A storage area network (SAN) is a specialized, high-speed network for data-block transfers between

computer systems and storage elements; thus, it is a critical element of a cloud infrastructure (see

Figure 7.13). A SAN consists of a communication infrastructure and a management layer. The Fibre

Channel (FC) is the dominant architecture of SANs.

FC is a layered protocol with several layers, as depicted in Figure 7.14:

A. The lower three layer protocols: FC-0, the physical interface; FC-1, the transmission protocol

responsible for encoding/decoding; and FC-2, the signaling protocol responsible for framing and flow

control.

FC-0 uses laser diodes as the optical source and manages the point-to-point fiber connections.When

the fiber connection is broken, the ports send a series of pulses until the physical connection is reestablished

and the necessary handshake procedures are followed.

FC-1 controls the serial transmission and integrates data with clock information. It ensures encoding

to the maximum length of the code, maintains DC balance, and provides word alignment.

FC-2 provides the transport methods for data transmitted in 4-byte ordered sets containing data

and control characters. It handles the topologies based on the presence or absence of a fabric, the

communication models, the classes of service provided by the fabric and the nodes, sequence and

exchange identifiers, and segmentation and reassembly.

B. Two upper layer protocols: FC-3, the common services layer; and FC-4, the protocol mapping

layer. FC-3 supports multiple ports on a single node or fabric using:

• Hunt groups-sets of associated ports assigned an alias identifier that allows any frames containing

that alias to be routed to any available port within the set.

• Striping to multiply bandwidth, using multiple ports in parallel to transmit a single information unit

across multiple links.

• Multicast and broadcast to deliver a single transmission to multiple destination ports or to all nodes.

To accommodate various application needs, FC supports several classes of service:

Class 1. Rarely used blocking connection-oriented service. Acknowledgments ensure that the frames

are received in the same order in which they are sent and reserve full bandwidth for the connection

between the two devices.

Class 2. Acknowledgments ensure that the frames are received. Allows the fabric to multiplex several

messages on a frame-by-frame basis. Because frames can take different routes, it does not guarantee

in-order delivery; it relies on upper layer protocols to take care of frame sequence.

Class 3. Datagram connection; no acknowledgments.

Class 4. Supports connection-oriented service. Virtual circuits (VCs) established between ports

guarantee in-order delivery and acknowledgment of delivered frames, but the fabric is responsible for

multiplexing frames of different VCs. Guaranteed QoS, including bandwidth and latency; intended for

multimedia applications.

Class 5. Supports isochronous service for applications requiring immediate delivery without

buffering.

Class 6. Supports dedicated connections for a reliable multicast.

Class 7. Similar to Class 2 but used for the control and management of the fabric. A connectionless

service with notification of nondelivery.

Although each device connected to a LAN has a unique physical address, also called a Media Access

Control (MAC) address, each FC device has a unique ID called theWorldWide Name (WWN), a 64-bit

address. Each port in the switched fabric has its own unique 24-bit address consisting of the domain

(bits 23–16), the area (bits 15–08), and the port physical address (bits 07–00).

The switch of a switched fabric environment assigns dynamically and maintains the port addresses.

When a device with a WWN logs into the switch on a port, the switch assigns the port address to that

port and maintains the correlation between that port address and the WWN address of the device using

the Name Server, a component of the fabric operating system, which runs inside the switch.

The format of an FCframe is shown inFigure 7.15. Zoning permits finer segmentation of the switched

fabric. Only the members of the same zone can communicate within that zone. It can be used to separate

different environments (e.g., a Microsoft Windows NT from a UNIX environment).

Several other protocols are used for SANs. Fibre Channel over IP (FCIP) allows transmission of Fibre

Channel information through the IP network using tunneling. Tunneling is a technique for network protocols

to encapsulate a different payload protocol. It allows a network protocol to carry a payload over

an incompatible delivery network or to provide a secure path through an untrusted network. Tunneling

allows a protocol that a firewall would normally block to cross it wrapped inside a protocol that the

firewall does not block. For example, an HTTP tunnel can be used for communication from network

locations with restricted connectivity (e.g., behind NATs, firewalls, or proxy servers) and most often

with applications that lack native support for communication in such conditions of restricted connectivity.

Restricted connectivity is a commonly used method to lock down a network to secure it against

internal and external threats.

Internet Fibre Channel Protocol (iFCP) is a gateway-to-gateway protocol that supports communication

among FC storage devices in a SAN or on the Internet using TCP/IP. iFCP replaces the lower-layer Fibre Channel transport with TCP/IP and Gigabit Ethernet. With iFCP, Fibre Channel devices connect

to an iFCP gateway or switch, and each Fibre Channel session is terminated at the local gateway and

converted to a TCP/IP session via iFCP.