Configuring Port Security

This chapter describes how to configure port security.

This chapter includes the following sections:

Configuring Port Security

Cisco SAN switches provide port security features that reject intrusion attempts and report these intrusions to the administrator.

Note Port security is supported on virtual Fibre Channel ports.

Information 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, using the following methods:

- Login requests from unauthorized Fibre Channel devices (N 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.

Note Port security is supported on virtual Fibre Channel ports.

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 N port connection for each device.
- Use the switch world wide name (sWWN) to specify the xE port connection for each switch.

Each N 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 configuration changes.

- 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.

Auto-Learning

You can instruct the switch to automatically learn (auto-learn) the port security configurations over a specified period. This feature allows the switch to automatically learn about devices and switches that connect to it. Use this feature when you activate the port security feature for the first time beacuse it saves tedious manual configuration for each port. You must configure auto-learning 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.

When auto-learning is enabled, learning occurs only for the devices or interfaces that were not already logged into the switch. Learned entries on a port are cleaned up after you shut down that port if auto-learning is still enabled.

Learning does not override the existing configured port security policies. For example, if an interface is configured to allow a specific pWWN, auto-learning does not add a new entry to allow any other pWWN on that interface. All other pWWNs are blocked even in auto-learning mode.

No entries are learned for a port in the shutdown state.

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

Note If you enable auto-learning before activating port security, you cannot activate port security until auto-learning is disabled.

Port Security Activation

By default, the port security feature is not activated.

When you activate the port security feature, the following operations occur:

- Auto-learning is also automatically enabled, which means the following:
  - From this point, auto-learning occurs only for the devices or interfaces that were not logged into the switch.
  - You cannot activate the database until you disable auto-learning.
- All the devices that are already logged in 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, excluding the auto-learned entries. You must disable auto-learning before the auto-learned entries become activated.

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

If a port is shut down because of a denied login attempt, and you subsequently configure the database to allow that login, the port does not come up automatically. You must explicitly enter the **no shutdown** command to bring that port back online.

Configuring Port Security

Configuring Port Security with Auto-Learning and CFS Distribution

You can configure port security using auto-learning and CFS distribution.

Procedure

Step 1 Enable port security.

Step 2 Enable CFS distribution.

Step 3 Activate port security on each VSAN.

This action turns on auto-learning by default.

Step 4 Issue a CFS commit to copy this configuration to all switches in the fabric.

All switches have port security activated with auto-learning enabled.

Step 5 Wait until all switches and all hosts are automatically learned.

Step 6 Disable auto-learning on each VSAN.

Step 7 Issue a CFS commit to copy this configuration to all switches in the fabric.

The auto-learned entries from every switch are combined into a static active database that is distributed to all switches.

Step 8 Copy the active database to the configure database on each VSAN.

Step 9 Issue a CFS commit to copy this configuration to all switches in the fabric.

This action ensures that the configured database is the same on all switches in the fabric.

Step 10 Copy the running configuration to the startup configuration, using the fabric option.

Related Topics

Activating Port Security, on page 5
Committing the Changes, on page 10
Copying the Port Security Database, on page 15
Disabling Auto-Learning, on page 7

Enabling Port Security, on page 4
Enabling Port Security Distribution, on page 9

Configuring Port Security with Auto-Learning without CFS

You can configure port security using auto-learning without Cisco Fabric Services (CFS).

Procedure

Step 1 Enable port security.

Step 2 Activate port security on each VSAN, which turns on auto-learning by default.

Step 3 Wait until all switches and all hosts are automatically learned.

Step 4 Disable auto-learning on each VSAN.

Step 5 Copy the active database to the configured database on each VSAN.

Step 6 Copy the running configuration to the startup configuration, which saves the port security configuration database to the startup configuration.

Step 7 Repeat the above steps for all switches in the fabric.

Related Topics

Activating Port Security, on page 5
Copying the Port Security Database, on page 15
Disabling Auto-Learning, on page 7
Enabling Port Security, on page 4

Configuring Port Security with Manual Database Configuration

You can configure port security and manually configure the port security database.

Procedure

Step 1 Enable port security.

Step 2 Manually configure all port security entries into the configured database on each VSAN.

Step 3 Activate port security on each VSAN. This action turns on auto-learning by default.

Step 4 Disable auto-learning on each VSAN.

Step 5 Copy the running configuration to the startup configuration, which saves the port security configuration database to the startup configuration.

Step 6 Repeat the above steps for all switches in the fabric.

Enabling Port Security

You can enable port security.

By default, the port security feature is disabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Port Security Activation

Activating Port Security

You can activate port security.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

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.
- The auto-learning feature was enabled before the activation. To reactivate a database in this state, disable auto-learning.
- The exact security is not configured for each port channel 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

You can forcefully activate the port security database.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Database Reactivation

You can reactivate the port security database.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no no port-security auto-learn vsan** *vsan-id* **Example:** `switch(config)# no no port-security auto-learn vsan 35`	Disables auto-learning and stops the switch from learning about new devices that access the switch. This command also enforces the database contents based on the devices learned up to this point.
Step 3	**exit** **Example:** `switch(config)# exit`	Exits the configuration mode.
Step 4	**port-security database copy vsan** *vsan-id* **Example:** `switch# port-security database copy vsan 35`	Copies from the active to the configured database.

Step 5	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Reenters configuration mode.

Step 6	**port-security activate vsan** *vsan-id* **Example:** `switch(config)# port-security activate vsan 35`	Activates the port security database for the specified VSAN, and automatically enables auto-learning.

Auto-Learning

About 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.

Enabling Auto-Learning

You can enable 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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**port-security auto-learn vsan** *vsan-id* **Example:** `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.

Disabling Auto-Learning

You can disable auto-learning.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no port-security auto-learn vsan** *vsan-id* **Example:** `switch(config)# no port-security auto-learn vsan 23`	Disables auto-learning and stops the switch from learning about new devices that access the switch. This command enforces the database contents based on the devices learned up to this point.

Auto-Learning Device Authorization

The following table summarizes the authorized connection conditions for device requests.

Table 1: Authorized Auto-Learning Device Requests

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

Port Security Manual Configuration

You can manually configure port security.

Procedure

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 Guidelines

The WWN Identification has the following configuration guidelines and limitations:

- Identify switch ports by the interface or by the fWWN.
- Identify devices by the pWWN or by the nWWN.
- If an N port is allowed to log in to a SAN switch port F, that N port can only log in through the specified F port.
- If an N port's nWWN is bound to an F port WWN, all pWWNs in the N port are implicitly paired with the F port.
- TE port checking is done on each VSAN in the allowed VSAN list of the VSAN trunk port.
- You must configure all port channel xE ports with the same set of WWNs in the same SAN port channel.
- 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, you can modify the configuration database 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.

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 throughout the fabric.

Enabling Port Security Distribution

You can enable port security distribution.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**port-security distribute** **Example:** `switch(config)# port-security distribute`	Enables distribution.

	Command or Action	Purpose
Step 3	**no port-security distribute** **Example:** `switch(config)# no port-security distribute`	Disables distribution.

Related Topics

Activation and Auto-Learning Configuration Distribution, on page 11

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

You can commit the port security configuration changes for the specified VSAN.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**port-security commit vsan** *vsan-id* **Example:** `switch(config)# port-security commit vsan 100`	Commits the port security changes in the specified VSAN.

Discarding the Changes

You can discard the port security configuration changes for the specified VSAN.

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**port-security abort vsan** *vsan-id* **Example:** `switch(config)# port-security abort vsan 35`	Discards the port security changes in the specified VSAN and clears the pending configuration database.

Activation and Auto-Learning Configuration Distribution

Activation and auto-learning configurations in distributed mode are remembered 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 auto-learning configuration when you commit the changes, the activation and auto-learning changes are consolidated and the resulting operation may change (see the following table).

Table 2: Scenarios for Activation and Auto-Learning 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 and D are logged in.	1. You activate the port security database and enable auto-learning.	configuration database = {A,B} active database = {A,B, C[1], D*}	configuration database = {A,B} active database = {null} pending database = {A,B + activation to be enabled}
	2. A new entry E is added to the configuration database.	configuration database = {A,B, E} active database = {A,B, C*, D*}	configuration database = {A,B} active database = {null} pending database = {A,B, E + activation to be enabled}
	3. You issue a commit.	Not applicable	configuration database = {A,B, E} active database = {A,B, E, C*, D*} pending database = empty

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

[1] The * (asterisk) indicates learned entries.

Merging the Port Security Database

A database merge refers to a union of the configuration database and static (unlearned) entries in the active database.

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

- Verify that the activation status and the auto-learning status is the same in both fabrics.
- Verify that the combined number of configurations for each VSAN in both databases does not exceed 2000.

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

Database Interaction

The following table lists the differences and interaction between the active and configuration databases.

Table 3: Active and Configuration Port Security Databases

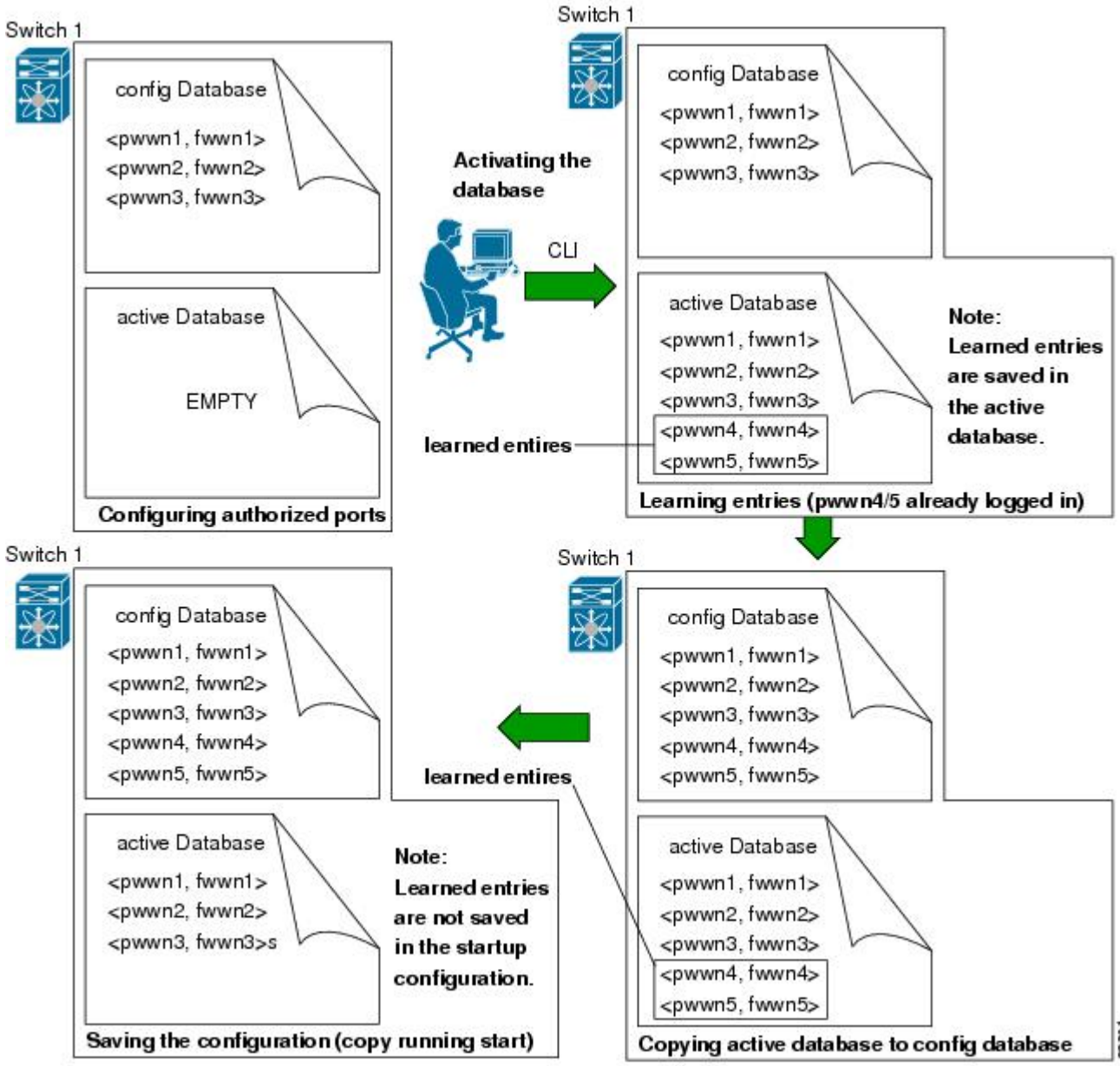
Active Database	Configuration Database
Read-only.	Read-write.
Saving the configuration only saves the activated entries. Learned entries are not saved.	Saving the configuration saves all the entries in the configuration database.

Active Database	Configuration Database
Once activated, all devices that have already logged into the VSAN are also learned and added to the active database.	Once activated, the configuration database can be modified without any effect on 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.	You can overwrite the configuration database with 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 vsan** command lists the differences between the active database and the configuration database.

The following figure shows various scenarios of the active database and the configuration database status based on port security configurations.

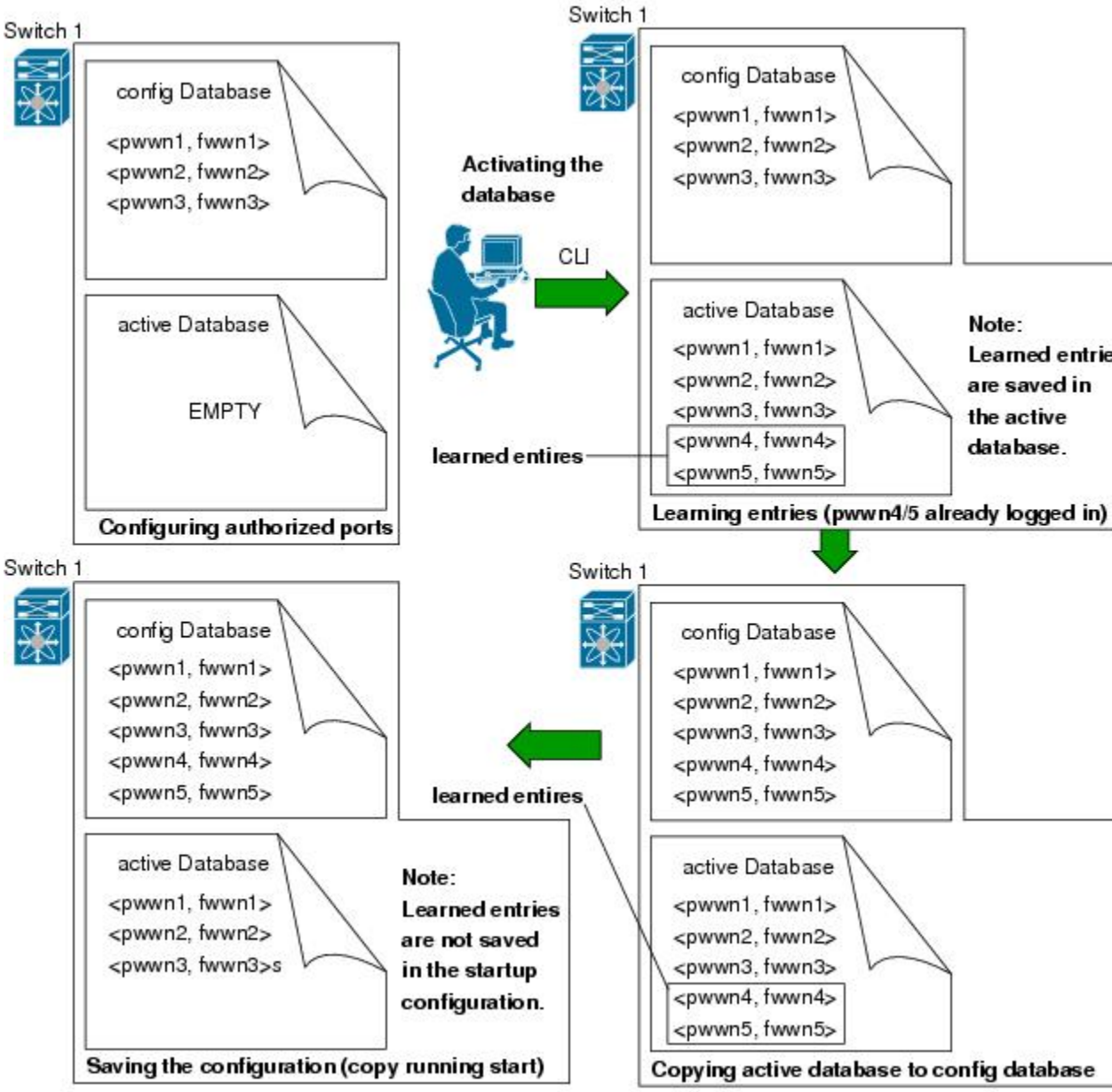
Figure 1: Port Security Database Scenarios



Database Scenarios

the following figure illustrates various scenarios showing the active database and the configuration database status based on port security configurations.

Figure 2: Port Security Database Scenarios



Copying the Port Security Database

Tip We recommend that you copy the active database to the config database after disabling auto-learning. This action ensures that the configuration database is in synchronization with the active database. If distribution is enabled, this command creates a temporary copy (and a fabric lock) of the configuration database. If you lock the fabric, you must commit the changes to the configuration databases in 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
```

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
```

Deleting the Port Security Database

Tip If the distribution is enabled, the deletion creates a copy of the database. You must enter the **port-security commit** command 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
```

Default Settings for Port Security

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

Table 4: Default Security Settings

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