# Locking Up Your Storage Network

## (Securing the SAN Infrastructure)

**Kamy Kavianian**
**Director, Product Marketing**
**Network Security and Architecture**
Brocade Communications Systems

BROCADE
The intelligent platform for networking storage

*April 2002*

# Why Secure SANs?

- Security is a fundamental requirement for enterprise SANs, just like any other network
- As SANs increase in size and are inter-networked over MAN/WANs, physical monitoring and management is no longer feasible or cost-effective
- Multi-tenant environments have new security requirements
  - Security enables sharing of SAN resources among multiple customers securely
  - Reduces xSP infrastructure costs and enables economies of scale

© Brocade Communications Systems, Inc

# SAN Security Requirements

- New levels of access control
- Strong authentication
- More controls in SAN Fabric Management
- Confidentiality (data privacy)

© Brocade Communications Systems, Inc

# New Levels of Access Control

- SAN fabrics require more controls to prevent unauthorized access:
  - To a switched fabric to gain access to sensitive information such as zoning data, security policies etc.
  - To SAN fabric switches (using a laptop) through unprotected connections (serial ports etc.)
  - Through the front panel of fabric switches and other SAN infrastructure devices
- SAN fabrics require more granularity in management access controls
  - Multiple user/administrator roles

© Brocade Communications Systems, Inc

# Strong Authentication

- Without authentication, SANs are susceptible to:
  - Spoofing: Hosts (servers) sign on with phony WWNs and get access to devices they shouldn't
  - Denial of service attack:  unauthorized host application sends out a high volume of dummy management messages or I/Os to a LUN it doesn't own
  - Rogue devices could be added to the fabric

© Brocade Communications Systems, Inc

# More Controls in SAN Fabric Management

- The need for controlling how a SAN fabric is managed
  - Ability to turn on or off certain management access to the fabric
  - Control of end points accessing management facilities within the fabric
  - Secure remote management access
  - Centralization of  configuration (security) parameters – secure distribution of critical management data

© Brocade Communications Systems, Inc

# Confidentiality

- Encryption is required to eliminate eavesdropping threats:
  - Cleartext passwords and other data
  - Secure Remote Access – Encrypted management data
  - Unauthorized analysis on the Fibre Channel line or other interfaces to analyze management or data traffic (e.g., Sniffers)

© Brocade Communications Systems, Inc

# SAN Security – An Infrastructure Decision

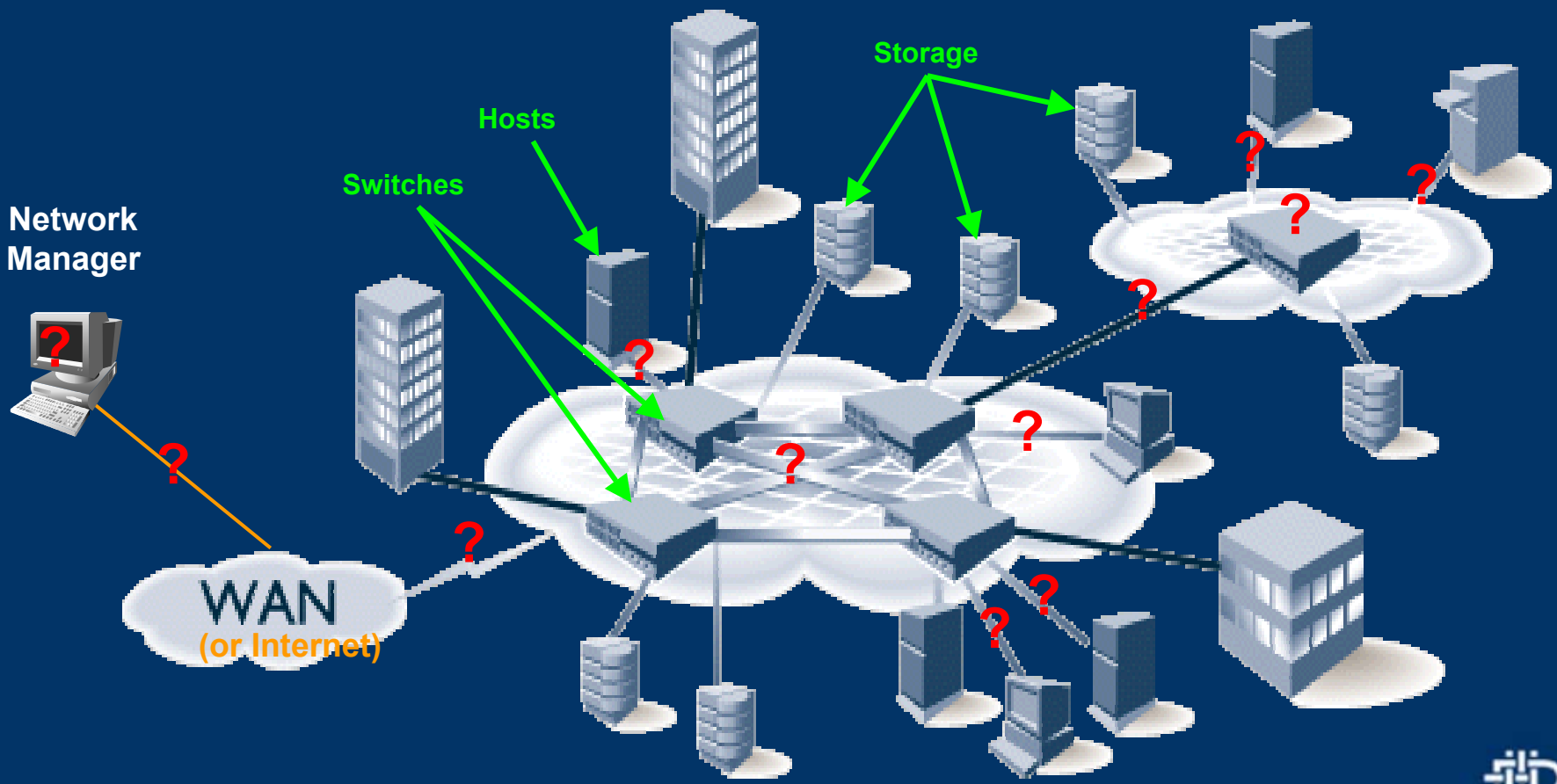
- Security is a fundamental consideration when designing SANs and selecting SAN infrastructure

- As with any network, SAN security must be:
  - Robust
  - Scalable
  - Policy-based
  - Based on proven, standards-based mechanisms
  - Manageable
  - Auditable

© Brocade Communications Systems, Inc

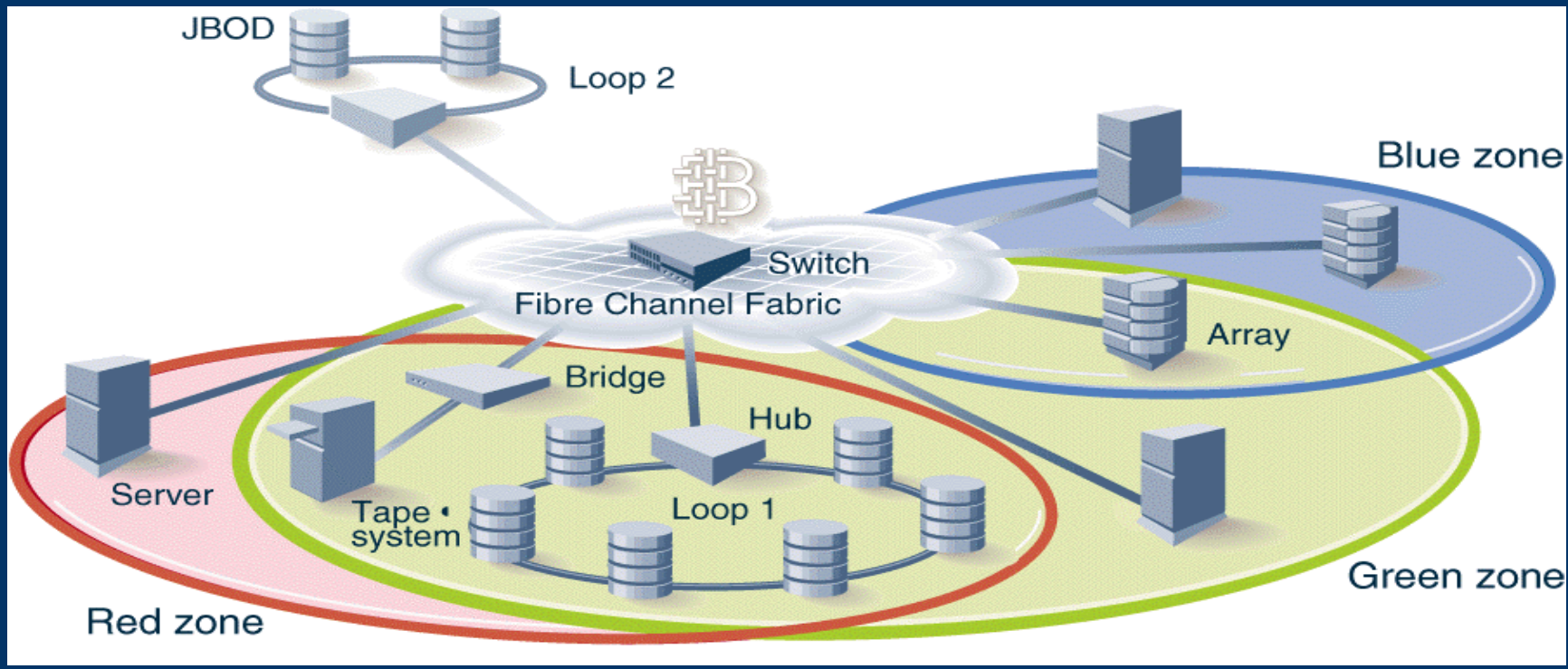
# SAN Fabric Security Vulnerabilities

? = Potential Security Control Points




© Brocade Communications Systems, Inc

# Zoning: Association of Storage with Servers (Today)




- Zoning: Logical association of storage with servers
  - Used for access control (I.e. No zone sees Loop 2)
  - Must be hardware enforced

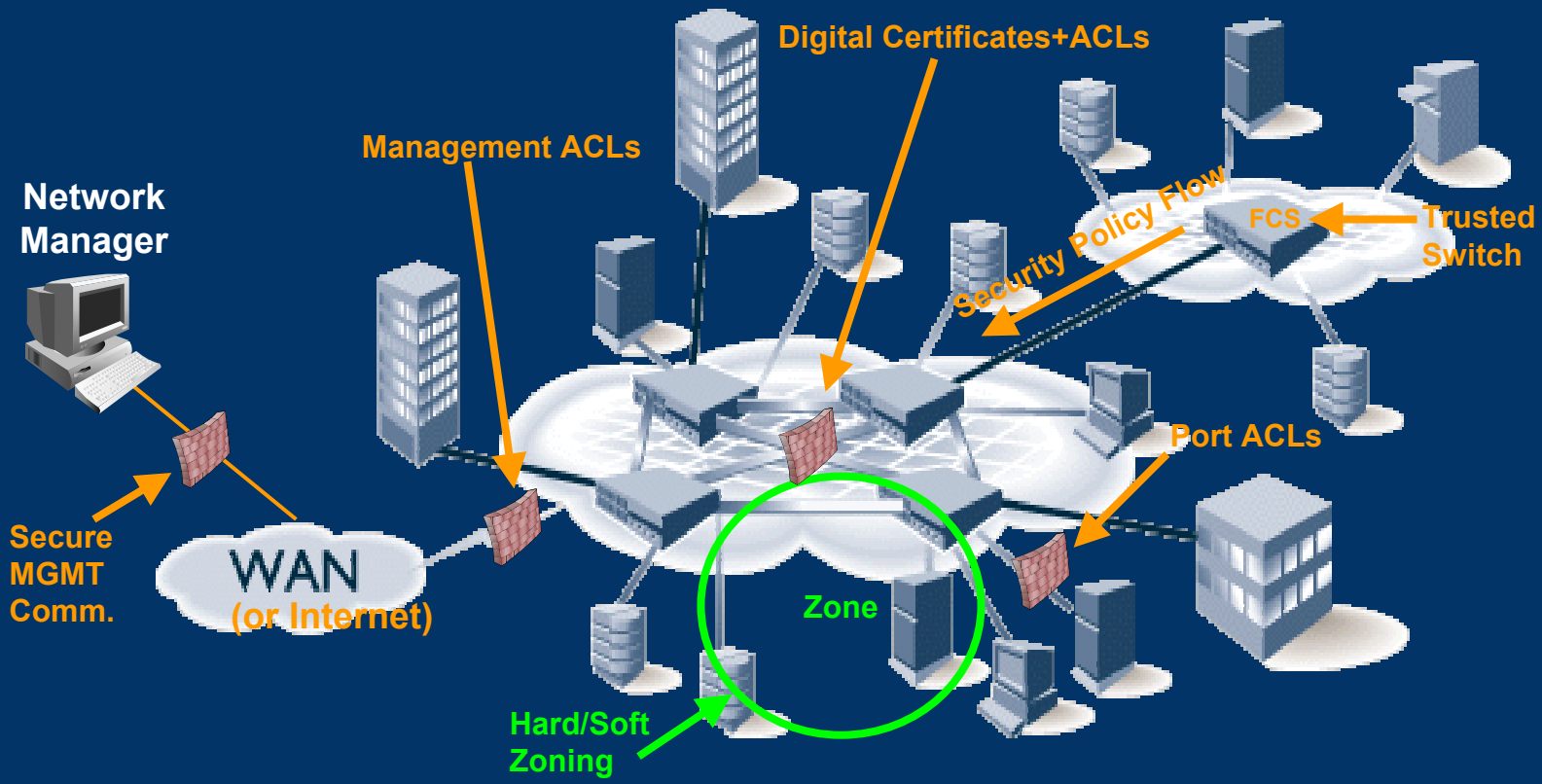
© Brocade Communications Systems, Inc

# Fabric Security Controls


MAC = Management Access Controls
ACL = Access Control List
ISL = Inter Switch Link

© Brocade Communications Systems, Inc

# A Secure SAN Infrastructure




© Brocade Communications Systems, Inc

# Security Threats and Best-in-Class Solutions

| *Threat/Risk* | *Best-In-Class Solutions* |
|---|---|
| Unauthorized/ Unauthenticated User Access | - Multilevel password control and encryption<br>- Strong authentication – Integrate with customer's existing RADIUS / TACACS+ / other infrastructure |
| Insecure Management Access | - Management access control policies<br>- Encrypt mgmt. information (user name/password) where applicable<br>Other Solutions : SSL, SSH, IPSEC |
| Spoofing of Device Names (WWNs) | - More granular access control for hosts/servers (at port level)<br>- Strong in-band authentication of SAN fabric logon attempts |
| Management Controls From Uncontrolled Access Points | - Asymmetric management approach-Trusted switches to set security controls<br>- Use of strong authentication (PKI) |

© Brocade Communications Systems, Inc

# For More Information

- Please access the Secure Fabric OS white paper and datasheet at:
  - http://www.brocade.com/SAN/white_papers.jhtml
  - http://www.brocade.com/SAN/data_sheets.jhtml
- Other Educational Tools
  - Brocade SAN Security Course (2 days)
  - SAN Security - A Best Practice's Guide
- Contact your Brocade Partner or Sales Executive
- E-mail: info@brocade.com

© Brocade Communications Systems, Inc

# Thank You

Brocade Communications Systems

BROCADE

The intelligent platform for networking storage