Fibre Channel Storage Area Network (FC SAN)

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

- Describe FC SAN and its components
- Describe FC architecture
- Describe FC SAN topologies and zoning
- Describe virtualization in a SAN environment

Lesson 1: Overview of FC SAN

During this lesson the following topics are covered:

- Evolution of FC SAN
- Components of FC SAN
- FC interconnectivity options
- FC port types

- An effective information management solution must provide:
  - Just-in-time information to business users
  - Flexible and resilient storage infrastructure
- Information management challenges in DAS environment:
  - Explosive growth of information storage that remains isolated and underutilized
  - Proliferation of new servers and applications
  - Complexity in sharing storage resources across multiple servers
  - High cost of managing information
- Storage area network (SAN) addresses these challenges

SAN

It is a high-speed, dedicated network of servers and shared storage devices.

Centralizes storage and management

Enables sharing of storage resources across multiple servers at block level

Meets increasing storage demands efficiently with better economies of scale

Common SAN deployments are:

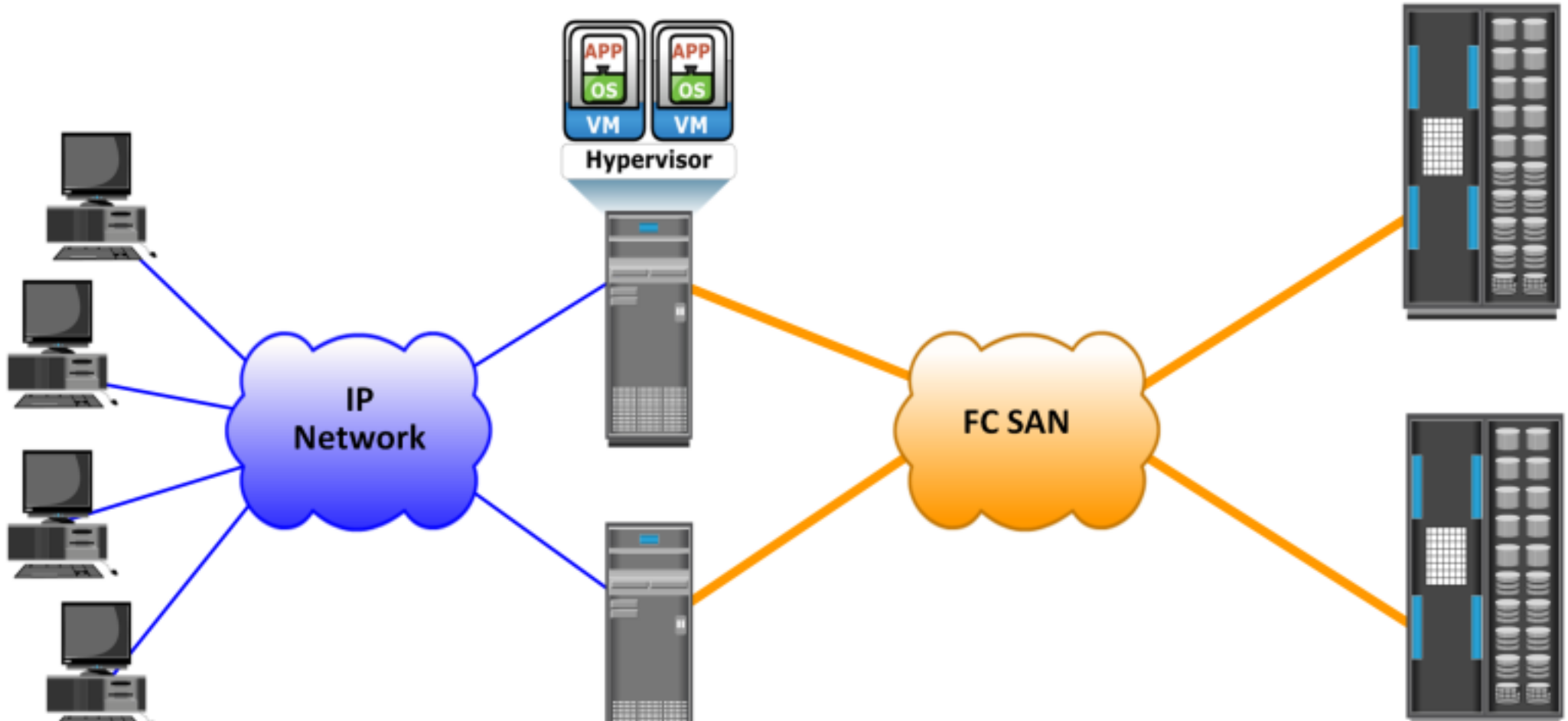
- Fibre Channel (FC) SAN: uses FC protocol for communication
- IP SAN: uses IP-based protocols for communication

High-speed network technology

- Latest FC implementation supports speed up to 16 Gb/s

Highly scalable

- Theoretically, accommodate approximately 15 million devices



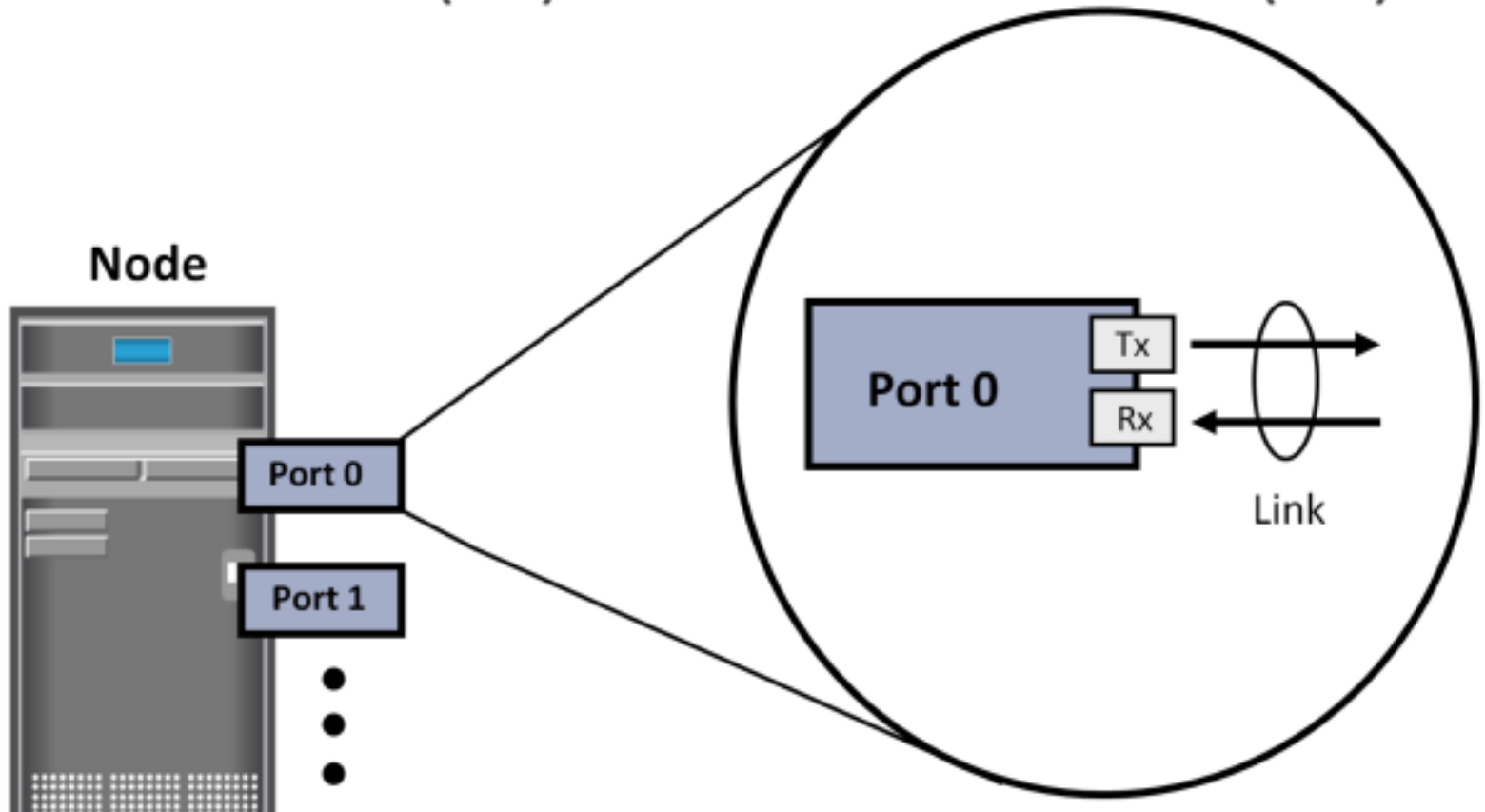
- Node (server and storage) ports
- Cables
- Connectors
- Interconnecting devices such as FC switches and hubs
- SAN management software

Provide physical interface for communicating with other nodes

Exist on

- HBA in server
- Front-end adapters in storage

Each port has a transmit (Tx) link and a receive (Rx) link

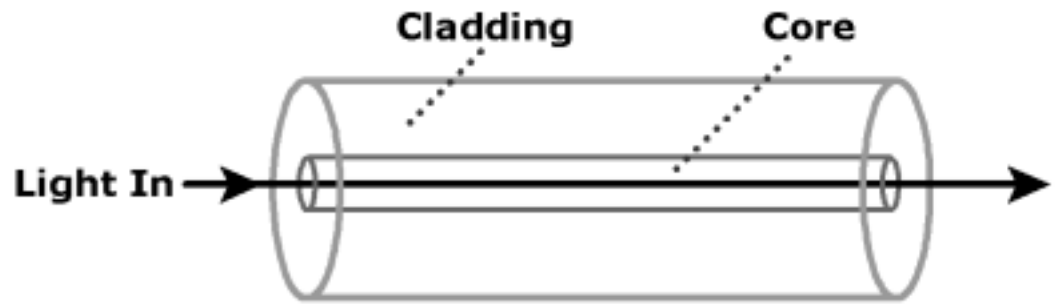


SAN implementation uses

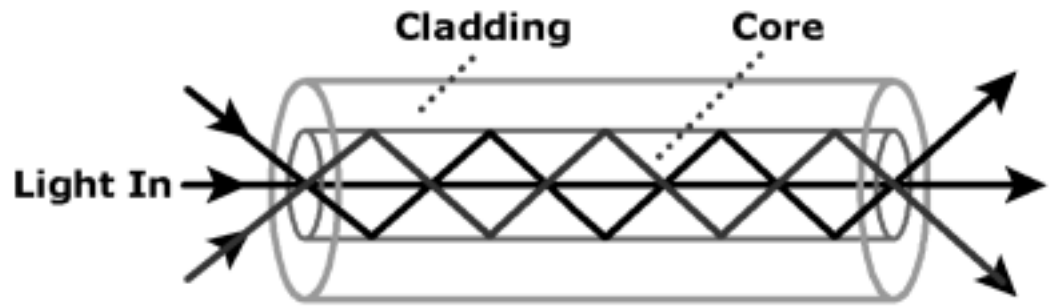
- Copper cables for short distance
- Optical fiber cables for long distance

Two types of optical cables: single-mode and multimode

Single-mode	Multimode
Carries single beam of light	Can carry multiple beams of light simultaneously
Distance up to 10km	Used for short distance (Modal dispersion weakens signal strength after certain distance)



Single-mode Fiber



Attached at the end of a cable

Enable swift connection and disconnection of the cable to and from a port

Commonly used connectors for fiber optic cables are:

- Standard Connector (SC)
  - Duplex connectors
- Lucent Connector (LC)
  - Duplex connectors
- Straight Tip (ST)
  - Patch panel connectors
  - Simplex connectors

Standard Connector

Lucent Connector

Commonly used interconnecting devices in FC SAN are:

- Hubs, switches, and directors

Hubs provide limited connectivity and scalability

Switches and directors are intelligent devices

- Switches are available with fixed port count or modular design
- Directors are always modular, and its port count can be increased by inserting additional 'line cards' or 'blades'
- High-end switches and directors contain redundant components

A suite of tools used in a SAN to manage interfaces between host and storage arrays

Provides integrated management of SAN environment

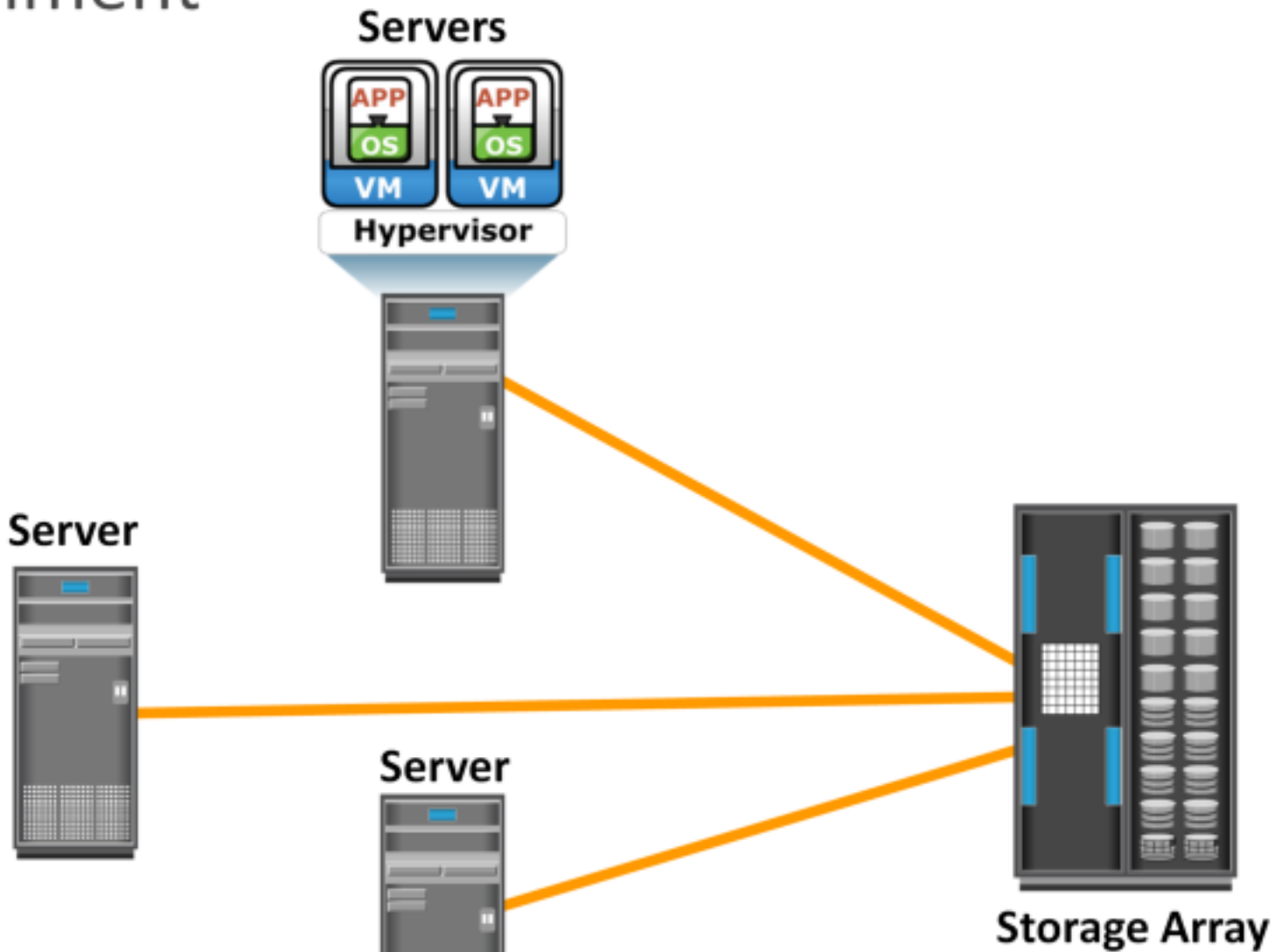
Enables web-based management using GUI or CLI

- Point-to-Point
- Fibre Channel Arbitrated Loop (FC-AL)
- Fibre Channel Switched Fabric (FC-SW)

Enables direct connection between nodes

Offers limited connectivity and scalability

Used in DAS environment



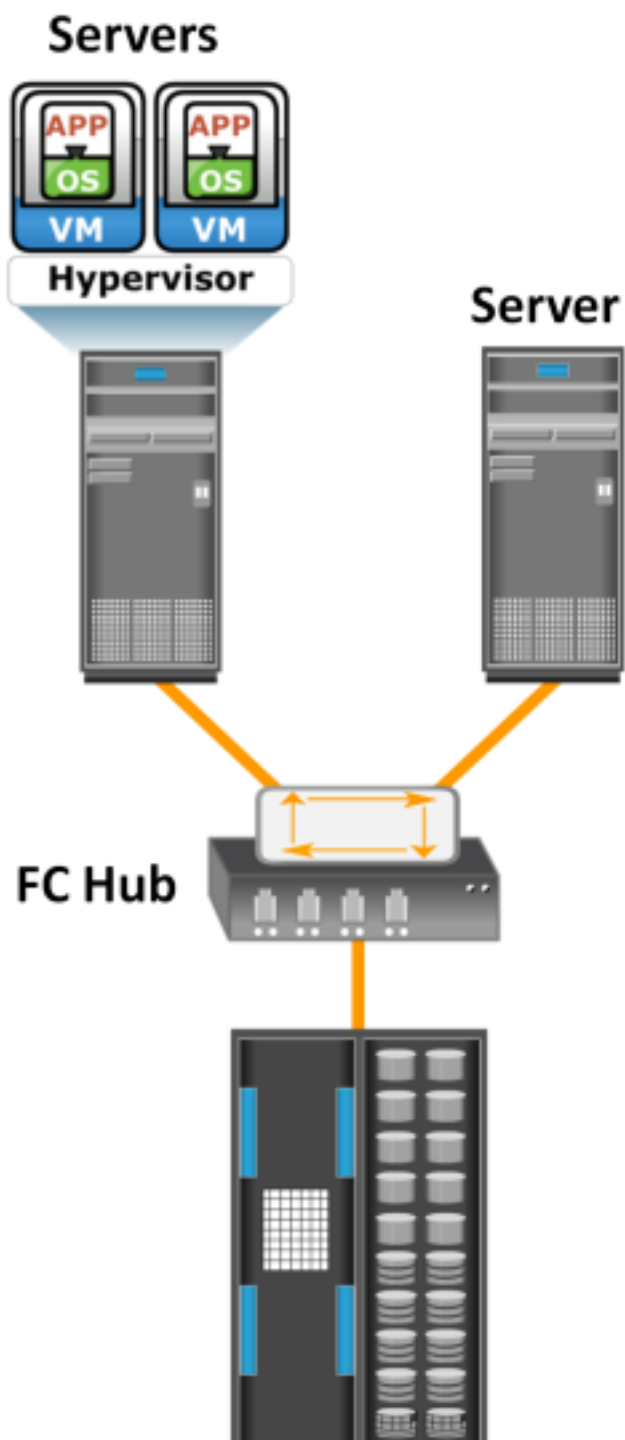
Provides shared loop to attached nodes

- Nodes must arbitrate to gain control

Implemented using ring or star topology

Limitations of FC-AL

- Only one device can perform I/O operation at a time
- Supports up to 126 nodes
- Addition or removal of a node causes momentary pause in loop traffic

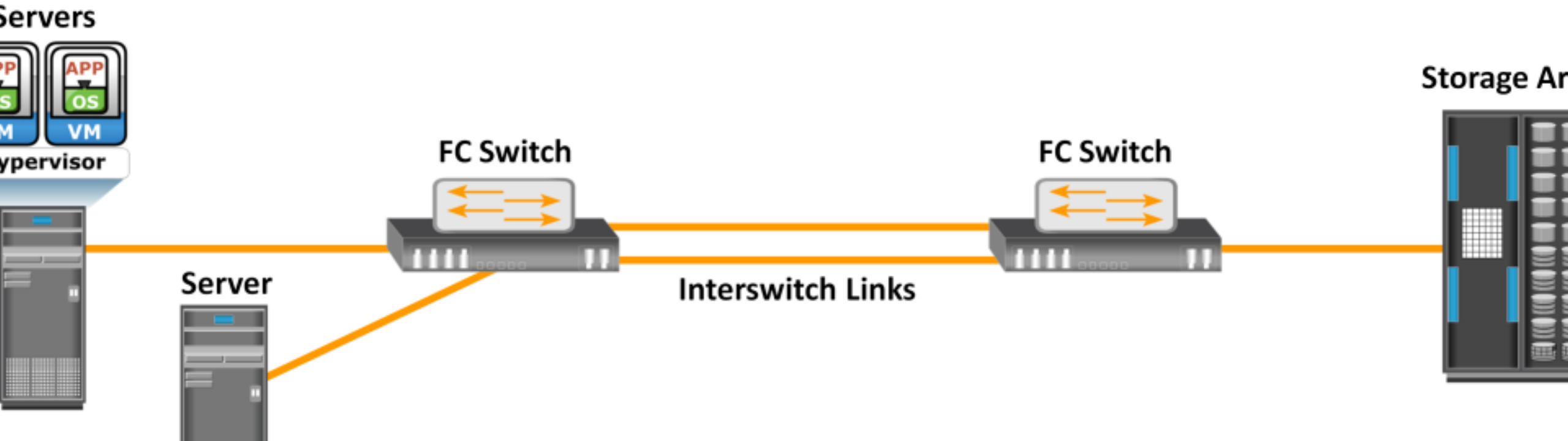


Creates a logical space (called fabric) in which all nodes communicate with one another using switches

- Interswitch links (ISLs) enable switches to be connected together

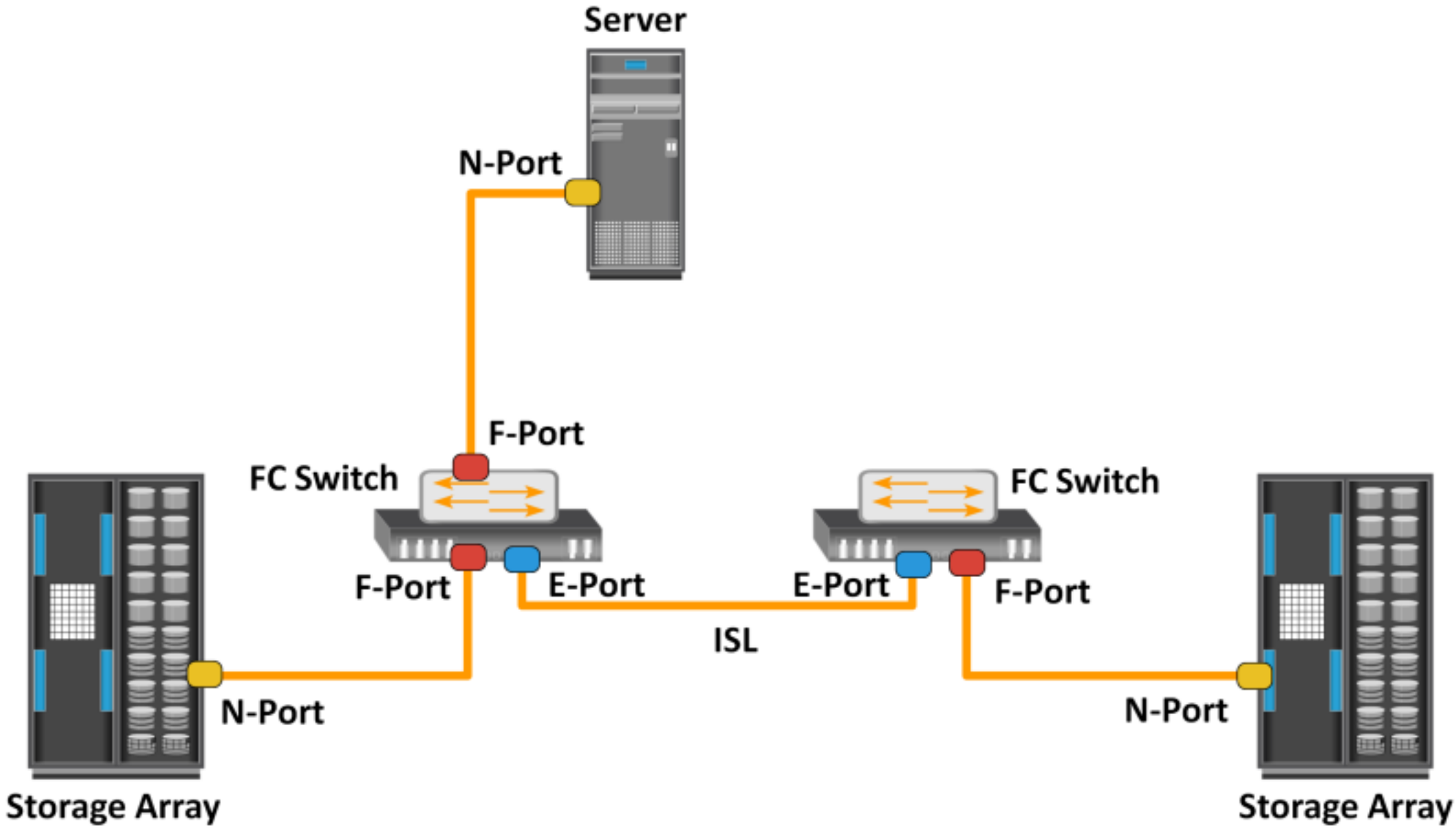
Provides dedicated path between nodes

Addition/removal of node does not affect traffic of other nodes



Ports in a switched fabric can be one of the following types:

- **N_Port:** An end point in the fabric. This port is also known as the node port. Typically, it is a host port (HBA) or a storage array port that is connected to a switch in a switched fabric.
- **E_Port:** A port that forms the connection between two FC switches. This port is also known as the expansion port. The E_Port on an FC switch connects to the E_Port of another FC switch in the fabric ISLs.
- **F_Port:** A port on a switch that connects an N_Port. It is also known as a fabric port.
- **G_Port:** A generic port on a switch that can operate as an E_Port or an F_Port and determines its functionality automatically during initialization.


Server
N-Port
F-Port
FC Switch
F-Port
E-Port
E-Port
FC Switch
F-Port
ISL
N-Port
N-Port
Storage Array
Storage Array

Lesson 2: Fibre Channel (FC) Architecture

During this lesson the following topics are covered:

- FC protocol stack
- FC addressing
- WWN addressing
- Structure and organization of FC data
- Fabric services
- Fabric login types

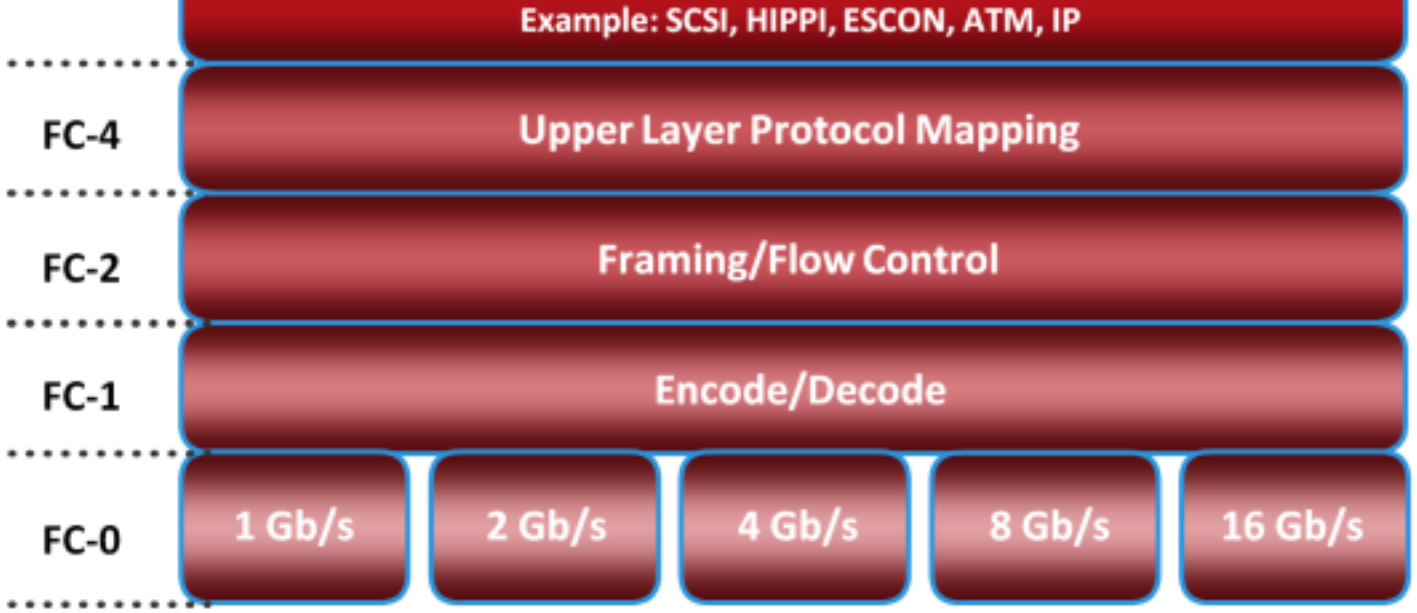
Provides benefits of both channel and network technologies

- Provides high performance with low protocol overheads
- Provides high scalability with long distance capability

Implements SCSI over FC network

- Transports SCSI data through FC network

Storage devices, attached to SAN, appear as local storage devices to host operating system

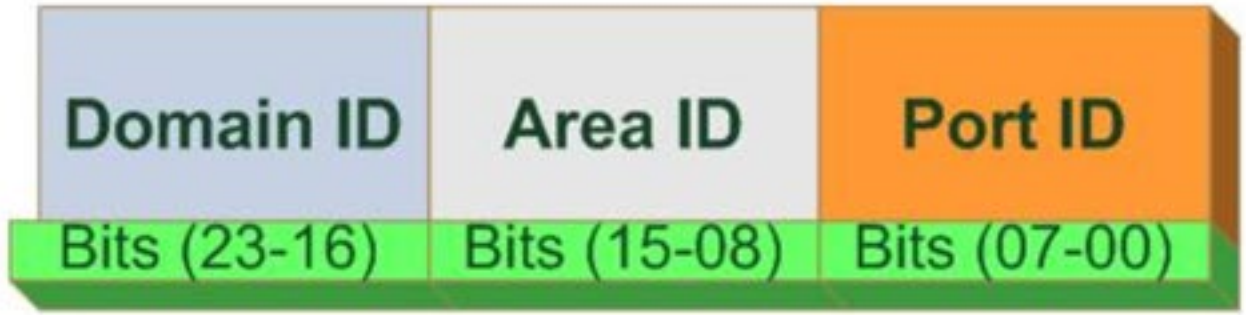


FC Layer	Function	Features Specified by FC Layer
FC-4	Mapping interface	Mapping upper layer protocol (e.g. SCSI) to lower FC layers
FC-3	Common services	Not implemented
FC-2	Routing, flow control	Frame structure, FC addressing, flow control
FC-1	Encode/decode	8b/10b or 64b/66b encoding, bit and frame synchronization

FC Address is assigned to nodes during fabric login

- Used for communication between nodes within FC SAN

Address format



Domain ID is a unique number provided to each switch in the fabric

- 239 addresses are available for domain ID

Maximum possible number of node ports in a switched fabric:

- 239 domains X 256 areas X 256 ports = 15,663,104

An FC address is dynamically assigned when a node port logs on to the fabric. The FC address has a distinct format, as shown in the slide. The first field of the FC address contains the domain ID of the switch. A Domain ID is a unique number provided to each switch in the fabric. Although this is an 8-bit field, there are only 239 available addresses for domain ID because some addresses are deemed special and reserved for fabric management services. For example, FFFFFC is reserved for the name server, and FFFFFE is reserved for the fabric login service. The area ID is used to identify a group of switch ports used for connecting nodes. An example of a group of ports with common area ID is a port card on the switch. The last field, the port ID, identifies the port within the group.

Therefore, the maximum possible number of node ports in a switched fabric is calculated as:

239 domains X 256 areas X 256 ports = 15,663,104

Unique 64 bit identifier

Static to node ports on an FC network

- Similar to MAC address of NIC
- WWNN and WWPN are used to uniquely identify nodes and ports respectively

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
ormat Type	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
ormat Type	Reserved 12 bits			Company ID 24 bits						Company Specific 24 bits					

FC data is organized as Exchange, Sequence, and Frame

C Data Structure	Description

xchange	• Enables two N_Ports to identify and manage a set of information units
	  • Information unit: upper layer protocol-specific information that is sent to another port to perform certain operation
	  • Each information unit maps to a sequence
	• Includes one or more sequences

equence	• Contiguous set of frames that correspond to an information unit
ame	• Fundamental unit of data transfer • Each frame consists of five parts: SOF, frame header, data field, CRC, and EOF

FC switches provide fabric services as defined in FC standards

Fabric Services	Description
Fabric Login Server	• Used during the initial part of the node's fabric login process • Located at pre-defined address of FFFFFE
Name Server	• Responsible for name registration and management of node ports • Located at pre-defined address FFFFFC
Fabric Controller	• Responsible for managing and distributing Registered State Change Notifications (RSCNs) to attached node ports • Responsible for distributing SW-RSCNs to every other switch – SW-RSCNs keep the name server up-to-date on all switches • Located at pre-defined address FFFFFD
Management Server	• Enables FC SAN management using fabric management software • Located at pre-defined address FFFFFA

Fabric login (FLOGI)

- Occurs between an N_Port and an F_Port
- Node sends a FLOGI frame with WWN to Fabric Login Server on switch
- Node obtains FC address from switch
- Immediately after FLOGI, N_Port registers with Name Server on switch, indicating its WWN, port type, assigned FC address, etc.
- N_Port queries name server about all other logged in ports

Port login (PLOGI)

- Occurs between two N_Ports to establish a session
- Exchange service parameters relevant to the session

Lesson 3: FC SAN Topologies and Zoning

During this lesson the following topics are covered:

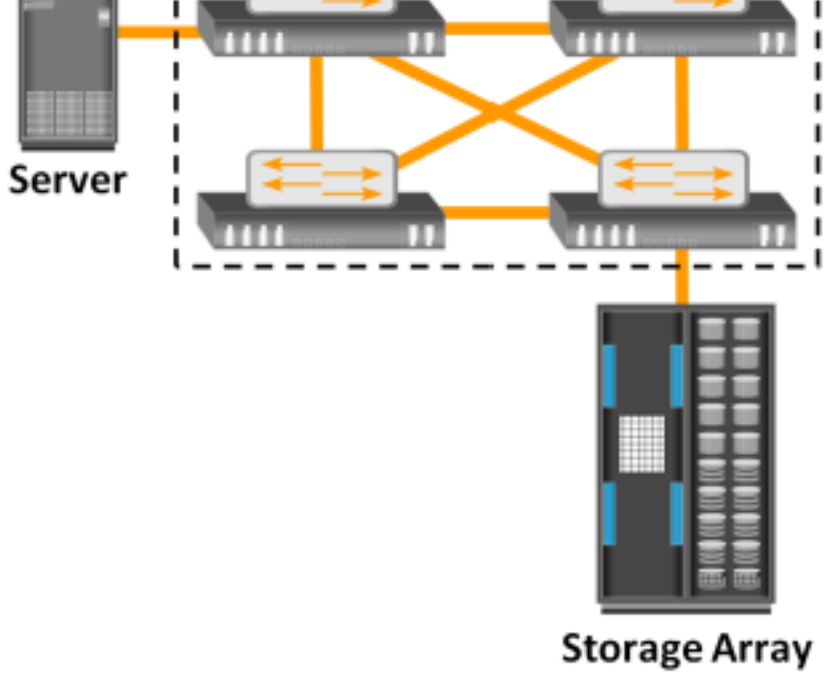
- Mesh and core-edge topologies
- Benefits of zoning
- Types of zoning

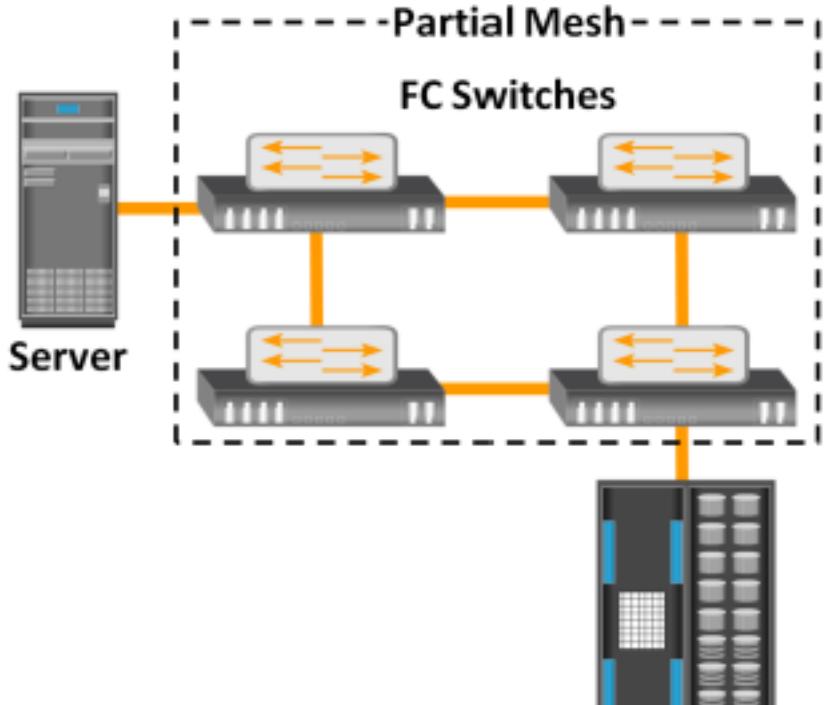
Full mesh

- Each switch is connected to every other switch
- Maximum of one ISL or hop is required for host-to-storage traffic
- Host and storage can be connected to any switch

Partial mesh

- Not all the switches are connected to every other switch





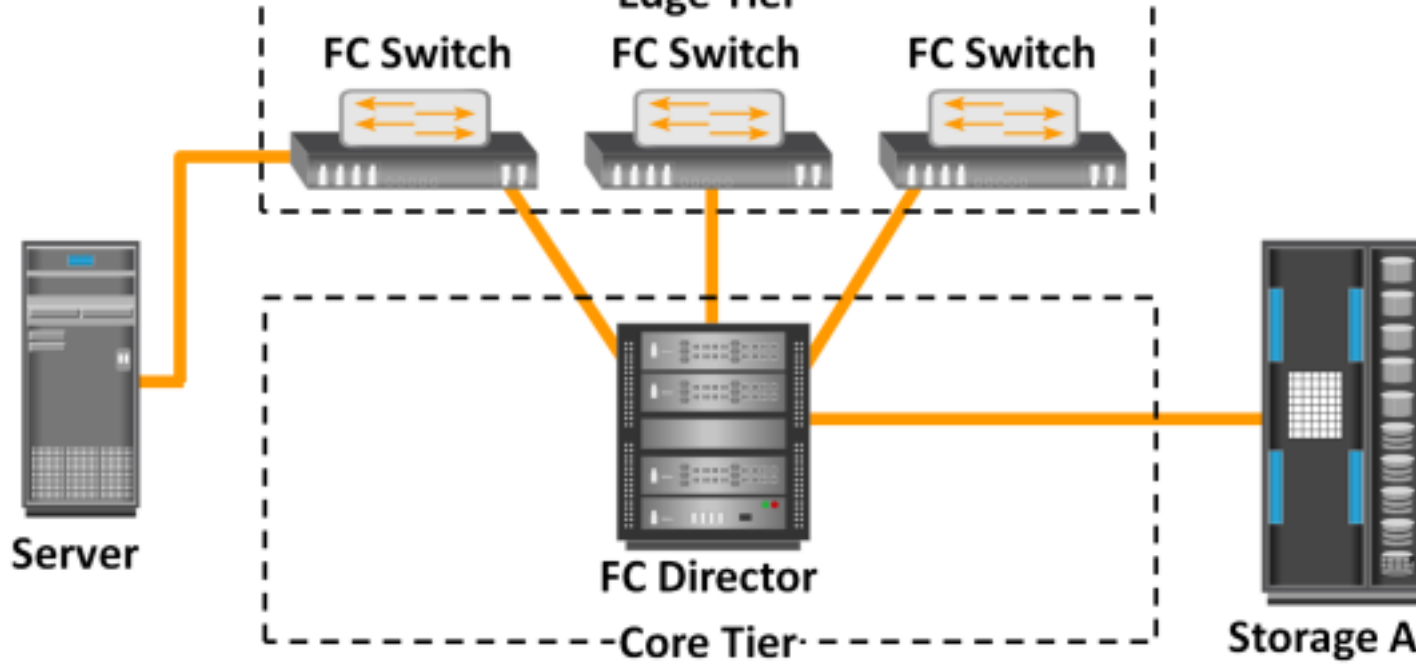
Consists of edge and core switch tiers

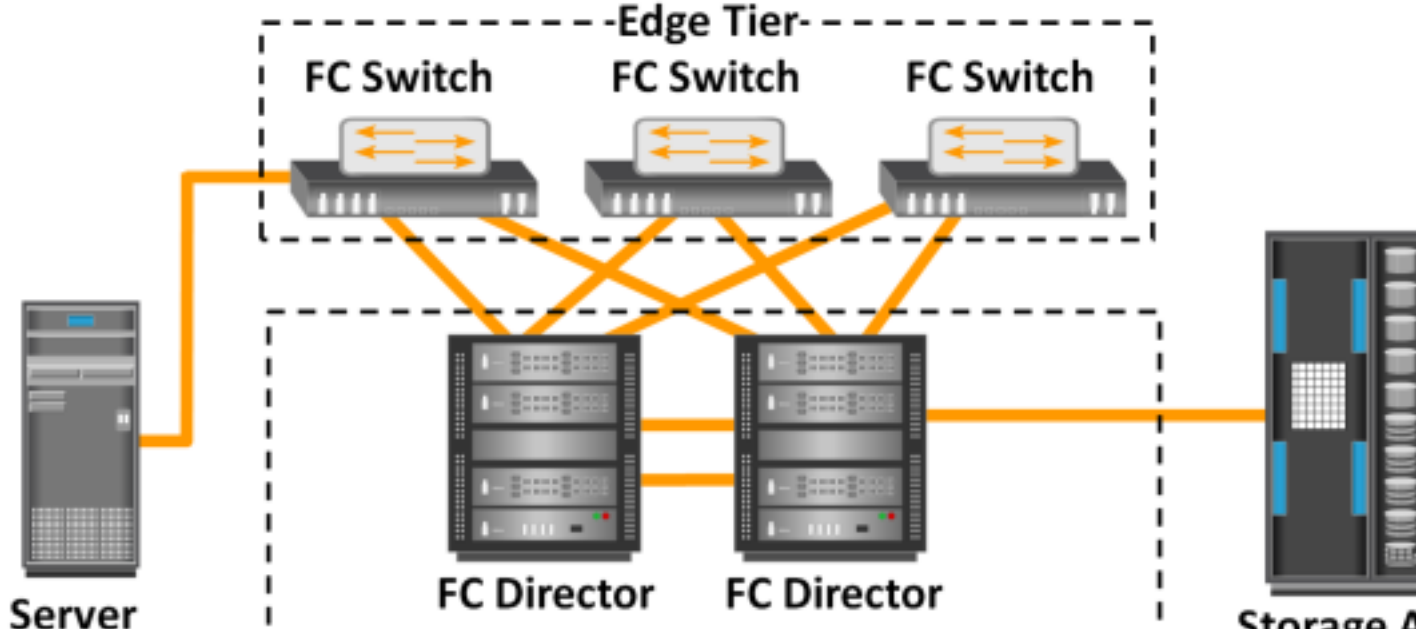
Network traffic traverses core tier or terminate at core tier

Storage is usually connected to the core tier

Benefits

- High availability
- Medium scalability
- Medium to maximum connectivity





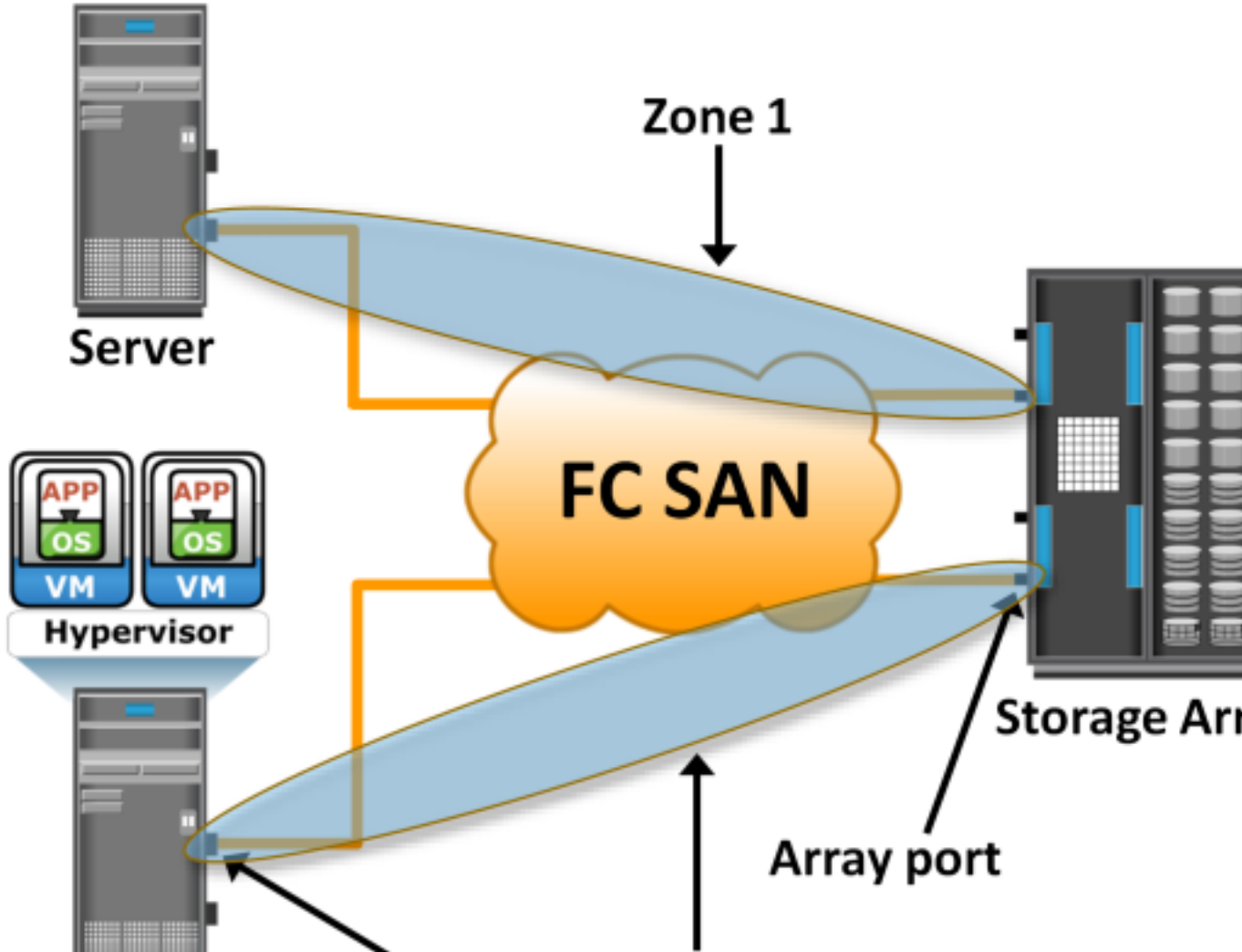
It is an FC switch function that enables node ports within the fabric to be logically segmented into groups, and communicate with each other within the group.

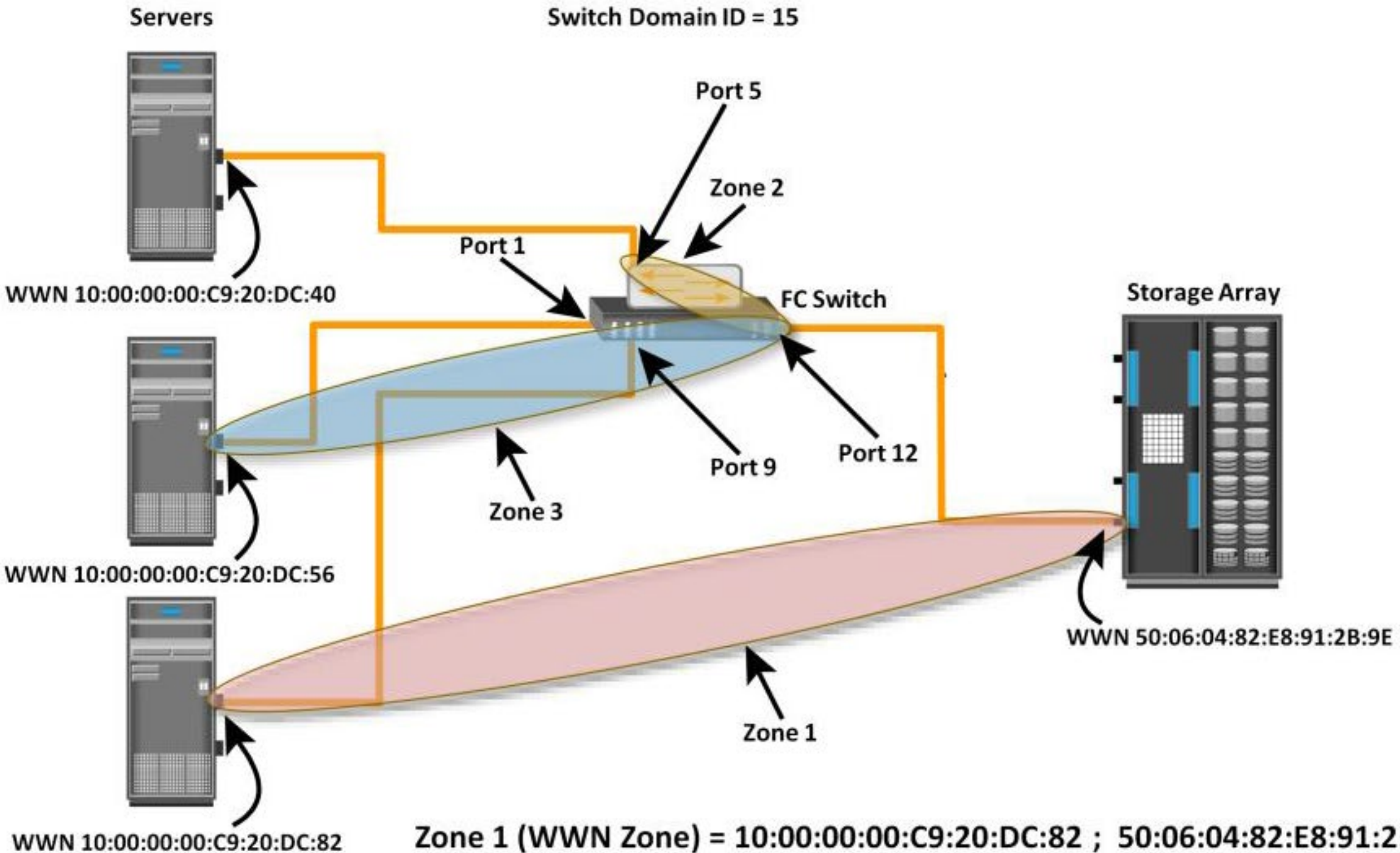
Zone set comprises zones

Each zone comprises zone members (HBA and array ports)

Benefits

- Restricts RSCN traffic
- Provides access control




Servers
Switch Domain ID = 15
Port 5
Zone 2
Port 1
FC Switch
Storage Array
WWN 10:00:00:00:C9:20:DC:40
WWN 10:00:00:00:C9:20:DC:56
WWN 10:00:00:00:C9:20:DC:82
Zone 3
Port 9
Port 12
Zone 1
WWN 50:06:04:82:E8:91:2B:9E
Zone 1 (WWN Zone) = 10:00:00:00:C9:20:DC:82 ; 50:06:04:82:E8:91:2B:9E

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

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

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

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

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

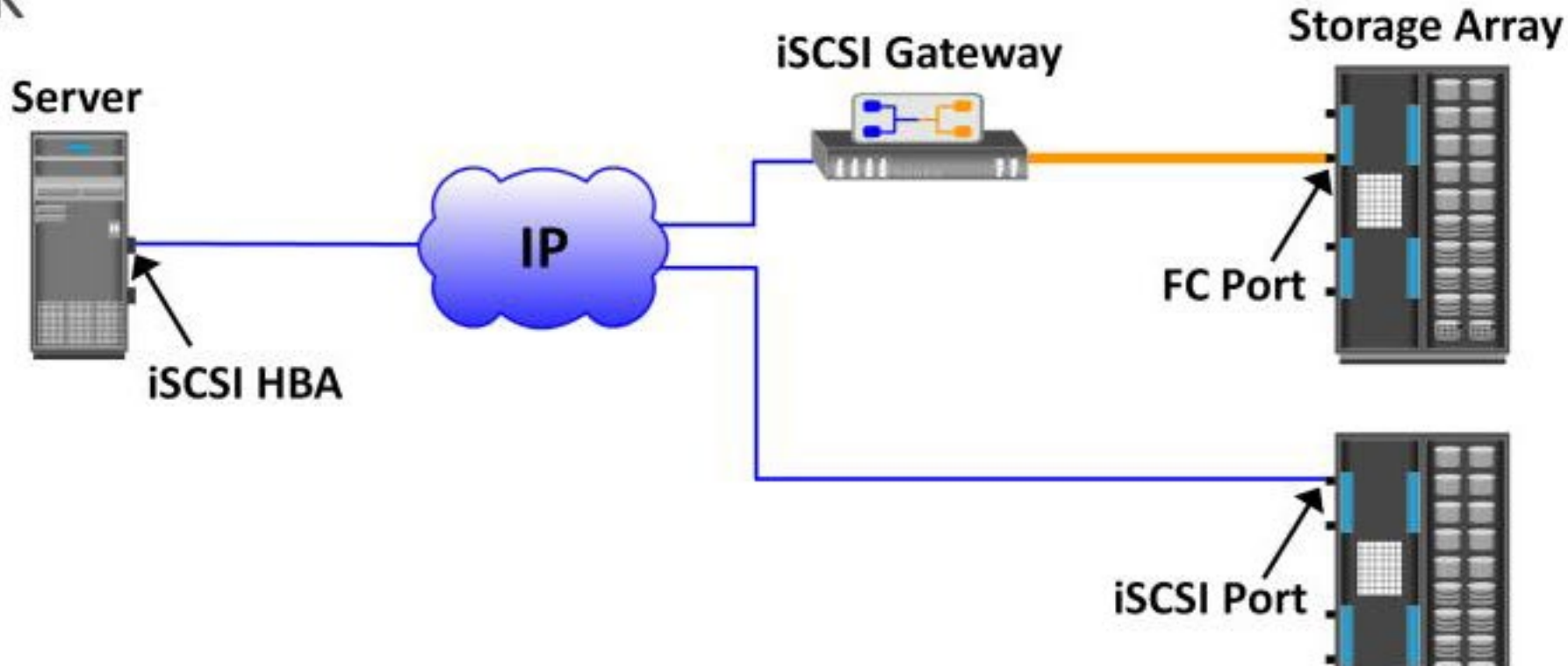
iSCSI initiator

- Example: iSCSI HBA

iSCSI target

- Storage array with iSCSI port
- iSCSI gateway – enables communication with FC storage array

IP network



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

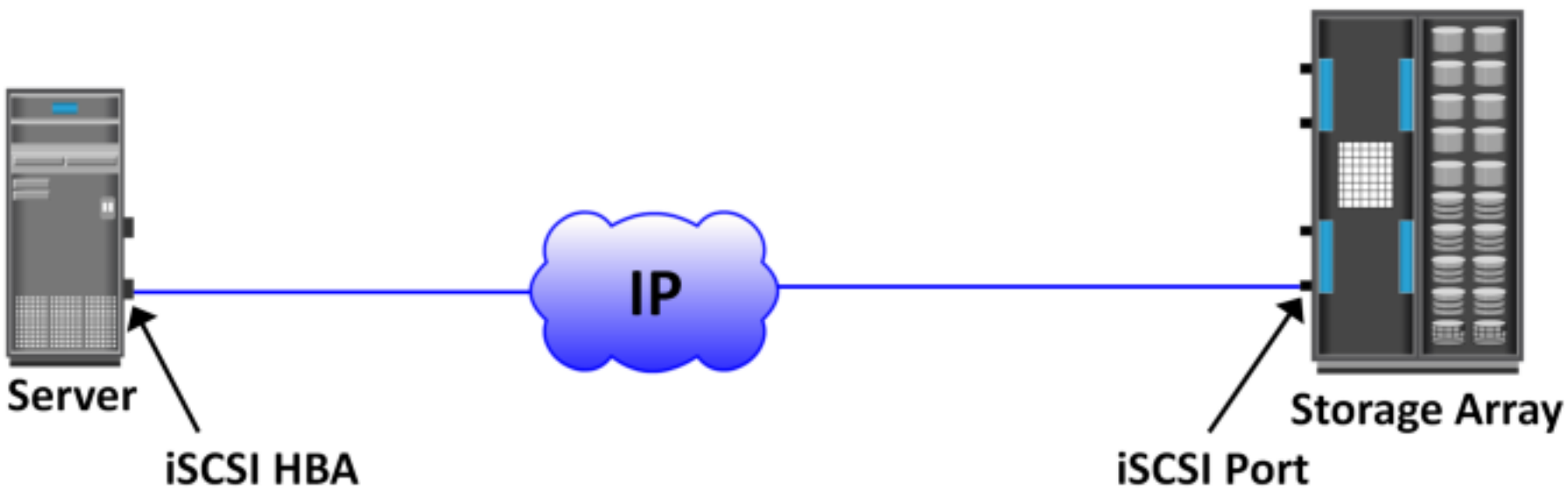
- Offloads both iSCSI and TCP/IP processing from host CPU
- Simplest option for boot from SAN

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



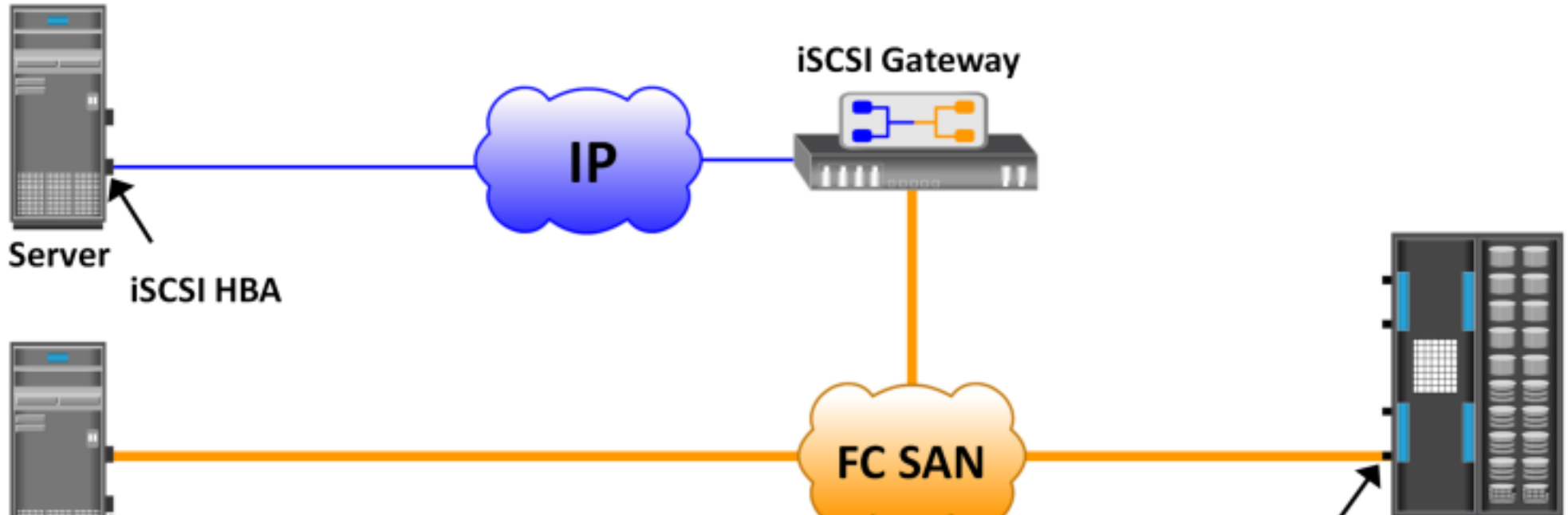
iSCSI gateway is used to enable communication between iSCSI host and FC storage

iSCSI gateway works as bridge between FC and IP network

- Converts IP packets to FC frames and vice versa

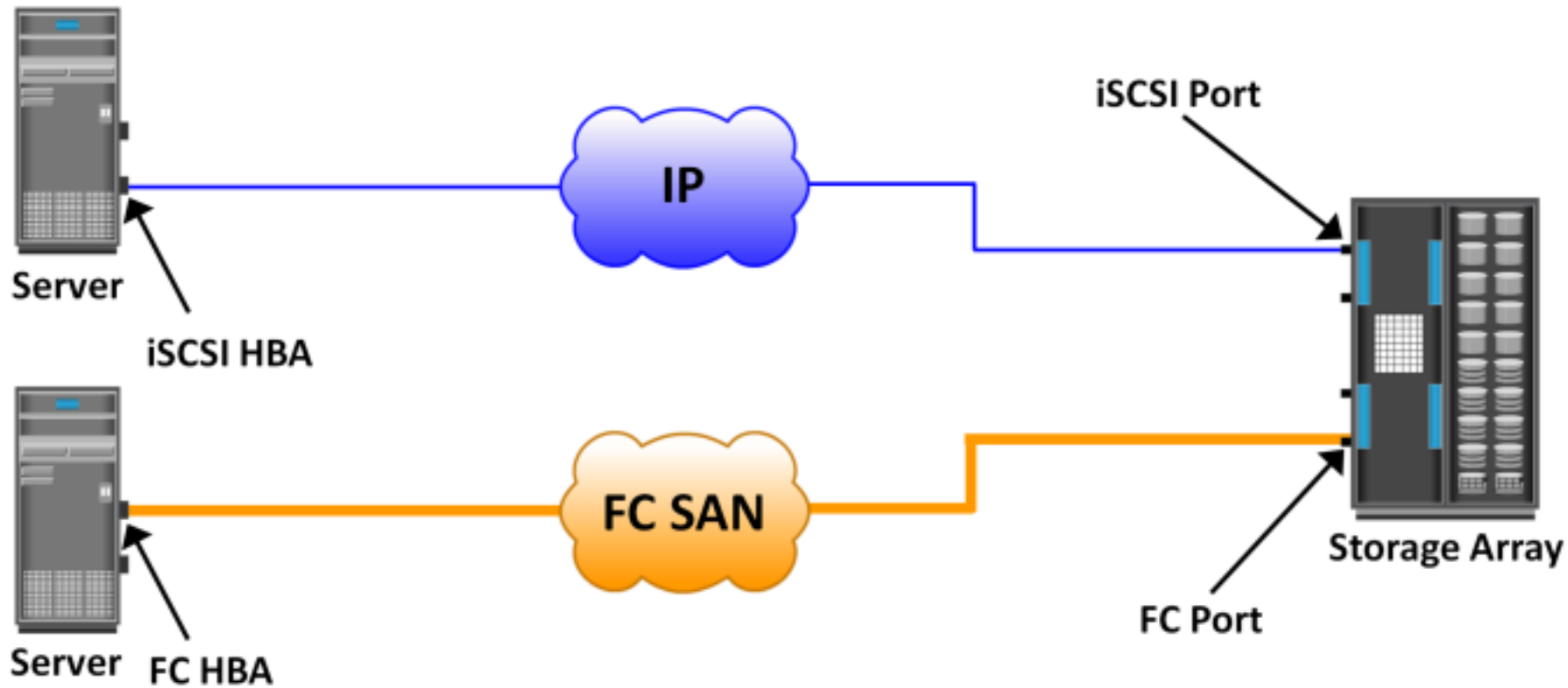
iSCSI initiator is configured with gateway's IP address as its target

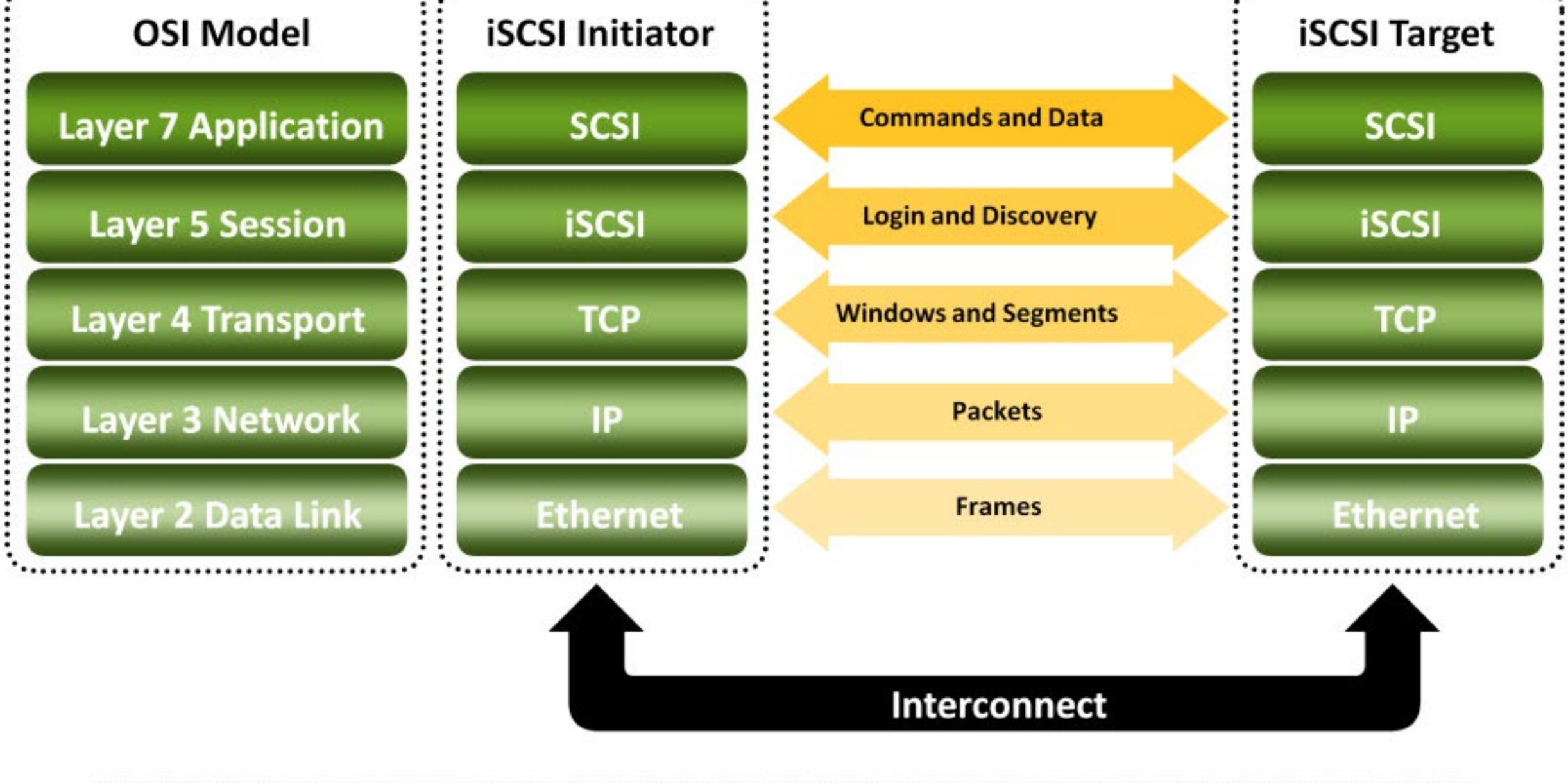
iSCSI gateway is configured as FC initiator to storage array



Array provides both FC and iSCSI ports

- Enable iSCSI and FC connectivity in the same environment
- No bridge devices needed




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


Ethernet
IP
TCP
iSCSI
SCSI
Data

- 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

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:

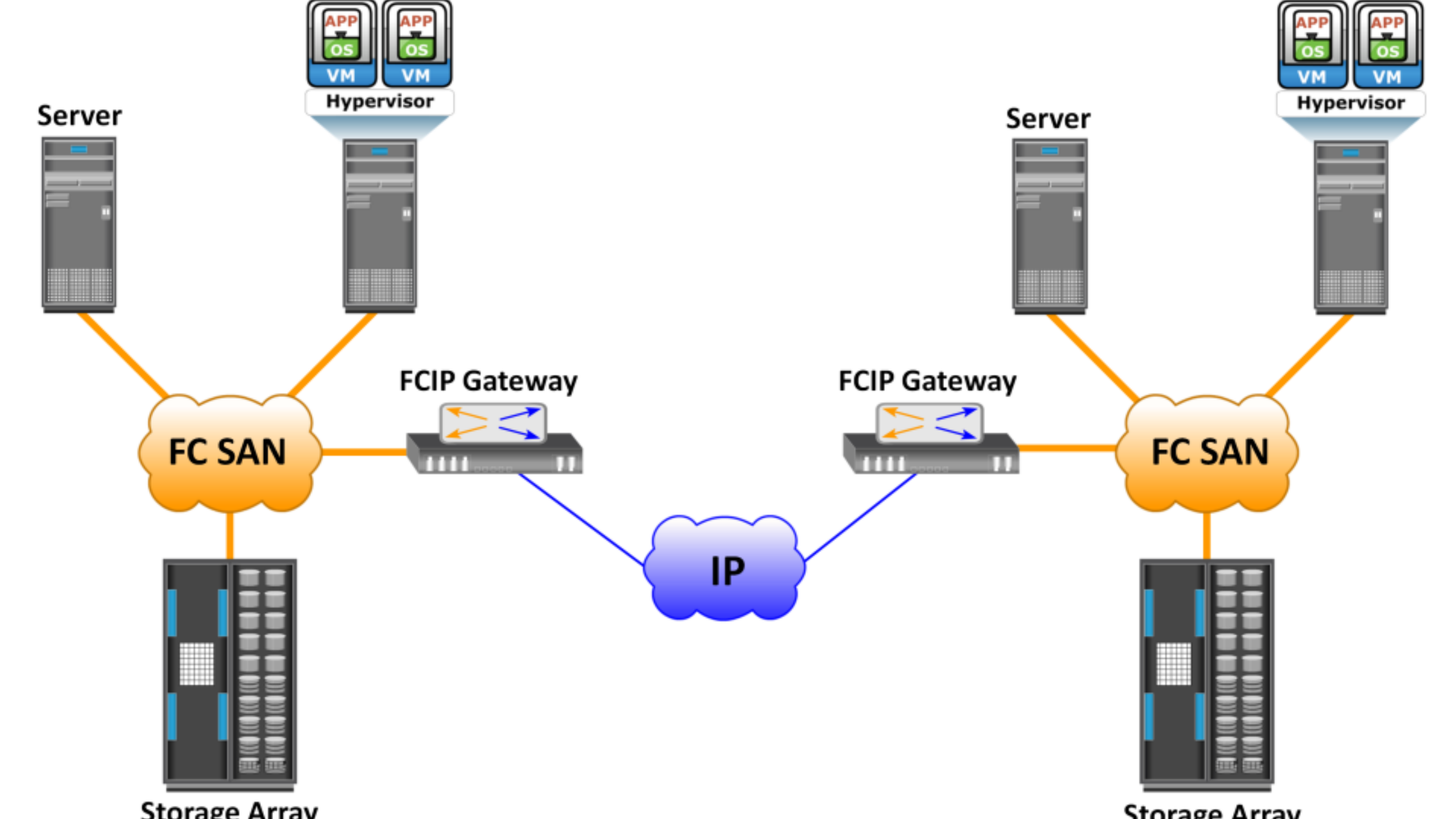
- iqn: iSCSI Qualified Name
  - iqn.2008-02.com.example:optional_string
- eui: Extended Unique Identifier
  - eui.0300732A32598D26

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


APP
OS
VM
APP
OS
VM
Hypervisor
Server
FC SAN
FCIP Gateway
IP
FCIP Gateway
Server
APP
OS
VM
APP
OS
VM
Hypervisor
FC SAN
Storage Array
Storage Array

Application

SCSI Commands, Data, and Status

FCP (SCSI over FC)

FC Frame

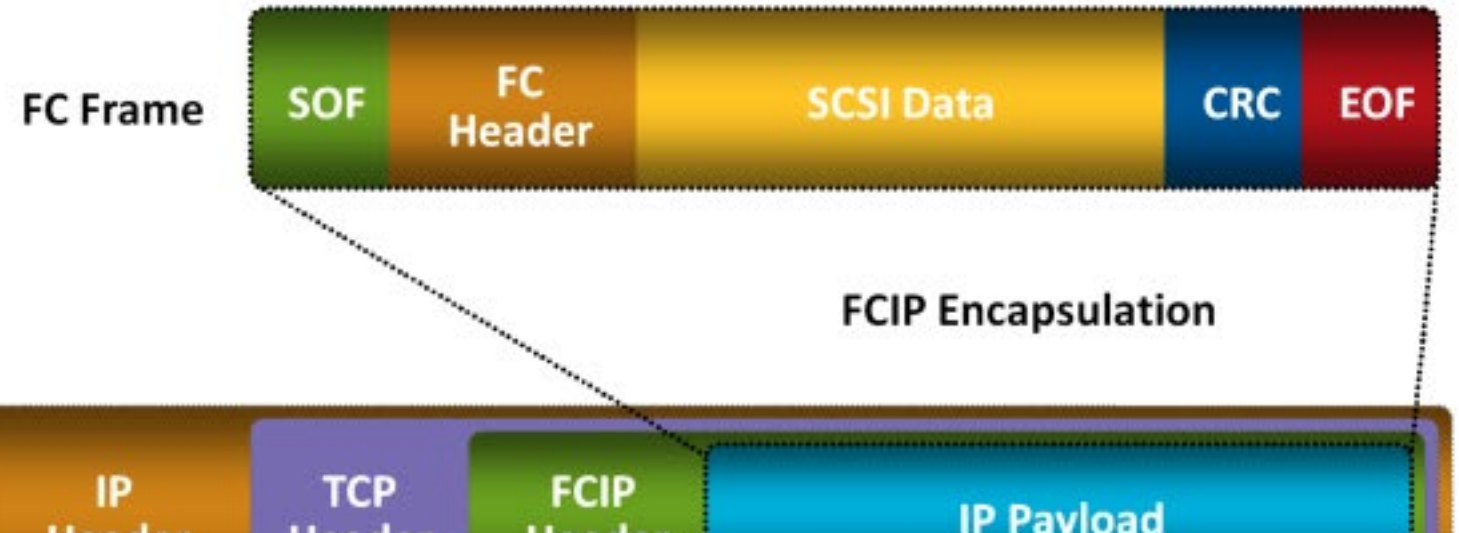
FCIP

TCP

IP

FC to IP Encapsulation

Physical Media



Network-Attached Storage (NAS

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

- Describe NAS, its benefits, and components
- Discuss NAS file-sharing protocols
- Describe different NAS implementations
- Describe file-level virtualization

Lesson 1: NAS Components and Benefits

During this lesson the following topics are covered:

- File sharing technology evolution
- Benefits of NAS
- NAS components
- NAS file sharing protocols
- NAS I/O operations

File sharing enables users to share files with other users

Creator or owner of a file determines the type of access to be given to other users

File sharing environment ensures data integrity when multiple users access a shared file at the same time

Examples of file sharing methods:

- File Transfer Protocol (FTP)
- Distributed File System (DFS)
- Network File System (NFS) and Common Internet File System (CIFS)
- Peer-to-Peer (P2P)

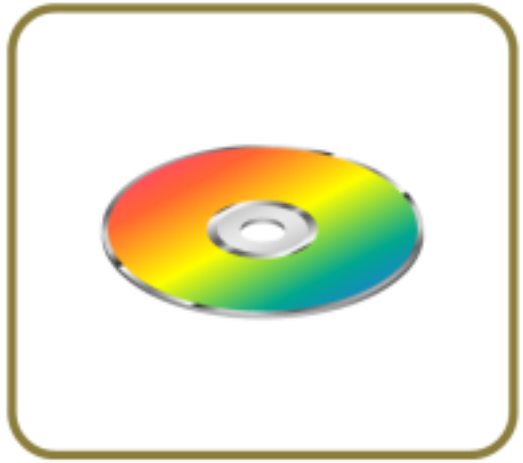
- File sharing, as the name implies, enables users to share files with other users. In a file-sharing environment, a user who creates the file (the creator or owner of a file) determines the type of access (such as read, write, execute, append, delete) to be given to other users and controls changes to the file. When multiple users try to access a shared file at the same time, a locking scheme is required to maintain data integrity and, at the same time, make this sharing possible.

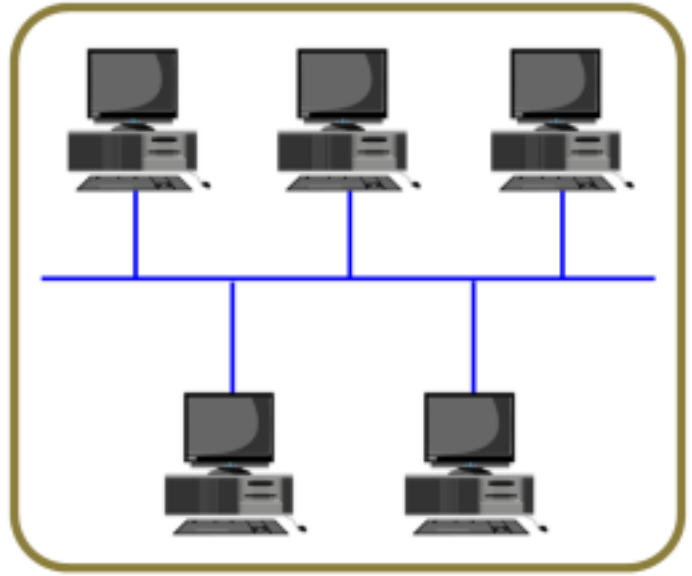
- Some examples of file-sharing methods are; File Transfer Protocol (FTP), Distributed File System (DFS), client-server models that use file-sharing protocols such as NFS and CIFS, and the peer-to-peer (P2P) model.
- FTP is a client-server protocol that enables data transfer over a network. An FTP server and an FTP client communicate with each other using TCP as the transport protocol.
- A distributed file system (DFS) is a file system that is distributed across several hosts. A DFS can provide hosts with direct access to the entire file system, while ensuring efficient management and data security.

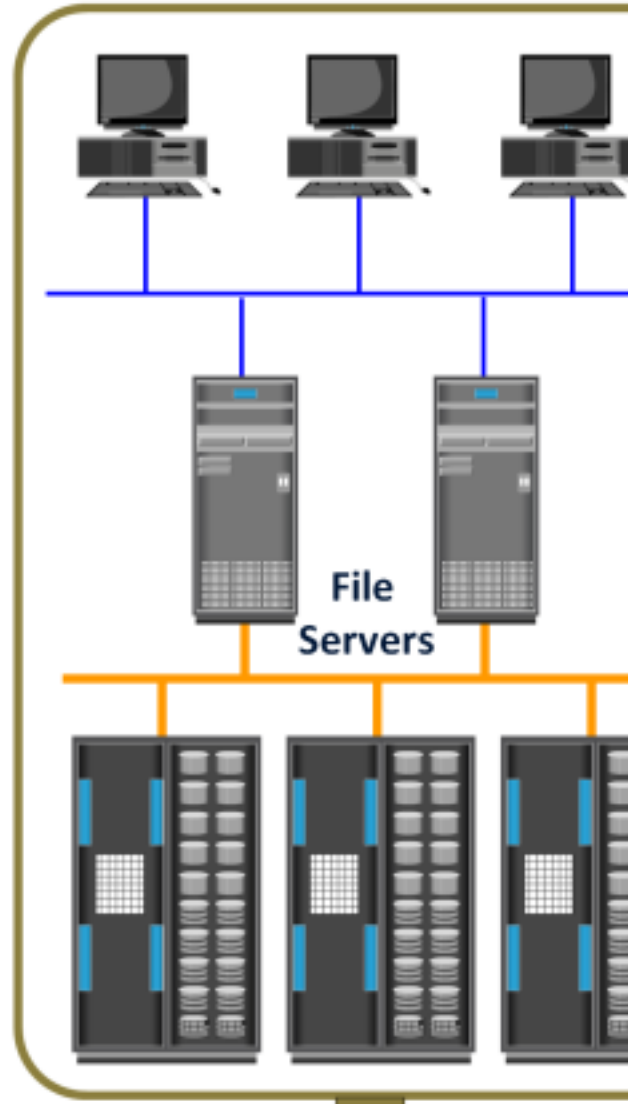
- The standard client-server file-sharing protocols, such asNFS and CIFS enable the owner of a file to set the required type of access, such as read-only or read-write, for a particular user or group of users. Using this protocol, the clients mount remote file systems that are available on dedicated file servers.
- A peer-to-peer (P2P) file sharing model uses peer-to-peer network. P2P enables client machines to directly share files with each other over a network. Clients use a file sharing software that searches for other peer clients. This differs from client-server model that uses file servers to store files for sharing.

tand Alone PC

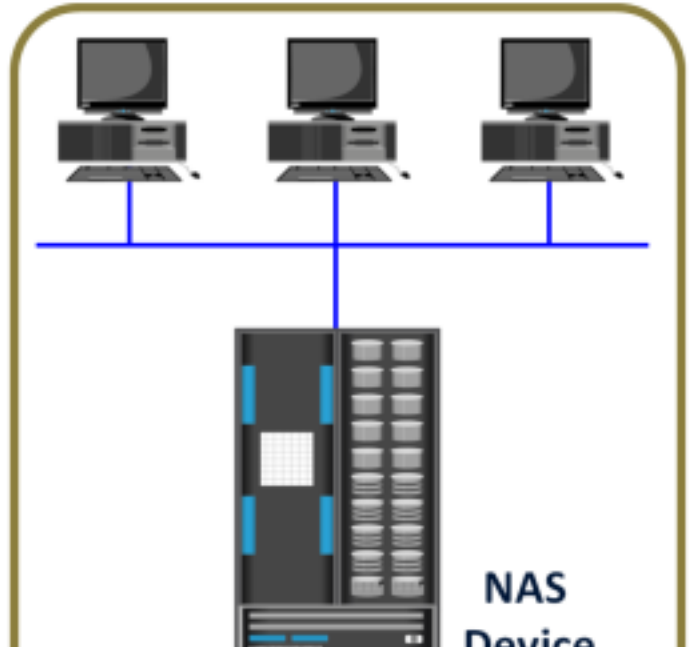
for File Sharing







File Sharing using NAS



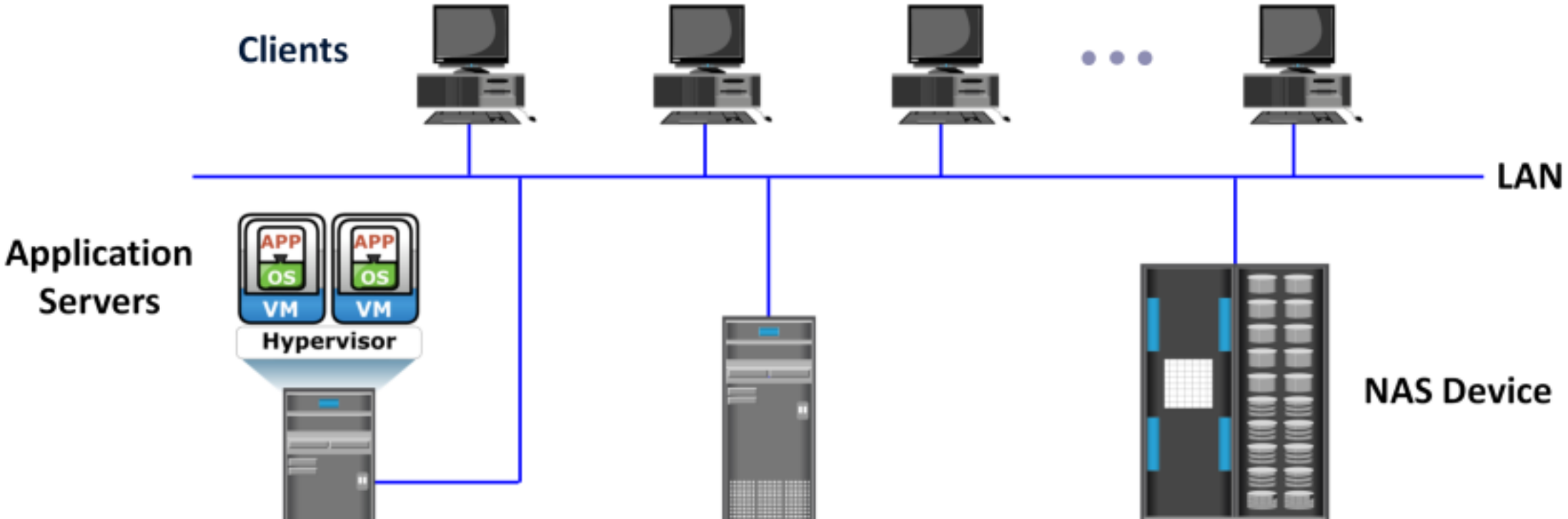
NAS

It is an IP-based, dedicated, high-performance file sharing and storage device.

Enables NAS clients to share files over IP network

Uses specialized operating system that is optimized for file I/O

Enables both UNIX and Windows users to share data

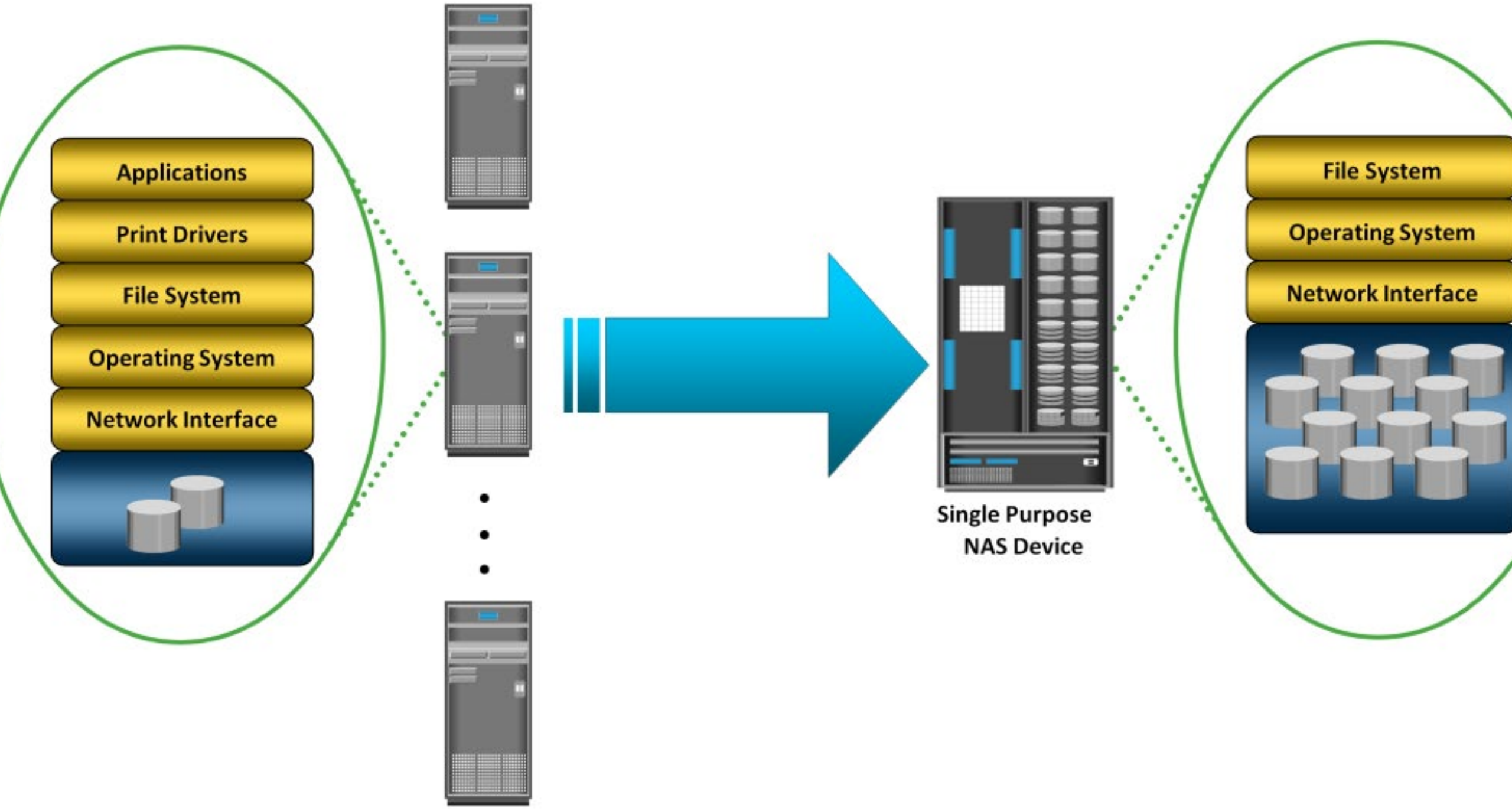


- NAS is a dedicated, high-performance file sharing and storage device. NAS enables its clients to share files over an IP network.
- NAS provides the advantages of server consolidation by eliminating the need for multiple file servers.
- It also consolidates the storage used by the clients onto a single system, making it easier to manage the storage.
- NAS uses network and file-sharing protocols to provide access to the file data. These protocols include TCP/IP for data transfer, and Common Internet File System (CIFS) and Network File System (NFS) for network file service. NAS enables both UNIX and Microsoft Windows users to share the same data seamlessly.

- A NAS device uses its own operating system and integrated hardware and software components to meet specific file-service needs.
- Its operating system is optimized for file I/O and, therefore, performs file I/O better than a general-purpose server. As a result, a NAS device can serve more clients than general-purpose servers and provide the benefit of server consolidation.

General Purpose Servers Vs. NAS Devices

- A NAS device is optimized for file-serving functions such as storing, retrieving, and accessing files for applications and clients. As shown in the slide, a general-purpose server can be used to host any application because it runs a general-purpose operating system. Unlike a general-purpose server, a NAS device is dedicated to file-serving. It has a specialized operating system dedicated to file serving by using industry standard protocols. Some NAS vendors support features, such as native clustering for high availability.


Applications
Print Drivers
File System
Operating System
Network Interface
Single Purpose
NAS Device
File System
Operating System
Network Interface

Improved efficiency

Improved flexibility

Centralized storage

Simplified management

Scalability

High availability – through native clustering and replication

Security – authentication, authorization, and file locking in conjunction with industry-standard security

Low cost

Ease of deployment

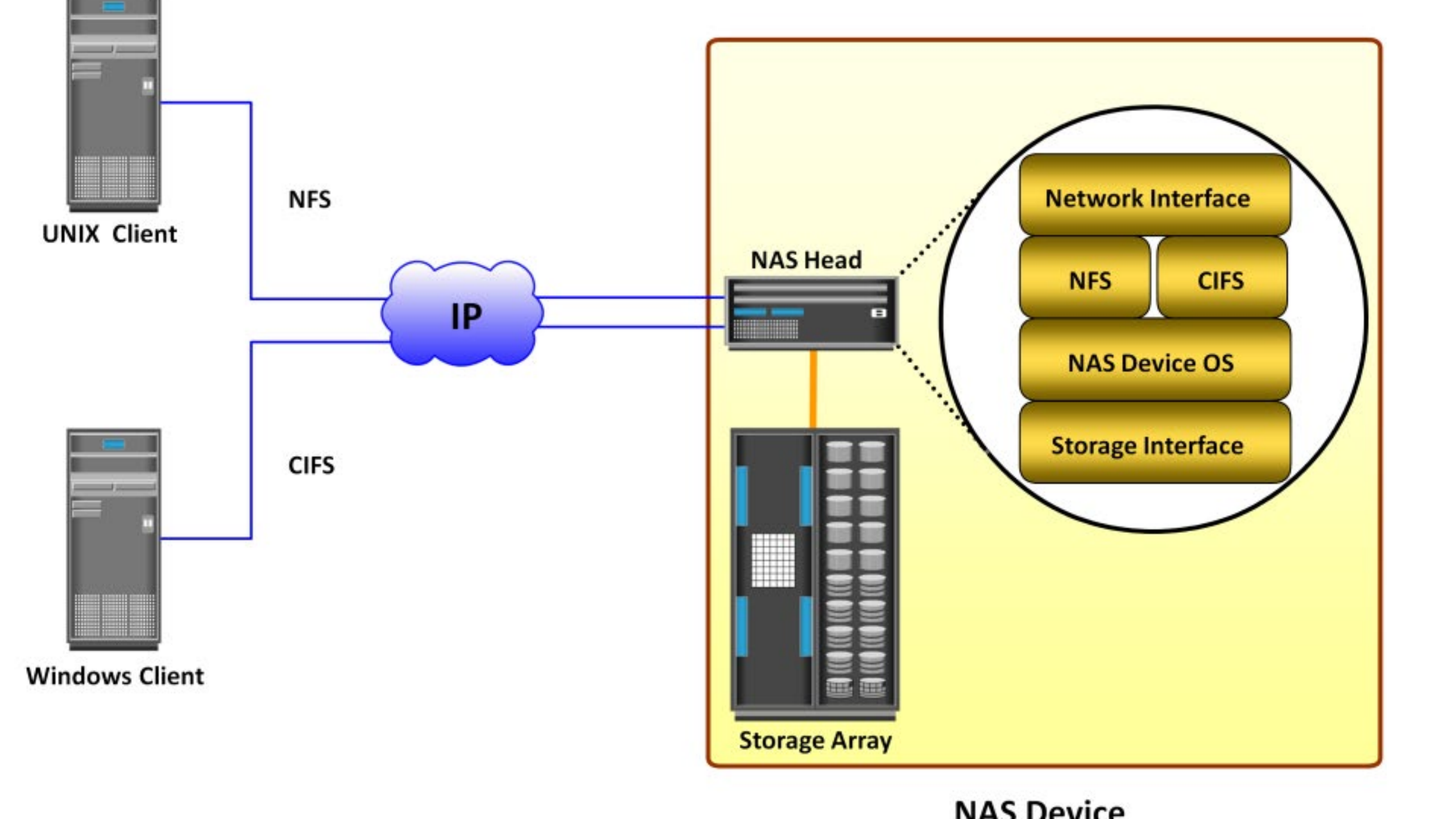
NAS offers the following benefits:

- **Improved efficiency:** NAS delivers better performance compared to a general-purpose file server because NAS uses an operating system specialized for file serving.
- **Improved flexibility:** Compatible with clients on both UNIX and Windows platforms using industry-standard protocols. NAS is flexible and can serve requests from different types of clients from the same source.
- **Centralized storage:** Centralizes data storage to minimize data duplication on client workstations, and ensure greater data protection.
- **Simplified management:** Provides a centralized console that makes it possible to manage file systems efficiently.

- **Scalability:** Scales well with different utilization profiles and types of business applications because of the high-performance and low-latency design.
- **High availability:** Offers efficient replication and recovery options, enabling high data availability. NAS uses redundant components that provide maximum connectivity options. A NAS device supports clustering technology for failover.
- **Security:** Ensures security, user authentication, and file locking with industry-standard security schemas.
- **Low cost**: NAS uses commonly available, and inexpensive Ethernet components
- **Ease of deployment:** Configuration at the client is minimal, because the clients have required NAS connection software built in.

A NAS device has two key components: NAS head and storage. In some NAS implementations, the storage could be external to the NAS device and shared with other hosts. The NAS head includes the following components:

- CPU and memory
- One or more network interface cards (NICs), which provide connectivity to the client network. Examples of network protocols supported by NIC include Gigabit Ethernet, Fast Ethernet, ATM, and Fiber Distributed Data Interface (FDDI)
- An optimized operating system for managing the NAS functionality. It translates file-level requests into block-storage requests and further converts the data supplied at the block level to file data
- NFS, CIFS, and other protocols for file sharing
- Industry-standard storage protocols and ports to connect and manage physical disk resources


UNIX Client
NFS
IP
NAS Head
Network Interface
NFS
CIFS
NAS Device OS
Storage Interface
CIFS
Windows Client
Storage Array

NAS Device

- Two common NAS file sharing protocols are:
  - Common Internet File System (CIFS)
  - Network File System (NFS)

- Most NAS devices support multiple file-service protocols to handle file I/O requests to a remote file system. As discussed earlier, NFS and CIFS are the common protocols for file sharing. NAS devices enable users to share file data across different operating environments and provide a means for users to migrate transparently from one operating system to another.

- **Common Internet File System (CIFS) is a client-server application protocol that enables client programs to make requests for files and services on remote computers over TCP/IP. It is a public, or open, variation of Server Message Block (SMB) protocol.**
- **The CIFS protocol enables remote clients to gain access to files on a server. CIFS enables file sharing with other clients by using special locks. Filenames in CIFS are encoded using Unicode characters. CIFS provides the following features to ensure data integrity:**
- **It uses file and record locking to prevent users from overwriting the work of another user on a file or a record.**

- It supports fault tolerance and can automatically restore connections and reopen files that were open prior to an interruption. The fault tolerance features of CIFS depend on whether an application is written to take advantage of these features. Moreover, CIFS is a stateful protocol because the CIFS server maintains connection information regarding every connected client. If a network failure or CIFS server failure occurs, the client receives a disconnection notification. User disruption is minimized if the application has the embedded intelligence to restore the connection. However, if the embedded intelligence is missing, the user must take steps to reestablish the CIFS connection.

Client-server application protocol

- An open variation of the Server Message Block (SMB) protocol

Enables clients to access files that are on a server over TCP/IP

Stateful Protocol

- Maintains connection information regarding every connected client
- Can automatically restore connections and reopen files that were open prior to interruption

Client-server application protocol

- An open variation of the Server Message Block (SMB) protocol

Enables clients to access files that are on a server over TCP/IP

Stateful Protocol

- Maintains connection information regarding every connected client
- Can automatically restore connections and reopen files that were open prior to interruption

Network File System (NFS) is a client-server protocol for file sharing that is commonly used on UNIX systems. NFS was originally based on the connectionless User Datagram Protocol (UDP). It uses a machine-independent model to represent user data. It also uses Remote Procedure Call (RPC) as a method of inter-process communication between two computers. The NFS protocol provides a set of RPCs to access a remote file system for the following operations:

- Searching files and directories
- Opening, reading, writing to, and closing a file
- Changing file attributes
- Modifying file links and directories

Client-server application protocol

Enables clients to access files that are on a server

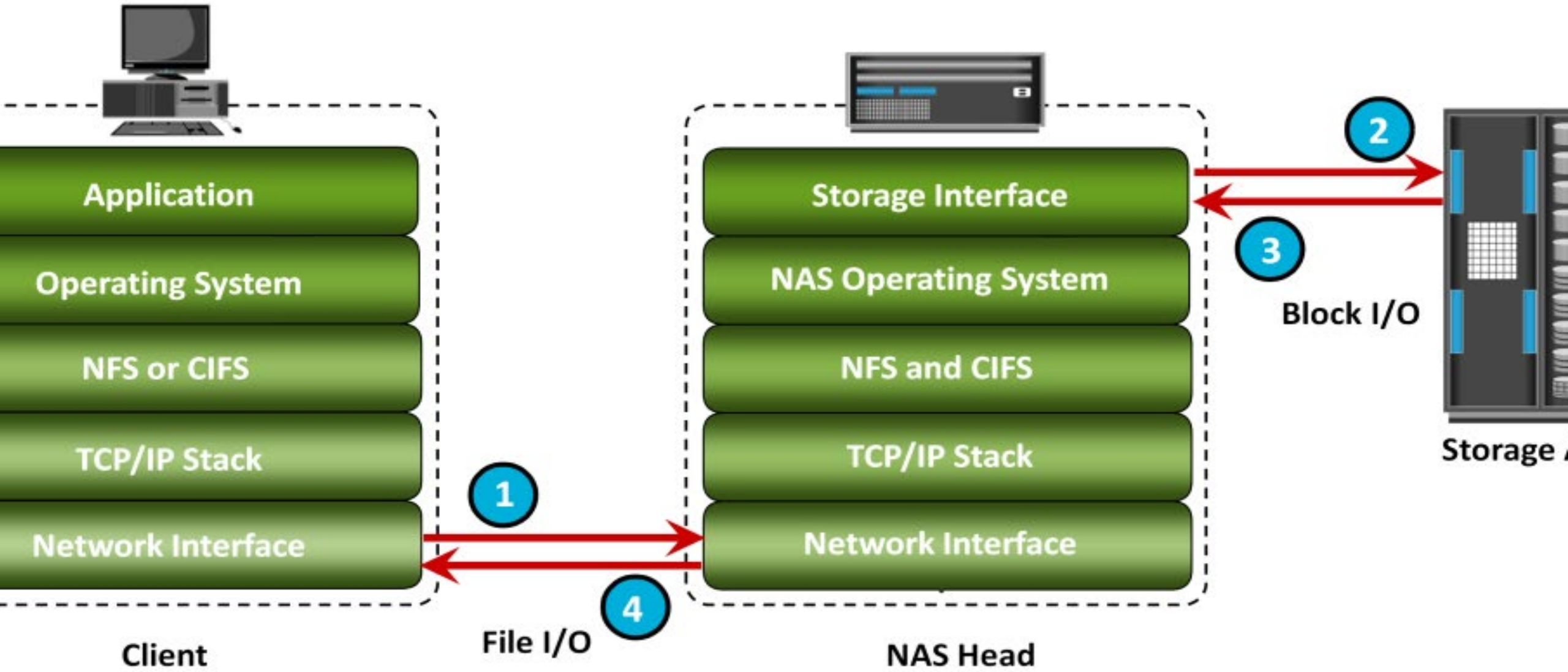
Uses Remote Procedure Call (RPC) mechanism to provide access to remote file system

Currently, three versions of NFS are in use:

- NFS v2 is stateless and uses UDP as transport layer protocol
- NFS v3 is stateless and uses UDP or optionally TCP as transport layer protocol
- NFS v4 is stateful and uses TCP as transport layer protocol

NAS provides file-level data access to its clients. File I/O is a high-level request that specifies the file to be accessed. For example, a client may request a file by specifying its name, location, or other attributes. The NAS operating system keeps track of the location of files on the disk volume and converts client file I/O into block-level I/O to retrieve data. The process of handling I/Os in a NAS environment is as follows:

1. The requestor (client) packages an I/O request into TCP/IP and forwards it through the network stack. The NAS device receives this request from the network.
2. The NAS device converts the I/O request into an appropriate physical storage request, which is a block-level I/O, and then performs the operation on the physical storage.
3. When the NAS device receives data from the storage, it processes and repackages the data into an appropriate file protocol response.
4. The NAS device packages this response into TCP/IP again and forwards it to the client through the network.


Application
Operating System
NFS or CIFS
TCP/IP Stack
Network Interface
Client
1
File I/O
4
Storage Interface
NAS Operating System
NFS and CIFS
TCP/IP Stack
Network Interface
NAS Head
2
3
Block I/O
Storage

Lesson 2: NAS Implementation and File-level Virtualization

During this lesson the following topics are covered:

- NAS implementations
- NAS use cases
- File-level virtualization

NAS Implementations

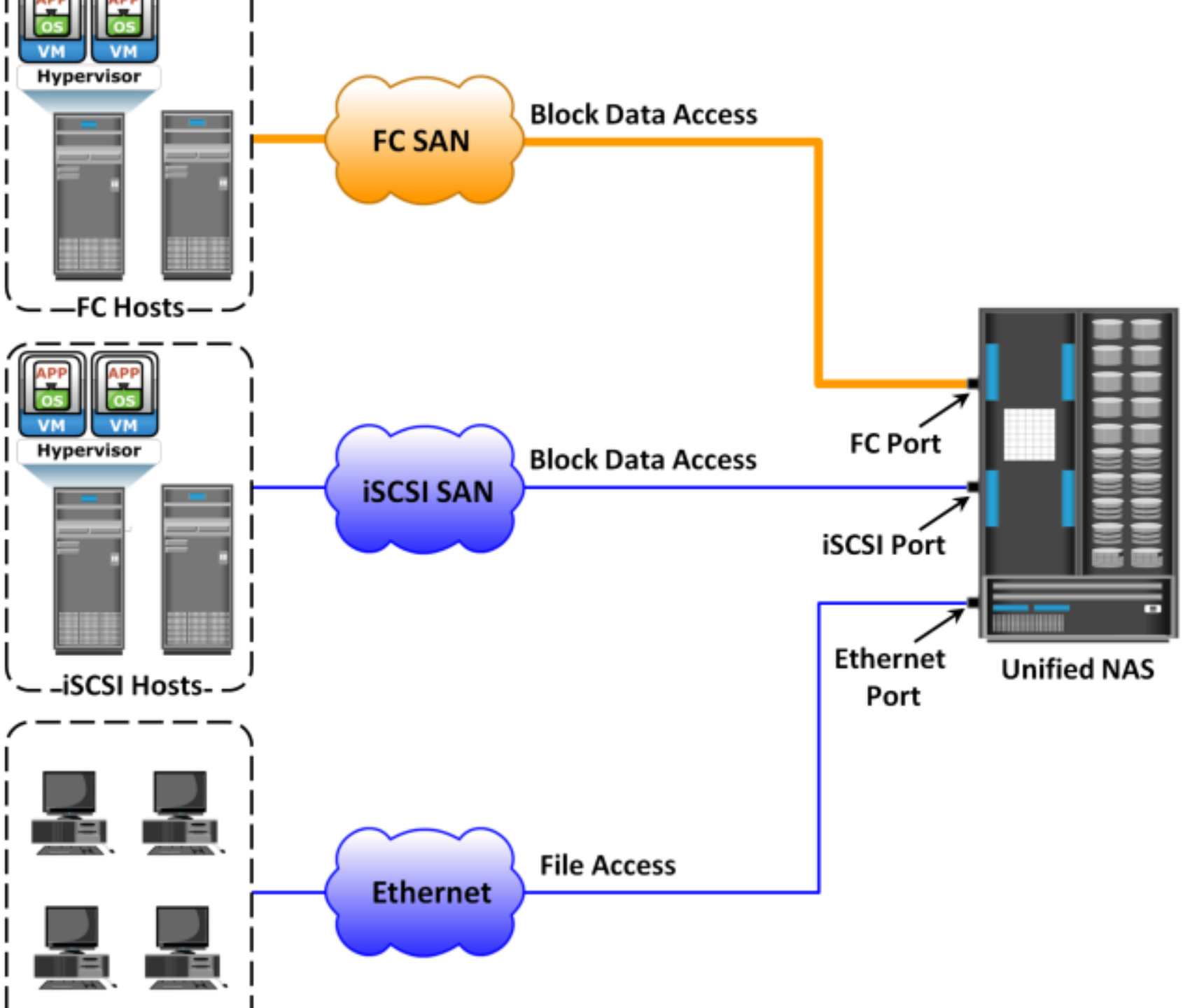
- Three common NAS implementations are unified, gateway, and scale-out. The *unified* NAS consolidates NAS-based and SAN-based data access within a unified storage platform and provides a unified management interface for managing both the environments.

- In a gateway implementation, the NAS device uses external storage to store and retrieve data, and unlike unified storage, there are separate administrative tasks for the NAS device and storage.
- The scale-out NAS implementation pools multiple nodes together in a cluster. A node may consist of either the NAS head or storage or both. The cluster performs the NAS operation as a single entity.

- Consolidates NAS-based (file-level) and SAN-based (block-level) access on a single storage platform
- Supports both CIFS and NFS protocols for file access and iSCSI and FC protocols for block level access
- Provides unified management for both NAS head and storage

Unified NAS

- Unified NAS performs file serving and storing of file data, along with providing access to block-level data. It supports both CIFS and NFS protocols for file access and iSCSI and FC protocols for block level access. **Due to consolidation of NAS-based and SAN-based access on a single storage platform, unified NAS reduces an organization's infrastructure and management costs.**


APP
OS
VM
Hypervisor
FC Hosts
FC SAN
Block Data Access
iSCSI Hosts
iSCSI SAN
Block Data Access
Ethernet
File Access
FC Port
iSCSI Port
Ethernet Port
Unified NAS

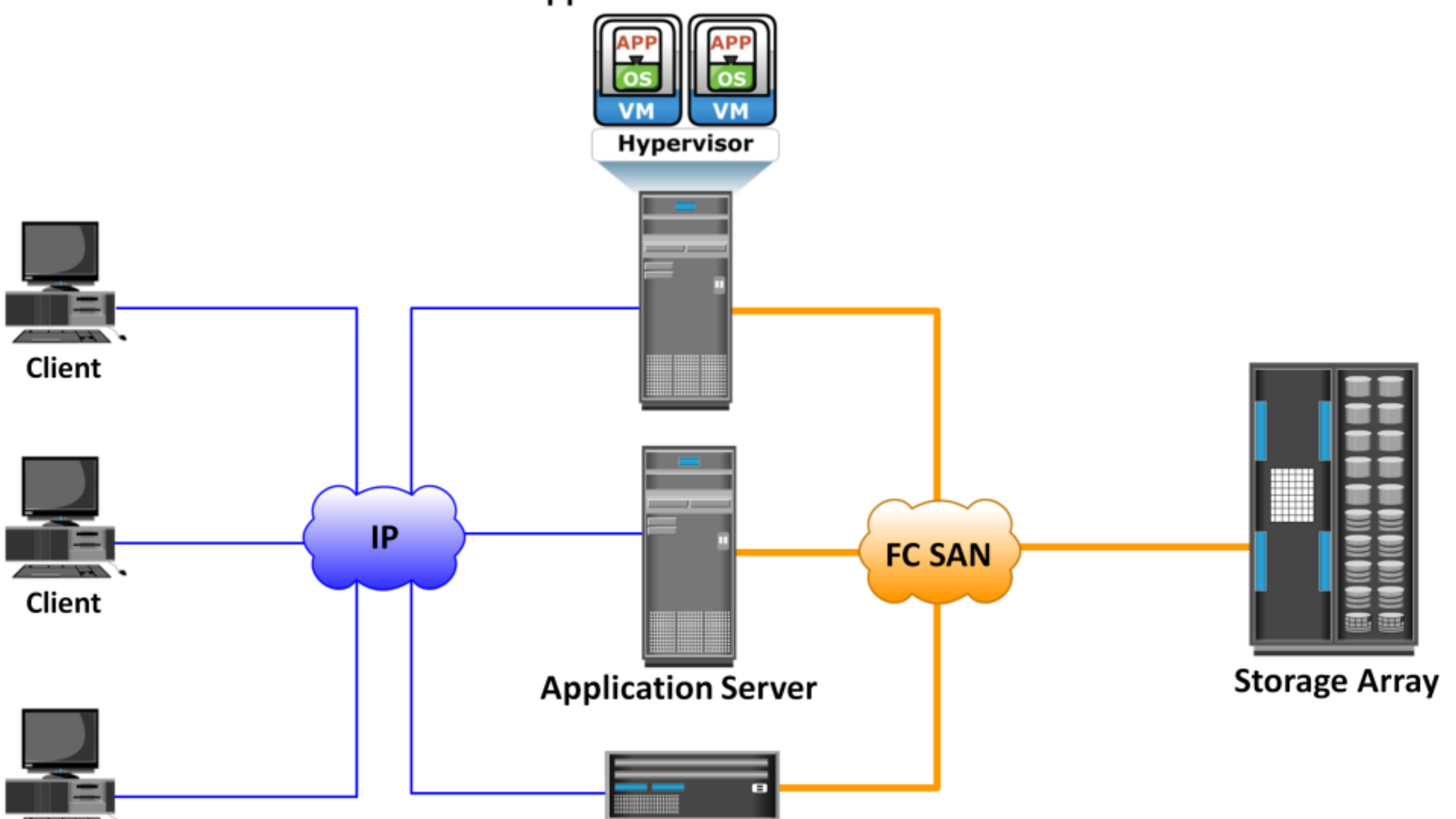
Uses external and independently-managed storage

- NAS heads access SAN-attached or direct-attached storage arrays

NAS heads share storage with other application servers that perform block I/O

Requires separate management of NAS head and storage

- In a gateway solution, the front-end connectivity is similar to that in a unified storage solution. Communication between the NAS gateway and the storage system in a gateway solution is achieved through a traditional FC SAN To deploy a gateway NAS solution, factors, such as **multiple paths for data, redundant fabrics, and load distribution, must be considered**


APP
OS
VM
APP
OS
VM
Hypervisor
Client
Client
IP
FC SAN
Application Server
Storage Array

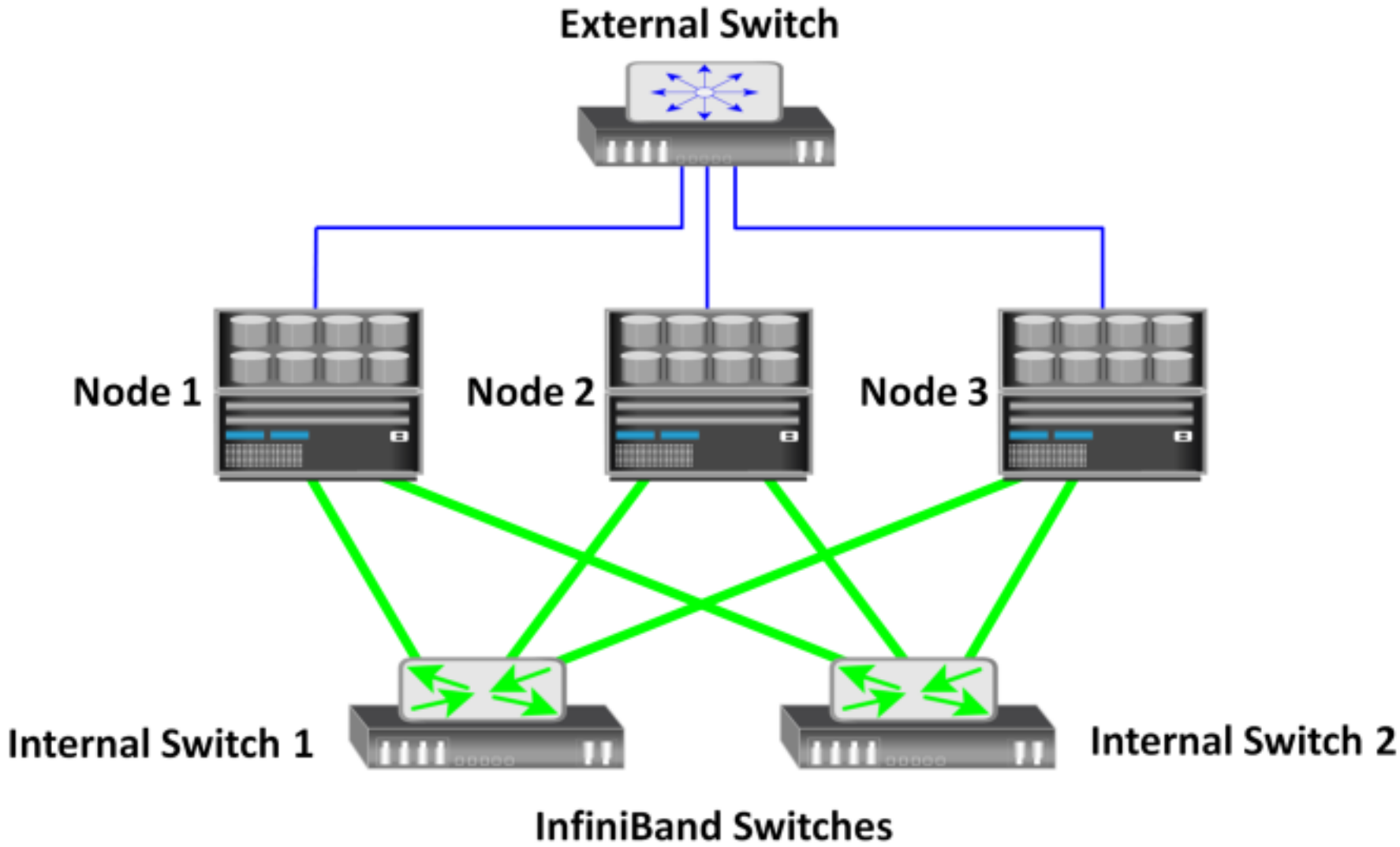
Pools multiple nodes together in a cluster that works as a single NAS device

- Pool is managed centrally

- Scales performance and/or capacity with addition of nodes to the pool non-disruptively
- Creates a single file system that runs on all nodes in the cluster
  - Clients, connected to any node, can access entire file system
  - File system grows dynamically as nodes are added
- Stripes data across all nodes in a pool along with mirror or parity protection

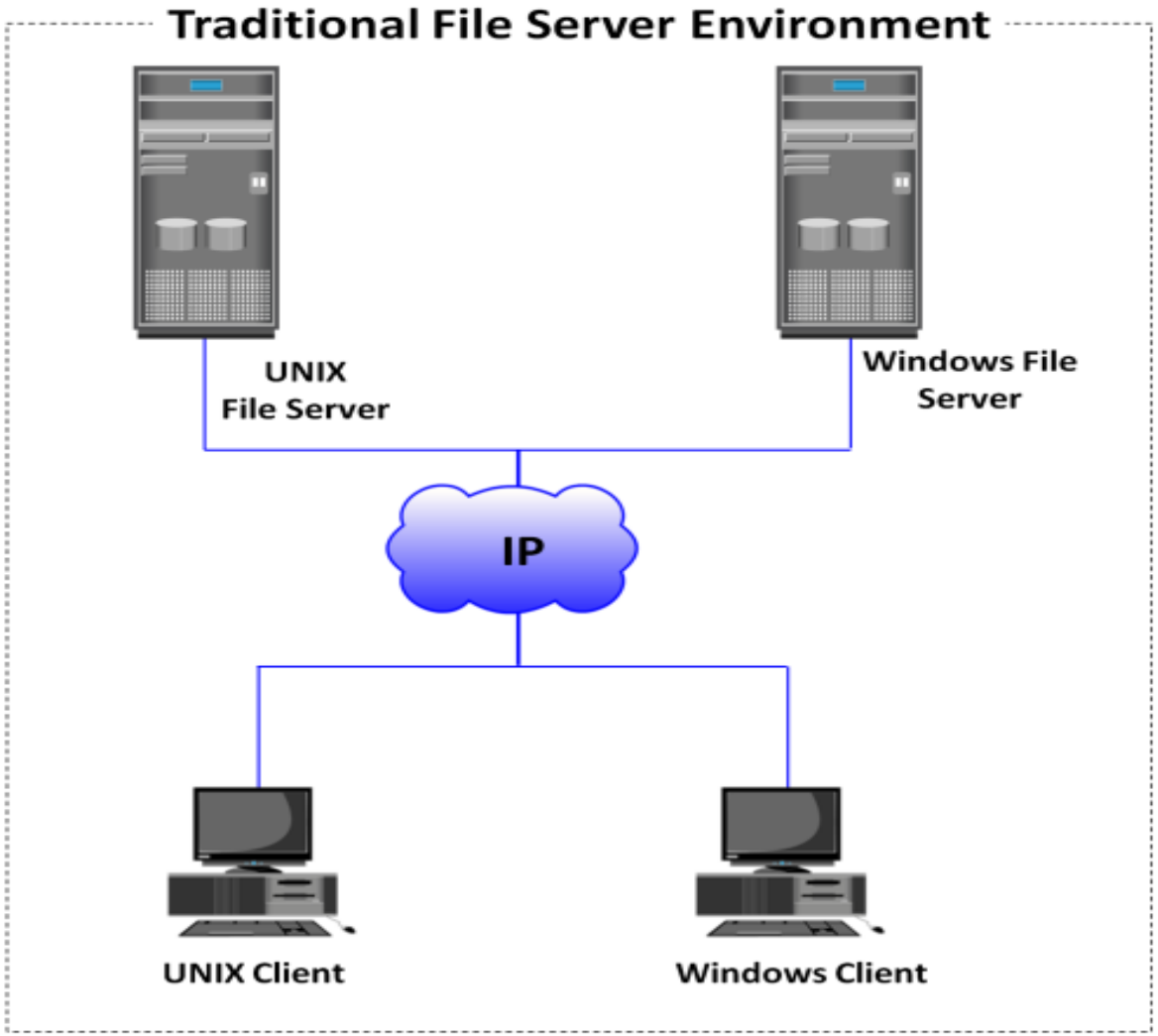
- The scale-out NAS implementation pools multiple nodes together in a cluster. A node may consist of either the NAS head or storage or both. The cluster performs the NAS operation as a single entity.
- A scale-out NAS provides the capability to scale its resources by simply adding nodes to a clustered NAS architecture. The cluster works as a single NAS device and is managed centrally. Nodes can be added to the cluster, when more performance or more capacity is needed, without causing any downtime. Scale-out NAS provides the flexibility to use many nodes of moderate performance and availability characteristics to produce a total system that has better aggregate performance and availability. It also provides ease of use, low cost, and theoretically unlimited scalability.

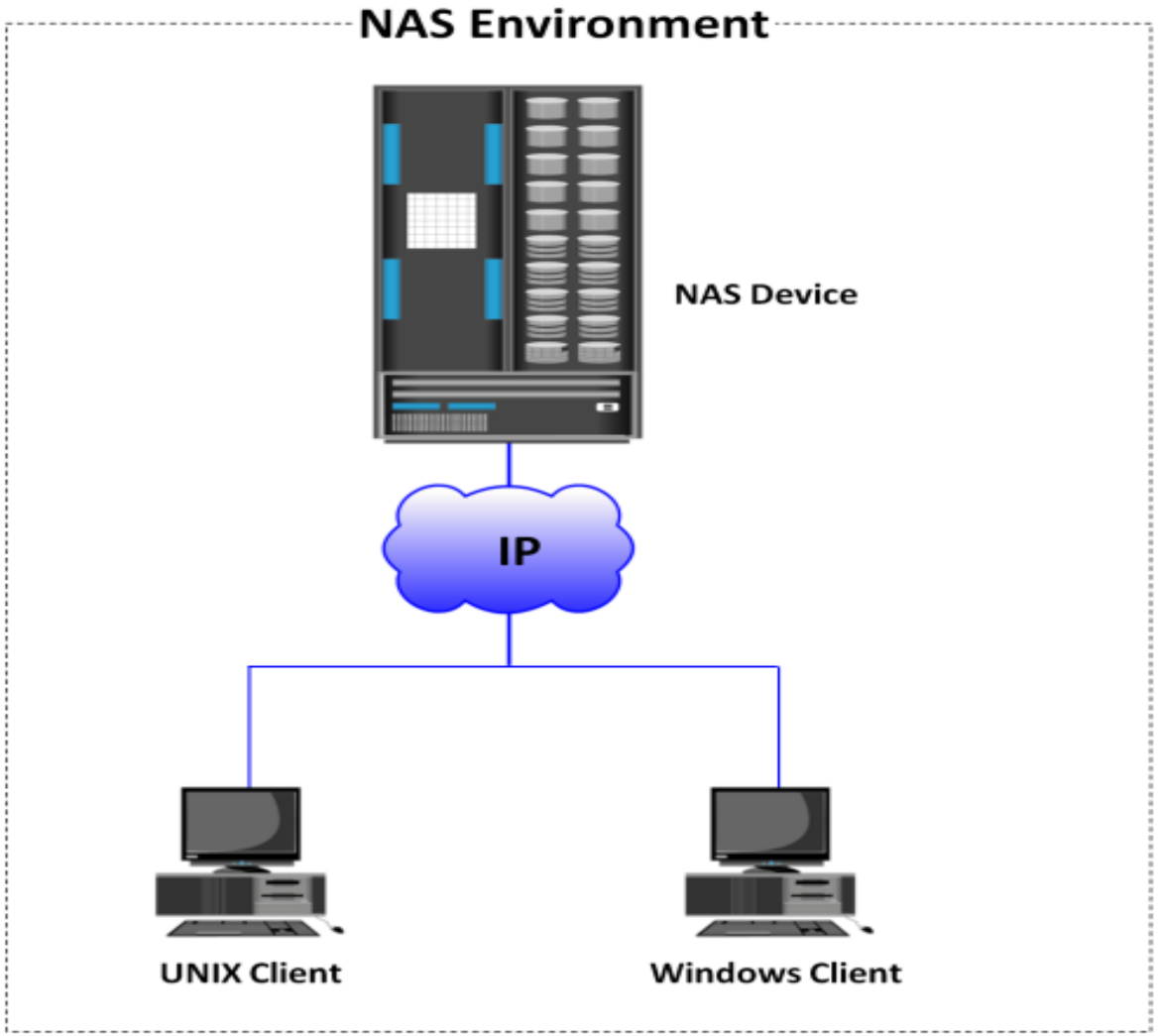
- Scale-out NAS creates a single file system that runs on all nodes in the cluster. All information is shared among nodes, so the entire file system is accessible by clients connecting to any node in the cluster. Scale-out NAS stripes data across all nodes in a cluster along with mirror or parity protection. As data is sent from clients to the cluster, the data is divided and allocated to different nodes in parallel. When a client sends a request to read a file, the scale-out NAS retrieves the appropriate blocks from multiple nodes, recombines the blocks into a file, and presents the file to the client. As nodes are added, the file system grows dynamically and data is evenly distributed to every node. Each node added to the cluster increases the aggregate storage, memory, CPU, and network capacity. Hence, cluster performance also increases.


External Switch
Node 1
Node 2
Node 3
Internal Switch 1
Internal Switch 2
InfiniBand Switches

- Scale-out NAS clusters use separate internal and external networks for back-end and front-end connectivity, respectively. An internal network provides connections for intracluster communication, and an external network connection enables clients to access and share file data. Each node in the cluster connects to the internal network. The internal network offers high throughput and low latency and uses high-speed networking technology, such as InfiniBandor Gigabit Ethernet. To enable clients to access a node, the node must be connected to the external Ethernet network. Redundant internal or external networks may be used for high availability. Slide provides an example of scale-out NAS connectivity.

NAS Use Case 1 – Server Consolidation with NAS

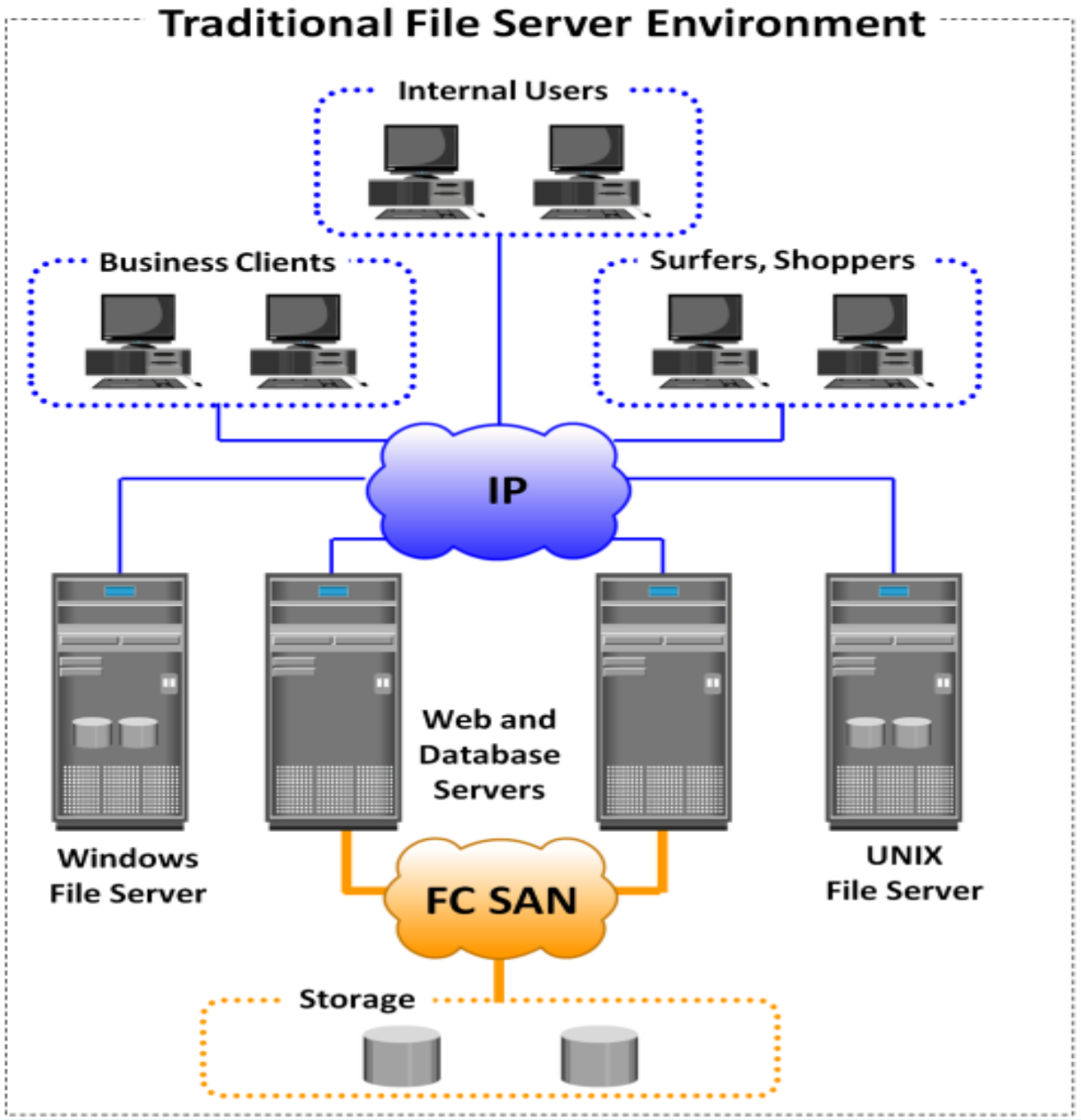


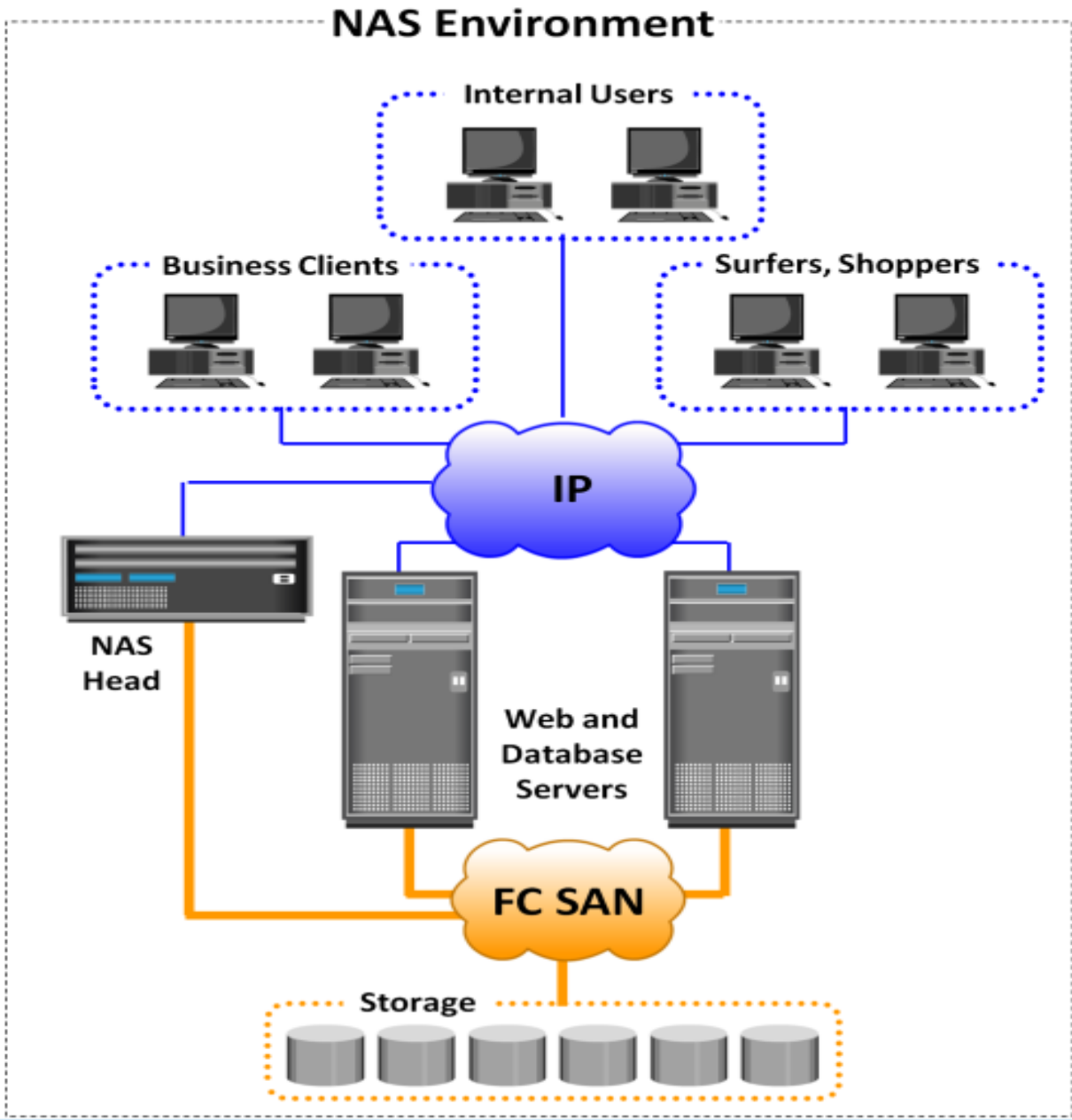


How a NAS enables consolidation of file servers

- Traditionally, network file system for UNIX and Microsoft Windows are housed on separate servers. This requires maintenance of both the environments.
- By implementation of NAS, both Windows and UNIX file structures can be housed together in a single system, while still maintaining their integrity. Using NAS, the same file system can be accessed via different protocols, either NFS or CIFS, and still maintain the integrity of the data and security structures, as long as the applications used for both methodologies understand the data structures presented

NAS Use Case 2 – Storage Consolidation with NAS

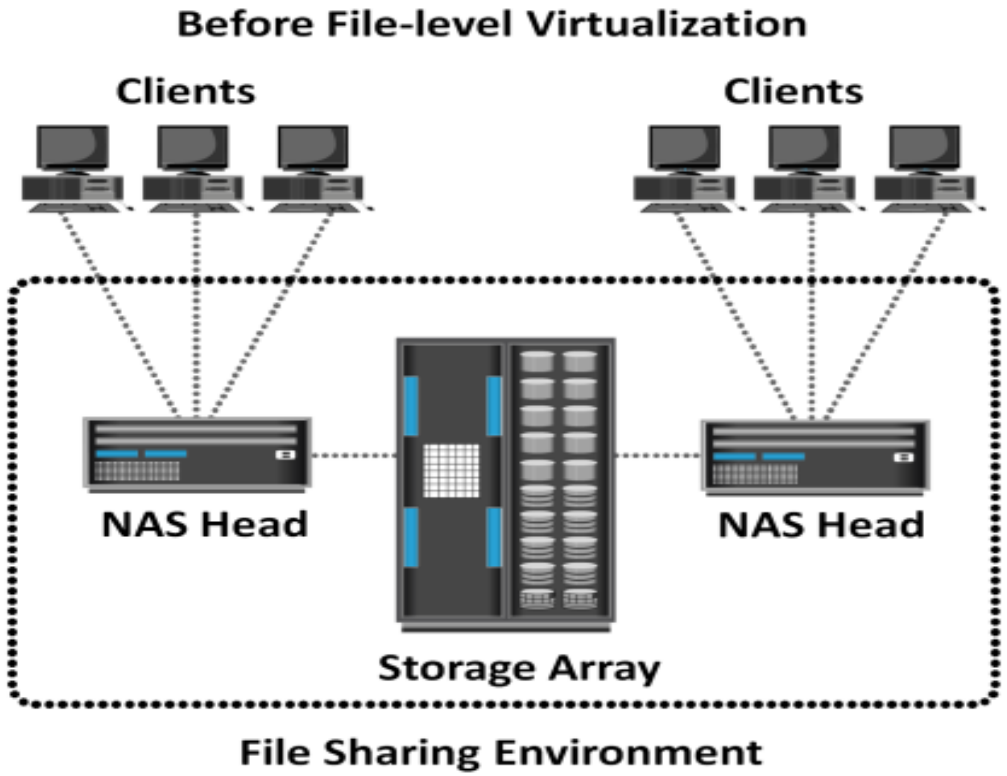


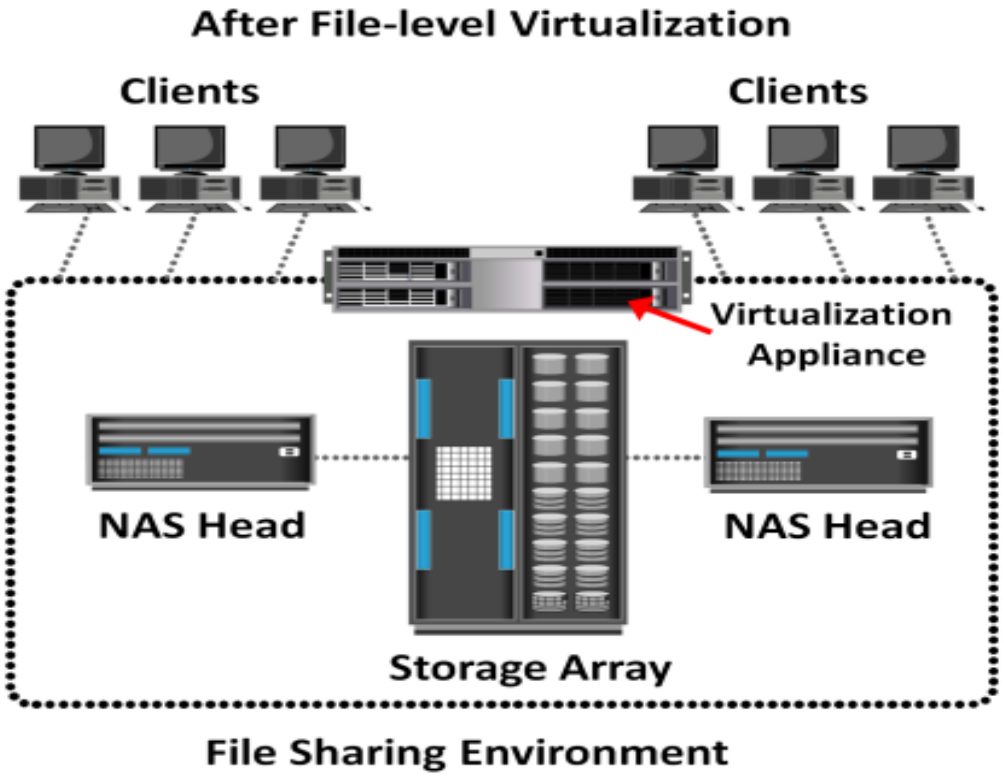


File-level virtualization

- A network-based file sharing environment is composed of multiple file servers or NAS devices. It might be required to move the files from one device to another due to reasons such as cost or performance. **File-level virtualization, implemented in NAS or the file server environment, provides a simple, non disruptive file mobility solution.**
- **File-level virtualization eliminates the dependencies between the data accessed at the file level and the location where the files are physically stored.** It creates a logical pool of storage, enabling users to use a logical path, rather than a physical path, to access files. A global namespace is used to map the logical path of a file to the physical path names. File-level virtualization enables the movement of files across NAS devices, even if the files are being accessed

Comparison: Before and After File-level Virtualization





- Dependency between client access and file location
- Underutilized storage resources
- Downtime is caused by data migrations

- Break dependencies between client access and file location
- Storage utilization is optimized
- Non-disruptive migrations

File-level virtualization

- Before virtualization, each host knows exactly where its file resources are located. This environment leads to underutilized storage resources and capacity problems because files are bound to a specific NAS device or file server. It may be required to move the files from one server to another because of performance reasons or when the file server fills up. Moving files across the environment is not easy and may make files inaccessible during file movement. Moreover, hosts and applications need to be reconfigured to access the file at the new location. This makes it difficult for storage administrators to improve storage efficiency while maintaining the required service level.

- File-level virtualization simplifies file mobility. It provides user or application independence from the location where the files are stored. File-level virtualization facilitates the movement of files across the online file servers or NAS devices. This means that while the files are being moved, clients can access their files non disruptively. Clients can also read their files from the old location and write them back to the new location without realizing that the physical location has changed.