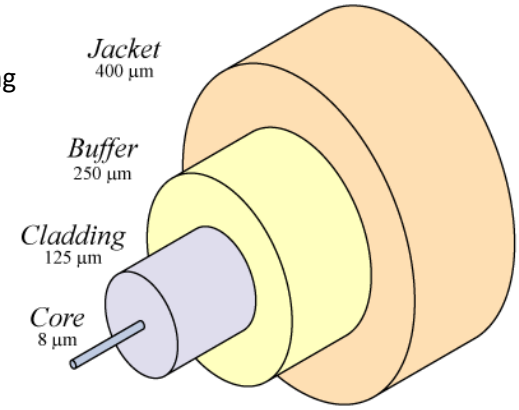
Chapter 1

Fiber Optic Transmission

Fiber-optic communication is a method of transmitting information from one place to another by sending **pulses** of light through an optical fiber.

- Fiber optic is the **fastest** and most cost effective means for high capacity data transmission over large distance.
- It uses **fiber glass** material for data transmission and the data transferred in the form of light.
- Data **loss** **is very** **less** 0.2dB/Km
- No regeneration and amplification is required up to **10,000 km**.

Fiber Optic Structure



1. **Core**
   - Glass or plastic with a higher index of refraction than the cladding
   - Carries the signal.
2. **Cladding**
   - Glass or plastic with lower index of refraction than the core
3. **Buffer**
   - Protects the fiber from damage and moisture.
4. **Jacket**
   - Holds one or more fibers in a cable.

Fiber Optic Advantages

- **Bandwidth** - Fiber optic cables have a much greater bandwidth than metal cables.
- **Low Power Loss** - An optical fiber offers low power loss.
- **Interference** - Fiber optic cables are immune to electromagnetic interference.
- **Size & Weight** - Fiber optic cables are much thinner and lighter than metal wires.
- **Security** - Optical fiber is difficult to tap. // As they do not radiate electromagnetic energy, emissions cannot be intercepted. As physically tapping the fiber takes great skill to do undetected, fiber is the most secure medium available for carrying sensitive data.

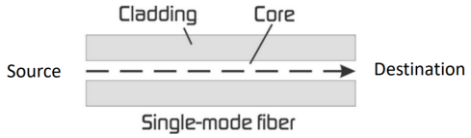
Fiber Optic Disadvantages

- **Cost** - Cables are expensive to install but last longer than copper cables.
- **Transmission** - transmission on optical fiber requires repeating at distance intervals.
- **Fragile** - Fibers can be broken or have transmission losses when wrapped around curves of only a few centimeters radius.
- **Protection** - Optical fibers require more protection around the cable compared to copper.

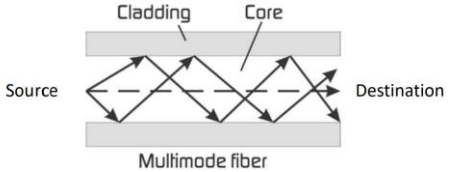
Fiber Optic Propagation

Propagation means how the light travels in the fiber optic cables from source to target.
There are 2 types of propagation mode in fiber optics cable

1. **Single Mode**
   the light is travelling in the lateral direction. There is only one angle that is straightway as the core of the diameter is very less.



2. **Multimode**
   has a large diameter core, so multiple modes of light propagate in it. It has more data carrying capacity due to multiple reflection inside.



Light Source

It is the heart of fiber optical systems. A hybrid device converts electrical signal to optical signal and launches these optical signals into optical fiber for data transmission.
The two commonly used light sources.

1. **LED (Light Emitting Diode)**
   It is a two led semiconductor light source. It is used for **Multimode** systems with 100-200 Mb/s rates. It works on low voltage and is inexpensive.
2. **LD (Laser Diode)**
   It is mainly used in **Single Mode** systems. Its light emission range is from 5 to 10 degrees. It Require Higher complex driver circuitry than LEDs therefore it is very expensive. It is also much more temperature sensitive than LEDs.

Photo Detectors

Photo detectors are used to convert optical signals into electrical signals to recover optically transmitted information.
// Photo detectors exploit the photoelectric effect: generation of an electron – hole pair in response to an absorbed photon.

Optical Modulation

The information can be transmitted on the optical carrier by varying any property of light like intensity, frequency etc. with respect to time. It is called as optical modulation.
// The **most common** optical modulation is **intensity**.
There are two types of optical modulation:

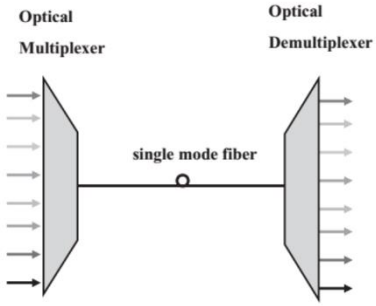
1. **Direct Modulation**
   Direct modulation is often used in optical communication systems because of its ease of implementation and low cost. Under this modulation scheme, a time - varying input current modulates the laser or LED output power directly .
2. **External Modulation**

WDM Basics

WDM is a technology that combines multiple wavelengths on a **Single Mode** fiber.
// The ability to multiplex wavelengths is of critical importance for creating high - bandwidth optical pipes to transport data. **WDM(Wavelength Division Multiplexing)** is a type of multiplexing

How wave multiplexing done

- In a WDM system the optical signals at different frequencies are launched into the inputs of a wavelength multiplexer.
- At the output of the wavelength multiplexer all wavelengths are effectively combined and coupled into a single - mode fiber. At the end of the transmission link the optical channels are separated again by means of a wavelength de-multiplexer.



WDM Bandwidth Capacity

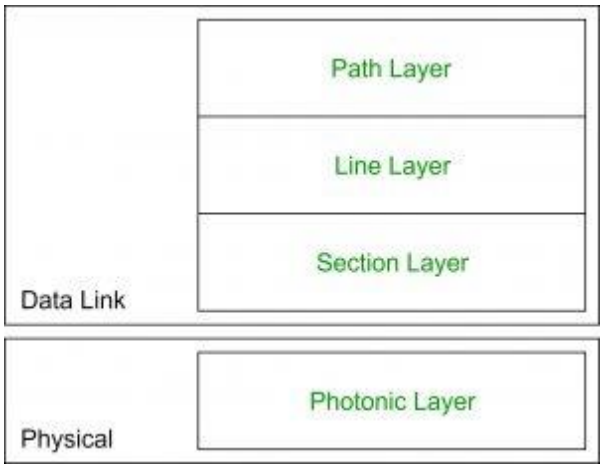
- The bandwidth of capacity is below 1280nm and 1650nm.
- If we convert this wavelength number to frequency using the formula $f = {}^{c}/_{\lambda}$ that is the $frequency = \frac{Speed\ of\ light}{Wavelength}$.
- So by this formula we get 235 and 182 THz for higher and lower bonds of that range.

Synchronous Optical Network (SONET)

It is used for optical transmission. SONET used **Time Domain Multiplexing** to send the bandwidth signals into one high-capacity signal that can be sent over optical fiber.

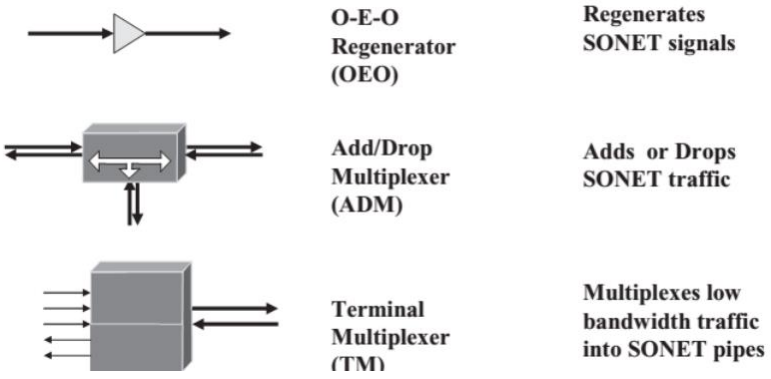
SONET Layers

1. **Path Layer**
   It is responsible for the movement of signals from its optical source to its optical destination.
2. **Line Layer**
   It is responsible for the movement of signal across a physical line.
3. **Section Layer**
   It is responsible for the movement of signal across a physical section.
4. **Photonic Layer**
   It corresponds to the physical layer of the OSI model.



The Classes Of SONET Networking Equipment

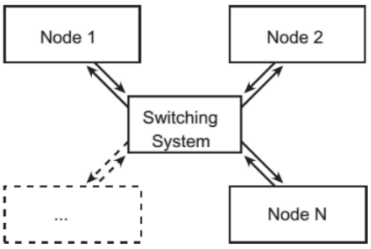
1. **O-E-O Regenerators**
   O-E-O regenerators are used to regenerate optical signals that travel long distances.
2. **Add/drop multiplexers (ADMs)**
   are the most versatile pieces of SONET networking gear, as they can add or drop any amount of SONET traffic, as desired by the network operations.
3. **Terminal Multiplexers(TMs)**
   Terminal multiplexers (TMs) are a specialized class of ADMs used at the edges of SONET networks.



Chapter 2

SWITCHING AND WHY IT IS IMPORTANT

Wherever a communications system brings multiple communications links together, and each of the **ingress** (Input) links carries one or more signals that must be sent out any of the **egress** (Output) links at one time or another, the functional unit that allows the multiple inputs to be varyingly connected to the multiple outputs is called a **switch**.



Abstract view of switching.

Switching Types

1. **Switching of physical circuit**
   - The physical layer of a protocol is either an electrical or an optical signal. In some applications it is necessary to switch at this fundamental layer.
   - Such switches typically have **N ingress** ports and **N egress** ports.
   - Connections can be made from **any** ingress port to **any one or more** egress ports.
2. **Switching of time division multiplexing signals.**

   TDM switching has **three** inherent components:
   a. capturing the ingress samples.
   b. holding the ingress samples in memory.
   c. communicating the ingress samples to the required outputs.

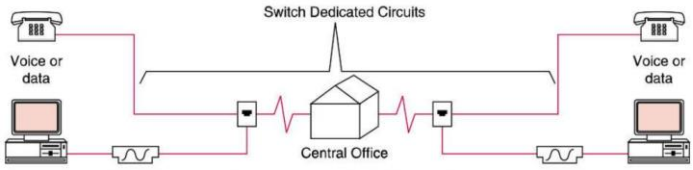
   Capturing the ingress sample means that logic in the receiver must discover the boundaries of bits, bytes, samples, and the repeating frame structure.

   // **Memory** is required because an ingress sample may appear in a time slot before it is assigned to be emitted on some egress port.
3. **Switching of cell and/or packets.**
   - Cell and packet protocols have no such semistatic repeating switching pattern. Instead, each cell or packet carries an address (or other routing instructions) that directs it to a particular output.
   - The most critical difference from TDM protocols is that cell and packet protocols require that the switch route each cell or packet, depending on requirements found within the cell or packet.

Switching Classification

1. **Circuit Switching**

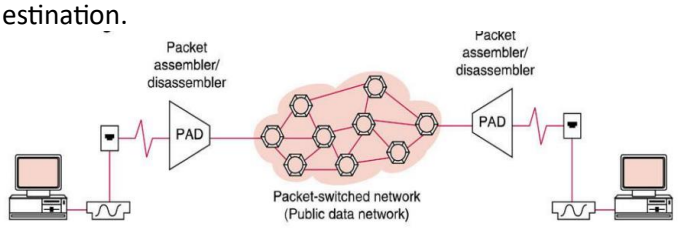
   In a circuit switched network, a switched dedicated circuit is created to connect the two or more parties, eliminating the need for source and destination address information.



All data or voice travel from source to destination over the *same* physical path

2. **Packet Switching**

   In a packet switched network, packets of data travel one at a time from the message source to the message destination.
   - The packet of data goes in one side of the PDN and comes out the other.
   - The physical path which any packet takes may be different than other packets and in any case, is unknown to the end users.
   - **Packet switches** pass packets among themselves as the packets are routed from source to destination.

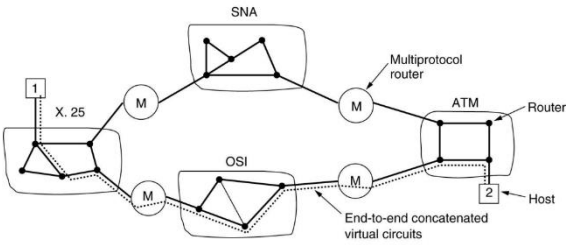


Data enter the packet-switched network one packet at a time;
Packets may take *different* physical paths within packet-switched networks.

Packet Switched Networks

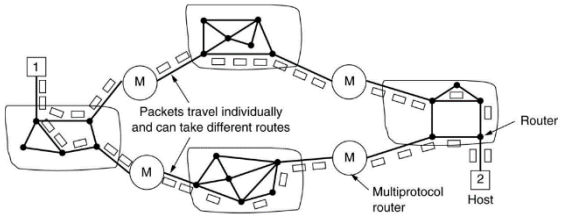
1. Connection-oriented Protocols

- A setup stage is used to determine the end-to-end path before a connection is established.
- Data flow streams are identified by some type of connection indicator.



2. Connectionless Protocols

- No set up is needed.
- Each packet contains information which allows the packet to be individually routed hop-by-hop through the network.



A connectionless internet

Optical Crossbar Switches

Photonic methods are used for the long - distance transmission of almost all network traffic. It would be a lovely simplification if all switching of network traffic could remain in the optical domain, as many conversions between the optical and electrical domains could be avoided.

Traffic pattern

The traffic pattern is the flow of frames in the network based on traffic load condition.

Types Of Traffic Load Conditions

1. Benign loads

A benign load is an ideal load. It consist of permutations of frames such that each ingress and each egress is kept equally busy.

// This is the simplest conceptual load model.

2. Hotspot loads

A hotspot load has some concentration of bandwidth at some subset or egress ports, such that the sum of bandwidth directed at these outputs exceeds their capacity for some period of time.

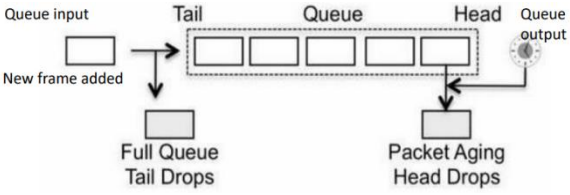
Realistic loads

Neither of the load model is intended as a realistic representation of actual network traffic. Actual behavior is much more complex, with dynamically changing requirements and traffic loads coming in periodic bursts.

Queues Structure

As we know router and switches holds temporarily frames in queue waiting for output link.

Each queue is a **First In First Out (FIFO)** data structure . This implies that a new frame is always added to the end of queue and the older frame is removed first.



Queuing System

Queuing systems are found inside the switches. It is found inside and outside ports, multiplexer, demultiplexer, control signals queues and communication system.

- **Ingress ports** inject a frame into the queuing system whenever a frame arrives at the port. There is little or no buffering in the ingress port, so the frame must be passed on to the rest of the queuing system nearly immediately.
- **Communication path** has no memory, so the frame move from one location to another location as sequence of bytes.
- **Queues** are the only components that offer storage of frames.
- **Multiplexers** merge multiple frame flows into one united flow.
- **De-multiplexers** accept one frame flow and separate it into multiple output flows..
- **Egress** ports accept one frame at a time and then emit it onto the egress link.
- Implicit in each queuing system is a set of control signals that effectively push frames from their ingress port sources into queues and pull frames from these queues toward ready egress ports.

Chapter 3

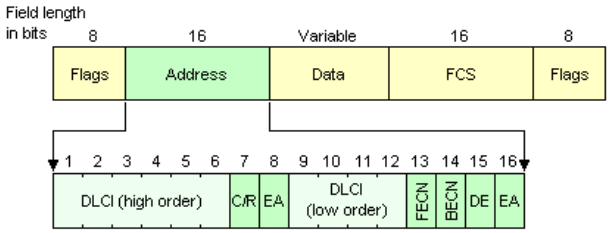
Frame Relay (FR)

Frame relay is a data link packet switching protocol that uses digital circuits to transmit data.
// It is a WAN protocol.

- Frame relay is a Connection-Oriented, that means connection must be establish before information can be sent to the remote device
- The **connection** used by frame relay are **provided by Virtual Circuits (VC),** a VC is a logical connection between two devices.
- Frame relay use **non broadcasting multi access technology**.

Frame Relay Frame Format

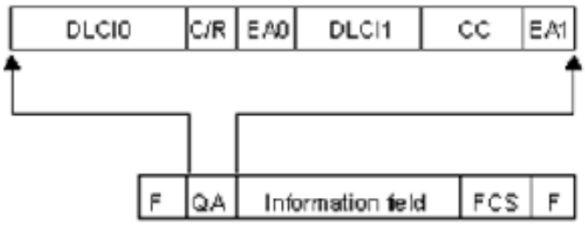
- **Flags** - a bit pattern that delimits the beginning and end of the frame (01111110)
- **Address** - contains four subfields:
- **Data**- up to 16,000 bytes of user data
- **Frame check sequence (FCS)** - used for error detection.



Frame Relay Address field format

Address - contains the following subfields:

- **Data-Link Connection Identifier (DLCI)**
  a 10-bit field that identifies a virtual connection.
- **Extended Address (EA)**
  if set to 1, the current byte is the last in the DLCI.
- **Command/Response (C/R)**
  Indicates command or response.
- **Congestion Control**
  a 3-bit field that contains the FECN, BECN and DE **(Discard Eligibility)** bits.



Data Link Connection Identifier (DLCI)

In a frame relay network routers are connected with a frame relay switch which creates virtual circuits, and these virtual circuits are identified by a number which is called DLCI.
// In other words, DLCI creates a virtual circuit in a frame relay network.

Discard Eligibility (DE)

There is one more bit in the address field of frame relay header, that is DE, during the congestion its value become 1 which tells that the frame is very low importance, so that it can be discarded.

Frame Relay Virtual Circuit

Frame Relay virtual circuit is a logical connection created between two data terminal equipment (DTE) devices [source and target] across a Frame Relay packet-switched network.
In frame relay network, the network is established virtually that means there is no physical direct connection between source and target, but it uses already **existing PSN**, **Public Service Network**.

Types Of Frame Relay Virtual Circuits.

- **Permanent Virtual Circuit (PVC)**
  A logical representation between two points that does not change. This is by far the most common form of VC for FR
- **Switched Virtual Circuit (SVC)**
  A logical representation between two points, but the connection is set up on-demand when data is transferred and then disconnected when data transfer is complete. SVC is similar to a telephone call in that a call is made, data/words are transferred, and then the connection is broken or taken down.

Frame Relay Components

1. **Access**: the local loop from customer site to the FR service provider's **Point of Presence (POP)** or central office
2. **Port**: The FR access port is the speed of the connection into the FR service provides switch.
3. **Virtual Circuit**: it is two types PVC and SVC

Congestion Control Mechanism

The congestion control in a frame relay is a simple congestion mechanism rather than flow control, by the use of notification.

There are two types of congestion notification.

// This FECN and BECN are the bits in the address field of frame relay header.

1. **Forward Explicit Congestion Notification [FECN]**
   FECN is handled by DTE Devices (Data terminal Equipment)
2. **Backward Explicit Congestion Notification [BECN]**
   BECN is handled by DCE Devices (Date circuit terminating Equipment)

The values of FECN and BECN is set 1, which gives the congestion notification if the network is congested.

Frame Relay CIR

// CIR stands for **C**ommitted **I**nformation **R**ate.

CIR is defined as the rate, in bits per second, at which the Frame Relay switch agrees to transfer data.

التعريف اللي فوق غير كافي على كلام الدكتور شل شوية من تحت

// In PVC point to point connectivity is established between FR access port to other FR access port. Here the data transfer is constant and in sequence as it was sent, which is similar to the dedicated private line. Suppose that a PVC is established of 56kbps it will give a through put of 56kbps only which is called as CIR committed information rate.

Frame Relay EIR

//EIR stands for **E**xcess **I**nformation **R**ate.

EIR is the maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR.

التعريف اللي فوق غير كافي على كلام الدكتور شل شوية من تحت

// If a switched virtual circuit (SVC) is established of 56kbps as it is a switched virtual circuit so there is no guarantee that it will give always 56kbps only, it may go beyond also, as per the network condition this extra information is called as Excess information rate.

Frame Relay LMI

The Frame Relay switch uses LMI to report the status of configured PVCs.

The three possible PVC states are as follows:

3. **Active state**
   Indicates that the connection is active and that routers can exchange data.
4. **Inactive state**
   Indicates that the **local connection** to the Frame Relay switch is working, but the **remote router connection** to the Frame Relay switch is not working.
5. **Deleted state**
   Indicates that no LMI is being received from the Frame Relay switch, or that there is no service between the CPE router and Frame Relay switch.

Advantages of Frame Relay

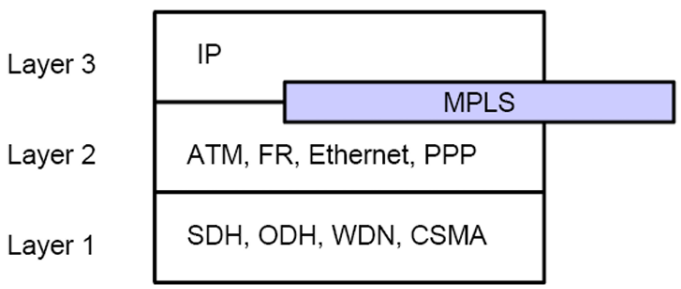
- The advantage is of cost saving
- High performance
- Circuit used are virtual
- Higher network availability

Disadvantages of Frame Relay

- The major disadvantage is due to network congestion it will slow down
- As there is a fluctuation in data transfer so the QOS (Quality of Service) is very less.

Multiprotocol Label Switching (MPLS)

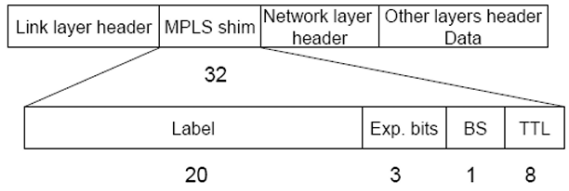
MPLS is data forwarding technology that increases the speed and controls the flow of network traffic. With MPLS, data is directed through a path via labels instead of requiring complex lookups in a routing table at every stop. MPLS is arranged between Layer 2 and Layer 3



MPLS Characteristics

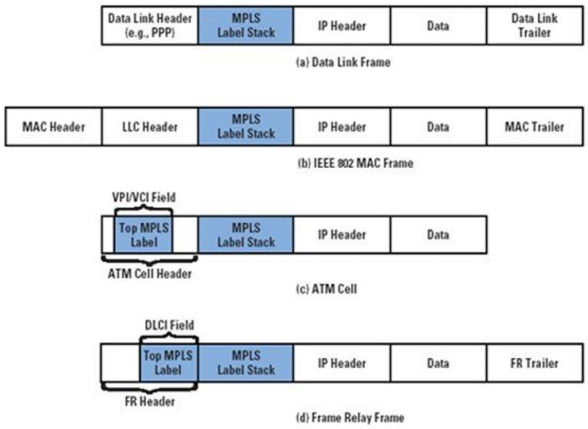
- Mechanisms to manage traffic flows of various granularities (Flow Management)
- Is independent of Layer-2 and Layer-3 protocols
- Maps IP-addresses to fixed length labels
- Interfaces to existing routing protocols (RSVP, OSPF)
- Supports ATM, Frame-Relay and Ethernet

Generic Label Format of MPLS

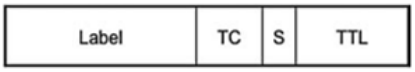


Exp.bits: Experimental Bits, often used for Class of Service
BS: Bottom of Stack bit, is set if no label follows
TTL: Time To Leave, used in the same way like in IP

Position of MPLS Label



Forwarding plane mechanisms in MPLS

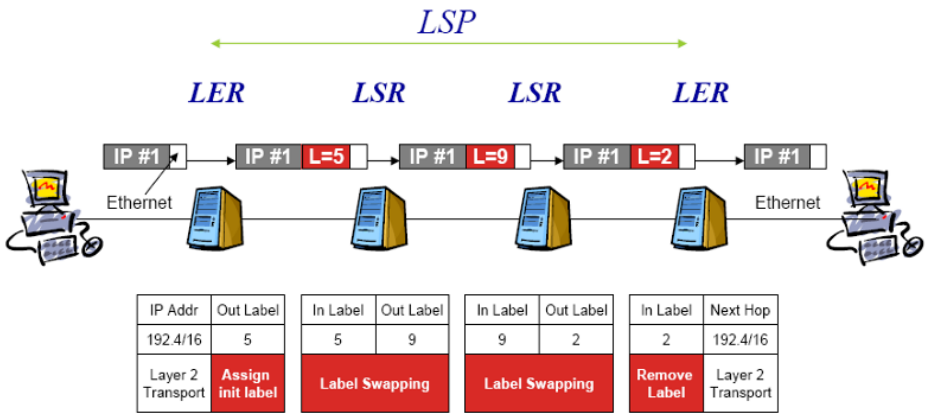


MPLS header structure

1. **20-bit label value**. MPLS packets are forwarded on the basis of this field. This value is used as an index into the MPLS forwarding table.
2. **Traffic Class (TC)** field (3 bits). it conveys the Class of Service to be applied to the packet. For example, LSRs and LERs can use these bits to determine the queue into should be placed. which the packet
3. **Bottom of stack bit (S-bit)**. The S-bit is set on the header of the MPLS packet at the bottom of the stack.
4. **Time-to-live (TTL)** field. This is used to avoid forwarding loops and can also be used for path-tracing.

LER & LSR in MPLS

1. **Label Edge Router - LER**
   Resides at the edge of an MPLS network and assigns and removes the labels from the packets. Support multiple ports connected to dissimilar networks (such as frame relay, ATM, and Ethernet).
2. **Label Switching Router - LSR**
   Is a high-speed router in the core on an MPLS network.
   ATM switches can be used as LSRs without changing their hardware. Label switching is equivalent to VP/VC switching.



"ROUTE AT EDGE, SWITCH IN CORE"

MPLS Tunnel Properties

1. Traffic can be explicitly routed, depending on which signaling protocol is used.
2. Recursion is provided for; hence tunnels can exist within tunnels.
3. There is protection against data spoofing, as the only place where data can be injected into an MPLS tunnel is at the head end of that tunnel.
4. The encapsulation overhead is relatively low (4 bytes per MPLS header).

Level Distribution Protocol (LDP) in MPLS

//**Goal** of LDP is **label distribution**, LDP **does not** attempt to **perform any routing function**.
LDP was specifically designed to distribute labels in the network. LDP operation is driven by message exchanges between peers. Potential peers, also known as neighbors, that are directly connected to each other over a point-to-point or LAN interface are automatically discovered via hello messages multicast to a well-known UDP port.
LDP is an application layer protocol for the distribution of label binding information to LSRs. It is used to map FECs to labels, which, in turn, create LSPs. LDP sessions are established between LDP peers in the MPLS network (not necessarily adjacent). Sometimes employs OSPF or BGP.

LDP message types in MPLS

1. **discovery messages**
   announce and maintain the presence of an LSR in a network
2. **session messages**
   establish, maintain, and terminate sessions between LDP peers
3. **advertisement messages**
   create, change, and delete label mappings for FECs
4. **notification messages**
   provide advisory information and signal error information

MPLS Advantages

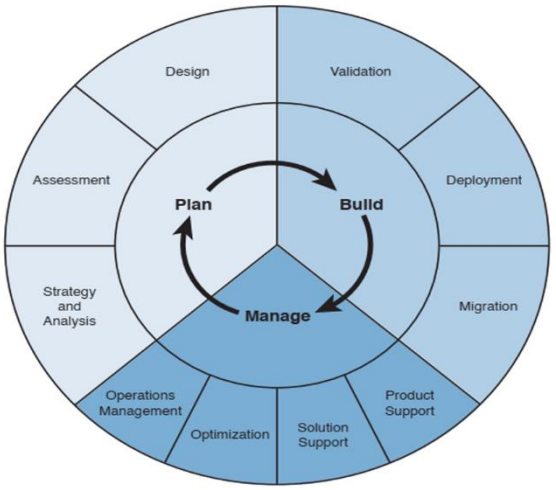
- Improves packet-forwarding performance in the network
- Supports QoS and CoS for service differentiation
- Supports network scalability
- Integrates IP and ATM in the network
- Builds interoperable networks

MPLS Disadvantages

- An additional layer is added
- The router has to understand MPLS

Chapter 4

Cisco Design Lifecycle (Network Life Cycle)



1. **Plan**: This phase includes processes for the assessment and network strategy, building the network design, and defining a plan.
2. **Build**: This phase includes processes for the validation of the solution, the deployment of new IT and network solutions, and the migration to new infrastructures.
3. **Manage**: This phase includes processes for product support, solution support, optimization, and operations management of the network.

Plan Phase

The Plan phase is divided into three processes:

1. **Strategy and Analysis process**: During the Strategy and Analysis process , network architecture strategies are created and roadmaps to transform the network architecture are developed.
2. **Assessment process**: The assessment determines gaps in the network operation team's ability to support the new technologies being.
3. **Design process**: The introduced. The design process creates a resilient and scalable network design that can support the business requirements.

Build Phase

The Build phase is divided into three processes:

1. **Validation process**: The Validation process confirms that the proposed solution meets your requirements for availability, security, reliability, and performance through assessment and lab environments. This will mitigate the risks associated with upgrading the network.
2. **Deployment process**: The Deployment process installs and configures new IT and network solutions with minimal disruption to your production network. It accomplishes the business and technical goals of the new solution.
3. **Migration process**: The Migration process upgrades the network infrastructure by a systematic and efficient approach, which could control costs, improve operational excellence, reduce network operation costs and system outages, and mitigate risk during device, network, and software refreshes.

Manage Phase

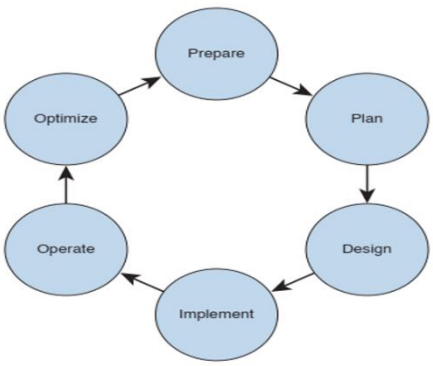
The Manage phase is divided into four processes:

1. **Product Support process**: The Product Support process provides automated network equipment inventory management, allowing better planning of equipment upgrades.
2. **Solution Support process**: The Solution Support process provides dedicated and focused resources to manage and troubleshoot issues that might arise in new complex solutions.
3. **Optimization process**: The Optimization process identifies gaps, delivers recommendations, and provides expert technical support to improve on the deployed solution.
4. **Operations Management process**: The Operation Management process ensures that the network staff has enough competence in the network technology to accelerate adoption of advanced technologies.

PPDIOO Network Life Cycle

Prepare, Plan, Design, Implement, Operate, and Optimize Phases

PPDIOO Phase	Description
Prepare	Establishes organization and business requirements, develops a network strategy, and proposes a high-level architecture
Plan	Identifies the network requirements by characterizing and assessing the network as well as performing a gap analysis
Design	Provides high availability, reliability, security, scalability, and performance
Implement	Installation and configuration of new equipment
Operate	Day-to-day network operations
Optimize	Proactive network management and modifications to the design



Network Design Methodology

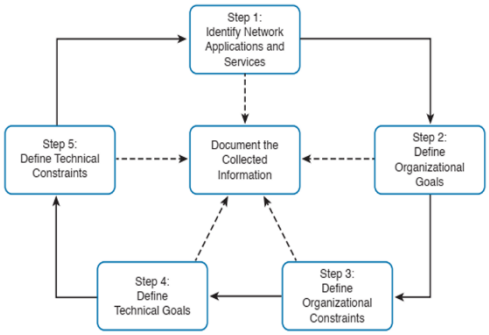
This design methodology has three steps:

Step 1. Identifying customer network requirements
Step 2. Characterizing the existing network
Step3. Designing the network topology and solutions

Identifying Customer Design Requirements

The steps to identify customer requirements are as follows:

- Identify network applications and services.
- Define the organizational goals.
- Define the possible organizational constraints.
- Define the technical goals.
- Define the possible technical constraints.



Characterizing the Existing Network

It identifies a network's major features, tools to analyze existing network traffic, and tools for auditing and monitoring network traffic.

Steps in Gathering Information

- Identify properties of the existing network: network topology, technologies, and applications. Use existing documentation and organizational input.
- Perform a network audit that adds detail to the description of the network.
- Analyze the gathered information.

Network Audit Tools

When performing a network audit, you have three primary sources of information:

- Existing documentation
- Existing network management software tools
- New network auditing tools

The network audit should provide the following information:

- Network device list.
- Hardware specifications
- Software versions
- Configuration of network devices
- Auditing tools' output information
- Interface speeds
- Link, CPU, and memory utilization.
- WAN technology types and carrier information.

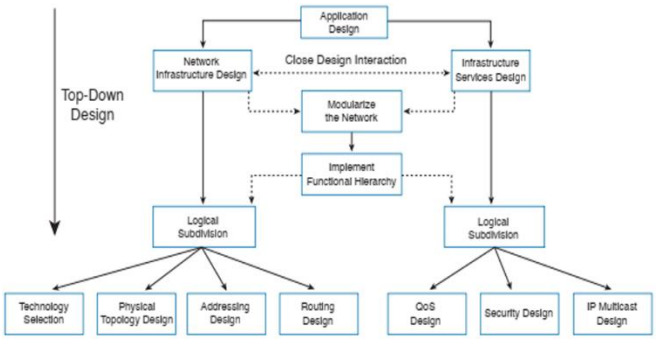
Top-Down Approach for Network Design

Top-down design just means starting your design from the top layer of the OSI model and working your way down.

// Top-down design adapts the network and physical infrastructure to the network application's requirements.

To complete a top-down design, the following is accomplished:

- Analysis of requirements. application and organization
- Design from the top of the OSI reference model:
  - Define requirements for upper layers (application, presentation, session).
  - Specify infrastructure for lower OSI layers (transport, network, data link, physical).
- Gather additional data on the network.



Network Design Document

The design document describes the business requirements; old network architecture; network requirements; and design, plan, and configuration information for the new network.

// The network architects and analysts use it to document the new network changes, and it serves as documentation for the enterprise.

The network design document should include the following sections:

- **Introduction**: This section describes the project's purpose and reasons for the network design.
- **Design Requirements**: This section lists organization's requirements, constraints, and goals.
- **Existing Network Infrastructure**: This section includes logical (Layer 3) topology diagrams; physical topology diagrams; audit results; network health analysis; routing protocols; a summary of applications; a list of network routers, switches, and other devices; configurations; and a description of issues.

Design Approach	Benefits	Disadvantages
Top-down	Incorporates the organization's requirements. Provides the big picture. The design meets current and future requirements.	More time-consuming.
Bottom-up	The design is based on previous experience and allows for a quick solution.	May result in inappropriate design. Organizational requirements are not included.

Chapter 5

Hierarchical Network Models

Hierarchical models enable you to design internetworks that use specialization of function combined with a hierarchical organization.

// Hierarchical models use layers to simplify the tasks for internetworking. Each layer can focus on specific functions, allowing you to choose the right systems and features for each layer.

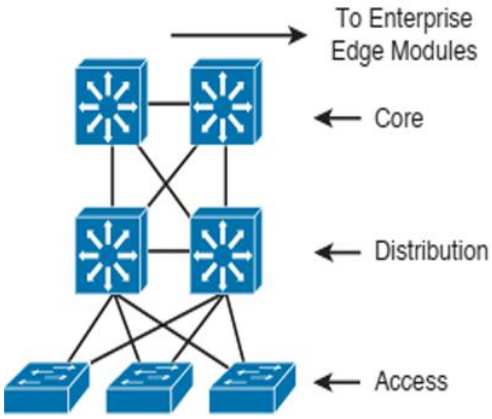
// Hierarchical models apply to both LAN and WAN design.

Benefits of the Hierarchical Model

- Cost savings
- Ease of understanding
- Modular network growth
- Improved fault isolation

Hierarchical Network Design

1. The core layer provides fast transport between distribution switches within the enterprise campus.
2. The distribution layer provides policy-based connectivity.
3. The access layer provides workgroup and user access to the network.



Core Layer

The core layer is the network's high-speed switching backbone that is crucial to corporate Communications. It is also referred as the backbone.

The core layer should have the following characteristics:

- Fast transport
- High reliability
- Redundancy
- Fault tolerance
- Low latency and good manageability
- Avoidance of CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes
- Limited and consistent diameter
- QoS

Distribution Layer

The network's distribution layer is the isolation point between the network's access and core layers.

The distribution layer have the following functions:

- Policy-based connectivity .
- Redundancy and load balancing
- Aggregation of LAN wiring closets
- Aggregation of WAN connections
- QoS
- Security filtering
- Address or area aggregation or summarization
- Departmental or workgroup access
- Broadcast or multicast domain definition
- Routing between virtual LANs (VLANs)
- Media translations
- Redistribution between routing domains
- Demarcation between static and dynamic routing protocols

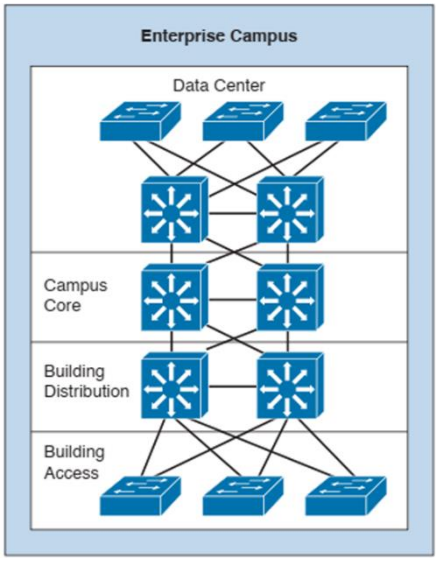
Access Layer

The access layer provides user access to local segments on the network. The access layer is characterized by switched LAN segments in a campus environment.

Functions of the access layer include the following:

- Layer 2 switching
- High availability
- Port security
- Broadcast suppression
- QoS classification and marking and trust boundaries
- Rate limiting/policing
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACLs)
- Spanning tree
- Trust classification
- Power over Ethernet (PoE) and auxiliary VLANs for VoIP
- Network Access Control (NAC)
- Auxiliary VLANs

Enterprise Campus Module



The enterprise campus consists of the following sub modules:

- Campus core
- Building distribution and aggregation switches
- Building access
- Server farm/data center

// The campus infrastructure consists of the campus core, building distribution, and building access layers.

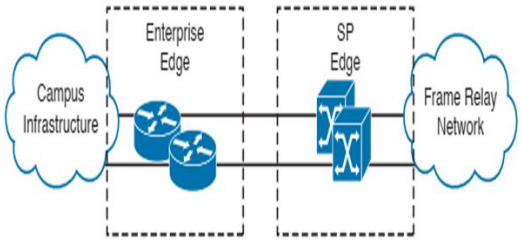
1. The **Campus Core** provides a high-speed switched Backbone between buildings, to the server farm, and towards the enterprise edge.
2. The **Building Distribution** layer aggregates all the closet access switches and performs access control, QoS, route redundancy, and load balancing.
3. The **Building Access** switches provide VLAN access, PoE for IP phones and wireless access points, broadcast suppression, and spanning tree.

Enterprise WAN

The enterprise edge of the enterprise WAN includes access to WANs.

WAN technologies Include the following:

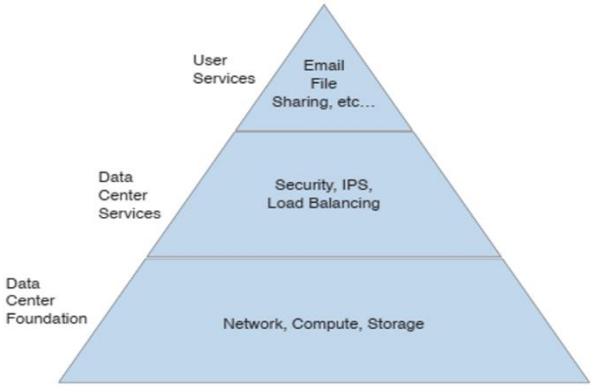
- Multiprotocol Label Switching (MPLS)
- Metro Ethernet
- Leased lines
- Synchronous Optical Network (SONET) and Synchronous
- Digital Hierarchy (SDH)
- PPP
- Frame Relay
- ATM
- Cable
- Digital subscriber line (DSL)
- Wireless



Enterprise DC(Data Center) Architecture

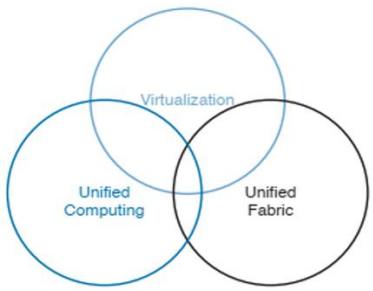
Enterprise DC architecture has three primary layers, called data center foundation, data center services, and user Services.

1. The **Data Center Foundation** layer provides the infrastructure for upper-layer services and applications that users rely on.
2. The **Data Center Services** layer resides above the data center foundation and provides the necessary security firewall and IPS services that protect the applications and critical data in the data center.
3. The top of the architecture for the data center is the **User Services**.

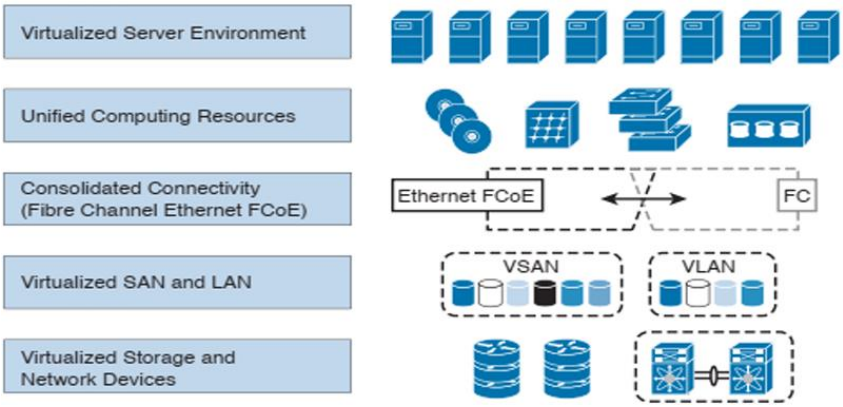


Data Center Foundation Components

1. **Virtualization**
   Virtual local area networks (VLANs), virtual storage area networks (VSANs), and virtual device contexts (VDCs) help to segment the LAN, SAN, and network devices instances.
2. **Unified fabric**
   Fibre Channel over Ethernet (FCoE) and Internet Small Computer Systems Interface (iSCSI) are two methods for implementing unified fabric in the data center over 10 Gigabit Ethernet networks.
3. **Unified computing**
   Cisco Unified Computing System (UCS) is an innovative next-generation data center platform that converges computing, network, storage, and virtualization together into one system.



Data Center Topology Components



Challenges in the DC

- Power required
- Physical rack space usage
- Limits to scale
- Management (resources, firmware)
- Server security
- Virtualization support
- Management effort required

Data Center Space

The data center space element defines the number of racks for servers and telecommunications equipment that can be installed.

There are several factors need to be considered for data center:

- The number of employees who will be supporting the data center
- The number of servers and the amount of storage gear and networking equipment that will be needed
- The space needed for non-infrastructure areas:
- Shipping and receiving
- Server and network staging
- Storage rooms, break rooms, and bath rooms
- Employee office space

Data Center Power

The power in the data center facility is used to power cooling devices, servers, storage equipment, the network, and some lighting equipment. Cooling down the data center requires the most power, next to servers and storage.

Here are some key points related to data center power:

- Defines the overall power capacity.
- Provides physical electrical infrastructure and addresses redundancy.

Power is consumed by the following:

- Cooling
- Servers
- Storage

Enterprise DC Infrastructure

Enterprise data center infrastructure follows the Cisco multilayer architecture, which includes a DC core connecting to the local area network (LAN) core at the center.

The LAN core provides access to the WAN, LAN, and the Internet/demilitarized zone (DMZ) via additional network connections.

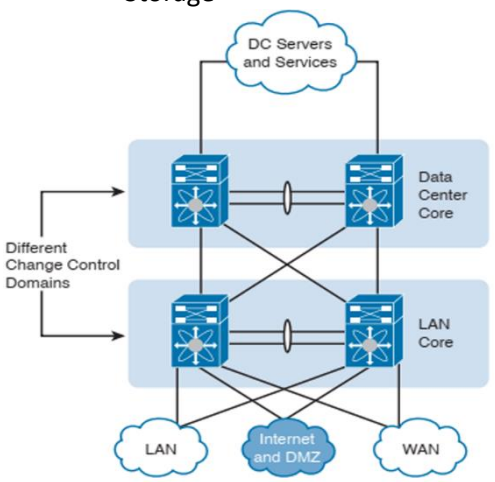


Figure 4-8 *Enterprise data center infrastructure overview*

Data Center Storage for Network

Servers can use locally attached storage or they can access storage over the storage area network (SAN).

Direct attached storage (DAS) is composed of local disks that are physically installed in the server.

// DAS is **not** very flexible because only the local host can use the storage in most cases.

Figure 4-9 illustrates the legacy LAN and SAN separation approach to storage in the data center.

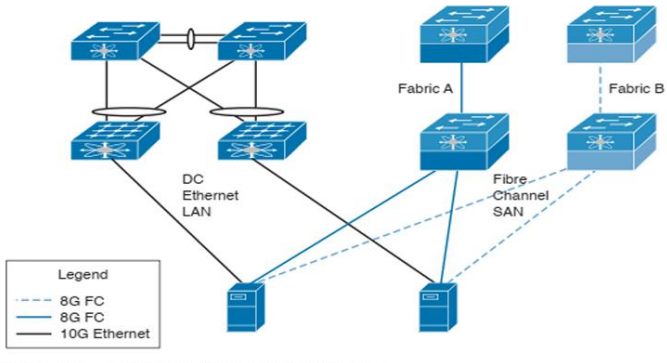


Figure 4-9 *Traditional LAN and SAN separation*