

Troubleshooting Switch Level Issues and Interswitch Connectivity

This chapter describes how to identify and resolve problems that affect basic connectivity between switches, hosts, and storage in the network fabric.

The most common problems a system administrator can face may be categorized by two different scenarios:

- Switch-to-switch basic interconnectivity problems, which can result in the isolation of a port or VSAN due to incorrect parameters or settings on an ISL or VSAN
- Fabric to Server/Storage connectivity problems: identified by a Fx port not coming up or caused by zone or VSAN configuration errors

This section will present some of the most common scenarios, in which either switch-to-switch basic connectivity problems or fabric to end-devices problems can be found.

These scenario are grouped in three different sections:

- [Troubleshooting E Port Connectivity - ISL Isolation, page 3-1](#)
- [Troubleshooting TE Port Connectivity - VSAN Isolation, page 3-10](#)
- [Troubleshooting Fx Port Connectivity, page 3-13](#)

Troubleshooting E Port Connectivity - ISL Isolation

This section describes how to troubleshoot Inter-Switch Link (ISL) isolation, which may occur when you try to merge two separate fabrics or add a new domain to an existing fabric. It includes the following topics:

- [Overview, page 3-2](#)
- [Troubleshoot Switch and Port Parameters, page 3-3](#)
- [Troubleshooting a ZONE Merge Failures, page 3-5](#)
- [Troubleshooting a VSAN Configuration Conflict, page 3-6](#)
- [Troubleshooting a Domain ID Conflict, page 3-7](#)

Send comments to mdsfeedback-doc@cisco.com.

Overview

On an E port, only one VSAN can be passed and possibly be isolated. However, in a trunking E port (TE), multiple VSANs can become isolated while others are passing traffic. The same troubleshooting approach applies in both cases, except that on a trunking E port the troubleshooting may need to be done on a per-VSAN basis and/or on multiple VSANs.

Step 1) Verify that each VSAN is able to see the other switches within the same VSAN.

To verify that each switch is able to see the other switches, issue the following command at the exec prompt. This command is VSAN-specific. If a specific VSAN is omitted from the command, it will list the output for all VSANs.

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

The output of the command lists set of domain IDs and associated WWNs for each switch within a VSAN. This list provides the WWN of the switches owning each domain ID and the information about the principality of those switches in the fabric or VSAN they belong to.

Sample output #1 (obtained in a fabric with just 2 switches in VSAN 1)

```
switch# sh fcdomain domain-list vsan 1

Number of domains: 2
Domain ID          WWN
-----
0x4a(74)           20:01:00:05:30:00:13:9f [Local]
0x4b(75)           20:01:00:05:30:00:13:9e [Principal]
-----
```

This is an output of VSAN 1 in which 2 switches are seen. This indicates that the switch where the command has been issued has built its adjacency on VSAN 1 with the other switch in the same VSAN.

Sample output #2

```
switch# sh fcdomain domain-list vsan 1

Number of domains: 1
Domain ID          WWN
-----
0x4a(74)           20:01:00:05:30:00:13:9f [Local] [Principal]
-----
```

In this output only one switch is seen. This indicates that the switch where the command has been issued has not established adjacency with the neighboring switch in VSAN 1.

Possible Causes for the problem

In the previous output one domain ID is missing. The reason of this can be found in the erroneous configuration of several parameters between adjacent switches.

In case of E port/VSAN isolation the following parameters and configurations should be checked in each switch:

- Zoning configuration
- VSAN configuration
- Domain ID parameters
- Fabric Parameters & Timers

Send comments to mdsfeedback-doc@cisco.com.

Troubleshooting steps

The first step in the process is to understand the nature of the problem by checking the status of the E port. The **show interface** command can be used to display the port status. This command is very useful in troubleshooting switch connectivity issues. In case of error, this command provides indication of the protocol error or configuration mismatch that caused the problem, between parenthesis, immediately after the port operational status.

Sample output#3

```
switch# show interface fc4/1
fc4/1 is up
  Hardware is Fibre Channel
  Port WWN is 20:c1:00:05:30:00:13:9e
  Peer port WWN is 21:89:00:05:30:00:18:a2
  Admin port mode is auto, trunk mode is on
  Port mode is E, FCID is 0x6b0000
  Port vsan is 1
  Speed is 2 Gbps
  Receive B2B Credit is 12
  Receive Buffer Size is 2112
  Encapsulation is normal
  Beacon is turned off
  5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    109 frames input, 9728 bytes, 0 discards
      0 CRC, 0 unknown class
      0 too long, 0 too short
    108 frames output, 6652 bytes, 0 discards
    1 input OLS, 3 LRR, 1 NOS, 2 loop inits
    4 output OLS, 3 LRR, 3 NOS, 0 loop inits
```

When the port operational status shows that the port is up, it means that the E port is up and is currently passing traffic. The output shown above represents the output of a working E port.

Different types of isolation problems can be recognized by running the **show interface** command:

- Isolation due to ELP failure and mismatch in the switch or port parameters
- Isolation due to zone merge failure
- Isolation due to port/VSAN mismatch
- Isolation due to domain overlap
- Isolation due to invalid fabric reconfiguration

Troubleshoot Switch and Port Parameters

One of the possible causes for E port isolation is a mismatch in the configured switch or port parameters. The problem will affect the link initialization process, and eventually the initial ELP exchange. An example of the expected **show interface** command output is shown below:

```
switch# show interface fc2/4
fc2/4 is down (Isolation due to ELP failure)
  Hardware is Fibre Channel, WWN is 20:44:00:05:30:00:18:a2
  vsan is 1
  Beacon is turned off
  1445517676 packets input, 727667035658 bytes, 0 discards
  0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
```

Send comments to mdsfeedback-doc@cisco.com.

```
Received 0 runs, 0 jabber, 0 too long, 0 too short
    0 EOF abort, 0 fragmented, 0 unknown class
    100 OLS, 67 LRR, 37 NOS, 0 loop inits

133283352 packets output, 1332969530 bytes
Transmitted 198 OLS, 50 LRR, 0 NOS, 10 loop inits
```

In this example the interface is indicating a link isolation caused by an ELP failure on an E port. The ELP is a frame sent between two switches to negotiate fabric parameters. If you get this failure, verify the fabric parameters are the same for both switches.

Since fabric parameters are configured on a per switch basis, however, they are required to be the same for all switches within a fabric.

If the interface indicates an ELP failure verify the following parameters match using the **show fctimer** command:

- ED_TOV Timer
- RA_TOV Timer
- FS_TOV timer

An example of the show fctimer command where all default value are in use, is shown below

```
switch# show fctimer
F_S_TOV : 5000 milliseconds
D_S_TOV : 15000 milliseconds
E_D_TOV : 2000 milliseconds
R_A_TOV : 10000 milliseconds
```

Another parameter to check, is the Rcxbuffer size on the interface. This value should match on both the ends of a ISL. To verify the value of the Rcxbuffer size, use the following command:

```
switch# show port internal info interface fc2/1

fc2/1 - if_index: 1080000
Admin Config - state(up), mode(Auto), speed(auto), trunk(no trunk)
    beacon(off), snmp trap(on), tem(false)
    bb_credit(default), rxbufsize(2112), encap(default)
    description()
Operational Info - state(down), mode(ALL), speed(auto), trunk(no trunk)
    state reason(Link failure or not-connected)
    phy port enable (1), phy layer (FC)
    participating(1), port_vsan(1), null_vsan(0), fcid(0x000000)
    current state [PI_FSM_ST_LINK_INIT]
    port_init_eval_flag(0x00000001), cfg wait for none
    Mts node id 0x202
    cnt_link_failure(0), cnt_link_success(0), cnt_port_up(0)
    cnt_cfg_wait_timeout(0), cnt_port_cfg_failure(0), cnt_init_retry(0)
Port Capabilities -
    Modes: E,TE,F,FL,TL,SD
    Min Speed: 1000
    Max Speed: 2000
    Max Tx Bytes: 2112
    Max Rx Bytes: 2112
    Max Tx Buffer Credit: 255
    Max Rx Buffer Credit: 16
    Max Private Devices: 63
    Max Sourceable Pkt Size: 2112
    Hw Capabilities: 0xb
    Connector Type: 0x0
```

Send comments to mdsfeedback-doc@cisco.com.

```
FCOT info -
  Min Speed: 1000
  Max Speed: 2000
  Module Type: 8
  Connector Type: 7
  Gigabit Eth Compliance Codes: 0
  FC Transmitter Type: 3
  Vendor Name: PICOLIGHT
  Vendor ID: 0:4:133
  Vendor Part Num: PL-XPL-00-S23-28
  Vendor Revision Level:
Trunk Info -
  trunk vsans (allowed active) (1)
```

In the above examples, the highlighted rxbuffsize is 2112 bytes. This represents the default settings on a Cisco MDS 9000 switch interface.

Troubleshooting a ZONE Merge Failures

In the example below the **show interface** command indicates that the E port did not come up due to a zone merge failure. (Zoning information is on a per VSAN basis. Therefore, for a TE port, it may be necessary to verify that the zoning information does not conflict for any allowed VSAN.)

```
switch# show interface fc2/14

fc2/14 is down (Isolation due to zone merge failure)
  Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
  vsan is 1
  Beacon is turned off
    40 frames input, 1056 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 3 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    79 frames output, 1234 bytes, 16777216 discards
    Received 23 OLS, 14 LRR, 13 NOS, 39 loop inits
    Transmitted 50 OLS, 16 LRR, 21 NOS, 25 loop inits
```

A E port will segment with (isolation due to zone merge failure) if the following are true.

- If the active zoneset is different on the two switches.
- If the active zoneset on both switches contain a zone with the same name but with different zone members

To verify the zoning information use the following commands:

```
switch# show zone vsan 1
switch# show zoneset vsan 1
```

Two different approaches may be followed to solve a zone merge failure:

- Overwrite the zoning configuration of one switch with the other switch's configuration. This can be done with the following commands:

```
switch# zone merge interface fc2/7 import vsan 1
switch# zone merge interface fc2/7 export vsan 1
```

The import option of the command will overwrite the local switch's active zoneset with that of the remote switch. The export command will overwrite the remote switch's active zoneset with the local switch's active zoneset.

Send comments to mdsfeedback-doc@cisco.com.

- If the zoning databases between the two switches are overwritten, this option is not possible (because the final configuration should be a combination of the configuration of the two switches). Another option is to manually change the content of the zone database on either of the switches, and then have another cycle up/down issued on the isolated port.

If the isolation is specific to one VSAN and not on a E port, the correct way to issue the cycle up/down, is to remove the VSAN from the list of allowed VSANs on that trunk port, and re-insert it.

Do not simply issue a **shut/no shut** sequence of commands on the port, because this would affect all the VSANs crossing the EISL instead of just the VSAN experiencing the isolation problem.

Using the Zone Merge Analysis tool in Fabric Manager, the compatibility of two active zonesets in two switches can be checked before actually merging the two zonesets. Refer to the *Cisco MDS 9000 Fabric Manager User Guide* for more information.

Troubleshooting a VSAN Configuration Conflict

In the following example, the E port has been isolated because the interfaces connecting the two switches belong to different VSANs.

```
switch# show interface fc2/4
fc2/4 is down fc2/4 is down (isolation due to port vsan mismatch)

Hardware is Fibre Channel, WWN is 20:44:00:05:30:00:63:5e
vsan is 2
Beacon is turned off
 30 frames input, 682 bytes, 0 discards
 0 runts, 0 jabber, 0 too long, 0 too short
 0 input errors, 0 CRC, 0 invalid transmission words
 0 address id, 0 delimiter
 0 EOF abort, 0 fragmented, 0 unknown class
 30 frames output, 583 bytes, 0 discards
Received 2 OLS, 2 LRR, 2 NOS, 5 loop inits
Transmitted 5 OLS, 3 LRR, 2 NOS, 4 loop inits
```

In the above example, the E port isolated because the interface of the 2 switches belong to different VSANS. To resolve this issue move the interfaces to the same VSAN.

You can check the VSAN membership with the switch interfaces with the following command.

```
switch# show vsan membership
vsan 1 interfaces:
    fc2/1  fc2/2  fc2/3  fc2/4  fc2/6  fc2/7  fc2/8  fc2/9
    fc2/10 fc2/11 fc2/12 fc2/14 fc2/15 fc2/16 fc7/1  fc7/2
    fc7/3  fc7/4  fc7/5  fc7/6  fc7/7  fc7/8  fc7/9  fc7/10
    fc7/11 fc7/12 fc7/13 fc7/14 fc7/15 fc7/16 fc7/17 fc7/18
    fc7/19 fc7/20 fc7/21 fc7/22 fc7/23 fc7/24 fc7/25 fc7/26
    fc7/27 fc7/28 fc7/29 fc7/30 fc7/31 fc7/32

vsan 2 interfaces:
    fc2/5  fc2/13

vsan 4094(isolated_vsan) interfaces:
```

The command shows that all the interfaces on the switch belong to VSAN 1, with the exception of interface 2/5 and 2/13 that are part of VSAN 2.

Send comments to mdsfeedback-doc@cisco.com.

Troubleshooting a Domain ID Conflict

In a Fibre Channel network, the principal switch is used to issue domain IDs when a new switch is added to an existing fabric. However, when two fabrics merge, the principal switch selection process determines which one of the pre-existing switches becomes that principal switch. The election of the new principal switch is characterized by the following rules:

1. A switch with a non-empty domain ID list has priority over a switch that has an empty domain ID list, and the principal switch will be the principal switch of the first fabric. In the case of a single switch fabric, it does not contain a domain ID list.
2. If both fabrics have a domain ID list, the priority between the two principal switches is determined by configured switch priority. This is a user-settable parameter - the lower the value the higher the priority.
3. If the principal switch cannot be determined by the two previous criteria, the principal switch is then determined by the World Wide Names of the two switches. The lower value has the higher priority.

When merging two fabrics, the administrator can expect the following behavior:

- When connecting a single-switch fabric to a multi-switch fabric, the multi-switch fabric always retains its principal switch regardless of the principal switch priority setting on the single switch fabric.
- When powering up a new switch that is connected to an existing fabric with two or more switches, the existing switch fabric always retains its principal switch, even if the new switch has a higher administratively assigned principal switch priority.
- When powering up a new switch that is connected to a standalone switch, the new principal switch is determined by the administratively set priority. If no priority is set (the default priority is used in every switch), it is determined by the World Wide Name. This also applies to connecting to two single-switch fabrics.
- When connecting a multi-switch fabric to another multi-switch fabric, the principal switch is determined by the administratively set priority. If no priority is set (default value is used by every switch) it is determined by the World Wide Name of the existing principal switches of the two fabrics.

There are several reasons why two switch fabrics would not merge:

- If two switch fabrics with two or more switches are connected, and both fabrics that have switches with the domain ID already assigned and the auto-reconfigure option is disabled (this option is disabled by default), the E ports that are used to connect the two fabrics will be isolated.

In this case, the following error message is returned in the **show interface** command.

```
switch# show interface fc2/14
fc2/14 is down (Isolation due to domain overlap)
  Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
  vsan is 2
  Beacon is turned off
    192 frames input, 3986 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 3 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    231 frames output, 3709 bytes, 16777216 discards
  Received 28 OLS, 19 LRR, 16 NOS, 48 loop inits
  Transmitted 62 OLS, 22 LRR, 25 NOS, 30 loop inits
```

To view which domain are currently in your fabric use the following command. This command can be issued to both fabrics to determine which domain IDs are overlapping.

Send comments to mdsfeedback-doc@cisco.com.

```
switch# sh fcdomain domain-list vsan 1

Number of domains: 2
Domain ID          WWN
-----
0x4a(74)           20:01:00:05:30:00:13:9f [Local]
0x4b(75)           20:01:00:05:30:00:13:9e [Principal]
-----
```

The output shown is representative of a simple two switches fabric.

If a domain is currently isolated due to domain overlap, and you later enable the auto-reconfigure option on both switches, the fabric continues to be isolated. However, if you enable the auto-reconfigure option on both switches before connecting the fabric, a disruptive reconfiguration (RCF) occurs. The RCF functionality would automatically force a new principal switch selection and cause new domain ID to be assigned to the different switches. A disruptive reconfiguration may affect data traffic.

To enable the auto-reconfigure option on a particular VSAN use the following command:

```
switch(config)# fcdomain auto-reconfigure vsan 10
```

There are different ways of resolving this issue. One possible solution is to cause an RCF in the fabric with a disruptive restart of the domain manager on the switch. The RCF functionality will cause all switches in both fabrics to empty their domain ID list and select a new principal switch. The overlapping domain ID would be assigned to which ever switch requests it first from the newly selected principal switch.

The second switch to request that same domain ID would be assigned a new domain ID. This will only work if the overlapping domain IDs are not statically defined on the switches. If the domain ID is statically defined on the switch, then the switch does not accept any other domain ID than the one that is configured. If its request for the configured domain ID is not granted, it isolates itself from the fabric. The RCF functionality is disruptive and can cause end nodes to be assigned new domain IDs. By default, Cisco MDS 9000 Family switches accept disruptive restarts. You can configure the switch in order to reject incoming RCFs on a per-VSAN and port level basis (enabling the **rcf-reject** option).

In case the **rcf-reject** option is on, in order to have the RCF propagated to the switches in the fabric, must have the RCF reject property disabled. To turn this option off use the following command:

```
switch(config-if)# no fcdomain rcf-reject vsan 1
```

At this point a disruptive restart should be triggered, by using the following command:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# fcdomain restart disruptive vsan 1
switch(config)#
```

When you do a disruptive restart on your switch and the switch on the other side does not have disruptive restart enabled the error on the E port would be the following

```
switch# show interface fc2/5
fc2/5 is down (isolation due to invalid fabric reconfiguration)
  Hardware is Fibre Channel
  Port WWN is 20:45:00:05:30:00:18:a2
  Admin port mode is auto, trunk mode is on
  Port vsan is 1
  Receive data field size is 2112
```


Send comments to mdsfeedback-doc@cisco.com.

```

Beacon is turned off
5 minutes input rate 16 bits/sec, 2 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
342 frames input, 9492 bytes, 199 discards
  0 CRC, 0 unknown class
  0 too long, 0 too short
143 frames output, 4184 bytes, 0 discards
2 input OLS, 4 LRR, 2 NOS, 12 loop inits
6 output OLS, 2 LRR, 5 NOS, 1 loop inits
switch#

```

If the overlapping domain IDs are statically assigned, or you want to manually assign the new domain IDs, it would be necessary to go into the switch with the overlapping domain ID, configure a new domain ID for that switch, and restart the domain manager process to merge the two fabrics. To configure a domain ID on the switch use the following command. Domain IDs are assigned on a per-VSAN basis.

```

switch(config)# fcdomain domain 3 preferred vsan 1
switch(config)# fcdomain domain 3 static vsan 1
switch(config)#

```

When configuring a domain ID on a switch, there are two options - static and preferred. The static option tells the switch to request that particular domain in the fabric. If it does get that particular address, it will isolate itself from the fabric. With the preferred option, the switch requests the domain ID, but if that ID is not available it will accept another ID. After configuring the domain ID it is necessary to restart the domain manager to merge the two fabrics.

```

switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcdomain restart vsan 1
switch(config)#

```

If a switch cannot get a statically configured address it would isolate itself from the fabric. When it isolates itself the **show interface** output is the following.

```

switch# show interface fc2/14
fc2/14 is down (isolation due to domain overlap )
Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
vsan is 2
Beacon is turned off
192 frames input, 3986 bytes, 0 discards
0 runts, 0 jabber, 0 too long, 0 too short
0 input errors, 0 CRC, 3 invalid transmission words
0 address id, 0 delimiter
0 EOF abort, 0 fragmented, 0 unknown class
231 frames output, 3709 bytes, 16777216 discards
Received 28 OLS, 19 LRR, 16 NOS, 48 loop inits
Transmitted 62 OLS, 22 LRR, 25 NOS, 30 loop inits

```

While of the neighbor switch E port the message would be the following

```

switch2# show interface fc9/4
fc9/4 is down (Isolation due to domain other side eport isolated)
Hardware is Fibre Channel
Port WWN is 22:04:00:05:30:00:13:9e
Admin port mode is auto, trunk mode is off
Port vsan is 1
Receive data field size is 2112
Beacon is turned off
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec

```

Send comments to mdsfeedback-doc@cisco.com.

```

2547 frames input, 173332 bytes, 0 discards
  0 CRC,  0 unknown class
  0 too long, 0 too short
2545 frames output, 120300 bytes, 0 discards
14 input OLS, 12 LRR, 9 NOS, 33 loop inits
31 output OLS, 17 LRR, 13 NOS, 11 loop inits
switch2#

```

To fix the issue, the administrator can either change the static domain ID that is overlapping by manually configuring a new static domain ID for the isolated switch, or disable the static domain assignment, and allow the switch to request a new domain ID after a fabric reconfiguration.

For example, two switches may be merging and one of the switches is already powered up, but the second switch has a domain ID preconfigured. In this case, the switch that is powered up will have the priority in keeping the conflicting domain ID. The presently powered-on switch, being the principal switch, will assign a new domain ID to the new switch.

The E port could still isolate if the new switch has the domain ID configured as static, thus it would not take any other domain ID except for the one configured. If this were the case, it would be necessary to configure a new domain ID on the switch before the two switches could merge.

Troubleshooting TE Port Connectivity - VSAN Isolation

Trunking E ports (TE ports) are similar to E ports except they carry traffic for multiple VSANs. E ports carry traffic for a single VSAN. Because TE ports carry traffic for multiple VSANs, ISL isolation can affect one or more VSANs. For this reason, on a TE port you must troubleshoot ISL isolation on each VSAN.

Even in case of VSAN isolation, the starting point for troubleshooting the problem is to issue the **show interface** command.

The following example shows what the result of the **show interface** command, issued on a TE port in case of no VSAN is isolated (normal behavior).

```

switch# show interface fc7/9
fc7/9 is trunking
  Hardware is Fibre Channel
  Port WWN is 21:89:00:05:30:00:18:a2
  Peer port WWN is 20:c1:00:05:30:00:13:9e
  Admin port mode is auto, trunk mode is on
  Port mode is TE
  Speed is 2 Gbps
  vsan is 1
  Beacon is turned off
  FCID is 0x000000
  Receive B2B Credit is 12
  Trunk vsans (allowed active) (1,333)
  Trunk vsans (operational)    (1,333)
  Trunk vsans (up)            (1,333)
  Trunk vsans (isolated)      ()
  Trunk vsans (initializing)  ()
  Counter Values (current):
    262 frames input, 18808 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 2 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    264 frames output, 16960 bytes, 0 discards
    Received 5 OLS, 3 LRR, 2 NOS, 11 loop inits
    Transmitted 8 OLS, 4 LRR, 2 NOS, 3 loop inits

```

Send comments to mdsfeedback-doc@cisco.com.

```

Counter Values (5 minute averages):
  0 frames input, 136 bytes, 0 discards
  0 runts, 0 jabber, 0 too long, 0 too short
  0 input errors, 0 CRC, 0 invalid transmission words
  0 address id, 0 delimiter
  0 EOF abort, 0 fragmented, 0 unknown class
  0 frames output, 117 bytes, 0 discards
  Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
  Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
switch#

```

In the above example, the TE port is carrying traffic for VSANs 1 and 333. This is an example of a working TE port. There are no isolated VSANs in the list.

The following example shows the output of the **show interface** command, if one or more VSANs are isolated:

```

switch# show interface fc2/14
fc2/14 is trunking
  Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
  Port mode is TE
  Speed is 2 Gbps
  vsan is 2
  Beacon is turned off
  Trunk vsans (allowed active) (1-3,5)
  Trunk vsans (operational)    (1-3,5)
  Trunk vsans (up)            (2-3,5)
  Trunk vsans (isolated)      (1)
  Trunk vsans (initializing)  ()
    475 frames input, 8982 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 3 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    514 frames output, 7509 bytes, 16777216 discards
    Received 30 OLS, 21 LRR, 18 NOS, 53 loop inits
    Transmitted 68 OLS, 25 LRR, 28 NOS, 32 loop inits

```

In the above example, the TE port has one VSAN isolated. The reason for VSAN isolation can be checked using the following command:

```
switch# sh interface fc2/14 trunk vsan 1
```

The command provides the same messages given by the **show interface**, in case of E port isolation. For example:

```

switch# sh interface fc2/14 trunk vsan 1
fc2/15 is trunking
  Vsan 1 is down (Isolation due to zone merge failure)

```

This output shows that VSAN 1 is isolated because of a zone merge error.

An alternative way to determine the cause of VSAN isolation, is to issue the following command:

```
switch#show port internal info interface fc2/14
```

The last few lines provide a description of the reason for VSAN isolation, for all the isolated VSANs.

```

switch# show port internal info int fc2/14

fc2/14 - if_index: 0x0109C000, phy_port_index: 0x3c
  Admin Config - state(up), mode(TE), speed(auto), trunk(on)

```

Send comments to mdsfeedback-doc@cisco.com.

```

beacon(off), snmp trap(on), tem(false)
rx bb_credit(default), rx bb_credit multiplier(default)
rxbufsize(2112), encap(default), user_cfg_flag(0x3)
description()
Operational Info - state(trunking), mode(TE), speed(2 Gbps), trunk(on)
state reason(None)
phy port enable (1), phy layer (FC)
participating(1), port_vsan(7), fcid(0x000000)
rx bb_credit multiplier(0), rx bb_credit(12)
current state [PI_FSM_ST_TEPOR_INIT_TRUNKING_ENABLED]
port_init_eval_flag(0x00000001), cfg wait for none
Mts node id 0x202
eport_init_flag(0x00000386), elp_chk_flag(0x0000000A)
elp_rcvd_fc2_handle(0x00000000), elp_sent_fc2_handle(0x0800864E)
esc_chk_flag(0x0000002A), esc_fc2_handle(0x0801864F)
elp_flags(0x0000), classes_supported(F,2,3), tx bb_credit(255)
cnt_link_failure(1), cnt_link_success(5), cnt_port_up(0)
cnt_cfg_wait_timeout(0), cnt_port_cfg_failure(0), cnt_init_retry(0)
oper trunk mode(on)
Port Capabilities -
Modes: E,TE,F,FL,TL,SD
Min Speed: 1000
Max Speed: 2000
Max Sourcedable Pkt Size: 2112
Max Tx Bytes: 2112
Max Rx Bytes: 2112
Max Tx Buffer Credit: 255
Max Rx Buffer Credit: 12
Max Rx Buffer Credit (ISL): 12
Default Rx Buffer Credit: 12
Default Rx Buffer Credit (ISL): 12
Default Rx Buffer Credit Multiplier: 0
Rx Buffer Credit change not allowed
Max Private Devices: 63
Hw Capabilities: 0xb
Connector Type: 0x0
FCOT info -
Min Speed: 1000
Max Speed: 2000
Module Type: 8
Connector Type: 7
Gigabit Eth Compliance Codes: 0
FC Transmitter Type: 3
Vendor Name: IBM
Vendor ID: 8:0:90
Vendor Part Num: IBM42P21SNY
Vendor Revision Level: AA20
Trunk Info -
trunk vsans (allowed active) (1,7-8)
trunk vsans (up) (7)
trunk vsans (isolated) (1,8)
TE port per vsan information
fc2/29, Vsan 1 - state(down), state reason(Isolation due to domain other side eport
isolated), fcid(0x000000)
port init flag(0x10000), current state [TE_FSM_ST_ISOLATED_DM_ZS]
fc2/29, Vsan 7 - state(up), state reason(None), fcid(0x690202)
port init flag(0x38000), current state [TE_FSM_ST_E_PORT_UP]
fc2/29, Vsan 8 - state(down), state reason(Isolation due to vsan not configure
d on peer), fcid(0x000000)
port init flag(0x0), current state [TE_FSM_ST_ISOLATED_VSAN_MISMATCH]

switch#

```

Send comments to mdsfeedback-doc@cisco.com.

In the example, VSAN 7 is up, while two VSANs are isolated (VSAN 1 and 8, the first one because of domain ID misconfiguration, and the second one because of VSAN misconfiguration).

Troubleshooting Fx Port Connectivity

This section describes how to troubleshoot problems with a switch interface in fabric mode (F port). An F port may be connected to a single N port, which is the mode used by peripheral devices (hosts or storage).

Two different major scenarios can be recognized in all the possible cases an administrator can incur in troubleshooting an Fx port:

- The port doesn't come up (just check the configuration of the interface, the cabling and the port connected to the switch).
- The port comes up, but the host is not able to communicate with the storage subsystem (in this case the configuration of VSAN and zones need to be checked)

Fx Port Fails to Achieve Up State

This section describes the troubleshooting steps to follow if, after connecting an N port to the switch, the port does not go into the up state.

In order for an Fx port to come up on a switch, the switch port must first acquire bit and word synchronization with the N port, and receive the FLOGI issued by the connected N port.

If any one of these steps does not occur, the switch port will not come up as an F port.

One of the first steps in troubleshooting an F port not coming up is to issue the **show interface** command from the CLI. This tells you where the process of interface initialization stops, and which steps to be used to solve the problem.

The following examples show different states of the interface, as displayed by the **show interface** command. In the examples, note the description of the problem that is printed immediately after the operational state of the interface.

FCOT Is Not Present

In the example below, the state of the interface is (Fcot is not present). This indicates that the switch does not detect the presence of an SFP on the interface. If this is the case verify that the SFP on the interface is seated properly. If reseating the SFP does not resolve the issue, replace the SFP or try another port on the switch.

```
switch# show interface fc7/31
fc7/31 is down (Fcot not present)
  Hardware is Fibre Channel
  Port WWN is 21:9f:00:05:30:00:18:a2
  Admin port mode is auto, trunk mode is on
  vsan is 1
  Beacon is turned off
  Counter Values (current):
    0 frames input, 0 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
```

Send comments to mdsfeedback-doc@cisco.com.

```

0 frames output, 0 bytes, 0 discards
Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
Counter Values (5 minute averages):
0 frames input, 0 bytes, 0 discards
0 runts, 0 jabber, 0 too long, 0 too short
0 input errors, 0 CRC, 0 invalid transmission words
0 address id, 0 delimiter
0 EOF abort, 0 fragmented, 0 unknown class
0 frames output, 0 bytes, 0 discards
Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits

```

Link_Failure or Not Connected

The following example shows the interface down as a result of a link failure or disconnect.

```

switch# show interface fc7/31
fc7/31 is down (Link_Failure or not connected)
  Hardware is Fibre Channel
  Port WWN is 21:9f:00:05:30:00:18:a2
  Admin port mode is auto, trunk mode is on
  vsan is 1
  Beacon is turned off
  Counter Values (current):
    0 frames input, 0 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    0 frames output, 0 bytes, 0 discards
    Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
  Counter Values (5 minute averages):
    0 frames input, 0 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    0 frames output, 0 bytes, 0 discards
    Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits

```

The message “Link_Failure” or “not connected” can happen if nothing is connected to the specific interface (as in the case of a broken fiber), or if there is no bit synchronization between the switch interface and the Nx port directly connected. (In the case of a broken fiber, if **only** the TX path from the F port to the N port is broken, the switch interface will still have an operational Rx path, and so will still obtain bit synchronization from the bit stream received from the N port. It will also be able to recognize an incoming NOS from the N port and reply with an OLS. But because the transmitted OLS never reaches the N port the R_T_TOV timer expires. In this scenario the status of the port will also show “Link_Failure or not connected”.)

The key difference between this case and the “no bit synchronization” case, is that the input and output counts for OLS & NOS increment (as there is bit synchronization but no word synchronization). In such a state, you can check that the Tx path from switch to the Rx input on N port interface is properly connected. A faulty transmitter on the switch’s SFP or a faulty receiver on the N port’s SFP could also cause the issue.

Send comments to mdsfeedback-doc@cisco.com.

If, on the other hand, just the Rx path to the switch was broken and the TX path was intact, there would be no bit synchronization. In this case, the switch would not attempt to move to the link initialization stage, and therefore the OLS & NOS counters would never increment. Some possible causes of the problem could be a faulty SFP, or a speed mismatch between the Fx port and the Nx port, in case speed autonegotiation is disabled or doesn't work properly with the specific HBA/Storage port.

One of the first steps in the effort to solve the incompatibility, is to verify the speed configuration on the switch port. If the switch port is configured for a specific speed, configure the switch port for auto-speed detection. If the port still does not come up or the speed autonegotiation was already in place, the next possible step is to statically configure the speed of the port in order to match the one of the Nx port directly connected.

In case this doesn't solve the issue, and the port stays in the same status, the problem is probably a physical issue. Verify all physical parts between and including the switch port, the SFP on the switch port, and if used on the HBA, the HBA itself and the fiber connections.

Interface Bouncing between Offline and Initializing

In the above example, the state of the link bounces between initializing and offline. This indicates that the link has acquired bit and word synchronization, but has not been able to negotiate the type of link the switch port needs to become operative (because the initialization failed or an FLOGI is not issued by the HBAs or the FLOGI has been rejected by the switch).

```
switch# show interface fc7/2
fc7/2 is down (Initializing)
  Hardware is Fibre Channel
  Port WWN is 21:82:00:05:30:00:18:a2
  Admin port mode is F, trunk mode is on
  vsan is 1
  Beacon is turned off
  Counter Values (current):
    143274267 frames input, 182897329172 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    3016111132 frames output, 6029792843852 bytes, 0 discards
    Received 14 OLS, 14 LRR, 0 NOS, 31 loop inits
    Transmitted 87 OLS, 23 LRR, 65 NOS, 37 loop inits
  Counter Values (5 minute averages):
    0 frames input, 41 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    0 frames output, 112 bytes, 0 discards
    Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits

switch# sh int fc7/2
fc7/2 is down (Offline)
  Hardware is Fibre Channel
  Port WWN is 21:82:00:05:30:00:18:a2
  Admin port mode is F, trunk mode is on
  vsan is 1
  Beacon is turned off
  Counter Values (current):
    143274267 frames input, 182897329172 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
```

Send comments to mdsfeedback-doc@cisco.com.

```

0 address id, 0 delimiter
0 EOF abort, 0 fragmented, 0 unknown class
3016111132 frames output, 6029792843852 bytes, 0 discards
Received 14 OLS, 14 LRR, 0 NOS, 31 loop inits
Transmitted 87 OLS, 23 LRR, 65 NOS, 37 loop inits
Counter Values (5 minute averages):
0 frames input, 41 bytes, 0 discards
0 runts, 0 jabber, 0 too long, 0 too short
0 input errors, 0 CRC, 0 invalid transmission words
0 address id, 0 delimiter
0 EOF abort, 0 fragmented, 0 unknown class
0 frames output, 112 bytes, 0 discards
Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits

```

Usually a port in this state cycles between the initializing state and the off-line state. If this the error, verify that the switch port is configured as an F port. A port that is mistakenly set to be E port could cause this error when connecting to an N port. If setting the switch port to autodetect mode still doesn't resolve the issue, try to statically configure the port type in order to match the Nx port behavior with respect to loop or point-to-point initialization. There are some limited case in which the port type auto negotiation could not work properly for incompatibility with some old HBAs. (The automatic detection for the port mode is not applicable on an OSM module where at maximum one TE/E port can be configured per quad.)

If after having statically configured the port mode, it still doesn't come up, verify that the HBA is working properly and possibly power-cycle the HBA (i.e. booting the server or resetting the adapter).

To check whether a FLOGI is issued to the switch during the Fx port initialization, the **fc analyzer** can be used.

In the example below, the fc analyzer tool has been used with the necessary filtering to capture the FLOGI sent by the N port. Refer to the *Cisco MDS 9000 Family Configuration Guide* for more information.

```

Frame 25 (176 bytes on wire, 176 bytes captured)
Ethernet II
MDS Header(SOFi3/EOft)
Fibre Channel
FC ELS
  Cmd Code: FLOGI (0x04)
  Common Svc Parameters
    B2B Credit: 3
    Common Svc Parameters: 0x0 (Normal B2B Credit Mgmt)
    0000 .... = BB_SC Number: 0
    .... 1000 0100 0000 = Receive Size: 2112
    Max Concurrent Seq: 0
    Relative Offset By Info Cat: 0
    E_D_TOV: 0
    N_Port Port_Name: 10:00:00:09:c9:28:c7:01 (00:09:c9)
    Fabric/Node Name: 10:00:00:09:c9:28:c7:01 (00:09:c9)
  Class 1 Svc Parameters
    Service Options: 0x0 (Class Not Supported)
  Class 2 Svc Parameters
    Service Options: 0x0 (Class Not Supported)
  Class 3 Svc Parameters
    Service Options: 0x8800 (Seq Delivery Requested)
    Initiator Control: 0x0 (Seq Delivery Requested)
    Recipient Control: 0x0 (Seq Delivery Requested)
    Class Recv Size: 0
    Total Concurrent Seq: 0
    End2End Credit: 0
    Open Seq Per Exchg: 0
  Class 4 Svc Parameters

```


Send comments to mdsfeedback-doc@cisco.com.

```
Service Options: 0x0(Class Not Supported)
Vendor Version: 00000000000000000000000000000000
```

If the FLOGI is received by the switch, but the port is still not coming up, further investigation is needed to determine if the FLOGI is rejected by the switch (i.e. still using the fcanalyzer) or the cause is a misbehaving host, a broken fiber or a flappy connection between the end device and the Fx port on the switch. (If an Nx port is considered faulty by the driver/firmware or the ASIC used on the HBA, it can be configured to be in optical bypass. This results in the RX and TX paths being internally connected in the loopback by the on-board circuitry. If this happens, the switch port connected to the faulty device will reach bit and word synchronization with itself. If the port is configured in auto mode, this will cause the port to issue an ELP and try to initialize as a TE/E Port, even if an end device is physically connected to that interface. In this case a port reason code of isolation due to ELP failure, can show up even if an ISL is not present. To fix the issue, one possible approach is to reset the HBA or changing it if the problem persists.)

Point-to-point link comes up as FL_Port

If a point-to-point link comes up as a FL port, it could be caused by any of the following issues.

The switch port could be configured as either an autodetect port, or forced to be F port. In order to verify the actual configuration of the port, again the **show interface** command can be used:

```
switch#show interface fc7/5
fc7/5 is up
  Hardware is Fibre Channel
  Port WWN is 20:4d:00:05:30:00:18:a2
  Admin port mode is auto, trunk mode is on
  Port mode is F, FCID is 0x660000
  Port vsan is 1
  Speed is 1 Gbps
  Receive B2B Credit is 16
  Receive data field size is 2112
  Beacon is turned off
  5 minutes input rate 256 bits/sec, 32 bytes/sec, 0 frames/sec
  5 minutes output rate 256 bits/sec, 32 bytes/sec, 0 frames/sec
    369288 frames input, 11823952 bytes, 0 discards
      0 CRC, 0 unknown class
      0 too long, 0 too short
    369288 frames output, 11826732 bytes, 0 discards
    1 input OLS, 0 LRR, 2 NOS, 0 loop inits
    3 output OLS, 3 LRR, 1 NOS, 0 loop inits
```

An alternative way to get the same information and also the information about the configured speed is to use the following command.

```
switch# show port internal info interface fc7/5
```

The second line of the long output generated by the command shows the administrative status of the port (that reflect what configured by the administrator on the switch).

For example, issuing the command on a switch interface fc7/5 where a no shutdown command has been issued and where the port mode has been configured to be auto-detected, with speed auto-negotiation enabled and trunking capabilities enabled, the following output is displayed:

```
switch# show port internal info interface fc7/5
fc7/5 - if_index: 0x 1304000, phy_port_index: 0x84
  Admin Config - state(up), mode(auto), speed(auto), trunk(on)
    beacon(off), snmp trap(on), tem(false)
    rx bb_credit(default), rx bb_credit multiplier(default)
    rxbufsize(2112), encap(default), user_cfg_flag(0x1)
```

Send comments to mdsfeedback-doc@cisco.com.

```

description()
Operational Info - state(up), mode(F), speed(1 Gbps), trunk(off)
state reason(None)
phy port enable (1), phy layer (FC)
participating(1), port_vsan(1), null_vsan(0), fcid(0xef0300)
rx bb_credit multiplier(0), rx bb_credit(12)
current state [PI_FSM_ST_F_PORT_UP]
port_init_eval_flag(0x00003001), cfg wait for none
Mts node id 0x702
cnt_link_failure(54), cnt_link_success(53), cnt_port_up(4)
cnt_cfg_wait_timeout(0), cnt_port_cfg_failure(0), cnt_init_retry(0)
Port Capabilities -
Modes: E,TE,F,FL,TL,SD
Min Speed: 1000
Max Speed: 2000
Max Sourcingable Pkt Size: 2112
Max Tx Bytes: 2112
Max Rx Bytes: 2112
Max Tx Buffer Credit: 255
Max Rx Buffer Credit: 12
Max Rx Buffer Credit (ISL): 12
Default Rx Buffer Credit: 12
Default Rx Buffer Credit (ISL): 12
Default Rx Buffer Credit Multiplier: 0
Rx Buffer Credit change not allowed
Max Private Devices: 63
Hw Capabilities: 0xb
Connector Type: 0x0
FCOT info -
Min Speed: 1000
Max Speed: 2000
Module Type: 8
Connector Type: 7
Gigabit Eth Compliance Codes: 0
FC Transmitter Type: 3
Vendor Name: CISCO-AGILENT
Vendor ID: 0:48:211
Vendor Part Num: QFBR-5796L
Vendor Revision Level:
Trunk Info -
trunk vsans (allowed active) (1)

```

If the configuration of the switch port is configured as auto, and the point-to-point link still comes up as an FL port, verify that the HBA is configured as an NL port also.

Some HBAs support only NL mode. Verify the HBA capabilities with the vendor.

Interface UP and Connectivity Problems - Troubleshooting VSANs and Zones

If a server is not able to see a storage device, it may be because of a VSAN or zone misconfiguration.

Zone problems are more likely to happen than VSAN issues. This is because zone configuration and the overall zone protocols are more complex than VSAN configuration, and the VSAN membership can be verified using the CLI or the GUI. Therefore, checking the zone configuration is the first step to take when the host is not able to access the storage, and the port are all up along the path between the server HBA and the storage subsystem interface.

Send comments to mdsfeedback-doc@cisco.com.

Troubleshooting Zones – Case of end devices belonging to the default zone

The first thing to check when performing zone troubleshooting is whether the storage subsystem port and the server HBAs have been configured to belong to a specific zone, or whether they belong to the default zone (any device that is not part of any active zone, it is considered to be part of the default zone).

In case the device does not belong to any zone, check whether the default zone default policy is set to “permit” on any switch in the fabric for the specific VSAN.

To set the default zone policy to “permit”, use the following command:

```
switch(config)# zone default-zone permit vsan 1
```

If the server is still not able to see the storage after you have configured the default-zone policy to “permit” on each switch in the fabric, check the VSAN configuration or the server and storage subsystem configuration.

Troubleshooting Zones – Case of end devices belonging to a specific zone

If zoning has been configured and the server and storage subsystem having the problem, it is important to check the correctness of the zoning configuration.

The following configuration steps should be followed in order to have zoning to work properly in the fabric or in a specific VSAN:

- The zone must be created in a VSAN.
- The correct FC IP, pwwn, or alias must be added to the Zone in the VSAN.
- A zoneset must be created in the VSAN.
- The zone must be added to the zoneset in the VSAN.
- The zone set must be activated in the VSAN.

It is important to verify the information contained in the active zoneset database for a particular VSAN. The active zoneset database is the only meaningful information for troubleshooting, because the active zoneset policy is applied to every switch in the fabric.

Verify active zoneset configuration

To verify that the zone has been created in a VSAN, use the **show zone active** command:

```
switch# show zone active
```

If there are configured active zones on the switch, the output of the command should look like:

```
switch# show zone active

zone name Zone1 vsan 1
  pwwn 50:06:0e:80:03:50:5c:03
  pwwn 20:00:00:e0:69:a1:b9:fc

zone name Zone2 vsan 1
  pwwn 10:00:00:e0:02:21:df:ef
  pwwn 20:00:00:e0:69:a1:b9:fc

zone name Zone3 vsan 1
  fwwn 20:42:00:05:30:00:63:9e
  fwwn 20:43:00:05:30:00:63:9e
```

Send comments to mdsfeedback-doc@cisco.com.

```
zone name zone-cc vsan 2
  pwwn 50:06:0e:80:03:50:5c:01
  pwwn 20:00:00:e0:69:41:a0:12
  pwwn 20:00:00:e0:69:41:98:93
```

If the output of this command doesn't show any information, this means that no zoneset has been activated in the fabric. If this is the case, you can use the two commands **show zone** or **show zoneset** to determine whether a zone configuration has been issued on the switch. (Zone configuration, and configuration changes do not get propagated to the other switches in the fabric, but only the changes to the active zones or active zoneset get propagated. For this reason if zone information is configured on one switch, it won't appear in the configuration of other switches).

Assuming that the zone configuration has been issued on the switch, but no active zoneset is shown, the next step is to enable the active zoneset in the specific VSAN to which the zoneset is supposed to belong.

To activate a zoneset in a defined VSAN, run the following command:

```
switch(config)# zoneset activate name ZonesetName vsan 1
```

The command must be issued on same switch the zone configuration took place. By copying the active zone database on the local zone database, it is possible to modify and apply those changes to the active zoneset on a different switch from the one initially used to issue the active zone configuration.

If no port shows as isolated, it means that all the switches in the fabric (or in the specific VSAN) share the same active zone database. This is ensured by the merge and change protocols used whenever any of the following occurs:

- two fabrics are connected
- a new ISL is configured in the fabric
- a new switch is connected to a pre-configured fabric
- changes are applied to the active zone database on any switch in the fabric

Verify active zoneset membership

In case no port shows as isolated, check that the HBA's FCID or pwwn and the storage subsystem FCID or pwwn are correctly configured to belong to the same zone. Or, if they have been added to an fcalias, check the correctness of the fcalias definition. Verify this information using the **show zone active** and **show zone** commands, or by using the Fabric Manager VSAN/Zoning View.

In the following example, only the server HBA's PWWN appears to be configured in the active zoneset belonging to zone-cc on VSAN 2.

```
switch# show zoneset active
zoneset name ZoneSet1 vsan 1
zone name Zone1 vsan 1
  pwwn 50:06:0e:80:03:50:5c:03
  pwwn 20:00:00:e0:69:a1:b9:fc

zone name Zone2 vsan 1
  pwwn 10:00:00:e0:02:21:df:ef
  pwwn 20:00:00:e0:69:a1:b9:fc

zone name Zone3 vsan 1
  fwwn 20:42:00:05:30:00:63:9e
  fwwn 20:43:00:05:30:00:63:9e

zone name zone-cc vsan 2
  pwwn 50:06:0e:80:03:50:5c:01
  pwwn 20:00:00:e0:69:41:a0:12
```

Send comments to mdsfeedback-doc@cisco.com.

```
pwwn 20:00:00:e0:69:41:98:93
```

To determine why, issue the **show zoneset** command.

```
switch# show zoneset
zoneset name ZoneSet1 vsan 1
zone name Zone1 vsan 1
    pwwn 50:06:0e:80:03:50:5c:03
    pwwn 20:00:00:e0:69:a1:b9:fc

zone name Zone2 vsan 1
    pwwn 10:00:00:e0:02:21:df:ef
    pwwn 20:00:00:e0:69:a1:b9:fc

zone name Zone3 vsan 1
    fwwn 20:42:00:05:30:00:63:9e
    fwwn 20:43:00:05:30:00:63:9e

zone name zone-cc vsan 2
    pwwn 50:06:0e:80:03:50:5c:01
    pwwn 20:00:00:e0:69:41:a0:12
    pwwn 20:00:00:e0:69:41:98:93
zone name Zone-cc vsan 2
    pwwn 50:00:00:20:37:6f:db:aa.
```

The output shows that the zone name was added incorrectly (names for both zones and zoneset are case sensitive), creating a new zone called Zone-cc instead of zone-cc. Therefore, the storage pwwn has been erroneously configured to belong to a zone in which that port is the only member. The pwwn of the storage subsystem disappears from the output of **show active zoneset** command, because Zone-cc is not be added to the active zoneset of VSAN2.

Other useful commands

Use the **show zone name** command to display members of a specific zone.

```
switch# show zone name Zone1
zone name Zone1 vsan 1
```

Use the **show fcalias** to show if and how aliases are configured.

```
switch# show fcalias vsan 1
fcalias name Alias2 vsan 1 pwwn 21:00:00:20:37:6f:db:dd
fcalias name Alias1 vsan 1 pwwn 21:00:00:20:37:9c:48:e5
```

Use the **show zone member** command to display all zones to which a member belongs using the FCID, the fcalias, or the pwwn.

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
VSAN: 1
zone Zone3
zone Zone1
fcalias Alias1
```

Use the **show zone statistics** command to display the number of control frames exchanged with other switches.

```
switch# show zone statistics
```

Send comments to mdsfeedback-doc@cisco.com.

```

Statistics For VSAN: 1
*****
Number of Merge Requests Sent: 24
Number of Merge Requests Recvd: 25
Number of Merge Accepts Sent: 25
Number of Merge Accepts Recvd: 25
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
Statistics For VSAN: 2
*****
Number of Merge Requests Sent: 4
Number of Merge Requests Recvd: 4
Number of Merge Accepts Sent: 4
Number of Merge Accepts Recvd: 4
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0

```

The **show zone internal vsan** command shows the internal state of the zone server for a specific VSAN.

```

switch# sh zone internal vsan 1
VSAN: 1 default-zone: deny distribute: active only
      E_D_TOV: 2000 R_A_TOV: 10000 F_S_TOV: 5000 Interop: Off
      DBLock:-(F count:0) Ifindex Table Size:2
Full Zoning Database :
      Zonesets:6 Zones:6 Aliases:0
Active Zoning Database :
      Name: ZoneSet6 Zonesets:1 Zones:1 Aliases:0
TCAM Info :
      cur_seq_num : 9, state : 0
      add_reqs = 4, del_reqs = 0, entries_added = 0
Change protocol info :
      local domain id = 102, ACA by 0xff
      State = Idle, reply_cnt = 0, req_pending = 0
      Remote domains :
Merge proto info :
      i/f fc2/15 | State = Isolated | notify = 0x8 | - -

```

Using the GUI to Troubleshoot Zoning Configuration Issues

Much of the information accessible through CLI commands can be accessed and summarized using the Fabric Manager VSAN/Zone view. For example, to check which devices belong to the active zoneset on a specific VSAN, click on the folder representing the active zoneset. This will display the set of devices belonging to that zoneset in that particular VSAN.

Similarly, by expanding the active zoneset folder content (clicking on the '+' next to the folder) the members of the active zoneset (the active zones) will be displayed as new folders.

Send comments to mdsfeedback-doc@cisco.com.

By recursively expanding the zone folders, the devices belonging to that zone will be listed in the left side column of the Fabric Manager window, and they will be highlighted in the topology view on the right side of the Fabric Manager window.

Troubleshooting VSANs

If VSANs are not configured properly, host devices will not be allowed to see storage devices configured to belong to different VSANs.

Hosts and storage ports must belong to the same VSAN, and VSANs cannot overlap.

VSAN membership for a specific port can be verified using the following command:

```
switch# show vsan membership interface fc2/1
fc2/1
      vsan:3
```

The output above shows interface fc2/1 is in VSAN 3.

To troubleshoot VSAN membership problems, issue the same command for both the port connected to the servers and the ones connecting the storage subsystem to the fabric. Then, verify that the VSAN is the same for both.

A more general command to verify the VSAN membership of all the ports on switch is:

```
switch# show vsan membership
vsan 1 interfaces:
      fc2/7   fc2/8   fc2/9   fc2/10  fc2/11  fc2/12  fc2/13  fc2/14
      fc2/15  fc2/16  fc7/1   fc7/2   fc7/3   fc7/4   fc7/5   fc7/6
      fc7/7   fc7/8   fc7/9   fc7/10  fc7/11  fc7/12  fc7/13  fc7/14
      fc7/15  fc7/16  fc7/17  fc7/18  fc7/19  fc7/20  fc7/21  fc7/22
      fc7/25  fc7/26  fc7/27  fc7/28  fc7/29  fc7/30  fc7/31  fc7/32

vsan 2 interfaces:
      fc2/6   fc7/23  fc7/24

vsan 3 interfaces:
      fc2/1   fc2/2   fc2/5

vsan 4 interfaces:
      fc2/3   fc2/4
```

If the devices are on different switches, issue the **show vsan membership** command on both devices. Then, verify that the trunks connecting the end switches are configured to transport the VSAN in question. This is done by issuing the **show interface** command, to verify that the port is in trunk mode and that the VSAN in question belongs to the trunk VSAN. Refer to the example below. If this is not the case, refer to the Troubleshooting ISL Isolation section at the beginning of this chapter to determine how to troubleshoot the connectivity issue.

```
switch# sh int fc2/14
fc2/14 is trunking
      Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
      Port mode is TE
      Speed is 2 Gbps
      vsan is 2
      Beacon is turned off
      Trunk vsans (allowed active) (1-3,5)
      Trunk vsans (operational)   (1-3,5)
      Trunk vsans (up)           (2-3,5)
      Trunk vsans (isolated)     (1)
      Trunk vsans (initializing) ()
      475 frames input, 8982 bytes, 0 discards
```

Send comments to mdsfeedback-doc@cisco.com.

```
0 runts, 0 jabber, 0 too long, 0 too short
0 input errors, 0 CRC, 3 invalid transmission words
0 address id, 0 delimiter
0 EOF abort, 0 fragmented, 0 unknown class
514 frames output, 7509 bytes, 16777216 discards
Received 30 OLS, 21 LRR, 18 NOS, 53 loop inits
Transmitted 68 OLS, 25 LRR, 28 NOS, 32 loop inits
```

Using the GUI to Troubleshoot VSAN Membership Problems

Checking the VSAN membership can also be done using the Device Manager.

Another tool that may be used to verify different categories of problems (VSANs, zoning, fcdomain, admin issues, or other switch-specific or fabric-specific issues) is the Fabric Analysis tool provided by Fabric Manager.

The possible configuration consistency check tool is also provided by this application. Refer to the *Cisco MDS 9000 Fabric Manager User Guide* for further information about this tool.