

---

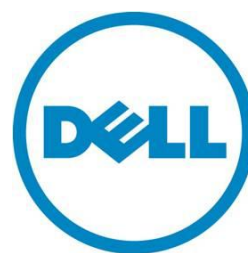
# Deploying FCoE (FIP Snooping) on Dell PowerConnect 10G Switches: M8024-k, 8024 and 8024F

---

**A Dell Deployment Guide**

## Authors

Network Enabled Solutions Team,  
Kevin Locklear



## Contributor

Kili Land

**This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.**

© 2011 - 2012 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, PowerConnect and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

March 2012 | Rev 2.0

## Contents

Introduction .....	6
Basic Terminology .....	6
FIP snooping .....	6
FIP snooping bridge (FSB) .....	6
FCF .....	6
PFC .....	7
NPIV .....	7
NPV .....	7
VSAN.....	7
Configuration scenarios.....	8
Important notes prior to deployment .....	9
Scenario 1: Deploying the Dell PowerConnect 8024 Series FSB in a Cisco 5000 Series Switch (NPIV) environment .....	10
Configuring the Dell PowerConnect M8024-k,8024, and 8024F for FIP Snooping .....	13
Configuring the Cisco 5000 series switch with firmware ver 5.x for a single connection from the Dell PowerConnect M8024-k or 8024()(F).....	17
Basic Validation for the PowerConnect M8024-k configuration.....	23
Basic Troubleshooting Areas .....	28
Scenario 2: Configuring Multiple Uplinks into LAG for Cisco Nexus 5000 Series Switch (NPIV) Environment .....	30
Configuring the Cisco Nexus 5000 series switch with firmware ver 5.x for a multiple link LAG (link aggregation) connection at the Top-of-Rack.....	31
Configuring the M8024-k,8024, and 8024F for FIP Snooping .....	33
Scenario 3: Configuring Multiple Uplinks into LAG for Cisco Nexus 5000 Series Switch (NPV mode) Environment .....	35
Configuring the Cisco Nexus 5000 series switch with firmware ver 5.0(3)N2(2a) in NPV mode for a multiple link LAG (link aggregation) connection from the Dell PowerConnect M8024-k or 8024()(F) .....	36
Configuring the Dell PowerConnect M8024-k,8024,and 8024F for FIP Snooping with Cisco Nexus 5000 series switch in NPV mode.....	37
ETS Behavior and CoS configurations on the PowerConnect 8024 series switches .....	37
Updating firmware .....	39
Command-line interface method .....	39
Web interface method .....	41
Appendix A - Full CLI examples .....	45
M8024-k CLI example.....	45

Cisco Nexus 5548UP CLI example .....	52
Appendix B - Network Switch Versions.....	56
References .....	56
About Dell.....	56

## Figures

Figure 1. Dell PowerConnect™ M8024-k Switch (10G Ethernet) .....	6
Figure 2. Dell PowerConnect™ 8024F (10G Ethernet).....	6
Figure 3. General overview of deployment.....	8
Figure 4. Disabling simple mode .....	9
Figure 5. Simple 1-link connection between devices .....	10
Figure 6. General Overview of the whole configuration and planning procedure .....	11
Figure 7. Overview of parallel configuration.....	12
Figure 8. Example commands for Dell PowerConnect M8024-k (can be copied and pasted) .....	13
Figure 9. Configuration overview of Dell PowerConnect M8024-k.....	16
Figure 10. Sample CLI for Cisco Nexus 5020 (can be copied and pasted) .....	17
Figure 11. Sample CLI for Cisco Nexus 5548 (can be copied and pasted) .....	18
Figure 12. Cisco Nexus 5000 series configuration sequence .....	20
Figure 13. M1000e Chassis Management Controller -> Server Overview -> Properties -> WWN/MAC information for Blade Server 3's "B" fabric CNA port 2 (B2). .....	21
Figure 14. Example of show interface brief command .....	22
Figure 15. show spanning-tree summary command showing current configuration with ports states .	23
Figure 16. show flogi database command showing devices that have completed fabric login .....	23
Figure 17. Example of show zoneset active command.....	23
Figure 18. Show interface status results .....	24
Figure 19. show spanning-tree blockedports command .....	25
Figure 20. Show fip-snooping command which gives a brief status on available ENode's, and FCF's..	25
Figure 21. show lldp dcbx interface all.....	26
Figure 22. Show lldp dcbx interface te1/0/20 detail .....	27
Figure 23. Multiple port link (LAG) configuration between switches and storage .....	30
Figure 24. Multiple port link (LAG) Cisco 5020 configuration (can be copied and pasted) .....	31
Figure 25. Multiple port uplink (LAG) M8024-k configuration (can be copied and pasted).....	33
Figure 26. Multiple link configuration between switches and storage .....	35
Figure 27. Multiple port link Cisco 5020 configuration (can be copied and pasted).....	36
Figure 28. CoS settings to establish minimum bandwidth for FCoE queue .....	37
Figure 29. Fabric separation as preferred method for management of networks and storage .....	38



## Introduction

The PowerConnect™ M8024-k, 8024 and 8024F switches are now DCB/DCBx capable with a downloadable update. **Starting with firmware 4.2**, the latest PowerConnect™ 10 Gigabit switches can now be used as an FCoE Transit Switch (FIP Snooping Bridge, T11, BB-5). With this new firmware implementation Converged Network Adapters (CNAs) can be used in the rack-mount or blade server to enable access to Fibre Channel networks and their storage.

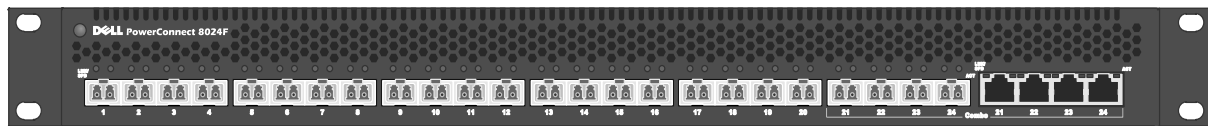
- NOTE: The PowerConnect™ M8024 (predecessor to the M8024-k) does not support the FIP Snooping capability and will not be supported for any of the described scenarios.

This document provides an easy to use guide for configuring FIP Snooping on the Dell PowerConnect™ [M8024-k Blade Switch](#) (Figure 1), and the [PowerConnect™ 8024F](#) (Figure 2).

Figure 1. Dell PowerConnect™ M8024-k Switch (10G Ethernet)



Figure 2. Dell PowerConnect™ 8024F (10G Ethernet)



## Basic Terminology

### FIP snooping

With FIP snooping enabled on the PowerConnect™ 8024 model switches, FIP logins, solicitations, and advertisements are monitored. In this monitoring or snooping process the switch gathers information pertaining to the ENode and FCF addresses. With this information the switch will then place filters that only allow access to ENode devices that have logged-in successfully. This enables the FCoE VLAN to deny all other traffic except this lossless FCoE storage traffic.

The filtering process also secures the end-to-end path between the ENode device and the FCF. The ENode will only be able to talk with the FCF in which it has logged into.

### FIP snooping bridge (FSB)

With a switch configured to performing FIP snooping the industry term for this switch is FSB or FIP snooping bridge. It is performing FIP snooping as described in the previous term.

### FCF

FCoE forwarders (FCFs) act as an Ethernet and FC switch combined. All typical termination functions that would occur on a FC switch occur on the FCF. FCF's give VF\_Ports and VE\_Ports for their virtual FC interfaces.

## PFC

Priority Flow Control (PFC), or Per-Priority Pause is defined in the IEEE 802.1Qbb standard. PFC is flow control based on priority settings and adds additional information to the standard pause frame. The additional fields added to the pause frame allow devices to pause traffic on a specific priority instead of pausing all traffic. (IEEE, 2009) Pause frames will be initiated by the FCF in most cases when its receive buffers are starting to reach a congested point. With PFC traffic is paused instead of dropped and retransmitted. This provides the lossless network behavior necessary for FC packets to be encapsulated and passed along the Ethernet paths.

## NPIV

N-port identifier virtualization which enables multiple N-port fabric logins at the same time on the same physical FC link (Cisco Systems, Inc., 2011). This term is in reference to the Cisco Nexus 5000 series switches implementation of NPIV.


## NPV

N-port virtualizer is a FC aggregation method which passes traffic through to end devices, while eliminating the need to use a domain ID for this device (Cisco Systems, Inc., 2011). This term is also in reference to configuration settings on the Cisco Nexus 5000 series switches.

## VSAN

Virtual SAN is a logical partitioning of physical connections to provide for fabric or SAN separation.

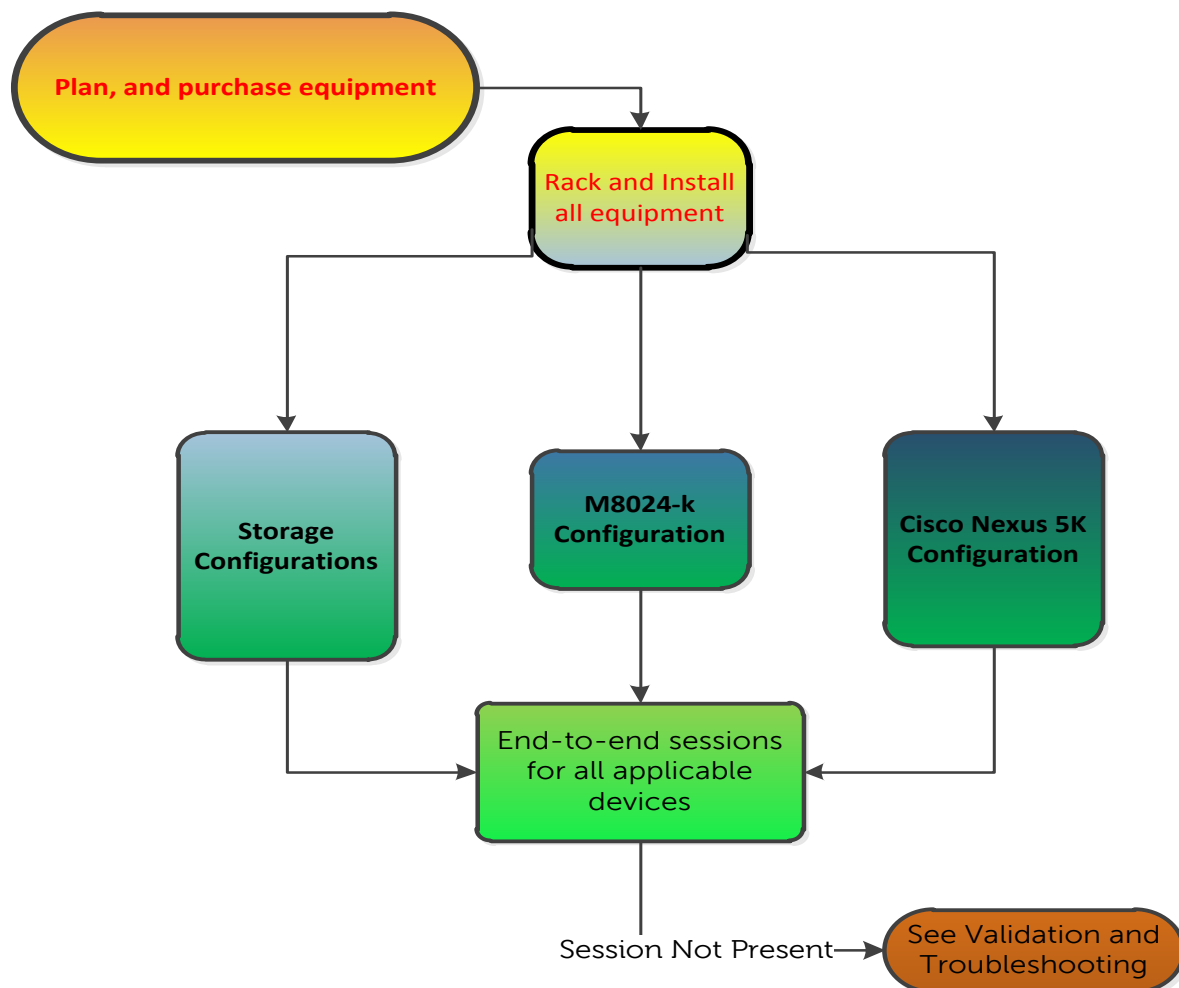
---

 Note: The Dell M1000e Server Chassis includes a console redirect feature that allows you to manage each PowerConnect M8024-k module from a single serial connection to the chassis. For more information about console redirect, see the Dell Blade Server CMC User's Guide at <http://support.dell.com/support/edocs/software/smdrac3/cmc/index.htm>.

## Configuration scenarios

The following sections will present very basic examples of deploying the 10G switches for FIP Snooping and will provide step-by-step explanations of the CLI commands as a guide. The GUI does not currently support configurations for FIP Snooping. Consult the table of contents above for a list of examples covered in this document.

Figure 3. General overview of deployment



The following suggested configurations used to deploy this solution is done in a sequential order for reading but as Figure 3 represents this is more of a simultaneous process. There are dependencies that will be occurring during the configuration that will rely on other parts of the process. Storage configuration is not covered in any depth due to the possibility for various supported storage devices as part of the whole solution.



## Important notes prior to deployment



### No Simple Mode

Each of the following scenarios in this document assume that the PowerConnect™ 8024 model switch being used is in **normal Switch Mode (not Simple Mode)** and is using firmware version 4.2.x.x or later.

- ☑ **NOTE:** If Simple Mode is enabled it will need to be disabled prior to implementing the deployment covered in this document. FCoE is not supported with the PowerConnect 8024 model switches in Simple Mode. The CLI command in the example may be used for disabling Simple Mode, but please consult the User Guide for more information on specifics of Simple Mode.

Figure 4. Disabling simple mode

```
configure
no mode simple
```



### Non-FIP-aware switches

If a Non-FIP-Aware switch is introduced anywhere in the data path FCoE will not be supported and can't be expected to work as designed. The Dell PowerConnect M8024-k and 8024F are considered non-FIP-aware switches until they have the 4.2 or greater firmware installed. See [updating firmware](#) section for instructions on performing this update.



### Stacking

Stacking is not recommended in an FCoE environment with the Dell PowerConnect 8024 Model Switches. If the switches are stacked the configuration should be changed to disable stacking. Please refer to the Dell PowerConnect 8024 4.2 firmware user's guide for further details on disabling or changing stacking ports. If the configuration is used in this manner lossless Ethernet and reliability can not be guaranteed.



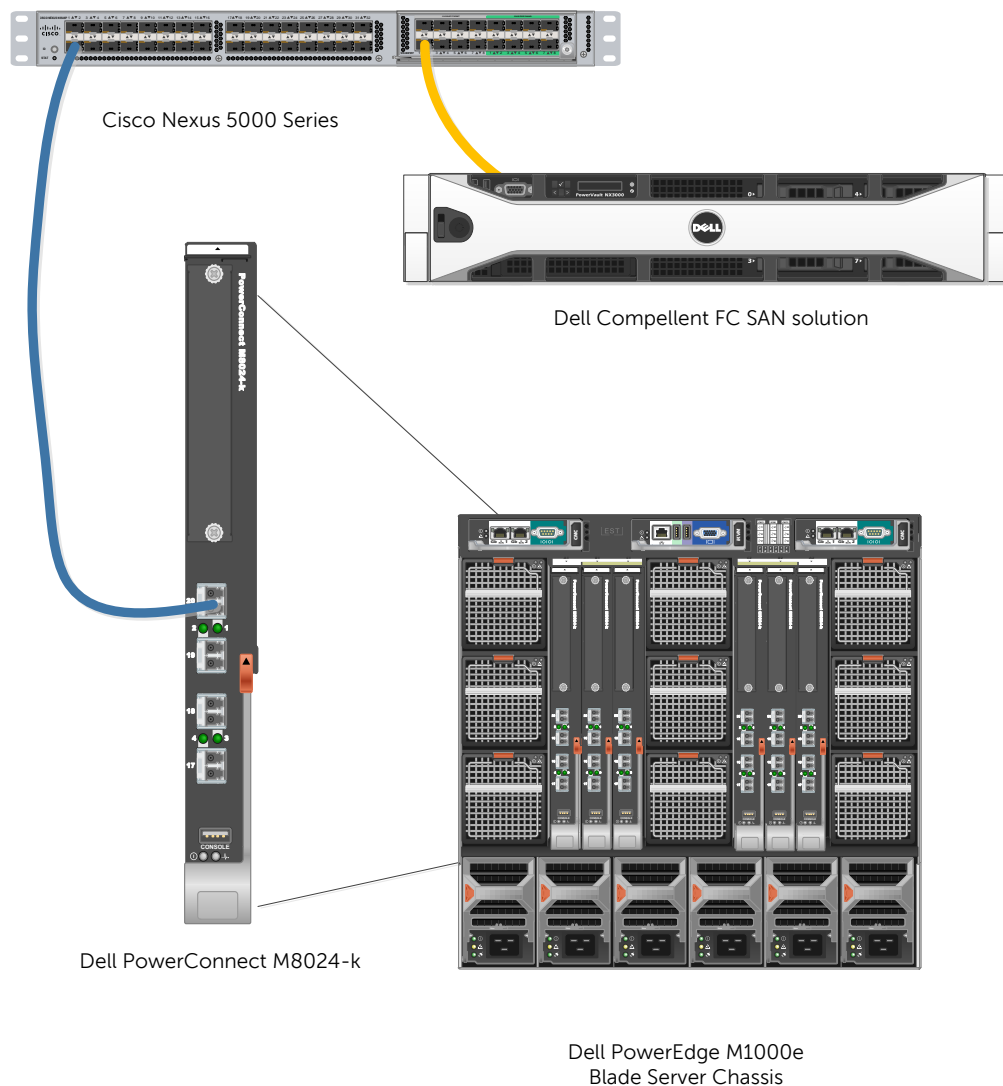
### Dell PowerConnect 4.2 or greater firmware on M8024-k or 8024F

As mentioned in the non-FIP-aware bullet the Dell PowerConnect Switches will not support FCoE or FIP snooping without 4.2 or greater firmware. See [updating firmware](#) section to perform this update.

## Scenario 1: Deploying the Dell PowerConnect 8024 Series FSB in a Cisco 5000 Series Switch (NPIV) environment

This first example is a basic, single connection between devices example using the Dell PowerConnect M8024-k. This configuration is being shown for the purposes of simplification and potentially easing into the progression of a more in-depth setup. It is also easier to use a simple configuration such as this setup to aid in troubleshooting of the initial install. In a typical business environment most configurations will be scaled to include several connections between servers and storage. The scenarios following this one will show some of these larger configurations. Note that this configuration will also work in the rack server environment with Dell PowerConnect 8024F switch

Figure 5. Simple 1-link connection between devices



The flowchart in Figure 8 is a general overview of how the deployment will occur. This includes the basic planning that will need to take place in order for most of the steps in the rest of the document to fall into place.

Figure 6. General Overview of the whole configuration and planning procedure

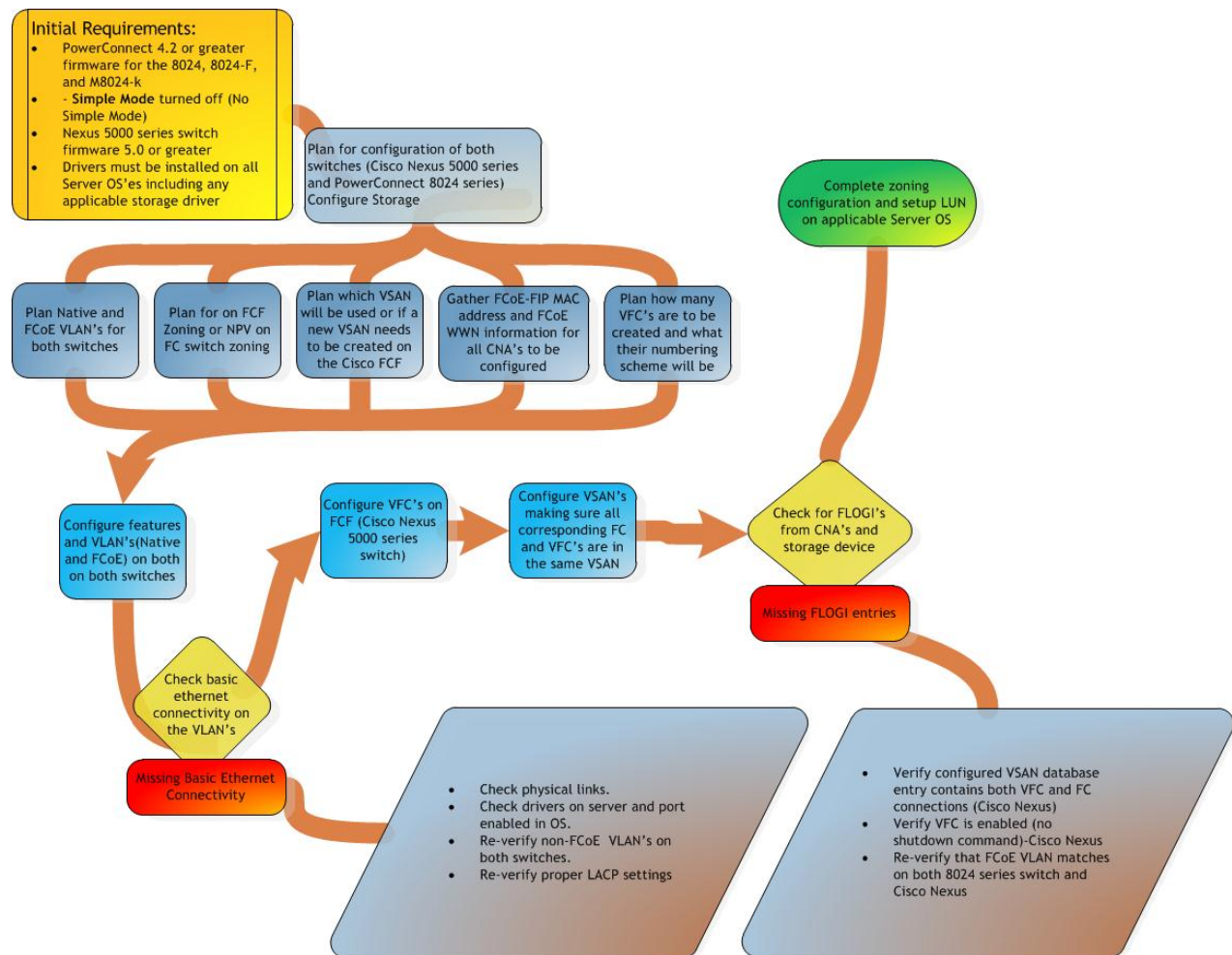
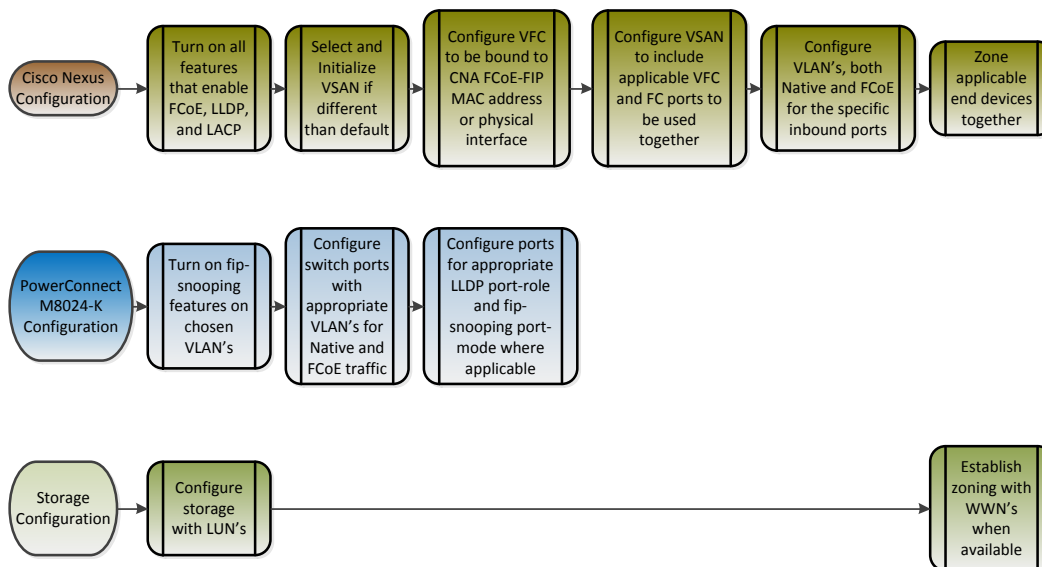


Figure 9 is a graphical representation of how many of the configuration pieces are considered parallel settings. Most of the configuration will depend heavily on configurations being completed in more than just one place.

Figure 7. Overview of parallel configuration



In many of the business environments where this configuration will be installed there will be different administrators for the different areas of the infrastructure. In other words there may be a LAN infrastructure administrator, a storage or SAN administrator, and potentially a server administrator. These different team members will have to work together for a successful deployment of all the involved parts. In an M1000e bladeserver environment it may be the server admin that deploys the blade servers, operating systems, network adapter drivers, and very possibly configures the blade IOM networking switches. If different admins are involved as described these tasks can be done in parallel to enable a quicker deployment.

It is important to understand certain checks or validations along the way may rely on configurations being completed in a different part of the infrastructure.

## Configuring the Dell PowerConnect M8024-k, 8024, and 8024F for FIP Snooping

The Dell PowerConnect 8024 model switches will monitor FIP packets and will establish the proper filtering, and priorities for the FCoE traffic that is passed through the configured links. To see an example of the full configuration see [Appendix-A](#) - M8024-K Example.

### Command-Line Interface Method

Figure 8. Example commands for Dell PowerConnect M8024-k (can be copied and pasted)

```
configure
no mode simple
vlan database
vlan 20,1000
exit
hostname "mySwitch"
vlan database
vlan 20,1000
exit
feature fip-snooping
vlan 20,1000
fip-snooping enable
exit
interface out-of-band
ip address 192.168.10.1 255.255.255.0 192.168.10.254
exit
classofservice dot1p-mapping 1 1
classofservice dot1p-mapping 2 2
classofservice dot1p-mapping 3 3
classofservice dot1p-mapping 4 4
classofservice dot1p-mapping 5 5
classofservice dot1p-mapping 6 6
exit

interface Te1/0/1
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
switchport mode general
lldp dcbx port-role auto-down
spanning-tree portfast
exit

interface Te1/0/20
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
spanning-tree cost 0
spanning-tree port-priority 0
switchport mode general lldp dcbx port-role auto-up
fip-snooping port-mode fcf
exit
```

- ⚠ **CAUTION:** The “copy running-configuration startup-configuration” command should be issued after several impacting steps so that the switch will retain the configuration settings put into place on the next boot.
- ⚠ Routed VLAN’s can’t have FIP-snooping enabled. VLAN 1 may be set for routing and this must be changed in the VLAN database if it is going to be used as the native VLAN or PVID.

### Step by Step explanation of CLI example

- **Configure** - this brings the prompt into the configuration interface
  - **no mode simple** - puts switch into normal mode
  - **vlan database** - moves down into the VLAN database interface
    - **vlan 20** - add VLAN 20 to used for untagged traffic or as the native VLAN
    - **vlan 1000** - add VLAN 1000 to the VLAN database, this will be the FCoE VLAN
    - **exit** - exit the current level of the interface configuration
  - **hostname "mySwitch"** - set the hostname of the switch in this example "mySwitch"
  - **feature fip-snooping** - this turns on the fip-snooping capability of the switch
  - **vlan 20,1000** - this moves the interface into vlan 20,1000
    - **fip-snooping enable** - this enables the fip-snooping capabilities on these particular VLAN's. Both must be included for the initial TLV negotiation to establish the FCoE VLAN
    - **exit** - exit interface configuration
  - **interface out-of-band** - move into the interface out-of-band configuration interface
    - **ip address 192.168.100.1 255.255.255.0 192.168.100.254** - this sets the out-of-band management interface IP address, subnet, and gateway for the switch
    - **exit** - exit the interface configuration
  - **classofservice dot1p-mapping x x** - establishes direct CoS mapping for the priorities (must be in place for certain CNA's)
  - **interface te1/0/1** - this moves into the interface te1/0/1 configuration
    - **switchport general pvid 20** - establishes the native VLAN as 20, you must remove VLAN 1 in order for this to function correctly
    - **switchport general allowed vlan add 20** - adds VLAN 20 the trunk as an untagged VLAN
    - **switchport general allowed vlan add 1000 tagged** - this sets up a trunk with a tagged VLAN of 1000 (the FCoE VLAN), and includes the native VLAN as untagged if general mode is enabled.
    - **switchport general allowed remove vlan 1** - this removes vlan 1 which would typically be the native vlan otherwise.
    - **switchport mode general** - this enables the port for general mode
    - **lldp dcbx port-role auto-down** - sets the DCBx port-role to be auto-down for an ENode connection
    - **spanning-tree portfast** - sets the ports to a portfast behavior since these are internal-facing server ports.
    - **exit** - exits the interface configuration

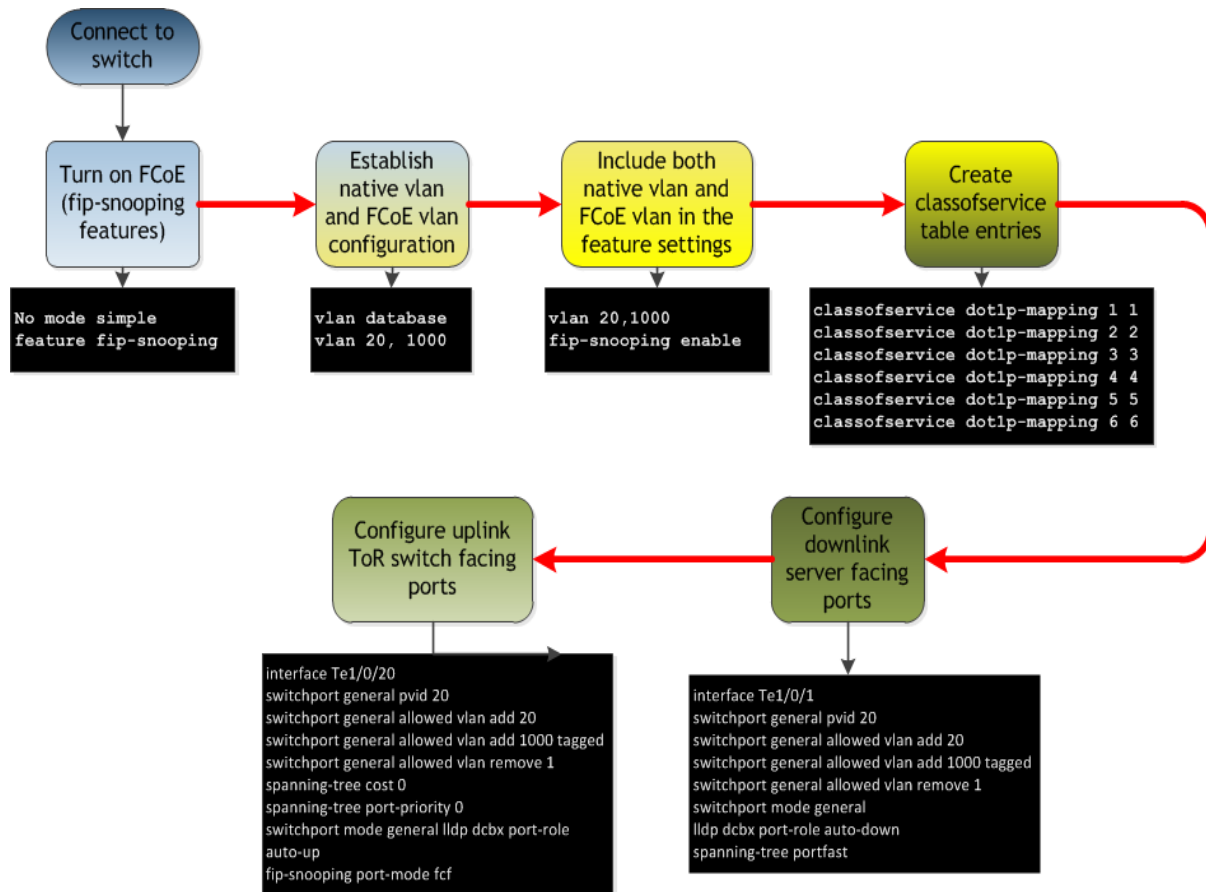
- **interface te1/0/20** - this moves into the interface te1/0/20 configuration
  - **switchport general pvid 20** - establishes the native VLAN as 20, you must remove VLAN 1 in order for this to function correctly
  - **switchport general allowed vlan add 20** - adds VLAN 20 the trunk as an untagged VLAN
  - **switchport general allowed vlan add 1000 tagged** - - this sets up a trunk with a tagged VLAN of 1000 (the FCoE VLAN), and includes the native VLAN as untagged if general mode is enabled.
  - **switchport general allowed remove vlan 1** - this removes vlan 1 which would typically be the native vlan otherwise.
  - **switchport mode general** - this enables the port for mode general
  - **spanning-tree cost 0** - sets spanning tree cost to 0
  - **spanning-tree port-priority 0** - sets this ports priority to 0 so that it has the lowest spanning tree priority in case a loop is created elsewhere on the switch
  - **lldp dcbx port-role auto-up** - sets the DCBx port-role to be auto-up which dynamically sets the configuration-source for an FCF connection
  - **fip-snooping port-mode fcf** - enables the port for fip-snooping from an FCF connection
  - **exit** - exits the interface configuration
  - **exit** - exits from configuration mode

✍ **Critical steps:** The “copy running-configuration startup-configuration” command should be issued after important steps so that the switch will retain the configuration settings when the switch is next rebooted or if a power loss occurs. It is also a good practice to copy a well-validated working configuration to a separate location such as the management station for the networks, and have a backup-configuration saved local to the switch.

#### Further explanation of [key points](#):

- The spanning-tree settings in this example are established to keep the port from being potentially blocked by spanning-tree. This could occur because another cable is plugged into a port with a lower priority, causing a loop. When the uplink port is set to 0 it will have the lowest priority and therefore most likely not end up in a blocked state.
- A second key setting to note is “switchport general allowed vlan remove 1”. This command must be entered if you are choosing to use a different PVID or native VLAN. A port cannot have two native VLANs. In this example the configuration is set to use VLAN 20 since typically the recommendation is to have regular untagged traffic on a different VLAN other than just 1 for segregation of the network. In addition when the FCF sends information to the fip-snooping bridge (FSB) or M8024-k in this case, the M8024-k is receiving the initial information for negotiation on its untagged vlan (vlan 20 in this case). Once the initial negotiations have occurred properly the FCoE traffic will traverse the FCoE VLAN (in this case VLAN 1000).
- The last configuration line “fip-snooping port-mode fcf” is also key to this configuration. This line establishes where the FCF is attached to the switch. With this setting the port is configured to make Fibre Channel aware of the connection via this port to the forwarder. The previous line “lldp dcbx port-role auto-up“, is setting this port to be aware of DCBx TLV's, the difference being the fip-snooping configuration line points to the port for using fip-snooping to the FCF, and the lldp configuration points to the point for doing DCBx negotiations.

Figure 9. Configuration overview of Dell PowerConnect M8024-k





## Configuring the Cisco 5000 series switch with firmware ver 5.x for a single connection from the Dell PowerConnect M8024-k or 8024()(F)

The CLI commands below are necessary for an un-configured Cisco 5020. The CLI will show additional lines that are either default or can't be changed and are not added for this example. The CLI will also show the lines in a different order after they have been entered. [Appendix-A Cisco Nexus 5548UP CLI example](#) will have a copy of the full configuration for a 5548UP for reference.

### Command-Line Interface Method

Figure 10. Sample CLI for Cisco Nexus 5020 (can be copied and pasted)

```
feature fcoe
feature npiv
feature telnet
feature lacp
feature lldp

system default switchport trunk mode auto

vlan 20
vlan 1000
    fcoe vsan 2

vsan database
    vsan 2
    vsan 2 interface vfc1
    vsan 2 interface fc2/1

interface vfc1
    bind interface Ethernet1/1
    no shutdown

interface fc2/1
    switchport trunk mode auto
    no shutdown

interface Ethernet1/1
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000

zone name blad1 vsan 2
    member interface fc2/1
    member pwnn xx:xx:xx:xx:xx:xx:xx:xx

zoneset name set1 vsan 2
    member blad1

zoneset activate name set1 vsan 2
```

The following CLI commands are necessary for an un-configured Cisco Nexus 5548UP or Cisco Nexus 5596. The full CLI will show additional lines that are either default or can't be changed and are not added for this example. The CLI will also show the lines in a different order after they have been entered. [Appendix-A Cisco Nexus 5548UP CLI example](#) will have a copy of the full configuration.

## Command-Line Interface Method

Figure 11. Sample CLI for Cisco Nexus 5548 (can be copied and pasted)

```
feature fcoe
feature npiv
feature telnet
feature lacp

system default switchport trunk mode auto

system qos
  service-policy type qos input fcoe-default-in-policy
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type network-qos fcoe-default-nq-policy

vlan 20
vlan 1000
  fcoe vsan 2

vsan database
  vsan 2
  vsan 2 interface vfc1
  vsan 2 interface fc2/1

interface vfc1
  bind interface Ethernet1/1
  no shutdown


interface fc2/1
  switchport trunk mode auto
  no shutdown

interface Ethernet1/1
  switchport mode trunk
  switchport trunk native vlan 20
  switchport trunk allowed vlan 1000

zone name blad1 vsan 2
  member interface fc2/1
  member pwnn xx:xx:xx:xx:xx:xx:xx:xx

zoneset name set1 vsan 2
  member blad1

zoneset activate name set1 vsan 2
```

-  Note that the provided Cisco commands should be referenced in the *Nexus 5000 Series NX-OS SAN Switching Configuration Guide*. The CLI entries above only cover the areas that must be added to enable FCoE capabilities on the particular ports being used of a Cisco Nexus 5020 and Nexus 5548. This topic will be covered after the Step by Step explanation of the CLI example.

## Step by Step explanation of the CLI example

- **Configure** - this brings you into the configuration interface.
  - **feature FCOE** - enables the feature for FCOE as long as the licensing and FC modules are installed.
  - **feature NPIV** - enables the FC ports to accept multiple logins (Necessary for Compellent).
  - **feature LACP** - enables the switch to be able to use port-channel groups in a LACP mode.
  - **feature LLDP** - enables the switch to use LLDP which is needed for DCBx negotiations. Some switch versions will have this on by default and the entry will not be needed.
  - **system qos**
    - **service-policy type qos input fcoe-default-in-policy**
    - service-policy type queuing input fcoe-default-in-policy**
    - service-policy type queuing output fcoe-default-out-policy**
    - service-policy type network-qos fcoe-default-nq-policy**
    - these are qos settings that are in place by default on the 5010 and 5020 Cisco Nexus switches. These settings will have to be input for the 5548 and 5596 Cisco Nexus switches.
  - **system default switchport trunk mode auto** - sets trunk mode to auto for FC ports; optionally this can be set to off, or on if needed.
  - **vlan 20** - this is the VLAN to be used for the Native VLAN.
  - **vlan 1000** - this is the VLAN being used for FCoE in this example
    - **fcoe vsan 2** - this establishes the previous VLAN 1000 as an FCoE VLAN in VSAN 2.
  - **vsan database** - enter into the vsan database interface.
    - **vsan 2** - initializes VSAN 2
    - **vsan 2 interface vfc1** - set interface vfc1 to be part of VSAN 2
    - **vsan 2 interface fc2/1** - set interface fc2/1 to be part of VSAN 2
  - **interface vfc1** - selects virtual fc interface vfc1 (vfc1 is an example and can be a different number based on the admin's choice at configuration time).
    - **Bind interface Ethernet1/1** - this binds interface Ethernet 1/1 to the virtual fc interface which in this case is vfc1. This is one form of binding the VFC. The other form would be to bind the VFC to the FCoE FIP MAC address of the CNA being used. Examples of this will be included later in the document.
    - **no shutdown** - turns the virtual interface on since default is shutdown.
  - **Interface fc2/1** - selects the fc2/1 interface (which will typically be the first fibre channel port on the Nexus 5020).
    - **no shutdown** - turns the fc2/1 interface on since default is shutdown.
  - **interface Ethernet 1/1** - selects interface Ethernet 1/1
    - **switchport mode trunk** - set switchport mode to trunk for the 2 VLAN's.
    - **switchport trunk allowed vlan 1000** - add allowed VLAN 1000 to the trunk.

- **Zone name blade1 vsan 2** - this will set the name for your zone (blade1 can be any chosen name); vsan 2 will match the vsan you have created.
  - **Member interface fc2/1** - this adds the fc2/1 interface as a member of the zone.
  - **member pwwn xx:xx:xx:xx:xx:xx:xx:xx** - adds the port WWN of the ENode device to the zone. (insert the port WWN of the device being used).
- **zoneset name set1 vsan 2** - move into the zoneset interface (in this case the name is set1 but could be any name and the VSAN number is based on the FCoE VLAN being used).
  - **member blade1** - this includes the blade1 zone into this zoneset.
- **zoneset activate name set1 vsan 2** - activates the zoneset containing these zones.

#### Further explanation of [key points](#):

- In order for devices to communicate end-to-end they must participate in the same VSAN. In this sample configuration the VFC is bound to either the FCoE FIP MAC Address of the Converged Network Adapter in the blade server or an actual interface that would be a connection from the modular switch (in this case M8024-K) connecting the blade servers. The recommended configuration for this is to bind to the FCoE FIP MAC address of the CNA.

However, as an easy setup step it is possible to bind a VFC to the physical interface or port-channel in order to determine which FCoE FIP MAC addresses will present from the CNA's. These can be noted and then matched with the M1000e's CMC -> Server Overview -> WWN/MAC Summary that can be seen in Figure 15 on the next page. This is applicable only to the M8024-k modular switch with blade servers. For the rack-mounted 8024 switches the CNA's would need to be verified on the servers themselves. This verification can be done through each adapters driver properties in the different operating systems.

Figure 12. Cisco Nexus 5000 series configuration sequence

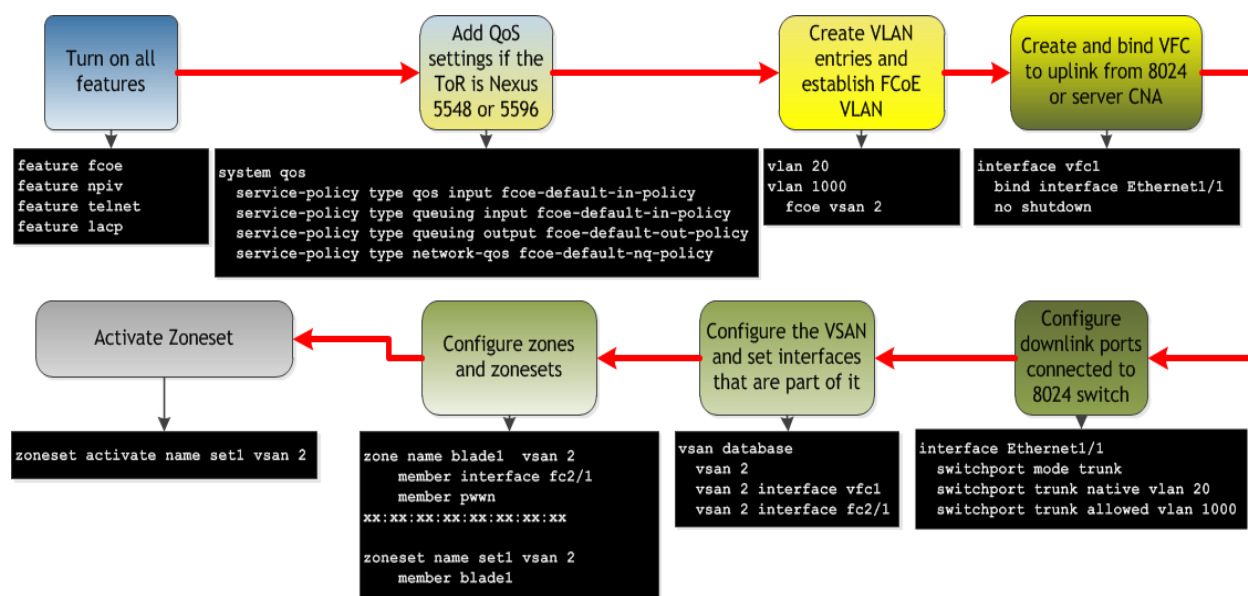


Figure 13. M1000e Chassis Management Controller -> Server Overview -> Properties -> WWN/MAC information for Blade Server 3's "B" fabric CNA port 2 (B2).

The screenshot shows the Dell Chassis Management Controller (CMC) interface. The left sidebar contains navigation options: Chassis Overview, Chassis Controller, Server Overview, and IO Module Overview. The main area displays the WWN/MAC Summary for Blade Server 3. The table lists network interfaces for various slots (A2, B1, C1, C2) and their corresponding WWN and MAC addresses. Annotations highlight the B2 port and its associated MAC address.

Slot	Interface	WWN	MAC
A2	10 GbE KR	00:10:18:A7:FA:B2	✓ 14:FE:B5:8E:5B:E2
	ISCSI	00:10:18:A7:FA:B3	✓ 14:FE:B5:8E:5B:E1
	FCoE-FIP	00:10:18:A7:FA:B3	✓ 14:FE:B5:8E:5B:E2
	FCoE-WWN	20:01:00:10:18:A7:FA:B3	✓ 20:01:14:FE:B5:8E:5B:E2
	10 GbE KR	00:10:18:A7:FA:B6	✓ 14:FE:B5:8E:5B:E6
	ISCSI	00:10:18:A7:FA:B7	✓ 14:FE:B5:8E:5B:E7
	FCoE-FIP	00:10:18:A7:FA:B7	✓ 14:FE:B5:8E:5B:E8
	FCoE-WWN	20:01:00:10:18:A7:FA:B7	✓ 20:01:14:FE:B5:8E:5B:E8
	10 GbE KR	00:10:18:A7:FA:BA	✓ 14:FE:B5:8E:5B:1C
	ISCSI	00:10:18:A7:FA:BB	✓ 14:FE:B5:8E:5B:1D
B1	FCoE-FIP	00:10:18:A7:FA:BB	✓ 14:FE:B5:8E:5B:1E
	FCoE-WWN	20:01:00:10:18:A7:FA:BB	✓ 20:01:14:FE:B5:8E:5B:1E
	10 GbE KR	00:10:18:A7:FA:BE	✓ 14:FE:B5:8E:5B:22
	ISCSI	00:10:18:A7:FA:BF	✓ 14:FE:B5:8E:5B:23
	FCoE-FIP	00:10:18:A7:FA:BF	✓ 14:FE:B5:8E:5B:24
	FCoE-WWN	20:01:00:10:18:A7:FA:BF	✓ 20:01:14:FE:B5:8E:5B:24
	10 GbE XAUI KR	00:1B:21:C0:4A:A4	✓ 14:FE:B5:8E:5B:EF
	FCoE-FIP	00:1B:21:C0:4A:A5	✓ 14:FE:B5:8E:5B:F0
	FCoE-WWN	20:01:00:1B:21:C0:4A:A5	✓ 20:01:14:FE:B5:8E:5B:F0
	B2	10 GbE XAUI KR	00:1B:21:C0:4A:A6
FCoE-FIP		00:1B:21:C0:4A:A7	✓ 14:FE:B5:8E:5B:F2
FCoE-WWN		20:01:00:1B:21:C0:4A:A7	✓ 20:01:14:FE:B5:8E:5B:F2
10 GbE KR		Not Installed	14:FE:B5:8E:5B:F3
C1	10 GbE KR	Not Installed	14:FE:B5:8E:5B:F4
	10 GbE KR	Not Installed	14:FE:B5:8E:5B:F5
C2	10 GbE KR	Not Installed	14:FE:B5:8E:5B:F6
	10 GbE KR	Not Installed	14:FE:B5:8E:5B:F6

Annotations:

- Blade Server 3 with Mezz cards installed in B and C fabric slots
- Blade Server 3 B2 port or the 2nd port on the B fabric Mezzanine CNA. The Cisco Nexus will use the FCoE-FIP MAC address to associate the CNA to the created VFC and it will use the FCoE-WWN for zoning purposes.

### Basic Validation for the Cisco Nexus 5000 series switch configuration

With connections made via fiber optic cable or direct connect cable (twin-ax) the basic connectivity on the port between the two switches can be verified. These cables or SFP+ transceivers must only be Cisco-branded products for the Cisco Nexus to link properly. The following command is used to give a port status overview: `SHOW INTERFACE BRIEF`. This example has been shortened from the actual results but will display the results of active ports and VFC interfaces. Verify that the ports which are expected to have links show up correctly.

Figure 14. Example of show interface brief command

```
Demo5548-1# show interface brief
```

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/31	2	auto	auto	up	sw1	F	4	--
fc1/32	2	auto	auto	up	sw1	F	4	--

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth1/1	20	eth	trunk	up	none	10G(D)	2
Eth1/2	20	eth	trunk	up	none	10G(D)	2
Eth1/3	1	eth	access	up	none	10G(D)	--
Eth1/4	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/5	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/6	1	eth	access	down	SFP not inserted	10G(D)	--

\*rest of the ports removed for sizing

Port-channel Interface	VLAN	Type	Mode	Status	Reason	Speed	Protocol
Po2	20	eth	trunk	up	none	a-10G(D)	lACP

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	172.25.188.100	1000	1500

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
vfc1	2	F	on	trunking	--	TF	auto	--
vfc3	2	F	on	down	--	--	--	--
vfc4	2	F	on	trunking	--	TF	auto	--
vfc5	2	F	on	down	--	--	--	--
vfc6	2	F	on	trunking	--	TF	auto	--
vfc7	2	F	on	down	--	--	--	--
vfc8	2	F	on	trunking	--	TF	auto	--

Check the spanning tree configuration. Blocking ports should be understood and when they show in this entry it should be the number expected. Otherwise it could be that an unintentional cable loop has been created that will need to be resolved. Type : `SHOW SPANNING-TREE SUMMARY`

Figure 15. `show spanning-tree summary` command showing current configuration with ports states

```
Demo-5020-1# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Port Type Default          is disable
Edge Port [PortFast] BPDU Guard Default is disabled
Edge Port [PortFast] BPDU Filter Default is disabled
Bridge Assurance           is enabled
Loopguard Default         is disabled
Pathcost method used       is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	1	1
1 vlan	0	0	0	1	1

Next, verify that negotiations have happened properly between the FCF and end devices, in this case the Cisco Nexus 5020 is the FCF. Type : `SHOW FLOGI DATABASE`

Figure 16. `show flogi database` command showing devices that have completed fabric login

```
Demo-5020-1# show flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc2/1	2	0xc6000c	20:04:00:20:c2:10:ab:cd	10:00:00:20:c2:10:ab:cd
vfc1	2	0xc60009	20:01:14:fe:b5:07:12:34	20:00:14:fe:b5:07:12:34

Total number of flogi = 2.

At this point the VFC and FC interfaces should be populated in the FLOGI database. This command is showing the devices that have done a valid FLOGI (fabric login) to the Cisco Nexus switch. The VFC should show the expected port and node WWN of the CNA being used in the server.

The following command will show the status of the zones that have been put into place. The asterisks will indicate devices that have an established session (have negotiated and logged in) with the Cisco Nexus 5020. Type : `SHOW ZONESET ACTIVE`. This command will show the current activated zoneset and all the participating zones with their individual members.

Figure 17. Example of `show zoneset active` command

```
Demo-5020-1# show zoneset active
zoneset name set1 vsan 2
zone name blade1 vsan 2
* fcid 0xc6000c [interface fc2/1 swwn 20:00:00:05:73:ab:12:34]
* fcid 0xc60009 [pwwn 20:01:14:fe:b5:07:12:34]
```

With all cables in place between the switches and the FC/FCoE SAN, use the following commands to validate your configuration.

First check general status of the ports, and links by using: `SHOW INTERFACE STATUS`

Figure 18. Show interface status results

```
PowerConnectM8024-k#show interfaces status
```

Port	Name	Duplex	Speed	Neg	Link State	Flow Control Status
-----	-----	-----	-----	-----	-----	-----
Tel1/0/1		N/A	Unknown	Auto	Down	Inactive
Tel1/0/2		N/A	Unknown	Auto	Down	Inactive
Tel1/0/3		Full	10000	Auto	Up	Inactive
Tel1/0/4		N/A	Unknown	Auto	Down	Inactive
Tel1/0/5		Full	10000	Auto	Up	Inactive
Tel1/0/6		N/A	Unknown	Auto	Down	Inactive
Tel1/0/7		Full	10000	Auto	Up	Inactive
Tel1/0/8		N/A	Unknown	Auto	Down	Inactive
Tel1/0/9		N/A	Unknown	Auto	Down	Inactive
Tel1/0/10		N/A	Unknown	Auto	Down	Inactive
Tel1/0/11		Full	10000	Auto	Up	Active
Tel1/0/12		Full	10000	Auto	Up	Inactive
Tel1/0/13		N/A	Unknown	Auto	Down	Inactive
Tel1/0/14		N/A	Unknown	Auto	Down	Inactive
Tel1/0/15		N/A	Unknown	Auto	Down	Inactive
Tel1/0/16		N/A	Unknown	Auto	Down	Inactive
Tel1/0/17		N/A	Unknown	Auto	Down	Inactive
Tel1/0/18		N/A	Unknown	Auto	Down	Inactive
Tel1/0/19		Full	10000	Off	Up	Inactive
Tel1/0/20		Full	10000	Off	Up	Inactive

Oob	Type	Link State
---	-----	-----
oob	Out-Of-Band	Up

Port	Type	Link State
-----	-----	-----
Po1	Link Aggregate	Down
Po2	Link Aggregate	Up

- - Po3-127 removed from example for spacing

Po128	Link Aggregate	Down
Flow Control:Enabled		



With the `SHOW SPANNING-TREE BLOCKEDPORTS` command the status of ports that may be impacted by spanning tree can be checked. This is also a good point to make sure that the spanning-tree behaviors are as expected, such as Priority, which switch is root, etc.

Figure 19. `show spanning-tree blockedports` command

```
PowerConnectM8024-k#show spanning-tree blockedports
Spanning tree Enabled (BPDU flooding : Disabled) mode rstp
CST Regional Root:      80:00:5C:26:0A:AD:0C:39
Regional Root Path Cost: 0

##### MST 0 Vlan Mapped: 1, 20, 1000
ROOT ID
      Priority      32768
      Address      5C26.0AAD.0C39
      This Switch is the Root.
      Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec

Interfaces

Name      State      Prio.Nbr  Cost      Sts  Role  RestrictedPort
-----
-----
```

On the PowerConnect M8024-k, 8024 or 8024F the sessions can be checked by using: `SHOW FIP-SNOOPING`. This will show the VLAN's that are snooped and configured, along with how many FCF's, and ENode devices that are available. If there is no entry or "0" FCF's or ENode's after running this command there is possibly a missed step in the configuration. Proceeding beyond this point will not be possible until this configuration error is corrected.

Figure 20. `Show fip-snooping` command which gives a brief status on available ENode's, and FCF's

```
PowerConnectM8024-k#show fip-snooping

Global Mode:      Enabled
FCoE VLAN List:   20,1000
FCFs:             1
ENodes:           1
Sessions:         2
Max VLANs:        8
Max FCFs in VLAN: 4
Max ENodes:       72
Max Sessions:     1024
```

The following command will show a set of vital information on the DCBX configuration. Type: `show LLDP DCBX INTERFACE ALL`. The important things to note with this command are that the configuration source selected is “True” and that the configuration source port is configured as expected to be the uplink to the top-of-rack FCF switch. It can also be noted that ports that are expected to be passing DCBX traffic should have counter statistics listed here.

Figure 21. `show lldp dcbx interface all`

```
PowerConnectM8024-k#show lldp dcbx interface all
```

Is configuration source selected..... True  
Configuration source port..... Te1/0/19

Interface	Status	Role	Version	DCBX Tx	DCBX Rx	DCBX Errors	unknown TLV
-----	-----	-----	-----	-----	-----	-----	-----
Te1/0/1	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/2	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/3	Enabled	Auto-down	Auto	22710	22562	1	0
Te1/0/4	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/5	Enabled	Auto-down	Auto	22420	22151	0	0
Te1/0/6	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/7	Enabled	Auto-down	Auto	22451	22292	0	0
Te1/0/8	Enabled	Auto-down	Auto	33	0	0	0
Te1/0/9	Enabled	Auto-down	Auto	22	35	0	0
Te1/0/10	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/11	Enabled	Auto-down	Auto	17175	0	0	0
Te1/0/12	Enabled	Auto-down	Auto	17179	17310	0	0
Te1/0/13	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/14	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/15	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/16	Enabled	Auto-down	Auto	0	0	0	0
Te1/0/17	Enabled	Manual	Auto	0	0	0	0
Te1/0/18	Enabled	Manual	Auto	0	0	0	0
Te1/0/19	Enabled	Auto-up	Auto	22707	22861	0	0
Te1/0/20	Enabled	Auto-up	Auto	22706	22865	0	0

The highlighted port lines show the ports that are actively taking part in FCoE traffic. The role shown by each of the server facing ports should always be auto-down, while the role for the uplinks to the FCF should be auto-up or configuration source. There should be both DCBX Tx counters as well as DCBX Rx counters to show that the negotiations actually occurred with the particular devices.

The following command will show a set of vital information on the DCBX configuration. Type: `show LLDP DCBX INTERFACE TE1/0/20 DETAIL`. This command will show more specific detail about the configuration that has been negotiated between the devices. In this example port `te1/0/20` is used as it is one of the uplink ports into the top-of-rack FCF switch.

Some key items in these results will be “true” for peer is configuration source, “Auto-up” for auto-configuration port role and local configuration PFC(3) En/Will/Error configured as Y/Y/N. As an additional note you should also see PFC enable vector: 3:1, this shows that priority queue 3 is set as “strict” and will be lossless.

Figure 22. Show lldp dcbx interface te1/0/20 detail

```
PowerConnectM8024-k#show lldp dcbx interface te1/0/20 detail

DCBX operational status:..... Enabled
Configured DCBX version:..... Auto
Peer DCBX version:..... CIN 1.0
Peer MAC:..... 54:7F:EE:56:55:48
Peer Description:..... Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
Auto-configuration Port Role:..... Auto-up
Peer Is configuration Source:..... True

Error counters:
PFC incompatible configuration..... 0
Disappearing neighbor..... 0
Multiple neighbors detected..... 0

Local configuration:

Type      Subtype      Oper/Max      En/Will/Error
-----
PFC(3) 0      0/0           Y/Y/N
APP(4) 0      0/0           Y/Y/N

Max PFC classes supported..... 2
PFC enable vector: 0:0 1:0 2:0 3:1 4:0 5:0 6:0 7:0

Application priority

Type      Application      Priority      Status
-----
Ethernet  0x8906           8            Enabled

Peer configuration:

Operational version: 0 Max version: 0 Seq no: 1 Ack no: 1

Type      Subtype      Oper/Max      En/Will/Error
-----
PFC(3) 0      0/0           Y/N/N
APP(4) 0      0/0           Y/N/N
PFC enable vector: 0:0 1:0 2:0 3:1 4:0 5:0 6:0 7:0

Peer application priority

Type      Application      Priority      Status
-----
Ethernet  0x8906           8            Enabled
```

Finally, after these validation steps, go into the disk management interface of the server. If the SAN is configured appropriately the server will have an available LUN to use for storage.

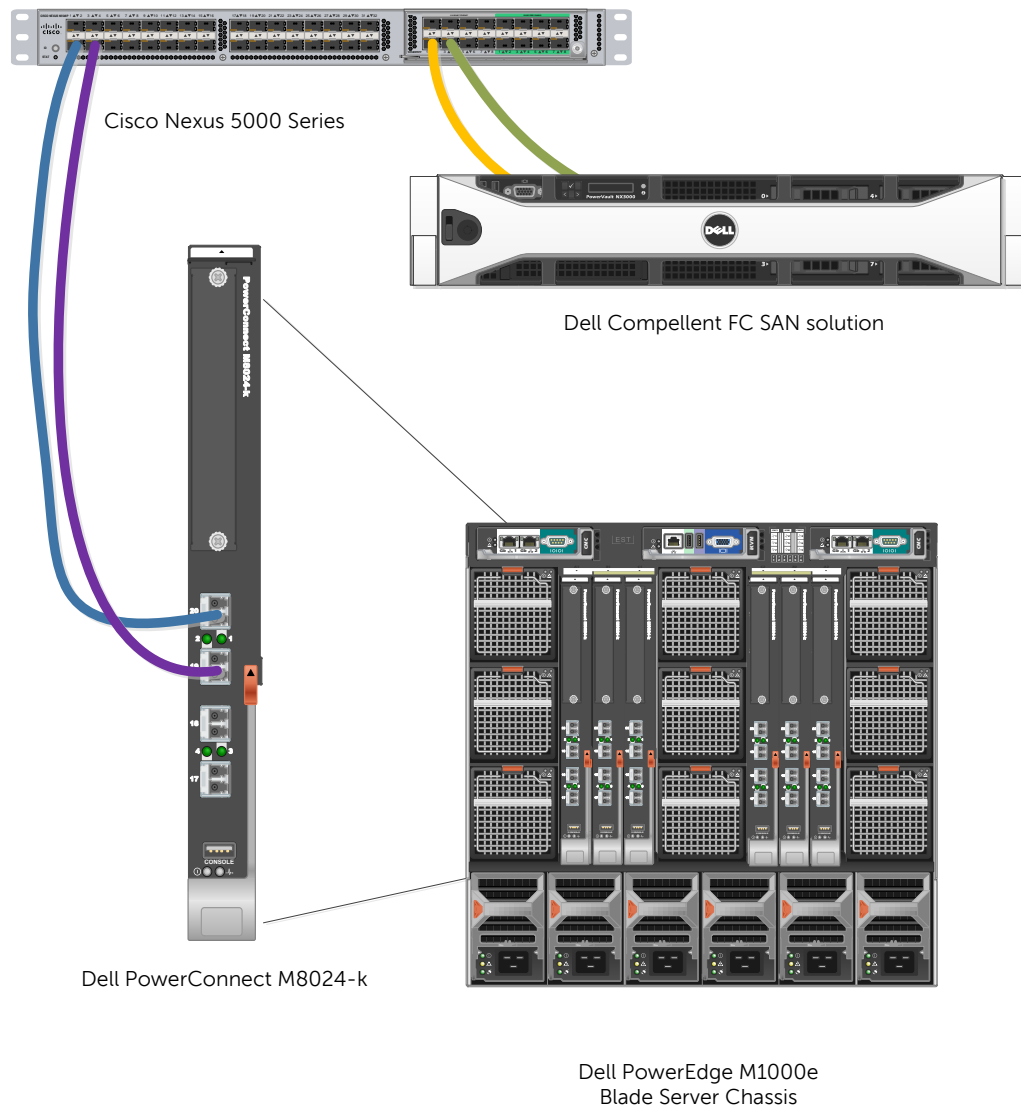
## Basic Troubleshooting Areas

Problem	Potential Problem Area	Potential Fix
Basic Connectivity Between CNA and 8024 Series switch is not present (ping between devices)	Cable is not connected or is failing	Connect or Change cable and reconnect
	The OS on the server is not configured to have the network card enabled or active	Check adapter settings in the OS and verify ports turned on or enabled
	The driver for the applicable OS is not loaded	Load driver and ensure both Ethernet and storage device drivers are in place for CNA (if applicable)
	Internal server facing ports on the M8024-k may not be enabled (no shutdown)	Determine which internal ports should be enabled and configure the ports on with the "no shutdown" command
	External or regular ports on the 8024 series switch or Cisco Nexus 5000 series switch may not be enabled (no shutdown)	Determine which external ports should be enabled and configure the ports on with the "no shutdown" command
	Untagged or Native VLAN's are not configured appropriately. If PVID is changed on 8024 series, VLAN 1 must be removed	Configure Native VLAN's appropriately. See PowerConnect 8024 CLI section or Cisco Nexus 5000 series CLI section for detail on this.
ENode's or FCF entries are not present on the PowerConnect 8024 series switch	See above basic connectivity problems	see above
	Applicable FCoE or storage driver is not configured in the server OS for the CNA	This could be an indication that the storage side of the CNA driver has not been fully installed.
	CNA may not be configured as willing (will negotiate values with the FCF switch)	Some CNA's have the option to configure the DCB settings manually. This will potentially cause misbehavior due to the DCBX negotiations not occurring as expected.
	PowerConnect 8024 may not have appropriate firmware in place, it must be 4.2.0.4 or greater	Download and install firmware 4.2.0.4 or greater see upgrade firmware section
ENode's or FCF entries are not present on the PowerConnect 8024 series switch-continued -	Cisco Nexus 5000 series switch may not have the supported firmware in place. Must be 5.0(2)N1(1) or greater	Download and install latest Cisco firmware.
	Feature FCoE may not be configured on Cisco Nexus 5000 series switch	Ensure FCoE feature is configured on Nexus 5000 Series switch
	fip-snooping may not be enabled on the native and FCoE VLAN on the Dell PowerConnect 8024 series switch	See PowerConnect 8024 CLI section for explanation of enabling both VLAN's for fip-snooping

Problem	Potential Problem Area	Potential Fix
	The VFC entries may not be present on the Cisco Nexus 5000 series switch	Ensure that VFC's are created that will be applicable to the connection. This can be bound to the FCoE-FIP MAC of the CNA or to the physical interface of the Cisco Nexus 5000 Series switch
	The VFC entry may not be enable (no shutdown)	Check VFC entries applicable to the connection and make sure "no shutdown" is part of the configuration for that interface
	The FCoE VLAN may not match on both sides (PowerConnect 8024 and Cisco Nexus 5000 series tagged VLAN entries matched to the FCoE feature)	The same tagged VLAN should pass FCoE traffic from the PowerConnect 8024 series switch to the Cisco Nexus 5000 series switch. Configure this VLAN appropriately - see CLI explanation sections
	LACP feature may not be enabled on Cisco Nexus 5000 series switch for applicable LAG's between the two switches	Configure feature LACP on the Cisco Nexus, and make sure the applicable port-channel is put into the configuration - see CLI explanation sections for further detail
	Configuration classofservice dot1p-mapping may not be in place on the PowerConnect switch	See PowerConnect 8024 CLI section for explanation of applying this configuration
	CNA's that have NPAR capabilities may not have the partitions configured appropriately for FCoE	See CNA documentation for applicable partition settings for FCoE use
FLOGI entries for CNA's are not present on Cisco Nexus 5000 series switch	See above basic connectivity problems	see above
	Verify above section on ENode's or FCF present on PowerConnect 8024 series switch	see above
FLOGI entries for FC devices are not present on Cisco Nexus 5000 series switch	Cable is not connected or is failing	Connect or Change cable and reconnect
	Storage license for Cisco Nexus may not be installed.	Check licenses on Cisco Nexus and install if necessary
	End storage device is not powered on	Power on Storage device
	Storage device is not configured to communicate with FCF or FC switch	Configure storage device to have applicable settings
	FC port on Cisco Nexus not configured	Configure FC ports for particular storage device and turn on (no shutdown)
	Cisco Nexus may be configured for NPV which allows for the logins to occur on FC switch further downstream	Check configuration of Cisco Nexus. If configured for NPV check for FLOGI logins on the FC switch that the Cisco Nexus is connected to.

## Scenario 2: Configuring Multiple Uplinks into LAG for Cisco Nexus 5000 Series Switch (NPIV) Environment

Figure 23. Multiple port link (LAG) configuration between switches and storage



## Configuring the Cisco Nexus 5000 series switch with firmware ver 5.x for a multiple link LAG (link aggregation) connection at the Top-of-Rack.

The typical scenario in a business environment consists of more than one connection or uplink. The following illustrations and examples describe a two link LAG from an M8024-k to the Cisco Nexus 5020.

### Command-Line Interface Method

Figure 24. Multiple port link (LAG) Cisco 5020 configuration (can be copied and pasted)

```
feature fcoe
system default switchport trunk mode auto
feature telnet
feature npiv
feature lacp

vlan 20
vlan 1000
  fcoe vsan 2

vsan database
  vsan 2
  vsan 2 interface vfc1
  vsan 2 interface fc2/1
  vsan 2 interface fc2/2

interface port-channel1
  switchport mode trunk
  switchport trunk native vlan 20
  switchport trunk allowed vlan 1000

interface vfc1
  bind interface port-channel1
  no shutdown

interface fc2/1
  no shutdown

interface fc2/2
  no shutdown

interface Ethernet1/1
  switchport mode trunk
  switchport trunk native vlan 20
  switchport trunk allowed vlan 1000
  channel-group 1 mode active

interface Ethernet1/2
  switchport mode trunk
  switchport trunk native vlan 20
  switchport trunk allowed vlan 1000
  channel-group 1 mode active

zone name blade1 vsan 2
  member interface fc2/1
  member pwwn xx:xx:xx:xx:xx:xx:xx:xx

zone name blade2 vsan 2
  member interface fc2/2
  member pwwn xx:xx:xx:xx:xx:xx:xx:xx

zoneset name set1 vsan 2
  member blade1
  member blade2

zoneset activate name set1 vsan 2
```

### Step by Step explanation of CLI example (only covering the differences from the single port configuration)

- **interface vfc1** – selects virtual fc interface vfc1 (vfc1 is an example and can be a different number based on choice at configuration time)
  - **bind interface port-channel1** – this binds interface port-channel1 to the virtual fc interface which in this case is vfc1.
  - **no shutdown** – turns the virtual interface on since default is shutdown
- **interface fc2/2** – selects the fc2/2 interface (this is an additional FC port for the 2 connections)
  - **no shutdown** – turns the fc2/1 interface on since default is shutdown
- **interface Ethernet 1/1** – selects interface Ethernet 1/1
  - **switchport mode trunk** - set switchport mode to trunk for the 2 VLAN's
  - **switchport trunk native vlan 20** - add native VLAN 20 to the trunk
  - **switchport trunk allowed vlan 1000** - add allowed VLAN 1000 to the trunk
  - **channel-group 1 mode active** - this interface is part of a port channel 1
- **interface Ethernet 1/2** – selects interface Ethernet 1/2
  - **switchport mode trunk** - set switchport mode to trunk for the 2 VLAN's
  - **switchport trunk native vlan 20** - add native VLAN 20 to the trunk
  - **switchport trunk allowed vlan 1000** - add allowed VLAN 1000 to the trunk
  - **channel-group 1 mode active** - this interface is part of port channel 1
- **zone name blade1 vsan 2** - this will set the name for your zone (blade1 can be any chosen name), vsan 2 will match the vsan you have created.
  - **member interface fc2/1** - this adds the fc2/1 interface as a member of the zone.
  - **member pwwn xx:xx:xx:xx:xx:xx:xx:xx** - adds the port WWN of the ENode device to the zone (this should match the CNA of the server being used, in this case blade 2).
- **zone name blade2 vsan 2** - this will set the name for your zone (blade1 can be any chosen name), vsan 2 will match the vsan you have created.
  - **member interface fc2/2** - this adds the fc2/1 interface as a member of the zone.
  - **member pwwn xx:xx:xx:xx:xx:xx:xx:xx** - adds the port WWN of the ENode device to the zone (this should match the CNA of the server being used, in this case blade 2).
- **zoneset name set1 vsan 2** - move into the zoneset interface (in this case the name is set1 but could be any name and the VSAN number is based on the FCoE VLAN being used).
  - **member blade1** - this includes the blade1 zone into this zoneset
  - **member blade2** - this includes the blade2 zone into this zoneset
- **zoneset activate name set1 vsan 2** - activates the zoneset containing these zones.



## Configuring the M8024-k, 8024, and 8024F for FIP Snooping

This is an example of the necessary CLI commands for 8024 model switches configured with two links in a LAG or port-channel uplinked to the Cisco 5020. This provides more bandwidth and fail-over capability which would be more typical in the larger scale infrastructure typically used.

### Command-Line Interface Method

Figure 25. Multiple port uplink (LAG) M8024-k configuration (can be copied and pasted)

```
configure
no mode simple
vlan database
vlan 1000
exit
hostname "mySwitch"
feature fip-snooping
vlan 1,1000
fip-snooping enable
exit
interface out-of-band
ip address 198.18.100.x 255.255.255.0 198.18.255.254
classofservice dot1p-mapping 3 3
exit

interface Te1/0/1
switchport general allowed vlan add 1000 tagged
switchport mode general
lldp dcbx port-role auto-down
exit

interface Te1/0/2
switchport general allowed vlan add 1000 tagged
switchport mode general
lldp dcbx port-role auto-down
exit

interface Te1/0/19
channel-group 1 mode active
lldp dcbx port-role auto-up
exit

interface Te1/0/20
channel-group 1 mode active
lldp dcbx port-role auto-up
exit

interface port-channel 1
switchport general allowed vlan add 1000 tagged
switchport mode general
fip-snooping port-mode fcf
exit
```

### Step by Step explanation of Dell PowerConnect M8024-k CLI example with multiple port (LAG) uplink (this only covers the differences from the single port configuration).

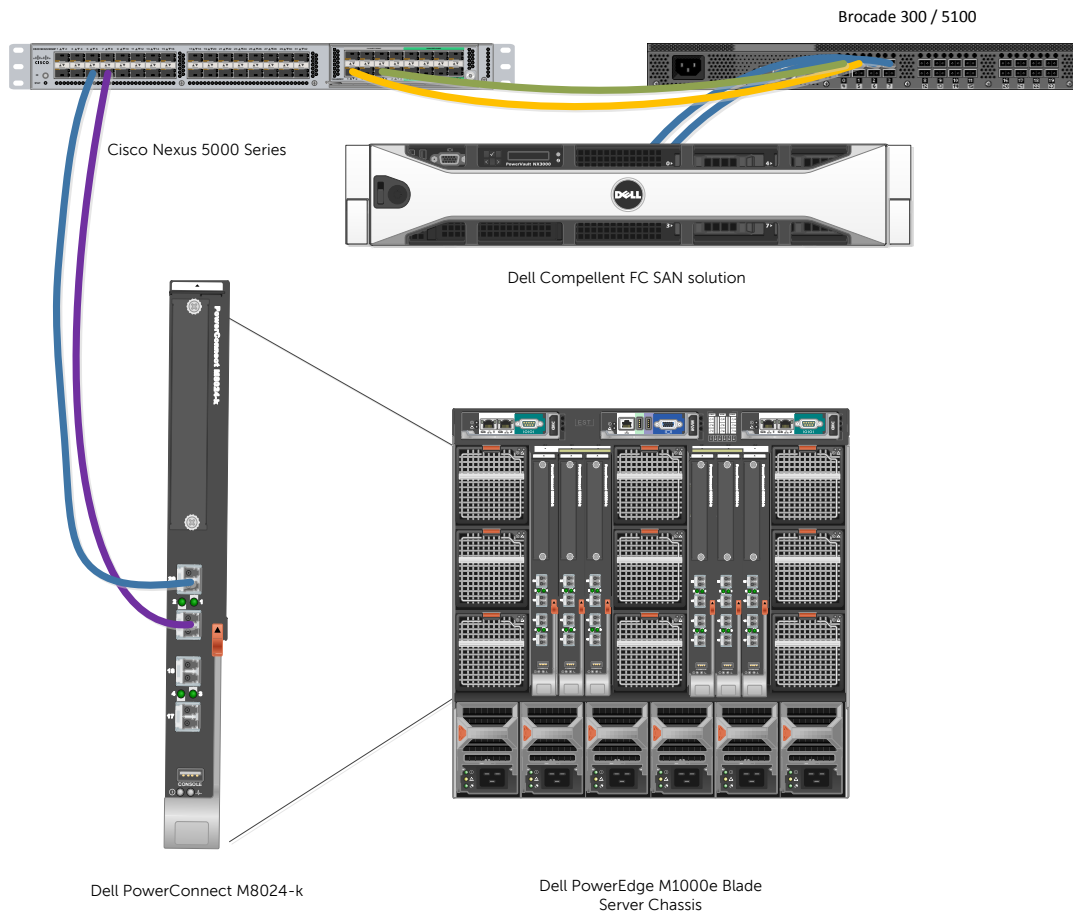
- **interface te1/0/19** – this moves into the interface te1/0/19 configuration
  - **channel-group 1 mode active** – adds this interface to the channel-group 1
  - **lldp dcbx port-role auto-up** – sets the DCBX port-role to be auto-up for an FCF connection
  - **exit** - exit the interface configuration
- **interface te1/0/20** – this moves into the interface te1/0/20 configuration
  - **channel-group 1 mode active** – adds this interface to the channel-group 1
  - **lldp dcbx port-role auto-up** – sets the DCBX port-role to be auto-up for an FCF connection
  - **exit** - exit the interface configuration
- **interface port-channel 1** – this moves into the interface te1/0/20 configuration
  - **switchport general allowed vlan add 1000 tagged -** – this sets up a trunk with a tagged VLAN of 1000 (the FCoE VLAN), and includes the native VLAN as untagged if general mode is enabled.
  - **switchport mode general** – this enables the port for mode general
  - **fip-snooping port-mode fcf** – enables the port for fip-snooping from an FCF connection
  - **exit** - exit the interface configuration
- **exit** – exit from configuration mode

### Validation

Follow the same [validation steps as mentioned with the single link steps](#) to ensure that this configuration is working correctly. The ideal method for troubleshooting or validation is to take one link at a time.

## Scenario 3: Configuring Multiple Uplinks into LAG for Cisco Nexus 5000 Series Switch (*NPV* mode) Environment

Figure 26. Multiple link configuration between switches and storage



## Configuring the Cisco Nexus 5000 series switch with firmware ver 5.0(3)N2(2a) in NPV mode for a multiple link LAG (link aggregation) connection from the Dell PowerConnect M8024-k or 8024(F)

The typical scenario in a business environment consists of more than one connection or uplink. The following pictures and examples describe a two link LAG from an M8024-k to the Cisco 5020.

### Command-Line Interface Method

Figure 27. Multiple port link Cisco 5020 configuration (can be copied and pasted)

```
feature fcoe
system default switchport trunk mode auto
feature telnet
feature lacp
feature npv
feature npiv

vlan 20
vlan 1000
    fcoe vsan 2

vsan database
    vsan 2
    vsan 2 interface vfc1
    vsan 2 interface vfc2
    vsan 2 interface fc2/1
    vsan 2 interface fc2/2

interface port-channel1
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000

interface vfc1
    bind mac-address xx:xx:xx:xx:xx:xx
    no shutdown
interface vfc2
    bind mac-address xx:xx:xx:xx:xx:xx
    no shutdown

interface fc2/1
    no shutdown

interface fc2/2
    no shutdown

interface Ethernet1/1
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000
    channel-group 1 mode active

interface Ethernet1/2
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000
    channel-group 1 mode active
```

## Step by Step explanation of CLI example for the Cisco Nexus 5000 Series using NPV (only covering the differences from the single port configuration)

- **feature NPV**- enables the NPV feature which turns off zoning. The FC side of the Nexus 5000 series switch effectively turns into just a FC gateway (just passing FC out to another switch). When this feature is enabled the Cisco Nexus 5000 series switch will have to do a full reload because it is completely changing the way it deals with the FC packet behavior. Be prepared for this reload because it may impact a currently running network environment.

## Configuring the Dell PowerConnect M8024-k, 8024, and 8024F for FIP Snooping with Cisco Nexus 5000 series switch in NPV mode.

The configuration will be the same as previously mentioned in the single or multiple port configurations. The simplicity of the PowerConnect 8024 series switch setup for FIP Snooping is one of the great advantages to using this in an FCoE network.


## ETS Behavior and CoS configurations on the PowerConnect 8024 series switches

The 8024 family devices will pass ETS information between end devices and the FCF but local settings are not changed in the 8024 series switches. This process allows for a best effort approach in the default configuration. This will be sufficient for the typical business usage model but for more in-depth settings the following CoS settings can be set in order to apply exact minimum thresholds for the queues that will be used for FCoE or iSCSI. These minimum thresholds are a guaranteed minimum bandwidth for the queues involved, in this case priority queue 3 for FCoE or 4 for iSCSI. The following example is applicable to the FCoE class of service queue 3 settings. (These settings can also be found in the [appendix in the full CLI example.](#))

Figure 28. CoS settings to establish minimum bandwidth for FCoE queue

```
! Default priority is 0 (CoS queue 0). Untagged frames receive the default priority treatment.
!
interface range te1/0/1-16
! Set CoS queue 3 to strict priority (not WRED) per 802.1Qaz
cos-queue strict 3
! Reserve 50% bw for CoS queue 3
cos-queue min-bandwidth 0 0 0 50 0 0 0
exit

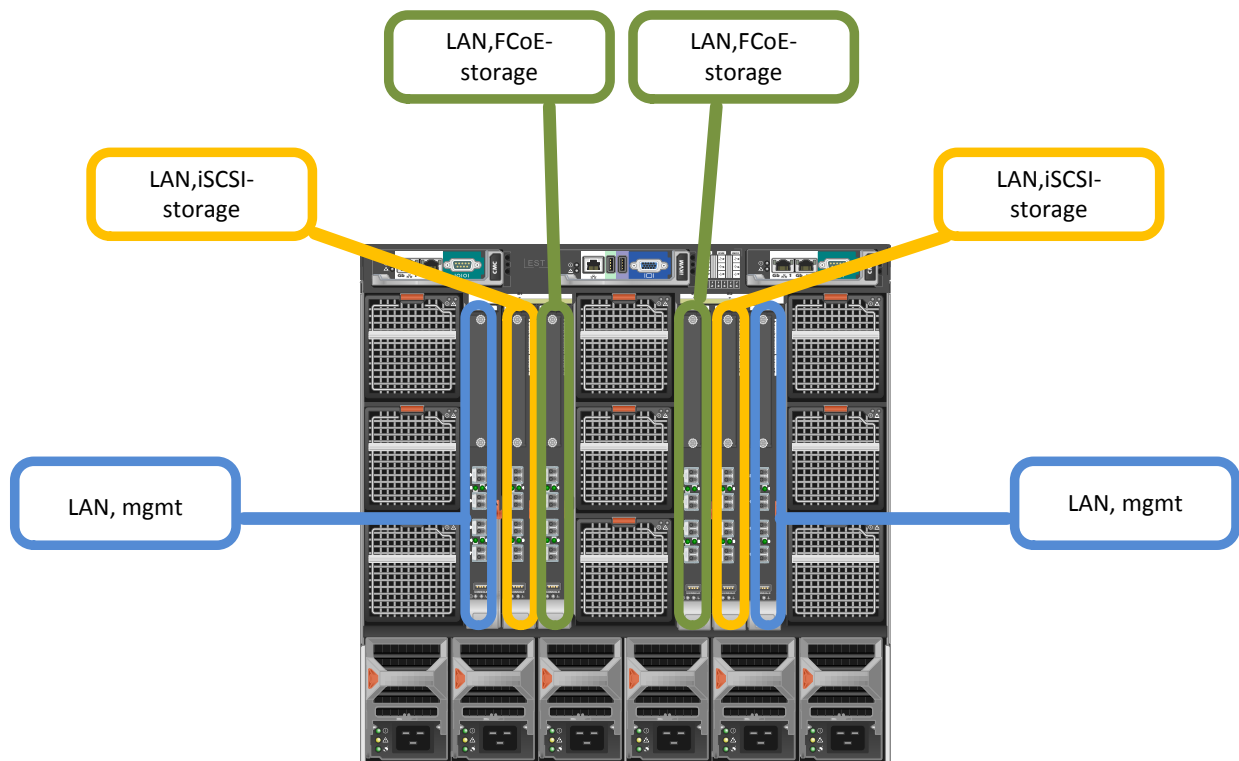
interface te1/0/20
! Set CoS queue 3 to strict priority (not WRED) per 802.1Qaz (traffic selection class 0)
cos-queue strict 3
! Reserve 50% bw for CoS queue 3 - other queues are best effort.
! This bandwidth is shared with other queues if not used
cos-queue min-bandwidth 0 0 0 50 0 0 0
Exit
```

 **NOTE:** In the above example the first setting is made on interfaces te1/0/1 through 16. These are all the internal server-facing ports on the M8024-k modular switch. The settings for te1/0/20 are based on this port being an uplink from the M8024-k modular switch to the Cisco Nexus 5000 series switch. As mentioned above the full configuration with these settings in place can be seen in the [Appendix A - M8024-k CLI example.](#)


### Further notes on ETS / CoS behavior settings

Careful consideration should be taken when establishing the strict priority queues and managing bandwidth reservations. If FCoE and iSCSI are configured on the same switch and these settings are used to configure both CoS queues it is possible to choke the bandwidth being allowed for regular LAN traffic. As a suggested method limiting the queues for these priorities to 30 or 40 percent would keep this from occurring. The preferred method for configuration is fabric separation or in simpler terms; separating the two storage types onto different switches for ease of management and bandwidth control.

Figure 29. Fabric separation as preferred method for management of networks and storage



## Updating firmware

 **NOTE:** Be sure to check the Release Notes and any special instructions that may have come with new firmware updates. It is important to follow instructions found in those documents if they deviate from this white paper.

Steps for upgrading the firmware on a stack of switches are similar to upgrading the firmware on a single switch. After downloading a new image to the Master by using the **File Download** page in the Web UI or the **copy** command in the CLI, the downloaded image is distributed to all member units of the stack. The instructions below will guide you through these steps.

### Command-line interface method

To find the firmware version the switch is using, enter the following command: **show version**

```
PowerConnectM8024-k #show version
```

Image Descriptions  
 image1 : default image  
 image2 :

Images currently available on Flash

unit	image1	image2	current-active	next-active
1	4.1.0.9	4.1.0.6	image1	image1

The commands below demonstrate how to copy the firmware file down to the switch via a TFTP server. The switch will need access to the TFTP server on the network and the firmware file will need to be present in the download folder of the TFTP server. Perform the following command from the CLI interface. Press Y when prompted.

```
console#copy tftp://198.18.1.64/PC8024v4.2.0.4.stk image
```

Transfer Mode..... TFTP  
 Server IP Address..... 198.18.1.64  
 Source File Path..... ./  
 Source Filename..... PC8024v4.2.0.4.stk  
 Data Type..... Code  
 Destination Filename..... image

Management access will be blocked for the duration of the transfer  
 Are you sure you want to start? (y/n) y

TFTP code transfer starting  
 12487236 bytes transferred...  
 File contents are valid. Copying file to flash...  
 File transfer operation completed successfully.

Be patient as this procedure may take a few minutes

Perform another **show version** command to confirm that the new firmware has been downloaded to the switch. Notice that the firmware was copied into the inactive image for each member.

```
console#show version
```

Images currently available on Flash				
unit	image1	image2	current-active	next-active
1	4.1.0.9	4.2.0.4	image1	image1

The current-active column now shows the same values as the next-active column. The next step is to activate the image that contains the new firmware. In this example, the switch will need *image2* activated. Perform the following commands.

```
console#boot system image2
Activating image image2 ..
```

Images currently available on Flash				
unit	image1	image2	current-active	next-active
1	4.1.0.9	4.2.0.4	image1	image2

Notice that the next-active column now shows different values than the current-active column.

Before performing the following **update bootcode** command, read the Release Notes and any special instructions for updating the firmware release. It is generally required that you update bootcode only on major releases of the firmware, whereas minor releases will not require the update to bootcode. It is recommended to only run this command if required. Press **Y** when prompted.

```
console#update bootcode
Update bootcode and reset (Y/N)?Y

Issuing boot code update command... Validating boot code from image...CRC
Valid.
```

Updating and rebooting the switch will take a few minutes. If the bootcode is not required, then a simple **reload** command will need to be performed. After reload, the firmware upgrade is complete.



To validate, login to the switch and perform a **show version** command. For the example given the following is displayed.

```
console#show version

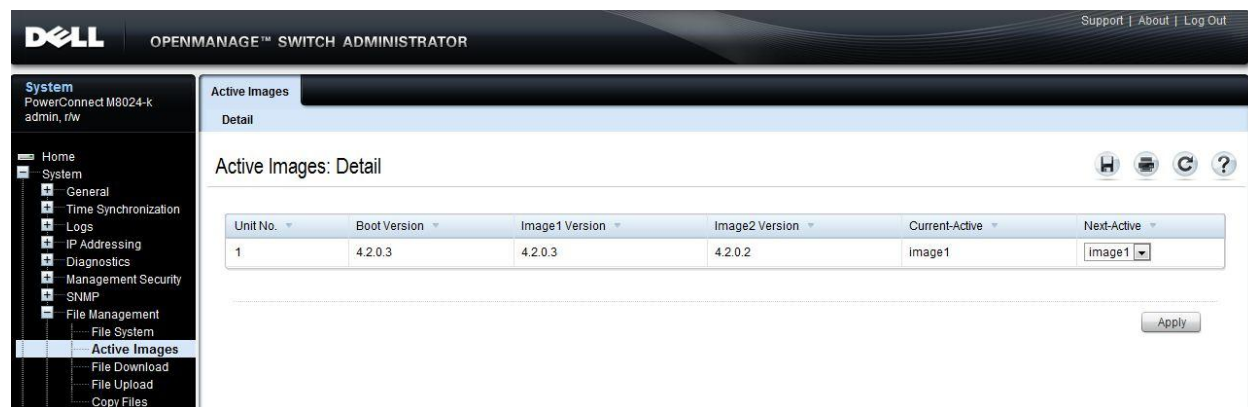
Images currently available on Flash
unit  image1      image2      current-active  next-active
-----
1      4.1.0.9        4.2.0.4      image2          image2
```

While downgrading to a previous firmware is supported, all features and functions that were not part of the previous firmware will be lost, including those features and functions that were introduced in the current firmware in use. Firmware version 4.2 or later must be active on all switches or stack members in order for stacking and DCB to work. Do not downgrade a switch or stack to firmware version 4.1.x.x or earlier.

## Web interface method

Find the firmware versions that the stack members are using.

1. Select System > File Management > Active Images.
2. Look in the Current-Active column to find which images are enabled
3. Since image2 is active, look in the *Image 2 Version* column to see what version each stack member is at. These firmware versions being used should be the same across all stack member units.



The commands below demonstrate how to copy the firmware file down to the switch via a TFTP server. The switch will need access to the TFTP server on the network and the firmware file will need to be present in the download folder of the TFTP server. If other methods are preferable over TFTP please see the User's Guide. Perform the following steps:

1. Select System > File Management > File Download.
2. Select **Firmware** for the File Type and **TFTP** for the Transfer Mode.

3. Enter the IP address of the TFTP server into the Server Address field, and enter the name of the Firmware file into the Source File Name field.
4. If not in the root directory of the TFTP server, enter the path of the firmware file.

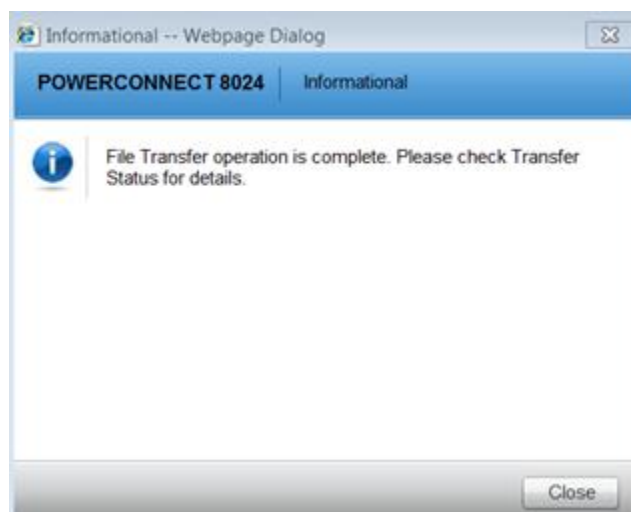
The screenshot shows the Dell OpenManage Switch Administrator interface. On the left is a navigation tree with categories like System, File Management, and Stack Management. The 'File Download' option is selected. The main area is titled 'File Download: Detail' and contains a form with the following fields:

- File Type:** A dropdown menu set to 'Firmware'.
- Transfer Mode:** A dropdown menu set to 'TFTP'.
- Download Section:**
  - Server Address:** A text box containing '198.18.12.64' with a hint '(Hostname or IP address)'.
  - Source File Name:** A text box containing 'PC8024v4.2.0.4.stk' with a hint '(1 to 32 characters)'.
  - Transfer File Path:** An empty text box with a hint '(0 to 160 characters)'.

At the bottom right of the form is an 'Apply' button. There are also 'Back to top' links on the right side of the form.

5. Click Apply.

The dialog box below will appear after a short period stating that the transfer is complete.



6. Click Close.
7. Select **System > File Management > Active Images**.

Notice that the firmware (i.e. 4.2.0.4) was copied into the *inactive* image for each member.

Also notice that the switch still has the same Current-Active image as before.



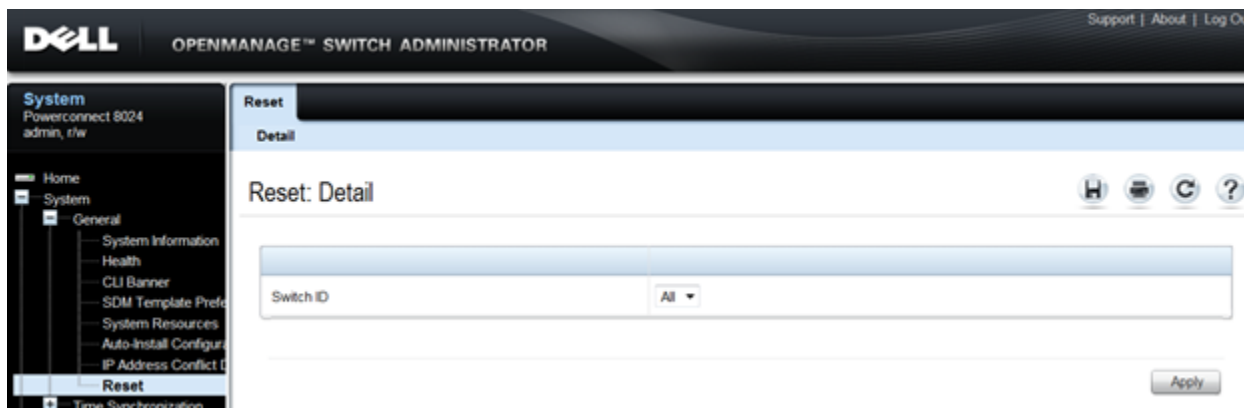
8. Under the Next-Active column, select the new image (i.e. image2) for the switch or stack.

Image1 Version	Image2 Version	Current-Active	Next-Active
4.2.0.3	4.2.0.4	image1	image1

9. Click Apply.

The Current-Active column should now show the opposite values as what is in the Next-Active column. A reload is required to activate the firmware.

10. Select **System > General > Reset**. Choose “All” in the Switch ID menu.

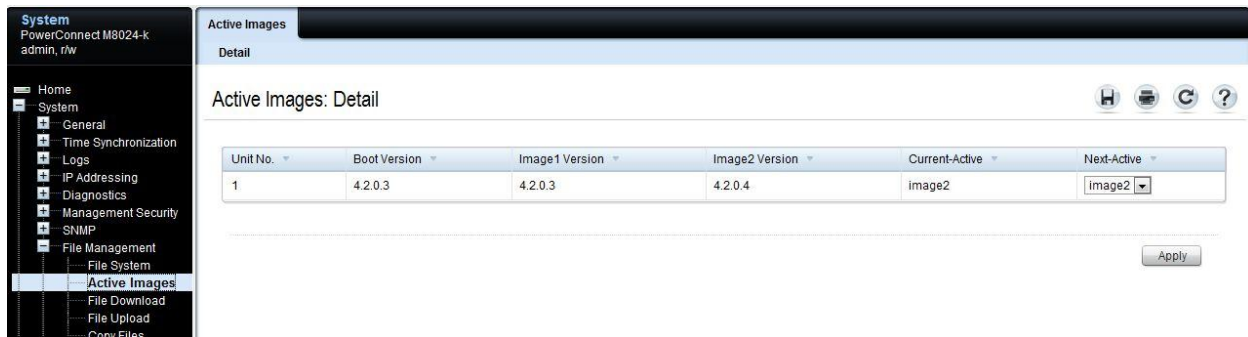


11. Click Apply.

12. After the stack resets, verify the new firmware has become active.

13. Select **System > File Management > Active Images** again.

Notice that the new firmware (i.e. 4.2.0.4) is now the Current-Active image for each member.



While downgrading to a previous firmware is supported, all features and functions that were not part of the previous firmware will be lost, including those features and functions that were introduced in the current firmware in use. Firmware version 4.2 or later must be active for the DCB or stacking features to work correctly. Do not downgrade the switch to firmware version 4.1.x.x or earlier.

## Appendix A - Full CLI examples

### M8024-k CLI example

```
show running-config
```

```
!Current Configuration:
!System Description "PowerConnect M8024-k, 4.2.1.3, VxWorks 6.6"
!System Software Version 4.2.1.3
!Cut-through mode is configured as disabled
!System Operational Mode "Normal"
!
configure
no mode simple
vlan database
vlan 20,1000
exit
slot 1/0 2      ! PCM8024-k
feature fip-snooping
vlan 20,1000
fip-snooping enable
exit
stack
member 1 1      ! PCM8024-k
exit
no logging console
username "root" password e6e66b8981c1030d5650da159e79539a privilege 15
encrypted
line console
exec-timeout 0
exit
classofservice dot1p-mapping 1 1
classofservice dot1p-mapping 2 2
classofservice dot1p-mapping 3 3
classofservice dot1p-mapping 4 4
classofservice dot1p-mapping 5 5
classofservice dot1p-mapping 6 6
!
interface Te1/0/1
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
```

```
!  
interface Tel1/0/2  
cos-queue min-bandwidth 0 0 0 50 0 0 0  
cos-queue strict 3  
shutdown  
spanning-tree port-priority 0  
mtu 2500  
switchport mode general  
switchport general pvid 20  
switchport general allowed vlan add 20  
switchport general allowed vlan add 1000 tagged  
switchport general allowed vlan remove 1  
lldp dcbx port-role auto-down  
exit  
!  
interface Tel1/0/3  
cos-queue min-bandwidth 0 0 0 50 0 0 0  
cos-queue strict 3  
mtu 2500  
switchport mode general  
switchport general pvid 20  
switchport general allowed vlan add 20  
switchport general allowed vlan add 1000 tagged  
switchport general allowed vlan remove 1  
lldp dcbx port-role auto-down  
exit  
!  
interface Tel1/0/4  
cos-queue min-bandwidth 0 0 0 50 0 0 0  
cos-queue strict 3  
shutdown  
spanning-tree port-priority 0  
mtu 2500  
switchport mode general  
switchport general pvid 20  
switchport general allowed vlan add 20  
switchport general allowed vlan add 1000 tagged  
switchport general allowed vlan remove 1  
lldp dcbx port-role auto-down  
exit  
!  
interface Tel1/0/5  
cos-queue min-bandwidth 0 0 0 50 0 0 0  
cos-queue strict 3  
spanning-tree port-priority 0  
mtu 2500  
switchport mode general  
switchport general pvid 20  
switchport general allowed vlan add 20  
switchport general allowed vlan add 1000 tagged  
switchport general allowed vlan remove 1  
lldp dcbx port-role auto-down
```

```
exit
!
interface Tel1/0/6
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/7
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/8
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/9
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
```

```
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/10
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/11
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/12
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Tel1/0/13
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
```



```
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Te1/0/14
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Te1/0/15
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Te1/0/16
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-down
exit
!
interface Te1/0/17
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
```

```

mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
exit
!
interface Tel/0/18
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
shutdown
spanning-tree port-priority 0
mtu 2500
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
exit
!
interface Tel/0/19
channel-group 2 mode active
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 0 3
spanning-tree port-priority 0
mtu 2500
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-up
exit
!
interface Tel/0/20
channel-group 2 mode active
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 0 3
spanning-tree port-priority 0
mtu 2500
switchport general allowed vlan add 20
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
lldp dcbx port-role auto-up
exit
!
interface port-channel 2
cos-queue min-bandwidth 0 0 0 50 0 0 0
cos-queue strict 3
spanning-tree port-priority 0
switchport mode general
switchport general pvid 20
switchport general allowed vlan add 20

```

## Deploying FCoE (FIP Snooping) on Dell PowerConnect 10G Switches: M8024-k, 8024, and 8024F

```
switchport general allowed vlan add 1000 tagged
switchport general allowed vlan remove 1
mtu 2500
fip-snooping port-mode fcf
exit
!
interface port-channel 3
mtu 2500
exit
!
interface port-channel 4
mtu 2500
exit
```

➔ Skipped port-channel 5 through 126 for space

```
interface port-channel 127
mtu 2500
exit
!
interface port-channel 128
mtu 2500
exit
enable password f611e082a05f5562f1d0d2bbcef2b5bf encrypted
exit

console#
```

## Cisco Nexus 5548UP CLI example

```
Technet5548-1# show running-config
```

```
!Command: show running-config
```

```
!Time: Tue Feb 14 22:47:07 2012
```

```
version 5.0(3)N2(2a)
```

```
feature fcoe
```

```
feature telnet
```

```
cfs ipv4 distribute
```

```
feature lacp
```

```
feature lldp
```

```
username admin password 5 $1$0bcPjaAd$t3MSaSb34/4QiOx/il5VM0 role
```

```
network-admin
```

```
ip domain-lookup
```

```
hostname Technet5548-1
```

```
class-map type qos class-fcoe
```

```
class-map type queuing class-fcoe
```

```
match qos-group 1
```

```
class-map type queuing class-all-flood
```

```
match qos-group 2
```

```
class-map type queuing class-ip-multicast
```

```
match qos-group 2
```

```
class-map type network-qos class-fcoe
```

```
match qos-group 1
```

```
class-map type network-qos class-all-flood
```

```
match qos-group 2
```

```
class-map type network-qos class-ip-multicast
```

```
match qos-group 2
```

```
system qos
```

```
service-policy type qos input fcoe-default-in-policy
```

```
service-policy type queuing input fcoe-default-in-policy
```

```
service-policy type queuing output fcoe-default-out-policy
```

```
service-policy type network-qos fcoe-default-nq-policy
```

```
slot 1
```

```
port 31-32 type fc
```

```
snmp-server user admin network-admin auth md5
```

```
0x18e86ba84d1d511fcb6fe4b5e02dc408 priv
```

```
0x18e86ba84d1d511fcb6fe4b5e02dc408 loca
```

```
lizedkey
```

```
snmp-server enable traps entity fru
```

```
vrf context management
```

```
ip route 0.0.0.0/0 172.25.188.254
```

```
vlan 1
```

```
vlan 20
```

```
name NATIVE_VLAN
```

## Deploying FCoE (FIP Snooping) on Dell PowerConnect 10G Switches: M8024-k, 8024, and 8024F

```
vlan 1000
  fcoe vsan 2
  name FCoE_VLAN
vsan database
  vsan 2

interface port-channel2
  switchport mode trunk
  switchport trunk native vlan 20
  switchport trunk allowed vlan 1000

interface vfc3
  bind mac-address 14:fe:b5:8e:5b:f2
  no shutdown

interface vfc4
  bind mac-address 14:fe:b5:8e:5b:f0
  no shutdown

interface vfc5
  bind mac-address 14:fe:b5:8e:5c:09
  no shutdown

interface vfc6
  bind mac-address 14:fe:b5:8e:5c:0b
  no shutdown

interface vfc7
  bind mac-address 14:fe:b5:8e:5c:26
  no shutdown

interface vfc8
  bind mac-address 14:fe:b5:8e:5c:24
  no shutdown
vsan database
  vsan 2 interface vfc3
  vsan 2 interface vfc4
  vsan 2 interface vfc5
  vsan 2 interface vfc6
  vsan 2 interface vfc7
  vsan 2 interface vfc8
  vsan 2 interface fc1/31
  vsan 2 interface fc1/32

feature npv
feature npiv

interface fc1/31
  switchport trunk mode on
  no shutdown
```

```
interface fc1/32
  switchport trunk mode on
  no shutdown

interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
interface Ethernet1/16
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
```

```
interface Ethernet1/25

interface Ethernet1/26
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000

interface Ethernet1/27
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000

interface Ethernet1/28
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000

interface Ethernet1/29
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000
    channel-group 2 mode active

interface Ethernet1/30
    switchport mode trunk
    switchport trunk native vlan 20
    switchport trunk allowed vlan 1000
    channel-group 2 mode active

interface mgmt0
    ip address 172.25.188.100/16
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N2.2a.bin
boot system bootflash:/n5000-uk9.5.0.3.N2.2a.bin
interface fc1/31
    switchport mode NP
interface fc1/32
    switchport mode NP
```

## Appendix B - Network Switch Versions

Version information for the network switches used in creating this document are as follows:

Table 1. Switch Firmware Versions

Network switch	Dell PowerConnect™ M8024k	Dell PowerConnect™ 8024/8024F	Cisco 5020
Software version	4.2.0.1, 4.2.0.2, 4.2.0.3, 4.2.0.4, 4.2.1.3	4.2.0.1, 4.2.0.2, 4.2.0.3, 4.2.0.4, 4.2.1.3	5.0(3)N2(2a), 5.0(3)N1(1b)

## References

Fibre Channel over Ethernet Initialization Protocol, Cisco,  
[http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/white\\_paper\\_c11-560403.html](http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/white_paper_c11-560403.html)

T11/08-264v0 FCoE: Increasing FCoE Robustness using FIP Snooping and FPMA, T11,  
<http://www.t11.org/ftp/t11/pub/fc/bb-5/08-264v0.pdf>

T11/09-291v0 FIP VLAN discovery updates, T11,  
<http://www.t11.org/ftp/t11/pub/fc/bb-5/09-291v1.pdf>

IEEE. (2008, November 24). 802.1Qaz/D0.2. Draft Standard for Local and Metropolitan Area Networks - Virtual.

IEEE. (2009, Feb 9). 802.1Qbb/D1.0. Draft Standard for Local and Metropolitan Area Networks - Virtual.

Cisco Systems, Inc. (2011). *Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide, Release 5.0(3)N2(1)*. San Jose: Cisco Systems, Inc.

## About Dell

Dell (NASDAQ: DELL) is a leading technology provider to commercial and public enterprises around the world.