



## APPENDIX **D**

# Managing Cisco FabricWare

---

The Cisco FabricWare software running on the MDS 9020 Switch offers Fibre Channel switching services that realize maximum performance. Cisco FabricWare provides networking features such as zoning, advanced security, nondisruptive software upgrades, diagnostics, a CLI with syntax resembling Cisco IOS, and standard interfaces for management applications.

This appendix contains the following sections:

- [Fibre Channel Support, page D-1](#)
- [Zone Configuration, page D-1](#)
- [Security, page D-2](#)
- [Events, page D-2](#)
- [Managing Cisco FabricWare with Fabric Manager, page D-3](#)

## Fibre Channel Support

Cisco FabricWare supports autoconfigured Fibre Channel ports capable of up to 4-Gbps bandwidth. Cisco FabricWare supports the following port types:

- E
- F
- FL
- Fx
- Auto

Cisco FabricWare supports Fabric Shortest Path First (FSPF) as the standard path selection protocol used by Fibre Channel fabrics. The FSPF feature is enabled by default on all Fibre Channel switches. Except in configurations that require special consideration, you do not need to configure any FSPF services. FSPF automatically calculates the best path between any two switches in a fabric.

## Zone Configuration

Zoning enables you to set up access control between storage devices or user groups. If you have administrator privileges in your fabric, you can create zones to increase network security and to prevent data loss or corruption. Zoning is enforced by examining the source-destination ID field. Cisco FabricWare does not support QoS, broadcast, LUN, or read-only zones.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

You can use the Fabric Manager zone configuration tool to manage zone sets, zones, and zone membership for switches running Cisco FabricWare. Cisco FabricWare supports zone membership by pWWN. Refer *Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide*.

## Security

Cisco FabricWare supports the following security features:

- RADIUS
- SSH
- User-based roles
- IP access control lists

Cisco FabricWare can use the RADIUS protocol to communicate with remote AAA servers. RADIUS is a distributed client/server protocol that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS 9000 Family switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

You can access the CLI using the console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console or Telnet and SSH), you can configure one or more of the following security control options: **local**, **remote (RADIUS)**, or **none**.

Using these access methods, you can configure the roles that each authenticated user receives when they access the switch. Cisco FabricWare supports two fixed roles: network administrator and network operator.

IP access lists (IP-ACLs) control management traffic over IP by regulating the traffic types that are allowed or denied to the switch. IP-ACLs can only be configured for the mgmt0 port.

Fabric Manager Server uses SNMPv1 and SNMPv2 to communicate with Cisco FabricWare.

## Events

You can monitor fabric and switch status for Cisco FabricWare switches through either a syslog server or an SNMP trap receiver.

The syslog, or system message logging software, saves messages in a log file or directs the messages to other devices. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting
- Allows you to select the types of captured logging information
- Allows you to select the destination server to forward the captured logging information

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. You can access logged system messages using the CLI or by saving them to a properly configured system message logging server.

You can configure the Cisco MDS 9020 Switch using the CLI to send notifications to SNMP managers when particular events occur. You can send these notifications as traps.

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***

# Managing Cisco FabricWare with Fabric Manager

Fabric Manager supports switches running Cisco FabricWare.

Table D-1 shows the supported features and where to find more information on that feature.

**Table D-1 FabricWare Features in Fabric Manager**

| Feature                            | FabricWare Capabilities                                                                                                                          | Guide                                                                                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Zones                              | Zone configuration<br>Zone membership by pWWN<br>No Cisco FabricWare support for QoS, broadcast, LUN, or read-only zones                         | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide</i>            |
| Interfaces                         | 1/2/4 Fibre Channel autonegotiating ports                                                                                                        | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Interfaces Configuration Guide</i>        |
| SNMP                               | SNMPv1 and SNMPv2c                                                                                                                               | Refer to the <i>Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide</i> |
| Software images                    | Automated upgrades<br>Manual upgrades                                                                                                            | Refer to the <i>Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide</i> |
| FLOGI, name server, FDMI, and RSCN | Displaying FLOGI details<br>Registering name server proxies<br>Displaying FDMI<br>RSCN statistics                                                | Refer to the <i>Cisco MDS 9020 Switch Configuration Guide and Command Reference</i> .          |
| Security                           | Configuring RADIUS<br>Configuring server groups<br>Configuring role-based authorization<br>Configuring user accounts<br>Configuring SSH services | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Security Configuration Guide</i> .        |
| Fibre Channel routing              | FSPF global configuration<br>FSPF interface configuration                                                                                        | Refer to the <i>Cisco MDS 9020 Switch Configuration Guide and Command Reference</i> .          |
| IP services                        | IP access control lists on mgmt0                                                                                                                 | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Security Configuration Guide</i> .        |
| System messages                    | System message logging configuration                                                                                                             | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Fundamentals Configuration Guide</i> .    |
| Advanced configuration             | FC timer                                                                                                                                         | Refer to the <i>Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide</i>            |

***Send documentation comments to [fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)***