FUTURE VISION BIE

One Stop for All Study Materials & Lab Programs

Future Vision

By K B Hemanth Raj

Scan the QR Code to Visit the Web Page

Or

Visit : https://hemanthrajhemu.github.io

Gain Access to All Study Materials according to VTU,
CSE – Computer Science Engineering,
ISE – Information Science Engineering,
ECE - Electronics and Communication Engineering
& MORE...

MODULE 2: STORAGE AREA NETWORKS

MODULE 2: STORAGE AREA NETWORKS

2.1 Business Needs and Technology Challenges

• Companies are experiencing an explosive growth in information.
• This information needs to be stored, protected, optimized, and managed efficiently.
• Challenging task for data-center managers:
Providing low-cost, high-performance information-management-solution (ISM).
• ISM must provide the following functions:

1) Just-in-time information to users

➢ Information must be available to users when they need it.
➢ Following key challenges must be addressed:
→ explosive growth in online-storage
→ creation of new servers and applications
→ spread of mission-critical data throughout the company and
→ demand for 24×7 data-availability

2) Integration of information infrastructure with business-processes

➢Storage-infrastructure must be integrated with business-processes w/o compromising on security

3) Flexible and resilient storage architecture

➢ Storage-infrastructure must provide flexibility that aligns with changing business-requirements.
➢ Storage should scale without compromising performance requirements of the applications.
➢ At the same time, the total cost of managing information must be low.

• Direct-attached storage (DAS) is often referred to as a stovepiped storage environment.
• Problem with DAS:
1) Hosts "own" the storage.
Hence, it is difficult to manage and share resources on these separated storage-devices.
• Solution:
1) Efforts to organize this dispersed data led to the emergence of the storage area network (SAN).

2.2 SAN

• SAN is a high-speed, dedicated network of servers and shared storage devices (Figure 2-1).

• SAN

→ enables storage consolidation (servers --> hosts)
→ enables storage to be shared across multiple-servers
→ enables companies to connect geographically dispersed servers and storage.

• Advantages:

1) Improves the utilization of storage resources compared to DAS architecture.
2) Reduces the total amount of storage an organization needs to purchase and manage.
3) Storage management becomes centralized and less complex.
4) Reduces the cost of managing information.
5) Provides effective maintenance and protection of data.
6) Meets the storage demands efficiently with better economies of scale

• Common SAN deployments are 1) Fibre Channel (FC) SAN and 2) IP SAN.

1) **FibreChannel SAN** uses Fibre Channel protocol for the transport of data, commands, and status information between servers and storage devices.

2) **IP SAN** uses IP-based protocols for communication.

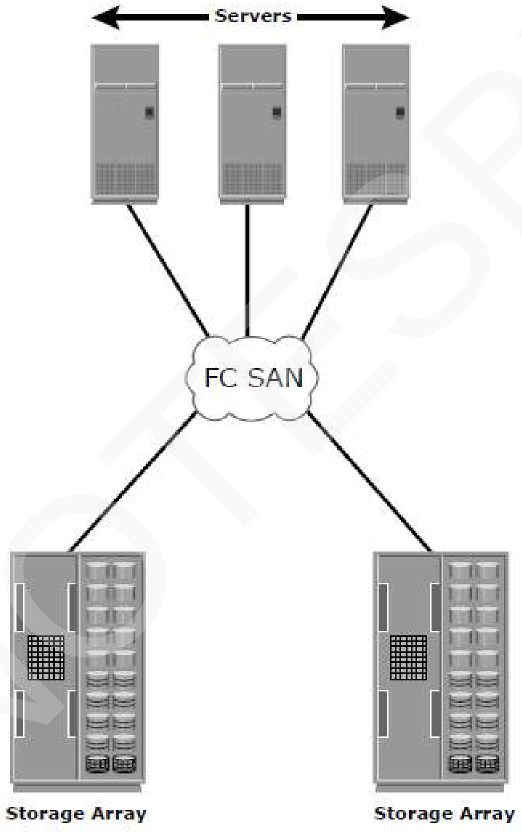

Figure 2-1: SAN implementation

2.3 Fibre-Channel: Overview

• The FC architecture forms the fundamental construct of the SAN-infrastructure.

• Fibre-channel is a high-speed network technology that runs on

i) high-speed optical-fiber cable and
ii) serial copper cable.

• Normally, optical-fiber cable is preferred for front-end SAN connectivity.
Serial copper cable is preferred for back-end disk connectivity.

• Advantages:

1) Developed to increase speeds of data-transmission b/w servers & storage devices.
2) Credit-based flow control mechanism delivers data as fast as the destination buffer is able to receive it, without dropping frames.
3) Has very little transmission overhead.
4) Highly scalable: A single FC network can accommodate approximately 15 million devices.

2.4 Components of SAN

• A SAN consists of 5 basic components:
  1) Node-ports
  2) Cabling
  3) Interconnecting-devices (such as FC-switches or hubs)
  4) Storage-arrays and
  5) Management-software.

2.4.1 Node-Ports

• Nodes refer to devices such as host, storage and tape libraries. (Figure 2-2)
• Each node is a source or destination of information.
• Each node has ports to provide a physical-interface for communicating with other nodes.
• The ports are integral components of an HBA and the storage front-end controllers.
• A port operates in full-duplex mode which has
  i) transmit (Tx) link and
  ii) receive (Rx) link.

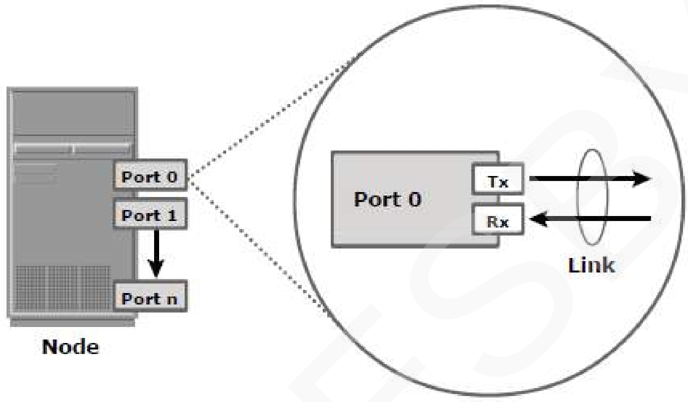

Figure 2-2: Nodes, ports, and links

2.4.2 Cabling

• For cabling, both optical-cable and copper-wire is used.
  1) Optical-fiber is used for long distances.
  2) Copper is used for shorter distances.
    This is because copper provides a better SNR for distances up to 30 meters.
• Optical-cable carry data in the form of light. (SNR --> signal-to-noise ratio)
• Two types of optical-cables: 1) multi-mode and
  2) single-mode.

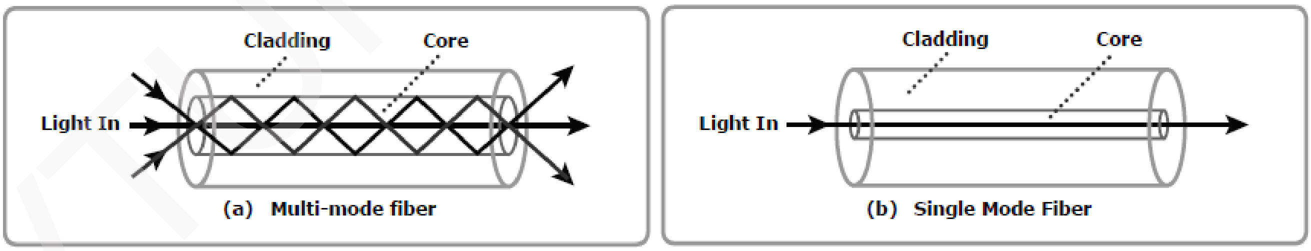

Figure 2-3: Multi-mode fiber and single-mode fiber

1) Multi-Mode Fiber (MMF)

• The cable carries multiple beams of light projected at different angles simultaneously onto the core of the cable.
• Based on the bandwidth, this is classified as
  → OM1 (62.5μm)
  → OM2 (50μm) and
  → laser optimized OM3 (50μm).

• Advantage:
  1) Used within data centers for shorter distances.
• Disadvantages:
  1) Modal-Dispersion
  ➢ Multiple light beams traveling inside the cable tend to disperse and collide (Figure 2-3 (a)).
    This collision weakens the signal strength.
      This process is known as **modal-dispersion**.
  2) Attenuation
  ➢ An MMF cable is typically used for short distances. This is because
    of signal degradation (attenuation) due to modal-dispersion.

2) Single-Mode Fiber (SMF)

• The cable carries a single ray of light projected at the center of the core (Figure 2-3 (b)).
• The cables are available in diameters of 7–11 microns. The most common size is 9 microns.
• Advantages:
  1) The small core and the single light wave limits modal-dispersion.
  2) Provides minimum signal attenuation over maximum distance (up to 10 km).
  3) Used for longer distances.
    The distance depends on
      i) power of the laser at the transmitter and
      ii) sensitivity of the receiver.

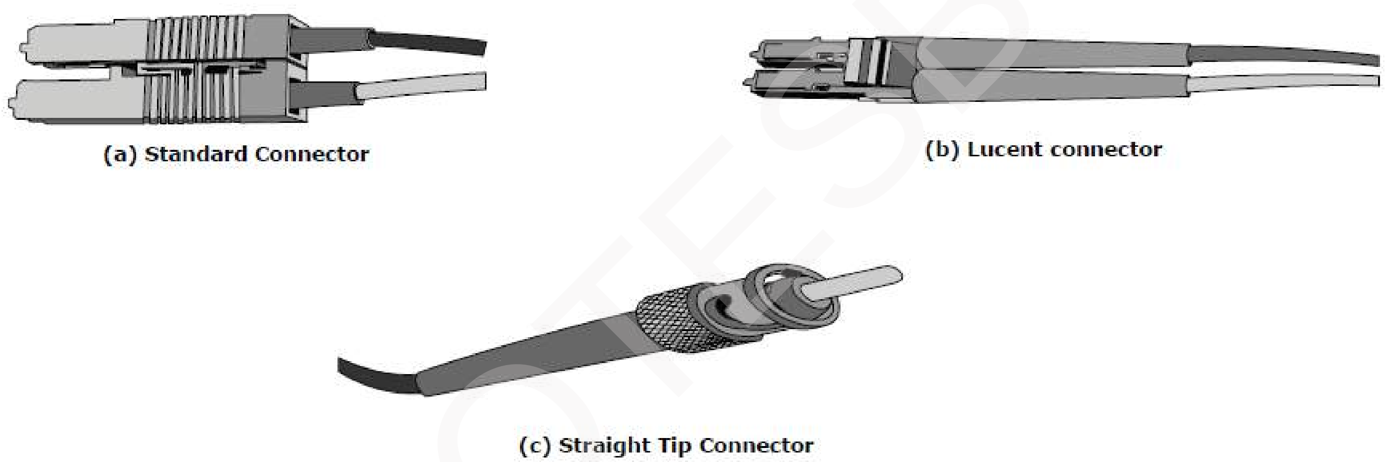

Figure 2-4: SC, LC, and ST connectors

2.4.2.1 Connector

• A connector is attached at the end of a cable
  → to enable swift connection and disconnection of the cable to and from a port.
• Three commonly used connectors (Figure 2-4):
  1) Standard Connector (SC)
  ➢ An SC is used for data-transmission speeds up to 1 Gbps.
  2) Lucent Connector (LC)
  ➢ An LC is used for data-transmission speeds up to 4 Gbps.
  3) Straight Tip (ST)
  ➢ An ST is used with Fibre patch panels.

2.4.3 Interconnect-Devices

• Three commonly used interconnect-devices are hubs, switches, and directors.

i) Hub

• Hub is used as interconnect-device in FC-AL implementations.
• It is used to connect nodes in a star-topology.
• All the nodes must share the bandwidth because data travels through all the connection-points.

ii) Switch

• Switch is more intelligent than hub.
• It is used to directly route data from one physical-port to another
• Advantage:
    1) Low cost
    2) High performance
    3) Each node has a dedicated path. This results in bandwidth aggregation.
• Switches are available
    → with a fixed port count or
    → with modular design.
• In a modular switch, port count is increased by installing additional port cards to open slots.

iii) Director

• Director is high-end switch with
    → higher port count and
    → better fault tolerance capabilities.
• It is larger than switch.
• It is deployed for data center implementations.
• In modular director, port count is increased by installing additional line cards to the director's chassis
• High-end directors and switches contain redundant components to provide high availability.
• Both directors and switches have management-ports for connectivity to management-servers.

2.4.4 Storage-Arrays

• The fundamental purpose of a SAN is to provide host-access to storage-resources.
• Modern storage-arrays are used for storage-consolidation and -centralization.
• Storage-array provides
    → high availability and redundancy
    → improved performance
    → business continuity and
    → multiple host connectivity.

2.4.5 Management-Software

• Management-software manages the interfaces between
    1) Hosts
    2) Interconnect-devices, and
    3) Storage-arrays.
• It provides a view of the SAN environment.
• It enables management of various resources from one central console.
• It provides key functions such as
    1) mapping of storage-devices, switches, and servers
    2) monitoring and generating alerts for discovered devices, and
    3) logical partitioning of the SAN called zoning.

2.5 FC Connectivity

- The FC architecture supports 3 basic interconnectivity options:
  1) Point-to-point
  2) Arbitrated loop (FC-AL) and
  3) Fabric-connect (FC-SW).

2.5.1 Point-to-Point

- Two devices are connected directly to each other (Figure 2-5).
- Advantage:
  1) Provides a dedicated-connection for data-transmission between nodes.
- Disadvantages:
  1) Provides limited connectivity, '.' only 2 devices can communicate with each other at given time
  2) Not Scalable: Cannot be scaled to accommodate a large number of network-devices.
- Standard DAS uses point-to-point connectivity.

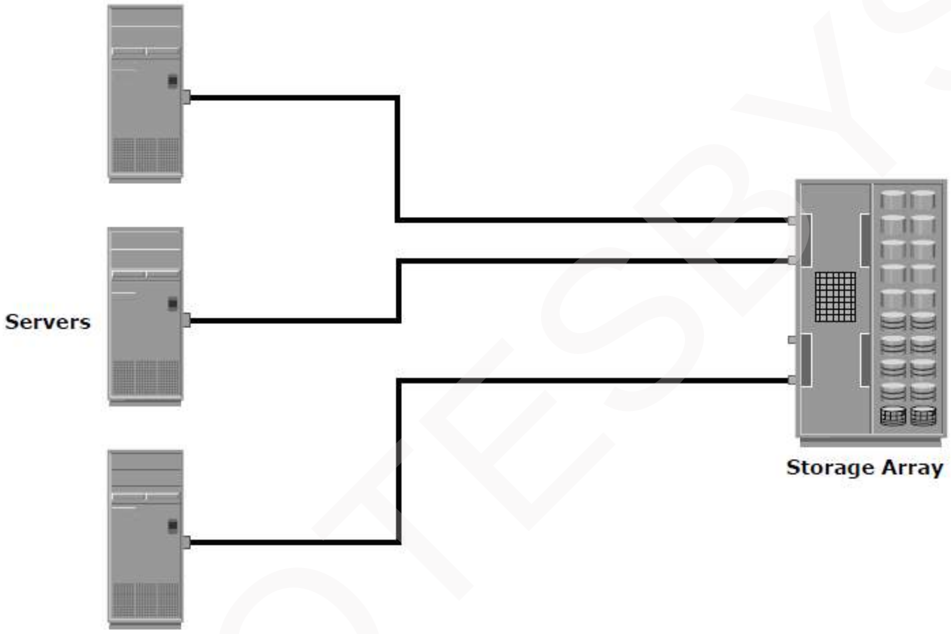

Figure 2-5: Point-to-point topology

2.5.2 FC-AL (Fibre-Channel Arbitrated Loop)

• Devices are attached to a shared loop (Figure 2-6).
• FC-AL has the characteristics of
  1) token ring topology and
  2) physical star-topology.
• Each device competes with other devices to perform I/O operations.
• All devices must compete to gain control of the loop.
• At any time, only one device can perform I/O operations on the loop.
• Two implementations:

1) FC-AL can be implemented without any interconnecting-devices.
   i.e. Devices are directly connected to one another in a ring through cables.
2) FC-AL can be implemented using hubs where the arbitrated loop is physically connected in a star topology.

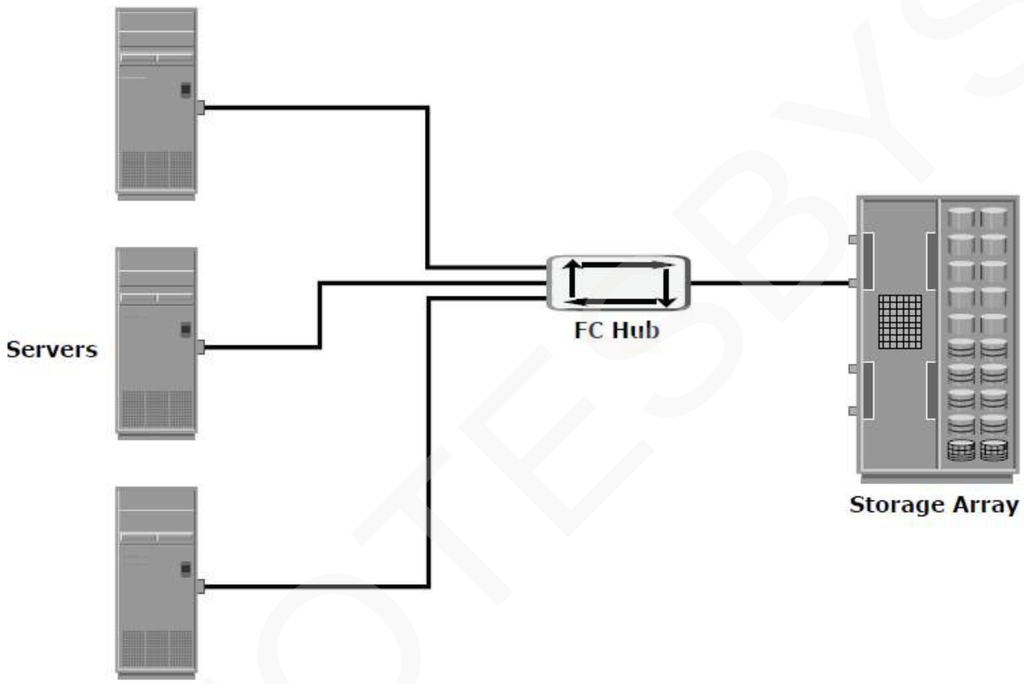

Figure 2-76: Fibre Channel arbitrated loop

• Disadvantages:

1) Low Performance
Since all devices share bandwidth in the loop, only one device can perform I/O operation at a time. Hence, other devices have to wait to perform I/O operations.
2) Addressing
Since 8-bit addressing is used, only up to 127 devices can be supported on a loop.
3) Not Scalable
Adding a device results in loop re-initialization. This causes a momentary pause in loop traffic.

2.5.3 FC-SW (Fibre-Channel Switched-Fabric)

- FC-SW is also referred to as fabric-connect.
- A fabric is a logical-space in which all nodes communicate with one another in a network (Figure 2-7)
- The logical-space can be created with a switch or a network-of-switches.
- In a fabric,
  - i) each switch contains a unique domain-identifier, which is part of the FC-address.
  - ii) each port has a unique 24-bit FC-address for communication.
  - iii) **ISL** refers to a link used to connect any two switches.
    - ➢ ISL is used to transfer
      - → data between host and storage (ISL --> Inter-Switch-Link)
      - → fabric-management-information between 2 switches.
    - ➢ ISL enables switches to be connected together to form a single-larger fabric.
- Advantages:
  - 1) Provides a dedicated-bandwidth for data-transmission between nodes.
  - 2) Scalable
    - ➢ New devices can be added without interrupting normal-operations.

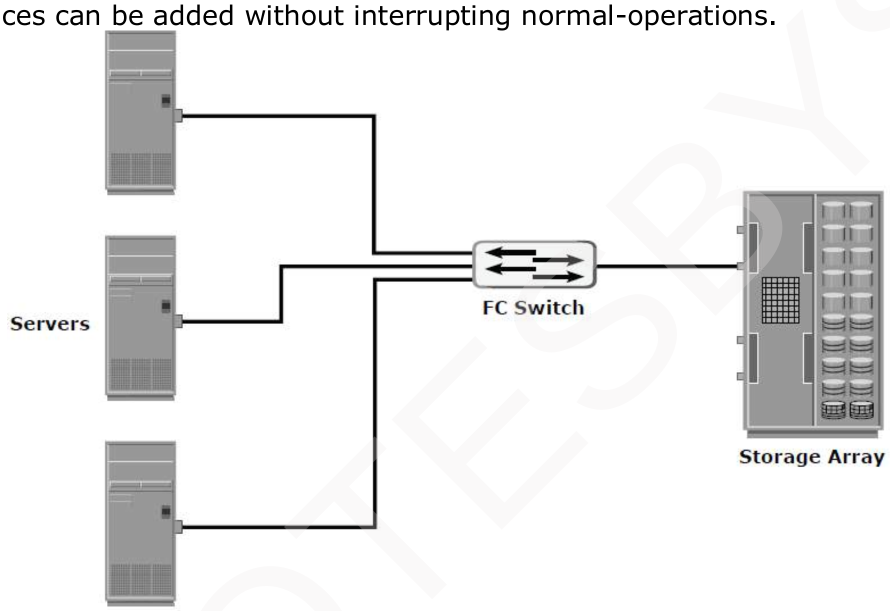

Figure 2-7: Fibre Channel switched fabric

- A fabric can have many tiers (Figure 2-8).
- When no. of tiers increases, the distance traveled by message to reach each switch also increases.
- As the distance increases, the time taken to propagate the message also increases.
- The message may include
  - → fabric-reconfiguration event such as the addition of a new switc or
  - → zone-set propagation event.
- Figure 2-8 illustrates two-tier and three-tier fabric architecture.(tiers --> levels)

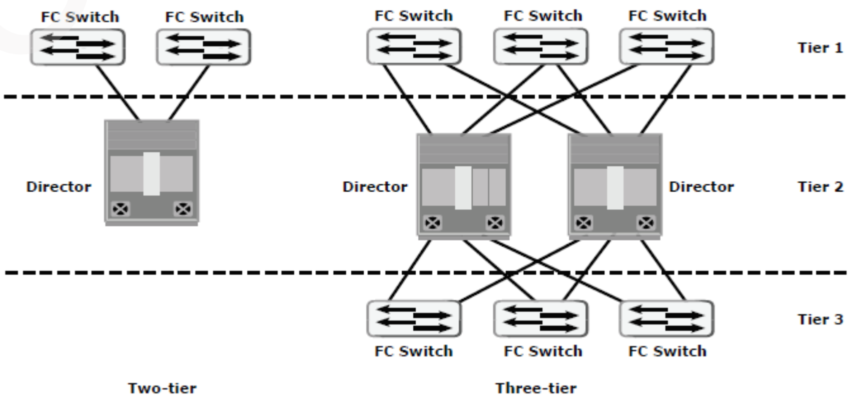

Figure 2-8: Tiered structure of FC-SW topology

2.5.3.1 FC-SW Transmission

- FC-SW uses switches that are intelligent-devices.
- Switch can be used to route data traffic between nodes directly through ports.
- Fabric can be used to route the frames between source and destination.
- For example (Figure 2-9):
  - ➢ If node-B wants to communicate with node-D, then
    - i) node-B must login first and
    - ii) Then, node-B must transmit data via the FC-SW.
  - ➢ This link is considered a dedicated-connection b/w initiator (node-B) and target (node-D).

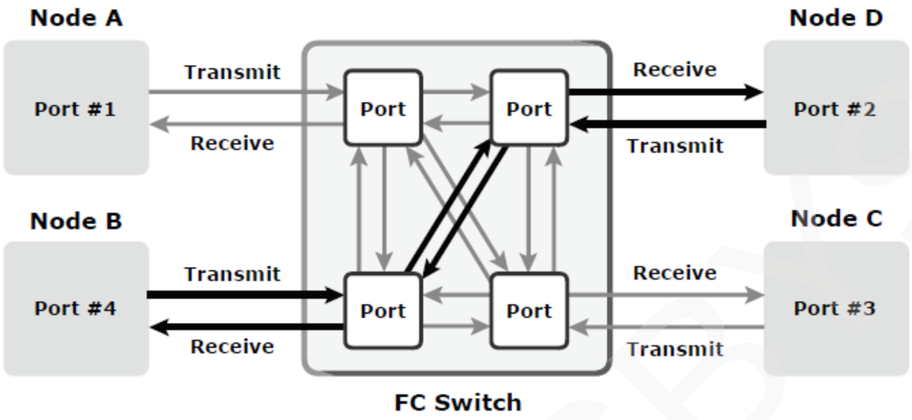

Figure 2-9: Data tansmission in FC-SW topology

2.6 Fibre-Channel Ports

• Ports are the basic building blocks of an FC-network.
• Ports on the switch can be one of the following types (Figure 2-10):

1) N_Port (node-port)

• N_port is an end-point in the fabric.
• It is used to connect to a switch in a fabric.
• It can be
→ host port (HBA) or
→ storage-array port

2) E_Port (expansion port)

• E_port is used to setup connection between two FC-switches.
• The E_Port on an FC-switch is connected to the E_Port of another FC-switch.

3) F_Port (fabric port)

• It is used to connect to a node in the fabric.
• It cannot participate in FC-AL.

4) G_Port (generic port)

• G_port can operate as an E_port or an F_port.
• It can determine its functionality automatically during initialization.

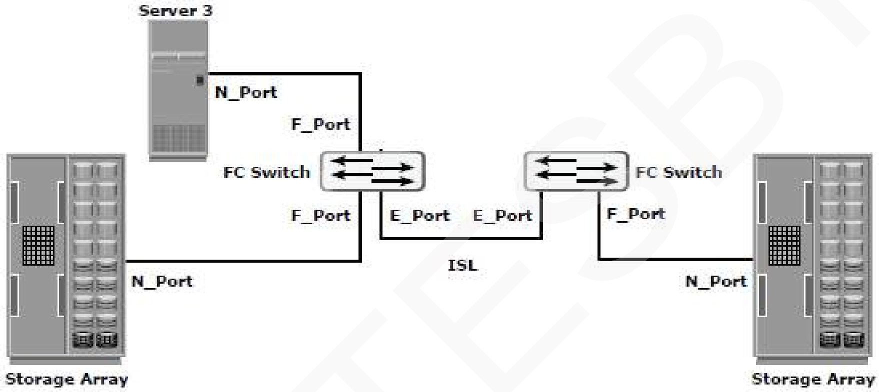

Figure 2-10: Fibre channel ports

2.7 Fibre-Channel Architecture

• The FC architecture represents true network integration with standard interconnecting-devices.
• FC is used for making connections in SAN.
• Channel technologies provide
→ high levels of performance (FCP --> Fibre-channel Protocol)
→ low protocol overheads.
• Such performance is due to the static nature of channels and the high level of hardware and software integration provided by the channel technologies.
• FCP is the implementation of serial SCSI-3 over an FC-network.
• All external and remote storage-devices attached to the SAN appear as local devices to the host OS.
• The key advantages of FCP are as follows:
1) Sustained transmission bandwidth over long distances.
2) Support for a larger number of addressable devices over a network.
Theoretically, FC can support over 15 million device addresses on a network.
3) Exhibits the characteristics of channel transport and provides speeds up to 8.5 Gb/s (8 GFC).

2.7.1 Fibre-Channel Protocol Stack

• A communication-protocol can be understood by viewing it as a structure of independent-layers.
• FCP defines the protocol in 5 layers (Figure 2-11):
1) FC-0 Physical-interface
2) FC-1 Transmission Protocol
3) FC-2 Transport Layer
4) FC-3 (FC-3 layer is not implemented).
5) FC-4 Upper Layer Protocol
• In a layered-model, the peer-layers on each node talk to each other through defined-protocols.

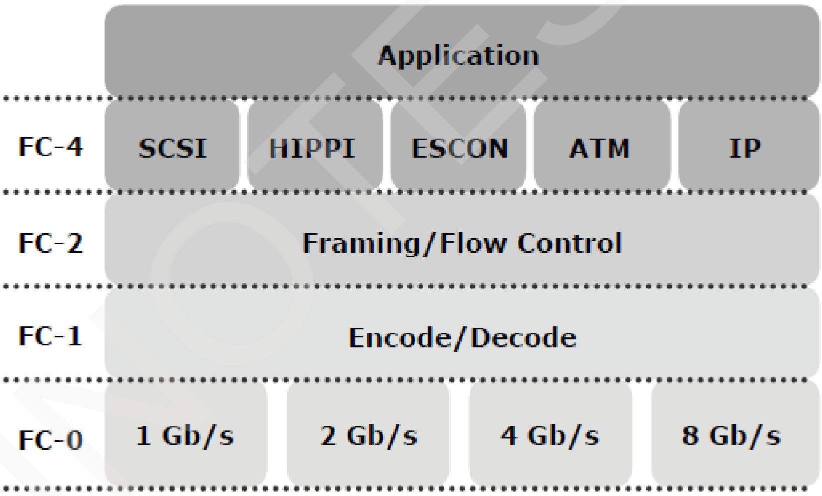

Figure 2-11: Fibre channel protocol stack

FC-4 Upper Layer Protocol

• FC-4 is the uppermost layer in the stack.
• This layer defines
→ application interfaces and
→ how ULP is mapped to the lower FC-layers.
• The FC standard defines several protocols that can operate on the FC-4 layer.
For example:
SCSI
HIPPI Framing Protocol
Enterprise Storage Connectivity (ESCON)
ATM
IP (ULP --> Upper Layer Protocol)

FC-2 Transport Layer

• This layer contains
 1) payload
 2) addresses of the source and destination ports and
 3) link-control-information.

• This layer provides
 → FC-addressing
 → structure & organization of data (frames, sequences, and exchanges).

• This layer also defines
 → fabric-services
 → classes of service (1, 2 or 3)
 → flow-control and
 → routing.

FC-1 Transmission Protocol

• This layer defines how data is encoded prior to transmission and decoded upon receipt.

• Here is how encoding and decoding is done:
 1) At the transmitter-node,
  i) FC-1 layer encodes an 8-bit character into a 10-bit transmissions character.
  ii) Then, this 10-bit character is transmitted to the receiver-node.
 2) At the receiver-node,
  i) 10-bit character is passed to the FC-1 layer.
  ii) Then, FC-1 layer decodes the 10-bit character into the original 8-bit character.

• This layer also defines the transmission words such as
 i) FC frame delimiters which identify the start and end of a frame and
 ii) primitive signals that indicate events at a transmitting port.

• This layer also performs link initialization and error recovery

FC-0 Physical-Interface

• FC-0 is the lowest layer in the stack.

• This layer defines
 → physical-interface
 → transmission medium used (e.g. copper-wire or optical-fiber)
 → transmission of raw bits.

• The specification includes
 i) cables
 ii) connectors (such as SC, LC) and
 iii) optical and electrical parameters for different data rates.

• The transmission can use both electrical and optical media.

2.7.2 Fibre-Channel Addressing

2.7.2.1 FC-Address

• An FC-address is dynamically assigned when a port logs on to the fabric.
• Various fields in FC-address are (Figure 2-12):

1) Domain ID

• This field contains the domain ID of the switch
• A Domain ID is a unique number provided to each switch in the fabric.
• Out of the possible 256 domain IDs,
  i) 239 are available for use;
  ii) remaining 17 addresses are reserved for fabric management services
• For example,
  FFFFFC is reserved for the name-server
  FFFFFE is reserved for the fabric login service.

2) Area ID

• This field is used to identify a group of ports used for connecting nodes.
• An example of a group of ports with common area ID is a port card on the switch.

3) Port ID

• This field is used to identify the port within the group.
• The maximum possible number of node ports in a fabric is calculated as
  239 domains × 256 areas × 256 ports = 15,663,104.

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Domain ID								Area ID								Port ID							

Figure 2-12: 24-bit FC address of N_port

2.7.2.2 WWN (World Wide Name)

• WWN refers to a 64-bit unique identifier assigned to each device in the FC-network.
• Two types of WWNs are used (Figure 2-13):
  i) WWNN (World Wide Node Name) and (MAC --> Media Access Control)
  ii) WWPN (World Wide Port Name).
• FC-address vs. WWN
  ii) FC-address is a dynamic name for each device on an FC-network.
  ii) WWN is a static name for each device on an FC-network.
• WWN is similar to the MAC-address used in IP-network.
• WWN is burned into the hardware or assigned through software.
• Normally, WWN is used for identifying storage-device and HBA.
• The name-server are used to store the mapping of WWNs to FC-addresses for nodes.
• Figure 2-13 illustrates the WWN structure for an array and the HBA.

World Wide Name - Array															
5	0	0	6	0	1	6	0	0	0	6	0	0	1	B	2
0101	0000	0000	0110	0000	0001	0110	0000	0000	0000	0110	0000	0000	0001	1011	0010
	Company ID 24 bits						Port	Model Seed 32 bits							

World Wide Name - HBA															
1	0	0	0	0	0	0	0	c	9	2	0	d	c	4	0
	Reserved 12 bits			Company ID 24 bits						Company Specific 24 bits					

Figure 2-13: World Wide Names

2.7.3 FC Frame

• An FC frame consists of five parts (Figure 2-14):

1) SOF (Start of frame)	2) Frame-header	3) Data field
4) CRC	5) EOF (End of frame).

1) SOF (Start of frame)

• This field acts as a delimiter.
• In addition, this field acts as a flag that indicates whether the frame is the first frame in a sequence.

2) Data field

• This field is used to carry the payload.

3) EOF (End of frame)

• This field also acts as a delimiter.

4) Frame-Header

• This field contains addressing information for the frame.
• Length of frame-header - 24 bytes
• This field includes the following information:

→ Source ID (S_ID) & Destination ID (D_ID)
→ Sequence ID (SEQ_ID) & Sequence Count (SEQ_CNT)
→ Originating Exchange ID (OX_ID) & Responder Exchange ID (RX_ID) and
→ Some other control-fields.

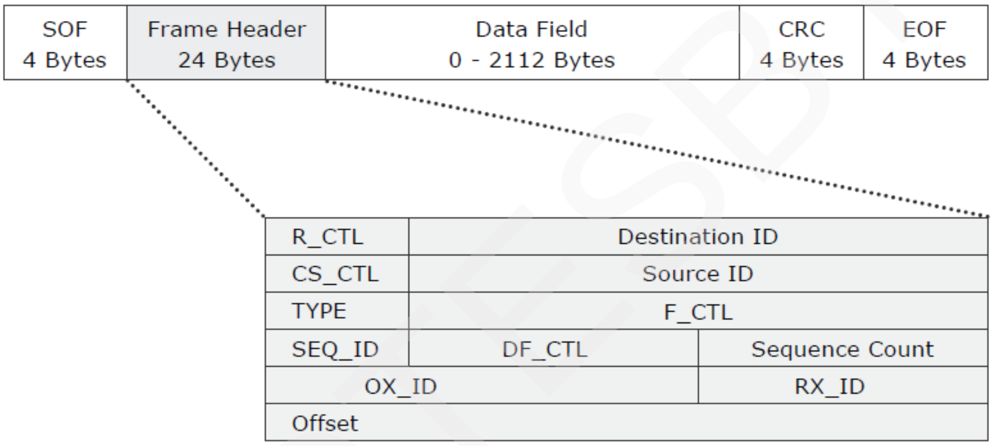

Figure 2-14: FC frame

• The frame-header also defines the following fields:

i) Routing Control (R_CTL)

• This field indicates whether the frame is a link-control-frame or a data-frame.
• Link-control-frames are non-data-frames that do not carry any payload.

Data-frame vs. Control-frame

➢ Data-frames are used carry the payload and thus perform data-transmission.
➢ On the other hand, control-frames are used for setup and messaging.

ii) Class Specific Control (CS_CTL)

• This field specifies link-speeds for class-1 and class-4 data-transmission.

iii) TYPE

• This field serves 2 purpose:

i) If the frame is a data-frame, this field describes the ULP to be carried on the frame.
The ULP can be SCSI, IP or ATM.
For example,
If the frame is a data-frame and TYPE=8, then SCSI will be carried on the frame.
ii) If the frame is a control-frame, this field is used to signal an event such as fabric-busy.

iv) Data Field Control (DF_CTL)

• This field indicates the presence of any optional-headers at the beginning of the data-payload.
• It is a mechanism to extend header-information into the payload.

v) Frame Control (F_CTL)

• This field contains control-information related to frame-content.
• For example,

One of the bits in this field indicates whether this is the first sequence of the exchange.

2.7.4. Structure and Organization of FC Data

• In an FC-network, data transport is analogous to a conversation between two people, wherein
→ frame represents a word
→ sequence represents a sentence and
→ exchange represents a conversation.

1) Exchange Operation

• This enables two node ports to identify and manage a set of information-units.
• Each ULP has its protocol-specific information that must be sent to another port.
• This protocol-specific information is called an information unit.
• The information-unit maps to a sequence.
• An exchange consists of one or more sequences.

2) Sequence

• It refers to a contiguous set of frames that are sent from one port to another.
• It corresponds to an information-unit, as defined by the ULP.

3) Frame

• It is the fundamental unit of data-transfer at Layer 2.
• Each frame can contain up to 2112 bytes of payload.

2.7.5 Flow-Control

• Flow-control defines the pace of the flow of data-frames during data-transmission.
• Two flow-control mechanisms: 1) BB_Credit and 2) EE_Credit.

1) BB_Credit (buffer-to-buffer credit)

• It is used for hardware-based flow-control.
• It controls the maximum number of frames that can be present over the link at any time.
• BB_Credit management may take place between any two ports.
• The transmitting-port
→ maintains a count of free receiver buffers and
→ continues to send frames if the count is greater than 0.
• It provides frame acknowledgment through the Receiver Ready (R_RDY) primitive.

2) EE_Credit (end-to-end credit)

• The function of EE_Credit is similar to that of BB_ Credit.
• When an initiator and a target establish themselves as nodes communicating with each other, they exchange the EE_Credit parameters (part of Port Login).
• The EE_Credit mechanism affects the flow-control for class 1 and class 2 traffic only.

2.7.6 Classes of Service

• Three different classes of service are defined to meet the requirements of different applications.
• The table below shows three classes of services and their features (Table 2-1).

	CLASS 1	CLASS 2	CLASS 3
Communication type	Dedicated connection	Nondedicated connection	Nondedicated connection
Flow control	End-to-end credit	End-to-end credit B-to-B credit	B-to-B credit
Frame delivery	In order delivery	Order not guaranteed	Order not guaranteed
Frame acknowl-edgement	Acknowledged	Acknowledged	Not acknowledged
Multiplexing	No	Yes	Yes
Bandwidth utilization	Poor	Moderate	High

Table 2-1: FC Class of Services

• Class F is another class of services.
Class F is intended for use by the switches communicating through ISLs.
• Class F is similar to Class 2 because
Class F provides notification of non-delivery of frames.
• Other defined Classes 4, 5, and 6 are used for specific applications.

2.8 Fabric Services

• FC switches provide a common set of services:

1) Fabric Login Server
2) Fabric Controller
3) Name Server, and
4) Management Server.

1) Fabric Login Server

• It is used during the initial part of the node's fabric login process.
• It is located at the predefined address of FFFFFE.

2) Name Server

• It is responsible for name registration and management of node ports.
• It is located at the predefined address FFFFFC and
• Each switch exchanges its Name Server information with other switches in the fabric to maintain a synchronized, distributed name service.

3) Fabric Controller

• It is responsible for managing and distributing Registered State Change Notifications (RSCNs) to the registered node ports.
• It also generates Switch Registered State Change Notifications (SW-RSCNs) to every other domain (switch) in the fabric.
• The RSCNs keep the name server up-to-date on all switches in the fabric.
• It is located at the predefined address FFFFFD.

4) Management Server

• It enables the FC SAN management software to retrieve information and administer the fabric.
• It is located at the predefined address FFFFFA

2.9 Zoning

• Zoning is an FC-switch function (Figure 2-15).
• Zoning enables nodes within the fabric to be logically segmented into groups, so that groups can communicate with each other.
• A name-server contains FC-address & world wide-name of all devices in the network.
• A device can be host or storage-array.
 1) When a device logs onto a fabric, it is registered with the name-server.
 2) When a port logs onto the fabric, it goes through a device discovery-process.
• The zoning function controls discovery-process by
 allowing only the members in the same zone to establish these link-level services.
• A zoning process can be defined by the hierarchy of members, zones, and zone-sets. (Figure 2-16).
 1) A **member** refers to
  a node within the SAN or
  a port within the switch
 2) A **zone** refers to a set of members that have access to one another.
 3) A **zone-set** refers to a set of zones.
 ➢ These zones can be activated or deactivated as a single entity in a fabric.
 ➢ Only one zone-set per fabric can be active at a time.
 ➢ Zone-sets are also referred to as zone configurations.

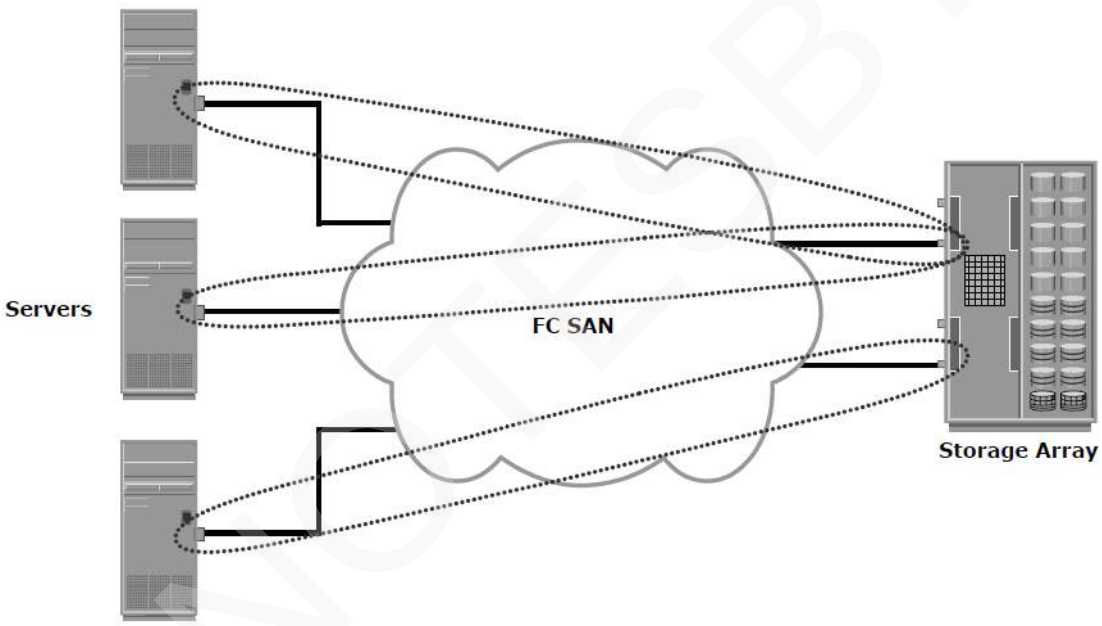

Figure 2-15: Zoning

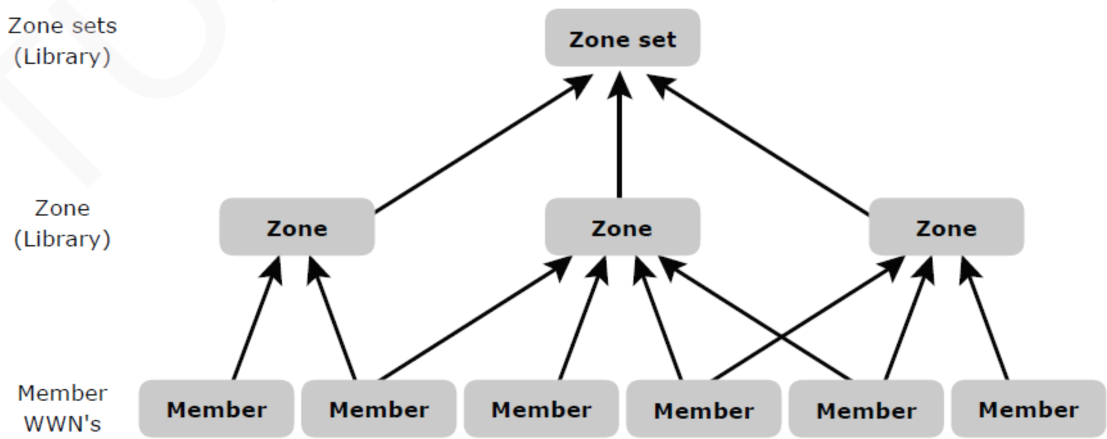

Figure 2-16: Members, zones, and zone sets

2.9.1 Types of Zoning

- Zoning can be classified into 3 types (Figure 2-17):

1) Port Zoning

- Port zoning is also called hard zoning.
- It uses FC-addresses of the physical-ports to define zones.
- The access to data is determined by the switch-port to which a node is connected.
- The FC-address is dynamically assigned when the port logs onto the fabric.
- Therefore, any change in the fabric-configuration affects zoning.
- Advantage:
  This method is secure
- Disadvantage:
  Has to update zoning configuration information in case of fabric-reconfiguration.

2) WWN Zoning

- WWN zoning is also called soft zoning.
- It uses World Wide Names to define zones.
- Advantage:
  i) Its flexibility.
  ii) Scalable: allows the SAN to be recabled without reconfiguring the zone information.
  This is possible because the WWN is static to the node-port.

3) Mixed zoning

- It combines the qualities of both WWN zoning and port zoning.
- Using mixed zoning enables a specific port to be tied to the WWN of a node.
- Figure 2-17 shows the three types of zoning on an FC-network.

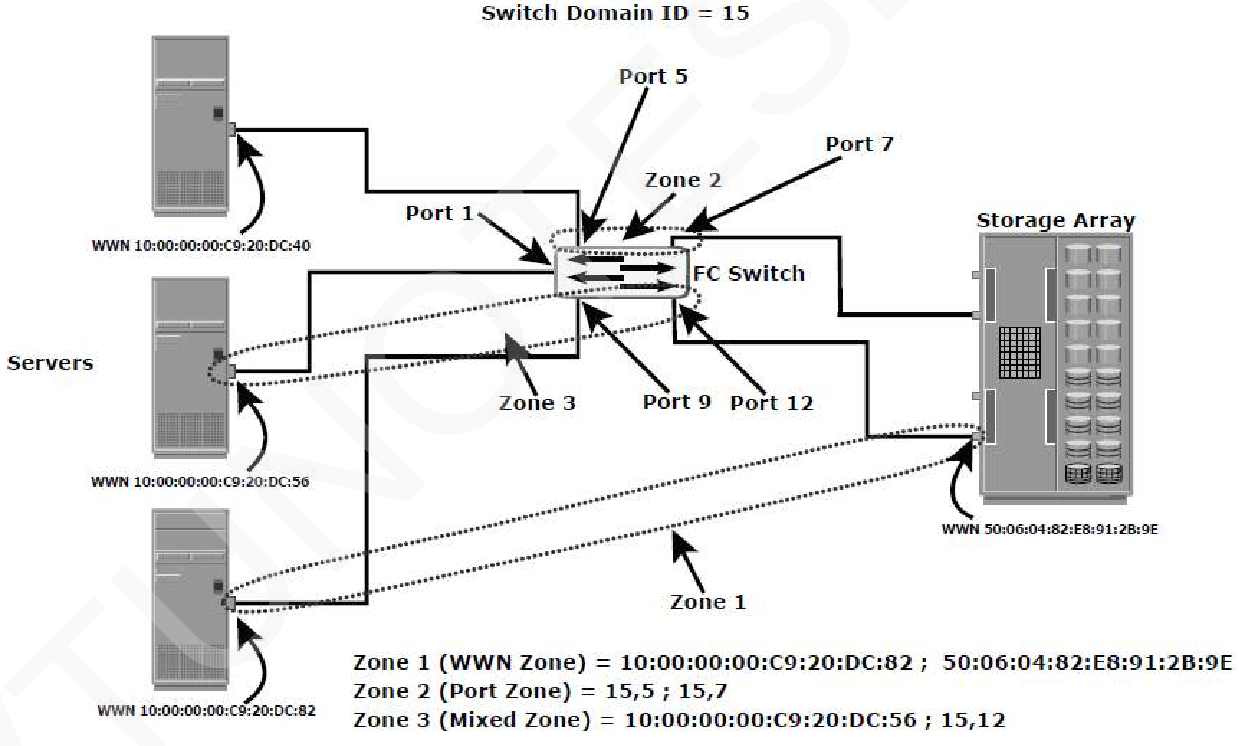

Figure 2-17: Types of zoning

2.10 Fibre-Channel Login Types

• Fabric-services define 3 login-types:

1) Fabric Login (FLOGI)

• Fabric login is performed between N_port and F_port.

• To log on to the fabric, a node sends a FLOGI frame to the login service at the FC-address FFFFFE.
The node also sends WWNN and WWPN parameters.

• Then, the switch
→ accepts the login and
→ returns an Accept (ACC) frame with the assigned FC-address for the node.

• Finally, the N_port registers itself with the local name-server on the switch.
The registered data includes WWNN, WWPN, and assigned FC-address.
(WWNN --> World Wide Node Name WWPN --> World Wide Port Name)

• After the N_Port has logged in, it can query the name server database for information about all other logged in ports.

2) Port Login (PLOGI)

• Port login is performed between two N_ports to establish a session.
i) Firstly, The initiator N_port sends a PLOGI frame to the target N_port.
ii) Then, the target N_port returns an ACC frame to the initiator N_port.
iii) Finally, the N_ports exchange service-parameters relevant to the session.

3) Process Login (PRLI)

• Process login is also performed between two N_ports.

• This login is related to the FC-4 ULPs such as SCSI.

• N_ports exchange SCSI-3-related service-parameters.

• N_ports share information about
FC-4 type in use
SCSI initiator or
SCSI target.

2.11 FC Topologies
• Fabric-design follows standard topologies to connect devices.
• Core-edge fabric is one of the popular topology designs.

2.11.1 Core-Edge Fabric
• There are two types of switch-tiers.
1) Edge-Tier
• The **edge-tier** consists of switches.
• Advantage:
Offers an inexpensive approach to adding more hosts in a fabric.
• Each switch at the edge tier is attached to a switch at the core tier through ISLs.
2) Core-Tier
• The core-tier consists of directors that ensure high fabric availability.
• In addition, typically all traffic must either traverse this tier or terminate at this tier.
• All storage devices are connected to the core tier, enabling host-to-storage traffic to traverse only one ISL.
• Hosts that require high performance may be connected directly to the core tier and consequently avoid ISL delays.
• The edge-tier switches are not connected to each other.
• Advantages:
1) This topology increases connectivity within the SAN while conserving overall port utilization.
2) If expansion is required, an additional edge-switch can be connected to the core.
3) The core of the fabric is also extended by adding more switches or directors at the core tier.

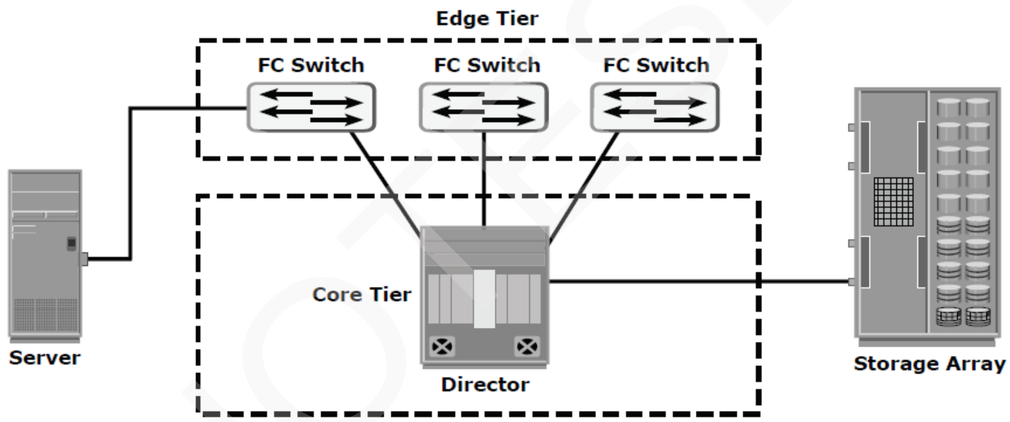

Figure 2-18: Single core topology

• This topology can have different variations.
1) In a single-core topology (Figure 2-18),
i) All hosts are connected to the edge-tier and
ii) The storage is connected to the core-tier.
2) In a dual-core topology (Figure 2-19), expansion can be done to include more core-switches.
However, to maintain the topology, it is essential that new ISLs are created to connect each edge-switch to the new core-switch that is added.

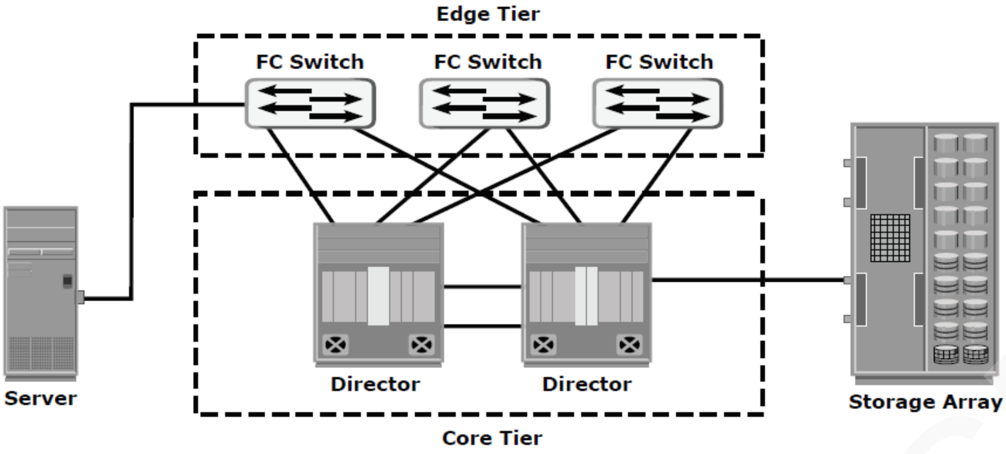

Figure 2-19: Dual-core topology

2.11.1.1 Benefits and Limitations of Core-Edge Fabric

Benefits

1) This fabric provides one-hop storage-access to all storage in the system.
• Each tier's switch is used for either storage or hosts.
Thus, i) it is easy to identify which resources are approaching their capacity.
ii) it is easy to develop a set of rules for scaling.
2) A well-defined, easily reproducible building-block approach makes rolling out new fabrics easier.
• Core-edge fabrics can be scaled to larger environments by
→ linking core-switches
→ adding more core-switches, or
→ adding more edge-switches.
3) This method can be used
→ to extend the existing simple core-edge model or
→ to expand the fabric into a compound core-edge model.

Limitations

1) The fabric may lead to some performance-related problems because
scaling a topology involves increasing the number of ISLs in the fabric.
• As no. of edge-switch increases, the domain count in the fabric increases.
2) A common best practice is to keep the number of host-to-storage hops unchanged, at one hop, in a core-edge.
• **Hop count** refers to total number of devices the data has to traverse from its source to destination.
• Generally, a large hop count means greater transmission-delay
3) As no. of core increases, it becomes difficult to maintain ISLs from each core to each edge-switch.
• When this happens, the Fabric-design can be changed to a compound core-edge design.

2.11.2 Mesh Topology

• Each switch is directly connected to other switches by using ISLs.
• Advantage:
  1) Promotes enhanced connectivity within the SAN.
• When no. of ports increases, the no. of communicating-nodes also increases.
• A mesh topology can be of two types (Figure 2-20):

1) Full Mesh Topology

- Every switch is connected to every other switch in the topology.
- Advantage:
  Appropriate when the number of switches involved is small.
- A typical deployment may involve up to four switches or directors.
- Each switch will service highly localized host-to-storage traffic.
- A maximum of one ISL or hop is required for host-to-storage traffic.

2) Partial Mesh Topology

- Several hops or ISLs may be required for the traffic to reach its destination.
- Advantage:
  Offers more scalability than full mesh topology
- Disadvantage:
  1) Traffic management might be complicated and
  2) ISLs could become overloaded due to excessive traffic aggregation.

• Hosts and storage can be located anywhere in the fabric.
• Storage can be localized to a director or a switch in both mesh topologies.

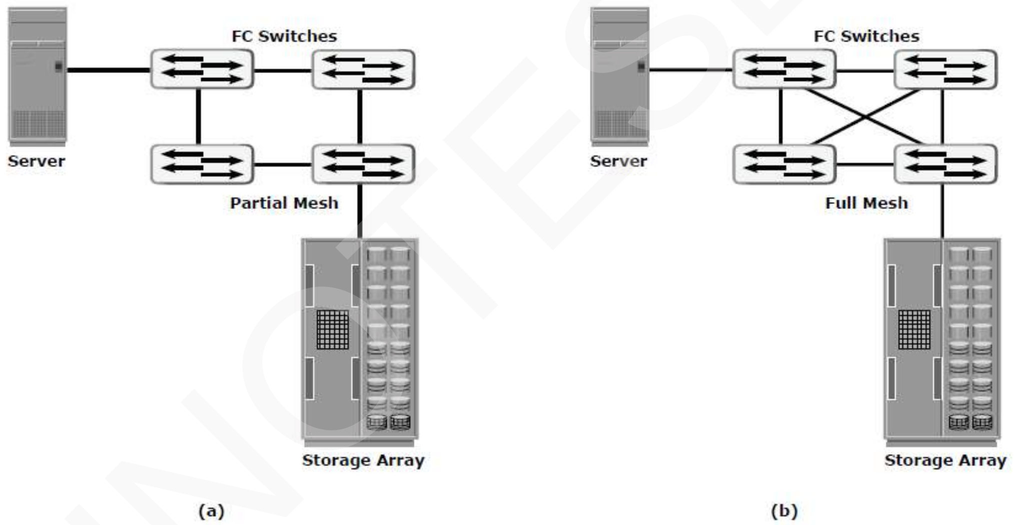

Figure 2-20: Partial mesh and full mesh topologies