Advanced Fibre Channel Features

This chapter describes how to configure advanced Fibre Channel features.

This chapter includes the following sections:

Advanced Fibre Channel Features and Concepts

Fibre Channel Timeout Values

You can modify Fibre Channel protocol-related timer values for the switch by configuring the following timeout values (TOVs):

- Distributed services TOV (D_S_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 5,000 milliseconds.

- Error detect TOV (E_D_TOV)—The valid range is from 1,000 to 10,000 milliseconds. The default is 2,000 milliseconds. This value is matched with the other end during port initialization.

- Resource allocation TOV (R_A_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds. This value is matched with the other end during port initialization.

Note The fabric stability TOV (F_S_TOV) constant cannot be configured.

Timer Configuration Across All VSANs

You can modify Fibre Channel protocol related timer values for the switch.

Caution The D_S_TOV, E_D_TOV, and R_A_ TOV values cannot be globally changed unless all VSANs in the switch are suspended.

> **Note** If a VSAN is not specified when you change the timer value, the changed value is applied to all VSANs in the switch.

You can configure Fibre Channel timers across all VSANs.

Procedure

	Command or Action	**Purpose**

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

Step 2	**fctimer R_A_TOV** *timeout* **Example:** `switch(config)# fctimer R_A_TOV 800`	Configures the R_A_TOV timeout value for all VSANs. The unit is milliseconds. This type of configuration is not permitted unless all VSANs are suspended.

Timer Configuration Per-VSAN

You can also issue the fctimer for a specified VSAN to configure different TOV values for VSANs with special links such as Fibre Channel. You can configure different E_D_TOV, R_A_TOV, and D_S_TOV values for individual VSANs. Active VSANs are suspended and activated when their timer values are changed.

> **Note** This configuration must be propagated to all switches in the fabric. Be sure to configure the same value in all switches in the fabric.

You can configure per-VSAN Fibre Channel timers.

Procedure

	Command or Action	**Purpose**

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

Step 2	**fctimer D_S_TOV** *timeout* **vsan** *vsan-id*
	
	Example:
	`switch(config#)# fctimer D_S_TOV 900`
	`vsan 15`
		Configures the D_S_TOV timeout value (in milliseconds) for the specified VSAN. Suspends the VSAN temporarily. You have the option to end this command, if required.

EXAMPLES

This example shows how to configure the timer value for VSAN 2:

```
switch(config#)# fctimer D_S_TOV 6000 vsan 2
Warning: The vsan will be temporarily suspended when updating the timer value This
configuration would impact whole fabric. Do you want to continue? (y/n) y
Since this configuration is not propagated to other switches, please configure the same
value in all the switches
```

fctimer Distribution

You can enable per-VSAN fctimer fabric distribution for all Cisco SAN switches in the fabric. When you perform fctimer configurations, and distribution is enabled, that configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you enter the first configuration command after you enabled distribution in a switch. The fctimer application uses the effective and pending database model to store or commit the commands based on your configuration.

For additional information, refer to Using Cisco Fabric Services in the System Management Configuration Guide for your device.

Enabling or Disabling fctimer Distribution

You can enable or disable fctimer fabric distribution.

Procedure

	Command or Action	**Purpose**

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

Step 2	**fctimer distribute** **Example:** `switch(config)# fctimer distribute`	Enables fctimer configuration distribution to all switches in the fabric. Acquires a fabric lock and stores all future configuration changes in the pending database.
Step 3	**no fctimer distribute** **Example:** `switch(config)# no fctimer distribute`	Disables (default) fctimer configuration distribution to all switches in the fabric.

Committing fctimer Changes

When you commit the fctimer configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the switches in the fabric receive the same configuration. When you commit the fctimer configuration changes without implementing the session feature, the fctimer configurations are distributed to all the switches in the physical fabric.

Procedure

	Command or Action	Purpose

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

Step 2	**fctimer commit** **Example:** `switch(config)# fctimer commit`	Distributes the fctimer configuration changes to all switches in the fabric and releases the lock. Overwrites the effective database with the changes made to the pending database.

Discarding fctimer Changes

After making the configuration changes, you can choose to discard the changes by discarding the changes instead of committing them. In either case, 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	**fctimer abort** **Example:** `switch(config)# fctimer abort`	Discards the fctimer configuration changes in the pending database and releases the fabric lock.

Overriding the Fabric Lock

If you have performed a fctimer fabric task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.

The changes are only available in the volatile directory and are subject to being discarded if the switch is restarted.

To use administrative privileges and release a locked fctimer session, use the **clear fctimer session** command.

```
switch# clear fctimer session
```

Fabric Database Merge Guidelines

When merging two fabrics, follow these guidelines:

- Be aware of the following merge conditions:

  ◦ The merge protocol is not implemented for distribution of the fctimer values. You must manually merge the fctimer values when a fabric is merged.

  ◦ The per-VSAN fctimer configuration is distributed in the physical fabric.

  ◦ The fctimer configuration is only applied to those switches containing the VSAN with a modified fctimer value.

  ◦ The global fctimer values are not distributed.

- Do not configure global timer values when distribution is enabled.

Note The number of pending fctimer configuration operations cannot be more than 15. After 15 operations, you must commit or abort the pending configurations before performing any more operations.

For additional information, refer to CFS Merge Support in the System Management Configuration Guide for your device.

Verifying Configured fctimer Values

Use the **show fctimer** command to display the configured fctimer values. The following example displays the configured global TOVs:

```
switch# show fctimer
F_S_TOV    D_S_TOV    E_D_TOV    R_A_TOV
--------------------------------------
5000 ms    5000 ms    2000 ms    10000 ms
```

Note The F_S_TOV constant, though not configured, is displayed in the output of the **show fctimer** command.

The following example displays the configured TOV for VSAN 10:

```
switch# show fctimer vsan 10
vsan no.   F_S_TOV    D_S_TOV    E_D_TOV    R_A_TOV
-----------------------------------------------
10         5000 ms    5000 ms    3000 ms    10000 ms
```

Cisco Nexus 5500 Series NX-OS SAN Switching Configuration Guide, Release 6.x

World Wide Names

The world wide name (WWN) in the switch is equivalent to the Ethernet MAC address. As with the MAC address, you must uniquely associate the WWN to a single device. The principal switch selection and the allocation of domain IDs rely on the WWN.

Cisco SAN switches support three network address authority (NAA) address formats. (see the following table).

Table 1: Standardized NAA WWN Formats

NAA Address	NAA Type	WWN Format	
IEEE 48-bit address	Type 1 = 0001b	000 0000 0000b	48-bit MAC address
IEEE extended	Type 2 = 0010b	Locally assigned	48-bit MAC address
IEEE registered	Type 5 = 0101b	IEEE company ID: 24 bits	VSID: 36 bits

⚠️

Caution   Changes to the world-wide names should be made by an administrator or individual who is completely familiar with switch operations.

Verifying the WWN Configuration

Use the **show wwn** commands to display the status of the WWN configuration. This example shows how to display the status of all WWNs:

```
switch# show wwn status
Type    Configured     Available     Resvd.  Alarm State
----    ----------    --------------  ------  -----------
   1           64         48 ( 75%)      16    NONE
 2,5       524288     442368 ( 84%)   73728    NONE
```
This example shows how to display the information for block ID 51:

```
switch# show wwn status block-id 51
WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256

Block Allocation Status: FREE
```
This example shows how to display the WWN for a specific switch:

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

Link Initialization WWN Usage

Exchange Link Protocol (ELP) and Exchange Fabric Protocol (EFP) use WWNs during link initialization. ELPs and EFPs both use the VSAN WWN by default during link initialization. However, the ELP usage changes based on the peer switch's usage:

- If the peer switch ELP uses the switch WWN, then the local switch also uses the switch WWN.

- If the peer switch ELP uses the VSAN WWN, then the local switch also uses the VSAN WWN.

Configuring a Secondary MAC Address

You can allocate secondary MAC addresses.

Procedure

	Command or Action	Purpose

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

Step 2	**wwn secondary-mac** *wwn-id* **range** *value*
	
	Example:
	`switch(config)# wwn secondary-mac`
	`33:e8:00:05:30:00:16:df range 55`
		Configures the secondary MAC address. This command cannot be undone.

EXAMPLES

This example shows how to configure the secondary MAC address:

```
switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
From now on WWN allocation would be based on new MACs. Are you sure? (yes/no) no
You entered: no. Secondary MAC NOT programmed
```

FC ID Allocation for HBAs

Fibre Channel standards require a unique FC ID to be allocated to an N port attached to an F port in any switch. To conserve the number of FC IDs used, Cisco SAN switches use a special allocation scheme.

Some HBAs do not discover targets that have FC IDs with the same domain and area. The switch software maintains a list of tested company IDs that do not exhibit this behavior. These HBAs are allocated with single FC IDs. If the HBA can discover targets within the same domain and area, a full area is allocated.

To allow further scalability for switches with numerous ports, the switch software maintains a list of HBAs that can discover targets within the same domain and area. Each HBA is identified by its company ID (also known as Organizational Unique Identifier, or OUI) used in the pWWN during a fabric log in. A full area is allocated to the N ports with company IDs that are listed and for the others, a single FC ID is allocated. Regardless of the type (whole area or single) of FC ID allocated, the FC ID entries remain persistent.

Default Company ID List

All Cisco SAN switches contain a default list of company IDs that require area allocation. Using the company ID reduces the number of configured persistent FC ID entries. You can configure or modify these entries using the CLI.

⚠️

Caution   Persistent entries take precedence over company ID configuration. If the HBA fails to discover a target, verify that the HBA and the target are connected to the same switch and have the same area in their FC IDs, then perform the following procedure:

1   Shut down the port connected to the HBA.
2   Clear the persistent FC ID entry.
3   Get the company ID from the port WWN.
4   Add the company ID to the list that requires area allocation.
5   Bring up the port.

The list of company IDs have the following characteristics:

- A persistent FC ID configuration always takes precedence over the list of company IDs. Even if the company ID is configured to receive an area, the persistent FC ID configuration results in the allocation of a single FC ID.

- New company IDs added to subsequent releases are automatically added to existing company IDs.

- The list of company IDs is saved as part of the running and saved configuration.

- The list of company IDs is used only when the fcinterop FC ID allocation scheme is in auto mode. By default, the interop FC ID allocation is set to auto, unless changed.

  🔍

  Tip   We recommend that you set the fcinterop FC ID allocation scheme to auto and use the company ID list and persistent FC ID configuration to manipulate the FC ID device allocation.

  Use the **fcinterop FCID allocation auto** command to change the FC ID allocation and the **show running-config** command to view the currently allocated mode.

- When you enter a **write erase**, the list inherits the default list of company IDs shipped with a relevant release.

Verifying the Company ID Configuration

You can view the configured company IDs by entering the **show fcid-allocation area** command. Default entries are listed first and the user-added entries are listed next. Entries are listed even if they were part of the default list and you later removed them.

This example shows how to display the list of default and configured company IDs:

```
switch# show fcid-allocation area
FCID area allocation company id info:
00:50:2E <--------------- Default entry
00:50:8B
00:60:B0
00:A0:B8
00:E0:69
00:30:AE + <------------- User-added entry
00:32:23 +
00:E0:8B * <------------- Explicitly deleted entry (from the original default list)
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

You can implicitly derive the default entries shipped with a specific release by combining the list of Company IDs displayed without any identification with the list of deleted entries.

You can also view or obtain the company IDs in a specific WWN by entering the **show fcid-allocation company-id-from-wwn** command. Some WWN formats do not support company IDs. In these cases, you many need to configure the FC ID persistent entry.

This example shows how to display the company ID for the specified WWN:

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted Company ID: 0x000530
```

Switch Interoperability

Interoperability enables the products of multiple vendors to interwork with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces.

Not all vendors follow the standards in the same way, which results in the need for interoperability modes. This section briefly explains the basic concepts of these modes.

Each vendor has a regular mode and an equivalent interoperability mode, which specifically turns off advanced or proprietary features and provides the product with a standards-compliant implementation.

Note   For more information on configuring interoperability for Cisco Nexus devices, see the *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*.

About Interop Mode

The software supports the following four interop modes:

- Mode 1— Standards-based interop mode that requires all other vendors in the fabric to be in interop mode.

- Mode 2—Brocade native mode (Core PID 0).

- Mode 3—Brocade native mode (Core PID 1).

- Mode 4—McData native mode.

For information about configuring interop modes 2, 3, and 4, see the *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*, available at the following location: http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/interoperability/guide/intopgd.html

The following table lists the changes in switch operation when you enable interoperability mode. These changes are specific to Cisco Nexus devices while in interop mode.

Table 2: Changes in Switch Operation When Interoperability Is Enabled

Switch Feature	Changes if Interoperability Is Enabled
Domain IDs	Some vendors cannot use the full range of 239 domains within a fabric. Domain IDs are restricted to the range 97 to 127, to accommodate McData's nominal restriction to this same range. Domain IDs can either be static or preferred, which operate as follows: • Static: Cisco switches accept only one domain ID; if a switch does not get that domain ID it isolates itself from the fabric. • Preferred: If the switch does not get its requested domain ID, it accepts any assigned domain ID.
Timers	All Fibre Channel timers must be the same on all switches as these values are exchanged by E ports when establishing an ISL. The timers are F_S_TOV, D_S_TOV, E_D_TOV, and R_A_TOV.
F_S_TOV	Verify that the Fabric Stability Time Out Value timers match exactly.
D_S_TOV	Verify that the Distributed Services Time Out Value timers match exactly.
E_D_TOV	Verify that the Error Detect Time Out Value timers match exactly.
R_A_TOV	Verify that the Resource Allocation Time Out Value timers match exactly.
Trunking	Trunking is not supported between two different vendor's switches. This feature may be disabled per port or per switch.
Default zone	The default zone operation of permit (all nodes can see all other nodes) or deny (all nodes are isolated when not explicitly placed in a zone) may change.

Switch Feature	Changes if Interoperability Is Enabled
Zoning attributes	Zones may be limited to the pWWN and other proprietary zoning methods (physical port number) may be eliminated. **Note** On a Brocade switch, use the **cfgsave** command to save fabric-wide zoning configuration. This command does not have any effect on Cisco SAN switches if they are part of the same fabric. You must explicitly save the configuration on each Cisco SAN switch.
Zone propagation	Some vendors do not pass the full zone configuration to other switches, only the active zone set gets passed. Verify that the active zone set or zone configuration has correctly propagated to the other switches in the fabric.
VSAN	Interop mode only affects the specified VSAN.
TE ports and SAN port channels	TE ports and SAN port channels cannot be used to connect Cisco switches to non-Cisco SAN switches. Only E ports can be used to connect to non-Cisco SAN switches. TE ports and SAN port channels can still be used to connect a Cisco switch to other Cisco SAN switches even when in interop mode.
FSPF	The routing of frames within the fabric is not changed by the introduction of interop mode. The switch continues to use src-id, dst-id, and ox-id to load balance across multiple ISL links.
Domain reconfiguration disruptive	This is a switch-wide impacting event. Brocade and McData require the entire switch to be placed in offline mode and/or rebooted when changing domain IDs.
Domain reconfiguration nondisruptive	This event is limited to the affected VSAN. Cisco SAN switches have the capability to restart only the domain manager process for the affected VSAN and not the entire switch.
Name server	Verify that all vendors have the correct values in their respective name server database.

Configuring Interop Mode 1

You can interop mode1 in Cisco SAN switches disruptively or nondisruptively.

Note   Brocade's **msplmgmtdeactivate** command must explicitly be run prior to connecting from a Brocade switch to either Cisco SAN switches or to McData switches. This command uses Brocade proprietary frames to exchange platform information, which Cisco SAN switches or McData switches do not recognize. Rejecting these frames causes the common E ports to become isolated.

Procedure

	Command or Action	Purpose
Step 1	Place the VSAN of the E ports that connect to the OEM switch in interoperability mode.	`switch# `**`configuration terminal`** `switch(config)# `**`vsan database`** `switch(config-vsan-db)# `**`vsan 1 interop 1`** `switch(config-vsan-db)# `**`exit`**
Step 2	Assign a domain ID in the range of 97 (0x61) through 127 (0x7F).	**Note** This is an limitation imposed by the McData switches. In Cisco SAN switches, the default is to request an ID from the principal switch. If the preferred option is used, Cisco SAN switches request a specific ID, but still join the fabric if the principal switch assigns a different ID. If the static option is used, the Cisco SAN switches do not join the fabric unless the principal switch agrees and assigns the requested ID. **Note** When changing the domain ID, the FC IDs assigned to N ports also change.

Step 3	Change the Fibre Channel timers (if they have been changed from the system defaults).	**Note** The Cisco SAN switches, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. The RA_TOV default is 10 seconds, and the ED_TOV default is 2 seconds. Per the FC-SW2 standard, these values must be the same on each switch within the fabric.
		`switch(config)# `**`fctimer e_d_tov ?`**
		`  <1000-100000> E_D_TOV in milliseconds(1000-100000)`
		
		`switch(config)# `**`fctimer r_a_tov ?`**
		`  <5000-100000> R_A_TOV in milliseconds(5000-100000)`

Step 4	When making changes to the domain, you may or may not need to restart the Domain Manager function for the altered VSAN.	• Force a fabric reconfiguration with the **disruptive** option. `switch(config)# `**`fcdomain restart disruptive vsan 1`** or

Command or Action	Purpose
	• Do not force a fabric reconfiguration. `switch(config# fcdomain restart vsan 1`

Verifying Interoperating Status

This section highlights the commands used to verify if the fabric is up and running in interoperability mode.

To verify the resulting status of entering the interoperability command in any Cisco Nexus device, perform this task:

Procedure

Step 1 Verify the software version.

Example:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software

TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.

Some parts of this software are covered under the GNU Public

License. A copy of the license is available at

http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.0(1a)N1(1)
  system:    version 4.0(1a)N1(1)
  BIOS compile time:      06/19/08
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.0.1a.N1.latest.bin
  kickstart compile time: 11/25/2008 6:00:00 [11/25/2008 14:17:12]
  system image file is:    bootflash:/n5000-uk9.4.0.1a.N1.latest.bin
  system compile time:    11/25/2008 6:00:00 [11/25/2008 14:59:49]
Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU with 2074308 kB of memory.
  Processor Board ID JAB120900PJ
  Device name: switch
  bootflash: 1003520 kB

Kernel uptime is 0 day(s), 1 hour(s), 29 minute(s), 55 second(s)

Last reset at 510130 usecs after Wed Nov 26 18:12:23 2008
  Reason: Reset Requested by CLI command reload
  System version: 4.0(1a)N1(1)
  Service:
```

```
plugin
  Core Plugin, Ethernet Plugin
```

Step 2   Verify if the interface states are as required by your configuration.

Example:
```
switch# show interface brief
```

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc3/1	1	E	on	trunking	swl	TE	2	--
fc3/2	1	auto	on	sfpAbsent	--	--		--
fc3/3	1	E	on	trunking	swl	TE	2	--
fc3/4	1	auto	on	sfpAbsent	--	--		--
fc3/5	1	auto	auto	notConnected	swl	--		--
fc3/6	1	auto	on	sfpAbsent	--	--		--
fc3/7	1	auto	auto	sfpAbsent	--	--		--
fc3/8	1	auto	auto	sfpAbsent	--	--		--

Step 3   Verify if you are running the desired configuration.

Example:
```
switch# show running-config

Building Configuration...

 interface fc2/1

no shutdown

 interface fc2/2

no shutdown

 interface fc2/3

 interface fc2/4
```
<snip>
```
interface mgmt0

ip address 6.1.1.96 255.255.255.0

switchport encap default

no shutdown

vsan database

vsan 1 interop

boot system bootflash:/nx5000-system-23e.bin
```

```
boot kickstart bootflash:/nx5000-kickstart-23e.bin

callhome

fcdomain domain 100 preferred vsan 1

ip route 6.1.1.0 255.255.255.0 6.1.1.1

ip routing

line console

  databits 5

  speed 110

logging linecard

ssh key rsa 512 force

ssh server enable

switchname switch

username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin
```

Step 4 Verify if the interoperability mode is active.

Example:
```
switch# show vsan 1

vsan 1 information

        name:VSAN0001  state:active

        interoperability mode:yes <------------------- verify mode

        loadbalancing:src-id/dst-id/oxid

        operational state:up
```

Step 5 Verify the domain ID.

Example:
```
switch# show fcdomain vsan 1

The local switch is a Subordinated Switch.

Local switch run time information:

        State: Stable

        Local switch WWN:    20:01:00:05:30:00:51:1f

        Running fabric name: 10:00:00:60:69:22:32:91

        Running priority: 128

        Current domain ID: 0x64(100) <---------------verify domain id

Local switch configuration information:

        State: Enabled

        Auto-reconfiguration: Disabled

        Contiguous-allocation: Disabled
```

```
            Configured fabric name: 41:6e:64:69:61:6d:6f:21

            Configured priority: 128

            Configured domain ID: 0x64(100) (preferred)

Principal switch run time information:

            Running priority: 2

Interface              Role          RCF-reject

---------------     -------------    ------------

fc2/1                 Downstream      Disabled

fc2/2                 Downstream      Disabled

fc2/4                 Upstream        Disabled

---------------     -------------    ------------
```

Step 6   Verify the local principal switch status.

Example:
```
switch# show fcdomain domain-list vsan 1

Number of domains: 5

Domain ID             WWN

---------     ----------------------

 0x61(97)     10:00:00:60:69:50:0c:fe

 0x62(98)     20:01:00:05:30:00:47:9f

 0x63(99)     10:00:00:60:69:c0:0c:1d

0x64(100)     20:01:00:05:30:00:51:1f [Local]

0x65(101)     10:00:00:60:69:22:32:91 [Principal]

---------     ----------------------
```

Step 7   Verify the next hop and destination for the switch.

Example:
```
switch# show fspf internal route vsan 1

FSPF Unicast Routes

--------------------------

 VSAN Number  Dest Domain   Route Cost    Next hops

----------------------------------------------

          1     0x61(97)          500       fc2/2

          1     0x62(98)         1000       fc2/1

                                            fc2/2

          1     0x63(99)          500       fc2/1

          1     0x65(101)        1000       fc2/4
```

Step 8 Verify the name server information.

Example:
```
switch# show fcns data vsan 1

VSAN 1:

-----------------------------------------------------------------

FCID       TYPE  PWWN                    (VENDOR) FC4-TYPE:FEATURE

-----------------------------------------------------------------

0x610400   N    10:00:00:00:c9:24:3d:90 (Emulex)    scsi-fcp

0x6105dc   NL   21:00:00:20:37:28:31:6d (Seagate)   scsi-fcp

0x6105e0   NL   21:00:00:20:37:28:24:7b (Seagate)   scsi-fcp

0x6105e1   NL   21:00:00:20:37:28:22:ea (Seagate)   scsi-fcp

0x6105e2   NL   21:00:00:20:37:28:2e:65 (Seagate)   scsi-fcp

0x6105e4   NL   21:00:00:20:37:28:26:0d (Seagate)   scsi-fcp

0x630400   N    10:00:00:00:c9:24:3f:75 (Emulex)    scsi-fcp

0x630500   N    50:06:01:60:88:02:90:cb             scsi-fcp

0x6514e2   NL   21:00:00:20:37:a7:ca:b7 (Seagate)   scsi-fcp

0x6514e4   NL   21:00:00:20:37:a7:c7:e0 (Seagate)   scsi-fcp

0x6514e8   NL   21:00:00:20:37:a7:c7:df (Seagate)   scsi-fcp

0x651500   N    10:00:00:e0:69:f0:43:9f (JNI)

Total number of entries = 12
```
Note The Cisco switch name server shows both local and remote entries, and does not time out the entries.

Default Settings for Advanced Fibre Channel Features

The following table lists the default settings for the features included in this chapter.

Table 3: Default Settings for Advanced Features

Parameters	Default
CIM server	Disabled
CIM server security protocol	HTTP
D_S_TOV	5,000 milliseconds
E_D_TOV	2,000 milliseconds
R_A_TOV	10,000 milliseconds

Parameters	Default
Timeout period to invoke fctrace	5 seconds
Number of frame sent by the fcping feature	5 frames
Remote capture connection protocol	TCP
Remote capture connection mode	Passive
Local capture frame limits	10 frames
FC ID allocation mode	Auto mode
Loop monitoring	Disabled
Interop mode	Disabled