



Configuring SAN Port Channels

SAN port channels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy.

On Cisco Nexus 5000 Series switches, SAN port channels can include physical Fibre Channel interfaces, but not virtual Fibre Channel interfaces. A SAN port channel can include up to eight Fibre Channel interfaces.

This chapter discusses the SAN port channel feature provided in the switch and includes the following sections:

- [Information About SAN Port Channels, page 14-1](#)
- [Configuring SAN Port Channels, page 14-5](#)
- [Interfaces in a SAN Port Channel, page 14-12](#)
- [Port Channel Protocol, page 14-15](#)
- [Verifying SAN Port Channel Configuration, page 14-19](#)
- [Default Settings, page 14-19](#)

Information About SAN Port Channels

A SAN port channel has the following functionality:

- Provides a point-to-point connection over ISL (E ports) or EISL (TE ports). Multiple links can be combined into a SAN port channel.
- Increases the aggregate bandwidth on an ISL by distributing traffic among all functional links in the channel.
- Load balances across multiple links and maintains optimum bandwidth utilization. Load balancing is based on the source ID, destination ID, and exchange ID (OX ID).
- Provides high availability on an ISL. If one link fails, traffic previously carried on this link is switched to the remaining links. If a link goes down in a SAN port channel, the upper layer protocol is not aware of it. To the upper layer protocol, the link is still there, although the bandwidth is diminished. The routing tables are not affected by link failure.

Cisco Nexus 5000 Series switches support a maximum of four SAN port channels (with eight interfaces per port channel). A port channel number refers to the unique (within each switch) identifier associated with each channel group. This number ranges from 1 to 256.

Send comments to nx5000-docfeedback@cisco.com

This section describes SANs and includes the following topics:

- [Understanding Port Channels and VSAN Trunking, page 14-2](#)
- [Understanding Load Balancing, page 14-3](#)

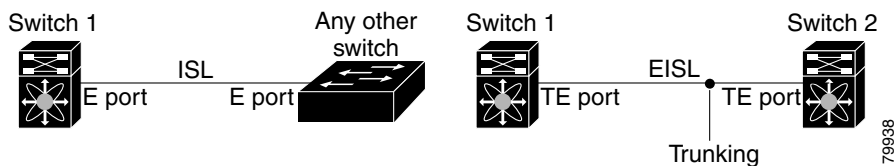
Understanding Port Channels and VSAN Trunking

Switches in the Cisco Nexus 5000 Series implement VSAN trunking and port channels as follows:

- A SAN port channel enables several physical links to be combined into one aggregated logical link.
- An industry standard E port can link to other vendor switches and is referred to as inter-switch link (ISL), as shown on the left side of [Figure 14-1](#).
- VSAN trunking enables a link transmitting frames in the EISL format to carry traffic for multiple VSAN. When trunking is operational on an E port, that E port becomes a TE port. EISLs connects only between Cisco switches, as shown on the right side of [Figure 14-1](#).

See [Chapter 13, “Configuring VSAN Trunking”](#) for information on trunk interfaces.

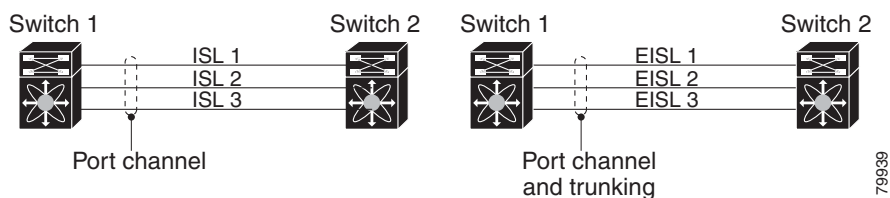
Figure 14-1 VSAN Trunking Only



You can create a SAN port channel with members that are E ports, as shown on the left side of [Figure 14-2](#). In this configuration, the port channel implements a logical ISL (carrying traffic for one VSAN).

You can create a SAN port channel with members that are TE-ports, as shown on the right side of [Figure 14-2](#). In this configuration, the port channel implements a logical EISL (carrying traffic for multiple VSANs).

Figure 14-2 Port Channels and VSAN Trunking



[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

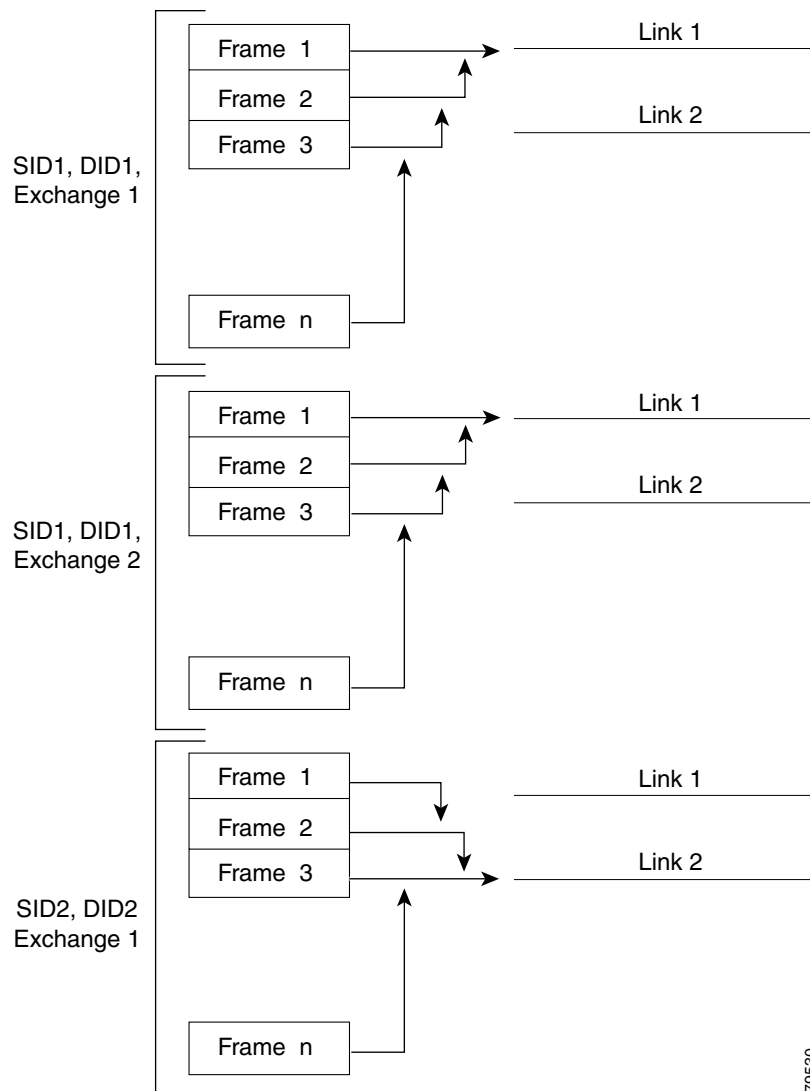
Understanding Load Balancing

Load-balancing functionality can be provided using the following methods:

- Flow based—All frames between source and destination follow the same links for a given flow. That is, whichever link is selected for the first exchange of the flow is used for all subsequent exchanges.
- Exchange based—The first frame in an exchange is assigned to a link, and then subsequent frames in the exchange follow the same link. However, subsequent exchanges can use a different link. This method provides finer granularity for load balancing while preserving the order of frames for each exchange.

Figure 14-3 illustrates how flow-based load balancing works. When the first frame in a flow is received on an interface for forwarding, link 1 is selected. Each subsequent frame in that flow is sent over the same link. No frame in SID1 and DID1 utilizes link 2.

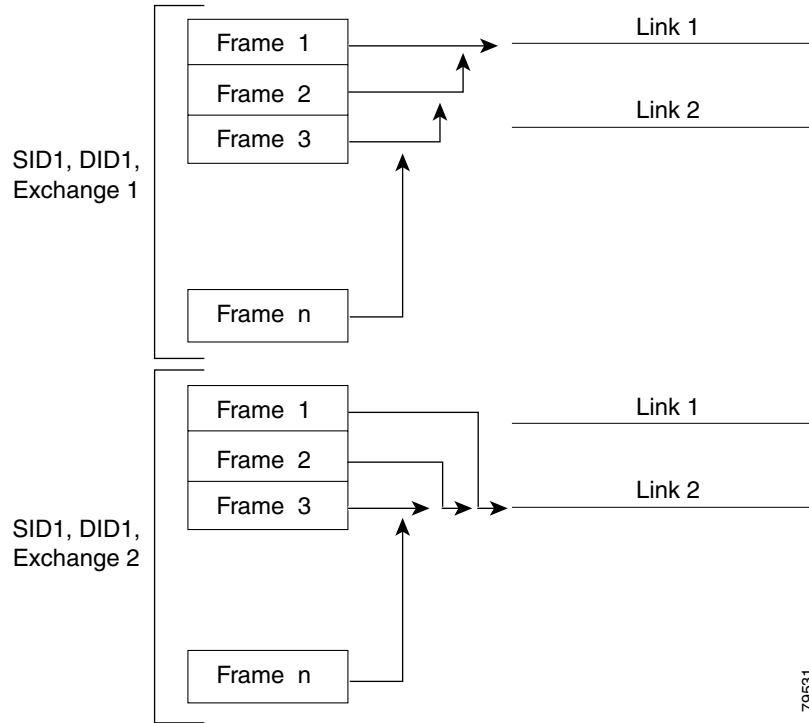
Figure 14-3 SID1, DID1, and Flow-Based Load Balancing



Send comments to nx5000-docfeedback@cisco.com

Figure 14-4 illustrates how exchange-based load balancing works. When the first frame in an exchange is received for forwarding on an interface, link 1 is chosen by a hash algorithm. All remaining frames in that particular exchange are sent on the same link. For exchange 1, no frame uses link 2. For the next exchange, link 2 is chosen by the hash algorithm. Now all frames in exchange 2 use link 2.

Figure 14-4 *SID1, DID1, and Exchange-Based Load Balancing*



[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Configuring SAN Port Channels

SAN port channels are created with default values. You can change the default configuration just as any other physical interface.

Figure 14-5 provides examples of valid SAN port channel configurations.

Figure 14-5 Valid SAN Port Channel Configurations

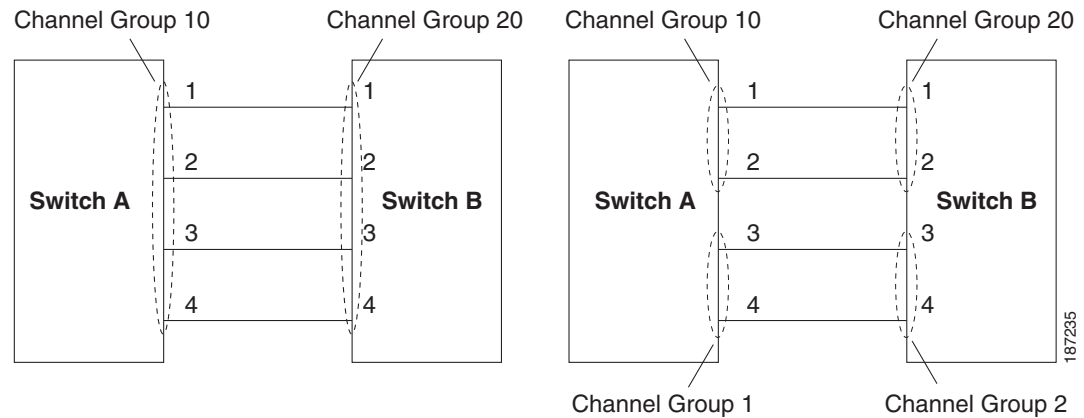
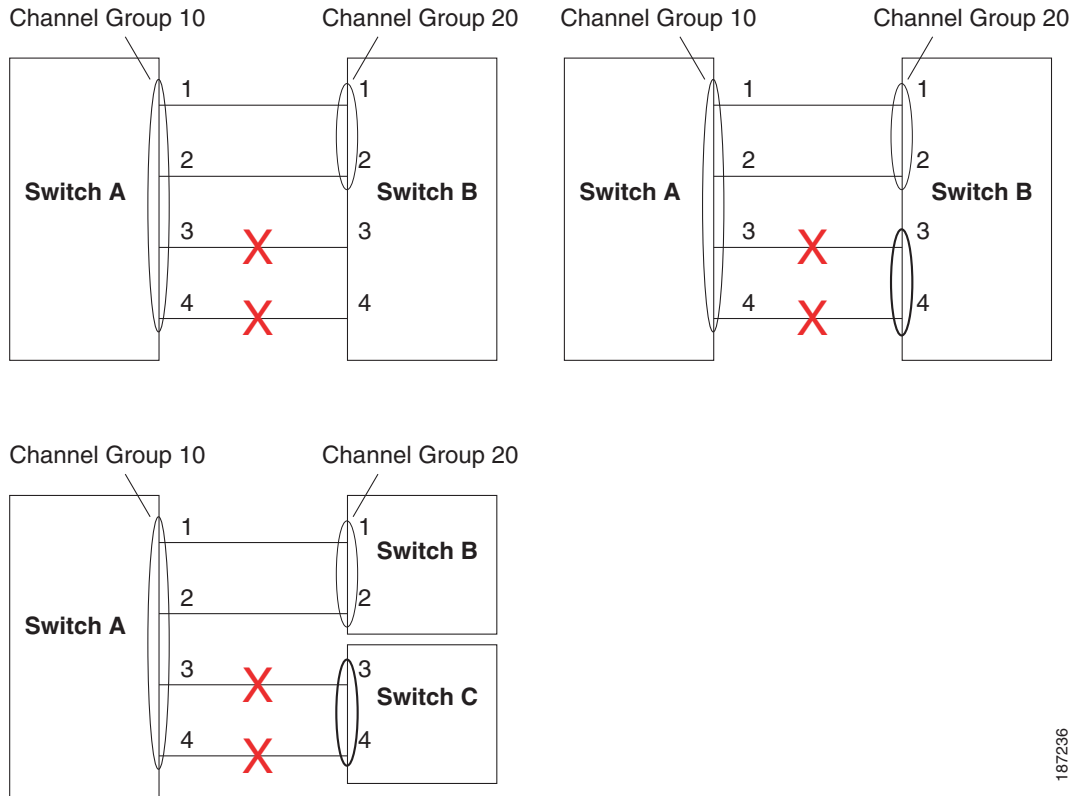


Figure 14-6 shows examples of invalid configurations. Assuming that the links are brought up in the 1, 2, 3, 4 sequence, links 3 and 4 will be operationally down as the fabric is misconfigured.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Figure 14-6 Misconfigured Configurations



187236

This section shows how to configure and modify SAN port channels and includes the following topics:

- [SAN Port Channel Configuration Guidelines, page 14-6](#)
- [Configuring SAN Port Channels, page 14-7](#)
- [About SAN Port Channel Modes, page 14-10](#)
- [About SAN Port Channel Deletion, page 14-11](#)
- [Deleting SAN Port Channels, page 14-11](#)

SAN Port Channel Configuration Guidelines

Before configuring a SAN port channel, consider the following guidelines:

- Configure the SAN port channel using Fibre Channel ports from both expansion modules to provide increased availability (if one of the expansion modules failed).
- Ensure that one SAN port channel is not connected to different sets of switches. SAN port channels require point-to-point connections between the same set of switches.

If you misconfigure SAN port channels, you may receive a misconfiguration message. If you receive this message, the port channel's physical links are disabled because an error has been detected.

Send comments to nx5000-docfeedback@cisco.com

If the following requirements are not met, a SAN port channel error is detected:

- Each switch on either side of a SAN port channel must be connected to the same number of interfaces.
- Each interface must be connected to a corresponding interface on the other side (see [Figure 14-6](#) for an example of an invalid configuration).
- Links in a SAN port channel cannot be changed after the port channel is configured. If you change the links after the port channel is configured, be sure to reconnect the links to interfaces within the port channel and reenables the links.

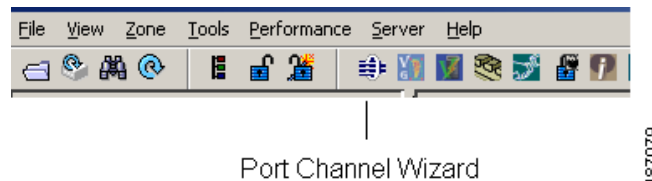
If all three conditions are not met, the faulty link is disabled.

Configuring SAN Port Channels

To create a SAN port channel using the Port Channel Wizard in Fabric Manager, perform this task:

- Step 1** Click the **Port Channel Wizard** icon in the toolbar (see [Figure 14-7](#)).

Figure 14-7 Port Channel Wizard Icon



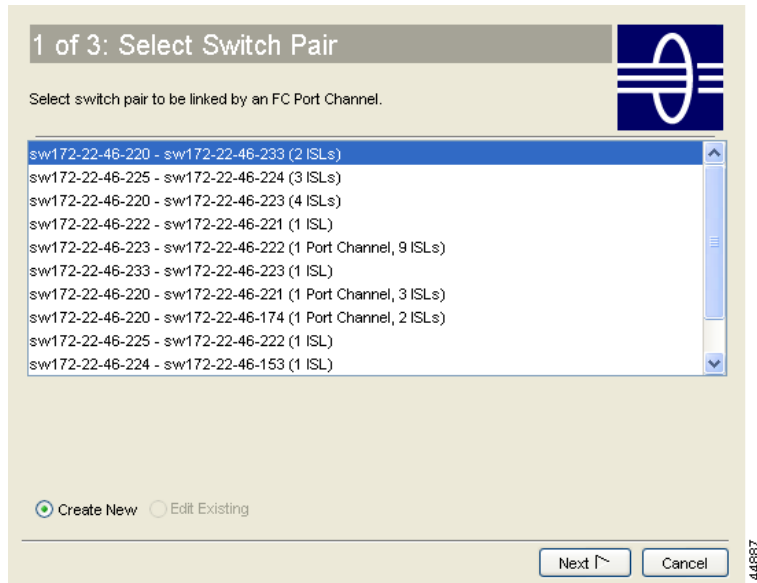
You see the first Port Channel Wizard screen.

- Step 2** Choose a switch pair.

[Figure 14-8](#) shows a list of the switch pairs.

Send comments to nx5000-docfeedback@cisco.com

Figure 14-8 Select Switch Pairs

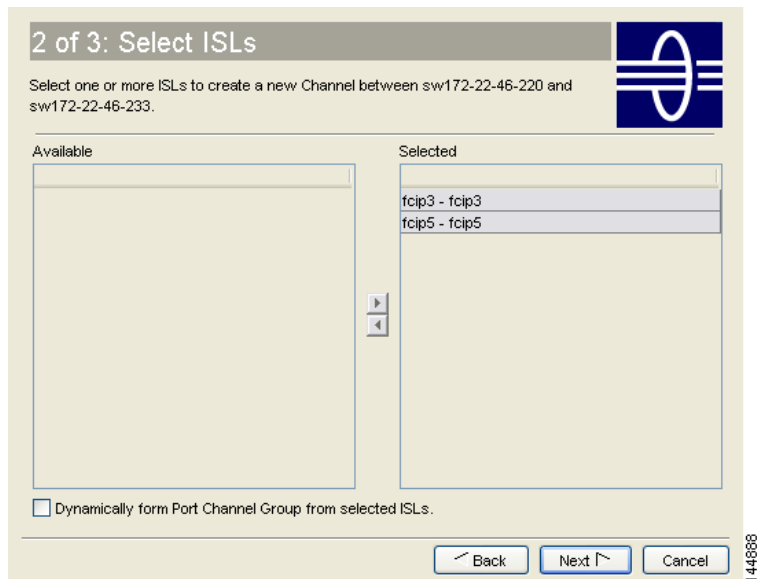


Step 3 Click **Next**.

Step 4 Select the ISLs.

Figure 14-9 shows a list of the ISLs.

Figure 14-9 Select ISLs



Step 5 (Optional) Check the **Dynamically form Port Channel Group from selected ISLs** check box if you want to dynamically create the SAN port channel and make the ISL properties identical for the Admin, Trunk, Speed, and VSAN attributes.

Step 6 Click **Next**.

Send comments to nx5000-docfeedback@cisco.com

- Step 7** If you chose to dynamically form a SAN port channel from selected ISLs, you see the final Port Channel Wizard screen (see [Figure 14-10](#)). Set the VSAN List, Trunk Mode, and Speed and proceed to [Step 11](#).

Figure 14-10 Dynamically Form a Port Channel

3 of 3: Create Port Channel

Specify the attributes which will be assigned to selected ISL ports of sw172-22-46-220 (fcip3, fcip5) and sw172-22-46-233 (fcip3, fcip5) to ensure automatic Port Channel creation. NOTE: the Channel may take time to appear in map.

Port Attributes

VSAN List: (1-4093) e.g. 1-22,29-45

Trunk Mode: nonTrunk trunk auto

Speed: auto 1Gb 2Gb 4Gb autoMax2G

- Step 8** If you did not choose to dynamically form a SAN port channel, you see the third Port Channel Wizard dialog box (see [Figure 14-11](#)).

Figure 14-11 Create a Port Channel

Switch	Interface, VSAN Id	FailureCause
sw172-22-46-174	fc3/2, 4001	vsanMismatchIsolation
sw172-22-46-220	fc3/2, 4001	portBindFailure

- Step 9** Change the channel ID or description for each switch, if necessary.
- Step 10** Review the attributes at the bottom of the screen, and set them if applicable.

The following attributes are shown in [Figure 14-11](#):

- VSAN List—A list of VSANs to which the ISLs belong.
- Trunk Mode—You can enable trunking on the links in the SAN port channel. Choose **trunking** if your link is between TE ports. Choose **nontrunking** if your link is between E ports. Choose **auto** if you are not sure.
- Force Admin, Trunk, Speed, and VSAN attributes to be identical—This check box ensures that the same parameter settings are used in all physical ports in the channel. If these settings are not identical, the ports cannot become part of the SAN port channel.
- Speed—The port speed values are **auto**, **1Gb**, **2Gb**, **4Gb**, and **autoMax2G**.

- Step 11** Click **OK**.

Send comments to nx5000-docfeedback@cisco.com

The SAN port channel is created. It may take a few minutes before the new port channel is visible in the Fabric pane.

About SAN Port Channel Modes

You can configure each SAN port channel with a channel group mode parameter to determine the port channel protocol behavior for all member ports in this channel group. The possible values for a channel group mode are as follows:

- **On (default)**—The member ports only operate as part of a SAN port channel or remain inactive. In this mode, the port channel protocol is not initiated. However, if a port channel protocol frame is received from a peer port, the software indicates its nonnegotiable status. Port channels configured in the On mode require you to explicitly enable and disable the port channel member ports at either end if you add or remove ports from the port channel configuration. You must physically verify that the local and remote ports are connected to each other.
- **Active**—The member ports initiate port channel protocol negotiation with the peer port(s) regardless of the channel group mode of the peer port. If the peer port, while configured in a channel group, does not support the port channel protocol, or responds with a nonnegotiable status, it will default to the On mode behavior. The Active port channel mode allows automatic recovery without explicitly enabling and disabling the port channel member ports at either end.

Table 14-1 compares On and Active modes.

Table 14-1 Channel Group Configuration Differences

On Mode	Active Mode
No protocol is exchanged.	A port channel protocol negotiation is performed with the peer ports.
Moves interfaces to the suspended state if its operational values are incompatible with the SAN port channel.	Moves interfaces to the isolated state if its operational values are incompatible with the SAN port channel.
When you add or modify a port channel member port configuration, you must explicitly disable (shut) and enable (no shut) the port channel member ports at either end.	When you add or modify a port channel interface, the SAN port channel automatically recovers.
Port initialization is not synchronized.	There is synchronized startup of all ports in a channel across peer switches.
All misconfigurations are not detected as no protocol is exchanged.	Consistently detect misconfigurations using a port channel protocol.
Transitions misconfigured ports to the suspended state. You must explicitly disable (shut) and enable (no shut) the member ports at either end.	Transitions misconfigured ports to the isolated state to correct the misconfiguration. Once you correct the misconfiguration, the protocol ensures automatic recovery.
This is the default mode.	You must explicitly configure this mode.

Send comments to nx5000-docfeedback@cisco.com

To configure active mode using Fabric Manager, perform this task:

-
- Step 1** Expand ISLs, and then choose **Port Channels** in the Physical Attributes pane. You see the port channels configured in the Information pane.
- Step 2** Click the **Protocols** tab. From the Mode drop-down list, choose the appropriate mode for the Port Channel.
- Step 3** Click the **Apply Changes** icon to save any modifications.
-

About SAN Port Channel Deletion

When you delete the SAN port channel, the corresponding channel membership is also deleted. All interfaces in the deleted SAN port channel convert to individual physical links. After the SAN port channel is removed, regardless of the mode (active and on) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the [“Setting the Interface Administrative State”](#) section on page 10-9).

If you delete the SAN port channel for one port, then the individual ports within the deleted SAN port channel retain the compatibility parameter settings (speed, mode, port VSAN, allowed VSAN, and port security). You can explicitly change those settings as required.

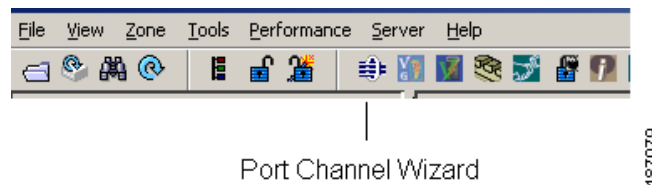
- If you use the default On mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the Active mode, then the port channel ports automatically recover from the deletion.

Deleting SAN Port Channels

To delete a port channel using the Port Channel Wizard in Fabric Manager, perform this task:

-
- Step 1** Click the **Port Channel Wizard** icon in the toolbar (see [Figure 14-12](#)).

Figure 14-12 Port Channel Wizard Icon



You see the first Port Channel Wizard screen.

- Step 2** Select the existing port channel that you want to delete and click **Next**. You see a list of the ISLs currently associated with this port channel.
- Step 3** Click **Next**. You see an editable list of associated ISLs and available ISLs for this port channel.
- Step 4** Click each associated ISL and click the **left arrow** to remove all ISLs from the port channel.

Send comments to nx5000-docfeedback@cisco.com

Step 5 Check the **Delete Port Channel If Empty** check box to delete this port channel.

Step 6 Click **Finish** to save any modifications or click **Cancel** to discard any changes.

Interfaces in a SAN Port Channel

You can add or remove a physical Fibre Channel interface (or a range of interfaces) to an existing SAN port channel. The compatible parameters on the configuration are mapped to the SAN port channel. Adding an interface to a SAN port channel increases the channel size and bandwidth of the SAN port channel. Removing an interface from a SAN port channel decreases the channel size and bandwidth of the SAN port channel.



Note

Virtual Fibre Channel interfaces cannot be added to SAN port channels.

This section describes interface configuration for a SAN port channel and includes the following topics:

- [About Interface Addition to a SAN Port Channel, page 14-12](#)
- [Adding an Interface to a SAN Port Channel, page 14-13](#)
- [Forcing an Interface Addition, page 14-14](#)
- [About Interface Deletion from a SAN Port Channel, page 14-14](#)
- [Deleting an Interface from a SAN Port Channel, page 14-14](#)

About Interface Addition to a SAN Port Channel

You can add a physical interface (or a range of interfaces) to an existing SAN port channel. The compatible parameters on the configuration are mapped to the SAN port channel. Adding an interface to a SAN port channel increases the channel size and bandwidth of the SAN port channel.

After the members are added, regardless of the mode (Active and On) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down.

Compatibility Check

A compatibility check ensures that the same parameter settings are used in all physical ports in the channel. Otherwise, they cannot become part of a SAN port channel. The compatibility check is performed before a port is added to the SAN port channel.

The check ensures that the following parameters and settings match at both ends of a SAN port channel:

- Capability parameters (type of interface, Fibre Channel at both ends).
- Administrative compatibility parameters (speed, mode, port VSAN, allowed VSAN, and port security).
- Operational parameters (speed and remote switch's WWN).

Send comments to nx5000-docfeedback@cisco.com

A port addition procedure fails if the capability and administrative parameters in the remote switch are incompatible with the capability and administrative parameters in the local switch. If the compatibility check is successful, the interfaces are operational and the corresponding compatibility parameter settings apply to these interfaces.

Suspended and Isolated States

If the operational parameters are incompatible, the compatibility check fails and the interface is placed in a suspended or isolated state based on the configured mode:

- An interface enters the suspended state if the interface is configured in the On mode.
- An interface enters the isolated state if the interface is configured in the Active mode.

See the “Reason Codes” section on page 10-5.

Adding an Interface to a SAN Port Channel

To add an interface or range of interfaces to a SAN port channel using Fabric Manager, perform this task:

- Step 1** Expand ISLs, and then choose **Port Channels** in the Physical Attributes pane. You see the SAN port channels configured in the Information pane (see [Figure 14-13](#)).

Figure 14-13 Port Channels

Switch	Channel	Force	Members Admin	Members Oper	Last Status	Last FailureCause	Last Time
sw172-22-46-223	channel1	<input type="checkbox"/>	fcip4	fcip4	successful		2006/02/22-12:15:38
sw172-22-46-220	channel1	<input type="checkbox"/>	fcip5,fcip7,fcip8,fcip9,fcip11	fcip5,fcip7,fcip8,fcip9,fcip11	successful		2006/02/23-12:33:53
sw172-22-46-233	channel10	<input type="checkbox"/>			successful		2006/02/22-12:15:20
sw172-22-46-174	channel1	<input type="checkbox"/>	fcip5,fcip7,fcip8,fcip9,fcip11	fcip5,fcip7,fcip8,fcip9,fcip11	successful		2006/02/22-12:15:33
sw172-22-46-223	channel10	<input type="checkbox"/>	gigE2/1	gigE2/1	successful		2006/02/22-12:15:38
sw172-22-46-220	channel2	<input type="checkbox"/>	fcip6		successful		2006/02/23-12:33:53
sw172-22-46-220	channel3	<input type="checkbox"/>			successful		2006/02/23-12:33:53
sw172-22-46-220	channel4	<input type="checkbox"/>	fcip4	fcip4	successful		2006/02/23-12:33:53
sw172-22-46-220	channel5	<input type="checkbox"/>			successful		2006/02/23-12:33:53
sw172-22-46-220	channel10	<input type="checkbox"/>	gigE9/5	gigE9/5	successful		2006/02/22-12:15:15

- Step 2** Click the **Channels** tab and find the switch and SAN port channel that you want to edit.
- Step 3** Set Members Admin to the interface or list of interfaces that you want to add to the SAN port channel.
- Step 4** Click the **Apply Changes** icon to save any modifications or click **Undo Changes** to discard any changes.

Send comments to nx5000-docfeedback@cisco.com

Forcing an Interface Addition

You can force the port configuration to be overwritten by the SAN port channel. In this case, the interface is added to a SAN port channel.

- If you use the default On mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the Active mode, then the port channel ports automatically recover from the addition.



Note

When SAN port channels are created from within an interface, the **force** option cannot be used.

After the members are forcefully added, regardless of the mode (Active and On) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the “[Setting the Interface Administrative State](#)” section on page 10-9).

To force the addition of a port to a SAN port channel using Fabric Manager, perform this task:

-
- Step 1** Expand **ISLs**, and then choose **Port Channels** in the Physical Attributes pane.
You see the port channels configured in the Information pane.
 - Step 2** Click the **Channels** tab and find the switch and SAN port channel that you want to edit.
 - Step 3** Set Members Admin to the interface or list of interfaces that you want to add to the SAN port channel.
 - Step 4** Check the **Force** check box to force this interface addition.
 - Step 5** Click the **Apply Changes** icon to save any modifications.
-

About Interface Deletion from a SAN Port Channel

When a physical interface is deleted from the SAN port channel, the channel membership is automatically updated. If the deleted interface is the last operational interface, then the port channel status is changed to a down state. Deleting an interface from a SAN port channel decreases the channel size and bandwidth of the SAN port channel.

- If you use the default On mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the Active mode, then the port channel ports automatically recover from the deletion.

After the members are deleted, regardless of the mode (Active and On) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down.

Deleting an Interface from a SAN Port Channel

To delete a physical interface (or a range of physical interfaces) from a SAN port channel using Fabric Manager, perform this task:

-
- Step 1** Expand **ISLs**, and then choose **Port Channels** in the Physical Attributes pane.
You see the SAN port channels configured in the Information pane.

Send comments to nx5000-docfeedback@cisco.com

- Step 2** Click the **Channels** tab and find the switch and SAN port channel that you want to edit.
 - Step 3** Remove the interface or list of interfaces that you want deleted in the Members the Admin column.
 - Step 4** Click the **Apply Changes** icon to save any modifications.
-

Port Channel Protocol

The switch software provides robust error detection and synchronization capabilities. You can manually configure channel groups, or they can be automatically created. In both cases, the channel groups have the same capability and configurational parameters. Any change in configuration applied to the associated port channel interface is propagated to all members of the channel group.

Cisco SAN switches support a protocol to exchange port channel configurations, which simplifies port channel management with incompatible ISLs. An additional autocreation mode enables ISLs with compatible parameters to automatically form channel groups without manual intervention.

The port channel protocol is enabled by default.

The port channel protocol expands the port channel functional model in Cisco SAN switches. It uses the exchange peer parameters (EPP) services to communicate across peer ports in an ISL. Each switch uses the information received from the peer ports along with its local configuration and operational values to decide if it should be part of a SAN port channel. The protocol ensures that a set of ports are eligible to be part of the same SAN port channel. They are only eligible to be part of the same port channel if all the ports have a compatible partner.

The port channel protocol uses two subprotocols:

- **Bringup protocol**—Automatically detects misconfigurations so you can correct them. This protocol synchronizes the SAN port channel at both ends so that all frames for a given flow (as identified by the source FC ID, destination FC ID and OX_ID) are carried over the same physical link in both directions. This helps make applications such as write acceleration work for SAN port channels over FCIP links.
- **Autocreation protocol**—Automatically aggregates compatible ports into a SAN port channel.

This section describes how to configure the port channel protocol and includes the following sections:

- [About Channel Group Creation, page 14-15](#)
- [Autocreation Guidelines, page 14-17](#)
- [Enabling and Configuring Autocreation, page 14-17](#)
- [About Manually Configured Channel Groups, page 14-18](#)
- [Converting to Manually Configured Channel Groups, page 14-18](#)

About Channel Group Creation

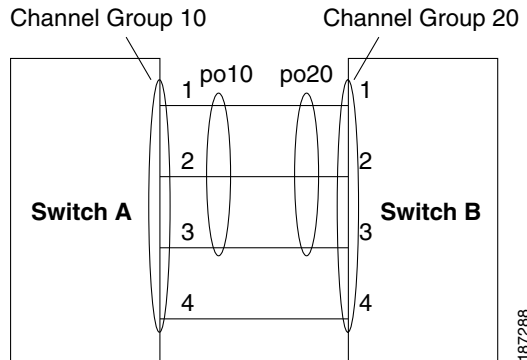
If channel group autocreation is enabled, ISLs can be configured automatically into channel groups without manual intervention. [Figure 14-14](#) shows an example of channel group autocreation.

The first ISL comes up as an individual link. In the example shown in [Figure 14-14](#), this is link A1-B1. When the next link comes up (A2-B2 in the example), the port channel protocol determines if this link is compatible with link A1-B1 and automatically creates channel groups 10 and 20 in the respective

Send comments to nx5000-docfeedback@cisco.com

switches. Link A3-B3 can join the channel groups (and the port channels) if the respective ports have compatible configurations. Link A4-B4 operates as an individual link, because it is not compatible with the existing member ports in the channel group.

Figure 14-14 Autocreating Channel Groups



The channel group numbers are assigned dynamically (when the channel group is formed).

The channel group number may change across reboots for the same set of port channels depending on the initialization order of the ports.

Table 14-2 identifies the differences between user-configured and auto-configured channel groups.

Table 14-2 Channel Group Configuration Differences

User-Configured Channel Group	Autocreated Channel Group
Manually configured by the user.	Created automatically when compatible links come up between two compatible switches, if channel group autcreation is enabled in all ports at both ends.
Member ports cannot participate in autcreation of channel groups. The autcreation feature cannot be configured.	None of these ports are members of a user-configured channel group.
You can form the SAN port channel with a subset of the ports in the channel group. Incompatible ports remain in a suspended or isolated state depending on the On or Active mode configuration.	All ports included in the channel group participate in the SAN port channel. No member port becomes isolated or suspended; instead, the member port is removed from the channel group when the link is found to be incompatible.
Any administrative configuration made to the SAN port channel is applied to all ports in the channel group, and you can save the configuration for the port channel interface.	Any administrative configuration made to the SAN port channel is applied to all ports in the channel group, but the configurations are saved for the member ports; no configuration is saved for the port channel interface. You can explicitly convert this channel group, if required.
You can remove any channel group and add members to a channel group.	You cannot remove a channel group. You cannot add members to the channel group or remove members. The channel group is removed when no member ports exist.

Send comments to nx5000-docfeedback@cisco.com

Autocreation Guidelines

When using the autocreation protocol, follow these guidelines:

- A port is not allowed to be configured as part of a SAN port channel when the autocreation feature is enabled. These two configurations are mutually exclusive.
- Autocreation must be enabled in both the local and peer ports to negotiate a SAN port channel.
- Aggregation occurs in one of two ways:
 - A port is aggregated into a compatible autocreated SAN port channel.
 - A port is aggregated with another compatible port to form a new SAN port channel.
- Newly created SAN port channels are allocated from the maximum possible port channel number in a decreasing order based on availability. If all port channel numbers are used up, aggregation is not allowed.
- You cannot change the membership or delete an autocreated SAN port channel.
- When you disable autocreation, all member ports are removed from the autocreated SAN port channel.
- Once the last member is removed from an autocreated SAN port channel, the channel is automatically deleted and the number is released for reuse.
- An autocreated SAN port channel is not persistent through a reboot. An autocreated SAN port channel can be manually configured to appear the same as a persistent SAN port channel. Once the SAN port channel is made persistent, the autocreation feature is disabled in all member ports.
- You can enable or disable the autocreation feature on a per-port basis or for all ports in the switch. When this configuration is enabled, the channel group mode is assumed to be active. The default for this task is disabled.
- If autocreation of channel groups is enabled for an interface, you must first disable autocreation before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.



Tip

When enabling autocreation in any switch in the Cisco Nexus 5000 Series, we recommend that you retain at least one interconnected port between the switches without any autocreation configuration. If all ports between two switches are configured with the autocreation feature at the same time, a possible traffic disruption may occur between these two switches as ports are automatically disabled and reenabled when they are added to an autocreated SAN port channel.

Enabling and Configuring Autocreation

To configure port channel autocreation, check the **Dynamically form Port Channel Group from selected ISLs** option in the Port Channel Wizard. See the [“Configuring SAN Port Channels”](#) section on page 14-7.

Send comments to nx5000-docfeedback@cisco.com

About Manually Configured Channel Groups

A user-configured channel group cannot be converted to an autogenerated channel group. However, you can convert an autogenerated channel group to a manual channel group. This task is irreversible. The channel group number does not change, but the member ports operate according to the properties of the manually configured channel group, and channel group autocreation is implicitly disabled for all the member ports.



Tip

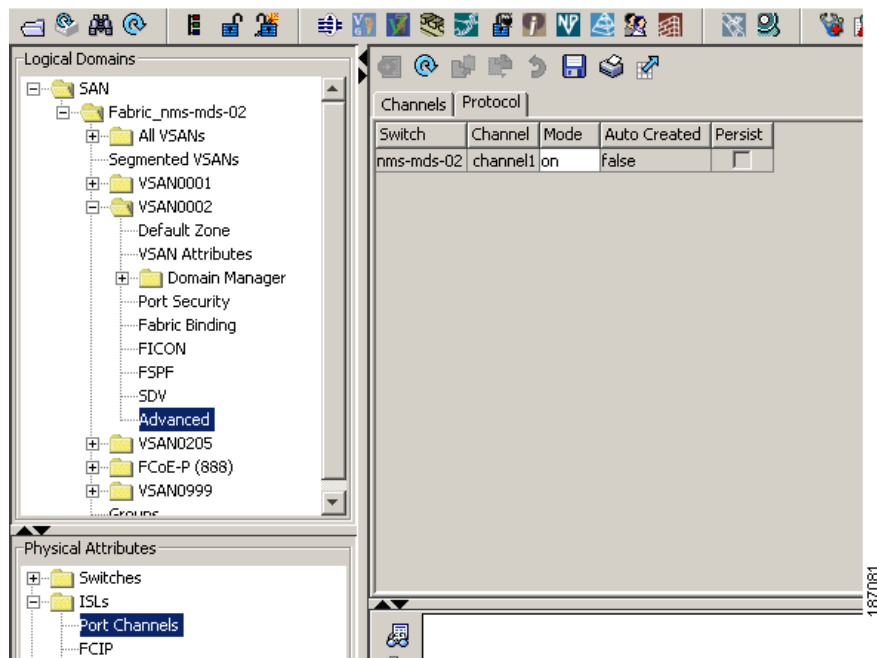
If you enable persistence, be sure to enable it at both ends of the SAN port channel.

Converting to Manually Configured Channel Groups

To convert an autogenerated channel group to a user-configured channel group using Fabric Manager, perform this task:

- Step 1** Expand **ISLs**, and then choose **Port Channels** in the Physical Attributes pane. Click the **Protocol** tab. You see the switch protocols as shown in [Figure 14-15](#).

Figure 14-15 Switch Protocols



- Step 2** Check the **Persist** check box for each channel that you want to convert to a manually configured channel group.
- Step 3** Click the **Apply Changes** icon to save any modifications.

[Send comments to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Verifying SAN Port Channel Configuration

You can use the Information pane in Fabric Manager to verify your port channel configuration (see Figure 14-16).

Figure 14-16 Port Channel Summary in Fabric Manager

Switch	Channel	Force	Members Admin	Members Oper	Last Status	Last FailureCause	Last Time	CreationTime
sw172-22-46-220	channel1	<input type="checkbox"/>	fcip3	fcip3	successful		2007/04/17-21:05:20	2007/04/17-21:05:20
sw172-22-46-223	channel1	<input type="checkbox"/>	fc1/1	fc1/1	successful		2007/04/17-13:57:37	2007/04/17-13:57:37
sw172-22-46-221	channel1	<input checked="" type="checkbox"/>	fc2/25	fc2/25	successful		2007/04/17-14:50:03	2007/04/17-14:50:03
sw172-22-46-174	channel1	<input checked="" type="checkbox"/>	fcip3	fcip3	successful		2007/04/19-11:24:16	2007/04/19-11:24:15
sw172-22-46-220	channel2	<input type="checkbox"/>	fc2/15	fc2/15	successful		2007/04/17-21:05:20	2007/04/17-21:05:20
sw172-22-46-223	channel10	<input type="checkbox"/>	gigE2/1	gigE2/1	successful		2007/04/17-13:57:37	2007/04/17-13:57:37
sw172-22-46-174	channel2	<input checked="" type="checkbox"/>	fcip4	fcip4	successful		2007/04/19-11:24:16	2007/04/19-11:24:15
sw172-22-46-220	channel3	<input type="checkbox"/>	fcip4	fcip4	successful		2007/04/17-21:05:20	2007/04/17-21:05:20
sw172-22-46-220	channelH	<input type="checkbox"/>	fc2/16	fc2/16	successful		2007/04/17-21:05:20	2007/04/17-21:05:20
sw172-22-46-220	channel10	<input type="checkbox"/>	gigE9/5	gigE9/5	successful		2007/04/17-21:05:20	2007/04/17-21:05:20

Default Settings

Table 14-3 lists the default settings for SAN port channels.

Table 14-3 Default SAN Port Channel Parameters

Parameters	Default
Port channels	FSPF is enabled by default.
Create port channel	Administratively up.
Default port channel mode	On.
Autocreation	Disabled.

Send comments to nx5000-docfeedback@cisco.com