SAN SECURITY OVERVIEW
Session # 8189

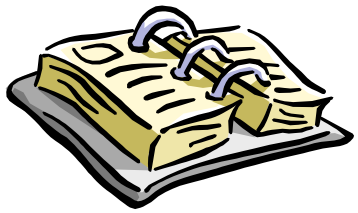
Tony Almeida
Consulting Systems Engineer
Cisco Mainframe Solutions
talmeida@cisco.com

Session 8189 Abstract

Security is a major concern in all aspects of the Enterprise. As the technology continues to evolve, it is important to review all of the technology. SAN Security will be discussed in the following areas: encryption of data in flight, encryption of data at rest, access control security and other areas of potential interest.

Agenda

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- Attacks and Mitigation
- Securing Data at Rest
- References



SCOPE OF STORAGE SECURITY

Why Is SAN Security Important?

- Governments have enacted a variety of strict security regulations mandating the privacy and integrity of sensitive customer and corporate data
  - Health Insurance Portability and Accountability Act (HIPPA)
  - Gramm-Leach-Blilely Act (GLBA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Sarbanes-Oxley Act (SOx)
  - European Privacy Directive
  - CA SB1386
- Many of the regulations and legislation require 'countermeasures against internal and external threats'

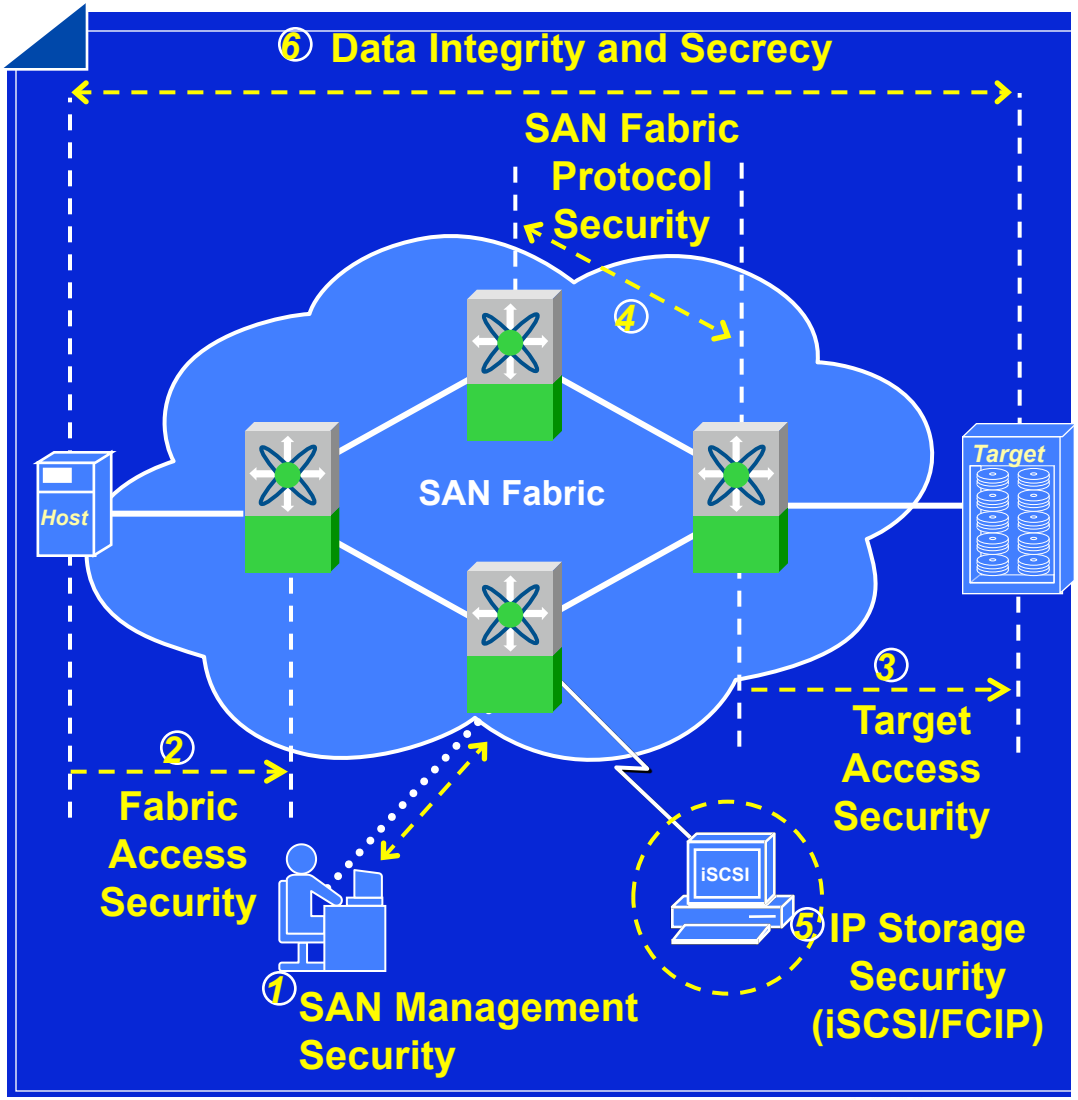
SAN Security
Several Threats—Few Solutions

- SAN security is commonly overlooked with most focus on Application integrity/LAN/Internet/Intranet
- 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-at-rest encryption, data-in-flight, LUN security
  - Datacenter physical security
  - Management
- SAN Security is only as good as the weakest link

STORAGE SECURITY ARCHITECTURE

Storage Security Architecture

- Fabric security augments overall application security
  - Not sufficient on its own—host and disk security also required
- Six key areas of focus
  1. SAN Management Access—secure access to management services
  2. Fabric Access—secure device access to fabric service
  3. Target Access—secure access to targets and LUNs
  4. SAN Protocol—secure switch-to-switch communication protocols
  5. IP Storage Access—secure FCIP and iSCSI services
  6. Data Integrity and Secrecy—Encryption of data both in transit and at rest



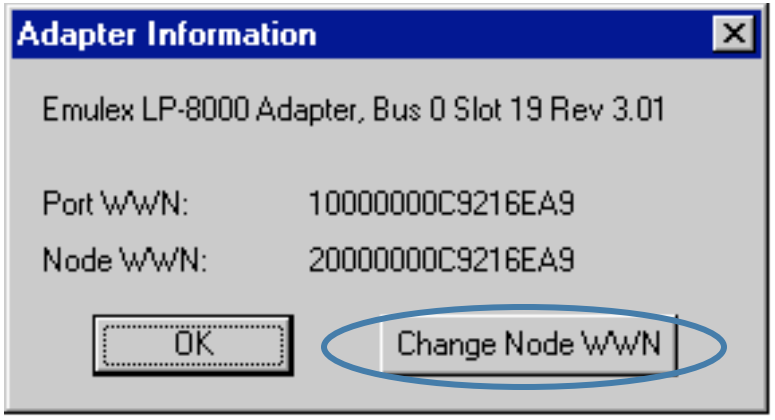
SECURING THE STORAGE LAYER – FIBRE CHANNEL

Securing Fibre Channel

- ✓ **'FC Zoning'** introduced to provide segregation between 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



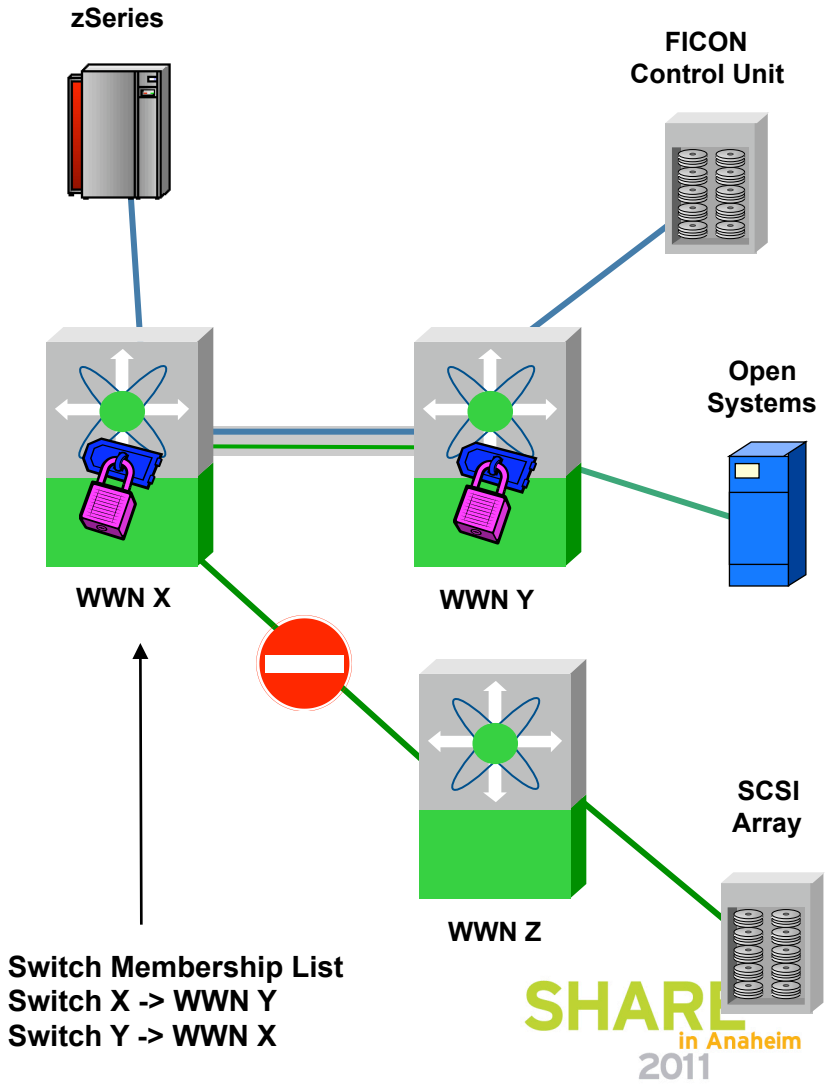
http://www.emulex.com/ts/fc/docs/wnt2k/2.00/pu.htm

Securing FICON

- ✓ '**Fabric Binding**' necessary for cascaded directors, keeps out unauthorized switches
- ✓ '**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) can be used to keep different workloads apart, or to segregate FICON and Open Systems
- ✓ **Roles Based Access Controls** can be used to defined different administrative functions to a specific Virtual SAN

Fabric Binding for Enhanced Cascading Security

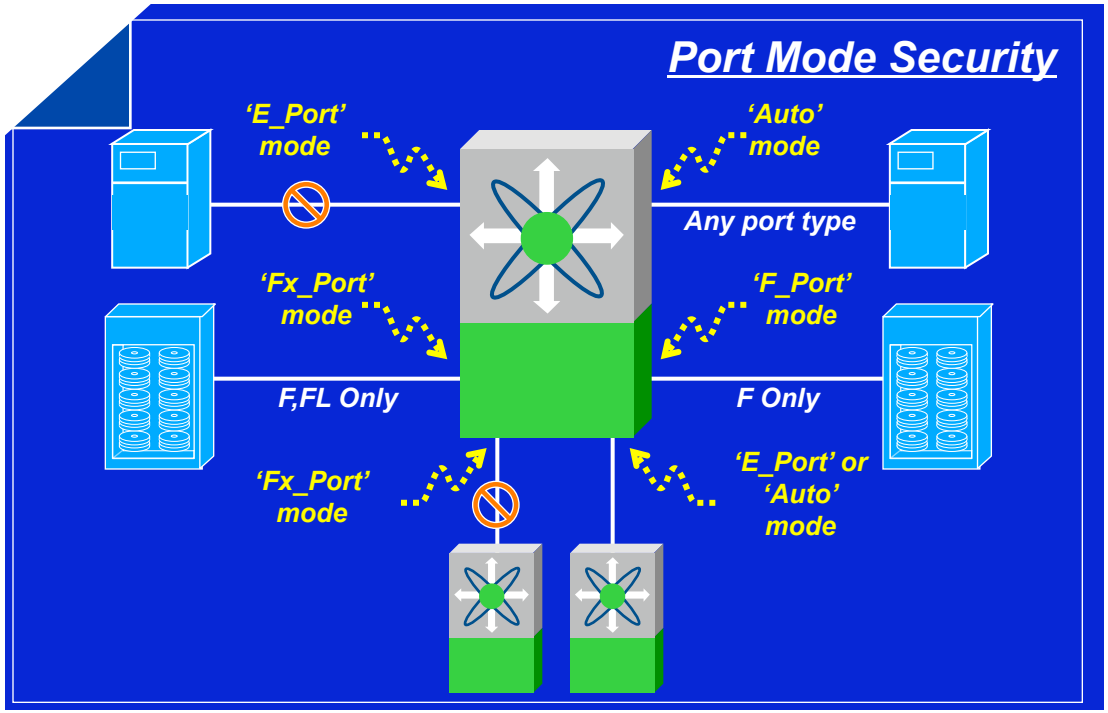
- Two Switches / One Hop
- Based on Switch WWNs
- Only authorized switches can connect to a secure fabric
  - Unauthorized switches result in attachment port being placed in 'Invalid Attachment' state
  - Query Security Attributes and Exchange Security Attributes ensure compliance
- Predictable error recovery
- Requires Insistent (static) Domain IDs



Fabric Access Security:
Port Mode Security

- **Port mode security**: Only allow edge ports to form F_Ports or FL_Ports only, ie. No ISL/EISL

- Cisco MDS 9000 Family supports an *Fx_Port* mode which allows F_Port or FL_Port only
- Limit users who can change port mode via Roles-Based Access Control assignments



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

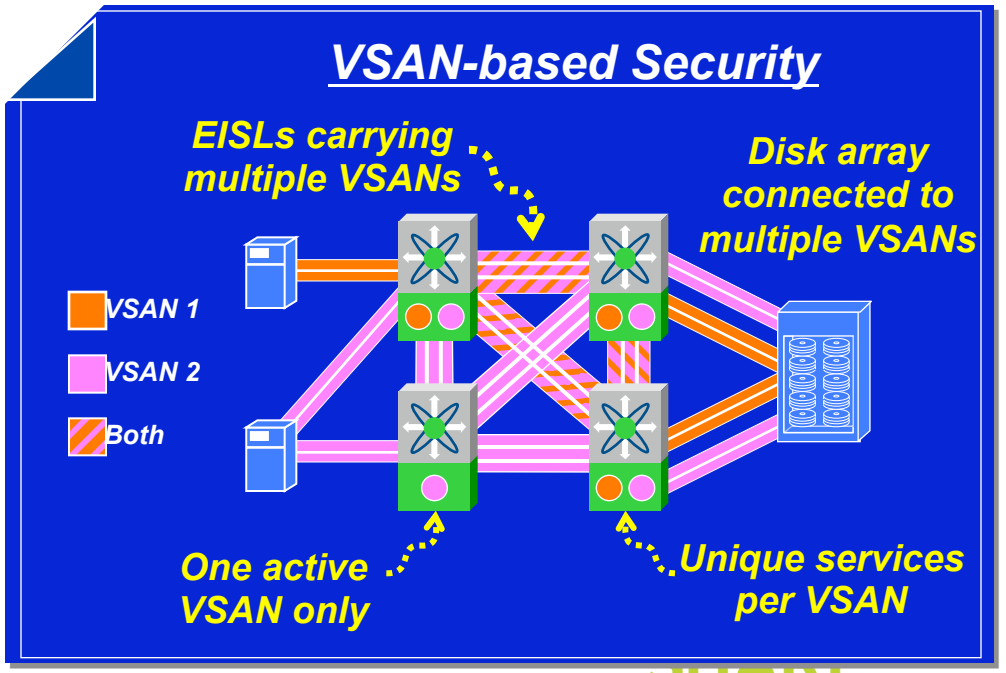
Per-VSAN fabric services

Independent fabric services, including nameserver, 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

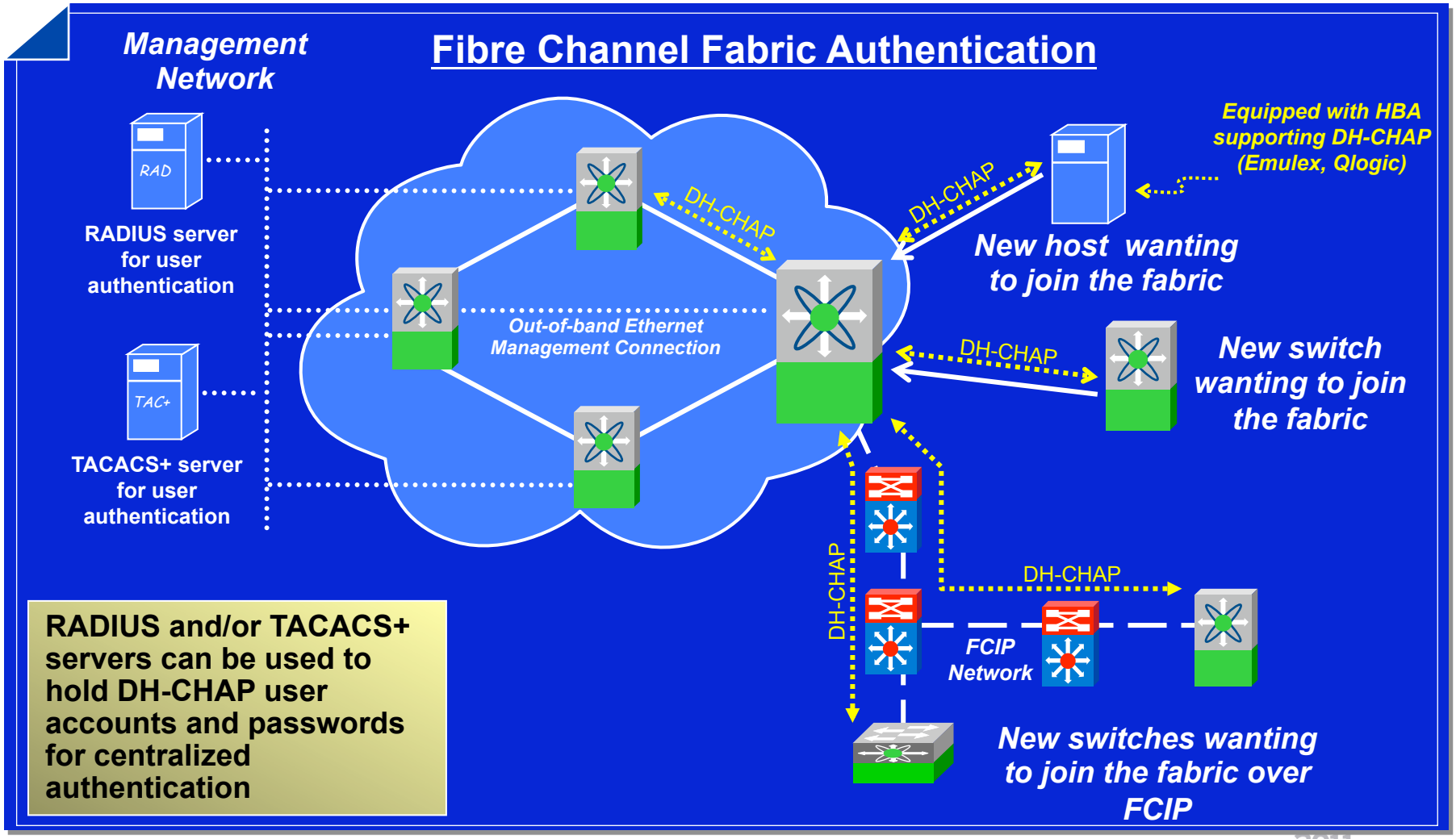
Multiple VSANs can share the same physical topology



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

- Fabric Login (FLOGI) & Port Login (PLOGI) procedures are extended to support authentication
  - Node-to-node (host to disk)
  - Node-to-switch (host/disk to switch)
  - Switch-to-switch
- A common authentication framework supports different mechanisms
  - Password based (DHCHAP or SRP)
  - Certificate based
- A shared key is generated as a by-product of the authentication exchange

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



SECURING STORAGE MANAGEMENT

Securing Storage Management

- Storage Management Security includes
  - Authentication, Authorization and Accounting (AAA) of management actions

    RADIUS/TACACS+ (Native LDAP integration now available)

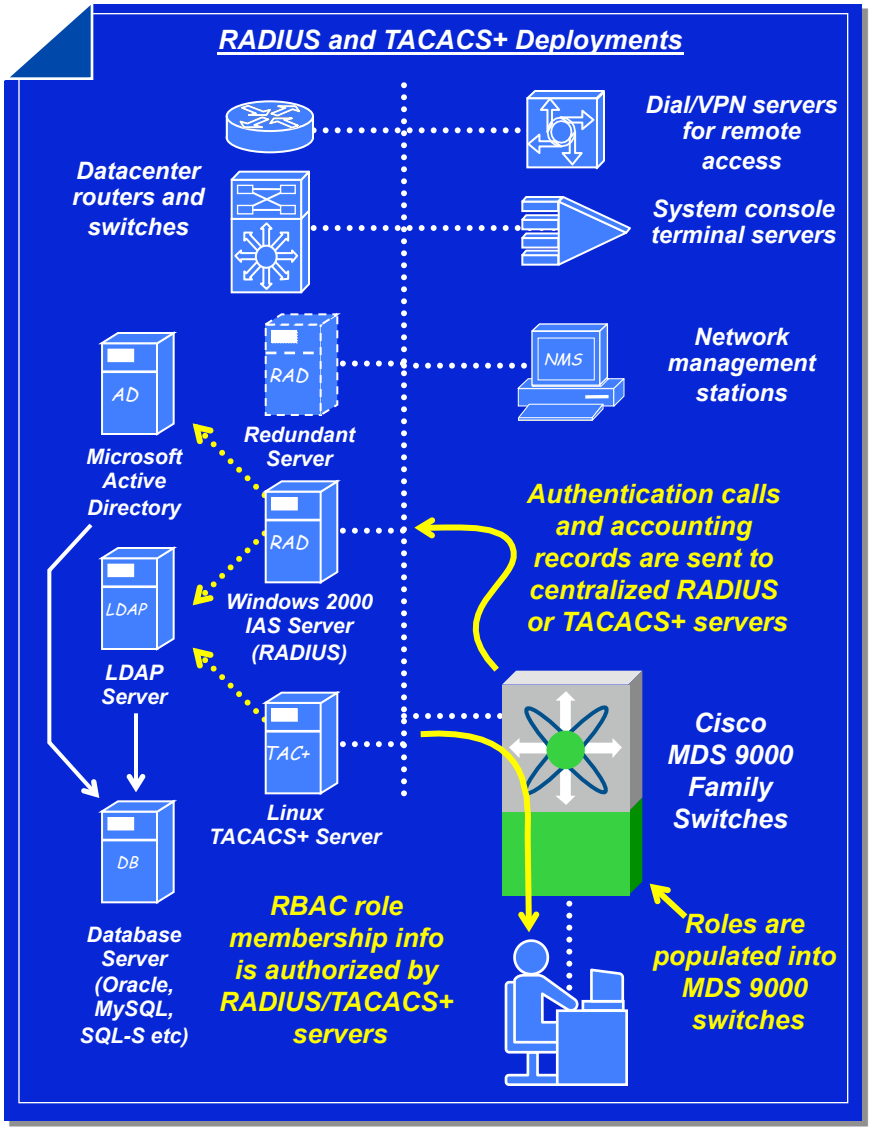
    Syslog

    SNMP Traps

    Call Home (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
  - UNIX: FreeRADIUS www.freeradius.org
  - Windows: IAS Server – in Windows 2000/2003
  - CiscoSecure ACS
- **TACACS+:** (based on RFC 1492 standard)
  - 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

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*

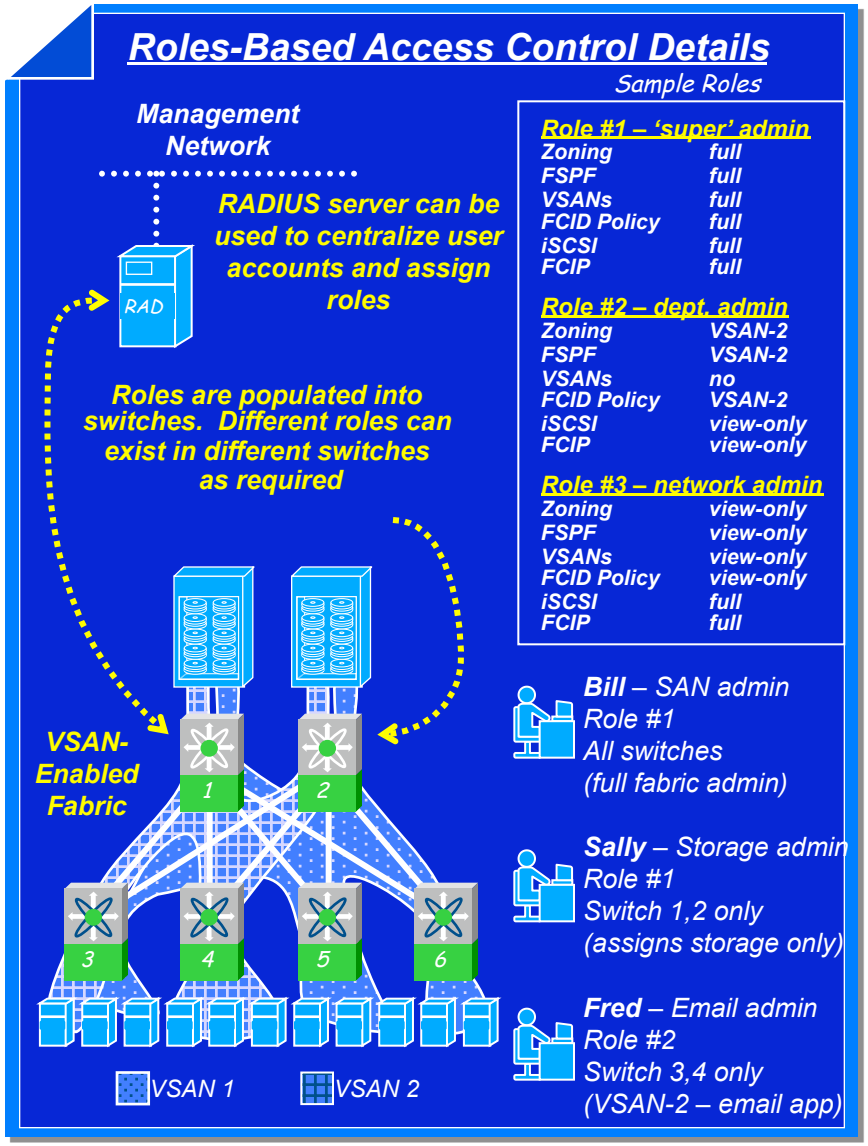
*172.19.48.87,tnosella,10/22/2003,11:51:08,…,**shell:roles=network-admin**,**MDS Policy**,172.19.48.87,core3,IBM305S1\tnosella,…*
*172.19.48.87,tnosella,10/22/2003,11:51:34,…,accounting:accountinginfo=**vsan:4001 values updated interoperability mode:1**,…*
*172.19.48.87,tnosella,10/22/2003,11:51:56,…,accounting:accountinginfo=**vsan:4001 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)

SHARE
Technology · Connections · Results

- **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 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

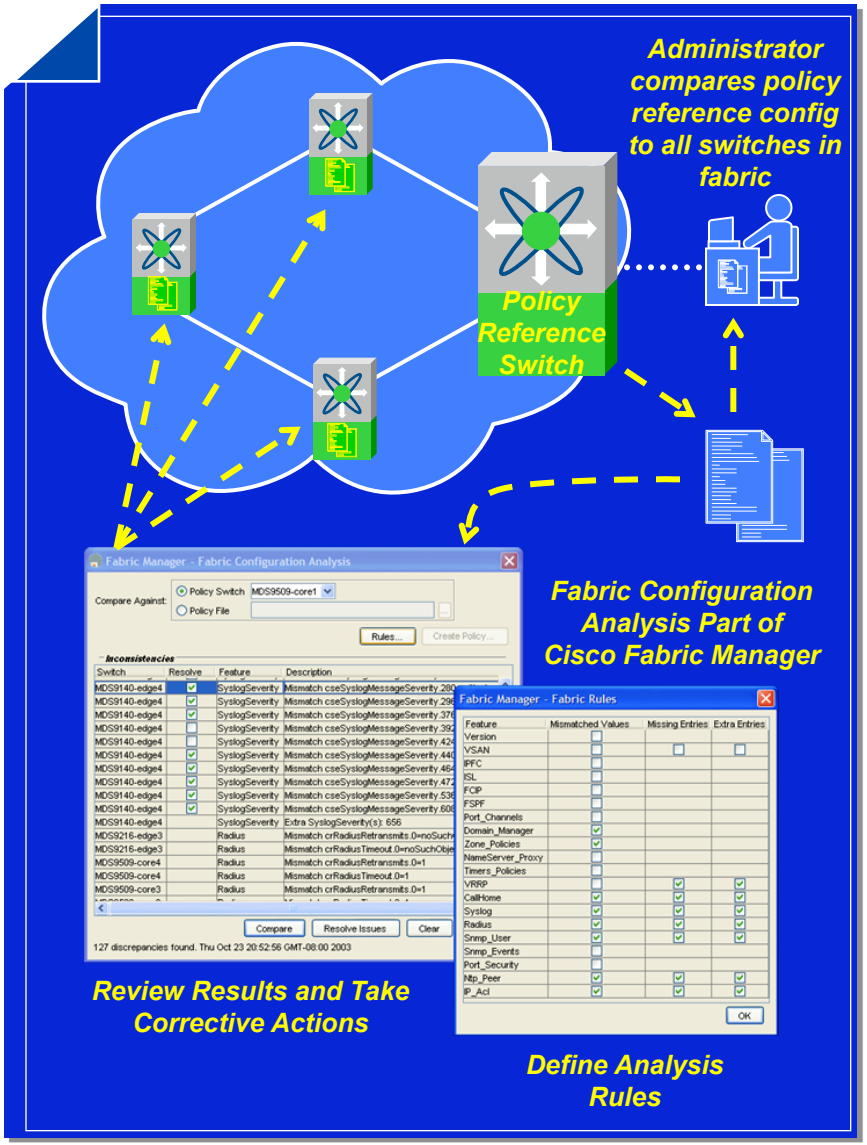
Storage Management Security:
Secure Management Transport

- **Simple Network Management Protocol (SNMP)**
  - An application layer protocol for the exchange of management information
  - SNMPv1 and SNMPv2 should be avoided
    - Both provide 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

SHARE
Technology · Connections · Results

- 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

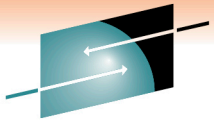


Secure Access to Management Services
Best Design Practices

- Use RBAC capability to grant adequate privilege to SAN administrators
  - Example: Not every administrator needs capability to change zoning
  - Reserve the following functions to fewer ‘super-admin’ RBAC role
    - VSAN definition, firmware upgrades, roles definition, RADIUS configuration, SSH configuration, etc.
- 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
- Use all secure forms of management protocols—disable others
  - SSH, SFTP, SCP, SNMPv3, SSL for SMI-S support
  - Disable Telnet, FTP, TFTP, SNMPv1,v2
- Enable NTP across all switches for consistent time stamping of events

ATTACKS AND MITIGATION

Port Security Best Practices



- Use port mode assignments:
  - Lock (E)ISL ports to E_Port mode
  - Lock access ports to Fx_Port mode
- 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 group of ports in case of port failure
  - Bind switches together at ISL ports – bind to specific port, not just switch
- Use FC-SP authentication for switch-to-switch fabric access:
  - Use device-to-switch when available
- Use unique passwords for each FC-SP connection
- Use RADIUS or TACACS+ for centralized FC-SP password administration

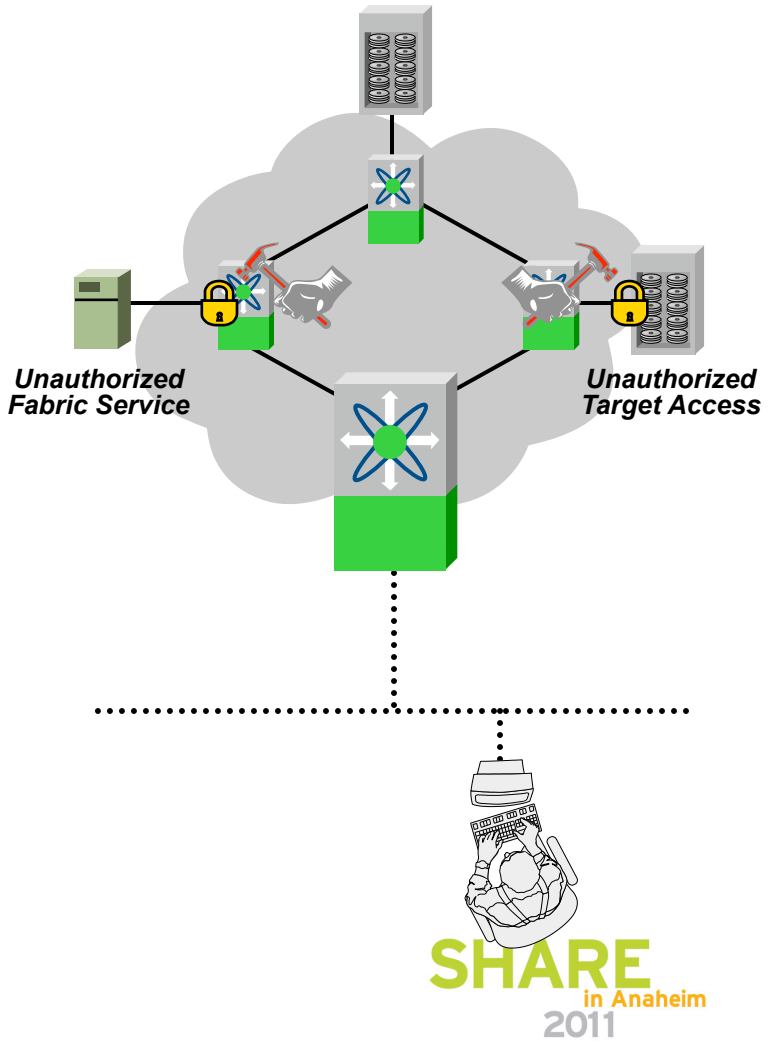
Secure Device Access to Fabric Service
Best Design Practices

- Use IP ACLs on management interfaces to block unused services
  - Enable logging of denied attempts – block denial-of-service attacks
- 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
- Use VSANs to isolate departments
  - Provides security AND availability benefits
  - RBAC management control per VSAN allows individual admin assignment
- 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
- Use FC-SP authentication for switch-to-switch fabric access
  - Use device-to-switch when available

Fabric and Target Access Potential Threats

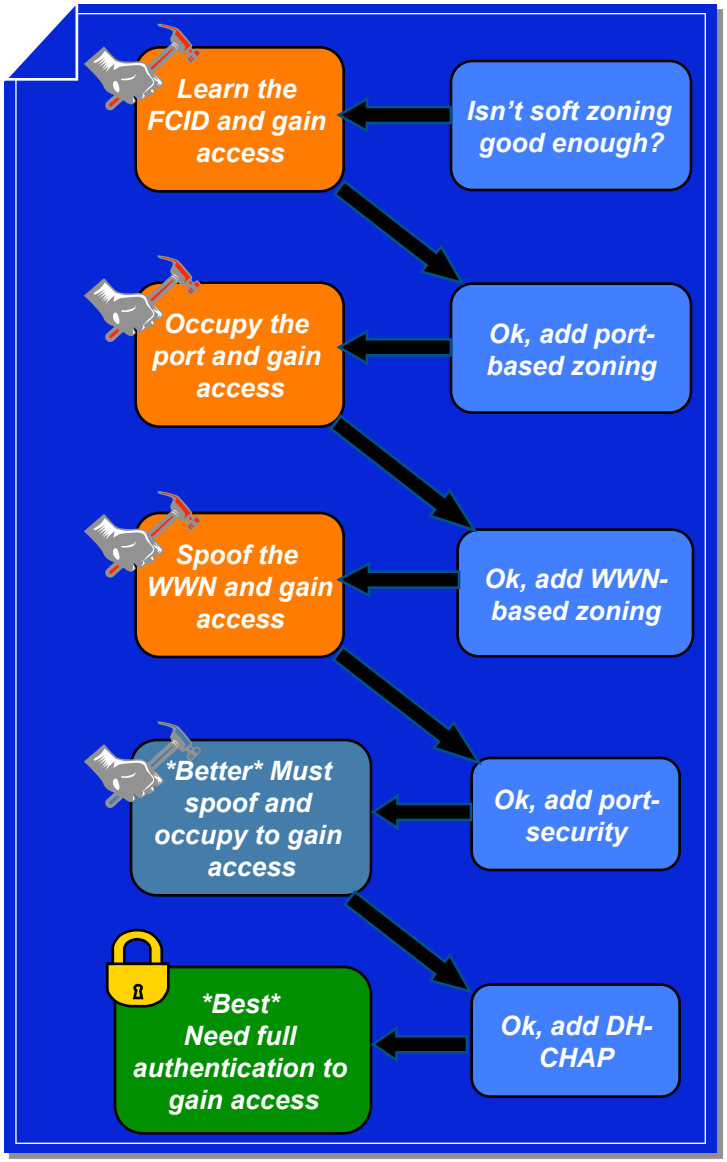
Three main areas of vulnerability

1. Compromised application data
   - Unauthorized access to targets and LUNs
   - High potential for data corruption, loss, or theft
   - Result: Unplanned down time, costly data loss
2. Compromised LUN integrity
   - LUN corruption due to unintentional OS mount
   - Accidental formatting of LUN – loss of data
   - Result: Unplanned down time, costly data loss
3. Compromised application performance
   - Unauthorized I/O potentially causing congestion
   - Injected fabric events causing disruption
   - ie. rogue HBA hammering fabric controller
   - Result: Unplanned down time, poor I/O performance



Target Access Recommendations

1. 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’
2. 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
3. Use WWN-based zoning for convenience and use port-security features to harden switch access

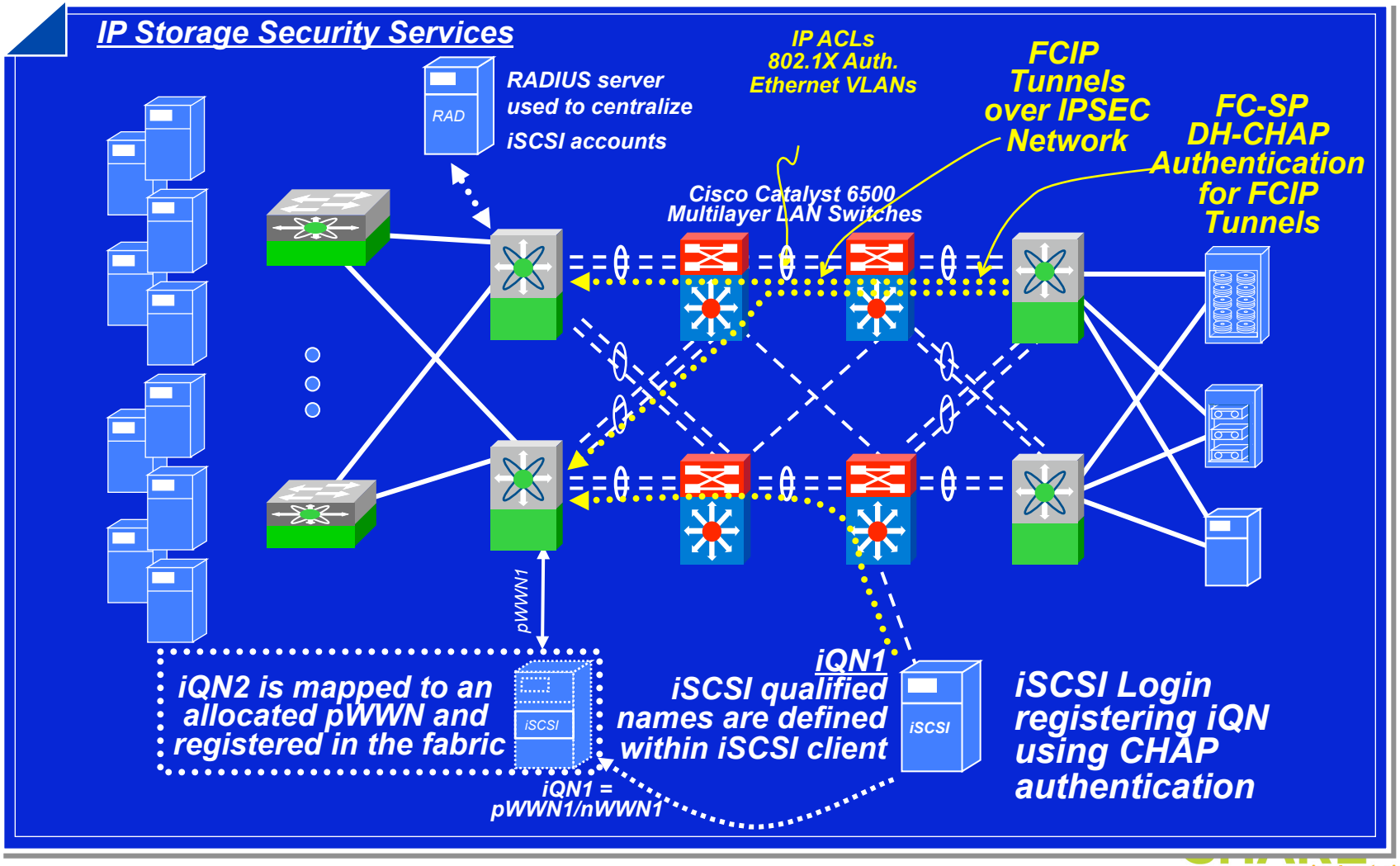


SECURING THE STORAGE LAYER – IP STORAGE (FCIP)

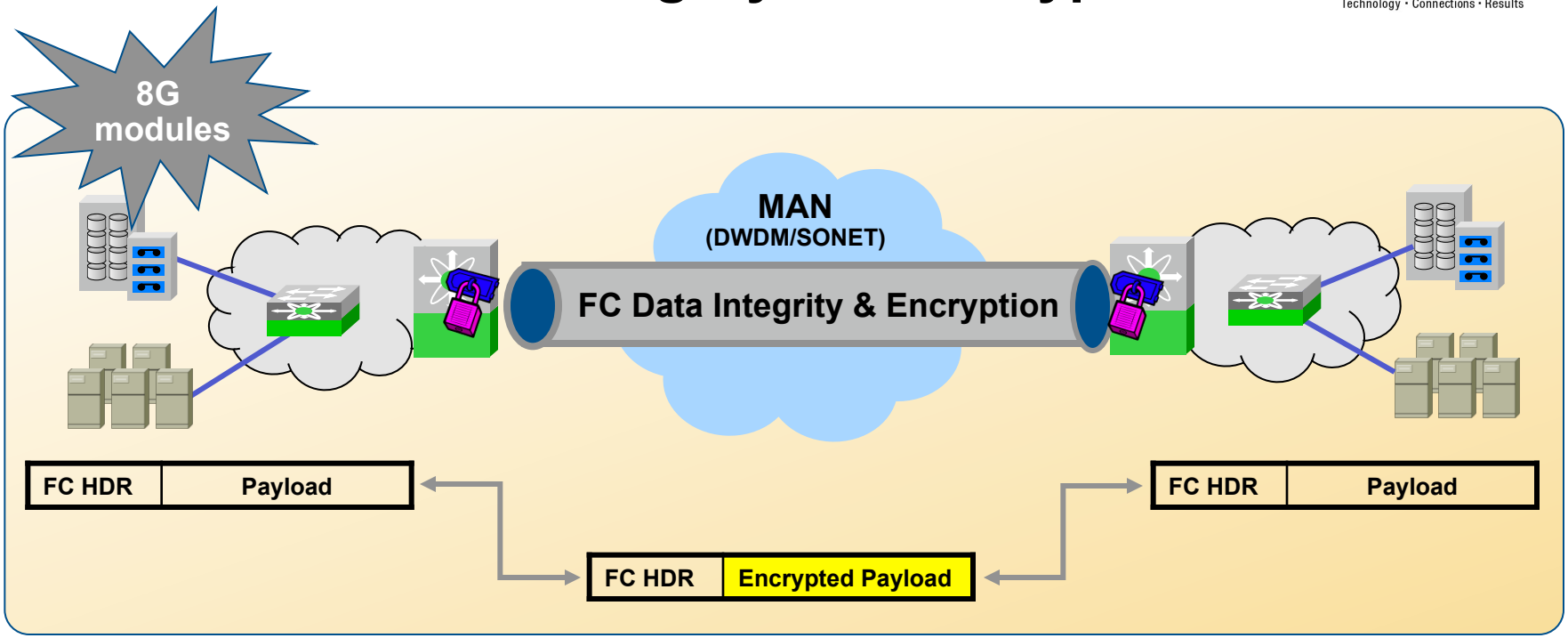
IP Storage Security:
FC-over-IP (FCIP)

- 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

IP Storage Security



FC Link-Level Data Integrity and Encryption



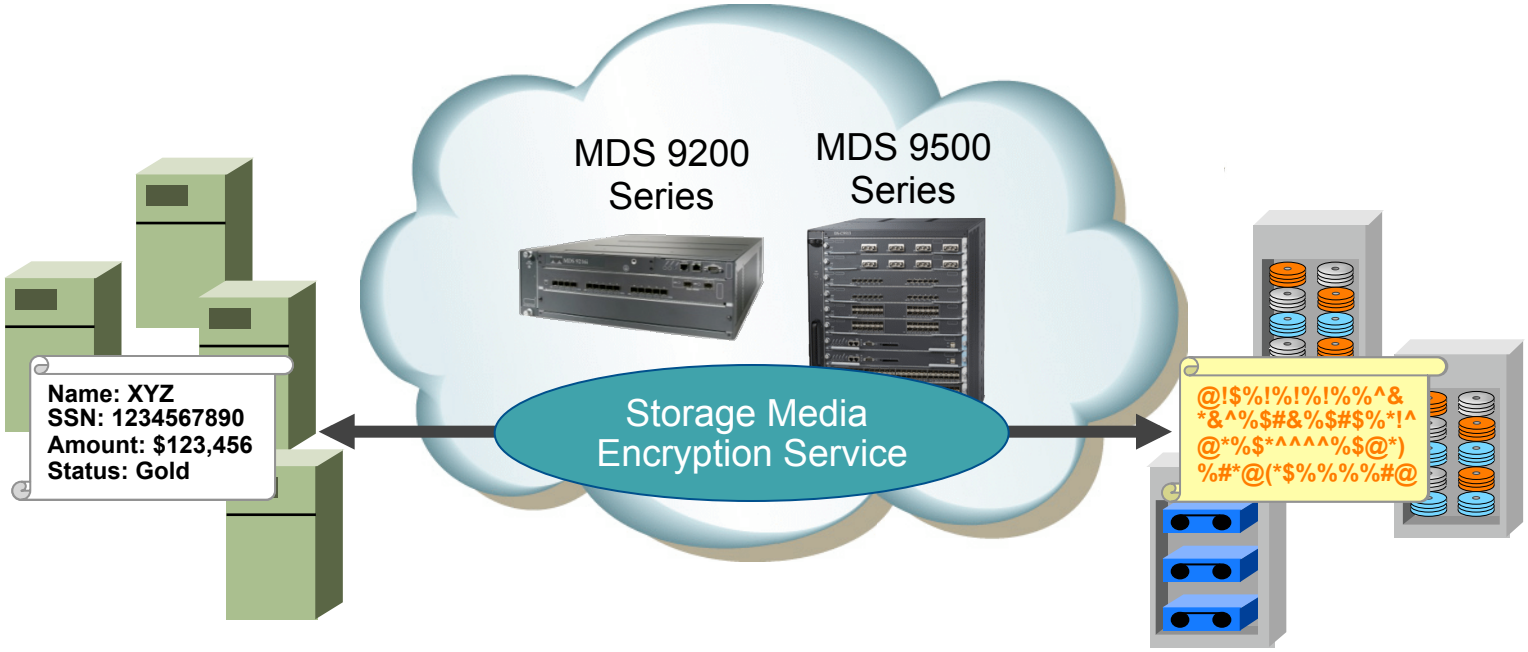
- Preserve integrity and confidentiality of FC traffic over MAN
- Integrated, high performance functionality
- No change to existing SAN, enable functionality only on edge switches

Encrypting Data at Rest

Encryption Solutions

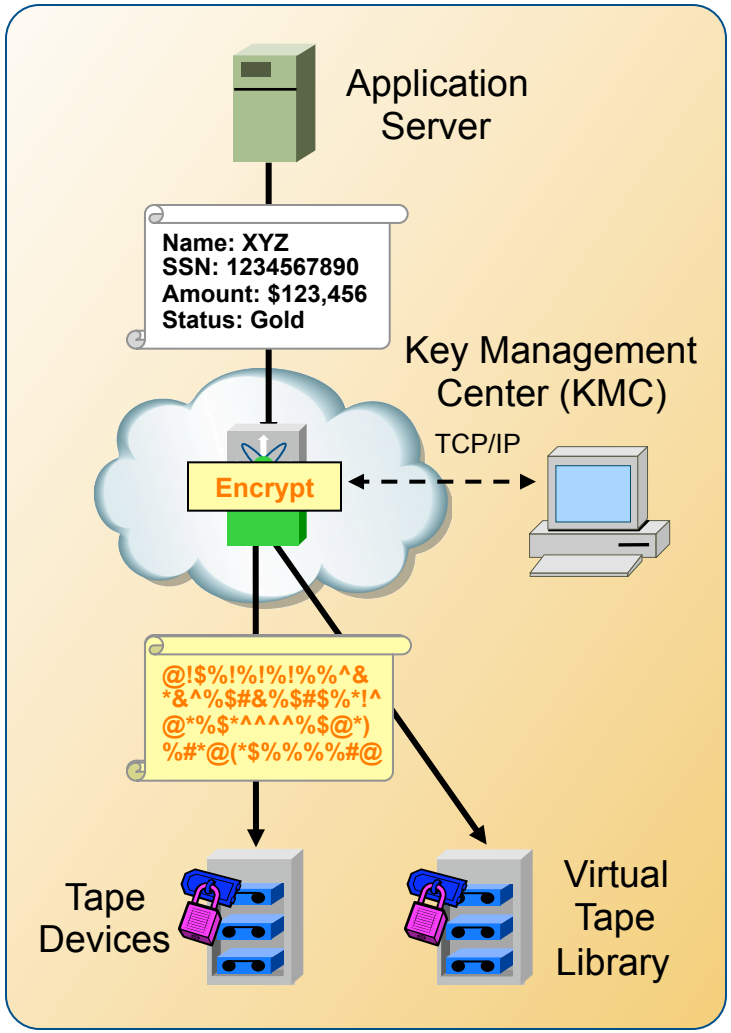
- Host/Software Based
  - Keys stored on database or application servers where data resides
  - CPU Intensive
- SAN Appliances
  - Scalable by adding more appliances
  - Rewire and reconfigure SAN ports and zoning
- Tape Drives
  - High Performance
  - New Drives and possibly new media needed
  - Could be costly
- Fabric Based
  - Ease of installation
  - Scalable
  - Integrated with Key Management Solutions

Delivering Encryption as a SAN Service



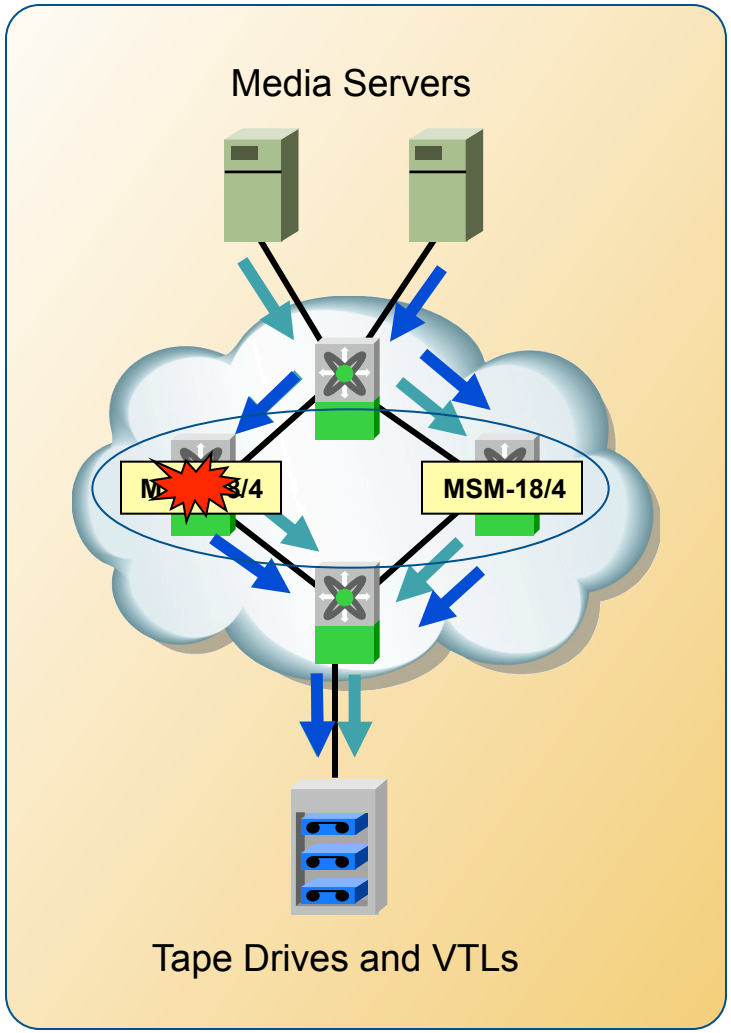
1. Insert Cisco MPS-18/4 modules or MDS 9222i switches
2. Enable Cisco SME and setup encryption service
3. Provision encryption for specific storage devices

Cisco SME - Secure, Integrated Solution



- Encrypts storage media (data at rest)
  - Strong, Std. IEEE AES-256 encryption
  - Integrates as transparent fabric service
  - Handles traffic from any virtual SAN (VSAN) in fabric
- Supports heterogeneous, SAN attached tape devices and virtual tape libraries
- Includes secure key management
  - Open API integrates with enterprisewide, lifecycle key managers
- Compresses tape data
- Allows offline, software only media recovery

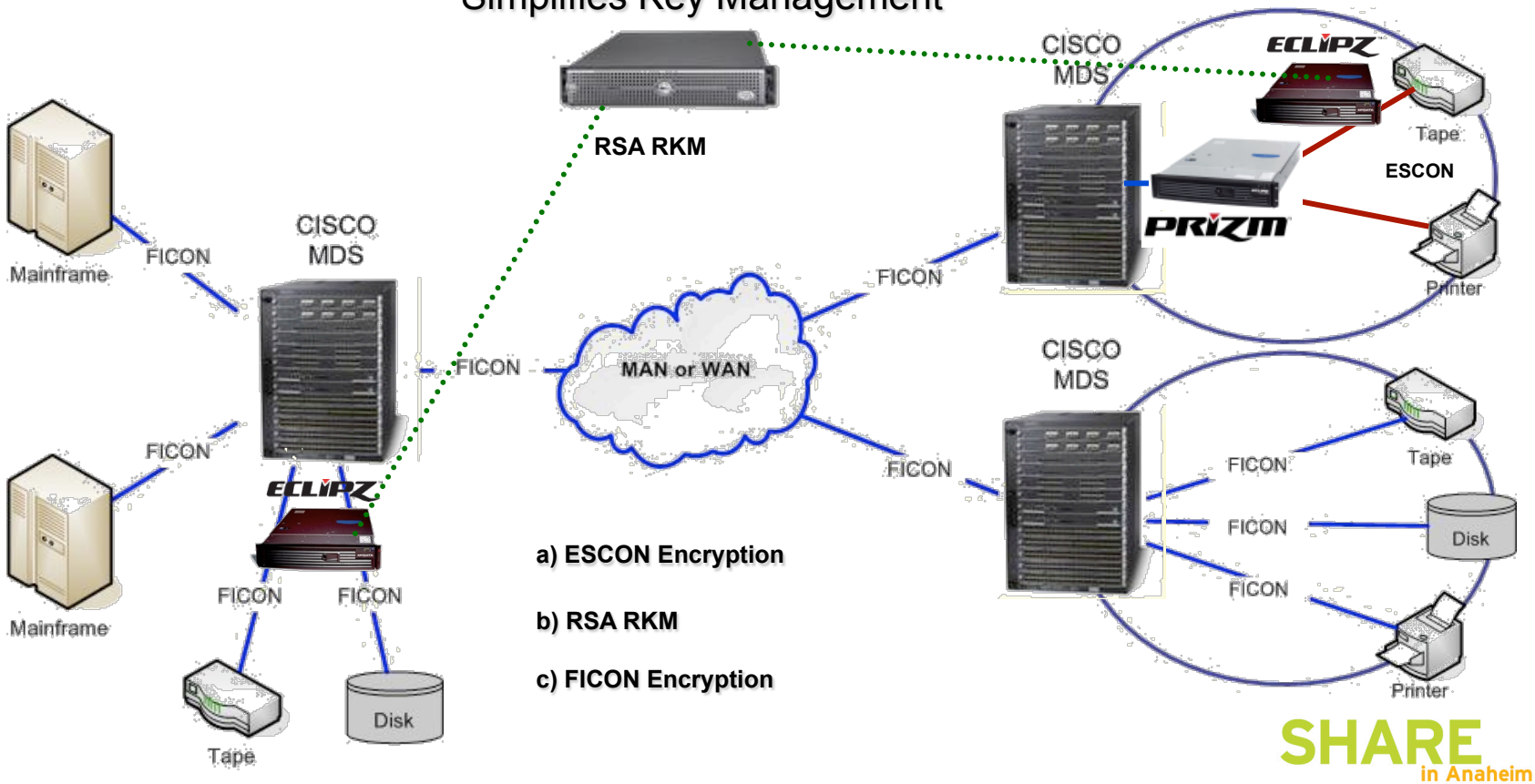
Cisco SME - Scaleable, Highly Available



- Integrates transparently in MDS fabrics
- Dramatically reduces deployment time
  - No SAN re-configuration or re-wiring to insert appliances
  - Provisioning becomes a simple, logical process of selecting what to encrypt
- Modular, clustered solution offers highly scaleable and reliable performance
- Load balances automatically
- Redirects traffic if a failure occurs
- Provisions quickly with Cisco Fabric Manager wizards

Cisco / Optica Encryption Solutions

Adds Value to MDS / SME Solution
Leverages Open Systems Success
Simplifies Key Management



Conclusion

- As SANs continue to grow and expand out of the datacenter, security must be addressed
- Cisco offers the industry's most comprehensive set of security features in the MDS 9000 Family
  - No impact on switch performance
  - Data path features are all hardware-based
  - Cisco rated A++ for complete end-to-end security solutions: *"Cisco supports just about every SAN security feature or protocol available today and has taken a real leadership position here."*

Nick Allen, Senior Analyst, Gartner, Gartner PlanetStorage

  - All security features are easily managed through Cisco's Fabric Manager application

Q and A

References

- Cisco Storage Networking
  - http://www.cisco.com/go/storagenetworks
- Standards:
  - http://www.t10.org (SCSI specs)
  - http://www.ietf.org/html.charters/ips-charter.html (IETF ips wg)
  - http://www.t11.org (FC-SP specs)
  - ftp://ftp.t11.org/t11/pub/fc/sp/06-157V3.PDF(FC-SP v1.8)
- Forums:
  - http://www.snia.org
  - http://www.snia.org/ssif


SHARE
Technology • Connections • Results


CISCO


SHARE
in Anaheim
2011