CHAPTER 31

Port Security

All switches in the Cisco MDS 9000 Family provide port security features that reject intrusion attempts and report these intrusions to the administrator.

Note Port Security is only supported for Fibre Channel ports.

This chapter includes the following sections:

About Port Security

Typically, any Fibre Channel device in a SAN can attach to any SAN switch port and access SAN services based on zone membership. Port security features prevent unauthorized access to a switch port in the Cisco MDS 9000 Family:

- Login requests from unauthorized Fibre Channel devices (Nx ports) and switches (xE ports) are rejected.
- All intrusion attempts are reported to the SAN administrator through system messages.

About Auto-Learn

You can instruct the switch to automatically learn (auto-learn) the port security configurations over a specified period. This feature allows any switch in the Cisco MDS 9000 Family to automatically learn about devices and switches that connect to it. Use this feature to activate the port security feature for the first time as it saves manual configuration for each port. Auto-learn is configured on a per-VSAN basis. If enabled, devices and switches that are allowed to connect to the switch are automatically learned, even if you have not configured any port access.

Auto-Learning Device Authorization

Table 31-1 summarizes the authorized connection for device requests.

Table 31-1 Auto-Learn Device Authorization

Device (pWWN, nWWN, sWWN)	Requests Connection to	Authorization	Condition
Configured with one or more switch ports	A switch on configured ports	Permitted	1
	A switch on other ports	Denied	2
Not configured	A port that is not configured	Permitted if auto-learn enabled	3
		Denied if auto-learn disabled	4
Configured or not configured	A switch port that allows any device	Permitted	5
Configured to log in to any switch port	Any port on the switch	Permitted	6
Not configured	A port configured with some other device	Denied	7

Port Security Enforcement

If you choose to manually configure port security, you must configure the devices and switch port interfaces through which each device or switch is connected:

- Use the port world wide name (pWWN) or the node world wide name (nWWN) to specify the Nx port connection for each device.
- Use the switch world wide name (sWWN) to specify the xE port connection for each switch.

Each Nx and xE port can be configured to restrict a single port or a range of ports.

Enforcement of port security policies are done on every activation and when the port tries to come up.

The port security feature requires all devices connecting to a switch to be part of the port security active database. The software uses this active database to enforce authorization.

By default, the port security feature is not activated in any switch in the Cisco MDS 9000 Family.

Configuring Port Security

To configure port security, follow these steps:

Step 1 Enable the port security feature on all participating switches. See the "Enabling Port Security" section on page 31-3.

Step 2 Activate with auto-learning, if you want to use the auto-learning feature to populate the port security database. See the "Activating Port Security with Auto-Learn" section on page 31-3.

Step 3 Optionally, manually configure the port security database and then activate it. See the "Manually Configuring Port Security" section on page 31-7.

Enabling Port Security

Before you can activate port security, you need to enable this feature on all switches in the fabric that will participate in port security.

To enable port security using Fabric Manager, follow these steps:

Step 1 Choose **VSAN*xxx* > Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **CFS** tab and enable CFS on all participating switches in the VSAN.

Step 3 Click the **Apply Changes** icon to enable CFS distribution for the port security feature.

Step 4 Click the **Control** tab. You see the port security enable state for all switches in the selected VSAN.

Step 5 Set the command column to **enable** for each switch in the VSAN.

Step 6 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 7 Click the **Apply Changes** icon to distribute the port security enable to all switches in the VSAN.

Activating Port Security with Auto-Learn

To activate port security with auto-learn, follow these steps:

Step 1 From Fabric Manager, choose **VSAN*xxx* > Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

From Device Manager, **Choose Security > Port...**.You see the Port Security dialog box.

Step 2 Click the **Actions** tab.

Step 3 Click the **Action** column under Activation, next to the switch or VSAN on which you want to activate port security. You see a drop-down menu with the following options:

- activate—Valid port security settings are activated.
- activate (TurnLearningOff)—Valid port security settings are activated and autolearn turned off.
- forceActivate—Activation is forced.

- forceActivate(TurnLearningOff)—Activation is forced and autolearn is turned off.
- deactivate—All currently active port security settings are deactivated.
- NoSelection— No action is taken.

Step 4 Select the option you want to specify a port security setting action for that switch.

Step 5 Check the **AutoLearn** check box for each switch in the VSAN to enable auto-learning.Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 6 Click the **Apply Changes** icon in Fabric Manager or **Apply** in Device Manager to save these changes or click **Undo Changes** in Fabric Manager or **Close** in Device Manager to discard any unsaved changes.

Displaying Activated Port Security Settings

To display active port security settings, follow these steps:

Step 1 Choose **VSAN*xxx* > Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Active Database** tab.

You see the active port security settings for that VSAN.

Displaying Port Security Statistics

To display port security statistics, follow these steps:

Step 1 Choose **VSAN*xxx* > Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Statistics** tab. You see the port security statistics for that VSAN.

Displaying Port Security Violations

Port violations are invalid login attempts (for example, login requests from unauthorized Fibre Channel devices). You can display a list of these attempts on a per-VSAN basis, using Fabric Manager.

To display port security violations, follow these steps:

Step 1 Choose **VSAN*xxx* > Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Violations** tab. You see the port security violations for that VSAN.

Turning Auto-Learning On or Off

To turn auto-learning on or off, follow these steps:

Step 1 Choose **VSAN*xxx* > Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Action** tab. You see the switches for that VSAN.

Step 3 Check the **AutoLearn** check box next to the switch if you want to enable auto-learning.

Step 4 Uncheck the **AutoLearn** check box next to the switch if you want to disable auto-learning.

Step 5 Click the **CFS** button at the top of the Information pane and select **commit** .

Step 6 Click the **Apply Changes** icon to save these changes or click **Undo Changes** to discard any unsaved changes.

Example of Port Security Authorization

Assume that the port security feature is activated and the following conditions are specified in the active database:

- A pWWN (P1) is allowed access through interface fc1/1 (F1).
- A pWWN (P2) is allowed access through interface fc1/1 (F1).
- A nWWN (N1) is allowed access through interface fc1/2 (F2).
- Any WWN is allowed access through interface fc1/3 (F3).
- A nWWN (N3) is allowed access through any interface.
- A pWWN (P3) is allowed access through interface fc1/4 (F4).
- A sWWN (S1) is allowed access through interface fc1/10-13 (F10 to F13).
- A pWWN (P10) is allowed access through interface fc1/11 (F11).

Table 31-2 summarizes the port security authorization results for this active database.

Table 31-2 Authorization Results for Scenario

Scenario	Device Connection Request	Authorization	Condition	Reason
1	P1, N2, F1	Permitted	1	No conflict.
2	P2, N2, F1	Permitted	1	No conflict.
3	P3, N2, F1	Denied	2	F1 is bound to P1/P2.
4	P1, N3, F1	Permitted	6	Wildcard match for N3.
5	P1, N1, F3	Permitted	5	Wildcard match for F3.
6	P1, N4, F5	Denied	2	P1 is bound to F1.
7	P5, N1, F5	Denied	2	N1 is only allowed on F2.
8	P3, N3, F4	Permitted	1	No conflict.
9	S1, F10	Permitted	1	No conflict.

Table 31-2 Authorization Results for Scenario (continued)

Scenario	Device Connection Request	Authorization	Condition	Reason
10	S2, F11	Denied	7	P10 is bound to F11.
11	P4, N4, F5 (auto-learn on)	Permitted	3	No conflict.
12	P4, N4, F5(auto-learn off)	Denied	4	No match.
13	S3, F5 (auto-learn on)	Permitted	3	No conflict.
14	S3, F5 (auto-learn off)	Denied	4	No match.
15	P1, N1, F6 (auto-learn on)	Denied	2	P1 is bound to F1.
16	P5, N5, F1 (auto-learn on)	Denied	7	P3 is bound to F1.
17	S3, F4 (auto-learn on)	Denied	7	P3 paired with F4.
18	S1, F3 (auto-learn on)	Permitted	5	No conflict.
19	P5, N3, F3	Permitted	6	Wildcard match for F3 and N3.
20	P7, N3, F9	Permitted	6	Wildcard match for N3.

Configuring Port Security Manually

Note Most tabs in the Information pane for features using CFS are dimmed until you click the CFS tab. The CFS tab shows which switches have CFS enabled and shows the master switch for this feature. Once the CFS tab is clicked, the other tabs in the Information pane that use CFS are activated.

To manually configure port security on any switch in the Cisco MDS 9000 Family, follow these steps:

Step 1 Identify the WWN of the ports that need to be secured.

Step 2 Secure the fWWN to an authorized nWWN or pWWN.

Step 3 Activate the port security database.

Step 4 Verify your configuration.

WWN Identification

If you decide to manually configure port security, be sure to adhere to the following guidelines:

- Identify switch ports by the interface or by the fWWN.
- Identify devices by the pWWN or by the nWWN.
- If an Nx port:
  - is allowed to login to SAN switch port Fx, then that Nx port can only log in through the specified Fx port.
  - nWWN is bound to a Fx port WWN, then all pWWNs in the Nx port are implicitly paired with the Fx port.

- TE port checking is done on each VSAN in the allowed VSAN list of the trunk port.
- All PortChannel xE ports must be configured with the same set of WWNs in the same PortChannel.
- E port security is implemented in the port VSAN of the E port. In this case the sWWN is used to secure authorization checks.
- Once activated, the config database can be modified without any effect on the active database.
- By saving the running configuration, you save the configuration database and activated entries in the active database. Learned entries in the active database are not saved.

Manually Configuring Port Security

To manually configure port security on a switch, follow these steps:

Step 1 Choose VSANxxx > **Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Config Database** tab. You see the configured port security settings for that VSAN.

Step 3 Click the **Create Row** icon to add an authorized port pair. You see the Create Port Security dialog box.

Step 4 Double-click the device from the available list for which you want to create the port security setting.

Step 5 Double-click the port from the available list to which you want to bind the device.

Step 6 Click **Create** to creating the port security setting, or click **Close** to close the Create Port Setting dialog without adding a new port security setting.

Step 7 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 8 Click the **Apply Changes** icon to save these changes or click **Undo Changes** to discard any unsaved changes.

Deleting a Port Security Pair

To delete a port security setting from the configured database on a switch, follow these steps:

Step 1 Choose VSANxxx > **Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Config Database** tab. You see the configured port security settings for that VSAN.

Step 3 Click the row you want to delete.

Step 4 Click the **Delete Row** icon.You see the confirmation dialog box.

Step 5 Click **Yes** to delete the row, or click **No** to close the confirmation dialog box without deleting the row.

Step 6 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 7 Click the **Apply Changes** icon to save these changes or click **Undo Changes** to discard any unsaved changes.

Database Interaction

Table 31-3 lists the differences and interactions between the active and configuration databases

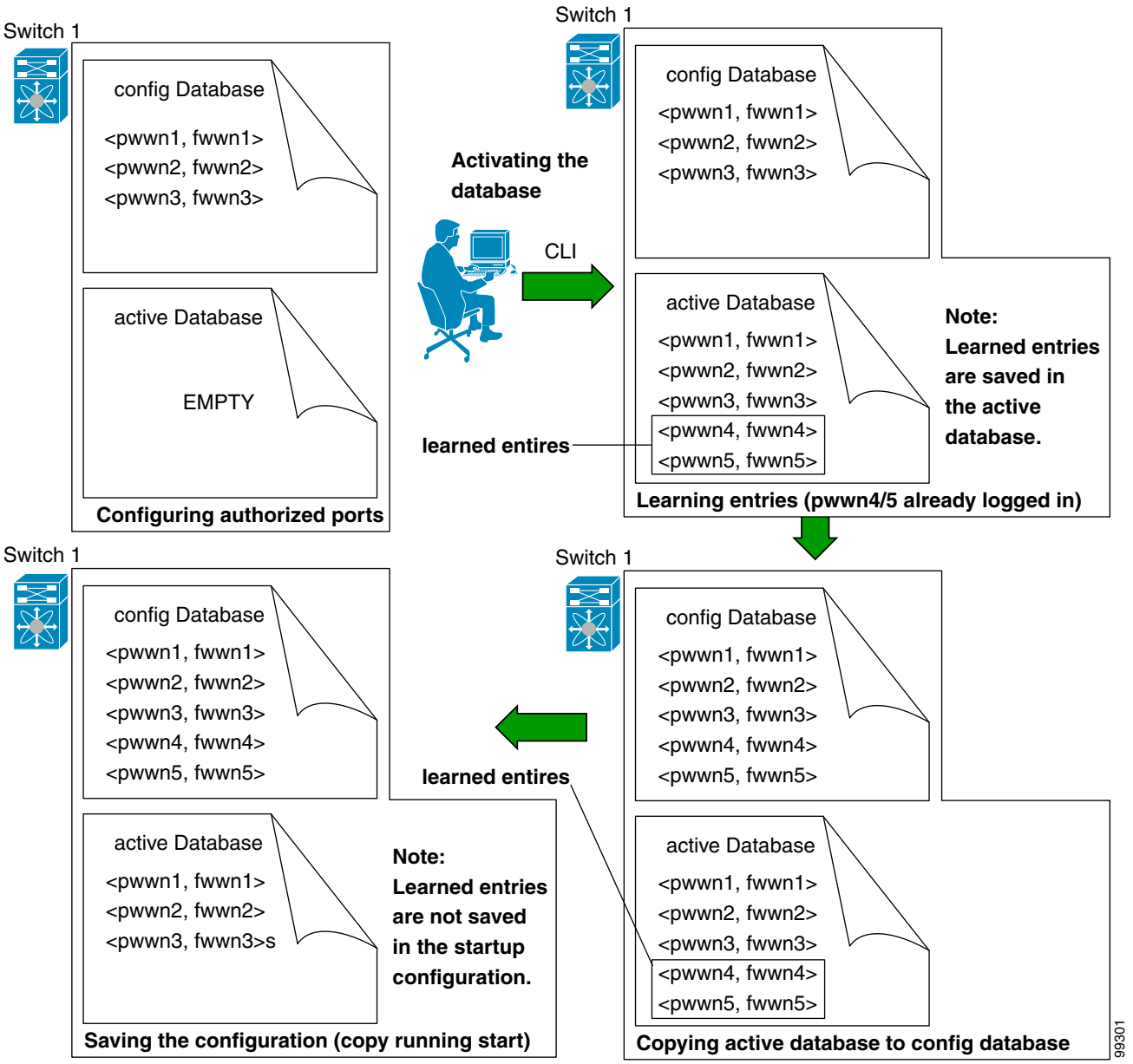
Table 31-3 Active and Configuration Port Security Databases

Configuration Database	Active Database
Read-write.	Read-only.
Saving the configuration saves all the entries in the configuration database.	Saving the configuration only saves the activated entries. Learned entries are not saved.
Once activated, the configuration database can be modified without any effect on the active database.	Once activated, all devices that have already logged into the VSAN are also learned and added to the active database.
You can overwrite the configuration database with the active database.	You can overwrite the active database with the configured database by activating the port security database. Forcing an activation may violate the entries already configured in the active database.

Database Scenarios

The various scenarios in Figure 31-1 depict the active database and the configuration database status based on port security configurations.

Figure 31-1 Port Security Database Scenarios



Activating the Port Security Database

When you activate the port security database, all entries in the configured database are copied to the active database. After the database is activated, subsequent device login is subject to the activated port bound WWN pairs. Additionally, all devices that have already logged into the VSAN at the time of activation are also learned and added to the active database. If the auto-learn feature is already enabled in a VSAN, you will not be allowed to activate the database.

To activate port security with auto-learn disabled, follow these steps:

Step 1 From Fabric Manager, choose VSANxxx > **Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

From Device Manager, **Choose Security > Port...**. You see the Port Security dialog box.

Step 2 Click the **Actions** tab.

Step 3 Click in the **Action** column under Activation, next to the switch or VSAN on which you want to activate port security. You see a drop-down menu with the following options:

- activate—Valid port security settings are activated.
- activate (TurnLearningOff)—Valid port security settings are activated and autolearn turned off.
- forceActivate—Activation is forced.
- forceActivate(TurnLearningOff)—Activation is forced and autolearn is turned off.
- deactivate—All currently active port security settings are deactivated.
- NoSelection— No action is taken.

Step 4 Set the Action field you want for that switch.

Step 5 Uncheck the **AutoLearn** check box for each switch in the VSAN to disable auto-learning.

Step 6 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 7 Click the **Apply Changes** icon in Fabric Manager or **Apply** in Device Manager to save these changes or click **Undo Changes** in Fabric Manager or **Close** in Device Manager to discard any unsaved changes.

Database Activation Rejection

Database activation is rejected in the following cases:

- Missing or conflicting entries exist in the configuration database but not in the active database.
- If the auto-learn feature was enabled before the activation. To reactivate a database in this state.
- The exact security is not configured for each PortChannel member.
- The configured database is empty but the active database is not.

If the database activation is rejected due to one or more conflicts listed in the previous section, you may decide to proceed by forcing the port security activation.

Forceful Port Security Activation

If the auto-learn option was enabled before the activation, reactivate the database.If the database activation is rejected due to one or more conflicts listed in the previous section, you may decide to proceed with the activation by using the forceActivate option.

See the "Activating the Port Security Database" section on page 31-10.

Note An activation using the forceActivate option logs out existing devices if they violate the active database.

Database Reactivation

Tip If the auto-learn option is enabled and you activate the database, you will not be allowed to proceed.

To reactivate the database using Fabric Manager, follow these steps:

Step 1 Disable auto-learning.

Step 2 Copy the active database to the configured database.

Tip If the active database is empty, you cannot perform this step.

Step 3 Activate the database.

Copying an Active Database to the Config Database

To copy the active database to the config database using Fabric Manager, follow these steps:

Step 1 Choose VSANxxx > **Port Securit**y from the Logical Domains pane. You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Actions** tab. You see the switches for that VSAN.

Step 3 Check the **CopyActive ToConfig** check box next to the switch for which you want to copy the database.

The active database is copied to the config database when the security setting is activated.

Step 4 Uncheck the check box if you do not want the database copied when the security setting is activated.

Step 5 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 6 Click the **Apply Changes** icon to save these changes or click **Undo Changes** to discard any unsaved changes.