CHAPTER 19

Configuring Fabric Security

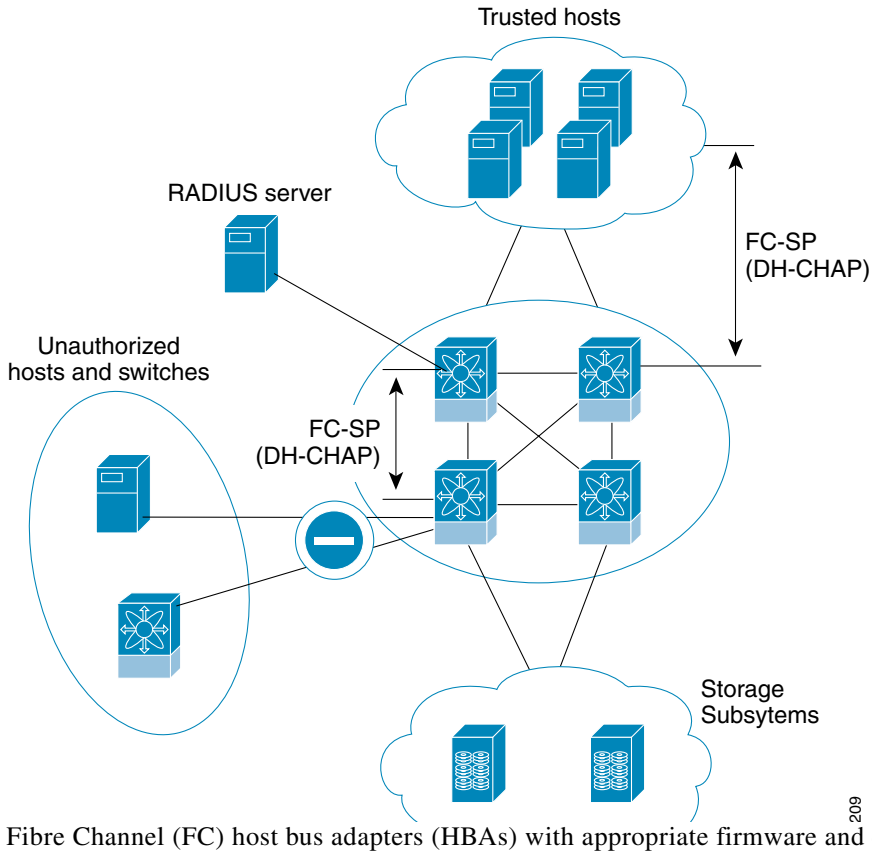
Fibre Channel Security Protocol (FC-SP) capabilities in SAN-OS 1.3(x) provides switch-switch and host-switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol implemented in SAN-OS1.3(x) to provide authentication between Cisco MDS switches and other devices. It consists of the CHAP protocol combined with the Diffie-Hellman exchange.

This chapter contains the following topics:

About Fabric Authentication

All switches in the Cisco MDS 9000 Family enable fabric-wide authentication from one switch to another switch, or from a switch to a host. These switches and hosts authentications are performed locally or remotely in each fabric. As storage islands are consolidated and migrated to enterprise-wide fabrics new security challenges arise. The approach of securing storage islands, cannot always be guaranteed in enterprise-wide fabrics. For example, in a campus environment with geographically distributed switches someone could maliciously interconnect incompatible switches or you could accidentally do so, resulting in inter-switch link (ISL) isolation and link disruption. This need for physical security is addressed by switches in the Cisco MDS 9000 Family.

Figure 19-1 Authentication between Switches and Hosts



Fibre Channel (FC) host bus adapters (HBAs) with appropriate firmware and drivers are required for host-switch authentication.

About DHCHAP

DHCHAP is an authentication protocol that authenticates the devices connecting to a switch. Fibre Channel authentication allows only trusted devices to be added to a fabric, thus preventing unauthorized devices from accessing the switch.

The terms FC-SP and DHCHAP are used interchangeably in this chapter.

DHCHAP is a mandatory password-based, key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication. DHCHAP negotiates hash algorithms and DH groups before performing authentication. It supports MD-5 and SHA-1 algorithm-based authentication.

Configuring the DHCHAP feature requires the ENTERPRISE_PKG license.

DHCHAP Compatibility with Existing MDS Features

This sections identifies the impact of configuring the DHCHAP feature along with existing MDS features:

- PortChannel interfaces—If DHCHAP is enabled for ports belonging to a PortChannel, DHCHAP authentication is performed at the physical interface level, not at the PortChannel level.
- FCIP interfaces—The DHCHAP protocol works with FCIP interface just as it would with a physical interface.
- Port security or fabric binding—Fabric binding policies are enforced based on identities authenticated by DHCHAP.
- VSANs—DHCHAP authentication is not done on per-VSAN basis.
- High availability--DHCHAP authentication works transparently with existing HA features.

Configuring DHCHAP Authentication

To configure DHCHAP authentication using the local password database, follow these steps:

Step 1 Enable DHCHAP.

Step 2 Identify and configure the DHCHAP authentication modes.

Step 3 Configure the hash algorithm and DH group.

Step 4 Configure the password for the local switch and other switches in the fabric.

Step 5 Configure the timeout value for reauthentication.

Step 6 Verify the DHCHAP configuration.

Enabling DHCHAP

By default, the DHCHAP feature is disabled in all switches in the Cisco MDS 9000 Family.

You must explicitly enable the DHCHAP feature to access the configuration and verification commands for fabric authentication. When you disable this feature, all related configurations are automatically discarded.

Configuring DHCHAP Authentication Modes

The DHCHAP authentication status for each interface depends on the configured DHCHAP port mode.

When the DHCHAP feature is enabled in a switch, each Fibre Channel interface or FCIP interface may be configured to be in one of four DHCHAP port modes:

- On—During switch initialization if the connecting device supports DHCHAP authentication, the software performs the authentication sequence. If the connecting device does not support DHCHAP authentication, the software moves the link to an isolated state.
- Auto-Active—During switch initialization if the connecting device supports DHCHAP authentication, the software performs the authentication sequence. If the connecting device does not support DHCHAP authentication, the software continues with the rest of the initialization sequence.
- Auto-Passive (default)—The switch does not initiate DHCHAP authentication, but participates in DHCHAP authentication if the connecting device initiates DHCHAP authentication.

- Off—Does not support DHCHAP authentication. Authentication messages sent to such ports return error messages to the initiating switch.

Whenever DHCHAP port mode is changed to a mode other than the Off mode, reauthentication is performed.

Table 19-1 identifies the switch-to-switch authentication behavior between two Cisco MDS switches in various modes.

Table 19-1 DHCHAP Authentication Status Between Two MDS Switches

Switch N	**Switch 1**
DHCHAP Modes	**on**
on	FC-SP authentication is performed
auto-Active	FC-SP authentication is not performed.
auto-Passive	FC-SP authentication is not performed.
off	Link is brought down

Configuring the DHCHAP Hash Algorithm

Cisco MDS switches support a default hash algorithm priority list of MD-5 followed by SHA-1 for DHCHAP authentication.

If you change the hash algorithm configuration, ensure to change it globally for all switches in the fabric.

RADIUS and TACACS+ protocols always use MD-5 for CHAP authentication. Using SHA-1 as the hash algorithm may prevent RADIUS and TACACS+ usage--even if these AAA protocols are enabled for DHCHAP authentication.

Configuring DHCHAP Groups

All switches in the Cisco MDS Family support all DHCHAP groups specified in the standard: 0 (null DH group which does not perform the Diffie-Hellman exchange), 1, 2, 3, or 4.

If you change the DH group configuration, ensure to change it globally for all switches in the fabric.

Configuring DHCHAP Passwords

DHCHAP authentication in each direction requires a shared secret password between the connected devices. To do this, you can use one of three approaches to manage passwords for all switches in the fabric which participate in DHCHAP:

- Approach 1—Use the same password for all switches in the fabric--the simplest approach. When you add a new switch, you will use the same password to authenticate that switch in this fabric. It is also the most vulnerable approach if someone from outside maliciously attempts to access any one switch in the fabric

- Approach 2—Use a different password for each switch and maintain that password list in each switch in the fabric--when you add a new switch, you create a new password list and update all switches with the new list. Accessing one switch yields the password list for all switches in that fabric.
- Approach 3—Use different passwords for different switches in the fabric--when you add a new switch, multiple new passwords corresponding to each switch in the fabric must be generated and configured in each switch. Even if one switch is compromised, the password of other switches are still protected. This approach requires considerable password maintenance by the user.

We recommend using RADIUS or TACACS+ for fabrics with more than five switches. If you need to use local password database, you can continue to do so using Approach 3 and using the Cisco MDS 9000 Family Fabric Manager to manage the password database. Refer to the Cisco MDS 9000 Family Fabric Manager User Guide for further information.

All passwords are restricted to 64 alphanumeric characters and can be changed, but not deleted.

Configuring Passwords for Other Devices

You can configure passwords in the local authentication database for other devices in a fabric. The other devices are identified by their device name, which is also know as the switch WWN or device WWN. The password is restricted to 64 characters and can be specified in clear text (0) or in encrypted text (7).

The switch WWN identifies the physical switch. This WWN is used to authenticate the switch and is different from the VSAN node WWN.

Configuring the DHCHAP Timeout Value

During the DHCHAP protocol exchange if the MDS switch does not receive the expected DHCHAP message within a specified time interval, authentication failure is assumed. The time ranges from 20 (no authentication is performed) to 1000 seconds. The default is 30 seconds.

When changing the timeout value consider the following factors:

- The existing RADIUS and TACACS+ timeout values.
- The same value must also be configured all switches in the fabric.

Default Fabric Security Settings

Table 19-2 lists the default settings for all fabric security features in any switch.

Table 19-2 Default Fabric Security Settings

Parameters	Default
DHCHAP feature	Disabled.
DHCHAP hash algorithm	A priority list of MD-5 followed by SHA-1 for DHCHAP authentication
DHCHAP authentication mode	auto-passive.

Table 19-2 Default Fabric Security Settings (continued)

DHCHAP group default priority exchange order	0, 4, 1, 2, and 3 respectively.
DHCHAP timeout value	30 seconds.