CHAPTER 19

Troubleshooting FC-SP, Port Security, and Fabric Binding

This chapter describes procedures used to troubleshoot Fibre Channel Security Protocol (FC-SP), port security, and fabric binding in Cisco MDS 9000 Family products. It includes the following sections:

FC-SP Overview

FC-SP capabilities provide switch-switch and host-switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol that provides authentication between Cisco MDS 9000 Family switches and other devices. You can configure FC-SP to authenticate locally or to use a remote AAA server for authentication.

Port Security Overview

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.

Fabric Binding Overview

The fabric binding feature ensures ISLs are only enabled between specified switches in the fabric binding configuration. Fabric binding is configured on a per-VSAN basis.

This feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations. It uses the Exchange Fabric Membership Data (EFMD) protocol to ensure that the list of authorized switches is identical in all switches in the fabric.

Domain IDs are mandatory for FICON-based fabric binding and optional for non-FICON based fabric binding. For non-FICON based fabric binding, not specifying a domain ID means that the switch with the matching WWN can login with any domain ID.

Initial Troubleshooting Checklist

Begin troubleshooting FC-SP issues by checking the following issues:

Checklist	Check off
Verify licensing requirements. See *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.	❑
Verify that your installed HBAs support FC-SP.	❑
Verify that you have configured MD5 for the hash algorithm if you are authenticating through a RADIUS or TACACS+ server. RADIUS and TACACS+ always use MD5 for CHAP authentication. Using SHA-1 as the hash algorithm may prevent RADIUS and TACACS+ usage—even if these AAA protocols are enabled for DHCHAP authentication.	❑
Verify that your AAA server is functioning properly.	❑

Begin troubleshooting port security issues by checking the following issues:

Checklist	Check off
Verify that you have the ENTERPRISE_PKG license installed on all switches.	❑
Verify that port security is activated and that the end devices are present in the port security active database.	❑
Verify that no unauthorized devices (host or switch) are connected to a port. (One unauthorized pWWN prevents the port from being active and blocks all other devices on that port.)	❑

Begin troubleshooting fabric binding issues by checking the following issues:

Checklist	Check off
Verify that you have the ENTERPRISE_PKG or the MAINFRAME_PKG license installed on all switches.	❑
Verify that you have activated fabric binding.	❑
Verify that all switches in the fabric have the same fabric binding database settings.	❑

Common Troubleshooting Tools in Fabric Manager

Use the following Fabric Manager procedure to troubleshoot FC-SP issues:

- **Switches > Security > FC-SP**

Use the following Fabric Manager procedure to troubleshoot port security issues:

- **Fabric***xx* **> VSAN***xx* **> Port Security**

Use the following Fabric Manager procedure to troubleshoot fabric binding issues:

- **Fabric***xx* **> VSAN***xx* **> Fabric Binding**

Common Troubleshooting Commands in the CLI

Us e the following CLI commands to troubleshoot FC-SP issues:

- **show fcsp interface**
- **show fcsp internal event-history errors**
- **show fcsp dhchap**
- **show fcsp dhchap database**

Us e the following CLI commands to troubleshoot port security issues:

- **show port-security status**
- **show port-security database vsan**
- **show port-security database active vsan**
- **show port-security violations**
- **show port-security internal global**
- **show port-security internal info vsan**
- **show port-security internal state-history vsan**
- **show port-security internal commit-history vsan**
- **show port-security internal merge-history vsan**

Us e the following CLI commands to troubleshoot fabric binding issues:

- **show fabric-binding status**
- **show fabric-binding database vsan**
- **show fabric-binding database active vsan**
- **show fabric-binding violations**

- **show fabric-binding internal global**
- **show fabric-binding internal info**
- **show fabric-binding internal event-history**
- **show fabric-binding internal efmd event-history**

FC-SP Issues

This section describes troubleshooting FC-SP issues and includes the following topic:

Switch or Host Blocked from Fabric

Symptom Switch or host blocked from joining the fabric.

Table 19-1 Switch or Host Blocked From Fabric

Symptom	Possible Cause	Solution
Switch or host blocked from joining the fabric.	FC-SP not enabled on all switches.	Choose **Switches > Security > FC-SP**, set the command field to **enable,** and click **Apply Changes** on Fabric Manager to enable FC-SP. Or use the **fcsp enable** CLI command on all switches in your fabric.
	Local switch FC-SP password does not match remote password.	Choose **Switches > Security > FC-SP**, select the **General/Password** tab, and set the GenericPassword field in Fabric Manager. Or use the **fcsp dhchap password** CLI command to set the local switch password.
	FC-SP DHCHAP configuration does not match remote switch or host.	See the "Verifying FC-SP Configuration Using Fabric Manager" section on page 19-5 or the "Verifying FC-SP Configuration Using the CLI" section on page 19-5.
	Switch or host not in authentication database.	Add switch or host to the local or remote FC-SP database. See the "Verifying Local FC-SP Database Using Fabric Manager" section on page 19-5 or the "Verifying Local FC-SP Database Using the CLI" section on page 19-6.
	Host or switch does not support FC-SP.	Upgrade host or switch or use the auto-active or auto-passive DHCHAP mode. Choose **Switches > Interfaces > FC logical**, select the **FC-SP** tab, set the Mode field to **autoActive** or **autoPassive**, and click **Apply Changes** in Fabric Manager. Or use the **fcsp auto-active** or **fcsp auto-passive** CLI command in interface mode to set the DHCHAP mode.

Verifying FC-SP Configuration Using Fabric Manager

To verify the FC-SP configuration using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > FC-SP** and select the **General/Password** tab to view the configured DHCHAP timeout value.

Step 2 Set the Timeout field to modify the timeout value.

Step 3 Set the DH-CHAP HashList field to modify the DHCHAP hash algorithm.

Step 4 Set the DH-CHAP GroupList field to modify the DHCHAP group settings.

Verifying FC-SP Configuration Using the CLI

To verify the FC-SP configuration using the CLI, follow these steps:

Step 1 Use the **show fcsp** command to view the configured DHCHAP timeout value.

```
switch# show fcsp
fc-sp authentication TOV:30
```

Step 2 Use the **fcsp timeout** command to modify the timeout value.

```
switch(config)# fcsp timeout 60
```

Step 3 Use the **show fcsp dhchap** command to view the hash algorithm and group

```
switch# show fcsp dhchap
Supported Hash algorithms (in order of preference):
DHCHAP_HASH_MD5
DHCHAP_HASH_SHA_1

Supported Diffie Hellman group ids (in order of preference):
DHCHAP_GROUP_1536
```

Step 4 Use the **fcsp dhchap hash** command to modify the DHCHAP hash algorithm.

```
switch(config)# fcsp dhchap hash MD5
```

Step 5 Use the **fcsp dhchap group** command to modify the DHCHAP group settings.

```
switch(config)# fcsp dhchap group 2 3 4
```

Verifying Local FC-SP Database Using Fabric Manager

To verify the local FC-SP database using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > FC-SP** and select the **Local Passwords** tab and the **Remote Password** tab to view the configured switches and hosts.

Step 2 Choose **Switches > FC Services > WWN Manager** to find the sWWN for the switch.

Step 3 Choose **Switches > Interfaces > FC Logical** and select the **FLOGI** tab to find the pWWN for the host that you want to add to the FC-SP local database.

Step 4 Choose **Switches > Security > FC-SP**, select the **Local Passwords** tab, and then click **Create Row** to add a host or switch to the local database.

Step 5 Fill in the WWN and password fields and click **Create**.

Verifying Local FC-SP Database Using the CLI

To verify the local FC-SP database using the CLI, follow these steps:

Step 1 Use the **show fcsp dhchap database** command to view the configured switches and hosts.

```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:********
        Password for device with WWN:29:11:bb:cc:dd:33:11:22 is ********
        Password for device with WWN:30:11:bb:cc:dd:33:11:22 is ********

Other Devices' Passwords:
        Password for device with WWN:00:11:22:33:44:aa:bb:cc is ********
```

Step 2 Use the **show wwn switch** command on the switch that you want to add to the FC-SP local database to find the sWWN.

```
MDS-9216# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

Step 3 Use the **show flogi database interface** command to find the pWWN for the host that you want to add to the FC-SP local database.

```
switch# show flogi database interface fc1/7
--------------------------------------------------------------------------------
Interface     VSAN   FCID               PORT NAME                 NODE NAME
--------------------------------------------------------------------------------
fc1/7          1     0xd10fee     20:00:00:33:8b:00:00:00    20:00:00:33:8b:00:00:00

Total number of flogi = 1
```

Step 4 Use the **fcsp dhchap devicename** command to add a host or switch to the local database.

```
switch(config)# fcsp dhchap devicename 20:00:00:33:8b:00:00:00 password rtp9509
```

Authentication Fails When Using Cisco ACS

Symptom Authentication fails when using Cisco ACS.

Table 19-2 Authentication Fails When Using Cisco ACS

Symptom	Possible Cause	Solution
Authentication fails when using Cisco ACS.	sWWN does not match ACS entry.	Verify the sWWN and ACS entry. Choose **Switches > FC Services > WWN Manager** in Fabric Manager to find the sWWN for the switch. Or use the **show wwn switch** CLI command. Use the **show fcsp asciiwwn** *sWWN* CLI command to get an ASCII equivalent of the sWWN. On the Cisco ACS server, choose **User Setup**. Search for the ASCII equivalent of the sWWN in the User column of the User List.

Port Security Issues

This section describes troubleshooting port security issues and includes the following topics:

Note After correcting a port security configuration issue, you do not have to disable the interface and reenable it. The port comes up automatically after a port security reactivation if the problem was fixed.

Device Does Not Log into a Switch When AutoLearn Is Disabled

Symptom Device does not log into a switch when autolearn is disabled.

Table 19-3 Device Does Not Log into a Switch When Autolearn Is Disabled

Symptom	Possible Cause	Solution
Device does not log into a switch when autolearn is disabled.	Device pWWN not allowed on port.	Manually add the device to the configured port security database. See the "Verifying the Active Port Security Database Using Fabric Manager" section on page 19-9 or the "Verifying the Active Port Security Database Using the CLI" section on page 19-9.
	Port not configured for any device.	Add a device to the port in the port security database or turn on autolearn. See the "Configuring Port Security with Autolearn Using Fabric Manager" section on page 19-14 or the "Configuring Port Security with Autolearn Using the CLI" section on page 19-15.
	Device is configured for some other port.	Manually add the device to the configured port security database. See the "Verifying the Active Port Security Database Using Fabric Manager" section on page 19-9 or the "Verifying the Active Port Security Database Using the CLI" section on page 19-9.
	Port is shut down because of port security violation.	Remove the device causing the port security violation or add that device to the database. See the "Verifying Port Security Violations Using Fabric Manager" section on page 19-10 or the "Verifying Port Security Violations Using the CLI" section on page 19-11.

Device Does Not Log into a Switch When Autolearn Is Enabled

Symptom Device does not log into a switch when autolearn is enabled.

Table 19-4 Device Does Not Log into a Switch When Autolearn Is Enabled

Symptom	Possible Cause	Solution
Device does not log into a switch when autolearn is enabled.	Device is configured for some other port.	Manually remove the device from the configured port security database. See the "Verifying the Active Port Security Database Using Fabric Manager" section on page 19-9 or the "Verifying the Active Port Security Database Using the CLI" section on page 19-9.
	Port is shut down because of port security violation.	Remove the device causing the port security violation or add that device to the database. See the "Verifying Port Security Violations Using Fabric Manager" section on page 19-10 or the "Verifying Port Security Violations Using the CLI" section on page 19-11.

Verifying the Active Port Security Database Using Fabric Manager

To verify the active port security database using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Port Security** and select the **Active Database** tab to view the active entries in the database.

Step 2 Select the **Actions** tab, check the **CopyToConfig** check box, and click **Apply Changes** to copy the active database to the configure database.

Step 3 Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 4 Select the **Config Database** tab and click **Add Row** to add a new entry into the configure database.

Step 5 Fill in the WWNs and interface fields and click **Create**.

Step 6 Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 7 Select the **Actions** tab, select **activate(TurnLearning off)** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and reactivate port security.

Step 8 Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Verifying the Active Port Security Database Using the CLI

To verify the active port security database using the CLI, follow these steps:

Step 1 Use the **show port-security database active** command to view the active entries in the database.

```
switch# show port-security database active
-------------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point     (Interface)         Learnt
-------------------------------------------------------------------------------------
3      21:00:00:e0:8b:06:d9:1d(pwwn)   20:0d:00:05:30:00:95:de(fc1/13)           Yes
3       50:06:04:82:bc:01:c3:84(pwwn)   20:0c:00:05:30:00:95:de(fc1/12)
4       20:00:00:05:30:00:95:df(swwn)   20:0c:00:05:30:00:95:de(port-channel 128)
5       20:00:00:05:30:00:95:de(swwn)   20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

Step 2 Use the **port-security database copy** command to copy the active database to the configure database. This ensures that no learned entries are lost.

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

Step 3 Use the **port-security database** command to add a new entry into the configure database.

```
switch(config)# port-security database vsan 3
switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80
interface fc1/13
```

Step 4 Use the **port-security activate** command to copy the configure database to the active database and reactivate port security.

```
switch(config)# port-security activate vsan 1
```

Step 5 If CFS distribution is enabled, use the **port-security commit** command to distribute these changes.

```
switch(config)# port-security commit vsan 3
```

Verifying Port Security Violations Using Fabric Manager

To verify port security violations using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Port Security** and select the **Violations** tab to search for an interface that is shut down.

Step 2 Optionally follow these steps to add the device to the port security database:

a. Choose **Fabric*xx* > VSAN*xx* > Port Security** and select the **Actions** tab.

b. Check the **CopyActive to Config** check box and click **Apply Changes** to copy the active database to the configure database. This ensures that no learned entries are lost.

c. Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

d. Select the **Config Database** tab and click **Add Row** to add a new entry into the configure database.

e. Fill in the WWNs and interface fields and click **Create**.

f. Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

g. Select the **Actions** tab, select **activate(TurnLearning off)** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and reactivate port security.

h. Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 3 Optionally, remove the device from the switch, choose **Switches > Interfaces > FC Physical** and select **up** from the Admin Status drop-down menu to bring the port back online. Click **Apply Changes**.

Note You may need to set the interface down and then up to bring it back online.

Verifying Port Security Violations Using the CLI

To verify port security violations using the CLI, follow these steps:

Step 1 Use the **show port-security violations** command and search for the interface that is shut down.

```
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]
```

In this example, pWWN `21:00:00:e0:8b:06:d9:1d` is causing interface fc1/13 to be shut down because of port security violations.

Step 2 Optionally follow these steps to add the device to the port security database:

a. Use the **port-security database copy** command to copy the active database to the configure database. This ensures that no learned entries are lost.

```
switch# port-security database copy vsan 3
```

b. Use the **port-security database** command to add a new entry into the configure database.

```
switch(config)# port-security database vsan 3
switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn
20:00:00:0c:85:90:3e:80 interface fc1/13
```

c. Use the **port-security activate** command to copy the configure database to the active database and reactivate port security.

```
switch(config)# port-security activate vsan 3
```

d. If CFS distribution is enabled, use the **port-security commit** command to distribute these changes.

```
switch(config)# port-security commit vsan 3
```

e. Use the **no shutdown** command in interface mode to bring the port back online.

Step 3 Optionally, remove the device from the switch and use the **no shutdown** command to bring the port back online.

Cannot Activate Port Security

Symptom Cannot activate port security.

Table 19-5 Cannot Activate Port Security

Symptom	Possible Cause	Solution
Cannot activate port security.	Autolearn is enabled.	See the "Disabling Autolearn Using Fabric Manager" section on page 19-13 or the "Disabling Autolearn Using the CLI" section on page 19-13.
	Conflicting entries in the configure database.	Remove the conflicting entries. Conflicting entries are those that when activated will cause existing logged in devices to logout. See the "Verifying the Active Port Security Database Using Fabric Manager" section on page 19-9 or the "Verifying the Active Port Security Database Using the CLI" section on page 19-9.
	Configure database is empty.	Choose **Fabric*xx* > VSAN*xx* > Port Security**, select the **Actions** tab, heck the **CopyActive to Config** check box, and click **Apply Changes** in Fabric Manager to copy the active database to the configure database. Or use the **port-security database copy** CLI command.
	Not all members of a PortChannel are configured for port security.	Add the missing members. Make sure that the sWWNs are the same for all the members. See the "Verifying the Active Port Security Database Using Fabric Manager" section on page 19-9 or the "Verifying the Active Port Security Database Using the CLI" section on page 19-9.

Unauthorized Device Gains Access to Fabric

Symptom Unauthorized device gains access to fabric.

Table 19-6 Unauthorized Device Gains Access to Fabric

Symptom	Possible Cause	Solution
Unauthorized device gains access to fabric.	Port security disabled.	See the "Configuring Port Security with Autolearn Using Fabric Manager" section on page 19-14 or the "Configuring Port Security with Autolearn Using the CLI" section on page 19-15.
	Port security not activated in the VSAN.	
	Autolearn is enabled.	Disable autolearn. See the "Disabling Autolearn Using Fabric Manager" section on page 19-13 or the "Disabling Autolearn Using the CLI" section on page 19-13.

Disabling Autolearn Using Fabric Manager

To disable autolearn using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Port Security** and select the **Actions** tab.

Step 2 Select **activate(TurnLearning off)** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and reactivate port security.

Step 3 Select the **CFS** tab, if CFS is enabled, and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 4 Copy the running configuration to the startup configuration, using the fabric option. This saves the port security configure database to the startup configuration on all switches in the fabric.

Disabling Autolearn Using the CLI

To disable autolearn using the CLI, follow these steps:

Step 1 Use the **no port-security auto-learn** command to disable autolearn.

```
switch# no port-security auto-learn vsan 2
```

Step 2 Use the **port-security database copy** command to copy the active database to the configure database. This ensures that no learned entries are lost.

```
switch# port-security database copy vsan 2
```

Step 3 If CFS distribution is enabled, use the **port-security commit** command to distribute these changes.

```
switch(config)# port-security commit vsan 2
```

Step 4 Copy the running configuration to the startup configuration, using the fabric option. This saves the port security configure database to the startup configuration on all switches in the fabric.

Port Security Settings Lost After Reboot

Symptom Port security settings were lost after a reboot.

Table 19-7 Port Security Settings Lost After Reboot

Symptom	Possible Cause	Solution
Port security settings were lost after a reboot.	Autolearn entries not saved to configure database and to startup configuration.	See the "Disabling Autolearn Using Fabric Manager" section on page 19-13 or the "Disabling Autolearn Using the CLI" section on page 19-13.

Merge Fails

Symptom Merge fails.

Table 19-8 Merge Fails

Symptom	Possible Cause	Solution
Merge fails	Activation or autolearn configuration in the separate fabrics do not match.	Disable autolearn. See the "Disabling Autolearn Using Fabric Manager" section on page 19-13 or the "Disabling Autolearn Using the CLI" section on page 19-13.
	Combined port security database contains more than 2047 entries.	Delete the port security database in one of the fabrics and then relearn the entries after the fabrics merge. See the "Configuring Port Security with Autolearn Using Fabric Manager" section on page 19-14 or the "Configuring Port Security with Autolearn Using the CLI" section on page 19-15.

Configuring Port Security with Autolearn Using Fabric Manager

To configure port security with autolearn using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Port Security** and select the **Control** tab.

Step 2 Select **enable** from the Command drop-down menu and click **Apply Changes**.

Step 3 Select the **CFS** tab and select **enable** from the Admin drop-down menu and select **enable** from the Global drop-down menu to enable CFS distribution.

Step 4 Select the **CFS** tab and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 5 Choose **Fabric*xx* > VSAN*xx* > Port Security**, select the **Actions** tab, and select **activate** from the Actions drop-down menu.

Step 6 Check the **AutoLearn** check box and click **Apply Changes** to enable autolearn.

Step 7 Select the **CFS** tab and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 8 Uncheck the **AutoLearn** check box and click **Apply Changes** to disable autolearn after all entries are learned.

Step 9 Select the **CFS** tab and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 10 Check the **CopyActive to Config** check box and click **Apply Changes** to copy the active database to the configure database. This ensures that no learned entries are lost.

Step 11 Select the **CFS** tab and select **commit** from the ConfigAction drop-down menu to distribute these changes to all switches in the fabric.

Step 12 Copy the running configuration to the startup configuration, using the fabric option. This saves the port security configure database to the startup configuration on all switches in the fabric.

Configuring Port Security with Autolearn Using the CLI

To configure port security with autolearn using the CLI, follow these steps:

Step 1 Use the **port-security enable** command to enable port security.

```
switch(config)# port-security enable
```

Step 2 Use the **port-security distribute** command to enable CFS distribution.

```
switch(config)# port-security distribute
```

Step 3 Use the **port-security activate** command to activate port security and enable autolearn.

```
switch(config)# port-security activate vsan 2
```

Step 4 If CFS distribution is enabled, use the **port-security commit** command to distribute these changes.

```
switch(config)# port-security commit vsan 2
```

Step 5 Use the **no port-security auto-learn** command in EXEC mode to disable autolearn after all entries have been learned.

```
switch# no port-security auto-learn vsan 2
```

Step 6 If CFS distribution is enabled, use the **port-security commit** command to distribute these changes.

```
switch(config)# port-security commit vsan 2
```

Step 7 Use the **port-security database copy** command to copy the active database to the configure database. This ensures that no learned entries are lost.

```
switch# port-security database copy vsan 2
```

Step 8 If CFS distribution is enabled, use the **port-security commit** command to distribute these changes.

```
switch(config)# port-security commit vsan 2
```

Step 9 Copy the running configuration to the startup configuration, using the fabric option. This saves the port security configure database to the startup configuration on all switches in the fabric.

Fabric Binding Issues

This section describes troubleshooting fabric binding issues and includes the following topic:

Note After correcting a fabric binding configuration issue, you do not have to disable the interface and reenable it. The port comes up automatically after a fabric binding reactivation if the problem was fixed.

Switch Cannot Attach to the Fabric

Symptom Switch cannot attach to the fabric.

Table 19-9 Switch Cannot Attach to the Fabric

Symptom	Possible Cause	Solution
Switch cannot attach to the fabric.	Fabric binding not activated on local switch. (It is activated on only one side of the ISL).	Activate fabric binding. Choose **Fabric*xx* > VSAN*xx* > Fabric Binding** and select the **Actions** tab**,** select **activate** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and activate fabric binding. Or use the **fabric-binding activate** CLI command.
	sWWN not present in fabric binding database.	Add sWWN to fabric binding database. See the "Verifying Fabric Binding Violations Using Fabric Manager" section on page 19-16 or the "Verifying Fabric Binding Violations Using the CLI" section on page 19-17
	Fabric binding database has sWWN with a different domain ID configured.	For non-FICON VSANs, you can remove the domain ID from the fabric binding database. Or update the domain ID in the fabric binding database (for FICON or NON-FICON VSANs). See the "Verifying Fabric Binding Violations Using Fabric Manager" section on page 19-16 or the "Verifying Fabric Binding Violations Using the CLI" section on page 19-17
	The local active fabric binding database is different from the other switches.	Update the fabric binding database and reactivate it. See the "Verifying Fabric Binding Violations Using Fabric Manager" section on page 19-16 or the "Verifying Fabric Binding Violations Using the CLI" section on page 19-17
	Switch blocked because of fabric binding violation.	Remove the device causing the fabric binding violation or add that device to the database. See the "Verifying Fabric Binding Violations Using Fabric Manager" section on page 19-16 or the "Verifying Fabric Binding Violations Using the CLI" section on page 19-17.

Verifying Fabric Binding Violations Using Fabric Manager

To verify fabric binding violations using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Fabric Binding** and select the **Violations** tab to search for an interface that is shut down.

Step 2 Optionally, remove the switch, choose **Switches > Interfaces > FC Physical,** and select **up** from the Admin Status drop-down menu to bring the port back online. Click **Apply Changes**.

Note You may need to set the interface down and then up to bring it back online.

Step 3 Optionally follow these steps to add the switch to the fabric binding database:

a. Choose **Fabric*xx* > VSAN*xx* > Fabric Binding** and select the **Actions** tab.

b. Check the **CopyActive to Config** check box and click **Apply Changes** to copy the active database to the configure database. This ensures that no learned entries are lost.

c. Select the **Config Database** tab and click **Add Row** to add a new entry into the configure database.

d. Fill in the WWNs and Domain ID fields and click **Create**.

e. Select the **Actions** tab, select **activate** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and reactivate fabric binding.

Verifying Fabric Binding Violations Using the CLI

To verify fabric binding violations using the CLI, follow these steps:

Step 1 Use the **show port-security violations** command and search for the interface that is shut down.

```
switch# show fabric-binding violations
-------------------------------------------------------------------------------
VSAN Switch WWN [domain] Last-Time [Repeat count] Reason
-------------------------------------------------------------------------------
2 20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003 [2] sWWN not found
3 20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003 [2] Domain mismatch
4 20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003 [1] Database mismatch
```

In VSAN 2, the sWWN itself was not found in the list. In VSAN 3, the sWWN was found in the list, but has a domain ID mismatch.

Step 2 Optionally, remove the switch and use the **no shutdown** command to bring the ISL back online.

Step 3 Optionally follow these steps to add the switch to the fabric binding database:

a. Use the **fabric-binding database copy** command to copy the active database to the configure database.

```
switch# fabric-binding database copy vsan 3
```

b. Use the **fabric-binding database** command to add a new entry into the configure database.

```
switch(config)# fabric-binding database vsan 3
switch(config-fabric-binding)# swwn 20:11:33:11:00:2a:4a:66
```

c. Use the **fabric-binding activate** command to copy the configure database to the active database and reactivate fabric binding.

```
switch(config)# fabric-binding activate vsan 3
```

d. **Use** the **no shutdown** command in interface mode to bring the port back online.

Cannot Activate Fabric Binding

Symptom Cannot activate fabric binding.

Table 19-10 Cannot Activate Fabric Binding

Symptom	Possible Cause	Solution
Cannot activate fabric binding.	Conflicting entries in the configure database.	Remove the conflicting entries. See the "Verifying the Config Fabric Binding Database Using Fabric Manager" section on page 19-18 or the "Verifying the Config Fabric Binding Database Using the CLI" section on page 19-18.

Verifying the Config Fabric Binding Database Using Fabric Manager

To verify the config fabric binding database using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Fabric Binding** and select the **Config Database** tab.

Step 2 Right-click on the conflicting entry and click **Delete Row** to remove this entry.

Step 3 Choose **Fabric*xx* > VSAN*xx* > Fabric Binding** and select the **Actions tab**

Step 4 Select **activate** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and reactivate fabric binding.

Verifying the Config Fabric Binding Database Using the CLI

To verify the config fabric binding database using the CLI, follow these steps:

Step 1 Use the **show fabric-binding database active** command to view the active entries in the database.

Step 2 Use the **fabric-binding database copy** command to copy the active database to the configure database.

```
switch# fabric-binding database copy vsan 1
```

Step 3 Use the fabric**-binding database** command to remove an entry from the configure database.

```
switch(config)# fabric-binding database vsan 3
switch(config-port-security)# no swwn 20:00:00:0c:85:90:3e:80
```

Step 4 Use the fabric**-binding activate** command to copy the configure database to the active database and reactivate fabric binding.

```
switch(config)# fabric-binding activate vsan 1
```

Unauthorized Switch Gains Access to Fabric

Symptom Unauthorized switch gains access to fabric.

Table 19-11 Unauthorized Switch Gains Access to Fabric

Symptom	Possible Cause	Solution
Unauthorized switch gains access to fabric.	Fabric binding disabled on both ends of an ISL.	See the "Configuring Fabric Binding Using Fabric Manager" section on page 19-19 or the "Configuring Fabric Binding Using the CLI" section on page 19-20.

Fabric Binding Settings Lost After Reboot

Symptom Fabric binding settings were lost after a reboot.

Table 19-12 Fabric Binding Settings Lost After Reboot

Symptom	Possible Cause	Solution
Fabric Binding settings were lost after a reboot.	Entries not saved to configure database and to startup configuration.	Save the fabric binding database. See the "Configuring Fabric Binding Using Fabric Manager" section on page 19-19 or the "Configuring Fabric Binding Using the CLI" section on page 19-20.

Configuring Fabric Binding Using Fabric Manager

To configure fabric binding using Fabric Manager, follow these steps:

Step 1 Choose **Fabric*xx* > VSAN*xx* > Fabric Binding** and select the **Control** tab.

Step 2 Select **enable** from the Command drop-down menu and click **Apply Changes**.

Step 3 Select the **Config Database** tab and click **Add Row** to add a new entry into the configure database.

Step 4 Fill in the WWNs and Domain ID fields and click **Create**.

Step 5 Select the **Actions** tab, select **activate** from the Action drop-down menu, and click **Apply Changes** to copy the configure database to the active database and reactivate fabric binding.

Step 6 Copy the running configuration to the startup configuration, using the fabric option. This saves the port security configure database to the startup configuration on all switches in the fabric.

Configuring Fabric Binding Using the CLI

To configure fabric binding using the CLI, follow these steps:

Step 1 Use the **fabric-binding enable** command to enable fabric binding.

```
switch(config)# fabric-binding enable
```

Step 2 Use the **fabric-binding database** command to add new entries into the configure database.

```
switch(config)# fabric-binding database vsan 3
switch(config-port-security)# swwn 20:00:00:0c:85:90:3e:80
```

Step 3 Use the **fabric-binding activate** command to activate fabric binding.

```
switch(config)# fabric-binding activate vsan 2
```

Step 4 Use the **fabric-binding database copy** command to copy the active database to the configure database.

```
switch# fabric-binding database copy vsan 2
```

Step 5 Copy the running configuration to the startup configuration, using the fabric option. This saves the fabric binding configure database to the startup configuration on all switches in the fabric.