



Best Practices for Configuring an FCoE Infrastructure with Dell Compellent and Cisco Nexus

Dell Storage Engineering
June 2014

Revisions

Date	Description
June 2014	Initial release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2013 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT:

<http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. QLogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

Revisions.....	2
Acknowledgements.....	5
Feedback	5
Executive summary	5
1 Introduction.....	6
1.1 Audience.....	6
1.2 Terminology.....	6
2 Technical overview.....	8
2.1 FCoE	8
2.2 DCB overview	8
2.3 Compellent storage.....	9
2.4 Cisco Nexus switches.....	9
3 Test configurations and methodology	10
3.1 Compellent storage.....	10
3.2 PowerEdge servers	11
3.3 Cisco Nexus switches.....	11
3.4 SAN topology.....	12
3.5 Block I/O simulation.....	13
3.6 Network I/O simulation	13
4 Results and analysis.....	14
4.1 Block SAN I/O	14
4.2 TCP network I/O	15
4.3 Converged workloads.....	15
5 Bandwidth oversubscription and Cisco FEX	18
6 Best practice recommendations.....	19
7 Conclusion.....	21
A Test configuration details.....	22
B Detailed switch configuration	23
B.1.1 Cisco Nexus 5548UP-1.....	23
B.1.2 Cisco Nexus 5548UP-2.....	27
C Detailed CNA configuration.....	31



C.1	QLogic QLE8262.....	32
C.1.1	Microsoft Windows configuration	33
C.1.2	VMWare ESXi 5.5 configuration	34
C.2	Broadcom 57800 series.....	35
C.2.1	Microsoft Windows configuration	35
C.2.2	VMware ESXi 5.x configuration.....	36
C.3	Intel X520.....	37
C.3.1	Microsoft Windows configuration	37
C.3.2	VMware ESXi 5.x configuration.....	38
D	Additional resources.....	40



Acknowledgements

This best practice white paper was produced by the following members of the Dell Storage team:

Engineering: Mike Kosacek

Editing: Camille Daily

Additional contributors: Rad Zafar Balanejad, Richard Golasky, Satish Subramanian

Feedback

We encourage readers of this publication to provide feedback on the quality and usefulness of this information by sending an email to SISfeedback@Dell.com.



SISfeedback@Dell.com

Executive summary

Fibre Channel over Ethernet (FCoE) is often thought of as a bridging technology that allows traditional Fibre Channel (FC) networks to interface with and converge with Ethernet networks. With Dell Compellent storage and Cisco Nexus switches, a converged infrastructure with only FCoE devices can be configured that allows both LAN and SAN traffic to share the same fabric. This whitepaper:

- Describes use cases for implementing a point-to-point FCoE infrastructure
- Provides guidance for sizing a converged infrastructure
- Provides best practices for designing, configuring and deploying an FCoE-only infrastructure



1 Introduction

FCoE was created to allow the convergence of traditional FC storage area networks (SANs) with traditional Ethernet LANs. By reducing the need for two network fabrics, cabling to hosts can be reduced resulting in less cabling complexity as well as possible energy savings due to a reduced number of host bus adapters (HBAs) and better airflow to host systems.

Many FCoE deployments simply enable the bridging of traditional FC and Ethernet technologies together. For enterprises that are familiar with FC concepts but are moving toward convergence on 10Gb or higher Ethernet fabrics, Compellent storage can also support a full end-to-end SAN consisting of both FCoE hosts and FCoE targets.

This white paper provides detailed guidance as well as Dell recommended best practices for designing and deploying a SAN with FCoE connected hosts and FCoE connected Compellent storage systems.

1.1 Audience

This technical white paper is intended for storage administrators, network administrators, SAN system designers, storage consultants, or anyone configuring a SAN infrastructure with Compellent storage. It is assumed that readers have experience in designing or administering a shared storage solution. Also, there are some assumptions made in terms of familiarity with all current Ethernet standards as defined by the Institute of Electrical and Electronic Engineers (IEEE) as well as TCP/IP standards as defined by the Internet Engineering Task Force (IETF) and FC standards as defined by the T11 committee and the International Committee for Information Technology Standards (INCITS).

1.2 Terminology

The following terms will be used throughout this document.

DCB: Data Center Bridging is a set of enhancements made to the IEEE 802.1 bridge specifications for supporting multiple protocols and applications in the same data center switching fabric. It is made up of several IEEE standards including Enhanced Transmission Selection (ETS), Priority-based Flow Control (PFC), Data Center Bridging Exchange (DCBX), and application Type-Length-Value (TLV). For more information, see <http://en.community.dell.com/techcenter/storage/w/wiki/4396.data-center-bridging-standards-behavioral-requirements-and-configuration-guidelines-by-sis.aspx>

FIP: FCoE Initialization Protocol (FIP) allows an FCoE node to discover devices and VLANs and login to another FCoE or FC device through a virtual FC link.

LAN: A Local Area Network is one that carries traditional IP-based client communications.

MPIO: Multi-Path I/O typically refers to a host-based software layer that manages multiple paths for load-balancing and redundancy in a storage environment.

N_Port: An end node port on a Fibre Channel fabric. Usually an HBA, CNA, or target port on a storage device.



NPIV: N_Port ID virtualization allows multiple Fibre Channel N_Port IDs to share a single physical N_Port.

SAN: A Storage area network is one that carries host to storage or storage inter-process communications and data traffic.

VFC: A Virtual Fibre Channel interface that is bound to a physical Ethernet port on a Cisco Nexus switch, enabled for FCoE, and allows the administrator to apply FC configuration commands.

vPC: The Cisco Virtual PortChannel feature allows links that are connected to two different physical Nexus switches to appear as a single portchannel to a third switch or device.



2 Technical overview

The following sections provide an overview of the SAN infrastructure components and technologies used in developing this white paper.

2.1 FCoE

FCoE is a storage protocol that enables Fibre Channel devices to communicate over high-speed (10 Gb and higher) Ethernet fabrics by encapsulating FC frames within Ethernet packets. FCoE was originally intended to allow hosts with Ethernet connectivity to access native FC storage, however, with a storage system such as Compellent, it is also possible to design SANs with end-to-end FCoE connectivity.

DCB support is a requirement of FCoE to enable lossless transmission of storage traffic. Therefore any switch, CNA, or storage device that claims support for FCoE must also support DCB. As a result, the first DCB-capable switches supported convergence of FCoE SAN and Ethernet LAN traffic.

FCoE was originally introduced around the time when FC speeds were at 4 Gb and Ethernet supported 10 Gb speeds. With the bandwidth capability differences, it is easy to see how FC and Ethernet traffic could share the same fabric and maybe even still have room to grow. Today, native FC systems can communicate at 16 Gbps. While 40 Gb Ethernet could easily accommodate this, most 40GbE ports are currently implemented between switching devices and are not yet widespread for host connectivity. With 10 Gb Ethernet to hosts and storage systems, there is now a potential trade-off when trying to converge two high-speed protocols onto a single fabric.

Before combining fabrics, current and future bandwidth requirements of both LAN and SAN should be carefully monitored and considered in the design of the converged fabric.

2.2 DCB overview

DCB is a set of enhancements made to the IEEE 802.1 bridge specifications for supporting multiple protocols and applications in the same data center switching fabric. It is made up of several IEEE standards including Enhanced Transmission Selection (ETS or 802.1Qaz), Priority-based Flow Control (PFC or 802.1Qbb), Data Center Bridging Exchange (DCBX, also part of 802.1Qaz), and application Type-Length-Value (TLV).

DCB allows a physical link to be shared by multiple traffic types, such as LAN and SAN. Traffic is classified and given priority based on Ethertype (for FCoE) or application TLVs (for iSCSI). ETS provides a guaranteed minimum bandwidth to a priority class such as FCoE. PFC ensures that during periods of congestion, the priority class is paused to avoid dropping any packets, while other traffic classes may potentially be dropped. LAN traffic can typically recover from drops without noticeable degradation. SAN traffic requires a lossless transmission and is therefore placed in the priority class since it is sensitive to drops, which can cause higher latency and even dropped connections.

DCBX, while technically not required, provides for the automatic configuration of end-devices by propagating the configuration parameters from the switch. The use of DCBX saves administrative time and



can also eliminate potential configuration mistakes due to user configuration error. Most host CNA and storage devices default to willing mode, which means they will use DCBX to negotiate and accept the configuration parameters provided by the switch. This is true for all CNAs and storage controllers used for this white paper.

Note: DCBX requires the LLDP protocol to be enabled.

DCB is enabled by default on Cisco Nexus switches. DCB is also enabled on the QLogic QLE8262 CNAs when the FCoE protocol is enabled.

2.3 Compellent storage

Compellent Storage Center is a Dell enterprise storage solution featuring multi-protocol support and self-optimizing, tiering capabilities. The SC8000 controller can be configured with any combination of FC, iSCSI, and FCoE front-end connectivity. With the addition of the FS8600 NAS appliance, Compellent Storage Center can also support NFS and SMB clients.

Storage Center can be configured with all flash, as a hybrid system, or with only traditional spinning disks and features automatic migration of data to the most cost-effective storage tier. Efficient thin provisioning and virtualization of the storage uses disk capacity only when data is actually written, therefore enabling a pay-as-you-grow architecture. This self-optimizing system can reduce overhead cost and provide the administrator with more time for other important tasks.

For FCoE connectivity, the SC8000 uses one or more QLogic QLE8152 CNAs configured for storage target support. These adapters fully support DCB for FCoE.

2.4 Cisco Nexus switches

The Cisco Nexus 5000 series are high-density, low-latency top of rack (ToR) switches suitable for datacenters where LAN and FC SAN fabrics will be converged. The Nexus 5000 series supports connectivity for 10 Gb Ethernet, FCoE and native FC storage devices. DCB support allows classification of multiple traffic types and the ability to create a lossless (no-drop) queue for SAN storage traffic.

The Cisco Nexus 5548UP allows either 10 GbE or native 8 Gb FC connectivity on each port simply by changing the SFP+ optics (for Ethernet or FC types). For the topology used in this white paper, only Ethernet ports are configured.

Nexus 5548UP switches also provide support for Fabric Services including FIP (FCoE Initialization Protocol) which allows an FCoE device (CNA) to discover other devices and VLANs on the fabric, and to login and logout from the FC fabric. The Nexus 5548UP also fully supports NPIV.



3 Test configurations and methodology

An I/O workload test utility was run to demonstrate how network bandwidth is shared with DCB when multiple traffic classes are in a converged fabric.

The following section discusses the topologies and the methodology used for testing conducted in Dell labs. This section also discusses the configuration of the host servers, network, and storage used for these tests.

3.1 Compellent storage

Two SC8000 controllers were configured with a dual-port FCoE interface in each controller for front-end connectivity. The 6 Gb SAS backend consisted of two SC220 enclosures each with twenty-four 146GB 15K disks (tier 1) and one SC220 with twenty-four 2TB 7.2K NL-SATA disks (tier 3). The FCoE connections were configured for **Virtual Port Mode** and two fault domains were created. To enable virtual port mode, NPIV must be enabled on the switch fabric.

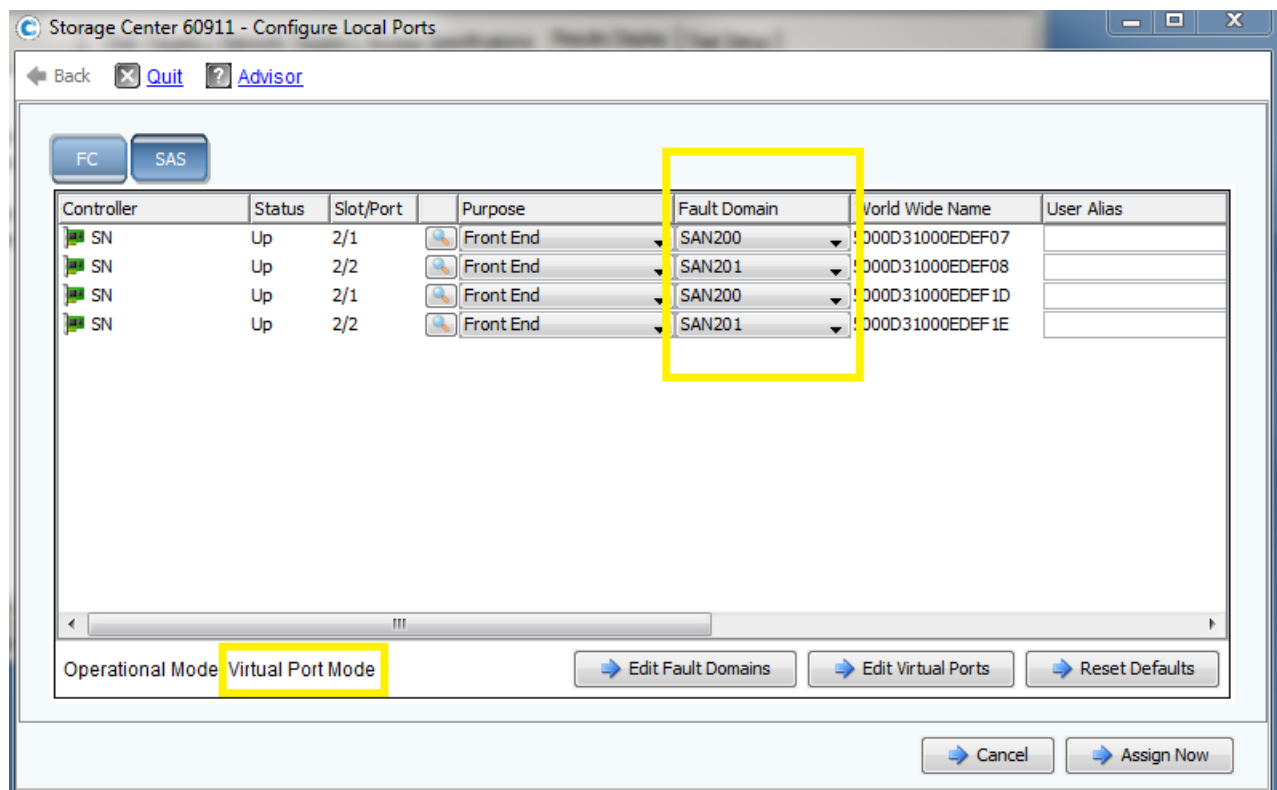


Figure 1 Front-end port configuration for Compellent Storage Center

For detailed information, see Appendix A.



3.2 PowerEdge servers

Two Dell PowerEdge R720 servers were configured with Windows 2012 R2 and QLogic QLE8262 converged network adapters (CNAs) and connected to the 10 Gb Ethernet switch fabric. DCB was configured on the Cisco Nexus switch fabric and the QLE8262 CNAs were in the default willing mode to accept the DCBX configuration parameters from the switch. Each Windows system was configured with two 10GB volumes on the SAN.

On the Windows servers, the QLogic QConverge graphical interface was installed and used to configure the Ethernet function of each CNA for VLAN 100. The Windows 2012 R2 NIC teaming feature (also known as Windows Load Balancing and Failover or LBFO) was used to create a team with the two QLogic Ethernet (NDIS) adapters to carry LAN traffic on the converged network. Because the VLAN tagging was already handled at the physical adapter level, LBFO was configured using the default VLAN.

The QLogic QLE8262 adapters default to a Max Frame Size (or MTU size) of 2500, which is also known as Baby Jumbo frame size. This is the only setting for FCoE and cannot be changed on the CNA. For the Ethernet function, the standard MTU of 1500 was used.

For detailed information, see Appendices A and C.

3.3 Cisco Nexus switches

A pair of Cisco Nexus 5548UP switches were configured with a vPC interconnect. In addition, the LACP, LLDP, FCOE, and NPIV features were enabled. The appropriate VLAN, VSAN, and VFC mappings were created to enable communication between the FCoE hosts and storage. Additionally, a second VLAN was enabled to carry LAN traffic.

The default policy-map for Nexus NX-OS 7.0 creates a no-drop queue for FCoE traffic and assigns the MTU size of 2158 bytes. This is standard for FCoE Baby Jumbo Frames that are sized to encapsulate the FC frame size of 2148 bytes (and the standard FC payload data size of 2112 bytes). The default policy map also specifies that all non-FCoE traffic belongs to the default class and uses the standard MTU size of 1500 bytes. The policy map specifies that queuing values (which translate to DCB ETS settings) for the class-fcoe and class-default are each set to a default bandwidth percentage of 50.

The bandwidth assigned to each traffic type ensures a minimum available for each type, however either traffic class is allowed to utilize more bandwidth than allocated, if there is no congestion or contention between the two types. For example, if the LAN is consuming only 10% of the available bandwidth, the SAN could utilize more than 50% (theoretically up to 90%).

Additional policies can be created on the Cisco Nexus to allow for customization of the parameters such as MTU size or ETS bandwidth allocation (queuing values).

For additional information, see Appendix B.



3.4 SAN topology

As shown in Figure 2, the tested SAN topology consisted of a dual-fabric design. Although the Cisco 5548UP switches were also configured as a vPC to allow host LAN traffic to flow between both switches, the SAN traffic was isolated through VLANs to appear to end-devices as two separate physical fabrics.

Two fault domains were configured on the Storage Center (shown as SAN A and SAN B) and two separate VLANs/VSANs (200/201) were configured, one on each switch. FC zones were created on each switch. A separate zone was created for all physical controller port worldwide names (pwwn) on the Compellent SC8000 controllers, and another for all virtual controller pwwns. Additional zones were created for each host containing one host initiator pwwn and two virtual controller pwwn.

For host LAN connectivity, a single VLAN (100) was configured across both switches (including the vPC link). This allowed the host to be configured with dual-redundant connections to the converged switch fabric (with the use of a host-based teaming driver).

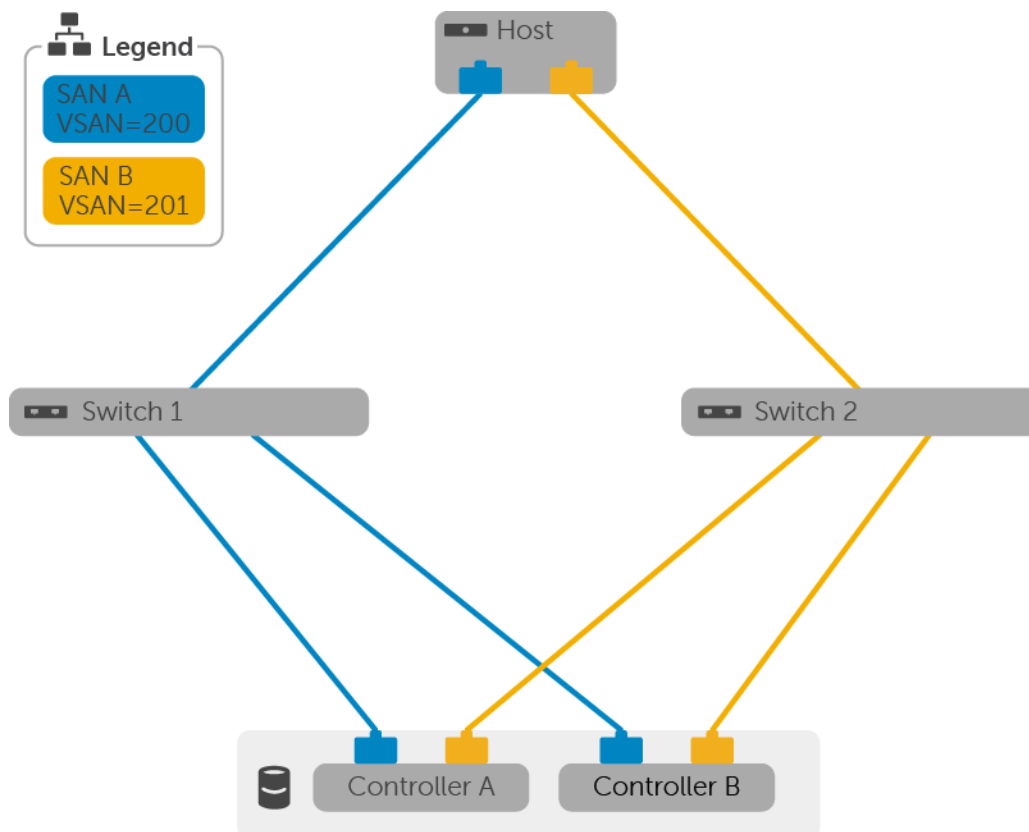


Figure 2 SAN topology

3.5 Block I/O simulation

To simulate block I/O from host servers, the open source tool Iometer was installed on the Windows host servers. Test parameters were configured to enable 100% sequential read access with a 256 KB request size. Two SAN volumes were assigned to each host. The volumes were configured as raw physical disks, with no file system. An Iometer worker was assigned to each physical disk with 64 outstanding I/Os per target. A large block request size was chosen to simulate an application using high storage network bandwidth.

The Iometer graphical interface (**iometer.exe**) was installed on a separate system to manage the workloads running on the systems under test. The systems running the workload, executed a script file to launch **dynamo.exe** and connect to the Iometer management system.

3.6 Network I/O simulation

Another open source simulation tool, **iperf.exe**, was used to generate large amounts of TCP LAN traffic between clients and servers. One system was configured as a server, and the other ran in client mode. Ten parallel threads were used. The maximum TCP window size was set to 64K and the maximum segment size (MSS) was set to 1460.



4 Results and analysis

The following sections discuss the results of tests conducted for the purpose of this white paper.

Note: The performance data in this paper is not intended to express maximum performance or benchmark results. Actual workload, host to array port ratios, and other factors may also affect performance.

4.1 Block SAN I/O

When Iometer was run and there was no additional LAN traffic on the converged network, an average throughput of nearly 3400MB/s was observed using the defined workload. This was roughly 68% of the total theoretical bandwidth available from the four 10 GbE ports that were in use on both the host servers (two 10GbE ports per host) and the storage (two 10GbE FCoE ports per SC8000 controller).

Note: Throughput calculation based on each 10 GbE/FCoE port with theoretical 1250 MB/s. With four front-end FCoE ports, the theoretical storage system maximum is 5000 MB/s. $3390/5000 = 67.8\%$

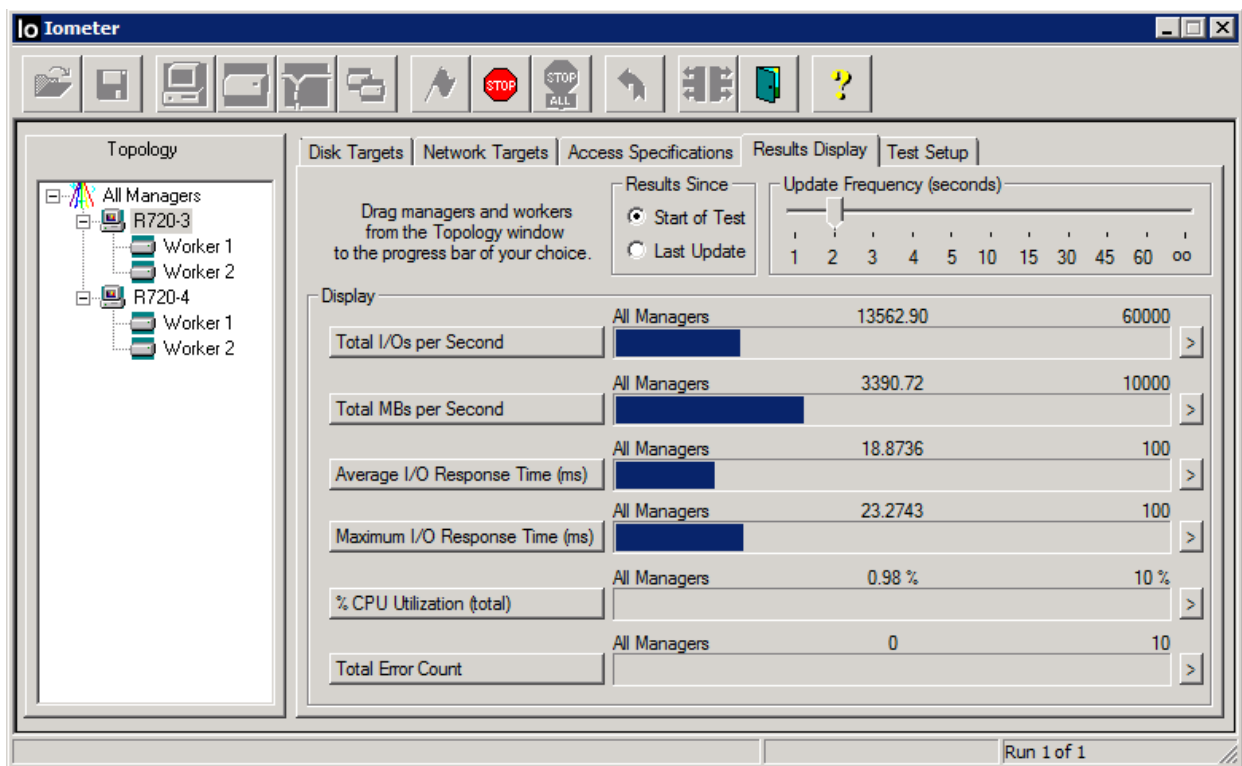


Figure 3 Iometer throughput for SAN traffic only

Because there was only FCoE SAN traffic on the network during this part of the test, the SAN was allowed to utilize greater than the 50% bandwidth allocated by the default Nexus policy map.

4.2 TCP network I/O

When only iperf.exe was run between two servers, the Windows 2012 Task Manager showed nearly 10 Gbps throughput across the team of QLogic Ethernet adapters (the Ethernet function of the CNA). This means that the workload was achieving roughly 50% of the theoretical bandwidth since the team consisted of two 10 GbE ports.

Higher network bandwidth utilization may be possible by configuring jumbo frames for the LAN traffic, however only standard MTU was used for the tests performed for this paper. The standard MTU of 1500 bytes is typical for most LAN configurations.

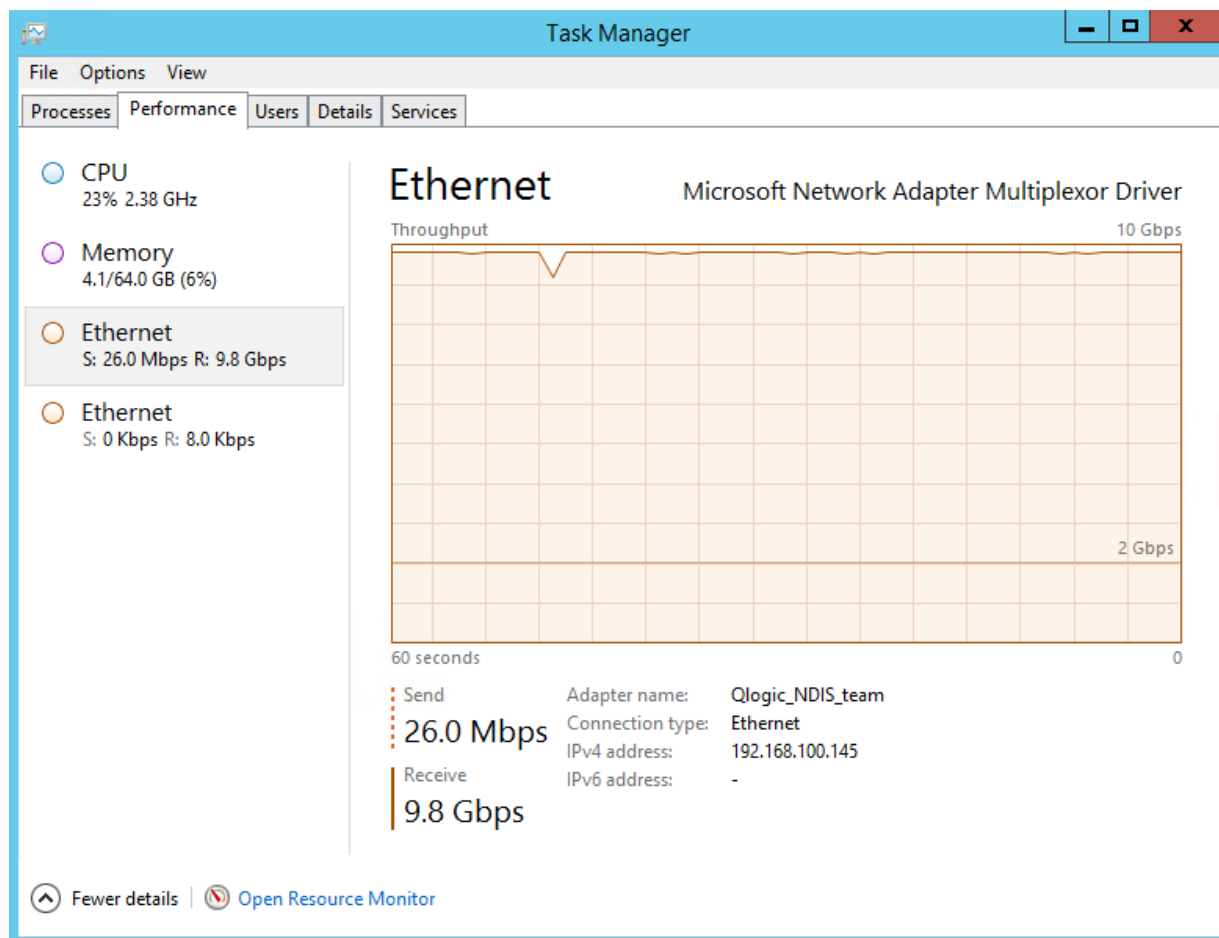


Figure 4 Task Manager showing throughput for iperf.exe LAN traffic only

4.3 Converged workloads

When both SAN and LAN workloads were run simultaneously, it was clear that there was an effect on the performance of both. The SAN throughput was reduced to below 2400 MB/s. Considering that the ETS bandwidth settings allowed for a minimum of 50%, this was in line with expectations since ETS allows for a +/- 10% difference of the administered setting.

The average response time of the storage I/O increased from 18.9ms to 27.8ms indicating that storage traffic was also being affected by network congestion and PFC.

Note: Throughput calculation based on each 10GbE/FCoE port with theoretical 1250 MB/s. With four front-end FCoE ports, the theoretical storage system maximum is 5000 MB/s. $2385/5000 = 47.7\%$

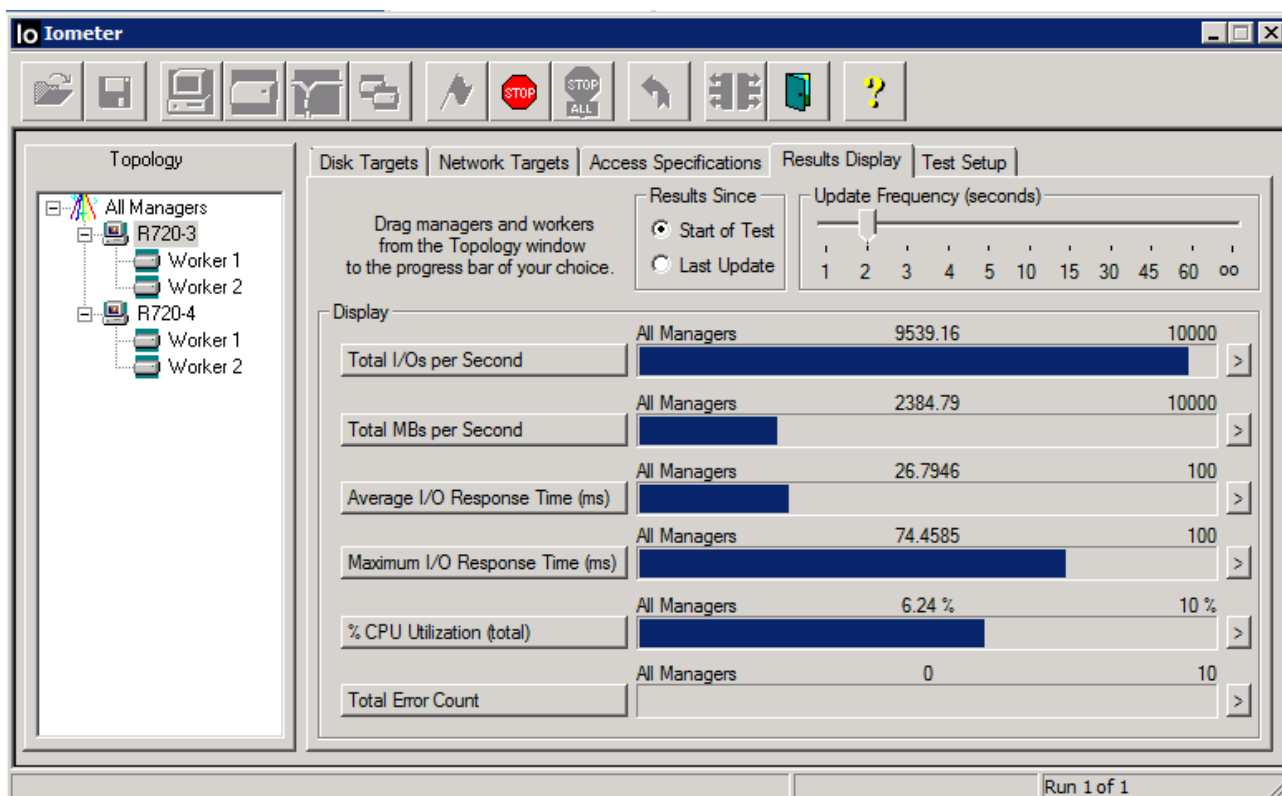


Figure 5 Iometer throughput showing effect of SAN and LAN workloads together

The LAN traffic was also greatly reduced as shown in Figure 6. When both workloads were run simultaneously, the throughput on the LAN dropped to around 4 Gbps total, again indicating network congestion.

Recall that each workload was capable of utilizing 50% or more. Adding the two workloads together resulted in greater than 100%, and therefore the throughput of each workload was reduced to conform to the ETS settings configured by the default Nexus policy map for FCoE. Furthermore, even with the high bandwidth utilization, there were no errors or disconnects encountered for the SAN workload, indicating that the lossless queue for FCoE traffic was in operation.

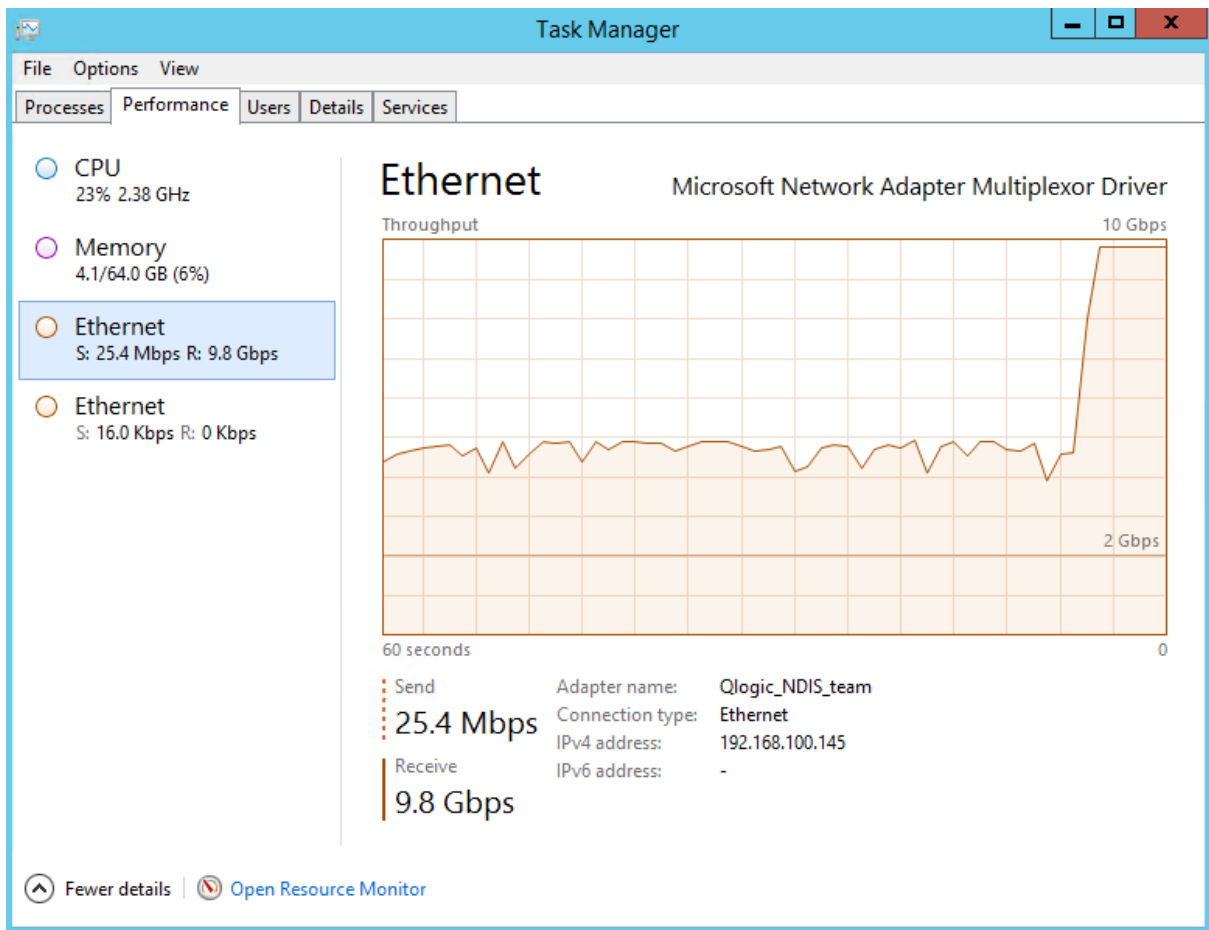


Figure 6 Task Manager showing the effect of LAN and SAN workloads together

As shown in Figure 7, with LAN and SAN workloads running simultaneously, the Nexus switch sends priority flow control as necessary to ensure that FCoE packets arrive reliably without loss.

```
Nexus5Ktop# sh int priority-flow-control
```

Port	Mode	Oper (VL bmap)	RxPPP	TxPPP
Ethernet1/1	Auto	On (8)	0	0
Ethernet1/2	Auto	On (8)	0	0
Ethernet1/3	Auto	On (8)	94867	0
Ethernet1/4	Auto	On (8)	146472	0
Ethernet1/31	Auto	On (8)	0	19838
Ethernet1/32	Auto	On (8)	0	19523

Figure 7 Output of **show interface priority-flow-control** command

5 Bandwidth oversubscription and Cisco FEX

The Cisco Fabric Extender (FEX) technology allows for expansion of the number of physical ports available on a Nexus switch. The FEX device itself has limited capabilities and packets must go up to the parent Nexus switch for all processing. This adds latency or propagation delay for each packet. However, it is typically sub-millisecond and therefore negligible in most cases when compared to hosts connected directly to the Nexus (parent) switch.

Most FEX allow for a limited number of uplinks (usually four to eight depending on the model) so bandwidth oversubscription is also inherent to the design. For example, a FEX device such as the Cisco 2232 has 32 ports available for host connectivity. If eight uplinks are made to the parent switch this still creates a possible oversubscription scenario of 4:1 when all 32 FEX ports are utilized.

Workloads that use medium to large I/O request sizes will consume more fabric bandwidth. Backup and restore, replication, or streaming workloads typically use large I/O request sizes (256KB or larger) and may not be the best candidates for connecting to a FEX. Virtualized host servers may also coalesce small application I/O (8KB or less) requests into medium sized requests (32-128KB size) before writing to SAN storage.

A converged fabric running DCB may reduce the available bandwidth even further if non-storage traffic flows are requesting high bandwidth or if the ETS setting for the FCoE (storage) priority group is too low. Therefore, a converged fabric design must also take into account the LAN activity on the shared CNA ports, and there should be a good understanding of both the SAN and LAN workloads and traffic patterns before attaching a host to a FEX.

While FEX may be appropriate for some host connectivity, Dell does not recommend using FEX devices for connectivity to the storage systems because of the potential bandwidth limitations. Host connectivity to a FEX should only be used after careful consideration is given to the total bandwidth requirements of each specific host.

Cisco FEX was not used with any of the tests performed for the purpose of this paper.



6 Best practice recommendations

The following Dell best practices are recommended when deploying a converged infrastructure with point-to-point FCoE SAN connectivity.

Switch Fabric

- Design and size a converged fabric appropriately with consideration of the possible bandwidth required by each type of traffic. As an example, if LAN and SAN traffic each require 6 Gb of bandwidth, which is more than the maximum of a 10GbE link, performance of one or more traffic flows will be reduced.
- Use Fabric Extenders (FEX) or line-card modules with inherent oversubscription with caution. Evaluate bandwidth needs before deploying such devices into production environments.
- FCoE requires a switch fabric that supports DCB. Furthermore, the switch fabric must provide FIP and FCF services to enable a point-to-point FCoE connection. To support virtual port mode on the SC8000, the fabric must support NPIV. The Cisco Nexus 5548UP can provide these necessary services for supporting an end-to-end FCoE deployment.
- Connecting converged fabric switches (such as the Cisco Nexus 5548UP used for the development of this white paper) together provides redundancy for Ethernet traffic (such as when a VPC link is created). For storage (FCoE) traffic, configure the fabric with two separate VLANs/VSANs so that it appears to be two separate and independent fabrics (i.e. SAN-A and SAN-B). Two separate fault domains must be configured on the storage controllers.
- Do not create Port-channels on edge ports that carry both LAN and SAN traffic (such as those connected to a CNA). The creation of a port channel (or vPC) will create a hierarchical dependency for the storage log-in process. If the port-channel is unable to form, the storage log-in process will fail and there will be no access to the storage.
- Configure ports connected to hosts and storage controllers as spanning-tree edge ports (enable portfast or type "edge" on these ports).
- FCoE cannot be configured to use a default or native VLAN. FCoE requires a tagged VLAN to carry the packet priority value so that FCoE traffic can be given priority over other types of traffic. For additional information, refer to Priority Code Point (PCP) in IEEE 802.1Q.
- Monitor and adjust ETS bandwidth percentages as necessary for each environment. The Cisco Nexus default value of 50% (the same used for this paper) is a good starting point. Monitoring of actual bandwidth utilization may dictate the need to adjust the value so that it is optimal for each unique network environment.
- On each switch, create FC zones for all physical front-end ports on the SC8000 controllers, another for all virtual front-end ports on the SC8000 controllers, and then create unique zones for each host port and its associated virtual front-end target ports (for example, one host initiator port and at least one target port per zone).



Host Connectivity

- On QLogic CNAs, set the **Link Down Timeout** to 60 seconds (the default is 30 seconds) in the *Advanced HBA Parameters*. This is necessary to ensure proper recovery or failover if a link fails or becomes unresponsive.
- Host-based teaming software can be used to provide load-balancing and redundancy for Ethernet LAN functions over a CNA port. To support this configuration, create a vPC or LACP LAG between switches and extend a VLAN across the switches to allow LAN traffic to continue if one of the redundant connections fails.

Storage

- Use MPIO to provide multi-path load-balancing and failover redundancy for storage (FCoE) connectivity between a CNA and storage controller port. MPIO software must be configured on the host.
- Create two fault domains. One for each physical fabric (if split) or logical fabric if two separate VLANs are used on a vPC joined fabric.
- For maximum redundancy, connect at least one port from each storage controller to each fabric (for example, one port from each controller connects to switch A, and one port from each controller connects to switch B).



Conclusion

With a properly designed and configured deployment, Cisco Nexus 5548UP switches and Dell Compellent Storage Center can be used together to enable the convergence of LAN and SAN onto a single fabric with point-to-point FCoE storage connectivity. Data Center Bridging simplifies the configuration of the converged fabric by automatically propagating the configuration to the storage and host devices.

Deployments implementing a converged LAN and SAN fabric may also realize the following benefits.

- Less complexity by reducing the number of cables, interfaces, and configuration steps
- Less power used through the reduction of physical NIC and HBA adapters and switches required
- Greater energy efficiency due to the improvement of air flow and more efficient cooling of systems through the reduction of the number of cables required
- Reduction in cost through the use of fewer host adapters, switches, and cables



A Test configuration details

Table 1 Tested Components

Component	Sub-component	Description/Version
Dell PowerEdge R720	BIOS	2.2.2
	Windows Server	2012 R2*
	vSphere ESXi	5.5 U1**
Dell PowerEdge R815	BIOS	3.2.1
	Windows Server	2012 R2*
	vSphere ESXi	5.5 U1**
Dell Compellent SC8000	Storage Center	6.0.4.01.075.01
Cisco Nexus 5548UP	NX-OS	7.0(0)N1(1)
QLE8262	Driver package	5.00.0019
	Firmware package	4.16.17
	QConverge Console	5.1.0.167
Intel X520-DA2	Family driver package	15.0.0
	Firmware	15.0.28
Broadcom 57810	Family driver package	18.2.2
	Firmware	7.8.16
Test Software	IOmeter.exe	2006.07.27
	iperf.exe	1.7.0

* Recommended Windows Updates applied as available at the time

**Recommended vSphere patches and updates applied as available at the time



B Detailed switch configuration

The following sections show portions of the **show running-config** from the tested switches. Some non-essential information that is not necessary to demonstrate the configuration was removed to make it easier to read.

B.1.1 Cisco Nexus 5548UP-1

```
version 7.0(0)N1(1)
feature fcoe
hostname Nexus5Ktop
feature npiv
feature telnet
cfs eth distribute
feature lacp
feature vpc
feature lldp
<edit>
system qos
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type qos input fcoe-default-in-policy
  service-policy type network-qos fcoe-default-nq-policy
class-map type control-plane match-any copp-system-class-rpf-fail
<edit>
vlan 1
vlan 100
  name LAN
vlan 200
  fcoe vsan 200
  name SAN200
vlan 300
  name vpc-keepalive
vrf context management
  ip route 0.0.0.0/0 10.211.17.190
vpc domain 1
  peer-keepalive destination 10.211.17.136 source 10.211.17.135
  auto-recovery
vsan database
  vsan 200
fcdomain fcid database
  vsan 200 wwn 50:00:d3:10:00:ed:ef:33 fcid 0x00af0000 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:ef:34 fcid 0x00af0020 dynamic
  vsan 200 wwn 20:01:00:0e:1e:0d:89:a6 fcid 0x00af0040 dynamic
  vsan 200 wwn 20:01:00:0e:1e:0d:89:d6 fcid 0x00af0060 dynamic
  vsan 200 wwn 20:01:00:0e:1e:0d:89:2e fcid 0x00af0080 dynamic
  vsan 200 wwn 20:01:00:0e:1e:0d:89:76 fcid 0x00af00a0 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:ef:35 fcid 0x00af0021 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:ef:07 fcid 0x00af0001 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:f0:08 fcid 0x00af0022 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:ef:1e fcid 0x00af0023 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:ef:1d fcid 0x00af0024 dynamic
  vsan 200 wwn 50:00:d3:10:00:ed:ef:31 fcid 0x00af0002 dynamic
  vsan 200 wwn 20:01:00:10:18:dd:c8:41 fcid 0x00af00c0 dynamic
  vsan 200 wwn 20:01:00:10:18:ef:82:05 fcid 0x00af0100 dynamic
```



```

    vsan 200 wwn 20:00:00:1b:21:7e:75:7a fcid 0x00af0120 dynamic
    vsan 200 wwn 20:00:00:1b:21:7e:7a:fe fcid 0x00af0140 dynamic
interface port-channel1
    description vpc-peer
    switchport mode trunk
    switchport trunk allowed vlan 1,100,300
    spanning-tree port type network
    vpc peer-link
interface vfc101
    bind interface Ethernet1/31
    switchport trunk allowed vsan 200
    switchport description VFC to SC8000
    no shutdown
interface vfc102
    bind interface Ethernet1/32
    switchport trunk allowed vsan 200
    switchport description VFC to SC8000
    no shutdown
interface vfc200
interface vfc201
    bind interface Ethernet1/1
    switchport trunk allowed vsan 200
    switchport description vfc to R720-1
    no shutdown
interface vfc202
    bind interface Ethernet1/2
    switchport trunk allowed vsan 200
    switchport description vfc to R720-2
    no shutdown
interface vfc203
    bind interface Ethernet1/3
    switchport trunk allowed vsan 200
    switchport description vfc to R720-3
    no shutdown
interface vfc204
    bind interface Ethernet1/4
    switchport trunk allowed vsan 200
    switchport description vfc to R720-4
    no shutdown
interface vfc205
    bind interface Ethernet1/17
    switchport trunk allowed vsan 200
    switchport description vfc to R815-1_Broadcom
interface vfc206
    bind interface Ethernet1/18
    switchport trunk allowed vsan 200
    switchport description vfc to R815-2_Broadcom
interface vfc207
    bind interface Ethernet1/19
    switchport trunk allowed vsan 200
    switchport description vfc to R815-1_Intel
    no shutdown
interface vfc208
    bind interface Ethernet1/20
    switchport trunk allowed vsan 200
    switchport description vfc to R815-2_Intel
    no shutdown
vsan database
    vsan 200 interface vfc101
    vsan 200 interface vfc102

```




```

vsan 200 interface vfc201
vsan 200 interface vfc202
vsan 200 interface vfc203
vsan 200 interface vfc204
vsan 200 interface vfc205
vsan 200 interface vfc206
vsan 200 interface vfc207
vsan 200 interface vfc208
interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
interface Ethernet1/2
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
interface Ethernet1/3
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
interface Ethernet1/4
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
<edit>
interface Ethernet1/17
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
interface Ethernet1/18
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
interface Ethernet1/19
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
interface Ethernet1/20
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  spanning-tree port type edge
<edit>
interface Ethernet1/31
  switchport mode trunk
  switchport trunk allowed vlan 200
  spanning-tree port type edge
interface Ethernet1/32
  switchport mode trunk
  switchport trunk allowed vlan 200
  spanning-tree port type edge
<edit>
interface Ethernet2/15
  description VPC link
  switchport mode trunk
  switchport trunk allowed vlan 1,100,300
  channel-group 1 mode active
interface Ethernet2/16
  description VPC link
  switchport mode trunk
  switchport trunk allowed vlan 1,100,300

```



```

    channel-group 1 mode active
interface mgmt0
    vrf member management
    ip address 10.211.17.135/26
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.7.0.0.N1.1.bin
boot system bootflash:/n5000-uk9.7.0.0.N1.1.bin
zone name CML-virtual-ports vsan 200
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
zone name CML-physical-ports vsan 200
    member pwnn 50:00:d3:10:00:ed:ef:07
    member pwnn 50:00:d3:10:00:ed:ef:1d
zone name R720-1 vsan 200
    member pwnn 20:01:00:0e:1e:0d:89:d6
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
zone name R720-2 vsan 200
    member pwnn 20:01:00:0e:1e:0d:89:2e
    member pwnn 50:00:d3:10:00:ed:ef:33
    member pwnn 50:00:d3:10:00:ed:ef:31
zone name R720-3 vsan 200
    member pwnn 20:01:00:0e:1e:0d:89:a6
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
zone name R720-4 vsan 200
    member pwnn 20:01:00:0e:1e:0d:89:76
    member pwnn 50:00:d3:10:00:ed:ef:33
    member pwnn 50:00:d3:10:00:ed:ef:31
zone name R815-1 vsan 200
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
    member pwnn 20:01:00:10:18:dd:c8:41
zone name R815-2 vsan 200
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
    member pwnn 20:01:00:10:18:ef:82:05
zone name R815-2-X520 vsan 200
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
    member pwnn 20:00:00:1b:21:7e:75:7a
zone name R815-1-X520 vsan 200
    member pwnn 50:00:d3:10:00:ed:ef:31
    member pwnn 50:00:d3:10:00:ed:ef:33
    member pwnn 20:00:00:1b:21:7e:7a:fe
zoneset name fcoe200test vsan 200
    member CML-virtual-ports
    member CML-physical-ports
    member R720-1
    member R720-2
    member R720-3
    member R720-4
    member R815-1
    member R815-2
    member R815-2-X520
    member R815-1-X520
zoneset activate name fcoe200test vsan 200

```



B.1.2 Cisco Nexus 5548UP-2

```
version 7.0(0)N1(1)
feature fcoe
hostname Nexus5Kbtm
feature npiv
feature telnet
cfs eth distribute
feature lacp
feature vpc
feature lldp
<edit>
system qos
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type qos input fcoe-default-in-policy
  service-policy type network-qos fcoe-default-nq-policy
class-map type control-plane match-any copp-system-class-rpf-fail
<edit>
vlan 1
vlan 100
  name LAN
vlan 201
  fcoe vsan 201
  name SAN201
vlan 300
  name vpc-keepalive
vrf context management
  ip route 0.0.0.0/0 10.211.17.190
vpc domain 1
  peer-keepalive destination 10.211.17.135 source 10.211.17.136
  auto-recovery
vsan database
  vsan 201
fcdomain fcid database
  vsan 201 wwn 20:01:00:0e:1e:0d:89:d7 fcid 0x00e50000 dynamic
  vsan 201 wwn 20:01:00:0e:1e:0d:89:a7 fcid 0x00e50020 dynamic
  vsan 201 wwn 20:01:00:0e:1e:0d:89:2f fcid 0x00e50040 dynamic
  vsan 201 wwn 20:01:00:0e:1e:0d:89:77 fcid 0x00e50060 dynamic
  vsan 201 wwn 50:00:d3:10:00:ed:ef:32 fcid 0x00e50080 dynamic
  vsan 201 wwn 50:00:d3:10:00:ed:ef:34 fcid 0x00e500a0 dynamic
  vsan 201 wwn 50:00:d3:10:00:ed:ef:08 fcid 0x00e500a1 dynamic
  vsan 201 wwn 50:00:d3:10:00:ed:f0:07 fcid 0x00e50081 dynamic
  vsan 201 wwn 50:00:d3:10:00:ed:ef:1d fcid 0x00e50082 dynamic
  vsan 201 wwn 50:00:d3:10:00:ed:ef:1e fcid 0x00e50083 dynamic
  vsan 201 wwn 20:01:00:10:18:dd:c8:43 fcid 0x00e500c0 dynamic
  vsan 201 wwn 20:01:00:10:18:ef:82:07 fcid 0x00e50100 dynamic
  vsan 201 wwn 20:00:00:1b:21:7e:75:7b fcid 0x00e50120 dynamic
  vsan 201 wwn 20:00:00:1b:21:7e:7a:ff fcid 0x00e50140 dynamic
interface port-channel1
  description vpc-peer
  switchport mode trunk
  switchport trunk allowed vlan 1,100,300
  spanning-tree port type network
  vpc peer-link
interface vfc101
  bind interface Ethernet1/31
  switchport trunk allowed vsan 201
  switchport description vfc to SC8000
```



```

    no shutdown
interface vfc102
    bind interface Ethernet1/32
    switchport trunk allowed vsan 201
    switchport description vfc to SC8000
    no shutdown
interface vfc201
    bind interface Ethernet1/1
    switchport trunk allowed vsan 201
    switchport description vfc to R720-1
    no shutdown
interface vfc202
    bind interface Ethernet1/2
    switchport trunk allowed vsan 201
    switchport description vfc to R720-2
    no shutdown
interface vfc203
    bind interface Ethernet1/3
    switchport trunk allowed vsan 201
    switchport description vfc to R720-3
    no shutdown
interface vfc204
    bind interface Ethernet1/4
    switchport trunk allowed vsan 201
    switchport description vfc to R720-4
    no shutdown
interface vfc205
    bind interface Ethernet1/17
    switchport trunk allowed vsan 201
    switchport description vfc to R815-1_Broadcom
interface vfc206
    bind interface Ethernet1/18
    switchport trunk allowed vsan 201
    switchport description vfc to R815-2_Broadcom
interface vfc207
    bind interface Ethernet1/19
    switchport trunk allowed vsan 201
    switchport description vfc to R815-1_Intel
    no shutdown
interface vfc208
    bind interface Ethernet1/20
    switchport trunk allowed vsan 201
    switchport description vfc to R815-2_Intel
    no shutdown
vsan database
    vsan 201 interface vfc101
    vsan 201 interface vfc102
    vsan 201 interface vfc201
    vsan 201 interface vfc202
    vsan 201 interface vfc203
    vsan 201 interface vfc204
    vsan 201 interface vfc205
    vsan 201 interface vfc206
    vsan 201 interface vfc207
    vsan 201 interface vfc208
interface Ethernet1/1
    switchport mode trunk
    switchport trunk allowed vlan 100,201
    spanning-tree port type edge
interface Ethernet1/2

```



```

    switchport mode trunk
    switchport trunk allowed vlan 100,201
    spanning-tree port type edge
interface Ethernet1/3
    switchport mode trunk
    switchport trunk allowed vlan 100,201
    spanning-tree port type edge
interface Ethernet1/4
    switchport mode trunk
    switchport trunk allowed vlan 100,201
    spanning-tree port type edge
<edit>
interface Ethernet1/17
    switchport mode trunk
    switchport trunk allowed vlan 101,201
    spanning-tree port type edge
interface Ethernet1/18
    switchport mode trunk
    switchport trunk allowed vlan 101,201
    spanning-tree port type edge
interface Ethernet1/19
    switchport mode trunk
    switchport trunk allowed vlan 101,201
    spanning-tree port type edge
interface Ethernet1/20
    switchport mode trunk
    switchport trunk allowed vlan 101,201
    spanning-tree port type edge
<edit>
interface Ethernet1/31
    switchport mode trunk
    switchport trunk allowed vlan 201
    spanning-tree port type edge
interface Ethernet1/32
    switchport mode trunk
    switchport trunk allowed vlan 201
    spanning-tree port type edge
<edit>
interface Ethernet2/15
    description VPC link
    switchport mode trunk
    switchport trunk allowed vlan 1,100,300
    channel-group 1 mode active
interface Ethernet2/16
    description VPC link
    switchport mode trunk
    switchport trunk allowed vlan 1,100,300
    channel-group 1 mode active
interface mgmt0
    vrf member management
    ip address 10.211.17.136/26
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.7.0.0.N1.1.bin
boot system bootflash:/n5000-uk9.7.0.0.N1.1.bin
zone name CML-virtual-ports vsan 201
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
zone name CML-physical-ports vsan 201
    member pwnn 50:00:d3:10:00:ed:ef:08

```



```

    member pwnn 50:00:d3:10:00:ed:ef:1e
zone name R720-1 vsan 201
    member pwnn 20:01:00:0e:1e:0d:89:d7
    member pwnn 50:00:d3:10:00:ed:ef:34
    member pwnn 50:00:d3:10:00:ed:ef:32
zone name R720-2 vsan 201
    member pwnn 20:01:00:0e:1e:0d:89:2f
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
zone name R720-3 vsan 201
    member pwnn 20:01:00:0e:1e:0d:89:a7
    member pwnn 50:00:d3:10:00:ed:ef:34
    member pwnn 50:00:d3:10:00:ed:ef:32
zone name R720-4 vsan 201
    member pwnn 20:01:00:0e:1e:0d:89:77
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
zone name R815-1 vsan 201
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
    member pwnn 20:01:00:10:18:dd:c8:43
zone name R815-2 vsan 201
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
    member pwnn 20:01:00:10:18:ef:82:07
zone name R815-2-X520 vsan 201
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
    member pwnn 20:00:00:1b:21:7e:75:7b
zone name R815-1-X520 vsan 201
    member pwnn 50:00:d3:10:00:ed:ef:32
    member pwnn 50:00:d3:10:00:ed:ef:34
    member pwnn 20:00:00:1b:21:7e:7a:ff
zoneset name fcoe201test vsan 201
    member CML-virtual-ports
    member CML-physical-ports
    member R720-1
    member R720-2
    member R720-3
    member R720-4
    member R815-1
    member R815-2
    member R815-2-X520
    member R815-1-X520
zoneset activate name fcoe201test vsan 201

```



C Detailed CNA configuration

For the testing described in the previous sections, the QLogic QLE8262 CNA was used for host connectivity, however, there are other viable solutions supported by Dell. This section provides detailed configuration of the Broadcom 57800 series and Intel X520 series CNAs in addition to the QLE8262. Configuration details for both Windows Server 2012 R2 and vSphere ESXi 5.5 are included even though only the QLE8262 with Windows Server 2012 R2 was used to produce the test results presented in this white paper.

Each Windows Server was configured with two 10 GB volumes on the SAN while each ESXi server was configured with two 100 GB volumes (datastores) on the SAN. A single Windows 2012 R2 virtual machine was created on each ESXi server and a single 10 GB VMDK volume was created on each of the 100 GB datastores.

For additional configurations with the Intel and Broadcom CNAs, two PowerEdge R815 servers were used, each with Windows 2012 R2 installed. A second pair of PowerEdge R815s was configured with ESXi 5.5 U1. For each pair of systems, one contained Broadcom 57810 CNAs and the other Intel X520-DA2 CNAs. Each Windows host was configured with two 10 GB volumes on the SAN, while each ESXi server was configured with two 100 GB volumes (datastores). A single Windows 2012 R2 virtual machine was created on each ESXi server and a single 10 GB VMDK volume was created on each of the datastores created on the two 100 GB volumes on the SAN.



C.1 QLogic QLE8262

The QLogic QLE8262 is a converged network adapter with separate functions for Ethernet and FCoE support. To enable FCoE support, enter the BIOS configuration utility by pressing CTRL+Q during the power-on-self-test (POST) of the host server. The following screen is displayed.

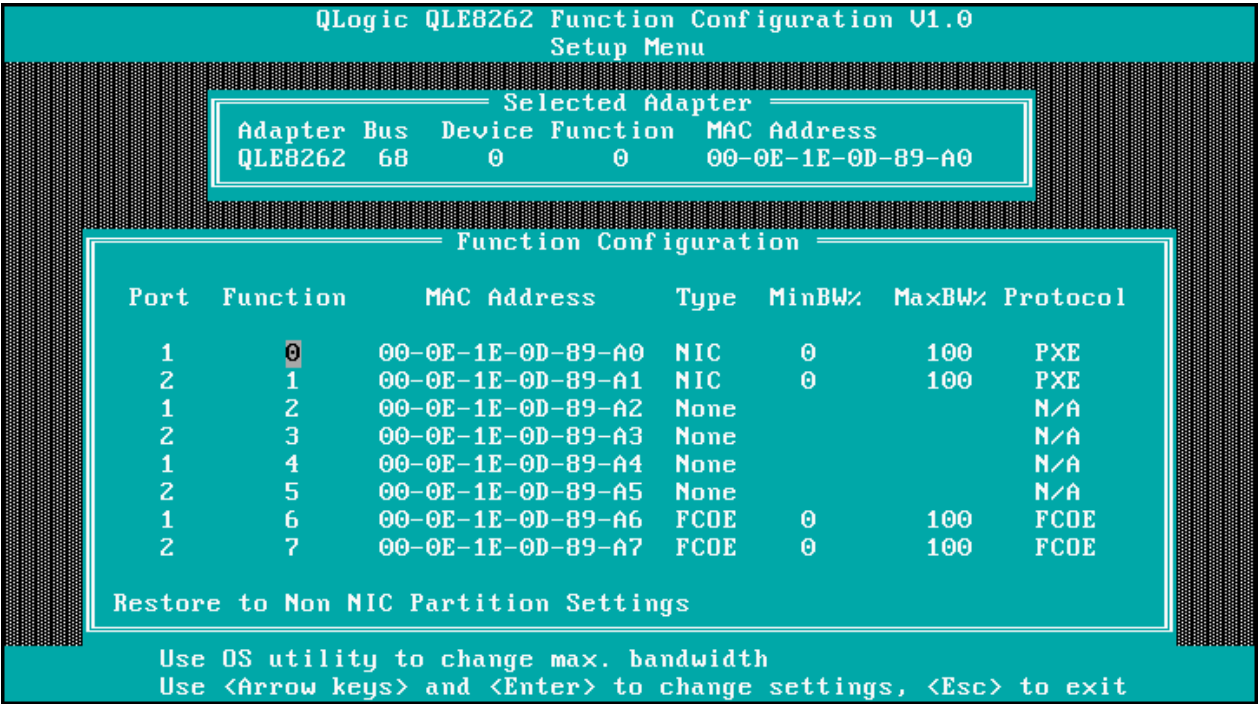


Figure 8 QLogic BIOS configuration utility showing FCoE protocol enabled

Ensure that the appropriate functions for Ethernet and FCoE are enabled. In this example, port 1 is assigned functions 0,2,4,6 while port 2 is assigned functions 1,3,5,7. Function 6 and 7 were modified to enable the FCoE protocol. In addition, the **Link Down Timeout** setting can be adjusted (Dell recommends changing it to 60 seconds) through this configuration utility. All other settings were left at factory defaults.



C.1.1 Microsoft Windows configuration

On each host, the QConvergeConsole utility was installed and used to configure the tagged VLAN that was used for carrying LAN traffic (VLAN ID 100).

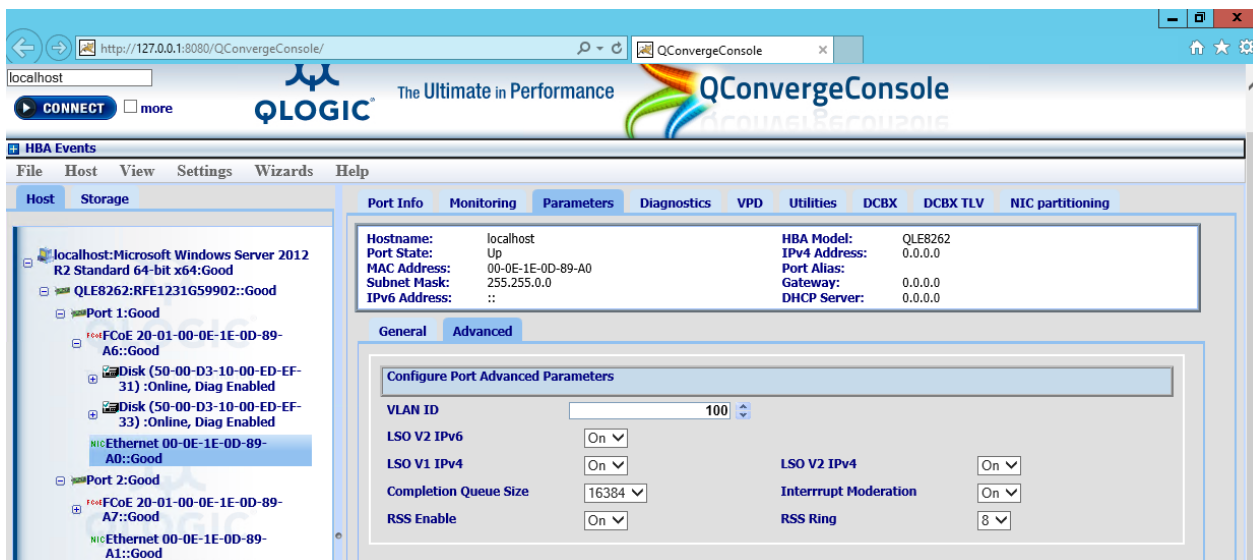


Figure 9 QConvergeConsole showing VLAN ID assignment for LAN traffic

For the NDIS Ethernet adapter, the native Windows 2012 R2 Load-balancing and Failover (teaming) driver were configured to create a single virtual interface with redundant links across both Cisco Nexus switches. The teaming mode was set to Switch Independent, which does not require further configuration on the switch ports that the CNAs are connected to. Because the VLAN was set on the CNA physical ports (using QConvergeConsole), the LBFO team was configured to use the default VLAN.



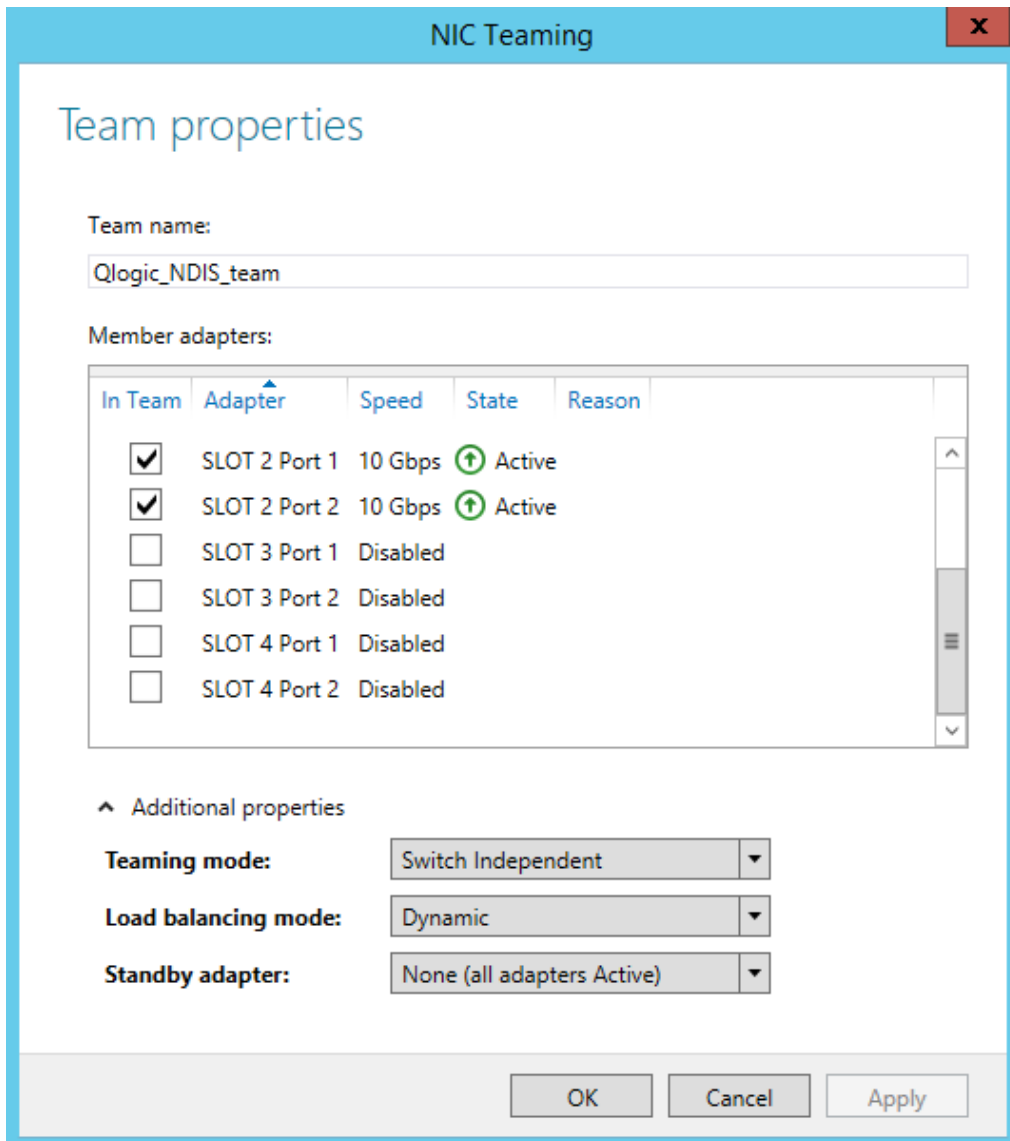


Figure 10 Windows 2012 R2 LBFO team using QLogic NDIS Ethernet adapters

C.1.2 VMWare ESXi 5.5 configuration

The QLogic Adapter CIM and vCenter Plug-in were installed on the vCenter system to enable management of the QLE8262 CNA from within vCenter. Once installed and enabled, a QConvergeConsole tab is available in the vSphere Client or vSphere Web Client.

ESXi 5.5 detects the FCoE-enabled function of the QLE8262 CNA as a storage adapter with the type **8200 Series 10GbE Converged Network Adapter (FCoE)**. A vSwitch was created containing the QLE8262 Ethernet adapters and VLAN 100 was set for VM client connectivity.

A new VMXNet3 network adapter was added to each VM and the appropriate IP address was configured.

C.2 Broadcom 57800 series

The Broadcom 57800 series family that includes the 57800, 57810 and 57840, all offer the ability to enable FCoE offload functionality on the adapter ports. By default, the 57800 series CNA has the Ethernet LAN function enabled and the additional FCoE offload functionality can be enabled with or without the use of NPAR (NIC partitioning).

Configuration of the CNA can be done by several methods. During the system BIOS initialization, a hot key (usually CTRL+S) can be invoked to enter the Broadcom BIOS setup. Some Dell PowerEdge servers also allow configuration of Broadcom 57800 series CNAs through the Lifecycle controller. Hitting F10 during the system initialization process will cause the system to enter the lifecycle controller.

Once the FCoE function is enabled and all appropriate switch configuration is performed, the newly added storage adapters should be visible from Storage Center, where they can be added to a server.

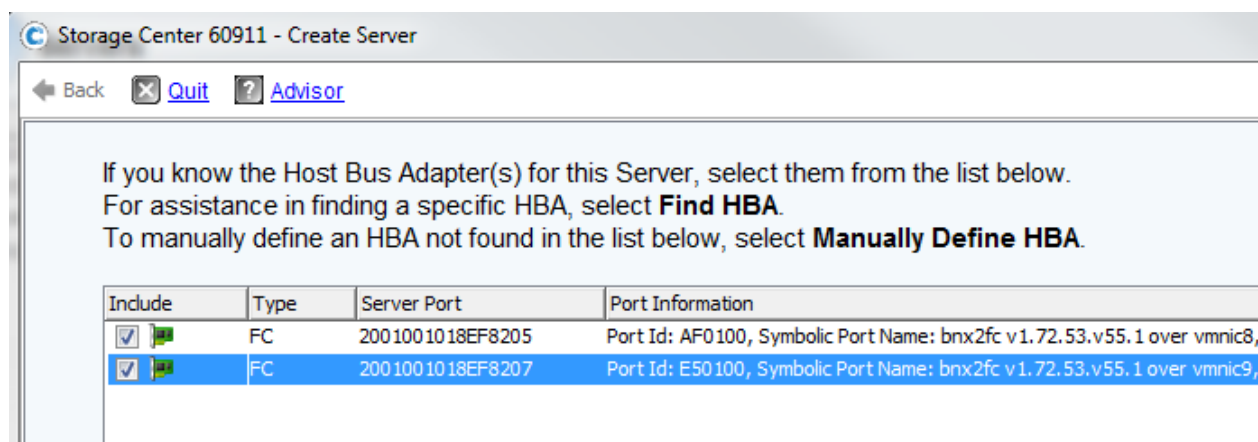


Figure 11 Adding a server to Compellent Storage Center

C.2.1 Microsoft Windows configuration

For Microsoft Windows 2008 or 2012 hosts, the Broadcom Advanced Configuration Suite (BACS) can also be installed and used to enable the FCoE offload function.

With Microsoft Windows, once the FCoE functionality is enabled, the appropriate storage controller port drivers will be loaded. Once the storage is visible to the host system, the MPIO feature should also be installed and configured. See the [Windows Server MPIO Best Practices for Dell Compellent Storage Center](http://en.community.dell.com/techcenter/extras/m/white_papers/20437917.aspx) guide for details on configuring MPIO at http://en.community.dell.com/techcenter/extras/m/white_papers/20437917.aspx.



C.2.2 VMware ESXi 5.x configuration

Currently, there is not an equivalent of BACS for VMWare ESXi 5.x. Configuration must be done from either the system or the CNA BIOS setup utilities.

Once ESXi is installed, the LAN function of each CNA should appear in the Network Adapters configuration section of the vSphere client. The administrator will need to correlate the vmnic assignment with the physical adapter and specifically the FCoE enabled function of the Broadcom CNA. The easiest way to do this is to record the MAC address of each port while in the system or CNA BIOS setup utility. Then from the Network Adapters, the associated vmnic assignment can be determined.















Hardware		Network Adapters				
Processors Memory Storage Networking Storage Adapters ▶ Network Adapters Advanced Settings Power Management		Device	Speed	Configured	Switch	MAC Address
		Broadcom Corporation Broadcom NetXtreme II BCM5709 1000Base-T				
		 vmnic3	Down	Negotiate	None	F0:4d:a2:3d:f6:34
		 vmnic2	Down	Negotiate	None	F0:4d:a2:3d:f6:32
		 vmnic1	Down	Negotiate	None	F0:4d:a2:3d:f6:30
		 vmnic0	1000 Full	Negotiate	vSwitch0	F0:4d:a2:3d:f6:2e
		Broadcom Corporation NetXtreme II BCM57810 10 Gigabit Ethernet Multi Function				
		 vmnic9	10000 F...	10000 Full	None	00:10:18:ef:82:06
		 vmnic8	10000 F...	10000 Full	None	00:10:18:ef:82:04
		 vmnic5	10000 F...	10000 Full	None	00:10:18:ef:82:02
		 vmnic4	10000 F...	10000 Full	None	00:10:18:ef:82:00
		 vmnic13	10000 F...	10000 Full	None	00:10:18:ef:82:0e
		 vmnic12	10000 F...	10000 Full	None	00:10:18:ef:82:0c
		 vmnic11	10000 F...	10000 Full	None	00:10:18:ef:82:0a
		 vmnic10	10000 F...	10000 Full	None	00:10:18:ef:82:08
		Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection				
		 vmnic7	Down	Negotiate	None	00:1b:21:7e:75:79
		 vmnic6	Down	Negotiate	None	00:1b:21:7e:75:78

Figure 12 ESXi 5.5 network adapters configuration

Even though the Broadcom 57800 series provides FCoE offload functionality, ESXi provides a software initiator for configuring FCoE and initiating connectivity. To enable the FCoE software initiator, go to the Storage Adapters configuration in the vSphere client and click **Add**. Choose the associated vmnic to be used for FCoE connectivity, and then repeat the process to add the second CNA. The VLAN will initially show a value of 0. Once the FIP VLAN discovery process completes, the correct VLAN should be automatically populated (wait a couple of minutes and then check the properties of the storage adapter to confirm).

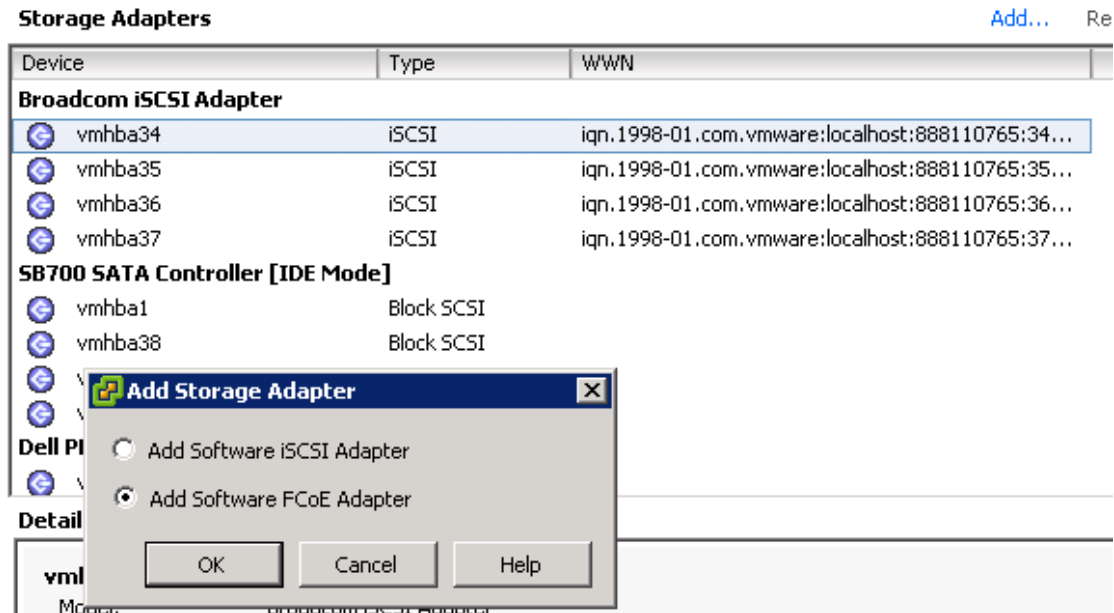


Figure 13 Configuration of vSphere ESXi 5.5 Software FCoE Adapter

C.3 Intel X520

The Intel X520 family adapters are also CNAs that support convergence of Ethernet LAN and FCoE SAN functionality.

C.3.1 Microsoft Windows configuration

Ensure that the latest Dell supported driver for the Intel X520 adapter (available from support.dell.com) is installed. During the installation, select the following optional components:

- Intel PROSet for Windows Device Manager
- FCoE using Data Center Bridging

These selections install and configure an optional DCB software layer provided by Intel to enable FCoE connectivity. The PROSet utility can be used to configure or verify settings for the CNA. For the version of drivers tested, the default settings were optimal and therefore no additional configuration was required.

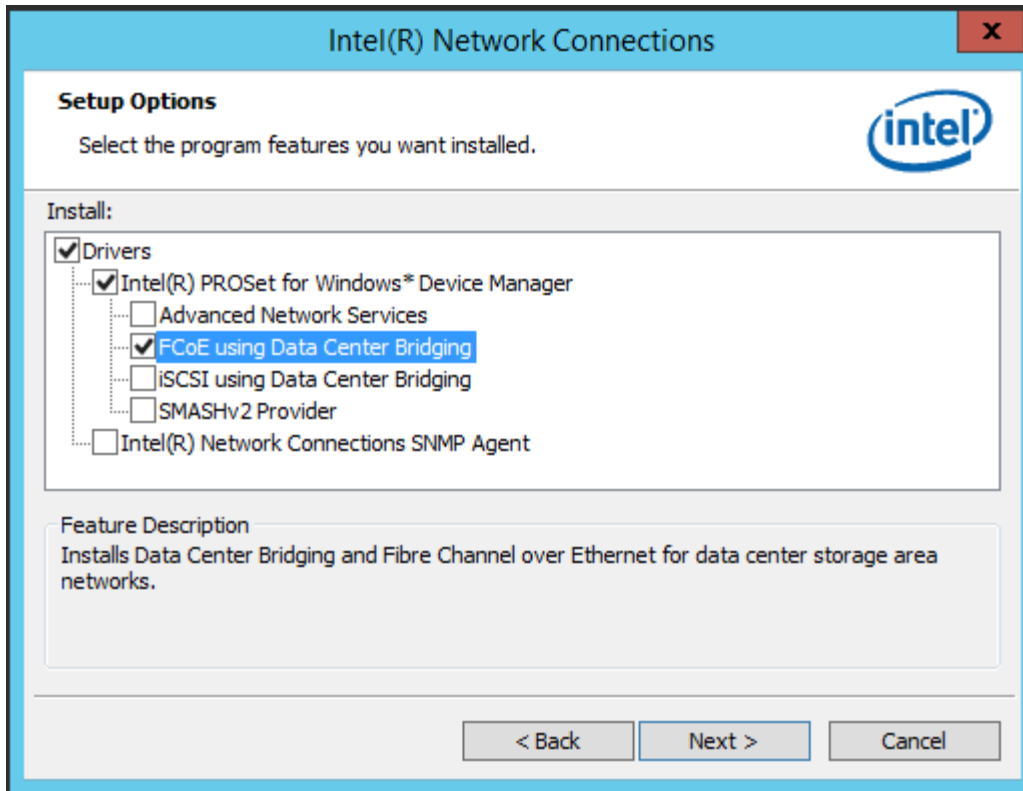


Figure 14 Windows driver installation options for Intel X520/X540 adapters

C.3.2 VMware ESXi 5.x configuration

Before the FCoE software initiator can be bound to an Intel X520, the network adapter must first be part of a virtual switch (vSwitch).

1. Using the vSphere client, click **Add Networking** from the network configuration
2. Create a Virtual Machine port group, and then add the appropriate vmnic ports to the vSwitch.
3. Ensure that the proper VLAN ID for LAN access is configured.

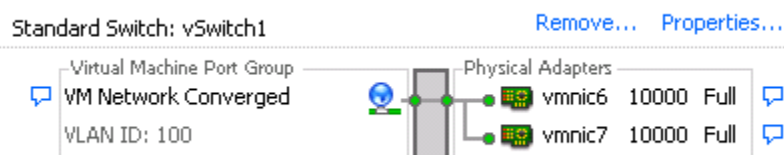


Figure 15 vSwitch configuration for Intel X520 adapter

4. Next, add a new Storage Adapter and select the appropriate vmnic that corresponds to the Intel X520 adapter port.

5. Right-click an adapter to open the properties. The VLAN field will initially show a value of 0 and will populate with the correct value after discovery completes.

If it does not, this is usually an indication of misconfiguration on the switch. In the following diagram, VLAN 200 was discovered.

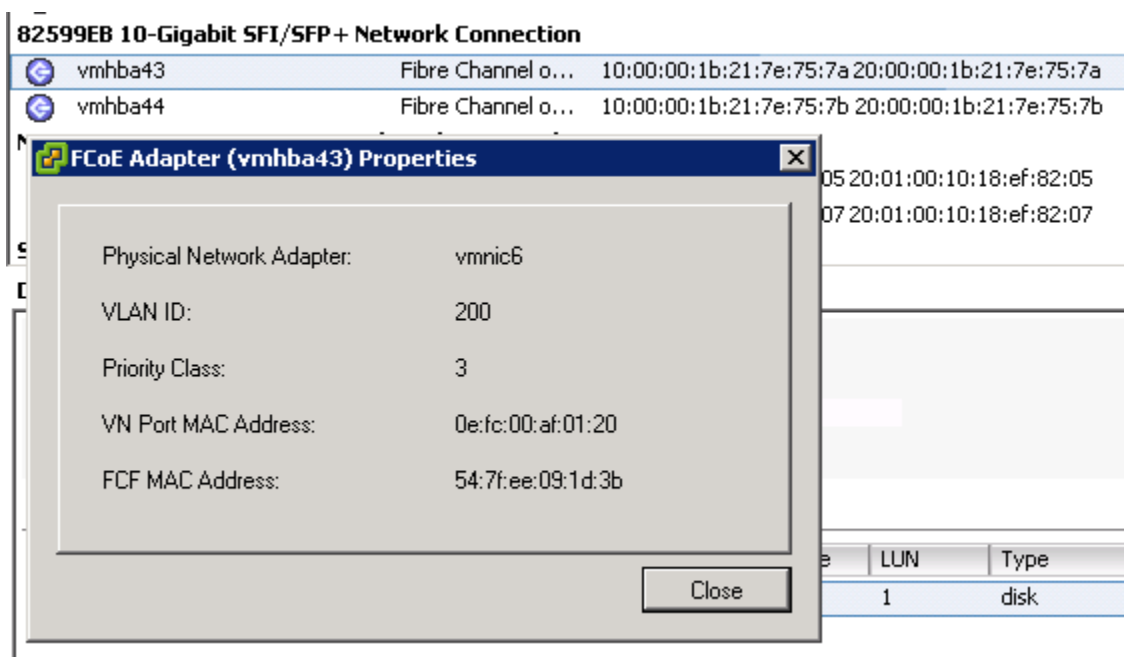


Figure 16 FCoE adapter properties showing VLAN ID

D Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- Dell EqualLogic Configuration Guide:
<http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19852516/download.aspx>
- Dell EqualLogic Compatibility Matrix
<http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19856862.aspx>
- Windows Server MPIO Best Practices for Dell Compellent Storage Center
http://en.community.dell.com/techcenter/extras/m/white_papers/20437917.aspx
- Data Center Bridging: Standards, Behavioral Requirements, and Configuration Guidelines
<http://en.community.dell.com/techcenter/storage/w/wiki/4396.data-center-bridging-standards-behavioral-requirements-and-configuration-guidelines-by-sis.aspx>

