Cisco Storage Networking
Security & Hot Topics

Ji Lim

Consulting Systems Engineer

jilim@cisco.com

Kontakt: Filip Koch, Datacenter PSS
+45 2149 8404 / fikoch@cisco.com

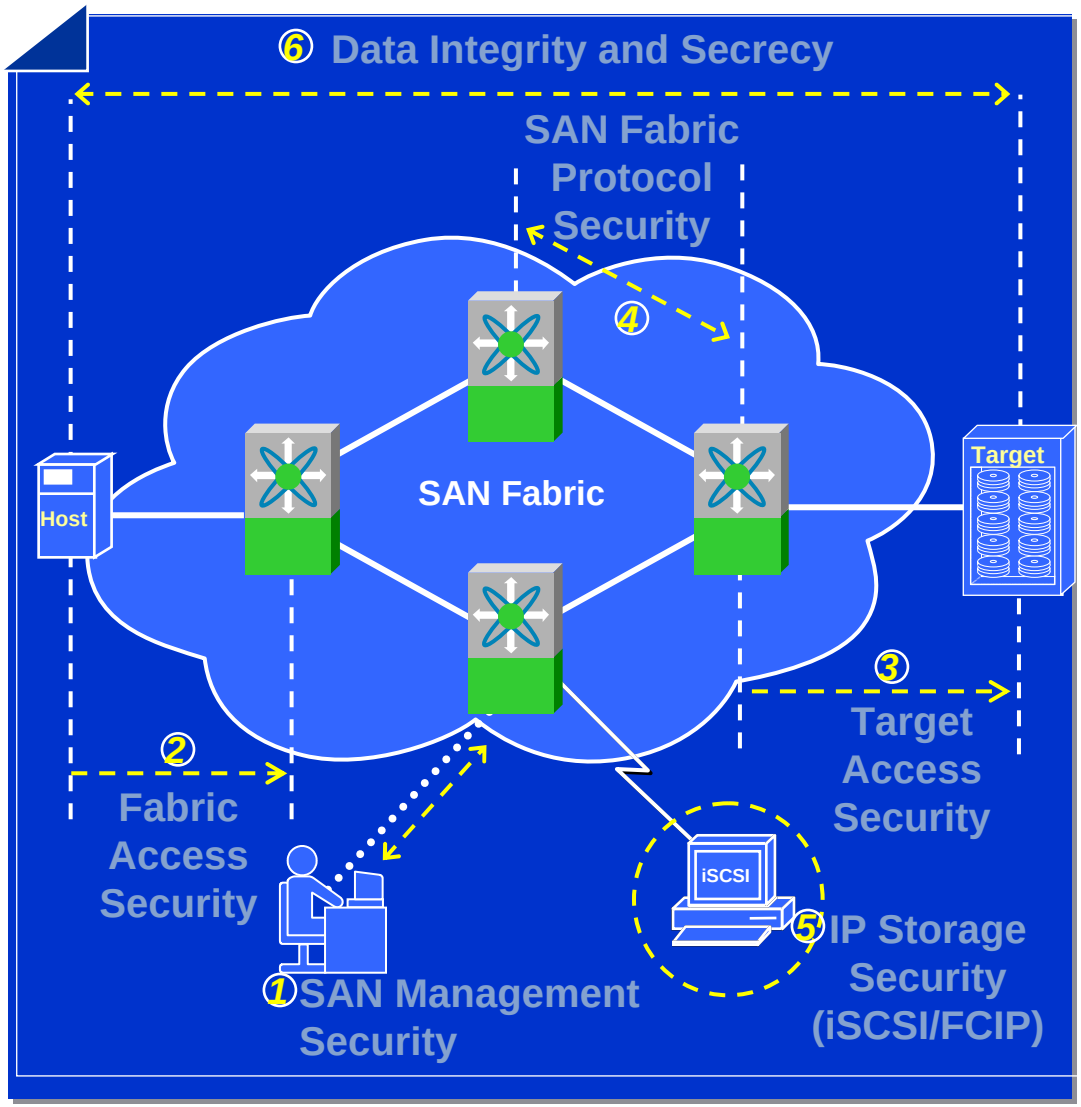
13 November 2007

SAN Security
Several Threats: Few Solutions

- SAN security is often overlooked as an area of concern but can have the most detrimental impact
- Application integrity and security is highly addressed, but back end storage and network carrying actual data is not
- SAN extension solutions now push SANs outside the datacenter boundaries
- Not all compromises are intentional—many accidental breaches—still have same effects
- SAN security is only one part of complete datacenter solution
  - Host access security—one-time passwords, audit logs, VPNs
  - Storage security—data in flight, data-at-rest encryption, LUN security
  - Datacenter physical security

Storage Security Architecture

- Six key areas of focus
  - **SAN Management Access** — secure access to management services
  - **Fabric Access** — secure device access to fabric service
  - **Target Access** — secure access to targets and LUNs
  - **SAN Protocol** — secure switch-to-switch communication protocols
  - **IP Storage Access** - secure FCIP and iSCSI services
  - **Data Integrity and Secrecy** — Encryption of data both in transit and at rest



SECURING THE STORAGE LAYER: **FIBRE CHANNEL**

Securing Fibre Channel

- 'FC Zoning' introduced to provide segregation among Storage devices
- 'Port Mode Security' introduced to prevent edge ports coming up as ISLs
- 'Port Security'/'Port Binding' introduced to help protect against WWN Spoofing
  - Locking WWNs to specific ports
- Virtual SANs (VSANs) introduced to provide segregation between (virtual) fabrics
- FC Security Protocol (FC-SP) is the final step required to secure FC
  - Device authentication, per message secrecy and integrity protection, policy management

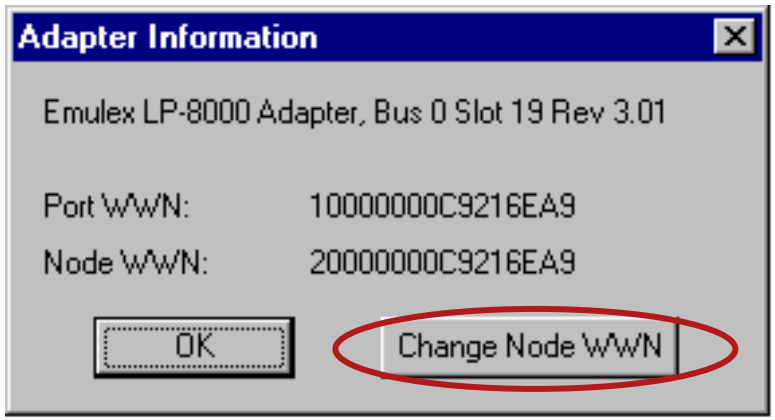
Fabric Access Security:
FC Zoning: Segregation of Devices

- Zoning provides segregation between groups of hosts and disks within a SAN

  Some operating systems attempt to access (write) all discovered disks causing data corruption or loss

- Zoning provides segregation, but lacks any form of authentication

  Circumventing zones through impersonation of a member (identity spoofing) is both possible and relatively trivial to do



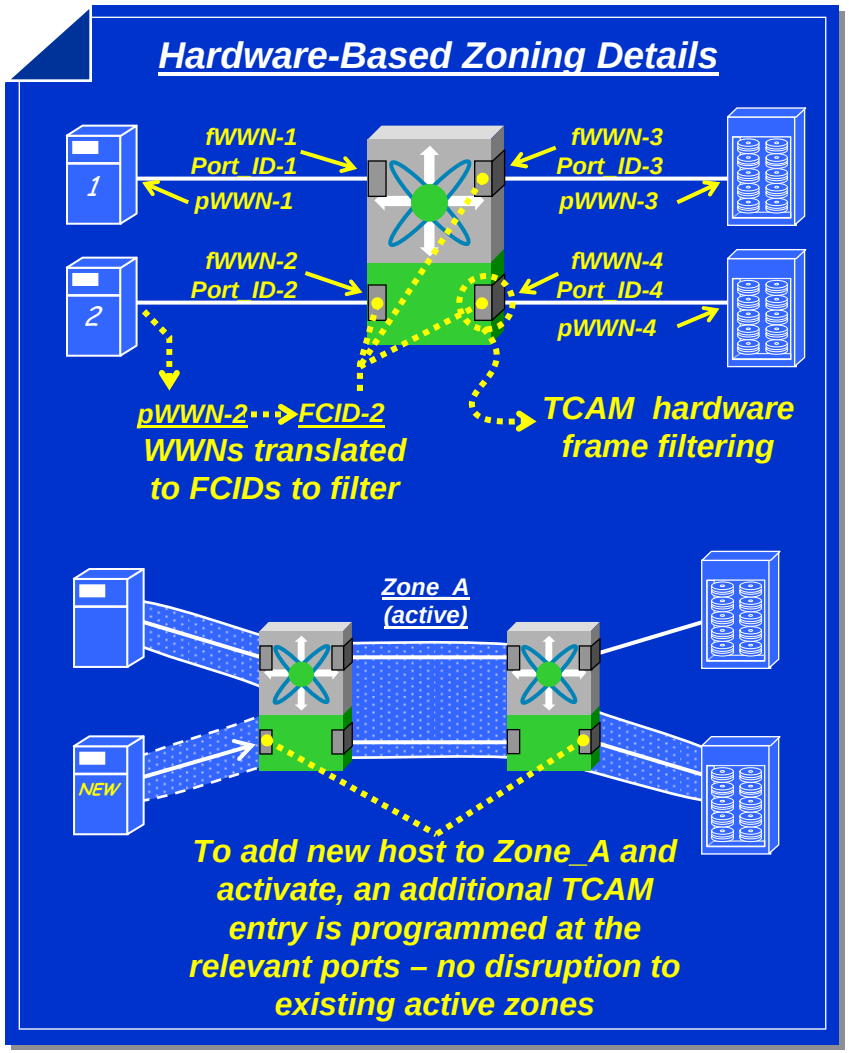
http://www.emulex.com/ts/fc/docs/wnt2k/2.00/pu.htm

Fabric Access Security:
FC Zoning: Soft Zoning and Hard Zoning

- Soft Zoning
  The fabric restricts information made available to non-members
  - Control-plane, software-enforced
  - A device logging into the fabric and contacting the nameserver to see what other devices exist will only be told about devices in the same zone(s) as itself
- Hard Zoning
  The fabric denies access to non-members, even if they attempt to do so
  - Hardware-enforced, per-frame ACLs
  - Standard doesn't mandate whether ingress/egress based

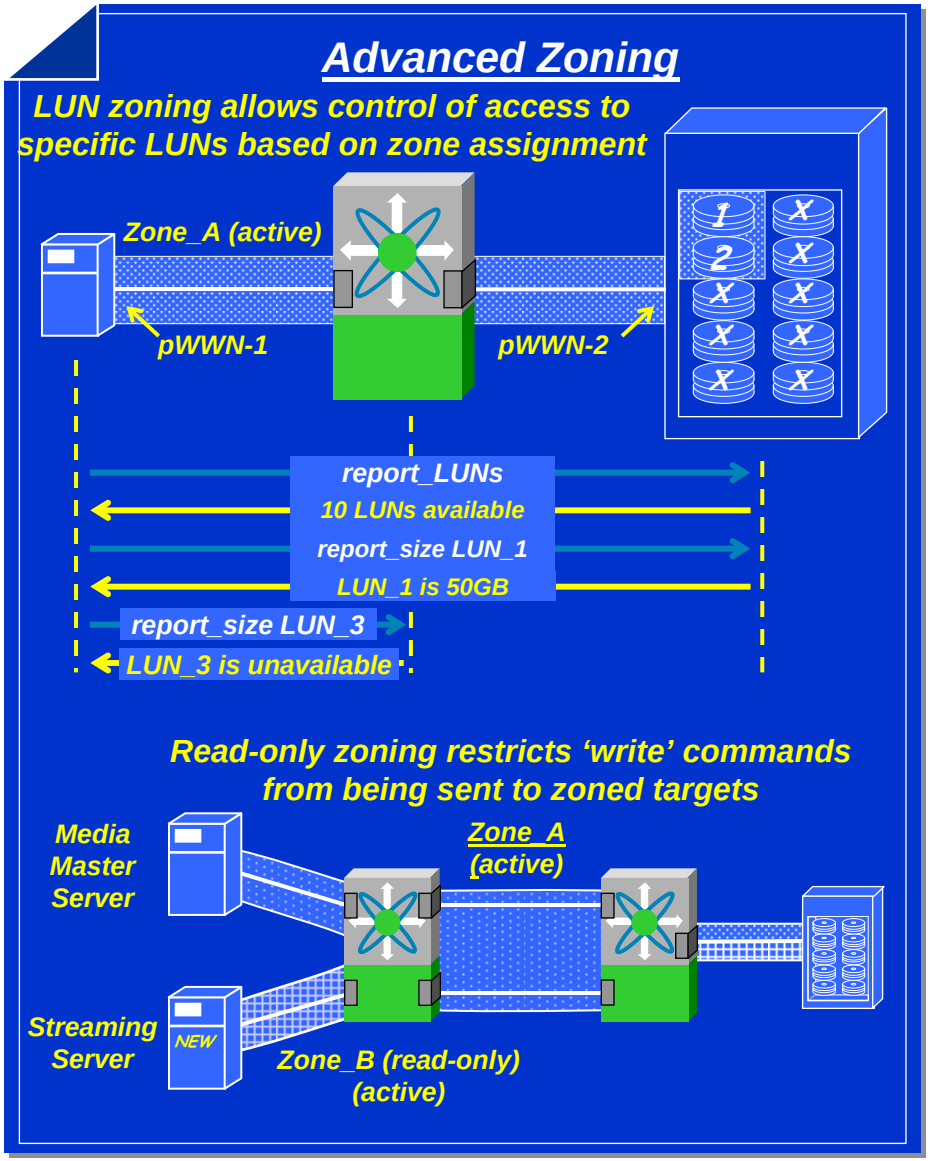
Cisco MDS 9000 Family Zoning Services

- All zoning services offered by Cisco are implemented in hardware
  - No dependence on whether using mix of WWNs and Port_IDs in a zone—all hardware based
  - WWN-based zoning implemented in software with hardware reinforcement (ie. no nameserver-only zoning)
  - WWNs are translated to FCIDs to be frame-filtered
- Dedicated high-speed port 'filters' called Ternary CAMs (TCAMs) filter each frame in hardware and reside in front of each port
  - Support up to 20,000 programmable entries consisting of zones and zone members
  - Very deep frame filtering for new innovative features
  - Wire-rate filtering performance—no impact regardless of number of zones or zone entries
  - Optimized programming during zoneset activation — incremental zoneset updates
- SCNs contained within zones in given VSAN and zones within VSAN
- Selective *Default zone* behavior—default is deny (Per VSAN setting)



Cisco Advanced Zoning Services

- LUN Zoning is the ability to zone an initiator with a subset of LUNs offered by a target
  - Host discovers all LUNs but can only login to those LUNs part of the zone
  - Inaccessible LUNs are busied-out by the switch at the ingress port
  - Provides powerful solution combined with array-based LUN security to add fabric enforcement
  - Accidental LUN exposure prevented by fabric
- Read-Only Zoning leverage the hardware-based frame processing of the MDS 9000 Family
  - Filters FC4-Command frames based on whether the command is a read or write command
  - Useful for systems that only need read access to a volume such as multimedia servers
  - Especially useful for media servers that need high speed access to rich content for broadcast—block level bypasses NAS service



Fabric Access Security:
Virtual SANs (VSANs)

- Virtual SANs (VSANs) achieve higher security and greater stability in FC fabrics by providing isolation among devices that are physically connected to the same physical fabric
- VSANs can be used to create multiple logical SANs over a common physical infrastructure
- VSANs provide:

  Traffic isolation

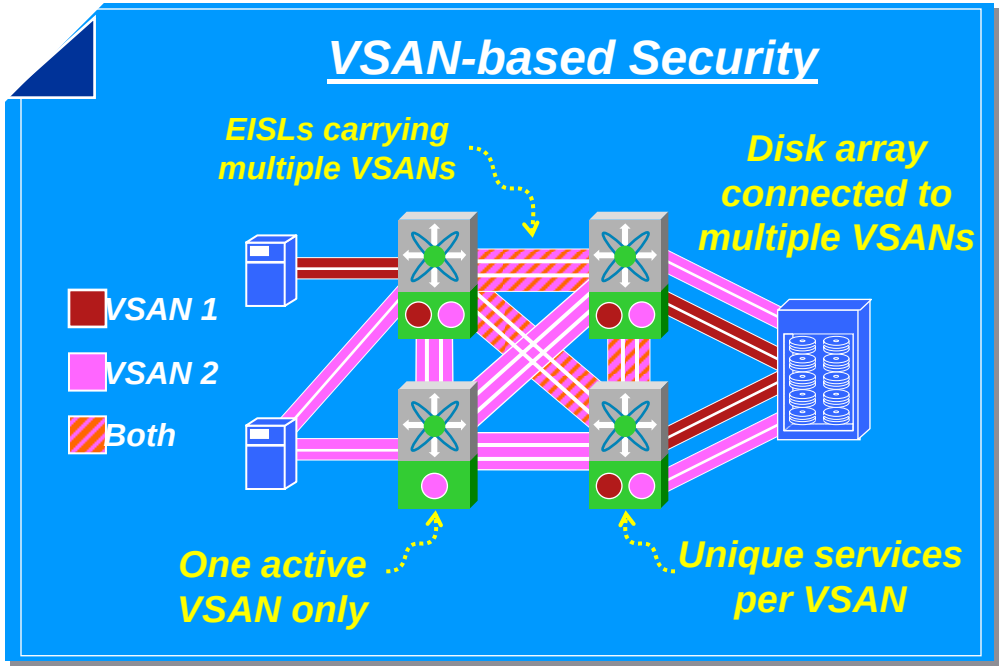
  Strict isolation between VSANs based on fabric service partitioning and explicit frame tagging

  Per-VSAN fabric services

  Independent fabric services, including name server, zoning, FSPF and domain manager on a per-VSAN basis Disruption of one of these services in one VSAN doesn't impact any other VSANs

  Shared Topology

  Multiple VSANs can share the same physical topology



- Part of ANSI T11 'Fabric Expansion' study group

Port Security

- Used to prevent deliberate unauthorized access to switch ports and inadvertent miscabling of existing switch ports
- Binds specific WWN(s) to having access to one or more switch ports, to prevent unauthorized access

  Port name (pWWN), node name (nWWN) or switch name (sWWN) is used to bind authorized devices to a given switch port
- Port security can be enabled on a per VSAN basis (default: disabled)
- When port security is enabled on a port:

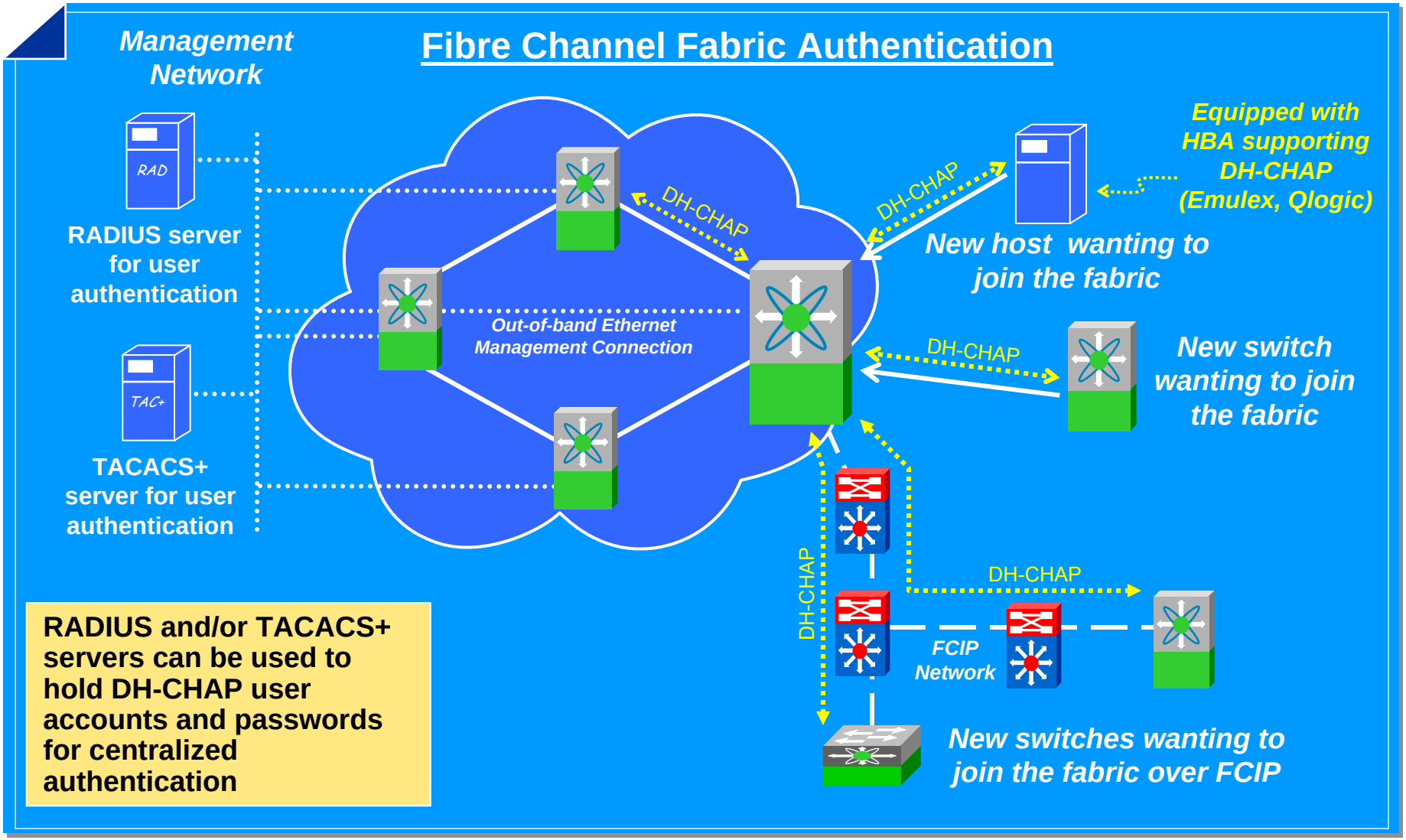
  Login requests from unauthorized FC devices (Nx ports) and switches (xE ports) are rejected

  All intrusion attempts are reported to the SAN administrator

Fabric Access Security:
FC Security Protocol (FC-SP) DH-CHAP

- Device authentication with FC-SP provides stronger means of ensuring device identity
  - – Switch-to-switch, switch-to-device, device-to-device authentication within the login phase
  - – Frame-by-frame FC-2 level encryption (FCsec) that provides origin authentication, integrity, anti-replay and privacy protection to each frame sent over the wire
  - – Consistent and secure policy distribution across the fabric.
- ANSI T11.3 FC-SP draft —Security Protocols working group
  - – Cisco is prime contributor to FC-SP draft standard
  - – Numerous protocols supported in draft including DH-CHAP (Cisco's chosen method) and FCAP
- Switch-to-switch authentication via FC-SP using DH-CHAP
- Device-to-switch authentication with help from HBA vendors supporting DH-CHAP DH-CHAP provides authentication mechanism
- FC-SP can be enabled/disable on a switch and activated on a per-port basis.

Fabric Access Security:
FC Security Protocol (FC-SP) DH-CHAP



SECURING THE STORAGE LAYER: **IP STORAGE (ISCSI & FCIP)**

IP Storage Security:
SCSI-over-IP (iSCSI)

- iSCSI uses in-band authentication
  - CHAP-based (other mechanisms are optional)
- The IESG recommends the use of IPSec tunnels where required for per message security, origin authentication, integrity, anti-relay protection and privacy
- iSCSI can leverage many of the security features already inherent in Ethernet and IP
  - Ethernet Access Control Lists (ACLs) ↔ FC zones
  - Ethernet VLANs ↔ FC VSANs
  - Ethernet 802.1x port security ↔ FC port security
  - iSCSI authentication ↔ FC DH-CHAP authentication
- iSCSI typically offers LUN mapping/masking capability as part of gateway function
- iSCSI may make use of FC Fabric Security features (e.g. Zoning) also, as well as mapping iSCSI initiators (IQN) into FC WWNs

IP Security (IPsec)

IPSec provides the following security features:

- **Data Confidentiality**

  IPsec sender can encrypt packets before transmitting them across a network

- **Data Integrity**

  IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission

- **Data Origin Authentication**

  IPsec receiver can authenticate the source of the IPsec packets sent.

- **Anti-Replay**

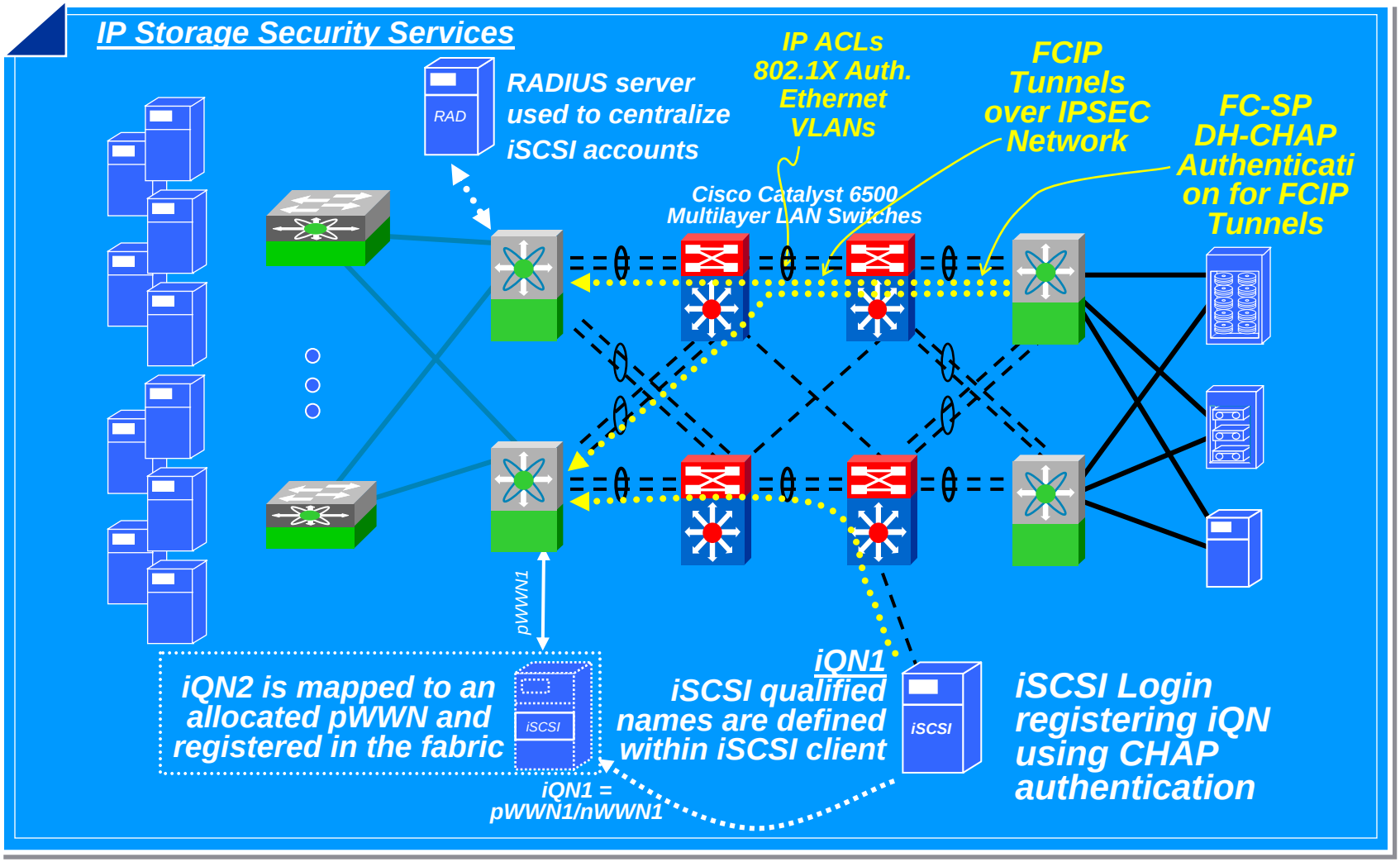
  IPsec receiver can detect and reject replayed packets.

Note: With IPsec, data can be transmitted over a public network without fear of observation, modification or spoofing.

IP Storage Security:
FC-over-IP (FCIP)

- FCIP allows for interconnection of SAN islands via IP networks
  - The FCIP standard doesn't provide for any in-band security mechanisms
  - Per message origin authentication, integrity, anti-replay protection, and privacy are provided, where required, by independent IPsec tunnels
- FCIP tunnel is a virtual ISL—can leverage existing FC Fabric security mechanisms
  - FC Port Security
  - FC-based FC-SP DH-CHAP switch-to-switch authentication – FC-SP used to authenticate remote FCIP tunnel endpoint

IP Storage Security



SECURING STORAGE **MANAGEMENT**

Securing Storage Management

Storage Management Security Includes

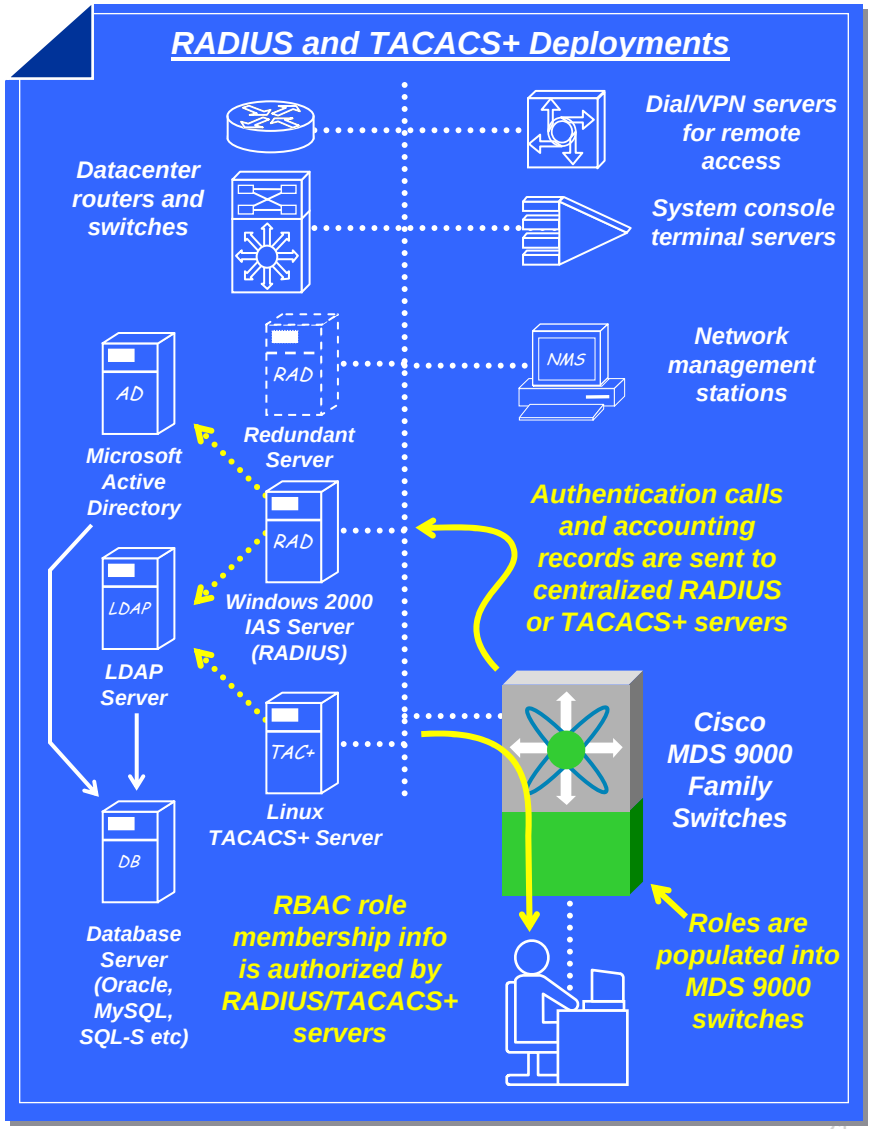
- Authentication, Authorization and Accounting (AAA) of management actions
  - RADIUS/TACACS+
  - SNMP Traps
  - Syslog
  - CallHome (SMTP)
- Role-based management access control
- Secure transport of management actions

  SSH, SNMPv3, SSL/TLS
- Access control to management interfaces

  Secure design of the network management module
- Consistent Security Policy across all devices

Storage Management Security:
Centralized Authentication, Authorization and Accounting (AAA)

- RADIUS—Remote Authentication Dial In User Service (IETF RFC 2865 standard)
- Initially used for dial-in networks—now greatly expanded to a variety of uses
  - System user account centralized authentication
  - Network device user account AAA services
  - Dial-in/VPN service AAA services
  - iSCSI host authentication
- Many different RADIUS servers available
  - Cisco SecureACS
  - UNIX—FreeRADIUS—www.freeradius.org
  - Windows—IAS Server—in Windows 2000/2003
- TACACS+—
  - Cisco SecureACS
  - Widely used and supported by Cisco
  - Freely available from Cisco—similar to RADIUS



Storage Management Security:
Centralized Accounting

- The following example shows a snapshot of a Microsoft IAS RADIUS record generated during an MDS 9509 CLI session
- 'start/stop' records are recorded by default, 'accounting' records of actual commands are enabled on the MDS 9000 as an option
- Similar record generated by TACACS+

NAS-IP-Address	: 172.19.48.87
User-Name	: **tnosella**
Record-Date	: 10/22/2003
Record-Time	: 11:51:08
Service-Name	: IAS
Computer-Name	: IBM305S1
NAS-Identifier	: **login**
NAS-Port-Type	: Virtual
NAS-Port	: 3001
Service-Type	: **Authenticate-Only**
Calling-Station-Id	: **sjc-1.cisco.com**
Client-IP-Address	: **172.19.48.87**
Client-Vendor	: **CISCO**
Client-Friendly-Name	: **core3**
SAM-Account-Name	: IBM305S1\tnosella
Fully-Qualified-Name	: **IBM305S1\tnosella**
Authentication-Type	: **PAP**
Class	: 311 1 172.19.48.54 10/22/2003 18:44:03 1
Packet-Type	: **Access-Request**
Reason-Code	: **The operation completed successfully.**

Decoded Microsoft IAS Radius accounting record using Microsoft's 'iasparse.exe' support tool (part of Windows 2000/2003 distribution)

Full RADIUS Accounting Record

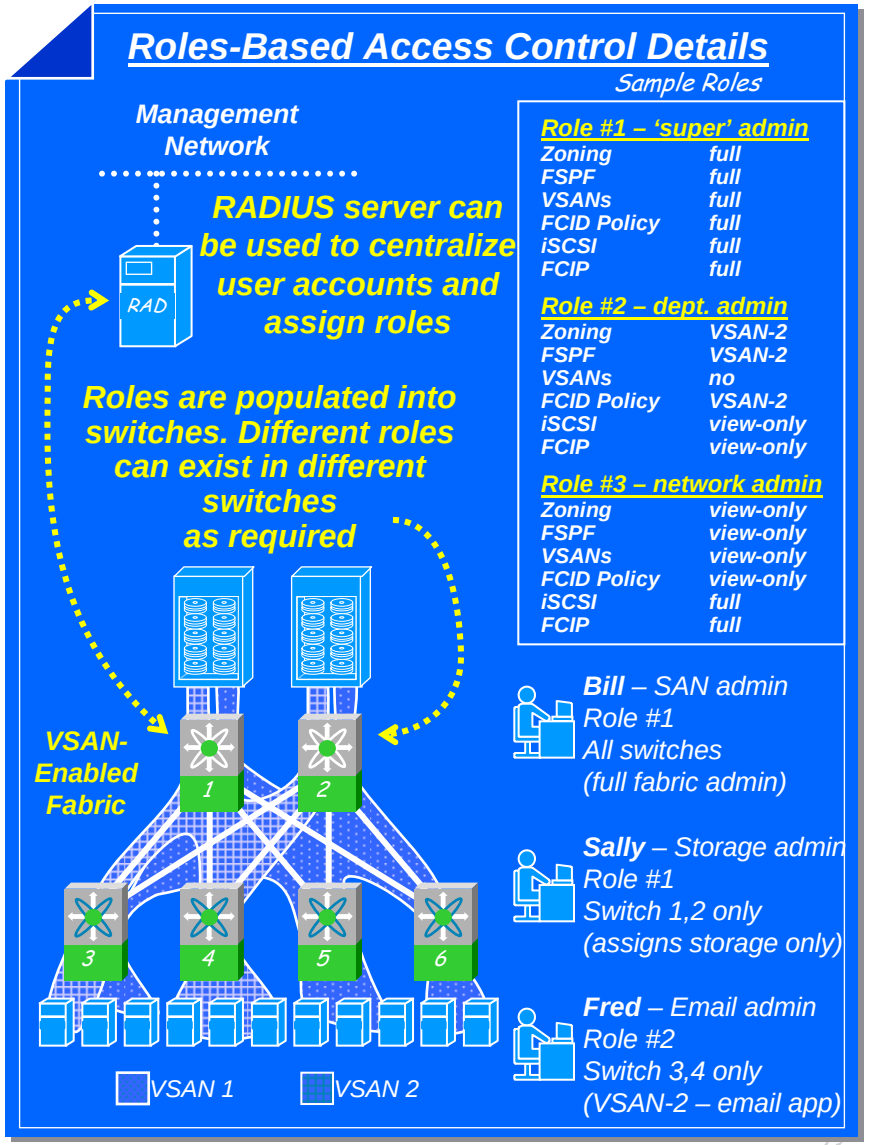
*172.19.48.87,tnosella,10/22/2003,11:51:08,IAS,IBM305S1,32,**login**,61,5,5,3001,6,8,31,**sjc-1.cisco.com**,4108,**172.19.48.87**,4116,*
*9,4128,**core3**,4129,IBM305S1\tnosella,4130,IBM305S1\tnosella,4127,1,25,311 1 172.19.48.54 10/22/2003 18:44:03 1,4136,1,4142,0*

*172.19.48.87,tnosella,10/22/2003,11:51:08,…,**shell:roles=network-admin**,**MDS Policy**,172.19.48.87,core3,IBM305S1\tnosella,…*
*172.19.48.87,tnosella,10/22/2003,11:51:34,…,accounting:accountinginfo=**vsan:4001 values updated interoperability mode:1**,…*
*172.19.48.87,tnosella,10/22/2003,11:51:56,…,accounting:accountinginfo=**vsan:4001 values updated loadbalancing:src-id/dst-id/oxid**,…*
*172.19.48.87,tnosella,10/22/2003,11:52:02,…,accounting:accountinginfo=**Interface fc3/1 admin state updated to down**,…*
*172.19.48.87,tnosella,10/22/2003,11:52:05,…,accounting:accountinginfo=**Interface fc3/1 admin state updated to up**,…*
*172.19.48.87,tnosella,10/22/2003,11:52:16,…,accounting:accountinginfo=**vsan:4001 deleted**,…*
*172.19.48.87,tnosella,10/22/2003,11:52:20,…,accounting:accountinginfo=**vsan:4000 deleted**,…*
*172.19.48.87,tnosella,10/22/2003,11:52:23,…,accounting:accountinginfo=**shell terminated**,…*

Some of these records have been shortened to fit them on this slide '…'

Storage Management Security:
Role-Based Access Control (RBAC)

- Partitioning management capabilities
  - Different roles for different user profiles (sys admin, network admin, super admin, etc)
- Integrated Roles-Based-Access-Control
  - Assign subsets of full command set to roles
  - Users are then assigned to roles
  - May have a maximum of 64 unique roles
  - Roles include IP storage features (iSCSI/FCIP)
  - Commands not visible if not part of assigned role
- VSAN-based RBAC
  - Roles can be assigned to specific VSAN(s) only
  - Enables administrator-per-VSAN model
  - Reduce infrastructure costs through consolidation using VSANs and still delegate fabric 'island' administration



Storage Management Security:
Secure Management Transport

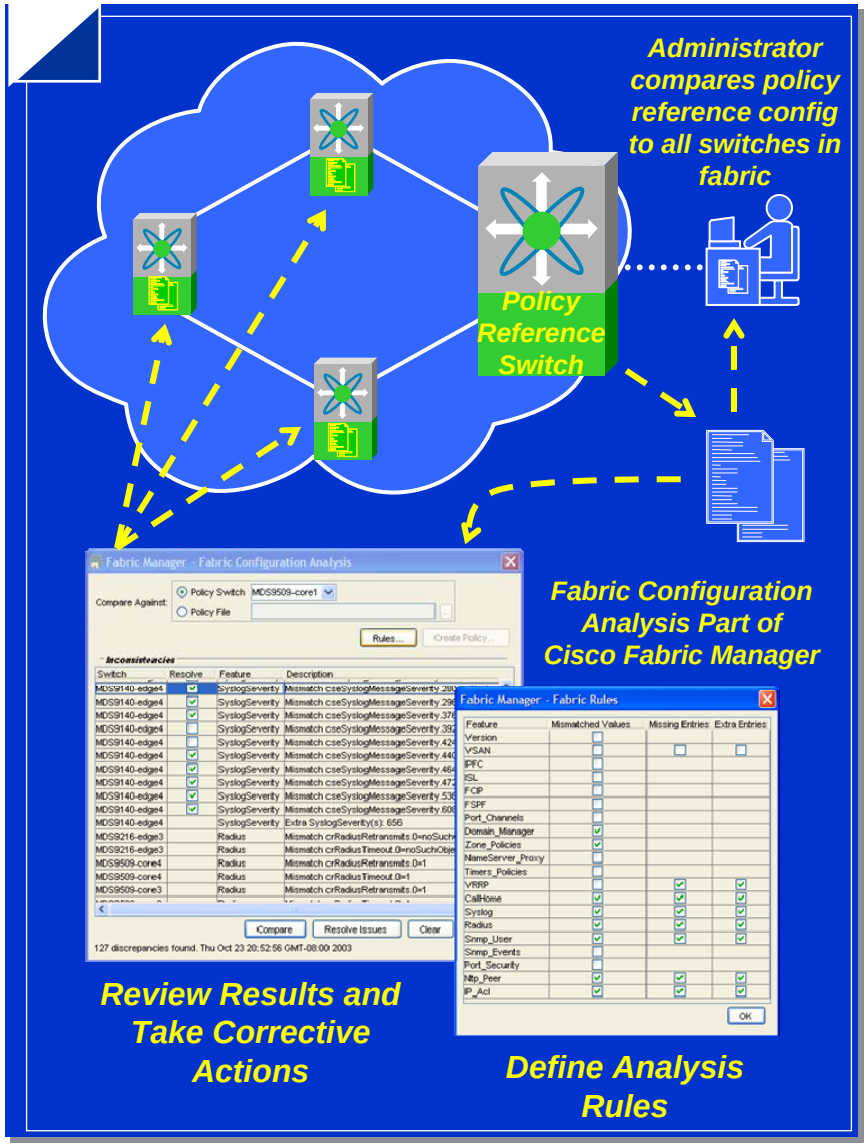
- Telnet to a storage device, as well as transfer of configuration files via FTP or TFTP, over an un-trusted network should be avoided
  - Authentication passwords are sent in clear over the network
  - No authentication at all is provided in the case of TFTP
  - An attacker can easily gain access to the device simply sniffing the un-trusted network
- Secure Shell (SSH) or Secure FTP (SFTP) should be used instead

Storage Management Security:
Secure Management Transport

- Simple Network Management Protocol (SNMP) is an application layer protocol for the exchange of management information
  - SNMPv1 and SNMPv2 should be avoided
    - Since they provides a weak form of authentication, based on a simple community string match
- SNMPv3 should be deployed instead, since it provides
  - User-based authentication
  - Group (roles)-based access control
  - Per-message origin authentication, integrity, anti-replay protection, and privacy

Storage Management Security:
Ensuring a Consistent Security Policy

- Its important to keep consistent configurations across all switches
  - Especially important for security features
    - RADIUS/TACACS+ config
    - Remote SYSLOG config
    - NTP config
    - SNMP communities config
    - Authentication config
    - Roles config
- MDS 9000 Family configurations can be extracted from switches as a flat text file
  - Allows for easy and regular archiving
- Cisco Fabric Manager provides "Fabric Configuration Analysis" tool
  - Checks all switch configurations against policy switch or file
  - Can take corrective action as necessary to fix configurations
  - Also has 'zone merge analysis' tool to validate zone merge validity



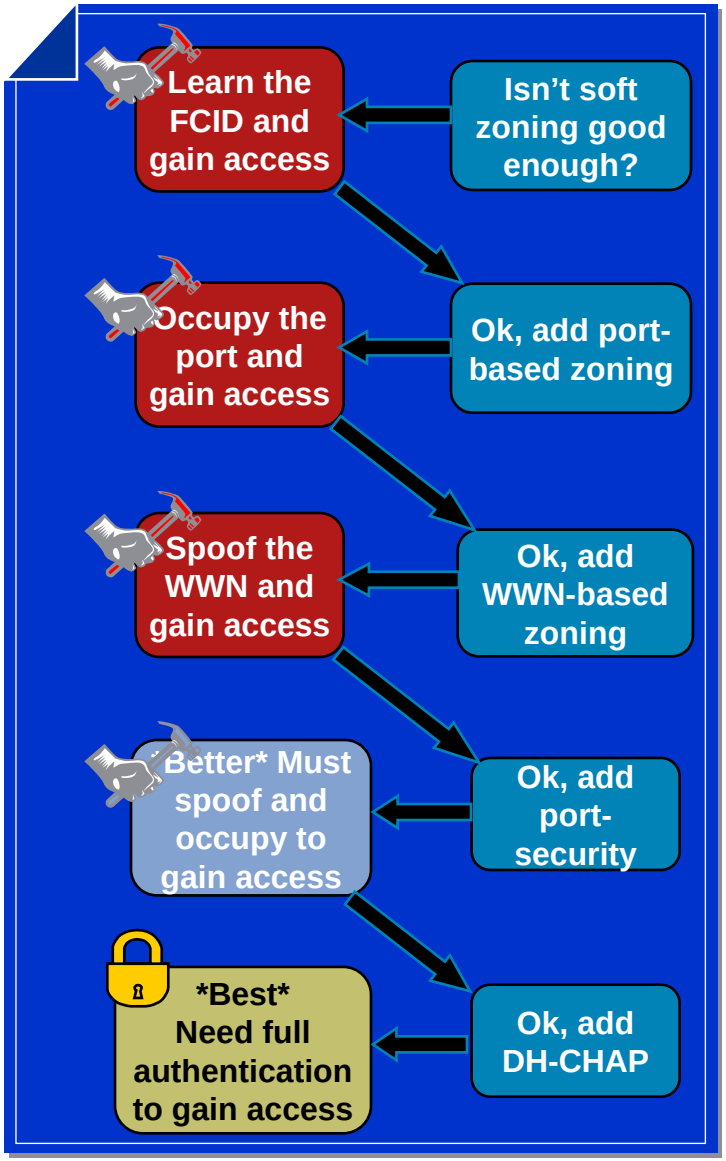
Best Practices

Fabric Access Recommendations

1. Use IP ACLs on management interfaces to block unused services
   - Enable logging of denied attempts—block denial-of-service attacks
2. Hard-fix switch port administrative modes to assigned port function
   - Lock (E)ISL ports to only be (T)E_Ports—set to ‘E_Port’ mode
   - Lock access ports to only be F(L)_Ports—set to ‘Fx_Port’ mode
3. Use VSANs to isolate departments
   - Provides security AND availability benefits
   - RBAC management control per VSAN allows individual admin assignment
4. Use port security features everywhere
   - Bind devices to switch as a minimum level of security
   - Bind devices to a port as an optimal configuration
     - Consider binding to line card in case of port failure
   - Bind switches together at ISL ports—bind to specific port, not just switch
5. Use FC-SP authentication for switch-to-switch fabric access
   1. Use device-to-switch when available

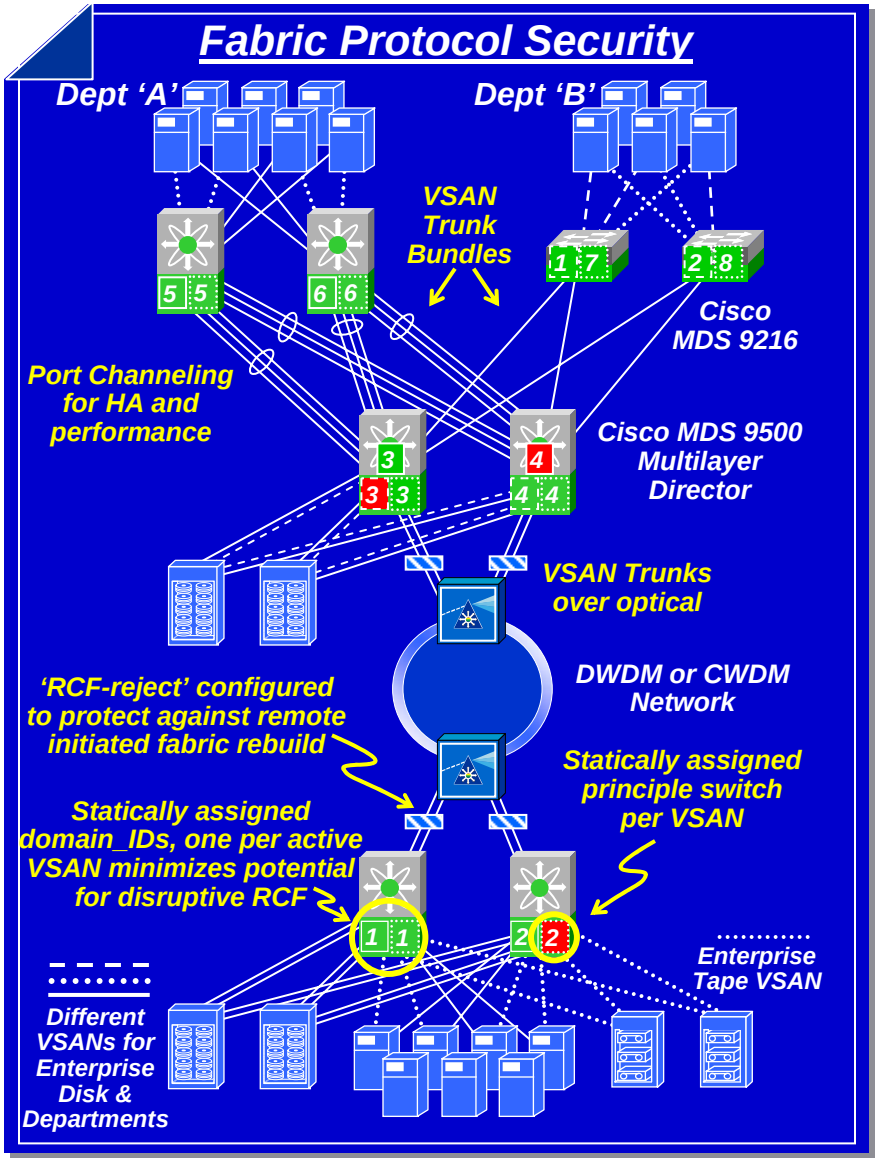
Target Access Recommendations

- Use zoning services to isolate where required
  - Port or WWN-based, all hardware enforced
  - Use read-only zones for read-only targets
  - Use LUN zoning as extra reinforcement
  - Set default-zone policies to ‘deny’
- Suggested to only allow zoning configuration from one or two switches to minimize access
  - Use RBAC to create two roles, only one allowing zoning configuration
  - Install ‘permit’ role on two switches, ‘deny’ role on remainder
  - Or, use RADIUS or TACACS+ to assign roles based on particular switch, more flexible
- Use WWN-based zoning for convenience and use port-security features to harden switch access



SAN Fabric Protocol Security

- Very important to secure the fabric control protocols to ensure fabric stability
  - Securing access to control protocol configuration via Cisco RBAC is first step
  - Enable port-security for locking of ISL ports
  - Using FC-SP for switch-to-switch authentication is next critical step to block rogue ISLs
- Plug-n-play fabric protocol configuration is convenient—however **static configuration** is more secure
  - Configure static principle switch
  - Enable static domain IDs
  - Enable static FCIDs
    optional but recommended
    Great benefit for HP/UX and AIX environments
  - Enable RCF-reject, especially on long-haul links
  - Enable RSCN-suppression where necessary
- Use VSANs to divide and manage individual fabric configuration and resiliency

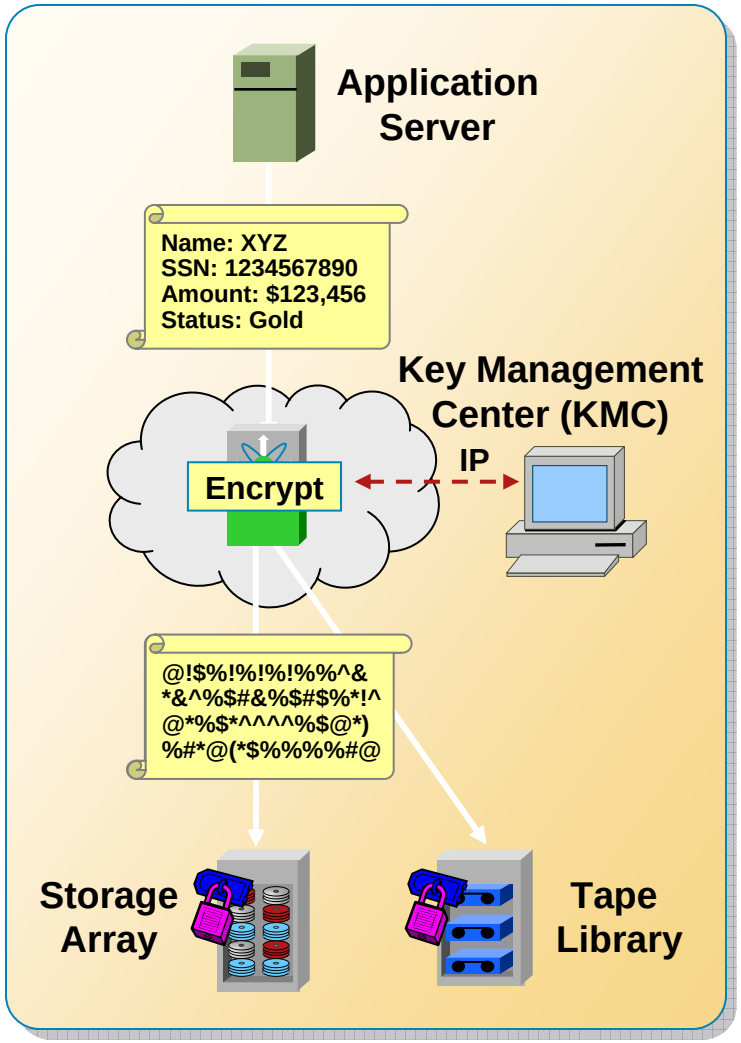


SAN Management Recommendations

1. Use RBAC capability to grant adequate privilege to SAN administrators
   - Example: Not every administrator needs capability to disable modules
   - Reserve select functions to fewer ‘super-admin’ RBAC role
     - VSAN DEFINITION, FIRMWARE UPGRADES, ROLES DEFINITION, RADIUS CONFIGURATION, SSH CONFIGURATION, ETC.
2. Use RADIUS or TACACS+ for centralized user account administration
   - Ensures consistent and timely removal of users if required
   - Use RADIUS accounting feature for audit log of configuration events
3. Use all secure forms of management protocols—disable others
   - SSH, SFTP, SCP, SNMPV3, SSL FOR SMI-S SUPPORT
   - DISABLE TELNET, FTP, TFTP, SNMPV1,V2
4. Enable NTP across all switches for consistent time stamping of events
5. Log and archive everything
   - Enable centralized SYSLOG
   - Take regular copies of MDS 9000 configurations (can use CiscoWorks RME)
   - Turn on Cisco MDS 9000 “Call Home” feature to alert of anomalies

Cisco MDS
New Features

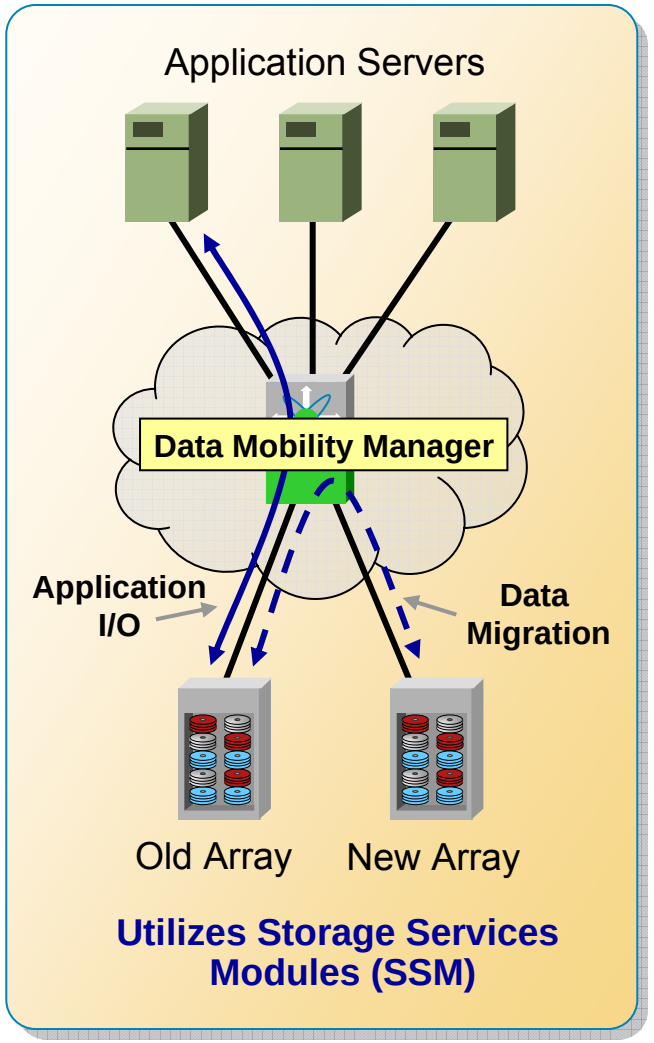
SME – Overview



- Encrypts storage media (data at rest)
  - Strong, Std. IEEE AES-256 encryption
  - Integrates as transparent fabric service
  - Encrypts traffic from any VSAN
- Supports heterogeneous tape devices (now), VTLs (now) and storage arrays (future)
- KMC offers secure, comprehensive key management
  - APIs for 3rd party key management
  - Example: RSA's Key Manager 2.1 technology to control access and deployment
- Compresses tape data
- Allows offline, software only media recovery
- FIPS level-3 system architecture
- Non-disruptive deployment
  - No SAN re-configuration or re-wiring to insert appliances
  - Redirects traffic after provisioning encryption (on-line)
  - Allows application I/Os to continue while encrypting existing disk data

Cisco Data Mobility Manager (DMM)

SAN-0S 3.2(1)



- Migrates data between storage arrays for
  - Technology refreshes
  - Workload balancing
  - Storage consolidation
- DMM offers
  - **Online migration of heterogeneous arrays**
  - Simultaneous migration of multiple LUNs
  - Unequal size LUN Migration
  - Rate adjusted migration
  - Verification of migrated data
  - Secure erase
  - Dual fabric support
  - CLI and wizard-based management with Cisco Fabric Manager
- Requires no SAN re-configuration or rewiring

N-Port Identifier Virtualization (NPIV)

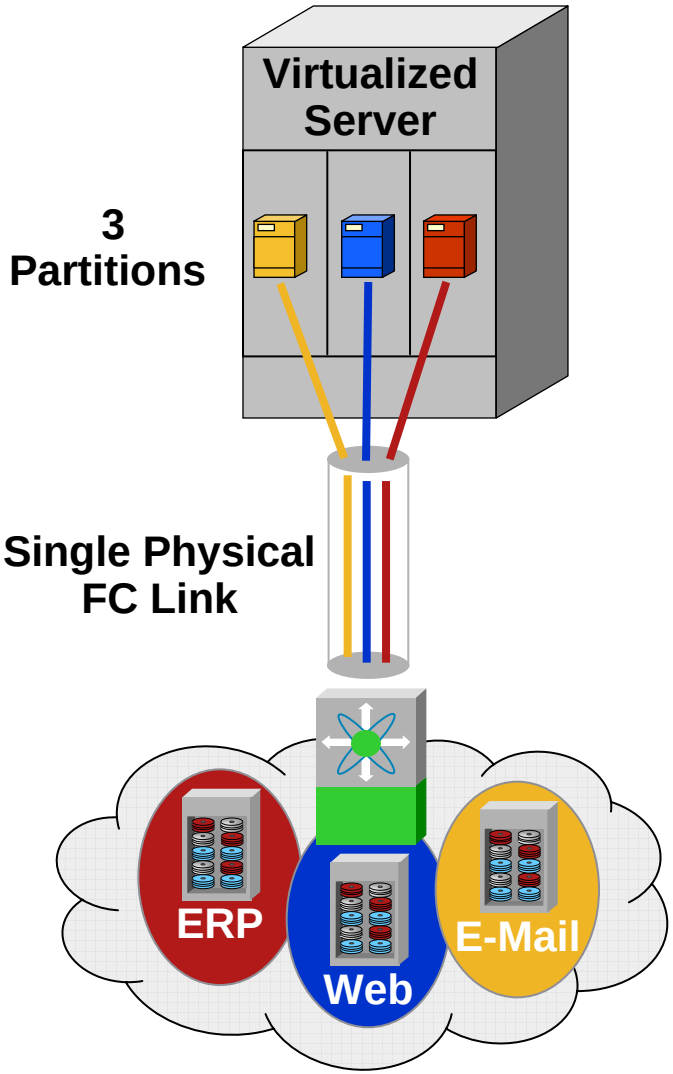
- NPIV is standards-based (T11)
- Allows HBA port sharing between server partitions or virtual machines (VM)

  Allow multiple FCIDs to a single N port
- Separate fabric log-in by server partitions or VM enables application level

  Zoning

  Security

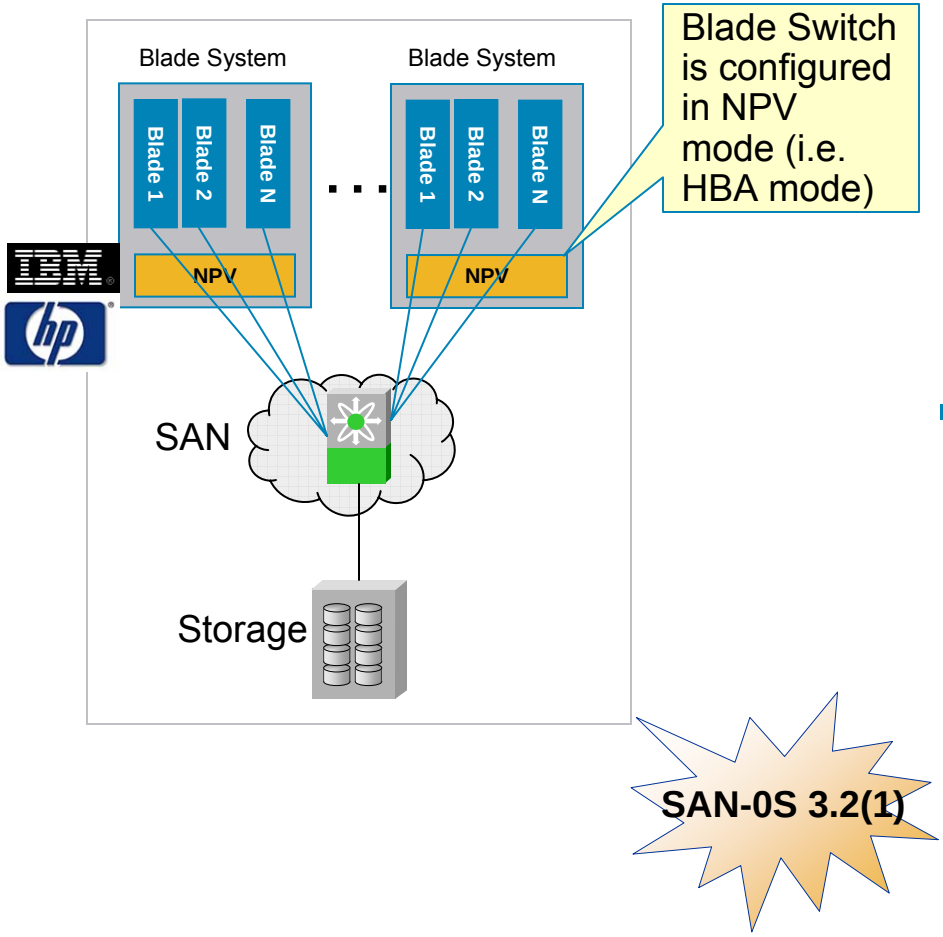
  Traffic mgmt (e.g. QoS)



SAN-0S 3.0

N-Port Virtualization (NPV)
Enabling Large-Scale Blade Server Deployments

Blade Switch Deployment Model – NPV Mode

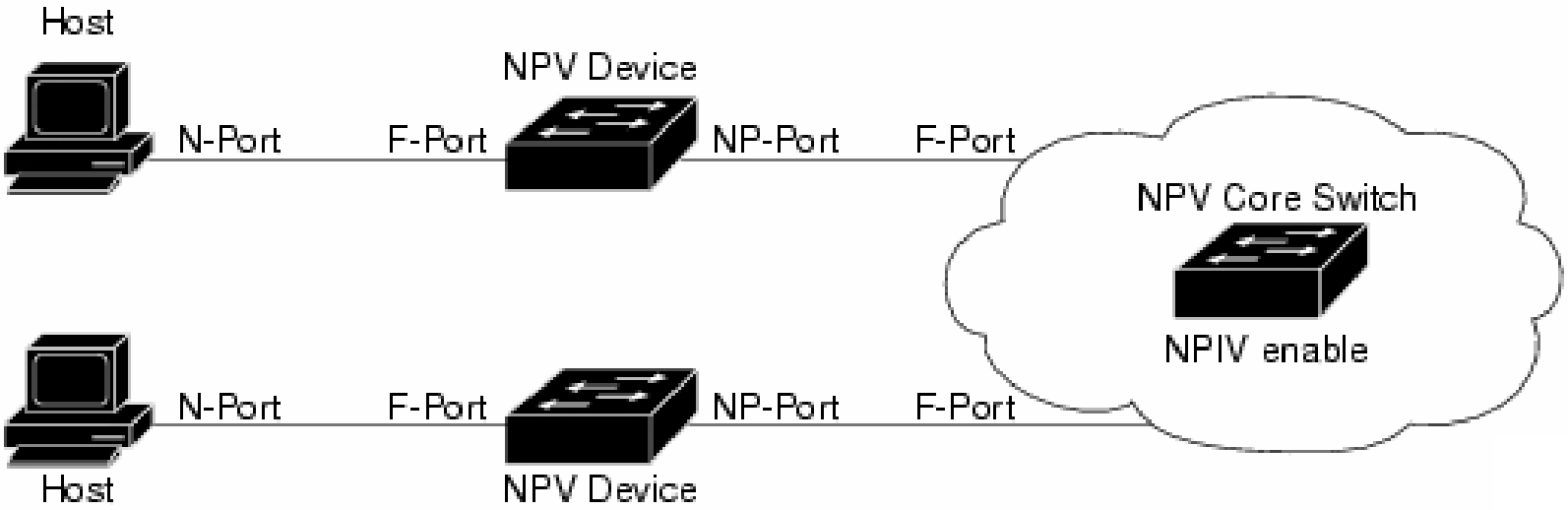


- NPV **simplifies** large scale **Blade Server** deployments:
  - **Reduces # of Domain IDs**
  - Minimizes interoperability issues with core SAN switches
  - Minimizes coordination between Server and SAN administrators
- **Blade Switch in NPV mode** operates as **"FC Switch" to a "FC HBA"**
  - No local switching
  - No Trunking or Port-Channeling
  - No QoS

Cisco NPV Fabric Configuration Example

NPV aggregates multiple local N ports into one or more external NP links.

Blade switches operating in NPV mode do not join fabric – they pass traffic between core switch links and end devices.

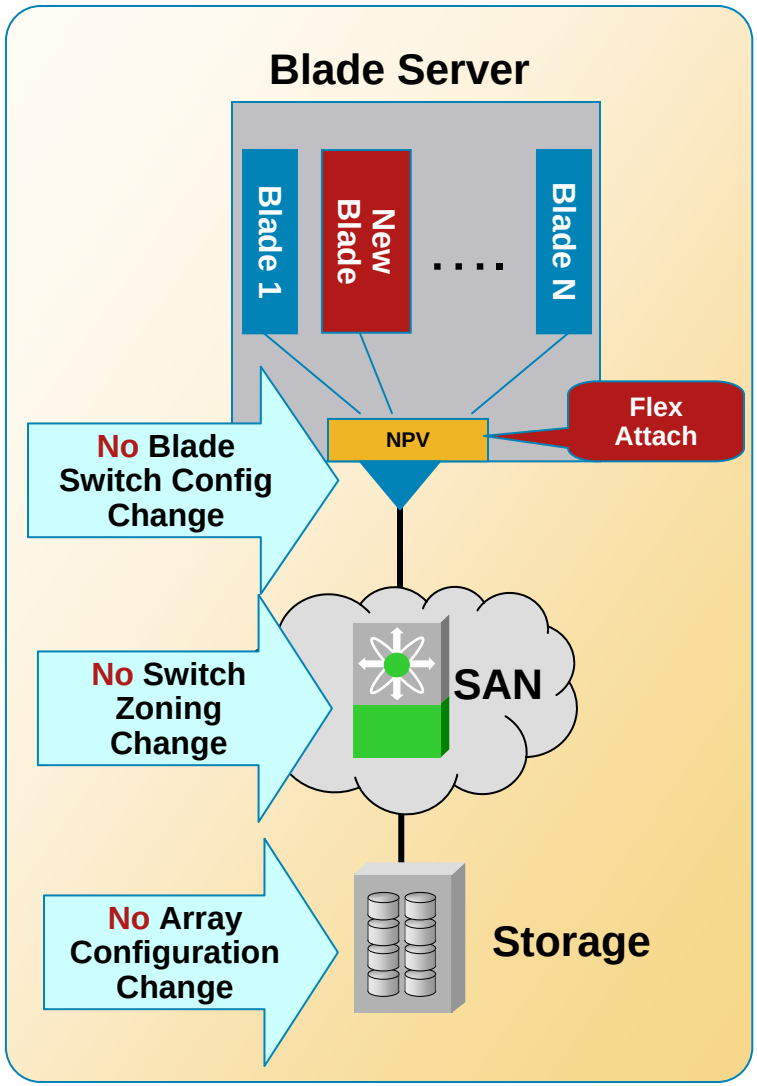


Terms:

•*NP port (proxy N port)* - port on device in NPV mode and connected to the NPV core switch using an F port; behave like N ports and also function as proxies for multiple, physical N ports.

•*NP Links* - NPIV uplink to a specific end device, established when the uplink to the NPV core switch comes up .

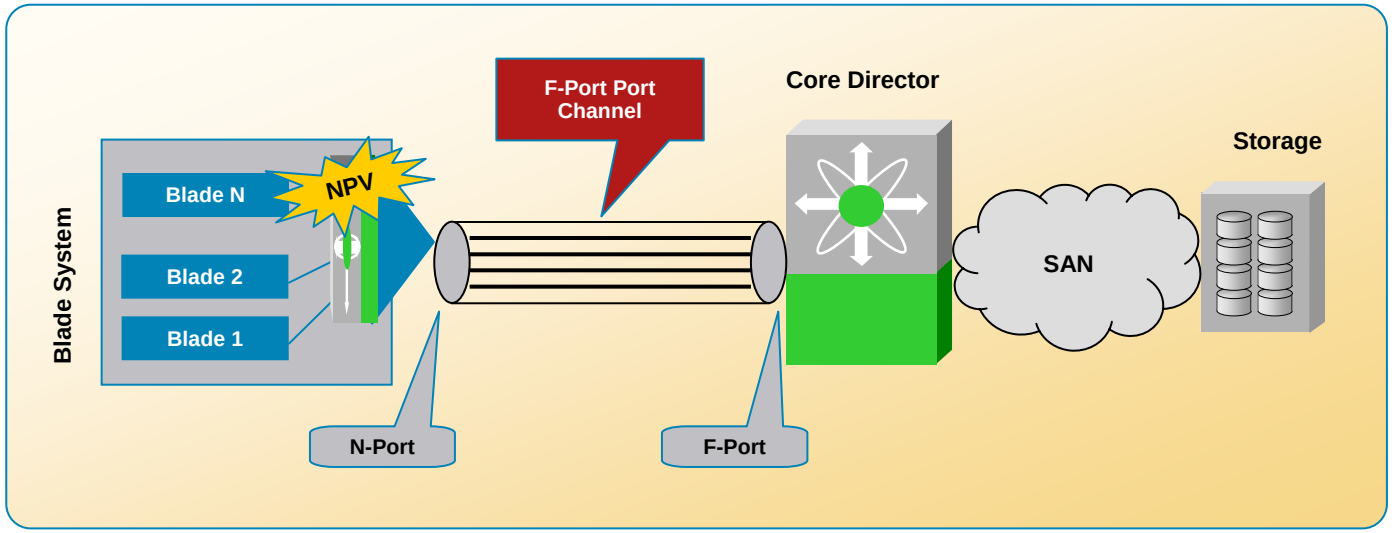
FlexAttach
Flexibility for Adds, Moves, and Changes



- FlexAttach (Based on WWN NAT)
  - Each Blade Switch F-Port assigned a virtual WWN
  - Blade Switch performs NAT operations on real WWN of attached server
- Benefits
  - No SAN re-configuration required when new Blade Server attaches to Blade Switch port
  - Provides flexibility for server administrator, by eliminating need for coordinating change management with networking team
  - Reduces downtime when replacing failed Blade Servers

Enhanced Blade Switch Resiliency

F-Port Port Channel



- F-Port PortChannels
  - Bundle multiple ports in to 1 logical link
  - Any port, any module
- High-Availability (HA)
  - Blade Servers are transparent if a cable, port, or line cards fails
- Traffic Management
  - Higher aggregate bandwidth
  - Hardware-based load balancing

Storage Networking Security Resources

- STANDARDS:
  - http://www.t10.org (SCSI specs)
  - http://www.ietf.org/html.charters/ips-charter.html (IETF ips wg)
  - http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-20.txt (iSCSI)
  - http://www.t11.org (FC-SP specs)
  - ftp://ftp.t11.org/t11/pub/fc/sp/04-112v3.pdf (FC-SP v1.6)
- FORUMS:
  - http://www.snia.org
  - http://www.snia.org/ssif
- WHITEPAPER:
  - ftp://ftp-eng.cisco.com/ltd/mds_security_whitepaper16.pdf