CHAPTER 32

# Configuring 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:

# 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 system messages.
- Configuration distribution uses the CFS infrastructure, and is limited to those switches that are CFS capable. Distribution is disabled by default.
- Configuring the port security policy requires the ENTERPRISE_PKG license (see Chapter 3, "Obtaining and Installing Licenses").

## Port Security Enforcement

To enforce port security, configure the devices and switch port interfaces through which each device or switch is connected, and activate the configuration.

- 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 uses two databases to accept and implement configurations.

- Configuration database—All configuration changes are stored in the configuration database.
- Active database—The database currently enforced by the fabric. 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.

# Port Security Initiation

By default, the port security feature is disabled in all switches in the Cisco MDS 9000 Family.

To enable port security, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t` | Enters configuration mode. |
| **Step 2** | `switch(config)# port-security enable` | Enables port security on that switch. |
| | `switch(config)# no port-security enable` | Disables (default) port security on that switch. |

# Port Security Manual Configuration

To 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.

## Authorized Port Pair Addition

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

**Tip** Remote switch binding can be specified at the local switch. To specify the remote interfaces, you can use either the fWWN or sWWN-interface combination.

To configure port security, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# port-security database vsan 1`<br>`switch(config-port-security)#` | Enters the port security database mode for the specified VSAN. |
| | `switch(config)# no port-security database vsan 1`<br>`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 log in through PortChannel 5. |
| | `switch(config-port-security)# any-wwn interface fc1/1 - fc1/8` | Configures any WWN to log in 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 log in through any port in the fabric. |
| | `switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80` | Configures the specified pWWN to log in through any interface in the specified switch. |
| | `switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80 interface fc3/1` | Configures the specified pWWN to log in through the specified interface in the specified switch |
| | `switch(config-port-security)# any-wwn interface fc3/1` | Configures any WWN to log in through the specified interface in any switch. |
| | `switch(config-port-security)# no any-wwn interface fc2/1` | Deletes the wildcard configured in the previous step. |

# Port Security Activation

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

When you activate the port security feature, the following apply:

- Auto-learning is also automatically enabled. When auto-learning is enabled, the following apply:
  - From this point, learning happens only for the devices or interfaces that were not activated.
  - You will not be allowed to activate the database till you disable learning.
- All the logged-in devices are learned and are added to the active 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.

When you activate the port security feature, the auto-learning is also automatically enabled. You can choose to activate the port security feature and disable autolearning.

To activate the port security feature, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# port-security activate vsan 1` | Activates the port security database for the specified VSAN, and automatically enables auto-learning. |
| | `switch(config)# port-security activate vsan 1 no-auto-learn` | Activates the port security database for the specified VSAN, and disables auto-learning. |
| | `switch(config)# no port-security activate vsan 1` | Deactivates the port security database for the specified VSAN, and automatically disables auto-learning. |

**Note** If required, you can disable autolearning (see the "Disabling Autolearning" section on page 32-7).

# 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.

# Forcing Port Security Activation

If the port security activation request is rejected, you can force the activation

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

You can view missing or conflicting entries using the **port-security database diff active vsan** command in EXEC mode.

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

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`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. |

# Database Reactivation

**Tip** If the auto-learning' is enabled and you activate the database, you will not be allowed to proceed.

To reactivate the database, 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** Make the required changes to the configuration database.

**Step 4** Activate the database.

To reactivate the port security database, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# no port-security auto-learn vsan 1` | Disables auto-learn and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learned up to this point. |
| **Step 3** | `switch(config)# exit`<br>`switch# port-security database copy vsan 1` | Copy from the active to the configured database. |
| **Step 4** | `switch# config t`<br>`switch(config)# port-security activate vsan 1` | Activates the port security database for the specified VSAN, and automatically enables auto-learn. |

# About Auto-Learning

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 tedious manual configuration for each port. You must configure auto-learning 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 you shut down that port. Learning does not override the enforced port security policies.

When you activate the port security feature autolearning is also automatically enabled. When auto-learning is enabled, the following apply:

- Learning happens only for the devices or interfaces that were not activated.
- You will not be allowed to activate the database.

## Enabling 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, auto-learning is disabled by default.
- If the port security feature is activated, auto-learning is enabled by default (unless you explicitly disabled this option).

**Tip** If auto-learning is enabled on a VSAN, you can only activate the database for that VSAN by using the **force** option.

To enable auto-learning, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# port-security auto-learn vsan 1` | Enables auto-learn 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. |

## Disabling Autolearning

To disable autolearning, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# no port-security auto-learn vsan 1` | Disables auto-learn and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learned up to this point. |

# Auto-Learning Device Authorization

Table 32-1 summarizes the authorized connection for device requests.

*Table 32-1 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 |

# Authorization Scenario

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 32-2 summarizes the port security authorization results for this active database.

*Table 32-2 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. |

*Table 32-2 Authorization Results for Scenario (continued)*

| Scenario | Device Connection Request | Authorization | Condition | Reason |
|---|---|---|---|---|
| 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. |
| 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. |

# Port Security Configuration Distribution

The port security feature uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management, provide a single point of configuration for the entire fabric in the VSAN, and enforce the port security policies on throughout the fabric (see Chapter 5, “Using the CFS Infrastructure”).

## Enabling Distribution

All the configurations performed in distributed mode are stored in a pending (temporary) database. If you modify the configuration, you need to commit or discard the pending database changes to the configurations. The fabric remains locked during this period. Changes to the pending database are not reflected in the configurations until you commit the changes.

To enable the port security distribution, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch#` **`config t`**<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)#` **`port-security distribute`** | Enables distribution. |
| | `switch(config)#` **`no port-security distribute`** | Disables distribution. |

## Locking The Fabric

The first action that modifies the existing configuration creates the pending database and locks the feature in the VSAN. Once you lock the fabric, the following situations apply:

- No other user can make any configuration changes to this feature.
- A copy of the configuration database becomes the pending database.

## Committing the Changes

If you commit the changes made to the configurations, the configurations in the pending database are distributed to other switches. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

To commit the port security configuration changes for the specified VSAN, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# port-security commit vsan 3` | Commits the port security changes in the specified VSAN. |

## Discarding the Changes

If you discard (abort) the changes made to the pending database, the configurations remains unaffected and the lock is released.

To discard the port security configuration changes for the specified VSAN, follow these steps:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `switch# config t`<br>`switch(config)#` | Enters configuration mode. |
| **Step 2** | `switch(config)# port-security abort vsan 5` | Discards the port security changes in the specified VSAN and clears the pending configuration database. |

## Activation and Autolearning Configuration Distribution

Activation and autolearning configurations in distributed mode are remembered merely as actions to be performed when you commit the changes in the pending database.

Learned entries are temporary and do not have any role in determining if a login is authorized or not. As such, learned entries do not participate in distribution. When you disable learning and commit the changes in the pending database, the learned entries become static entries in the active database and are distributed to all switches in the fabric. After the commit, the active database on all switches are identical and learning can be disabled.

If the pending database contains more than one activation and autolearning configuration when you commit the changes, then the activation and autolearning changes are consolidated and the behavior may change (see Table 32-3).

If you activate port security, follow up by disabling auto-learning , and finally commit the changes in the pending database, then the net result of your actions is the same as issuing a **port-security activate vsan** *vsan-id* **no-auto-learn** command.

*Table 32-3 Scenarios for Activation and Autolearning Configurations in Distributed Mode*

| Scenario | Actions | Distribution = OFF | Distribution = ON |
|---|---|---|---|
| A and B exist in the configuration database, activation is not done and devices C,D are logged in. | **1.** You activate the port security database and enable autolearning. | configuration database = {A,B}<br>active database = {A,B, C[1], D*} | configuration database = {A,B}<br>active database = {null}<br>pending database = {A,B + activation to be enabled} |
| | **2.** A new entry E is added to the configuration database. | configuration database = {A,B, E}<br>active database = {A,B, C*, D*} | configuration database = {A,B}<br>active database = {null}<br>pending database = {A,B, E + activation to be enabled} |
| | **3.** You issue a commit. | Not applicable | configuration database = {A,B, E}<br>active database = {A,B, E, C*, D*}<br>pending database = empty |
| A and B exist in the configuration database, activation is not done and devices C,D are logged in. | **1.** You activate the port security database and enable autolearning. | configuration database = {A,B}<br>active database = {A,B, C*, D*} | configuration database = {A,B}<br>active database = {null}<br>pending database = {A,B + activation to be enabled} |
| | **2.** You disable learning. | configuration database = {A,B}<br>active database = {A,B, C, D} | configuration database = {A,B}<br>active database = {null}<br>pending database = {A,B + activation to be enabled +<br>learning to be disabled} |
| | **3.** You issue a commit. | Not applicable | configuration database = {A,B}<br>active database = {A,B} and devices C and D are logged out. This is equal to an activation with autolearning disabled.<br>pending database = empty |

1. The * (asterisk) indicates learned entries.

**Tip** In this case, we recommend that you perform a commit at the end of each operation: after you activate port security and after you enable auto learning.

# Database Merge Guidelines

A database merge refers to a union of the configuration database and static (unlearned) entries in the active database. See the "CFS Merge Support" section on page 5-7 for detailed concepts.

When merging the database between two fabric, follow these guidelines:

- Verify that the activation status and the auto-learn status is the same is both fabrics.
- Verify that the combined number of configuration for each VSAN in both databases does not exceed 2K.

**Caution** If you do not follow these two conditions, the merge will fail. The next distribution will forcefully synchronize the databases and the activation states in the fabric.

# Database Interaction

Table 32-4 lists the differences and interaction between the active and configuration databases.

***Table 32-4 Active and Configuration Port Security Databases***

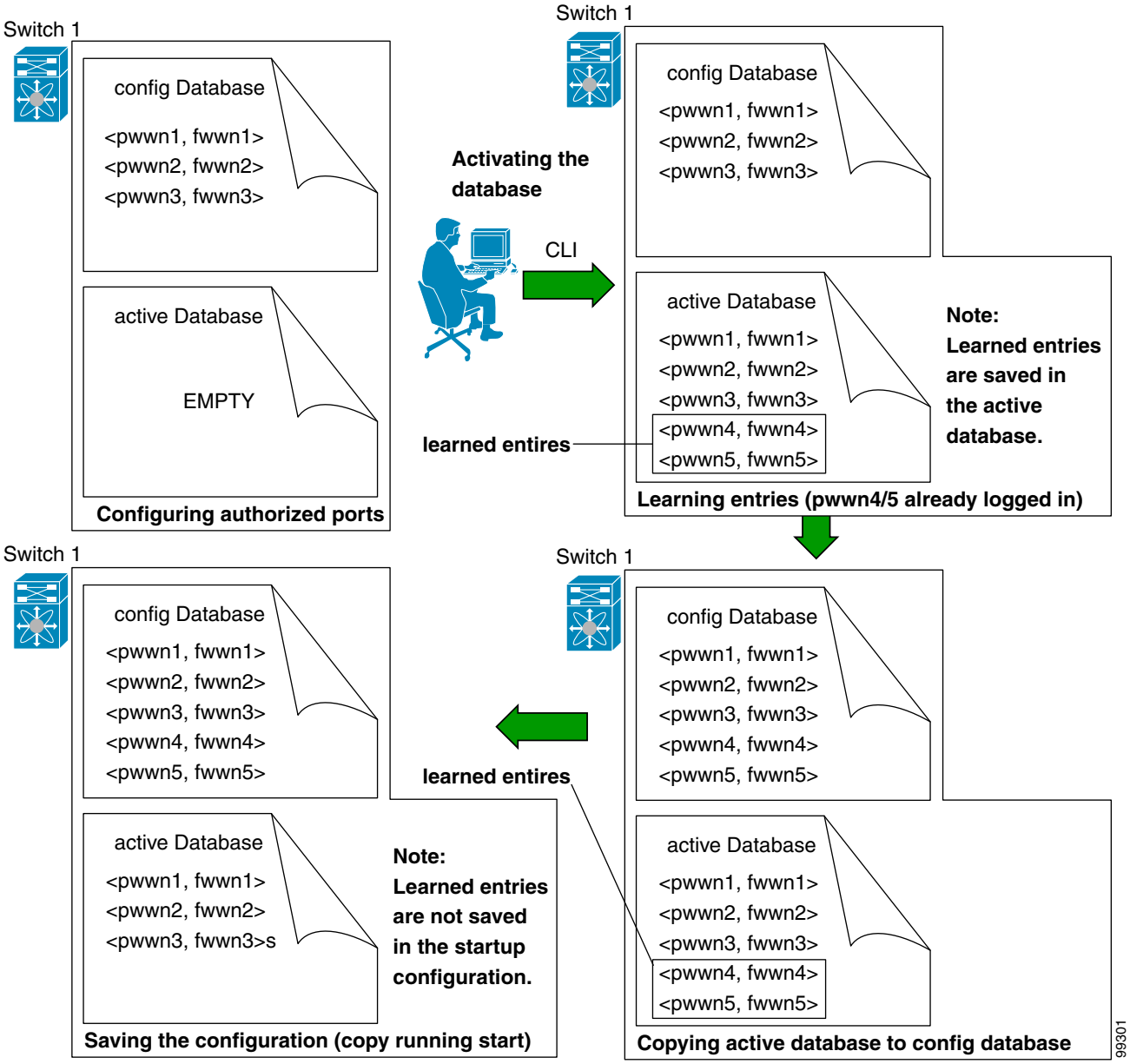
| Configuration Database | Active Database |
|---|---|
| Read-write. | Read-only. |
| Saving the configuration saves all the entries in the configuration database. | Saving the configuration only saves the activated entries. Learned entries are not saved. |
| Once activated, the configuration database 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. |

**Note** You can overwrite the configuration database with the active database using the **port-security database copy vsan** command. The **port-security database diff active vsa**n command in EXEC mode lists the differences between the active database and the configuration database.

## Database Scenarios

Figure 32-1 depicts various scenarios to depict the active database and the configuration database status based on port security configurations.

*Figure 32-1 Port Security Database Scenarios*




# Port Security Database Copy

**Tip** We recommended that you issue **port-security database copy vsan** command after disabling autolearning. This action will ensure that t the configuration database is in sync with the active database. If distribution is enabled, this command results in acquire of temporary copy (and consequently a fabric lock) of the configuration database. If you lock the fabric, you need to commit the changes to the configuration database of all the switches.

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
```

# Port Security Database Deletion

**Tip** If the distribution is enabled, the deletion creates a copy of the database. An explicit **port-security commit** command is required to actually delete the database.

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

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

# Port Security Database Cleanup

Use the **clear port-security statistics vsan** 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 learned entries in the active database for a specified interface within a VSAN.

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

Use the **clear port-security database auto-learn vsan** command to clear any learned entries in the active database up to for the entire VSAN.

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

**Note** The **clear port-security database auto-learn** and **clear port-security statistics** commands are only relevant to the local switch and do not acquire locks. Also, learned entries are only local to the switch and do not participate in distribution.

Use the **port-security clear vsan** command to clear the pending session in the VSAN from any switch in the VSAN.

```
switch# clear port-security session vsan 5
```

# Displaying Port Security Configurations

The **show port-security database** commands display the configured port security information (see Examples 32-1 to 32-11).

***Example 32-1 Displays the Contents of the Port Security Configuration 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 32-2).

***Example 32-2 Displays the Port Security Configuration 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 32-3 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]
```

*Example 32-4 Displays the Contents of the Temporary Configuration Database*

```
switch# show port-security pending vsan 1
Session Context for VSAN 1
--------------------------
Activation Status: Active
Auto Learn Status: On
Force activate: No
Config db modified: Yes
Activation done: Yes
Session owner: admin(2)
Session database:
-------------------------------------------------------------------------------
VSAN Logging-in Entity Logging-in Point (Interface)
-------------------------------------------------------------------------------
1 20:11:00:33:22:00:2a:4a(pwwn) 20:41:00:05:30:00:4a:1e(fc2/1)
[Total 1 entries]
```

*Example 32-5 Displays the Difference between the Temporary Configuration Database and the Configuration Database*

```
switch# show port-security pending-diff vsan 1
Session Diff for VSAN: 1
------------------------
Database will be activated
Learning will be turned ON
Database Diff:
+pwwn 20:11:00:33:22:00:2a:4a fwwn 20:41:00:05:30:00:4a:1e
```

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 32-6 to 32-8).

*Example 32-6 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 32-7 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 32-8 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 32-9).

***Example 32-9 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 32-10).

***Example 32-10 Displays the Port Security Status***

```
switch# show port-security status
Fabric Distribution Enabled
VSAN 1 :No Active database, learning is disabled, Session Lock Taken
VSAN 2 :No Active database, learning is disabled, Session Lock Taken
...
```

The **show port-security** command displays the previous 100 violations by default (see Example 32-11).

***Example 32-11 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 Settings

Table 32-5 lists the default settings for all port security features in any switch.

*Table 32-5 Default Security Settings*

| Parameters | Default |
|---|---|
| Auto-learn | Enabled if port security is enabled. |
| Port security | Disabled. |
| Distribution | Disabled.<br>**Note** Enabling distribution enables it on all VSANs in the switch. |