Brocade Guide to Understanding Zoning

Volume 1

The benefits of Zoning

In this day and age of "high stakes" corporate poker, SANs are growing by leaps and bounds, not only in computer rooms, but also now extend across wide geographical locations.

Switch based Zoning is often an afterthought, typically due to confusions about the benefits of switch based zoning in conjunction with storage based LUN zoning. When zoning comes up in conversation, it's usually along the lines of, "We need to put Group A here and Group B over there." Whether it is Hard Zoning or Soft Zoning, users need Zoning Architecture, just like they need SAN architecture. With zone architecture, the user can layout and decide what their company's zoning needs.

The Importance of Zoning

The security of zoning is critical to the existence of a company, whether it is financial, intellectual property, etc.

Switch based zoning is critical even in systems with storage based LUN zoning. Often storage based zoning is viewed as a replacement for switch based zoning, however this is just not the case. Switch zoning is rather complimentary to existing storage zoning in that it allows administrators to secure not just their storage, but also their servers from interaction/access by creating zones that allow storage access, but isolate servers from each other…especially in a heterogeneous server environment. Switch based zoning is also important as there is typically some storage devices that do not support storage based zoning such as older storage subsystems or tape libraries that can benefit from the added level of security the switches can offer.

Hard Zoning or Soft Zoning

One way to explain soft and soft zoning is to think in terms on your unlisted home phone number. It might not be in the phone book or the operator might tell you that it is unlisted. However, your phone will still ring if someone dialed the correct number. For hard zoning, think of caller ID blocking. Even if you do know the number, there is no access.

Both types of zoning have been used in the past, due to implementation differences and switch vendor capabilities. In the past Brocade's hardware zoning was only enabled when port level zoning was used. This is not the case with all vendors, as many have port zoning, which is still based on software and not secure. The benefit of Brocade port zoning was hardware enforcement of zoning, however the trade off was a loss of flexibility in that the zones were not tied to a device address. For software based zoning Brocade and others use the devices specific address or World Wide Name (WWN) to link a device to a zone. This has the benefit of flexibility in that the device can be moved to any port in the fabric and the zone would follow the device. So administrators had to balance the value of security with the benefits of flexibility, with security usually winning. The good news is that administrators no longer have to make this choice or sacrifice if implementing a SAN solution with Brocade's new 2Gb/s switches. With Brocade's 3rd generation 2Gb/s switch ASIC Brocade has implemented Advanced Fabric Zoning, which provide secure hardware enforced zoning at both port and WWN levels, providing both security and flexibility. Competitors are starting to offer hardware zoning, at the port level, however many are still only able to implement software based zoning. Before an administrator decides whether they want zoning architecture based on hard or soft zoning, the user MUST

know that the switches they will be using in the Fabric will be SECURED; with Brocade there is no longer a need for this decision in that all zoning is secure.

This means that the zone type a user chooses will not "break". "Break" means that a node outside of the zone cannot access storage inside the active zone configuration. This creates a security violation, and the phrases "application breaking" as well as "node(s) panicking" apply.

It is uncommon in the user community, for switch salespeople to be questioned about whether their zoning has any vulnerability (I.e. does it work or not). It is no secret in the SAN world that Brocade has some bitter rivals. Brocade-based zoning works as advertised and their main competitor's zoning does not work. It is unsecured. Please refer to Appendix A for an example of a competitor Zoning Vulnerability.

Brocade is continually pushing the envelope as it relates to Zoning, with the likes of LUN level and Protocol based zoning on the horizon. Another major differentiator with zoning is Brocade's ability to be able to loop based zoning within the same fabric. There are competitors who are not even able to support loop direct attached anything to their Director class switch much less do any loop based zoning.

Another key differentiator is Brocade's ability to support overlapping hard zones or fabric wide hardware zones versus vendors who can do it only on a single chassis.

Zoning Enforcement

With the Brocade SilkWorm 2000 series of switches the distinction between hardware enforcement and software enforcement was relatively straightforward. Hardware enforcement was only possible with zones only containing port numbers. If WWN names were used it was software based.

With the new 2Gb product families, the new switch ASIC now can support hardware zoning with WWN as well, however there are certain configurations that fall back to software enforcement.

When zoning 2Gb switches, both zoning by port and zoning by WWN are hardware enforceable. This means that the zoning is done in the switch ASIC. There are three types of zoning enforcement:

- Hard Port: Port numbers define all the members of the zone.
- Hard WWN: all the members are defined by their WWN names, whether it is Port Name or Node Name.
- Soft Porting: Ports define some members of the zone and WWN defines some members of the zone. This type of enforcement reverts to the Name Server.

There are two methods to determine the Zone Enforcement is for a given port:

- Use the "`portZoneShow`" command.
- Use the "`filterPortShow -slot<slot> <port>`" command.

Please refer to section "*What is soft porting*" for an example.

Zoning enforcement mechanisms:

- Soft Zoning: Name Server assisted
    1. Name Server restricts visibility
    2. Always available when zoning enabled
    3. No reduction in performance
- Hard Zoning: Hardware Enforced
    1. Available when certain rule checking criteria are met through hardware logic checking.
    2. Provides additional security in addition to Soft zoning
    3. Prevents illegal access from “bad” citizens.
    4. No reduction in performance with hard-Port level zoning.

Zone Object types:

- Configurations
    1. Allows one or more “Defined Configuration”.
    2. Up to one “Effective Configuration”
    3. Can consist of one or more Zones.
- Zones
    1. Can consist of one or more Zone members.
    2. May exist across multiple zone configurations.
- Zone Members
    1. Domain/Port or WWN or Aliases
    2. Properties
    3. Special handling when defined across zones.

Zoning Features

SilkWorm 2.x

- Soft Zoning: This type of zoning is based on WWNs and enforced by the NameSever
- Hard Port Zoning: This type of zoning is based on Domain ID & Port Number
- Fabric Assists Zoning: A zone that is configured with a private loop host and all attached storage that it needs to communicate with. The storage can be private loop, public loop, or fabric aware. The private loop host appears to reside on a dedicated private loop with all of the storage in FA Zone.
- QuickLoop Zoning: A QuickLoop zone is a subset of a QuickLoop and can only include QL devices.

SilkWorm (3800, 12000)

- Hard Port Zoning – enforced in hardware
- WWN Zoning – enforced in hardware
- Soft Port Zoning –enforced by Name Server

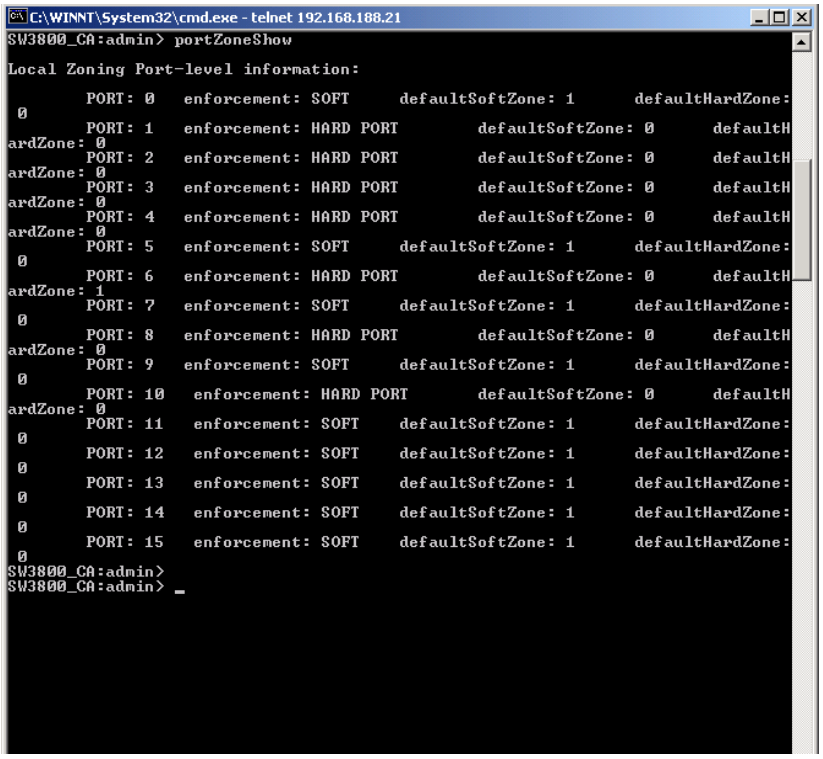
"Soft Port" Zoning

With 2Gb switches, the zone consists of port numbering or WWN only. The entire zone will be hardware-enforced in the ASIC. If there is a port that is a part of both the port zone and WWN zone, that port is referred to as a "soft port". The soft port is no longer having its zone enforced in the ASIC, but will be enforced through the Name Server.

A fabric will not segment if a user wants to join a 2Gb fabric with the Brocade SilkWorm 2000 1Gb family of switches. In fact, if WWN hardware enforcement is used on the 2Gb switches then it will also enforce zoning on the 1Gb switches if the data passes through a 2Gb switch.

By using either of the two following commands, the user can discern if it is hardware-enforced: "`portZoneShow`" command and the "`filterPortShow -slot <slot> <port>`"

Figure 1



Security

The Brocade SilkWorm 3000 Family of switches offer the following security features:

- WWN spoofing – match WWN and PID at PLOGI
- Probing possible for ports with no hardware enforcement

Zoning Rules

Example: The following configuration will guarantee hardware enforcement in zones a1 and a2 and Name Server enforcement on a3.

```
zoneCreate "a1","1,3","1,4"
zoneCreate "a2","WWN2","WWN3"
zoneCreate "a3","1,6","WWN6"
```

When WWN devices fall into a1 ports, the hardware enforcement at that port will be turned "off" and the Name Server will handle the zoning control. This is "soft porting".

Zoning with E_Ports

Regarding past problems concerning zoning with E_Ports: Early in the life of the SilkWorm switches, particularly with FOS 2.2.1a, when the user changed the zone configuration and re-enabled the zone, the configuration was not always propagated through out the entire fabric. This issue is resolved in 2.4.1.

E_Ports when creating zones

If the user creates a zone that includes E_Port(s), it will be a zone based upon Domain/Port numbers. Although the E_Port can zoned in by port number the system will not lock down its path or use this zoned path exclusively. In fact E_Ports are beyond zones, in that any zone can use any E_Port. This prevents events like lost unrouteable data paths where an E_Port is disconnected and data cannot use an alternate E_Port, poor performance problems due to limit routes through a zone, and other issues if you were able to lock E_Ports to particular zones. The user will not have the option to select the Domain/Port when creating a zone using WWN's. E_Ports do not have a WWN. They are just a part of the zone if it includes multiple switches. The Name Server just recognizes it as a path to get to its final destination, as well as a path to propagate RSCN's when they occur in the Fabric.

So if a user creates a zone based on WWN's and it extends beyond one switch, E_Ports will be a part of this WWN-based zone. It will be transparent to the user when he creates the zone.

Auto-sensing ports and security

The user may lock down what the particular port(s) can be. If that is the case, lock the ports down that will be E_Ports and effectively shut down autosensing.

Zones based on Domain/Port numbers

There is no noticeable benefit to include E_Ports on zones based on Domain/Port numbers. In your Zoning Architecture, whether WWN or Port number-based or mixed, the only "things" that should be a part of your zones are devices, nodes, storage, tapes devices etc. E_Ports are a pathway to get to another location in your Fabric.

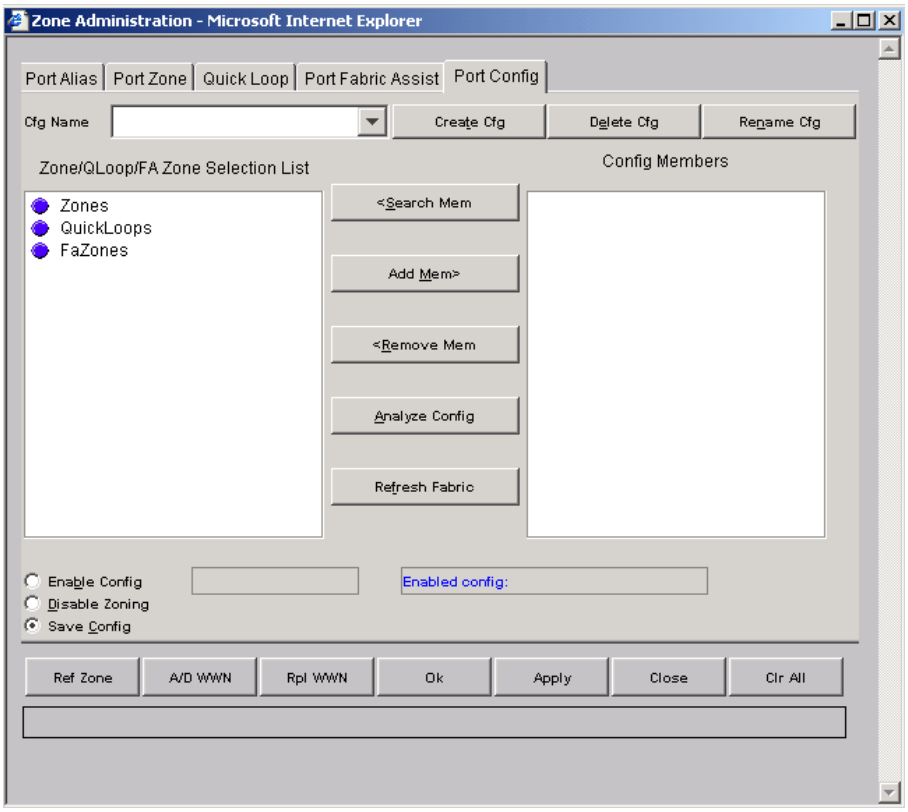
Note: Do not zone a trunk. There is no benefit in doing this.

RSCN

With FOS 2.x, when a user did a `cfgEnable`, an RSCN went out. With Web Tools, users have more control about when RSCNs are sent out. By bringing up the Zone Administrator in Web Tools, there will either be four or five tabs to work with, depending on the version of Web Tools. Also, in the **Port Config Tab**, in the lower left hand corner, there will only be two buttons to choose from-- "**Enable Config**" and "**Disable Config**".

Under the "**Port Config**" Tab, in the lower left-hand corner, there are three buttons to use when configuring zones. A user can create a zone and save it without sending out an RSCN by clicking on the "**Save Config**" button. The newer versions of Web Tools have this button. Below is an example of the "Port Config" tab.

Figure 2



Web Tools and RSCN Behavior within the Fabric

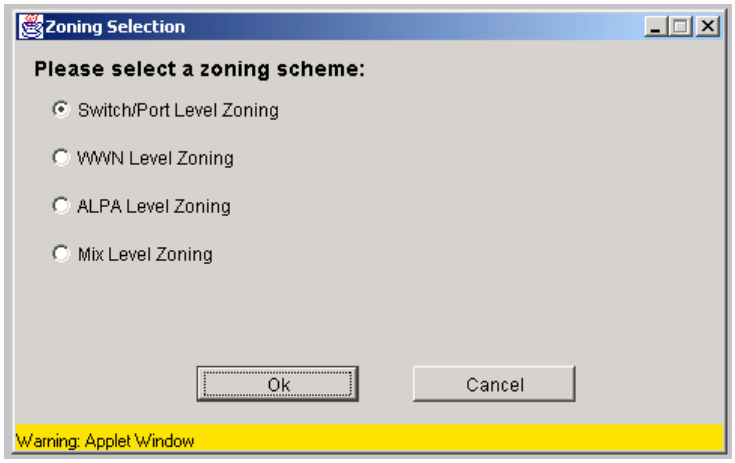
FOS 2.6 Web Tools RSCN behavior is the same as FOS 3.0 Web Tools RSCN behavior.

- Under Zoning, on the '**Config**' tab, if the "**Save Config**" radio button is selected, then an RSCN is not sent out when a Zoning change are made and applied to the 'defined'/'effective' configurations.
- Under Zoning, on the '**Config**' tab, if the "**Enable Config**" radio button is selected, then an RSCN is sent out when a Zoning change are made and applied to the 'defined'/'effective' configurations

Zoning Schemes

After invoking Zoning via Web Tools and entering a User name and password, the *Zoning Selection* screen will appear as shown in Figure 3.

Figure 3



Definitions of Zone Schemes:

Switch/Port Level Zoning: All zone definitions must be on ports. Aliases, zones, and configuration files that have objects other than ports cannot be selected or operated on.

WWN Level Zoning: All zone definitions must be on WWN. Aliases, zones, and configurations that have objects other then WWN cannot be selected or operated on.

AL_PA Zoning: All zoning operations must be on AL_PA in a QuickLoop. Aliases, zones, and configurations that have objects other then AL_PA's in a QL cannot be selected or operated on.

Mixed Level Zoning: Any object can be selected to be a member of the zone, alias, or configuration file.

Analyze Zone Configuration

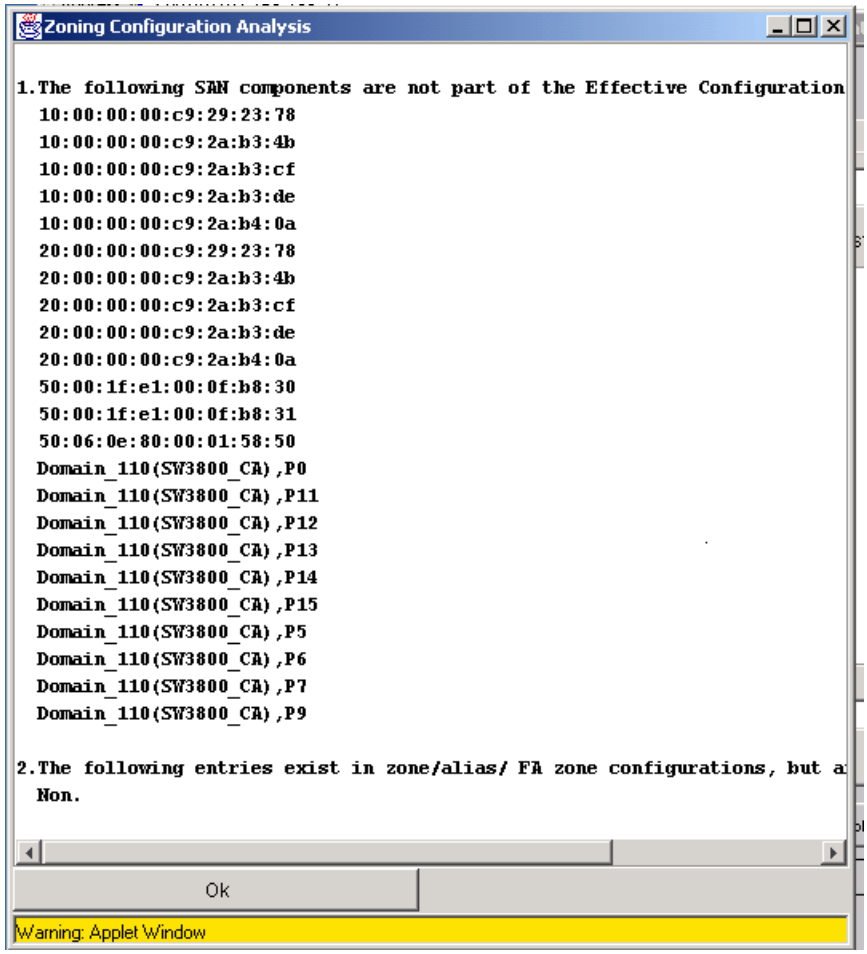
After creating and saving a zone configuration, we recommend the following as part of the Zoning Architecture Best Practice. Before committing a newly created zone into production, a user should "Analyze" the zone configuration before putting it into production. Doing this will save a lot of time and potential headache.

The Zoning Configuration Analyze screen displays a summary of the saved configuration and warns of the zoning conflicts before enabling them. Some of the potential errors that might be caught are:

- Ports/WWN/Devices that are part of the selected configuration but are not part of the fabric.
- Zones with a single member.

To access the *Zoning Configuration Analysis* screen, select the **Analyze Config** button, which is available in various zoning windows. The following is an example of the output after running the Zoning Configuration Analyze on a zone configuration:

Figure 4



Zoning Components

Zones in a fabric are made up of several components. In addition to the zone themselves, zoning uses: zone license, zone members, aliases, and configurations.

Zone Definitions

A Zone in a fabric is a set of devices that have access to one another. All devices connected to a Fabric may be configured into one or more zones. Every zone has at least one member. Empty zones are not allowed. The members are described by a semi-colon separated list of member definitions.

The maximum number of zones and members in a zone are constrained by memory usage. However, since these maximums are far larger than the number of devices that can be connected to a Fabric, they are effectively unlimited.

Zone definitions are consistent across reboots and power cycles. If two switches are connected in a fabric, they can become islands unto themselves (for example, due to an ISL failure). When rejoined, they will maintain the same fabric configuration unless one of the switches has had a configuration change.

Zoning License

Zoning requires a license to operate in a fabric. Without a license, zoning configurations may be built and saved, but may not be enabled. To install a license for zoning:

- Obtain a license key from Brocade
- Install the license key using the "`licenseAdd`" command
- Save any zoning created using the "`cfgSave`" command
- Reboot the switch.

Zone Members

Zone members may be defined by:

- Physical port number on switch
- Node Worldwide Name
- Port Worldwide name

Fabric ports are specified as a pair of decimal numbers "`d,pn`", where "`d`" is the Domain ID of the switch and "`pn`" is the port number on that switch (0 to 15).

For example, "3,13" specifies port 13 on switch number 3. When the physical port number specifies a member of a zone, then any and all devices connected to that port are in the zone. If this physical port is an arbitrated loop, then all devices on the loop are part of the zone.

Worldwide names are specified as an eight hexadecimal number separated by semi-colons, for example "10:00:00:90:69:00:00:8a". Zoning has no knowledge of the fields within a Worldwide Name. The eight bytes are compared with the Node and Port Names presented by devices in a login frame (FLOGI or PLOGI).

When Node Name specifies a zone member, then all ports on that device are in the zone. When Port Name specifies a zone member, then only that single port is in the zone.

The types of zone members used to define a zone may be mixed and matched. For example, a zone defined with the following members: "2,12; 2,14; 10:00:00:80:33:3f:aa: 11" would contain whatever devices are connected to switch 2 ports 12 and 14, and the device with either Node Name or Port Name "10:00:00:80:33:3f:aa:11", depending on the port in the fabric to whom it is connected.

Zone Aliases

Zone aliases simplify repetitive entry of port numbers or Worldwide Names. For example, the name "Eng" could be used as an alias for "10:00:00:80:33:3f:aa:11".

Zone Configurations

A zone configuration is a set of zones. Zoning may be disabled at any time. When a zone configuration is in effect, all zones that are members of that configuration are in effect.

The set of zone configurations defined in a Fabric may not be the same as the configuration that is currently in effect. This may also not be the same as the configurations saved in the switch's flash memory. The following three terms are used to differentiate between these "configurations":

- **Defined Configuration:** The "defined configuration" is the complete set of all zone objects that have been defined in the fabric.
- **Effective Configuration:** The "effective configuration" is a single zone configuration that is currently in effect. The "effective configuration" is built when an administrator enables a specified zone configuration. This configuration is "compiled" by checking for undefined zone names, or zone alias names, or other issues.
- **Saved Configuration:** The "saved configuration" is a copy of the "defined configuration" plus the name of the "effective configuration" which is saved in flash memory by the "`cfgSave`" command. There may be differences between the "saved configuration" and the "defined configuration" if the system administrator has modified any of the zone definitions and has not saved the configuration.

On power up, the switch automatically reloads the "saved configuration", and if a configuration was in effect when it was saved, the same configuration will be reinstated with an "auto" run of the "`cfgEnable`" command.

Zone Management

Zoning may be managed one of two ways: either by logging into the switch via telnet, or via Web Tools. Any switch in the fabric can be used to make changes to the zoning configuration. The changes will be replicated to all the other switches in the fabric.

The following CLI commands are used to manage zones, zones aliases, and zone configurations.

CLI commands used to manage zones, zones aliases, and zone configurations	
`aliadd`	Add a member to a zone alias
`aliCreate`	Create a zone alias
`aliDelete`	Delete a zone alias
`aliRemove`	Remove a member from a zone alias
`aliShow`	Show zone alias definition
`cfgCreate`	Create a zone configuration
`cfgAdd`	Add a zone to a configuration
`cfgDelete`	Delete a zone configuration
`cfgRemove`	Remove a zone from a configuration
`cfgShow`	Show a zone configuration
`zoneAdd`	Add a member to a zone
`ZoneCreate`	Create a zone
`zoneDelete`	Delete a zone
`ZoneRemove`	Remove a member from a zone
`zoneShow`	Show a zone configuration
`cfgClear`	Clear all zone configuration
`cfgDisable`	Disable a zone configuration
`cfgEnable`	Enable a zone configuration
`cfgSave`	Save a zone configuration to flash
`cfgShow`	Show zone configuration definition

Web Tools 4.0 Zoning

With the first release of the 2Gb switches like the SilkWorm 3800, and the upcoming SilkWorm 12000, Web Tools has been enhanced with the following features as related to zoning:

- Display slot (blade) information for SilkWorm 12000 switches
- Drag and Drop from left to right
- Multi selection wherever possible for addition/subtraction
- Replace/add/delete WWN
- `CfgClear` from Web Tools
- Refresh Zones
- Asynchronous zoning configuration committing process
- Analyze configuration
- Ability to right click on a Fabric WWN and display all aliases containing that WWN
- Display device WWNs and symbolic names under Domain/Ports
- Dynamic refreshes Zone button flashing to inform user of zoning changes.
- Sorted display of objects in all selection list

Functions not supported in Brocade Fabric OS v4.0

- QuickLoop Zoning
  - QL/QL zones cannot run on v4.0 switches
  - V4.0 switch can still manage (create, remove, update) QL zones on any non-v4.0 switch
  - QuickLoop Fabric Assist
- V4.0 switch cannot have a Fabric Assist host directly connected to it.
- V4.0 switch can still be part of a Fabric Assist zone if a Fabric Assist host is connected to a non-v4.0 switch.
- LUN Zoning
- Protocol Zoning
- Fabric Assist Zoning

Merging and Segmentation

Checked when Fabric configure/reconfigure during power-up or when a switch is disabled/enabled, or when a port switches to an F-port.

The entire “Defined Configuration” is merged with adjacent switches, before the Effective Configuration Name is sent, if one exists.

There are two databases used with zoning. The first database is the zone configuration database. This is the data displayed as the “defined configuration” in the “`cfgShow`” command. It is stored in flash by the “`cfgSave`” command. This database is a replicated database, which means that all switches in the fabric will have copy of this database. When a change is made to the defined configuration, the switches where the changes were made send out fabric-wide RSCNs to update all other switches in the fabric with the updated database.

The second database used with zoning is the N_Port login database. It is stored locally on each switch and is used for translating the World Wide Names into physical port numbers when WWN are used in zoning. The checking is run locally when the port number can make a match on that switch alone. When the port number is not enough, that switch has to query the remote switches to get the needed login information. This information is cached on the local switch until RSCN renders it stale.

If debugging is required, the local login data can be viewed using the "`portLoginShow pn`" command, where "pn" is the port number on that switch. The cache of remote logins can be viewed by making a query to the Name Server or using `zoneCheck` with two valid D_Ids, then use the "`cfgRemoteShow`" command.

Adding a New Switch

A "new" switch is a switch that has not been connected to a Fabric with zoning configured, and has no zone configuration data entered into it. If a switch has been connected to a Zone Fabric, or a configuration has been previously defined, the switch that has been configured for zoning may be returned to this "new" state by using the "`cfgClear`" command before connecting it to the zoned fabric.

When a "new" switch has been networked to a fabric, all the zone configuration data is immediately copied from the existing fabric into the "new" switch. By using the "`cfgShow`" command, the zoning information displayed will be the same on each switch in the Fabric.

Adding a New Fabric

Adding a new fabric that has no zone configuration information to an existing fabric is very similar to adding a new switch. All switches in the new fabric inherit the zoning configuration data. If a zone configuration is in effect, then the same configuration becomes the enabled configuration. The "`cfgShow`" command will display the same information on all switches in the newly formed Fabric.

Merging Two Fabrics

The simplest scenario for merging two fabrics is when both fabrics have identical zones and the same configuration enabled. The two fabrics will join to make one larger fabric with the same zone configuration in effect across this newly created fabric.

If two fabrics that both contain the same zone information are joined together, merging is more difficult. The two fabrics will attempt to merge the two sets of zone configuration databases together.

If the two fabrics have different zone configurations, then the two sets of information will be merged, or the ISL between the switches will be segmented if the two fabrics cannot join. See the section titled "Merging to v4.0 Fabric *on page 22*" for more information.

Merging fabrics is not possible:

- If there is a configuration mismatch, i.e. different zone configuration is enabled.
- If there is a type mismatch, i.e. the name of a zone object in one fabric is used for a different type of zone object in the other fabric.
- If there is a content mismatch, i.e. if the definition of one zone object is different from what is defined in the other fabric.

Splitting a Fabric

If an ISL goes down, causing the fabric to split into two separate fabrics, each new fabric will retain the same zone configuration.

If the ISL is replaced and no changes have been made to the zone configuration in either of the two fabrics, then the two fabrics are guaranteed to merge back into one single fabric. If any changes have been made to either zone configuration, then the fabrics will segment.

Enabling a zone in a Brocade Fabric

When a zone configuration is enabled, all zones within the configuration are enabled. All devices within an enabled zone are visible to one another; however, they cannot communicate outside their zone. Zones can overlap within a zone configuration.

When a zone configuration is enabled, the following happens:

1. All aliases are expanded if any are defined in the zone configuration.
2. Inconsistencies are checked, If inconsistencies are found, an error occurs and the previous state of the Fabric is preserved. For example, if zoning has been disabled, it will remain disabled.
3. Switch hardware is loaded with the zoning information.
4. Zone members are then loaded.
5. A Registered State Change Notification (RSCNs) are generated and sent out to the entire Fabric to notify the other switches in Fabric of the changes.

Transaction Model

Zoning commands are executed under what is known as the “transaction model”. This means copying all information from zone or cfg list at the start of a transaction creates a working copy of the defined configuration.

The following is a short list of some of the commands that can open a transaction:

`aliAdd`	Add member to a zone alias
`aliCreate`	Create a zone alias
`cfgAdd`	Add a member to a configuration
`qloopCreate`	Create a loop
`qloopRemove`	Remove a member from a configuration

The following commands can end a transaction:

`cfgClear`	Clear all zone configurations
`cfgSave`	Save a zone configuration in flash
`cfgEnable`	Enable a zone configuration
`cfgDisable`	Disable a zone configuration
`cfgTransAbort`	Abort a configuration transaction

When a transaction is opened, all new zoning information is placed in a "transactional buffer". Unless a transaction is closed by one of the "end transaction" commands, the changes will not be applied to the Fabric. A transaction is aborted by the `cfgTransAbort` command, or when another switch closes its transaction. When a transaction is closed, all new and existing zoning information is saved to memory and applied to the Fabric.

QuickLoop Fabric Assist

Fabric Assist allows a private host to talk to public/private targets located anywhere within the fabric (if no zoning exists). Private hosts and targets are put into a single Fabric Assist Zone, and are identified either by domain, port number or by WWN. The user will need QuickLoop and Zoning licenses to use these features.

Fabric Assist Zone Setup

New zoning commands with the prefix "`fazone`" that mirror other zoning commands are listed below: `fazoneCreate`, `fazoneAdd`, `fazoneDelete`, `fazoneRemove`, and `fazoneShow`

Private hosts are indicated within a fazone or alias by "H{}". Within a single fazone or alias, multiple initiators are detected during zone creation process. `CfgEnable` can fail if multiple initiators are found in a single fazone.

Fabric Assist Zone Creation

Each private host within a fazone has its own AL_PA domain space. A target that is zoned with multiple hosts may be given different AL_PAs. A max of 125 unique targets may be zoned with private hosts on any given switch. A fazone private host must be on a loop by itself. Sharing a loop with other nodes will cause the fazone to fail.

Fabric Assist Operation

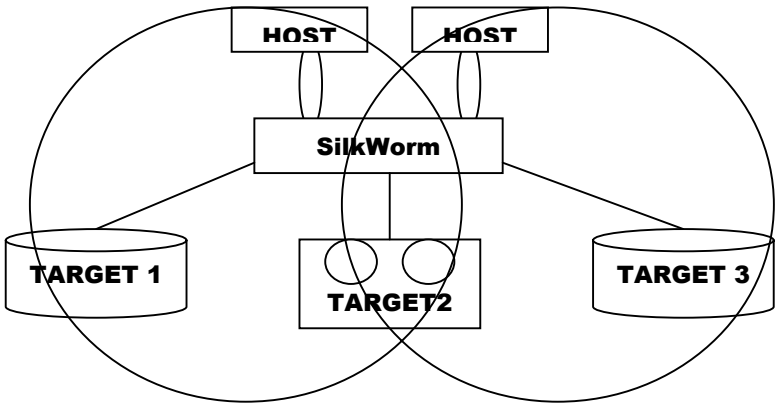
When "cfg" is enabled, ALPAs are created for all zoned targets that are online, on the private host's loop. The private host's loop is re-LIPed so that it may "see" any added ALPAs.

As additional targets join the fabric, if they are within the fazone, they will have an ALPA created on the private host's loop. This is triggered off of the RSCN. A target may be zoned with one or more private hosts, and will have a unique ALPA created on each host's loop. Loop targets that have an ALPA value shall be assigned the same ALPA as their phantom ALPA. Phantom ALPAs are consistent for a device as long as the switch where they were created is operational. When a switch reboots, the phantom addresses for the targets may change. This means that they are not consistent across rebooting of the switch. When a target leaves the fabric, their ALPAs are removed from the corresponding loops.

LIP Propagation

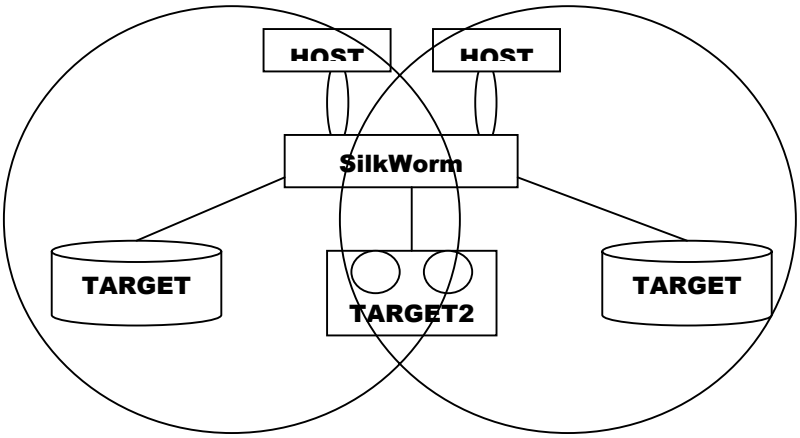
LIPs are only propagated to the private hosts. LIPs are not sent to the targets within a fazone. LIPs are only sent when a new phantom ALPA needs to be created, i.e. when a fazone target comes online. A loop of fazone targets that are re-LIPed, but do NOT add any new targets will not propagate a LIP to any private hosts. The private host loop is not LIPed when a phantom is removed.

Figure 5: Host Isolation Picture



- FazoneA contains Host1 and Targets1 and 2
- FazoneB contains Host2 and Targets 2 & 3
- Host1 is performing a tape backup to Target2 and Host2 reboots
- No LIPs are sent to Host1 or any of the targets
- Host1's backup operation is not interrupted

Figure 6: LIP Propagation Picture



- Target1 goes offline
  - Phantom removed from Host1
- Target1 comes back online
  - Host1 goes thru an LIP
- Target2 goes offline
  - Phantoms removed from both Host1 and Host2
- Target2 comes back online

Fabric Assist Debugging

Below is a list of commands that can help troubleshoot FA issues:

- `bloomAlpaShow`: Displays all APLAs, phantom or real, that exist on a loop
- `bloomPhantomShow`: Displays the phantom translation tables for the given port.
- `Setdbg "QL",9`: Displays the maximum level of Fabric Assist debug tracing.
- `FaDebugShow`: Displays the internal Fabric Assist tables.

Introduction to The Zoning Architecture

Discussions about "architecture" are typically philosophical in nature. Below are some guidelines for setting up zoning in your fabric, including some considerations.

1. Create a detailed diagram of the fabric, showing all the switches with their ISLs. The diagram will assist with accountability. It will help to account for every port in the fabric.
2. Create a "blowup" diagram of each switch in the fabric. This diagram will account for every port type in the fabric. (F_Port, FL_Port, E_Port etc.)
3. If the fabric is going to contain private loop devices, then the user will need to account for this. Refer to The Ten Rules of Zoning Architecture on page 21.
4. If the fabric is going to contain Brocade 2Gb based switches, the user will need to take this into account when setting up zoning, especially as it relates to QLFA (QuickLoop Fabric Assist). Refer to The Ten Rules of Zoning Architecture on page 21.
5. If the zoned fabric is going to contain unused ports, with nothing connected to them, the user may consider turning off the port. This is a decision that will affect the security of the fabric.
6. If the fabric is has multiple zones enabled within it, it is probably best to configure one zone at a time and then test it with the Zone Analyzer via Web Tools. Do not create all the zones at once; it will be troublesome to debug. After the first zone is setup in the fabric, the user may plug in devices and then test the connections to confirm that everything is functioning properly. This process may seem a little tedious, but it will save time and money trying to debug this after creating all the zones and then plugging in the devices.

What is described above will work for almost any user. The one issue left to cover is manageability. Manageability means that an unauthorized user could telnet into any of the switches in the fabric described above or connects to it via Web Tools tamper with the zone configuration in the Fabric.

This is controllable using:

1. Physical access to the Fabric
2. Access to IP addresses of the switches
3. Password to the switches

Why Secure Fabric OS

Some of the issues with security in the SAN are listed below:
SAN Security Risk

1. Unauthorized and/or unauthenticated SAN access
2. Insecure Management Access
3. World Wide Name (WWN) spoofing
4. Management controls allowed from different access points in the Fabric

Secure Fabric OS Solutions

1. Multilevel password controls
2. ACL and encryption of passwords to certain interfaces
3. Port Level ACL
4. Trusted Switches, Public Key-based authentication and digital certificates

With Secure Fabric OS, the following security components are included:

1. Fabric Configuration Server: One or more switches act as trusted devices in charge of zoning changes as well as other security-related features.
2. Management Access Controls (ACL): Management policies and ACLs control access to the switch from different management services.
3. Secure Management Communication: Secure management communications interface to the fabric by encrypting certain data elements, such as passwords.
4. Switch Connection Controls: ACLs and digital certificates within the switch authenticate new switches and ensure that they can join the fabric.
5. Device Connection Controls: Port-Level ACLs lock particular WWNs to certain physical ports on the switch.

As part of Zoning Architecture, the user will need to determine which of the two basic Zoning Architectures will work best for their fabric. With time and planning, the basic hard zone configuration will work for most sites. If a site has additional security needs, the user will need to add the additional layer of Secure Fabric OS to lock down the fabric, in addition to the standard Zoning Architecture.

The Ten Rules of Zoning Architecture

Rule 1: Type of Zoning (Hard, Soft, Hardware Enforced, Soft Porting) – If security is a priority, then a Hard Zone-based architecture coupled with Hardware Enforcement is recommended

Rule 2: Use of Aliases – Aliases are optional with zoning. Using aliases should force some structure when defining your zones. Aliases will also aid future administrators of the zoned fabric. Structure is the word that comes to mind here.

Rule 3: Does the site need an extra level of security that Secure Fabric OS provides? – Add Secure Fabric OS into the Zone Architecture if extra security is required.

Rule 4: From where will the fabric be managed? – If a SilkWorm 12000 is part of the fabric, then the user should use it to administer zoning within the Fabric

Rule 5: Interoperability Fabric – If the fabric includes a SilkWorm 12000 and the user needs to support a third-party switch product, then he will only be able to do WWN zoning, no QuickLoop etc. This is documented in the SilkWorm 12000 documentation.

Rule 6: Is the fabric going to have QLFA or QL in it? – If the user is running Brocade Fabric OS v4.0, then there are a couple things to consider before creating and setting up QLFA zones:

- QuickLoop Zoning
  QL/QL zones cannot run on switches running Brocade Fabric OS v4.0. Brocade Fabric OS v4.0 can still manage (create, remove, update) QL zones on any non-v4.0 switch.
- QuickLoop Fabric Assist
  Brocade Fabric OS v4.0 cannot have a Fabric Assist host directly connected to it. However, Brocade Fabric OS v4.0 can still be part of a Fabric Assist zone if a Fabric Assist host is connected to a non-v4.0 switch.

Rule 7: Testing a (new) zone configuration. – Before implementing a zone the user should run the Zone Analyzer and isolate any possible problems. This is especially useful, as fabrics increase in size.

Rule 8: Prep work needed before enabling/changing a zone configuration. – Before enabling or changing a fabric configuration, the user should verify that no one is issuing I/O in the zone that will change. This can have a serious impact within the fabric like databases breaking, node panics etc. This goes the same for disk(s) that are mounted. If the user changes a zone, and a node is mounting the storage in question, it may "vanish" due to the zone change. This may cause nodes to panic, applications to break etc. Changes to the zone should be done during preventative maintenance. Most sites have an allocated time each day to perform maintenance work.

Rule 9: Potential post work requirements after enabling/changing a zone configuration. – After changing or enabling a zone configuration, the user should confirm that nodes and storage are able to see and access one another. Depending on the platform, the user may need to reboot one or more nodes in the fabric with the new changes to the zone.

Rule 10: LUN masking in general. – LUN Masking should be used in conjunction with fabric zoning for maximum effectiveness.

Merging to v4.0 Fabric

If the user has a SilkWorm 12000-based fabric, or other switches running Brocade Fabric OS V4.0, firmware can operate in the same fabric with the SilkWorm 3800 switches running Fabric OS 3.0.1a or later firmware.

Switches running Brocade Fabric OS V4.0 firmware can operate in the same fabric with all SilkWorm 2000 series switches running v2.6_Beta4 or later.

All 8-port and 16-port SilkWorm 2000 and 3000 family switches that are to communicate with a SilkWorm 12000 must have the Core Switch PID format enabled (i.e. set to 1). This is done via the "configure" command after logging into the switch.

```
Switch0:admin> configure
Configure…
Fabric parameters (yes, y no, n): [no] y
….
Core Switch PID Format: (0..1) 1
```

Note: If this is not done on all the switches that will be a part of the Brocade Fabric OS V4.0 based fabric, and then the Fabric will segment.

Appendix A: Testing Zoning Vulnerability

There are two simple tests that a field person or an end user can do to test whether zoning works or not.

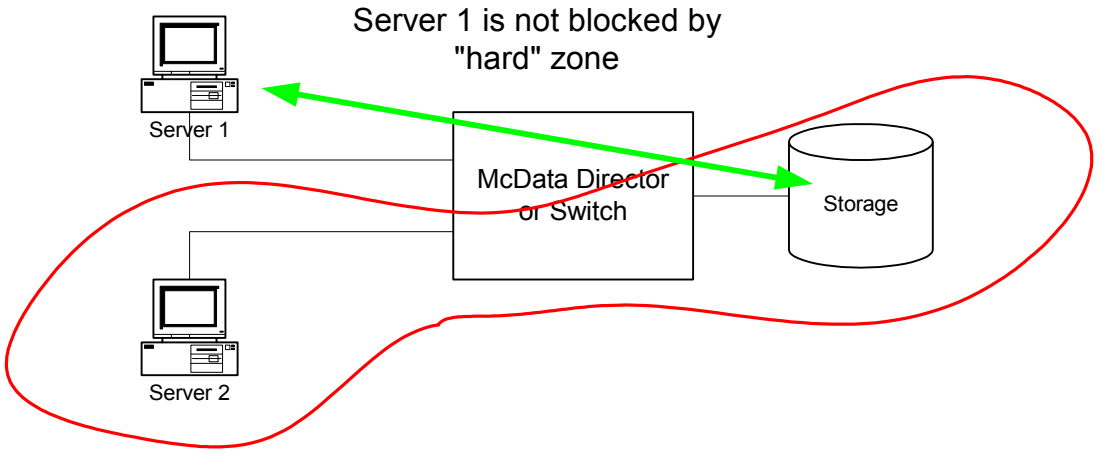
McData has caused a lot of confusion in the customer base by misrepresenting their inability to do “hardware-enforced zoning”, by calling it “hard zoning”. This is their ability to zone by ports. Unlike the Brocade SilkWorm 2000 family which enables hardware zoning by ports, McData’s port zoning is merely a reverse lookup of WWN for that port.

Their port zoning is a less secure, software-based zoning with no actual blocking of inappropriate frames. Brocade SilkWorm 2000 family-based switches stop the data in the hardware ASIC if zoned by port. With the Brocade based 2Gb products, users zone completely by “Hardware Enforcement” for both port-based and WWN-based zones. Below describes a very simple test that will show McData’s Hard Zoning and demonstrate that their zoning is still software enforced, but unsecured.

Test Configuration

- McData ED-6064 Director
- (2) Hosts (Windows NT, Windows 2000)
- (2) HBA’s (testing was done using Emulex LP9002L)
- (1) Array that has F_Port ability, this is due to the fact that there Director or ED-3032 and 16 port switches have no loop support. You could use their ES-1000, but you are only able to do zoning WWN based zoning.
- Load Generator (Iometer was used for the testing)

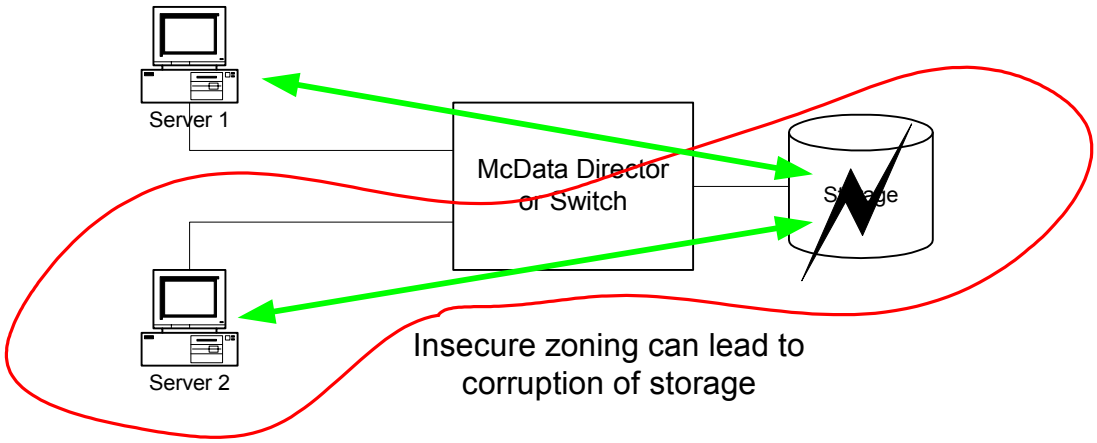
Figure 7



Test Process

1. Connect the systems as shown in Figure 7 using any available port on the Director or switch. Make sure both nodes can see the LUN configured on the array via LDM and that it's formatted and a drive letter is assigned to it.
2. Have Server 1 mount the storage and establish I/O using the Iometer load generator.
3. Create a McData "Hard Zone" using the port number of the storage and Host 1 using the EFCM. After making that Zone Set active, your I/O will still continue.
4. While I/O is still going on between Server 1 and the storage, deactivate that Zone Set and create another Zone set that contains Server 2 and the storage. After you activate the new Zone Set, you will notice a pause of 30 to 40 seconds. Then you will see I/O resume to the storage in question from Server 1. This Server should NOT be able to access the storage in a zone it does not belong to.
5. By looking at Iometer or by standing in front of the Director, you will see I/O coming from Server 1 to the storage as shown in Figure 8.

Figure 8



6. With I/O from Server 1 still going through the Hard Zone to the storage, begin Iometer on Server 2. The I/O will start, but may exhibit errors on Server 1 and Server 2 over time if they write to the same data spaces. In some of the tests, I was able to cause a major error on an FPM (Fibre Port Module) card. This also causes trouble in one of the Windows 2000 Servers to while trying to update some information regarding its storage configuration. Rebooting the Windows 2000 Server cleared it up.

This same test can be repeated with WWN Zoning on McData with the same results. These results show how insecure software-based zoning can be.

The same test can be repeated using Brocade SilkWorm 2000 family switches showing secure Hardware Zoning which blocks inappropriate access.

With the SilkWorm 3800, and the soon-to-be-released SilkWorm 12000, Hardware Enforced Zoning is based upon Port numbers or WWN, which stops unauthorized traffic. Either type of zoning is "enforced" in the ASIC's of these Bloom-based switches.

Results

The test uses a McData ED-6064 running firmware 1.02.0023. The hosts used were Windows 2000 using Emulex LP9002L in a Point-to-Point configuration and can plug into any port.

The HBAs were tested with RSCN on and off, but it did not seem to make a difference. Some HBAs support dismounting the storage when the RSCN variable is changed, however this is pushing security out to the edge rather than into the core switching. It is also less secure, as it requires specific administration for it to work.

The storage used was the Compaq HSG60/MA6000 configured with a single LUN with general access. Many storage systems have LUN-level zoning, which can help prevent access, however switch zoning can be viewed as a supplement to this security. This way, if an administrator forgets to change the LUN zoning or makes a mistake, the devices are still blocked by the switches in the fabric. LUN zoning is not a solution itself.

Once the hosts were up and running, the LDM in Windows 2000 was brought up to make sure both nodes could see the storage. The storage was formatted and assigned a drive letter. Iometer was invoked, and set up to run on the disk controlled by LDM.

While Iometer was running on the Compaq LUN, EFCM was brought up and the server and storage were zoned together. The I/O continued as expected.

Through EFCM, the Zone Set was deactivated and a new Zone Set created using the other server and the Compaq storage. Even after making this new Zone Set active, I/O was still coming from the first node (that is NOT part of this new Zone Set) to the Compaq storage that is part of this active Zone Set.

Next Iometer was setup on Server 2 and started, causing Server 1 and 2 to both accesses the same storage, even though only one server is properly zoned. After a period of time, the I/O stopped with a corrupted message from the node that is not a part of the zone. This also caused the McData FPM card in question to suffer a major error and be rendered unusable.

This test was repeated on a SilkWorm 12000 and, as expected with Brocade Hardware Enforced Zoning, once the zones were changed the server could not access storage if it was zoned out. The Windows 2000 Operating System reported that the storage was not accessible, which is both desirable and expected. This was also repeated with WWN-based zoning, proving that new advanced zoning enforces both port and WWN-based zones in the ASIC.

Conclusion

McData's Hard Zoning or Port level zones are NOT hardware-enforced, but are less secure software-based port zoning with a lookup to the name server. Devices that were mounted or get the address of a storage system are never blocked from inappropriate access. The McData solution pushes the responsibility of securing the data out to the HBA, storage or administrators, rather than the switch where it is more enforceable.

McData uses "hard zoning" as a marketing term for their port-level zoning in an attempt to confuse end users into believing that they have a secure product, which they do not. It cannot compare to Brocade's Hardware-Enforced zoning in the SilkWorm 2000 line, let alone the more advanced hardware zoning in the SilkWorm 3800 and 12000-product line.

Copyright

IMPORTANT NOTICE

This document is the property of Brocade. It is intended solely as an aid for installing and configuring Storage Area Networks constructed with Brocade switches. This document does not provide a warranty to any Brocade software, equipment, or service, nor does it imply product availability. Brocade is not responsible for the use of this document and does not guarantee the results of its use. Brocade does not warrant or guarantee that anyone will be able to recreate or achieve the results described in this document. The installation and configuration described in this document made use of third party software and hardware. Brocade does not make any warranties or guarantees concerning such third party software and hardware.

Brocade Communications Systems, Incorporated
1745 Technology Drive
San Jose, CA 95110

Evaluation Form

Your feedback is valued by Brocade. In particular, we are interested in understanding how the SOLUTIONware report helped make a difference in a SAN task, problem, or decision. Please FAX this form back to: FAX (408) 392-5200.

SOLUTIONware Title: **Brocade Guide to Understanding Zoning**

Document number: 53-0000213-01

Review:

What other subjects would you like to see SOLUTIONware reports on?

Please rate your overall satisfaction: ( )very satisfied ( )satisfied ( )not satisfied

Please identify yourself as belonging to one of these groups:

( ) End-User Customer

( ) Fabric Integrator

( ) Master Reseller

( ) Partner

( ) Brocade Employee

( ) Brocade OEM

( )Other