xrootd Proxies

Andrew Hanushevsky (SLAC)

Middleware Security Group Meeting

5-6 June 2006

http://xrootd.slac.stanford.edu

xrootd is largely funded by the US Department of Energy
Contract DE-AC02-76SF00515 with Stanford University

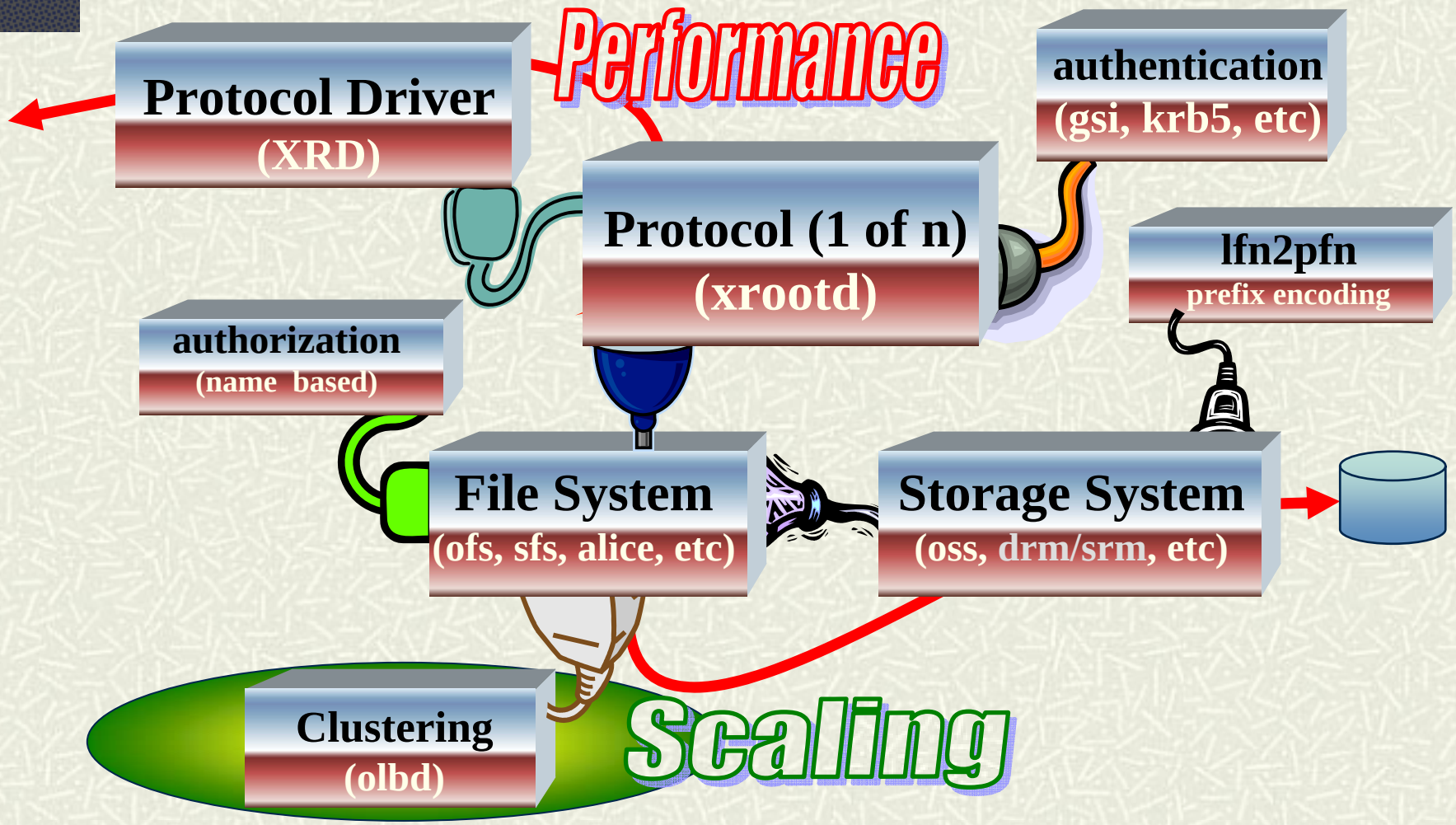
Stanford Linear Accelerator Center

Outline

- xrootd Architecture Overview
  - Terms and Concepts
  - Clustering
- Proxies
  - Single and double firewalls
  - Proxy clusters for scalability
- Security transformations
- Conclusions & Acknowledgements

Stanford Linear Accelerator Center

xrootd Plugin Architecture



Acronyms, Entities & Relationships

olbd

Control Network

Managers, Supervisors & Servers

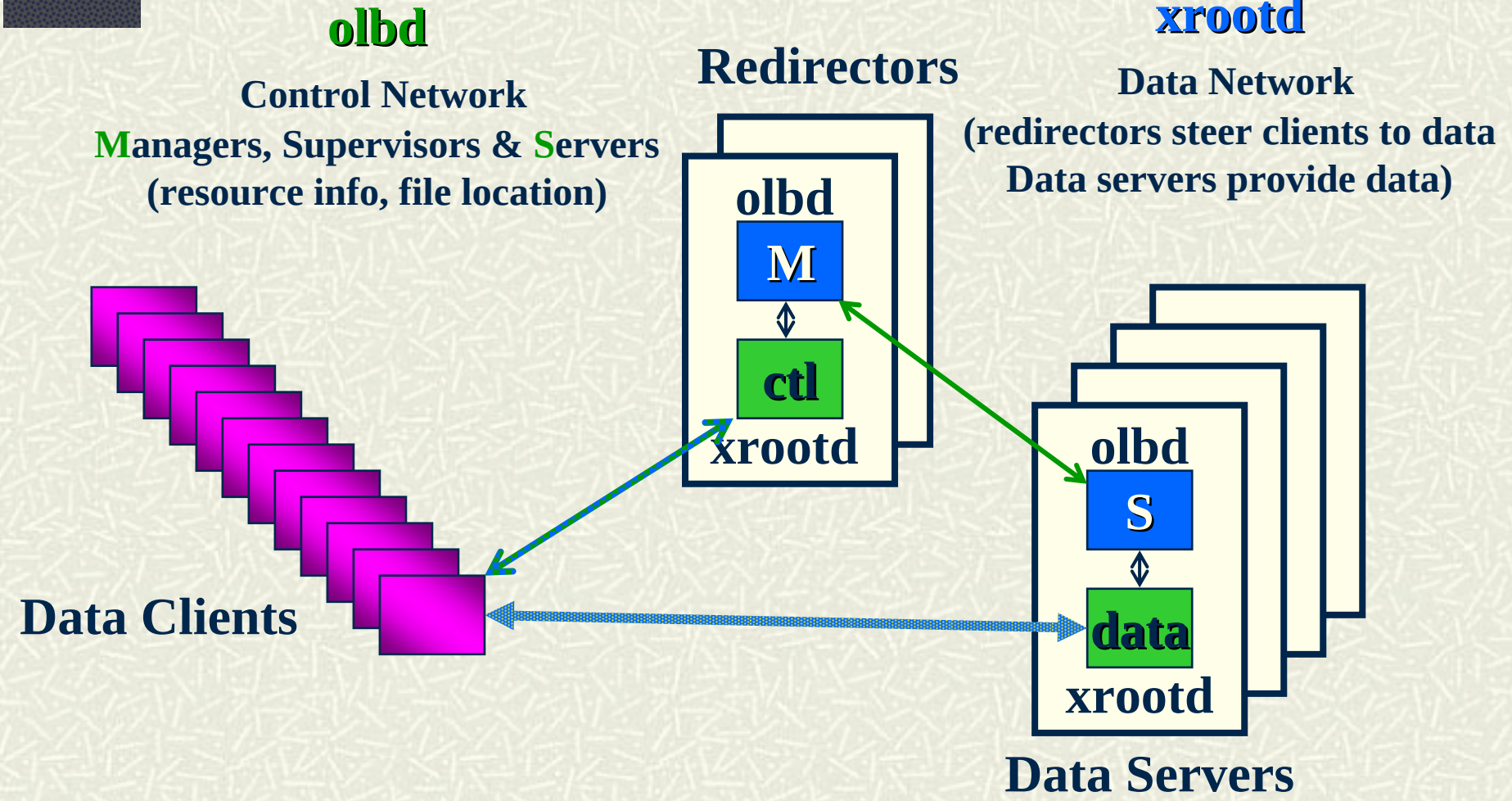
(resource info, file location)

xrootd

Data Network

(redirectors steer clients to data

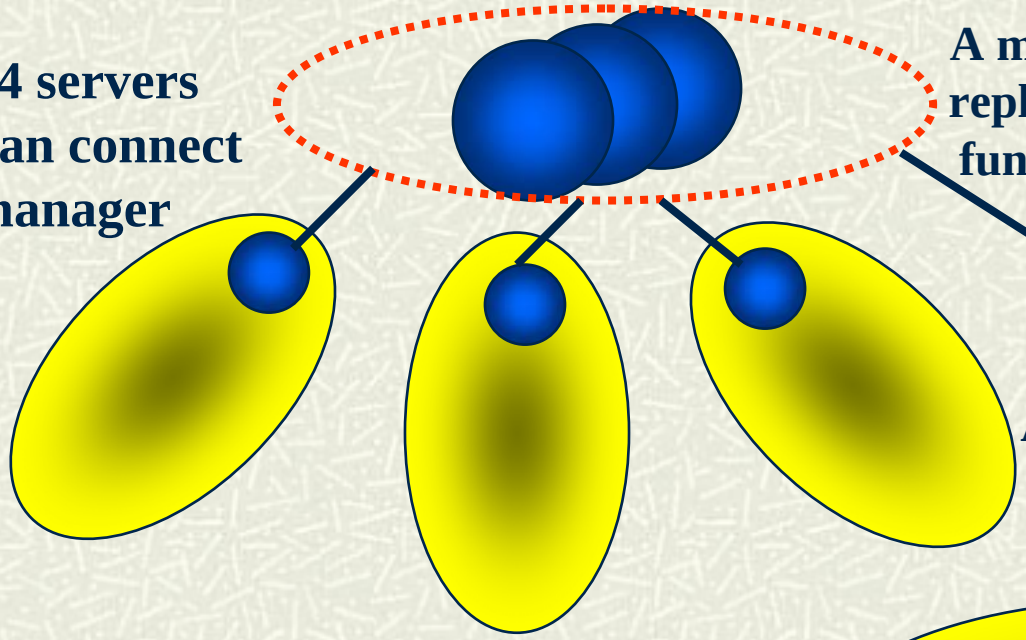
Data servers provide data)



Cluster Architecture

Up to 64 servers or cells can connect to a manager

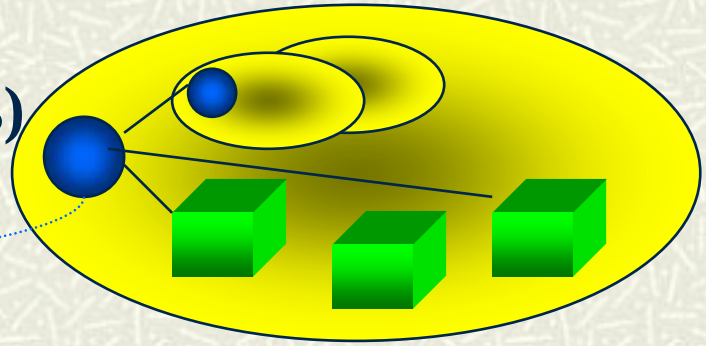
A manager is an optionally replicated xrootd/olbd pair functioning as a root node



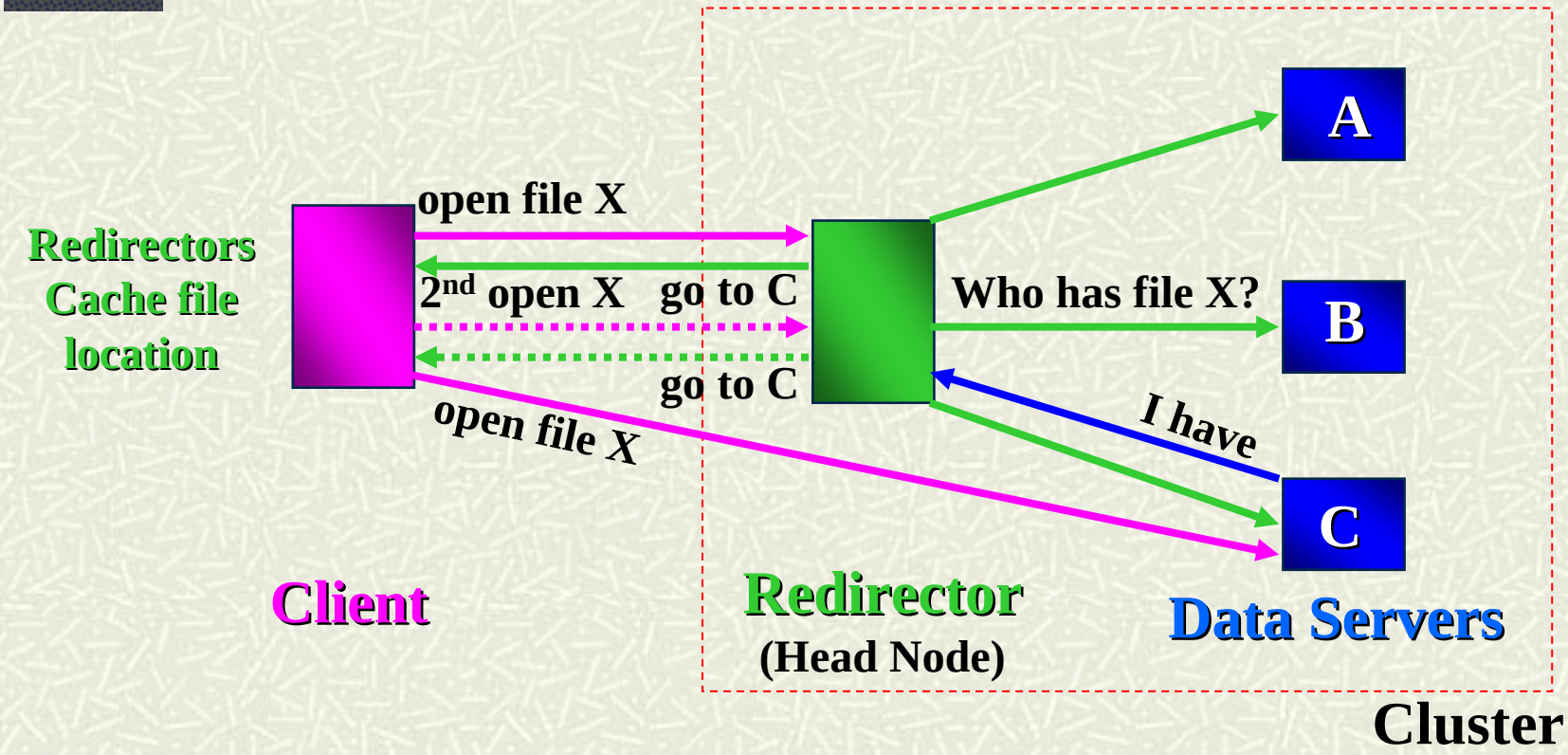
Server

A server is an xrootd/olbd pair leaf node that delivers data

A cell is 1-to-64 entities (servers or cells) clustered around a cell manager called a supervisor

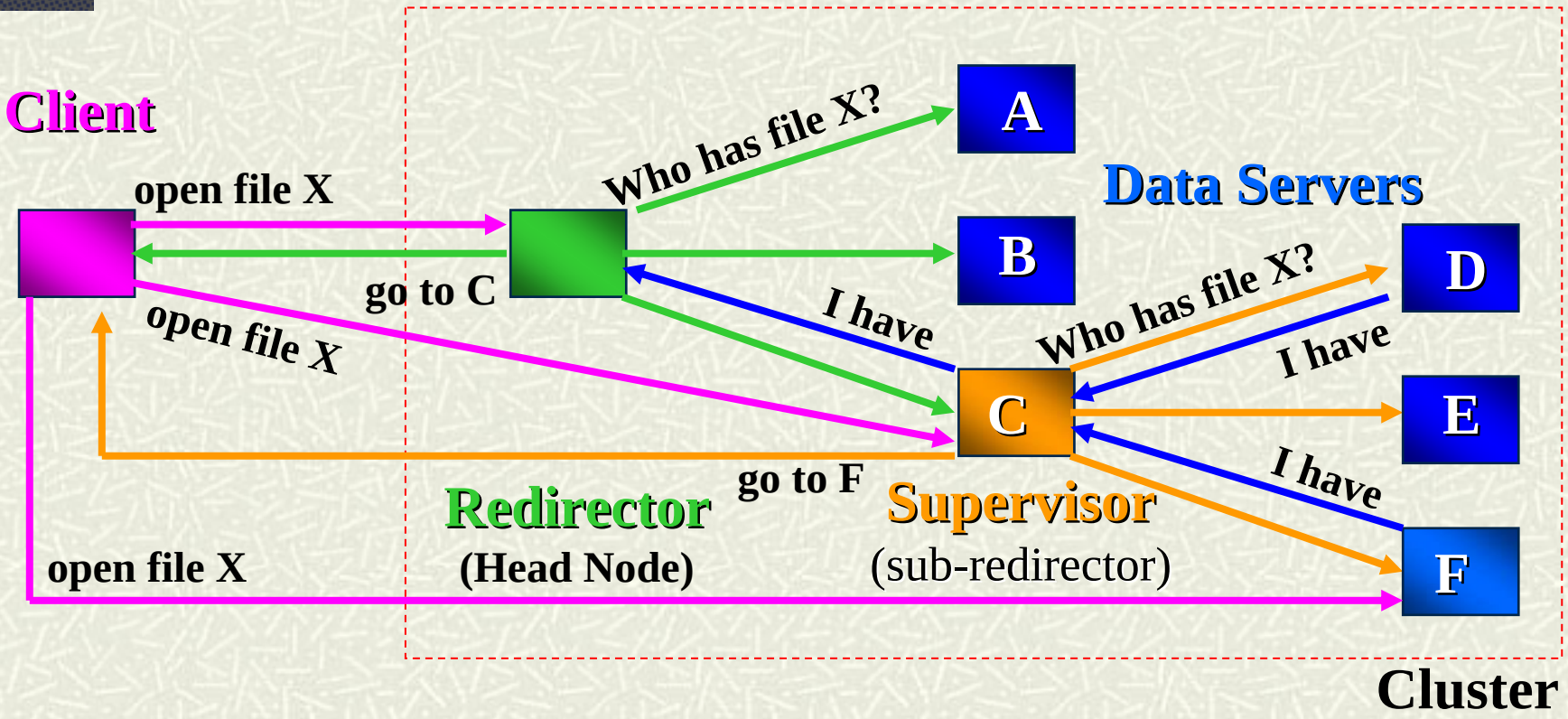


Single Level Switch



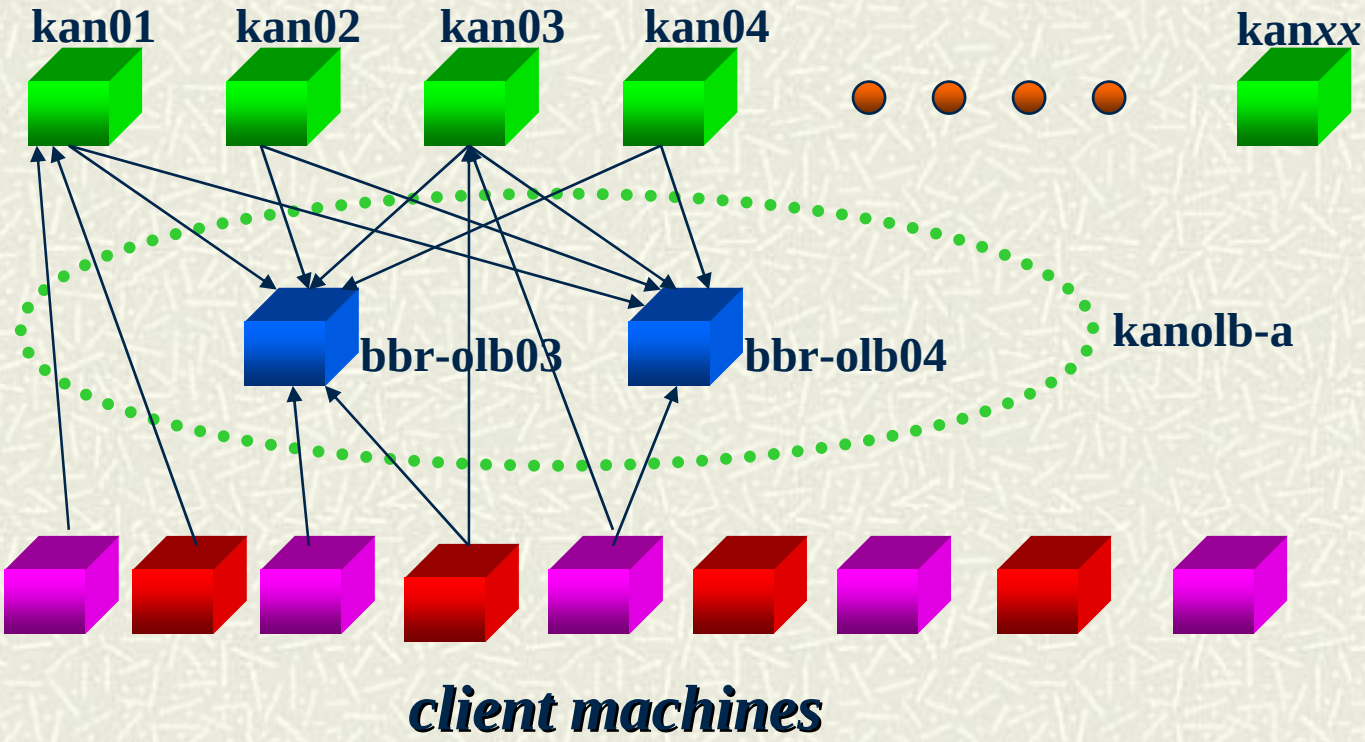
Client sees all servers as xrootd data servers

Two Level Switch



Client sees all servers as xrootd data servers

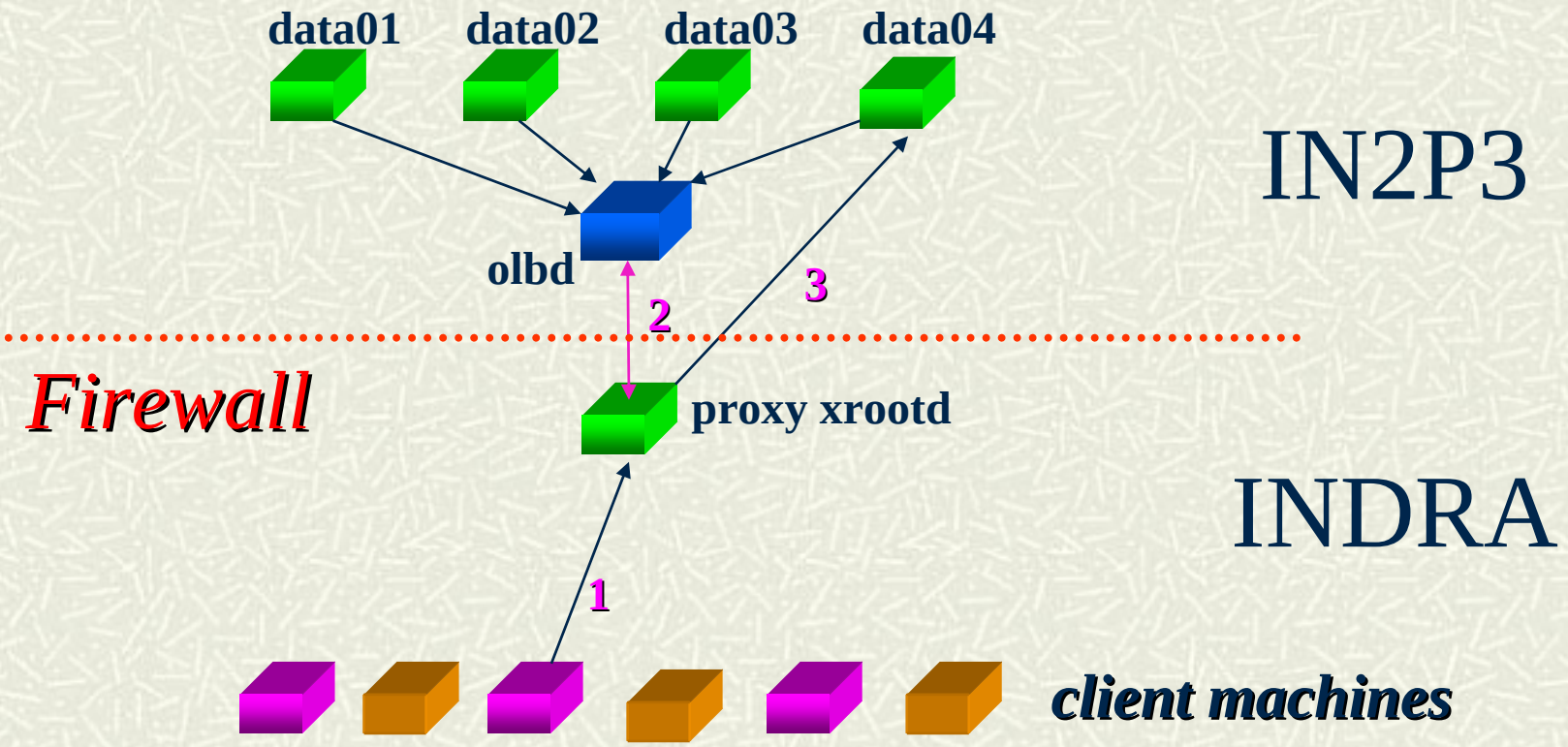
SLAC Configuration



Extending Access

- Easy clustered local access
  - Everyone sees everyone
  - Simple configuration
  - Low human overhead to maintain
- Remote access
  - Difficult because of connection constraints
  - Want to make it humanly administrable
    - Critical to minimize cross-domain knowledge
- Utilize the peer-to-peer nature of xrootd

Proxies I (single firewall)



IN2P3

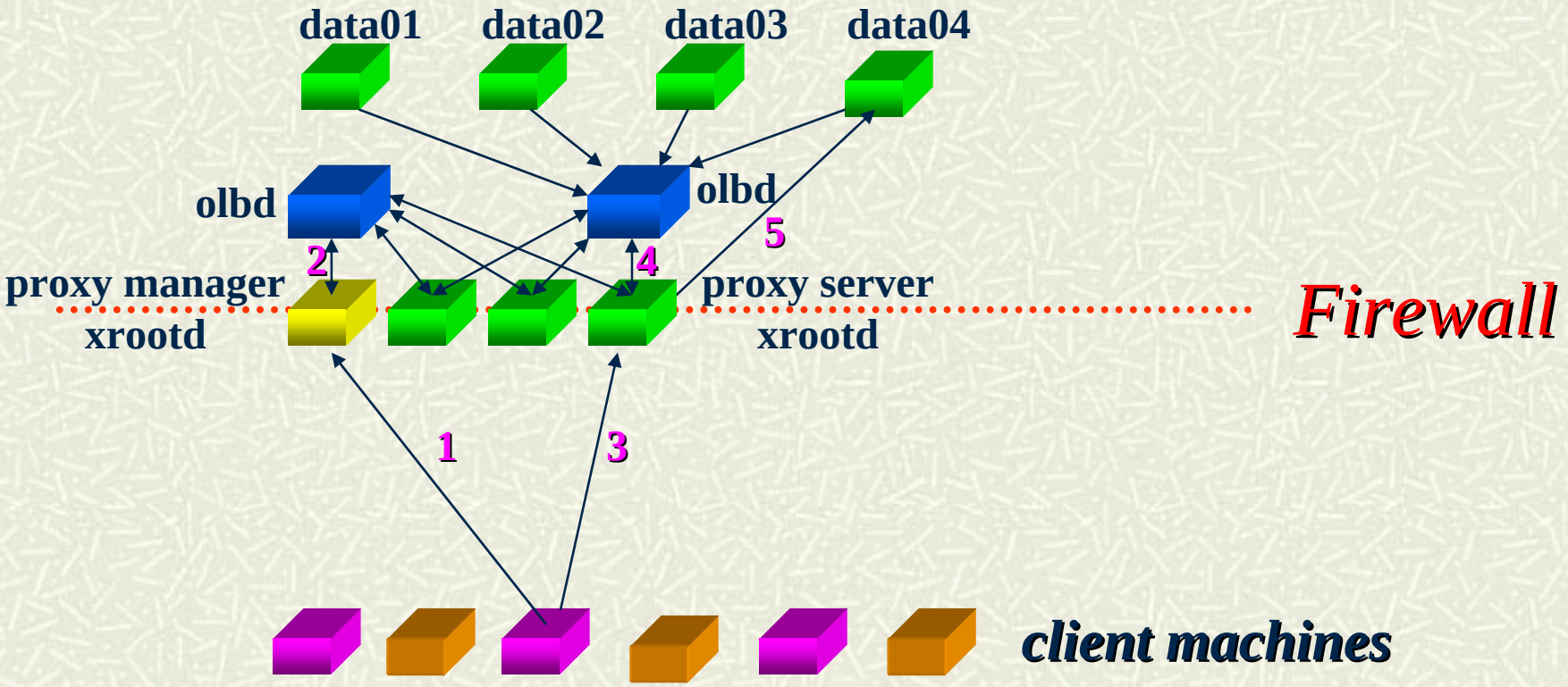
INDRA

Stanford Linear Accelerator Center

Scaling Proxies

- Need to provide more than one proxy
  - Selection criteria for proxies?
- Utilize natural rooted clustering
  - Create proxy clusters
  - Automatically load balance
  - No practical limit on number

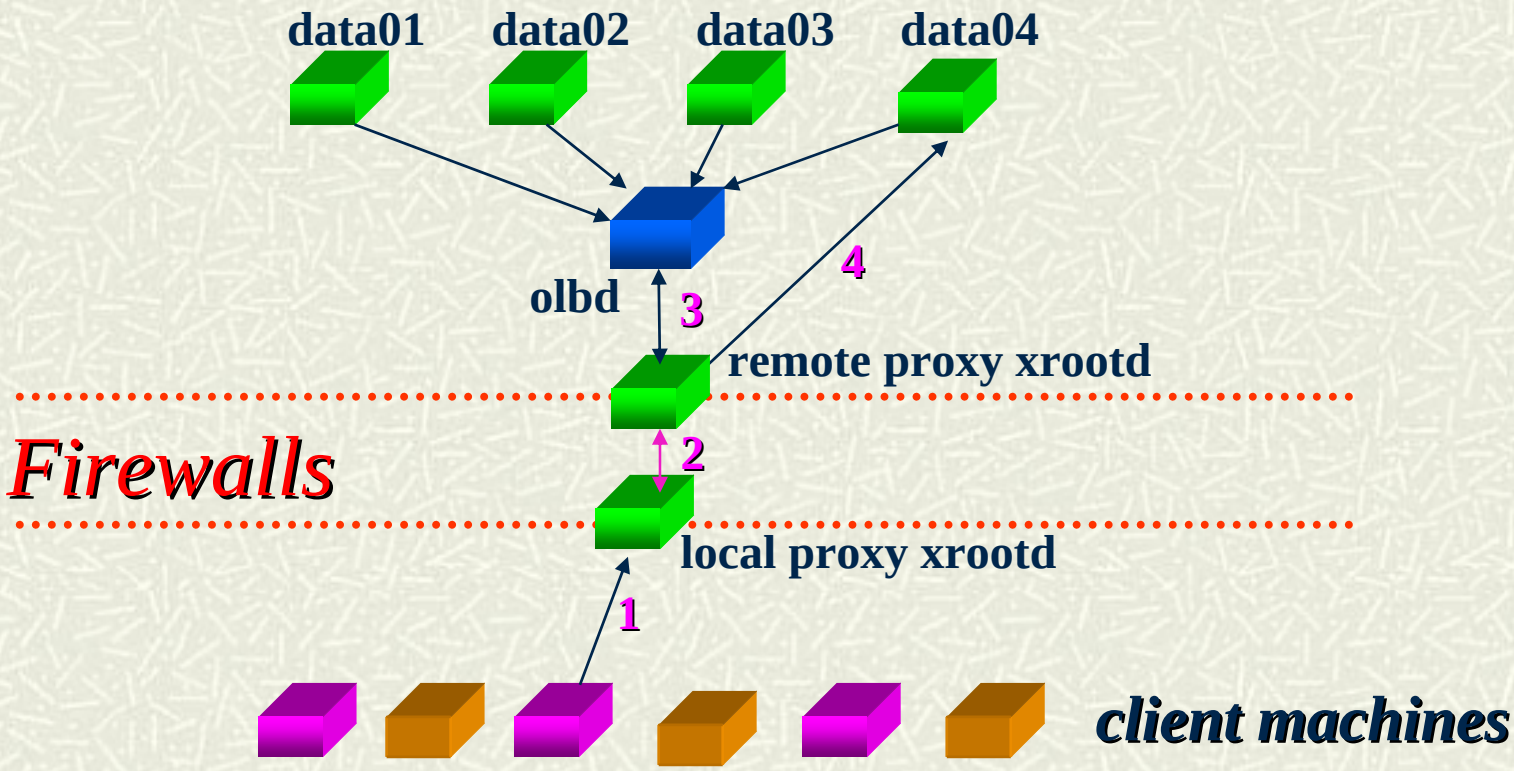
Proxy Clusters (single firewall)



Dealing With Lockdowns

- Double Firewalls
  - Reality sets in.
    - Incoming *and* outgoing traffic limited
- Utilize peer-to-peer nature of rooted
  - Maintains practical simplicity
- Alternative not particularly appealing
  - Application controlled firewall
    - LBL and ANL models for gridFTP.
  - Could use xrootd's for this as well, though.

Proxies II (double firewall, simplified)

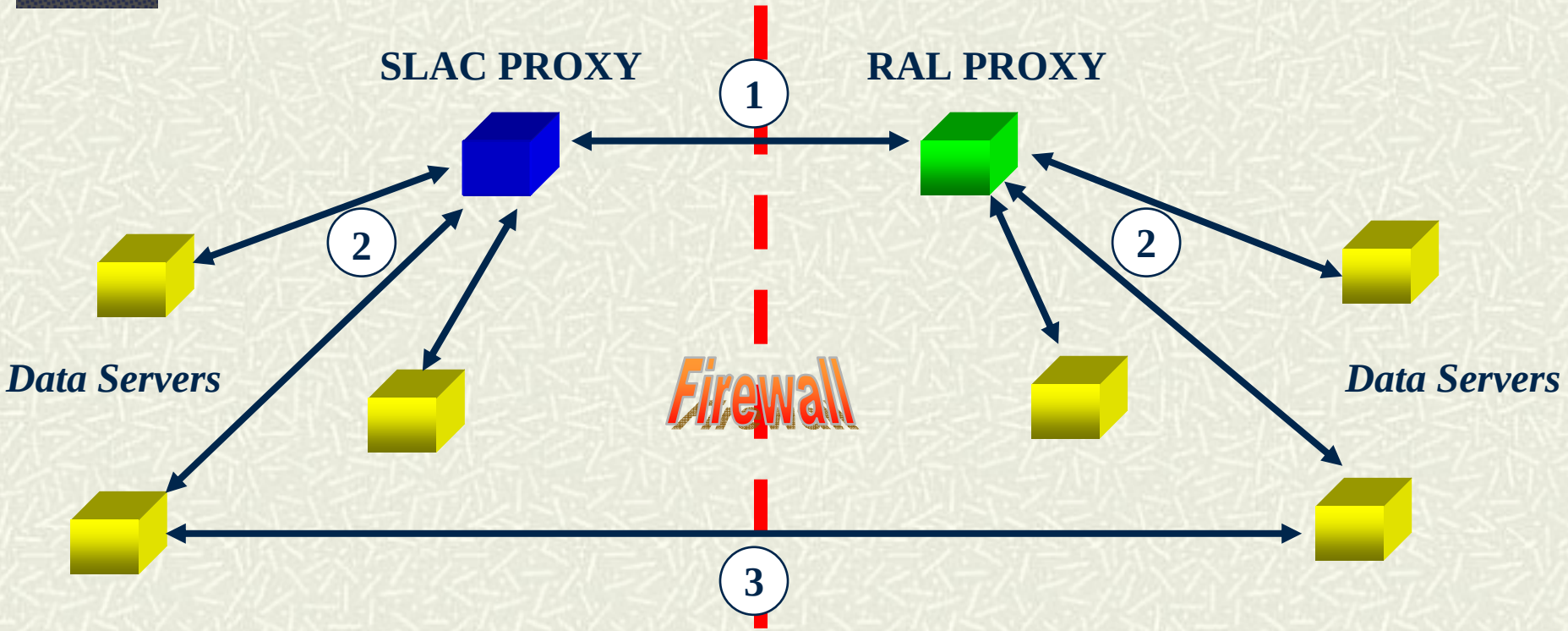


Stanford Linear Accelerator Center

N-to-M Authentication issues

- Clusters of proxies on each side
  - Random server-server connections
  - Authentication key management issues
    - Complex because of size and interactions
    - Would like to simplify key distribution
  - Use a security transformation
    - GSI to global session key

Scalable Proxy Security

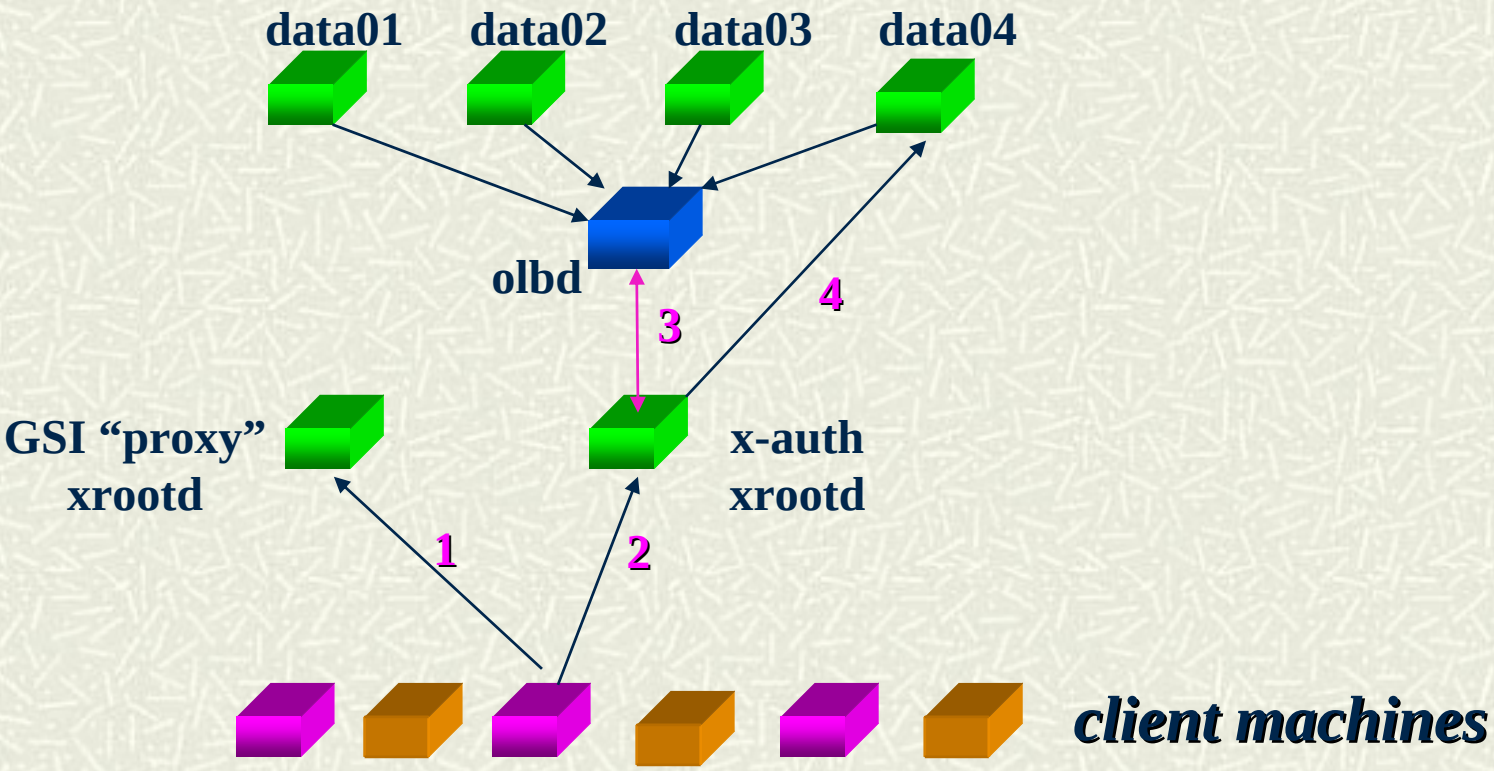


1 Authenticate & develop session key
2 Distribute session key to authenticated subscribers
3 Servers can log into each other using session key

Extending Security Transforms

- xrootd protocol allows security transforms
  - Redirect can pass along a CGI string
    - Anyone can redirect!
    - No practical redirect limit.
  - Allows security framework substitutions
    - Minimizes GSI intra-cluster overhead

Security Transforms



Stanford Linear Accelerator Center

Conclusion

- xrootd has a security enabling architecture
  - Protocol was designed with security in mind
  - Accommodates security transforms
    - Server-to-server
    - Client-server
  - Very easy to administer
    - Critical for maintaining security

Acknowledgements

- Software collaborators
  - INFN/Padova: Fabrizio Furano, Alvise Dorigao
  - Root: Fons Rademakers, Gerri Ganis
  - Alice: Derek Feichtinger, Guenter Kickinger, Andreas Peters
  - Cornell: Gregory Sharp
  - SLAC: Jacek Becla, Tofigh Azemoon, Wilko Kroeger, Bill Weeks
  - Princeton: Pete Elmer
- Operational collaborators
  - BNL, CNAF, FZK, INFN, IN2P3, RAL, SLAC