CHAPTER 20

Configuring Port Security

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

Note Port security is only supported for Fibre Channel ports.

This chapter contains the following topics:

Port Security Features

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 syslog messages.

Enforcing Port Security

To enforce port security, 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.

Configuring a Port Binding

To configure a port binding on a switch, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays port security information for that VSAN.

Step 2 Click the **Config** tab.

You see a list of the port security configured port bindings for that VSAN.

Step 3 Click the **Create Row** icon.

The Create Binding dialog box displays.

Step 4 Choose the switch for which you want to create the port binding from drop-down list.

Step 5 Choose the WWN DEVICE device type for that switch.

Step 6 Enter the PORT ID of the switch to bind to.

Step 7 Enter the port type.

Step 8 Enter the interface (e.g. fc1/1)

Step 9 Click **Create** to creating the port binding, or click **Close** to close the Create Binding dialog box without creating a port binding.

Copying an Active Configuration to the Running Configuration

To copy the active configuration to the running configuration, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Action** tab.

You see a list of switches for that VSAN.

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

The active configuration is copied to the running configuration when the binding is activated.

Step 4 Uncheck the check box if you do not want the configuration copied when the binding is activated.

Deleting a Port Binding

To delete a port binding on a switch, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Config** tab.

You see a list of the port security configured port bindings for that VSAN.

Step 3 Click the row you want to delete.

Step 4 Click the **Delete Row** icon.

You see a confirmation dialog box.

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

About Auto-Learn

You can instruct the switch to automatically learn (auto-learn) the port security configurations over a specified period. The **auto-learn** option 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 port security feature for the first time as it saves tedious 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. Learned entries on a port are cleaned up after a **shutdown** command is issued on that port.

Activating Port Security

By default, the port security feature is not activated.

When you activate the port security feature, the **auto-learn** option is also automatically enabled. You can choose to activate the port-security feature and disable auto-learn. In this case, you need to manually populate the port security database by individually securing each port.

Activating a Port Binding

To activate a port security port binding, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Action** tab.

You see a list of switches for that VSAN.

Step 3 Click in the Action column under Activation, next to the switch for which you want to activate a port binding.

Step 4 Choose the port binding option that you want to apply to the switch from the drop-down menu. Choose from the following options:

- Activate—Valid port bindings are activated.
- Activate (TurnLearningOff)—Valid port bindings are activated and the **auto-learn** option is turned off.
- ForceActivate—Activation is forced.
- ForceActivate (TurnLearningOff)—Activation is forced and the **auto-learn** option is turned off.
- Deactivate—Deactivates all currently active port bindings.
- NoSelection—No action is taken

Displaying Activated Port Bindings

To display port security active port bindings, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays port security information for that VSAN.

Step 2 Click the **Active** tab.

You see a list of the port security active port bindings for that VSAN.

Configuring Auto-Learning

The state of the auto-learning configuration depends on the state of the port security feature:

- If the port security feature is not activated, the **auto-learn** option is disabled by default.
- If the port security feature is activated, the **auto-learn** option is enabled by default.

If the **auto-learn** option is enabled on a VSAN, you cannot activate the database for that VSAN without the **force** option.

Table 20-1 summarizes the authorized connection for device requests.

Table 20-1 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	Aport that is not configured	Permitted if **auto-learn** option enabled	3
Denied if **auto-learn** disabled	4		

Table 20-1 Auto-learn Device Authorization (continued)

Configured or not configured	A switch port that allows any device	Permitted	5
Configured to login to any switch port	Any port on the switch	Permitted	6
Not configured	A port configured with some other device	Denied	7

Authorization Scenario

Assuming 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 20-2 summarizes the port security authorization results for this active database.

Table 20-2 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
10	S2, F11	Denied	7	P10 is bound to F11

Table 20-2 Authorization Results for Scenario (continued)

Scenario	Device Connection Request	Authorization	Condition	Reason
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

Turning Auto-Learning On or Off

To turn Auto-learning on or off, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays Port Security information for that VSAN.

Step 2 Click the **Action** tab.

You see a list of switches for that VSAN.

Step 3 Click in the AutoLearn column next to the switch for which you want to enable AutoLearning.

Step 4 Choose **on** from the drop-down menu to turn on AutoLearning; choose **off** to turn off AutoLearning for that switch.

Manually Configuring Port Security

To configure port security in 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.

Identifying WWNs to Configure Port Security

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

- Identify switch ports by the interface or the fWWN.
- Identify devices by the pWWN or 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.
- Saving the running configuration saves the configuration database and activated entries in the active database. Learned entries in the active database are not saved.

Securing Authorized Ports

After identifying the WWN pairs that need to be bound, add those pairs to the port security database.

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** option is already enabled in a VSAN, you will not be allowed to activate the database.

Database activation is rejected in the following cases:

- Missing or conflicting entries exist in the configuration database but not in the active database.
- The **auto-learn** option was enabled before the activation.
- The exact security is not configured for each PortChannel member.
- If the configured database is empty and the active database is not.

Forcing Port Security Activation

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 **force** option.

An activation using the **force** option logs out existing devices if they violate the active database.

Reactivating the Database

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

Database Scenarios

Table 20-3 lists the differences and interaction between the active and configuration databases.

Table 20-3 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. An activation using the **force** option may violate the entries already configured in the active database.

Displaying Port Security Statistics

To display port security statistics, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays port security information for that VSAN.

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, perform the following steps.

Step 1 From the Fabric Manager, choose **Port Security** from one of the VSANs on the menu tree.

The Information pane of the Fabric Manager displays port security information for that VSAN.

Step 2 Click the **Violations** tab.

You see a list of the port security violations for that VSAN.

Default Port Security Settings

Table 20-4 lists the default settings for all security features in any switch.

Table 20-4 Default Security Settings

Parameters	Default
Auto-learn	Enabled if port security is enabled
Port security	Disabled