Fibre Channel Gateway Overview

This chapter describes the Fibre Channel gateways and includes the following sections:

- About the Fibre Channel Gateway, page 5-1
- Terms and Concepts, page 5-2
- Cisco SFS 3500 Fibre Channel Gateway Features, page 5-4
- How the Fibre Channel Gateway Works, page 5-10

About the Fibre Channel Gateway

The Fibre Channel gateway expansion module optimizes connection performance between your server switch and your Fibre Channel SAN. The gateway associates a dynamically-generated WWNN and associated WWPNs with each connected IB host, or initiator, to provide seamless connectivity between Fibre Channel and IB fabrics. Because the gateway creates Fibre Channel-compatible identifiers for IB elements, you can manage storage without changing current SAN management tools and practices.

The Cisco SFS 3504 Series Switch supports the Cisco SFS 3500 Fibre Channel gateway module, a 4-port 4 G gateway module that supports an extensive feature set. (See Figure 5-1.) With the Fibre Channel gateway expansion modules, you can perform the following tasks:

- Add a gateway card to your server switch to expand your current port count
- Hot-swap expansion modules without disrupting other network configurations
- Replace gateways

For details about Fibre Channel features, see the “Cisco SFS 3500 Fibre Channel Gateway Features” section on page 5-4.

Figure 5-1 Cisco SFS 3500 Fibre Channel Gateway
Terms and Concepts

This guide refers to a number of terms, concepts, and identifiers that apply to the Fibre Channel gateway modules and the elements that interact with the gateways. Table 5-1 presents and defines key Fibre Channel gateway terms and concepts. (For a list of expanded term names, see Appendix A, “Acronyms and Abbreviations.”)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-bind</td>
<td>The auto-bind feature of the Fibre Channel gateway automatically binds the initiator with all possible gateway ports in the chassis, and it dynamically assigns WWNNs and WWPNs to new initiators. When you configure an initiator, you can manually configure these values, but you might create duplicate values that create network conflicts. The auto-bind feature creates unique WWNNs and WWPNs to save you time and prevent network conflicts.</td>
</tr>
<tr>
<td>initiator</td>
<td>Your host, HCA, and server switch emulate a Fibre Channel-attached host, or initiator. The HCA and host drivers render the host SRP-capable. For the purposes of this document, the term “initiator” refers to an SRP host.</td>
</tr>
<tr>
<td>IT</td>
<td>An initiator-target pair represents a logical association made by the software running on the gateway. For example, that association may be made between an SRP host and a storage device target port through a Fibre Channel gateway. A connection is established when the initiator logs in to the target port.</td>
</tr>
<tr>
<td>ITL</td>
<td>ITLs serve as the logical connections (or paths) between InfiniBand hosts and Fibre Channel storage. ITLs consist of an initiator, a target, a LU, and the switches between them.</td>
</tr>
<tr>
<td>logical unit (LU)</td>
<td>A logical unit is an absolute identifier for a partition, disk, or tape on a Fibre Channel storage device. A given LU identifies one specific storage unit. Your Fibre Channel gateway maps LUs to LUNs, and then your hosts use the LUN identifier to access storage.</td>
</tr>
<tr>
<td>logical unit number (LUN)</td>
<td>Each logical unit number, or LUN, identifies a Fibre Channel storage unit. LUNs are not absolute identifiers. Up to 4 different LUNs can represent the same LU. Your Fibre Channel gateway automatically assigns LUNs to LUs. LUNs are initiator-side identifiers. Initiators must be able to see LUNs to write information to the LUs that the LUNs represent.</td>
</tr>
<tr>
<td>random device</td>
<td>A random device is a storage device with LUs that can be accessed randomly (non-sequentially). RAID devices and JBODs qualify as random devices.</td>
</tr>
<tr>
<td>sequential device</td>
<td>A sequential device is a storage device with LUs that can only be accessed sequentially. Tape devices qualify as sequential devices. The Fibre Channel gateway lets you configure separate connection defaults for random devices and sequential devices. For instance, because tape (sequential) devices may require more time to access data, you may want to extend time-out values. You can configure random and sequential configuration options when you configure global attributes and ITLs.</td>
</tr>
<tr>
<td>service name</td>
<td>A service name is an identifier for a Fibre Channel feature. Service names apply to all Fibre Channel components. The Fibre Channel gateway dynamically creates service names for IB components.</td>
</tr>
</tbody>
</table>
### Terms and Concepts

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRP host</td>
<td>The term “SRP host” means the same thing as <em>initiator</em> (above), but it emphasizes the fact that, in an ITL, it is a host that runs SRP communicates with Fibre Channel storage devices.</td>
</tr>
<tr>
<td>target</td>
<td>A target is a Fibre Channel storage device port. In this document, “target” refers to the <em>port</em> on the storage device through which initiators access disks or tapes. A storage device with two ports will appear as two targets.</td>
</tr>
<tr>
<td>transparent topology emulation</td>
<td>The transparent topology emulation feature of the Fibre Channel gateway assigns Fibre Channel identifiers to all IB elements, so your SAN can access IB elements as though they were Fibre Channel devices. Transparent topology emulation eliminates any need for you to make changes to your SAN for it to communicate with your IB fabric.</td>
</tr>
<tr>
<td>VSAN</td>
<td>A VSAN is a virtual storage area network, or virtual SAN. A SAN is a dedicated network that interconnects hosts and storage devices, primarily to exchange SCSI traffic. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs you can create multiple logical SANs over a common physical infrastructure. Fibre Channel fabrics maintain higher security and greater stability by using VSANs. VSANs are supported on the Cisco SFS 3500 Fibre Channel gateway only.</td>
</tr>
<tr>
<td>WWNN</td>
<td>World-wide node names serve as Fibre Channel identifiers for initiators in the SAN. The Fibre Channel gateway dynamically associates WWNNs with SRP initiators. The Fibre Channel gateway also assigns a WWNN to itself.</td>
</tr>
<tr>
<td>WWPN</td>
<td>World-wide port names serve as Fibre Channel identifiers for initiator ports in the SAN. When you configure an SRP host (initiator), the Fibre Channel gateway creates a WWPN for each initiator per Fibre Channel gateway. If multiple Fibre Channel gateways are present in the chassis, then a WWPN is created for each initiator per gateway.</td>
</tr>
<tr>
<td>Zoning</td>
<td>Zoning grants or denies hosts access to ports on storage targets in the SAN. Soft zones dictate which hosts can access which servers based on WWNNs and WWPNs. You can include in a zone any IB host that connects to the SAN through the Fibre Channel gateway. Zoning takes place on the switch and on the gateway.</td>
</tr>
</tbody>
</table>
Cisco SFS 3500 Fibre Channel Gateway Features

Cisco SFS 3500 Fibre Channel Gateway Features

Fibre Channel gateways add bandwidth and speed to your environment. For information about installing Fibre Channel gateways, see the Cisco SFS InfiniBand 3504 Server Switch Hardware Installation Guide.

This section includes the following topics:

- Cisco SFS 3500 Fibre Channel Gateway Hardware Features, page 5-4
- Cisco SFS 3500 Fibre Channel Gateway Software Features, page 5-8

Cisco SFS 3500 Fibre Channel Gateway Hardware Features

This section includes the following topics:

- Topologies, page 5-4
- Bandwidth and Speed, page 5-6
- Port Masking, page 5-7
- Load Balancing, page 5-7
- Failover, page 5-7
- Load Distribution, page 5-7
- Trunking, page 5-7
- VSAN SRP Initiator Access, page 5-7
- Individual VSAN IDs, page 5-8

Topologies

The Cisco SFS 3500 Fibre Channel gateway supports the following topologies:

- E port—A port connected to a switch. In expansion port (E port) mode, an interface functions as a fabric expansion port. This port may be connected to another E port to create an ISL between two switches. E ports carry frames between switches for configuration and fabric management. They serve as conduits between switches for frames destined to remote N ports and NL ports. E ports support class 2, class 3, and class F service. An E port can be connected to the E port of another Fibre Channel gateway switch, but two Cisco 3500 Fibre Channel gateway E ports cannot be connected. (See Figure 5-2.) For information about setting the E-port operating mode, see the “Setting the Connection Type” section on page 6-9.
F port—A port directly attached to storage or a target. In a fabric port, (F port) mode, an interface functions as a fabric port. This port may be connected to a storage device operating as an N port. An F port can be attached to only one N port. F ports support class 2 and class 3 service. An arbitrated loop device is not supported by the Fibre Channel gateway. (See Figure 5-3.) For information about setting the F-port operating mode, see the “Setting the Connection Type” section on page 6-9.

Redundant Topologies

High availability for Fibre Channel gateways depends upon redundant topologies. Every SRP host must be able to reach each storage device port through multiple Fibre Channel gateways on the same IB fabric and subnet.

Figure 5-4 displays a sample redundant topology.
In the simple example topology, both Fibre Channel gateways provide the host with a route to the same LUNs, and all ports in each Fibre Channel gateway can access the same LUNs. The server switches in the example topology both run on the same IB fabric and in the same subnet (as they directly connect to each other). Because the server switches reside in the same IB fabric and subnet, the device manager monitors the status of both and directs one Fibre Channel gateway to adopt all traffic if the other gateway fails. Because all ports on each gateway access the same LUNs, ITLs over the gateways can support dynamic load balancing and dynamic port failover.

### Bandwidth and Speed

The Cisco SFS 3500 Fibre Channel gateway is supported in the Cisco SFS 3504 Server Switch chassis only. Each of the four ports on the gateway provides up to 4 Gbps of bandwidth. The switch backplane has two SDR 4x IB ports. You can configure the ports on a module to run at either 1 Gbps, 2 Gbps, or 4 Gbps. Auto-negotiation can be configured to automatically negotiate connection parameters. If auto-negotiation is enabled, the connection speed and mode (duplex, half-duplex) are determined when the Fibre Channel gateway port on establishes a connection with a Fibre Channel device.
Port Masking

You can configure a Fibre Channel gateway to grant or deny a given initiator access to one or more of the Fibre Channel ports on the gateway. Port masking lets you control the routes that SRP hosts can use to access storage devices on the SAN.

Load Balancing

When multiple ports of a Fibre Channel gateway provide paths to the same storage ports, you can configure load balancing to distribute traffic evenly across all active ports.

Failover

When multiple ports of a Fibre Channel gateway provide paths to the same storage, you can configure failover so that one port manages traffic while the other ports remain dormant. If the active port fails, the dormant ports on the gateway adopt the traffic.

Load Distribution

Fibre Channel gateways support load distribution on Fibre Channel ports to improve network performance. Load distribution improves reliability by evenly dispersing traffic to different nodes or routes so that one route or node is not overused.

Trunking

Trunking, also known as VSAN trunking, enables interconnected ports to transmit and receive frames in more than one VSAN over the same physical link and using the EISL frame format. Trunking is supported on the E port when it is in native mode with interopMode “0.” When trunking is enabled, the E port becomes a TE port. When trunking is disabled on an E port, the port and all its I-WWPN are disabled, and only the initiators that have the same VSAN ID as the port VSAN will be active. Users can enable and disable trunking on the Fibre Channel ports with the CLI.

VSAN SRP Initiator Access

The Cisco 3500 Fibre Channel gateway has the ability to support VSANs. All SRP initiators belong to a user-configurable VSAN. Each SRP initiator can be assigned to one VSAN per gateway. If multiple gateways exist on the chassis, the initiators can appear on multiple VSANs. After placing the initiator in a VSAN, the administrator has the capability to disable SRP initiator access to a VSAN and enable it later.

The Cisco 3500 Fibre Channel gateway allows users to configure Fibre Channel ports and IB initiators on a VSAN. This feature can be used only when the Fiber Channel ports are connected to Cisco MDS switches.
Individual VSAN IDs

Each VSAN has a globally unique VSAN ID that should be unique across all E ports in a Cisco SFS 3504 Server Switch chassis:

- ID 1—This ID is the default. When no VSANs are configured, all devices in the fabric are part of the default VSAN.
- ID 4094—This ID is assigned to isolated VSANs. All F ports and first generation Fibre Channel ports, which are not supported by VSANs, are always assigned this VSAN ID, as are E ports on which trunking has been disabled.
- ID 2 to 4093—When a physical fabric is sub-divided into multiple virtual fabrics, each virtual fabric can be assigned a VSAN ID from the range of 2 to 4093.

For more information, see the "About VSANs" section on page 5-11.

Cisco SFS 3500 Fibre Channel Gateway Software Features

Fibre Channel gateway software features provide the ability to distribute traffic evenly across connections, ensure uninterrupted traffic, and control host/storage access.

This section includes the following topics:

- Boot over SAN and LUN Remapping, page 5-8
- Access Control, page 5-8
- Zoning, page 5-9
- Redundancy and High Availability, page 5-9
- A/B Partitions, page 5-9
- Virtual I/O for Fibre Channel, page 5-9
- Interoperability, page 5-9
- Hardware Acceleration, page 5-9
- Multiple Fabrics per Card, page 5-10
- One WWPN per Initiator per Gateway, page 5-10

Boot over SAN and LUN Remapping

Boot over SAN enables InfiniBand-attached servers to boot remotely over the SAN by LUN remapping.

To a SAN, your Fibre Channel gateway appears as a Fibre Channel switch with Fibre channel-attached nodes. To the IB fabric, Fibre channel targets appear as SRP-native storage arrays.

Access Control

The Fibre Channel gateway supports industry-standard Fibre Channel access controls that use port-based zoning or LUN-based restrictions and permissions. The gateway also provides additional security filters that you can apply individually or collectively to initiators and Fibre Channel storage targets and LUNs.

The Storage Manager on your server switch provides access filters as an additional level of access control. Access filters grant or deny hosts access to ports or to LUNs.
Zoning

Zoning grants or denies hosts access to ports on storage targets in the SAN. Soft zones dictate which hosts can access which servers based on WWNNs and WWPNs. You can include in a zone any IB host that connects to the SAN through the Fibre Channel gateway. Zoning enforcement takes place on the switch and on the gateway; however, you should configure zones on Fibre Channel switches, not on the gateways.

Redundancy and High Availability

Redundancy can be achieved in the Cisco 3500 Fibre Channel gateway environment by using two Fibre Channel gateways. Cisco SFS 3500 Fibre Channel gateways do not support redundancy and HA when you have a single gateway.

A/B Partitions

Partitions enable the switch to maintain two active types of active operating system software and to switch quickly between the active (A) and the dormant (B) operating systems, analogous to a dual boot scheme.

Virtual I/O for Fibre Channel

Virtual I/O allows a group of servers to share a pool of centralized Fibre Channel I/O resources. Virtual I/O translates between SRP and FCP at the gateway and allows an SRP initiator to concurrently communicate through multiple shared connections.

Interoperability

The Fibre Channel gateway interoperates with Cisco MDS, Brocade, and McData switches (through an E port) and supports direct-attached storage (through an F port). (For more information about switch interoperability, see the “Configuring Port Parameters” section on page 6-7 or the Cisco MDS 9000 Family Switch-to-Switch Interoperability Guide.) The Cisco SFS 3500 gateway comes up in E port mode when connected to Fibre Channel switches and behaves as any other Fibre Channel switch. The Cisco SFS 3500 gateway participates in the following:

- Link initialization
- VSAN and trunk initialization (if connected to MDS switches)
- Fabric initialization
- Zone merging

Hardware Acceleration

SRP data path is handled by hardware. Slow path is handled by software, and Fast Path is handled by hardware, which improves performance.
Multiple Fabrics per Card

The E ports on the Cisco 3500 gateway module can connect to different physical fabrics. However, the Cisco 3500 gateway is connected to two discreet switches (fabrics) that remain two different fabrics and are not unified as one.

One WWPN per Initiator per Gateway

Each initiator has one WWPN per Fibre Channel gateway.

How the Fibre Channel Gateway Works

The Fibre Channel gateway performs transparent topology emulation to connect IB hosts and SANs. The Fibre Channel gateway dynamically allocates world-wide node names (WWNNs) and world-wide port names (WWPNs) to IB hosts to emulate Fibre Channel-attached hosts. The Fibre Channel gateway and IB hosts appear to the SAN as groups of hosts on a Fibre Channel switch (see Figure 5-5) with the dedicated bandwidth advantages of a switch-based architecture. The Fibre Channel gateway translates between the FCP of the SAN and the SRP of the IB hosts. In this way, SANs and IB-attached hosts communicate seamlessly. SAN management tools recognize IB and Fibre Channel devices alike in Fibre Channel terms, which permits all management paradigms and security infrastructures to operate normally.

After the Fibre Channel gateway assigns WWNNs and WWPNs to initiators, you must configure access control policies to associate Fibre Channel-attached LUNs to initiators.
About VSANs

The VSAN trunking feature works with Cisco MDS switches only. Brocade and McData ISLs come up in non-trunking mode.

A Cisco SFS 3500 Fibre Channel gateway can achieve higher security and greater stability in Fibre Channel fabrics by using VSANs. A VSAN is a virtual storage area network that provides isolation among devices that are physically connected to the same fabric. With VSANs you can create multiple logical SANs over a common physical infrastructure.

VSANs offer the following advantages:

- Traffic isolation—Traffic is contained within VSAN boundaries, and devices reside only in one VSAN, ensuring absolute separation between user groups, if desired.
- Scalability—VSANs are overlaid on top of a single physical fabric. The ability to create several logical VSAN layers increases the scalability of the SAN.
- Per VSAN fabric services—Replication of fabric services on a per-VSAN basis provides increased scalability and availability.
Redundancy—Several VSANs created on the same physical SAN ensures redundancy. If one VSAN fails, protection (to another VSAN in the same physical SAN) is configured using a backup path between the host and the device.

Ease of configuration—Users can be added, moved, or changed between VSANs without changing the physical structure of a SAN. Moving a device from one VSAN to another requires configuration at the port level only, not at the physical level.

Each initiator can be assigned to a VSAN per gateway. If there is a need to assign that initiator to multiple VSANs you have to use multiple gateways. For example, if an initiator needs to be assigned to three VSANs, then you would need three gateways.