



Cluster-based Online Measurement of Web Traffic

Yun Mao, Kang Chen,
DS. Wang, WM. Zheng, XT. Deng

High Performance Computing Institute

Computer Science & Technology Dept.

Tsinghua University

Beijing 100084, P.R. China

maoyun00@mails.tsinghua.edu.cn



Presentation Outline

- Introduction
- Design & Implementation
- Preliminary Results
- Summary



Presentation Outline

- Introduction
- Design & Implementation
- Preliminary Results
- Summary



Why care about Web?

- Web applications become dominant
 - ~ 72% flows, ~ 55% packets, ~ 56% bytes
- Web is undergoing changes
 - HTTP 1.0 -> HTTP 1.1, multimedia
- Web is based on other protocols
 - TCP, DNS
- How to understand Web?
 - Measure, then analyze



How to measure?

- From log-files of Web servers
 - Specific, not representative
- From users running modified browsers
 - Lack enough volunteers
- From log-files of Web proxies
 - Bottleneck, level of detail in logs is low
- From log-files of packet sniffing
 - rich, transparent, passive, complicated



Why Complicated?

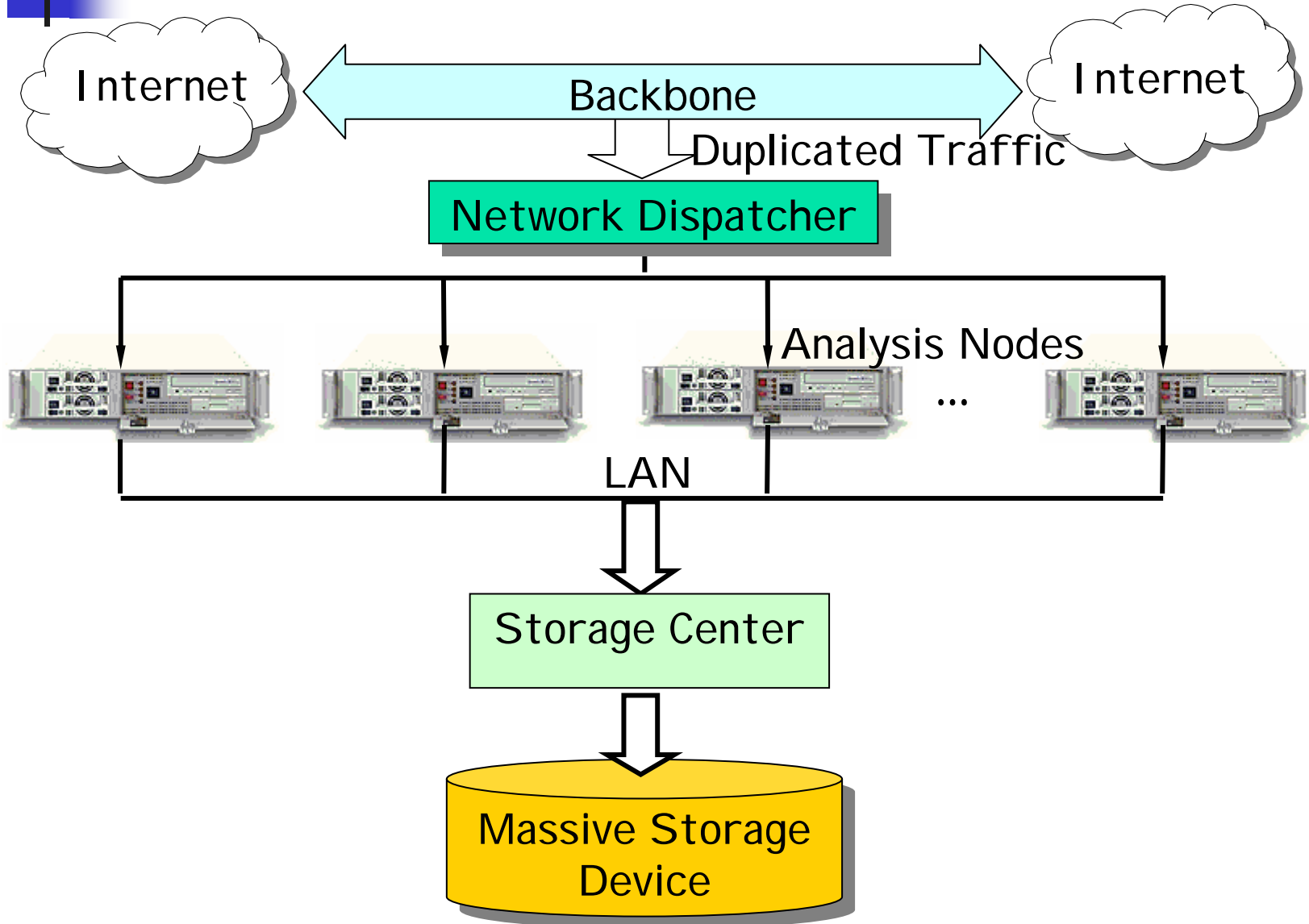
- Network bandwidth is increasing
 - CPU, network adapters, disk I/O
- TCP reconstruction
 - Packet loss, retransmission, IP fragmentation
- HTTP reconstruction
 - Persistent connections, pipeline
 - incompatible client/servers
 - Inaccurate Content-Length
 - Non-80 port service



Presentation Outline

- Introduction
- Design & Implementation
- Preliminary Results
- Summary

Cluster-based Architecture





Dispatch Algorithm

- Requirements
 - convenience of HTTP reconstruction
 - Load balance
- Candidates
 - Round Robin, Dynamic Route
 - Static Route
- **Semi-Static Route!**



Semi-Static Route Algorithm

- Network segmentation
 - n nodes, m segments $\{S_1, S_2, \dots, S_m\}$
 - $T_{j,i}$: traffic volume of the i-th 12-hour period of S_j
- Traffic volume estimation
 - $E_{j,k} = (T_{j,k-2} + T_{j,k-4} + T_{j,k-6})/3$
- Routing table varies every 12 hrs
 - According to E
 - A classical NP-Hard Problem!
 - Greedy algorithm in polynomial time



Reconstruction in Memory

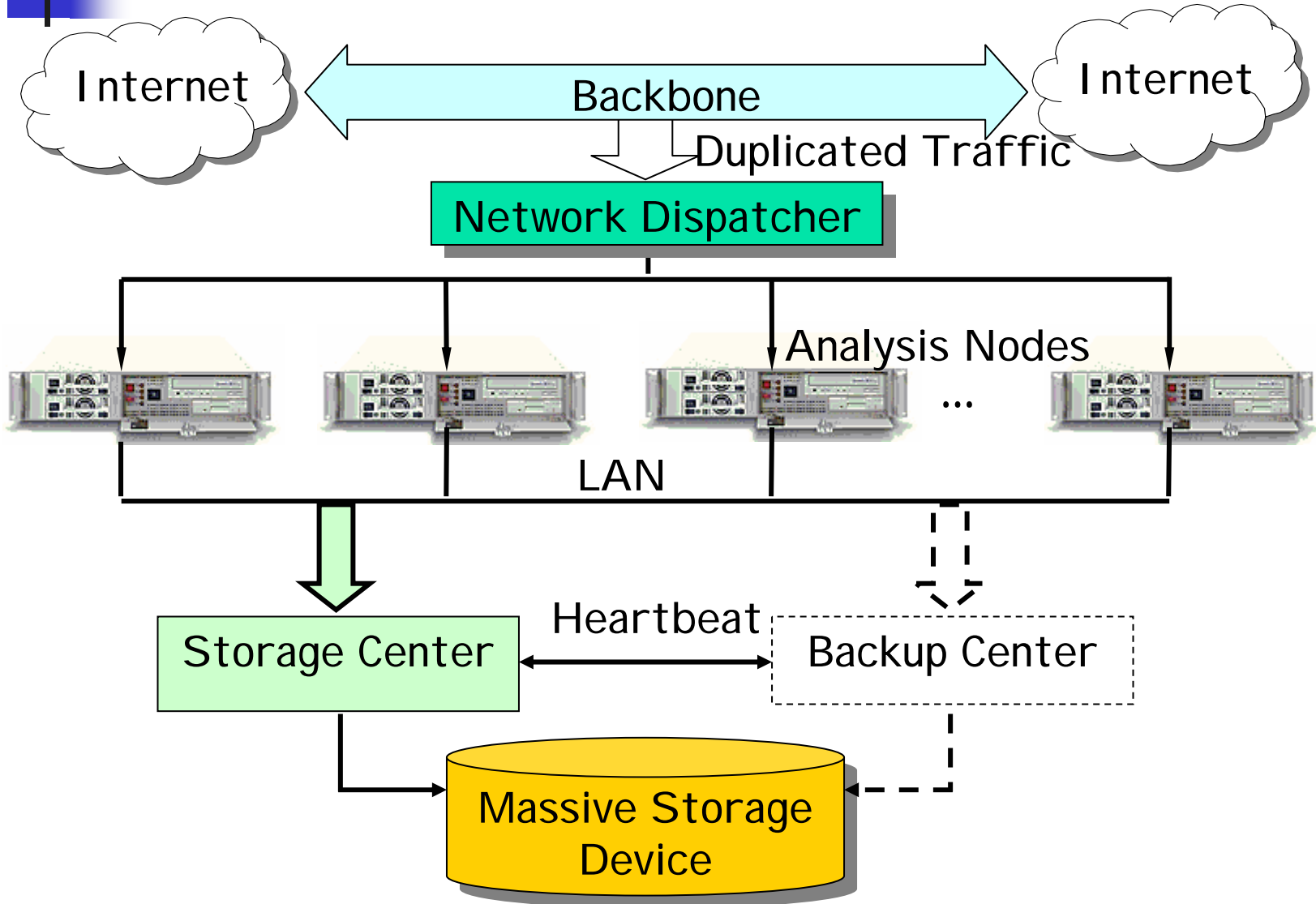
- Not all the Internet traffic is Web data
 - Non-TCP: UDP, ICMP, ..
 - Well-known ports: 20,21 FTP, 25 SMTP, ..
 - Kernel filter
- Protocol headers
- Only HTTP headers, no contents
- Disk I/O is reduced!



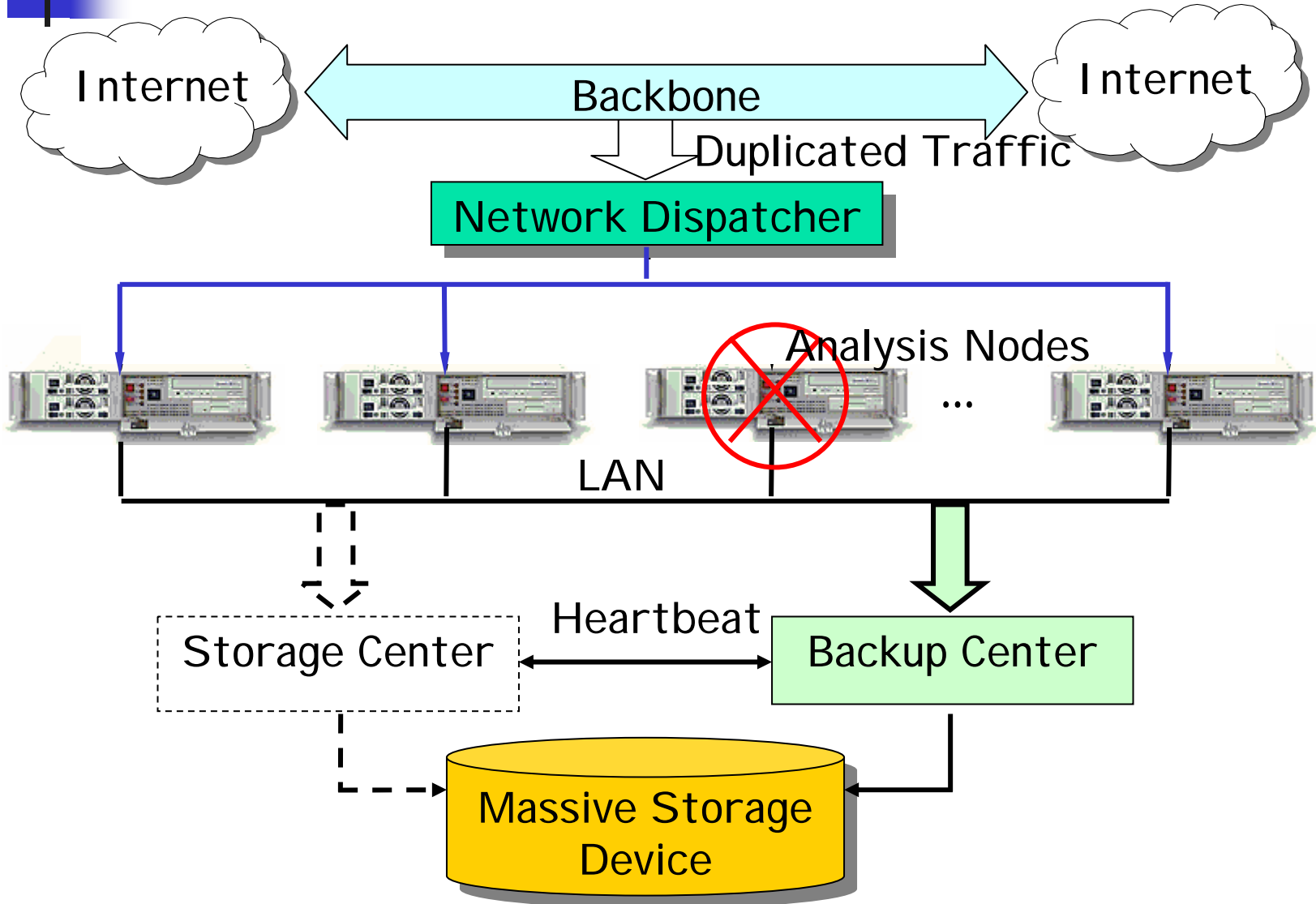
Availability Issues

- What if storage server fail
 - Backup storage server
 - Heartbeat
 - Fake-IP to take over
- What if analysis nodes fail
 - Monitor daemon detection
 - Routing table change

Availability



Availability

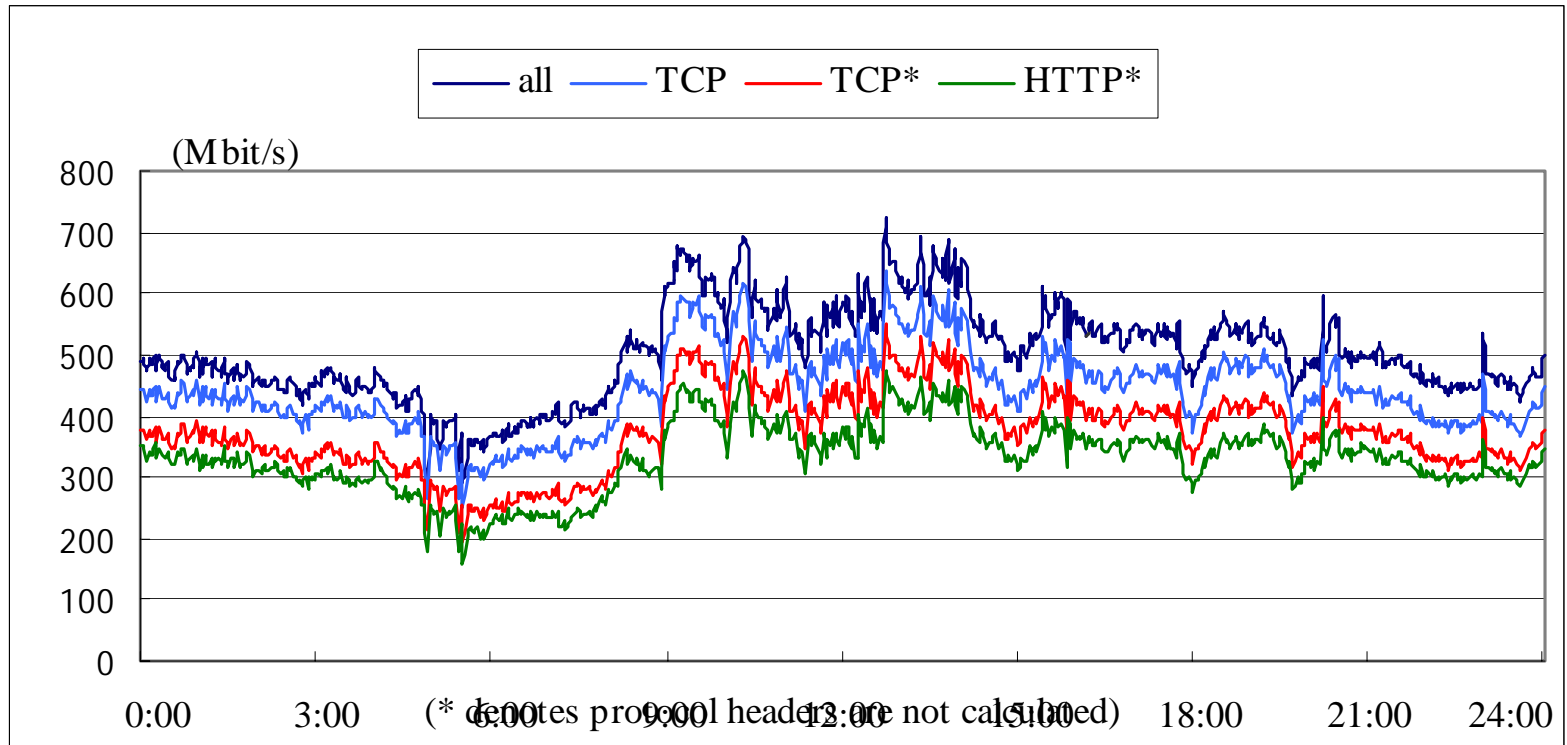




Presentation Outline

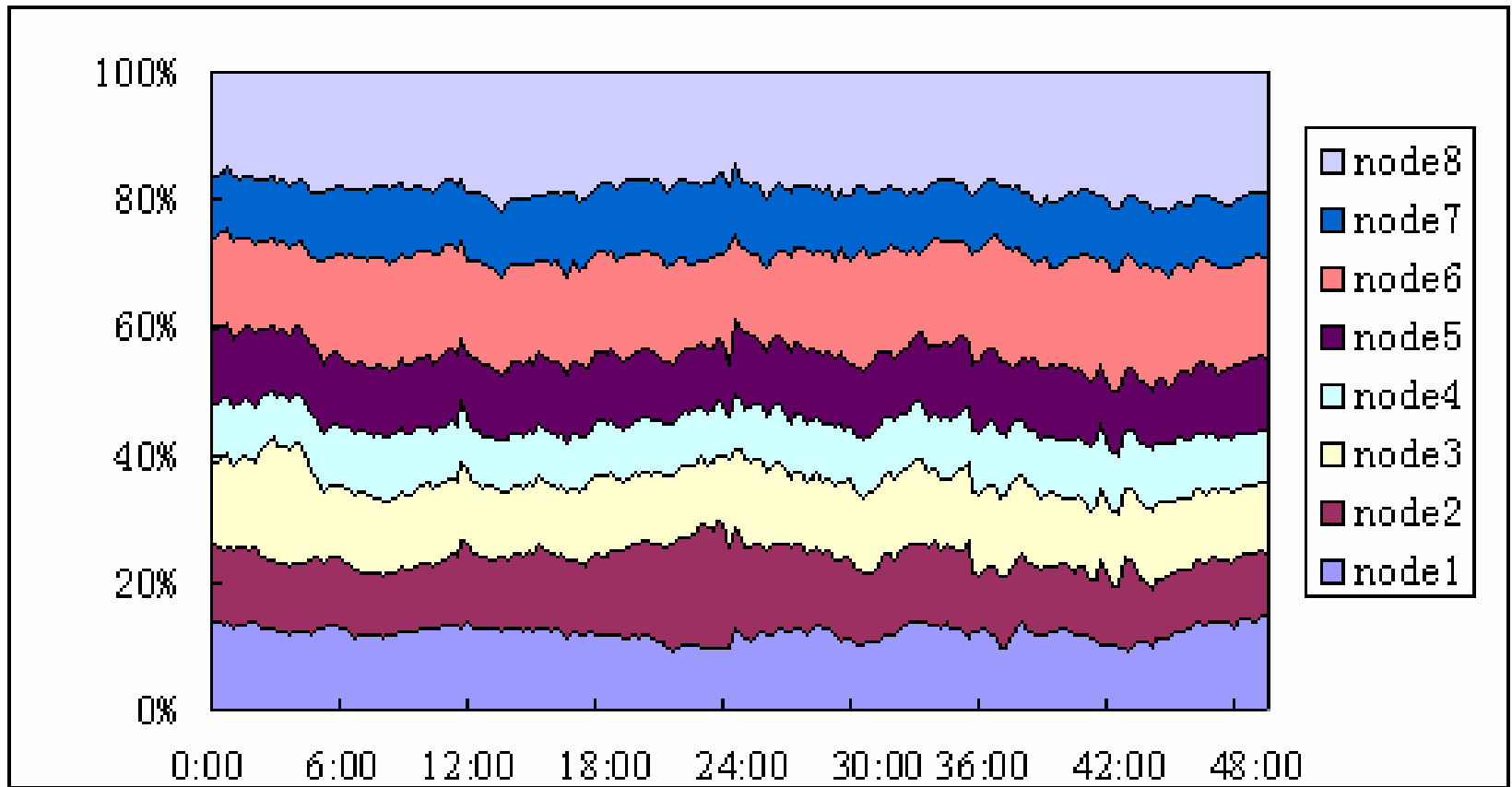
- Introduction
- Design & Implementation
- **Preliminary Results**
- Summary

Preliminary Results



Traffic Composition of Common Protocols in Bit-Rate Over 24-hour

Preliminary Results (cont'd)

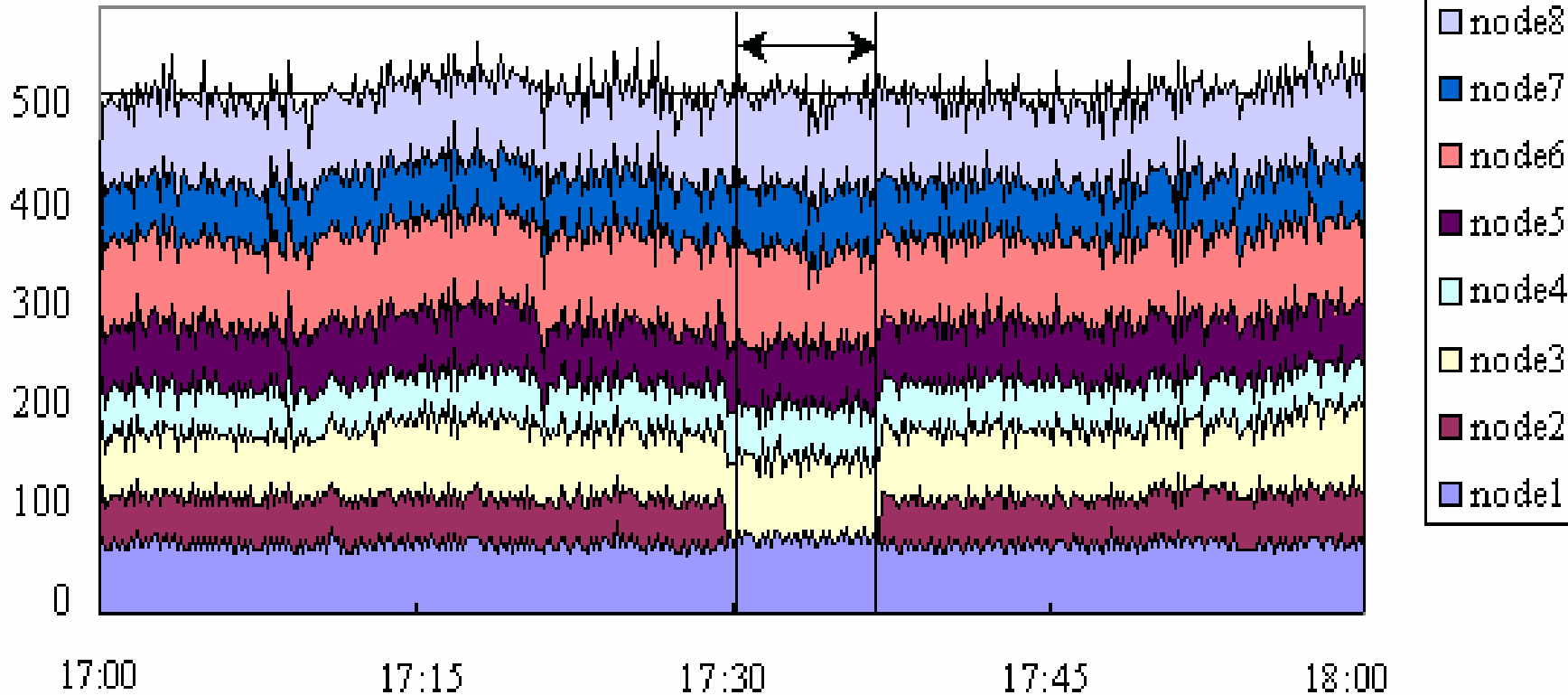


Bit Rate in Each Analysis Node During 2 Consecutive Days

Preliminary Results (cont'd)

Fault Injection in Node 2

(Mbit/s)



Traffic Distribution in Bit-rate During 1-hour Period



Presentation Outline

- Introduction
- Design & Implementation
- Preliminary Results
- **Summary**



Summary & Conclusion

- Cluster-based Solution
 - Cost-effectiveness
 - Scalable to high speed links
 - Highly available due to redundancy
- Processing in Memory
 - Reduce disk I/O -> high performance
 - Prevent some privacy problems
- A useful measurement system
 - Link analysis, Web change analysis, performance evaluation (bi-layer)

