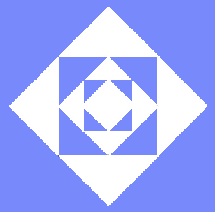


IBM

Capability based Secure Access Control to Networked Storage Devices

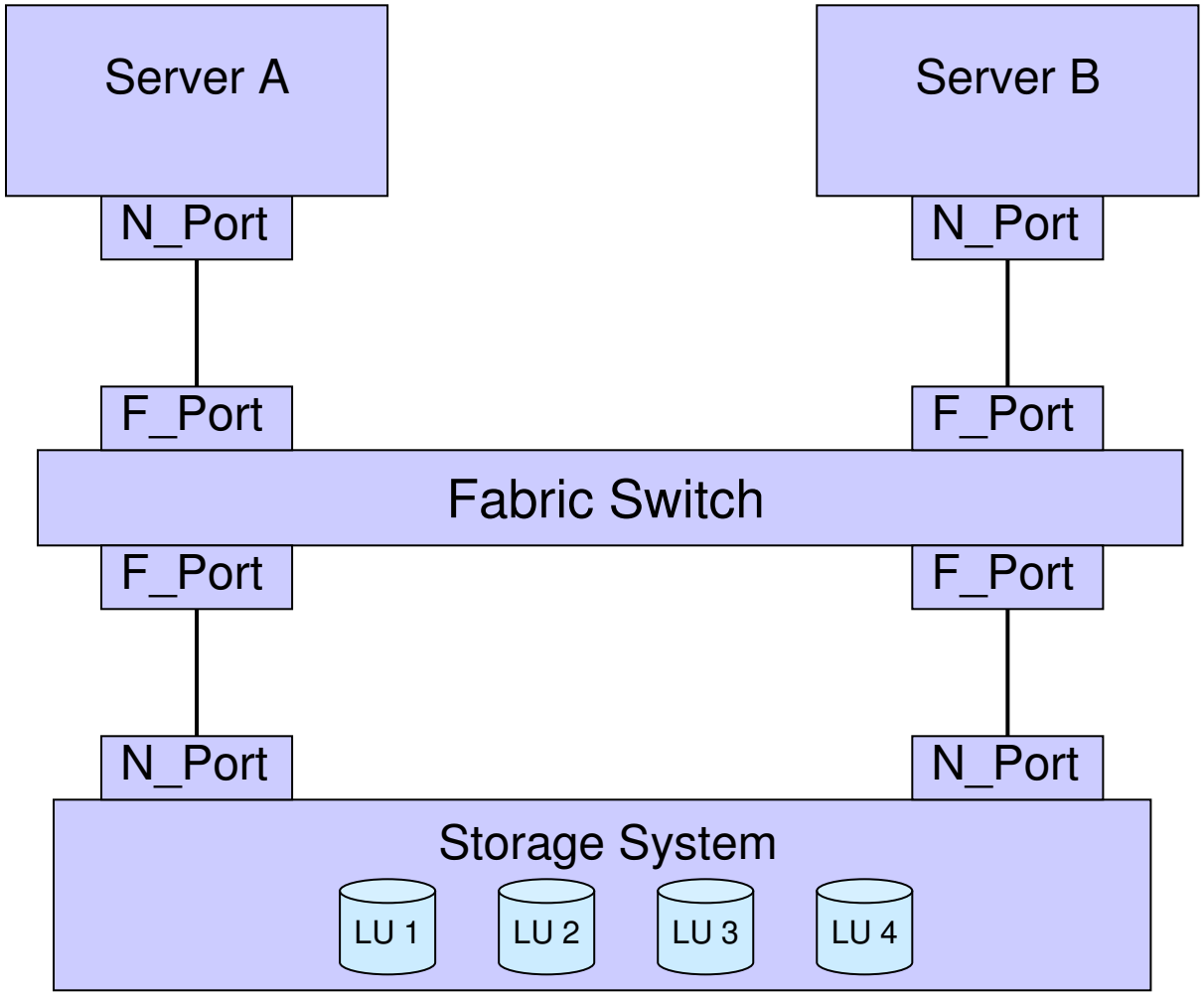
Michael Factor, Dalit Naor, Eran Rom, Julian Satran, Liran Shour and Sivan Tal

IBM Haifa Research Lab

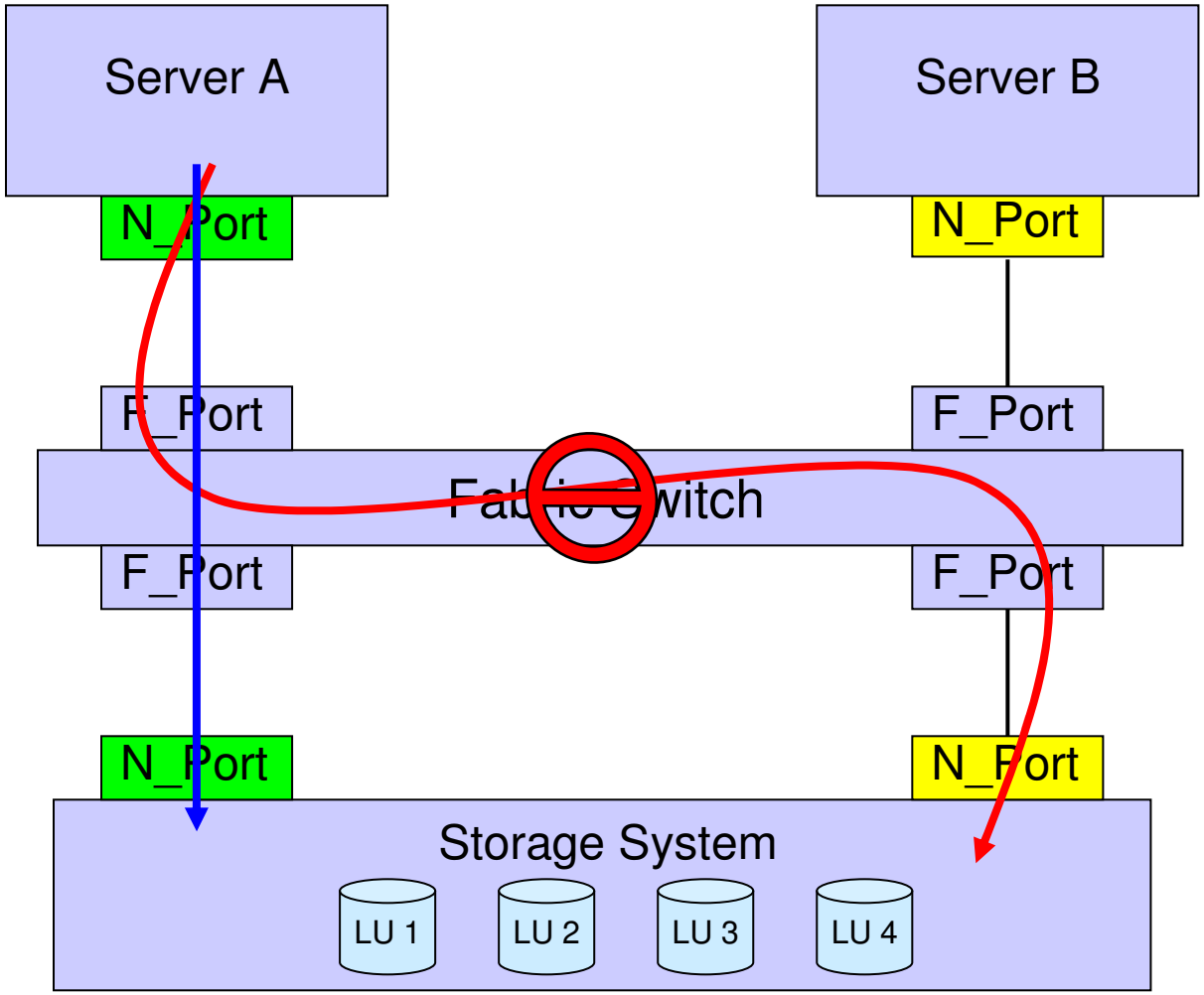
Agenda

- Current Access Control in the SAN.
- The OSD/CbCS Security protocol.
- The Implementation Architecture.
- I/O Path Performance Analysis.

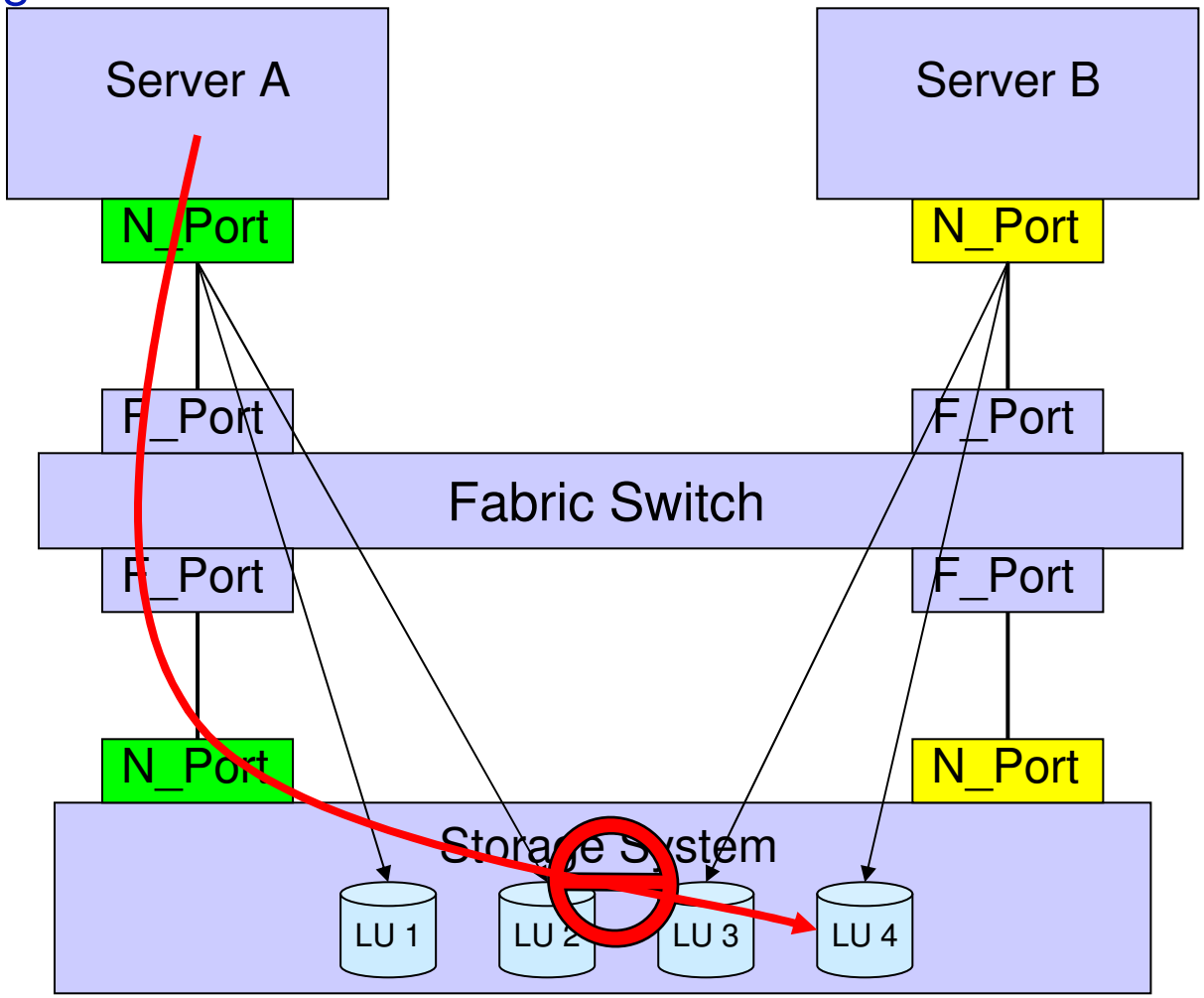
Storage Area Network



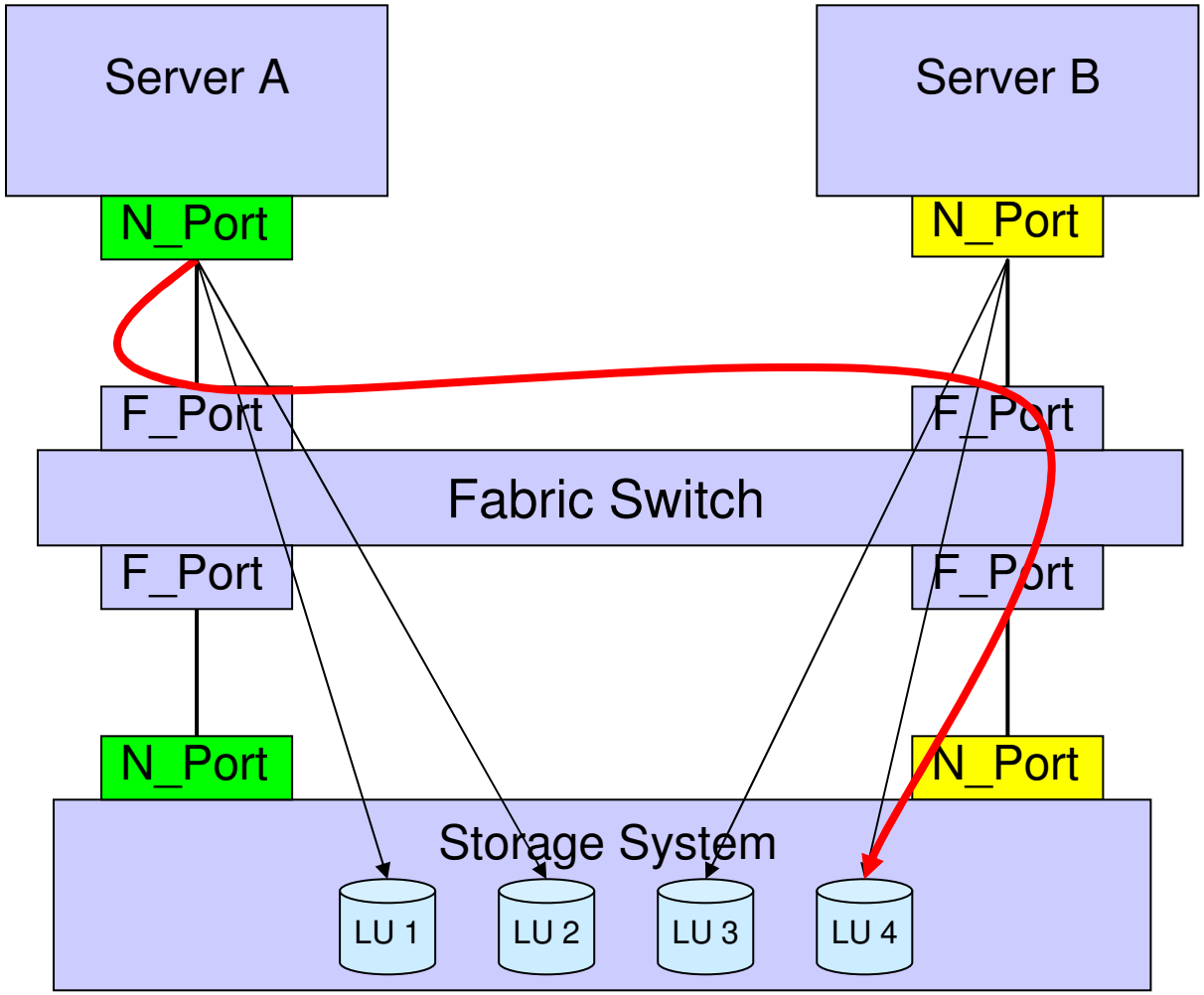
Access Control in the SAN Port Zoning



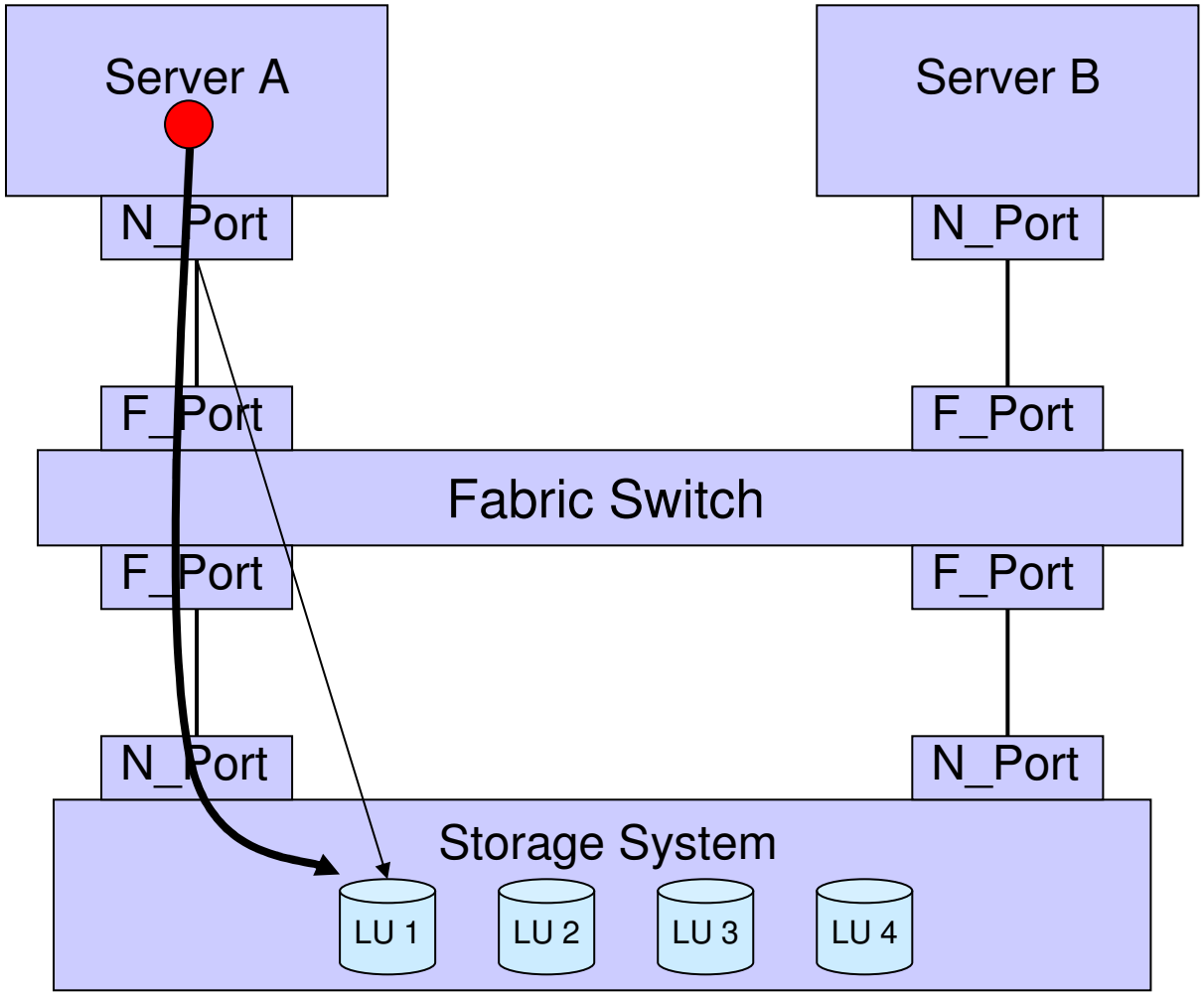
Access Control in the SAN
LUN Masking



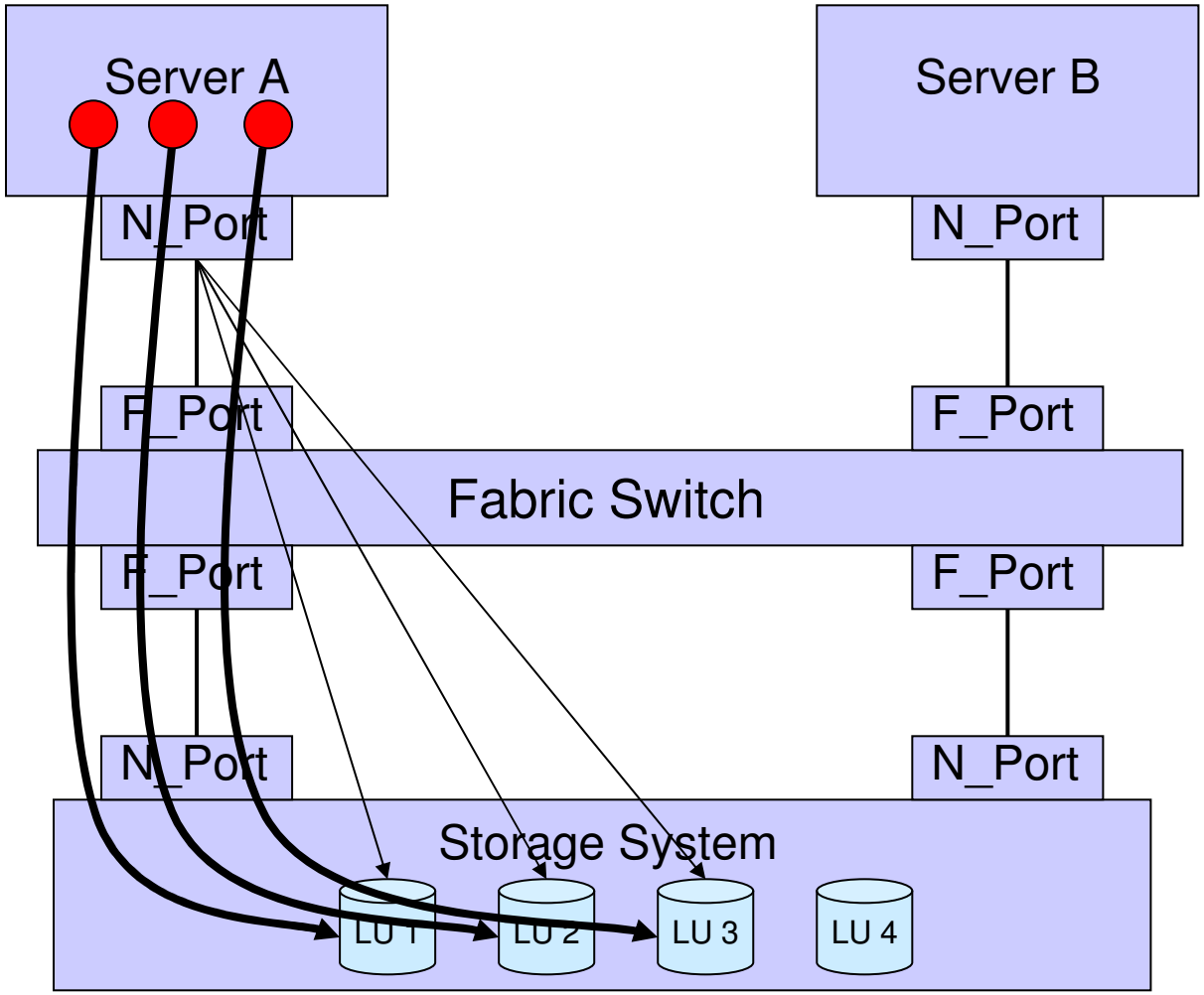
The Security Problem



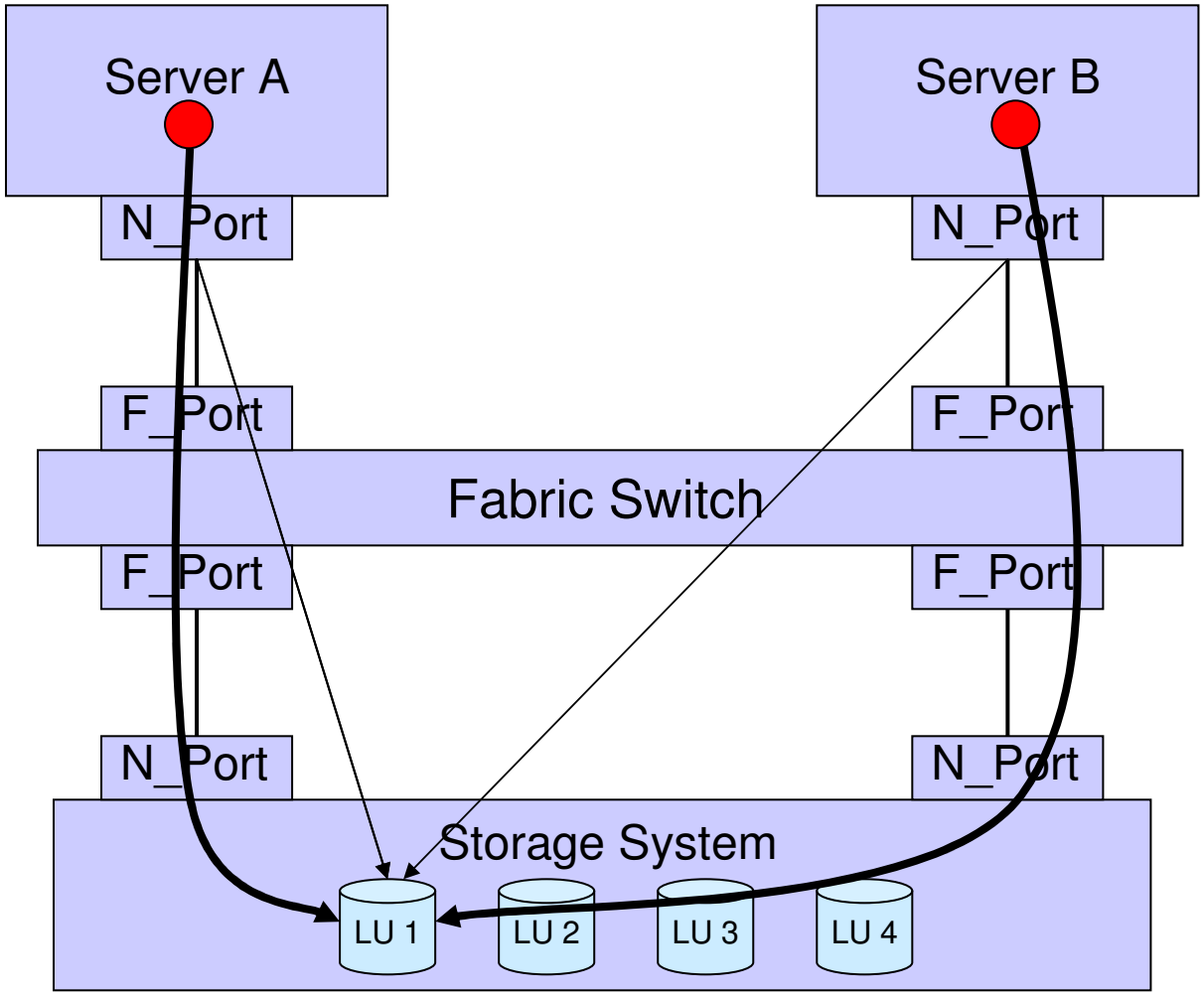
The Manageability Problem -1



The Manageability Problem -2



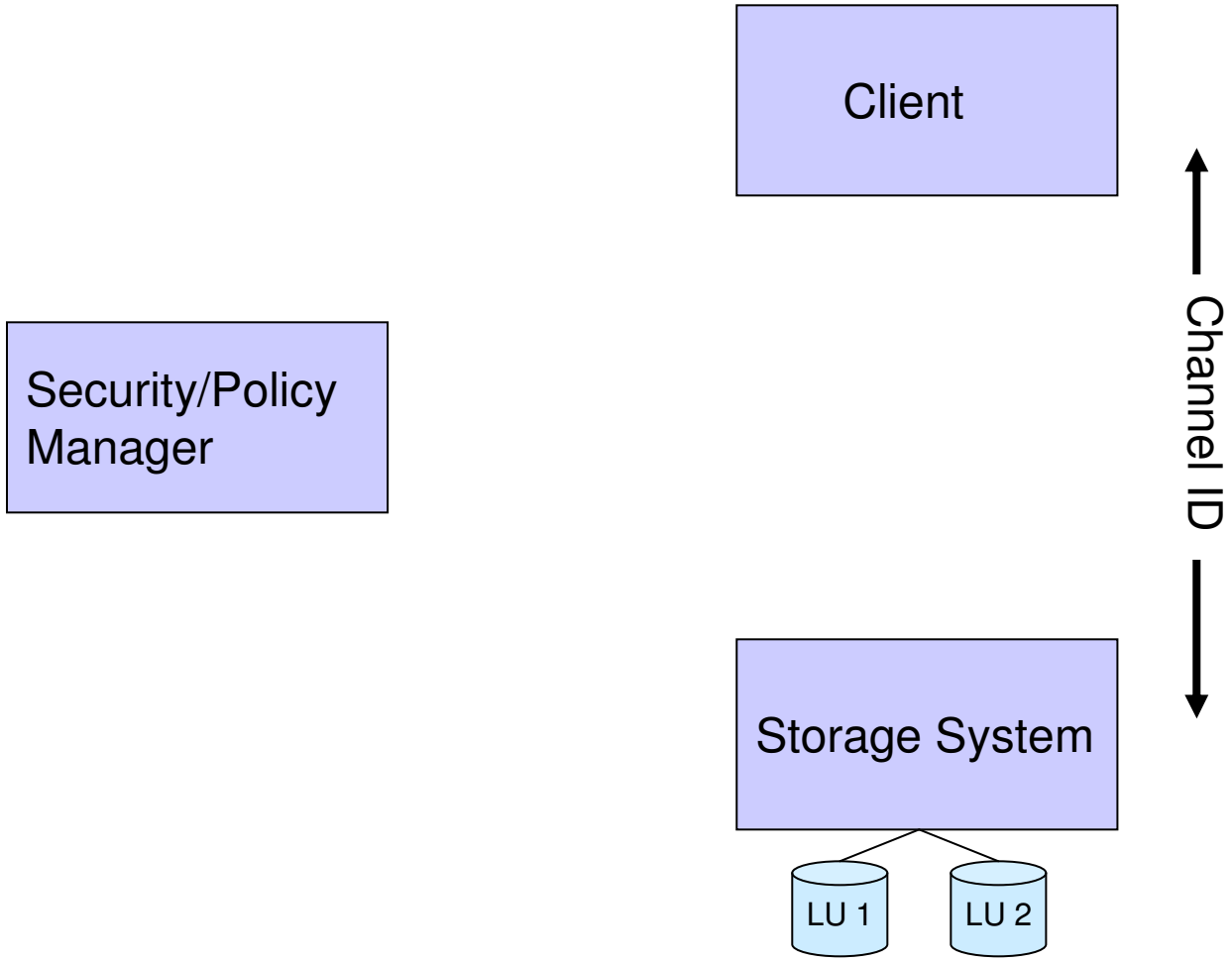
The Manageability Problem -3



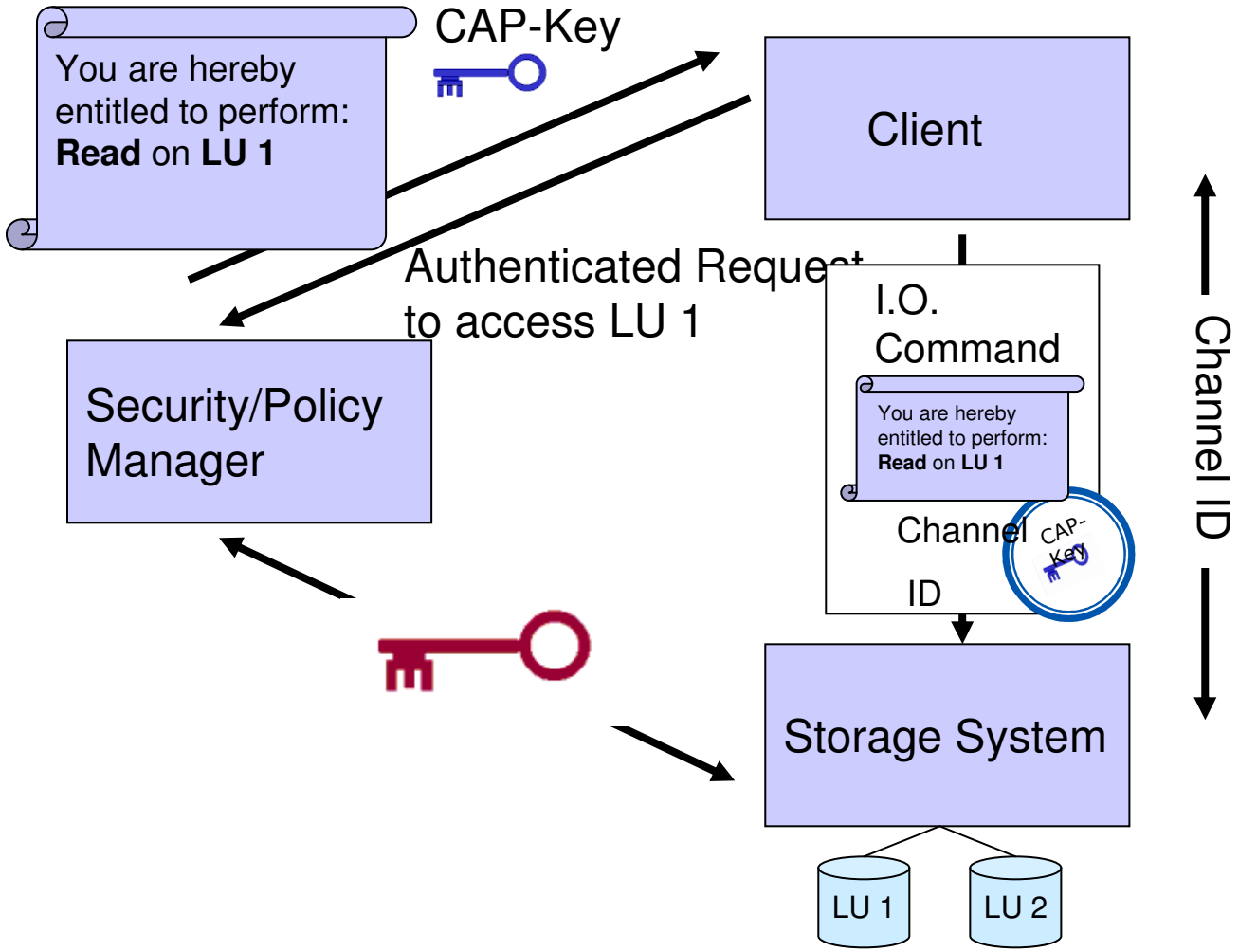
CbCS – Capability based Command Security

- Independent of the underlying transport layer
- Access control is enforced using cryptographically hardened capabilities validated at the storage
- The Capabilities are presented to the storage with every I/O command
- The Capabilities are retrieved from security manager – a single point of management
- The cryptographic hardening of capabilities assures that they cannot be forged, modified or replayed over different channels

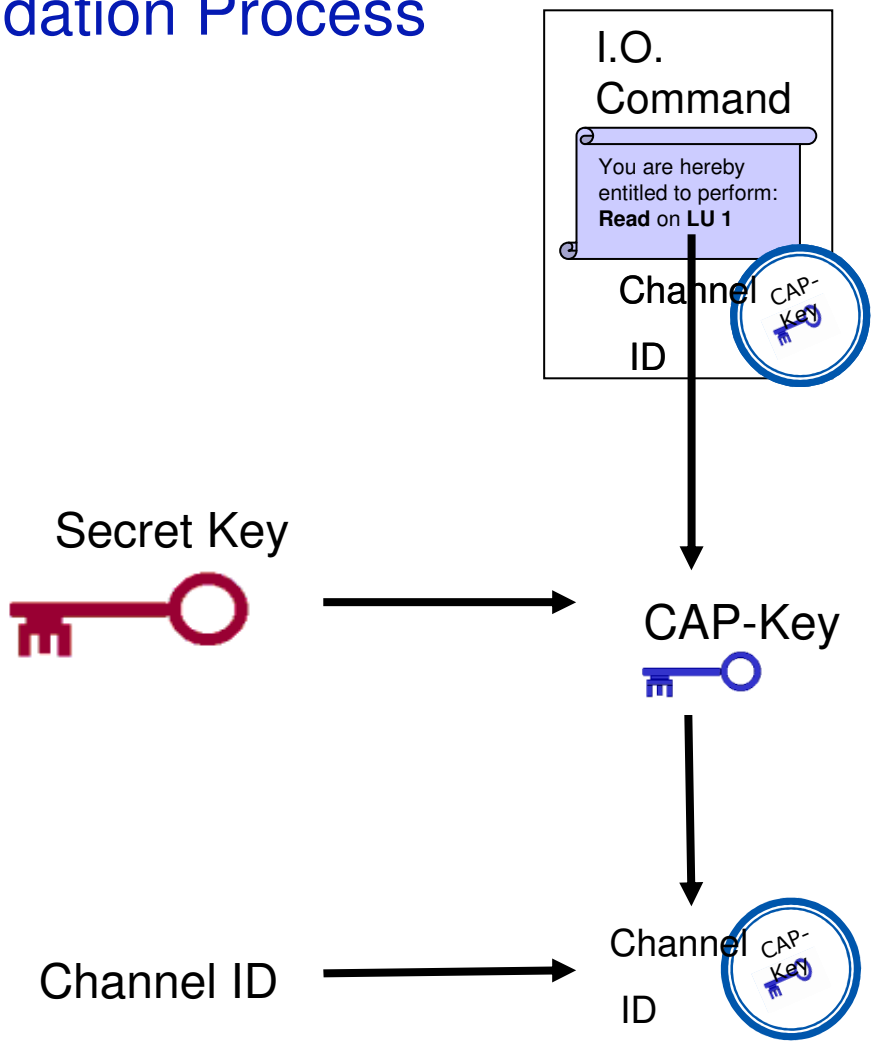
The OSD/CbCS Model



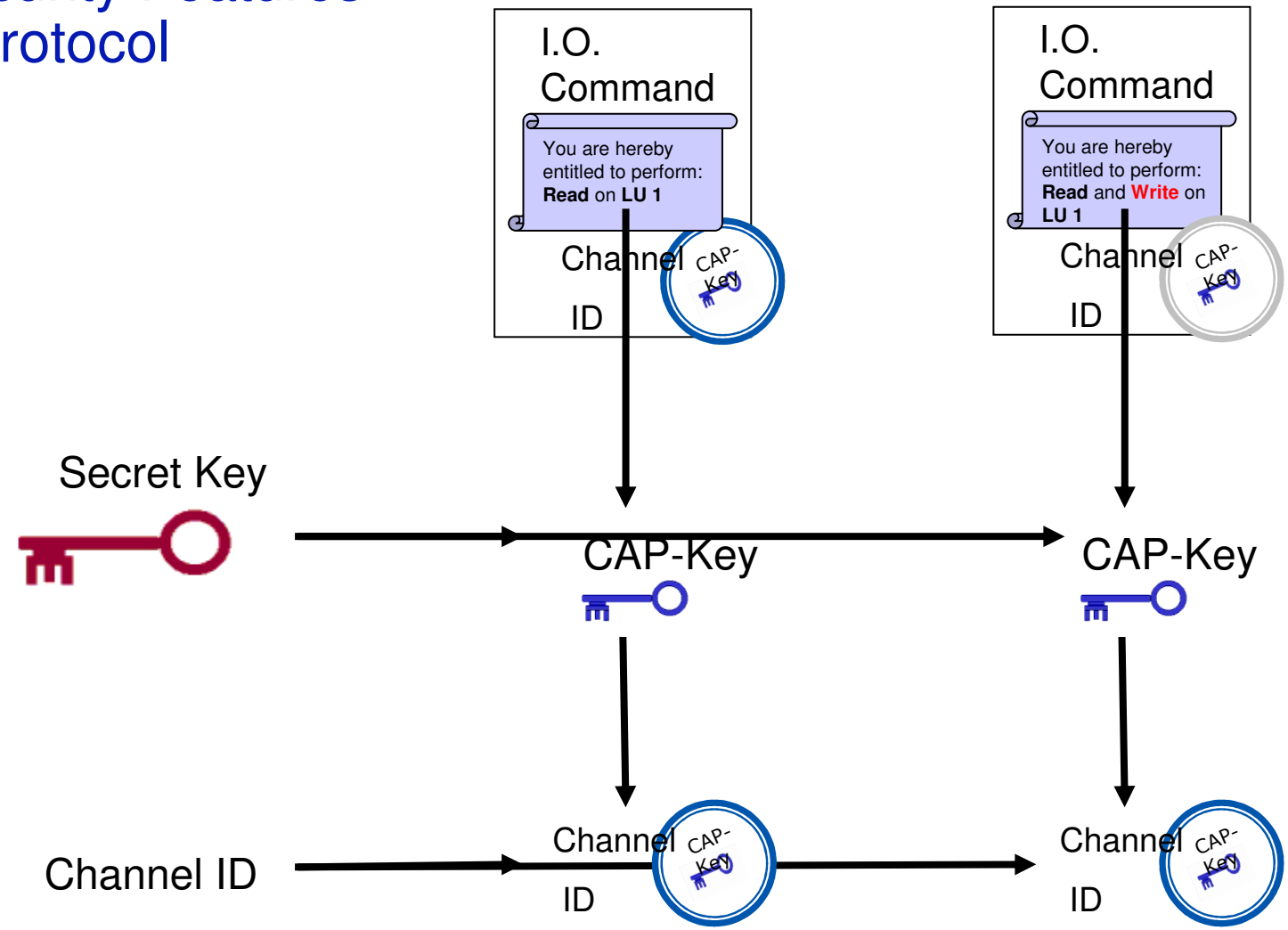
The OSD/CbCS Protocol



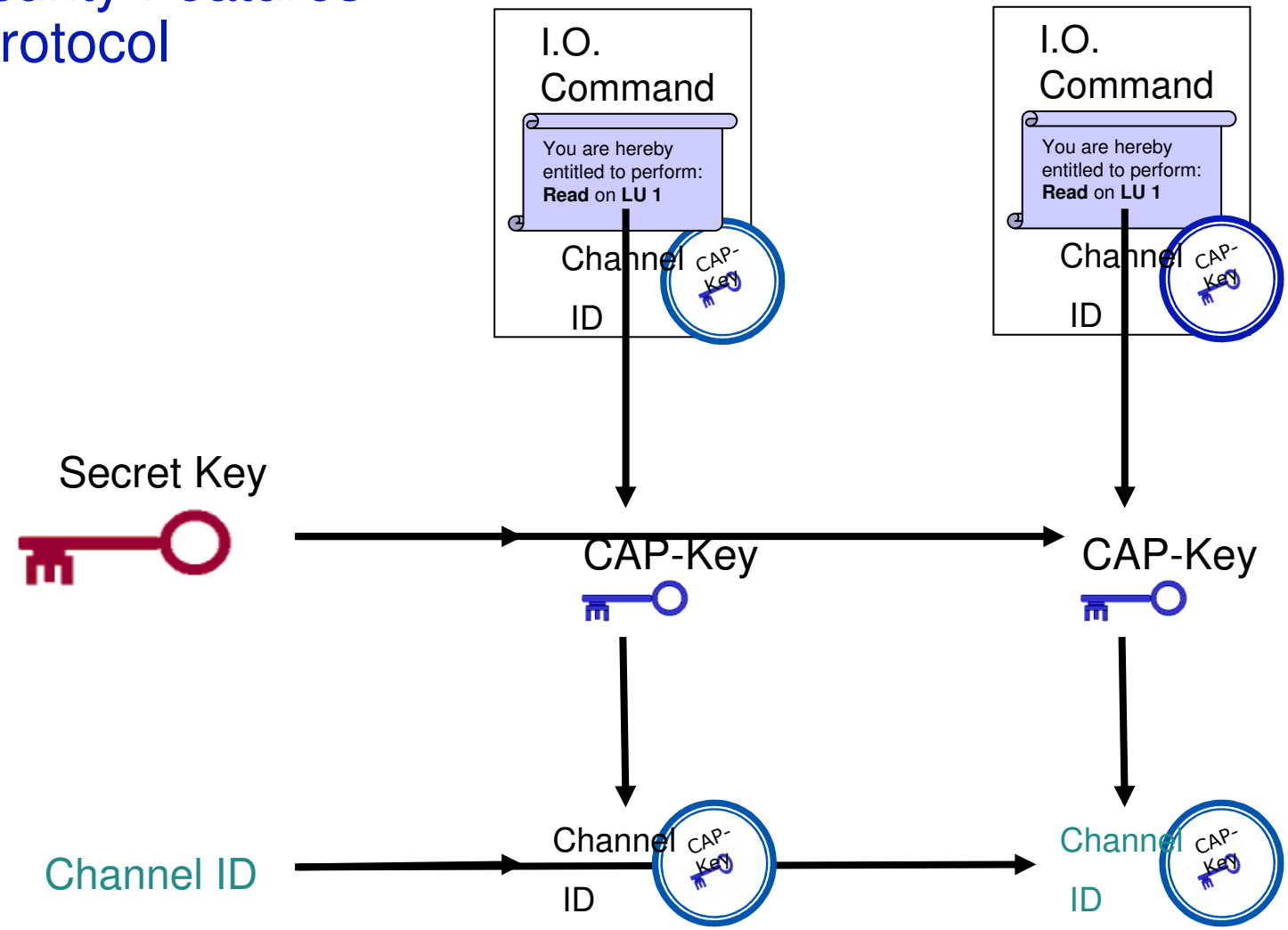
The Validation Process



The Security Features of the Protocol



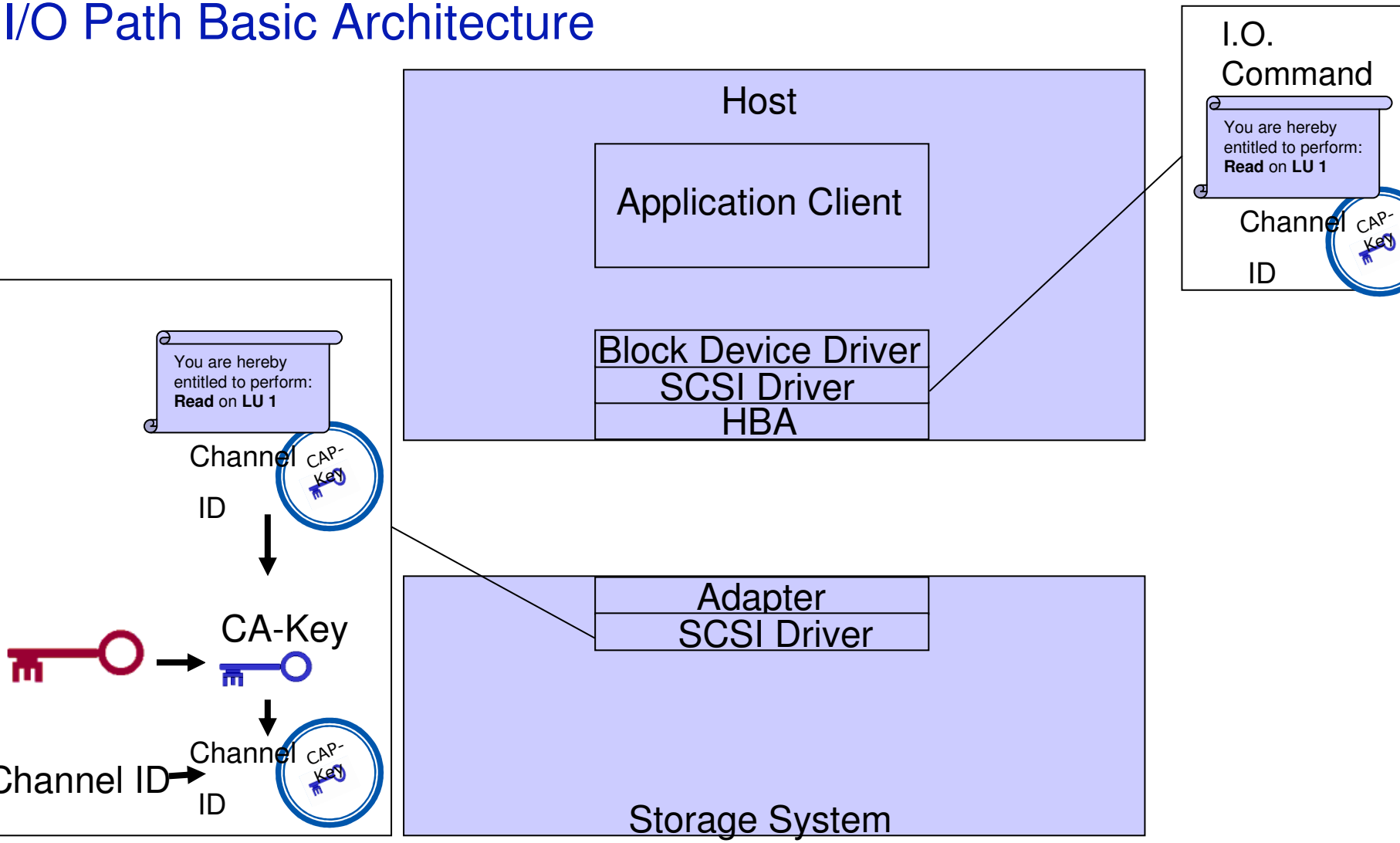
The Security Features of the Protocol



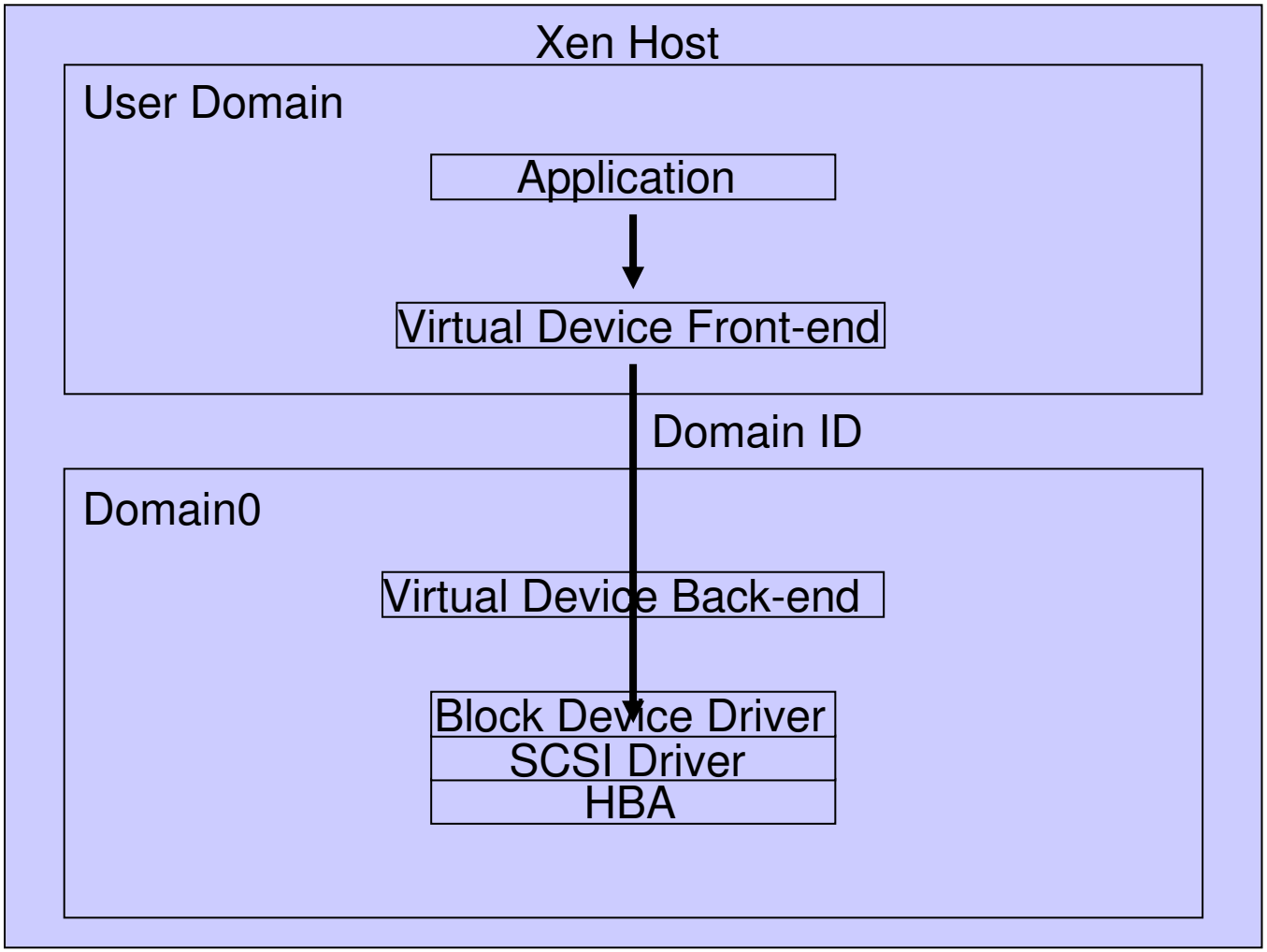
CbCS Vs. Zoning/Masking

	Traditional zoning/Masking	Zoning/Masking with NPIV/FC-SP	CbCS
Prevents identity spoofing	No	Yes	Yes
Supports differentiated access per command	No	No	Yes
Supports physical adapter/port sharing	No	Yes	Yes
Transport layer independent	No	No	Yes
Single point of management	No	No	Yes

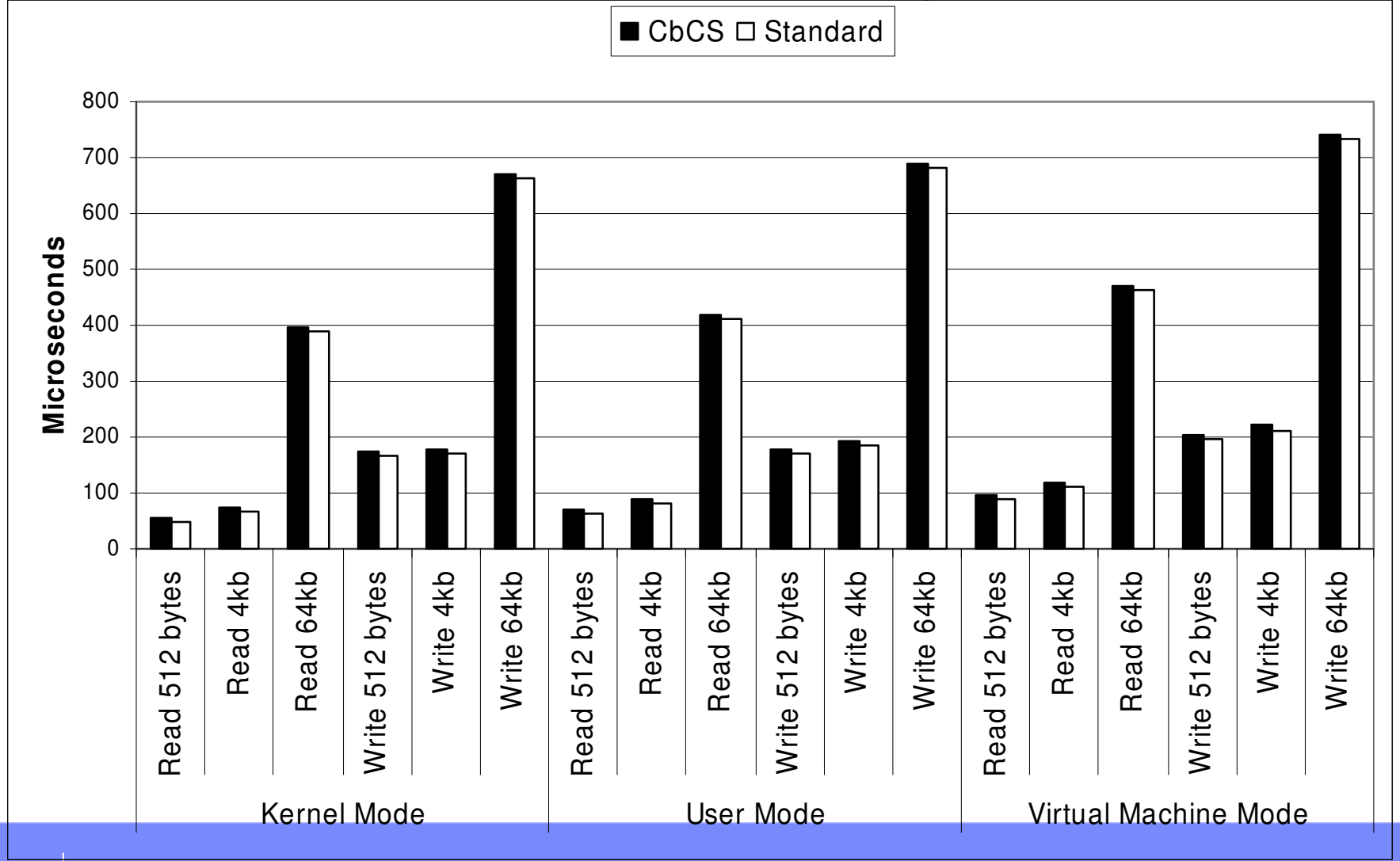
I/O Path Basic Architecture



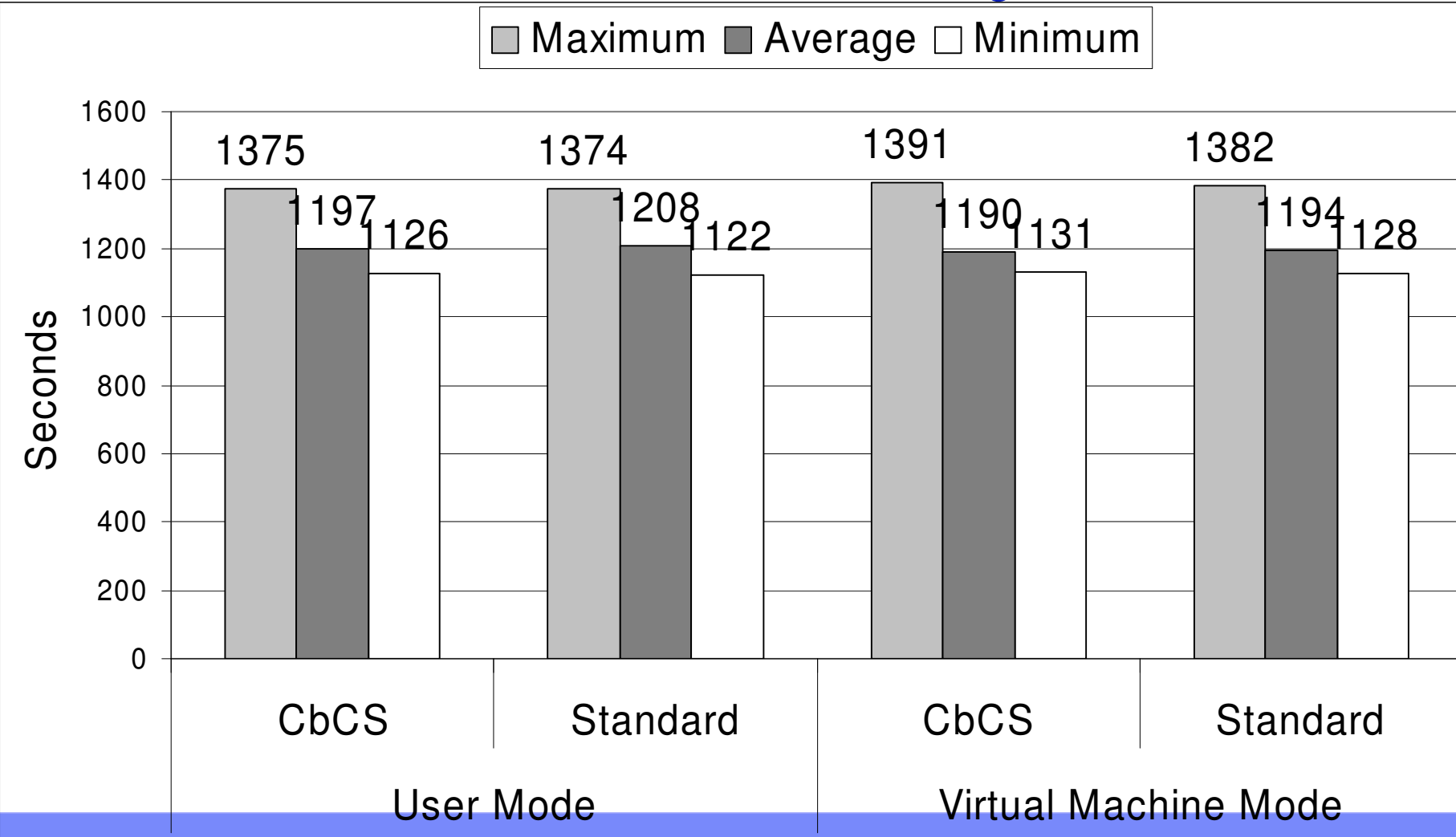
I/O Path Implementation in Xen



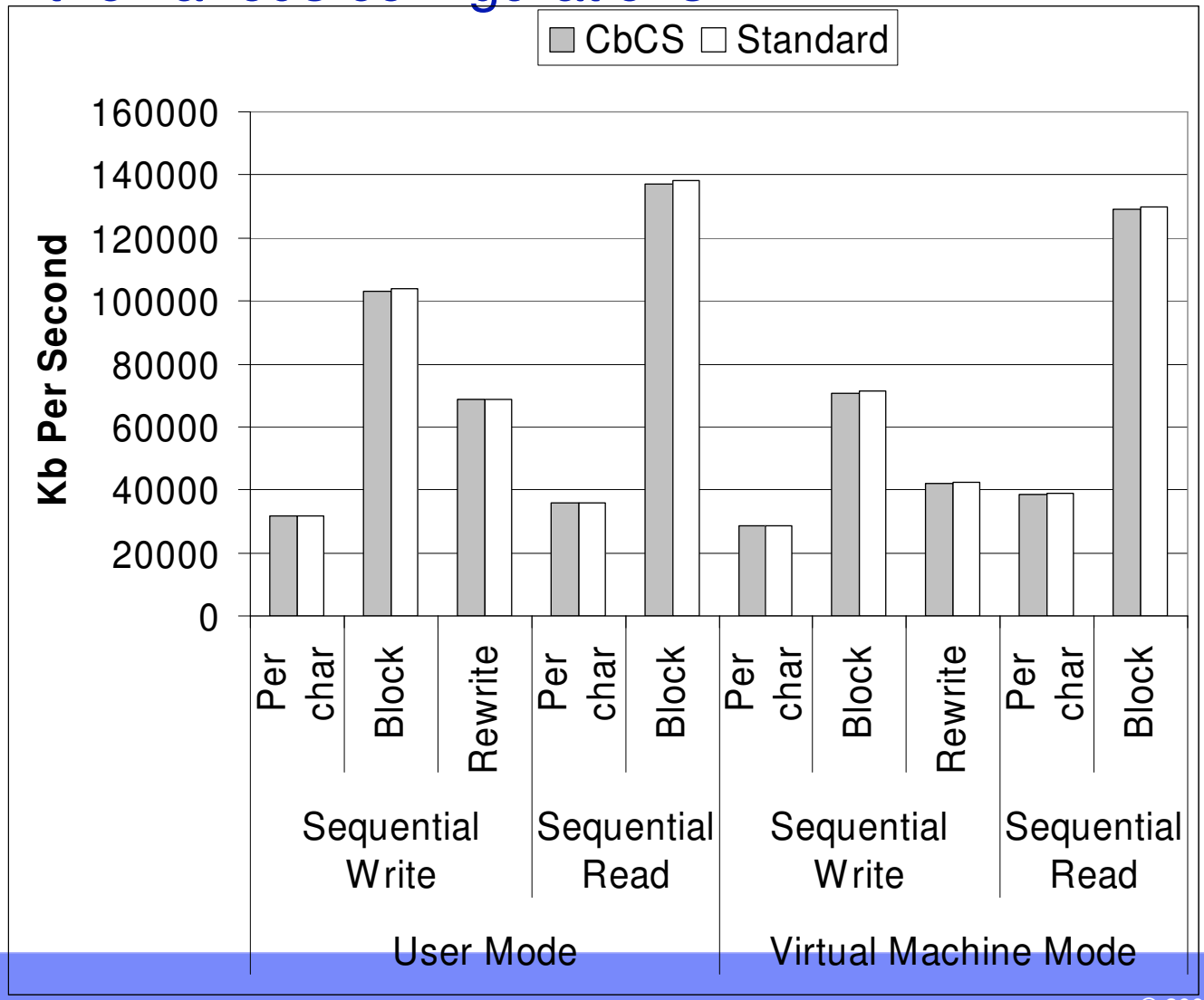
Synthetic Sequential I/O: Constant Overhead of ~8 Microseconds per Command



Postmark Benchmark – Minimum, Average and Maximum of total 50 execution times in the various configurations



Bonnie++ Benchmark – Sequential Read and Write Average Rates in the various configurations



Concluding Remarks

- CbCS presents a good manageable and secured solution for access control in the SAN.
- The solution can be implemented without changing the underlying storage network, workloads or storage layout.
- CbCS incurs minimal time overhead.
- CbCS is a proposed standard, currently under review in the T10 technical committee.