



Configuring FC-SP and DHCHAP

This chapter describes how to configure the Fibre Channel Security Protocol (FC-SP) and the Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP).

This chapter includes the following sections:

- [Information About FC-SP and DHCHAP, on page 1](#)

Information About FC-SP and DHCHAP

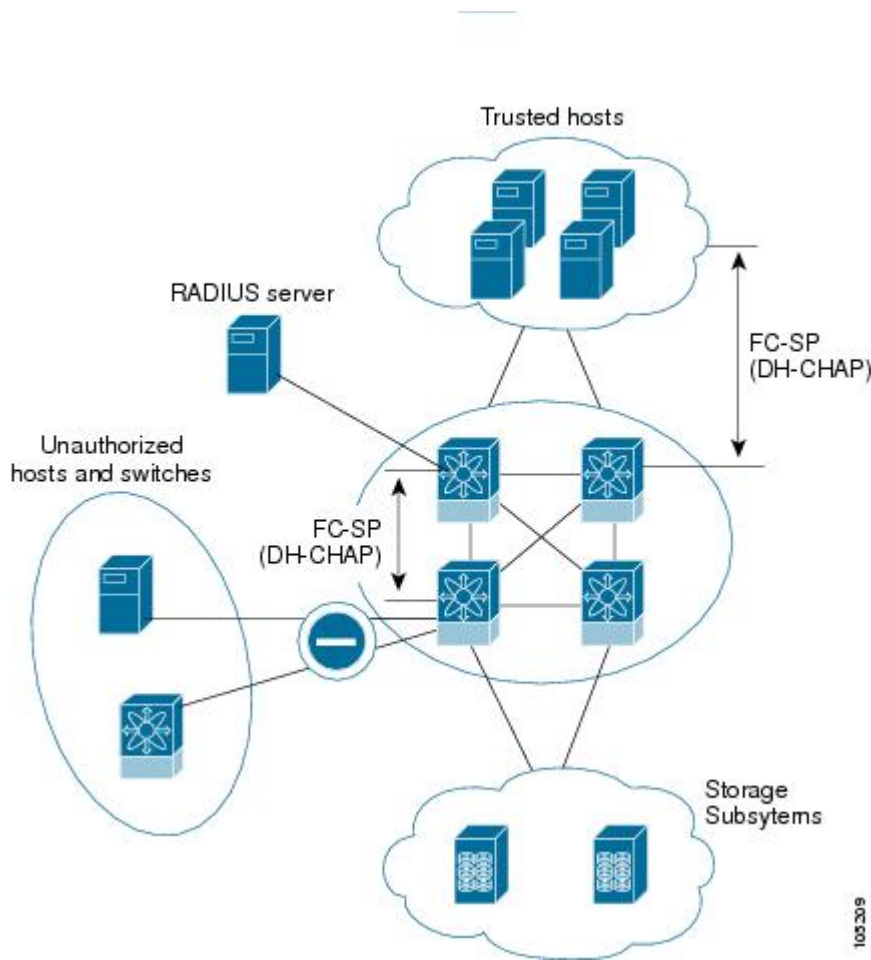
The Fibre Channel Security Protocol (FC-SP) capabilities provide switch-to-switch and host-to-switch authentication to overcome security challenges for enterprise-wide fabrics. The Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol that provides authentication between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

Fabric Authentication

All Cisco SAN switches 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 or accidentally interconnect incompatible switches, resulting in Inter-Switch Link (ISL) isolation and link disruption.

Cisco SAN switches support authentication features to address physical security (see the following figure).

Figure 1: Switch and Host Authentication



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

Configuring DHCHAP Authentication

You can configure DHCHAP authentication using the local password database.

Before you begin

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.

Procedure

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.
-

DHCHAP Compatibility with Fibre Channel Features

When configuring the DHCHAP feature along with existing Cisco NX-OS features, consider these compatibility issues:

- SAN port channel interfaces—If DHCHAP is enabled for ports belonging to a SAN port channel, DHCHAP authentication is performed at the physical interface level, not at the port channel level.
- 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.

By default, the DHCHAP feature is disabled in all Cisco SAN switches.

About Enabling DHCHAP

By default, the DHCHAP feature is disabled in all Cisco SAN switches.

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.

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 link is placed in 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—The switch does not support DHCHAP authentication. Authentication messages sent to ports in this mode 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.

The following table identifies switch-to-switch authentication between two Cisco switches in various modes.

Table 1: DHCHAP Authentication Status Between Two SAN Switches

Switch N DHCHAP Modes	Switch 1 DHCHAP Modes			
	on	auto-active	auto-passive	off
on	FC-SP authentication is performed.	FC-SP authentication is performed.	FC-SP authentication is performed.	Link is brought down.
auto-Active			FC-SP authentication is <i>not</i> performed.	
auto-Passive				
off	Link is brought down.	FC-SP authentication is <i>not</i> performed.		

DHCHAP Hash Algorithm

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

If you change the hash algorithm configuration, 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.

Configuring the DHCHAP Hash Algorithm

You can configure the hash algorithm.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	fcsp dhchap hash [md5] [sha1] Example: switch(config)# fcsp dhchap hash md5 sha1	Configures the use of the the MD5 or SHA-1 hash algorithm.
Step 3	no fcsp dhchap hash sha1 Example: switch(config)# no fcsp dhchap hash sha1	Reverts to the factory default priority list of the MD5 hash algorithm followed by the SHA-1 hash algorithm.

DHCHAP Group Settings

All Cisco SAN switches 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, change it globally for all switches in the fabric.

Configuring the DHCHAP Group Settings

You can change the DH group settings.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	fcsp dhchap dhgroup [0 1 2 3 4] Example: <pre>switch(config)# fcsp dhchap dhgroup [0 1 2 3 4]</pre>	Prioritizes the use of DH groups in the configured order.
Step 3	no fcsp dhchap dhgroup [0 1 2 3 4] Example: <pre>switch(config)# no fcsp dhchap dhgroup [0 1 2 3 4]</pre>	Reverts to the DHCHAP factory default order of 0, 1, 2, 3 and 4.

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 configurations to manage passwords for all switches in the fabric that participate in DHCHAP:

- Configuration 1—Use the same password for all switches in the fabric. This is the simplest configuration. When you add a new switch, you use the same password to authenticate that switch in this fabric. It is also the most vulnerable configuration if someone from the outside maliciously attempts to access any one switch in the fabric.
- Configuration 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.
- Configuration 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 configuration requires considerable password maintenance by the user.



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

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 Configuration 3 and using to manage the password database.

Configuring DHCHAP Passwords for the Local Switch

You can configure the DHCHAP password for the local switch.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	fcsp dhchap password [0 7] password [wwn wwn-id] Example: <pre>switch(config)# fcsp dhchap password [0 7] myword wwn 11:22:11:22:33:44:33:44</pre>	Configures a clear text password for the local switch.

Password Configuration for Remote 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 known 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.

Configuring DHCHAP Passwords for Remote Devices

You can locally configure the remote DHCHAP password for another switch in the fabric.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	fcsp dhchap devicename <i>switch-wwn</i> password <i>password</i> Example: <pre>switch(config)# fcsp dhchap devicename 21:00:05:30:23:1a:11:03 password mypassword</pre>	Configures a password for another switch in the fabric that is identified by the switch WWN device name.
Step 3	<pre>switch(config)# no fcsp dhchap devicename switch-wwn password password</pre> Example: <pre>switch(config)# no fcsp dhchap devicename 21:00:05:30:23:1a:11:03 password mypassword</pre>	Removes the password entry for this switch from the local authentication database.

DHCHAP Timeout Value

During the DHCHAP protocol exchange, if the 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 on all switches in the fabric.

Configuring the DHCHAP Timeout Value

You can configure the DHCHAP timeout value.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	fcsp timeout <i>timeout</i> Example: <pre>switch(config)# fcsp timeout 60</pre>	Configures the reauthentication timeout to the specified value. The unit is seconds.
Step 3	no fcsp timeout <i>timeout</i> Example: <pre>switch(config)# no fcsp timeout 60</pre>	Reverts to the factory default of 30 seconds.

Configuring DHCHAP AAA Authentication

You can configure AAA authentication to use a RADIUS or TACACS+ server group. If AAA authentication is not configured, local authentication is used by default.

Configuration Examples for Fabric Security

This example shows how to set up authentication:

Procedure

Step 1 Obtain the device name of the Cisco SAN switch in the fabric. The Cisco SAN switch in the fabric is identified by the switch WWN.

Example:

```
switch# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

Step 2 Explicitly enable DHCHAP in this switch.

Note When you disable DHCHAP, all related configurations are automatically discarded.

Example:

Step 3 Configure a clear text password for this switch. This password is used by the connecting device.

Example:

```
switch(config)# fcsp dhchap password rtp9216
```

Step 4 Configure a password for another switch in the fabric that is identified by the switch WWN device name.

Example:

```
switch(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

Step 5 Enable the DHCHAP mode for the required interface.

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

Example:

```
switch(config)# interface fc2/4
switch(config-if)# fcsp on
```

Step 6 Verify the protocol security information configured in this switch by displaying the DHCHAP local password database.

Example:

```
switch# show fcsp dhchap database
DHCHAP Local Password:
    Non-device specific password:*****
Other Devices' Passwords:
```



```
Password for device with WWN:20:00:00:05:30:00:38:5e is *****
```

Step 7 Display the DHCHAP configuration in the interface.

Example:

```
switch# show fcsp interface fc2/4
fc2/4

fcsp authentication mode:SEC_MODE_ON
Status:Successfully authenticated
```

Step 8 Repeat these steps on the connecting switch.

Example:

```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# fcsp enable
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:

Non-device specific password:*****
Other Devices' Passwords:

Password for device with WWN:20:00:00:05:30:00:54:de is *****
MDS-9509# show fcsp interface fc2/4
Fc2/4

fcsp authentication mode:SEC_MODE_ON
Status:Successfully authenticated
```

You have now enabled and configured DHCHAP authentication for the sample setup.

Default Settings for Fabric Security

The following table lists the default settings for all fabric security features in any switch.

Table 2: Default Fabric Security Settings

Parameters	Default
DHCHAP feature	Disabled
DHCHAP hash algorithm	A priority list of MD5 followed by SHA-1 for DHCHAP authentication
DHCHAP authentication mode	Auto-passive

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