CHAPTER 15

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.

This chapter includes the following sections:

Note Port security is only supported for Fibre Channel ports.

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.

The security enforcement is performed when the port tries to come up (**no shutdown** command).

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.

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 learnt, even if you have not configured any port access. Learnt 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.

To enable the port security feature, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.

	Command	Purpose
Step 2	`switch(config)# port-security activate vsan 1`	Activates the port security database for the specified VSAN, and automatically enables auto-learn.
	`switch(config)# no port-security activate vsan 1`	Deactivates the port security database for the specified VSAN, and automatically disables auto-learn.

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** using the **port-security activate vsan** *number* **no-auto-learn** command. In this case, you need to manually populate the port security database by individually securing each port.

To enable the port security feature, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security activate vsan 1 no-auto-learn`	Disables the auto-learn feature for the port security database in VSAN 1.

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 (unless it is turned off using the **port-security activate vsan** *number* **no-auto-learn** command).

To enable the auto-learn option, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security auto-learn vsan 1`	Enables auto-learning so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database.
	`switch(config)# no port-security auto-learn vsan 1`	Disables auto-learning and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learnt up to this point.

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

Table 15-1 summarizes the authorized connection for device requests.

Table 15-1 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 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 15-2 summarizes the port security authorization results for this active database.

Table 15-2 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

Table 15-2 Authorization Results for Scenario (continued)

Scenario	Device Connection Request	Authorization	Condition	Reason
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
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

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 (see the "Identifying WWNs to Configure Port Security" section on page 15-5).

Step 2 Secure the fWWN to an authorized nWWN or pWWN (see the Securing Authorized Ports, page 15-6).

Step 3 Activate the port security database (see the Activating the Port Security Database, page 15-6).

Step 4 Verify your configuration (see the Displaying Port Security Commands, page 15-10)

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 (using the **copy running start** command) saves the configuration database and activated entries in the active database. Learnt 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.

To configure port security, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security database vsan 1` `switch(config-port-security)#`	Enters the port security database mode for the specified VSAN.
	`switch(config)# no port-security database vsan 1` `switch(config)#`	Deletes the port security configuration database from the specified VSAN.
Step 3	`switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5`	Configures the specified sWWN to only login through PortChannel 5.
	`switch(config-port-security)# any-wwn interface fc1/1 - fc1/8`	Configures any WWN to login through the specified interfaces.
	`switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e`	Configures the specified pWWN to only log in through the specified fWWN.
	`switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e`	Deletes the specified pWWN configured in the previous step.
	`switch(config-port-security)# nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e`	Configures the specified nWWN to log in through the specified fWWN.
	`switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66`	Configures the specified pWWN to login through any port on the local switch.
	`switch(config-port-security)# any-wwn interface fc3/1`	Configures any WWN to log in through the specified interface.
	`switch(config-port-security)# no any-wwn interface fc2/1`	Deletes the wildcard configured in the previous step.

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 learnt 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 (see the About Auto-Learn, page 15-2).

To activate the port database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security activate vsan 1` `switch(config-port-security)#`	Activates the port security database for the specified VSAN, and automatically turns on the auto-learn feature.
	`switch(config)# no port-security activate vsan 1`	Deactivates port security, deletes the active database, and disables auto-learn.

Database activation is rejected in the following cases:

- Missing or conflicting entries exist in the configuration database but not in the active database. View such entries using the **port-security database diff active vsan** command.
- The **auto-learn** option was enabled before the activation. See the "Forcing Port Security Activation" section on page 15-7 to reactivate a database in this state.
- 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.

Note An activation using the **force** option does not log out existing devices even if they violate the active database.

To forcefully activate the port security database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security activate vsan 1 force`	Forces the VSAN 1 port security database to activate despite conflicts.
	`switch(config)# no port-security activate vsan 1 force`	Reverts to the previously-configured state or to the factory default (if no state is configured).

Reactivating the Database

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

To reactivate the database, follow these steps:

Step 1 Disable the **auto-learn** option (the **no port-security auto-learn vsan** *number* command).

Step 2 Copy the active database to the configured database (the **port-security database copy vsan** command). This command will overwrite the configuration database with the active database.

Step 3 Activate the database using the **port-security activate vsan** *number* command.

Copying the Port Security Database

Use the **port-security database copy vsan** command to copy from the active to the configured database. If the active database is empty, this command is not accepted.

```
switch# port-security database copy vsan 1
switch#
```

Use the **port-security database diff active vsan** command to view the differences between the active database and the configuration database. This command can be used when resolving conflicts.

```
switch# port-security database diff active vsan 1
```

Use the **port-security database diff config vsan** command to obtain information on the differences between the configuration database and the active database.

```
switch# port-security database diff config vsan 1
```

Database Scenarios

Table 15-3 lists the differences and interaction between the active and configuration databases.

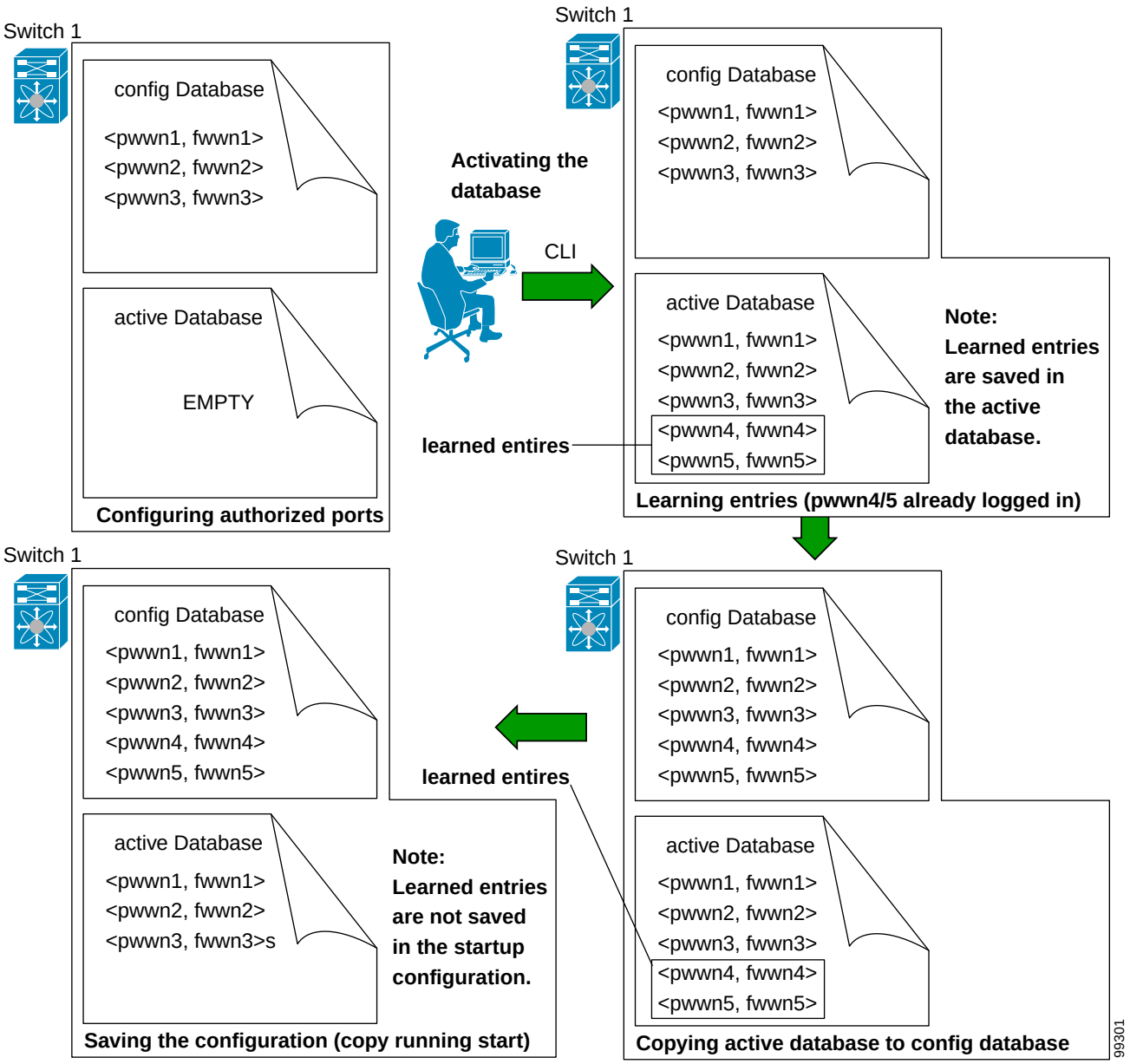
Table 15-3 Active and Configuration Port Security Databases

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. Learnt 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 learnt and added to the active database.
You can overwrite the configuration database with the active database using the **port-security database copy vsan** command).	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.

The **port-security database diff active vsa**n command lists the differences between the active database and the configuration database.

Figure 15-1 depicts various scenarios to depict the active database and the configuration database status based on port security configurations.

Figure 15-1 Port Security Database Scenarios



Clearing the Port Security Database

Use the **clear port-security statistics** command to clear all existing statistics from the port security database for a specified VSAN.

```
switch# clear port-security statistics vsan 1
```

Use the **clear port-security database auto-learn interface** command to clear any learnt entries in the active database for a specified interface within a VSAN. The active database is read-only and this command can be used when resolving conflicts.

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

Use the **clear port-security database auto-learn** command to clear any learnt entries in the active database up to for the entire VSAN. The active database is read-only and this command can be used when resolving conflicts.

```
switch# clear port-security database auto-learn vsan 1
```

Deleting the Port Security Database

Use the **no port-security** command in configuration mode to delete the configured database for a specified VSAN

```
switch(config)# no port-security database vsan 1
switch(config)#
```

Displaying Port Security Commands

The **show port-security database** commands display the configured port security information (see Examples 15-1 to 15-9). The

Example 15-1 Displays the Contents of the Port Security Database

```
switch# show port-security database
--------------------------------------------------------------------------------
VSAN    Logging-in Entity             Logging-in Point(     Interface)
--------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn) 20:0d:00:05:30:00:95:de(fc1/13)
1       50:06:04:82:bc:01:c3:84(pwwn) 20:0c:00:05:30:00:95:de(fc1/12)
2       20:00:00:05:30:00:95:df(swwn) 20:0c:00:05:30:00:95:de(port-channel 128)
3       20:00:00:05:30:00:95:de(swwn) 20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

You can optionally specify a fWWN and a VSAN, or an interface and a VSAN in the **show port-security** command to view the output of the activated port security (see Example 15-2).

Example 15-2 Displays the Port Security Database in VSAN 1

```
switch# show port-security database vsan 1
--------------------------------------------------------------------------------
Vsan   Logging-in Entity             Logging-in Point        (Interface)
--------------------------------------------------------------------------------
```

```
1                  *                  20:85:00:44:22:00:4a:9e (fc3/5)
1      20:11:00:33:11:00:2a:4a(pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]
```

Example 15-3 Displays the Activated Database

```
switch# show port-security database active
--------------------------------------------------------------------------------
VSAN    Logging-in Entity             Logging-in Point(     Interface)     Learnt
--------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn) 20:0d:00:05:30:00:95:de(fc1/13)          Yes
1       50:06:04:82:bc:01:c3:84(pwwn) 20:0c:00:05:30:00:95:de(fc1/12)          Yes
2       20:00:00:05:30:00:95:df(swwn) 20:0c:00:05:30:00:95:de(port-channel 128)Yes
3       20:00:00:05:30:00:95:de(swwn) 20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

The access information for each port can be individually displayed. If you specify the fwwn or interface options, all devices that are paired in the active database (at that point) with the given fWWN or the interface are displayed (see Examples 15-4 to 15-6).

Example 15-4 Displays the Wildcard fWWN Port Security in VSAN 1

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
Any port can login thru' this fwwn
```

Example 15-5 Displays the Configured fWWN Port Security in VSAN 1

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

Example 15-6 Displays the Interface Port Information in VSAN 2

```
switch# show port-security database interface fc 1/1 vsan 2
20:00:00:0c:88:00:4a:e2(swwn)
```

The port security statistics are constantly updated and available at any time (see Example 15-7).

Example 15-7 Displays the Port Security Statistics

```
switch# show port-security statistics
Statistics For VSAN: 1
-----------------------
Number of pWWN permit: 2
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0

Total Logins permitted  : 4
Total Logins denied     : 0
Statistics For VSAN: 2
-----------------------
Number of pWWN permit: 0
Number of nWWN permit: 0
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
```

```
Number of sWWN deny  : 0
...
```

To verify the status of the active database and the auto-learn configuration, use the **show port-security status** command (see Example 15-8).

Example 15-8 Displays the Port Security Status

```
switch# show port-security status
VSAN 1 :Activated database, auto-learning is enabled
VSAN 2 :No Active database, auto-learning is disabled
...
```

The **show port-security** command displays the previous 100 violations by default. (see Example 15-9).

Example 15-9 Displays the Violations in the Port Security Database

```
switch# show port-security violations


-------------------------------------------------------------------------------
VSAN    Interface      Logging-in Entity             Last-Time              [Repeat count]
-------------------------------------------------------------------------------
1       fc1/13         21:00:00:e0:8b:06:d9:1d(pwwn) Jul  9 08:32:20 2003   [20]
                       20:00:00:e0:8b:06:d9:1d(nwwn)
1       fc1/12         50:06:04:82:bc:01:c3:84(pwwn) Jul  9 08:32:20 2003   [1]
                       50:06:04:82:bc:01:c3:84(nwwn)
2       port-channel 1 20:00:00:05:30:00:95:de(swwn) Jul  9 08:32:40 2003   [1]
[Total 2 entries]
```

The **show port-security** command issued with the **last** *number* option displays only the specified number of entries that appear first.

Default Port Security Settings

Table 15-4 lists the default settings for all security features in any switch.

Table 15-4 Default Security Settings

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