Harnessing Multicore Processors for High Speed Secure Transfer

Raj Kettimuthu
Argonne National Laboratory

Security

- Clear
  - No security at all
- Authentication
  - Verify the connection only, data is clear
- Integrity
  - Verify each packet, data is clear
  - High processing requirements
- Private
  - Encrypt all data
  - Very high processing requirements

Security

- Security context
  - Includes a symmetric key
  - Associated with each TCP connection
  - Used for faster security processing
- Cipher Block Chaining
  - TLS/SSL, GSI, etc
  - Previously encrypted cipher text is used in the encryption of the current block
  - Cannot parallelize

High Performance Transfers

- True security makes the CPU the bottleneck
  - Thus auth or clear are selected
  - there is no data integrity
- Post transfer checksums
  - Used to verify data once transfer completes
  - Should be considered part of transfer time
  - Less efficient (most re-open and read data)
  - cannot parallelize

Parallel Streams

- Multiple TCP streams between endpoints
  - Network optimization
  - Used to work around TCP backoff
- A security context with each stream
  - Can use to parallelize security processing
  - Each stream has own context
  - cipher block chain associated with that context

Multiple Cores

- Up coming technologies
  - Quad core commodity
  - Future will bring .....
- Parallel processing power
  - No increase in memory
  - No increase in bus bandwidth
  - No increase in NIC bandwidth
- Increases the ratio of processing power to network speed

Transfer Resources and Streams

- Memory needed is a function of BWDP
  - $BWDP_{total}$ = RTT * BW
- Parallel streams do not increase the BDWP
  - Each stream shares an equal portion
  - $BWDP_{stream}$ = RTT * (BW/|streams|)
- Required resources are not a function of |streams|
  - memory is function of BWDP
  - bus/disk/NIC speed is a function of transfer rate

Full Encryption

- Perfect application of multiple cores
  - 1 stream per processor
  - Allows parallelism of security processing
  - Requires a core, but no more memory
  - Results show linear or close to linear increase on different dual-core architectures
  - Some interesting results on dual-core architectures with hyper threading

Results

- Pentium Dual Core 1.1 GHz

Security Level	Single P1	Single P2	Pool P1	Pool P2
Clear	814	818	816	818
Authenticated	812	814	813	816
Safe	169	178	164	285
Private	76	78	75	138

Results

- Itanium Dual Core 1.2 GHz

Security Level	Single P1	Single P2	Pool P1	Pool P2
Clear	903	905	903	906
Authenticated	899	899	899	899
Safe	488	517	488	770
Private	177	183	177	340

the globus alliance
www.globus.org

Results

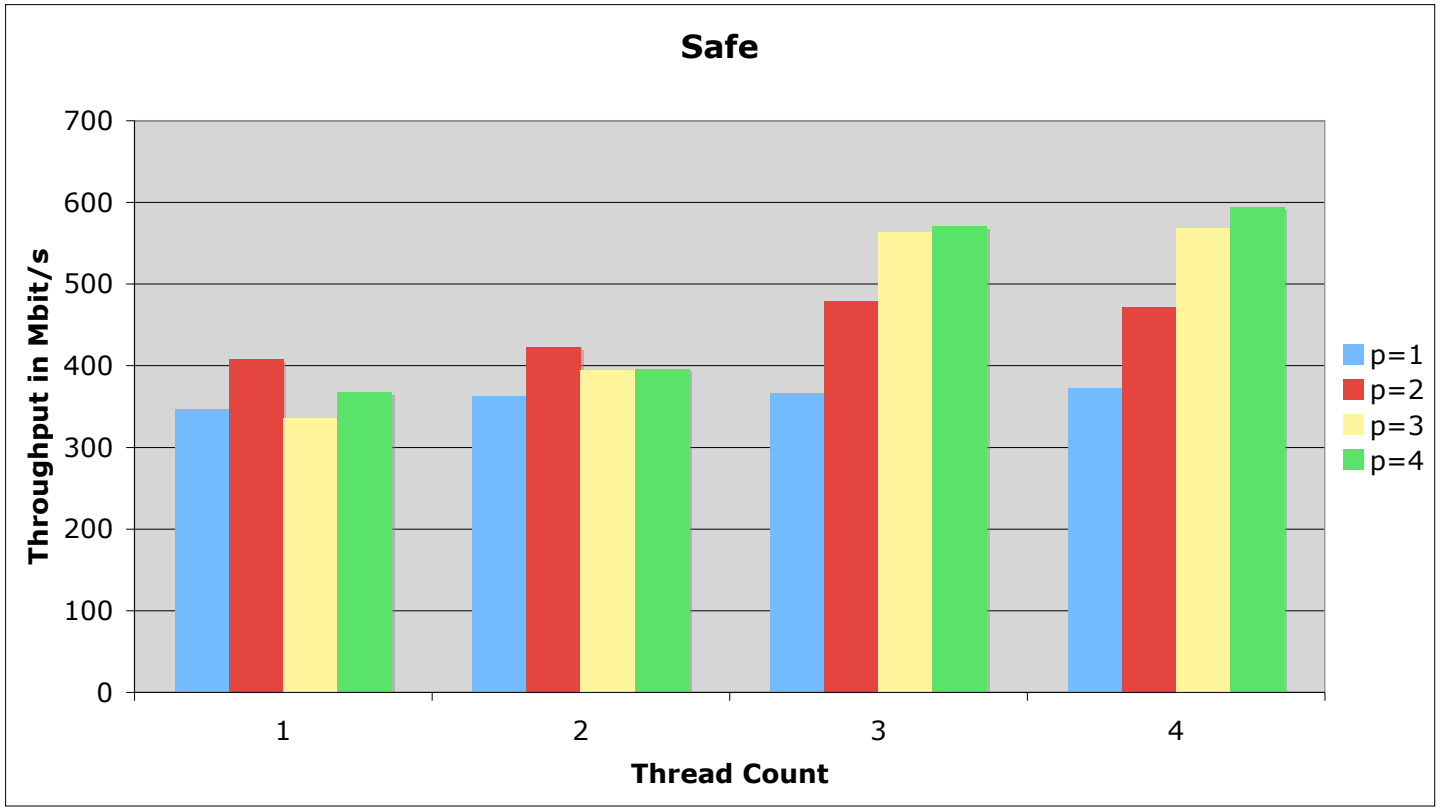
- Opteron 64 bit Dual Core 2.4 GHz

Security Level	Single P1	Single P2	Pool P1	Pool P2
Clear	897	897	897	897
Authenticated	897	897	897	897
Safe	254	268	254	471
Private	100	101	100	196

the globus alliance
www.globus.org

Results

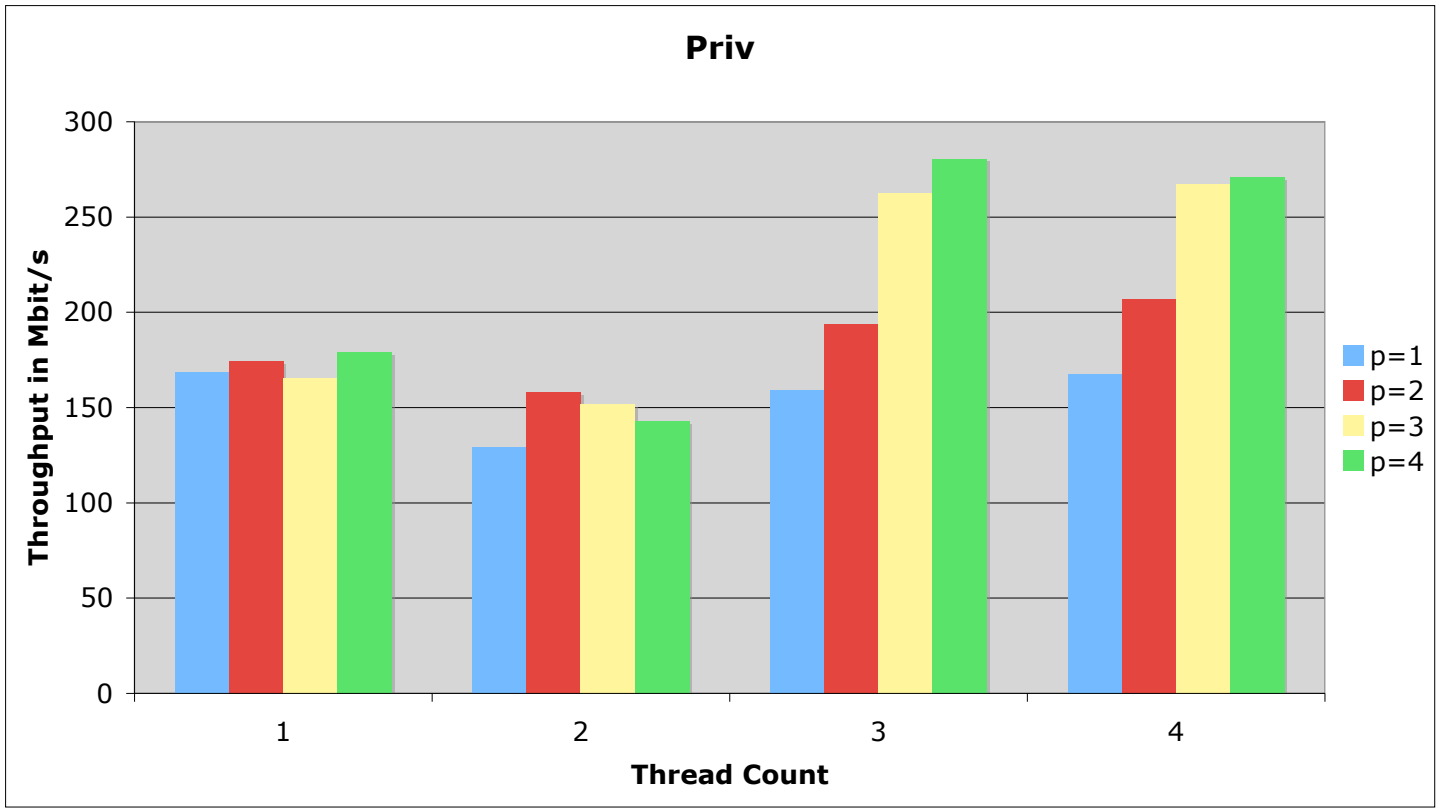
- Xeon dual core 2.8 GHz with hyper threading



the globus alliance
www.globus.org

Results

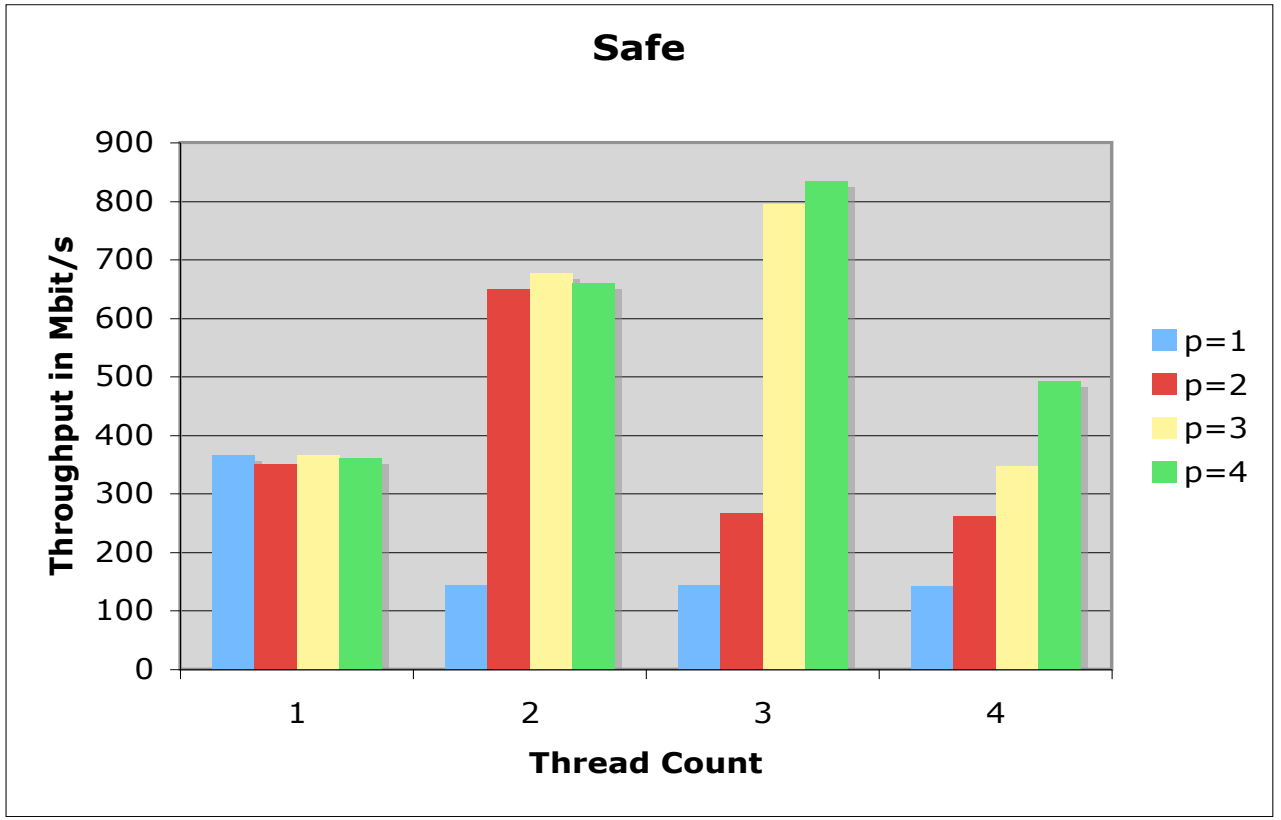
- Xeon dual core 2.8 GHz with hyper threading



the globus alliance
www.globus.org

Results

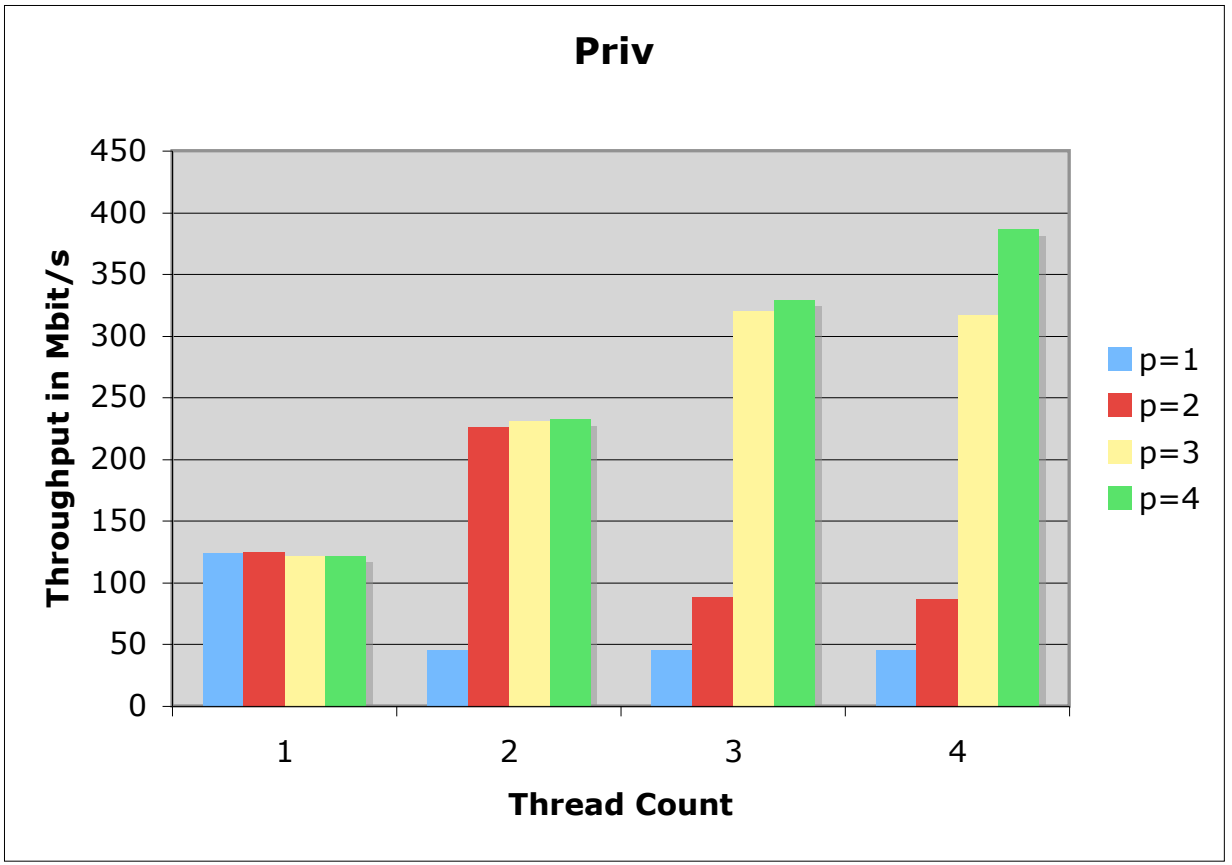
- Opteron dual core 1GHz with hyper threading



the globus alliance
www.globus.org

Results

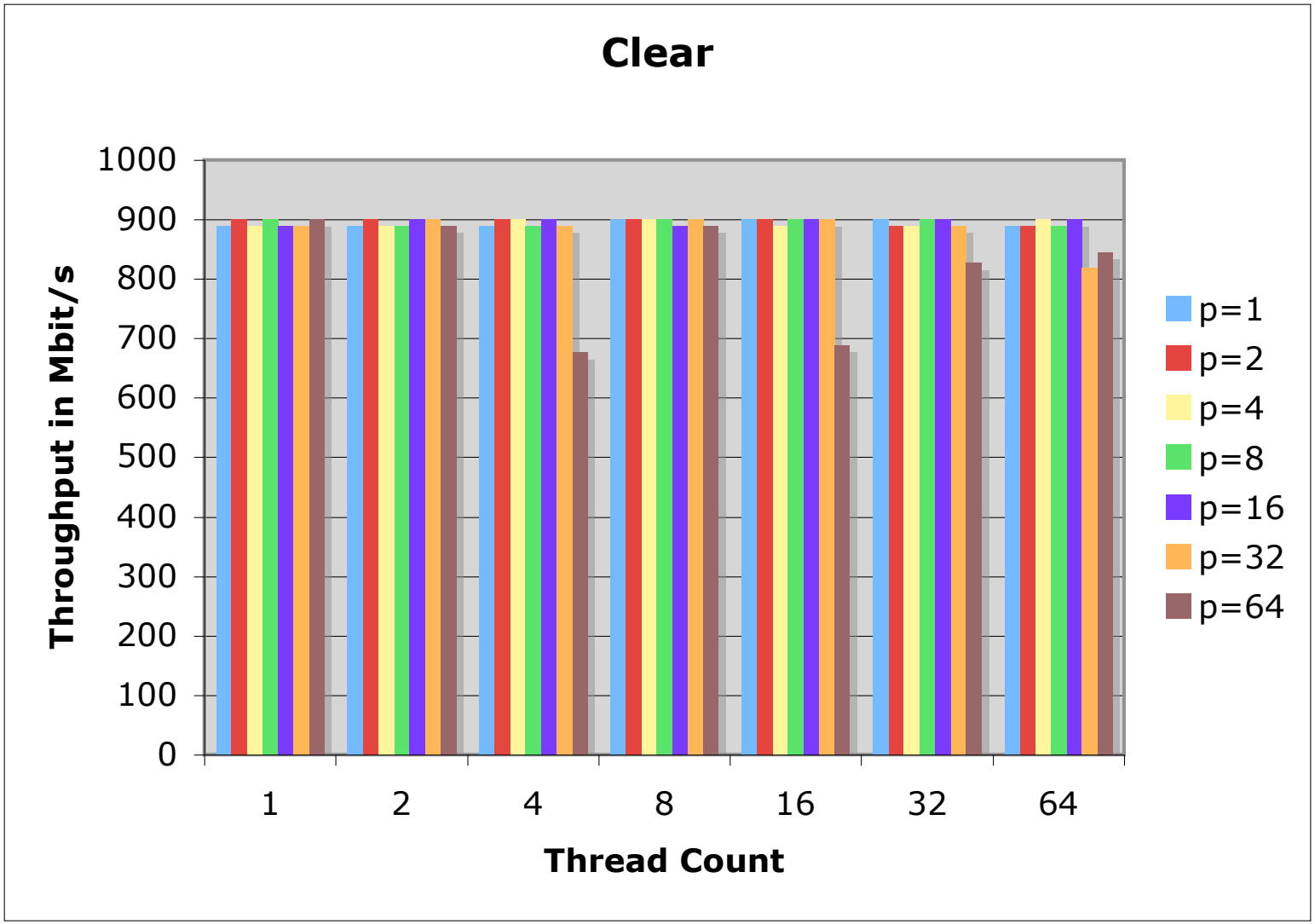
- Opteron dual core 1GHz with hyper threading



Results

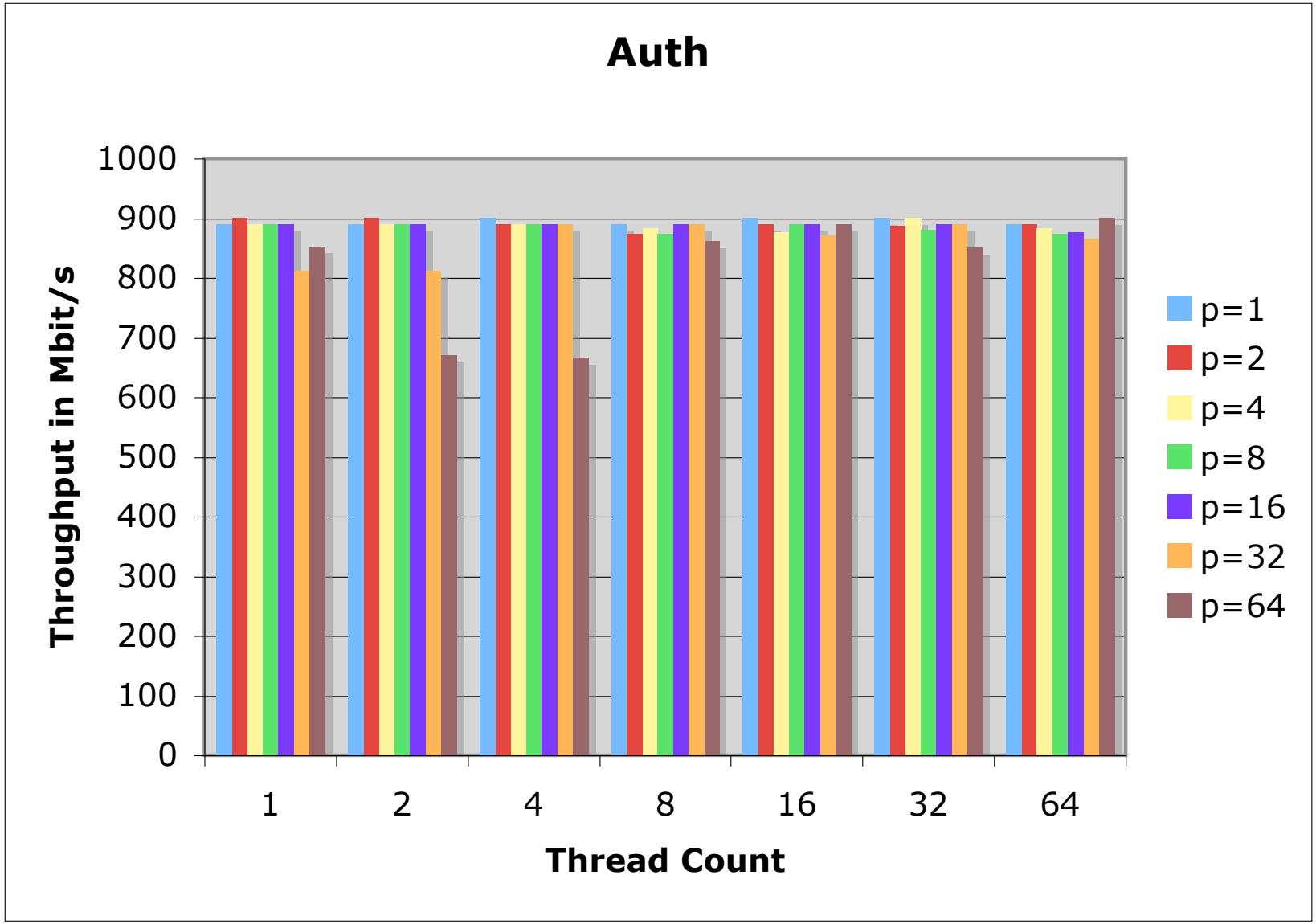
- Experiments to see the effect of high thread count and high number of parallel streams
- |Stream| > min(|CPU|, |Thread|) does not fetch much benefit
- |Thread| > |CPU| does not fetch any benefit - it seems to hurt the performance

Results


Clear
Throughput in Mbit/s
1000
900
800
700
600
500
400
300
200
100
0
1
2
4
8
16
32
64
Thread Count
p=1
p=2
p=4
p=8
p=16
p=32
p=64

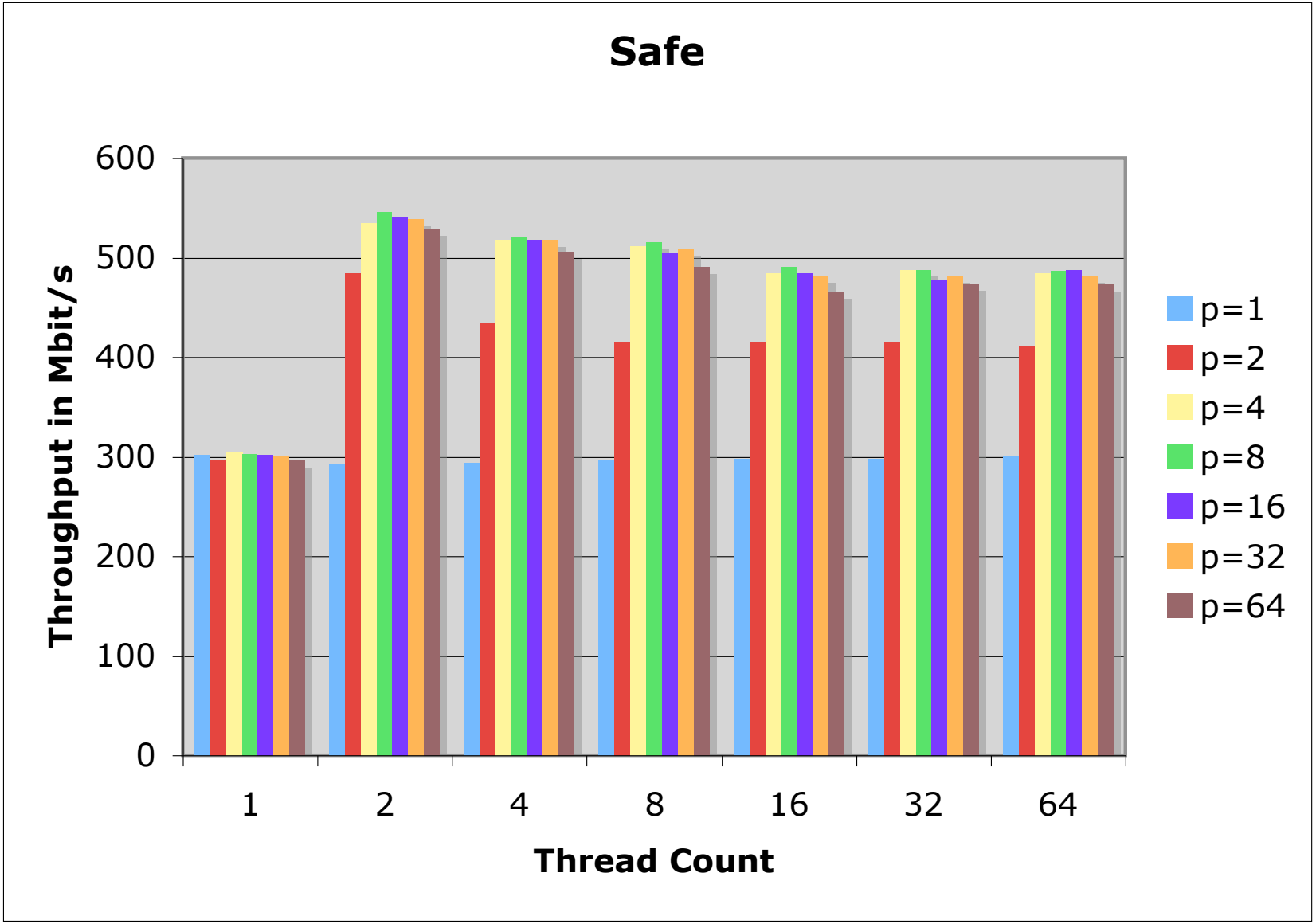
the globus alliance
www.globus.org

Results



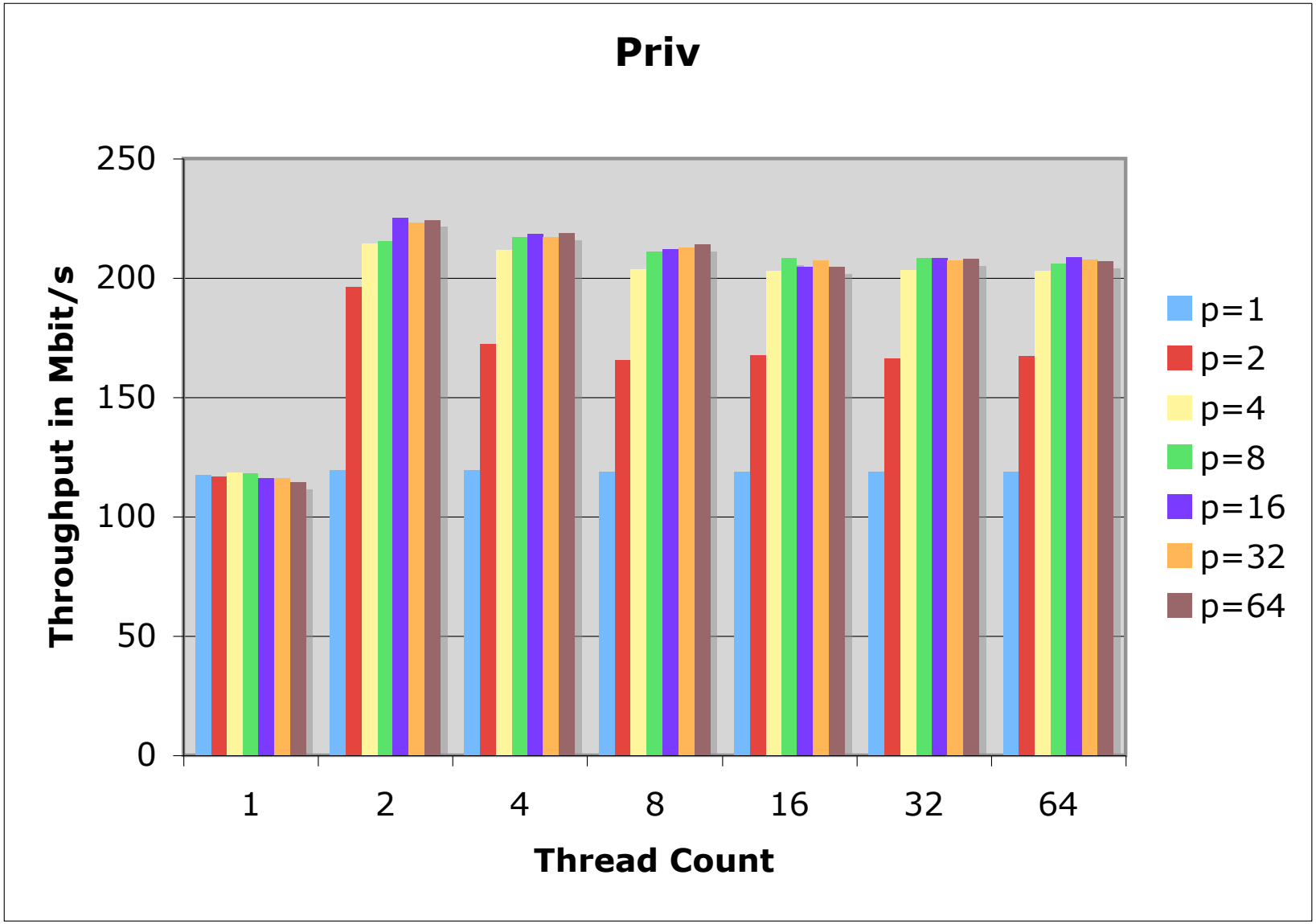
the globus alliance
www.globus.org

Results



the globus alliance
www.globus.org

Results

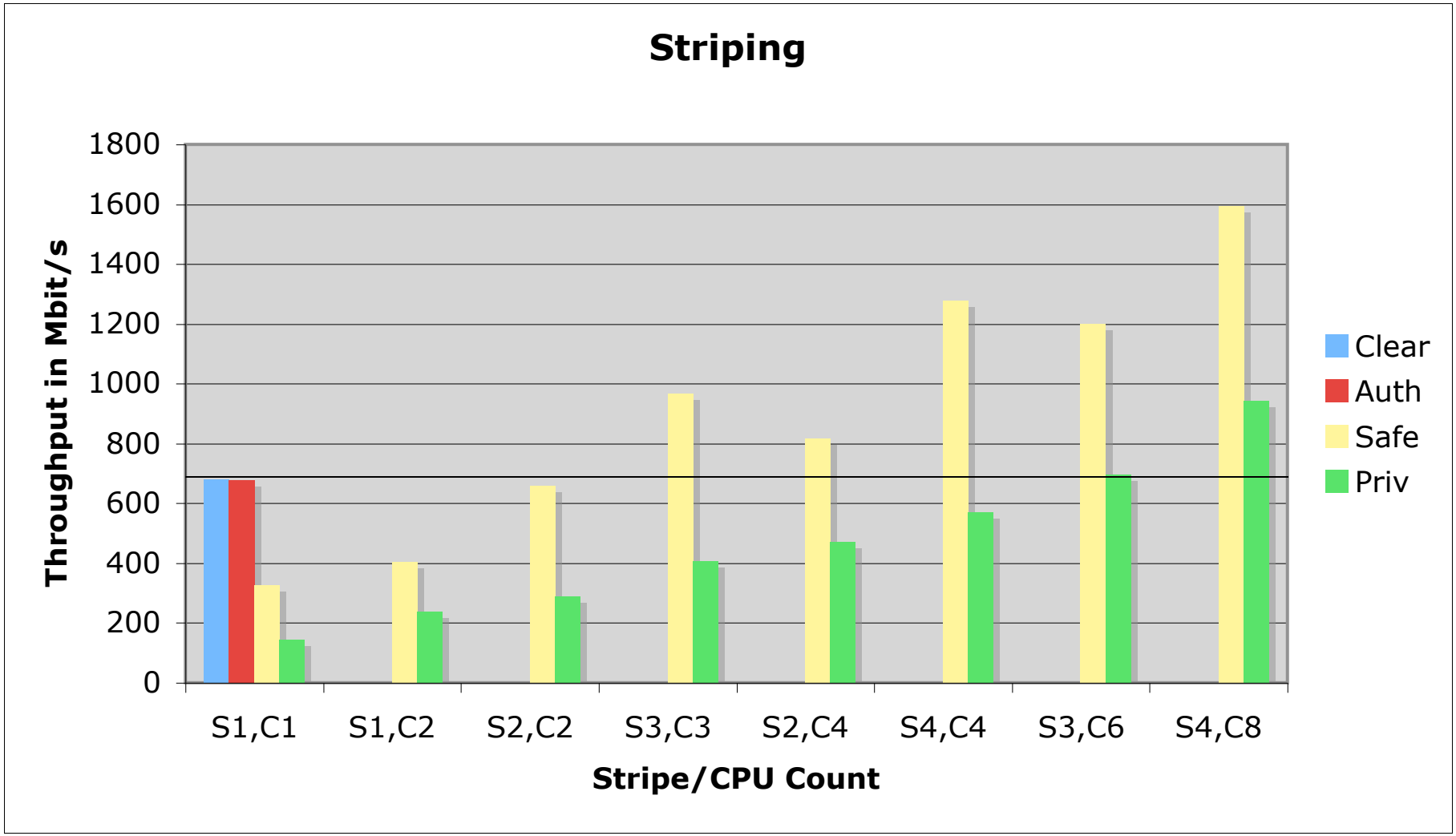


Stripes

- Striping to extrapolate for higher number of cores
- 4 way striping with dual cores on each stripe
- Results show that 6 cores may be sufficient to get a throughput for fully encrypted transfers that is equivalent to that of a clear transfer with Gigabit NICs
  - Intel Xeon dual core 2.4 GHz
- 2 way stripe with 1 thread per stripe is better than 1 way stripe with 2 threads
  - Suspected cause is availability of 2 Gigabit NICs for 2 way stripe
  - Need to do more tests to verify this

the globus alliance
www.globus.org

Stripes



Stripes

- S1,C2

- S2,C2