Measurement of Campus Network with Network Telescope

2004-11-5

Youngseok Lee

lee@cnu.ac.kr

http://networks.cnu.ac.kr

Chungnam National Univ.

Contents

- Introduction
  - Network telescope
- CNU case study
- Summary

Introduction

- Internet measurement
  - Basic monitoring, capacity planning, accounting, security
- What to monitor ?
  - Active
    - loss, delay, jitter, bandwidth (IPPM)
      - End-to-end path, access/core links, node
  - Passive
    - Packet, netflow (IPFIX)
      - Link, router/switch

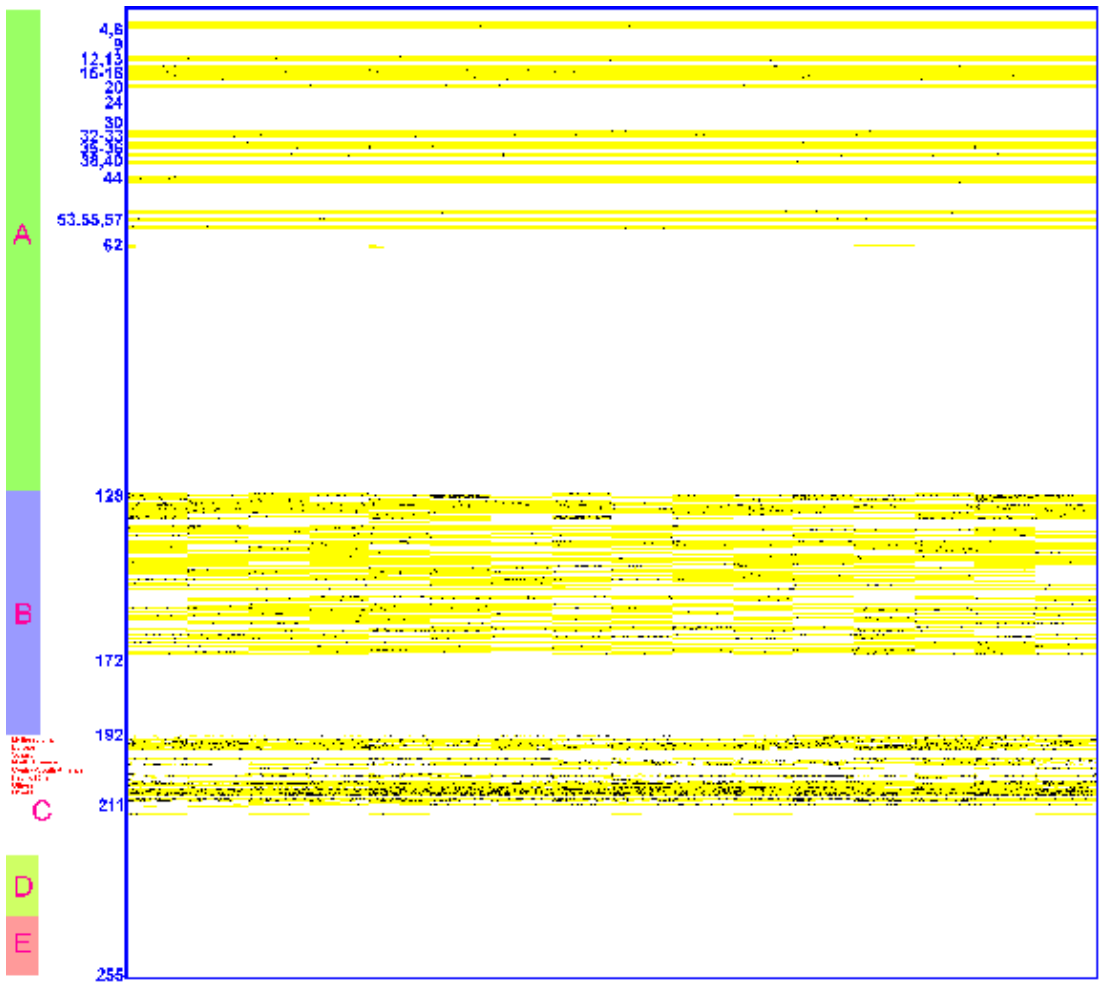
Passive Monitoring

- Link monitor
  - CAIDA coralreef
  - DAG project at U. of Waikato, New Zealand
    - Endace measurement systems
    - ATM, POS, GE, 10-GE
  - Wise Trafview project at ETRI
  - Sprint IPMON
- Router monitor
  - NetFlow v5/v9 : IETF IPFIX WG
    - Flow collectors
      - Flow-tools
    - Flow probe
      - fprobe, nprobe
    - Flow analyzer
      - Flow-scan
      - Arbor netowrks

Network Telescope

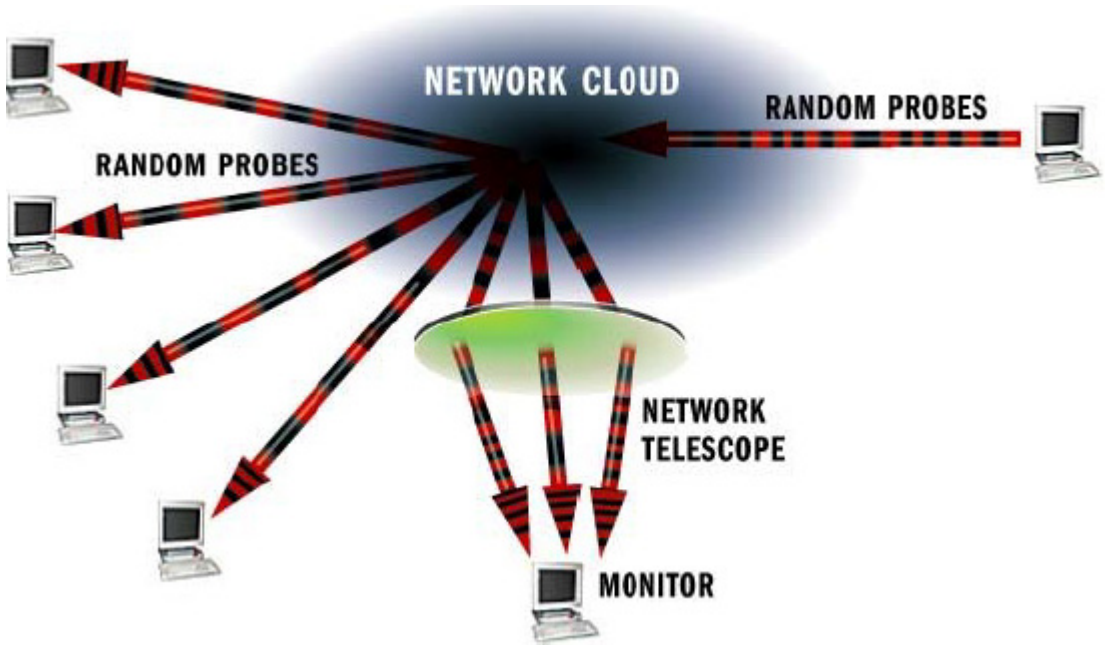
- CAIDA
- What is a network telescope ?
  - a portion of routed IP address space in which little or no legitimate traffic exists.
  - A way of seeing remote security events, without being there
- Can see
  - various forms of flooding denial-of-service attacks
  - infection of hosts by Internet worms
  - network scanning
  - misconfiguration

IPv4 Address Utilization



http://www.caida.org/outreach/resources/learn/ipv4space/

Basic Idea



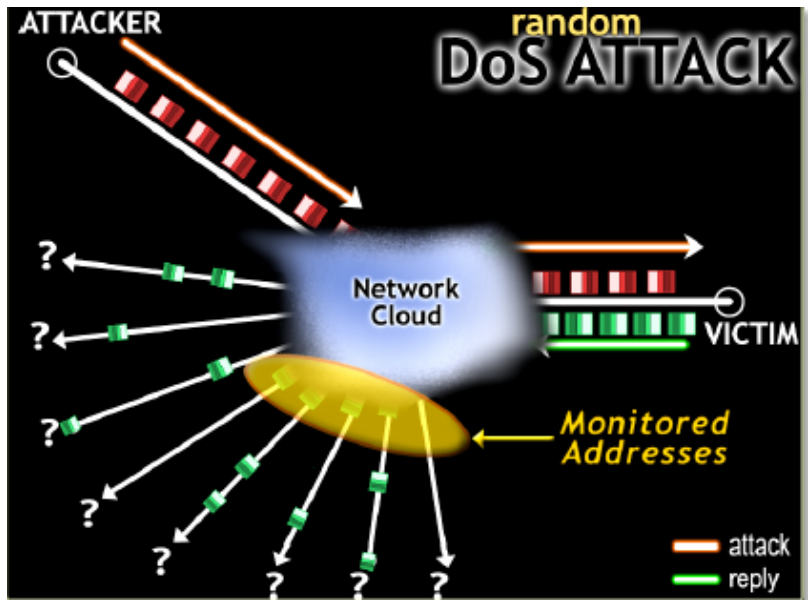
If a computer sends packets to IP addresses *randomly*,
we should see some of the packets
if we monitor enough
address space.

Network Telescope

- Chunk of (globally) routed IP address space
- Little or no legitimate traffic (or easily filtered)
  - might be "holes" in a real production network
- Unexpected traffic arriving at the network
  - telescope can imply remote network/security events
- Generally good for seeing explosions, not small events
  - Depends on statistics/randomness working

Network Telescope: Denial-of-Service Attacks

- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- With a /8 ("class A"), one can observe 1/256th of all *victim responses* to spoofed



Backscatter Analysis Technique

- Flooding-style DoS attacks
  - e.g. SYN flood, ICMP flood
- Attackers spoof source address randomly
  - True of many major attack tools
  - i.e. not SMURF or reflector attack
- Victims, in turn, respond to attack packets
- Unsolicited responses (backscatter) equally distributed across IP space
- Received backscatter is evidence of an attacker elsewhere

Backscatter Analysis

- Monitor block of *n* IP addresses
- Expected number of backscatter packets given an attack of *m* packets

$$E[X] = \frac{nm}{2^{32}}$$

- Extrapolated attack rate R is a function of measured backscatter rate R′:

$$R \geq R' \frac{2^{32}}{n}$$

Assumption and Biases

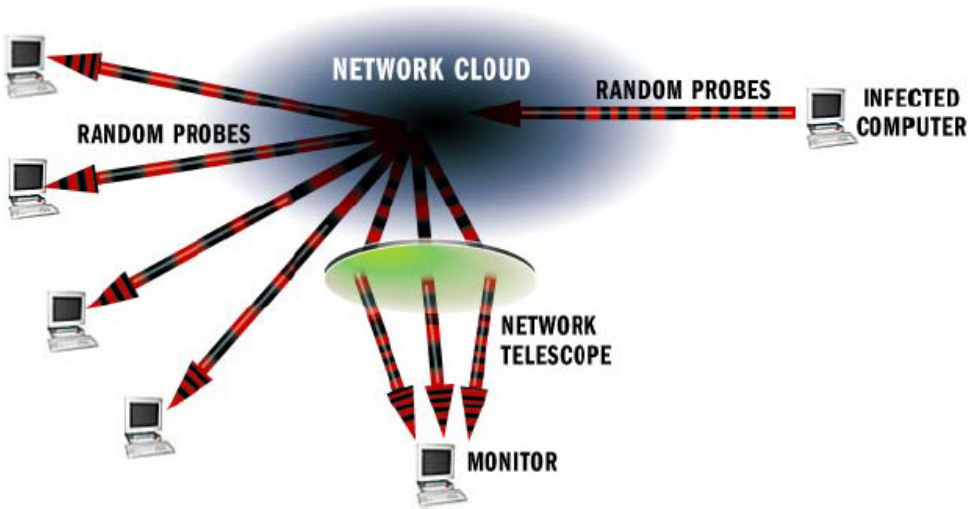
- *Address uniformity*
  - Ingress filtering, reflectors, etc. cause us to **underestimate** number of attacks
  - Can bias rate estimation (can we test uniformity?)
- *Reliable delivery*
  - Packet losses, server overload & rate limiting cause us to **underestimate** attack rates/durations
- *Backscatter hypothesis*
  - Can be biased by purposeful unsolicited packets
    - Port scanning (minor factor at worst in practice)
  - Can we verify backscatter at multiple sites?

What is a Network Worm?

- Self-propagating self-replicating network program
  - Exploits some vulnerability to infect remote machines
    - No human intervention necessary
  - Infected machines continue propagating infection

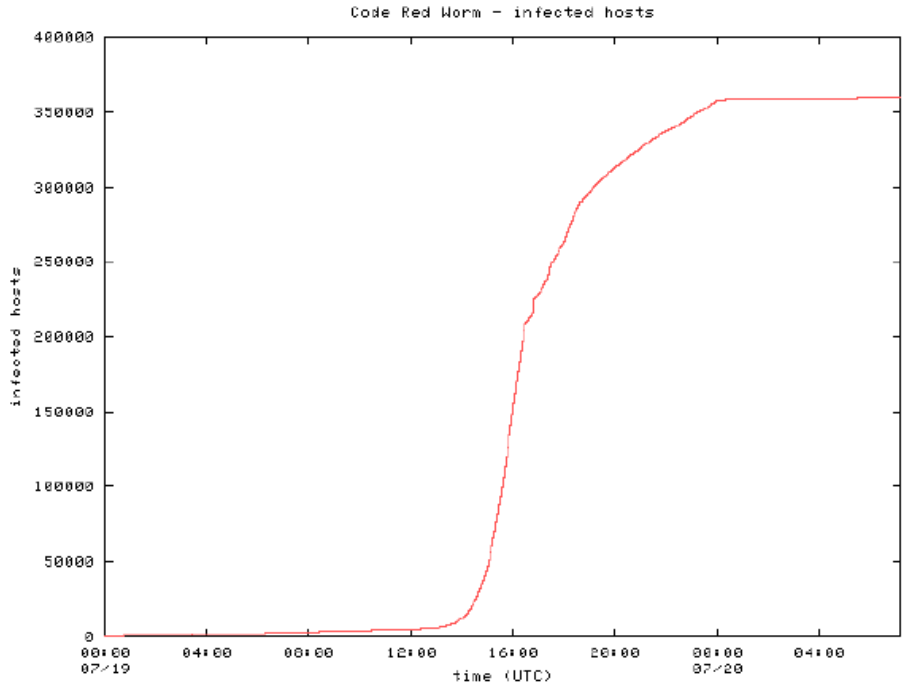
Network Telescope: Worm Attacks

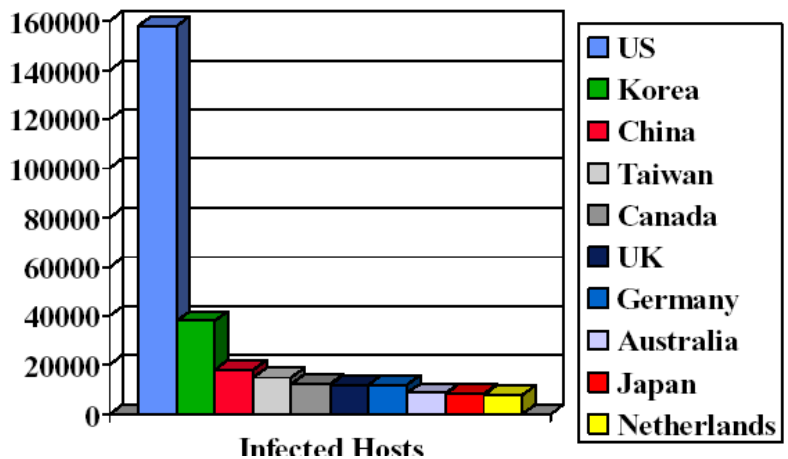
- Infected host scans for other vulnerable hosts by randomly generating IP addresses
- /8 monitor 1/256th of all IPv4 addresses
- /8 see 1/256th of all worm traffic of worms (when no bias or bugs)



Code-Red Worm

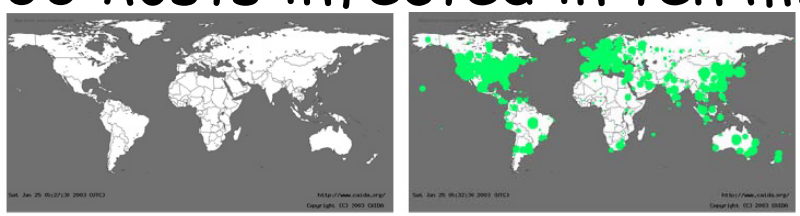
- Exploits a vulnerability in Microsoft IIS
- July 2001
- 359,000 hosts infected in 24 hour period
  - 2,000 hosts infected per minute





Saphhire/Slammer Worm

- Exploited bug in MSSQL 2000 and MSDE 2000
- Worm fit in a single UDP packet (404 bytes)
- Sapphire
  - > 1 min : > 20,000 scans/sec
  - Peaks at 3 min: 55 million IP scans/sec
  - 90% of Internet scanned in < 10 mins
  - ~ 100,000 hosts infected in ten minutes



Before 9:30PM (PST) After 9:40PM (PST)

What can we do ?

- **Measurement**
  - What are worms doing?
  - What types of hosts are infected?
  - Are new defense mechanisms working?
- **Develope operational defense**
  - Can we build an automated system to stop worms?

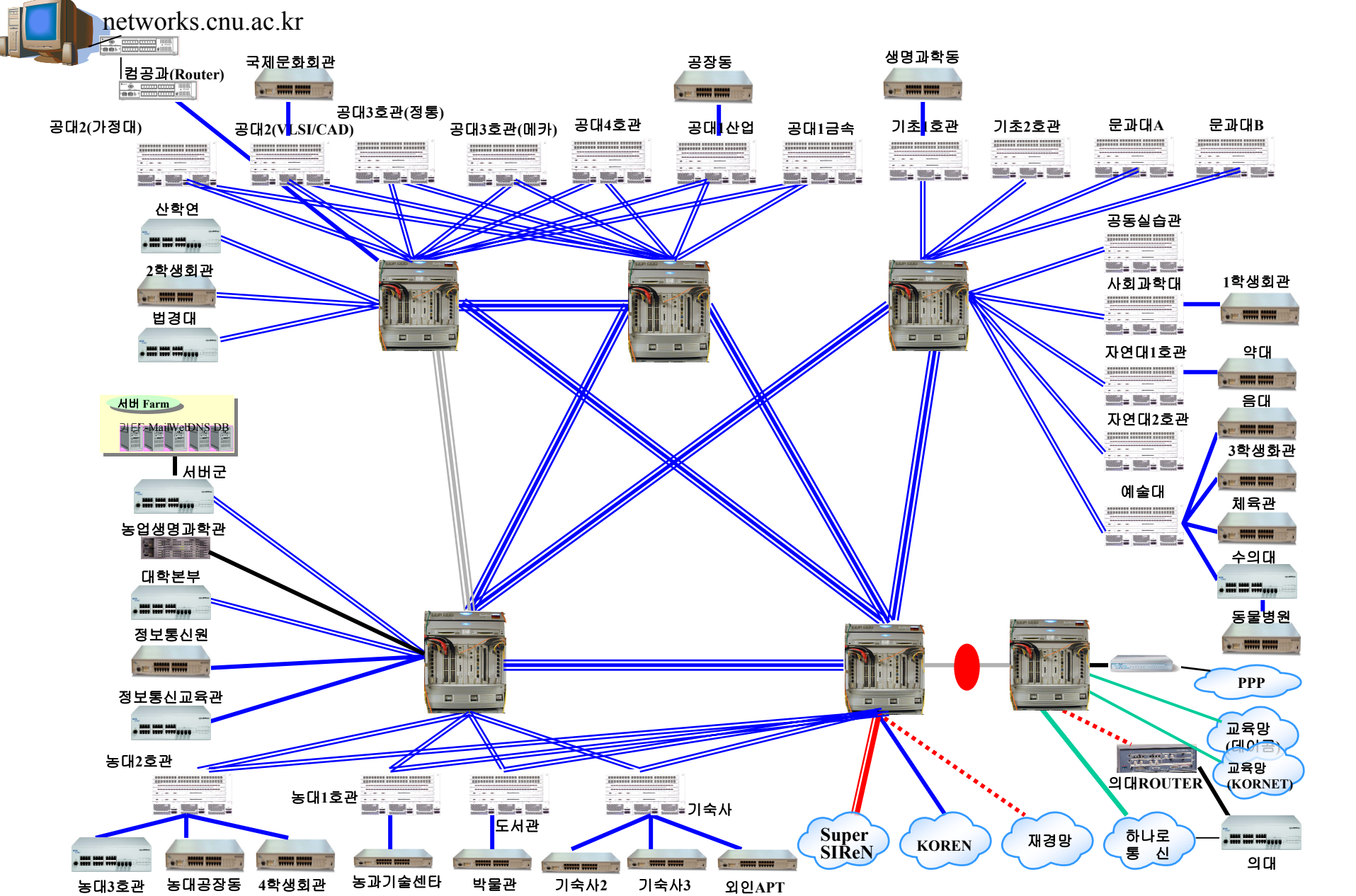
How to use Network Telescope ?

- Small telescopes may not be useful for observing external events
- Organizational network telescope
  - Useful for identifying internal problems
  - Capture data for hosts connecting to unallocated IP address space by
    - Find unallocated IP address space
      - BGP routing table
      - Flow collection on your edge router/link
    - Announce a couple unallocated networks

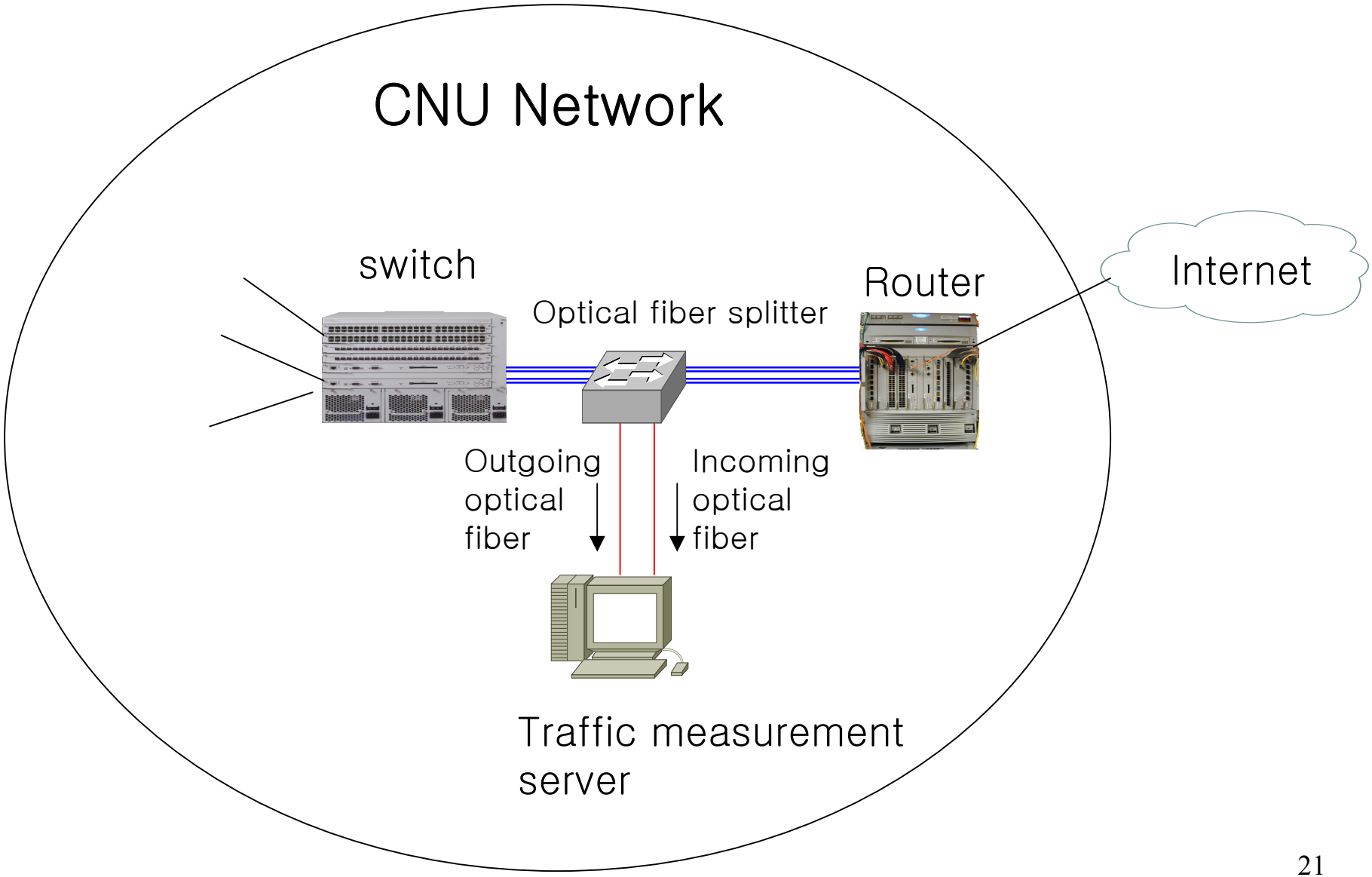
CNU Telescope

- /16 prefix
  - 255 /24 prefix blocks
  - Usually 134 /24 prefixes are not used
    - ~/17 prefix

- Let's see all incoming packets to 134 /24 prefix blocks


networks.cnu.ac.kr
컴공과(Router)
국제문화회관
공장동
생명과학동
공대2(가정대)
공대2(VLSI/CAD)
공대3호관(정통)
공대3호관(메카)
공대4호관
공대1산업
공대1금속
기초1호관
기초2호관
문과대A
문과대B
산학연
2학생회관
법경대
공동실습관
사회과학대
1학생회관
자연대1호관
약대
자연대2호관
음대
3학생화관
예술대
체육관
수의대
동물병원
서버 Farm
서버군
농업생명과학관
대학본부
정보통신원
정보통신교육관
농대2호관
농대1호관
도서관
기숙사
농대3호관
농대공장동
4학생회관
농과기술센타
박물관
기숙사2
기숙사3
외인APT
PPP
교육망
교육망
(KORNET)
의대ROUTER
의대
Super SIReN
KOREN
재경망
하나로 통 신
4Gbps Trunk
2Gbps Trunk
1Gbps
E1
155Mbps
100Mbps
T3
10Gbps
Router
8610CO
8606
Bay380
Bay420
Cisco 7513
Cisco 7204

Measurement Point



Measurement System

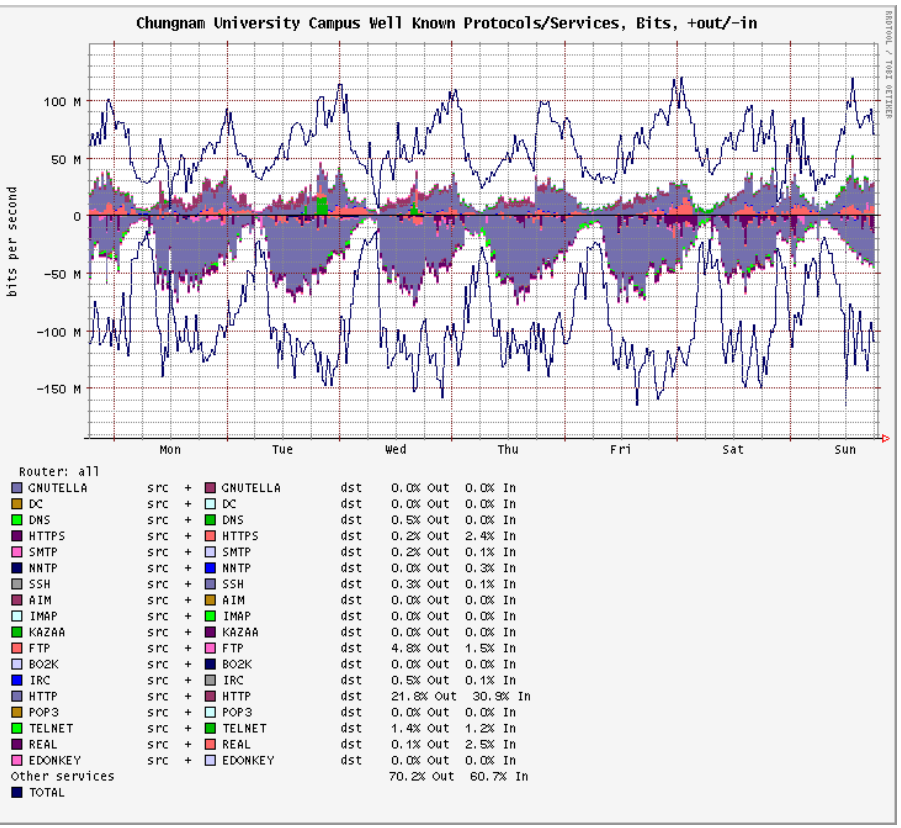
- OS: Linux 2.4.18-14
- 1GE Nic: Intel Express Pro 1000 MF
  - Two nics for inbound/outbound traffic
- Measurement S/W
  - Pcaplib
  - Tcpdump/nProbe
  - Flow-tools
  - Flow-scan

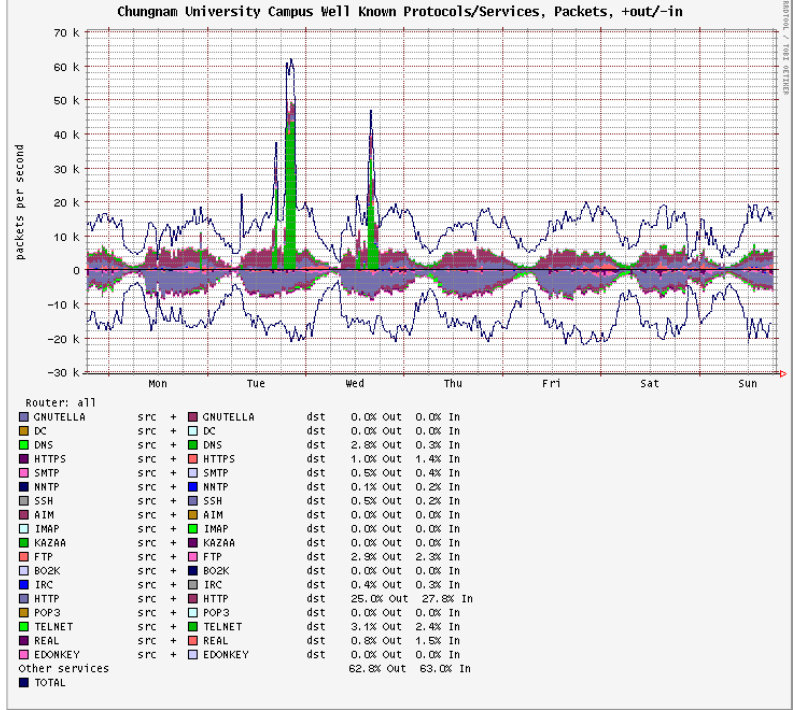
- CNU traffic
  - http://168.188.2.119/measurement

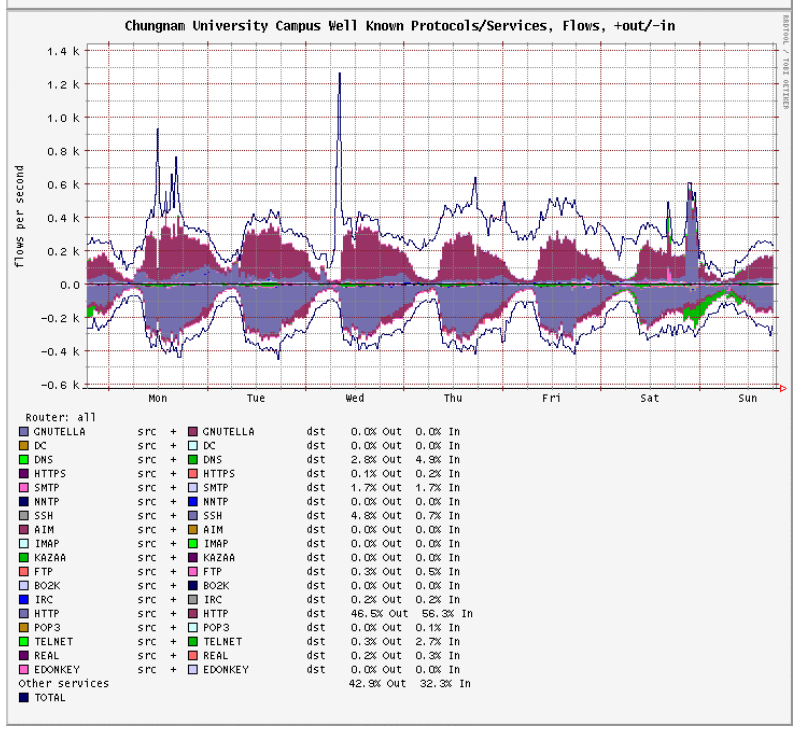
From Captured Flows to Graph

1. Capture a packet
   - Software-based: pcaplib (e.g., tcpdump)
2. Generate netflow v5 flow
   - Tool: nProbe with pcaplib
     - Send netflow v5 in UDP datagram
3. Store flows into a file
   - Tool: flow-tools (flow-capture)
4. Analysis
   - update DB and plot graphs every 5 minutes
     - Graph of RRD DB with processed 5-minute aggregated file
     - Tools: flowscan, rrd
   - Offline
     - Tools: flow-tools, gnuplot, ppmtogif, gifsicle

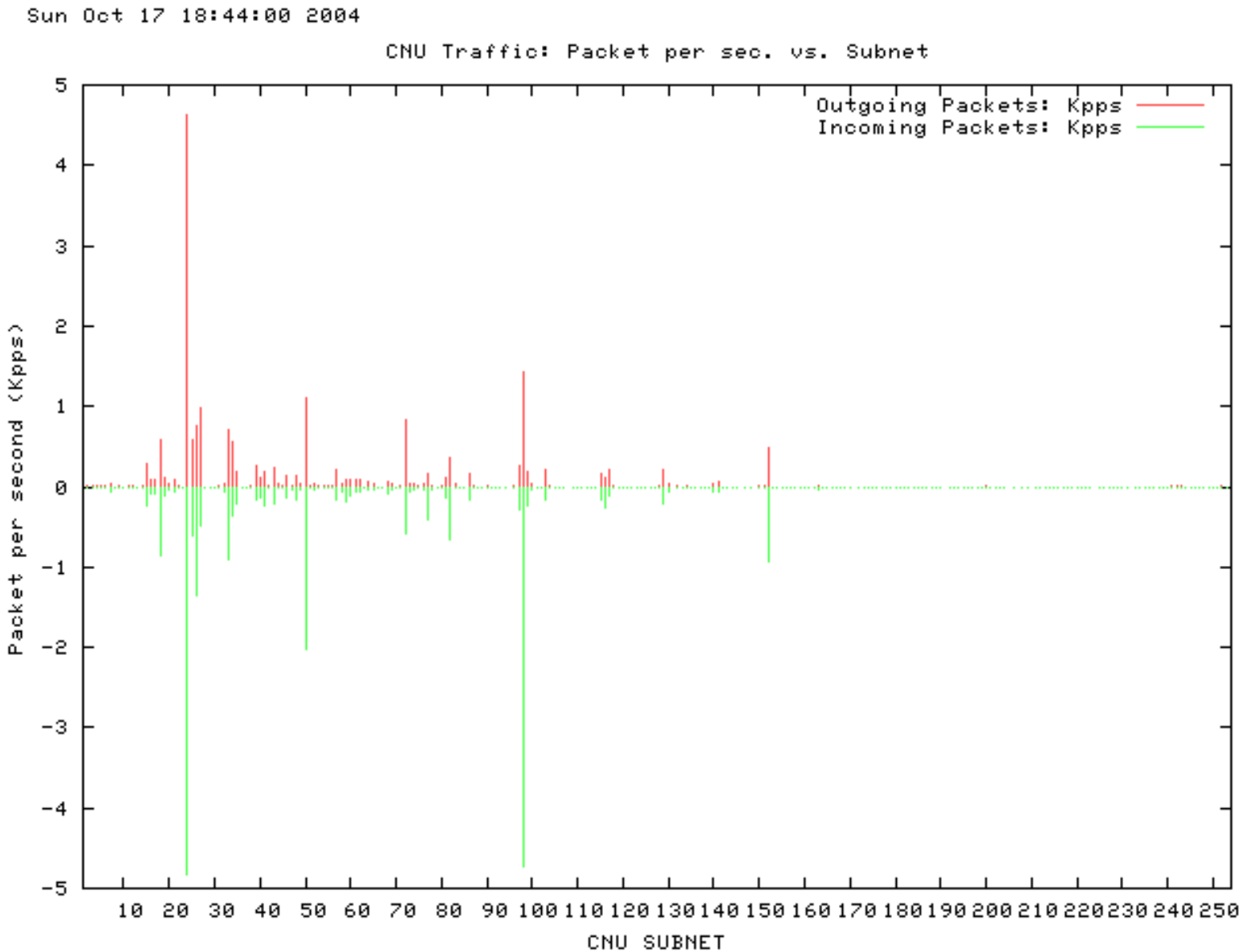
CNU 트래픽


Chungnam University Campus Well Known Protocols/Services, Bits, +out/-in
bits per second
100 M
50 M
0
-50 M
-100 M
-150 M
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Router: all
GNUTELLA src + GNUTELLA dst 0.0% Out 0.0% In
DC src + DC dst 0.0% Out 0.0% In
DNS src + DNS dst 0.5% Out 0.0% In
HTTPS src + HTTPS dst 0.2% Out 2.4% In
SMTP src + SMTP dst 0.2% Out 0.1% In
NNTP src + NNTP dst 0.0% Out 0.3% In
SSH src + SSH dst 0.3% Out 0.1% In
AIM src + AIM dst 0.0% Out 0.0% In
IMAP src + IMAP dst 0.0% Out 0.0% In
KAZAA src + KAZAA dst 0.0% Out 0.0% In
FTP src + FTP dst 4.8% Out 1.5% In
BO2K src + BO2K dst 0.0% Out 0.0% In
IRC src + IRC dst 0.5% Out 0.1% In
HTTP src + HTTP dst 21.8% Out 30.9% In
POP3 src + POP3 dst 0.0% Out 0.0% In
TELNET src + TELNET dst 1.4% Out 1.2% In
REAL src + REAL dst 0.1% Out 2.5% In
EDONKEY src + EDONKEY dst 0.0% Out 0.0% In
Other services 70.2% Out 60.7% In
TOTAL

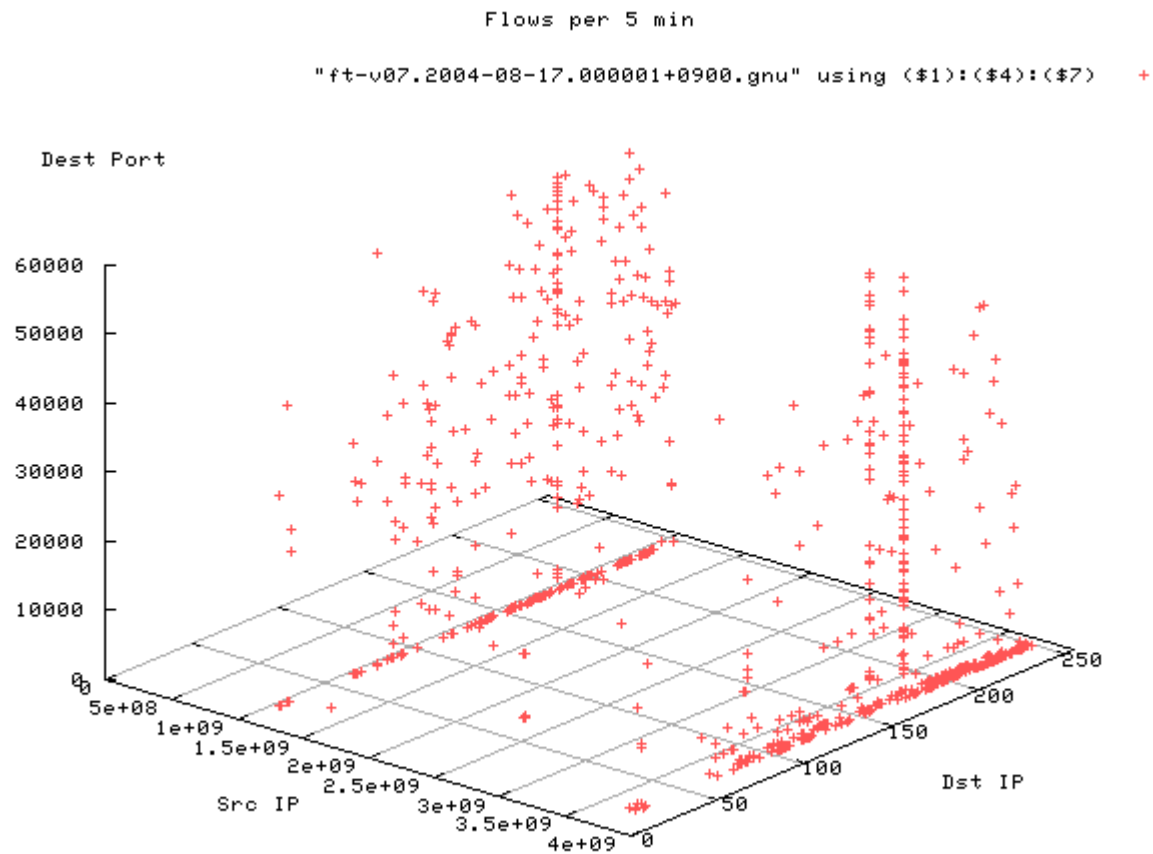

Chungnam University Campus Well Known Protocols/Services, Packets, +out/-in
packets per second
70 k
60 k
50 k
40 k
30 k
20 k
10 k
0
-10 k
-20 k
-30 k
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Router: all
GNUTELLA src + GNUTELLA dst 0.0% Out 0.0% In
DC src + DC dst 0.0% Out 0.0% In
DNS src + DNS dst 2.8% Out 0.3% In
HTTPS src + HTTPS dst 1.0% Out 1.4% In
SMTP src + SMTP dst 0.5% Out 0.4% In
NNTP src + NNTP dst 0.1% Out 0.2% In
SSH src + SSH dst 0.5% Out 0.2% In
AIM src + AIM dst 0.0% Out 0.0% In
IMAP src + IMAP dst 0.0% Out 0.0% In
KAZAA src + KAZAA dst 0.0% Out 0.0% In
FTP src + FTP dst 2.3% Out 2.3% In
BO2K src + BO2K dst 0.0% Out 0.0% In
IRC src + IRC dst 0.4% Out 0.3% In
HTTP src + HTTP dst 25.0% Out 27.8% In
POP3 src + POP3 dst 0.0% Out 0.0% In
TELNET src + TELNET dst 3.1% Out 2.4% In
REAL src + REAL dst 0.8% Out 1.5% In
EDONKEY src + EDONKEY dst 0.0% Out 0.0% In
Other services 62.8% Out 63.0% In
TOTAL


Chungnam University Campus Well Known Protocols/Services, Flows, +out/-in
flows per second
1.4 k
1.2 k
1.0 k
0.8 k
0.6 k
0.4 k
0.2 k
0.0
-0.2 k
-0.4 k
-0.6 k
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Router: all
GNUTELLA src + GNUTELLA dst 0.0% Out 0.0% In
DC src + DC dst 0.0% Out 0.0% In
DNS src + DNS dst 2.8% Out 4.3% In
HTTPS src + HTTPS dst 0.1% Out 0.2% In
SMTP src + SMTP dst 1.7% Out 1.7% In
NNTP src + NNTP dst 0.0% Out 0.0% In
SSH src + SSH dst 4.8% Out 0.7% In
AIM src + AIM dst 0.0% Out 0.0% In
IMAP src + IMAP dst 0.0% Out 0.0% In
KAZAA src + KAZAA dst 0.0% Out 0.0% In
FTP src + FTP dst 0.3% Out 0.5% In
BO2K src + BO2K dst 0.0% Out 0.0% In
IRC src + IRC dst 0.2% Out 0.2% In
HTTP src + HTTP dst 46.5% Out 56.3% In
POP3 src + POP3 dst 0.0% Out 0.1% In
TELNET src + TELNET dst 0.3% Out 2.7% In
REAL src + REAL dst 0.2% Out 0.3% In
EDONKEY src + EDONKEY dst 0.0% Out 0.0% In
Other services 42.9% Out 32.3% In
TOTAL

CNU Telescope: Unused Prefix



Traffic captured by CNU Telescope

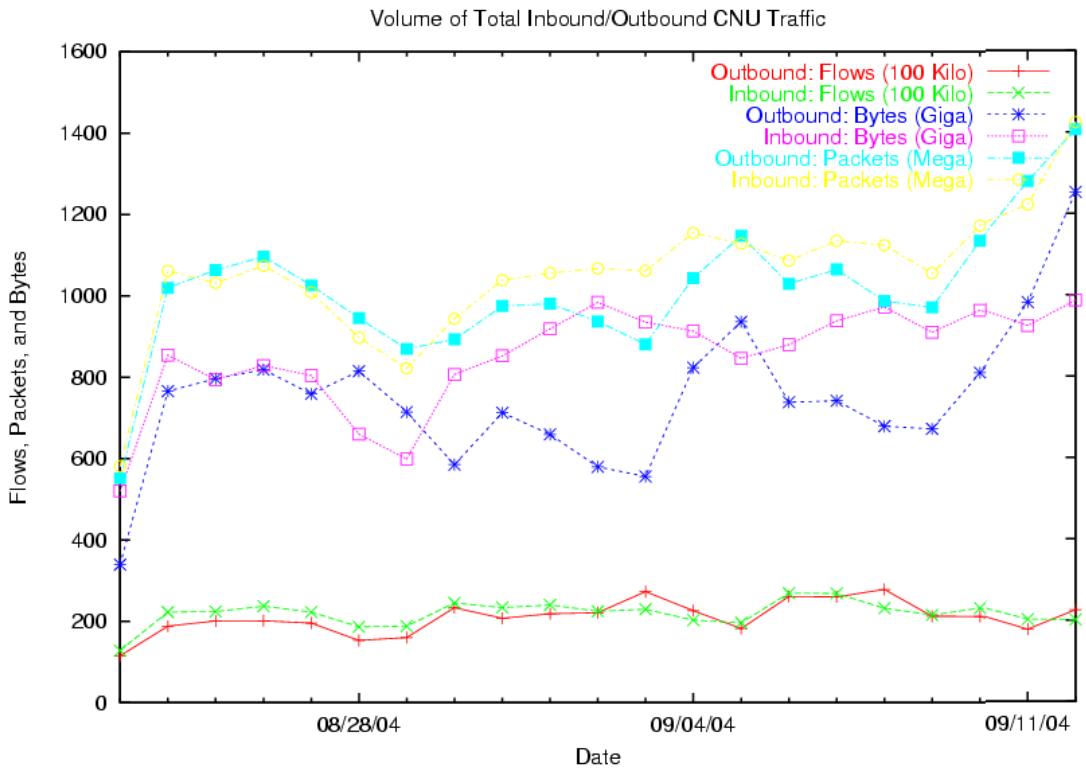


Flows of (src IP, dst IP, dst port) : 1 day traffic every 5 minutes

Traffic Statistics by CNU Telescope

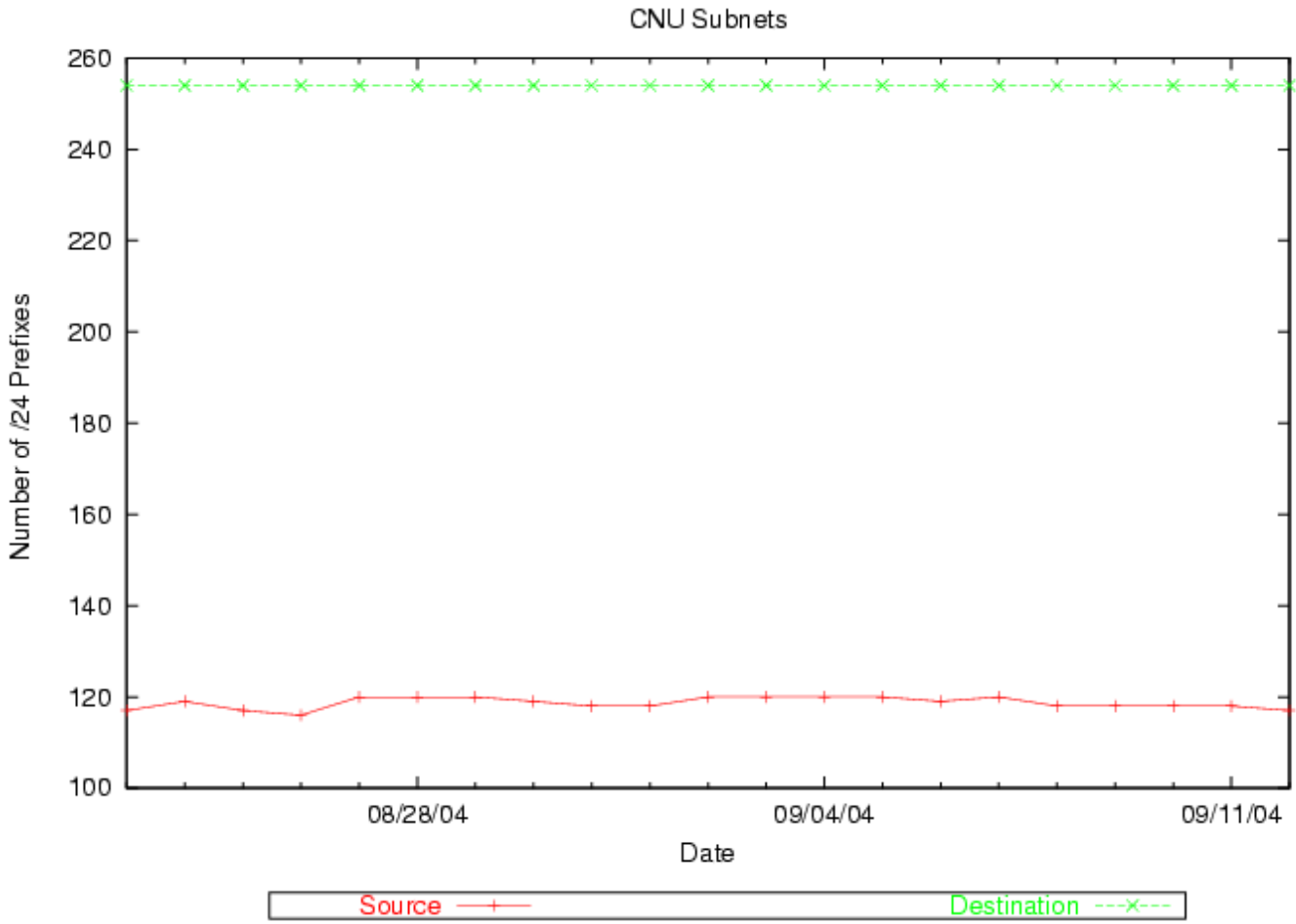
- Period
  - 2004.8.23 – 2004.9.12 (3 weeks)
- NetFlow v5 flow data
  - Packet traces collected by tcpdump

CNU Normal Traffic

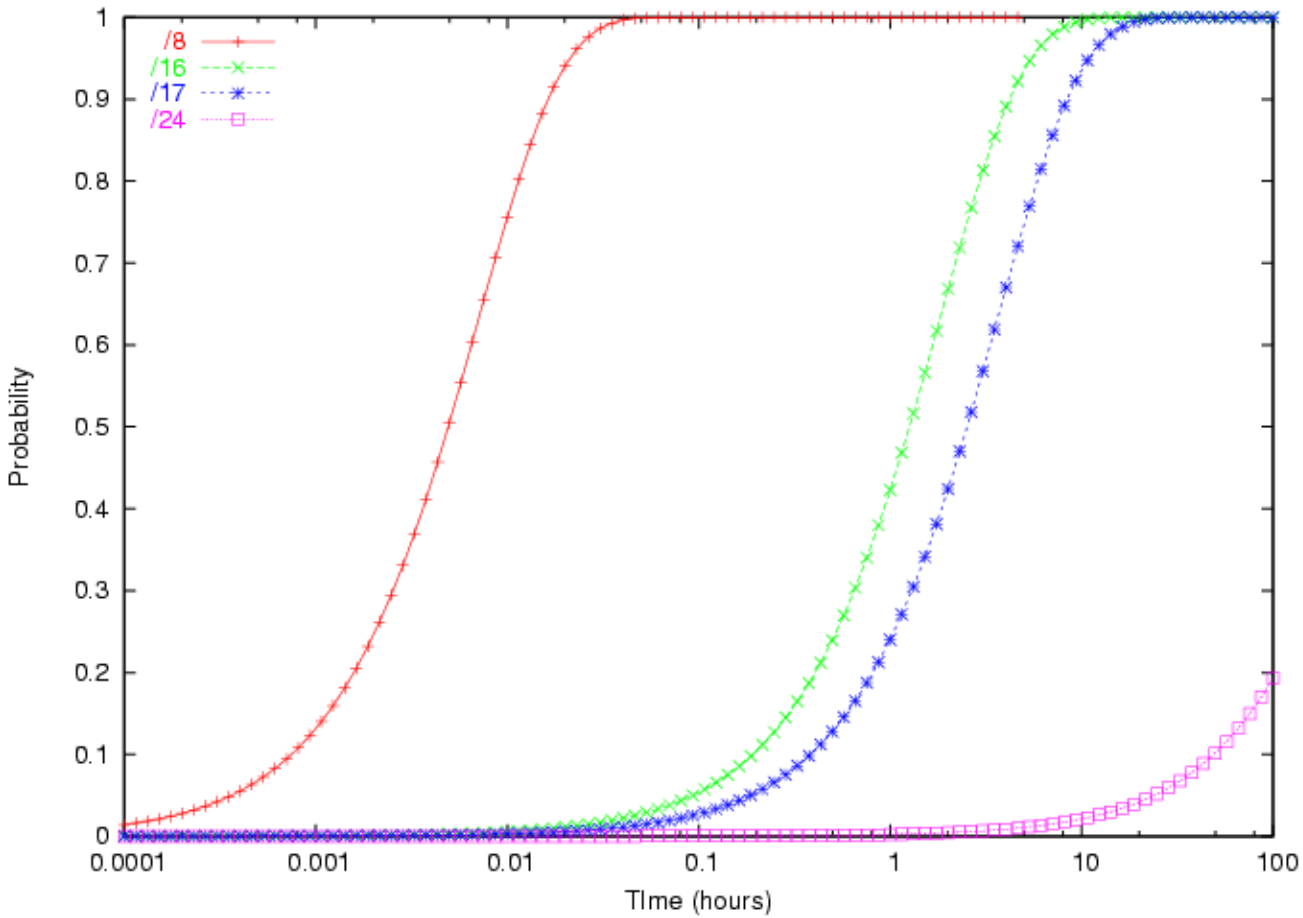


	Flows	Bytes	Packets
Inbound	21,936,820	852,079,335,590	1,054,645,523
Outbound	20,978,303	749,515,362,245	1,014,432,313

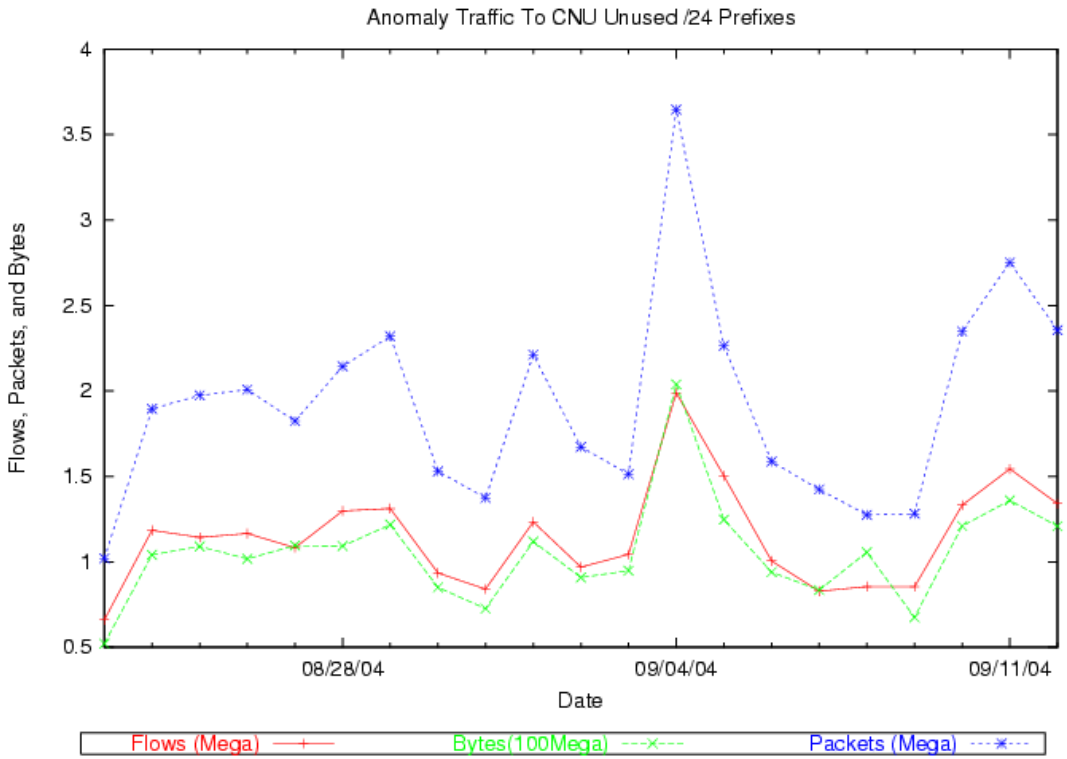
Utilization of /24 Prefix Blocks



/17 Prefix Telescope

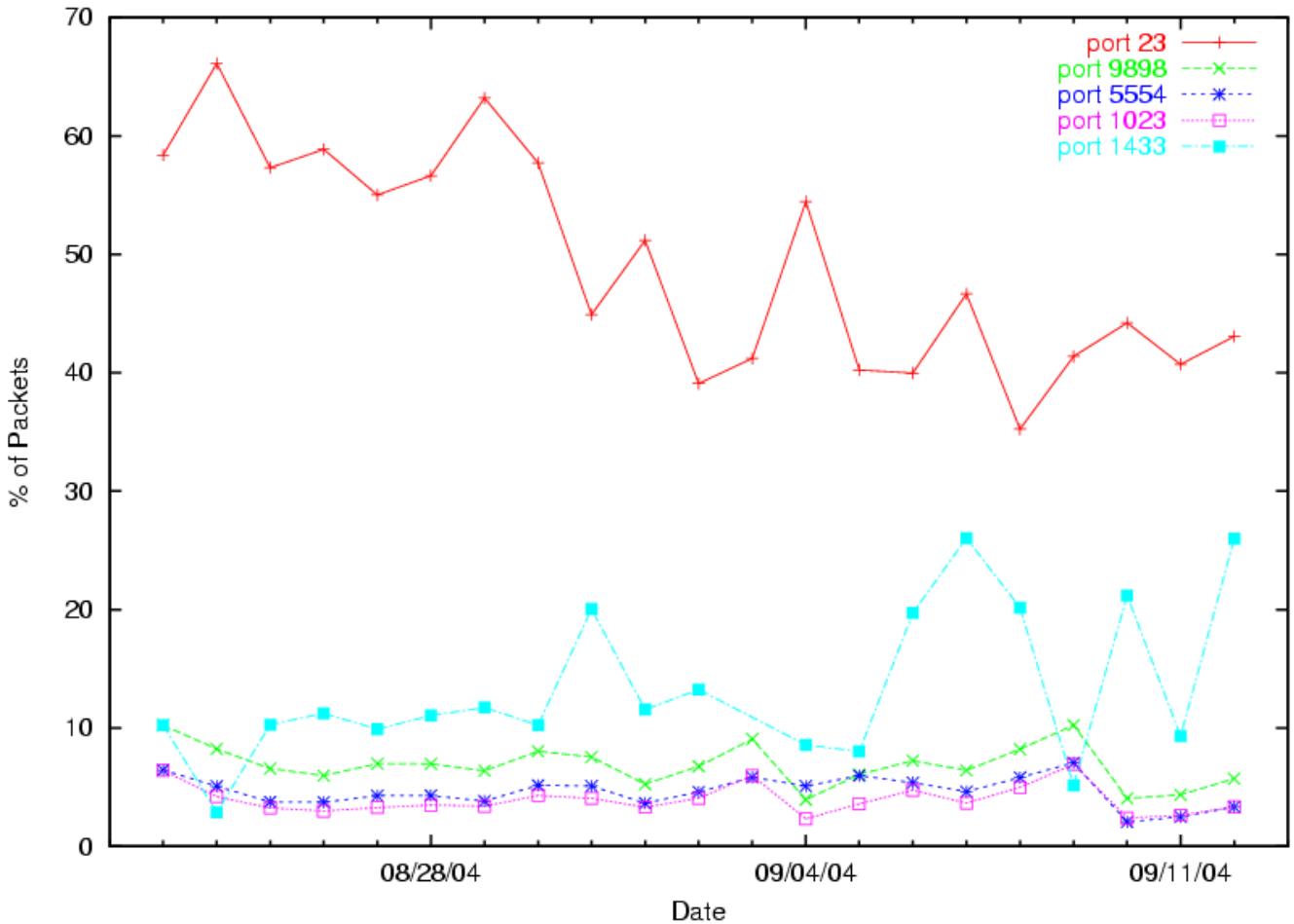


Anomaly Traffic

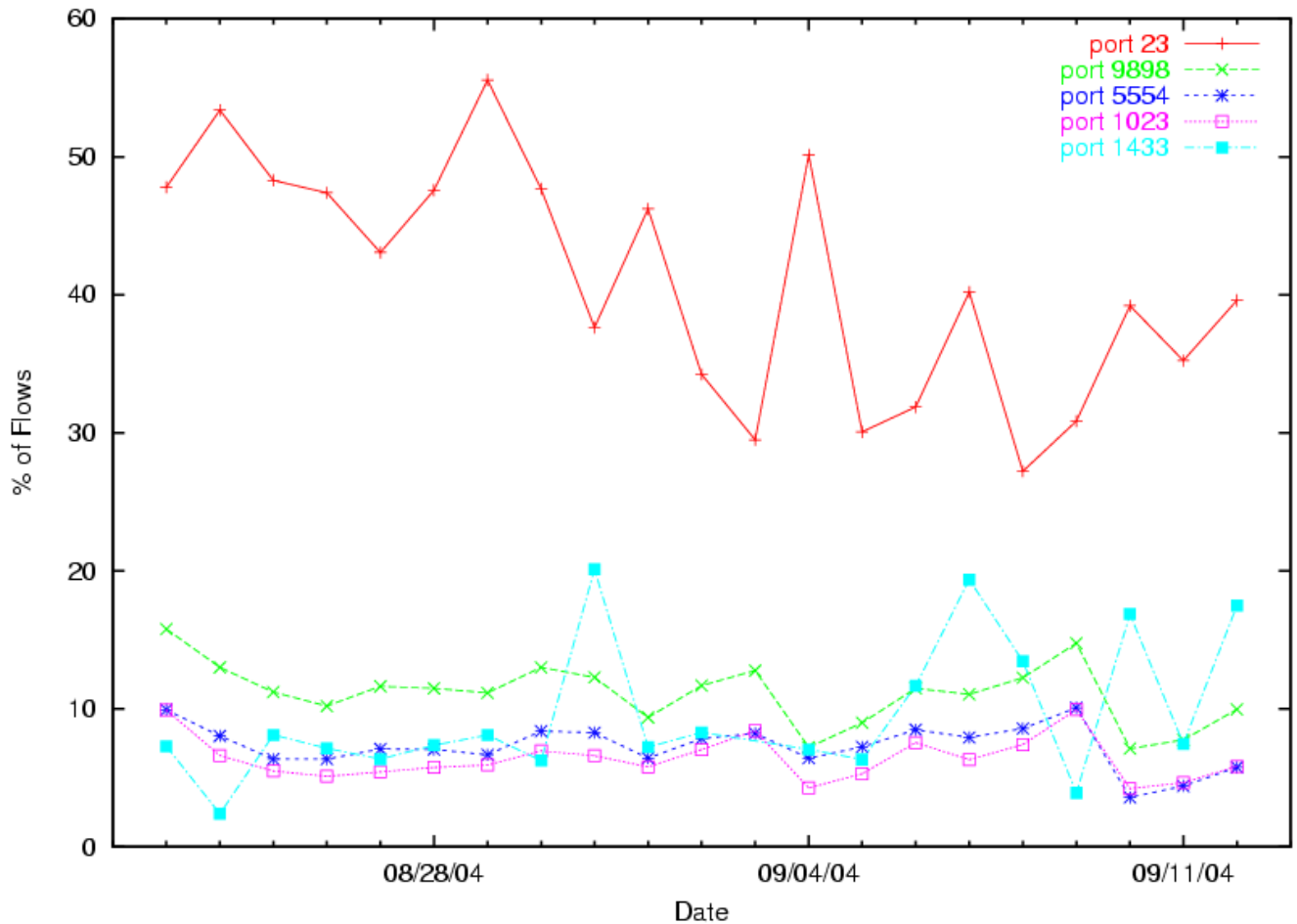


	Flows	Bytes	Packets
Total	1,148,913	105,728,303	1,924,957
TCP	1,097,147	90,716,670	1,843,960
UDP	21,675	10,806,172	23,684
ICMP	30,088	4,205,142	57,310

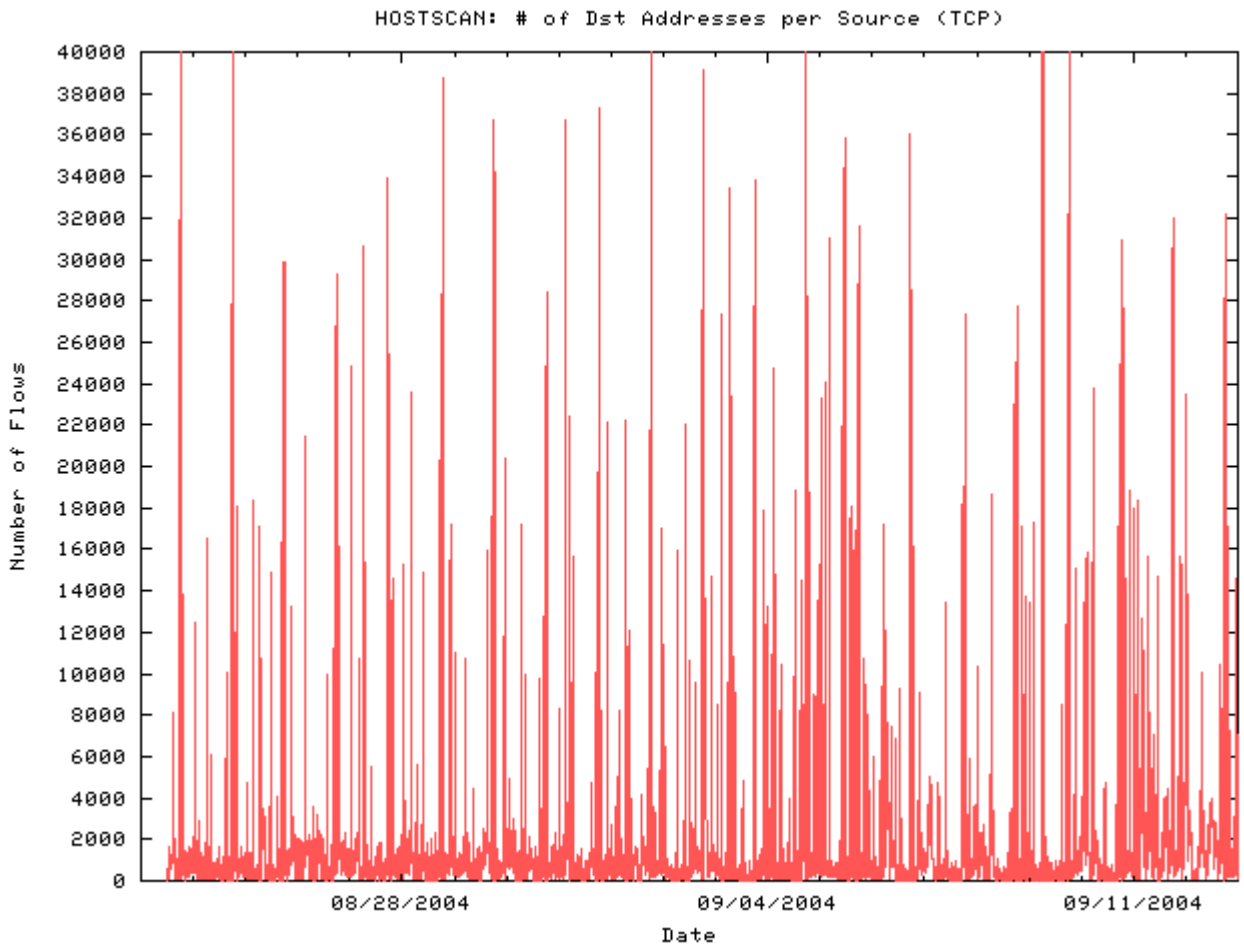
Anomaly Traffic : Port Breakdown (1)



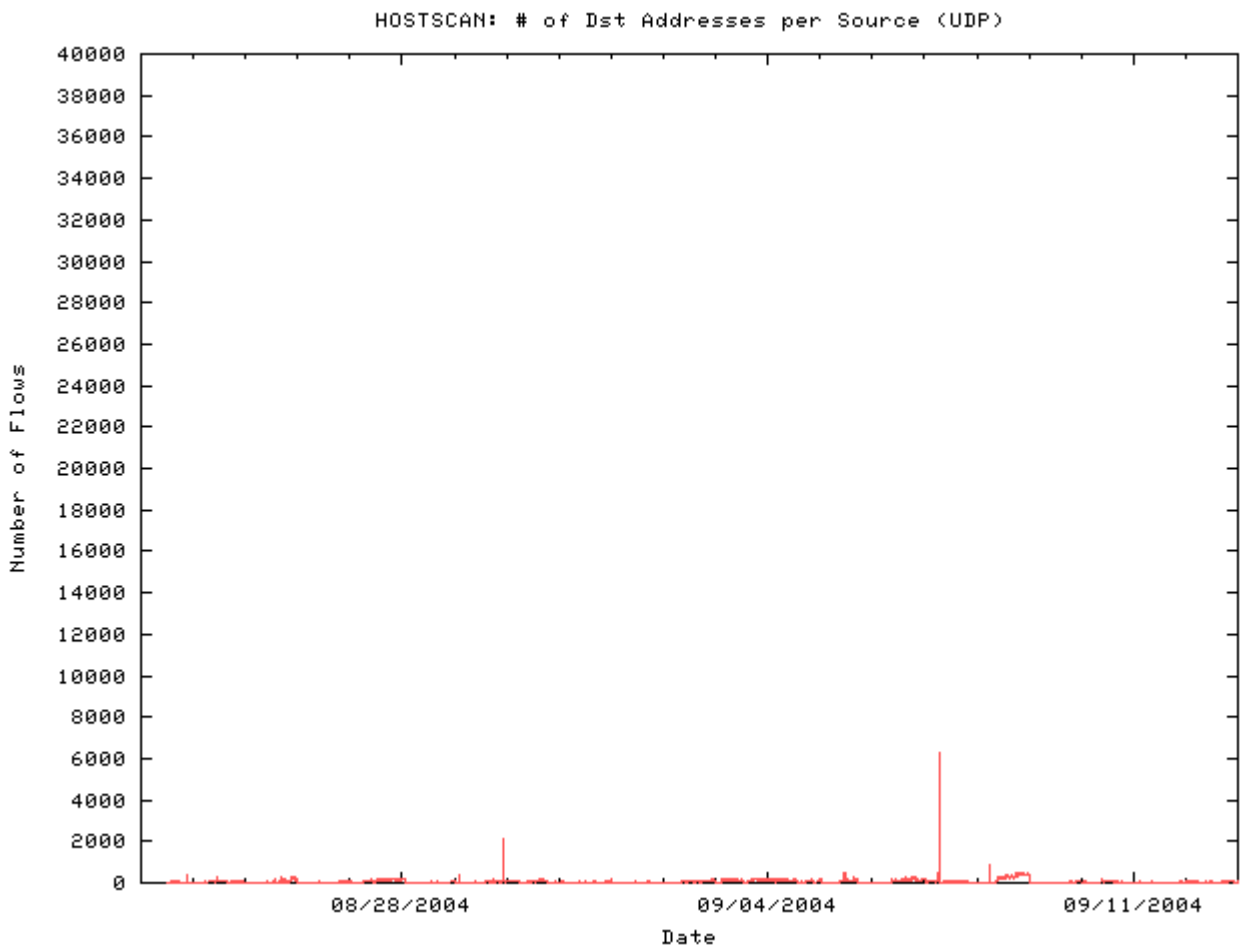
Anomaly Traffic : Port Breakdown (2)



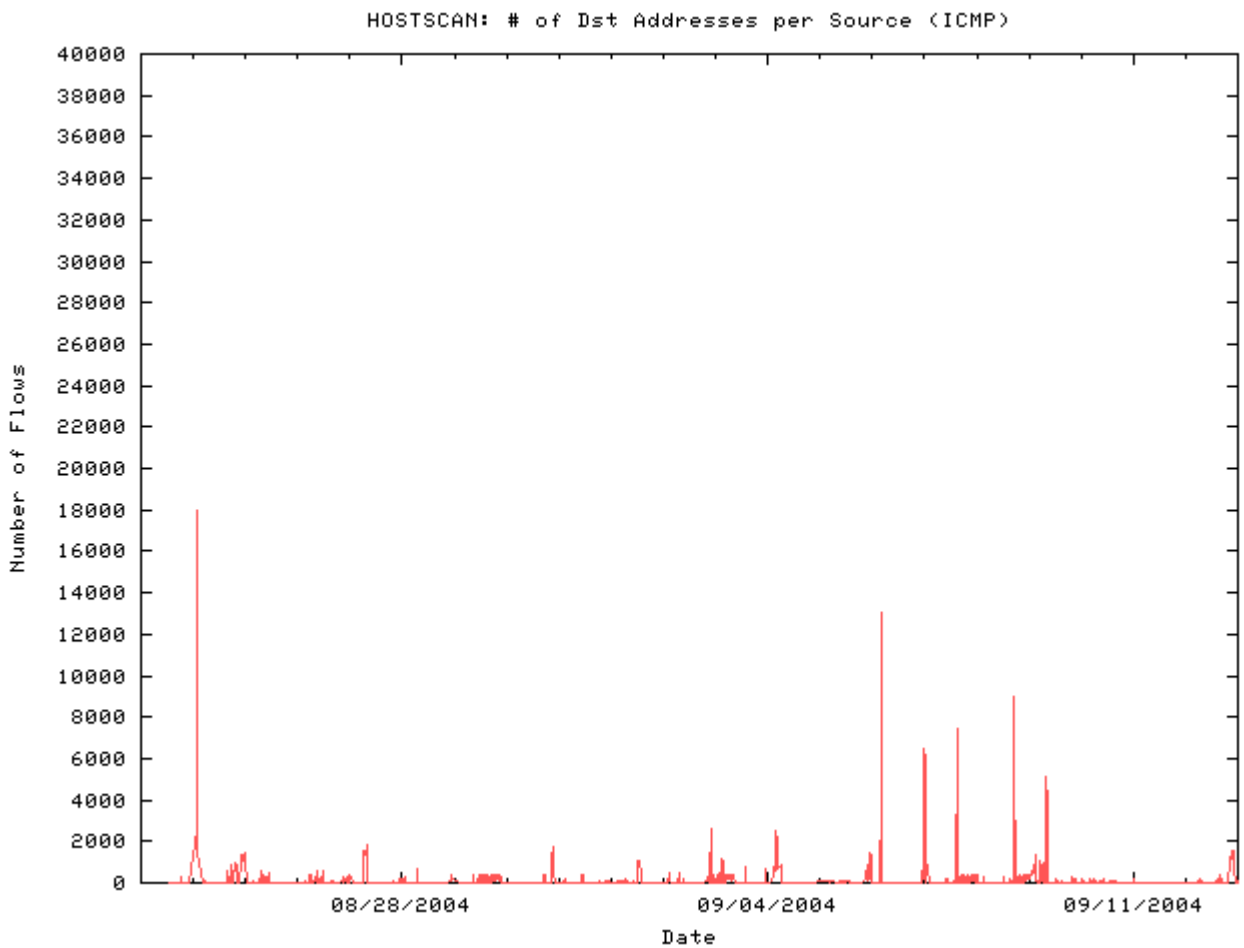
of Scanned IP Addresses (TCP)



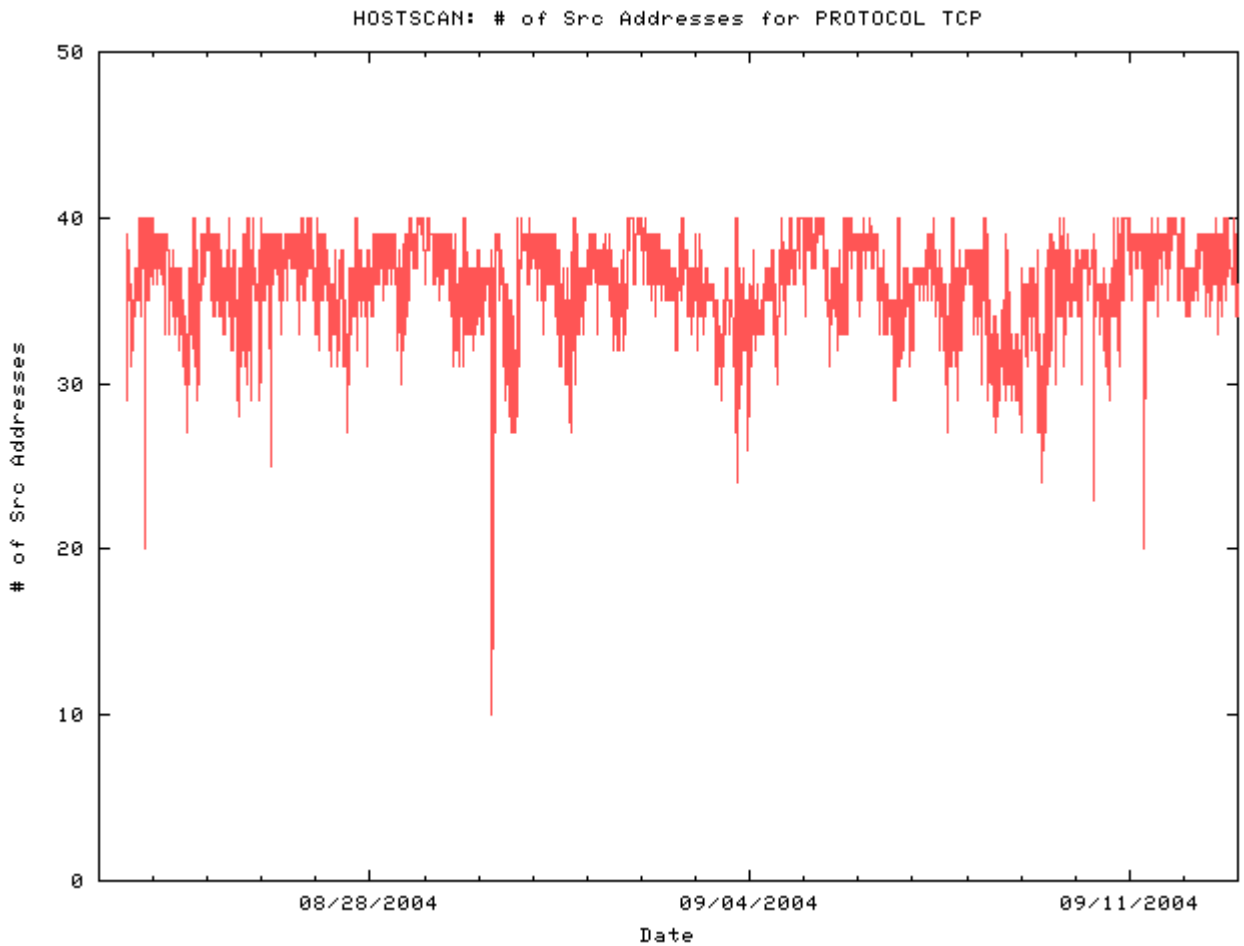
of Scanned IP Addresses (UDP)



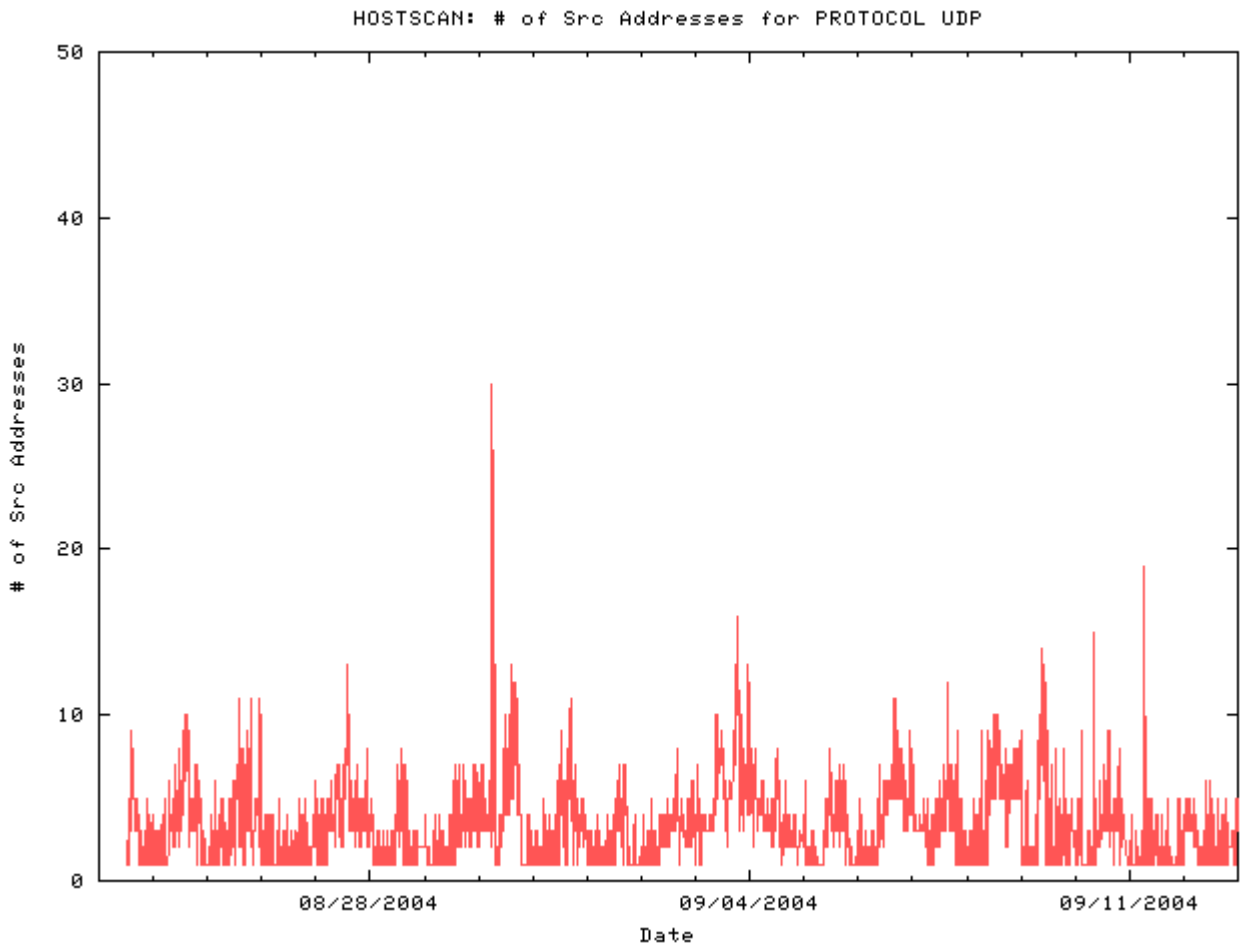
of Scanned IP Addresses (ICMP)



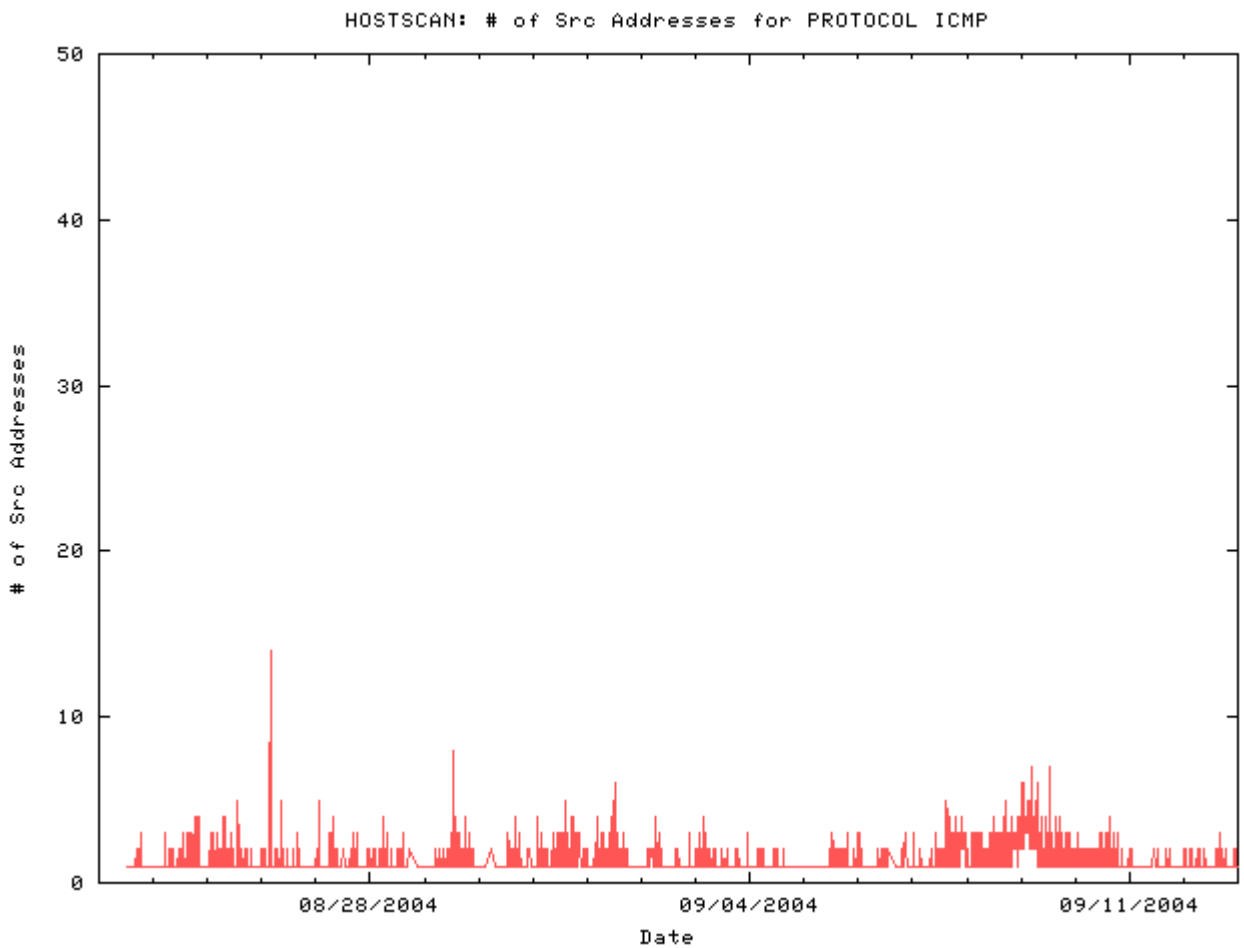
of Senders (TCP)



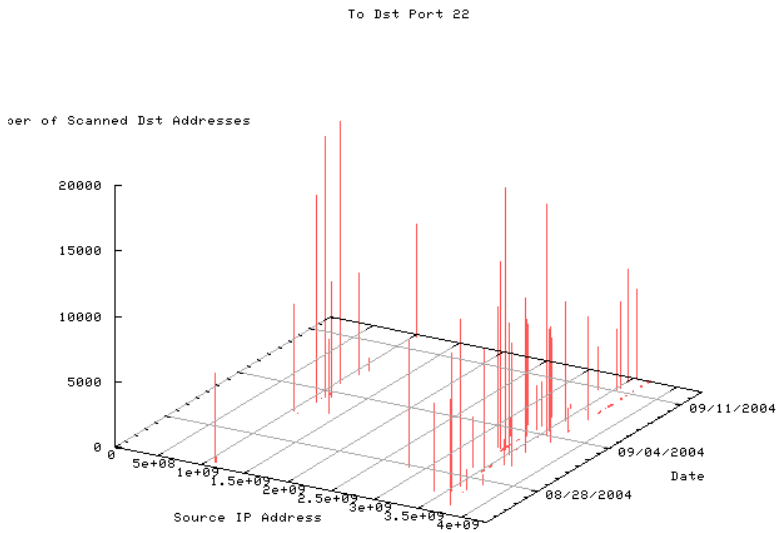
of Senders (UDP)

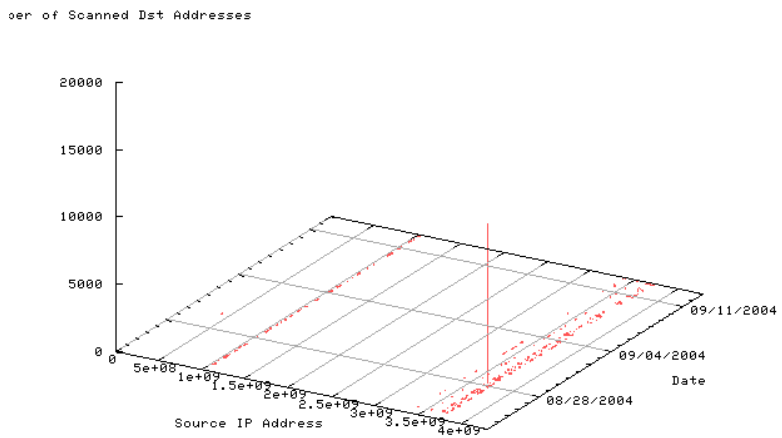


of Senders (ICMP)

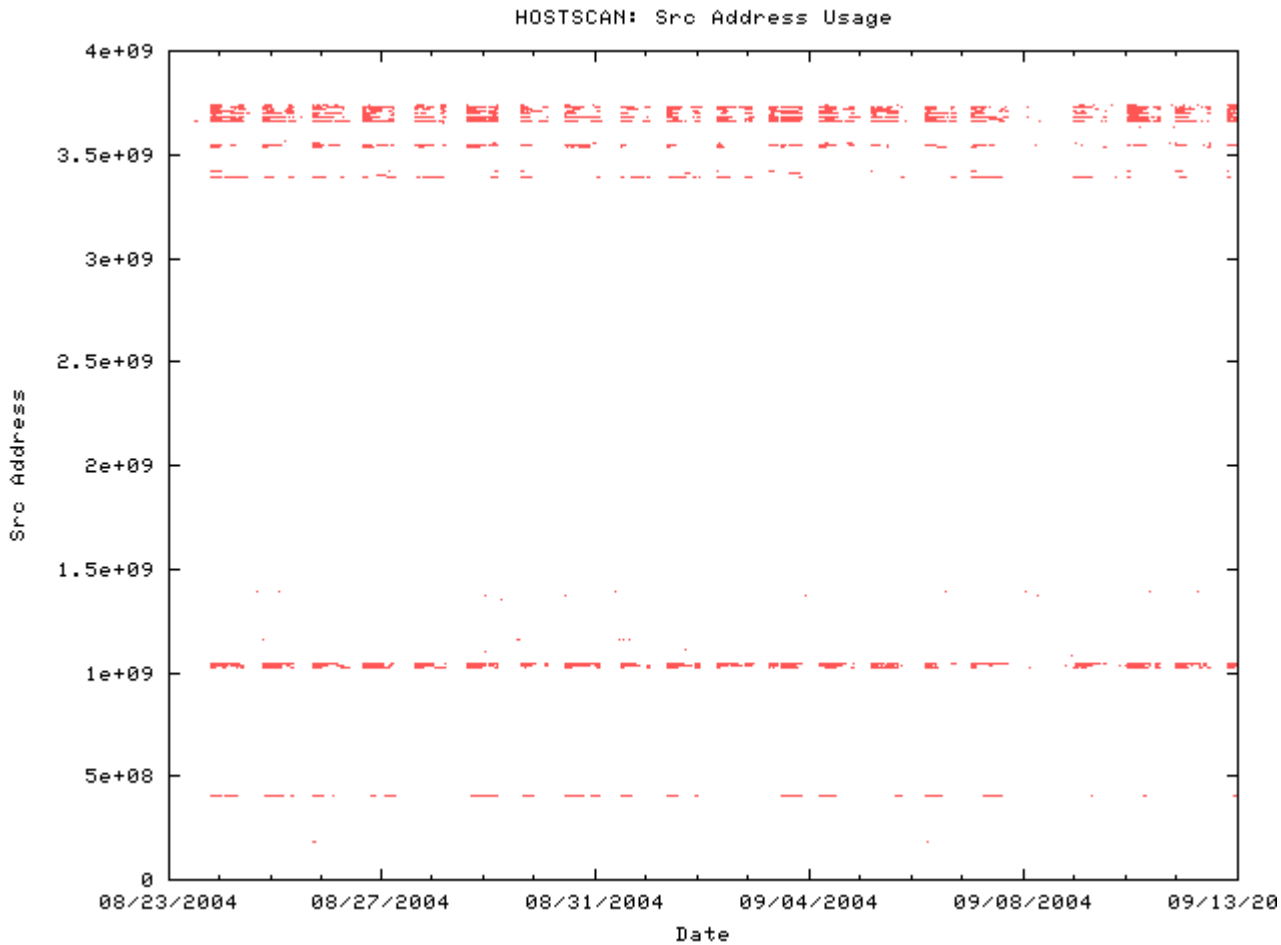


Port 22,23

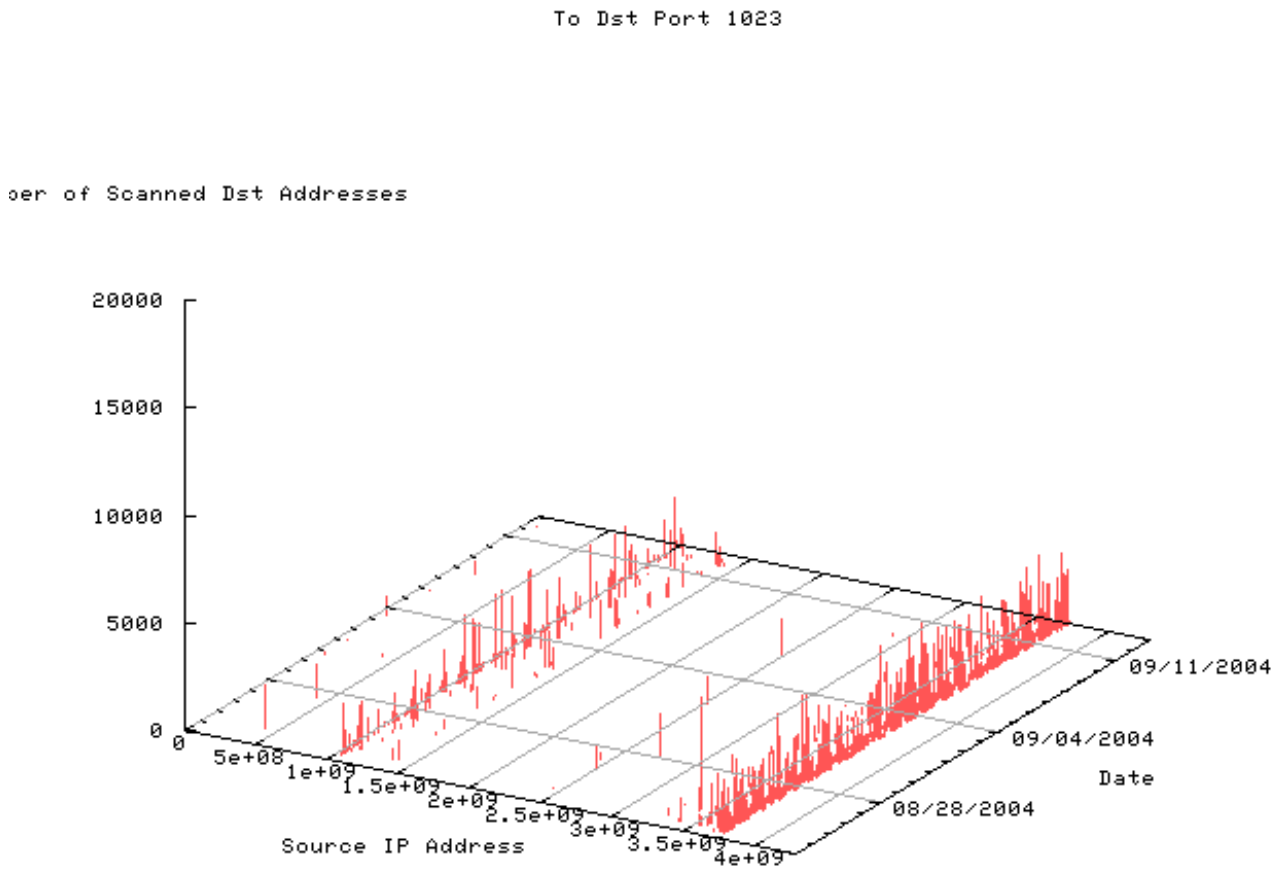

To Dst Port 22
oer of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
08/28/2004
09/04/2004
09/11/2004
Date


oer of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
08/28/2004
09/04/2004
09/11/2004
Date

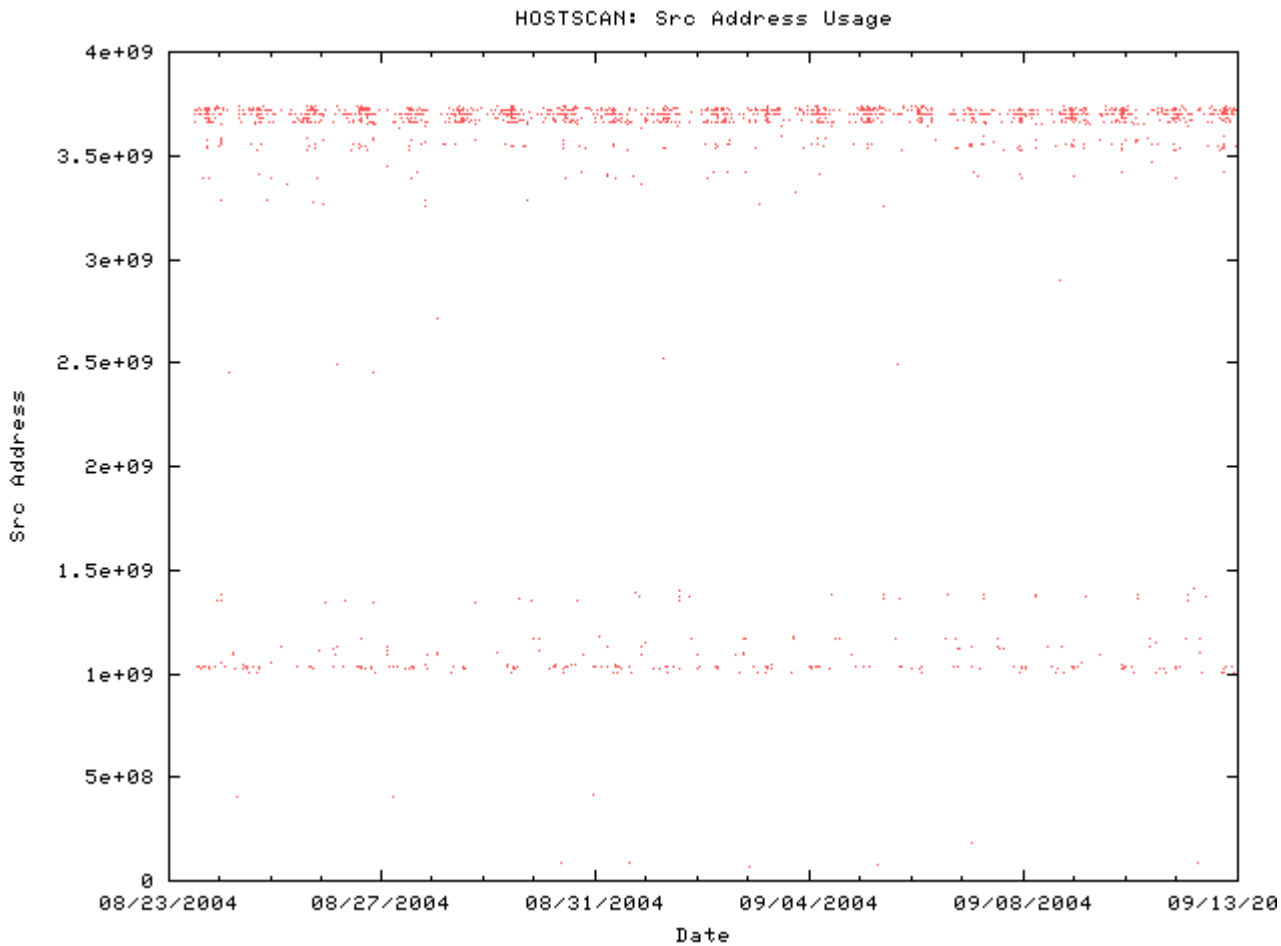
Src Addr toward port 23



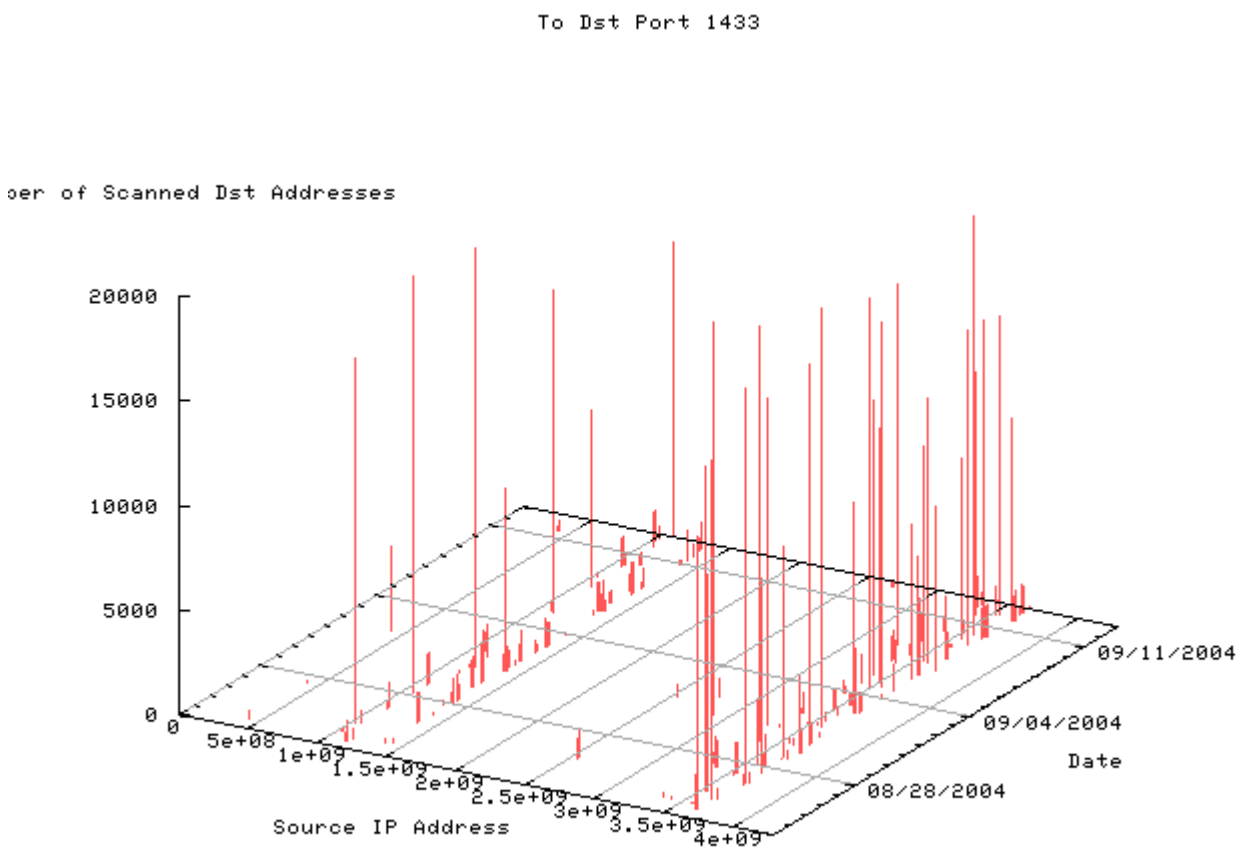
Port 1023


To Dst Port 1023
oer of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
09/11/2004
09/04/2004
08/28/2004
Date

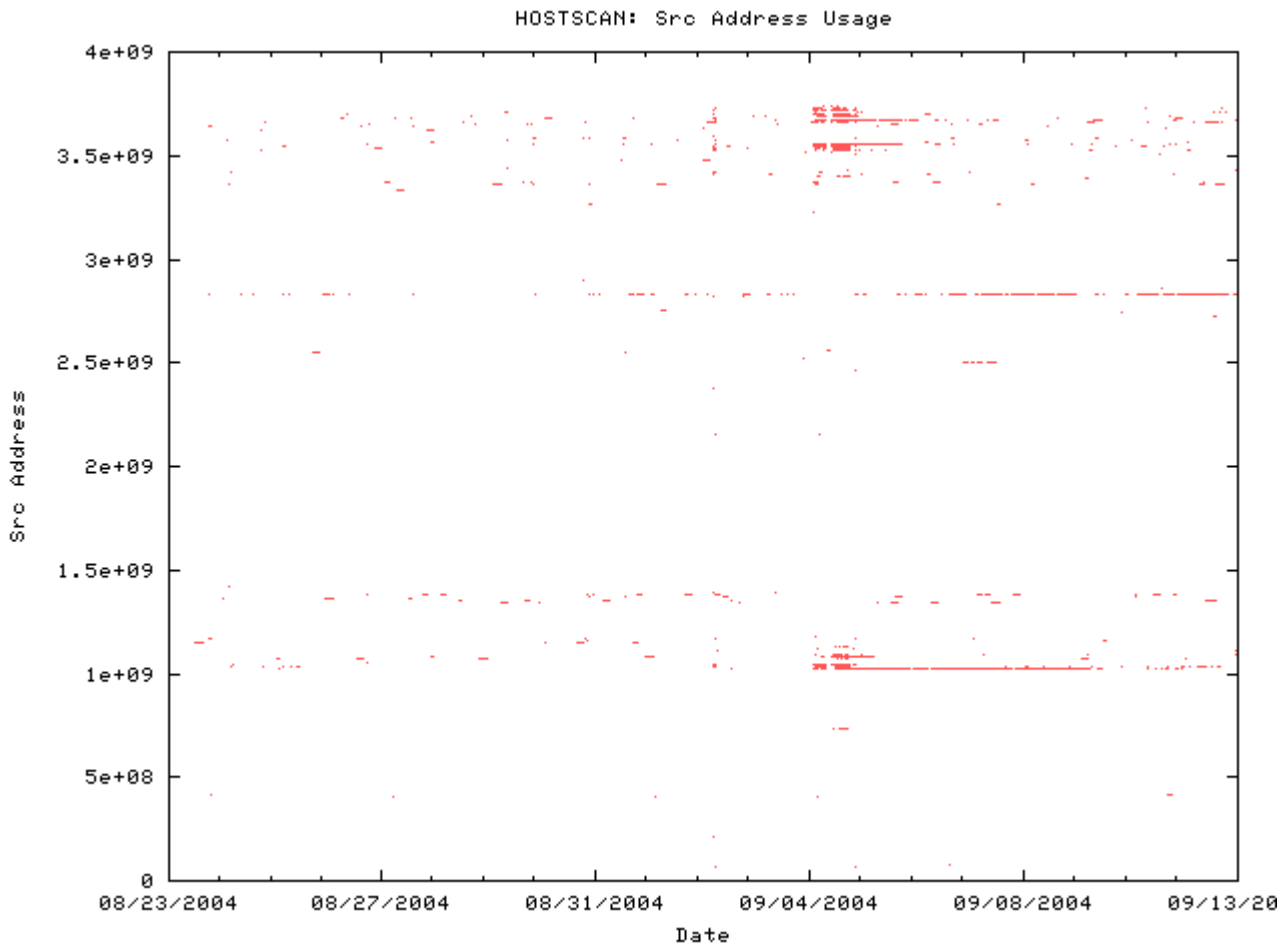
Src Addr toward port 1023



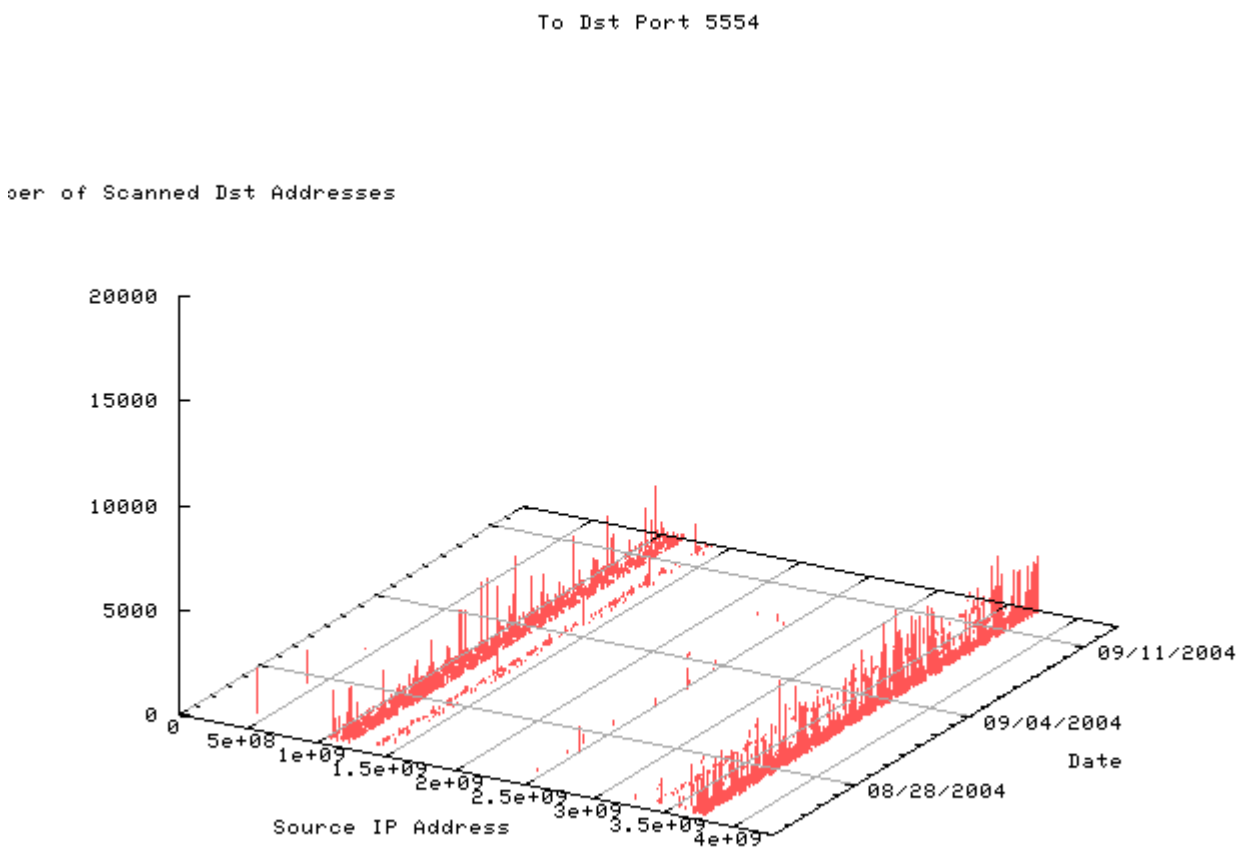
Port 1433


To Dst Port 1433
ber of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
09/11/2004
09/04/2004
08/28/2004
Date

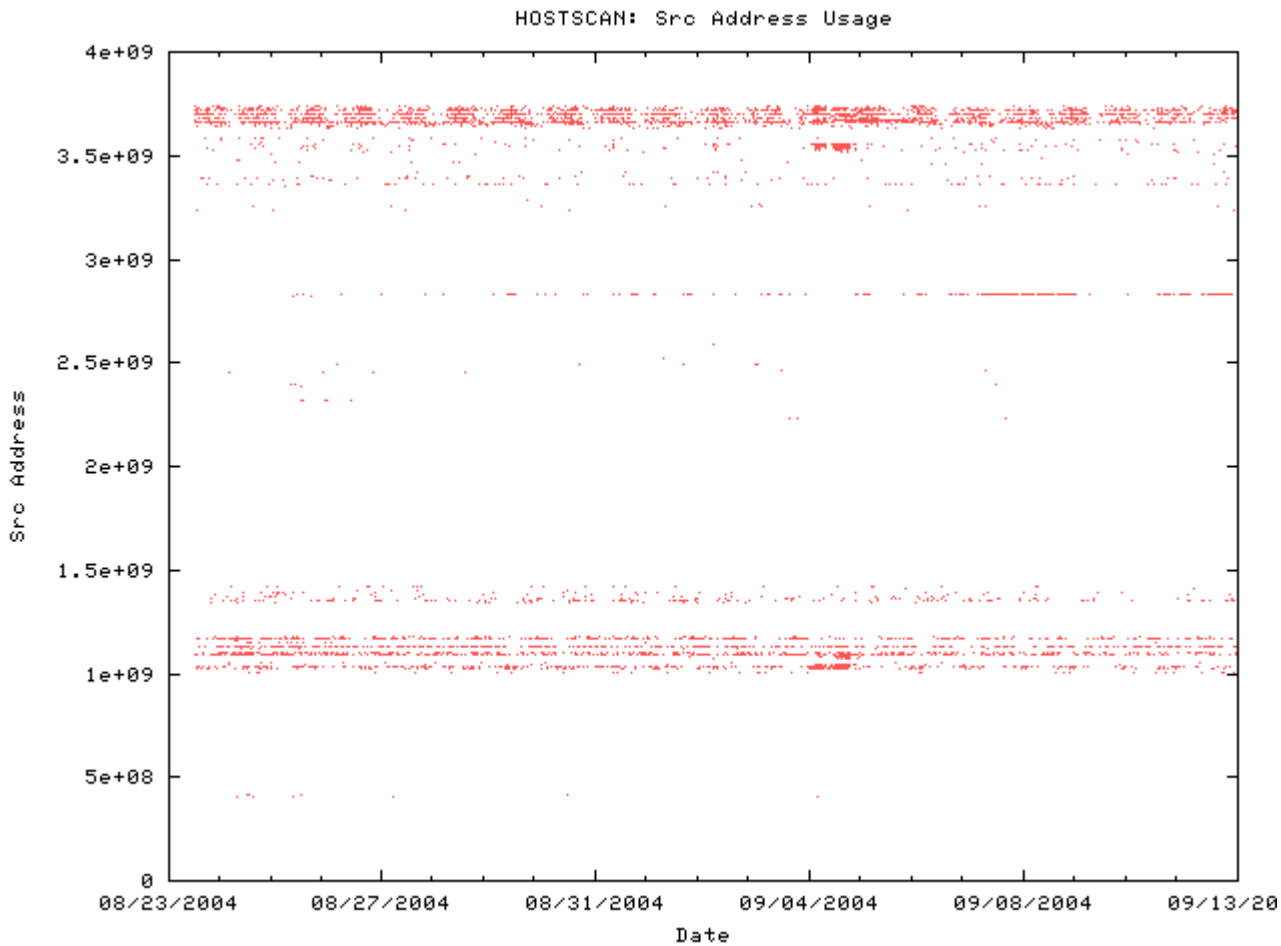
Src Addr toward port 1433



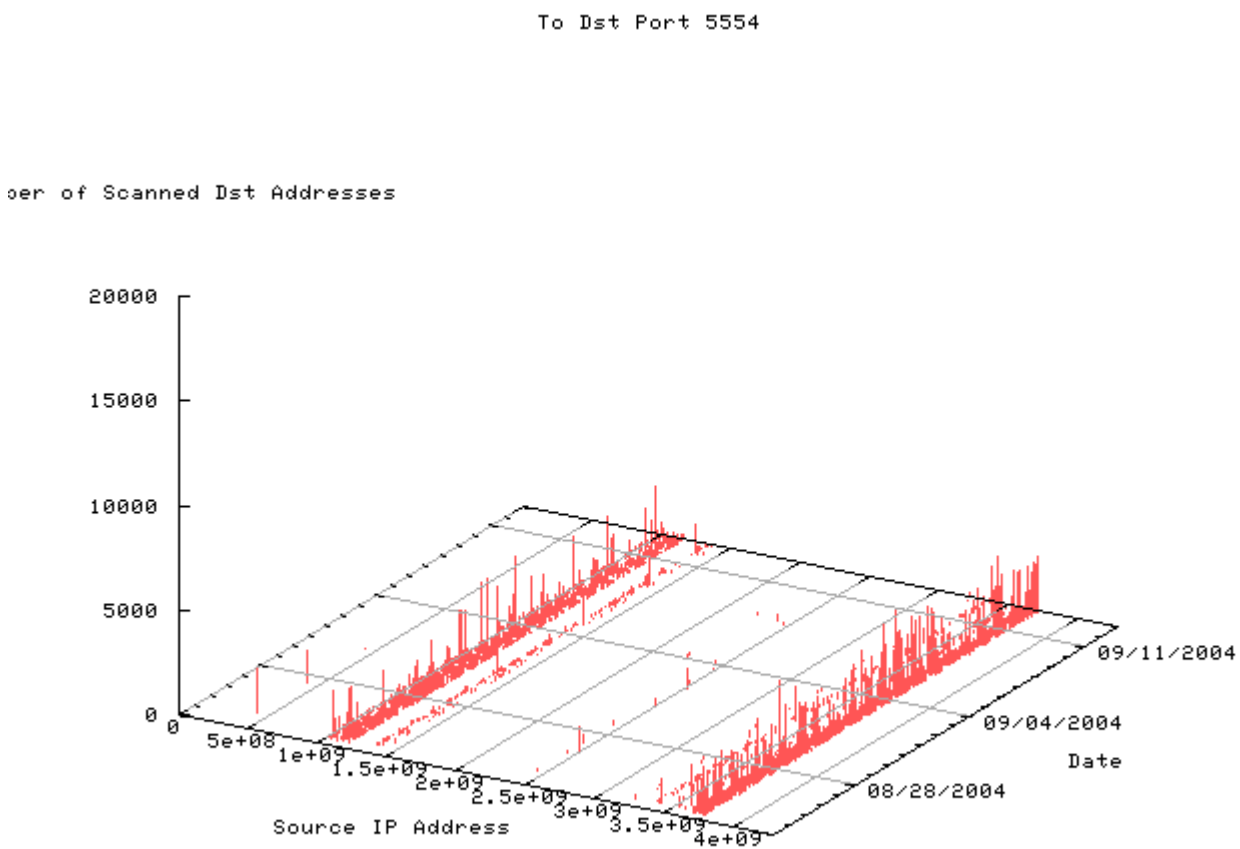
Port 5554


To Dst Port 5554
ber of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
09/11/2004
09/04/2004
08/28/2004
Date

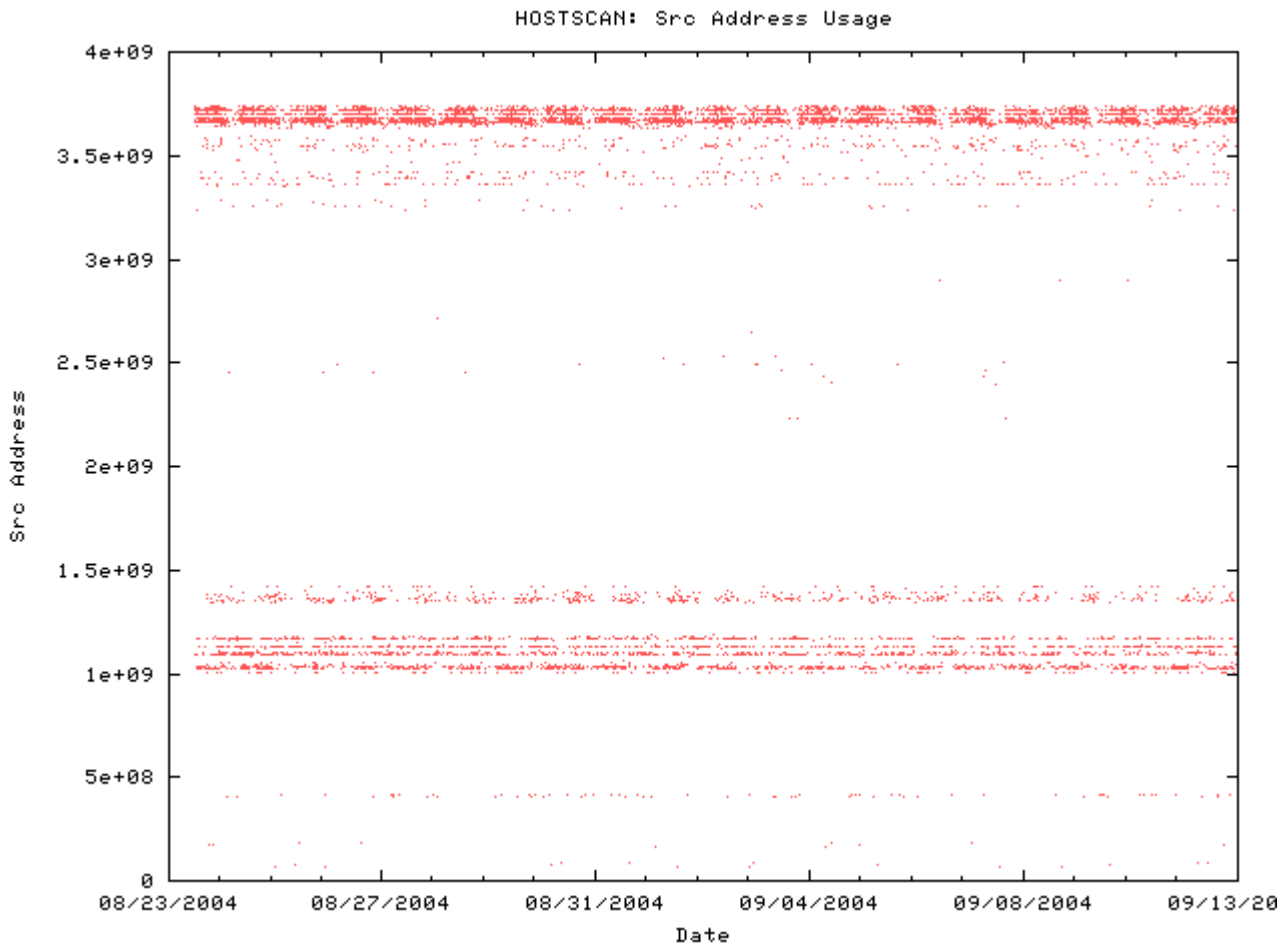
Src Addr toward port 5554



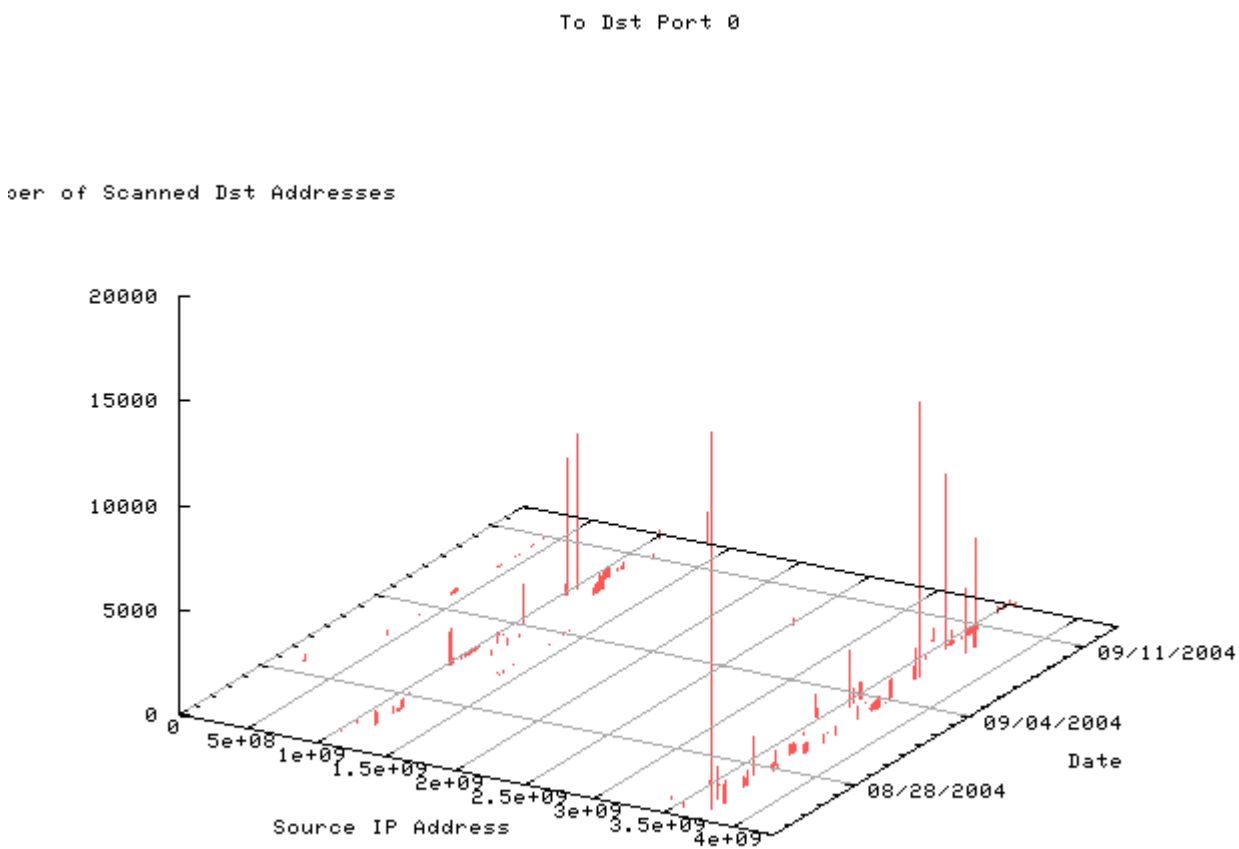
Port 9898


To Dst Port 5554
ber of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
09/11/2004
09/04/2004
08/28/2004
Date

Src Addr toward port 9898



ICMP


To Dst Port 0
ber of Scanned Dst Addresses
20000
15000
10000
5000
0
0
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
3.5e+09
4e+09
Source IP Address
09/11/2004
09/04/2004
08/28/2004
Date

Summary

- Network telescope
  - Useful for monitoring anomaly traffic
- CNU network telescope
  - ~/17 prefix
    - Network scanning traffic
- Issues
  - Large telescope
  - Distributed monitoring multiple telescopes
  - Sharing traffic data with large storage server

Reference

- D. Moore, C. Shannon, G. M. Voelker, and S. Savage, ''Network Telescopes," CAIDA technical report, 2004.
- nProbe, http://www.ntop.org/nProbe.html
- Caida, http://www.caida.org
- H. Kim, I. Kang, and S. Bahk, ''Real-time Visualization of Network Attacks on High-Speed Link," IEEE Network Magazine, vol. 18 no. 5, pp. 30-39, Sep./Nov. 2004.