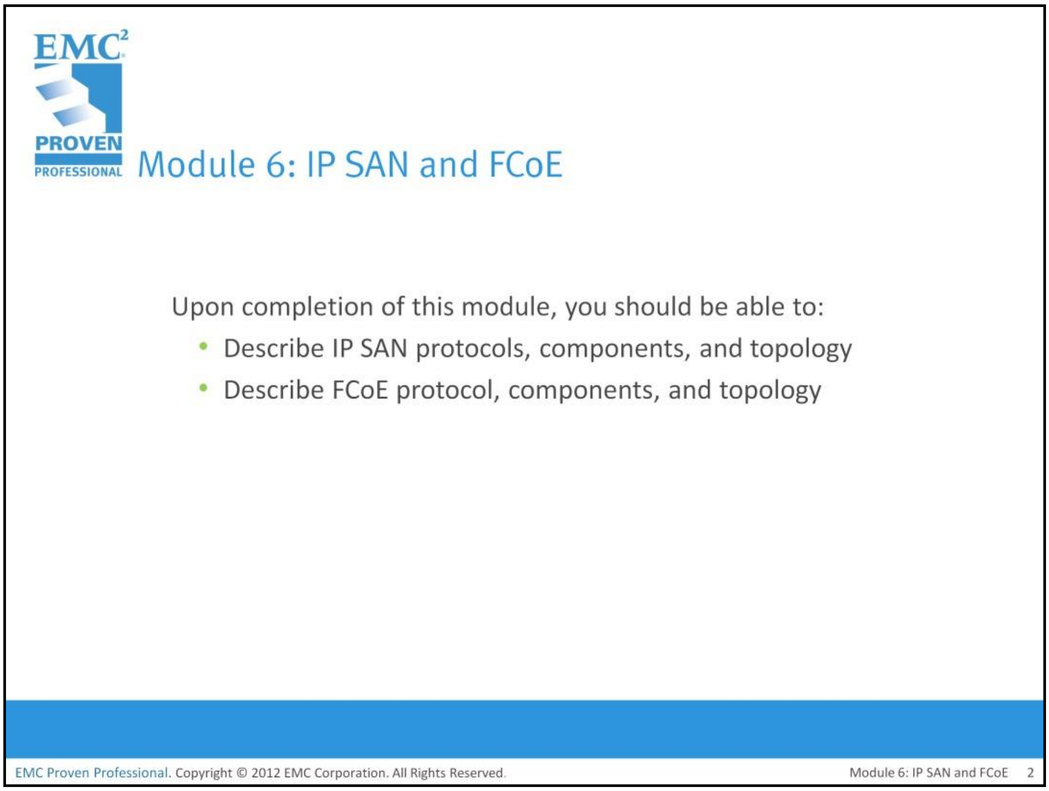
Module – 6
IP SAN and FCoE

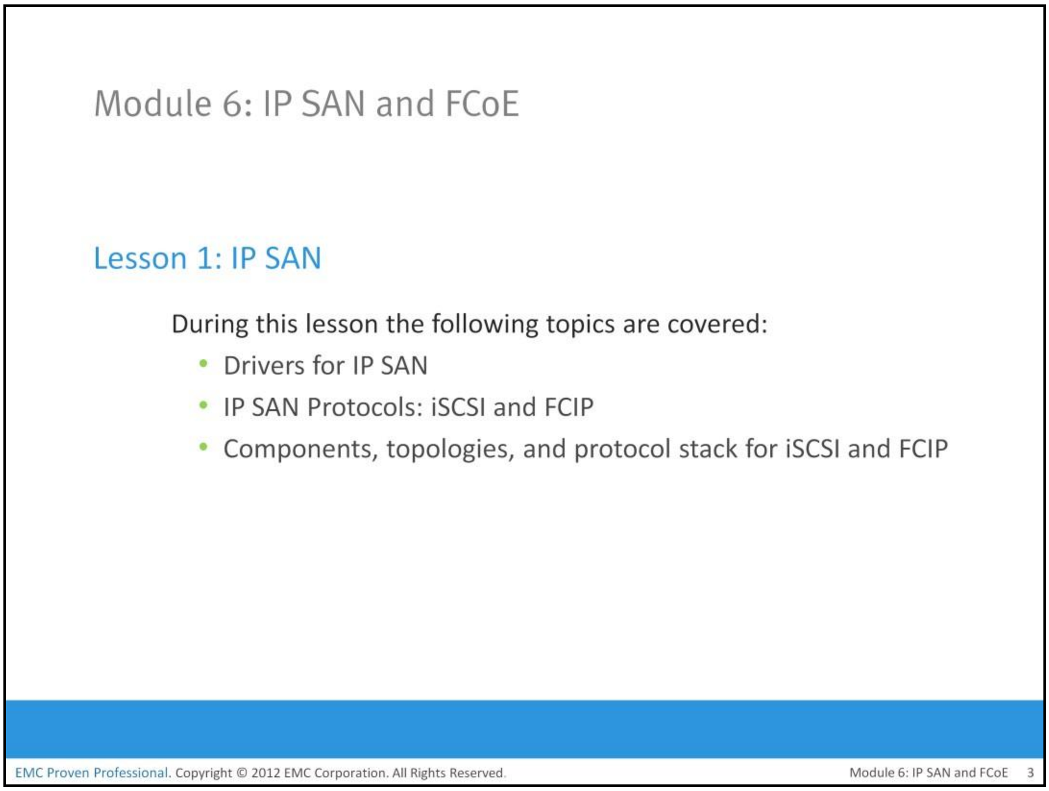


Module 6: IP SAN and FCoE

Upon completion of this module, you should be able to:

- Describe IP SAN protocols, components, and topology
- Describe FCoE protocol, components, and topology

This module focuses on IP SAN protocols such as Internet SCSI (iSCSI) and Fibre Channel over IP (FCIP), infrastructure components, and topology. It also focuses on Fibre Channel over Ethernet (FCoE) protocol, infrastructure components, and topology.



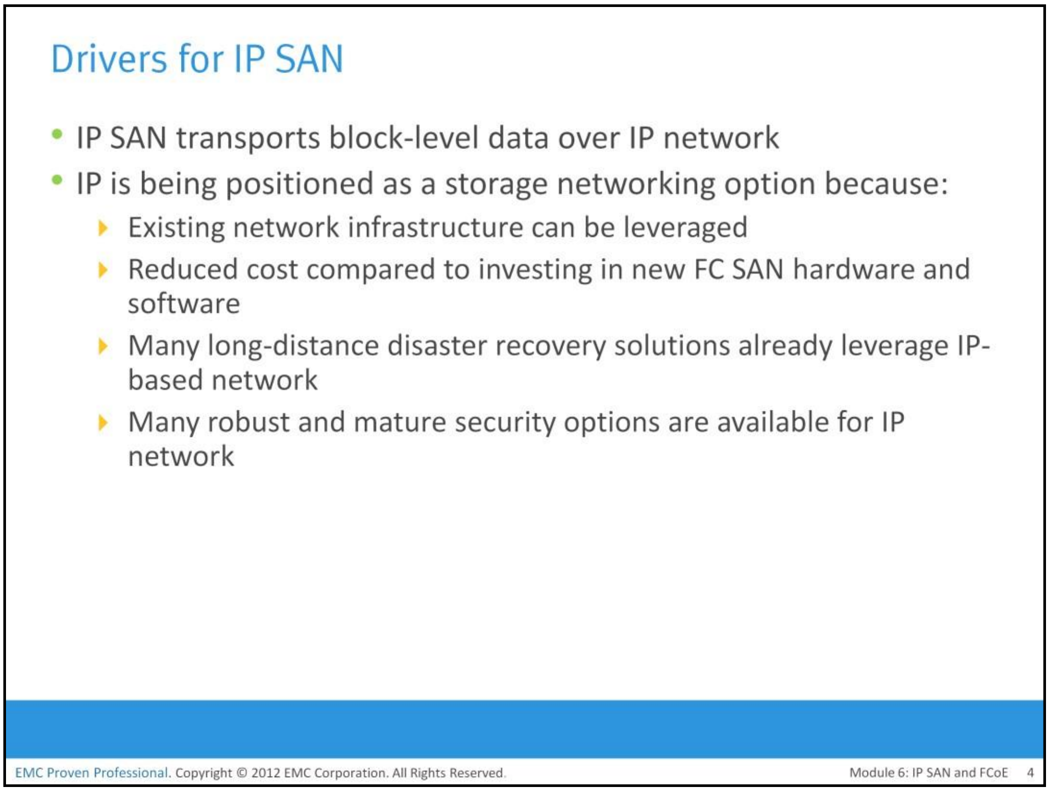
Module 6: IP SAN and FCoE

Lesson 1: IP SAN

During this lesson the following topics are covered:

- Drivers for IP SAN
- IP SAN Protocols: iSCSI and FCIP
- Components, topologies, and protocol stack for iSCSI and FCIP

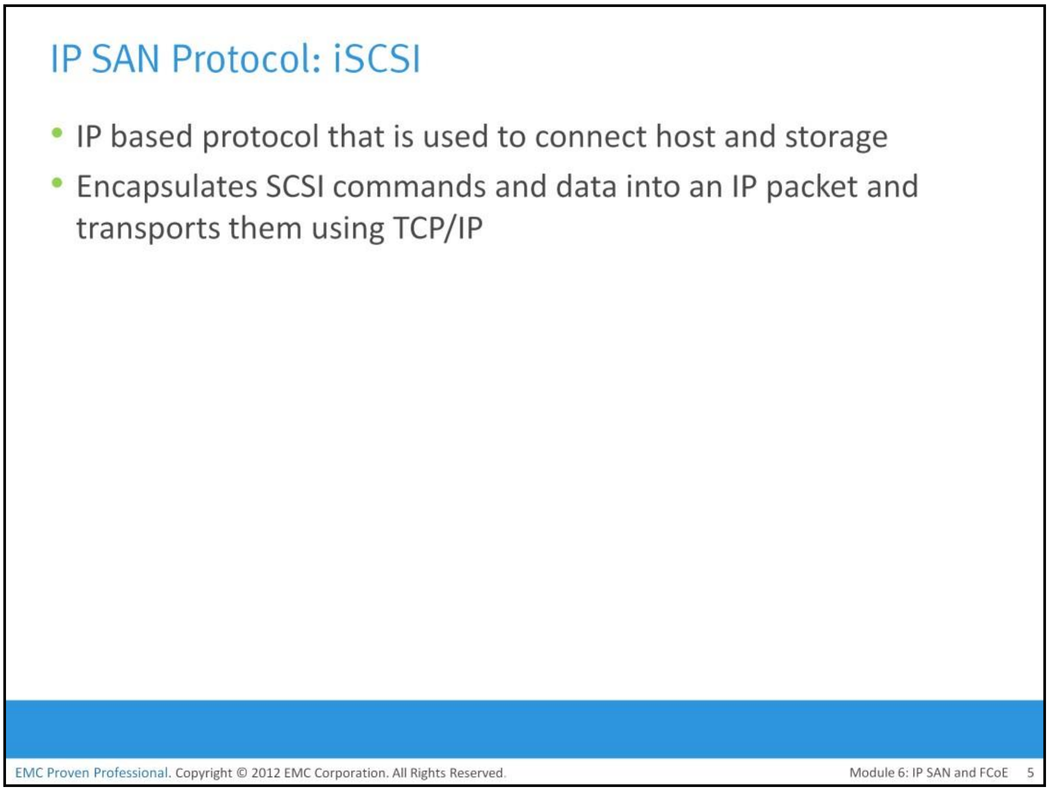
Two primary protocols that leverage IP as the transport mechanism are Internet SCSI (iSCSI) and Fibre Channel over IP (FCIP). This lesson covers the drivers for IP SAN and iSCSI components, topologies, protocol stack, and discovery methods. It also covers FCIP protocol stack and topology.



Drivers for IP SAN

- IP SAN transports block-level data over IP network
- IP is being positioned as a storage networking option because:
  - Existing network infrastructure can be leveraged
  - Reduced cost compared to investing in new FC SAN hardware and software
  - Many long-distance disaster recovery solutions already leverage IP-based network
  - Many robust and mature security options are available for IP network

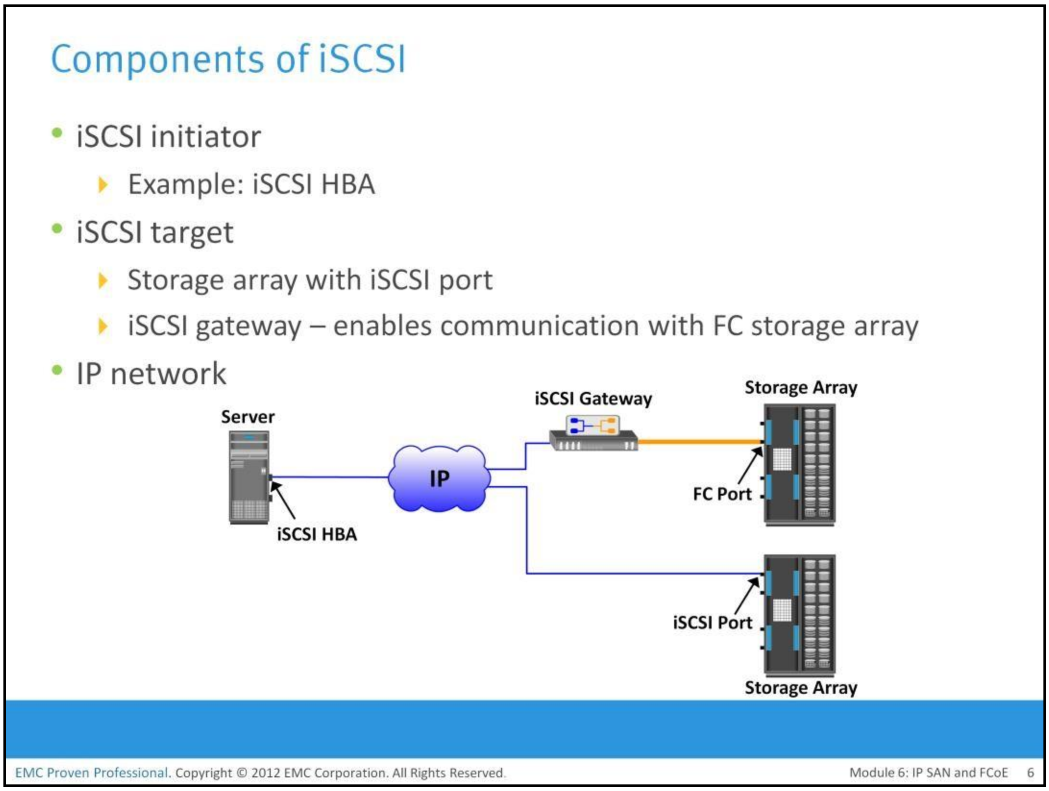
Traditional SAN enables the transfer of block I/O over Fibre Channel and provides high performance and scalability. These advantages of FC SAN come with the additional cost of buying FC components, such as FC HBA and switches. Organizations typically have an existing Internet Protocol (IP)-based infrastructure, which could be leveraged for storage networking. Advancements in technology have enabled IP to be used for transporting block I/O over the IP network. This technology of transporting block I/Os over an IP is referred to as IP SAN. IP is a mature technology, and using IP as a storage networking option provides several advantages. When block I/O is run over IP, the existing network infrastructure can be leveraged, which is more economical than investing in a new SAN infrastructure. In addition, many robust and mature security options are now available for IP networks. Many long-distance, disaster recovery (DR) solutions are already leveraging IP-based networks. With IP SAN, organizations can extend the geographical reach of their storage infrastructure.



IP SAN Protocol: iSCSI

- IP based protocol that is used to connect host and storage
- Encapsulates SCSI commands and data into an IP packet and transports them using TCP/IP

iSCSI is encapsulation of SCSI I/O over IP. iSCSI is an IP based protocol that establishes and manages connections between host and storage over IP. iSCSI encapsulates SCSI commands and data into an IP packet and transports them using TCP/IP. iSCSI is widely adopted for connecting servers to storage because it is relatively inexpensive and easy to implement, especially environments in which an FC SAN does not exist.

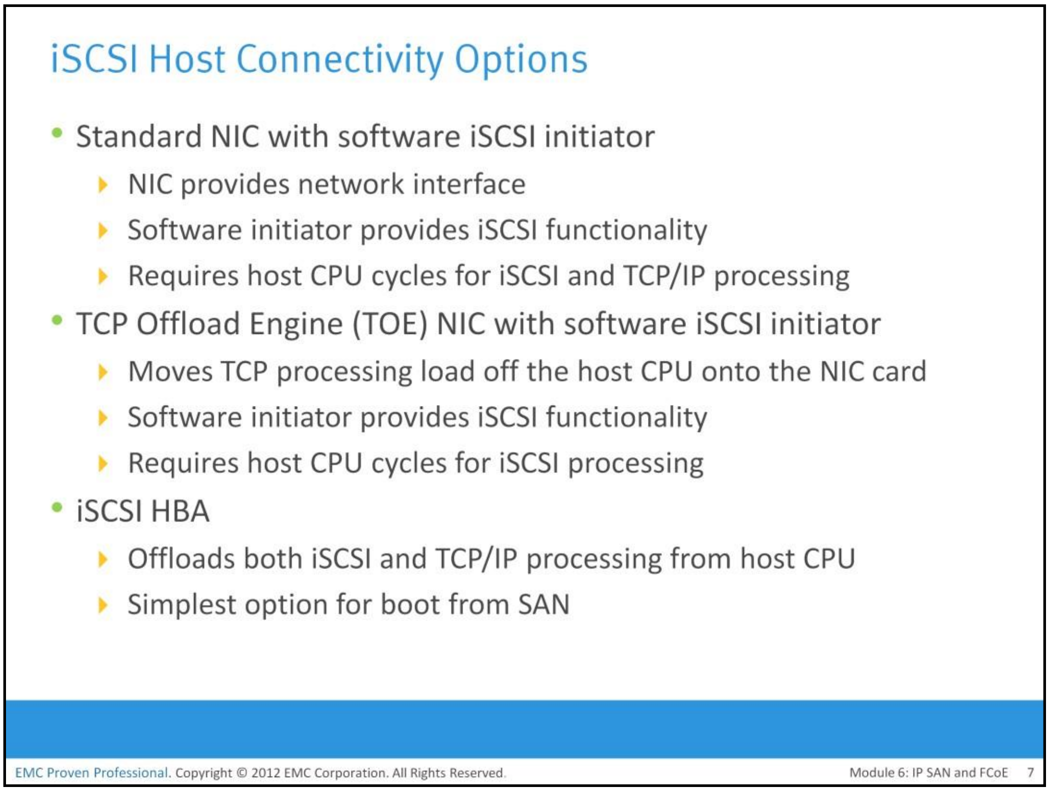


Components of iSCSI

- iSCSI initiator
  - Example: iSCSI HBA
- iSCSI target
  - Storage array with iSCSI port
  - iSCSI gateway – enables communication with FC storage array
- IP network

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 6

An initiator (host), target (storage or iSCSI gateway), and an IP-based network are the key iSCSI components. If an iSCSI-capable storage array is deployed, then a host with the iSCSI initiator can directly communicate with the storage array over an IP network. However, in an implementation that uses an existing FC array for iSCSI communication, an iSCSI gateway is used. These devices perform the translation of IP packets to FC frames and vice versa, thereby bridging the connectivity between the IP and FC environments.



iSCSI Host Connectivity Options

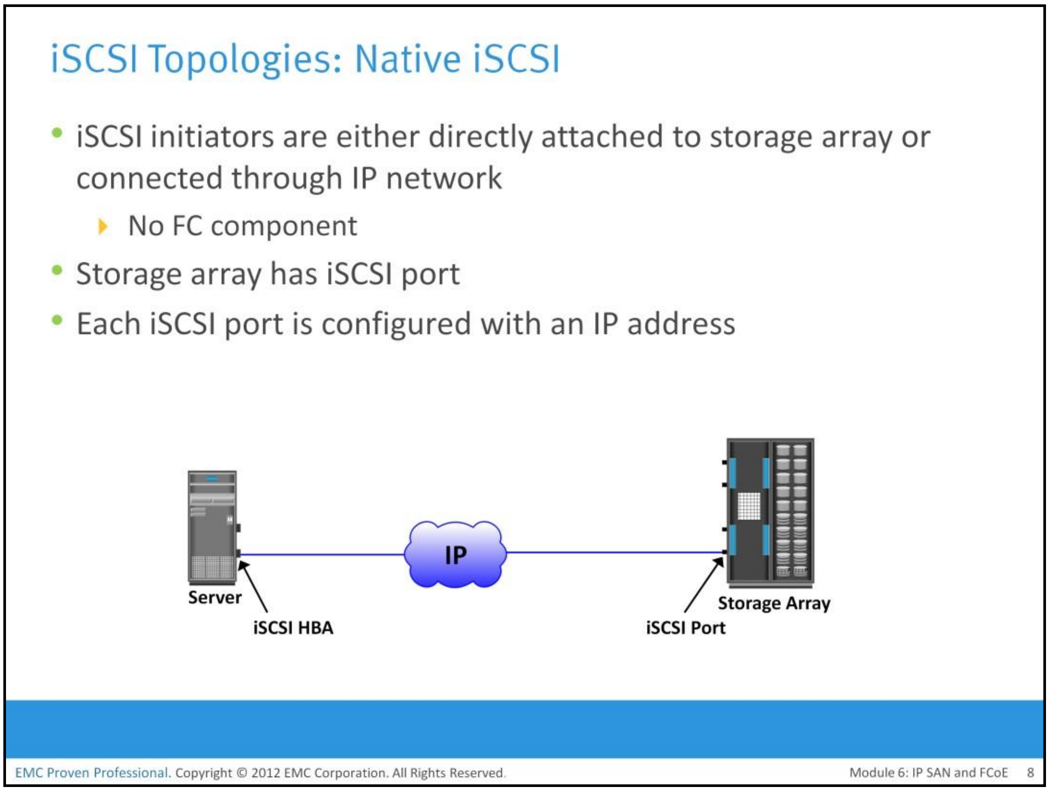
- Standard NIC with software iSCSI initiator
  - NIC provides network interface
  - Software initiator provides iSCSI functionality
  - Requires host CPU cycles for iSCSI and TCP/IP processing
- TCP Offload Engine (TOE) NIC with software iSCSI initiator
  - Moves TCP processing load off the host CPU onto the NIC card
  - Software initiator provides iSCSI functionality
  - Requires host CPU cycles for iSCSI processing
- iSCSI HBA
  - Offloads both iSCSI and TCP/IP processing from host CPU
  - Simplest option for boot from SAN

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 7

A standard NIC with software iSCSI initiator, a TCP offload engine (TOE) NIC with software iSCSI initiator, and an iSCSI HBA are the three iSCSI host connectivity options. The function of the iSCSI initiator is to route the SCSI commands over an IP network.

A standard NIC with a software iSCSI initiator is the simplest and least expensive connectivity option. It is easy to implement because most servers come with at least one, and in many cases two, embedded NICs. It requires only a software initiator for iSCSI functionality. Because NICs provide standard IP function, encapsulation of SCSI into IP packets and decapsulation are carried out by the host CPU. This places additional overhead on the host CPU. If a standard NIC is used in heavy I/O load situations, the host CPU might become a bottleneck. TOE NIC helps alleviate this burden. A TOE NIC offloads TCP management functions from the host and leaves only the iSCSI functionality to the host processor. The host passes the iSCSI information to the TOE card, and the TOE card sends the information to the destination using TCP/IP. Although this solution improves performance, the iSCSI functionality is still handled by a software initiator that requires host CPU cycles.

An iSCSI HBA is capable of providing performance benefits because it offloads the entire iSCSI and TCP/IP processing from the host processor. The use of an iSCSI HBA is also the simplest way to boot hosts from a SAN environment via iSCSI. If there is no iSCSI HBA, modifications must be made to the basic operating system to boot a host from the storage devices because the NIC needs to obtain an IP address before the operating system loads. The functionality of an iSCSI HBA is similar to the functionality of an FC HBA.



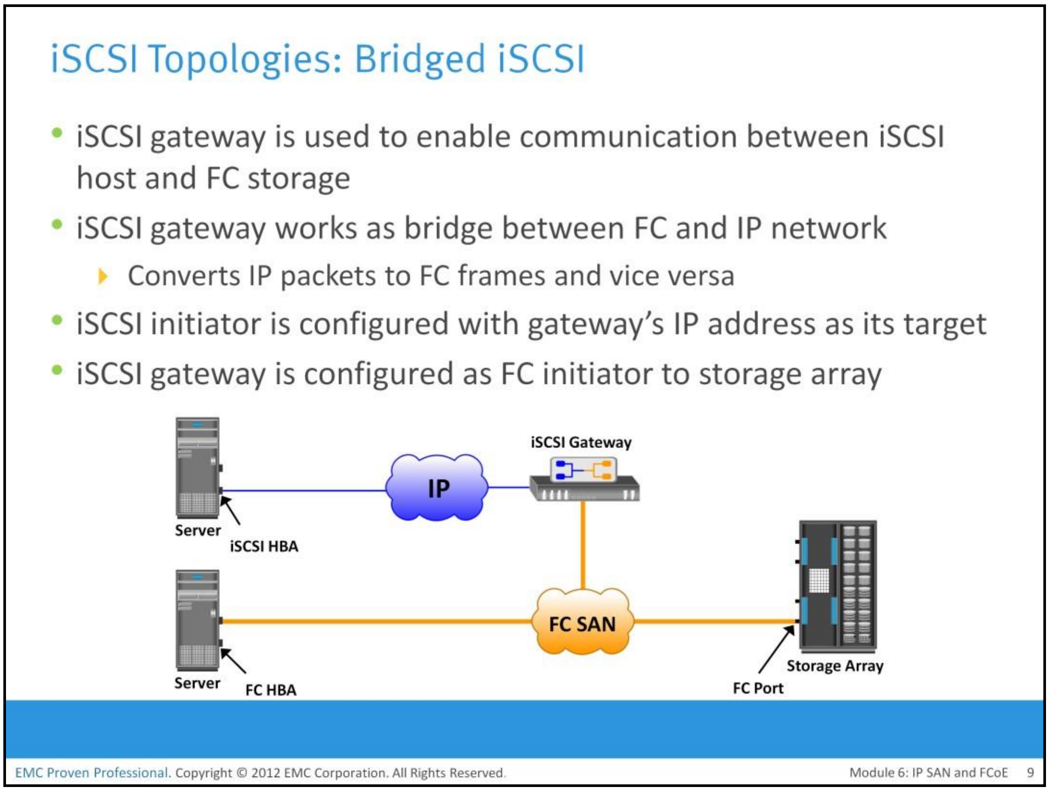
iSCSI Topologies: Native iSCSI

- iSCSI initiators are either directly attached to storage array or connected through IP network
  - No FC component
- Storage array has iSCSI port
- Each iSCSI port is configured with an IP address

Module 6: IP SAN and FCoE 8

Two topologies of iSCSI implementations are native and bridged. Native topology does not have FC components. The initiators may be either directly attached to targets or connected through the IP network.

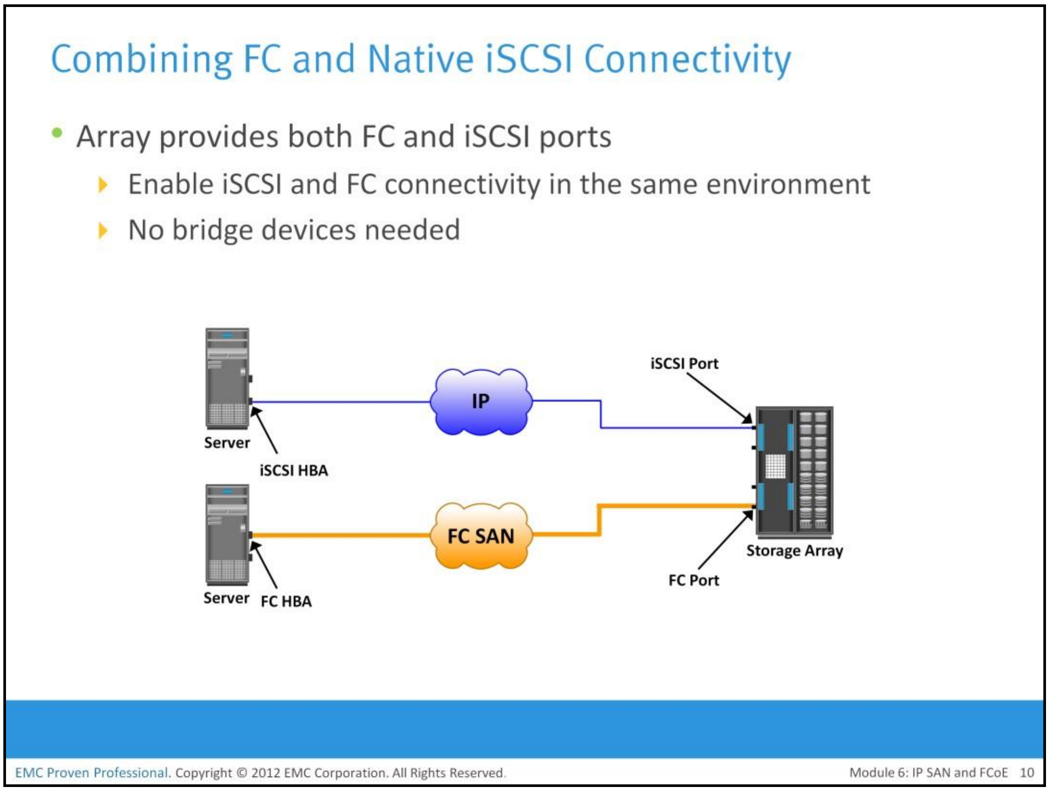
FC components are not required for iSCSI connectivity if an iSCSI-enabled array is deployed. In figure in the slide, the array has one or more iSCSI ports configured with an IP address and connected to a standard Ethernet switch. After an initiator is logged on to the network, it can access the available LUNs on the storage array. A single array port can service multiple hosts or initiators as long as the array port can handle the amount of storage traffic that the hosts generate.



iSCSI Topologies: Bridged iSCSI

- iSCSI gateway is used to enable communication between iSCSI host and FC storage
- iSCSI gateway works as bridge between FC and IP network
  - Converts IP packets to FC frames and vice versa
- iSCSI initiator is configured with gateway's IP address as its target
- iSCSI gateway is configured as FC initiator to storage array

Bridged topology enables the coexistence of FC with IP by providing iSCSI-to-FC bridging functionality. Figure in the slide illustrates an iSCSI host connectivity to an FC storage array. In this case, the array does not have any iSCSI ports. Therefore, an external device, called a gateway or a multiprotocol router, must be used to facilitate the communication between the iSCSI host and FC storage. The gateway converts IP packets to FC frames and vice versa. The bridge devices contain both FC and Ethernet ports to facilitate the communication between the FC and IP environments. In bridged iSCSI implementation, the iSCSI initiator is configured with the gateway's IP address as its target destination. On the other side, the gateway is configured as an FC initiator to the storage array.

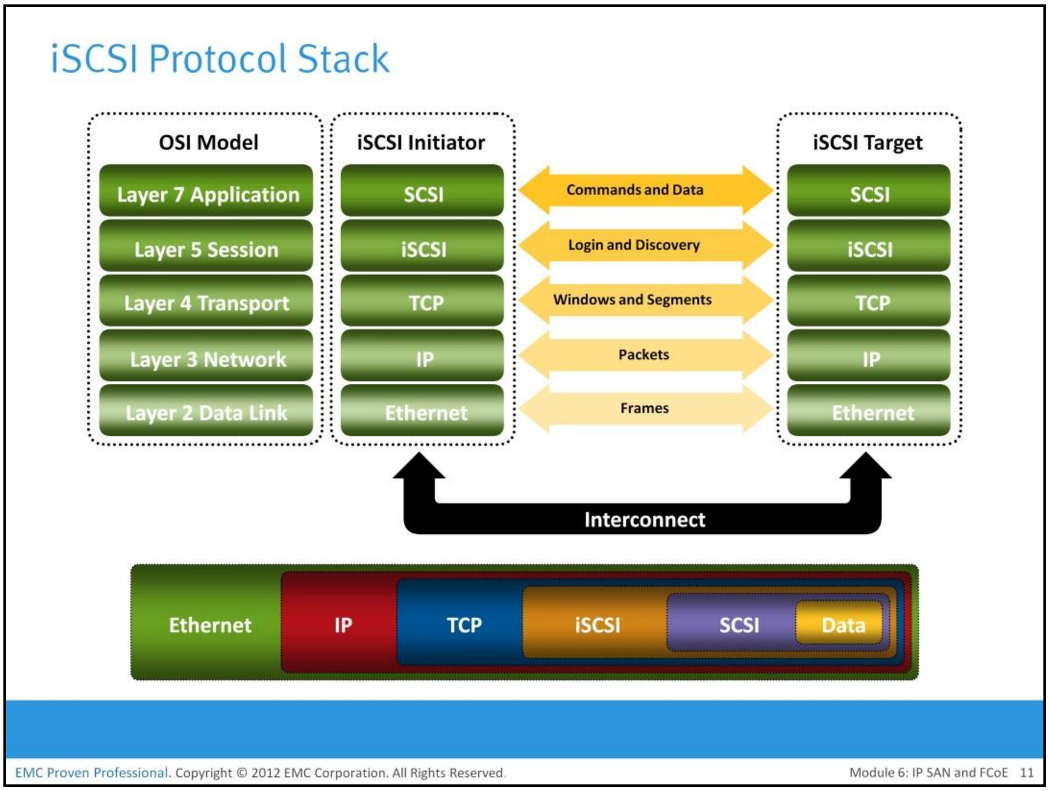


Combining FC and Native iSCSI Connectivity

- Array provides both FC and iSCSI ports
  - Enable iSCSI and FC connectivity in the same environment
  - No bridge devices needed

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 10

The most common topology is a combination of FC and native iSCSI. Typically, a storage array comes with both FC and iSCSI ports that enable iSCSI and FC connectivity in the same environment, as shown in the slide.



iSCSI Protocol Stack

OSI Model	iSCSI Initiator		iSCSI Target
Layer 7 Application	SCSI	Commands and Data	SCSI
Layer 5 Session	iSCSI	Login and Discovery	iSCSI
Layer 4 Transport	TCP	Windows and Segments	TCP
Layer 3 Network	IP	Packets	IP
Layer 2 Data Link	Ethernet	Frames	Ethernet

Interconnect

Ethernet IP TCP iSCSI SCSI Data

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved.

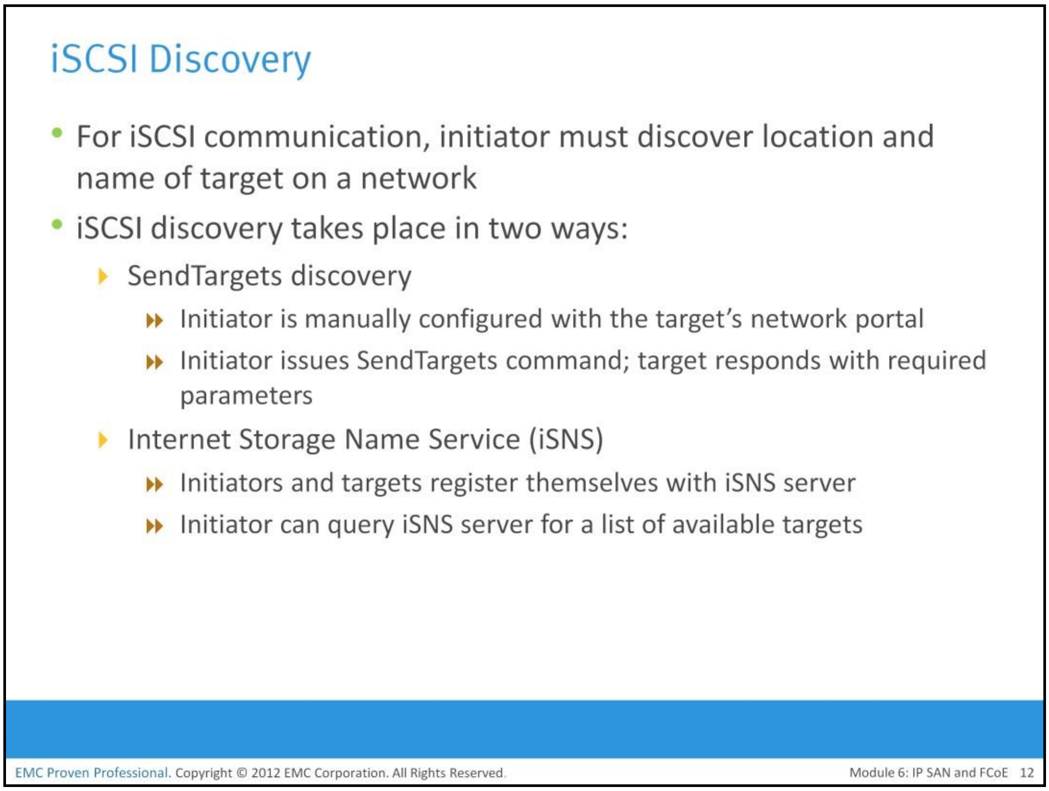
Module 6: IP SAN and FCoE 11

Figure in the slide displays a model of the iSCSI protocol layers and depicts the encapsulation order of the SCSI commands for their delivery through a physical carrier.

SCSI is the command protocol that works at the application layer of the Open System Interconnection (OSI) model. The initiators and targets use SCSI commands and responses to talk to each other. The SCSI command descriptor blocks, data, and status messages are encapsulated into TCP/IP and transmitted across the network between the initiators and targets.

iSCSI is the session-layer protocol that initiates a reliable session between devices that recognize SCSI commands and TCP/IP. The iSCSI session-layer interface is responsible for handling login, authentication, target discovery, and session management. TCP is used with iSCSI at the transport layer to provide reliable transmission.

TCP controls message flow, windowing, error recovery, and retransmission. It relies upon the network layer of the OSI model to provide global addressing and connectivity. The Layer 2 protocols at the data link layer of this model enable node-to-node communication through a physical network.



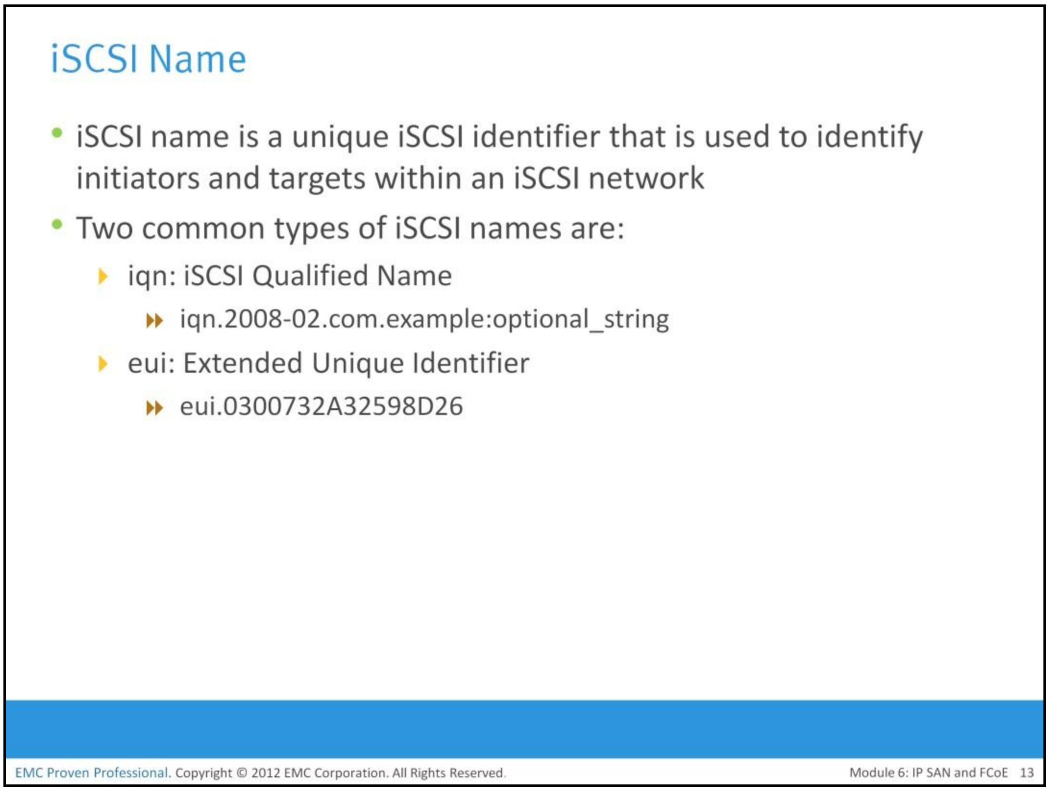
iSCSI Discovery

- For iSCSI communication, initiator must discover location and name of target on a network
- iSCSI discovery takes place in two ways:
  - SendTargets discovery
    - Initiator is manually configured with the target’s network portal
    - Initiator issues SendTargets command; target responds with required parameters
  - Internet Storage Name Service (iSNS)
    - Initiators and targets register themselves with iSNS server
    - Initiator can query iSNS server for a list of available targets

An initiator must discover the location of its targets on the network and the names of the targets available to it before it can establish a session. This discovery can take place in two ways: SendTargets discovery or internet Storage Name Service (iSNS).

In SendTargets discovery, the initiator is manually configured with the target’s network portal to establish a discovery session. The initiator issues the SendTargets command, and the target network portal responds with the required parameters of the targets available to the host.

iSNS enables automatic discovery of iSCSI devices on an IP network. The initiators and targets can be configured to automatically register themselves with the iSNS server. Whenever an initiator wants to know the targets that it can access, it can query the iSNS server for a list of available targets.



iSCSI Name

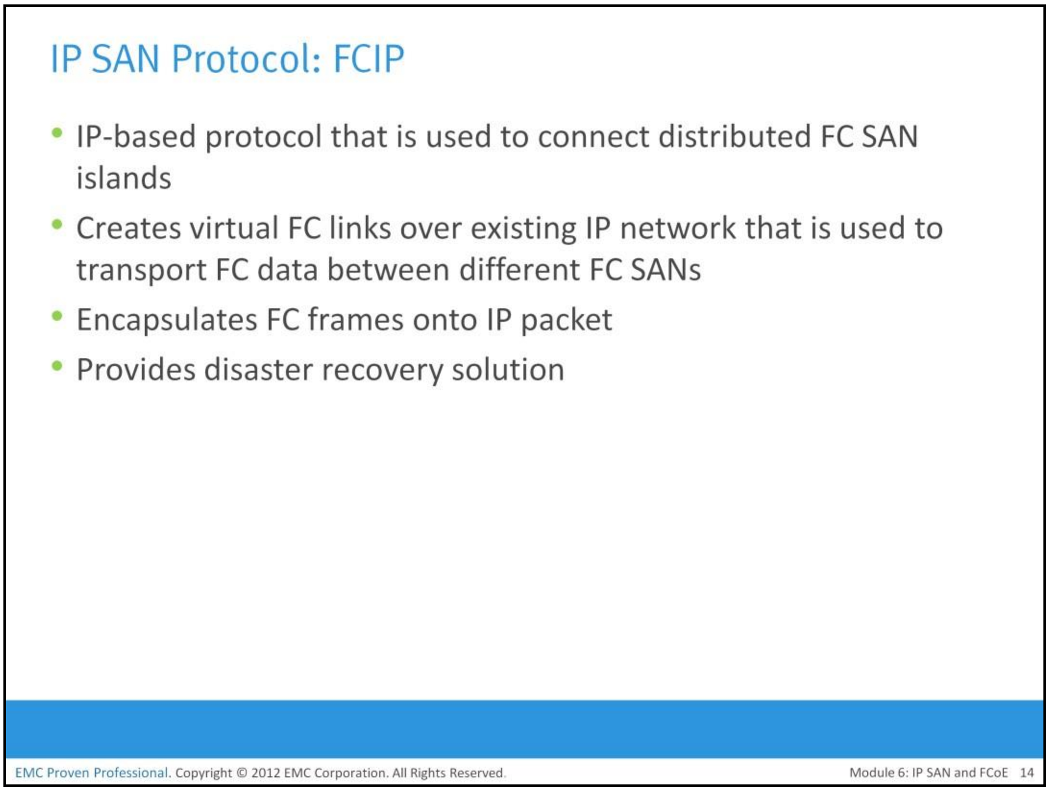
- iSCSI name is a unique iSCSI identifier that is used to identify initiators and targets within an iSCSI network
- Two common types of iSCSI names are:
  - iqn: iSCSI Qualified Name
    - iqn.2008-02.com.example:optional_string
  - eui: Extended Unique Identifier
    - eui.0300732A32598D26

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 13

A unique worldwide iSCSI identifier, known as an iSCSI name, is used to identify the initiators and targets within an iSCSI network to facilitate communication. The unique identifier can be a combination of the names of the department, application, or manufacturer, serial number, asset number, or any tag that can be used to recognize and manage the devices. Following are two types of iSCSI names commonly used:

- **iSCSI Qualified Name (IQN):** An organization must own a registered domain name to generate iSCSI Qualified Names. This domain name does not need to be active or resolve to an address. It just needs to be reserved to prevent other organizations from using the same domain name to generate iSCSI names. A date is included in the name to avoid potential conflicts caused by the transfer of domain names. An example of an IQN is iqn.2008-02.com.example:*optional_string.* The *optional_string* provides a serial number, an asset number, or any other device identifiers. An iSCSI Qualified Name enables storage administrators to assign meaningful names to iSCSI devices, and therefore, manage those devices more easily.
- **Extended Unique Identifier (EUI):** An EUI is a globally unique identifier based on the IEEE EUI-64 naming standard. An EUI is composed of the eui prefix followed by a 16-character hexadecimal name, such as eui.0300732A32598D26.

In either format, the allowed special characters are dots, dashes, and blank spaces.



IP SAN Protocol: FCIP

- IP-based protocol that is used to connect distributed FC SAN islands
- Creates virtual FC links over existing IP network that is used to transport FC data between different FC SANs
- Encapsulates FC frames onto IP packet
- Provides disaster recovery solution

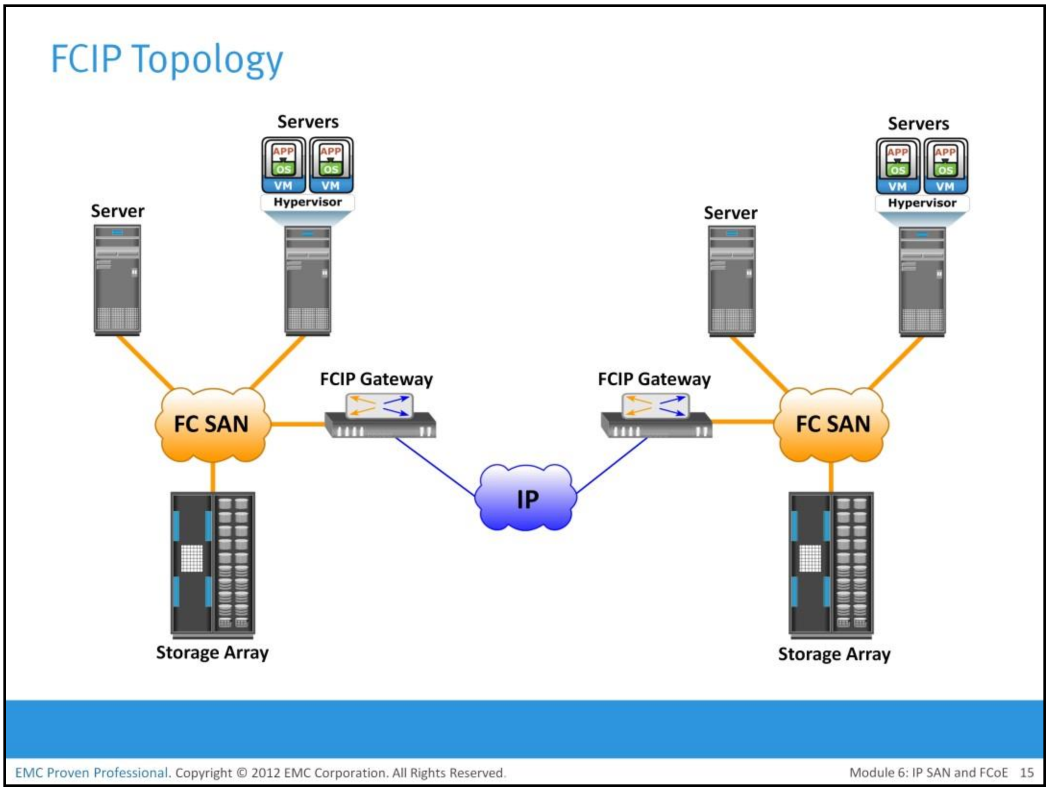
EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved.

Module 6: IP SAN and FCoE 14

FC SAN provides a high-performance infrastructure for localized data movement. Organizations are now looking for ways to transport data over a long distance between their disparate SANs at multiple geographic locations. One of the best ways to achieve this goal is to interconnect geographically dispersed SANs through reliable, high-speed links. This approach involves transporting the FC block data over the IP infrastructure. FCIP is a tunneling protocol that enables distributed FC SAN islands to be interconnected over the existing IP-based networks.

FCIP is a protocol in which FCIP entity such as FCIP gateway is used to tunnel FC fabrics through an IP network. In FCIP FC frames are encapsulated onto the IP payload. An FCIP implementation is capable to merge interconnected fabrics into a single fabric. Frequently, only a small subset of nodes at either end requires connectivity across fabrics. Thus, the majority of FCIP implementations today use switch-specific features such as IVR (Inter-VSAN Routing) or FCRS (Fibre Channel Routing Services) to create a tunnel. In this manner, traffic may be routed between specific nodes without actually merging the fabrics.

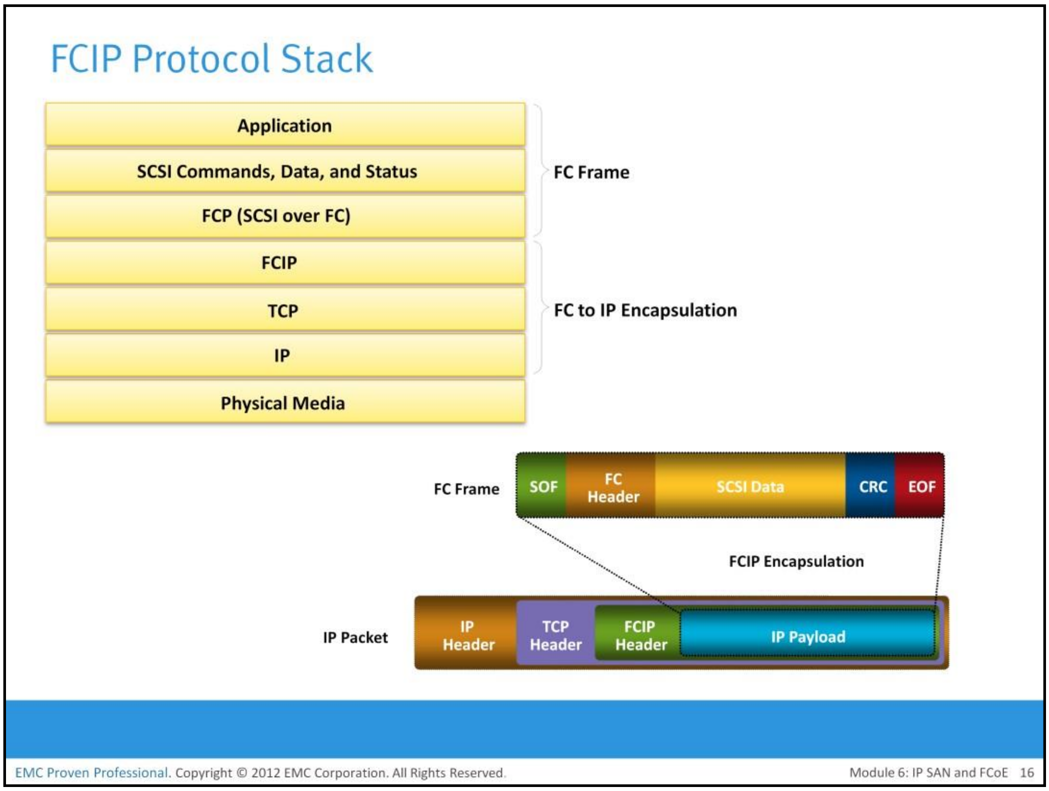
The FCIP standard has rapidly gained acceptance as a manageable, cost-effective way to blend the best of the two worlds: FC SAN and the proven, widely deployed IP infrastructure. As a result, organizations now have a better way to store, protect, and move their data by leveraging investments in their existing IP infrastructure. FCIP is extensively used in disaster recovery implementations in which data is duplicated to the storage located at a remote site.



FCIP Topology

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 15

In an FCIP environment, an FCIP gateway is connected to each fabric via a standard FC connection. The FCIP gateway at one end of the IP network encapsulates the FC frames into IP packets. The gateway at the other end removes the IP wrapper and sends the FC data to the layer 2 fabric. The fabric treats these gateways as layer 2 fabric switches. An IP address is assigned to the port on the gateway, which is connected to an IP network. After the IP connectivity is established, the nodes in the two independent fabrics can communicate with other.



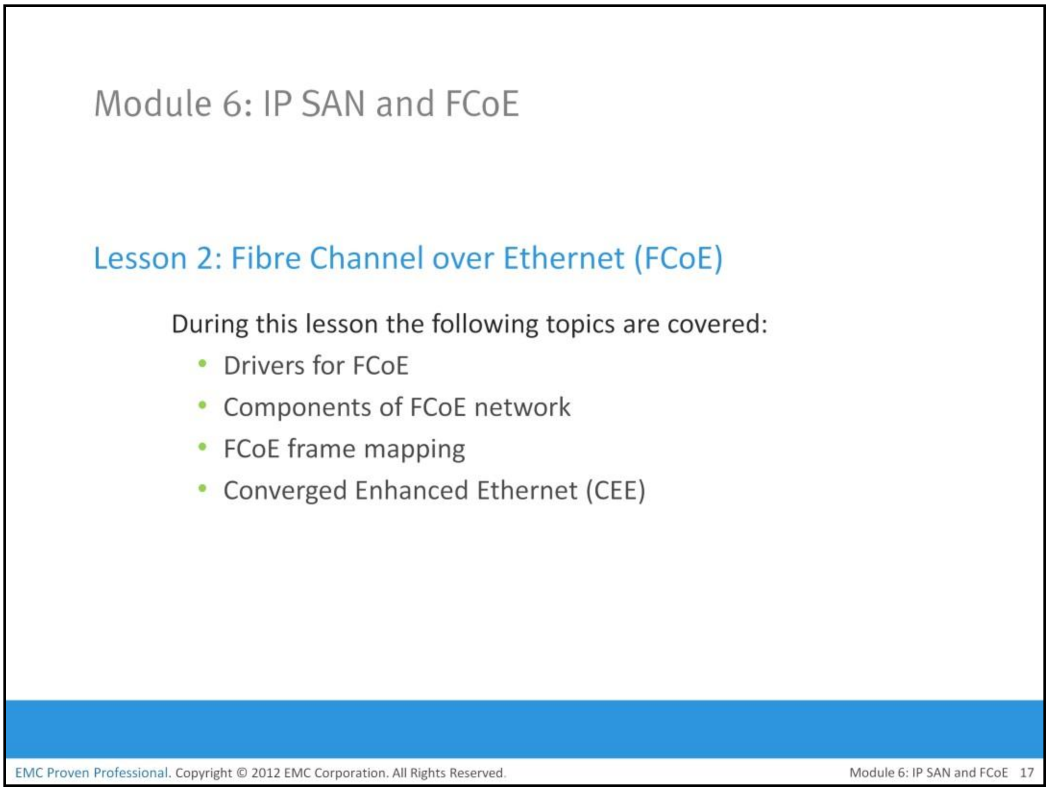
FCIP Protocol Stack

Application
SCSI Commands, Data, and Status
FCP (SCSI over FC)
FCIP
TCP
IP
Physical Media

Module 6: IP SAN and FCoE 16

The FCIP protocol stack is shown in the slide. Applications generate SCSI commands and data, which are processed by various layers of the protocol stack. The upper layer protocol SCSI includes the SCSI driver program that executes the read-and-write commands. Below the SCSI layer is the Fibre Channel Protocol (FCP) layer, which is simply a fibre channel frame whose payload is SCSI. The FCP layer rides on top of the Fibre Channel transport layer. This enables the FC frames to run natively within a SAN fabric environment. In addition, the FC frames can be encapsulated into the IP packet and sent to a remote SAN over the IP. The FCIP layer encapsulates the Fibre Channel frames onto the IP payload and passes them to the TCP layer. TCP and IP are used for transporting the encapsulated information across Ethernet, wireless, or other media that support the TCP/IPtraffic.

Encapsulation of FC frame on to IP packet could cause the IP packet to be fragmented when the data link cannot support the maximum transmission unit (MTU) size of an IP packet. When an IP packet is fragmented, the required parts of the header must be copied by all fragments. When a TCP packet is segmented, normal TCP operations are responsible for receiving and re-sequencing the data prior to passing it on to the FC processing portion of the device.



Module 6: IP SAN and FCoE

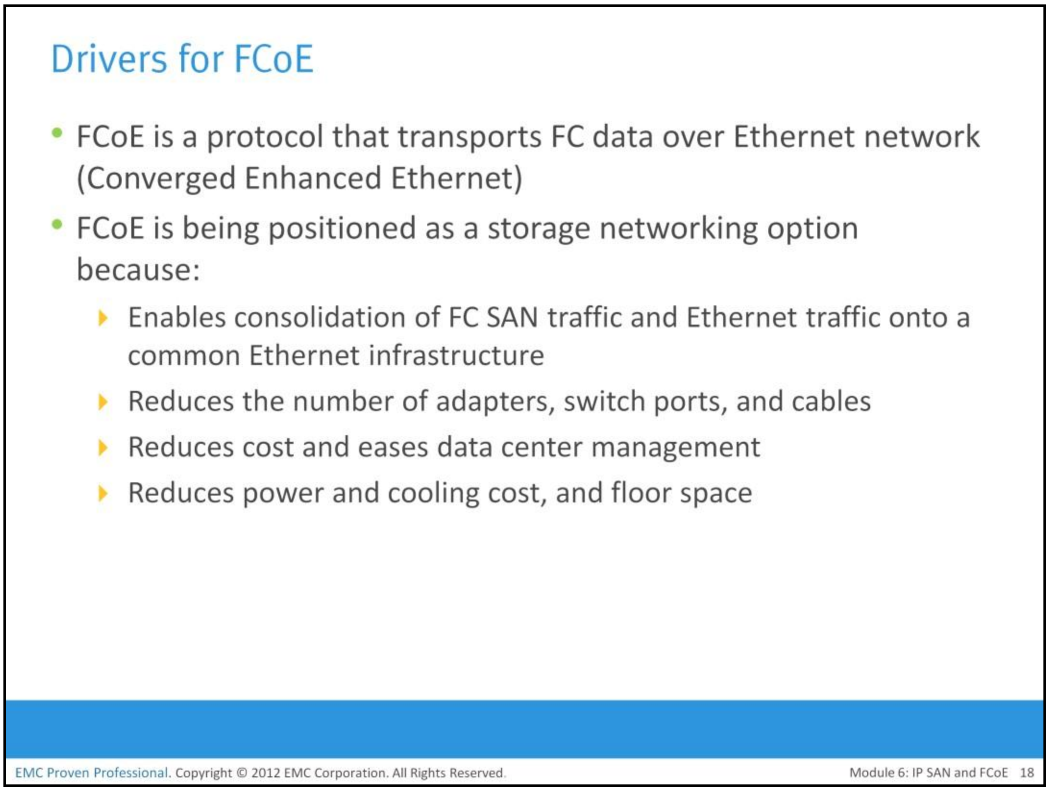
Lesson 2: Fibre Channel over Ethernet (FCoE)

During this lesson the following topics are covered:

- Drivers for FCoE
- Components of FCoE network
- FCoE frame mapping
- Converged Enhanced Ethernet (CEE)

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 17

This lesson covers the drivers of FCoE, components of FCoE network, and FCoE frame mapping. It also covers converged enhanced ethernet (CEE).



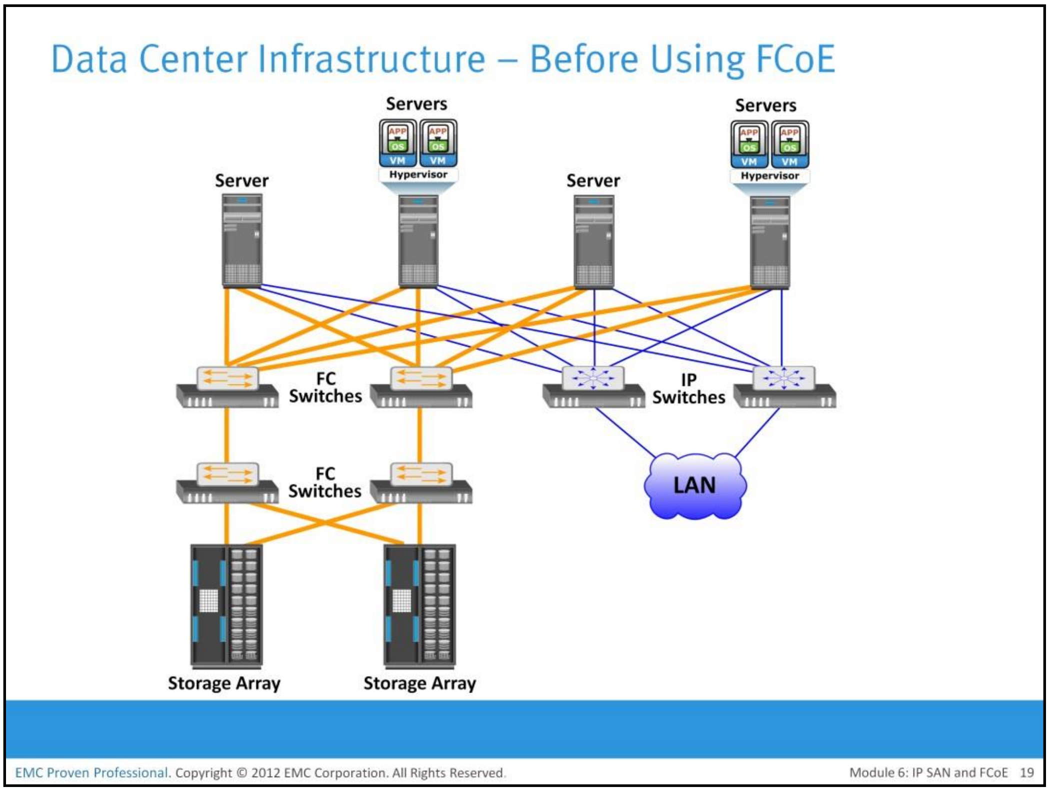
Drivers for FCoE

- FCoE is a protocol that transports FC data over Ethernet network (Converged Enhanced Ethernet)
- FCoE is being positioned as a storage networking option because:
  - Enables consolidation of FC SAN traffic and Ethernet traffic onto a common Ethernet infrastructure
  - Reduces the number of adapters, switch ports, and cables
  - Reduces cost and eases data center management
  - Reduces power and cooling cost, and floor space

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 18

Data centers typically have multiple networks to handle various types of I/O traffic—for example, an Ethernet network for TCP/IP communication and an FC network for FC communication. TCP/IP is typically used for client-server communication, data backup, infrastructure management communication, and so on. FC is typically used for moving block-level data between storage and servers. To support multiple networks, servers in a data center are equipped with multiple redundant physical network interfaces—for example, multiple Ethernet and FC cards/adapters. In addition, to enable the communication, different types of networking switches and physical cabling infrastructure are implemented in data centers. The need for two different kinds of physical network infrastructure increases the overall cost and complexity of data center operation.

Fibre Channel over Ethernet (FCoE) protocol provides consolidation of LAN and SAN traffic over a single physical interface infrastructure. FCoE helps organizations address the challenges of having multiple discrete network infrastructures. FCoE uses the Converged Enhanced Ethernet (CEE) link (10 Gigabit Ethernet) to send FC frames over Ethernet.

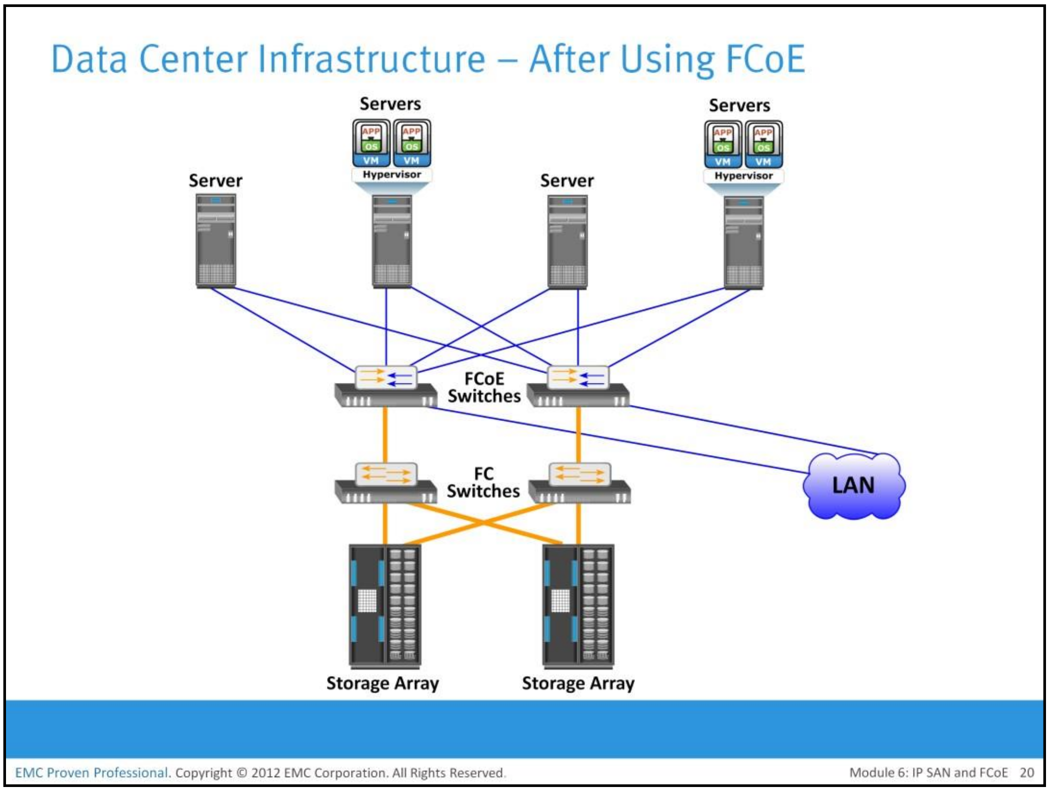


Data Center Infrastructure – Before Using FCoE

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved.

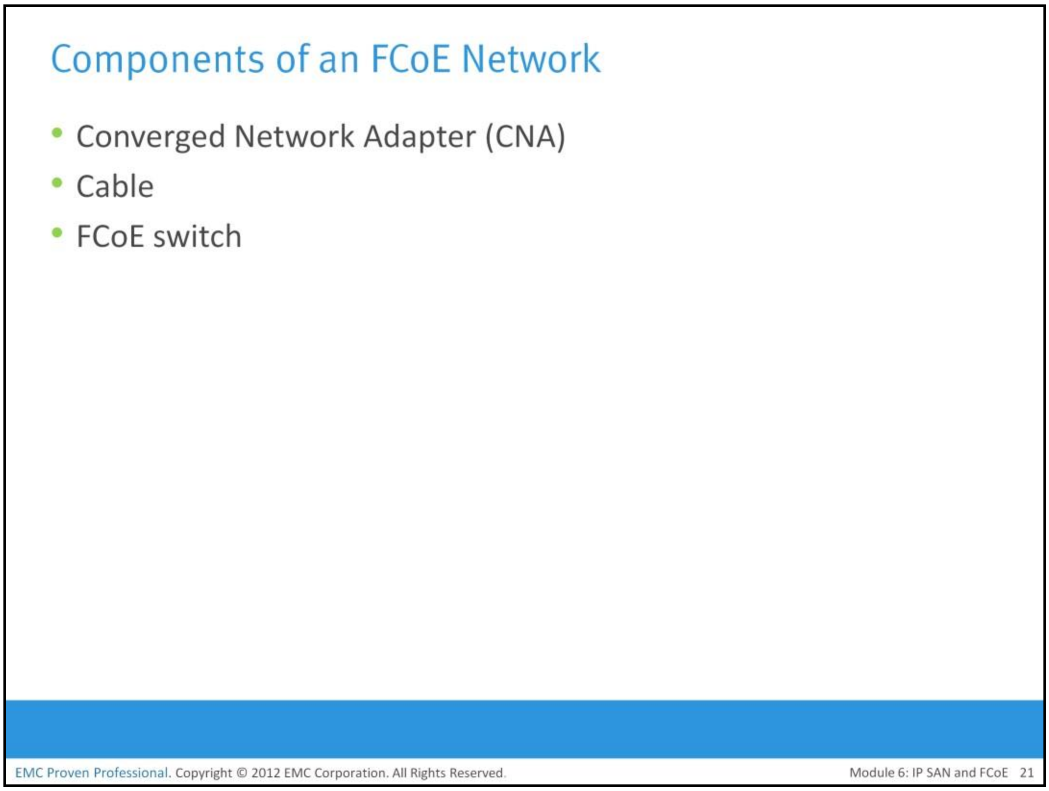
Module 6: IP SAN and FCoE 19

Figure in the slide represents the infrastructure before FCoE deployment. Here, the storage resources are accessed using HBAs, and the IP network resources are accessed using NICs by the servers. Typically, in a data center, a server is configured with 2 to 4 NIC cards and redundant HBA cards. If the data center has hundreds of servers, it would require a large number of adapters, cables, and switches. This leads to a complex environment, which is difficult to manage and scale. The cost of power, cooling, and floor space further adds to the challenge.



Data Center Infrastructure – After Using FCoE

Figure in the slide shows the I/O consolidation with FCoE using FCoE switches and Converged Network Adapters (CNAs). A CNA replaces both HBAs and NICs in the server and consolidates both the IP and FC traffic. This reduces the requirement of multiple network adapters at the server to connect to different networks. Overall, this reduces the requirement of adapters, cables, and switches. This also considerably reduces the cost and management overhead.

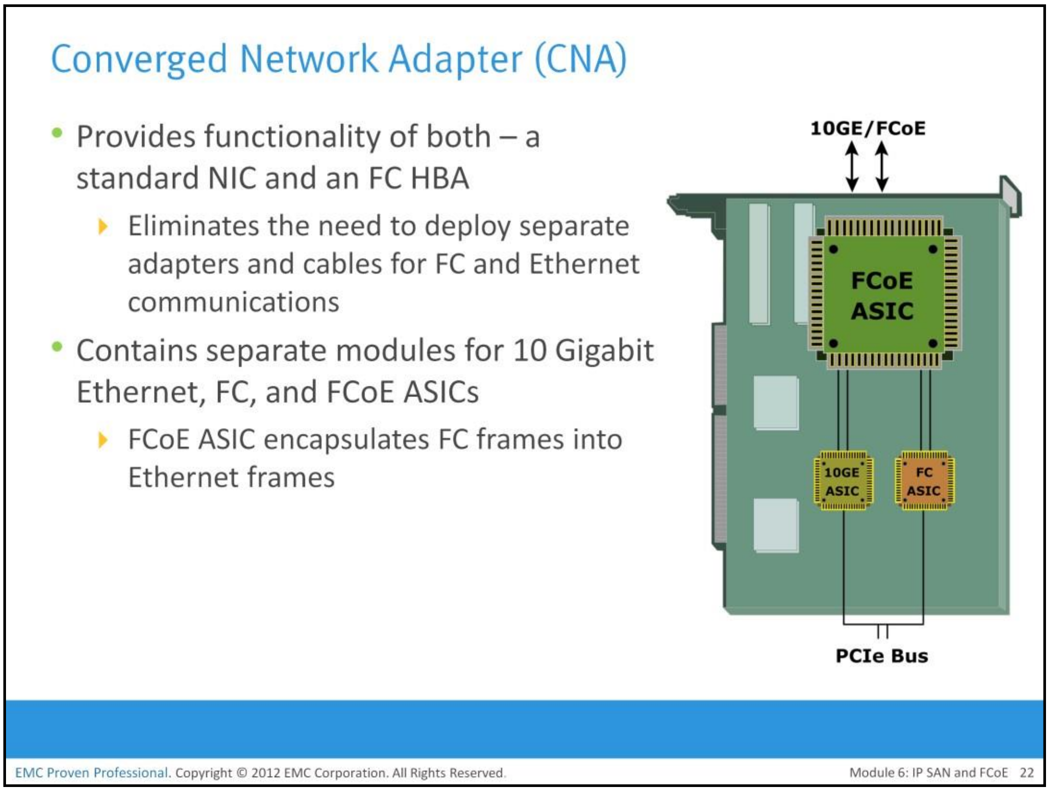


Components of an FCoE Network

- Converged Network Adapter (CNA)
- Cable
- FCoE switch

The key FCoE components are:

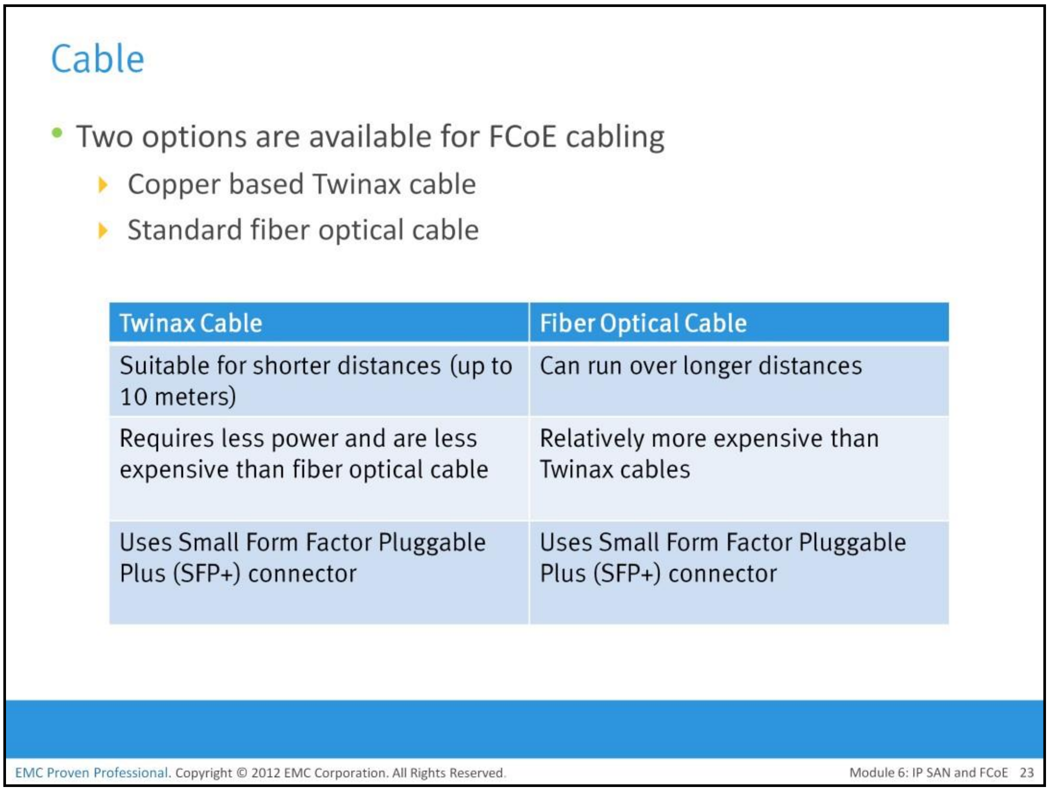
- Converged Network Adapter (CNA)
- Cable
- FCoE switch



Converged Network Adapter (CNA)

- Provides functionality of both – a standard NIC and an FC HBA
  - Eliminates the need to deploy separate adapters and cables for FC and Ethernet communications
- Contains separate modules for 10 Gigabit Ethernet, FC, and FCoE ASICs
  - FCoE ASIC encapsulates FC frames into Ethernet frames

A CNA provides the functionality of both a standard NIC and an FC HBA in a single adapter and consolidates both types of traffic. CNA eliminates the need to deploy separate adapters and cables for FC and Ethernet communications, thereby reducing the required number of server slots and switch ports. CNA offloads the FCoE protocol processing task from the server, thereby freeing the server CPU resources for application processing. A CNA contains separate modules for 10 Gigabit Ethernet, Fibre Channel, and FCoE Application Specific Integrated Circuits (ASICs). The FCoE ASIC encapsulate FC frames into Ethernet frames. One end of this ASIC is connected to 10GbE and FC ASICs for server connectivity, while the other end provides a 10GbE interface to connect to an FCoE switch.



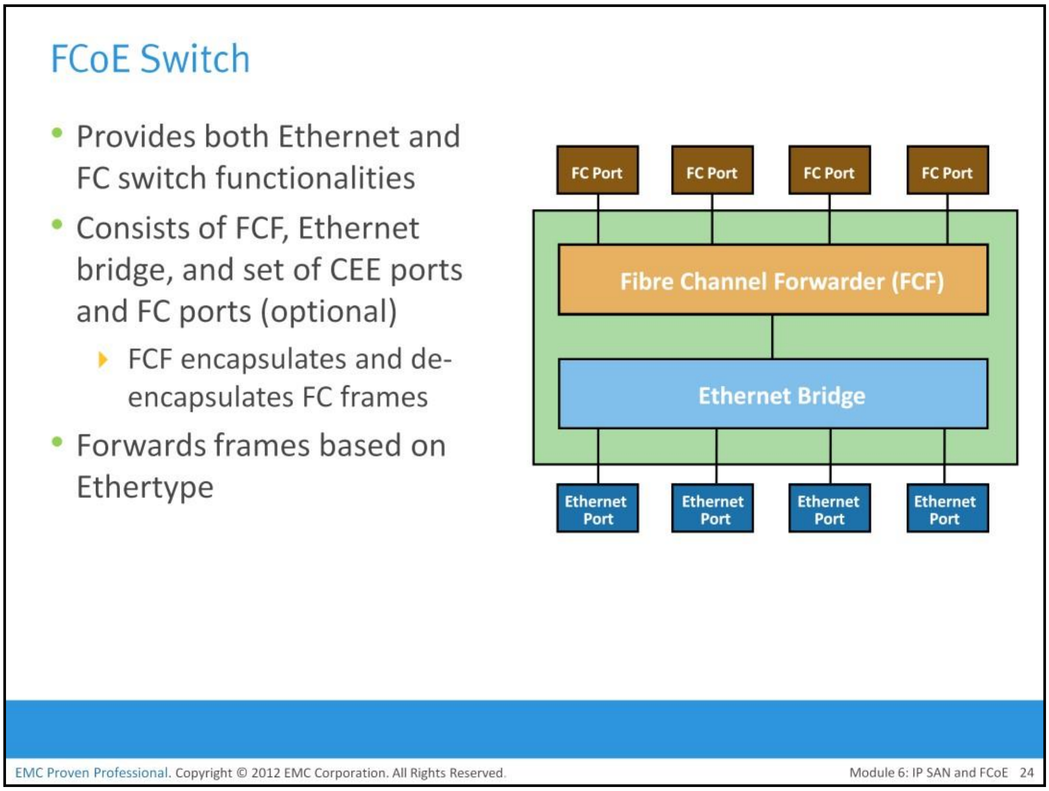
Cable

- Two options are available for FCoE cabling
  - Copper based Twinax cable
  - Standard fiber optical cable

Twinax Cable	Fiber Optical Cable
Suitable for shorter distances (up to 10 meters)	Can run over longer distances
Requires less power and are less expensive than fiber optical cable	Relatively more expensive than Twinax cables
Uses Small Form Factor Pluggable Plus (SFP+) connector	Uses Small Form Factor Pluggable Plus (SFP+) connector

Currently two options are available for FCoE cabling: Copper based Twinax and standard fiber optical cables. A Twinax cable is composed of two pairs of copper cables covered with a shielded casing. The Twinax cable can transmit data at the speed of 10 Gbps over shorter distances up to 10 meters. Twinax cables require less power and are less expensive than fiber optic cables.

The Small Form Factor Pluggable Plus (SFP+) connector is the primary connector used for FCoE links and can be used with both optical and copper cables.



FCoE Switch

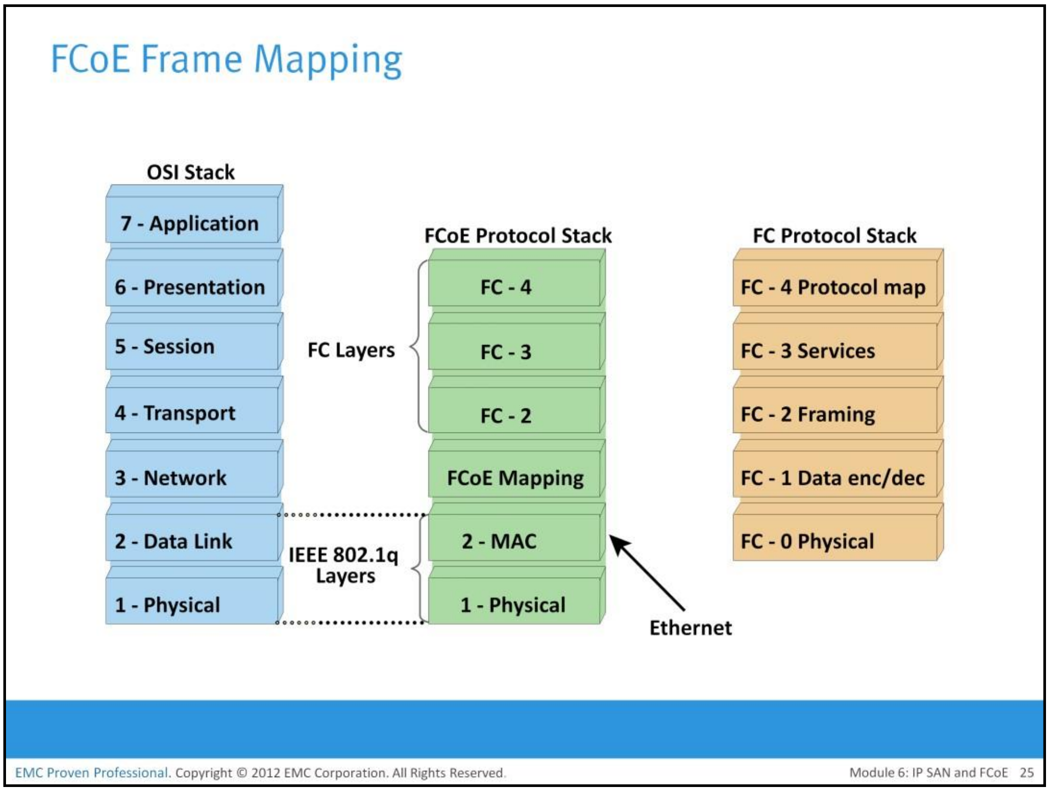
- Provides both Ethernet and FC switch functionalities
- Consists of FCF, Ethernet bridge, and set of CEE ports and FC ports (optional)
  - FCF encapsulates and de-encapsulates FC frames
- Forwards frames based on Ethertype

FC Port
FC Port
FC Port
FC Port
Fibre Channel Forwarder (FCF)
Ethernet Bridge
Ethernet Port
Ethernet Port
Ethernet Port
Ethernet Port

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved.
Module 6: IP SAN and FCoE 24

An FCoE switch has both Ethernet switch and Fibre Channel switch functionalities. The FCoE switch has a Fibre Channel Forwarder (FCF), Ethernet Bridge, and set of Ethernet ports and optional FC ports. The function of the FCF is to encapsulate the FC frames, received from the FC port, into the FCoE frames and also to de-encapsulate the FCoE frames, received from the Ethernet Bridge, to the FC frames.

Upon receiving the incoming traffic, the FCoE switch inspects the Ethertype (used to indicate which protocol is encapsulated in the payload of an Ethernet frame) of the incoming frames and uses that to determine the destination. If the Ethertype of the frame is FCoE, the switch recognizes that the frame contains an FC payload and forwards it to the FCF. From there, the FC is extracted from the FCoE frame and transmitted to FC SAN over the FC ports. If the Ethertype is not FCoE, the switch handles the traffic as usual Ethernet traffic and forwards it over the Ethernet ports.



FCoE Frame Mapping

OSI Stack

7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network

2 - Data Link

1 - Physical

FC Layers

IEEE 802.1q Layers

FCoE Protocol Stack

FC - 4

FC - 3

FC - 2

FCoE Mapping

2 - MAC

1 - Physical

Ethernet

FC Protocol Stack

FC - 4 Protocol map

FC - 3 Services

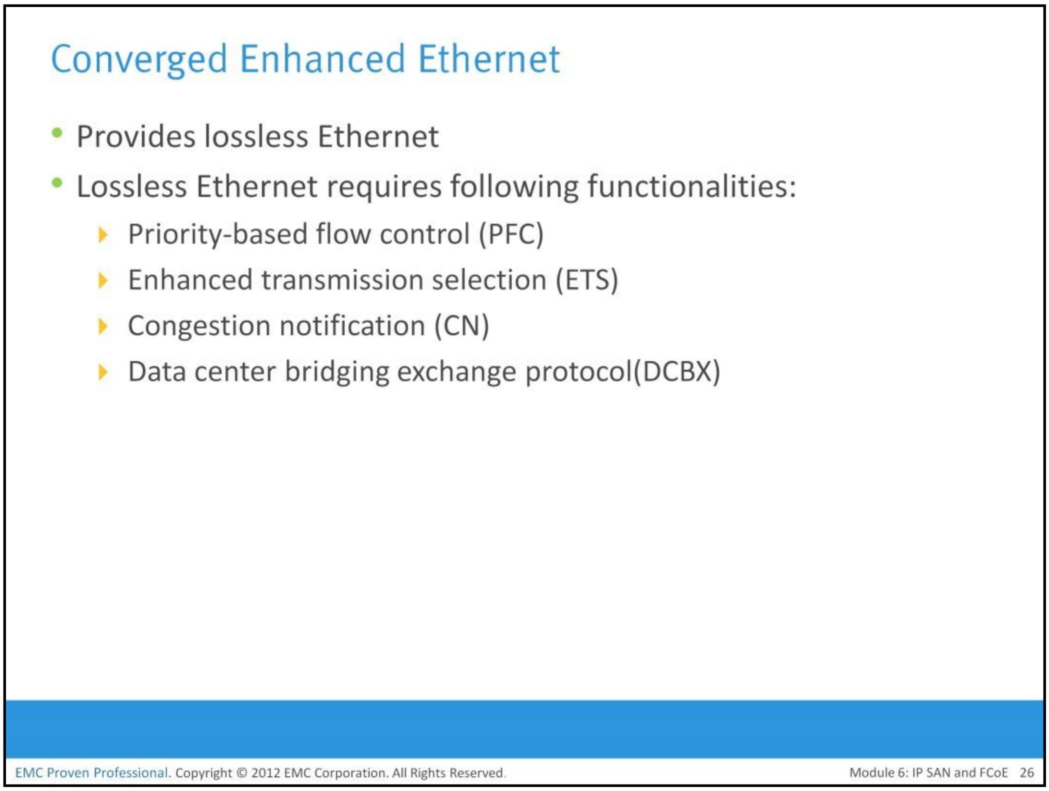
FC - 2 Framing

FC - 1 Data enc/dec

FC - 0 Physical

The encapsulation of the Fibre Channel frame occurs through the mapping of the FC frames onto Ethernet, as shown in the slide. Fibre Channel and traditional networks have stacks of layers where each layer in the stack represents a set of functionalities. The FC stack consists of five layers: FC-0 through FC-4. Ethernet is typically considered as a set of protocols that operates at the physical and data link layers in the seven-layer OSI stack. The FCoE protocol specification replaces the FC-0 and FC-1 layers of the FC stack with Ethernet. This provides the capability to carry the FC-2 to the FC-4 layer over the Ethernet layer.

A typical Fibre Channel data frame has a 2,112-byte payload, a 24-byte header, and an FCS. A standard Ethernet frame has a default payload capacity of 1,500 bytes. To maintain good performance, FCoE must use jumbo frames to prevent a Fibre Channel frame from being split into two Ethernet frames.

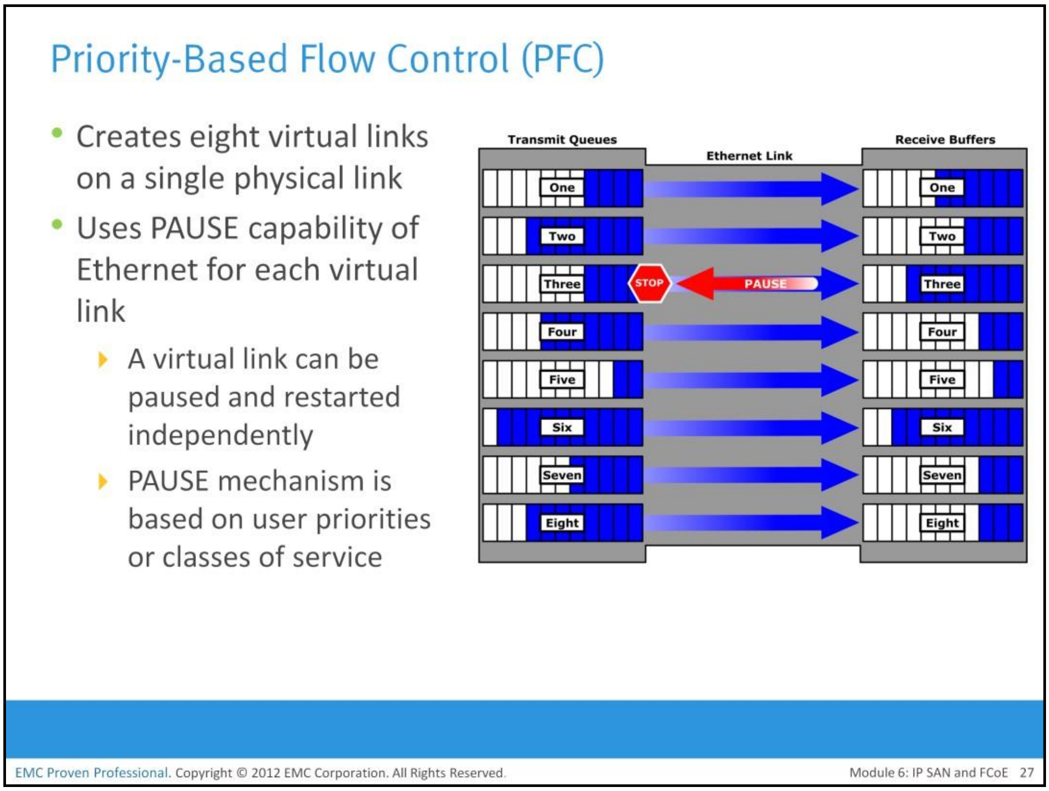


Converged Enhanced Ethernet

- Provides lossless Ethernet
- Lossless Ethernet requires following functionalities:
  - Priority-based flow control (PFC)
  - Enhanced transmission selection (ETS)
  - Congestion notification (CN)
  - Data center bridging exchange protocol(DCBX)

Conventional Ethernet is lossy in nature, which means that frames might be dropped or lost during transmission. Converged Enhanced Ethernet (CEE) or lossless Ethernet provides a new specification to the existing Ethernet standard that eliminates the lossy nature of Ethernet. This makes 10 Gb Ethernet a viable storage networking option, similar to FC. Lossless Ethernet requires certain functionalities. These functionalities are defined and maintained by the data center bridging (DCB) task group, which is a part of the IEEE 802.1 working group and they are:

- Priority-based flow control
- Enhanced transmission selection
- Congestion notification
- Data center bridging exchange protocol

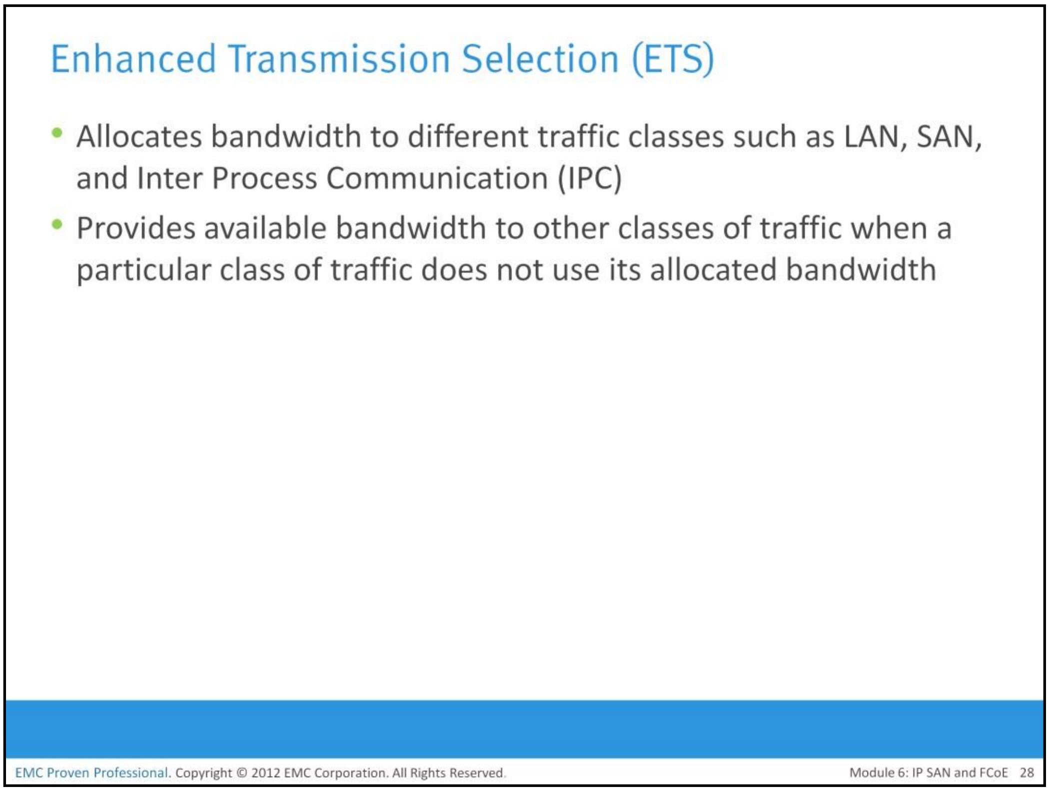


Priority-Based Flow Control (PFC)

- Creates eight virtual links on a single physical link
- Uses PAUSE capability of Ethernet for each virtual link
  - A virtual link can be paused and restarted independently
  - PAUSE mechanism is based on user priorities or classes of service

Traditional FC manages congestion through the use of a link-level, credit-based flow control that guarantees no loss of frames. Typical Ethernet, coupled with TCP/IP, uses a packet drop flow control mechanism. The packet drop flow control is not lossless. This challenge is eliminated by using an IEEE 802.3x Ethernet PAUSE control frame to create a lossless Ethernet. A receiver can send a PAUSE request to a sender when the receiver's buffer is filling up. Upon receiving a PAUSE frame, the sender stops transmitting frames, which guarantees no loss of frames. The downside of using the Ethernet PAUSE frame is that it operates on the entire link, which might be carrying multiple traffic flows.

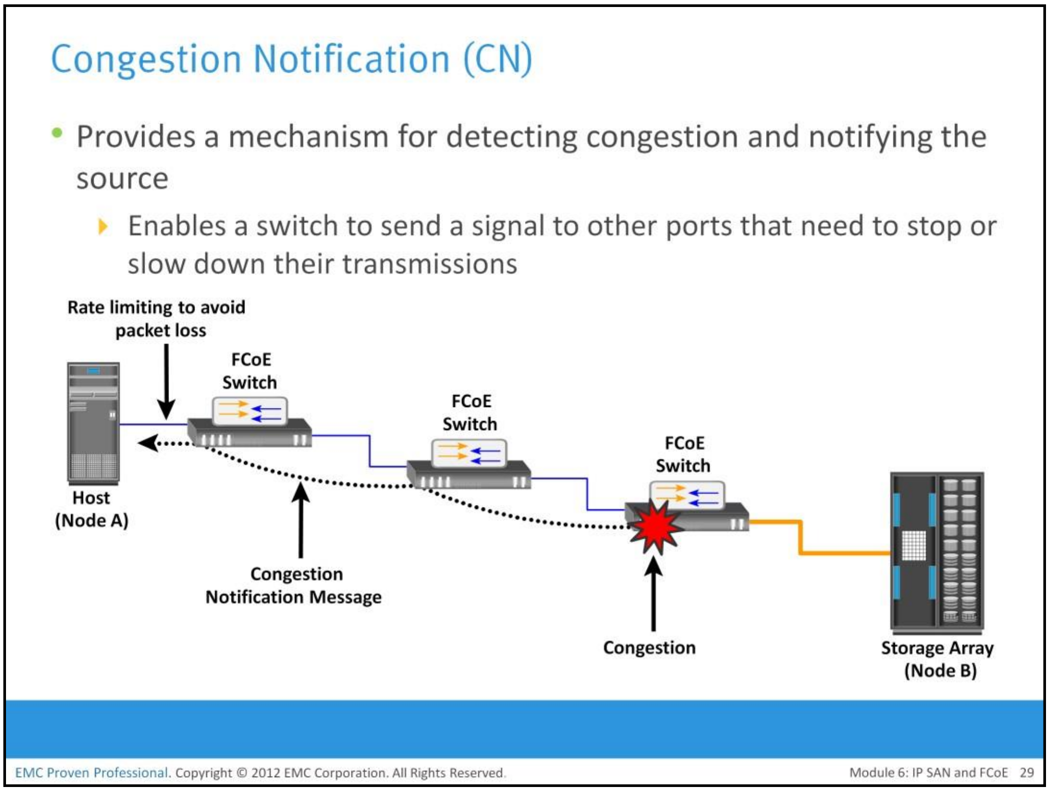
PFC provides a link level flow control mechanism. PFC creates eight separate virtual links on a single physical link and allows any of these links to be paused and restarted independently. PFC enables the pause mechanism based on user priorities or classes of service. Enabling the pause based on priority allows creating lossless links for traffic, such as FCoE traffic. This PAUSE mechanism is typically implemented for FCoE while regular TCP/IP traffic continues to drop frames. Figure in the slide illustrates how a physical Ethernet link is divided into eight virtual links and allows a PAUSE for a single virtual link without affecting the traffic for the others.



Enhanced Transmission Selection (ETS)

- Allocates bandwidth to different traffic classes such as LAN, SAN, and Inter Process Communication (IPC)
- Provides available bandwidth to other classes of traffic when a particular class of traffic does not use its allocated bandwidth

Enhanced transmission selection provides a common management framework for the assignment of bandwidth to different traffic classes, such as LAN, SAN, and Inter Process Communication (IPC). When a particular class of traffic does not use its allocated bandwidth, ETS enables other traffic classes to use the available bandwidth.

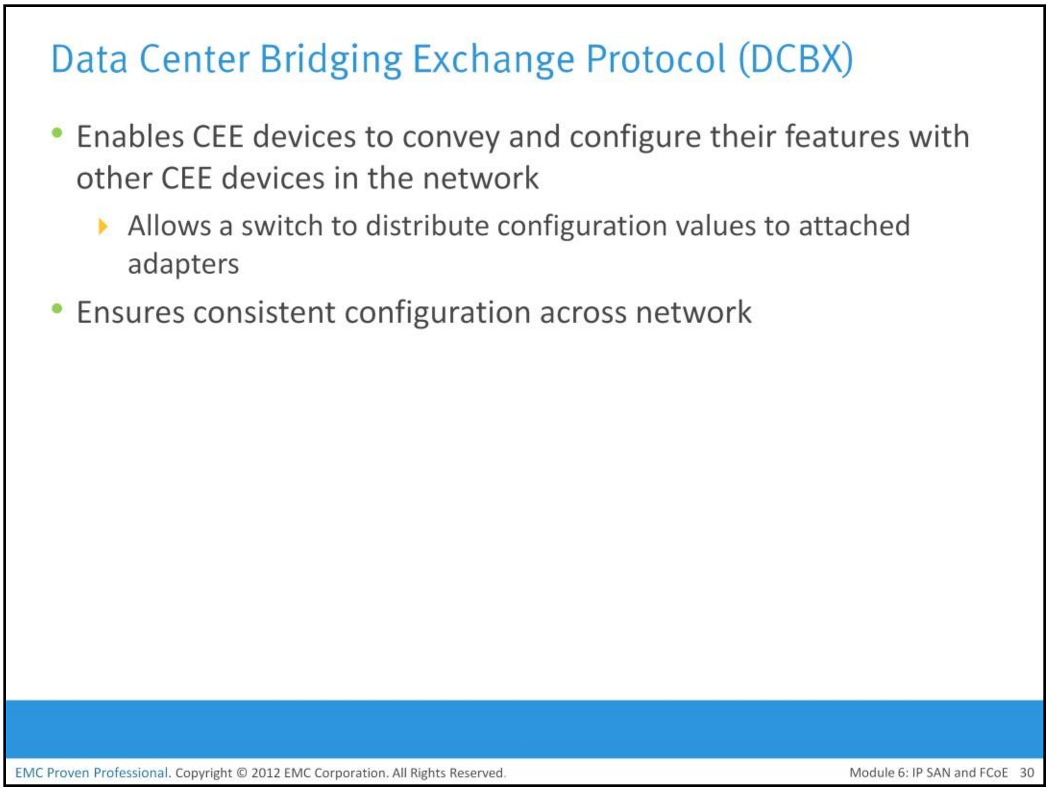


Congestion Notification (CN)

- Provides a mechanism for detecting congestion and notifying the source
  - Enables a switch to send a signal to other ports that need to stop or slow down their transmissions

EMC Proven Professional. Copyright © 2012 EMC Corporation. All Rights Reserved. Module 6: IP SAN and FCoE 29

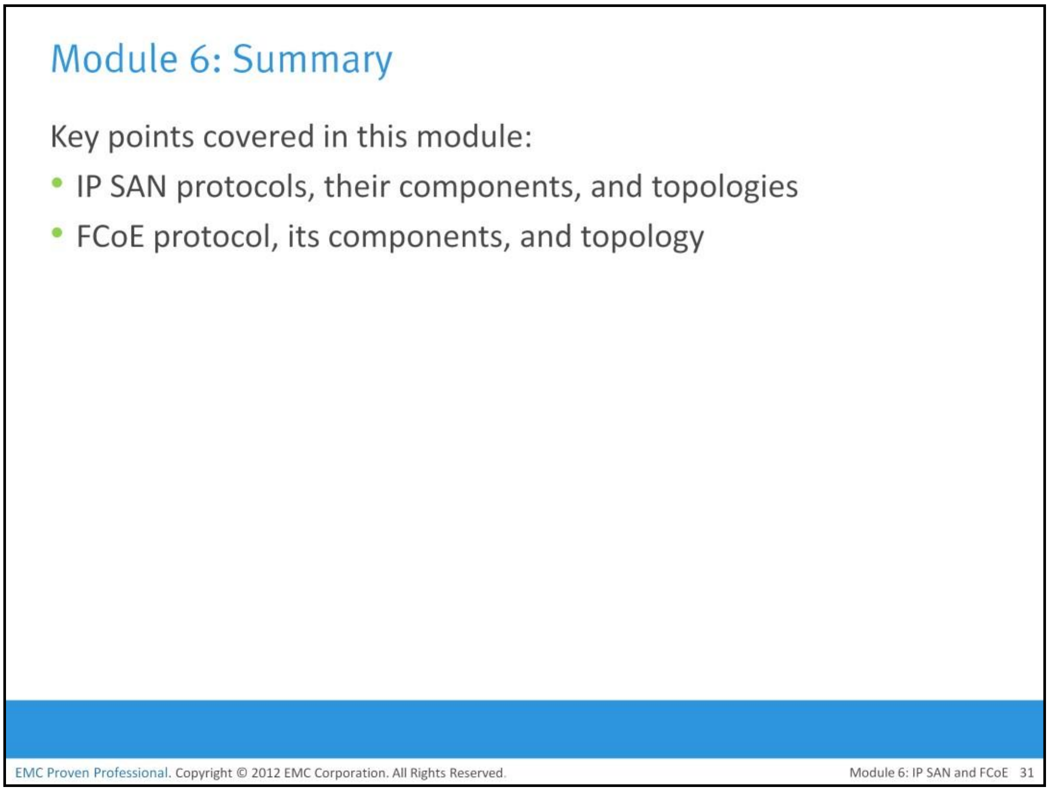
Congestion notification provides end-to-end congestion management for protocols, such as FCoE, that do not have built-in congestion control mechanisms. Link level congestion notification provides a mechanism for detecting congestion and notifying the source to move the traffic flow away from the congested links. Link level congestion notification enables a switch to send a signal to other ports that need to stop or slow down their transmissions. The process of congestion notification and its management is shown in the slide, which represents the communication between the nodes A (sender) and B (receiver). If congestion at the receiving end occurs, the algorithm running on the switch, generates a congestion notification (CN) message to the sending node (Node A). In response to the CN message, the sending end limits the rate of data transfer.



Data Center Bridging Exchange Protocol (DCBX)

- Enables CEE devices to convey and configure their features with other CEE devices in the network
  - Allows a switch to distribute configuration values to attached adapters
- Ensures consistent configuration across network

DCBX protocol is a discovery and capability exchange protocol, which helps Converged Enhanced Ethernet devices to convey and configure their features with the other CEE devices in the network. DCBX is used to negotiate capabilities between the switches and the adapters, and it allows the switch to distribute the configuration values to all the attached adapters. This helps to ensure consistent configuration across the entire network.

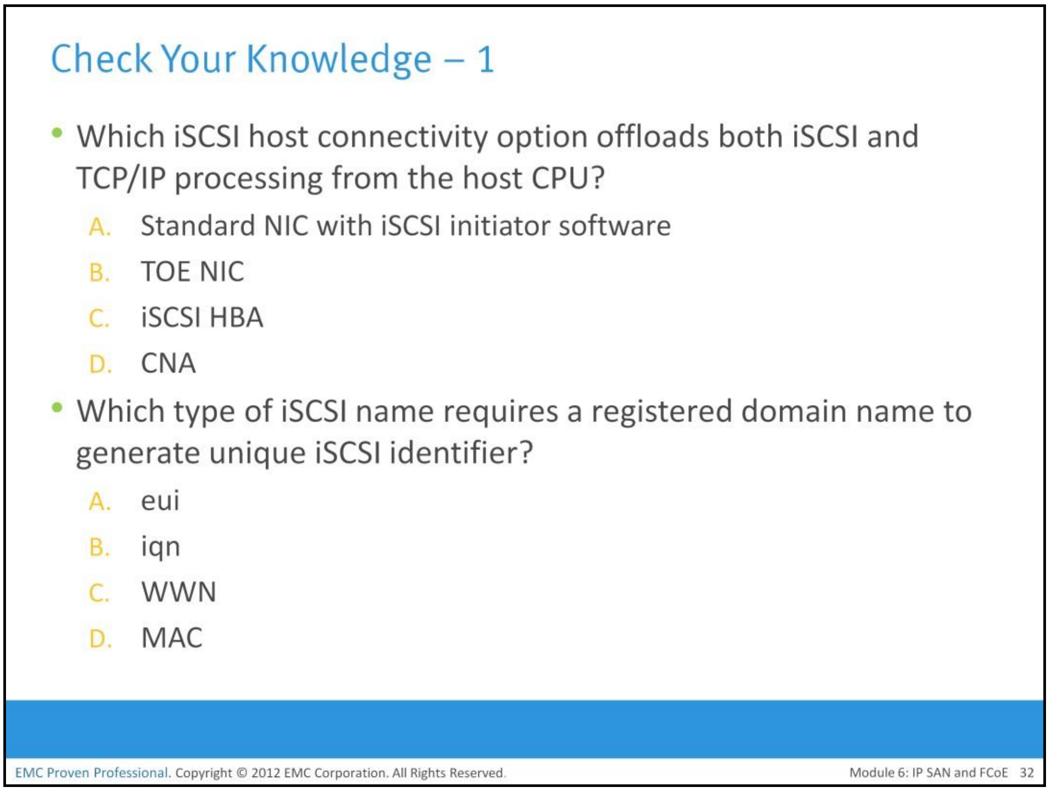


Module 6: Summary

Key points covered in this module:

- IP SAN protocols, their components, and topologies
- FCoE protocol, its components, and topology

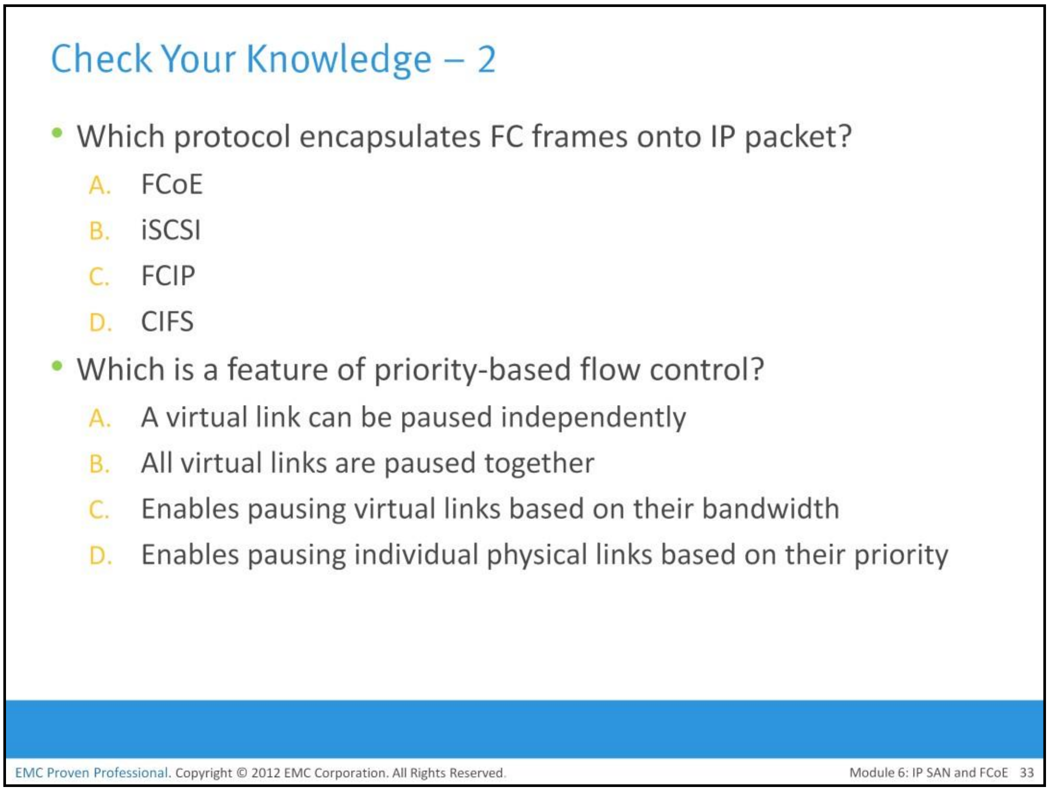
This module covered IP SAN protocols such as iSCSI and FCIP, their components, and topologies. It also covered FCoE protocol, its components, and topology.



Check Your Knowledge – 1

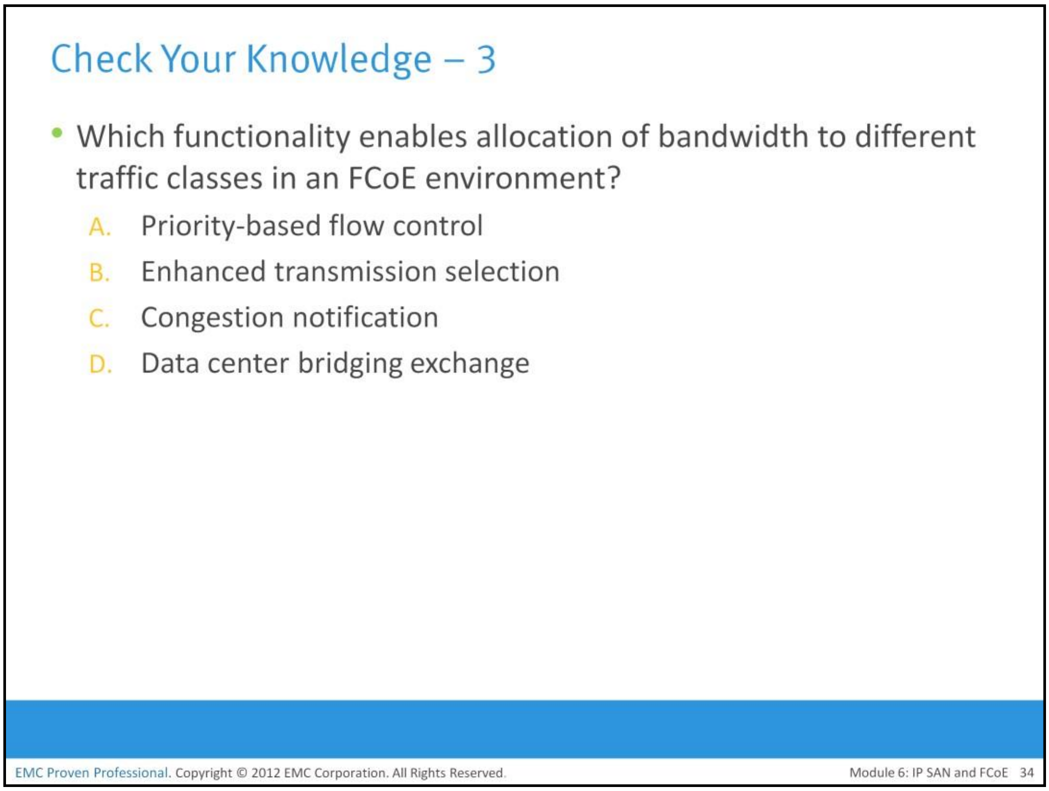
- Which iSCSI host connectivity option offloads both iSCSI and TCP/IP processing from the host CPU?
  A. Standard NIC with iSCSI initiator software
  B. TOE NIC
  C. iSCSI HBA
  D. CNA
- Which type of iSCSI name requires a registered domain name to generate unique iSCSI identifier?
  A. eui
  B. iqn
  C. WWN
  D. MAC

EMC Proven Professional. Module 6: IP SAN and FCoE 32



Check Your Knowledge – 2

- Which protocol encapsulates FC frames onto IP packet?
  A. FCoE
  B. iSCSI
  C. FCIP
  D. CIFS
- Which is a feature of priority-based flow control?
  A. A virtual link can be paused independently
  B. All virtual links are paused together
  C. Enables pausing virtual links based on their bandwidth
  D. Enables pausing individual physical links based on their priority



Check Your Knowledge – 3

- Which functionality enables allocation of bandwidth to different traffic classes in an FCoE environment?
  A. Priority-based flow control
  B. Enhanced transmission selection
  C. Congestion notification
  D. Data center bridging exchange