

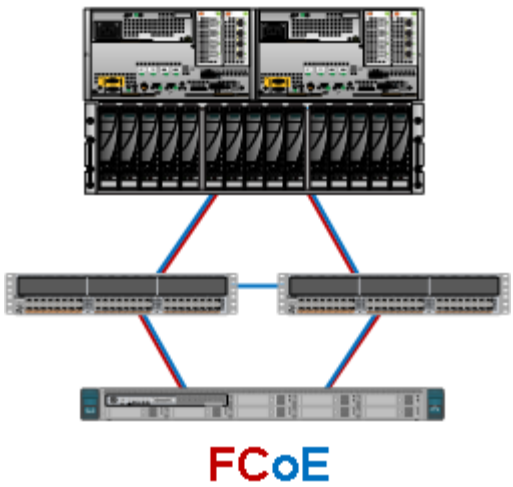
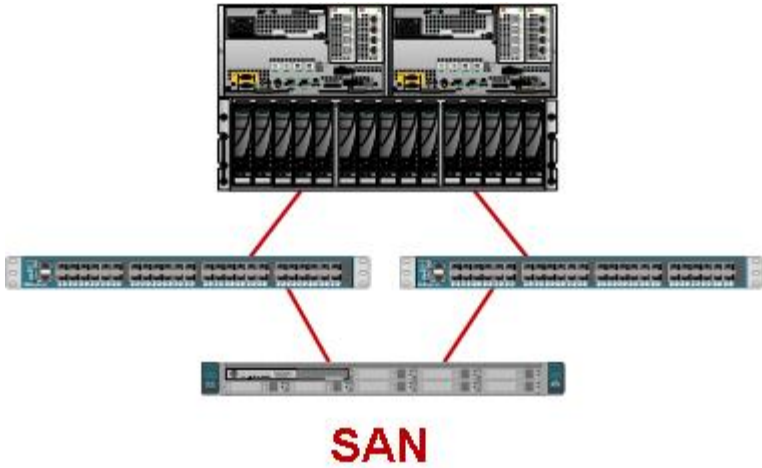
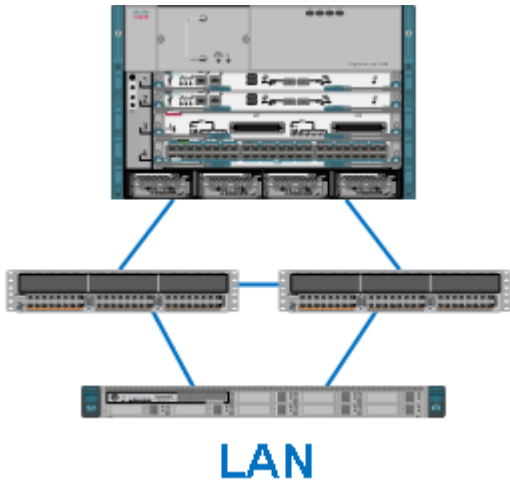
# What You Make Possible



# Operational Models for FCoE Deployments - Best Practices and Examples

BRKSAN-2282

# How Does This Apply?



# Session Objectives

## Why Are We Here?

- Review the business drivers and common challenges
- Share best practices, case studies, and configuration examples
- Help you determine the FCoE operational model for your organisation

# This Session is NOT

- An FCoE primer
  - See BRKDCT-1044 - FCoE for the IP Network Engineer
  - See BRKSAN-2047 - FCoE - Design, Implementation, and Management Best Practices
  - LTRCRT-5206 - Configuring Nexus 5000 Fibre Channel over Ethernet (FCoE) Lab
- A review of all possible FCoE deployment models

# Agenda

- Business drivers and FCoE recap
- Challenges for FCoE adoption
- Case studies
- Management of the Unified Fabric

# Business Drivers



# Why Should I Be Interested in FCoE?

If It Ain't Broke, Don't Fix It ...

- Storage Team happy with Fibre Channel
- LAN team not familiar with FC technology
- Storage Area Networks (SAN) are deterministic and highly available

**However... What are the key trends in the Data Centre?**

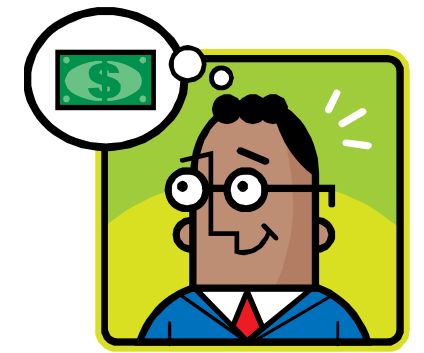
- The need to optimise... **EVERYTHING** (cost, power, cooling, space...)
- IT as business enabler – Increase Agility
- Server Virtualisation & Workload Mobility
- 10 Gigabit Ethernet to the Server – Enables Consolidation
- Investment Protection – Preparing for the future





# The Need to Optimise... EVERYTHING

Cost, Power, Cooling and Space Reduction




## TCO Comparison

- 5-years
- PUE 2.5
- Cost of power per kWhr \$0.20
- 500 Servers
- Annual growth rate of servers 10%

	Unconsolidated	Unified Fabric
Server Connections	3,000 1GE LAN 1,000 FC	1000 Converged <b>75% Reduction</b>
Access/Edge Switches	12 x Cat6509 2 x MDS 9513	4 x Nexus 7018 <b>71% Reduction</b>
CAPEX - 1 <sup>st</sup> year (NIC, HBA, LAN, SAN, Cabling, CNA)	\$11,940,105.00	\$5,966,825.00 <b>50% Savings</b>
Hardware Maintenance (5 years)		\$3,568,513.00 <b>Savings</b>
Power and Cooling (5 years)		\$904,592.00 <b>Savings</b>


# End-to-End Unified Fabric TCO Calculator

Compare the cost of a converged network to the cost of an unconsolidated



## End-to-End Unified Fabric TCO Comparison Tool

Welcome to the **Cisco End-to-End Unified Fabric TCO Tool**. This tool will help you demonstrate financial justification for a unified fabric networking solution by modeling a comparison between the total cost of ownership of a greenfield unconsolidated network architecture consisting of separate LAN and SAN infrastructures and a unified fabric network architecture, consisting of a converged 10 GbE/FCoE access layer and, optionally, a unified core layer network infrastructure.



We welcome you to use this tool to evaluate the impact of unified fabric on your data center and encourage you to contact your Cisco representative for further information.

Learn more about the value proposition for Cisco Unified Fabric from this IDC whitepaper: [Benefits of Unified Fabric Beyond the Access Layer](#).

The logic and assumptions in this tool have been [validated by IDC](#).

To configure an analysis enter the required information and click **Continue**.

### Access Layer Architecture

Please choose whether you prefer a fixed port, top-of-rack Access layer switch architecture or a modular port Access layer architecture (typically end-of-row or middle-of-row).

Modular Port Access Layer Switches

Fixed Port Access Layer Switched

[Home](#) [Continue](#)

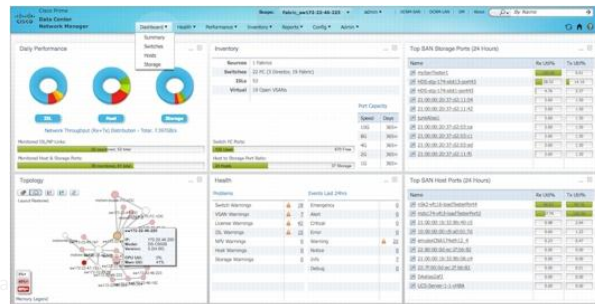
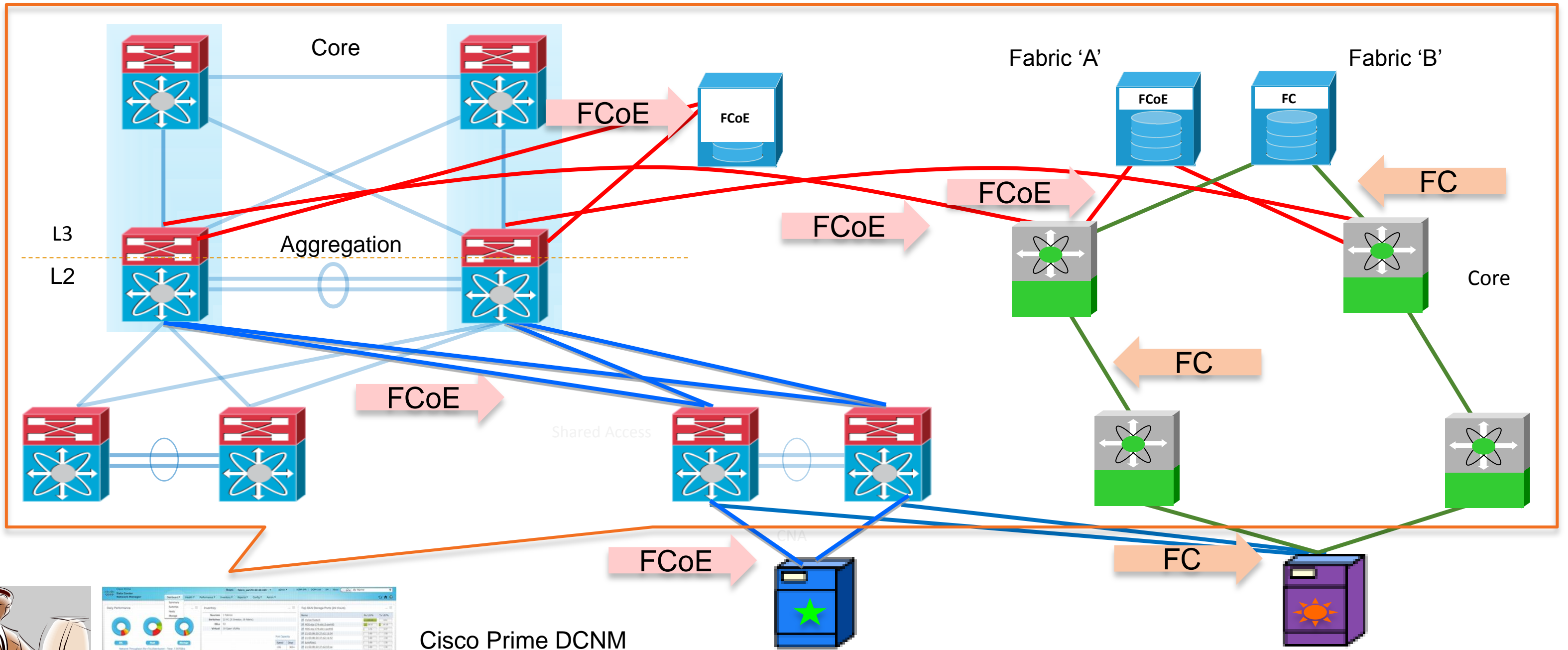


**For Your Reference**

<https://express.salire.com/go/cisco/end-to-end-unified-fabric-tco-comparison-tool.aspx>

# Incremental Deployment

Evolution, preserve existing knowledge and investment on FC



Cisco Prime DCNM

# Recap of FCoE Technology



# Converged Network Adapters

Host Bus Adapter (HBA) + Network Interface Controller (NIC)



First Generation  
Mid-2008

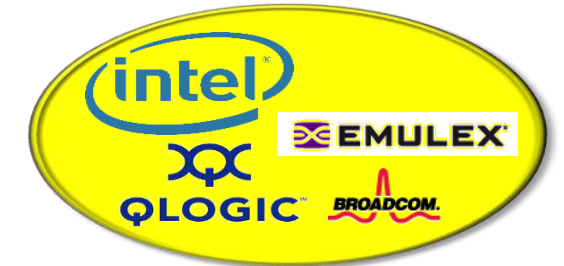
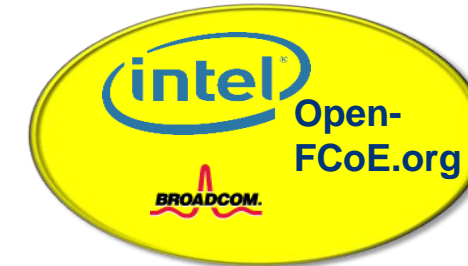
Second Generation  
Mid-2009

Third Generation  
2010

Fourth Generation  
Mid-2012

Standard 10GE  
FCoE in Software

mLoM CNA, CNAoM and  
10GE LoM+OpenFCoE



- Multiple components
- Full height/length
- Higher power consumption

- Single chip
- Half height/length
- Less than half the power
- Same support as HBAs

- Next-gen Single chip
- Less power consumption
- Same support as HBAs
- Increased IOPS

- Next-gen Single chip
- Less power consumption
- Same support as HBAs
- More than 1 million FCoE IOPS

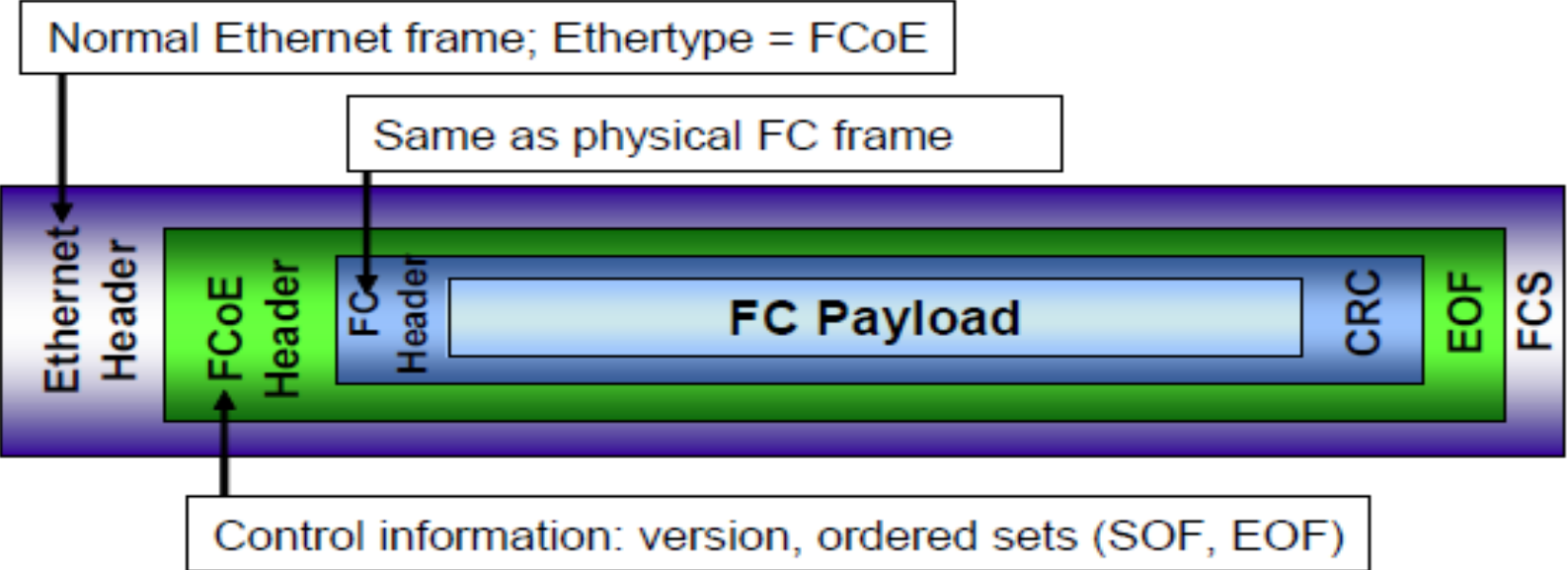
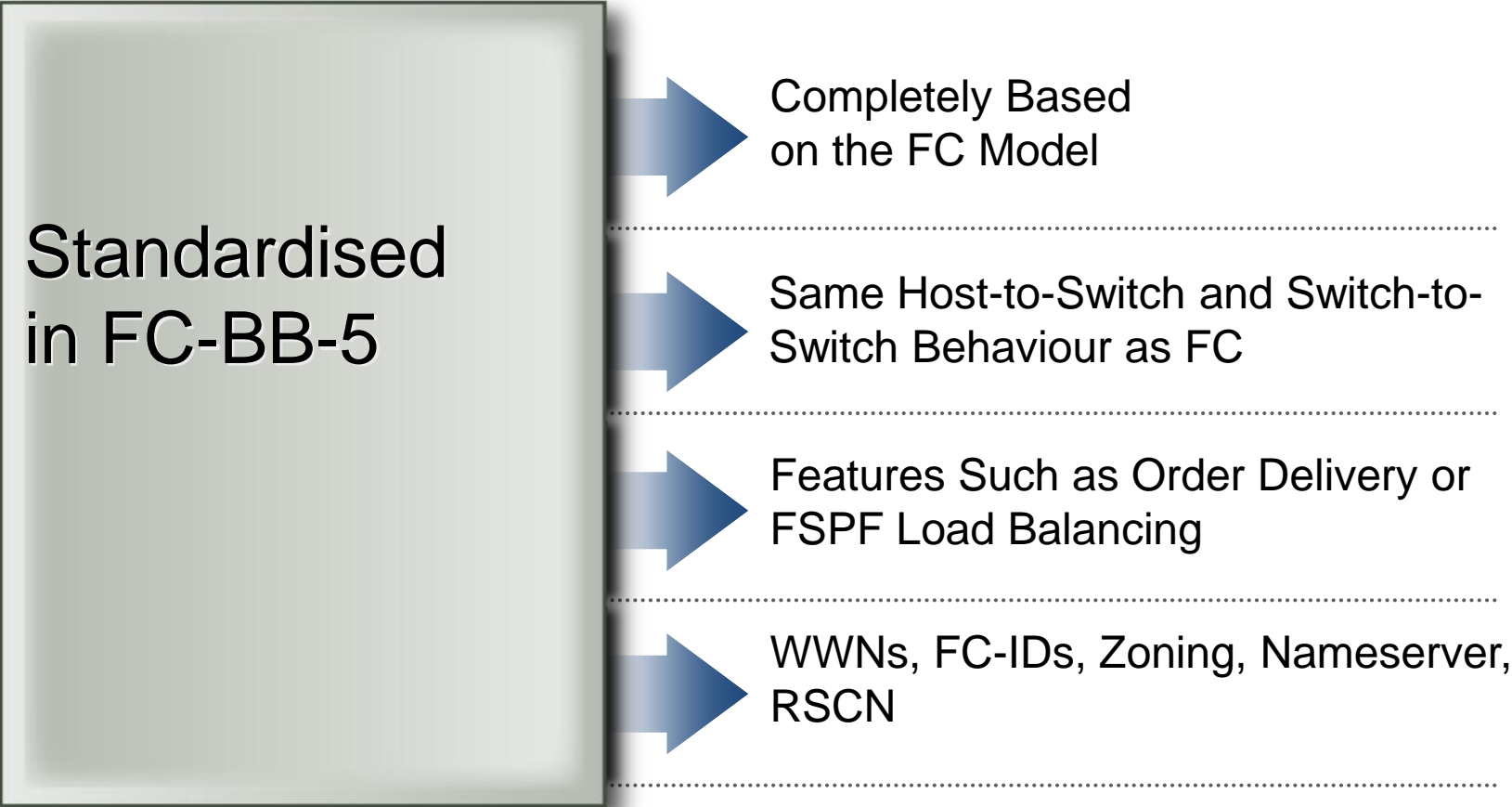
- Brings the economy of scale of Ethernet to SAN
- Native FCoE initiators in OS
- Windows, Linux and vSphere 5
- FREE

- Every Server is now 10GE enabled
- FCoE is a software license or runs for free

All Server Vendors (IBM, HP, Cisco, Dell) have certified CNAs and some have CNAoM. Check the connectivity options for your CNA, they may vary - Twinax Active/Passive and SFP+.

# What is FCoE?

It's Fibre Channel



### FCoE

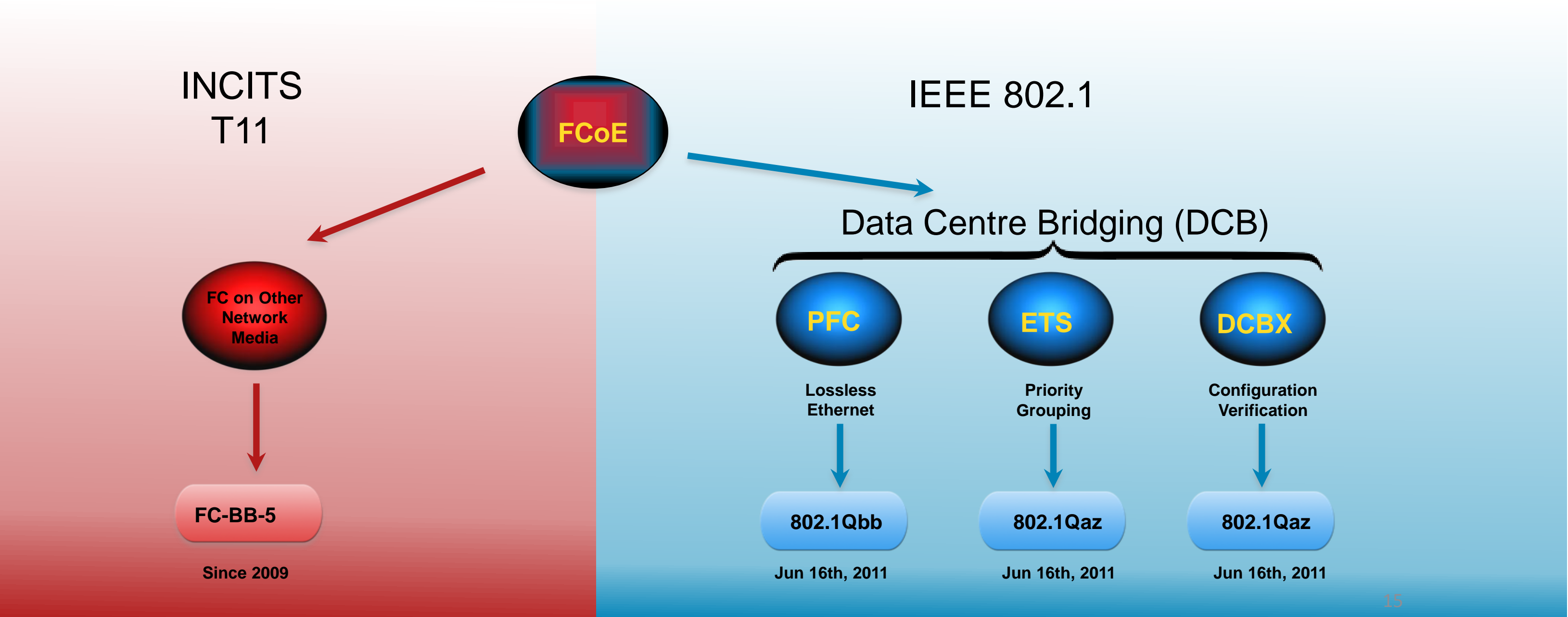
- Mapping of FC Frames over Ethernet
- Enables FC to Run on a Lossless Ethernet Network

The diagram shows a large blue cylinder representing an Ethernet network. Inside it, a smaller orange cylinder represents Fibre Channel traffic. Arrows point from the labels 'Ethernet' and 'Fibre Channel Traffic' to their respective cylinders.

# Standards for FCoE

All relevant standards are complete

- FCoE is fully defined in FC-BB-5 standard



# LAN and SAN Team Intersection with FCoE

## LAN Team

VLANs, QoS, Routing

GE, 10GE, LOM

Single Fabric High Availability

Network Isolation and Security

Modular, Top of Rack

CLI, SNMP Based Tools

## SAN Team

VSANs, Zoning, I/O Performance

Dedicated HBAs

Dual Fabrics

Storage Virtualisation

Director, Fabric Edge

Vendor Specific Management Tools

Host Adapter  
Network Switch  
Change Control  
Troubleshooting



# Top 5 Challenges in FCoE Deployments

## ■ Organisation Structure

- ❌ SAN and LAN Teams not under same management until Director level
- ❌ Budget may come from different departments
- ❌ Two groups that had never spoken before except in rare cases
- ✓ Usually no push back from server team as they see HBA and Ethernet ports
- ✓ Both teams should be part of testing
- ✓ LAN Team is adopting Nexus, the foundation exists
- ✓ FCoE License/Storage License much cheaper than isolated Hardware

# Top 5 Challenges in FCoE Deployments

- Education for both LAN and SAN Teams
  - ❌ Education in general is a challenge
  - ✓ Provide training building on existing knowledge
    - ✓ Great Example: FCoE for the IP Network Engineer (BRKDCT-1044)
- Insertion point
  - ❌ Retrofit an existing installation
  - ✓ Usually happens as part of a refresh, migration or upgrade activity
  - ✓ New servers or applications will be added into a new or existing Data Centre
  - ✓ Baseline current FC bandwidth consumption

# Top 5 Challenges in FCoE Deployments

- Who maintains the converged network devices?
  - ❌ In particular Software / Firmware Upgrades
    - ✓ Nexus 5000 using NPV = Dependency upon fewer FCFs
    - ✓ Both Teams need to discuss together, change control process must be agreed:
      - Example: LAN team request the upgrade based upon their requirements for more features
      - SAN team would be given sufficient notice and time to:
        - Review any open caveats and bugs
        - Verify code version on Interoperability matrixes
        - “**Veto**” the upgrade if there were issues that would impact the SAN

# Top 5 Challenges in FCoE Deployments

- How does FCoE affect troubleshooting procedures?
  - ❌ Different support teams
  - ❌ LAN and SAN Team may utilise different tools
  - ✓ Utilise tools that are aligned with Converged Networks – DCNM
  - ✓ Establish processes that facilitate the communication between teams
  - ✓ Evolve the roles and responsibilities of the support teams

# Case Study: Maximum Separation with Nexus 7000



# Max Separation in a Converged Environment

LAN and SAN operated by two different organisations

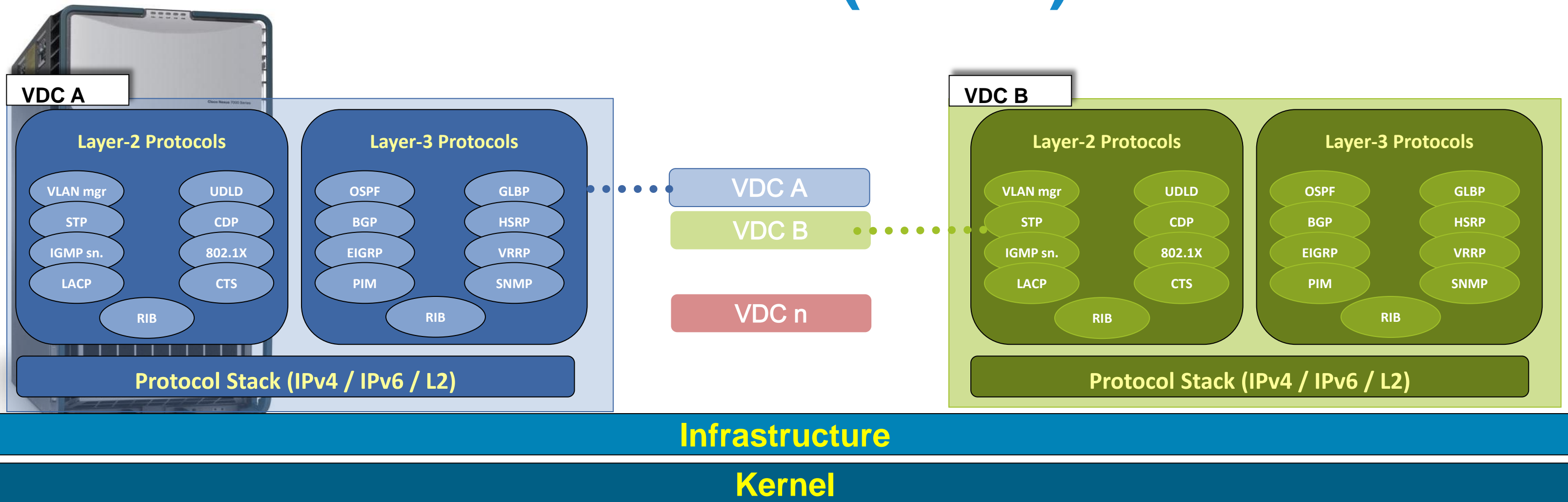
## Company A (Enterprise)

- Outsourced the LAN (IP) network to Company B
- Retained server and storage operations
- Concerned about Company B having access to data
- Concerned about Company B operations impacting Storage
- Have its own systems for Syslog, AAA, SNMP, NTP

## Company B (Service Provider)

- Concerned about Company A operations impacting LAN
- Have its own systems for Syslog, AAA, SNMP, NTP

# Virtual Device Contexts (VDCs)



## ■ VDC—Virtual Device Context

- Flexible separation/distribution of **Software Components**
- Flexible separation/distribution of **Hardware Resources**
- Securely delineated **Administrative Contexts**

## ■ VDCs are not...

- The ability to run different OS levels on the same box at the same time
- based on a **hypervisor** model; there is a single 'infrastructure' layer that handles h/w programming...

For your Reference see:  
BRKDCT-2121 - Virtual Device Context (VDC) Design and Implementation Considerations with Nexus 7000

# Admin VDC

Available on Supervisor 2/2E

Provides pure administrative context

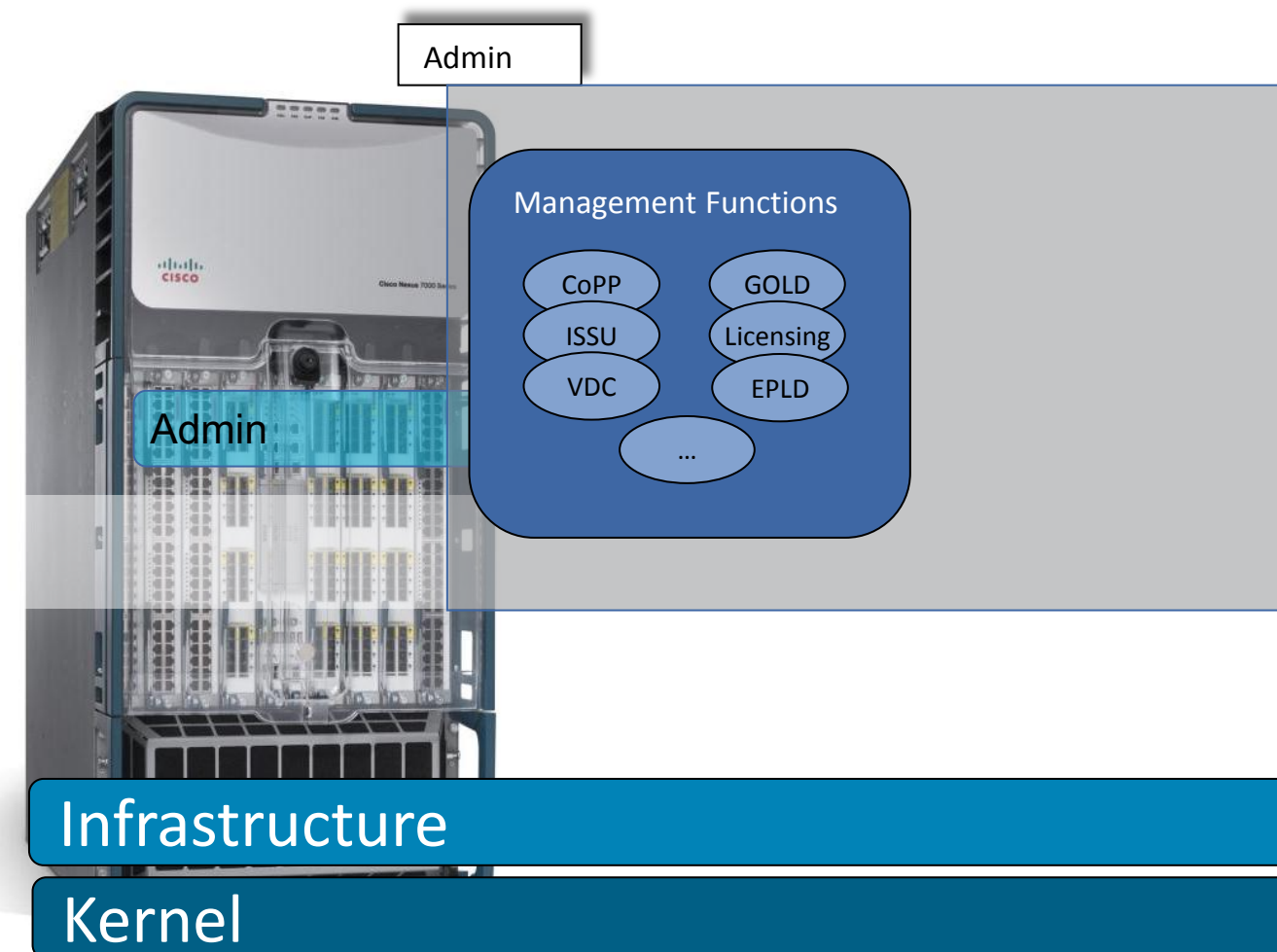
- CoPP configuration
- ISSU and EPLD
- VDC creation, suspension and deletion, interface allocation
- Show tech-support, tac-pac, debugs, GOLD Diagnostics
- System-wide QoS, Port Channel load-balancing

Simplify configuration for data plane VDCs

- No boot statements, CoPP policies, etc in non-Admin VDCs

Doesn't require Advanced or VDC License

- Can use 1 Admin VDC + 1 Data VDC (1+1)





# Storage VDC

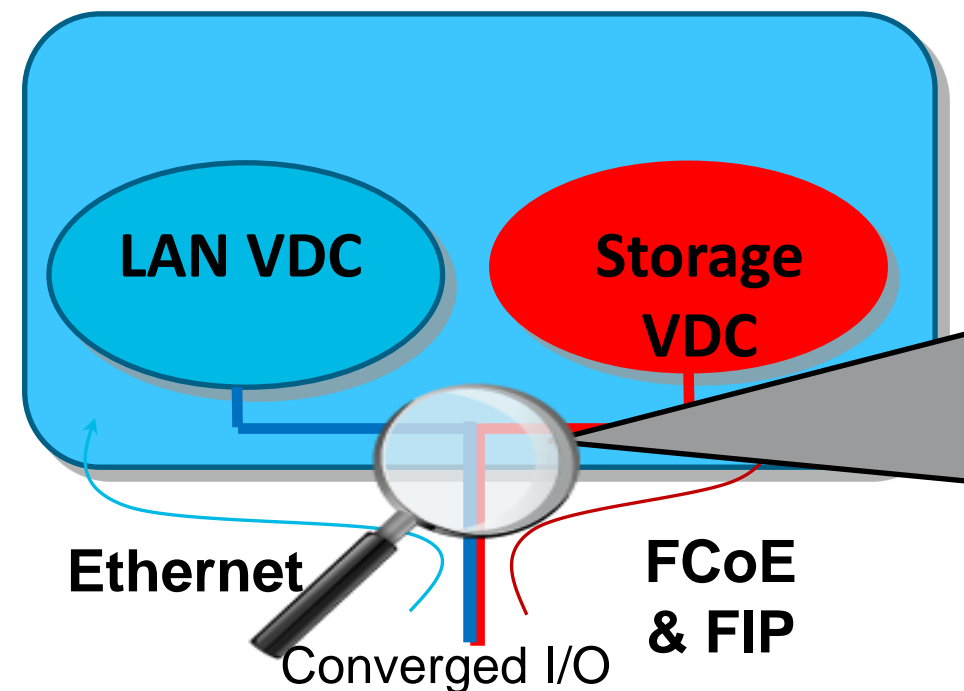
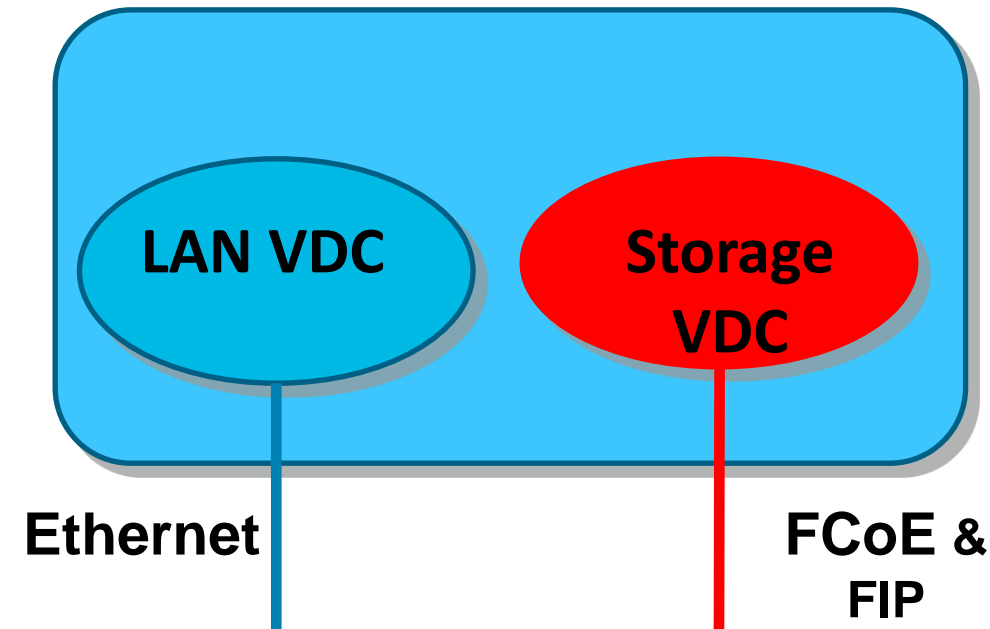
## Implementing FCoE on Nexus 7000

### Storage VDC

- Creates a “virtual” MDS within the Nexus 7000
- Only one such VDC can be created
- Does not require Advanced License (VDCs) and count towards total VDC count (4 with Sup1)

### Shared Interfaces

- Model for host interfaces, not ISLs
- FCoE traffic is processed in the context of the Storage VDC

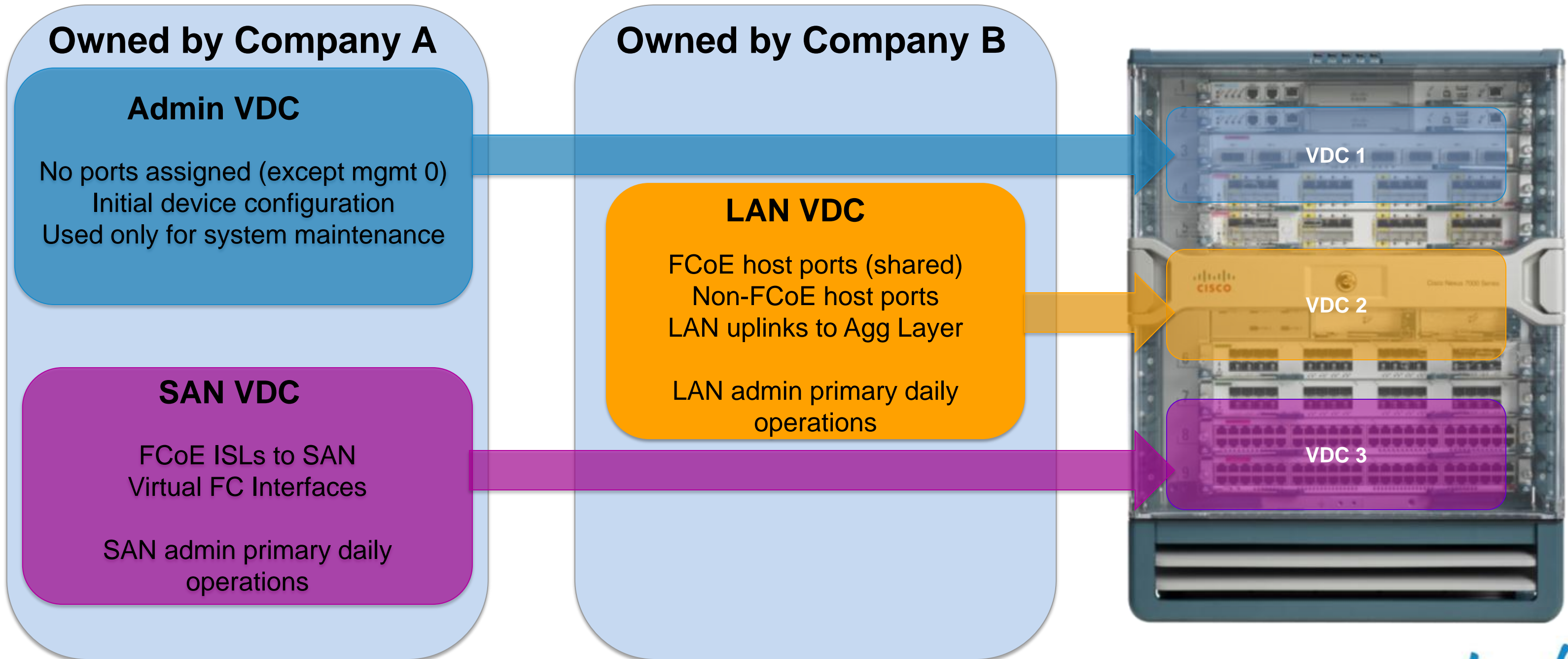


- Exception to the rule allowing an interface to exist in only one VDC
- Splits traffic based on Ethertype
- Ethernet VDC “owns” interface
- Storage VDC sees the interface as well

FCoE Initialisation Protocol (FIP) Ethertype 0x8914 and FCoE 0x8906 only are directed to the storage VDC. All other Ethertypes are directed toward the Ethernet VDC

# VDC Enables Sharing of the Physical Device

It allow us to solve Layer 8 issues...



# Role Based Access Control - RBAC

Limit access to operations on the device based on who you are

- Four default user roles
  - network-admin - Complete read-and-write access to the entire device (**only available in the admin/default VDC**)
  - network-operator - Complete read access to the entire device (only available in the admin/default VDC)
  - VDC-admin - Read-and-write access limited to a VDC
  - VDC-operator - Read access limited to a VDC
- You can create custom roles within a VDC
- VDCs on the same physical device do not share user roles

# Users and Roles

## Example of RBAC implementation



For Your Reference

VDC	Role	User	Description
Admin	network-admin (exist by default on Default VDC)	Example: A-ADMIN	Super User.  Used for initial configuration, software upgrades and VDC management (i.e. add more interfaces).
Admin	network-operator (exist by default on Default VDC)	Example: A-OPS	Read-only User, read access to all VDCs.  Not to be used.
Admin	vdc-admin (exist by default on All VDCs but it's independent from one VDC to the other)	Example: A-VDC-ADMIN	Admin Users for Default VDC.  They cannot take actions that impact the other VDCs.  Not able to switch to other VDCs, not able to reload the switch, not able to move interfaces between VDCs.

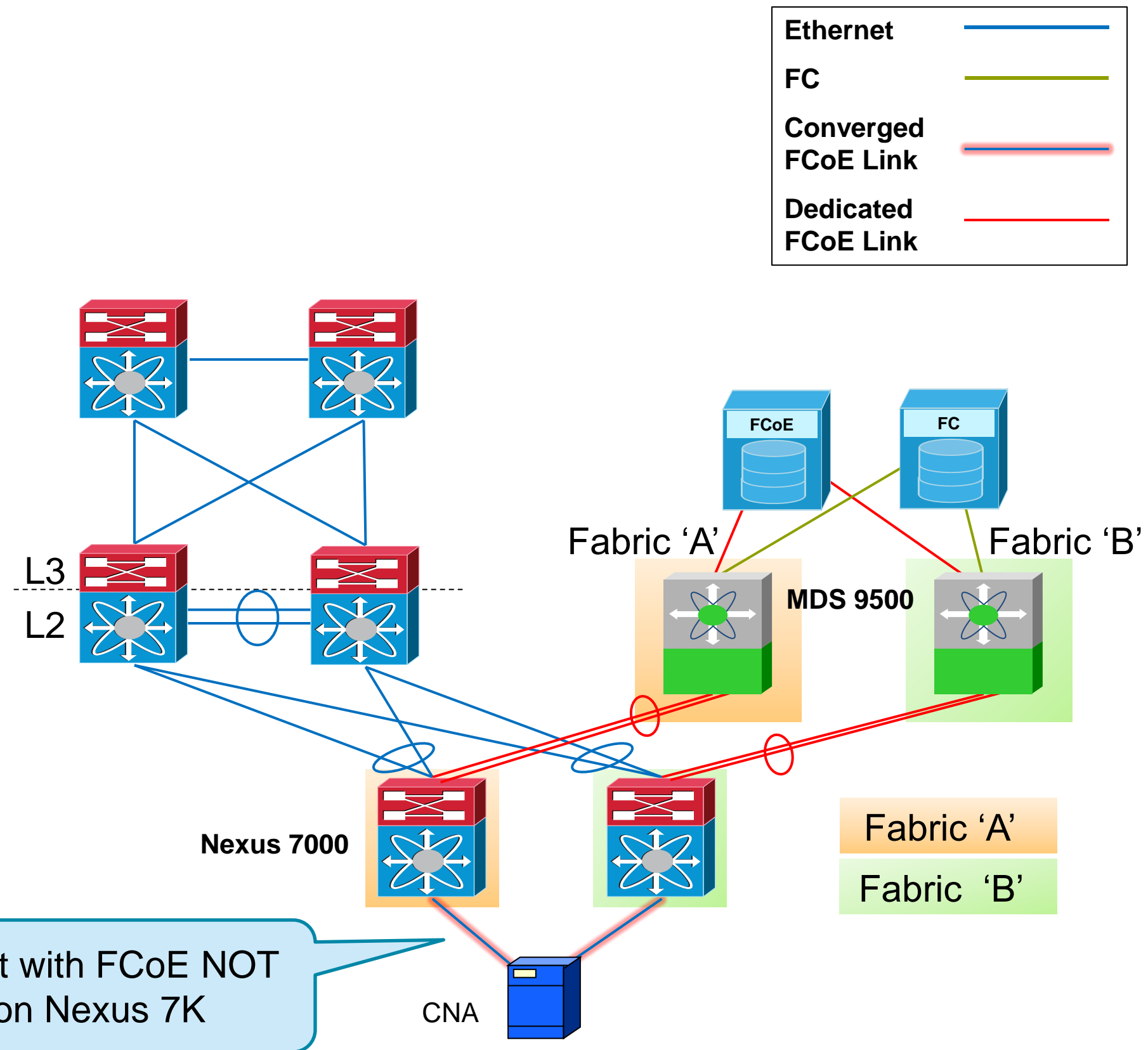
VDC	Role	User	Description
LAN	vdc-admin (exist by default on All VDCs but it's independent from one VDC to the other)	Example: B-LAN-ADMIN	LAN administrator. To be used by Company B to manage the LAN VDC, similar to user to manage a LAN Switch.  Users cannot take actions that impact the other VDCs.  Not able to switch to other VDCs, not able to reload the switch, but able to reload the LAN VDC (like a LAN Switch).
LAN	vdc-operator (exist by default on All VDCs but it's independent from one VDC to the other)	Example: B-LAN-OPS	LAN Operator. Read-only access limited to the VDC, can only read the parameters  Used by B for Level 1 teams
LAN	"Custom"		Allow flexibility to Company B for them to create Roles that match their existing operational models for LAN Switches.

VDC	Role	User	Description
SAN	vdc-admin (exist by default on All VDCs but it's independent from one VDC to the other)	Example: A-SAN-ADMIN	SAN Administrator. To be used by Company A to manage the SAN VDC, similar to user to manage a SAN Switch.  Users cannot take actions that impact the other VDCs.  Not able to switch to other VDCs, not able to reload the switch, but able to reload the SAN VDC (like a SAN Switch),
SAN	vdc-operator (exist by default on All VDCs but it's independent from one VDC to the other)	Example: A-SAN-OPS	SAN Operator. Read-only access limited to the VDC, can only read the parameters, not able to make any changes.  Used by A for Level 1 teams.
SAN	"Custom"		Allow flexibility to Company A for them to create Roles that match their existing operational models for SAN Switches.

# Converged Access

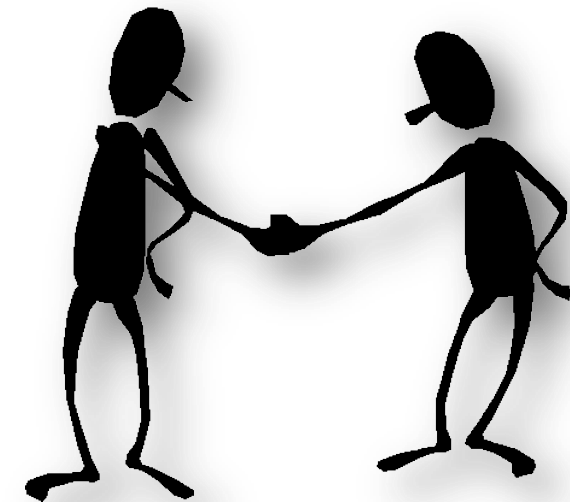
## Sharing Access Layer for LAN and SAN

- Shared Physical, Separate Logical LAN and SAN traffic at Access/Edge Layer
- Physical and Logical separation of LAN and SAN traffic at Aggregation/Core Layer
- Additional Physical and Logical separation of SAN fabrics
- Investment protection, Integrates into existing FC SAN



# Initial Configuration

What needs to be agreed before configuration?



- NX-OS Version to Run
- VDC Structure
  - Number for the VDC
  - Admin + Ethernet + Storage - 3 VDCs (Best Practice)
- The Host Facing Ports
- Bandwidth allocated to FCoE on the converged links
- The Uplink ports for LAN and SAN
- VLANs/VSANs/VFCs to be used for FCoE
  - Unique, dedicated VLAN for each VSAN
  - Best Practice: Reserve a range based upon the number of expected VSANs

# Initial Configuration

## Things to do in the Admin VDC



- 1) Install FCoE license
- 2) Install feature-set fcoe and associate the license with the F module
- 3) Enable feature lldp
- 4) Enable system QoS and policy for FCoE
- 5) Create a VDC for LAN and SAN (Storage)

```
7010-1(config)# VDC LAN
```

Note: Creating VDC, one moment please ...

```
7010-1(config)# VDC SAN type storage
```

```
7010-1(config-VDC)# limit-resource module-type f1
```

### Use the “where” command

```
7010-1(config-VDC)# where  
Conf;VDC LAN admin@7010-1%default
```

Helpful  
Tips

# Initial Configuration

Things to do in the LAN VDC



- 6) Enable feature lldp
- 7) Enable feature lacp



LACP is best practice for port-channels  
Don't forget to enable LLDP on all VDCs!



# Initial Configuration

Things to do in the Storage VDC



- 8) Enable feature lldp
- 9) Enable feature lacp



LACP is best practice for port-channels  
Don't forget to enable LLDP on all VDCs!

# Initial Configuration

## Things to do in the Admin VDC



- 1) Install FCoE license
- 2) Install feature-set fcoe and associate the license with the F module
- 3) Enable feature lldp
- 4) Enable system QoS and default policy for FCoE
- 5) Create a VDC for LAN and SAN (Storage)
- 10) Allocate host interfaces to LAN VDC
  - Host Facing Ports are allocated to LAN VDC
- 11) Allocate interfaces for uplink to SAN and LAN VDC
  - Ports used for uplinks for FCoE ISL (SAN VDC)
  - Ports used for uplinks towards LAN Aggregation Layer (LAN VDC)

### Use the “where” command

```
7010-1(config-VDC)# where  
Conf;VDC LAN admin@7010-1%admin
```

Helpful  
Tips

# Initial Configuration

## Things to do in the LAN VDC



- 6) Enable feature lldp
- 7) Enable feature lacp



LACP is best practice for port-channels  
Don't forget to enable LLDP on all VDCs!



### 12) Configure host ports within the LAN VDC

```
7010-1-LAN(config)# interface Ethernet 7/19-22
7010-1-LAN(config-if-range)# switchport
7010-1-LAN(config-if-range)# switchport mode trunk
7010-1-LAN(config-if-range)# switch trunk allowed vlan 1,10-20
7010-1-LAN(config-if-range)# spanning-tree port type edge trunk
```

# Initial Configuration

## Things to do in the Admin VDC



- 1) Install FCoE license
- 2) Install feature-set fcoe and associate the license with the F module
- 3) Enable feature lldp
- 4) Enable system QoS and default policy for FCoE
- 5) Create a VDC for LAN and SAN (Storage)
- 10) Allocate interfaces to LAN VDC
  - Host Facing Ports are allocated to LAN VDC
- 11) Allocate interfaces to SAN VDC
  - Ports used for uplinks into the SAN fabrics (ISL)
- ➔ 13) Allocate FCoE VLANs and shared interfaces
  - 7010-1(config)# VDC SAN
  - 7010-1(config-VDC)# allocate fcoe-vlan-range 40 from **VDCs LAN**
  - 7010-1(config-VDC)# allocate shared interface ethernet 7/19-22
  - Ports that share the port group of the interfaces you have specified will be affected as well. Continue (y/n)? [yes]

### Use the “where” command

```
7010-1(config-VDC)# where  
Conf;VDC LAN admin@7010-1%admin
```

Helpful  
Tips

# Initial Configuration

## Things to do in the Storage VDC



8) Enable feature lldp

9) Enable feature lacp

LACP is best practice for port-channels  
Don't forget to enable LLDP on all VDCs!

14) Create a VSAN and a VLAN and configure the mapping

15) Configure FCoE port channel towards MDS

16) Configure VFC interface for VE port

17) Configure MDS for FCoE

18) Configure host ports on SAN VDC, create VFC interfaces and assign to VSAN

```
7010-1-SAN(config)# interface eth7/19-22
```

```
7010-1-SAN(config-if-range)# switchport trunk allowed vlan 40
```

```
7010-1-SAN(config-if-range)# no shut
```

```
7010-1-SAN(config)# interface vfc 721
```

```
7010-1-SAN(config-if)# bind interface ethernet 7/21
```

```
7010-1-SAN(config-if)# switchport mode f
```

```
7010-1-SAN(config-if)# switchport trunk allowed vsan 40
```

```
7010-1-SAN(config-if)# no shut
```

```
7010-1-SAN(config-if)# vsan database
```

```
7010-1-SAN(config-vsan-db)# vsan 40 interface vfc721
```

Best Practice:

Formulate a method to map  
VFC number to port. Example:  
7/21 = vfc 721

Helpful  
Tips

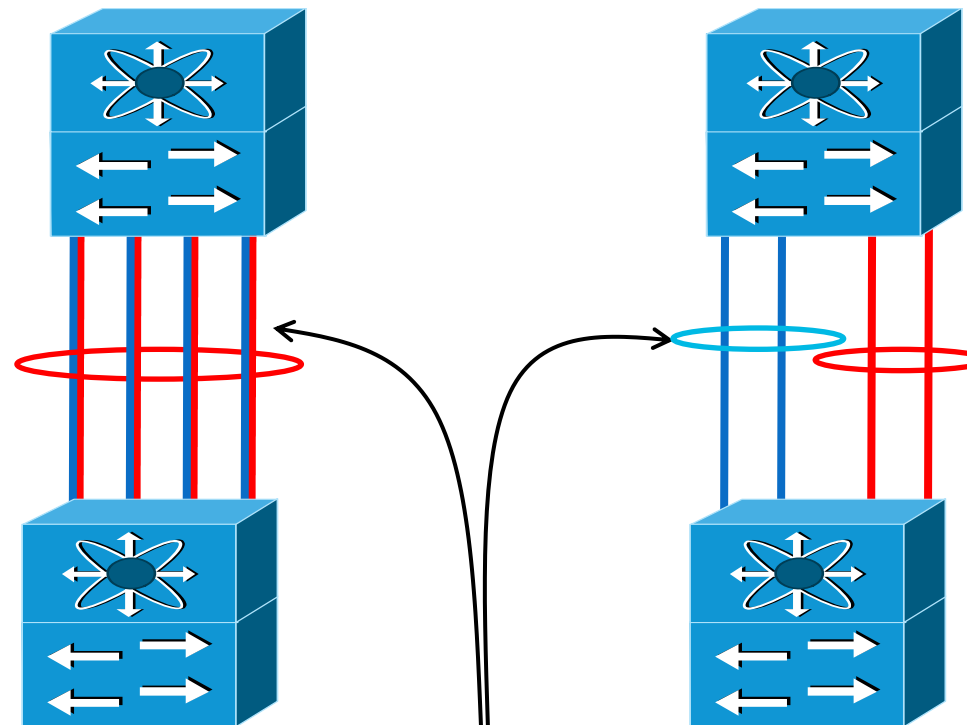
# Converged vs. Dedicated ISLs

Why support dedicated ISLs as oppose to Converged?

## Converged

- One wire for all traffic types
- QoS guarantees minimum bandwidth allocation
- No clear port ownership
- Desirable for DCI connections

Available on Nexus 5x00  
Nexus 7000 not supported



*Agg BW:* **40G**  
*FCoE:* **20G**  
*Ethernet:* **20G**

## Dedicated

- Dedicated wire for a traffic type
- No extra output feature processing
- Distinct port ownership
- Complete Storage traffic separation





Available on  
Nexus 5x00 and Nexus 7000

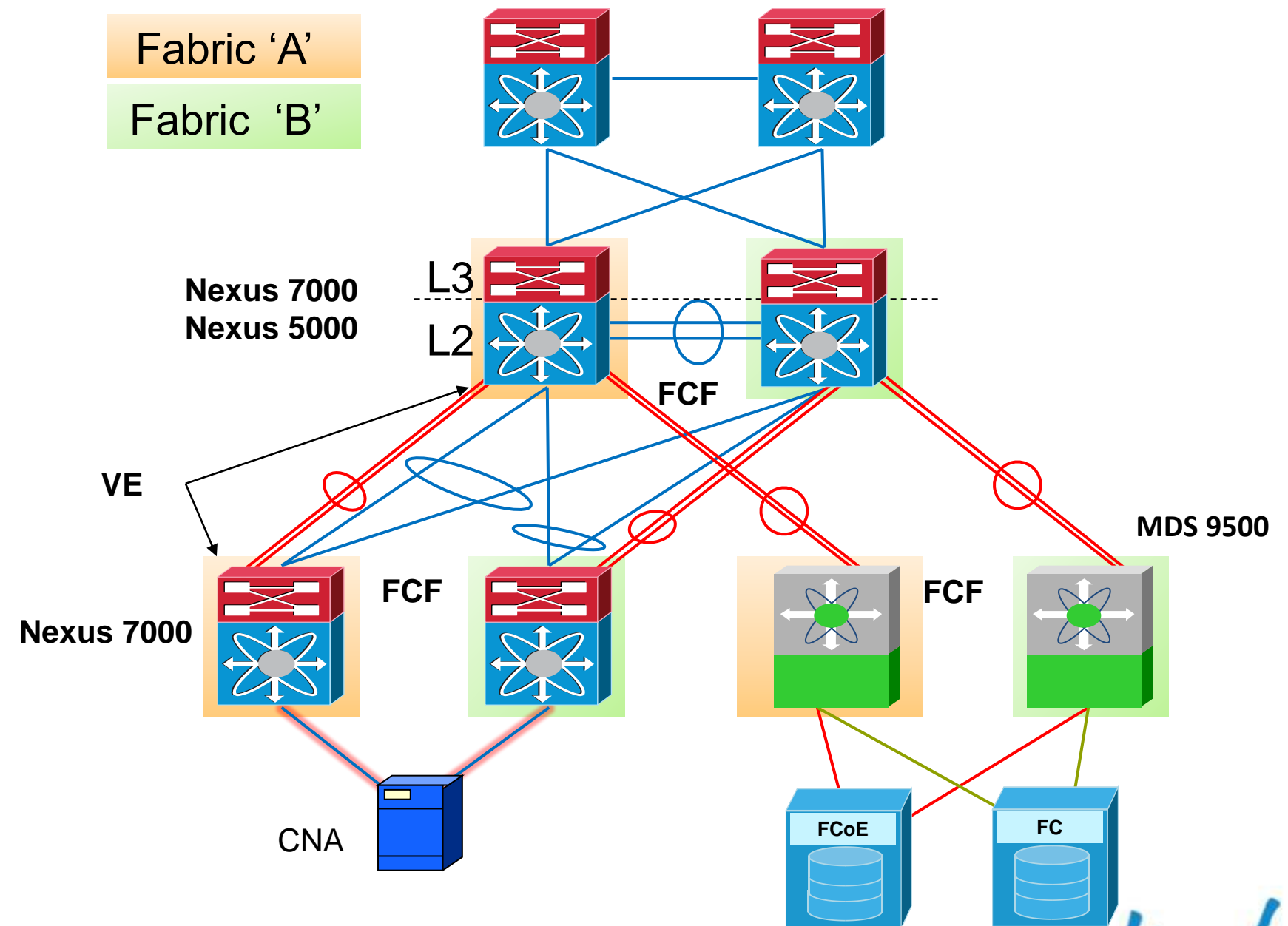
Different methods, producing the same aggregate bandwidth  
Dedicated Links provide additional isolation of Storage traffic

# Converged Beyond Access Layer

## Multi-hop FCoE

- LAN and SAN traffic share physical switches
- LAN and SAN traffic use dedicated links between switches
- All Access and Aggregation switches are FCoE FCF switches
- Dedicated links between switches are VE\_Ports
- Storage VDC for additional operation separation at high function Agg/Core

Ethernet	
FC	
Converged FCoE Link	
Dedicated FCoE Link	



# FCoE Requirements: Nexus 7000 and MDS

## Hardware and Software



For Your  
Reference

- Nexus 7000
  - Supervisor 1 or Supervisor 2/2E
  - F1-Series Module - N7K-F132XP-15
  - F2-Series Module - N7K-F248XP-25 (FCoE on F2 **requires** SUP2/2E)
  - FCoE license, one per F1/F2 line card - N7K-FCOEF132XP / N7K-FCOEF248XP
  - Optional License that enables IVR - one per chassis - N7K-SAN1K9
- MDS 9500
  - 8-Port FCoE line card - DS-X9708-K9 - Requires Sup2A in all 9500 Chassis, requires Fabric 2 or Fabric 3 in MDS 9513 (no extra license required)
- Minimum Software Required 5.2(1)
  - Minimum Recommended for MDS is 5.2(2)
  - Minimum Recommended for Nexus 7000 is 5.2(4) or 6.0(3). 6.1(x) required for F2



# Enhanced Transmission Selection

## Bandwidth Management – Nexus 7000

n7k-50-fcoe-2# show queuing interface ethernet 4/17

### Egress Queuing for Ethernet4/17 [System]

-----  
Template: 4Q7E  
-----

Group Bandwidth% PrioLevel Shape%

-----  
0 80 - -  
**1 20 - -**  
-----

Que# Group Bandwidth% PrioLevel Shape% CoSMap

-----  
0 0 - High - 5-7  
**1 1 100 - - 3**  
2 0 50 - - 2,4  
3 0 50 - - 0-1  
-----

### Ingress Queuing for Ethernet4/17 [System]

-----  
Trust: Trusted  
-----

Group Qlimit%

-----  
0 70  
**1 30**  
-----

Que# Group Qlimit% IVL CoSMap

-----  
0 0 45 0 0-1  
1 0 10 5 5-7  
**2 1 100 3 3**  
3 0 45 2 2,4  
-----

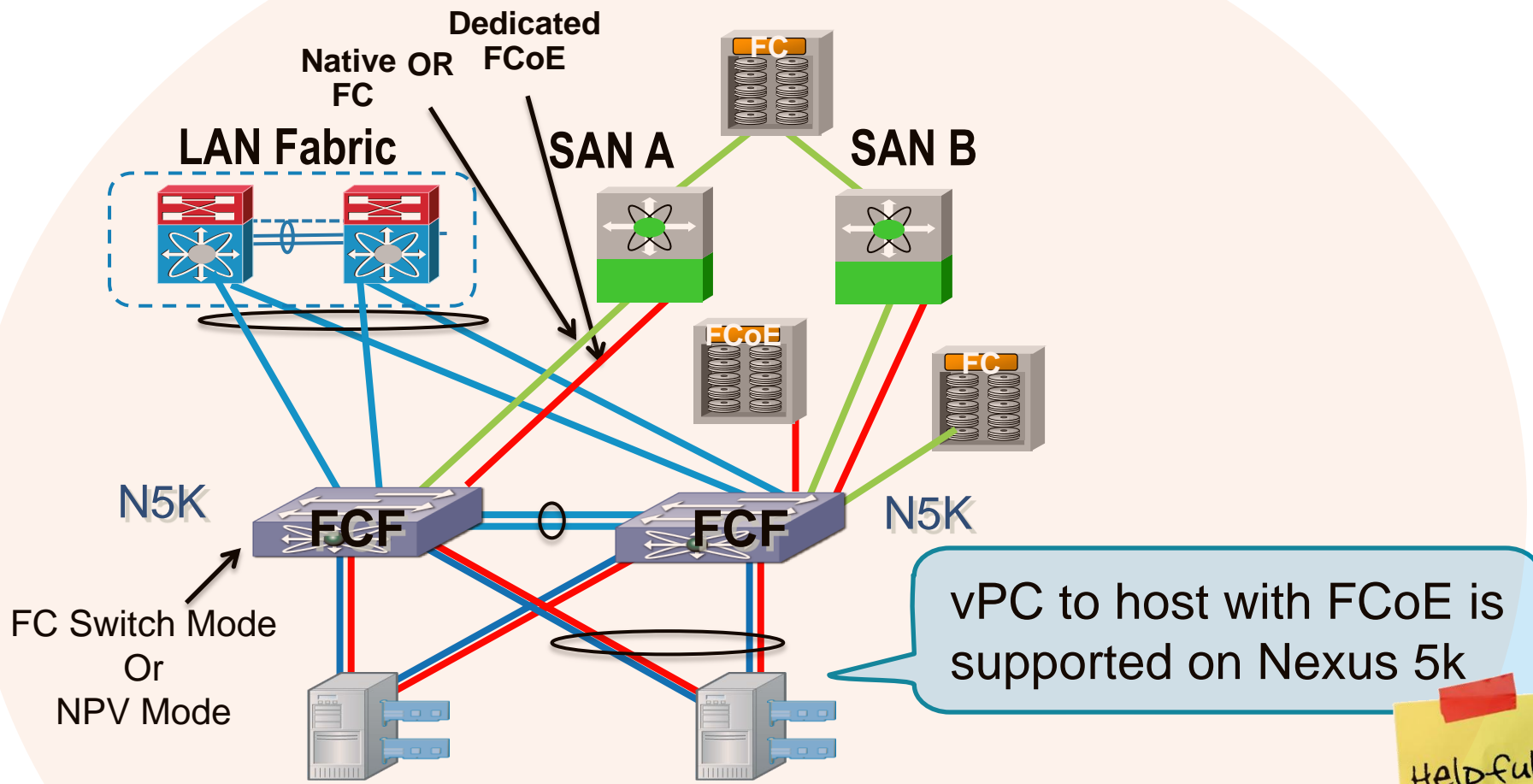
 Adjust as needed and remember Nexus 5x00 allocation is 50/50 by default

# Case Study: Converged Access With Nexus 5x00



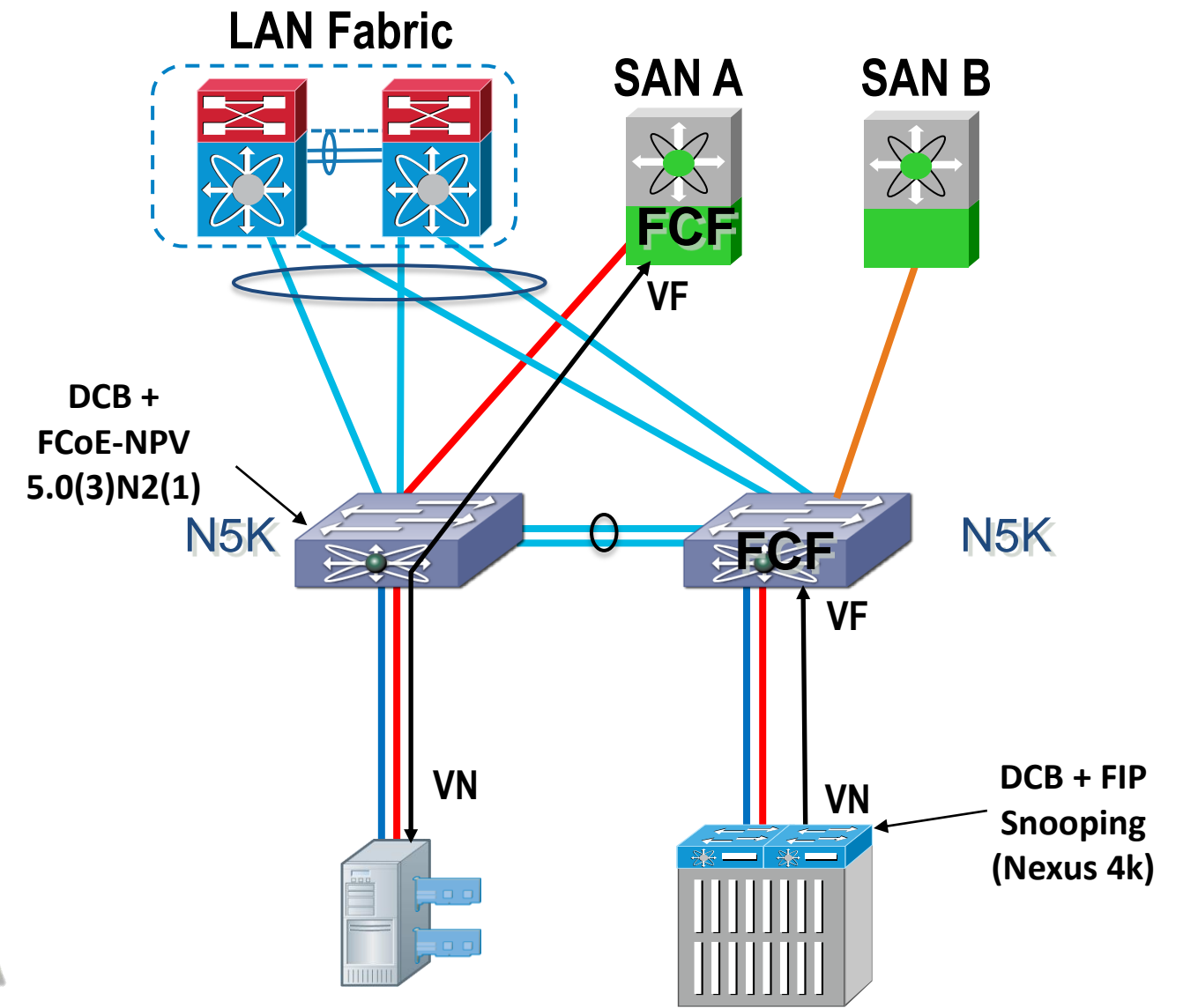
# Converged Access FCoE Designs

## Nexus 5000 Connectivity Models



### FCoE Direct Attach to Nexus 5k

- Simplest and Most Deployed Model
- Recommended to use N5k in NPV Mode



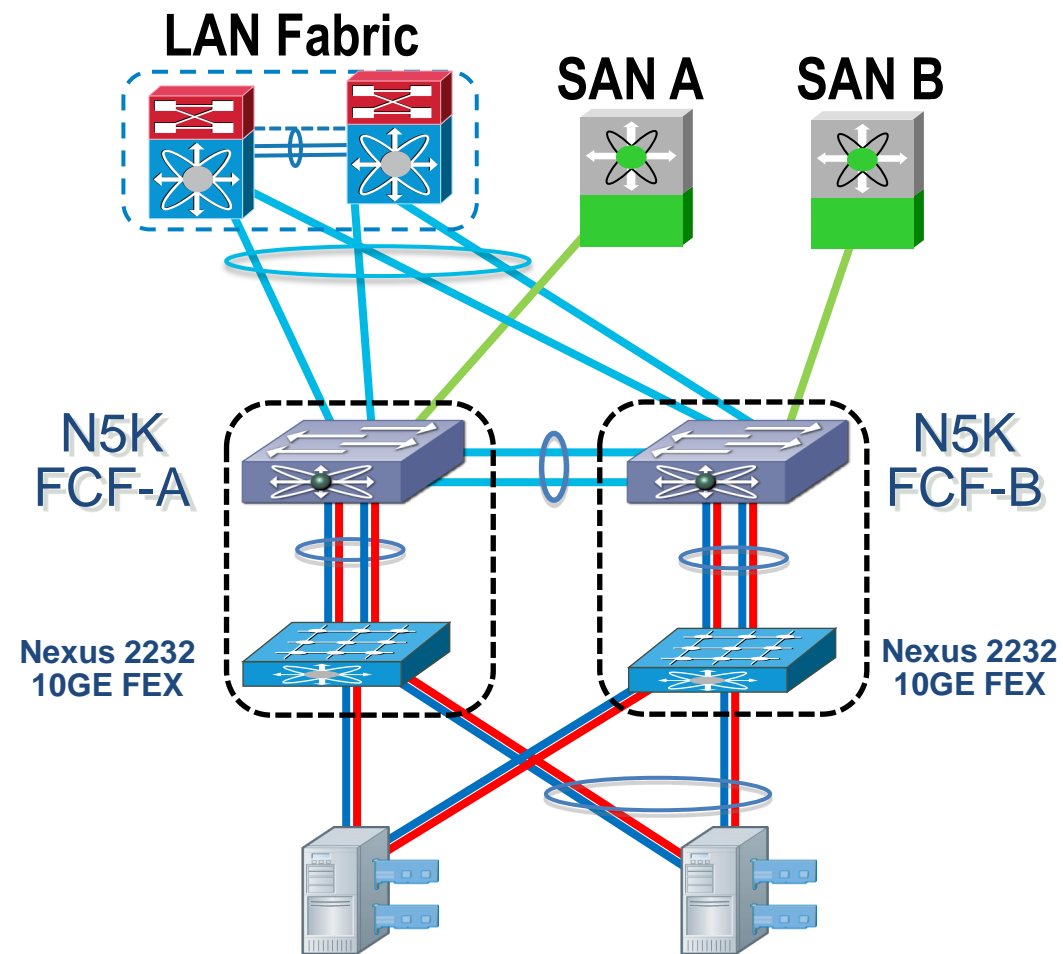
### FCoE Pass-Through Designs



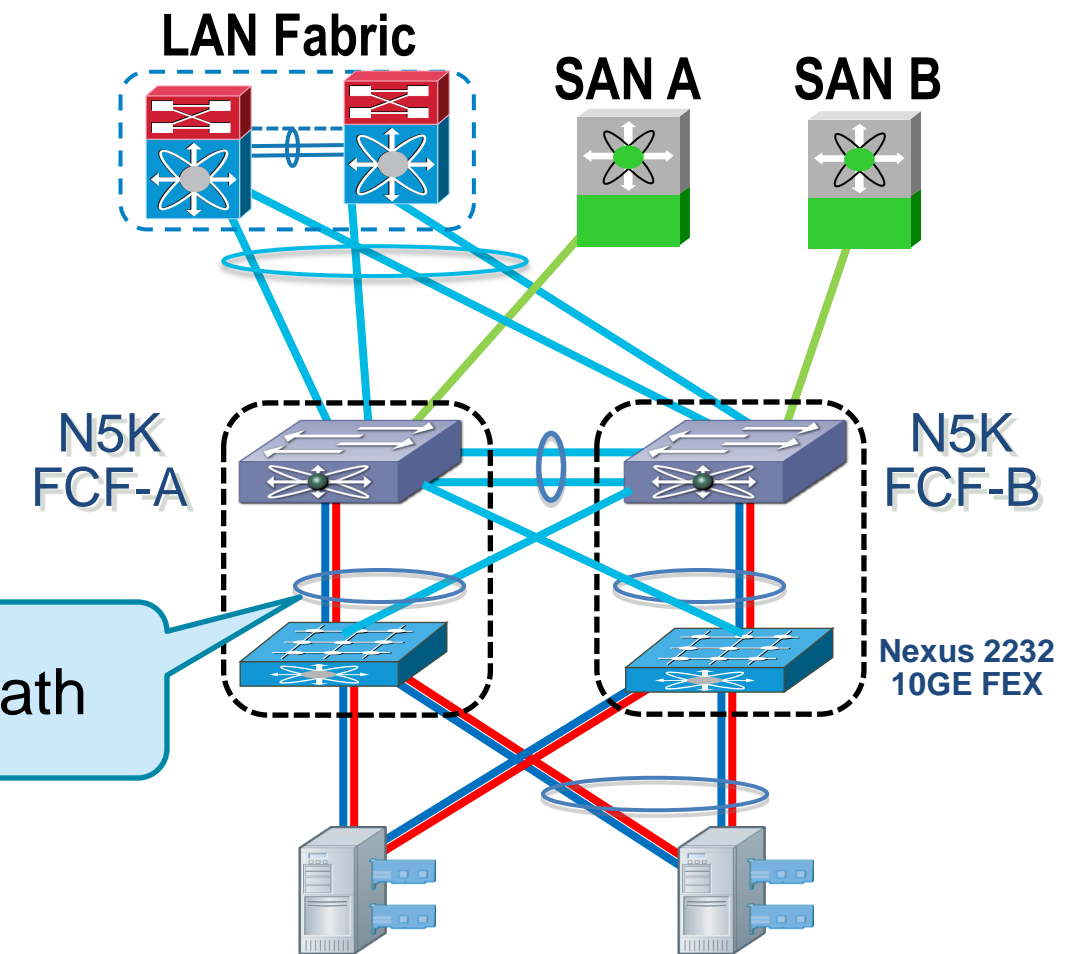
BRKSAN-2282

# Converged Access FCoE Designs

## Nexus 5000 + Nexus 2232 Connectivity Models



FCoE with Single-Homed FEX



FCoE with Dual-Homed FEX

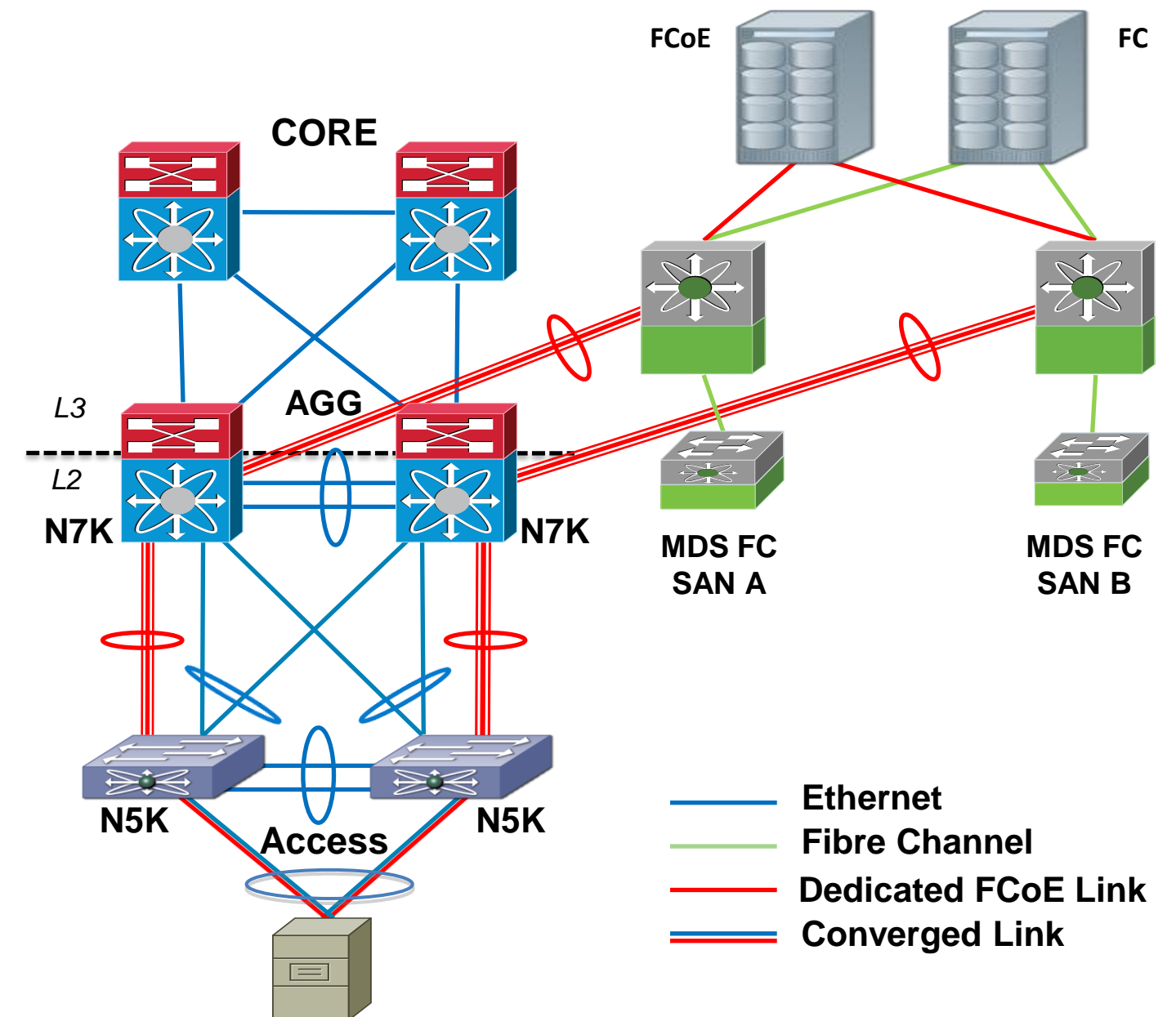
- Supported on Nexus 55xx from 5.1(3)N1(1)

- Ethernet
- Fibre Channel
- Dedicated FCoE Link
- Converged Link

# Multi-Hop FCoE Design

## Extending FCoE Through Aggregation

- Leverage FC SAN to Ethernet DCB switches in Aggregation layer with Dedicated links
- Maintain the A – B SAN Topology with Storage VDC and Dedicated links
- N5k as Consolidated Access layer
- Dedicated FCoE Ports between:
  - Access and Aggregation
  - FC SAN and Aggregation
- Zoning controlled by SAN A/B Core Switches



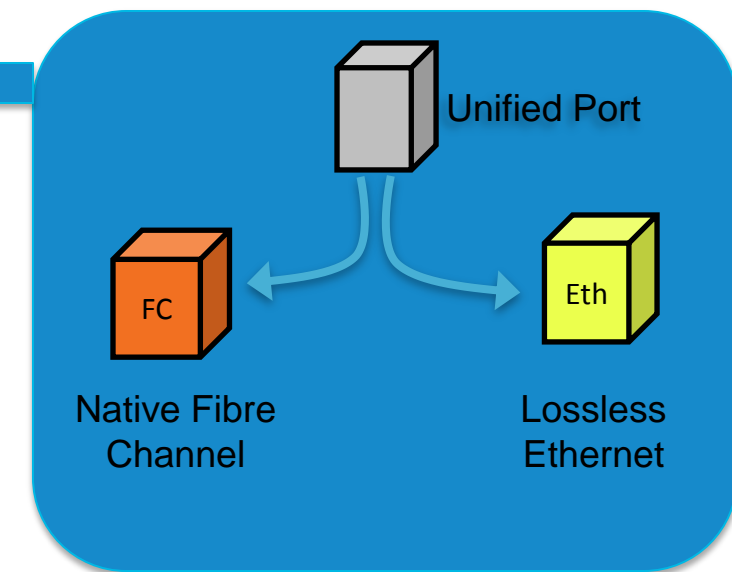
# FCoE Requirements

## Hardware and Software Licensing



For Your  
Reference

- Nexus 5010/5020
  - FC Module and transceivers (SAN uplinks or local storage connectivity)
  - Storage Services License (one per switch)
  - Optional FCoE NPV License (one per switch)
  - Optional License for DCNM-SAN (one per switch)
- Nexus 5548P/5548UP/5596UP
  - FC Module (5548P only)
  - FC transceivers (SAN uplinks or local storage connectivity)
  - Storage Services License (licensing in 8-port increments)
  - Optional FCoE NPV License (one per switch)
  - Optional License for DCNM-SAN (one per switch)



# Case Study: Converged Access with N5K

LAN and SAN Teams Working Together

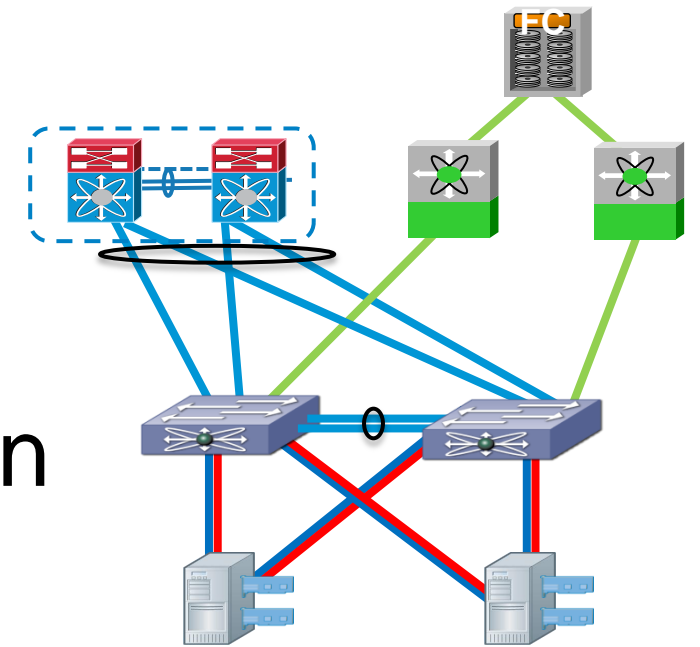


- FCoE ROI understood by network, storage, and server teams
- Rack mount servers with ToR Nexus 5548UP switches
- Physical and Virtual servers with 2-port CNAs
- Dual-fabric MDS SAN Core
- Nexus 5500 running in NPV mode

# Case Study: Converged Access with N5K

## LAN and SAN Teams Working Together

- LAN team owns the Nexus 5500 device
- SAN and LAN teams work together on initial configuration
- LAN Team :
  - uses lan-admin role for daily tasks on IP network
  - Manages all Ethernet functions that don't impact Storage
  - uses network-admin role for system upgrades and changes

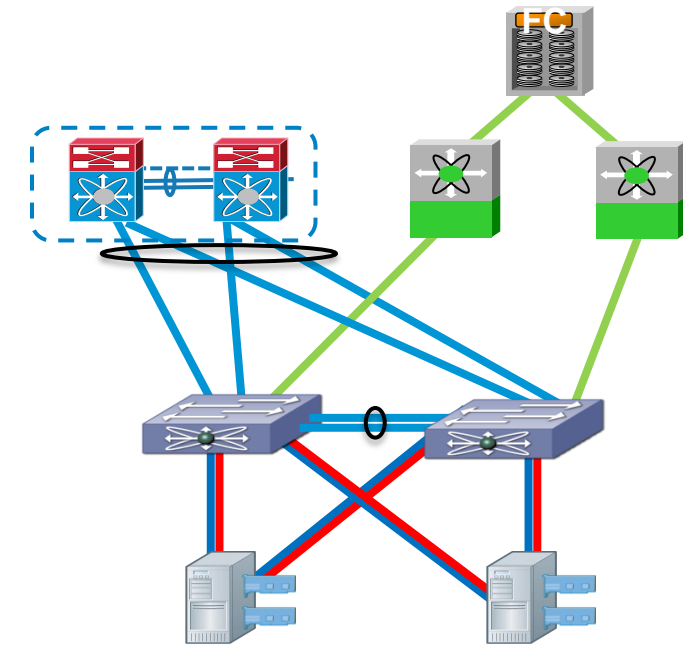




# Case Study: Converged Access with N5K

## LAN and SAN Teams Working Together

- SAN team:
  - Uses san-admin role for all access
  - Manages FC and vFC ports on Nexus 5500
  - All zoning done on SAN Core
  - Coordinates with LAN team for system level changes
- For firmware upgrades, LAN team schedules, but SAN team:
  - Is made aware of scheduled change
  - Is given time to research firmware and test
  - Can veto the upgrade if there are expected impacts to SAN



# Role-Based Access Control (RBAC)

## Role Definitions for FCoE Deployments

- network-admin (*system predefined*)
  - Admin privileges for the converged switch
- lan-admin (*user defined*)
  - IP network admin privileges (vlan, STP, ACLs, QoS, etc...)
- san-admin (*user defined*)
  - SAN admin privileges (zoning, vsans, aliases, fspf, etc...)



FCoE and RBAC Configuration Template:

[http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/operations/n5k\\_fcoe\\_ops\\_appA.html](http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/operations/n5k_fcoe_ops_appA.html)

# Role-Based Access Control (RBAC)

## lan-admin Role

```
role name lan-admin
! fcoe vlan is 3010
! vfc9 has been bound to eth1/9
!
rule 37 deny command config t ; spanning-tree vlan 3010
rule 36 permit command config t ; spanning-tree vlan *
rule 35 deny command config t ; spanning-tree *
...
rule 31 deny command config t ; vlan 3010 *
rule 30 deny command config t ; no vlan 3010 *
...
rule 1 permit read-write
!
interface policy deny
    permit interface eth1/1-40
!
vlan policy deny
    permit vlan 3010, 100-200
vsan policy deny
```

### Basic Premise for LAN-admin:

- Read access to everything
- Permit daily network admin tasks
- Prevent modifications to things that can impact Storage traffic

Default VLAN, VSAN, and interface policy is permit all. To restrict to a subset, change policy to deny and add specific permits.

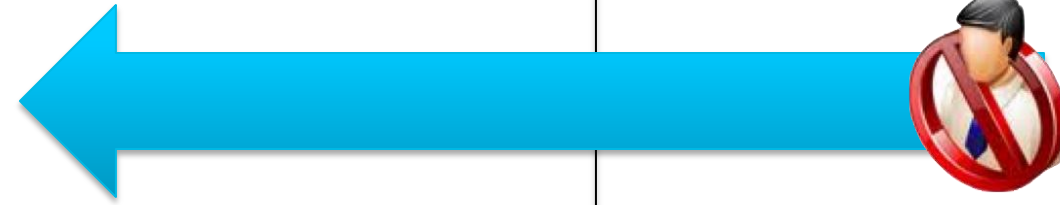
Helpful  
Tips

# Role-Based Access Control (RBAC)

## Can the LAN Admin Change the SAN Configuration?

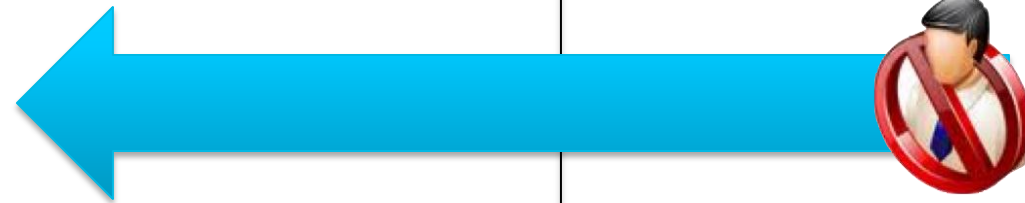


```
n5548-1(config-if)# switchport trunk allowed vlan remove 3010
% VLAN permission denied
```



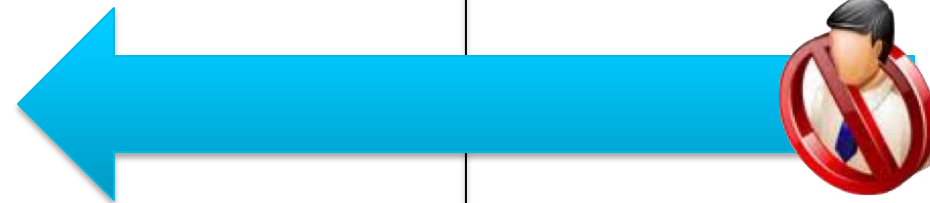
Can't Remove FCoE VLAN from Host Port

```
n5548-1(config)# int vfc 9
% Interface permission denied
```



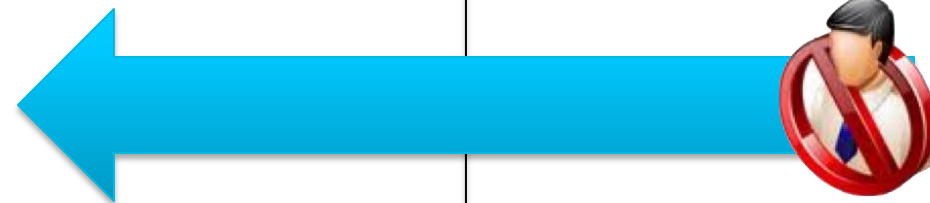
Can't Configure Virtual FC Port

```
n5548-1(config)# int eth 1/9
n5548-1(config-if)# shut
% Permission denied
```



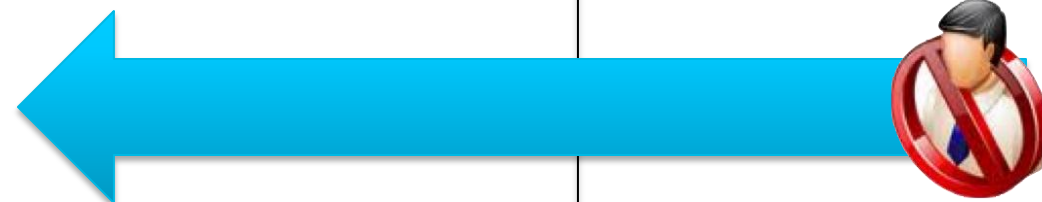
Can't Shut Down FCoE Host Port

```
n5548-1(config)# vsan database
% Permission denied
```



Can't Modify VSAN Database

```
n5548-1(config)# zone ?
^
% Invalid command at '^' marker.
```



No Zoning Commands Available

```
n5548-1(config)# fc?
fcoe FCOE command
```



No FC Commands Available

# Role-Based Access Control (RBAC)

## san-admin Role

```
role name san-admin
! fcoe vlan is 3010
! vfc9 has been bound to eth1/9
!
rule 83 permit command config t ; vlan * ; fcoe *
rule 82 deny command config t ; vlan * ; *
...
rule 53 deny command config t ; interface * ; spanning-
tree bpduguard
rule 52 deny command config t ; interface * ; spanning-
tree cost *
rule 51 deny command config t ; interface * ; spanning-
tree guard *
...
rule 1 permit read-write
!
vlan policy deny
  permit vlan 3010-3010
interface policy deny
  permit interface fc2/1-8
  permit Ethernet 1/9
  permit interface vfc 1-50
```

Basic premise for san-admin:

- Read access to everything
- Permit daily SAN admin tasks
- Prevent modifications to all things not related to Storage

Default VLAN, VSAN, and interface policy is permit all. To restrict to a subset, change policy to deny and add specific permits.

Helpful  
Tips

# Role-Based Access Control (RBAC)

## Can the SAN Admin Change the LAN Configuration?



```
n5548-1(config-if)# switchport trunk allowed vlan remove 10
% Permission denied
```



Can't remove non-FCoE VLAN on Host Port

```
n5548-1(config)# int eth 1/5
% Interface permission denied
```



Can't Configure non-FCoE Ethernet Ports

```
n5548-1(config)# vlan 10
% Permission denied
```



Can't Modify non-FCoE VLANs

```
n5548-1(config)# spanning?
^
% Invalid command at '^' marker.
```



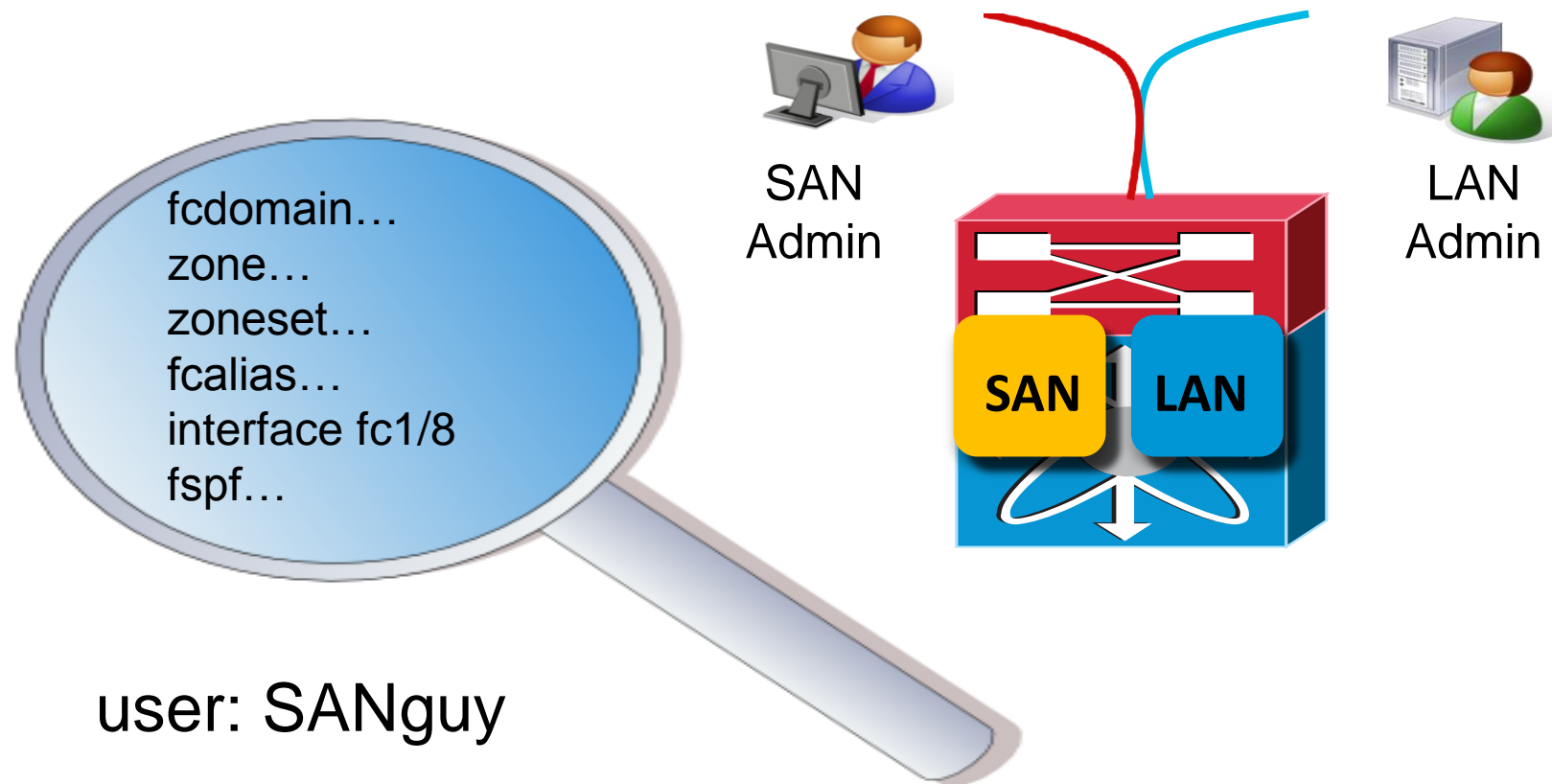
No Spanning Tree Commands Available

```
n5548-1(config)# class-map ?
^
% Invalid command at '^' marker.
```



No QoS Commands Available

# Predefined san-admin Role



Requires  
NX-OS 5.2

- Nexus 5000 now includes a predefined san-admin role
- This role cannot be changed and cannot be removed
- A custom role can be created with san-admin as a baseline for granularity

# RBAC and SNMP

- NX-OS supports SNMPv3 user access with RBAC:

```
n5548-1(config)# snmp-server user user1-san san-admin
```

- NX-OS also supports SNMP v1/v2c communities with RBAC:

```
n5548-1(config)# snmp-server community SNMPstring group san-admin
```

- N7K NX-OS 6.0 added SNMP OID filtering rules to RBAC:

```
n7010-1(config)# role name OID_ONLY  
n7010-1(config-role)# rule 1 permit read oid snmp_oid_name  
n7010-1(config-role)# rule 2 deny read
```

```
n7010-1(config-role)# snmp-server community PUBLIC group OID_ONLY
```

```
n7010-1(config)# snmp-server user user1-san OID_ONLY
```

This feature is not yet supported on the Nexus 5k.

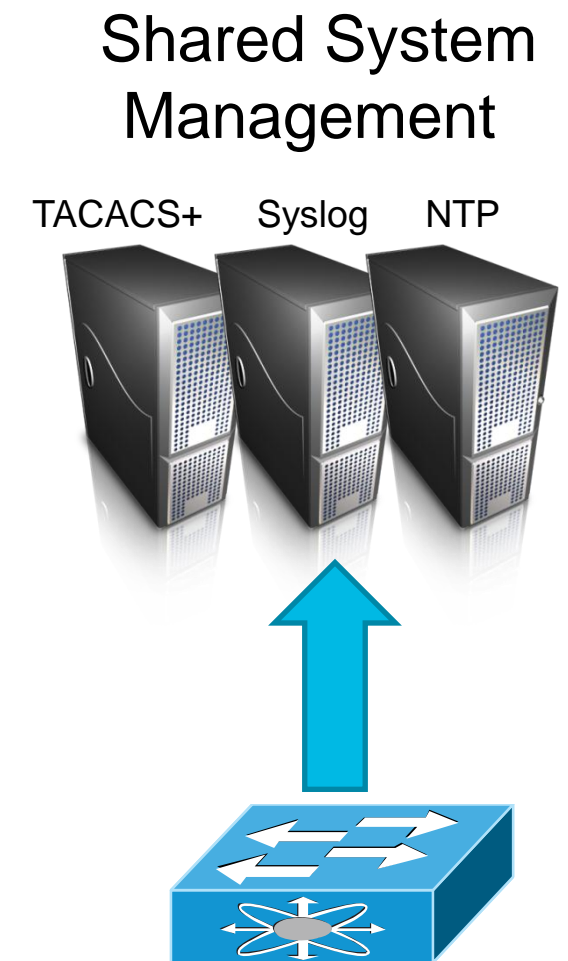
Helpful  
Tips



# System Management

- Nexus 5k uses shared system management
  - AAA
  - Syslog
  - NTP

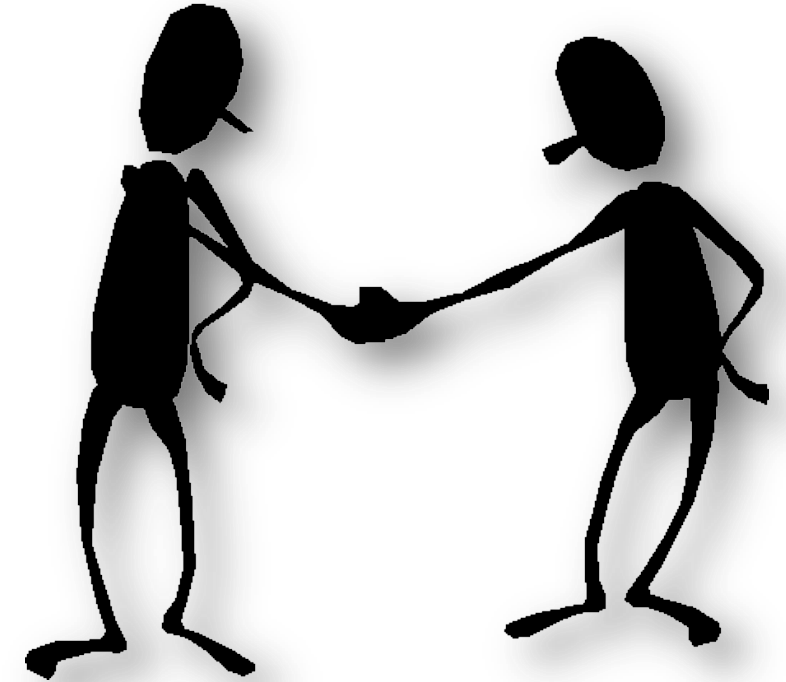
This is different than Nexus 7000 with Storage VDC, which allows for distinct management services for LAN and SAN



# Initial Configuration

What needs to be agreed before configuration?

- Determine NX-OS version to run
- Define the Host Facing ports
- Define the Uplink ports for LAN and SAN
- Define VLANs/VSANs/VFCs to be used for FCoE
  - Best Practice: Reserve a Range with same number of VSANs expected to be used



# Initial Configuration

What are the steps? What's different?



- 1) Configure core SAN switch for NPIV
- 2) Install Storage Services (FC\_FEATURES\_PKG) license

## 3) Enable feature npv

```
n5548-1(config)# feature npv
```

Verify that boot variables are set and the changes are saved. Changing to npv mode erases the current configuration and reboots the switch in npv mode. Do you want to continue? (y/n)

It's recommended to enable NPV first, as it will require a reload of the switch.

Helpful  
Tips

## 4) Enable feature fcoe

## 5) Enable feature lacp

# Initial Configuration

What are the steps? What's different?



## 6) Enable system QoS and policy for FCoE:

```
n5548-1(config)# system qos
n5548-1(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
n5548-1(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
n5548-1(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
n5548-1(config-sys-qos)# service-policy type network-qos fcoe-default-nq-policy
```

This step is only required on Nexus 55xx platforms prior to release 5.1(3)N1(1). The Nexus 50xx platforms have FIP/FCoE in no-drop class by default.

Helpful  
Tips

## 7) Create VSAN and assign native FC interfaces to VSAN

## 8) Configure Fibre Channel interfaces to SAN

## 9) Create FCoE VLAN and map to VSAN

```
n5548-1(config)# vlan 800
n5548-1(config-vlan)# fcoe vsan 800
```

Best Practice:  
Formulate a method to map VSAN to VLAN. Examples:  
VLAN 800 = VSAN 800

Helpful  
Tips

# Initial Configuration

What are the steps? What's different?



## 10) Configure host ports for FCoE traffic

```
n5548-1(config)# interface ethernet 101/1/1-10
n5548-1(config-if-range)# switchport mode trunk
n5548-1(config-if-range)# switch trunk allowed vlan 200,800
n5548-1(config-if-range)# spanning-tree port type edge trunk
```

FCoE VLAN is defined here.

VLAN 200 = Ethernet only  
VLAN 800 = FCoE

Helpful  
Tips

## 11) Create virtual FC interface and bind to host interface

```
n5548-1(config)# interface vfc 1101
n5548-1(config-if)# bind interface ethernet 101/1/1
n5548-1(config-if)# switchport trunk allowed vsan 800
```

Best Practice:  
Formulate a method to assign  
vfc number.

Helpful  
Tips

## 12) Assign vfc interface to VSAN

```
n5548-1(config)# vsan database
n5548-1(config-vsantdb)# vsan 800 interface vfc 1101
```

# Unified Fabric Management with DCNM

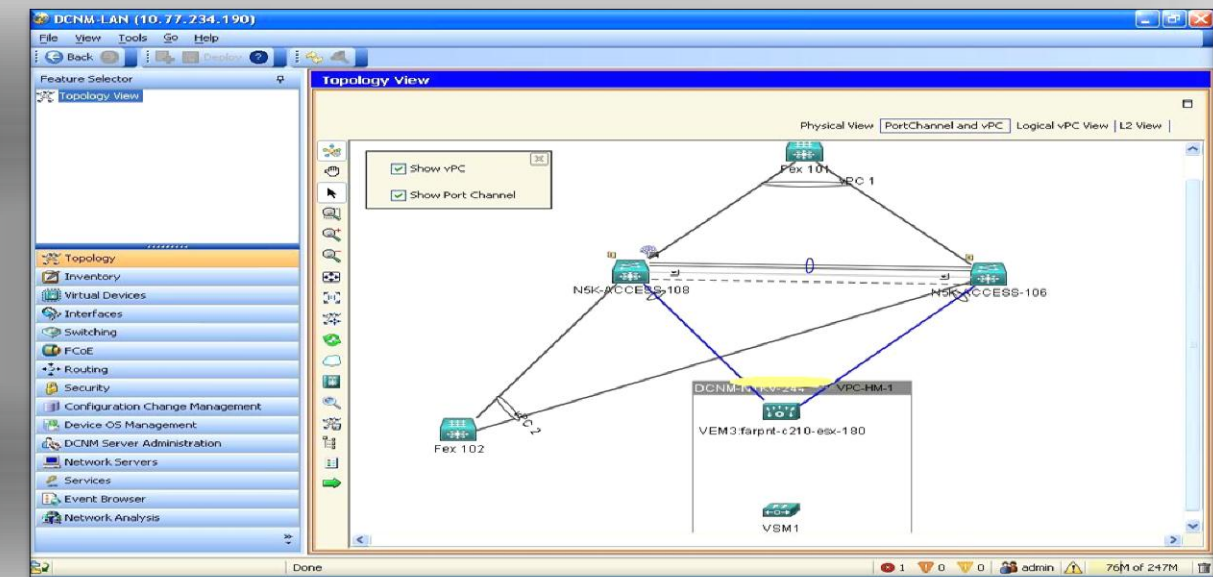


# Cisco Prime Data Centre Network Manager

Single Pane of Glass for Converged DC Management



Fault Management  
Resource Management  
Change Management  
Provisioning/Configuration  
API Integration  
Security RBAC



## UNIFIED FABRIC



MDS



NEXUS CORE



NEXUS ACCESS



Storage

Network

DMM

FABRICPATH

IOA

VDC

SME

VPC

FCoE

OTV



# DCNM: FCoE Management

The screenshot shows the DCNM interface with a table of switch interfaces and a network topology diagram. The table lists switches and their interfaces with various configuration parameters. The topology diagram shows a network of switches including MDS9509-sw67, fm-n7k, MDS9509-sw67, MDS9509-sw64, and npv1.

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin	Status Oper	FailureCause	Was Enabled	LastCh
fm-n7k	vfc100	E	TE	5	n/a		auto	10 Gb	shared	in	up	up	none	true	2011/03
MDS9509-sw67	vfc100	E	TE	5	n/a		auto	10 Gb	shared	in	up	up	none	true	2011/03

The screenshot shows the FCoE Configuration Wizard - /DataCenter, Step 4 of 4: Configure Ethernet Interfaces. It displays a table of interfaces and their configuration status for switch MDS9509-sw67.

Interface	VLAN(VSAN) Mapping	Configure Action Status
eth-channel400		Interface speed is less than the minimum necessary for vFC configu...
Ethernet8/1		Interface mapped to vfc8/1.
Ethernet8/2		
Ethernet8/3		
Ethernet8/4	5(5),7(7),12(12),45...	vfc8/4 created, bound and enabled.
Ethernet8/5	45(45)	vfc8/5 created, bound and enabled.
Ethernet8/6	45(45)	vfc8/6 created, bound and enabled.
Ethernet8/7		Interface mapped to vfc8/7.
Ethernet8/8		
Ethernet8/9	45(45)	vfc8/9 created, bound and enabled.
Ethernet8/10		
Ethernet8/11		
Ethernet8/12		Interface mapped to vfc8/12.
Ethernet8/13		Interface mapped to vfc8/13.

- Simplified FCoE provisioning, configuration and monitoring
- FCoE management paradigm consistent with FC management
- **FC** ↔ **Ethernet** mapping; ISL performance/health monitoring
- **FCoE overlays** on Data Centre topology views



# VMPath – VM to Storage Visibility



The screenshot displays the Cisco Prime Data Center Network Manager interface. The top navigation bar includes 'Cisco Prime Data Center Network Manager' and various menu options like 'Dashboard', 'Health', 'Performance', 'Inventory', 'Reports', 'Config', and 'Admin'. The main content area is divided into several sections:

- Host Enclosures (139 Items):** A table listing various host enclosures with columns for Name, IP Address, #Macs, Mac Address(es), #WWNs, Port WWN(s), OS, #VMs, and VHost Name.
- Members of 10.29.190.234:** A detailed view of VMs on a specific host, showing columns for Name, OS, IP Address, Mac Address(es), #CPU, Mem, Rea, Wri, Status, and Data Store/Storage Port.
- Topology - 10.29.190.234:** A network diagram showing the connectivity between the host and various network devices like CPOC-N5K1, CPOC-N5K2, EBC-MDS9506-1, EBC-MDS9506-2, and NetApp0890ace31.
- CPU & Memory - 10.29.190.234:** A performance graph showing CPU % and Memory % over a 24-hour period for the host 10.29.190.234.

- VM-aware discovery and correlation with SAN and LAN infrastructure
- Path analytics from VM to storage ports

# Key Takeaways

- ✓ FCoE delivers an optimised infrastructure
- ✓ Several FCoE deployment models exist
- ✓ Features are available for both isolation and convergence
- ✓ Converged networks require technology, tools, and processes



# Q & A



# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

[www.ciscoliveaustralia.com/portal/login.wv](http://www.ciscoliveaustralia.com/portal/login.wv)

Cisco *live!*

