QuickLoop Guidelines in a Secure Fabric OS environment

Version 1.0

May 21, 2003

TABLE OF CONTENTS

Notes and Guidelines 3
1. Overview and Objectives 4
2. Understanding QuickLoop and QuickLoop Zoning Design 4
2.1 QuickLoop 4
2.2 QuickLoop Basics 4
2.3 Address Translation 5
2.4 QuickLoops and Fabric Zoning 5
2.5 QuickLoop Zoning and Fabric Zoning 5
2.6 QuickLoop Zones 6
3 QuickLoop Design and Deployment Considerations when used with Secure Fabric OS 6
3.1 Guidelines for QuickLoop Zoning in a Secure Fabric OS Architecture 7
3.2 Designing SANs With Secure Fabric OS and QuickLoop Zones 7
3.3 QuickLoop Deployment 8
3.3.1 Configuring QuickLoop Zones 8
3.3.2 Create a QuickLoop 8
3.3.3 Define a QuickLoop Zone 9
3.3.4 Define a QuickLoop Zone Configuration 9
3.4 QuickLoop Zoning Plan 10
3.5 Planning for Secure Fabric OS Security Measures 10
4 Case Study- Implementing QuickLoop Zoning in a Secure SAN 11
4.1 QuickLoop Zoning in a Secure Fabric Environment 11
4.2 QuickLoop Zoning Validation 15
A.1. Brocade Documentation 16
A.2. Additional Resource Information 16

Notes and Guidelines

Note: Notes emphasize important information.

Guideline: Guidelines are recommendations for consideration. The adoption of these guidelines is a function of the user's ability to interpret and correlate relevant SAN information and make decisions based upon their organization and SAN requirements.

Warning: Warnings alert you to potential damage to hardware, firmware, software, or data.

1. Overview and Objectives

This document is directed at Partners and End Users who are planning on implementing QuickLoop in a Secure Fabric OS environment. It is meant as a supplement to the Brocade Users Manuals and SilkWorm Design, Deploy and Manage Guide (DDM). The first section provides an overview of QuickLoop and QuickLoop Zoning, the next section covers QuickLoop design and deployment considerations in a Secure SAN environment and the final section is a Case Study that ties the content together into an elaborate configuration to apply the concepts covered in this document.

2. Understanding QuickLoop and QuickLoop Zoning Design

The following section provides an overview of QuickLoop and QuickLoop Zoning.

2.1 QuickLoop

Brocade QuickLoop is a unique Fibre Channel topology that combines arbitrated loop and fabric topologies. An arbitrated loop or private loop supports communication between private devices that are not fabric aware or capable. Public or private hosts located elsewhere on the fabric can access private targets on arbitrated loops. Devices attached to QuickLoop can communicate with all other devices attached to the same QuickLoop. However, private host devices attached to QuickLoop can communicate only with devices within the same QuickLoop. Public devices in an arbitrated loop mode are considered private devices when connected to QuickLoop ports.

2.2 QuickLoop Basics

A QuickLoop consists of multiple private arbitrated looplets (a set of devices connected to a single port) connected by a fabric. All devices in a QuickLoop share a single AL_PA bit-map and operate as if they are in one loop. This allows private devices to communicate with other devices over the fabric, provided they are in the same QuickLoop. A QuickLoop can consist of selected devices or looplets connected to the ports of one switch, or to a cascaded switch pair.

QuickLoop can be enabled or disabled on the entire switch or on individual ports. When QuickLoop is disabled on a port, that port returns to Fabric mode. When QuickLoop is enabled on a port, the device on that port is forced into private mode operation.

QuickLoop can be enabled on single switch or dual switch configurations, known as “QuickLoop partners”. QuickLoop can include all or some of the ports on a switch or switch pair, and can have several private hosts.

A switch can be configured to operate in any of the following three modes:

- *QuickLoop mode*
All ports on the switch, except for E_Ports or loopback ports, are enabled for QuickLoop and participate in a logical Private Loop Direct Attach (PLDA). This mode can be set by the telnet command **`qlEnable`**, or it can be configured in the Zoning configuration by using the **`qloopcreate`** command.
- *Fabric mode*
No ports are QuickLoop-enabled, and all ports operate as FC-FLA compliant devices. This mode can be set by the telnet command **`qlDisable`**.

• *Mixed mode*
Each port is enabled for QuickLoop separately. The port operating mode can be reset during operation. Ports set to QuickLoop become looplets on the same switch. Particular ports can be taken in and out of the QuickLoop by entering the **`qlportdisable`** and **`qlportenable`**.

2.3 Address Translation

Address translation is transparent and requires no user interaction. By using the hardware translative mode (also known as phantom mode), a device not physically located in a looplet can be addressed by a unique AL_PA in that looplet. There are two hardware translative modes available to a QuickLoop enabled switch:

• *Standard translative mode*
Allows a public host to communicate with private target devices across the fabric. Standard translative mode is available as an integral part of Fabric OS, and does not require QuickLoop; the hardware supports it by default. The switch will probe the device and populate the name server with the private device information so as to notify other public devices of the private device.
• *QuickLoop mode*
Allows a private host to communicate with private target devices across the fabric when configured in the same QuickLoop. LIPS propagate to all devices in a QuickLoop. Zoning can limit LIP propagation.

Note: Refer to the *Brocade QuickLoop User's Guide Version 3.1.0 (publication number 53-0000513-02)* for detailed information about QuickLoop.

Note: QuickLoop is supported on Fabric OS v3.1.0 switches; however, it is not supported on Fabric OS v4.x switches. For this reason Private Hosts can not be directly connected to switches with Fabric OS 4.x. However, Private Targets may be connected to switches with Fabric OS 4.x (the **`portcfglport`** command may be used to lock down the device as a Private Target) and can be communicated through by Translative mode or QuickLoop Fabric Assist (refer to the *Brocade QuickLoop User's Guide Version 3.1.0 publication number 53-0000513-02* for detailed information about QuickLoop/Fabric Assist). Please refer to the switch vendors support information regarding Translative mode or QuickLoop/Fabric Assist for specific devices.

2.4 QuickLoops and Fabric Zoning

Fabric Zones and QuickLoops work independent of each other until QuickLoop Zones are created in the fabric. Fabric Zones and QuickLoops can co-exist in the same fabric and QuickLoop devices can be included within a fabric zone configuration. However, while fabric devices within the Fabric Zones can only see other devices in that zone, QuickLoop devices can be seen by other Private devices within each QuickLoop. Before any QuickLoop Zones are implemented the QuickLoop is one consistent PLDA address space. Until a specific "QuickLoop Zone" is created, QuickLoop devices that might exist on one switch or a pair of switches are part of a "Single Private Loop", in which all devices can see any other device that is part of that QuickLoop.

Guideline: In a Secure Brocade Fabric it is important to create pure QuickLoop Zones (every member of a pure QuickLoop Zone must be a qlenabled port within a single QuickLoop and a Private device must be attached) and ensure they remain QuickLoop Zones during user configuration changes (i.e. adding/removing private hosts or storage or adding/removing switches either by connecting or removing ISLs either explicitly or due to a device or ISL outage).

2.5 QuickLoop Zoning and Fabric Zoning

In addition to Fabric Zoning, zoning can also be used to zone QuickLoop devices explained in Chapter 3 *(Brocade Advanced Zoning User's Guide Version 3.1.0/4.1.0 publication number 53-0000523-02*). By

partitioning selected devices within a QuickLoop into a QuickLoop Zone you can enhance management of a Fibre Channel Arbitrated Loop (FC-AL) in a legacy environment.

Guideline: To ensure the most secure SAN environment one should implement both Fabric Zones and QuickLoop Zones in a Secure Fabric OS environment. This prevents both accidental and un-intended access between devices.

2.6 QuickLoop Zones

QuickLoop Zones are hardware enforced. Switch hardware prevents unauthorized data transfer between ports within the zone allowing devices to be partitioned into zones to restrict system access to selected devices. When devices are included in a zone, they are visible only to other devices within that zone. QuickLoop zone members are designated by looplet (domain, port number), or by Arbitrated Loop Physical Address (AL_PA).

Fabric Zones and QuickLoop Zones are independent of each other; both types of zones can co-exist in the same zone configuration and QuickLoop devices can be included within a fabric zone configuration. However, QuickLoop Zones can only contain qlenabled ports. In QuickLoop Zoning, devices within a QuickLoop can be partitioned off within that QuickLoop to form QuickLoop zones; in other words, a QuickLoop Zone is a subset of a QuickLoop and can include only QuickLoop devices. Every member of a QuickLoop Zone must be a "qlenabled" port within a single QuickLoop and a Private device must be attached.

QuickLoop Zoning can protect devices from disruption by unrelated devices during a critical process, for example, preventing the propagation of LIPs during a tape backup session. In a QuickLoop Zone, transmission of the loop initialization primitive (LIP) signal and loop initialization are controlled by the switch; the LIP is transmitted only to looplets within the affected zone; other looplets on the QuickLoop are not affected. In this way, unwanted disruption to devices can be controlled.

3 QuickLoop Design and Deployment Considerations when used with Secure Fabric OS

Zoning is an important element of a secure and healthy SAN. Zoning does have an impact on SAN designs. The *Brocade Advanced Zoning User's Guide Version 3.1.0/4.1.0 (publication number 53-0000523-02)* provides a solid overview of how zoning works and guidelines for implementing zoning. This section highlights key elements of QuickLoop Zoning that relate to a Secure Brocade SAN design.

To rephrase the concepts covered above there are 3 distinct modes of operation that need to be considered in a Secure Fabric OS environment with QuickLoop:

1. By far the most Secure Access restriction for QuickLoops is Zoning within a QuickLoop: In a Zoning configuration which contains one or more pure QuickLoop Zones that have a subset of devices within the same QuickLoop, QuickLoop devices will no longer be able to access every other device in the QuickLoop, but will be only limited to access the subset of devices defined in the same zone.
2. Mutually exclusive access between a QuickLoop and Fabric Zones: In a Zoning configuration which contains only Fabric or only QuickLoop devices, a QuickLoop device can only access devices within the same QuickLoop, and a Fabric device can only access devices within its Fabric Zone.
3. The least Secure Access restriction is Shared access to QuickLoop device with no pure QuickLoop Zones present: In a Zoning configuration which contains one or more Zones that have both QuickLoop devices and Fabric devices, Fabric devices can access the QuickLoop devices in the same zone, and all QuickLoop devices in the same QuickLoop can access to each other.

3.1 Guidelines for QuickLoop Zoning in a Secure Fabric OS Architecture

If the user should wish to create a Secure Fabric with Secure QuickLoop Zones, the following rules apply when configuring zones.

Rule 1: QuickLoop Zones are required to prevent unintended disruption by other devices, this can be as simple as a single zone entity around a single private target device or as complex as a separate QuickLoop Zone for each Private Host / Private Target pair.

Guideline: To Secure a QuickLoop fabric against any external event that may change the QuickLoop Zoning configuration (i.e. introduction of new host or ISL disconnection), one should create a single device QuickLoop Zone on any switch that contains QuickLoop devices. (The Case Study at the end provides an example of creating a single device QuickLoop Zone.) This acts to prevent an unintentional change in the operating modes from a SAN with pure QuickLoop Zones to a SAN without any QuickLoop Zones present, and prevents a newly entered QuickLoop device from gaining access to storage devices it should not have explicit access to.

Rule 2: All Private devices required to communicate to each other are required to exist in the same QuickLoop. The QuickLoop and QuickLoop Partner switches must be defined in the zoning configuration.
Rule 3: Evaluate if the fabric will have QuickLoop (QL) or QuickLoop Fabric Assist (QLFA) in it. If the user is running Brocade Fabric OS v4.x consider the following before creating and setting up QLFA zones:

QuickLoop Zoning
QuickLoop/QuickLoop Zones cannot run on switches with Brocade Fabric OS v4.x. However, Brocade Fabric OS v4.1.0 can still manage (create, remove, update) QuickLoop Zones on any non-v4.1.0 switch.
QuickLoop Fabric Assist
Brocade Fabric OS v4.x cannot have a QLFA host directly connected to it. However, Brocade Fabric OS v4.x can still be part of a QLFA Zone if a QLFA host is connected to a non-v4.1.0 switch.
Please refer to the switch vendors support information regarding support for QuickLoop/Fabric Assist (QLFA)

Rule 4: Testing a (new) zone configuration. Before implementing a zone, the user should run the Zone Analyzer from Web Tools to isolate any possible problems. This is especially useful as fabrics increase in size.
Rule 5: Zone changes in a production fabric can result in a disruption of I/O under conditions where an RSCN is issued as a result of a zone change and the HBA is unable to process the RSCN fast enough. Though RSCNs are a normal part of a functioning SAN, the pause in I/O may not be acceptable. For these reasons, it is recommended to perform zone changes only when the resulting behavior is predictable and acceptable. Changing HBA drivers can rectify the situation.
Rule 6: After changing or enabling a zone configuration, the user should confirm that the nodes and storage are able to identify 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.

Note: Inter-operability Fabric - If the fabric includes a Brocade switch and the user is supporting a third-party switch product, QuickLoop and QuickLoop Zoning are not supported.

3.2 Designing SANs With Secure Fabric OS and QuickLoop Zones

A secured fabric must be *entirely* secured and all switches in a secured fabric must run a version of Fabric OS that supports security and these switches must be licensed to run security. Please reference the *Brocade Secure Fabric OS User's Guide Version 3.1.0 /4.1.0 (publication number 53-0000526-02)* for further detail about Secure Fabric OS. Zoning allows the hosts to access specific storage devices on the SAN. For those

SANs with multiple OS platforms, zoning allows for OS separation and co-existence. With no zoning defined on the SAN, any device can see any other device. This is the default setting. Once zoning is in place, all devices must be members of a defined zone. Those devices that are not will be blind to all others. This section will provide some guidelines as to QuickLoop zoning plan definition. For additional information reference the *Brocade SilkWorm Design, Deployment, and Management Guide SAN DDM Version 2.0 (publication number 53-0000366-01)*. QuickLoop Zoning requires careful thought and planning. Armed with the information in the previous section, and understanding the requirements, allows the creation of a zoning plan. Creativity is important here as there is no one "correct" zoning configuration for a given SAN fabric configuration. In general, follow any specific zoning recommendations provided by the switch vendor.

Guideline: When implementing QuickLoop in a Secure environment, ensure that all QuickLoop devices are part of at least one QuickLoop Zone.

Guideline: Be cautious of configuration changes that would change a QuickLoop Zone to a mixed Fabric Zone or no QuickLoop Zoning enforcement at all (i.e. adding/removing private hosts or storage or adding/removing switches either by connecting or removing ISLs either explicitly or due to a device or ISL outage).

3.3 QuickLoop Deployment

3.3.1 Configuring QuickLoop Zones

To configure QuickLoop zoning, perform the following:
- Create a QuickLoop
- Define a QuickLoop Zone
- Define a QuickLoop Zone Configuration

3.3.2 Create a QuickLoop

There are two ways to create a QuickLoop :
1. The first way to create a QuickLoop is effective for every port on the switch, one may use the **`qlenable`** command or the **`qloopcreate`** command. The **`qloopcreate`** command allows the user to reference up to two switch WWNs for a QuickLoop. This will create a QuickLoop in the zoning definition. In two-switch QuickLoop configurations the **`qlpartner`** command is required to indicate the partner switch as well.
2. The second way is to create a QuickLoop on a port-by-port basis. Each port is enabled for QuickLoop separately. Particular ports can be taken in and out of the QuickLoop by entering the **`qlportenable`** and **`qlportdisable`**.

However, this is not a QuickLoop Zone yet, it only defines a region for the QuickLoop PLDA naming space. If one wishes to create a QuickLoop Zone a QuickLoop should be defined and present in the zoning configuration. Refer to the *Brocade QuickLoop User's Guide Version 3.1.0 (publication number 53-0000513-02)* for additional information regarding creating a QuickLoop.

Example of **`qloopcreate`**:

```
switch:admin> qloopcreate "quickloop1","10:00:00:60:69:c0:07:19"
switch:admin>
switch:admin> cfgshow
Defined configuration:
 qloop: quickloop1
                10:00:00:60:69:c0:07:19

Effective configuration:
 no configuration in effect
```

3.3.3 Define a QuickLoop Zone

A QuickLoop Zone is a group of L_ports or AL_PAs that can communicate with each other. These ports and AL_PAs must reside within the same QuickLoop. To be a QuickLoop Zone, every member must be either a looplet (L_port) or an AL_PA within a single QuickLoop. QuickLoop Zones can overlap looplets, but they must be confined to a single QuickLoop. QuickLoop Zones are hardware enforced, but zones within a single looplet are not enforceable; therefore, it is recommended that you do not partition devices within a single looplet into different zones.

Example :

```
switch:admin> zonecreate "qlzone1","1,0;1,1"
switch:admin> zonecreate "qlzone2","1,6;1,7"
switch:admin> zonecreate "qlzone3","quickloop1[01,02,04,e0,e1,e2]"
switch:admin> zonecreate "qlzone4","1,4;1,5;quickloop1[ca,cb]"
switch:admin>
switch:admin> cfgshow
Defined configuration:
 zone:  qlzone1 1,0; 1,1
 zone:  qlzone2 1,6; 1,7
 zone:  qlzone3 quickloop1[01,02,04,e0,e1,e2]
 zone:  qlzone4 1,4; 1,5; quickloop1[ca,cb]
 qloop: quickloop1
                10:00:00:60:69:c0:07:19

Effective configuration:
 no configuration in effect

switch:admin>
```

3.3.4 Define a QuickLoop Zone Configuration

To define a QuickLoop Zone configuration, assign a zone configuration name and specify the QuickLoop Zones by zone name. If a QuickLoop was created using the “qloopcreate” this should be included in the zone configuration as well.

Note: The “qloop” name is only required if all devices on the switch will be Private devices and all ports will be “qlenabled”.

An example of a QuickLoop Zone configuration is:

```
switch:admin> cfgcreate "QuickLoopcfg","qlzone1;qlzone2;qlzone3;qlzone4;quickloop1"
switch:admin> cfgshow
Defined configuration:
 cfg:   QuickLoopcfg
                qlzone1; qlzone2; qlzone3; qlzone4; quickloop1
 zone:  qlzone1 1,0; 1,1
 zone:  qlzone2 1,6; 1,7
 zone:  qlzone3 quickloop1[01,02,04,e0,e1,e2]
 zone:  qlzone4 1,4; 1,5; quickloop1[ca,cb]
 qloop: quickloop1
                10:00:00:60:69:c0:07:19
Effective configuration:
 no configuration in effect

switch:admin> cfgenable "QuickLoopcfg"
Starting the Commit operation...
Setting switch to Quick Loop mode,
Committing configuration...done.
Initialize Quick Loop...
cfgEnable successfully completed
switch:admin>
switch:admin> cfgshow
Defined configuration:
 cfg:   QuickLoopcfg
```

```
                qlzone1; qlzone2; qlzone3; qlzone4; quickloop1
 zone:  qlzone1 1,0; 1,1
 zone:  qlzone2 1,6; 1,7
 zone:  qlzone3 quickloop1[01,02,04,e0,e1,e2]
 zone:  qlzone4 1,4; 1,5; quickloop1[ca,cb]
 qloop: quickloop1
                10:00:00:60:69:c0:07:19

Effective configuration:
 cfg:   QuickLoopcfg
 zone:  qlzone1 1,0
                1,1
 zone:  qlzone2 1,6
                1,7
 zone:  qlzone3 quickloop1[01,02,04,e0,e1,e2]
 zone:  qlzone4 1,4
                1,5
                quickloop1[ca,cb]
 qloop: quickloop1
                10:00:00:60:69:c0:07:19
switch:admin>
```

Note: Although it is possible to have many zoning configurations defined on a fabric, there is only one active zoning configuration allowed.

3.4 QuickLoop Zoning Plan

This section will provide some guidelines as to the QuickLoop Zoning plan definition. For additional zoning planning and guideline information reference the *Brocade SilkWorm Design, Deployment, and Management Guide SAN DDM Version 2.0 (publication number 53-0000366-01)*.

QuickLoop Zoning Plan Checklist

1. Gather the list of host and storage devices to be zoned from the device spreadsheet.
2. Define the storage requirements for each host based upon software application requirements.
3. Adhere to recommended storage device configurations such as LUN masking, LUN security, and other specific features supported by the vendor.
4. Consider specific host requirements for storage value-added feature sets such as Server Free backup, LUN snapshots, or LUN mirroring over distance.

3.5 Planning for Secure Fabric OS Security Measures

There are many SAN Security measures that should be in place before implementing Secure Fabric OS (SFOS). Refer to the *Brocade Secure Fabric OS User's Guide Version 3.1.0 /4.1.0 (publication number 53-0000526-02)* , *Brocade SilkWorm Design, Deployment, and Management Guide SAN DDM Version 2.0* and the *SAN Security: A Best Practices Guide Revision 2 (publication number GA-RG-250-00)* for more in-depth coverage of these SAN Security measures.

Guideline: One specific feature of Brocade Secure Fabric OS that can be used in conjunction with QuickLoop Zoning is the Device Connection Control (DCC) policy, which allows only specific devices into the fabric (per their WWNs) from a specific port or group of ports. The default DCC policy is set to "No Policy": any device can connect to any port. The powerful combination of the DCC policy and Hardware Enforced Zoning prevents rogue connection attempts and accidental connections from gaining access or disrupting devices in the fabric.

4 Case Study- Implementing QuickLoop Zoning in a Secure SAN

This Case Study is intended to provide an example mixed Fabric and QuickLoop topology in which we can apply the Guidelines from above to ensure a Secure environment for device access.

4.1 QuickLoop Zoning in a Secure Fabric Environment

The case study SAN consists of one fabric (Figure 4-1). This fabric contains two switches cascaded together. The switches are connected with one ISL for simplicity. The attached hosts include: Host A (Public Host), Host B (Public Host). The attached storage includes: Target 1 (Private Target), Target 2 (Public Target). There are also two un-attached devices: Host C (Private Host), and Target 3 (Private Target). The switches have been "qlpartnered" and the QuickLoop has been created on a port-by-port basis.

To create this Case Study environment the User enabled each port for QuickLoop separately. As indicated in Chapter 1 ports set to QuickLoop become looplets of the same switch. Particular ports can be taken in and out of the QuickLoop by entering the **`qlportdisable`** and **`qlportenable`** so that there are a mix of QuickLoop and Fabric devices on each switch. This is a fairly complex configuration but provides us a good base to understand the relationship between QuickLoop Zones and Fabric Zones in a Secure San environment. This can be considered a "Mixed Mode" environment.

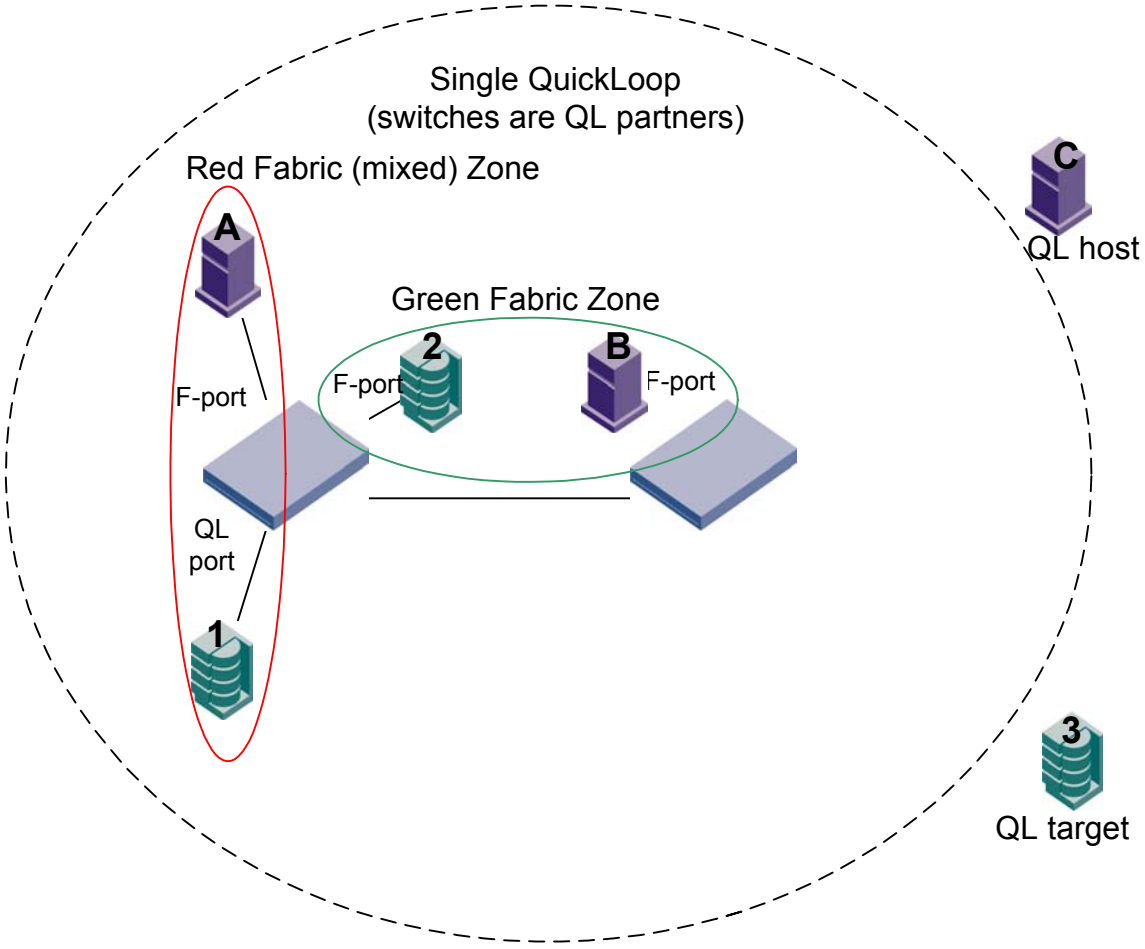
In this case study, two Zones have been defined :

1) A Red Zone consisting of one Public Host (A) and one Private Target (#1). In this case the Private Target #1 was configured as a QuickLoop Port and Host A communicates to Target #1 through Translative mode. This can be considered a Mixed Zone.
2) The other Green Zone consists of one Public Host (B) and one Public Target (#2). In this case the Public Target #2 is a fabric device and Host B communicates to Target #2 through Fabric mode. This is a pure Fabric Zone.

At this point in the example, there are no QuickLoop Zones defined in the Zoning configuration. The end result is a Single QuickLoop Address Space that spans the 2 switches.

One great concern in this scenario occurs if Host C or Target #3 is added to the Fabric at this time on "qlenabled" ports. In this case Host C could see Targets #1 and #3 because they are part of the same QuickLoop and there are no pure QuickLoop Zones present in the configuration. Also, the newly introduced Host C and Target #3 could disrupt Target #1 because a LIP from Host C or Target #3 would cause a LIP on Target #1 because they exist in the same QuickLoop.

Figure 4-1 Case Study - One Fabric Zone, one Mixed Zone, and no QuickLoop Zones defined



In order to make this environment more Secure, there are 2 ways to prevent general access to Target #1 (Figure 4-2).

1) Follow the steps under Section 3 QuickLoop deployment. Create a QuickLoop Zone by creating a single QuickLoop Zone around Target #1 (Blue QuickLoop Zone) and make this a part of the existing Zoning Configuration. This will prevent access to Target #1 of any newly introduced QuickLoop device that is not explicitly in a Zone.
2) The alternative is to disable QuickLoop on both switches and qldisable the port on Target #1. Then use the **`portcfglport`** command to lock down the device as a Private Target. In this case because QuickLoop is not active there is no single PLDA address space created across the ports/switches.
   Note: Please refer to the switch vendors support information regarding whether the portcfglport command is supported for specific devices.

If Host C or Target #3 are added to the Fabric in Figure 4-2 they will be isolated until they are explicitly entered into a QuickLoop Zone of their own. In this case Host C could not see Targets #1 and #3. Also

Targets #1 and #3 would not disrupt each other because if either device LIP'd, the LIP would not go outside the QuickLoop Zone around Target #1.

Figure 4-2 Case Study - Create QuickLoop and QuickLoop Zones in Zoning Configuration.

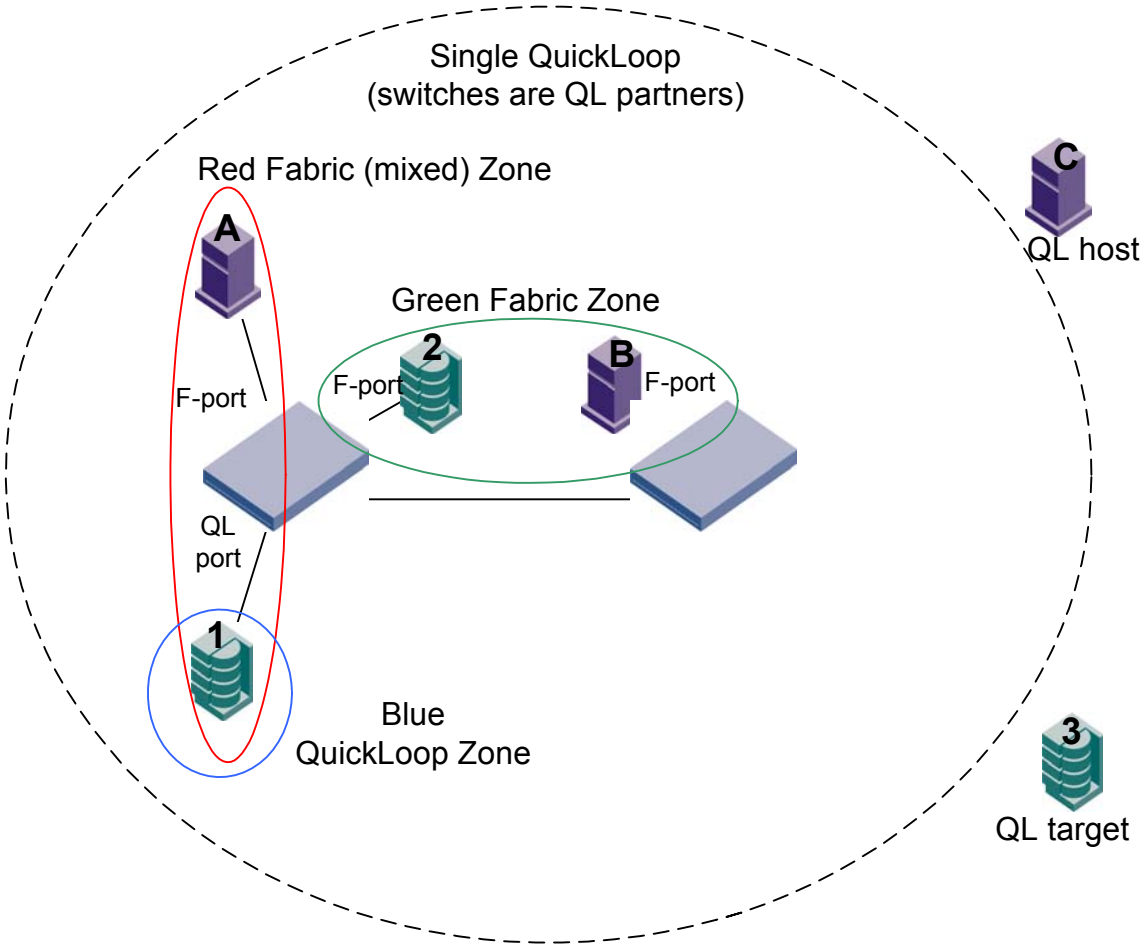
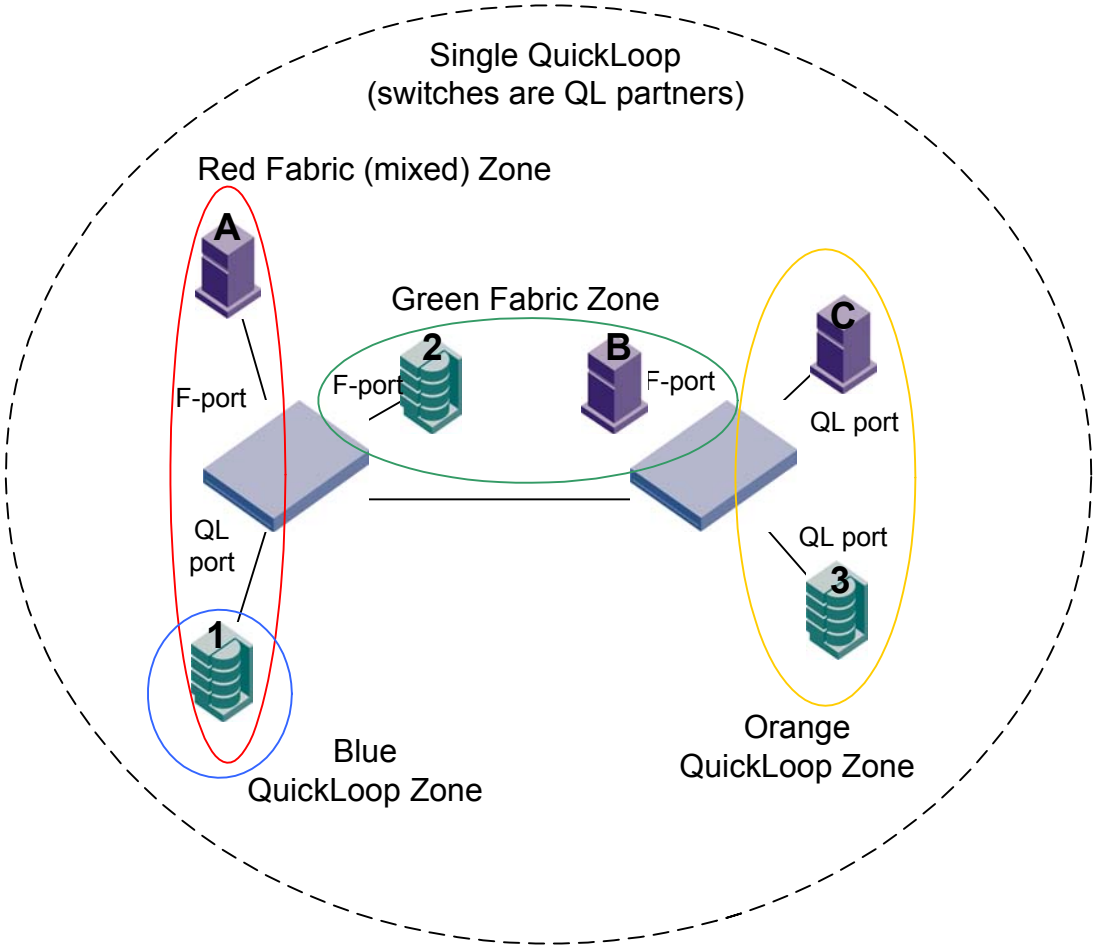


Figure 4-3 shows a final configuration in which all the devices are in a Secure QuickLoop Zoning configuration. In this Diagram there are four Zones :

1) A Red Zone consisting of one Public Host (A) and one Private Target (#1). In this case the Private Target #1 was configured as a QuickLoop Port and Host A communicates to Target #1 through Translative mode. This is a Mixed Fabric/QuickLoop Zone.
2) There is also a Blue QuickLoop Zone around Target #1. This is a pure QuickLoop Zone.
3) The Green Zone consists of one Public Host (B) and one Public Target (#2). In this case the Public Target #2 is a fabric device and Host B communicates to Target #2 through Fabric mode. This is a pure Fabric Zone.
4) The Orange QuickLoop Zone consists of one Private Host (C) and one Private Target (#3). Host C communicates to Target #3 through QuickLoop mode. This is a pure QuickLoop Zone.

Figure 4-3 Case Study – Add new devices and create additional QuickLoop Zones.


Single QuickLoop
(switches are QL partners)
Red Fabric (mixed) Zone
A
Green Fabric Zone
2
B
C
F-port
F-port
F-port
QL port
QL
port
QL port
3
1
Blue
QuickLoop Zone
Orange
QuickLoop Zone

4.2 QuickLoop Zoning Validation

Once the SAN is staged, it is highly recommended to verify its functionality and robustness before going into production. While less important for the entry-level environments, validation becomes critical for SANs with higher port counts. If at all possible, it is a good idea to do a set of tests with generated I/O, preferably with the application up and running. Sample tests can be obtained in the document "*Brocade SilkWorm Design, Deployment, and Management Guide : SAN DDM Version 2.0" (publication number 53-0000366-01).*

A.1. Brocade Documentation

The following related publications are provided on the Brocade Documentation CD-ROM and on the Brocade web site. To access the Brocade Partner web site go to *www.brocade.com* and click on the **Partner Login** link.

- **Brocade Fabric OS optional features documentation**
  - *Brocade QuickLoop User's Guide Version 3.1.0 (publication number 53-0000513-02)*
  - *Brocade Zoning User's Guide Version 3.1.0/4.1.0 (publication number 53-0000523-02)*
  - *Brocade Secure Fabric OS User's Guide Version 3.1.0 / 4.1.0 (publication number 53-0000526-02)*

A.2. Additional Resource Information

The following related publications are provided on the Brocade Partner web site and are an excellent resource for additional information.

- *Brocade SilkWorm Design, Deployment, and Management Guide : SAN DDM Version 2.0 (publication number 53-0000366-01)*
- *SAN Security: A Best Practices Guide Revision 2 (publication number GA-RG-250-00)*
- *Zoning Implementation Strategies for Brocade SAN Fabrics (White Paper Available on the Brocade Website)*