



CHAPTER 10

Configuring Fabric Binding

This chapter describes the fabric binding feature provided in the Cisco MDS 9000 Family of directors and switches. It includes the following sections:

This chapter includes the following topics:

- [Information About Fabric Binding, page 10-291](#)
- [Licensing Requirements for Fabric Binding, page 10-292](#)
- [Default Settings, page 10-293](#)
- [Configuring Fabric Binding, page 10-293](#)

Information About Fabric Binding

The fabric binding feature ensures ISLs are only enabled between specified switches in the fabric binding configuration. Fabric binding is configured on a per-VSAN basis.

This feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations. It uses the Exchange Fabric Membership Data (EFMD) protocol to ensure that the list of authorized switches is identical in all switches in the fabric.

This section includes the following topics:

- [Port Security Versus Fabric Binding, page 10-291](#)
- [Fabric Binding Enforcement, page 10-292](#)

Port Security Versus Fabric Binding

Port security and fabric binding are two independent features that can be configured to complement each other. [Table 10-1](#) compares the two features.

Table 10-1 *Fabric Binding and Port Security Comparison*

Fabric Binding	Port Security
Uses a set of sWWNs and a persistent domain ID.	Uses pWWNs and nWWNs or fWWNs and sWWNs.
Binds the fabric at the switch level.	Binds devices at the interface level.

Table 10-1 Fabric Binding and Port Security Comparison (continued)

Fabric Binding	Port Security
Authorizes only the configured sWWN stored in the fabric binding database to participate in the fabric.	Allows a preconfigured set of Fibre Channel devices to logically connect to a SAN ports. The switch port, identified by a WWN or interface number, connects to a Fibre Channel device (a host or another switch), also identified by a WWN. By binding these two devices, you lock these two ports into a group (or list).
Requires activation on a per VSAN basis.	Requires activation on a per VSAN basis.
Allows specific user-defined switches that are allowed to connect to the fabric, regardless of the physical port to which the peer switch is connected.	Allows specific user-defined physical ports to which another device can connect.
Does not learn about switches that are logging in.	Learns about switches or devices that are logging in if learning mode is enabled.
Cannot be distributed by CFS and must be configured manually on each switch in the fabric.	Can be distributed by CFS.

Port-level checking for xE ports is as follows:

- The switch login uses both port security binding and fabric binding for a given VSAN.
- Binding checks are performed on the port VSAN as follows:
 - E port security binding check on port VSAN
 - TE port security binding check on each allowed VSAN

While port security complements fabric binding, they are independent features and can be enabled or disabled separately.

Fabric Binding Enforcement

To enforce fabric binding, configure the switch world wide name (sWWN) to specify the xE port connection for each switch. Enforcement of fabric binding policies are done on every activation and when the port tries to come up. In a FICON VSAN, the fabric binding feature requires all sWWNs connected to a switch and their persistent domain IDs to be part of the fabric binding active database. In a Fibre Channel VSAN, only the sWWN is required; the domain ID is optional.



Note

All switches in a Fibre Channel VSAN using fabric binding must be running Cisco MDS SAN-OS Release 3.0(1) and NX-OS Release 4.1(1b) or later.

Licensing Requirements for Fabric Binding

Fabric binding requires that you install either the MAINFRAME_PKG license or the ENTERPRISE_PKG license on your switch.

See the *Cisco MDS 9000 Family NX-OS Licensing Guide* for more information on license feature support and installation.

Default Settings

Table 10-2 lists the default settings for the fabric binding feature.

Table 10-2 Default Fabric Binding Settings

Parameters	Default
Fabric binding	Disabled

Configuring Fabric Binding

Detailed Steps

To configure fabric binding in each switch in the fabric, follow these steps:

-
- Step 1** Enable the fabric configuration feature.
 - Step 2** Configure a list of sWWNs and their corresponding domain IDs for devices that are allowed to access the fabric.
 - Step 3** Activate the fabric binding database.
 - Step 4** Copy the fabric binding active database to the fabric binding config database.
 - Step 5** Save the fabric binding configuration.
 - Step 6** Verify the fabric binding configuration.
-

This section includes the following topics:

- [Enabling Fabric Binding, page 10-293](#)

Enabling Fabric Binding

The fabric binding feature must be enabled in each switch in the fabric that participates in the fabric binding. By default, this feature is disabled in all switches in the Cisco MDS 9000 Family. The configuration and verification commands for the fabric binding feature are only available when fabric binding is enabled on a switch. When you disable this configuration, all related configurations are automatically discarded.

