


# A Perspective on Passive Measurement

Greg Miller

January 14, 1999

http://www.vbns.net

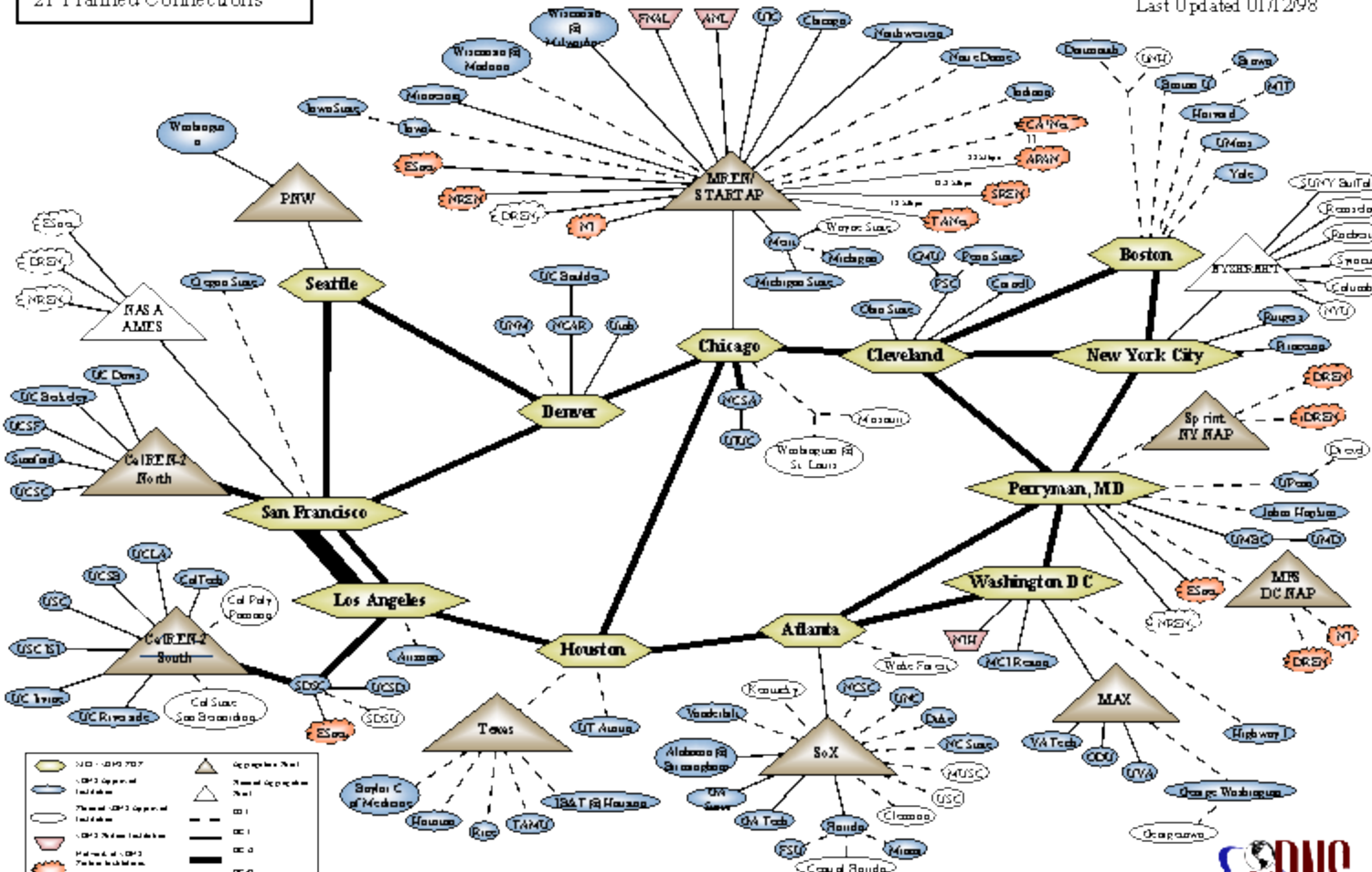
# Outline

- Where am I coming from?
- What is OCxMON?
- What can OCxMON do?
  - the basics
  - cool "researchy" stuff
  - practical things that have come in handy for us
  - what we *don't* use OCxMON for (yet?)

77 Operational Connections
21 Planned Connections

# vBNS Logical Network Map

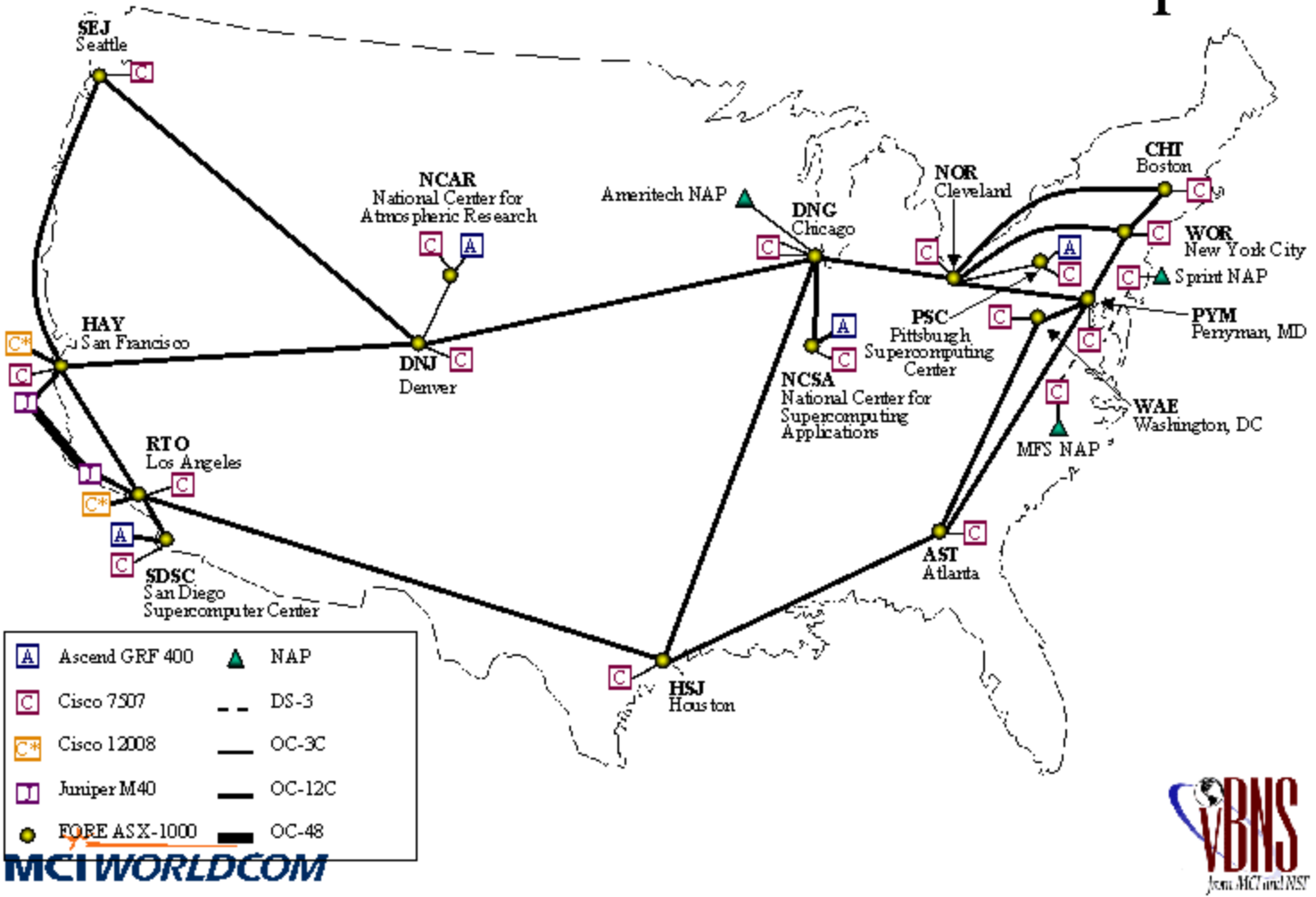
Last Updated 01/12/98



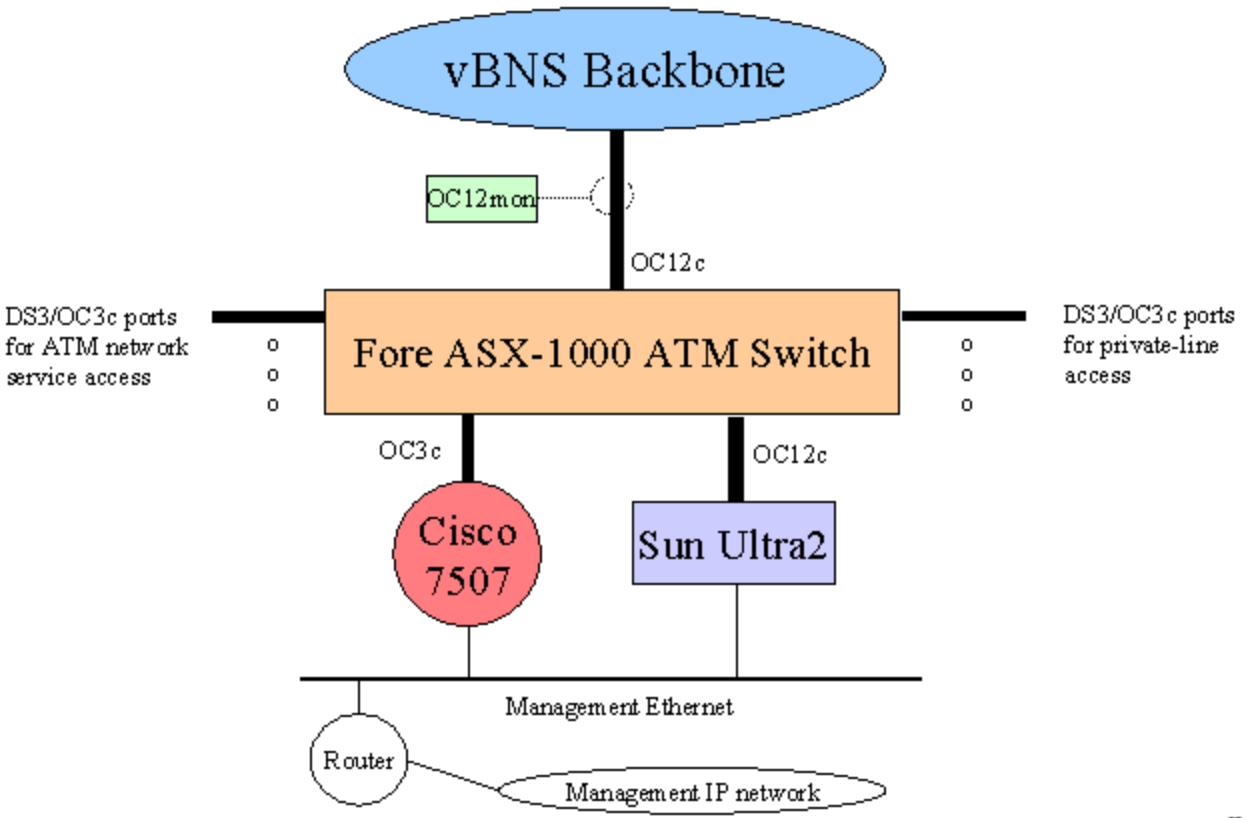

MCI WORLDCOM

vBNS
from MCI and NSF

# vBNS Backbone Network Map



# vBNS POP Architecture




MCI WORLDCOM

vBNS from MCI and NSF

# What is OCxMON?

- Passive traffic monitor, built from PC hardware and ATM NICs
- uses optical splitter to snoop on fiber
- runs DOS, custom firmware and software
- OC3MON and OC12MON exist; OC48MON in development
- specs, instructions, source code are publicly available

# OCxMON Modes of Operation

- Statistics gathering mode - continuous stats
  - per byte, packet, and flow stats
  - per protocol stats
  - AS and port usage stats
- Raw capture modes - time-stamped traces
  - entire first cell of every packet (AAL5 frame)
  - only ATM header of every cell
  - all of every cell
- Special statistics mode
  - collect statistics of interest in real-time

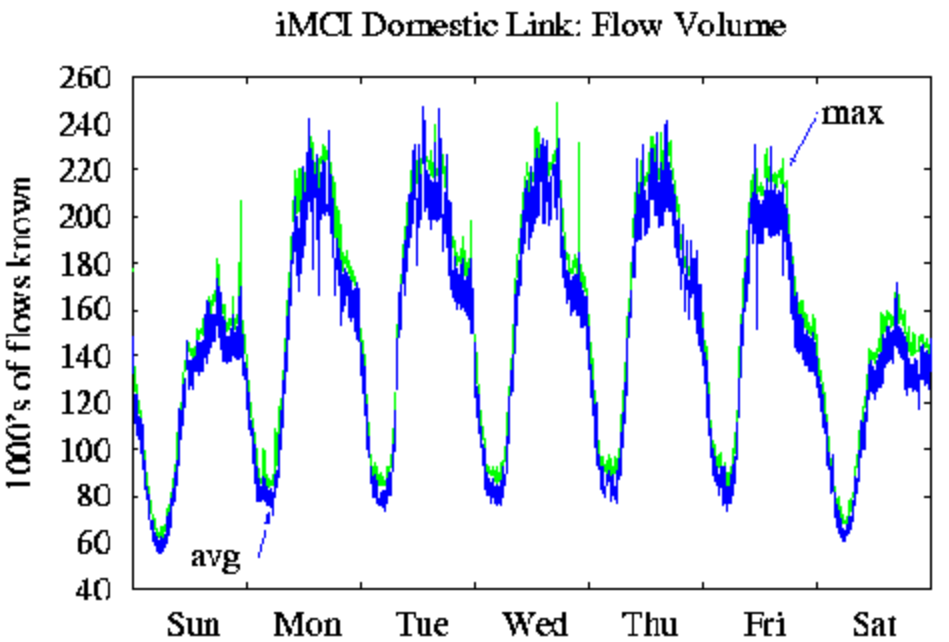
MCI WORLDCOM

VBNS
from MCI and NSF

# What is a flow?

- kc's flow definition:
  - unidirectional stream of packets
  - same IP addresses, IP protocol, and port numbers
  - ends after 64 secs without seeing a packet
- Like nearly everything else in OCxMON, this definition is configurable

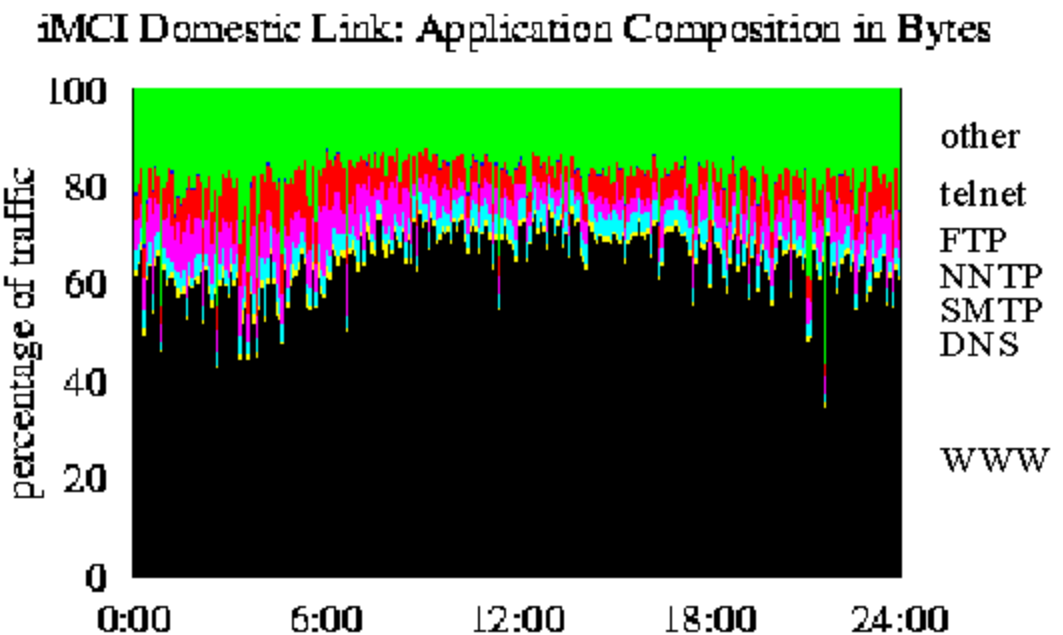
# Flow volume for 1 week




MCI WORLDCOM

VBNS
from MCI and NSF

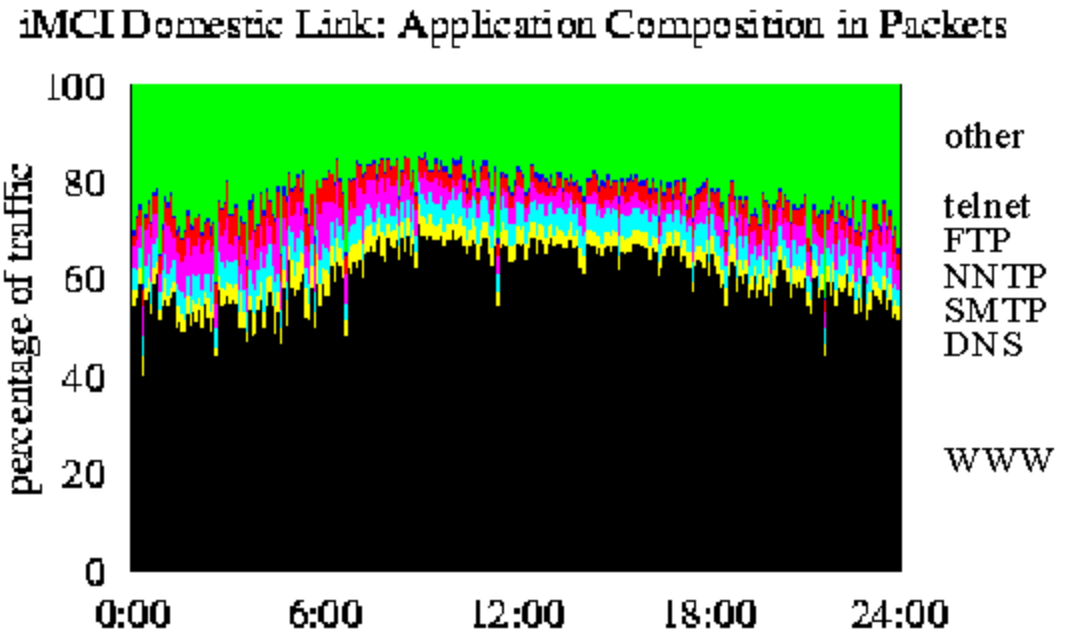
# Traffic by application (in bytes)




MCI WORLDCOM

vBNS
from MCI and NSF

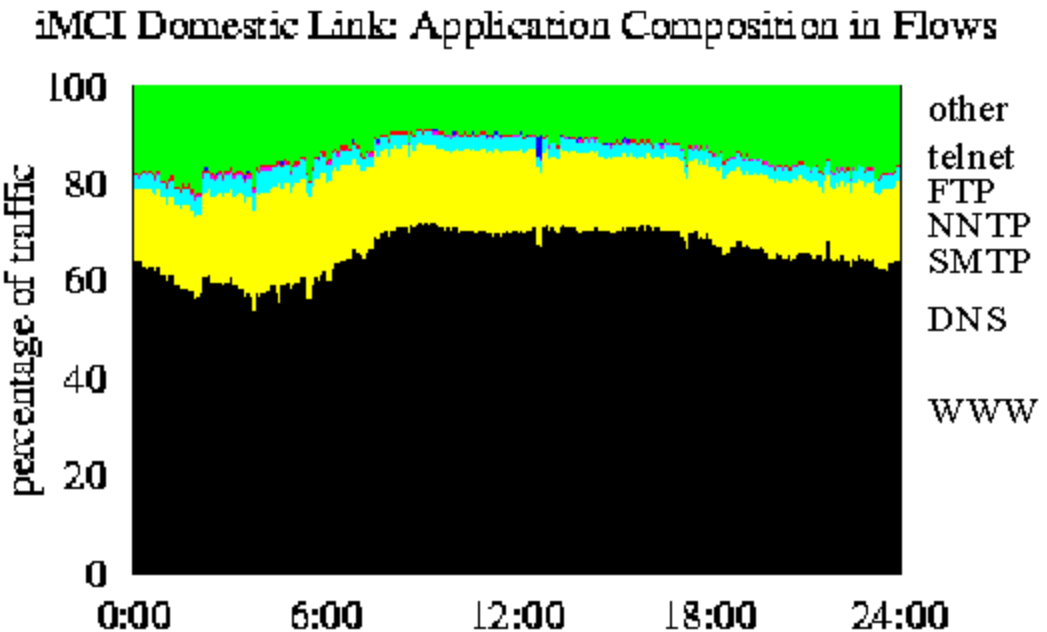
# Traffic by application (in packets)




MCI WORLDCOM

VBNS
from MCI and NSF

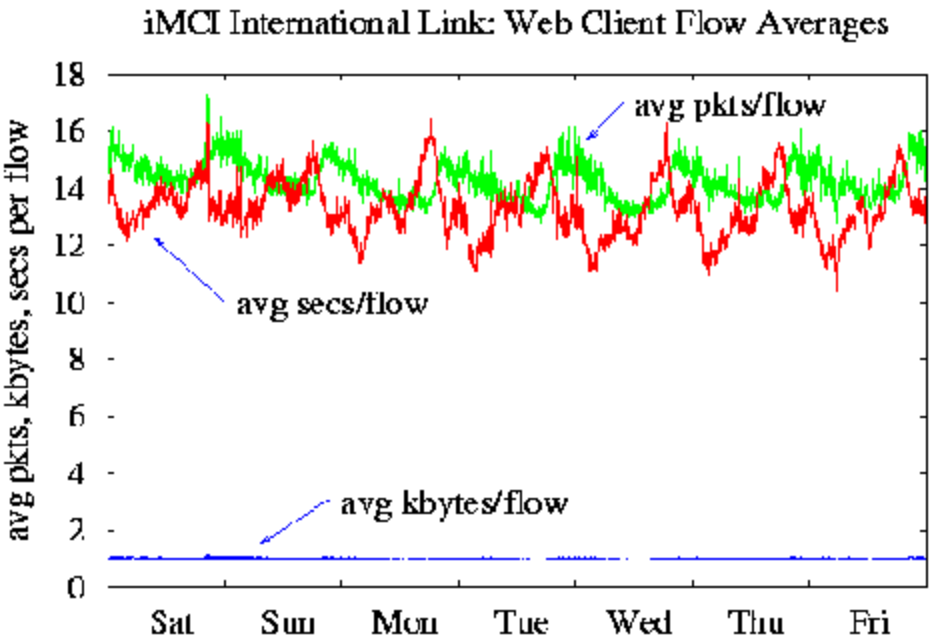
# Traffic by application (in flows)




MCI WORLDCOM

VBNS
from MCI and NSF

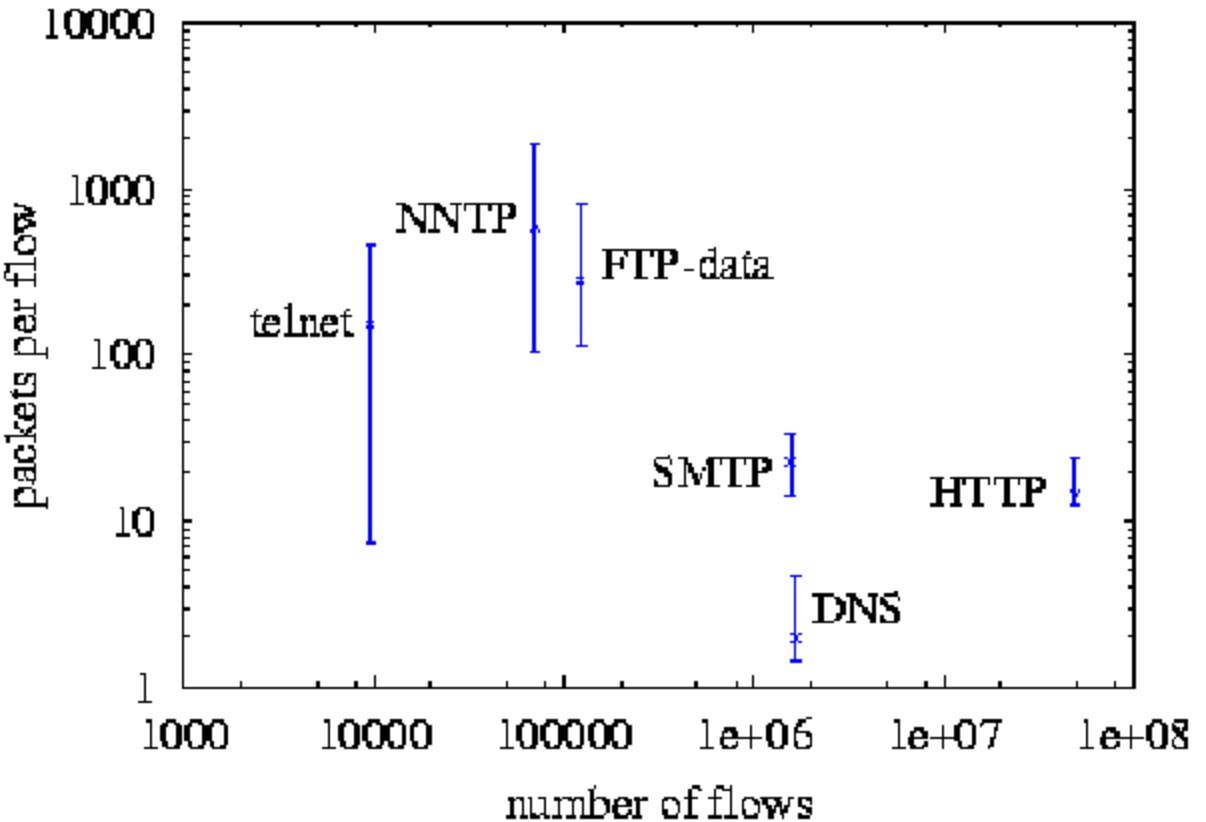
# Web client averages




MCI WORLDCOM

VBNS
from MCI and NSF

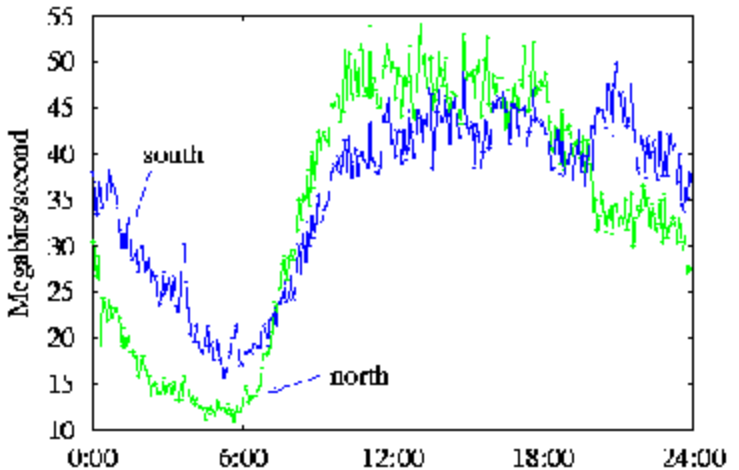
# Characterization of application flows

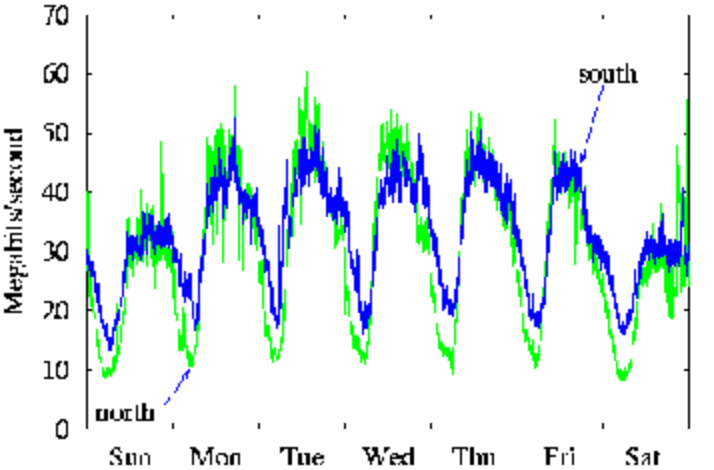



MCI WORLDCOM

VBNS
from MCI and NSF

# Long-term traffic variability

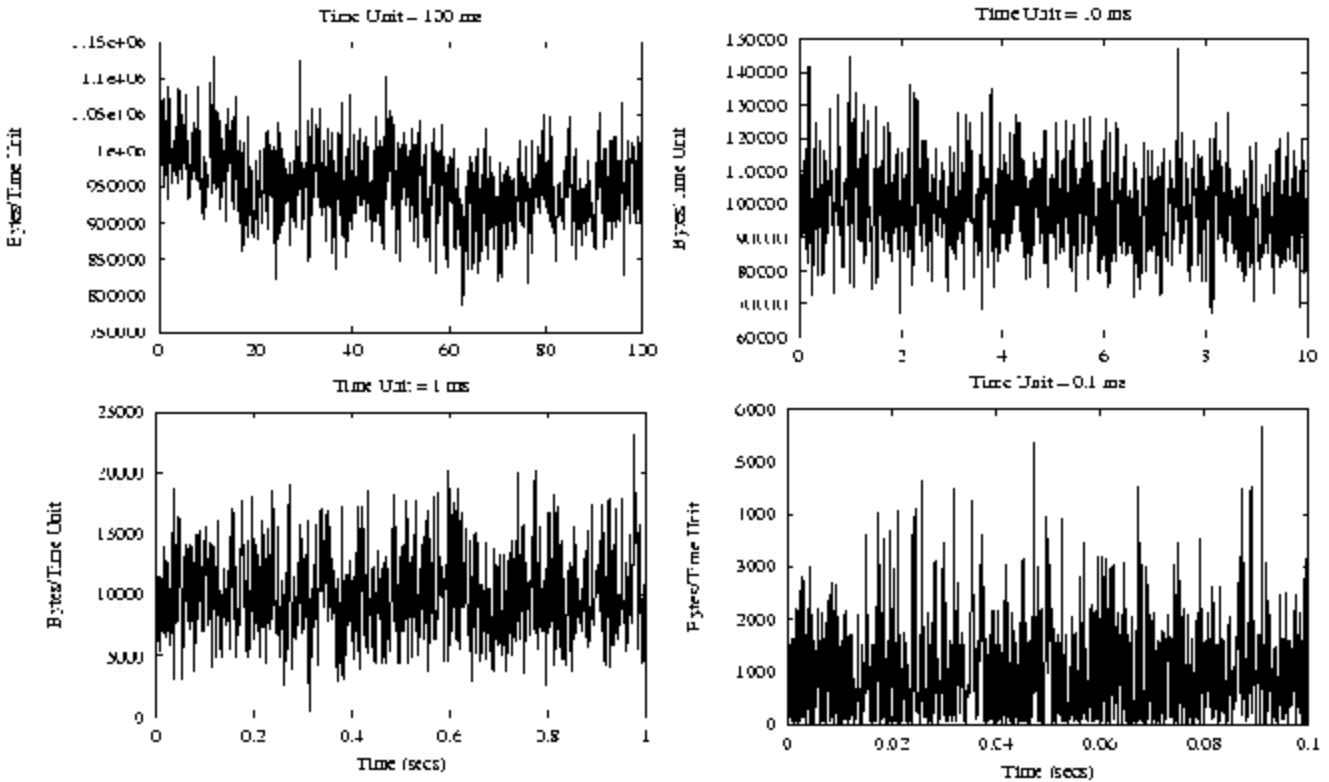



MCI WORLDCOM

VBNS
from MCI and NSF

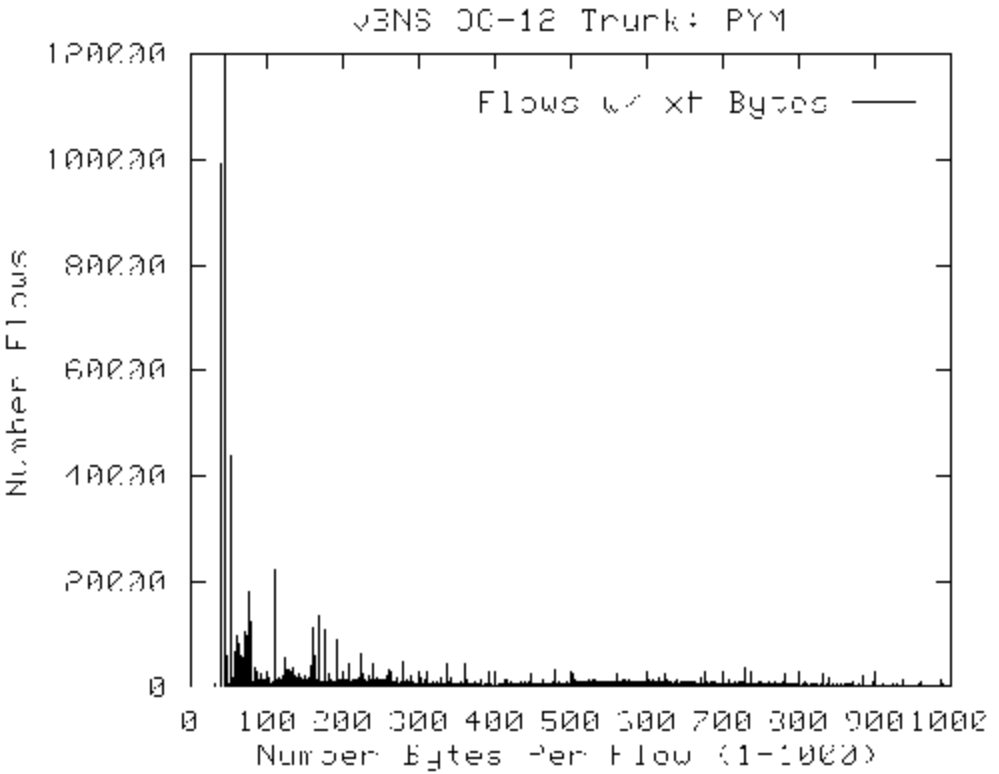
# Variability over multiple time scales




MCI WORLDCOM

vBNS from MCI and NSF

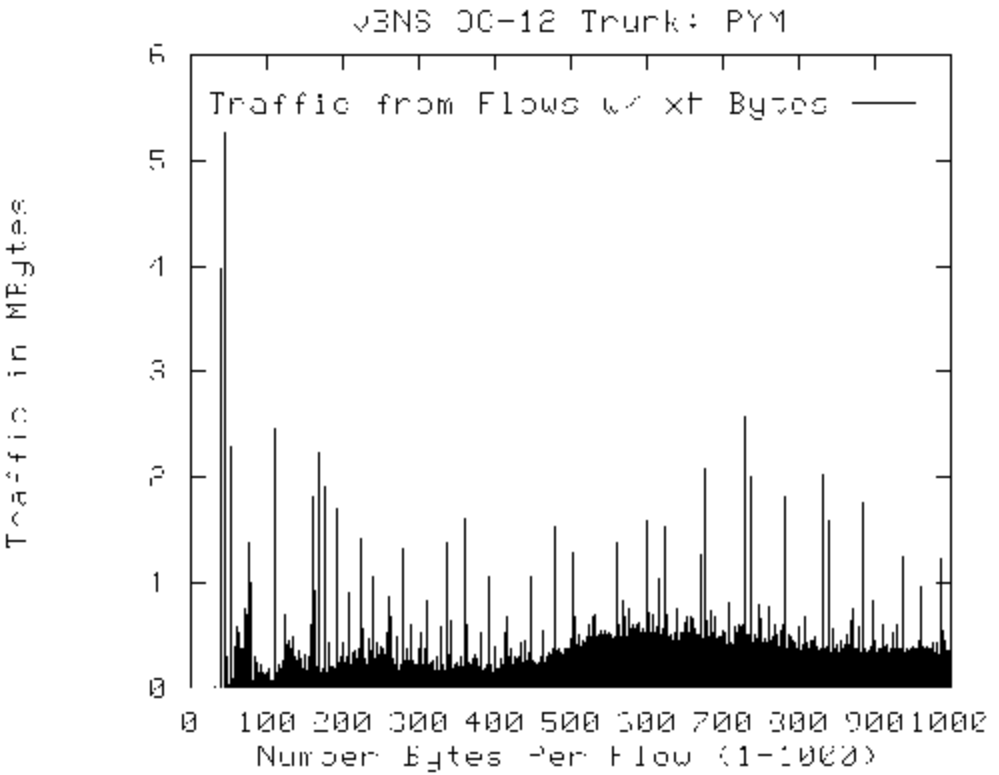
# Flow size histogram - small flows dominate




MCI WORLDCOM

vBNS from MCI and NSF

# Traffic from small flows



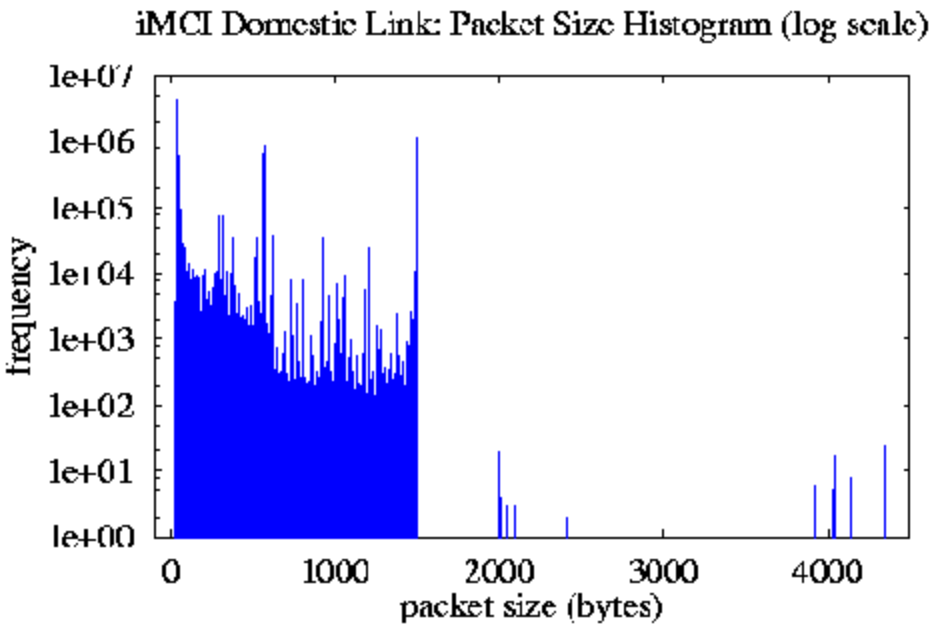

MCI WORLDCOM

vBNS
from MCI and NSF

# Packet size data

- size distribution with 1-byte granularity
- meaningfulness of average packet size
- time-of-day fluctuation
- run-length of similar size packets
- protocol overhead analysis

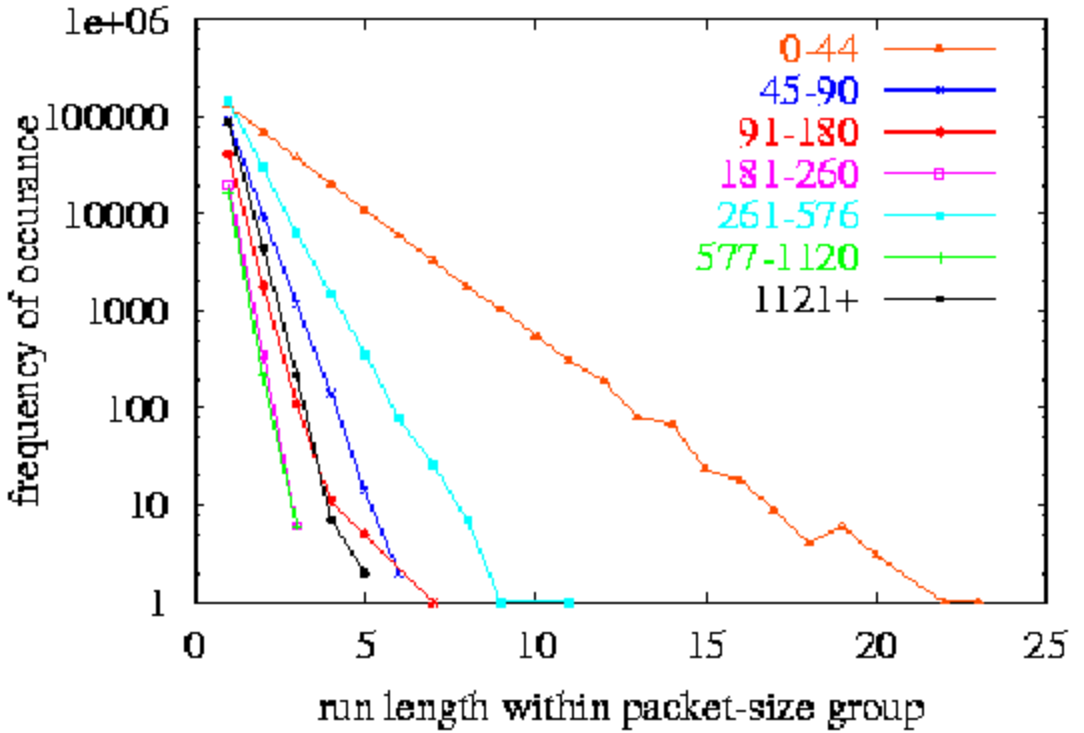
# Packet size histogram (log scale)




MCI WORLDCOM

VBNS
from MCI and NSF

# Packet run lengths




MCI WORLDCOM

VBNS
from MCI and NSF

# Protocol overhead analysis

| | ATM | SONET |
|---|---|---|
| IP payload bytes | 5,777,615,952,291 | 5,777,615,952,291 |
| Total bytes | 7,233,116,621,345 | 6,121,916,426,350 |
| Bit efficiency | 80% | 94% |

# Specialized analyses

- TCP analysis (rexmits, window size, MSS, options, flags, etc.)
- number of simultaneous reassemblies in progress
  - we've never seen more than ~20
- TOS and precedence bits usage
- individual flow tracing
- multicast measurement

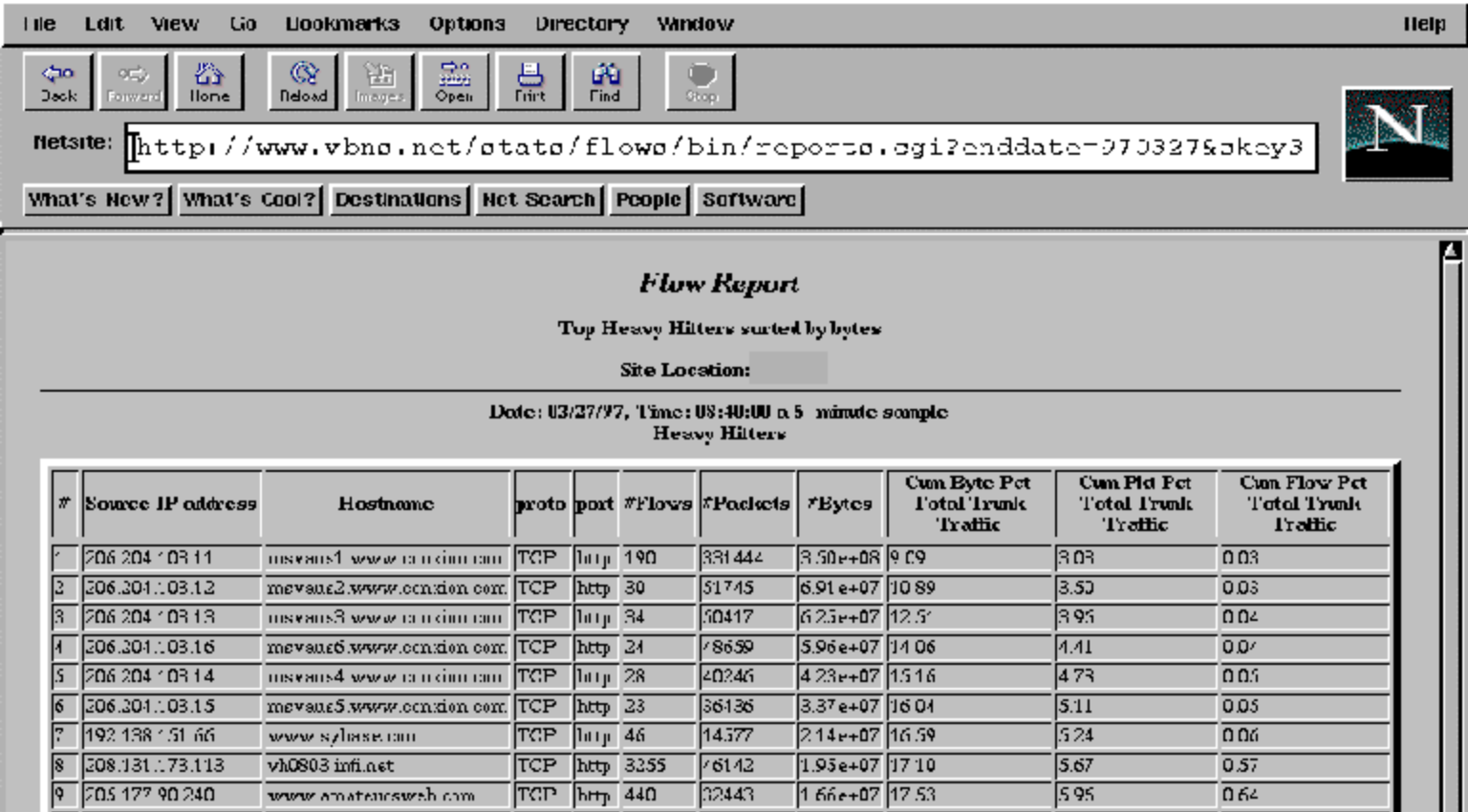
# Specialized analyses cont.- ATM CLP-bit analysis

interface 1 VPI 196 CLP 0: saw 84476 cells
interface 1 VPI 196 CLP 1: saw 42 cells
interface 1 VPI 206 CLP 0: saw 515 cells
interface 1 VPI 206 CLP 1: saw 30 cells
interface 1 VPI 215 CLP 0: saw 6029385 cells
interface 1 VPI 215 CLP 1: saw 40 cells
interface 1 VPI 229 CLP 0: saw 6930019 cells
interface 1 VPI 229 CLP 1: saw 41 cells
interface 1 VPI 230 CLP 0: saw 6055944 cells

# Specialized analyses cont. - Cell loss analysis

16 AAL5 packets ended with missing cells
only saw 93 of 94 cells sent on iface:0 block:388 offset:13763 with timestamp 0x00024D93F0D40003
last cell's ATM header was GFC:0 VPI:200 VCI:1887 OAM:0 CE:0 LAST:1 CLP:0 whole:0x0C8075F2
only saw 93 of 94 cells sent on iface:0 block:1471 offset:9078 with timestamp 0x00025350FC6D4003
last cell's ATM header was GFC:0 VPI:200 VCI:342 OAM:0 CE:0 LAST:1 CLP:0 whole:0x0C801562
only saw 93 of 94 cells sent on iface:0 block:2516 offset:4295 with timestamp 0x000258BD324F7003
last cell's ATM header was GFC:0 VPI:200 VCI:382 OAM:0 CE:0 LAST:1 CLP:0 whole:0x0C8017E2
only saw 93 of 94 cells sent on iface:0 block:3416 offset:13015 with timestamp 0x00025D701ED9D003
last cell's ATM header was GFC:0 VPI:200 VCI:339 OAM:0 CE:0 LAST:1 CLP:0 whole:0x0C801532

# “Heavy Hitters”



File Edit View Go Bookmarks Options Directory Window Help

Back Forward Home Reload Images Open Print Find Stop

Netsite: http://www.vbns.net/stats/flows/bin/reports.cgi?enddate=970327&skey3

What's New? What's Cool? Destinations Net Search People Software

## *Flow Report*

**Top Heavy Hitters sorted by bytes**

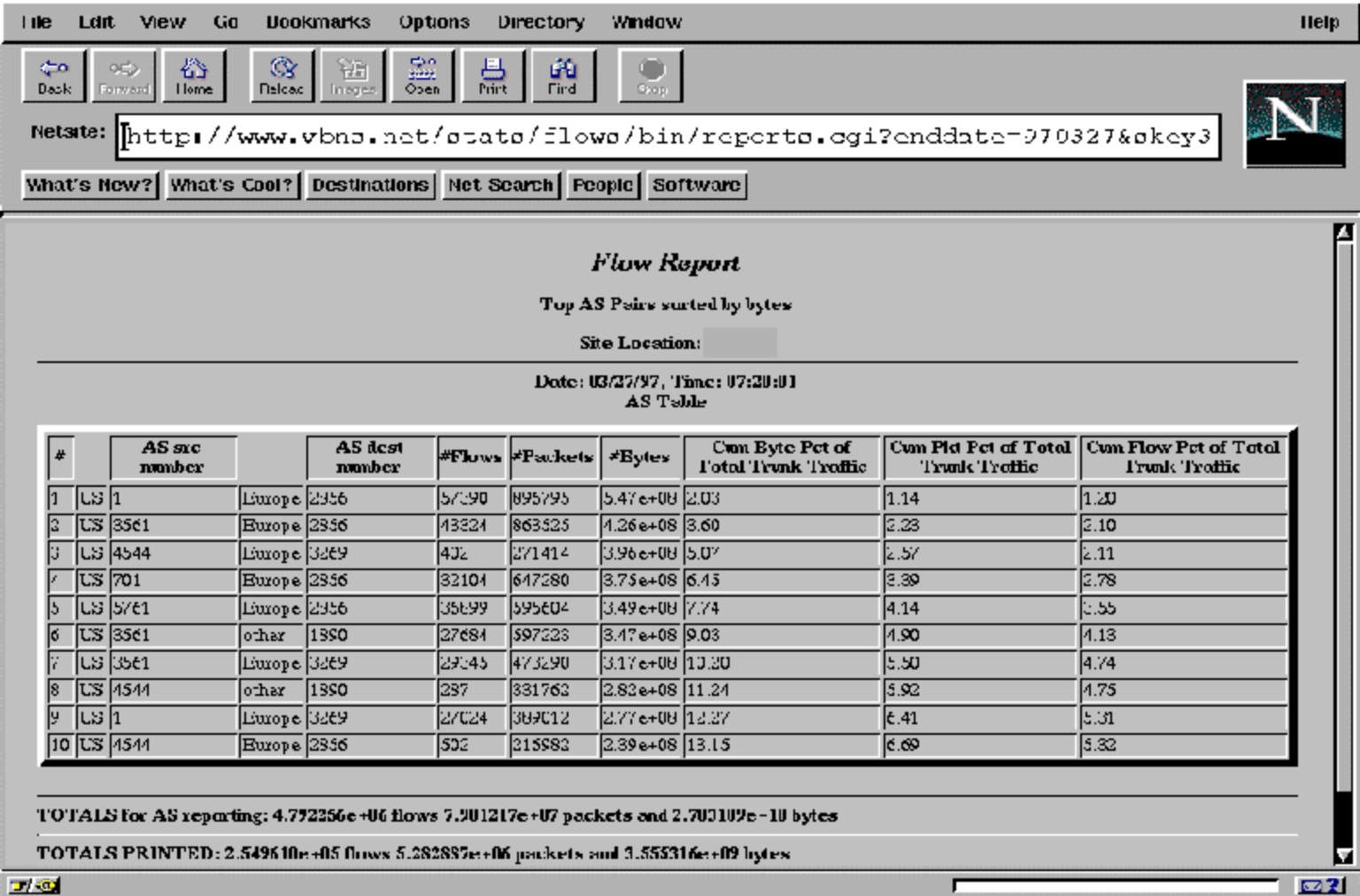
**Site Location:**

**Date: 03/27/97, Time: 08:40:00 a 5 minute sample**
**Heavy Hitters**

| # | Source IP address | Hostname | proto | port | #Flows | #Packets | #Bytes | Cum Byte Pct Total Trunk Traffic | Cum Pkt Pct Total Trunk Traffic | Cum Flow Pct Total Trunk Traffic |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 206.204.103.11 | mevaus1.www.conxion.com | TCP | http | 190 | 331444 | 3.50e+08 | 9.09 | 3.03 | 0.03 |
| 2 | 206.204.103.12 | mevaus2.www.conxion.com | TCP | http | 30 | 51745 | 6.91e+07 | 10.89 | 3.50 | 0.03 |
| 3 | 206.204.103.13 | mevaus3.www.conxion.com | TCP | http | 34 | 50417 | 6.25e+07 | 12.51 | 3.95 | 0.04 |
| 4 | 206.204.103.16 | mevaus6.www.conxion.com | TCP | http | 24 | 48659 | 5.96e+07 | 14.06 | 4.41 | 0.04 |
| 5 | 206.204.103.14 | mevaus4.www.conxion.com | TCP | http | 28 | 40246 | 4.23e+07 | 15.16 | 4.73 | 0.05 |
| 6 | 206.204.103.15 | mevaus5.www.conxion.com | TCP | http | 23 | 36436 | 3.37e+07 | 16.04 | 5.11 | 0.05 |
| 7 | 192.138.151.66 | www.sybase.com | TCP | http | 46 | 14577 | 2.14e+07 | 16.59 | 5.24 | 0.06 |
| 8 | 208.131.173.113 | vh0803.infi.net | TCP | http | 3255 | 46142 | 1.95e+07 | 17.10 | 5.67 | 0.57 |
| 9 | 205.177.90.240 | www.amateurswab.com | TCP | http | 440 | 32443 | 1.66e+07 | 17.53 | 5.95 | 0.64 |
| 10 | 206.204.65.14 | msie3.www.conxion.com | TCP | http | 7 | 9550 | 1.43e+07 | 17.90 | 6.05 | 0.64 |

**TOTALS as reported for Heavy-Hitters: 1.887767e+06 packets and 1.496452e+09 bytes**

# AS Pairs Table




*Flow Report*

**Top AS Pairs sorted by bytes**

**Site Location:**

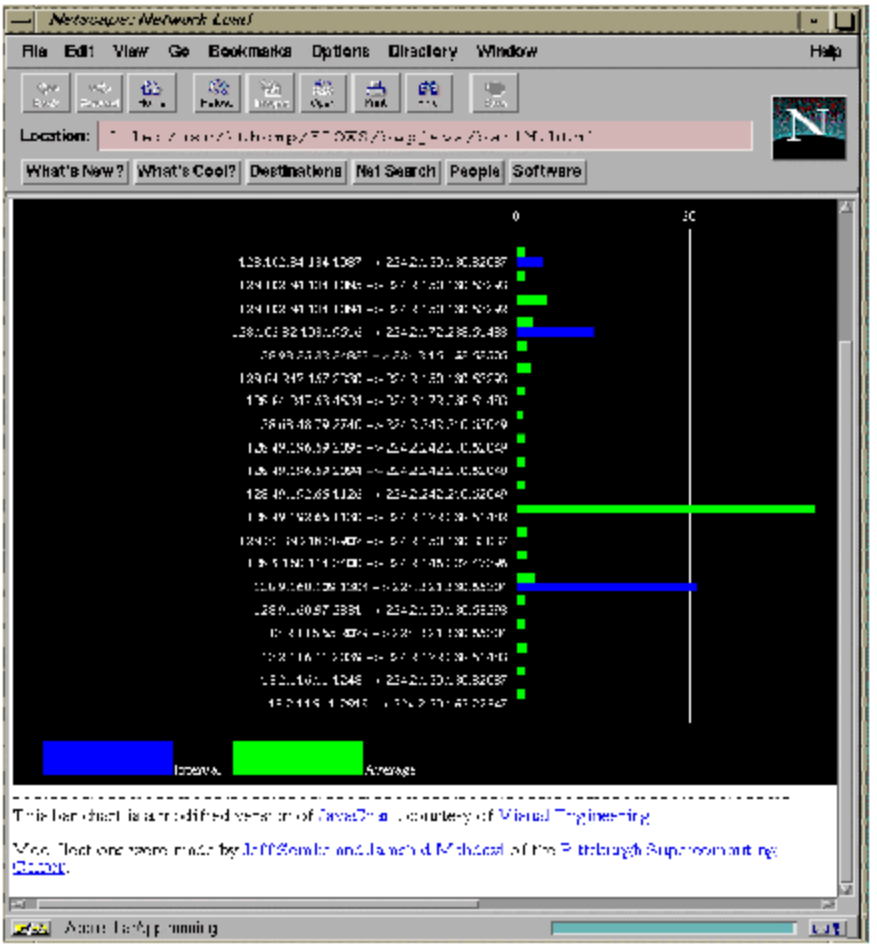
**Date: 03/27/97, Time: 07:20:01**
**AS Table**

| # | | AS src number | | AS dest number | #Flows | #Packets | #Bytes | Cum Byte Pct of Total Trunk Traffic | Cum Pkt Pct of Total Trunk Traffic | Cum Flow Pct of Total Trunk Traffic |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | US | 1 | Europe | 2856 | 57290 | 895795 | 5.47e+08 | 2.03 | 1.14 | 1.20 |
| 2 | US | 3561 | Europe | 2856 | 43824 | 863525 | 1.26e+08 | 3.60 | 2.23 | 2.10 |
| 3 | US | 4544 | Europe | 3269 | 402 | 271414 | 3.96e+08 | 5.07 | 2.57 | 2.11 |
| 4 | US | 701 | Europe | 2856 | 32104 | 647280 | 3.75e+08 | 6.45 | 3.39 | 2.78 |
| 5 | US | 5761 | Europe | 2856 | 35699 | 595604 | 3.49e+08 | 7.74 | 4.14 | 3.55 |
| 6 | US | 3561 | other | 1880 | 27684 | 597228 | 3.47e+08 | 9.03 | 4.90 | 4.13 |
| 7 | US | 3561 | Europe | 3269 | 29345 | 473290 | 3.17e+08 | 10.30 | 5.50 | 4.74 |
| 8 | US | 4544 | other | 1880 | 287 | 331763 | 2.82e+08 | 11.24 | 5.92 | 4.75 |
| 9 | US | 1 | Europe | 3269 | 27024 | 389012 | 2.77e+08 | 12.27 | 6.41 | 5.31 |
| 10 | US | 4544 | Europe | 2856 | 502 | 215883 | 2.39e+08 | 13.15 | 6.69 | 5.32 |

**TOTALS for AS reporting: 4.772256e+06 flows 7.901217e+07 packets and 2.703102e+10 bytes**

**TOTALS PRINTED: 2.549610e+05 flows 5.282887e+06 packets and 3.555316e+09 bytes**

# Real-time Active Flows Display




MCI WORLDCOM

VBNS
from MCI and NSF

# What we *don't* use OCxMON for (yet?)

- billing, accounting
- traffic engineering
- capacity planning
- security incidents
- SLA verification

# Conclusions

- I don't know what's important to measure
- OCxMON has come in handy numerous times
- I think the key to a useful monitor is configurability
- Dealing with large data sets and visualizing the data can be a challenge