 43.01 Gbit/s and was designed to transport an OC-768 or STM-256 signal or a 40 Gigabit Ethernet signal.[2]
- **OTU3e2** has a line rate of approximately 44.58 Gbit/s and was designed to transport up to four OTU2e signals.
- **OTU4** has a line rate of approximately 112 Gbit/s and was designed to transport a 100 Gigabit Ethernet signal.

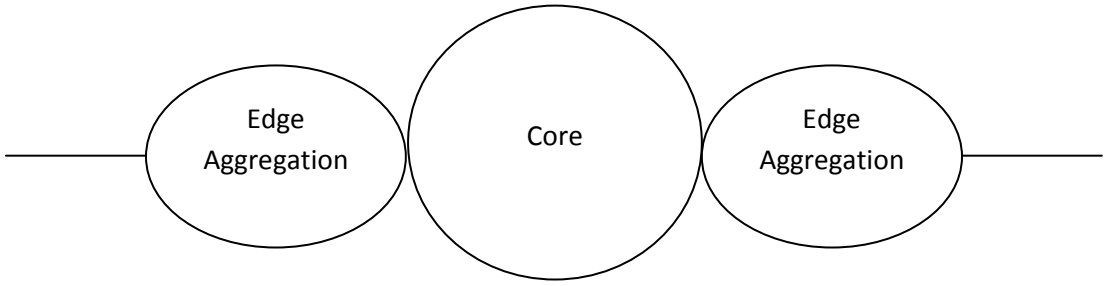
The OTUk (k=1/2/2e/3/3e2/4) is an information structure into which another information structure called ODUk (k=1/2/2e/3/3e2/4) is mapped. The ODUk signal is the server layer signal for client signals. The following ODUk information structures are defined in ITU-T Recommendation G.709

The optical transport network (OTN) was created with the intention of combining the benefits of SONET/SDH technology with the bandwidth expansion capabilities offered by dense wavelength-division multiplexing (DWDM) technology.

In addition to further enhancing the support for operations, administration, maintenance and provisioning (OAM&P) functions of SONET/SDH in DWDM networks, the purpose of the ITU G.709 standard (based on ITU G.872) is threefold.
First, it defines the optical transport hierarchy of the OTN; second, it defines the functionality of its overhead in support of multiwavelength optical networks; and third, it defines its frame structures, bit rates and formats for mapping client signals.
In order to begin describing the OTN as defined by the ITU G.709 standard, we must first enumerate its critical elements,
their termination points, and the way they relate to one another in terms of hierarchy and function.
In essence, the OTN consists of the following parts, which are often referred to as layers:
Optical Transport Section (OTS)
Optical Multiplex Section (OMS)
Optical Channel (OCh)
Optical Transport Unit (OTU)
Optical Data Unit (ODU)
Optical Channel Payload Unit (OPU)

5.9 Edge / Aggregation Network

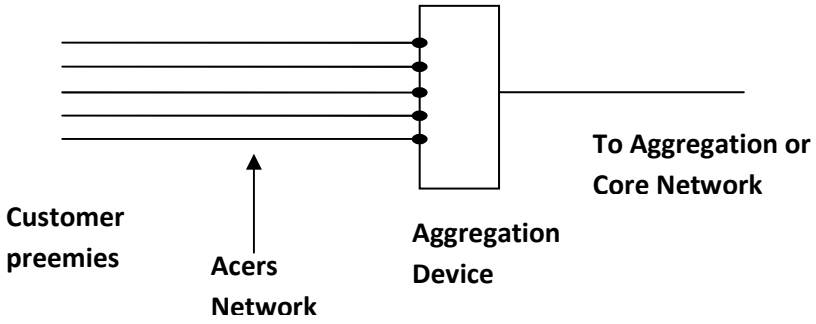
In large networks, edge or aggregation network is introduced in between Access and Core networks.



The physical Edge network is normally fiber. It can be layer 2 network. Metro Ethernet or Ethernet Aggregation networks can use as an Edge network.

5.10 Aggregation Devices

The Access network is connected to the Aggregation devices such as DSLAM or MSAN



DSLAM

MSAN

6. Public Switched Telephone Network

6.1Invention of Telephone