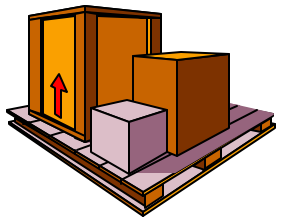
A Proposal for Access Controls

(aka SAN Boxes)



SAN Promise and Problem

- **Promise**: pool Storage Devices on SAN for ease of management
- **Problem**: SCSI not suited for "big shared bus"
  - data integrity and privacy at risk
  - Reservations are inadequate

Why Not Reservations?

- All hosts are peers so
  - Reserve/Release can be preempted by resets
  - Persistent Reservations can be preempted
- Only one reservation owner (initiator)
  - for ACs, need AC manager independent of owner (can't claim access autonomously)

AC Manager Application Client =
PAM, Partition Access Manager

Design Goals

- Access Controls by LU or ELEMENT within LU (same scope as reservations)
  - only authorized hosts can access restricted targets
  - targets can be configured as unrestricted (default state)
- Support ALL device types (not just storage)
  - controllers, disks, tape drives, etc.
  - allow limited resource devices to participate
- Minimize performance impact (minimal access checking per IO)
- Distribute "workload" across targets/hosts/PAM

Access Controls

- Maintained at the target; determine which initiator/hosts can access device
  - facilitates "reservation groups"
  - restricted cmds same as reservations
- Managed by PAM via Password authenticated CDBs
- Hosts identified in AC by either
  - *private* AccessID (new in proposal)
  - Transport Identifiers (like FC NodeName)

Why Two Naming Schemes?

- Why new AccessID:
  - host based not initiator/HBA based -- correct granularity for access controls
  - Transport Independent
  - Ease of management
    - no discovery of HBA WWNs required
    - HBA change/move/remove actions simplified
  - Foundation for more secure versions of protocol

Why Two Naming Schemes? *(continued)*

- Why Transport-specific identifiers:
  - already used in Reservations and Extended Copy
  - some controllers already use these for similar functions
  - does not require additional host behavior (Send AccessID)
  - PROXY requires some identifier different from AccessID (details to come)

Highlights

- Two new CDBs (with service actions):
  - ACCESS CONTROL IN
  - ACCESS CONTROL OUT
- "SIGNED" service actions:
  - contain a self-validating password
  - come from Application Client (PAM)
- Unsigned service actions for generic hosts/initiators
- (Mostly) Transport Independent

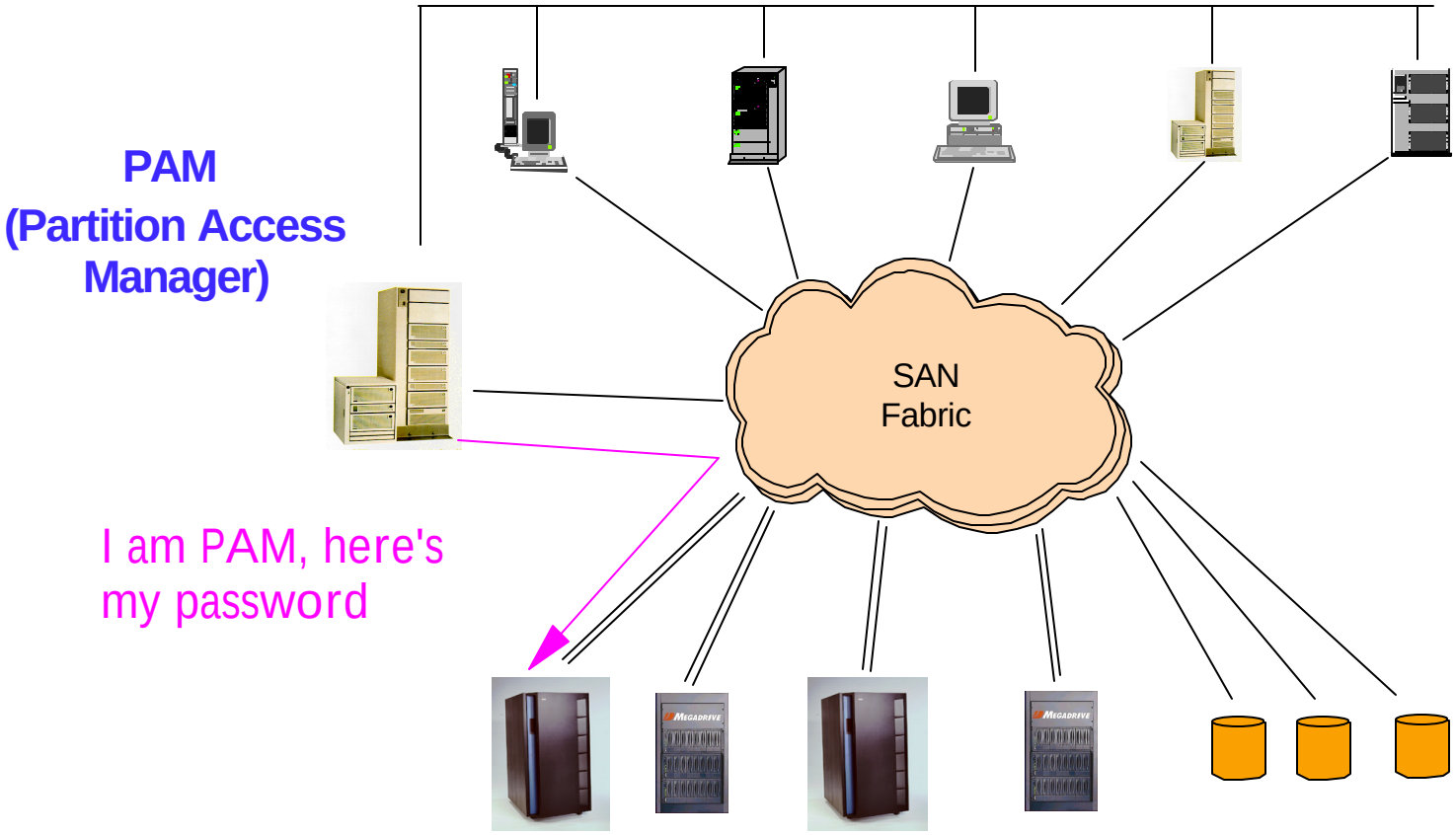
Highlights *(continued)*

- Two "Identification" service actions (OUT)
  - Set/Change Password (SIGNED PASSWORD REGISTER)
  - Host Send ID (ACCESS ID REGISTER)
- Two "Grant/Revoke Access" service actions (OUT)
  - SIGNED AUTHORIZATIONS (for PAM)
  - PROXY AUTHORIZATIONS (for generic hosts)
- Two "Query" service actions (IN)
  - SIGNED REPORT AUTHORIZATIONS (get all info about ACs)
  - REPORT AUTHORIZATIONS (get those relevant to specific host)

CDBs with Passwords

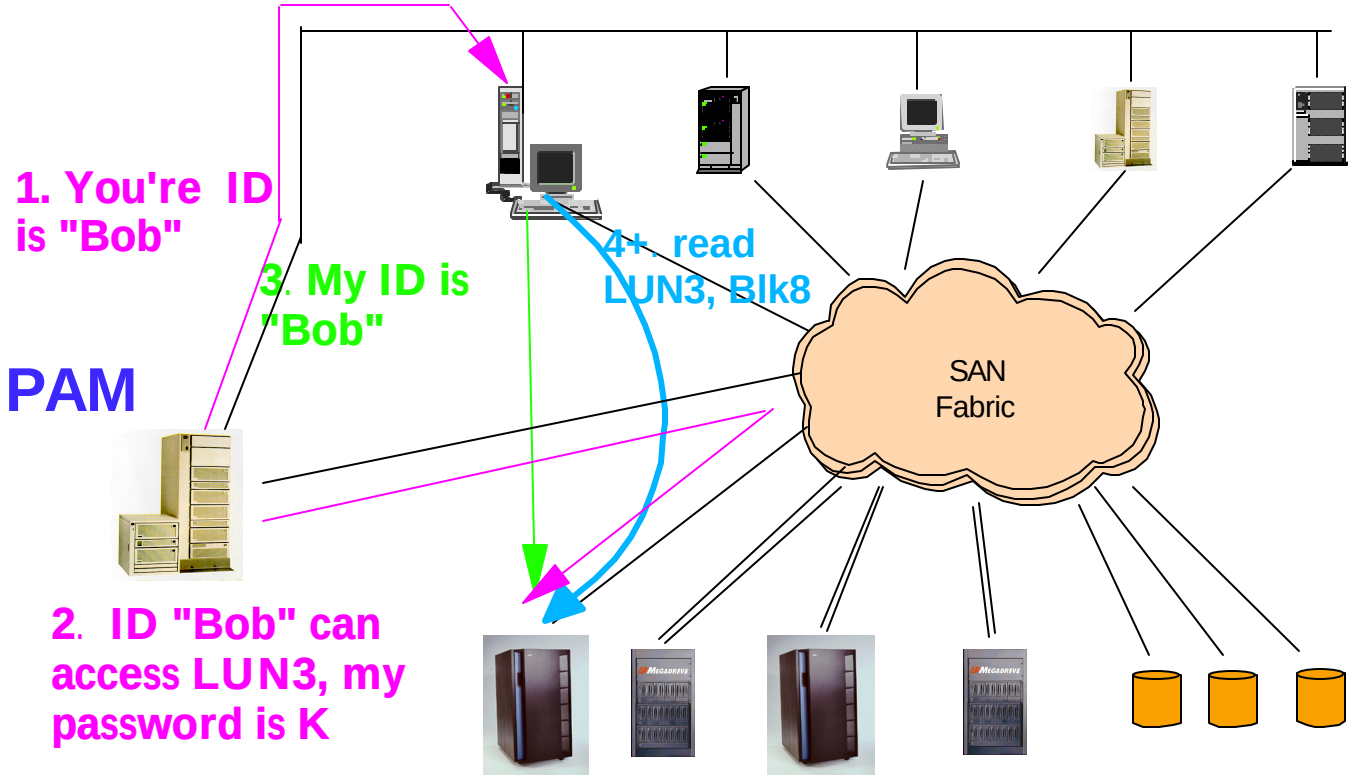
- New to SCSI?
- Validate the Application Client (PAM)
- Initiator independent
- Passwords are private at the device server
  - cannot be queried!
- Available for additional service actions:
  - e.g., RAID controller LU configuration
  - VS service actions available

PAM to Device Server Protocol



- Server accept all commands until PAM configures it
- PAM initializes password at the server
- Configuration cmds to server include PAM's password
- Server can be reset with special reset password (on box)

Operating Protocol



Step 1. PAM assigns AccessID to host - once

Step 2. PAM sends access grant for AccessID to server - once

Step 3. Host identifies itself to server (server maps AccessID to address) - on SAN reconfig

Step 4+. Access request (server infers AC rights from address) - per request

Passwords (in detail)

- 8 bytes long, to fit within 16 byte CDB
- Two types
  - Current Registered Password
    - initially unset
    - set/changed by service action from PAM
    - can be unset (to default state)
  - Permanent HW password
    - requires physical access to device to discover
    - used for recovery if PAM "looses" current PW

Access Controls (more details)

- Device server should be able to maintain at least one such entry for each LU at device
  - guarantees at least one host can have exclusive access
- Should be kept non-volatile (not required)
- Some cmds not subject to access controls
  - in general, if not reservation controlled, then not access controlled
  - some access control service actions subject to access controls
- New ASC/ASCQ to report access conflict