

# I/O StreamGuard

## Implementation and Uses

## Table of Contents

I.	Overview.....	3
II.	What's the problem? .....	3
III.	Feature Description .....	4
IV.	Is there another way?.....	6
V.	Simplifying Zoning in the Small SAN with I/O StreamGuard.....	7
VI.	Conclusion .....	9

## I. Overview

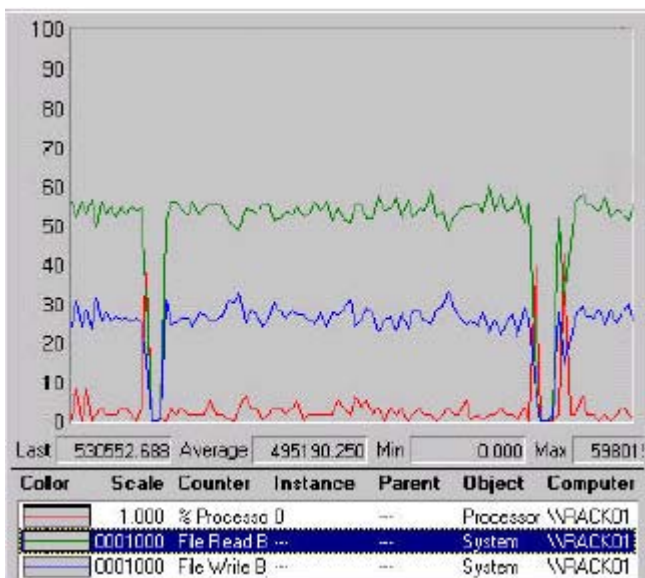
I/O StreamGuard is a QLogic specific feature that addresses the problem of guaranteeing un-interrupted data flow, specifically in Sequential Data applications. The two most predominant sequential data uses in Storage Area Networks are backup of centralized storage and streaming media applications such as video or audio. I/O StreamGuard is implemented on QLogic SANbox and SANbox2 Switches as a standard feature. I/O StreamGuard is used to manage Registered State Change Notification, RSCNs.

RSCNs are a vital part of a Fibre Channel SAN fabric. They are part of the Fibre Channel Specification and all Fibre Channel devices are required to accept and handle them in a fabric implementation. When a SAN fabric changes, and these changes could include a server coming on-line, a change in zoning, addition of storage ports, or an addition of another switch to the fabric, the fabric has changed and all of the devices on the fabric normally need to be aware of the change. The RSCN will notify the devices and the fabric will be updated to account for these changes.

## II. What's the problem?

In normal random data storage operations, small transactions are the norm. Some of the applications that people will recognize as random are Database oriented, such as on-line transaction processing of airline reservations, stock transactions, banking, insurance, and accounting. These random access storage applications are typically 8K or 16K in size and consist of approximately 80% reads and 20% writes. Approximately 65% of computer storage is in a random environment. In these types of environments, an RSCN and the resultant minor interruption to the fabric is largely inconsequential, as the commands are re-tried and upon completion, are no longer a problem. However, this data is vital to the company or concern and is relied on for day to day operations. As such, it needs to be backed up, normally to tape.

Tape back up is a sequential operation, meaning that the data is streamed in a linear fashion from the storage to the tape backup. Similarly, recovery from tape is also a linear or sequential operation. In a sequential data operation, it is vital that the data flow be un-interrupted, as an interruption will result in a failed backup.



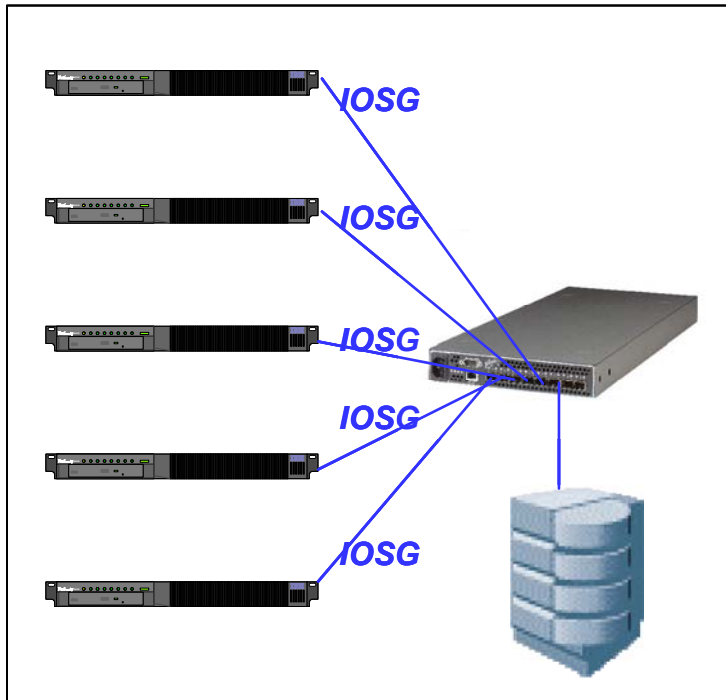
RSCNs will cause an interruption in sequential data flow if the change comes from a device other than a storage target. The most likely cause of an RSCN is the insertion or removal of a device from the fabric, such as a reboot, startup or crash of a server. The diagram at left shows the result of a reboot of a server. The green line is sequential reads, the blue line is sequential writes, and the red line is processor activity. This setup has two servers, attached via Fibre Channel HBAs (Host Bus Adapters) and a Fibre Channel Switch to a common storage target. Note that there are two events happening here as there are two RSCNs. One happens when the server goes off-line at the reboot and the second happens

when the server comes on line and the driver puts the HBA on to the fabric. In each of these instances, the “state” of the fabric has changed. When the server goes off-line during the reboot, the fabric goes from 3 entries( 2 Servers + 1 Storage device) to 2 entries (1 Server + 1 Storage device). Therefore, the fabric has changed, and hence, an RSCN is generated and the new state of the fabric is realized. Similarly, when the server comes back online, the state changes as the fabric goes from 2 entries to 3 entries. Once again, an RSCN is generated. In both instances, as can be seen from the graph, there is an interruption in data flow. In the event that a tape back up is happening at this time, the backup has a high potential for failure.

The real problem is that backup windows are well defined and the time for them to happen is finite. Backup is described as a “race to daylight” as most backups occur during off-production hours. Unfortunately, this window is also shared by IT maintenance for server and software upgrades. Most of us have gotten Emails from our IT department that certain servers or services will be down for routine maintenance and software upgrades at certain times. These times are typically in the evening or night-time hours. In the case that an upgrade or system maintenance is done on a server that resides on a SAN, there exists a high probability that the storage attached to that SAN will be backed up at the same time as the upgrade; off-production times. Most times when this type of maintenance is done, it requires a reboot of the server, the previously illustrated scenario will occur, and the tape backup fails.

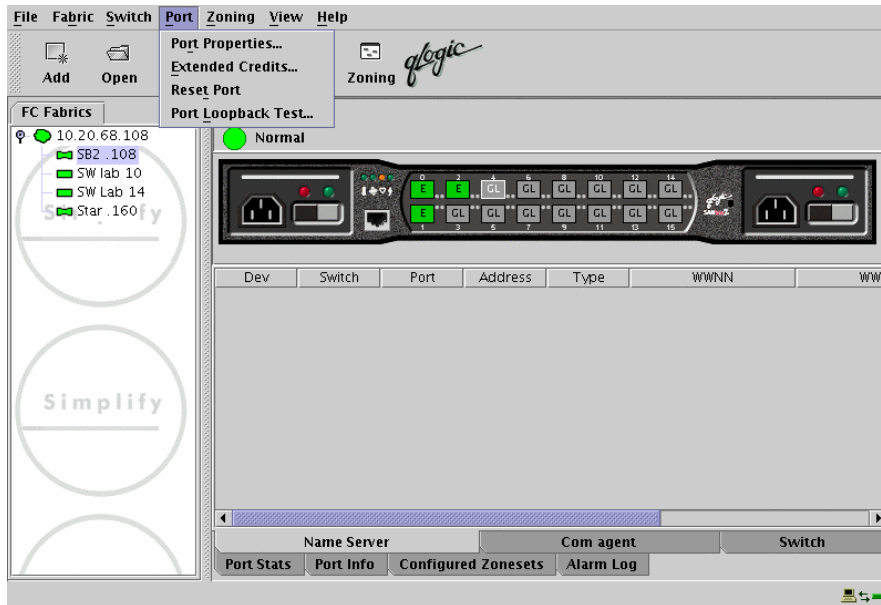
If we ask an IT professional when their backups fail, their usual answer is that the failure occurred the day before a restore from tape is necessary and that extraordinary effort is required to restore the data, hence the need for the feature I/O StreamGuard.

### III. Feature Description

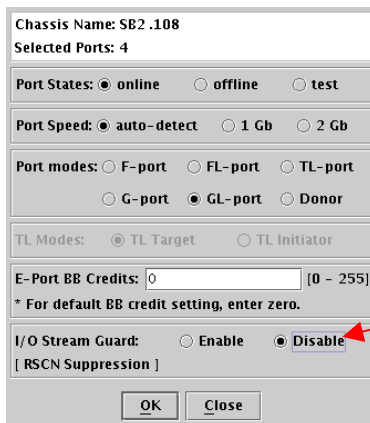


I/O StreamGuard intercepts RSCNs and handles them in an intelligent fashion. There are certain conditions where RSCNs can be intercepted and managed to keep interruptions from happening. I/O StreamGuard works by intercepting RSCNs generated by initiators on I/O StreamGuard enabled ports and stopping them from being transmitted to other I/O StreamGuard enabled ports. As shown in the diagram at left, All of the ports that are attached to the SANbox2 switch from the servers have the I/O StreamGuard enabled.

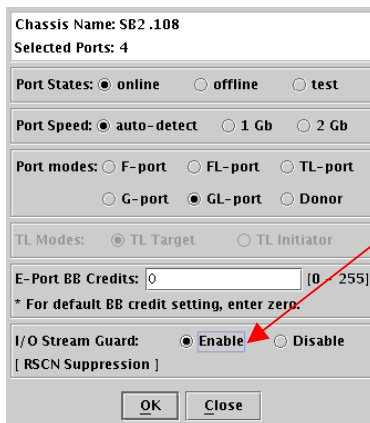
While it may seem like this is an advanced feature, the implementation is rather simple.



To enable I/O StreamGuard, simply open the SANbox Manager application to the faceplate view of the switch that you want to apply I/O StreamGuard. Choose the port that you want to configure. Then under the Port menu heading choose port properties as shown at left.



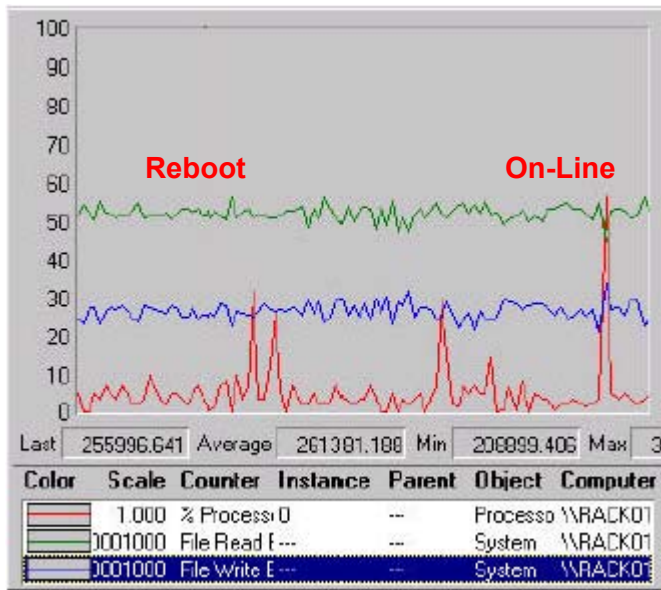
The screen shown at left will be the default view that is shown. Note that the I/O StreamGuard option is disabled by default.



Simply choose the enable option on the port, and click the OK box. I/O StreamGuard is now enabled on this port. Do this for each of the initiator ports that are in your SAN and you will have secured your SAN against backup failures.

There are instances where it will be important that RSCNs get through to a device that is on an I/O StreamGuard port. Some examples would be RSCNs that are generated when a zone would change or if a switch or new device were added to a fabric. In these cases, I/O StreamGuard allows these RSCNs through to the initiators, as the fabric has changed to a degree that the initiators on the servers would need to be aware of the change. This is what is meant by intelligent handling of RSCNs.

Now that we have enabled I/O StreamGuard on the fabric, let's look at the results:

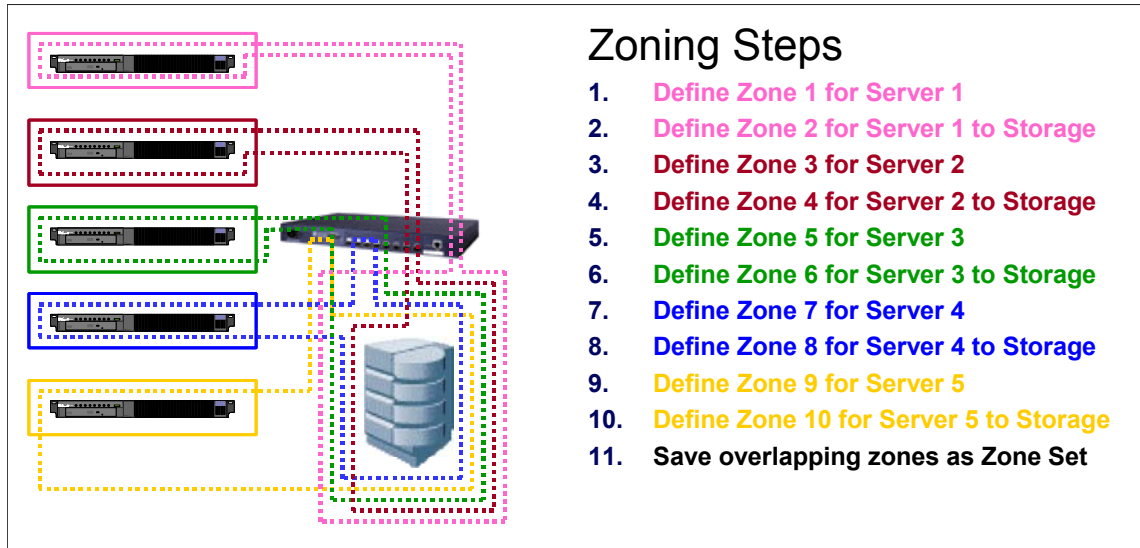


The diagram at left shows the result of a reboot of the same server as the original configuration. The green line is sequential reads, the blue line is sequential writes, and the red line is processor activity. This setup has the same two servers, attached via Fibre Channel HBAs (Host Bus Adapters) and a Fibre Channel Switch to a common storage target. We have enabled I/O StreamGuard on the two ports that are attached to the initiators in the servers. Note the spikes in the processor activity that denote the Reboot and On-Line of the Server. As you can see, the reads and writes are unaffected, and in the event that a backup was being done during this event, the sequential data would continue to flow without interruption.

#### IV. Is there another way?

Another method of handling this is to zone against RSCNs. This method can be cumbersome, as every contingency will need to be accounted for. In the event that a contingency is not accounted for, and an RSCN causes an interruption, the backup will still fail. I/O StreamGuard does not preclude zoning, but is rather a complimentary feature to zoning. In heterogeneous Server SANs, it is important that zoning be done to ensure that different Operating Systems are zoned from each other.

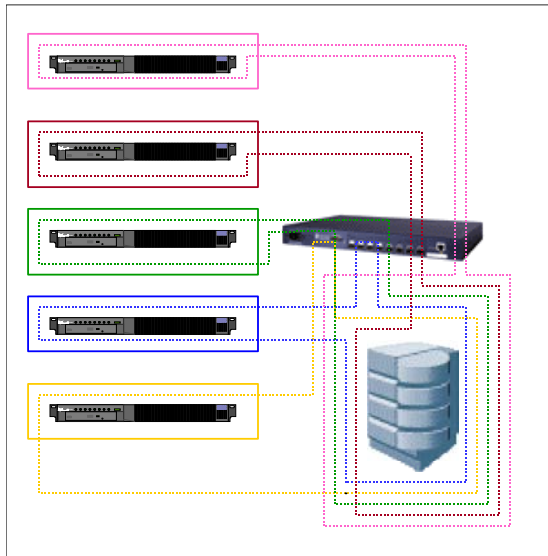
The diagram below, shows how the zones would be set up to accomplish RSCN isolation.



## V. Simplifying Zoning in the Small SAN with I/O StreamGuard

Smaller SANs, those with 3 to 6 servers are becoming more prevalent as the Storage Area Network becomes more affordable and easier to set up and use. These SANs are typically homogeneous Operating System SANs and therefore do not require as complicated a zoning scheme as in a mixed OS environment.

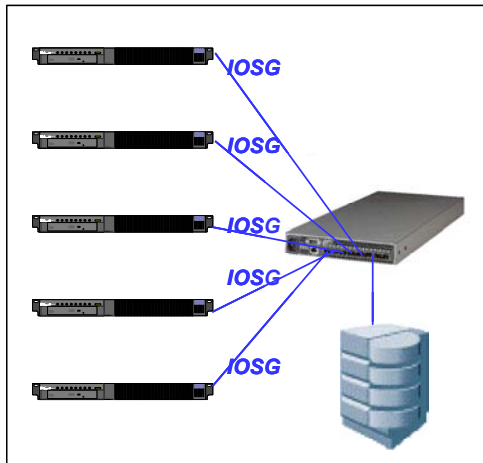
However, these SANs still need to be backed up to tape, and as such require protection from a



## The old way

1. Define Zone 1 for Server 1
2. Define Zone 2 for Server 1 to Storage
3. Define Zone 3 for Server 2
4. Define Zone 4 for Server 2 to Storage
5. Define Zone 5 for Server 3
6. Define Zone 6 for Server 3 to Storage
7. Define Zone 7 for Server 4
8. Define Zone 8 for Server 4 to Storage
9. Define Zone 9 for Server 5
10. Define Zone 10 for Server 5 to Storage
11. Save overlapping zones as Zone Set
12. Pray you didn't mess up on the zoning assignments
13. Plan other zone set to account for backup strategy
14. Set LUN assignments on storage
15. Test your new configuration

fabric event during the backup. The diagram above shows the steps necessary to set up the zoning and the assignment of the Logical Unit Numbers (LUN) on the storage that must be mapped to the individual servers. This is still a complicated set up and the potential for mis-configuration is high.



## The Simplify (QLogic) way

1. Turn on I/O Stream Guard on the Initiator ports on SANbox2
2. Set LUN assignments on storage
3. Use the configuration

I/O StreamGuard offers an innovative approach, whereby zoning is not necessary for the small SAN, thereby eliminating one of the hardest portions of SAN set up. The above diagram details the simple way to accomplish the same end result as a complex zoning scheme. Simply enable I/O StreamGuard on all of the initiator ports on the SANbox switch, assign the LUNs to the Servers, and begin using the SAN. Zoning is not necessary.

## VI. Conclusion

I/O Stream Guard offers two industry unique benefits, protection and simplicity. By enabling I/O StreamGuard in any SAN, the savvy IT administrator will have eliminated potential data loss as well as eased the administration of their SAN. I/O StreamGuard is a standard feature on all QLogic SANbox switches and has been developed in cooperation with our OEM and end user customers. While I/O StreamGuard is a QLogic unique feature, it interoperates with other vendor's switches that are FC-SW-2 and SANmark compliant, as well as all Host Bus Adapters.

© 2002 QLogic Corporation. All rights reserved. The QLogic logo is a trademark of QLogic Corporation, which may be registered in some jurisdictions. All other brands and product names are trademarks or registered trademarks of their respective holders. Information supplied by QLogic Corporation is believed to be accurate and reliable. QLogic Corporation assumes no responsibility for any errors that appear in this brochure. QLogic Corporation reserves the right, without notice, to make changes in product design or specifications. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify products or services of their respective owners.