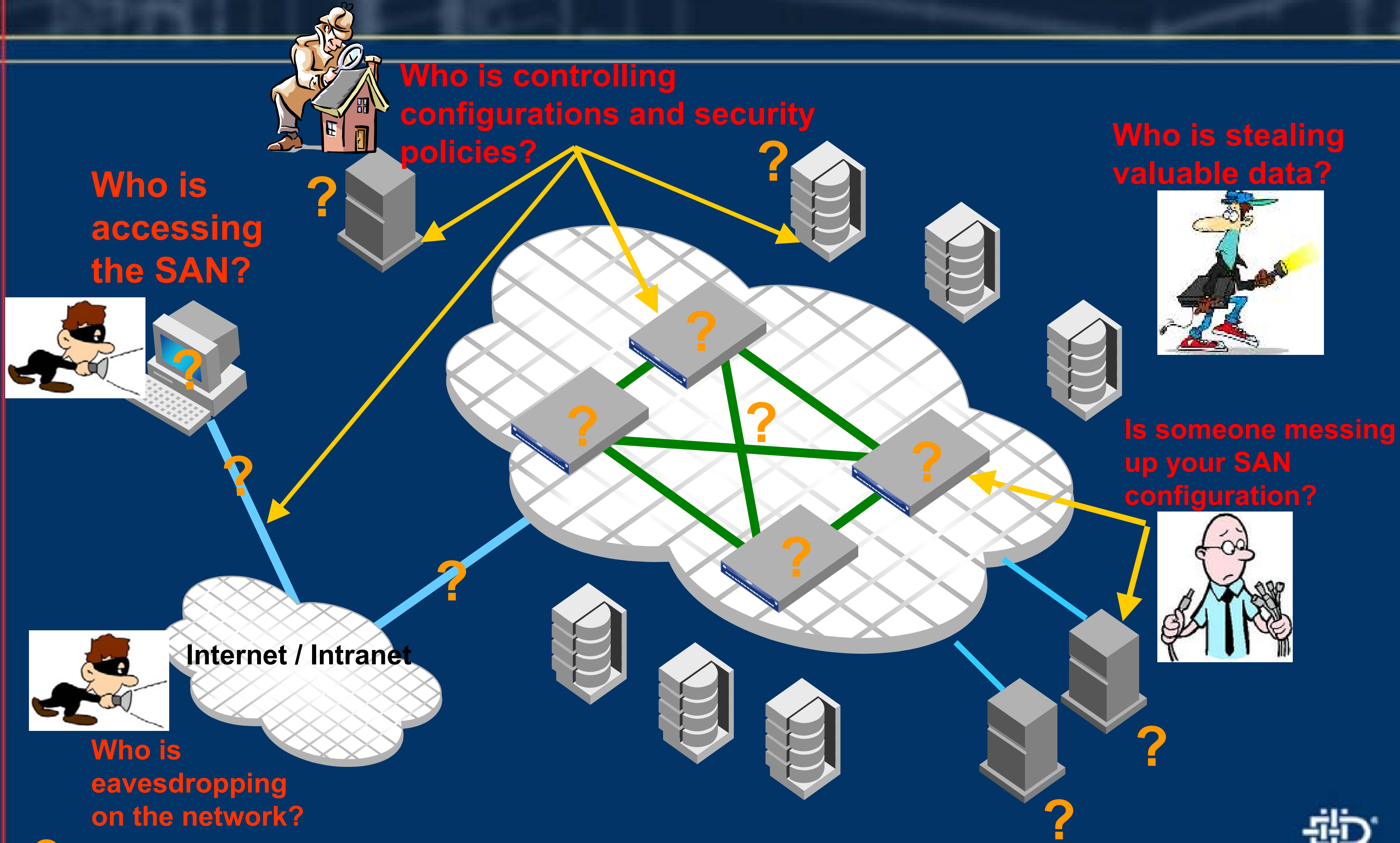
What security problems are we addressing? Threats!

- Lack of adequate (or granular) administrator and user access control and authentication
  - Threats: The most common attack. Unauthorized access by individuals to sensitive data or SAN security parameters.
- Lack of strong or binding authentication and authorization among SAN devices (switches and servers)
  - Threats: IP or WWN spoofing. Masquerading. Unauthorized access by devices or other switches.
  - Unintentional changes, errors, and misconfigurations - network disruptions
- Inadequate controls and granularity in SAN Management access and security policy distribution
  - Threats: Management access from uncontrolled sources. Denial of Service (DOS) attacks through open management ports.
  - Unintentional changes, errors, and misconfigurations– network disruptions
- Lack of privacy for sensitive management data such as passwords, files etc.
  - Threats: Eavesdropping. Ability to view or intercept sensitive data such as passwords or data files.

How secure is your SAN?



Who is controlling configurations and security policies?

Who is stealing valuable data?

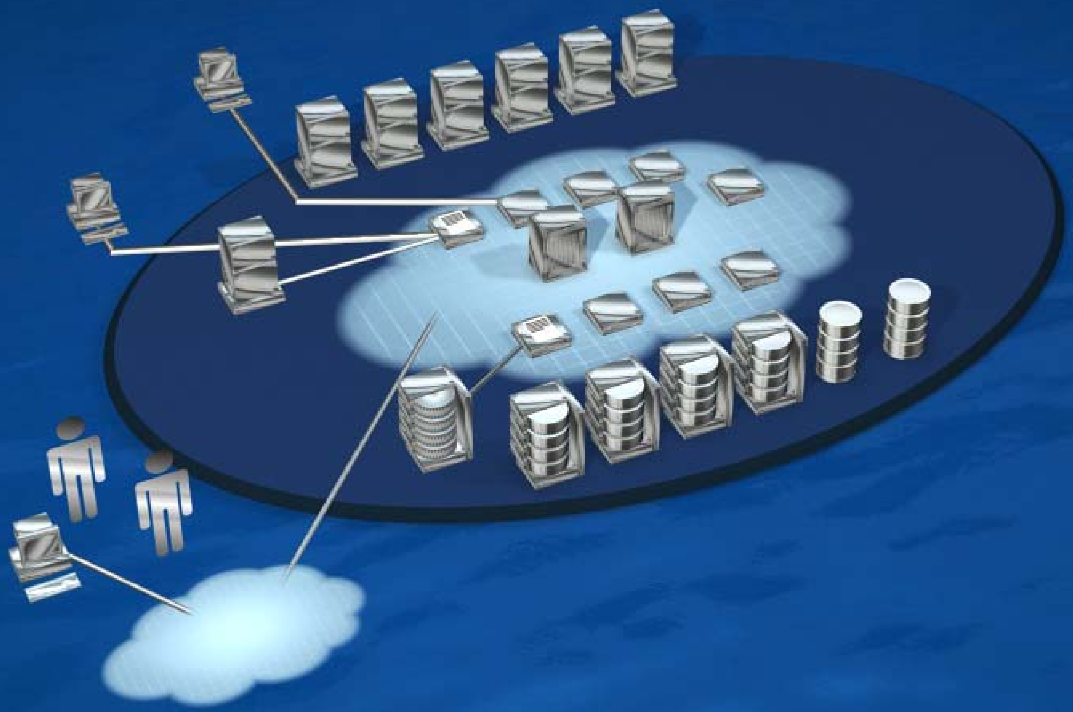
Who is accessing the SAN?

Is someone messing up your SAN configuration?

Who is eavesdropping on the network?

? = Security attack points

SAN security must ensure Configuration and Change Management Integrity



- Comprehensive *fabric* based security
- Assure Configuration Integrity
- Active Change management
- Protection from unauthorized access, loss or corruption
- Reduced system downtime
- Strong Authentication and Access Control
- Policy-based Management

SAN Security must provide for management path encryption ensures secure access to your SAN

- Secure Management Communications *Channels*
- Encryption of Admin IDs and passwords
- Protect passwords over public or internal networks
- Secure unprotected log-ins to the SAN
- Prevent eavesdropping on sensitive data

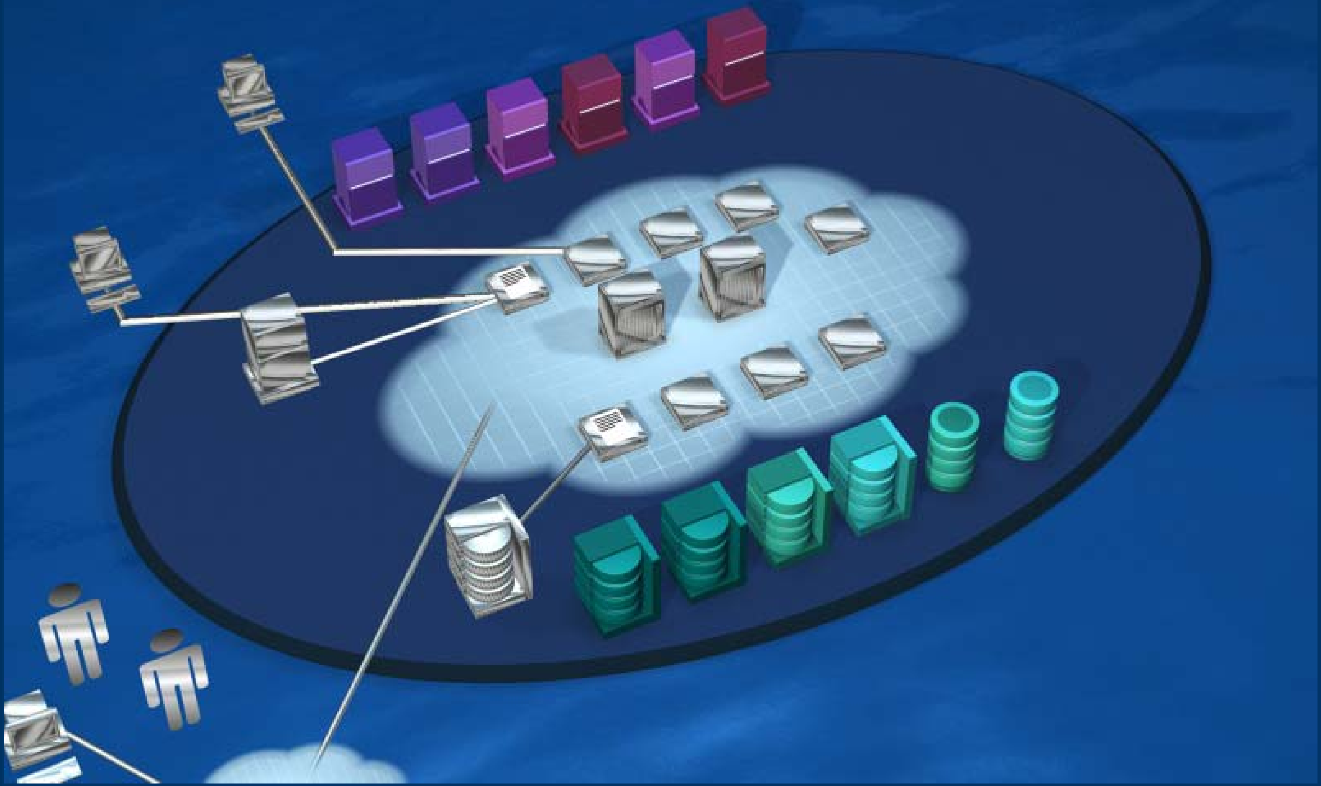
SAN security must control management and administrative access

- Management ACLs control access to the fabric from different sources
- Policy-based Infrastructure with centralized control
- Passive or active control allowed to admins

SAN security must provide for authentication of switches and infrastructure

- Digital certificates within the SAN switches provide the strongest authentication for new switches
- Ensure a new switch is authorized to join the fabric

Assure configuration integrity and change management controls



- Device access controls (port level ACLs)
- Port-level access policies tightly control server access to the fabric
- Access Control Lists lock Hosts/Servers by WWNs to specific physical ports