Dell Compellent Storage Center Switch Connectivity

Best Practices

Document revision

Date	Revision	Comments	Author
8/10/09	A	Initial Release	BR

Contents

Document revision 3
Contents 4
General syntax 6
Conventions 6
Introduction 7
Purpose 7
Storage area network 8
Fibre Channel 8
Storage Center Front-End Ports 8
Primary and Reserve Front-End Ports 8
Fault domains with cluster controllers 9
Fabrics and zoning 9
Fabrics 9
Zones 9
Ethernet and iSCSI VLANS 10
VLANs with Storage Area Networks 10
Storage Center Front-End Ports 11
Primary and Reserve Front-End Ports 11
Fault Domains with cluster controllers 11
Cisco MDS Switches 12
Cisco Fibre Channel Switches 12
VSAN Technology 12
Default VSAN 12
Default Port State 13
Multi-Switch Fabric 13
ISL Trunk Mode 13
Switch Management Standalone 14
Switch Management Enterprise 14
Dell Compellent Storage Center 15
Storage Center Front-End Ports 15
Front-end Zoning 15
Multi-Path with Multi-Fabric 15
Best Practice Summary 16
Fibre Channel 16

Best Practice Summary 17
iSCSI and Ethernet *17*
Best Practice Summary 18
Jumbo Frame Notes *18*
Best Practice Summary 19
Replication with Remote Instant Replay *19*
Appendix 20
Appendix A 20
McData Fabric Switches 20
Abridged McData Information *20*
Appendix B 23
Brocade Fabric Switches 23
Abridged Brocade Information *23*
Appendix C 26
Glossary 26
Appendix D 28
Technical Support Information 28
Appendix Z 35
Complete Cisco switch configuration guide for installation. 35

Tables

Table 1. Document syntax 6

General syntax

Table 1. Document syntax

Item	Convention
Menu items, dialog box titles, field names, keys	**Bold**
Mouse click required	Click:
Command to run	# command
User Input	`Monospace Font`
User typing required	Type:
Website addresses	http://www.compellent.com
Email addresses	info@compellent.com

Conventions

Notes are used to convey special information or instructions.

Timesavers are tips specifically designed to save time or reduce the number of steps.

Caution indicates the potential for risk including system or data damage.

Warning indicates that failure to follow directions could result in bodily harm.

Introduction

Purpose

This document is intended to provide a general overview of switch connectivity to the Dell™ Compellent™ Storage Center™ SAN. Both Ethernet and Fibre Channel network switches will be discussed. In each given technology, the basic concepts will be discussed in relation to the storage centric nature of the Dell Compellent product. Examples given can be considered best practice for most cases under general use. However they are not to be considered the only possible solutions for storage connectivity. Each individual user will need to determine what their specific storage and connectivity needs are. Use this paper as a guide to deploy the specific topology needed to satisfy each unique customer's requirements.

The intended audience for this document is SAN administrators with a working knowledge of both iSCSI and Fibre Channel networks. The switch fabric discussed here will be Cisco centric with both FC and Ethernet. However all concepts will apply to any network that complies with the industry standards.

Storage area network

Fibre Channel

The Storage Center product serves up block level storage to hosts through the use of interconnecting switches. This allows for both the higher fan-out count and higher availability through clustered controllers. Without the use of a storage area network, you would be limited to direct connections. The Storage Center does support point-to-point connections. However this does not scale as well or have the high availability of the clustered controllers. For these reasons most Storage Centers are installed into a storage area network. A common term for this storage area network is a "fabric". In this paper the two terms may be used interchangeably. Hosts connect to the Storage Center through Fibre Channel Host Bus Adapters, iSCSI Host Bus Adapters or through standard Ethernet Network Interface Cards.

Storage Center front-end ports

The Dell Compellent Storage Center can be setup in a variety of different configurations. Network ports on the Storage Center are referred to as Front-End or Back End. Hosts connect to the controllers through the Front-End ports. The controllers connect to the physical disks through the Back End ports. Since a network can give the clustered controllers the most benefit, this paper will focus on a clustered Storage Center configuration.

Each controller has two or more ports connecting hosts. These are the Front-End ports. For the disk connectivity to the Storage Center there are Back End ports. Currently these back end ports are Fibre Channel or SAS. Back End ports are in their own private network from the controllers to the disk enclosures. Once these are cabled up, there are no further configuration tasks.

Primary and reserve front-end ports

The Front-End ports are used for host to storage connectivity. With the Storage Center today, these are either 4Gb/s Fibre Channel or 1Gb/s Ethernet. The Front-End ports work in pairs with the cluster configuration. Each primary port on a controller has a corresponding reserve port on the peer controller. This pairing of Front-End ports is referred to as a Fault Domain.

Fault domains with cluster controllers

The host has connectivity to the Storage Center cluster through one or more primary ports. During a firmware upgrade, controller reboot or hardware failure, the primary port to the host will go off line. The reserve port in the same fault domain will now assume the identity of the primary port. The host will see the connectivity stop for a brief time, and then receive an RSCN (Registered State Change Notification) from the fabric. This will tell the host to retry and then find the original connectivity now found on the reserve port in the fabric. This procedure is all handled by the fabric, HBA and driver. The OS will have little or no knowledge of the event (it may be logged or there may be a console message). The I/O continues on the reserve port until the event is finished or resolved. The administrator can now intervene to set the main I/O path back to the original primary port in the fault domain.

Fabrics and zoning

One or more switches connected together can be considered "one fabric". Within the fabric you can further partition with a function known as zoning. Zoning restricts communication within the network. Fibre Channel fabrics are partitioned off, or zoned in two basic ways. This fabric function segregates ports among themselves to isolate communication.

Fabrics

A fabric can consist of just one switch or many. They interconnect and can interact as one larger virtual switch. The host sees only a fabric and is not aware of how many switches are involved. All inter-switch routing is done by the fabric services and no manual intervention is required. There are also newer technologies that will allow communications between fabrics. This like-IP routing would be a manual configuration. These technologies will not be discussed in this paper.

Zones

Within the fabric it will become necessary to restrict communications between ports. This is done through the use of Fibre Channel zoning. A zone will isolate traffic by means of a port address (hard zone) or by worldwide name used on the device itself (soft zone). Either method will restrict fibre channel frames to within the defined zone. Each vendor may have slight differences in implementing these methods but the overall operation is the same.

Since block level storage over a network is an extension of the SCSI protocol from the host to the LUN, zoning prevents one host from interfering with another host. A zone with each host port to one Storage Center cluster is a recommended best practice. Each host only knows of one target to communicate with. Even though all hosts have the Storage Center ports in common, fabric services still isolate all hosts. With this scenario the host has a private connection to a public device with the same security as a dedicated SCSI cable.

Ethernet and iSCSI VLANS

Ethernet networks have many similar characteristics to Fibre Channel along with others that are unique. Ethernet evolved with different designs and uses. Gigabit Ethernet can be used for Storage Area Network the same as Fibre Channel. However there are differences in technology that need to be considered.

Like the Fibre Channel fabric, the Gigabit Ethernet network (or fabric, since storage is the primary use here) can consist of one or many switches. They interconnect in a similar manner. The two major differences of the topologies are the native speed and the partitioning used. Today the majority of Ethernet is still 1Gb/s with 10Gb/s still in early adoption. Contrast that with the majority of Fibre Channel using 2G/s or 4Gb/s links.

VLANs with storage area networks

As with Fibre Channel, there is typically a need to control communication with the network. The partitioning commonly used for Ethernet networks is a method of segmenting the broadcast domain. This is defining the network boundaries. This is either physical or using a virtual local area network or VLAN. The major advantage of Gigabit Ethernet is the ubiquitous nature of the technology which in turn gives it the much lower cost of implementation. This is quite different from Fibre Channel in that you are not isolating host to storage but a group of hosts to storage. This technology is not as granular as Fibre Channel zoning. All ports in the network or virtual network can communicate with each other. The upper layer iSCSI protocols take this into account and can be used to control node communication.

Each vendor may have slightly different methods of implementing VLAN technology. They all operate similar in theory. With VLANs you can separate networks. The data network can be separate from the storage network. For most host storage this will be a flat network connection from HBA to Storage Center without any gateway. Storage traffic can be routed off the flat network, however this may affect performance. All of the management techniques used for the data network do apply to the storage network. The administrator should realize that the storage network is being used in a different fashion that the data network and manage it accordingly.

Storage Center front-end ports

The Storage Center iSCSI ports are Gigabit Ethernet and can be setup in a host facing Front-End configuration only. The Back End port configuration is the same for either an iSCSI Front-End or a Fibre Channel Front-End. Both types of systems talk to the physical disks in the same fashion. Again, the network will give the Storage Center controllers more flexibility so we will focus on that configuration.

Primary and reserve front-end ports

The Front-End is configured in the same manor with iSCSI as with Fibre Channel. The Front-End ports work in pairs with the controller cluster configuration. Each primary port on a controller has a corresponding reserve port on the peer controller. This pairing of Front-End ports is referred to as a Fault Domain.

Fault domains with cluster controllers

As with Fibre Channel, the host has connectivity to the Storage Center cluster through one or more primary ports. During a firmware upgrade, controller reboot or hardware failure, the primary port to the host will go offline. The reserve port in the same fault domain will now assume the identity of the primary port. The high level operation is similar to Fibre Channel failover, but the mechanics underneath are very different. With Ethernet, there will be more host software involved with no network services providing feedback of the event. The host's network software stack will see that the communication to the Storage Center has abruptly ended a session. The host will rebroadcast on the network to find the original port. The reserve port in the fault domain will now have the primary's address. The host will find the same address now on a different physical network port and continue communications. The OS will have little or no knowledge of the event. The HBA and the network driver should be handling this procedure.

Cisco MDS switches

Cisco Fibre Channel switches

The following section will give some examples of switch configuration examples using the Cisco 91xx series of MDS switches with the Storage Center. These are intended to be followed as a guide and not an exact step by step manual. This document will not explore every feature of the Cisco MDS Fibre Channel switch. Each installation and site will have unique properties that must be taken into consideration. For those questions beyond this guide, further online help or phone help from Dell Compellent copilot may be required.

VSAN technology

With the MDS Fibre Channel switches, Cisco has the concept of a Virtual Storage Area Network with in the switch. This would be very similar to the VLAN concept used in Ethernet switches. The VSAN is a complete and isolated fabric which can be then partitioned down further with the use of zones. Like the fabric, the Cisco VSAN can be one or many switches. Also the switch or switches can contain many VSANs. It is up to the administrator to determine the method of implementing VSAN technology. Cisco also provides the method of routing between these VSANs with their IVR or Inter VSAN Routing. This can be a useful tool in merging exiting fabrics or migrating legacy equipment. The details of implementing IVR are beyond the scope of this document.

Default VSAN

The Cisco MDS switch will have a default VSAN, this will be VSAN 1. This is fully functional and could be used for production use. However it is considered a best practice to not use VSAN 1 and create another VSAN for production use. Any number between 2 and 4093 can be used. VSAN 1 must be available for the switch operating system to function. If there were ever a problem and the VSAN needed to be removed, VSAN 1 would not allow this. Whereas the next numbered VSAN could be deleted and then recreated to resolve the issue. This configuration can also add another layer of security since all ports by default will be in VSAN 1. The ports will be completely isolated until the administrator places the port in the proper VSAN for operation. This is a similar concept that is used with Cisco Ethernet switch and their VLAN numbering scheme.

Default port state

The port will have certain default configuration characteristics before the administrator intervenes. On initial configuration, the administrator is asked whether to allow the port to power on in the "enable" state or the "disable" state. For a matter of security, the default is a "disable" state. This means the administrator must enable the specific port before it can participate in the fabric. It must also be placed in the correct VSAN. Another layer of security is that the default zoning rules for new ports are to implicitly "deny all" communications to other ports. For the new port to communicate to any ports in the VSAN, it must be placed into a zone and the zone into the zoneset, and then the zoneset activated. These steps are by default and are in place for a higher level of security.

Multi-switch fabric

With the Cisco MDS switches there is no direct correlation between the VSAN and the physical switch. One switch can have several VSANs or many physical switches can just be one VSAN. When using multiple switches tied together, it can be advantageous to connect them with multiple links. As with Cisco's Ethernet technology, these links (or ISL's for Inter Switch Link) can be bundled together to have the aggregate bandwidth of all the links working together. The hosts and the Storage Center do not have any knowledge of the ISL's and treat the entire fabric as one switched entity.

When multiple ISL's are tied together, Cisco refers to this as a “port channel.” You can configure up to 16 individual links together to form a port channel. In most cases there are only two to three links used in the port channel. This port channel is treated as a physical interface. You can view statistics and configure the port channel as you would any physical interface. The multiple links also can provide for a higher availability of the ISL.

ISL trunk mode

The Fibre Channel ports can be configured in a variety of ways. If the port has a host or storage port connected, then the port is in "access" mode. When another switch is connected to that port, it is in "trunk" mode. With this trunk mode, you have the ability to either allow or deny any traffic from any VSAN you choose. In most cases you will allow every VSAN to propagate to every switch. This can be done by naming the specific VSAN numbers or by stating "allow VSAN all".

Switch management standalone

The Cisco switches can be managed from the command line on a switch-by-switch basis. Most administrators will choose not to use this method exclusively. There are two GUI based products used to manage the switches, Device Manager and Fabric Manager.

The individual physical switches are managed by Device Manager. The administrator points a browser to the switch IP address and the switch will install a Device Manager applet. If Java is not installed yet, the administrator will be prompted to do so. For VSAN and zone management, the GUI product is Fabric Manager. This is a Java based application that must be installed from a separate CD. The workstation at which the install takes place will have a database to correspond to the configuration of the fabric. Each of these management applications follows the version of firmware on the switch. So if the firmware is upgraded, you may be prompted to upgrade your management applet. You can manage switches from an offset of one or two revisions, but in a major revision difference, there may be some key elements missing. Therefore it is best practice to keep your management programs at the same revision level as the switch firmware.

When managing multiple switches in the fabric, one switch should be designated as the "seed" switch. Even though all the switches are peers in the fabric, this seed switch will be the main contact into the fabric. There should only be one administrator managing the fabric at a time. After each configuration change, the administrator should distribute the database to all switches and save the configurations of each switch. Also the configuration can be copied off to a TFTP server or FTP server for archive. In that manor the site is protected against power failure or device failure.

Switch management enterprise

In larger accounts, there will be the need to have multiple administrators from many different client stations. To address this requirement, Cisco has Fabric Manager Enterprise Edition. This application can be installed on a separate server and then the administrators will connect as clients to this installation. The database for the fabric and its configuration will now be in one place with proper file and configuration locking to accommodate multiple administrators. This should be a separate server for this dedicated application. It does not however have to be a physical server and can be run in a virtual server environment. At this level a complete change level log and history should be implemented. With many switches and administrators involved each change does have a potential for disruption. Each installation will need to evaluate how they approach these challenges.

Dell Compellent Storage Center

Storage Center front-end ports

The Storage Center front-end ports and used to communicate to the hosts on the SAN needing storage. In a clustered Storage Center configuration there will be at a minimum 4 total front-end ports. There will be 2 ports from each controller, 1 primary and 1 reserve for a total of 4. All 4 of these ports are paired up for operation. Therefore they all must reside in the same VSAN. If more front-end ports are used, typically these are place into the second fabric. In the case of Cisco, these ports will be placed into a second VSAN.

Front-end zoning

All the front-end ports should be placed into a Storage Center zone. This zone will be used by Storage Center to help determine the health and status of each controller. Each host which requires storage from Dell Compellent should have its own zone. The host need only see the Front-end primary ports. However, in most cases it does not affect operation if all primary and reserve ports are in the host zone. Within the zone, the host port and the Storage Center front-end ports should reside. This can be done manually for each host or the administrator can create an alias for the Storage Center and put the host in a zone with the alias. This is an administrator preference and not a technical one.

Multi-path with multi-fabric

The purpose of clustered Storage Center controllers and dual fabrics (or two VSANs) is to provide higher availability of storage to the host. If the Storage Center has 8 front-end ports, 4 in each VSAN or fabric, then the host can have two connections to storage. This will provide redundant paths to storage. If there were to be an issue with one fabric or VSAN, the host is still able to access storage from the other path. The two paths to storage must be managed by the driver and or the operating system on the host. Configuration of multi-path I/O to storage is operating system specific. Refer to your OS vendor for details.

Best practice summary

Fibre Channel

Each switch vendor may implement features unique to their specific model. Below are some general guidelines to follow when implementing a Fibre Channel network. Each tip may or may not apply to a specific installation. Be aware that this is not an all-inclusive list.

- The Dell Compellent Storage Center Front-End ports should reside in their own zone for inter controller communications. This includes both the Primary ports and the Reserve ports together. This should be independent of the host zones. Hard (port zone) zoning is recommended here but soft zoning will also work.
- Upon initial installation, all Front-End ports must see each other. If the WWN is not known to the switch, a hard zone may be required at startup.
- Hard zoning or soft zoning is an administrative preference. The Storage Center will operate in either switch environment.
- Create an Alias of the Storage Center Front-End ports.
- Zone each host individually with the Storage Center Front-End Alias. Cisco can use soft or hard zoning together. The host can be WWN or switch port.
- Each port within a host should be in a separate zone. Certain cluster technologies may be the only exception. This may require all host ports to be in one zone. Consult OS vendor or Co-Pilot.
- Keep consistent on the zone type and naming convention.
- Always create new VSAN for production. VSAN 1 is then used for management tasks.
- For higher availability use isolated dual fabrics or VSANs. Implement Multi-Path I/O from hosts.
- Leave the default Cisco zoning policy to deny port communications.
- Always manage the Cisco fabric from the same switch. This will give Fabric Manager the same consistent view of the fabric each session.
- Oversubscription ratio can vary greatly depending on server I/O load. Each installation should monitor both storage utilization and switch port utilization.
- Inter switch links (ISLs) should be at least two, for redundancy and bandwidth. ISLs can be added as more bandwidth is needed.
- ISLs should be bundled together into a port channel.

Best practice summary

iSCSI and Ethernet

Each manufacturer of Gigabit Ethernet switch may implement features unique to their specific model. Below are some general tips to look for when implementing an iSCSI network infrastructure. Each tip may or may not apply to a specific installation. Be aware that this is not an all-inclusive list.

- Bi-Directional Flow Control enabled for all Switch Ports that carry iSCSI traffic, including any inter switch links.
- Separate networks or VLANs from data.
- Separate iSCSI traffic multi-path traffic also.
- Unicast storm control disabled on every switch that handles iSCSI traffic.
- Multicast disabled at the switch level for any iSCSI VLANs.
    - Multicast storm control enabled (if available) when multicast cannot disabled.
- Broadcast disabled at the switch level for any iSCSI VLANs.
    - Broadcast storm control enabled (if available) when broadcast cannot disabled.
- Routing disabled between regular network and iSCSI VLANs.
    - Use extreme caution if routing any storage traffic, performance of the network can be severely affected. This should only be done under controlled and monitored conditions.
- Disable Spanning Tree (STP or RSTP) on ports which connect directly to end nodes (the server or Dell Compellent controller's iSCSI ports.) If you must use it, enable the Cisco PortFast option on these ports so that they are configured as edge ports.
- Ensure that any switches used for iSCSI are of a non-blocking design.
- Hard set for all switch ports and server ports for Gigabit Full Duplex if applicable.
- When deciding which switches to use, remember that you are running SCSI traffic over it. Be sure to use a **quality managed enterprise class** networking equipment. It is not recommended to use SBHO (small business/home office) class equipment outside of lab/test environments.

Best practice summary

Jumbo Frame notes

Be aware that enabling Jumbo Frames will not automatically improve network performance. It will improve certain types of data transfer that will take advantage of the 9K frame size. The type of storage I/O on the network, network interface cards, NIC driver and switch type all can determine the performance of an iSCSI network. Jumbo Frames is just one part of an overall network configuration.

- Some switches have limited buffer sizes and can only support Flow Control or Jumbo Frames, but not both at the same time. Dell Compellent strongly recommends choosing Flow Control.
- **All** devices connected through iSCSI network need to support 9k Jumbo Frames to take full advantage of it.
    - This means **every** switch, router, WAN Accelerator and any other network device that will handle iSCSI traffic needs to support 9k Jumbo Frames.

- If the customer is not **100%** positive that every device in their iSCSI network supports 9k Jumbo Frames, then they should NOT turn on Jumbo Frames.
- QLogic 4010 series cards (Early Dell Compellent iSCSI Cards) do not support Jumbo Frames.
    - In the Storage Center GUI default screen, expand the tree in the following order Controllers->SN#(for the controller)->IO Cards->iSCSI->Highlight the port and the general tab should list the model number in the description.

- Because devices on both sides (server and SAN) need Jumbo Frames enabled, the change to enable to disable Jumbo Frames is recommended during a maintenance window. If servers have it enabled first, the Storage Center will not understand their packets. If Storage Center enables it first, servers will not understand its packets.

Best practice summary

Replication with remote instant replay

There are two types of replication between systems, Synchronous and Asynchronous. With Sync replication, all writes at the primary site must be written at the secondary site before the host is given the Acknowledgement that the data has been placed on disk. Therefore the network speed between Sync replicating systems should be line speed. This would mean 1 Gigabit per second or higher. Slower speeds can work, but the host will wait longer for the write Ack. This will affect performance and may not be acceptable.

Async replication is a Storage Center feature that can be used over slower communication links. It will also work well over faster links as well. The amount of data changing and the time to recovery are the limiting factors to how well the solution will work. If the site has very little data changing from hour to hour or day to day, a very slow link can keep the sites mirrored. There will be some time delay between mirror copies; this is the period of time in which data may be risk. This is where replication and recovery planning must take place. Each customer will need to evaluate their uptime needs. The longer the time that is tolerated, the slower the communication link can be. If less time is tolerated, then a faster and more expensive communication link must be in place. The Storage Center is very flexible and can be configured to meet the specific business requirements of the end user.

- Have a comprehensive plan on replication and recovery from the remote site.
- Test recovery procedures after any changes to the environment.
- Monitor link between sites for utilization.
- With Fibre Channel, have all Storage Center Front-End ports from both systems in one zone.
- With iSCSI be sure proper routing is in place between sites. If using NAT, use the properties/advanced tab to input the IQN of the target system.
- Under properties/advanced adjust the Window size to link speed. Slower links use small size, faster can use larger size window.
    - Adjust size to link. If a WAN accelerator is used, adjust size of window to the accelerator box and let that appliance handle the speed of the WAN link.

- Latency can have a dramatic effect on any applications using remote storage. Anything less than LAN/SAN speed should be thoroughly tested.
- Synchronous replication should be site, campus or metro centric. Write latency will be a factor with some applications not tolerant of longer times.
- Network health monitoring from each site will help guide design decisions. Real time statistics will tell the administrator what type of replication to use and how to configure it.

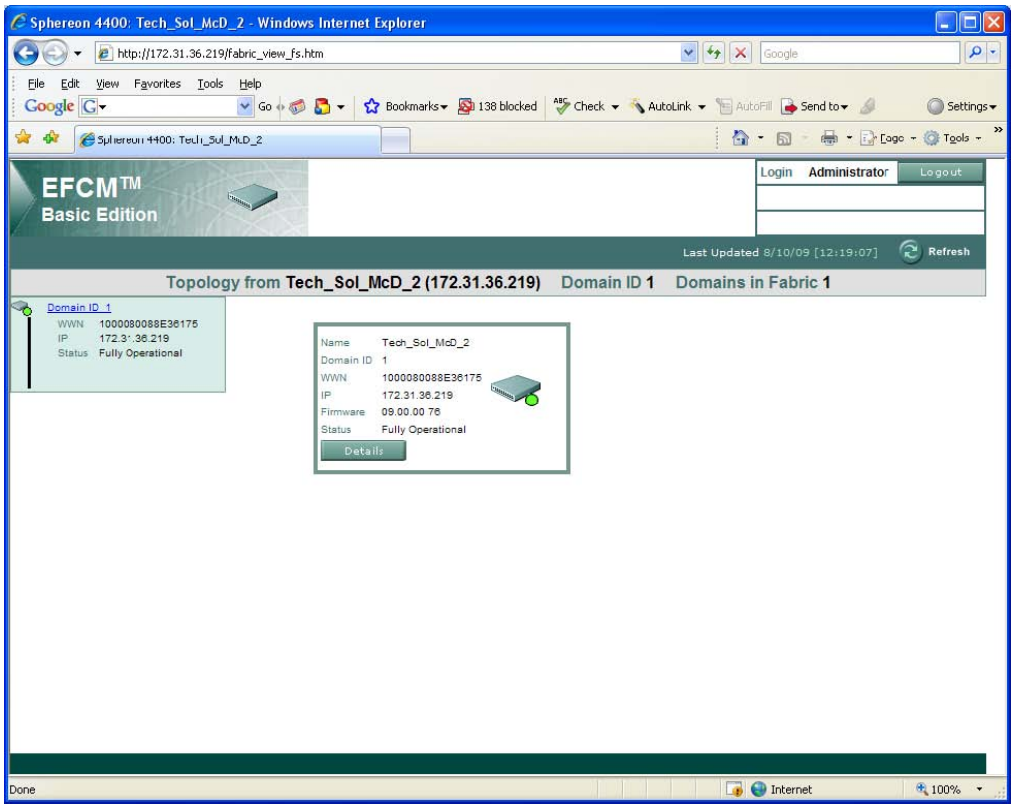
Appendix

Appendix A

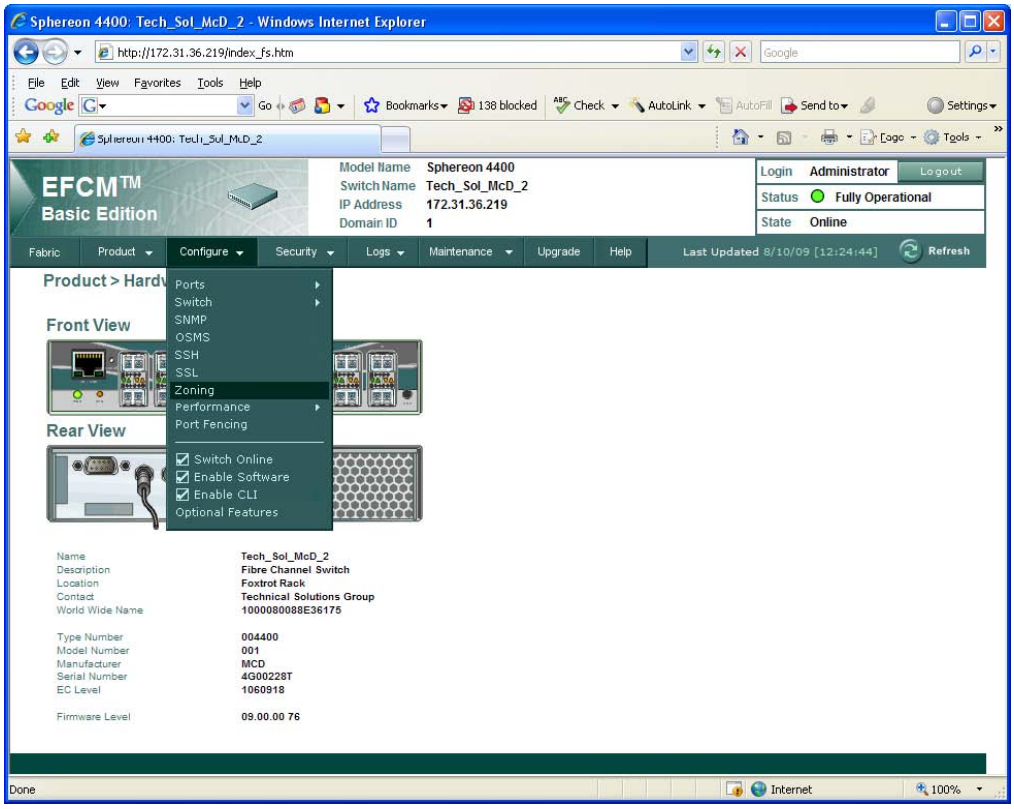
McData fabric switches

Abridged McData information

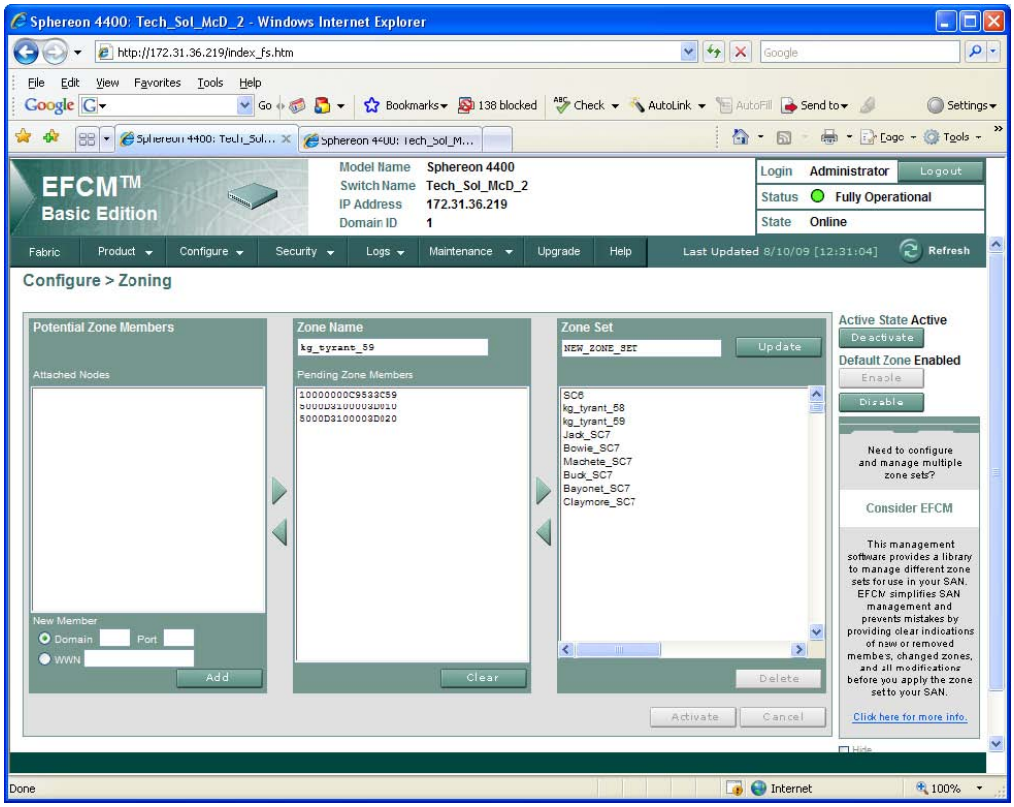
The following is a few screen examples from a McData switch. Refer to copilot for complete McData information. Switch administration with McData is done thru a standard browser to the IP address of the switch. Enterprise Fabric Connectivity Manager (EFCM) is the imbedded program for managing the switch.



Port and switch information is listed under the details tab.
Under Configure you will find the zoning tab.



From this screen is where you can choose hard zone (domain and port) or soft zone (WWN). The zone is created and placed in a zoneset. When the zoneset is activated, the zoning is live on the switch.

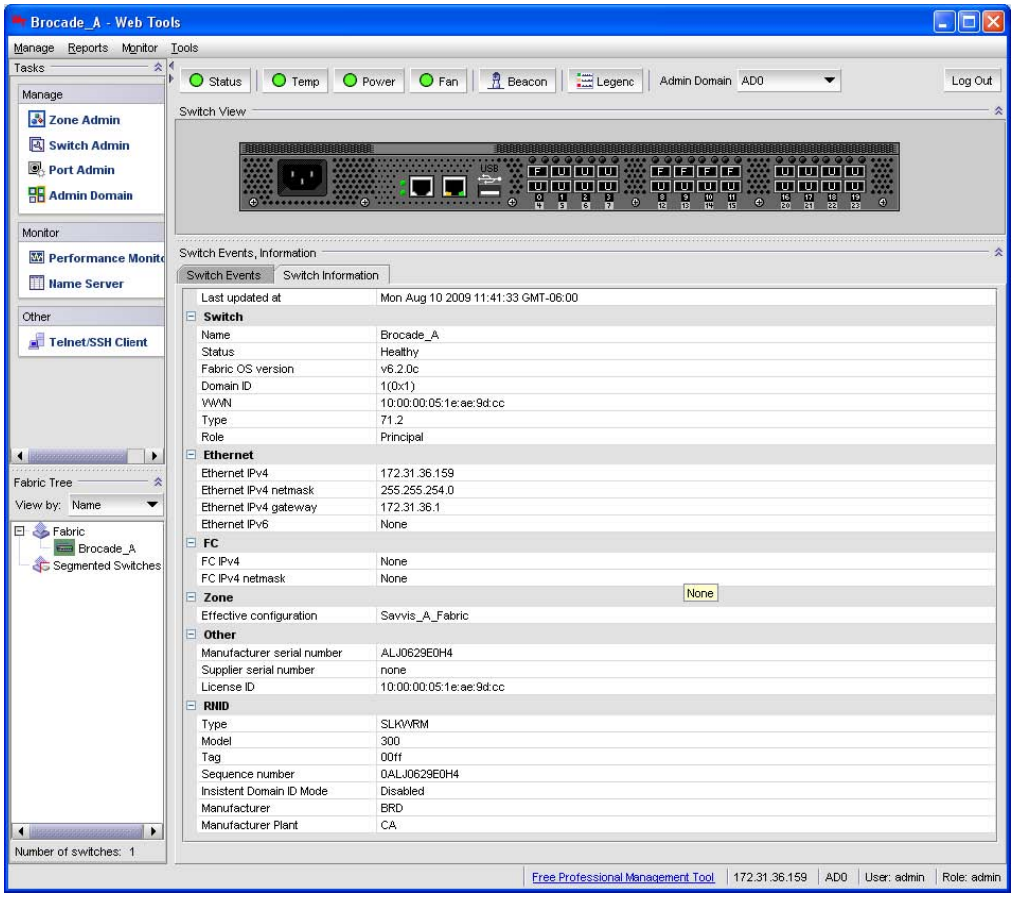


Appendix B

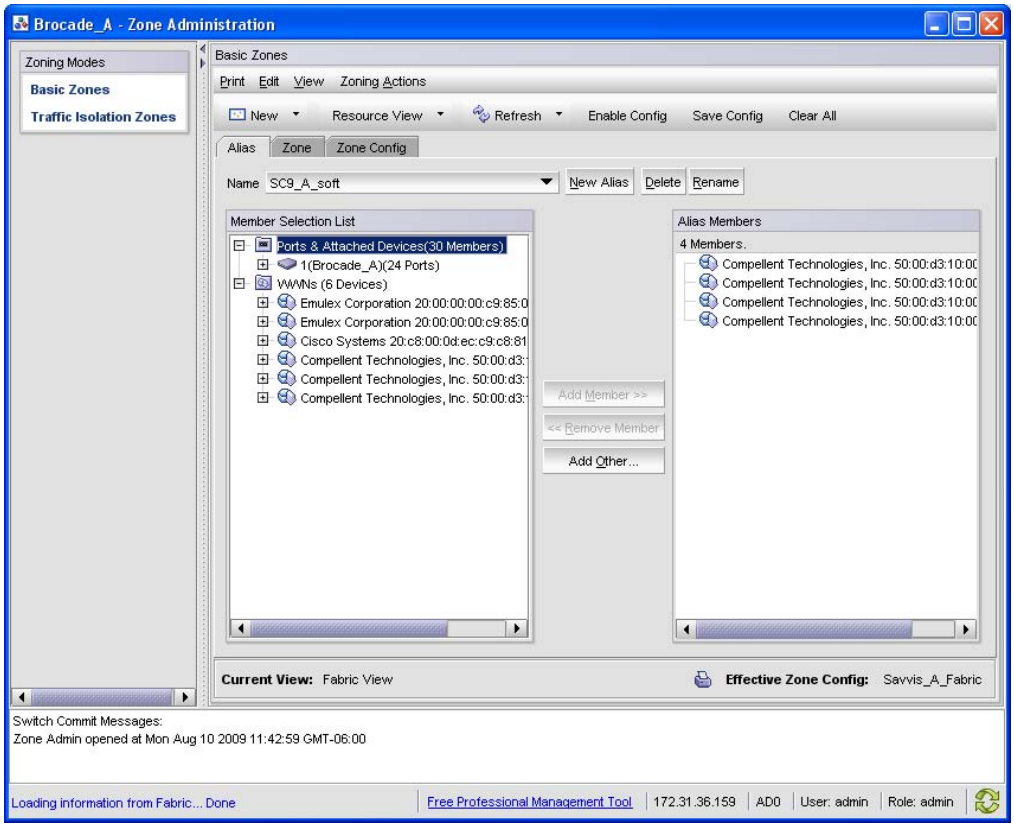
Brocade fabric switches

Abridged Brocade information

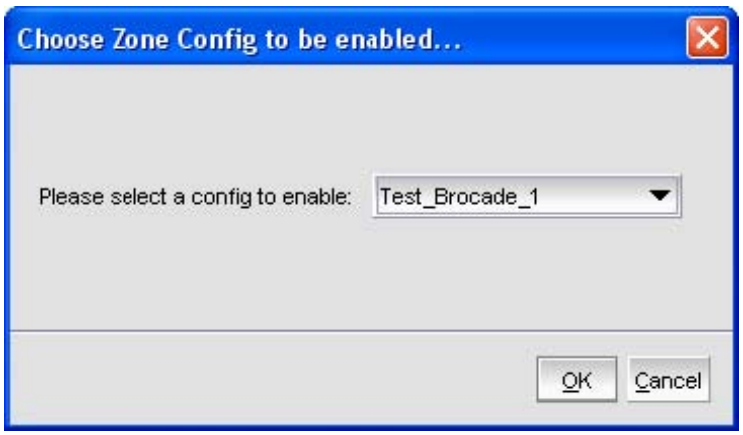
The following is a few screen examples from a Brocade switch. Refer to copilot for any additional Brocade information. Switch administration with Brocade is done thru a standard browser to the IP address of the switch. Brocade Web Tools is the java based program for managing the switch.



Under the zoning tab, the administrator has the choice of hard zoning (ports) or soft zoning (WWNs). The administrator creates zones into which the ports or WWNs are inserted. Then a Zone Config is created, this is analogous to a zoneset with Cisco or McData.



With zones in the Zone Config, you must enable the config (activate zoneset with the other brands). It is best practice to save the config should you lose power.



Additional Brocade information:

On initial install on a Dell Compellent Storage Center and a Brocade Fibre Channel switch, be aware of the following. This statement depends upon the Brocade switch model and FOS, Fabric Operating System. It has been a common question for the Dell Compellent copilot support team. Brocade and Storage Center firmware versions do factor into the following statements. If the administrator observes suspect behavior, gather revision information and contact copilot for further direction.

> "Many Brocade Switches will not recognize Dell Compellent Ports when they are first plugged in. They will show as down, even when plugged in and turned on. In order for the Dell Compellent Ports to be seen, please Port Zone all of the Dell Compellent Ports together. The Dell Compellent Ports will then log in to the switch and the switch will now recognize their WWNs. If you will be port zoning the switch, no further work is needed. If WWN zoning is desired, you can now create a WWN Zone and delete the initial Port Zone. The Port Zone was only needed for initial recognition."

If hard port zoning is not possible, the WWN of each Front-End port of the Storage Center can be derived from the management GUI and input into a soft zone in the Brocade. The SAN administrator would then need to create a soft zone and input the WWN from each Front-End port and put that new zone into the config and then enable the config for the Storage Center to fully initialize into a dual controller system. Assistance on this procedure can be obtained from Dell Compellent copilot.

Also with Brocade switches, it has been noted that Storage Center installation into an existing fabric with certain features enabled may be an issue.

> Be aware that inband Management Server Topology Discover should be disabled on the Storage Center switch. On default installation, this will be disabled. However if it was enabled at some point, this may cause issues on installation. To view status, from the CLI, mstdreadconfig will list the status of this feature. The CLI command mstddisable will turn this feature off.

Appendix C

Glossary

Arbitrated Loop - a Fibre Channel topology where information is routed around the loop from port to port until it arrives at its destination. This is a private loop configuration.

Back End Ports - Disk facing communication ports from the Storage Center. These ports are on a private network that only the controllers and disk enclosures share. These are Fibre Channel ports.

Cascading - an interconnection of individual switches used to create larger Fabric configurations.

Domain - the first field of the 3-byte address assigned to an attached N_Port in a Fabric configuration. The domain is generally associated with an instance of the switch.

E-port - A connection that links multiple Fibre Channel fabrics.

F_Port - (Fabric Port) - a port within the Fabric used to route frames from N_Port to N_Port. The F_Port is the access point to a Fibre Channel switch.

Fabric - a term used to describe an interconnection of Fibre Channel host ports, device ports and switch ports where frames from a source N_Port are routed through a switch (Fabric) to a destination N_Port based on the frame's destination address.

FC adapter - Fibre Channel adapter or host bus adapter (HBA). A Fibre Channel I/O bus adapter board operates from 1Gb/s, up to 8Gb/s.

FC-AL - (Fibre Channel Arbitrated Loop) - the ANSI standard that describes how several Fibre Channel ports can share a single communication ring.

FC-SW - (Fibre Channel Switch Fabric) - the standard that describes how Fibre Channel switches are required to behave.

FC switch - Fibre Channel switch. Intelligently manages connections between ports, routing frames dynamically. A non-blocking topology, it allows multiple exchanges of information to occur at the same time between ports. A switch offers better system throughput than a hub, but at greater expense. Some switches have a special FL-port to link arbitrated loops and other devices on the switch. By cascading multiple switches, more than 16 million devices can be connected together.

Frame - Data packet, a unit of data transmitted within a Fibre Channel system.

Front-End Ports - Host facing communication ports from the Storage Center. These are either Fibre Channel or iSCSI Ethernet.

Hard Zone - Using the physical ports of the switch grouped together for Fibre Channel communication. Different vendors will use different terms when defining the physical port of the switch. With hard zoning, whatever devices are plugged into those ports can participate and communicate within the zone. The switch does not look at any soft addressed with this method.

LIP - (Loop Initialization Primitive) used to initiate a procedure on the loop. This initialization state usually causes activity on the loop to suspend briefly. It can be caused by new devices being added or moved on the loop, arbitrated loop address assignment, recovery from loop failure, or resetting a node.

LRC - Loop Resiliency Circuit. Hub circuitry that allows devices to be inserted into or removed from an active FC-AL loop.

N_Port - a node port (or device port) used to route information to or from other nodes or to devices. The N_Port is the access point to a Fibre Channel adapter.

Node - Device connected to a Fibre Channel fabric, possibly a PC, disk drive, or RAID array, as well as an FC-AL.

Point to Point - Fibre Channel direct connection topology between N_Ports. Typically a server directly connected to a storage array.

Port - the third field of the 3-byte address assigned to an attached N_Port in a Fabric configuration. The port is generally associated with the Hard Physical Address (HPA) of a Fibre Channel target device.

SAN - Storage Area Network. A centralized storage repository that provides physical security in an environmentally regulated location. The data in a SAN can be easily managed (i.e., backed up regularly, etc.) and is protected from equipment, software, and procedural failures

Soft Zoning - Using the device address of who is plugged into a physical port for Fibre Channel communication. With soft zoning, the switch looks to the address of the device attached to determine who it can talk to. All addresses listed within the zone can communicate regardless of where they are physically plugged in. With this method, the device can move to any physical port in the fabric and the zone is still valid.

Zoning - a logical grouping of Fabric-attached devices that are isolated from other devices and other zones by the switch. Whether using soft zoning or hard zoning, it is more of an administrative preference rather than a technical one. There are advantages and disadvantages of each.

Appendix D

Technical support information

To gather switch information for support personal, several methods may be used. The command line is one way to do this but is not the only method. A telnet or ssh session to the CLI of the switch can gather the needed information in text form. Each utility will have a slightly different method of capture. In some cases, an ftp server may come into play to gather and save off large files of configuration information. Below are some examples of information gathering.

Zone information:

Cisco>show zoneset
Brocade>zoneshow

Port information:

Cisco>show interface fc1/1 (fibre channel slot# / port#)
Brocade>portshow 2/1 (slot# / port#)

Full configuration:

Cisco>show tech-support brief (many options, no brief option give all info)
Brocade>supportshow (gives everything to the console)
Brocade>supportsave (sends all info to ftp server)

Cisco Examples:

```
Cisco-FC-Foxtrot# show zoneset
zoneset name Tech_Sol_set1 vsan 1
 zone name Comp_864-865 vsan 1
  fcalias name SC05_Soft_Full vsan 1
   pwwn 50:00:d3:10:00:03:60:01
   pwwn 50:00:d3:10:00:03:60:05
   pwwn 50:00:d3:10:00:03:60:09
   pwwn 50:00:d3:10:00:03:60:0d

zone name JB_Fury vsan 1
    interface fc1/1 swwn 20:00:00:0d:ec:49:49:80
  fcalias name SC05_Soft_Full vsan 1
   pwwn 50:00:d3:10:00:03:60:01
   pwwn 50:00:d3:10:00:03:60:05
   pwwn 50:00:d3:10:00:03:60:09
   pwwn 50:00:d3:10:00:03:60:0d

Cisco-FC-Foxtrot# show interface fc1/4
fc1/4 is down (Administratively down)
  Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
  Port WWN is 20:04:00:0d:ec:5b:ec:80
  Admin port mode is auto, trunk mode is on
  snmp link state traps are enabled
  Port vsan is 1
  Receive data field Size is 2112
  Beacon is turned off
  Belongs to port-channel 6
  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
   40535855641 frames input, 53391442268800 bytes
    0 discards, 0 errors
    0 CRC, 0 unknown class
    0 too long, 0 too short
   35715702204 frames output, 52998888998672 bytes
    1 discards, 0 errors
   1 input OLS, 1 LRR, 0 NOS, 6 loop inits
   1 output OLS, 1 LRR, 1 NOS, 1 loop inits
```

Cisco-FC-Foxtrot# show tech-support brief
Switch Name : Cisco-FC-Foxtrot
Switch Type
Kickstart Image : 4.1(3a) bootflash:/m9100-s2ek9-kickstart-mz.4.1.3a.bin
System Image : 4.1(3a) bootflash:/m9100-s2ek9-mz.4.1.3a.bin
IP Address/Mask : 172.31.37.246/23
IP Address/Mask : 172.31.37.246/23
Switch WWN : 20:00:00:0d:ec:5b:ec:80
No of VSANs : 2
Configured VSANs : 1-2

VSAN 1: name:VSAN0001, state:active, interop mode:default domain id:0x35(53), WWN:20:01:00:0d:ec:5b:ec:81 active-zone:size:, default-zone:deny

VSAN 2: name:VSAN0002, state:active, interop mode:default domain id:0x83(131), WWN:20:02:00:0d:ec:5b:ec:81 active-zone:size:, default-zone:deny

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/1	1	auto	on	trunking	swl	TE	4	6
fc1/2	1	auto	on	trunking	swl	TE	4	6
fc1/3	1	auto	on	trunking	swl	TE	4	6
fc1/4	1	auto	on	down	swl	--	6	
fc1/5	1	auto	on	trunking	swl	TE	4	10
fc1/6	1	auto	on	trunking	swl	TE	4	10
fc1/7	1	auto	on	trunking	swl	TE	4	20
fc1/8	1	auto	on	trunking	swl	TE	4	20
fc1/9	1	auto	on	down	swl	--	--	
fc1/10	1	auto	on	down	swl	--	--	
fc1/11	1	auto	on	down	swl	--	--	
fc1/12	1	auto	on	down	swl	--	--	
fc1/13	1	auto	off	down	swl	--	--	
fc1/14	1	auto	off	down	swl	--	--	
fc1/15	1	auto	off	down	swl	--	--	
fc1/16	1	auto	off	down	swl	--	--	
fc1/17	2	auto	off	notConnected	swl	--	--	
fc1/18	2	auto	off	notConnected	swl	--	--	
fc1/19	1	auto	off	notConnected	swl	--	--	
fc1/20	1	auto	off	notConnected	swl	--	--	
fc1/21	1	auto	off	up	swl	F	4	--
fc1/22	1	auto	off	up	swl	F	4	--
fc1/23	2	auto	off	up	swl	F	4	--
fc1/24	2	auto	off	up	swl	F	4	--
fc1/25	1	auto	on	trunking	swl	TE	4	15
fc1/26	1	auto	on	trunking	swl	TE	4	15
fc1/27	1	auto	on	trunking	swl	TE	4	15
fc1/28	1	auto	on	trunking	swl	TE	4	15
fc1/29	1	auto	on	trunking	lwcr	TE	4	99

Brocade examples:

```
VS1:FID1:admin> zoneshow
Defined configuration:
  cfg: xavvis_A_Fabric
          Blazer_2; Challenger_A_1; Charger_A_1; KG_Barron_A;
          KG_Filet_2; KG_Kabar_2; KG_Tyrant_A; KG_Tyrant_SC03; SC9_A
  zone: Blazer_2
          20:00:00:0d:60:d3:cd:67; 50:00:d3:10:00:00:65:00;
          50:00:d3:10:00:00:65:01; 50:00:d3:10:00:00:65:02
  zone: Challenger_A_1
          20:00:00:00:c9:85:02:5c; SC9_A_soft
  zone: Charger_A_1
          20:00:00:00:c9:85:08:c0; SC9_A_soft
  zone: KG_Barron_A
          20:00:00:00:c9:72:fa:9f; 50:00:d3:10:00:00:65:00;
          50:00:d3:10:00:00:65:01; 50:00:d3:10:00:00:65:02
  zone: KG_Barron_SC3
          20:00:00:00:c9:72:fa:9f; 50:00:d3:10:00:03:8e:07;
          50:00:d3:10:00:03:8e:08; 50:00:d3:10:00:03:8e:13;
          50:00:d3:10:00:03:8e:14
  zone: KG_Filet_2
          20:01:00:e0:8b:bb:25:41; 50:00:d3:10:00:00:65:00;
          50:00:d3:10:00:00:65:01; 50:00:d3:10:00:00:65:02
  zone: KG_Kabar_2
          20:01:00:1b:32:25:98:9c; 50:00:d3:10:00:00:65:00;
          50:00:d3:10:00:00:65:01; 50:00:d3:10:00:00:65:02
  zone: KG_Tyrant_A
          20:00:00:00:c9:53:3c:58; 50:00:d3:10:00:00:65:00;
          50:00:d3:10:00:00:65:01; 50:00:d3:10:00:00:65:02
  zone: KG_Tyrant_SC03
          20:00:00:00:c9:53:3c:58; 50:00:d3:10:00:03:8e:07;
          50:00:d3:10:00:03:8e:08; 50:00:d3:10:00:03:8e:13;
          50:00:d3:10:00:03:8e:14
  zone: SC9_A SC9_A_soft
  zone: SC9_A_hard
          1,8; 1,9; 1,10; 1,11
  alias: SC9_A_soft
          50:00:d3:10:00:00:65:0b; 50:00:d3:10:00:00:65:0c;
          50:00:d3:10:00:00:65:1b; 50:00:d3:10:00:00:65:1c

Effective configuration:
  cfg: xavvis_A_Fabric
  zone: Blazer_2
          20:00:00:0d:60:d3:cd:67
          50:00:d3:10:00:00:65:00
          50:00:d3:10:00:00:65:01
          50:00:d3:10:00:00:65:02
```

```
zone: Challenger_A_1
          20:00:00:00:c9:85:02:5c
          50:00:d3:10:00:00:65:0b
          50:00:d3:10:00:00:65:0c
          50:00:d3:10:00:00:65:1b
          50:00:d3:10:00:00:65:1c

VS1:FID1:admin> portshow 2/1
portName:
portHealth: OFFLINE

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x1  PRESENT U_PORT
portType: 17.0
portState: 2 Offline
Protocol: FC
portPhys: 4  No_Light     portScn: 2 Offline
port generation number: 0
state transition count: 1

portId: 0bef80
portIfId: 43220039
portWwn: 20:41:00:05:1e:ac:36:01
portWwn of device(s) connected:

Distance: normal
portSpeed: N8Gbps

LE domain: 0
FC Fastwrite: OFF
Interrupts: 0       Link_failure: 0       Frjt: 0
Unknown: 0       Loss_of_sync: 0       Fbsy: 0
Lli:          2 Loss_of_sig: 2
Proc_rqrd: 0       Protocol_err: 0
Timed_out: 0       Invalid_word: 0
Rx_flushed: 0       Invalid_crc: 0
Tx_unavail: 0       Delim_err: 0
Free_buffer: 0       Address_err: 0
Overrun: 0       Lr_in: 0
Suspended: 0       Lr_out: 0
Parity_err: 0       Ols_in: 0
2_parity_err: 0       Ols_out: 0
CMI_bus_err: 0
```

```
VS1:FID1:admin> supportshow
\VF
==========================
Date:
Mon Feb 8 22:05:37 UTC 2010

Time Zone:
Time Zone Hour Offset: 0
Time Zone Minute Offset: 0

Version:
Kernel: 2.6.14.2
Fabric OS: v6.3.0
Made on: Wed Aug 19 18:40:41 2009
Flash:   Tue Jan 19 18:24:45 2010
BootProm: 1.0.15

supportshow groups enabled:
os        enabled
exception         enabled
port      enabled
fabric    enabled
services          enabled
security          enabled
network           enabled
portlog enabled
system  enabled
extend  disabled
filter    disabled
perfmon           disabled
ficon     disabled
iswitch enabled
asic_db           enabled
iscsi     enabled
fcip      enabled
ag        enabled
dce_hsl           enabled
crypto  disabled

**** Begin start_port_log_cmd group ****
Mon Feb 8 22:05:37 UTC 2010
portlogdump:
portlogdump:
CURRENT CONTEXT   0 , 128
/fabos/cliexec/portlogdump:
```

```
VS1:FID1:admin> supportsave
This command collects RASLOG, TRACE, supportShow, core file, FFDC data and other support
information from both active and standby CPs and then transfer them to a FTP/SCP server or a USB
device. Local CP, remote CP and BPs' information will be saved, but supportShow information is
available only on the Active CP. This operation can take several minutes.
NOTE: supportSave will transfer existing trace dump file first, then automatically generate and transfer
latest one. There will be two trace dump files transferred after this command. OK to proceed? (yes, y,
no, n): [no] y

Host IP or Host Name: 172.31.37.52
User Name: user
Password:
Protocol (ftp or scp): ftp
Remote Directory: /junk

Saving support information for chassis:Brocade_DCX4S, module:RAS
.........
Saving support information for chassis:Brocade_DCX4S, module:CTRACE_OLD...
Saving support information for chassis:Brocade_DCX4S, module:CTRACE_NEW...
Saving support information for chassis:Brocade_DCX4S, module:FABRIC...
```

Appendix Z

Complete Cisco switch configuration guide for installation

Appendix Z is a step by step guide for a Cisco MDS 9124 switch installation. It is for example only and should be used as such. Each customer site will have different requirements to the configuration of the switches. The given example is from 3.x switch firmware. Most examples given will transcend the later revisions of Fabric Manager and switch firmware. Be aware there may be subtle differences in window pane or in feature set of the given revision.

Cisco MDS-9000 Switch Configuration

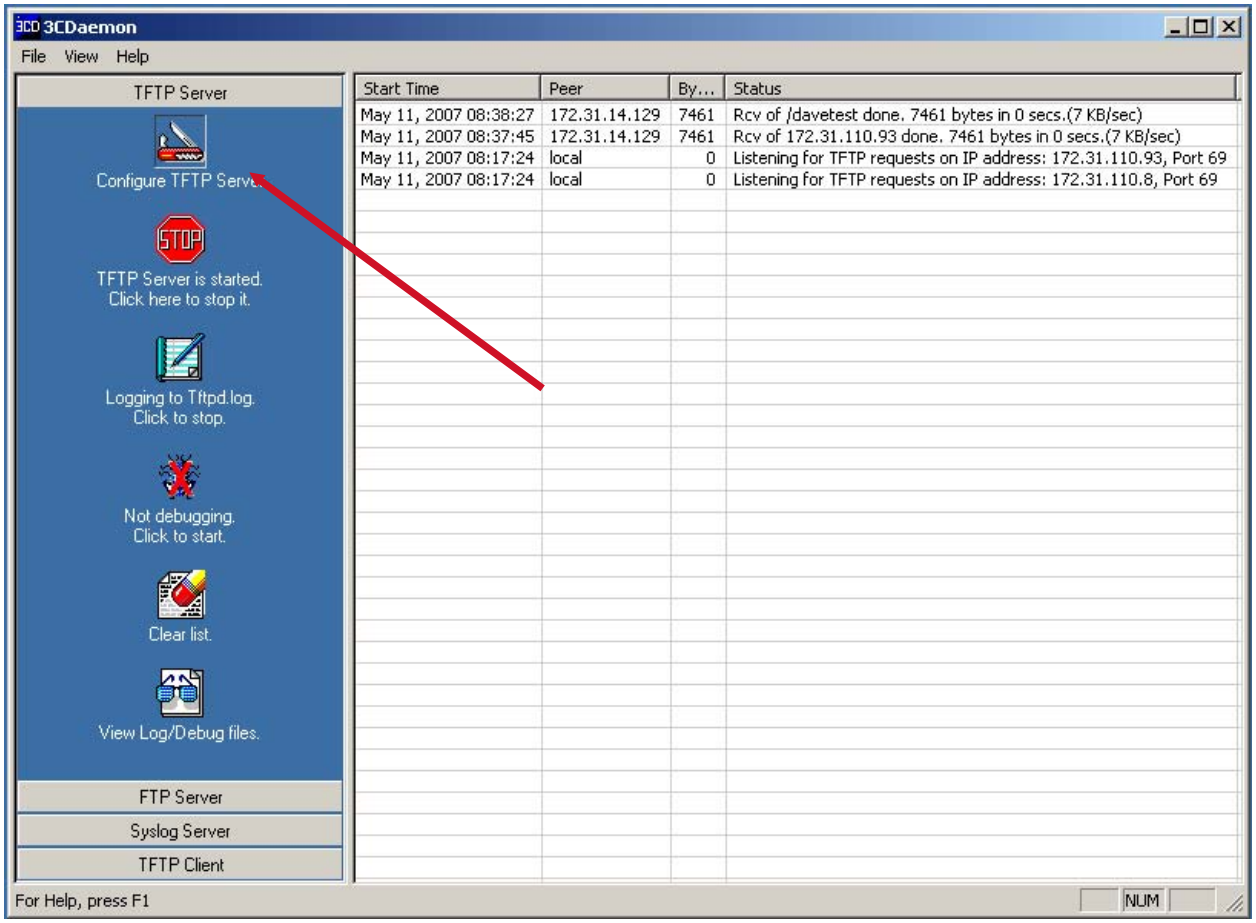
This document is to help the installer configure a new Cisco MDS-9000 series switch on a new installation.

Things you should do before going out on site:
I recommend loading 3CDaemon and PUtty on your systems. You will need them for console configuration and copying files to and from the switch.

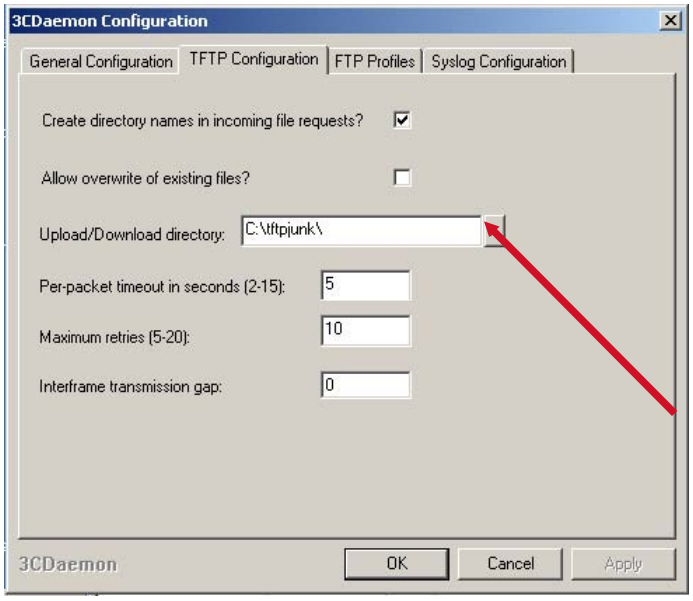
Software Tools: (Found under \\samadams\public\installations\cisco\softwaretools) 3CDaemon (for setting up a TFTP server on your laptop) Pumpkin (another tool for setting up an TFTP server) You can use either one. I'm using 3CDaemon
Putty (Terminal/Console tool like QVTterm but it allows you to set different profiles. If you use this one for Cisco and QVTterm for our equipment, you won't need to reset the communication settings.)

TFTP Server setup:

- Create a folder off of the root of your C drive (I called mine tftpjunk)
- Load 3CDaemon
- Open 3CDaemon



- Click on Configure TFTP Server on the upper left hand side



- Click the box with 3 dots at the end of the Upload/Download directory.
- Select your tftpjunk folder.
- Click OK to select the directory.
- Click OK.

You now have a folder on your laptop that will be used to copy files to or from the switch.

Basic Switch Configuration:

Plug the Blue cable into your Com port and the other end into the console port on the switch.
You will need a terminal program like QVT, PUtty or Hyperterminal to connect. Set the communication to the following: 9600 Baud,8,N,1

Out of the box, the system will start up and go through a setup program.
READ the screen to answer the questions.
You can hit Enter to take the default on any question.
Unless otherwise noted, take the default answer.

- You will be asked to enter a password for the admin user

Note: There is no "default" password; a strong password must be configured.

- Would you like to enter the basic configuration dialog? Y/N: answer Y
- Enter the switch name: <enter a name>
- Mgmt0 IPv4 Address: Enter the management IP address
- Mgmt0 IPv4 netmask: Enter the subnet mask
- Configure the default gateway? (yes/no): answer Y
- IPv4 address of the default gateway: <Enter the gateway>
- Configure the ntp server? (yes/no): Answer Y if you have one, otherwise take the default of N
- NTP server IP address: <Enter the NTP address>
- Configure default switchport interface state (shut/noshut): Shut

This disables all ports by default; use Device Manager to individually enable a port.

- Enable full zoneset distribution (yes/no): Default is N

If you are linking the switch to another switch change this to Y A summary of the config will be displayed, Press Enter twice to save the configuration.

Licensing

The first 8 ports are already licensed however, if you need to add ports you will need to get a license key. This will require copying a file from your system to the switch. The email you receive from Cisco will have directions.

1. Get the Product Authorization Key from the vendor (located on a piece of paper that is mailed to the customer.)
2. You need the switch serial number. Go to the console and type: **show license host-id**

The serial number is the character string after the "=" sign

3. You will need to go out to www.cisco.com/go/license/public website to register and setup an account.

You will be required to register (the end user should do this or you can register yourself and get an account)

4. Enter the Product Authorization Key and the Switch Serial Number.
5. The license key will be emailed to the registered account.
6. The email will contain instructions on how to enter the license key
7. The license file will need to be copied to the switch via TFTP, if 3CDaemon is configured, you have a TFTP server. **Note: this can also be configured as an FTP server too.**
8. Obtain your systems IP address
9. Open 3CDaemon and verify the TFTP server is running, click the Start sign on the left column to start it if needed
10. Open a command window and telnet to the switch
    - telnet <switch IP address>
    - enter the username: admin
    - enter the admin password

You are now logged into the switch

11. Change to the bootflash: directory
    - Cd bootflash:

12. Copy the new configuration file from your laptop to this directory
    - Copy tftp:<filename> bootflash:
    - On the next line enter your laptops IP address

Do a directory to verify the file has been copied.

13. To Load the license file, type: **Install license bootflash:license_file.loc**

Configuring the switch

Configuring a switch involves the following:

- Loading Fabric Manager
- Loading Device Manager
- Creating a new VSAN
- Creating Zonesets and Zones

Loading Fabric Manager

Fabric Manager can be installed from either a CD or from the Cisco website: http://cisco.com/cgi-bin/tablebuild.pl/mds-fm

- Click the **FM Installer** link.
- Click Next at the Welcome screen.

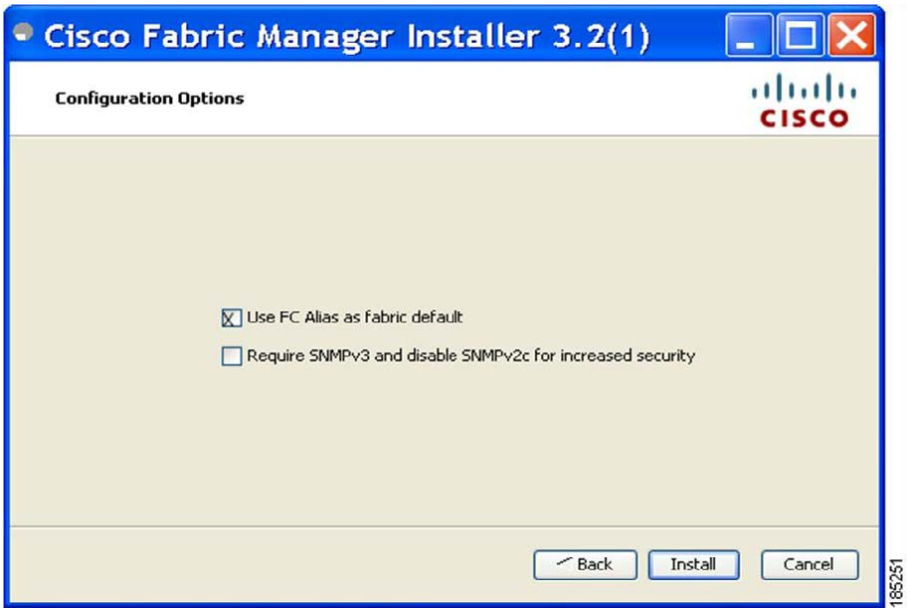
- Accept the End User License Agreement and click **Next.**

- On the Install Options Box, select Fabric Manager Standalone and click **Next.**

- On the Database Options box, select Install PostgreSQL.
- Enter a username and password.
- NOTE: This is YOUR username and password to logon to your system.
- Click **Next.**

- On the User Options box, enter a username and password for the local FM database.
- NOTE: suggest you use just admin and password; keep it simple.
- Click **Next.**

- On the Configurations Options box, select "Use FC Alias as fabric default."
- Click **Install.**



- Once the install is complete, click **Finish.**

To Open Fabric Manager:

- Double click on the Fabric Manager icon, the following login screen will open.

- Use LocalHost
- User name: admin
- Use password as the password.
- Click Login.

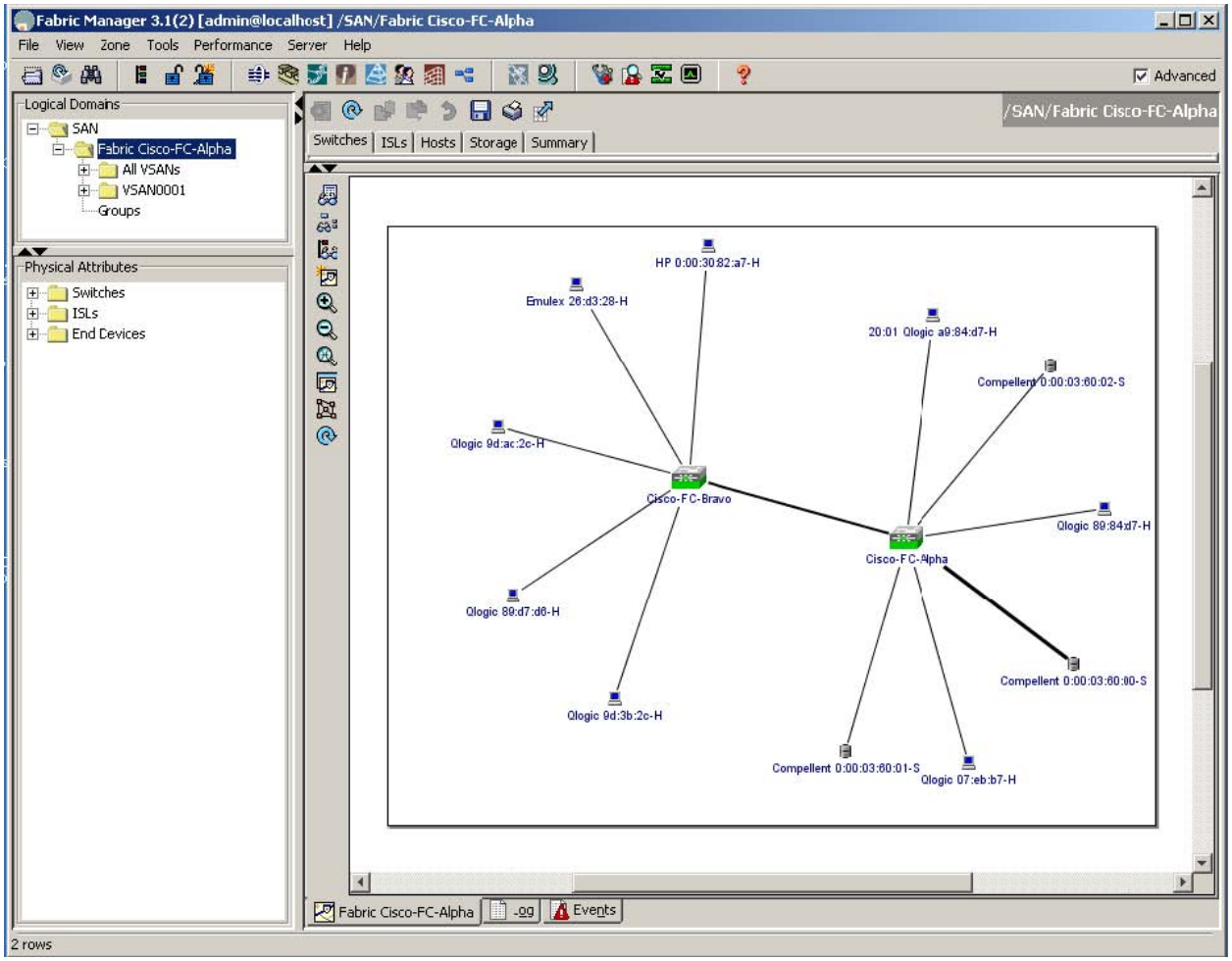
You will be presented with another login screen.

- Enter the mgmt IP address and the admin password that you set for the switch.
- Leave the check boxes checked.
- Click Discover.

The system will discover the fabrics.

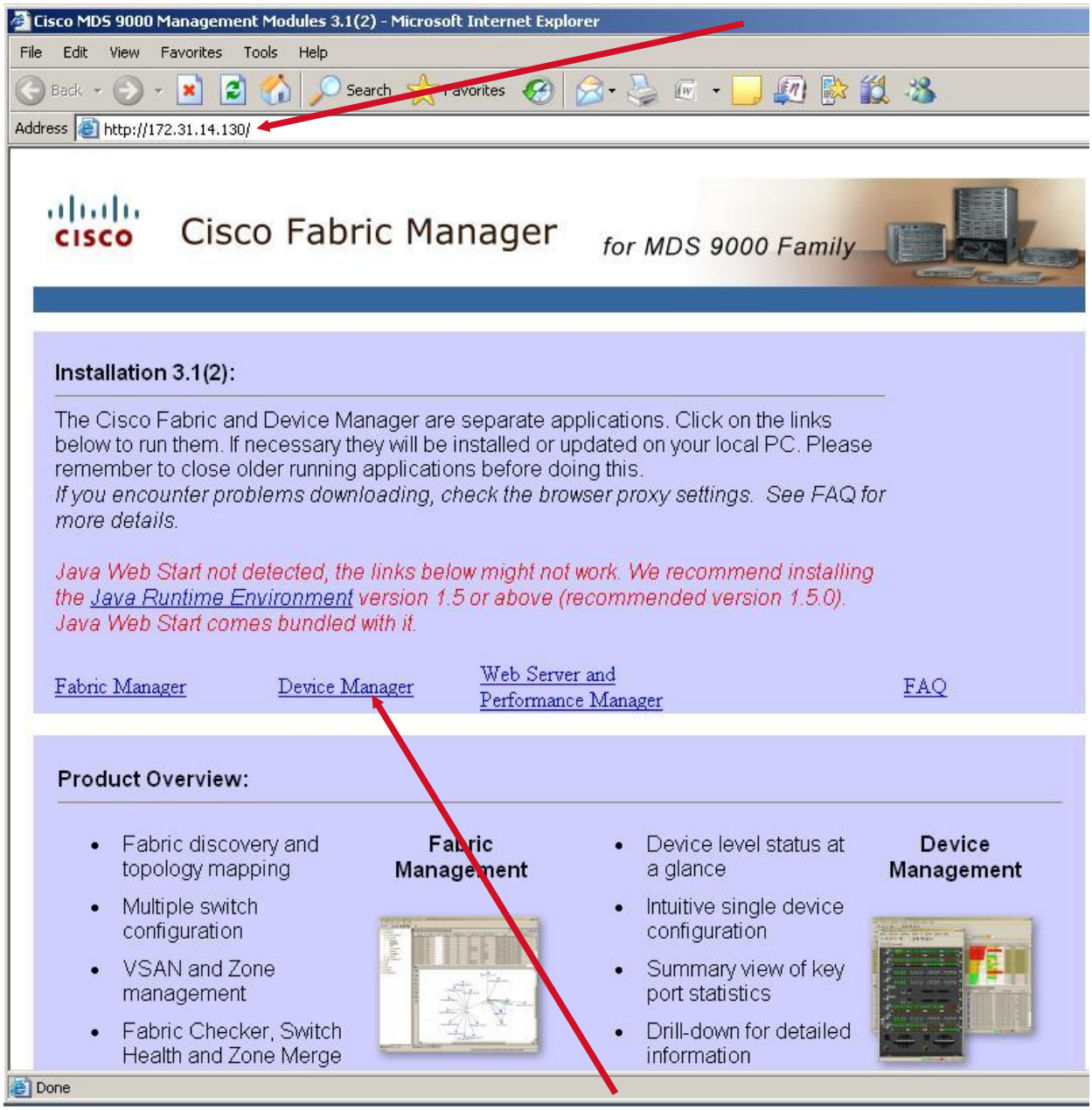
- Check the box to select the correct fabric.
- Click Open.

Fabric Manger will open.



Loading Device Manager

Open a web browser and enter the Mgmt IP address that you set for mgmt0 on the switch.



- Click on the link in the website and Device Manager will be loaded.
- Once loaded, double click on the Device Manager icon.

- Enter the mgmt IP address of the switch and admin password.
- Click Open.

Device Manager is now loaded.

Configuration uses:

- Use Device Manger for enabling ports.
- Use Fabric Manager for creating VSANs and zones.

Zoning your switch:

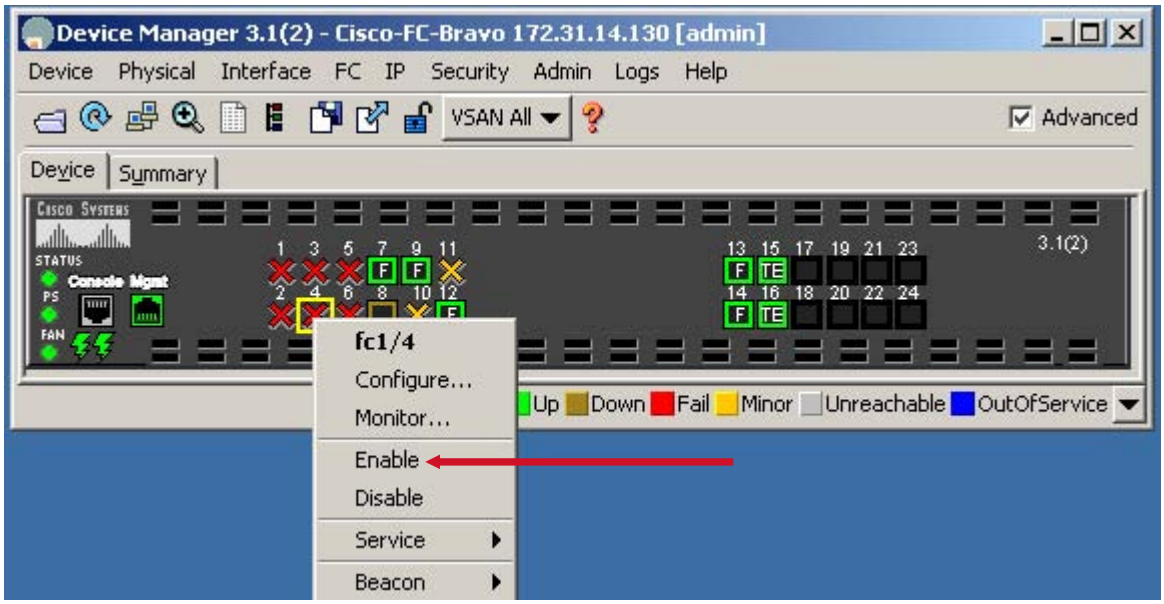
You will first enable the ports that you need on the switch through Device Manager. Then you will use Fabric Manager to create a VSAN, then a Zoneset and finally the Zones.

Step 1: Enabling ports on the switch

To enable the ports you need for Dell Compellent and Servers:

- Open Device Manager.

- Right click on the ports you want to enable.



- Select Enable.

The ports are now active.

Step 2: Opening Fabric Manager for zoning

- Double click on the Fabric Manager icon.

- FM Server Address: LocalHost
- FM Server User Name: admin
- FM Server Password: password
- Click Login

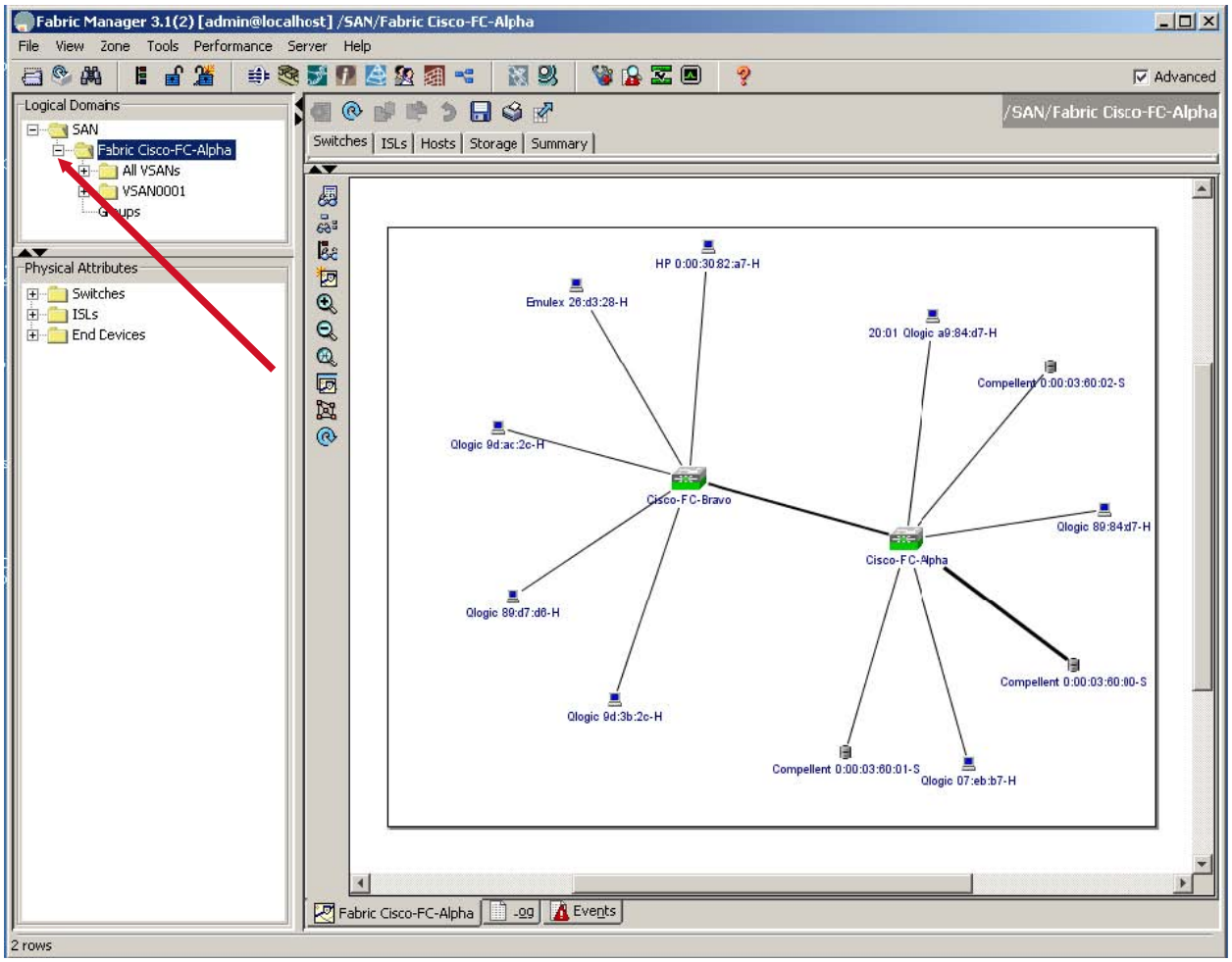
You will be presented with another login screen.

- Seed Switch: Enter the mgmt IP address
- User Name: admin
- Password: password that you set for the switch
- Leave the check boxes checked.
- Click Discover.

The system will discover the Fabric.

- Check the box to select the correct fabric.
- Click Open.

Fabric Manager will now open.



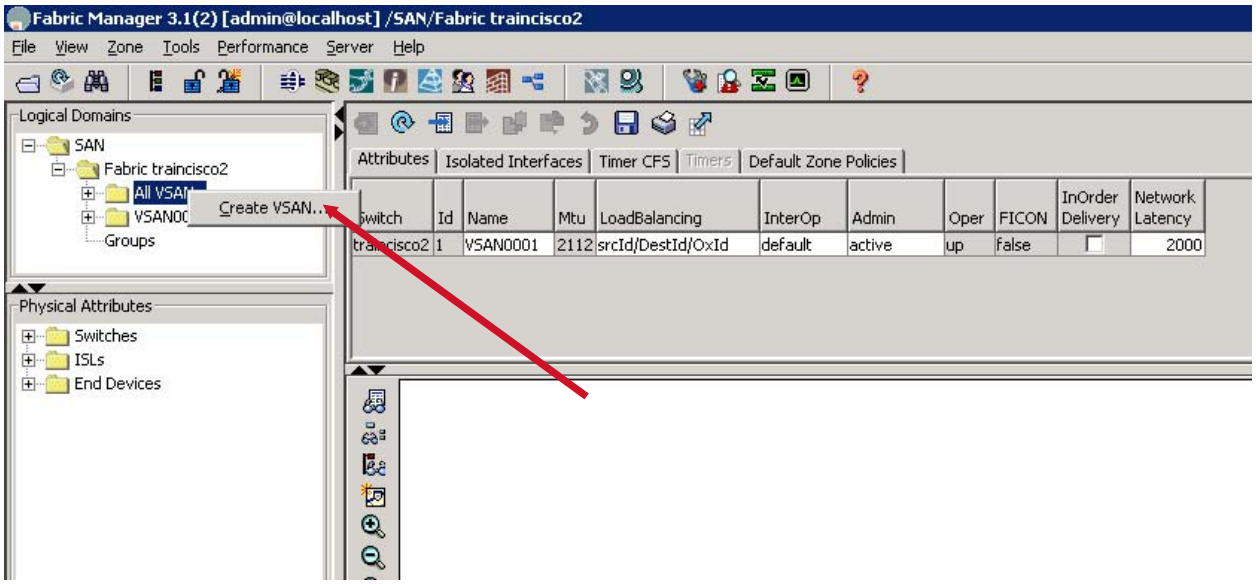
- Expand your fabric

Step 3: Creating a VSAN

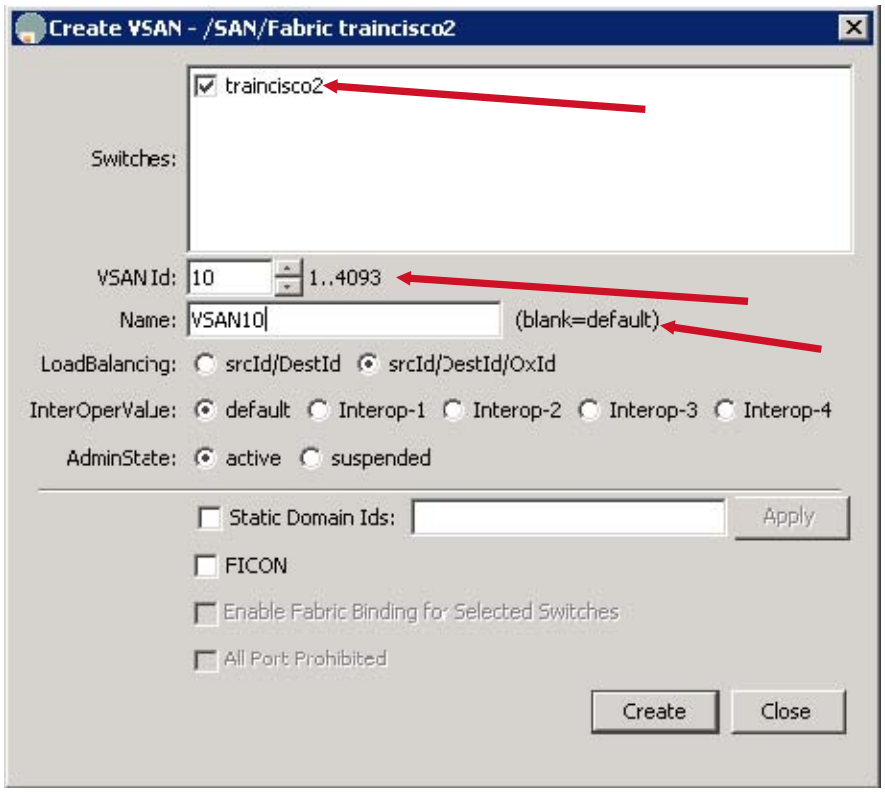
You will see All VSANs and VSAN0001

Create a new VSAN

- Right Click on All VSANs
- Select Create VSAN...



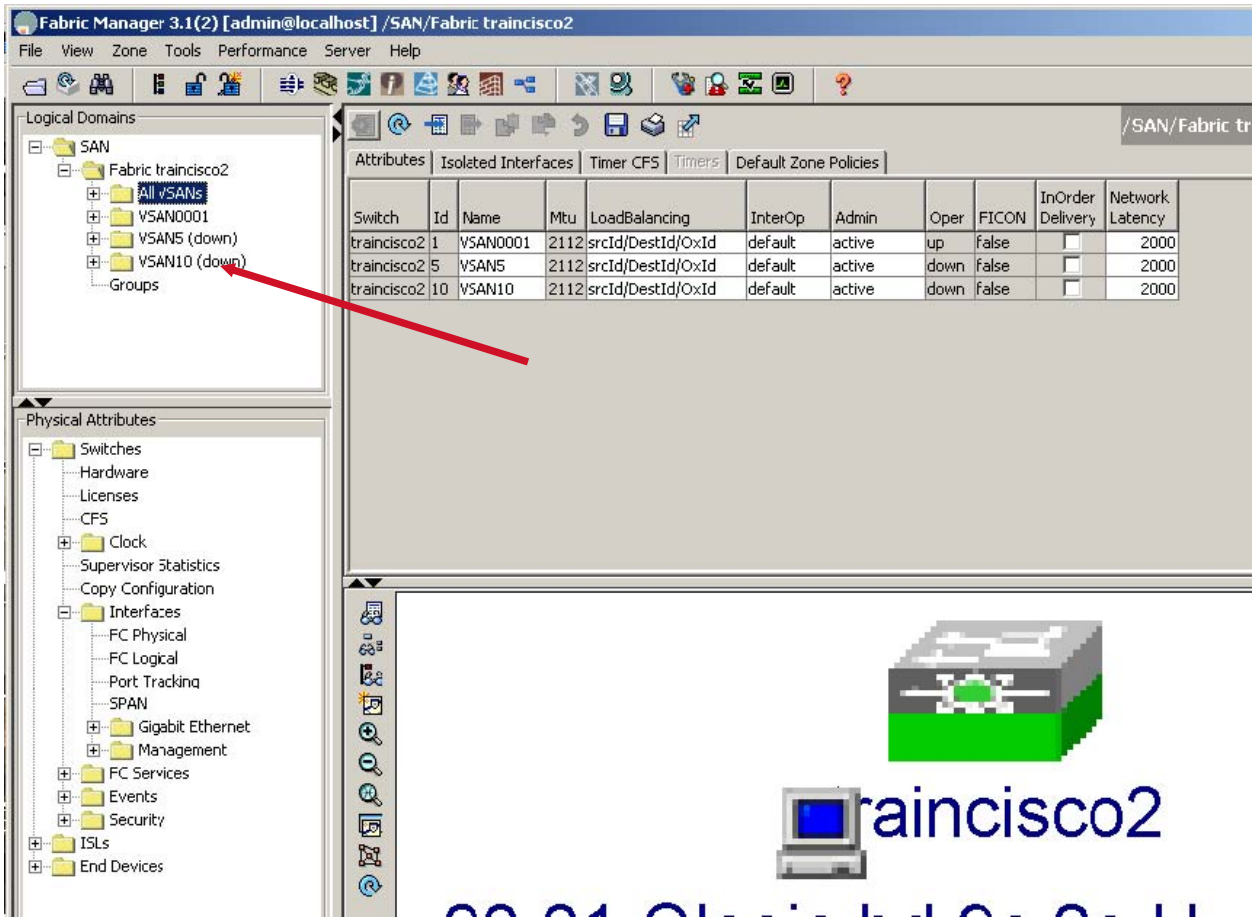
The Create VSAN screen opens



- Select your switch
- Set your new VSAN Id:
- Enter a new name for the VSAN

- Click Create

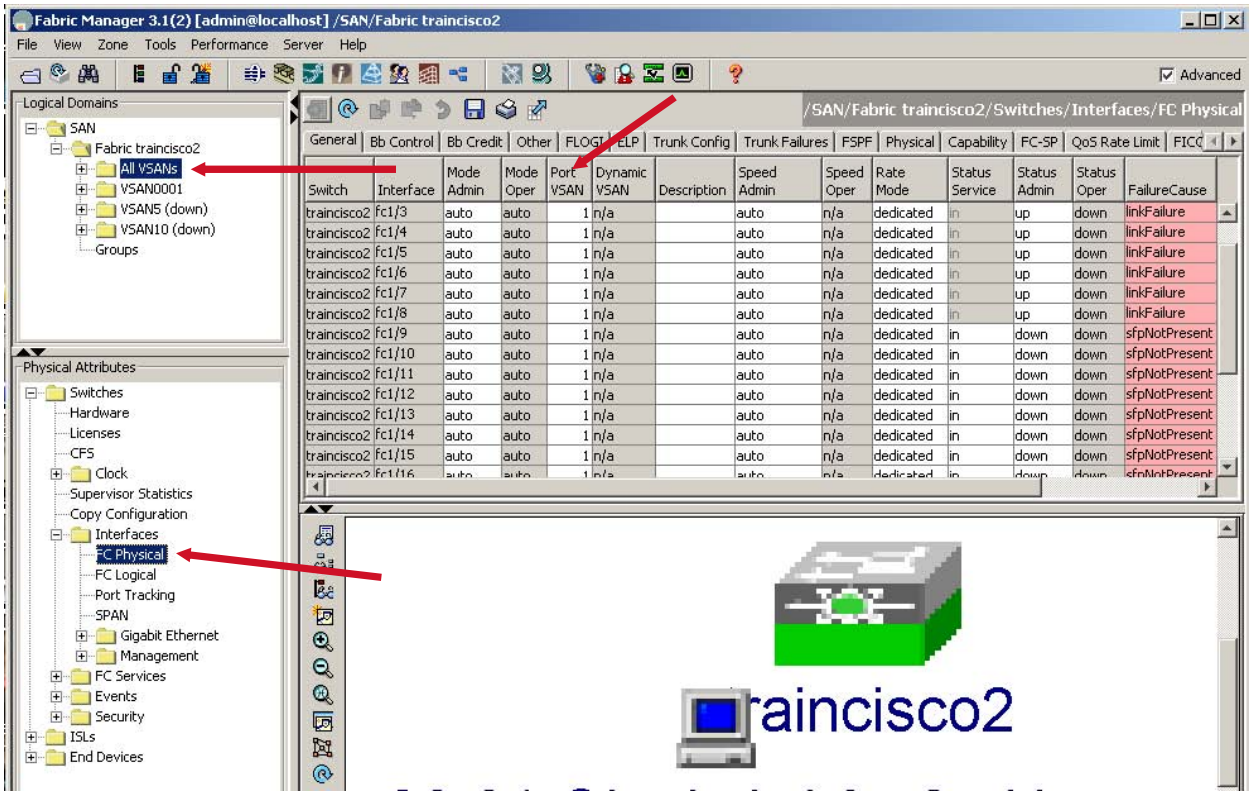
Your new VSAN will show up in the list



- Highlight All VSANs

On the lower Left Hand side:

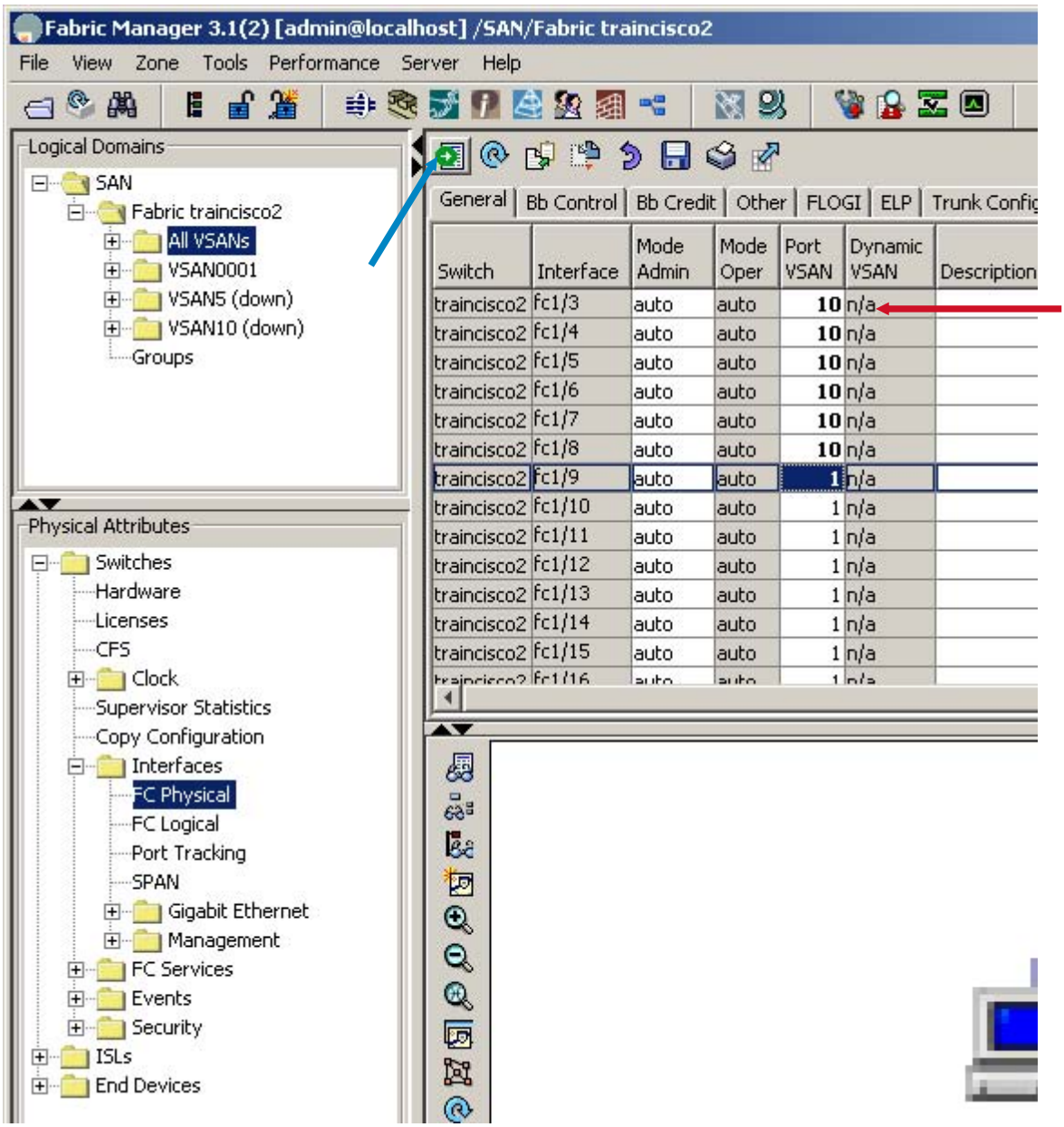
- Expand Switches
- Expand Interfaces
- Click FC Physical



- You need to change the Port VSAN number to the new VSAN ID

Example: If you created a VSAN with ID 10 and you wanted to add port 1 to it; you would double click inside the Port VSAN box for port 1 and change it to read 10

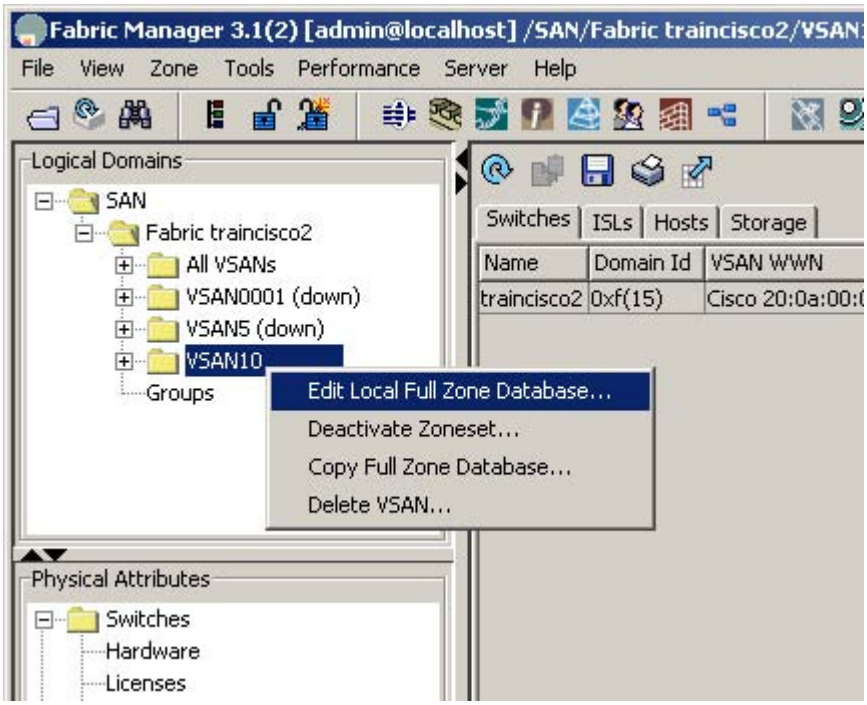
- Change all ports to the new VSAN ID (For new installs, you should add ALL of the ports)



- Click the Apply Changes button (Blue Arrow)

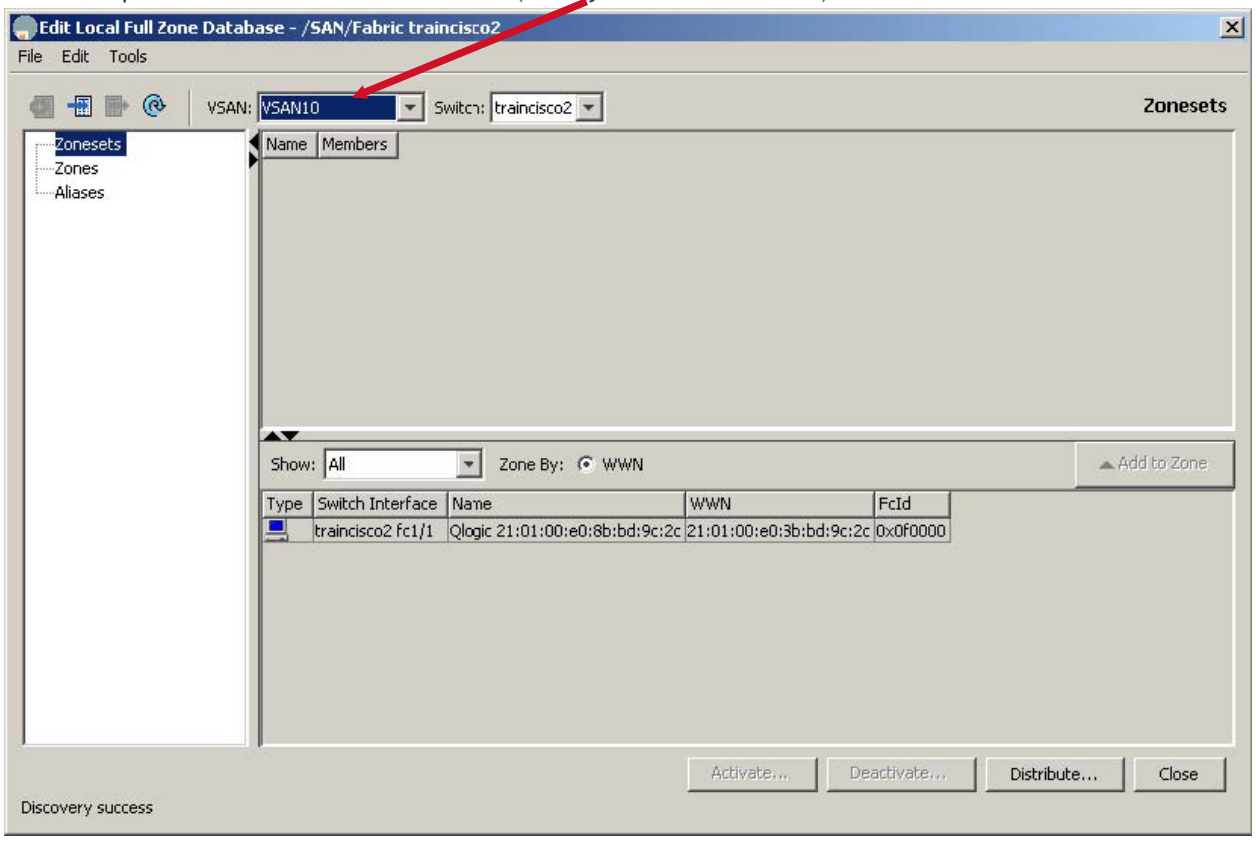
You are now ready to create zone sets and zones.

- Right click on the VSAN you created.



- Select Edit Local Full Zone Database.

This will open the Zone Database window. (Note your VSAN is listed.)



You are presented two folders: Zonesets and Zones
From here you will create your Zoneset and Zones.

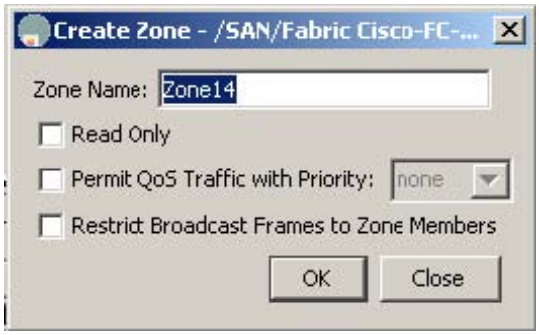
Step 4: Creating Zonesets
To create a Zoneset

- Right click Zoneset
- Select Insert

- Enter a zoneset name
- Click OK

Step 5: Create Zones
To create Zones

- Right click Zones
- Select Insert

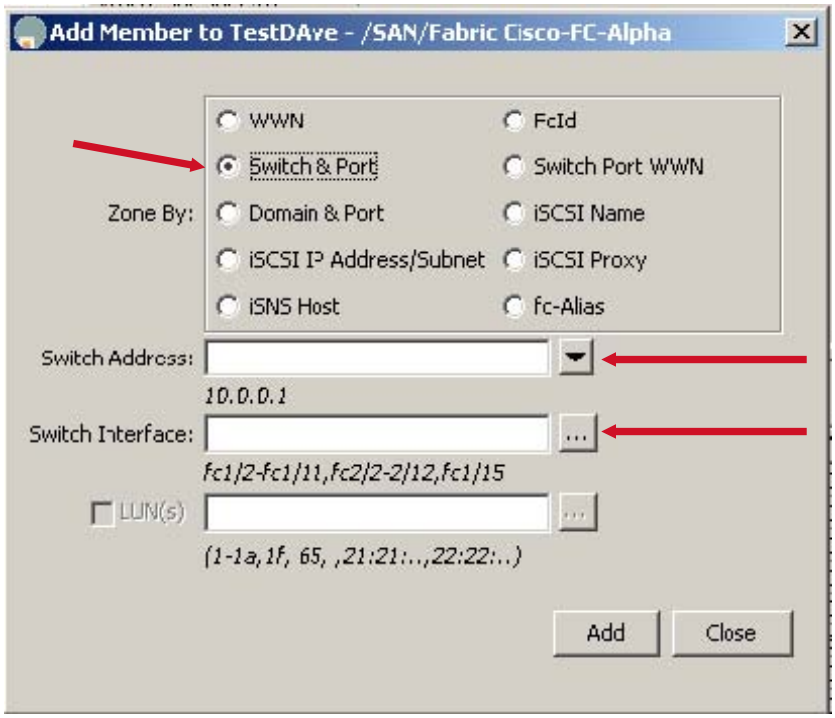


- Enter a Zone name
- Click OK

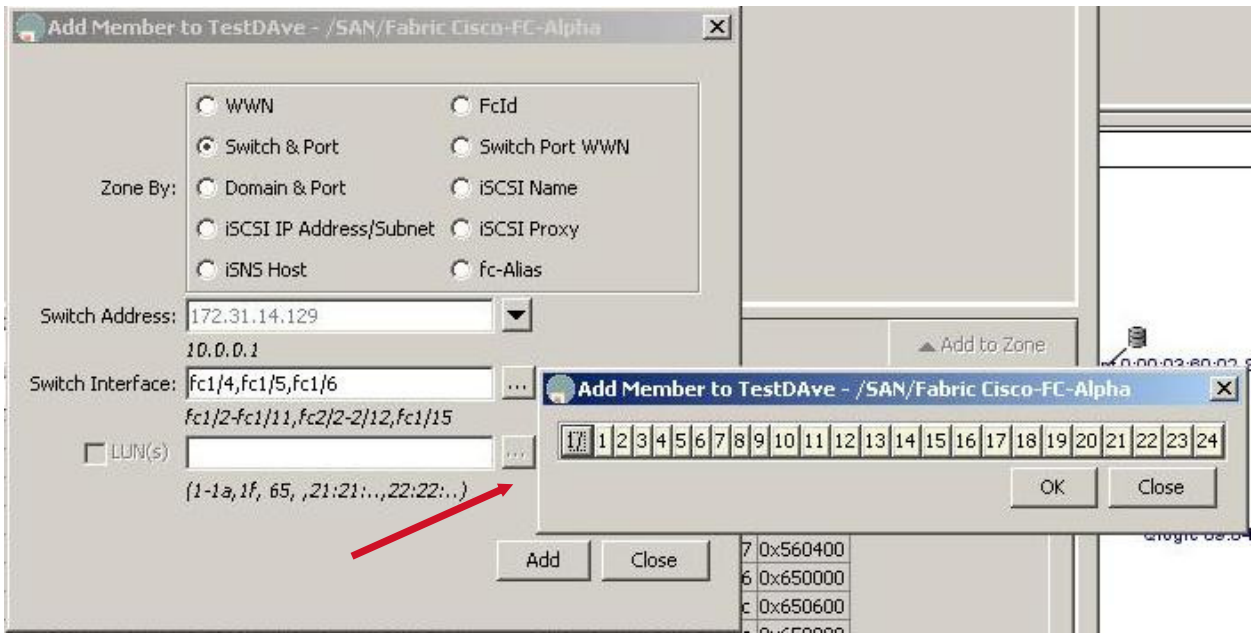
Step 6: Adding ports to your Zone

You will see your new zone under the Zone folder (Expand the Zone folder to see all zones)

- Right Click on your Zone name
- Select Insert



- Select Switch & Port
- Click the down arrow next to **Switch Address** and select the switches address
- Click the box next to the Switch Interface field



You will see a box come up with all of your ports

- Select your ports and click OK

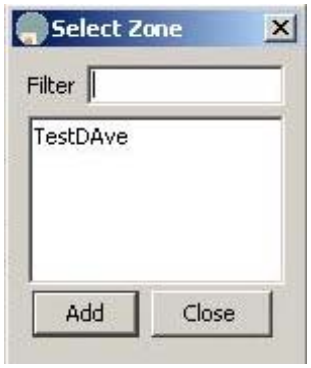
This will populate the switch Interface box

- Click Add
- Click Close

You have a zone using those port numbers

Step 7: Adding your Zone to the Zoneset

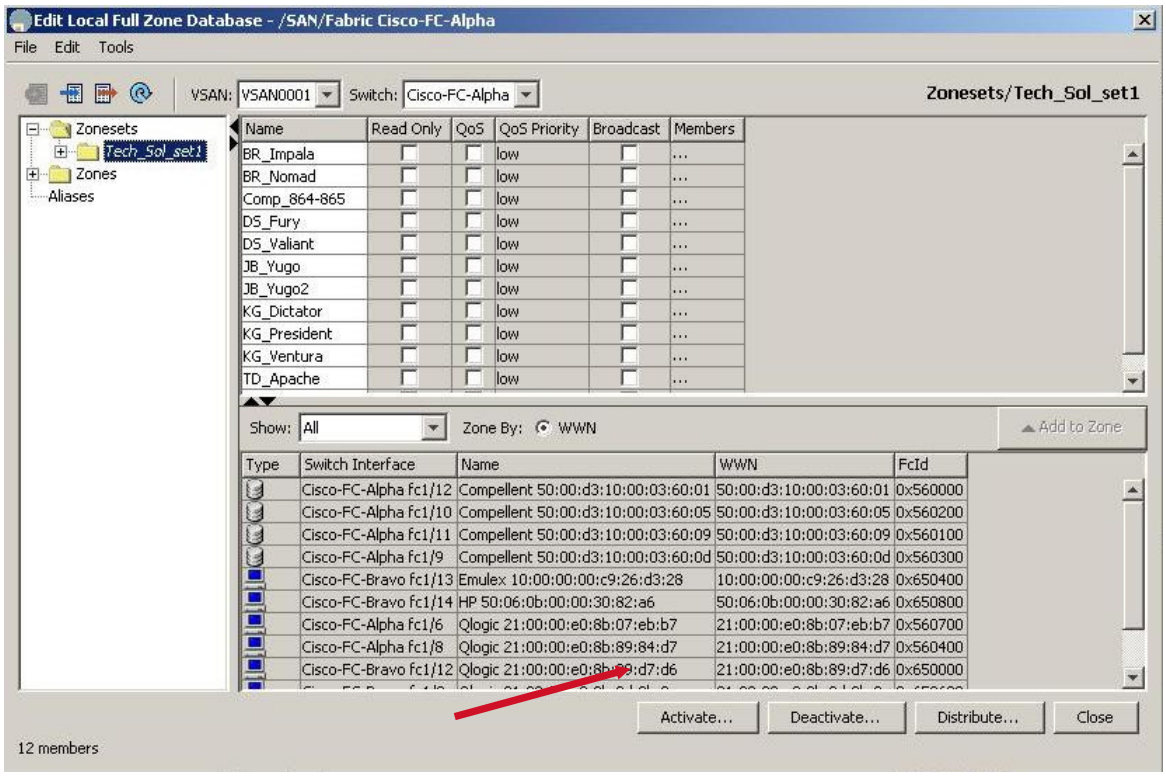
- Right click your Zoneset name
- Click Insert



You will see a dialog box with your available zones

- Select your zone
- Click Add

Your Zone is now part of the Zoneset



- Click Activate to activate your zoneset (You must have the ZoneSet highlighted)
- Click Close

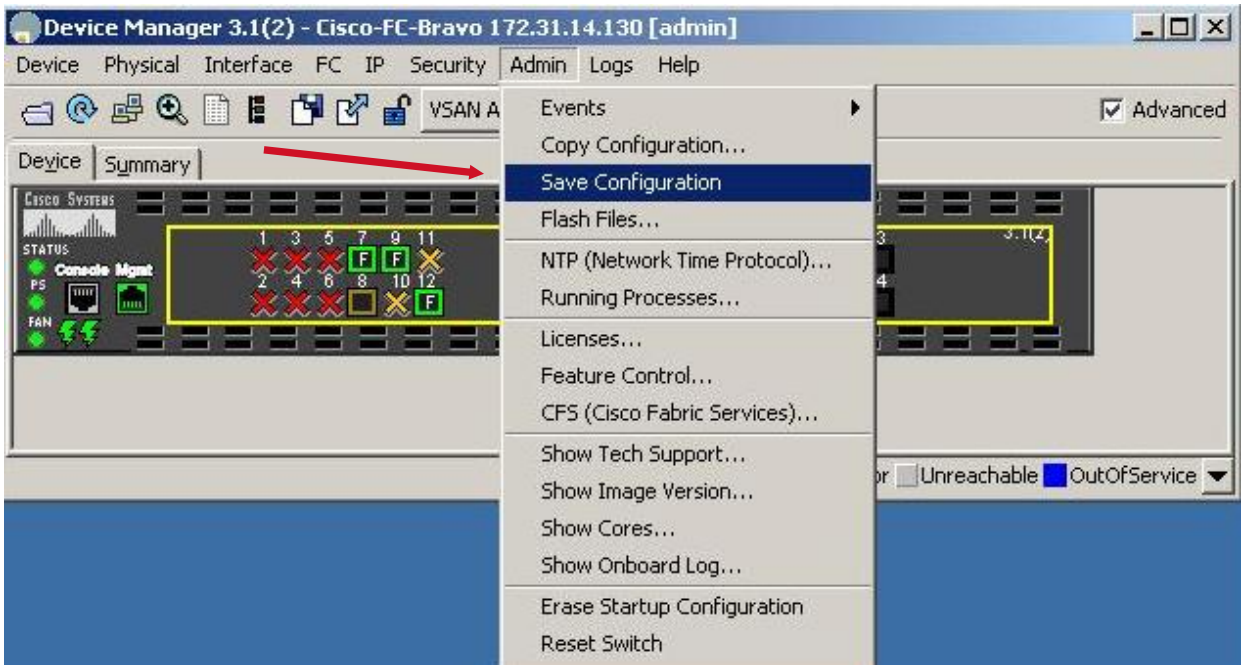
Your switch is now up and running.

Step 8: Saving your configuration

- The configuration can be saved in a couple of ways. When activating it will ask you if you want to save, or:
- When closing Fabric Manager, you will be prompted to save the running configuration to the startup configuration.
- Either way; **SAVE THE RUNNING CONFIGURATION TO THE STARTUP CONFIGURATION**

Optionally you can do the following:

- Go to your Device Manager
- Select Admin



- Select Save Configuration

You have saved your configuration. The switch is now ready for normal operation.

Console commands:
The following are a list of commands that you will find useful when dealing with Cisco switches. You must be connected to the switch either through the blue console cable or the network ports. In most cases you will connect just through the network port.

The switches configuration operates from a run file. It also contains a startup file. It is important that if you make changes to the switches configuration that you copy the run file to the startup file. Otherwise the next time the switch is rebooted, your changes will be lost.

NOTE: You can type the first few characters of a command and then hit TAB to fill in the rest

To save a running configuration to the startup file, type:
copy run start
Hit Enter

To save the running configuration to a new filename, type:
copy run bootflash:<filename>
Hit Enter

To load a configuration from a file, type:
copy bootflash:<filename> run
Hit Enter

To read a file, type:
Sh file bootflash:<filename>
Hit Enter

To copy a configuration file from the switch to your laptop, do the following:

- Obtain your systems IP address
- Open 3CDaemon
- Open a command window and telnet to the switch by typing:
  - telnet <switch IP address>
  - enter the username: admin (no caps)
  - enter the admin password

You are now logged into the switch

- Change to the bootflash: directory by typing:
  - cd bootflash:
- Do a directory of the bootflash: directory:
  - dir
- Copy the running configuration to a new filename:
  - copy run bootflash:<filename>
  - Example: copy bootflash:davetest
- Do a directory to verify the new file exists
- To copy the file from the switch to your system, do the following:

- Copy bootflash:<filename> tftp:
- Enter your systems IP address on the next line

The file should now be in the C:\tftpjunk folder that you created and pointed 3CDaemon to.

To copy a configuration or license file from your system to the switch, do the following:

- Obtain your systems IP address
- Open 3CDaemon
- Open a command window and telnet to the switch
  - telnet <switch IP address>
  - enter the username: admin
  - enter the admin password

You are now logged into the switch

- Change to the bootflash: directory
  - Cd bootflash:

- Copy the new configuration file from your laptop to this directory
  - Copy tftp:<filename> bootflash:
  - On the next line enter your laptops IP address

Do a directory to verify the file has been copied.

To load the new configuration file, type:

Copy bootflash:<filename> run

To save this configuration, copy it to the startup file:

Copy run start

To Load the license file, type:

Install license bootflash:license_file.lic

If the admin password isn't known, start console session, power cycle switch, hold down ctrl and right bracket keys

The following example shows how to disable the management interface.

switch# **config terminal**
switch(config)# **interface mgmt 0**
switch(config-if)# **shutdown**

The following example shows how to enable the management interface.

switch# **config terminal**
switch(config)# **interface mgmt 0**
switch(config-if)# **no shutdown**

Manually Setting an IP address on the Mgmt0 port:

Command	**Command**
Step 1 At the prompt enter the following: `switch# config terminal`	**Enters the configuration Mode**
`switch(config)#` ^-Prompt Changes to this	

Step 2
Enter the Interface Configuration Mode
```
switch(config)# interface mgmt 0
switch(config-if)#  ←Prompt Changes to this
```

Step 3
Enter the IP address for Mgmt0
```
switch(config-if)# ip address 1.1.1.0 255.255.255.0
```

Step 4
You can set the port speed by typing the following:
```
switch(config-if)# switchport speed 100
```

Configures the port speed in Mbps. Valid values are **10**, **100**, and **1000** (Supervisor-2 module only).

Step 5
`switch(config-if)# no shutdown` Enables the interface.

Step 6
`switch(config-if)# exit` Returns to configuration mode.

Step 7
Configure the IPv4 default gateway address.
```
switch(config)# ip default-gateway 1.1.1.1
```

REMEMBER TO COPY THE RUNNING CONFIG TO THE STARTUP CONFIG FILE!

Console switch configuration

The following are commands to configure the switch through the console without using Device Manager or Fabric Manager.

1 Establish VSAN ((config)# vsan database)

1. Define the VSAN.
    - (config-vsan-db)# **vsan** *vsan-number* **name** *vsan-name*
2. Assign Port interfaces to the vsan.
    - (config-vsan-db)# **vsan** *vsan-number* **interface** *interface*
3. Activate the VSAN.
    - (config-vsan-db)# **no vsan** *vsan-number* **suspend**
4. Create the VSAN Interface.
    - (config)# **interface vsan** vsan-number
5. Turn On (no shut) the VSAN Interface.
    - (config-if)# **no shut**
6. Assign the mode to the Port interface.
    - (config-if)# **switchport mode** *F | Auto*
7. Turn On the Port Interface(s).
    - (config-if)# **no shut**

2 Establish Zones within the VSAN, by defining interfaces that are to be members of the zone(s).

1. Define the Zone.
    - (config)# **zone name** *zone-name* **vsan** *vsan-number*
2. Add Port interfaces (members) to the zone.
    - (config-zone)# **member interface** *interface*

3 Establish Zoneset(s) and add the appropriate zones to the Zoneset(s).

1. Define the Zoneset.
    - (config)# **zoneset name** *zoneset-name* **vsan** *vsan-number*
2. Assign Zone(s) to the Zoneset.
    - (config-zoneset)# **member** *zone-name*

4 Activate the Zoneset(s).

1. Activate the Zoneset(s).
    - (config)# **zoneset activate name** *zoneset-name* **vsan** *vsan-number*