FCoE - Design, Operations and Management Best Practices

Ron Fuller – CCIE #5851 (R&S/Storage)
Technical Marketing Engineer, Nexus 7000
rfuller@cisco.com
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
Unified Fabric and FCoE

What?
Unified Fabric & FCoE

Why?

**FCoE**
- Encapsulation of FC Frames over Ethernet
- Enables FC to Run on a Lossless Ethernet Network

**Benefits**
- Fewer Cables
  - Both block I/O & Ethernet traffic co-exist on same cable
- Fewer adapters needed
- Overall less power
- Interoperates with existing SAN’s
  - Management of SAN’s remains constant
- No Gateway
Unified Fabric

Why?

Ethernet Model has Proven Benefits

**Ethernet Economic Model**
- Embedded on Motherboard
- Integrated into O/S
- Many Suppliers
- Mainstream Technology
- Widely Understood
- Interoperability by Design

**FC Economic Model**
- Always a stand alone Card
- Specialized Drivers
- Few Suppliers
- Specialized Technology
- Special Expertise
- Interoperability by Test
Unified Fabric

Why?

- Ability to re-provision any compute unit to leverage any access method to the data stored on the ‘spindle’
- Serialized Re-Use – (e.g. Boot from SAN and Run from NAS)
- Virtualization requires that the Storage Fabric needs to exist everywhere the IP fabric does
Unified Fabric & FCoE
When? – FCoE Projected Growth

Source: Infonetics

<table>
<thead>
<tr>
<th>Product segment</th>
<th>Revenue (US$M)</th>
<th>% Change QoQ</th>
<th>% Change YoY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN switches</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC switches</td>
<td>$477</td>
<td>$491</td>
<td>$467</td>
</tr>
<tr>
<td>FCoE switches</td>
<td>$25.4</td>
<td>$36.2</td>
<td>$83.0</td>
</tr>
<tr>
<td>SAN adapters</td>
<td>$185</td>
<td>$222</td>
<td>$205</td>
</tr>
<tr>
<td>FC HBAs</td>
<td>$158</td>
<td>$185</td>
<td>$168</td>
</tr>
<tr>
<td>iSCSI HBAs</td>
<td>$18.2</td>
<td>$22.8</td>
<td>$24.7</td>
</tr>
<tr>
<td>FCoE CNAs</td>
<td>$8.4</td>
<td>$13.9</td>
<td>$12.5</td>
</tr>
<tr>
<td>Total SAN</td>
<td>$687</td>
<td>$749</td>
<td>$755</td>
</tr>
</tbody>
</table>

© 2012 Cisco and/or its affiliates. All rights reserved.
Cisco Public
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
FCoE Protocol Fundamentals
Standards for I/O Consolidation

FCoE

www.T11.org

Fibre Channel on network media
FC-BB-5

Completed June 2009
Published by ANSI in May 2010

IEEE 802.1

DCB

PFC

IEEE 802.1Qbb
Priority-based Flow Control

ETS

IEEE 802.1Qaz
Priority Grouping
Enhanced Transmission Selection

DCBx

IEEE 802.1Qaz
Configuration Verification

Completed March 2011
Forwarded to RevCom for publication
FCoE Protocol Fundamentals
Fibre Channel over Ethernet (FCoE)

- Fibre Channel over Ethernet provides a high capacity and lower cost transport option for block based storage
- Two protocols defined in the standard
  - FCoE – Data Plane Protocol
  - FIP – Control Plane Protocol
- FCoE is a standard - June 3rd 2009, the FC-BB-5 working group of T11 completed its work and unanimously approved a final standard for FCoE
- FCoE ‘is’ Fibre Channel
FCoE Protocol Fundamentals
Protocol Organization – Data and Control Plane

- **FC-BB-5** defines two protocols required for an FCoE enabled Fabric

### FCoE
- Data Plane
- It is used to carry most of the FC frames and all the SCSI traffic
- Uses Fabric Assigned MAC address (dynamic) : FPMA
- IEEE-assigned Ethertype for FCoE traffic is 0x8906

### FIP (FCoE Initialization Protocol)
- It is the control plane protocol
- It is used to discover the FC entities connected to an Ethernet cloud
- It is also used to login to and logout from the FC fabric
- Uses unique BIA on CNA for MAC
- IEEE-assigned Ethertype for FCoE traffic is 0x8914

FCoE Protocol Fundamentals
It’s Fibre Channel Control Plane + FIP

- From a Fibre Channel standpoint it’s
  FC connectivity over a new type of cable called… Ethernet

- From an Ethernet standpoints it’s
  Yet another ULP (Upper Layer Protocol) to be transported

Diagram:
- FC-0 Physical Interface
- FC-1 Encoding
- FC-2 Framing & Flow Control
- FC-3 Generic Services
- FC-4 ULP Mapping
- FCoE Logical End Point
- Ethernet Media Access Control
- Ethernet Physical Layer
Neighbour Discovery and Configuration (VN – VF and VE to VE)

Step 1: FCoE VLAN Discovery
- FIP sends out a multicast to ALL_FCF_MAC address looking for the FCoE VLAN
- FIP frames use the native VLAN

Step 2: FCF Discovery
- FIP sends out a multicast to the ALL_FCF_MAC address on the FCoE VLAN to find the FCFs answering for that FCoE VLAN
- FCF’s responds back with their MAC address

Step 3: Fabric Login
- FIP sends a FLOGI request to the FCF_MAC found in Step 2
- Establishes a virtual link between host and FCF

** FIP does not carry any Fibre Channel frames
FCoE Protocol Fundamentals
Fibre Channel Forwarder - FCF

- FCF (Fibre Channel Forwarder) is the Fibre Channel switching element inside an FCoE switch
  - Fibre Channel logins (FLOGIs) happens at the FCF
  - Consumes a Domain ID

- FCoE encap/decap happens within the FCF
  - Forwarding based on FC information

```
FCoE Switch

FC Domain ID : 15

FCF

Ethernet Bridge

FC port
FC port
FC port
FC port
```

- FCF (Fibre Channel Forwarder) is the Fibre Channel switching element inside an FCoE switch
  - Fibre Channel logins (FLOGIs) happens at the FCF
  - Consumes a Domain ID

- FCoE encap/decap happens within the FCF
  - Forwarding based on FC information

```
FCoE Switch

FC Domain ID : 15

FCF

Ethernet Bridge

FC port
FC port
FC port
FC port
```
FCoE Protocol Fundamentals
Explicit Roles still defined in the Fabric

- FCoE does not change the explicit port level relationships between devices (add a ‘V’ to the port type when it is an Ethernet wire)
  - Servers (VN_Ports) connect to Switches (VF_Ports)
  - Switches connect to Switches via Expansion Ports (VE_Ports)
FCoE Protocol Fundamentals
CNA: Converged Network Adapter

- Converged Network Adapter (CNA) presents two PCI address to the Operating System (OS)
- OS loads two unique sets of drivers and manages two unique application topologies
- Server participates in both topologies since it has two stacks and thus two views of the same ‘unified wire’
  - SAN Multi-Pathing provides failover between two fabrics (SAN ‘A’ and SAN ‘B’)
  - NIC Teaming provides failover within the same fabric (VLAN)
- Operating System sees:
  - Dual port 10 Gigabit Ethernet adapter
  - Dual Port 4 Gbps Fibre Channel HBAs
FCoE, Same Model as FC
Connecting to the Fabric

- Same host to target communication
  - Host has 2 CNA’s (one per fabric)
  - Target has multiple ports to connect to fabric
- Connect to a DCB capable switch
  - Port Type Negotiation (FC port type will be handled by FIP)
  - Speed Negotiation
  - DCBX Negotiation
- Access switch is a Fibre Channel Forwarder (FCF)
- Dual fabrics are still deployed for redundancy
My port is up…can I talk now?

FIP and FCoE Login Process

- **Step 1: FIP Discovery Process**
  - FCoE VLAN Discovery
  - FCF Discovery
  - Verifies Lossless Ethernet is capable of FCoE transmission

- **Step 2: FIP Login Process**
  - Similar to existing Fibre Channel Login process - sends FLOGI to upstream FCF
  - FCF assigns the host a Enode MAC address to be used for FCoE forwarding (Fabric Provided MAC Address - FPMA)

---

**Diagram:**

- **Target**
  - FC or FCoE Fabric
  - E_ports or VE_Port

- **VN_Port**

- **VF_Port**

- **CNA**
  - **FC-MAC**

- **ENode**
  - FC-MAP (0E-FC-xx)
  - FC-ID 10.00.01

- **FIP FLOGI**

- **FIP Discovery**

---

**Table:**

| FC-MAP Address | FC-MAP (0E-FC-xx) | FC-ID | 7.8.9
|----------------|-------------------|-------|---

---

TECDT-2001  © 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public

19
# FCoE Protocol Fundamentals

Fibre Channel over Ethernet Addressing Scheme

- Enode FCoE MAC assigned for each FCID
- Enode FCoE MAC composed of a FC-MAP and FCID
  - FC-MAP is the upper 24 bits of the Enode’s FCoE MAC
  - FCID is the lower 24 bits of the Enode’s MAC
- FCoE forwarding decisions still made based on FSPF and the FCID within the Enode MAC
- For different physical networks the FC-MAP is used as a fabric identifier
  - FIP snooping will use this as a mechanism in realizing the ACLs put in place to prevent data corruption

<table>
<thead>
<tr>
<th>FC-MAP Address</th>
<th>FC-MAP (0E-FC-xx)</th>
<th>FC-ID 10.00.01</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-MAC Address</td>
<td>FC-MAP (0E-FC-xx)</td>
<td>FC-ID 7.8.9</td>
</tr>
</tbody>
</table>
My port is up…can I talk now?
FIP and FCoE Login Process

- The FCoE VLAN is manually configured on the Nexus 5K

```
    tme-n5k-2# conf t
    Enter configuration commands, one per line. End with CNTL/Z.
    tme-n5k-2(config)# vlan 2
    tme-n5k-2(config)# fcoe vsan 2
    tme-n5k-2(config-vlan)# show vlan fcoe
    VLAN  VSAN  Status
    ------  ------  ------
    2       2       Operational
```

- The FCF-MAC address is configured on the Nexus 5K by default once `feature fcoe` has been configured
  - This is the MAC address returned in step 2 of the FIP exchange
  - This MAC is used by the host to login to the FCoE fabric

```
    tme-n5k-2# show fcoe
    Global FCF details
    FCF-MAC is 00:0d:ec:df:5f:80
    FC-MAP is 0e:fc:00
    FCF Priority is 128
    FKA Advertisement period for FCF is 8 seconds
```

** FIP does not carry any Fibre Channel frames
Login complete...almost there

Fabric Zoning

- Zoning is a feature of the fabric and is independent of Ethernet transport
- Zoning can be configured on the Nexus 5000/7000 using the CLI or Fabric Manager
- If Nexus 5000 is in NPV mode, zoning will be configured on the upstream core switch and pushed to the Nexus 5000
- Devices acting as Fibre Channel Forwarders participate in the Fibre Channel security (Zoning) control
- DCB ‘only’ bridges do not participate in zoning and require additional security mechanisms (ACL applied along the forwarding path on a per FLOGI level of granularity)
Login complete
Flogi and FCoE Databases are populated

- Login process: **show flogi database** and **show fcoe database** show the logins and associated FCIDs, xWWNs and FCoE MAC addresses

```
<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>VfC1</td>
<td>2</td>
<td>0xb00000</td>
<td>21:00:00:00:00:c0:dd:11:29:1d</td>
<td>20:00:00:00:c0:dd:11:29:1d</td>
</tr>
<tr>
<td>VfC2</td>
<td>2</td>
<td>0xb00004</td>
<td>21:00:00:00:00:c0:dd:11:2c:61</td>
<td>20:00:00:00:c0:dd:11:2c:61</td>
</tr>
<tr>
<td>VfC14</td>
<td>2</td>
<td>0xb0004</td>
<td>21:00:00:00:00:c0:dd:12:13:8f</td>
<td>20:00:00:00:c0:dd:12:13:8f</td>
</tr>
<tr>
<td>VfC15</td>
<td>2</td>
<td>0xb0005</td>
<td>21:00:00:00:00:c0:dd:12:13:83</td>
<td>20:00:00:00:c0:dd:12:13:83</td>
</tr>
<tr>
<td>VfC16</td>
<td>2</td>
<td>0xb0006</td>
<td>21:00:00:00:00:c0:dd:12:14:23</td>
<td>20:00:00:00:c0:dd:12:14:23</td>
</tr>
</tbody>
</table>
```

Total number of flogi = 8.

```
<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>MAC ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VfC1</td>
<td>0xb0000</td>
<td>21:00:00:00:00:c0:dd:11:29:1d</td>
<td>00:c0:dd:11:29:1d</td>
</tr>
<tr>
<td>VfC2</td>
<td>0xb0001</td>
<td>21:00:00:00:00:c0:dd:11:2c:61</td>
<td>00:c0:dd:11:2c:61</td>
</tr>
<tr>
<td>VfC14</td>
<td>0xb0004</td>
<td>21:00:00:00:00:c0:dd:12:13:8f</td>
<td>00:c0:dd:12:13:8f</td>
</tr>
<tr>
<td>VfC15</td>
<td>0xb0005</td>
<td>21:00:00:00:00:c0:dd:12:13:83</td>
<td>00:c0:dd:12:13:83</td>
</tr>
<tr>
<td>VfC16</td>
<td>0xb0006</td>
<td>21:00:00:00:00:c0:dd:12:14:23</td>
<td>00:c0:dd:12:14:23</td>
</tr>
</tbody>
</table>
```
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
Nexus 5500 Series
Fibre Channel, FCoE and Unified Ports

- Nexus 5000 and 5500 are full feature Fibre Channel fabric switches
  - No support for IVR, FCIP, DMM
- Unified Port supports multiple transceiver types
  - 1G Ethernet Copper/Fibre
  - 10G Ethernet Copper/Fibre
  - 10G DCB/FCoE Copper/Fibre
  - 1/2/4/8G Fibre Channel
- Change the transceiver and connect evolving end devices,
  - Server 1G to 10G NIC migration
  - FC to FCoE migration
  - FC to NAS migration

Any Unified Port can be configured as
- Ethernet
- or
- Fibre Channel

Unified Port – ‘Any’ device in any rack connected to the same edge infrastructure
Nexus 5500 Series
5548UP/5596UP – UPC (Gen-2) and Unified Ports

- With the 5.0(3)N1 and later releases each module can define any number of ports as Fibre Channel (1/2/4/8 G) or Ethernet (either 1G or 10G)
- Initial SW releases supports only a continuous set of ports configured as Ethernet or FC within each ‘slot’
  - Eth ports have to be the first set and they have to be one contiguous range
  - FC ports have to be second set and they have to be contiguous as well
- Future SW release will support per port dynamic configuration

```
no n5k(config)# slot <slot-num>
n5k(config-slot)# port <port-range> type <fc | ethernet>
```
**Nexus 2000 Series**

**FCoE Support**

- 32 server facing 10Gig/FCoE ports
  - T11 standard based FIP/FCoE support on all ports
- 8 10Gig/FCoE uplink ports for connections to the Nexus 5K
- Support for DCBx
- N7K will support FCoE on 2232 (Future)

**N2232PP**
32 Port 1/10G FCoE Host Interfaces
8 x 10G Uplinks

**N2232TM**
32 Port 1/10GBASE-T Host Interfaces
8 x 10G Uplinks (Module)

- FCoE not ‘yet’ certified for 10GBaseT
- Undesired coupling of signal between adjacent cables
- Main electrical parameter limiting the performance of 10G
- Cannot be cancelled
- Re-Training is a major barrier to use of 10GBaseT for block level storage (FCoE)
DC Design Details – Blade Chassis
Nexus B22 Series Fabric Extender

- B22 extends FEX connectivity into the HP blade chassis
- Cisco Nexus 5000 Switch is a single management point for all the blade chassis I/O modules
- 66% decrease in blade management points*
- Blade & rack networking consistency
- Interoperable with Nexus 2000 Fabric Extenders in the same Nexus parent switch
- End-to-end FCoE support
- Support for 1G & 10G, LOM and Mez
- Dell supports Pass-Thru as an alternative option to directly attaching Blade Servers to FEX ports
Nexus 7000 F-Series SFP+ Module
FCoE Support Q2CY11

- 32 & 48 port 1/10 GbE for Server Access and Aggregation
- F1 Supports FCoE
- F2 support for FCoE targeted 1HCY12
  FEX + FCoE support – 2HCY12
- 10 Gbps Ethernet supporting Multiprotocol Storage Connectivity
  - Supports FCoE, iSCSI and NAS
  - Loss-Less Ethernet: DCBX, PFC, ETS
- Enables Cisco FabricPath for increased bisectional bandwidth for iSCSI and NAS traffic
- FCoE License (N7K-FCOEF132XP)
  - $10,000 Cisco List
  - One license per F1/F2 module
- SAN Enterprise (N7K-SAN1K9)
  - $15,000 Cisco List – per chassis
  - IVR, VSAN Based Access Control, Fabric Binding
Storage VDC on the Nexus 7000

Supported VDC models

- Separate VDC running ONLY storage related protocols
- Storage VDC: a *virtual* MDS FC switch
- Running only FC related processes
- Only one such VDC can be created
- Provides control plane separation

**Shared Converged Port**

Model for host/target interfaces, *not* VE_Port

Ingress Ethernet traffic is split based on frame ether type

FCoE traffic is processed in the context of the Storage VDC
Creating the Storage VDC
Port and VLAN allocations

- Create VDC of type storage and allocate non-shared interfaces:

N7K-50(config)# vdc fcoe id 2 type storage
N7K-50(config-vdc)# allocate interface Ethernet4/1-16, Ethernet4/19-22

- Allocate FCoE vlan range from the Owner VDC to the Storage VDC. This is a necessary step for sharing interfaces to avoid vlan overlap between the Owner VDC and the Storage VDC

N7K-50(config) vdc fcoe id 2
N7K-50(config-vdc)# allocate fcoe-vlan-range 10-100 from vdcs n7k-50

- Allocated the shared interfaces:

N7K-50(config-vdc)# allocate shared interface Ethernet4/17-18

- Install the license for the FCoE Module.

n7k-50(config)# license fcoe module 4
Storage VDC
F2 line cards

- Some restrictions when using mixed line cards (F1/F2/M1)
  - F2 ports need to be in a dedicated VDC if using ‘shared ports’

**Shared Ports**

- NX-OS 5.2
  - Storage VDC
  - F1/M1 VDC
  - F1

- NX-OS 6.1 (1HCY12)
  - Storage VDC
  - F2 VDC
  - F2

**Dedicated Ports**

- NX-OS 6.1 (1HCY12)
  - F2 VDC
  - Storage VDC
  - F1/M1 VDC
  - F2
  - F1
  - Any non-F2
MDS 9000 8-Port 10G FCoE Module

FCoE Support

- Enables integration of existing FC infrastructure into Unified Fabric
  - 8 FCoE ports at 10GE full rate in MDS 9506, 9509, 9513
  - No FCoE License Required

- Standard Support
  - T11 FCoE
  - IEEE DCBX, PFC, ETS

- Connectivity – FCoE Only, No LAN
  - VE to Nexus 5000, Nexus 7000, MDS 9500
  - VF to FCoE Targets

- Optics Support
  - SFP+ SR/LR, SFP+ 1/3/5m Passive, 7/10m Active CX-1 (TwinAx)

- Requirements
  - SUP2A
  - Fabric 2 modules for the backplane (applicable to 9513 only)
MDS 9000 8-Port 10G FCoE Module

FCoE Support

There is no need to enable FCoE explicitly on the MDS switch. The following features will be enabled once an FCoE capable linecard is detected.

Install feature-set fcoe
feature lldp
feature-set fcoe
feature vlan-vsans-mapping

Create VSAN and VLAN, Map VLAN to VSAN for FCoE

```
pod3-9513-71(config)# vsan database
pod3-9513-71(config-vsan-db)# vsan 50
pod3-9513-71(config-vsan-db)# vlan 50
pod3-9513-71(config-vlan)# fcoe vsan 50
```

Build the LACP Port Channel on the MDS
Create VE port and assign to the LACP Port-channel

```
pod3-9513-71(config-if-range)# interface vfc-port-channel 501
pod3-9513-71(config-if)# switchport mode e
pod3-9513-71(config-if)# switchport trunk allowed vsan 50
pod3-9513-71(config-if)# no shut
```
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
Network vs. Fabric
Differences & Similarities

- Ethernet is non-deterministic.
  Flow control is destination-based
  Relies on TCP drop-retransmission / sliding window

- Fibre-Channel is deterministic.
  Flow control is source-based (B2B credits)
  Services are fabric integrated (no loop concept)

Networks
- Connectionless
- Logical circuits
- Unreliable transfers
- High connectivity
- Higher latency
- Longer distance
- Software intense

Channels
- Connection service
- Physical circuits
- Reliable transfers
- High speed
- Low latency
- Short distance
- Hardware intense
Network vs. Fabric
LAN Design – Access/Aggregation/Core

- Servers typically dual homed to two or more access switches
- LAN switches have redundant connections to the next layer
- Distribution and Core can be collapsed into a single box
- L2/L3 boundary typically deployed in the aggregation layer
  - Spanning tree or advanced L2 technologies (vPC) used to prevent loops within the L2 boundary
  - L3 routes are summarized to the core
- Services deployed in the L2/L3 boundary of the network (load-balancing, firewall, NAM, etc)
Network vs. Fabric
SAN Design – Two ‘or’ Three Tier Topology

- “Edge-Core” or “Edge-Core-Edge” Topology
- Servers connect to the edge switches
- Storage devices connect to one or more core switches
- HA achieved in two physically separate, but identical, redundant SAN fabric
- Very low oversubscription in the fabric (1:1 to 12:1)
- FLOGI Scaling Considerations

Example: 10:1 O/S ratio
60 Servers with 4 Gb HBAs
240 G
24 G
24 G
Network vs. Fabric
Converged and Dedicated Links

- **Converged Link** to the access switch
  - Cost savings in the reduction of required equipment
  - “cable once” for all servers to have access to both LAN and SAN networks

- **Dedicated Link** from access to aggregation
  - Separate links for SAN and LAN traffic - both links are same I/O (10GE)
  - Advanced Ethernet features can be applied to the LAN links
  - Maintains fabric isolation

[Diagram with labels: Core, Agg, Access, Nexus, MDS FC SAN A, MDS FC SAN B, Converged FCoE Link, Dedicated FCoE Links/Port-Channels, Converged FCoE Link, Dedicated FCoE Link, Port Channel]
Converged Links and vPC

Shared wire and VPC – does it break basic SAN design fundamentals?

Now that I have Converged Link Support. Can I deploy vPC for my Storage Traffic?

- vPC with Converged Links provides an Active-Active connection for FCoE traffic
- Seemingly more bandwidth to the Core...
- Ethernet forwarding behavior can break SAN A/B separation

Currently Not supported on Nexus Switches (exception is the dual homed FEX)
“Fabric vs. Network” or “Fabric & Network”
SAN Dual Fabric Design

- Will you migrate the SAN dual fabric HA model into the LAN full meshed HA model
  - Is data plane isolation required? (traffic engineering)
  - Is control plane isolation required? (VDC, VSAN)
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
Ethernet Enhancements
Can Ethernet Be Lossless?

- Yes, with Ethernet PAUSE Frame

- Defined in IEEE 802.3—Annex 31B

- The PAUSE operation is used to inhibit transmission of data frames for a specified period of time

- Ethernet PAUSE transforms Ethernet into a lossless fabric, a requirement for FCoE
## Ethernet Enhancements

### IEEE DCB

- Developed by IEEE 802.1 Data Center Bridging Task Group (DCB)
- All Standards Complete

<table>
<thead>
<tr>
<th>Standard / Feature</th>
<th>Status of the Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1Qbb</td>
<td>Completed</td>
</tr>
<tr>
<td>Priority-based Flow Control (PFC)</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.3bd</td>
<td>Completed</td>
</tr>
<tr>
<td>Frame Format for PFC</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1Qaz</td>
<td>Completed</td>
</tr>
<tr>
<td>Enhanced Transmission Selection (ETS) and Data Center Bridging eXchange (DCBX)</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1Qau</td>
<td>Complete, published March 2010</td>
</tr>
<tr>
<td>Congestion Notification</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1Qbh Port Extender</td>
<td>In its first task group ballot</td>
</tr>
</tbody>
</table>

CEE (Converged Enhanced Ethernet) is an informal group of companies that submitted initial inputs to the DCB WGs.
Ethernet Enhancements
DCB “Virtual Links”

Ability to support different forwarding behaviours, e.g. QoS, MTU, … queues within the “lanes”
NX-OS QoS Requirements
CoS or DSCP?

- We have non IP based traffic to consider again
  - FCoE – Fibre Channel Over Ethernet
  - RCoE – RDMA Over Ethernet

- DSCP is still marked but CoS will be required and used in Nexus Data Center designs

<table>
<thead>
<tr>
<th>PCP/COS</th>
<th>Network priority</th>
<th>Acronym</th>
<th>Traffic characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 (lowest)</td>
<td>BK</td>
<td>Background</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>BE</td>
<td>Best Effort</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>EE</td>
<td>Excellent Effort</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>CA</td>
<td>Critical Applications</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>VI</td>
<td>Video, &lt; 100 ms latency</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>VO</td>
<td>Voice, &lt; 10 ms latency</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>IC</td>
<td>Internetwork Control</td>
</tr>
</tbody>
</table>

IEEE 802.1Q-2005
Data Center Bridging Control Protocol
DCBX Overview - 802.1Qaz

- Negotiates Ethernet capability’s: PFC, ETS, CoS values between DCB capable peer devices
- Simplifies Management: allows for configuration and distribution of parameters from one node to another
- Responsible for Logical Link Up/Down signaling of Ethernet and Fibre Channel
- DCBX is LLDP with new TLV fields
- The original pre-standard CIN (Cisco, Intel, Nuova) DCBX utilized additional TLV’s
- DCBX negotiation failures result in:
  - per-priority-pause not enabled on CoS values
  - vfc not coming up – when DCBX is being used in FCoE environment


dc11-5020-3# sh lldp dcbx interface eth 1/40
Local DCBXP Control information:
Operation version: 00  Max version: 00  Seq no: 7  Ack no: 0
Type/ Subtype  Version  En/Will/Adv Config
006/000  000  Y/N/Y  00
<snip>
Priority Flow Control

FCoE Flow Control Mechanism – 802.1Qbb

- Enables lossless Ethernet using PAUSE based on a COS as defined in 802.1p
- When link is congested, CoS assigned to “no-drop” will be PAUSED
- Other traffic assigned to other CoS values will continue to transmit and rely on upper layer protocols for retransmission
- Not only for FCoE traffic

---

Diagram:

- Transmit Queues
  - Fibre Channel
  - B2B Credits

- Ethernet Link
  - One
  - Two
  - Three
  - Four
  - Five
  - Six
  - Seven
  - Eight

- Receive Buffers
  - One
  - Two
  - Three
  - Four
  - Five
  - Six
  - Seven
  - Eight

- Eight Virtual Lanes

- PAUSE
  - STOP

---

B2B Credits

---

Enables lossless Ethernet using PAUSE based on a COS as defined in 802.1p.
Enhanced Transmission Selection (ETS)
Bandwidth Management – 802.1Qaz

- Prevents a single traffic class of “hogging” all the bandwidth and starving other classes
- When a given load doesn’t fully utilize its allocated bandwidth, it is available to other classes
- Helps accommodate for classes of a “bursty” nature

![Diagram of Offered Traffic and 10 GE Link Realized Traffic Utilization](image-url)
Nexus QoS
QoS Policy Types

- There are three QoS policy types used to define system behavior (qos, queuing, network-qos)
- There are three policy attachment points to apply these policies to
  - Ingress interface
  - System as a whole (defines global behavior)
  - Egress interface

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Function</th>
<th>Attach Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
<td>Define traffic classification rules</td>
<td>system qos ingress Interface</td>
</tr>
<tr>
<td>queuing</td>
<td>Strict Priority queue</td>
<td>system qos egress Interface</td>
</tr>
<tr>
<td></td>
<td>Deficit Weight Round Robin</td>
<td>ingress Interface</td>
</tr>
<tr>
<td>network-qos</td>
<td>System class characteristics (drop or no-drop, MTU), Buffer size, Marking</td>
<td>system qos</td>
</tr>
</tbody>
</table>
Configuring QoS on the Nexus 5500
Create New System Class

Step 1 Define qos Class-Map

N5k(config)# ip access-list acl-1
N5k(config-acl)# permit ip 100.1.1.0/24 any
N5k(config-acl)# exit
N5k(config)# ip access-list acl-2
N5k(config-acl)# permit ip 200.1.1.0/24 any
N5k(config)# class-map type qos class-1
N5k(config-cmap-qos)# match access-group name acl-1
N5k(config-cmap-qos)# class-map type qos class-2
N5k(config-cmap-qos)# match access-group name acl-2
N5k(config-cmap-qos)#

Step 2 Define qos Policy-Map

N5k(config)# policy-map type qos policy-qos
N5k(config-pmap-qos)# class type qos class-1
N5k(config-pmap-c-qos)# set qos-group 2
N5k(config-pmap-c-qos)# class type qos class-2
N5k(config-pmap-c-qos)# set qos-group 3

Step 3 Apply qos Policy-Map under “system qos” or interface

N5k(config)# system qos
N5k(config-sys-qos)# service-policy type qos input policy-qos

N5k(config)# interface e1/1-10
N5k(config-sys-qos)# service-policy type qos input policy-qos

- Create two system classes for traffic with different source address range
- Supported matching criteria
  N5k(config)# class-map type qos class-1
  N5k(config-cmap-qos)# match access-group Access group
cos  IEEE 802.1Q class of service
dscp  DSCP in IP(v4) and IPv6 packets
ip    IP
precedence  Precedence in IP(v4) and IPv6 packets
protocol  Protocol
N5k(config-cmap-qos)# match

- Qos-group range for user-configured system class is 2-5
- Policy under system qos applied to all interfaces
- Policy under interface is preferred if same type of policy is applied under both system qos and interface
Configuring QoS on the Nexus 5500

Create New System Class (Continue)

Step 4 Define network-qos Class-Map

N5k(config)# class-map type network-qos class-1
N5k(config-cmap-nq)# match qos-group 2
N5k(config-cmap-nq)# class-map type network-qos class-2
N5k(config-cmap-nq)# match qos-group 3

- Match qos-group is the only option for network-qos class-map
- Qos-group value is set by qos policy-map in previous slide

Step 5 Define network-qos Policy-Map

N5k(config)# policy-map type network-qos policy-nq
N5k(config-pmap-nq)# class type network-qos class-1
N5k(config-pmap-nq-c)# class type network-qos class-2

- No action tied to this class indicates default network-qos parameters.
- Policy-map type network-qos will be used to configure no-drop class, MTU, ingress buffer size and 802.1p marking
- Default network-qos parameters are listed in the table below

Step 6 Apply network-qos policy-map under system qos context

N5k(config-pmap-nq-c)# system qos
N5k(config-sys-qos)# service-policy type network-qos policy-nq
N5k(config-sys-qos)#

- Match qos-group is the only option for network-qos class-map
- Qos-group value is set by qos policy-map in previous slide

Default network-qos parameters are listed in the table below

<table>
<thead>
<tr>
<th>Network-QoS Parameters</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Type</td>
<td>Drop class</td>
</tr>
<tr>
<td>MTU</td>
<td>1538</td>
</tr>
<tr>
<td>Ingress Buffer Size</td>
<td>20.4KB</td>
</tr>
<tr>
<td>Marking</td>
<td>No marking</td>
</tr>
</tbody>
</table>
Configuring QoS on the Nexus 5500
Strict Priority and Bandwidth Sharing

- Create new system class by using policy-map qos and network-qos (Previous two slides)
- Then Define and apply policy-map type queuing to configure strict priority and bandwidth sharing
- Checking the queuing or bandwidth allocating with command show queuing interface

N5k(config)# class-map type queuing class-1
N5k(config-cmap-que)# match qos-group 2
N5k(config-cmap-que)# class-map type queuing class-2
N5k(config-cmap-que)# match qos-group 3
N5k(config-cmap-que)# exit

N5k(config)# policy-map type queuing policy-BW
N5k(config-pmap-que)# class type queuing class-1
N5k(config-pmap-que-c-que)# priority
N5k(config-pmap-que-c-que)# class type queuing class-2
N5k(config-pmap-que-c-que)# bandwidth percent 40
N5k(config-pmap-que-c-que)# class type queuing class-fcoe
N5k(config-pmap-que-c-que)# bandwidth percent 40
N5k(config-pmap-que-c-que)# class type queuing class-default
N5k(config-pmap-que-c-que)# bandwidth percent 20

N5k(config-pmap-que-c-que)# system qos
N5k(config-sys-qos)# service-policy type queuing output policy-BW
N5k(config-sys-qos)#
Priority Flow Control – Nexus 5000/5500
Operations Configuration – Switch Level

- On Nexus 5000 once **feature fcoe** is configured, 2 classes are made by default

  ```
  policy-map type qos default-in-policy
  class type qos class-fcoe
  set qos-group 1
  class type qos class-default
  set qos-group 0
  ```

- **class-fcoe** is configured to be **no-drop** with an MTU of 2158

  ```
  policy-map type network-qos default-nq-policy
  class type network-qos class-fcoe
  pause no-drop
  mtu 2158
  ```

Enabling the FCoE feature on Nexus 5548/96 does ‘**not**’ create no-drop policies automatically as on Nexus 5010/20

Must add policies under system QOS:

```
system qos
service-policy type qos input fcoe-default-in-policy
service-policy type queuing input fcoe-default-in-policy
service-policy type queuing output fcoe-default-out-policy
service-policy type network-qos fcoe-default-nq-policy
```
Enhanced Transmission Selection - N5K
Bandwidth Management

- When configuring FCoE by default, each class is given 50% of the available bandwidth

- Can be changed through QoS settings when higher demands for certain traffic exist (i.e. HPC traffic, more Ethernet NICs)

N5k-1# show queuing interface ethernet 1/18
Ethernet1/18 queuing information:
  TX Queuing
    qos-group sched-type oper-bandwidth
      0  WRR  50
      1  WRR  50

- Best Practice: Tune FCoE queue to provide equivalent capacity to the HBA that would have been used (1G, 2G, …)
Priority Flow Control – Nexus 7K & MDS
Operations Configuration – Switch Level

N7K-50(config)# system qos
N7K-50(config-sys-qos)# service-policy type network-qos default-nq-7e-policy

- No-Drop PFC w/ MTU 2K set for Fibre Channel

show policy-map system
Type network-qos policy-maps
==================================================================================================
policy-map type network-qos default-nq-7e-policy
class type network-qos c-nq-7e-drop
   match cos 0-2,4-7
   congestion-control tail-drop
   mtu 1500
   class type network-qos c-nq-7e-ndrop-fcoe
       match cos 3
       match protocol fcoe
       pause
       mtu 2112

show class-map type network-qos c-nq-7e-ndrop-fcoe
Type network-qos class-maps
==================================================================================================
class-map type network-qos match-any c-nq-7e-ndrop-fcoe
   Description: 7E No-Drop FCoE CoS map
   match cos 3
   match protocol fcoe

Policy Template choices

<table>
<thead>
<tr>
<th>Template</th>
<th>Drop CoS (Priority)</th>
<th>NoDrop CoS (Priority)</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-nq-8e-policy</td>
<td>0,1,2,3,4,5,6,7</td>
<td>5,6,7</td>
</tr>
<tr>
<td>default-nq-7e-policy</td>
<td>0,1,2,4,5,6,7</td>
<td>5,6,7</td>
</tr>
<tr>
<td>default-nq-6e-policy</td>
<td>0,1,2,5,6,7</td>
<td>5,6,7</td>
</tr>
<tr>
<td>default-nq-4e-policy</td>
<td>0,5,6,7</td>
<td>5,6,7</td>
</tr>
</tbody>
</table>
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
FCoE Edge
N-Port Virtualizer (NPV)

- N-Port Virtualizer (NPV) utilizes NPIV functionality to allow a “switch” to act like a server performing multiple logins through a single physical link

- Physical servers connected to the NPV switch login to the upstream NPIV core switch
  - Physical uplink from NPV switch to FC NPIV core switch does actual “FLOGI”
  - Subsequent logins are converted (proxy) to “FDISC” to login to upstream FC switch

- No local switching is done on an FC switch in NPV mode

- FC edge switch in NPV mode does not take up a domain ID
Unified Fabric Design
The FCoE VLAN

- Each FCoE VLAN and VSAN count as a VLAN HW resource – therefore a VLAN/VSAN mapping accounts for TWO VLAN resources
- FCoE VLANs are treated differently than native Ethernet VLANs: no flooding, broadcast, MAC learning, etc.
- **BEST PRACTICE**: use different FCoE VLANs/VSANs for SAN A and SAN B
- The FCoE VLAN must not be configured as a native VLAN
- Shared Wires connecting to HOSTS must be configured as trunk ports and STP edge ports
- **Note**: STP does not run on FCoE vlans between FCFs (VE_Ports) but does run on FCoE VLANs towards the host (VF_Ports)

```
! VLAN 20 is dedicated for VSAN 2 FCoE traffic
(config)# vlan 20
(config-vlan)# fcoe vsan 2
```
Unified Fabric Design
F_Port Trunking and Channeling

- With NX-OS release 4.2(1) Nexus 5000 supports F-Port Trunking and Channeling
- VSAN Trunking and Port-Channel on the links between an NPV device and upstream FC switch (NP port -> F port)
- F_Port Trunking: Better multiplexing of traffic using shared links (multiple VSANs on a common link)
- F_Port Channeling: Better resiliency between NPV edge and Director Core (avoids tearing down all FLOGIs on a failing link)
- Simplifies FC topology (single uplink from NPV device to FC director)
Fabric Extender - FEX
Unified Fabric and FCoE

- Nexus 5000 access switches operating in NPV mode
- With NX-OS release 4.2(1) Nexus 5000 supports F-Port Trunking and Channeling on the links between an NPV device and upstream FC switch (NP port -> F port)
- F_Port Trunking: Better multiplexing of traffic using shared links (multiple VSANs on a common link)
- F_Port Channeling: Better resiliency between NPV edge and Director Core
  - No host re-login needed per link failure
  - No FSPF recalculation due to link failure
- Simplifies FC topology (single uplink from NPV device to FC director)
Unified Fabric Design
FCoE and vPC together

- vPC with FCoE are ONLY supported between hosts and N5k or N5k/2232 pairs...AND they must follow specific rules
  - A ‘vfc’ interface can only be associated with a single-port port-channel
  - While the port-channel configurations are the same on N5K-1 and N5K-2, the FCoE VLANs are different

- FCoE VLANs are ‘not’ carried on the vPC peer-link (automatically pruned)
  - FCoE and FIP ethertypes are ‘not’ forwarded over the vPC peer link either

- vPC carrying FCoE between two FCF’s is NOT supported

- Best Practice: Use static port channel configuration rather than LACP with vPC and Boot from SAN (this will change with future releases)
**EvPC & FEX**

**Nexus 5550 Topologies starting with NX-OS 5.1(3)N1**

- In an Enhanced vPC (EvPC) SAN ‘A/B’ isolation is configured by associating each FEX with either SAN ‘A’ or SAN ‘B’ Nexus 5500
- FCoE & FIP traffic is forwarded only over the links connected to the specific parent switch
- Ethernet is hashed over ‘all’ FEX fabric links
vPC & Boot from SAN
Pre 5.1(3)N1 Behaviour

- VFC1 is bound to port-channel 1
- Port-channel 1 is using LACP to negotiate with host
- The VFC/port-channel never comes up and the host isn’t able to boot from SAN
As of NX-OS Release 5.1(3)N1(1) for N5K, new VFC binding models will be supported

In this case, we now support VF_Port binding to a member port of a given port-channel

Check the configuration guide and operations guide for additional VFC binding changes
Transparent Bridges?
FIP Snooping

- What does a FIP Snooping device do?
  - FIP solicitations (VLAN Disc, FCF Disc and FLOGI) sent out from the CNA and FIP responses from the FCF are “snooped”

- How does a FIP Snooping device work?
  - The FIP Snooping device will be able to know which FCFs hosts are logged into
  - Will dynamically create an ACL to make sure that the host to FCF path is kept secure

- A FIP Snooping device has NO intelligence or impact on FCoE traffic/path selection/load balancing/login selection/etc

- Mentioned in the Annex of the FC-BB-5 (FCoE) standard as a way to provide security in FCoE environments

- Supported on Nexus 5000/5500 – 4.1(3)
- Supported on Nexus 7000 - 6.1(1) with F2, F1 cards
Fibre Channel Aware Device

FCoE NPV

- What does an FCoE-NPV device do?
  - "FCoE NPV bridge" improves over a "FIP snooping bridge" by intelligently proxying FIP functions between a CNA and an FCF

- Active Fibre Channel forwarding and security element
  - FCoE-NPV load balance logins from the CNAs evenly across the available FCF uplink ports
  - FCoE NPV will take VSAN into account when mapping or ‘pinning’ logins from a CNA to an FCF uplink

- Emulates existing Fibre Channel Topology (same mgmt, security, HA, …)

- Avoids Flooded Discovery and Configuration (FIP & RIPv)

NOTE: FCoE NPV does NOT convert server FLOGI to FDISC like FC NPV
FCoE-NPV configuration Details

Proper no drop QOS needs to be applied to all NPIV VDC's and NPV switches as shown in earlier slides.

LACP Port-channels can be configured between switches for High availability.
## FCoE NPV
### Edge Capabilities

<table>
<thead>
<tr>
<th>Benefits</th>
<th>DCB</th>
<th>FIP Snooping</th>
<th>FCoE NPV</th>
<th>FCoE Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability (Server connectivity)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Support for Lossless Ethernet</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>FCoE Traffic Engineering</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Security (Man in the middle attack)</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>FC to FCoE Migration (Ease of FCoE device migration from FC fabric to FCoE network)</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>FCoE Traffic Load Balancing</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SAN Administration (VSAN, VFC visibility for SAN Administration)</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
FCoE - Design, Operations and Management Best Practices

Agenda

- Unified Fabric – What and When
- FCoE Protocol Fundamentals
- Nexus FCoE Capabilities
- FCoE Network Requirements and Design Considerations
- DCB & QoS - Ethernet Enhancements
- Single Hop Design
- Multi-Hop Design
- Futures
FCoE Multi-Tier Fabric Design
Using VE_Ports

- With NX-OS 5.0(2)N2, VE_Ports are supported on/between the Nexus 5000 and Nexus 5500 Series Switches
- VE_Ports are run between switches acting as Fibre Channel Forwarders (FCFs)
- VE_Ports are bound to the underlying 10G infrastructure
  - VE_Ports can be bound to a single 10GE port
  - VE_Ports can be bound to a port-channel interface consisting of multiple 10GE links

All above switches are Nexus 5X00 Series acting as an FCF.
What happens when FCF’s are connected via VE_Ports

- 10Gig Ethernet ISL or LACP port-channel must first be established between FCF Switches expanding the L2 ethernet network
- LLDP frames with DCBx TLV’s, sourcing the MAC addresses of each switch are exchanged across the ethernet Link to determine abilities.
- FIP Control exchange is done between switches
- FSPF routing established
- Fibre Channel Protocol is exchanged between the FCF’s and a Fibre Channel merge of Zones is accomplished building out the FC SAN.
- You now have established a VE_Port between two DCB switches
Differences in Trunking VSANs with FCoE VE_Ports

- In FC on the MDS, trunking is used to carry multiple VSANs over the same physical FC link. With FCoE, a physical link is replaced by a virtual link, a pair of MAC addresses.

- FCoE uses assigned MAC addresses that are unique only in the context of a single FC fabric. Carrying multiple fabrics over a single VLAN would then mean having a strong possibility for duplicated MAC addresses.

- In FCoE there cannot be more than one VSAN mapped over a VLAN.
- The net result is that trunking is done at the Ethernet level, not at the FC level.

- FC trunking is not needed and the Fibre Channel Exchange Switch Capabilities (ESC) & Exchange Port Parameters (EPP) processing is not required to be performed as on the MDS.
FCoE Extension Options

Short Distance Options

- **Requirement:** Maintain loss-less behavior across the point-to-point link
- Supported distance is governed by the ingress buffer size available on the switch

<table>
<thead>
<tr>
<th>Speed (Gbps)</th>
<th>Max Distance (KM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8000</td>
</tr>
<tr>
<td>2</td>
<td>4000</td>
</tr>
<tr>
<td>4</td>
<td>2000</td>
</tr>
<tr>
<td>8</td>
<td>1000</td>
</tr>
<tr>
<td>10</td>
<td>680</td>
</tr>
</tbody>
</table>

1. Limited by supported Optics
Multi - Hop Design
Extending FCoE to MDS SAN from Aggregation

- **Converged Network into the existing SAN Core**
  - Leverage FCoE wires between Fibre Channel SAN to Ethernet DCB switches in Aggregation layer using Dedicated ports
  - Maintain the A – B SAN Topology with Storage VDC and Dedicated wires
  - Using N7K director Class Switches at Access layer
  - Dedicated FCoE Ports between access and Aggregation, vPC’s for Data
  - Zoning controlled by Core A-B SAN
Storage on MDS
Extending FCoE to MDS SAN from Access

- **Converged Network capabilities to the existing SAN Core**

  Leverage FCoE wires between Fibre Channel SAN to Ethernet DCB switches (VE_Ports)

  N5K access switches can be in Fibre Channel switch node and assigned Domain ID, or
  N5K access switches can run in FCoE-NPV mode, no FC services running local.
  Zoning controlled by Core A-B SAN
Migration of Storage to Aggregation

- Different requirements for LAN and SAN network designs
- Factors that will influence this use case
  - Port density
  - Operational roles and change management
  - Storage device types
- Potentially viable for smaller environments
- Larger environments will need dedicated FCoE ‘SAN’ devices providing target ports
  - Use connections to a SAN
  - Use a “storage” edge of other FCoE/DCB capable devices
Data Center Network Manager

One converged product
- Single pane of glass (web 2.0 dashboard)
- Can be licensed for SAN and/or LAN.
- Common operations (discovery, topology)
- Single installer, Role based access control
- Consistent licensing model (licenses on server)
- Integration with UCS Manager and other OSS tools
LAN/SAN Roles

Data Center Network Manager

- Collaborative management
- Defined roles & functions
- FCoE Wizards

<table>
<thead>
<tr>
<th>Nexus 7000</th>
<th>Tasks</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Admin</td>
<td>Storage VDC provisioning VLAN management Ethernet config (L2, network security, VPC, QoS, etc. DCB Configuration (VL, PFC, ETS Templates)</td>
<td>DCNM-LAN</td>
</tr>
<tr>
<td>SAN Admin</td>
<td>Discovery of Storage VDCs VLAN- VSAN mapping (use reserved pool) Wizard vFC provisioning Wizard Zoning</td>
<td>DCNM-SAN</td>
</tr>
</tbody>
</table>
Recommended Reading
Q&A
We value your feedback.
Please be sure to complete the Evaluation Form for this session.

Access today’s presentations at cisco.com/ca/plus

Follow @CiscoCanada and join the #CiscoPlusCA conversation