CHAPTER 30

FC-SP and DHCHAP

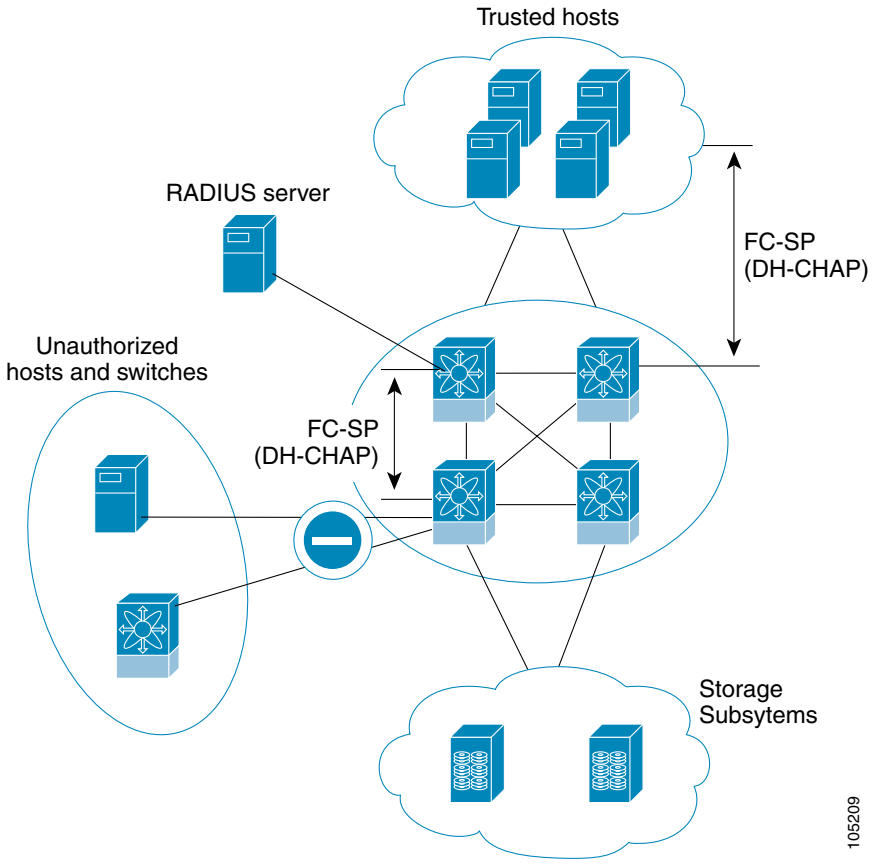
Fibre Channel Security Protocol (FC-SP) capabilities provide switch-switch and host-switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol that provides authentication between Cisco MDS 9000 Family switches and other devices. It consists of the CHAP protocol combined with the Diffie-Hellman exchange.

This chapter includes the following sections:

Fibre Channel Security Protocol

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 switch and host 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 (see Figure 30-1).

Figure 30-1 Switch and Host Authentication



Note Fibre Channel 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.

Note 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 Diffie-Hellman groups before performing authentication. It supports MD5 and SHA-1 algorithm-based authentication.

Configuring the DHCHAP feature requires the ENTERPRISE_PKG license (see Chapter 9, “Obtaining and Installing Licenses”).

DHCHAP Compatibility with Existing Cisco MDS Features

This sections identifies the impact of configuring the DHCHAP feature along with existing Cisco 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 the 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 a 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 DHCHAP password for the local switch and other switches in the fabric.

Step 5 Configure the DHCHAP 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.

To enable DHCHAP and FC-SP, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security > FC-SP**. You see the FC-SP configuration in the Information pane.

From Device Manager, choose **Security > FC-SP**. You see the FC-SP Enable dialog box. Click **Yes** to enable FC-SP and DHCHAP for this switch.

Step 2 Choose the **Control** tab in Fabric Manager. You see the FC-SP enable state for all switches in the fabric.

Step 3 Set the Command drop-down menu to **enable** for all switches that you want to enable FC-SP on.

Step 4 Click the **Apply Changes** icon to enable FC-SP and DHCHAP on the selected switches.

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.
- AutoActive—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.
- AutoPassive (default)—The switch does not initiate DHCHAP authentication, but participates in DHCHAP authentication if the connecting device initiates DHCHAP authentication.
- Off—The switch does not support DHCHAP authentication. Authentication messages sent to such ports return error messages to the initiating switch.

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

Table 30-1 identifies the switch-to-switch authentication behavior between two Cisco MDS switches in various modes.

Table 30-1 DHCHAP Authentication Status Between Two MDS Switches

<table>
<tr><th>Switch N DHCHAP Modes</th><th colspan="4">Switch 1 DHCHAP Modes</th></tr>
<tr><th></th><th>on</th><th>auto-active</th><th>auto-passive</th><th>off</th></tr>
<tr><td>on</td><td rowspan="3">FC-SP authentication is performed.</td><td rowspan="3">FC-SP authentication is performed.</td><td rowspan="2">FC-SP authentication is performed.</td><td>Link is brought down.</td></tr>
<tr><td>auto-Active</td><td rowspan="2">FC-SP authentication is not performed.</td></tr>
<tr><td>auto-Passive</td><td>FC-SP authentication is not performed.</td></tr>
<tr><td>off</td><td>Link is brought down.</td><td colspan="3">FC-SP authentication is not performed.</td></tr>
</table>

To configure the DHCHAP port authentication mode, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Interfaces > FC Physical**. You see the FC-SP configuration in the Information pane.

From Device Manager, choose **Security > FC-SP**. You see the FC-SP Configuration dialog box.

Step 2 Choose the **FC-SP** tab. You see the DHCHAP authentication mode for each interface.

Step 3 Set the Mode drop-down menu to the DHCHAP authentication mode you want to configure for that interface.

Step 4 Click the **Apply Changes** icon in Fabric Manager or click **Apply** in Device Manager to save these DHCHAP port mode settings.

Changing the DHCHAP Hash Algorithm

Cisco MDS switches support a default hash algorithm priority list of MD5 followed by SHA-1 for DHCHAP authentication.

Tip If you change the hash algorithm priority list, then change it globally for all switches in the fabric.

Caution RADIUS and TACACS+ protocols always use MD5 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.

To change the DHCHAP hash algorithm priority list using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > FC-SP**. You see the FC-SP configuration in the Information pane.

Step 2 Choose the **General/Password** tab. You see the DHCHAP general settings mode for each switch.

Step 3 Change the HashList for each switch in the fabric.

Step 4 Click the **Apply Changes** icon to save the updated hash algorithm priority list or click the **Undo Changes** icon to discard any unsaved changes.

Changing DHCHAP Group Settings

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.

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

To change the DH group list using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > FC-SP**. You see the FC-SP configuration in the Information pane.

Step 2 Choose the **General/Password** tab. You see the DHCHAP general settings mode for each switch.

Step 3 Change the GroupList for each switch in the fabric.

Step 4 Click the **Apply Changes** icon to save the updated DH group lists or click the **Undo Changes** icon to discard any unsaved changes.

Configuring the DHCHAP Password

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 that participate in DHCHAP.

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

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

Tip We recommend using RADIUS or TACACS+ for fabrics with more than five switches. If you need to use a 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.

Configuring the DHCHAP Password for the Local Switch

To configure the DHCHAP password for the local switch, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security > FC-SP**. You see the FC-SP configuration in the Information pane.

From Device Manager, choose **Security > FC-SP**. You see the FC-SP Enable dialog box.

Step 2 Choose the **Local Passwords** tab. You see the DHCHAP local password for each switch.

Step 3 Click the **Create Row** icon in Fabric Manager or **Create** in Device Manager to create a new local password. You see the Create Local Passwords dialog box.

Step 4 Optionally, check the switches that you want to configure the same local password on in Fabric Manager.

Step 5 Select the switch **WNN** and set the Password.

Step 6 Click the **Create** to save the updated password or click **Close** to discard any unsaved changes.

Configuring Remote 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).

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

To configure the DHCHAP password for remote switches, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security > FC-SP**. You see the FC-SP configuration in the Information pane.

From Device Manager, choose **Security > FC-SP**. You see the FC-SP Enable dialog box.

Step 2 Choose the **Remote Passwords** tab. You see the DHCHAP local password for each switch.

Step 3 Click the **Create Row** icon in Fabric Manager or **Create** in Device Manager to create a remote password. You see the Create Remote Passwords dialog box.

Step 4 Optionally, check the switches that you want to configure the same remote password on in Fabric Manager.

Step 5 Select the switch **WNN** and set the Password.

Step 6 Click the **Create** to save the updated password or click **Close** to discard any unsaved changes.

Setting 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.

To change the DHCHAP timeout value using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > FC-SP** in Fabric Manager. You see the FC-SP configuration in the Information pane.

Step 2 Choose the **General/Password** tab. You see the DHCHAP general settings mode for each switch.

Step 3 Change the DHCHAP timeout value for each switch in the fabric.

Step 4 Click the **Apply Changes** icon to save the updated timeout value or click the **Undo Changes** icon to discard any unsaved changes.

Configuring DHCHAP AAA Authentication

You can individually set authentication options. If authentication is not configured, local authentication is used by default.

Enabling FC-SP on ISLs

There is a new ISL pop-up menu called Enable FC-SP that enables FC-SP on switches at either end of the ISL. You are prompted for an FC-SP generic password, then asked to set FC-SP interface mode to ON for affected ports. Right-click an ISL and click **Enable FC-SP** to access this feature.