Slammer Afterthought in Korea

Prepared for IEPG in Vienna, Austria

2003.7.13

Woohyong Choi
choi@bfbi.net

Agenda

- Korean Internet Infrastructure
  - Interconnections
  - DNS
  - Access
- Stats
  - Internet Exchange
  - International and Metro Links
  - DNS
- Observations and Follow-On Actions

Interconnections

- “IX”
  - Has unique meaning in Korea
  - Somewhat similar to “Tier-1” debate in other places
  - Started as private peering points between KT, Dacom and NCA in 95/96 timeframe; all three are sometimes called “KIX” which are actually domestic transit services
  - Many tried and still trying to own their own “IX”
- Internet Exchange
  - INET was left cold and went on to create IX-Seoul; others joined the effort and it’s now an independent neutral internet exchange called KINX; Korea Internet Neutral Exchange
  - A regional exchange in Busan and IPv6 exchange both of which operated by government through NCA
- Private Peerings
  - Major source of bandwidth among large providers like everywhere else

“IX” or “KIX”

Actually mean “domestic transit” to most people, providers usually use them to get connectivity to respective provider;
Three of them are widely recognized

- KIX/KIX-KT operated by Korea Telecom (AS4766)
  - Limiting service to competitors by refusing to carry customer routes
  - http://www.kix.net/ for general description (seems to be offline)
  - http://kix.net/ for looking glass
- DIX/KIX-Dacom operated by Dacom (AS3786)
  - Also has a layer-2 exchange (called L2IX)
  - http://www.bora.net/eng/products/ix_ind.html
  - http://looking-glass.bora.net/
- KIX/KIX-NCA operated by National Computerization Agency (AS3608)
  - Provide service to government funded networks, participates in KINX
  - http://www.kix.ne.kr/
- Others
  - Tying to claim “IX” status; Hanaro Telcom, Enterprise Networks, …

Internet Exchanges

- KINX – Korea Internet Neutral Exchange
  - http://www.kinx.net/
  - Started operation in 1999 as a consortium of 16 participating ISPs, incorporated in 2000
  - Major exchange point other than “IX”
- BIX – Busan IX
  - http://www.busanix.net/
  - First regional exchange; Limited to exchange of regional prefixes only; Funded and operated by government through NCA; a mixture of “IX” and internet exchange
- 6NGIX
  - http://www.ngix.ne.kr/
  - IPv6 only exchange operated by NCA; limited participants

Interconnection Summary

Almost all traffic exchanged in Seoul only

Public/Private Peering Links aggregated at a single PoP in each providers

DNS

- Authoritative servers
  - .kr primary server running 8.3.4 with 8bit patches
  - glue records for NS RR has very short TTL; 3600 or 7200
  - 8 out of 10 largest companies have lame servers
- Caching servers at most ISPs running a 8.3.3-based proprietary extension for localized keyword service
  - All queries with double-byte characters or unknown TLD return a single address for HTTP based redirection; sort of an alternate root
  - No access control for off-net DNS queries

Access

Most residential cable/dsl customers are guaranteed 2Mbps+ downstream bandwidth for US$15~30/month and

Upstream mileage varies but around 500Kbps on the average

There are around 11M+ such customers

- Population 46M+, Households 14M+
- Broadband penetration is over 75%

Stats

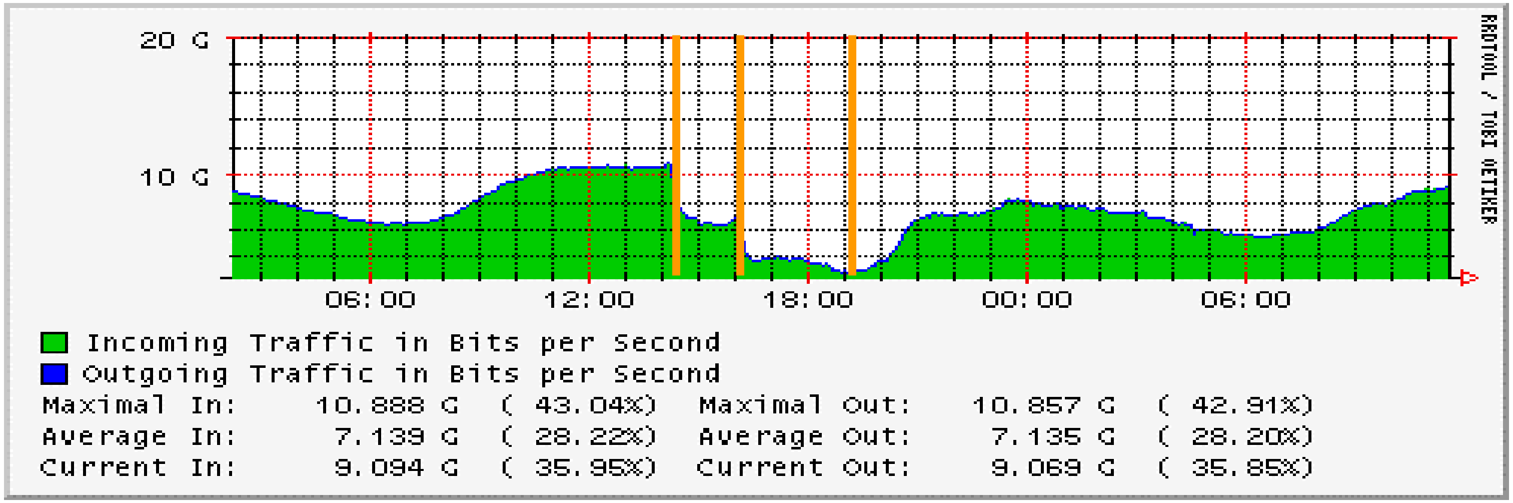
Exchange Traffic at KINX

Link stats at Service Providers

DNS stats

Exchange Traffic at KINX

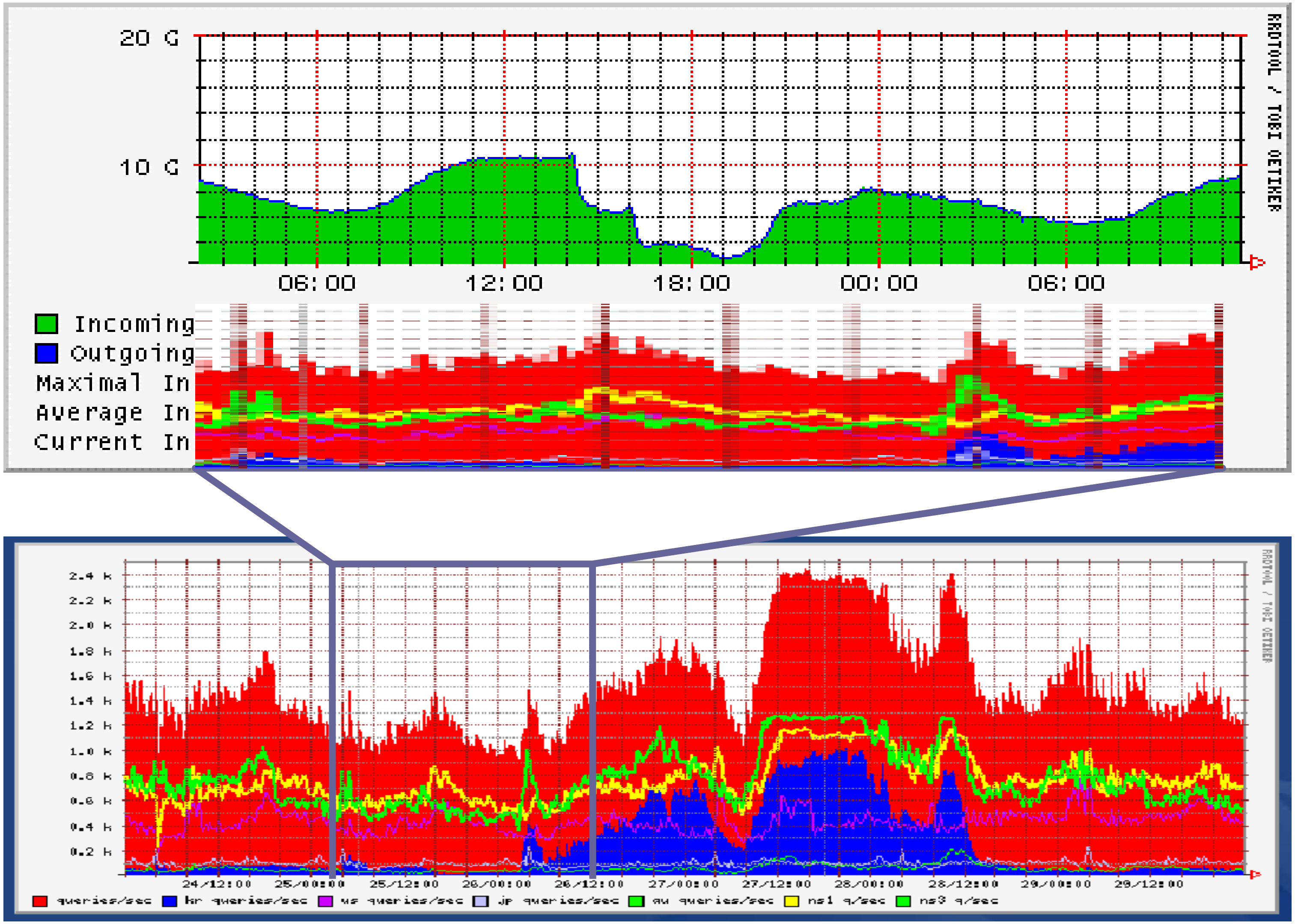
Seriously disrupted but the network actually seemed to work for sometime; Outbreak was around 14:30 KST (GMT+9)



🟩 Incoming Traffic in Bits per Second
🟦 Outgoing Traffic in Bits per Second

```
Maximal In:     10.888 G  ( 43.04%)  Maximal Out:    10.857 G  ( 42.91%)
Average In:      7.139 G  ( 28.22%)  Average Out:     7.135 G  ( 28.20%)
Current In:      9.094 G  ( 35.95%)  Current Out:     9.069 G  ( 35.85%)
```

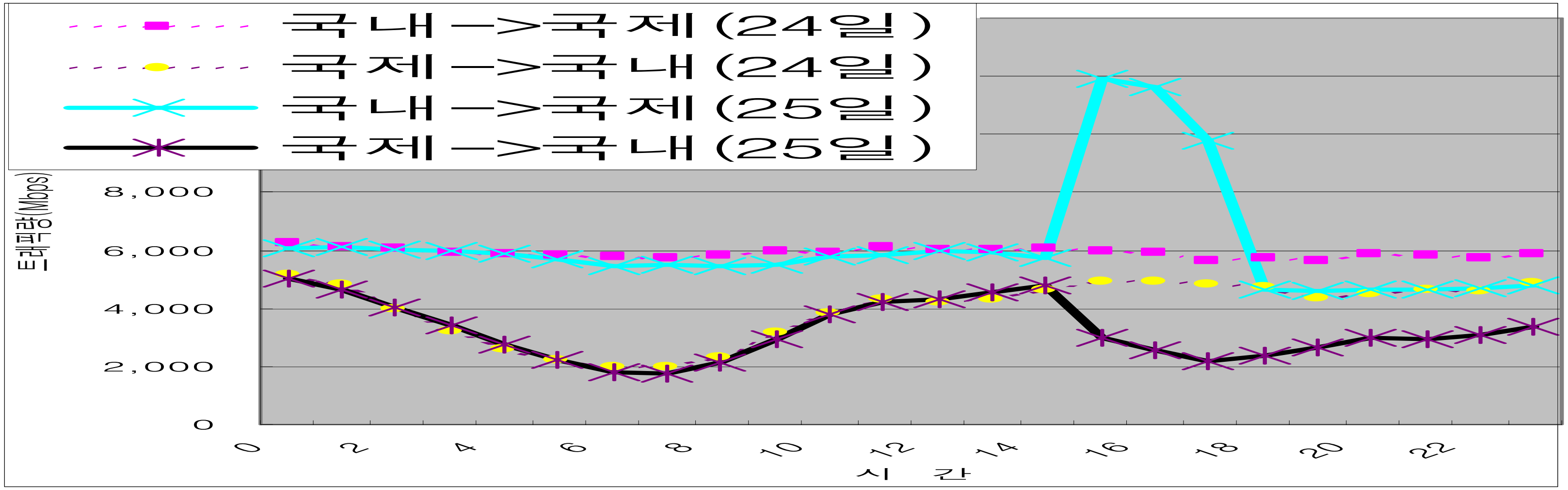
Comparing with APNIC Stat

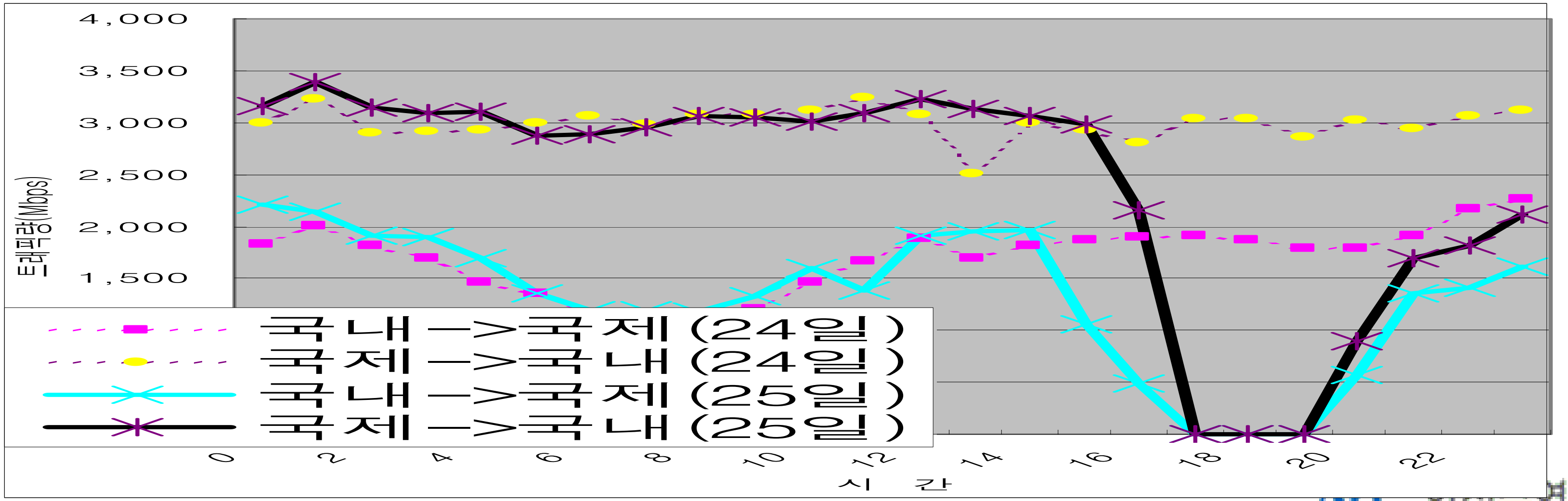


APNIC graph assumed to be in GMT+10

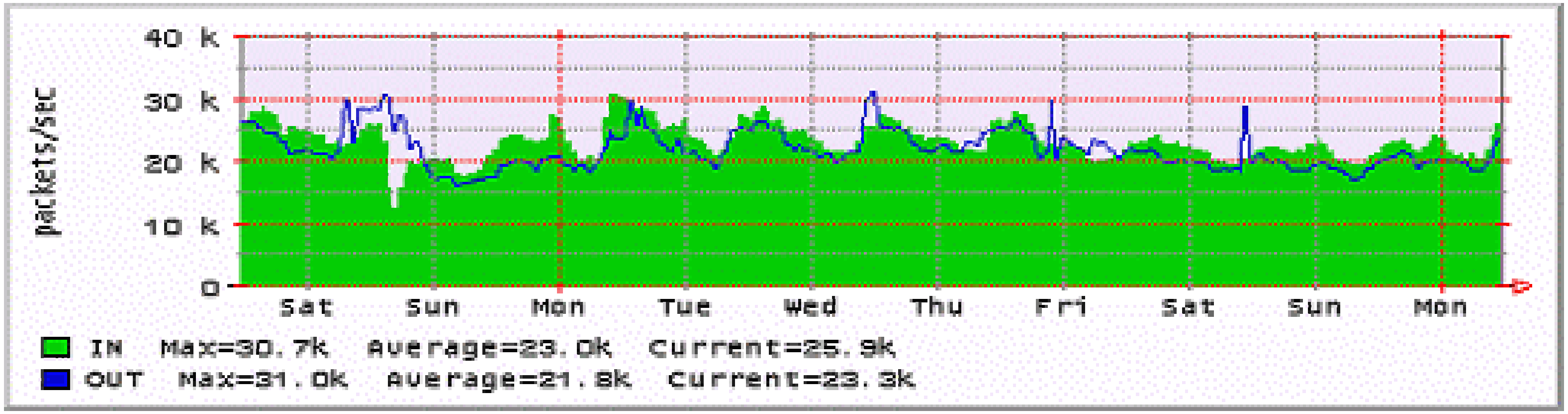
안철수연구소
www.ahnlab.com

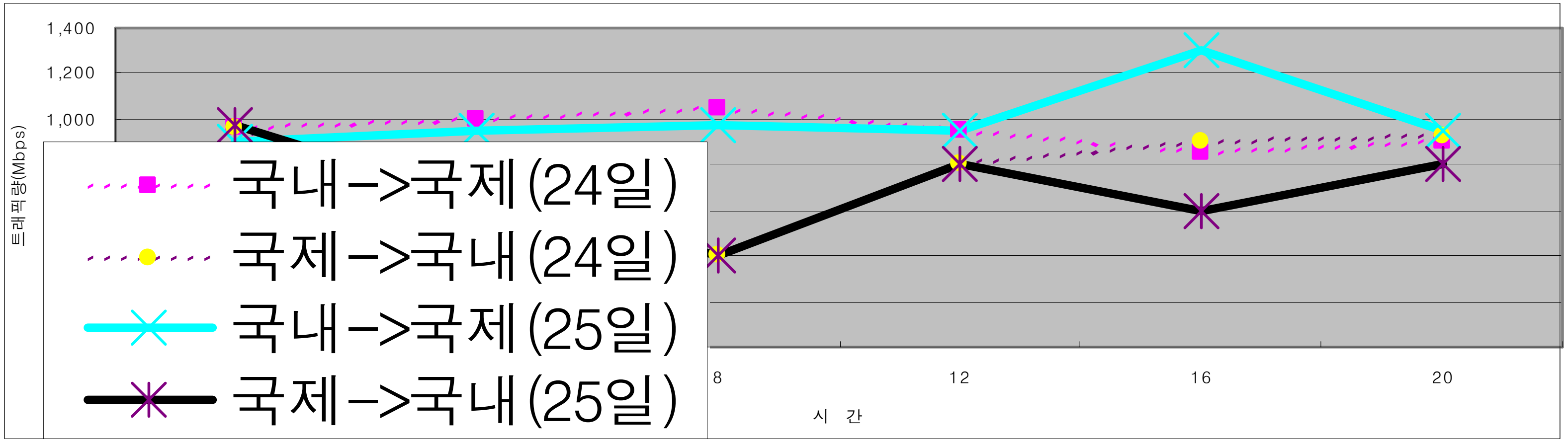
Int’l Links at Major Providers





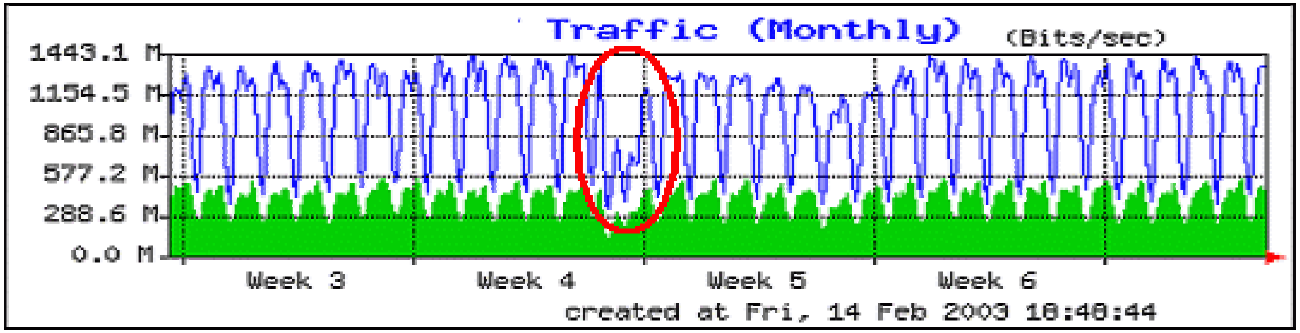
Int’l Links at Major Providers



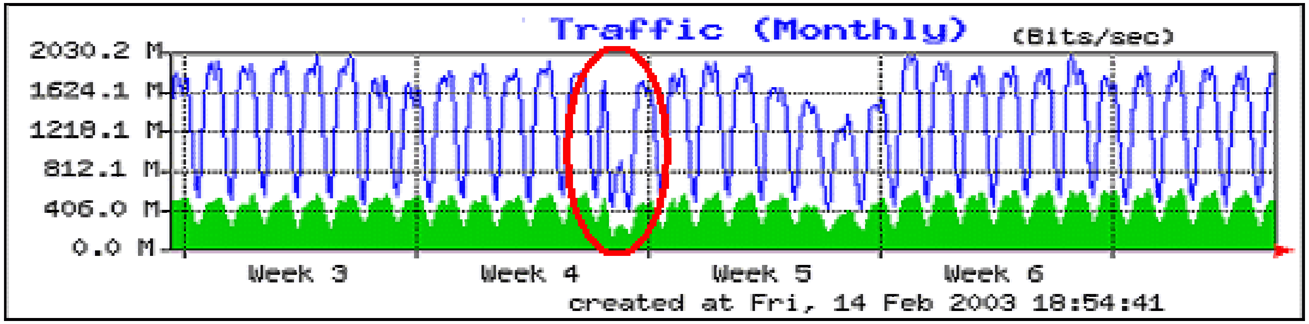


Metro Links of a Provider

Within Seoul



Inter-City



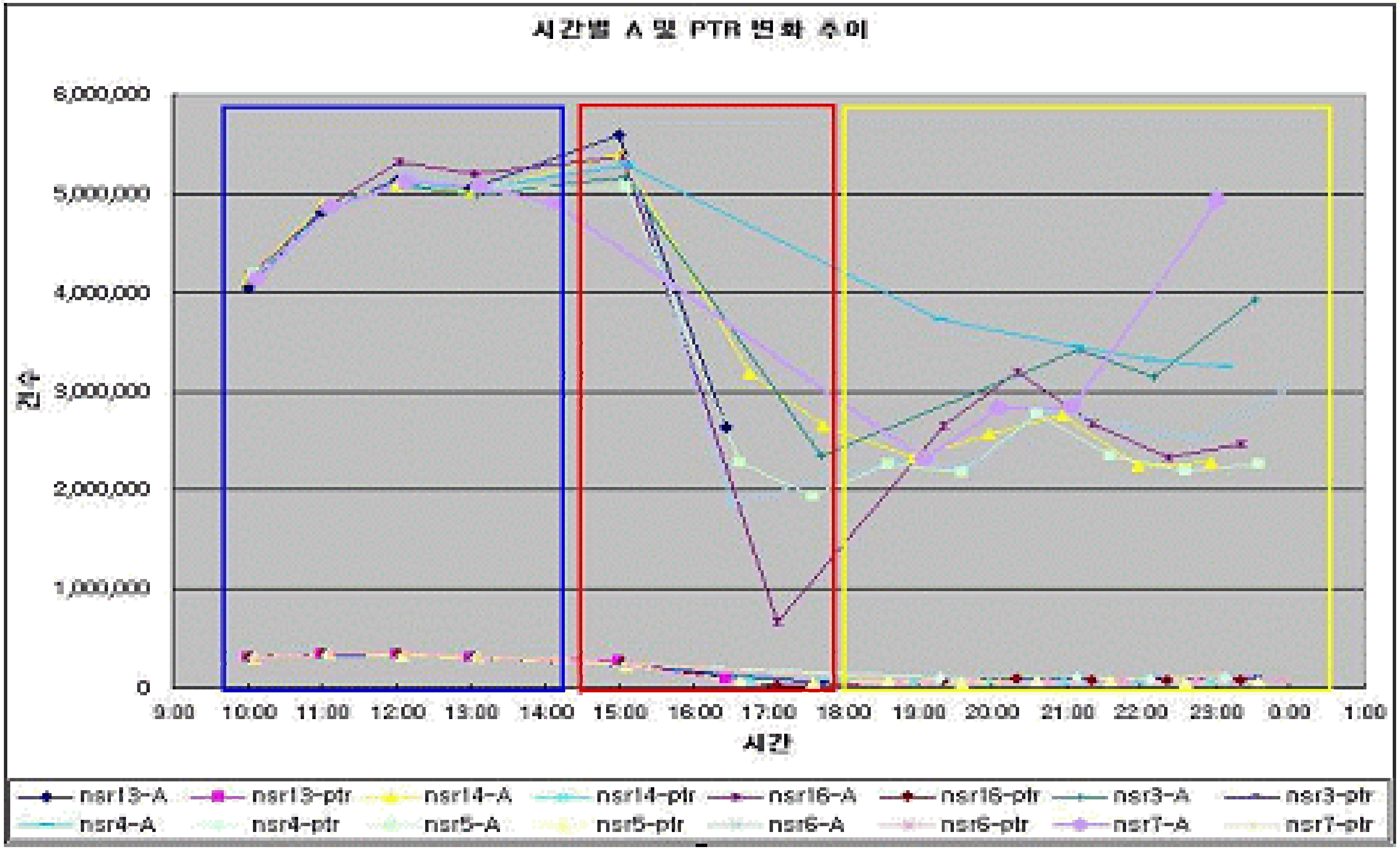
What the fuss about DNS?

Net so much essential to most Koreans; major disruption in the middle of a day leads to huge media coverage and panics

Korea Telecom (which account for more than half of all access customers) told the press they have issues with DNS which they believe is an activity of cyber-terrorism!

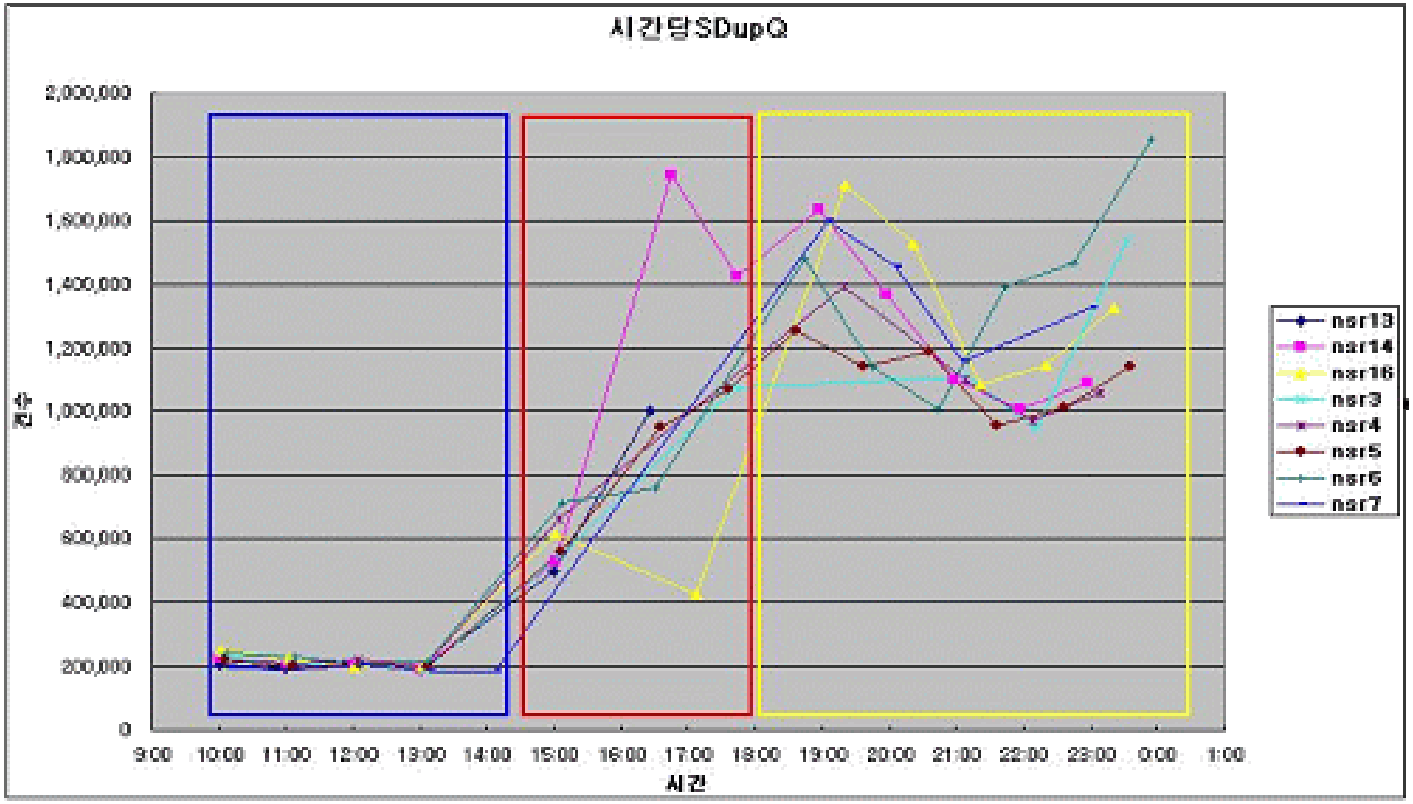
Ministry steps in, and it suddenly became all politics from then on

DNS: Queries


시간별 A 및 PTR 변화 추이
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
건수
9:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
0:00
1:00
시간
nsr13-A
nsr13-ptr
nsr14-A
nsr14-ptr
nsr16-A
nsr16-ptr
nsr3-A
nsr3-ptr
nsr4-A
nsr4-ptr
nsr5-A
nsr5-ptr
nsr6-A
nsr6-ptr
nsr7-A
nsr7-ptr

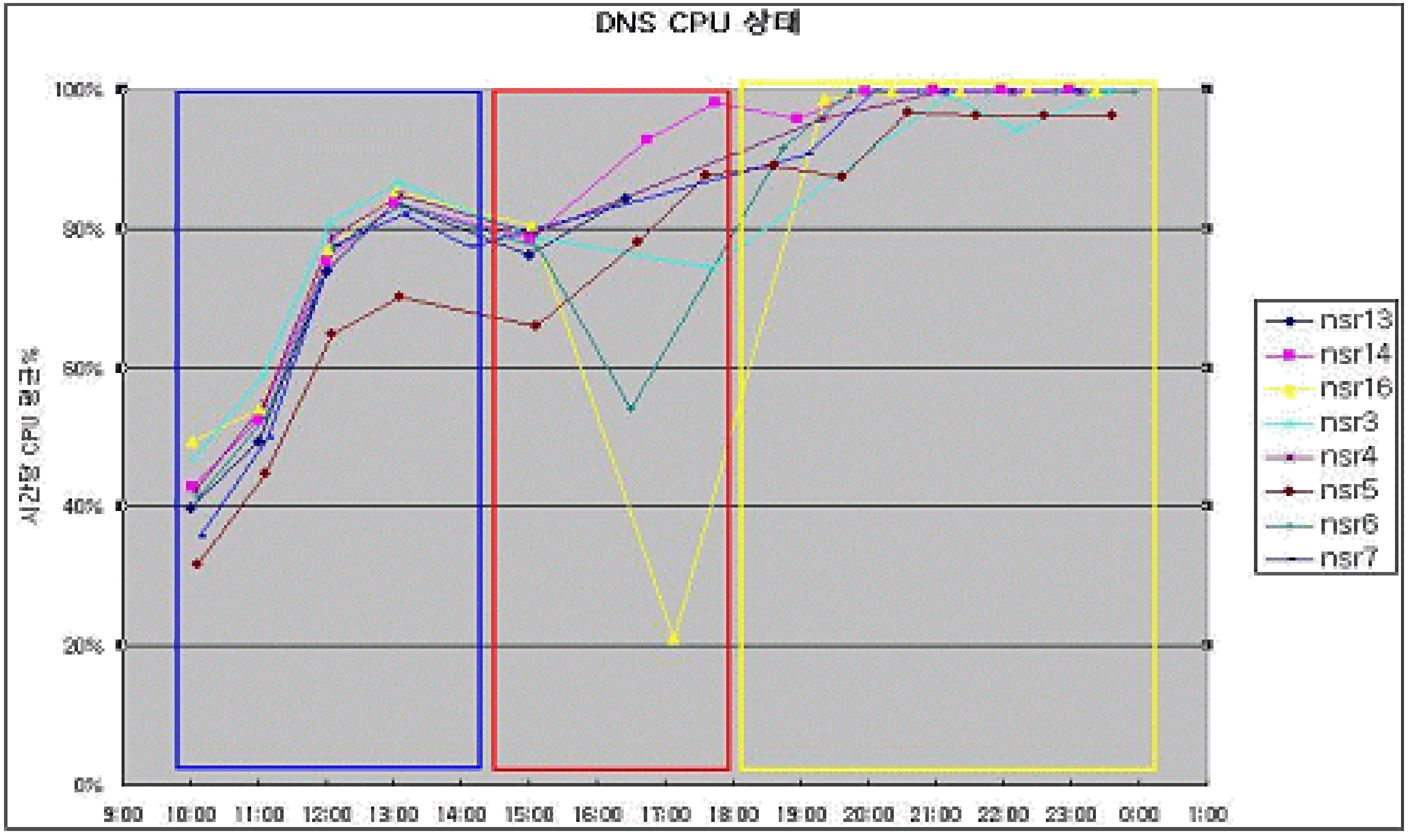
DNS: Retries

To which authoritative servers?



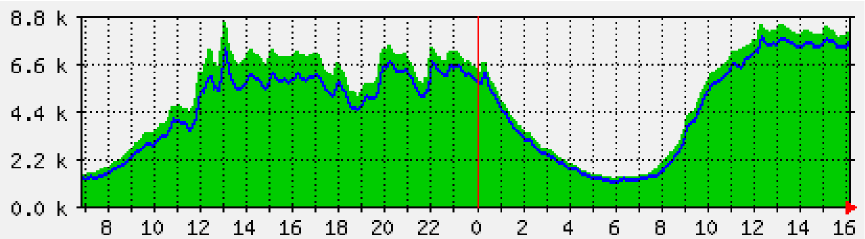
DNS: CPU Utilization

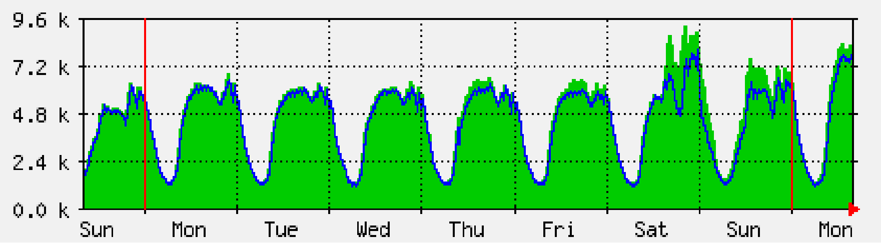
Must have been peaking at 100% before?



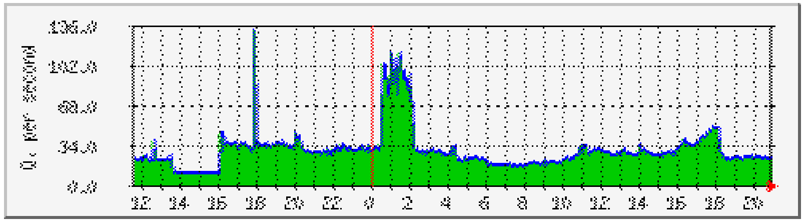
DNS Queries from Elsewhere

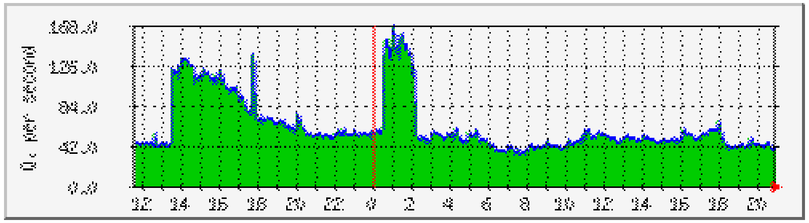
From another provider in Korea

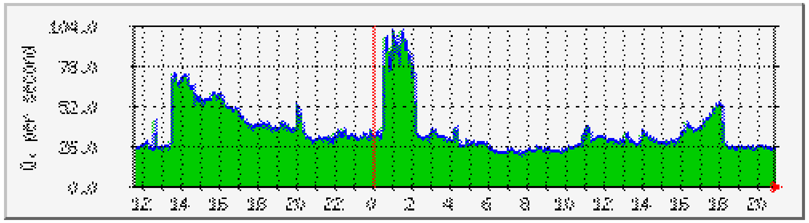


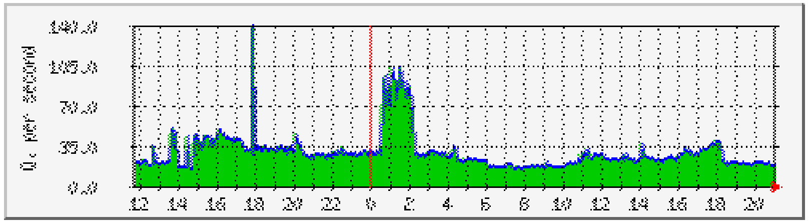


Taiwan CERT Slides from APRICOT









What Ministry’s Report Says

“Most of worm generated traffic was aggregated on the international link

Due to the fact, caching DNS servers had problems reaching root DNS servers

This generated huge amount of load to caching DNS servers making local services also unavailable”

Doesn’t sound very convincing to me ☹

More Observations

Most providers seemed to have installed filters within 3~4 hours max; blaming roots … wrong!

Some providers had syslogd setup to allow peers based on hostnames; generating lots of reverse lookups

Some providers didn’t seem to experience catastrophic disruption other than being slowed down

In certain cases, worm generated packets only destined to multicast addresses

What's Happening Thereafter

- Internet Engineering Community
  - Collapsed since late 90s, rebuilding seems to be so hard
- Industry
  - Providers hired some computer security experts and trying to upgrade their network monitoring systems
  - Great passion in hosting root/gtld mirrors
- Government
  - Various parties are competing to take the lead; all of which doesn't seem to have "networking" expertise
    - Ministry of Communication / Korea Information Security Agency
    - National Intelligence Service
    - Ministry of National Defense / Defense Security Command
- Legal
  - Class action is not permitted in Korea; very limited liabilities
  - Civil activism organizations have gathered plaintiffs and filed a suit; defendants are government, service providers, and Microsoft

Experiments in Monitoring

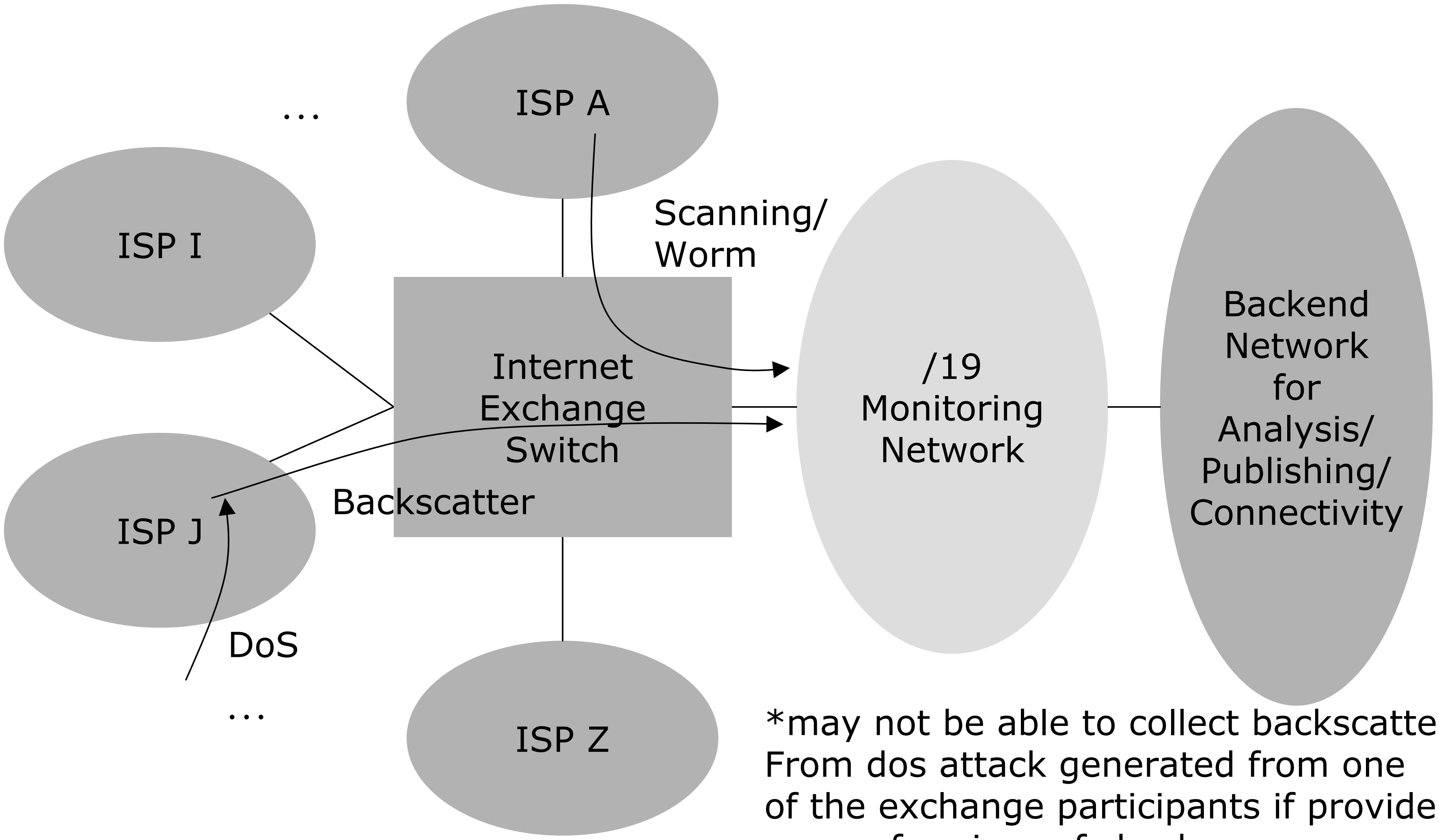
Goal is in building a monitor and a human network together

Setup a /19 honey-pot network to gather active scanning/worm and backscatters samples for trend analysis and posture monitoring

The network is placed at an exchange point

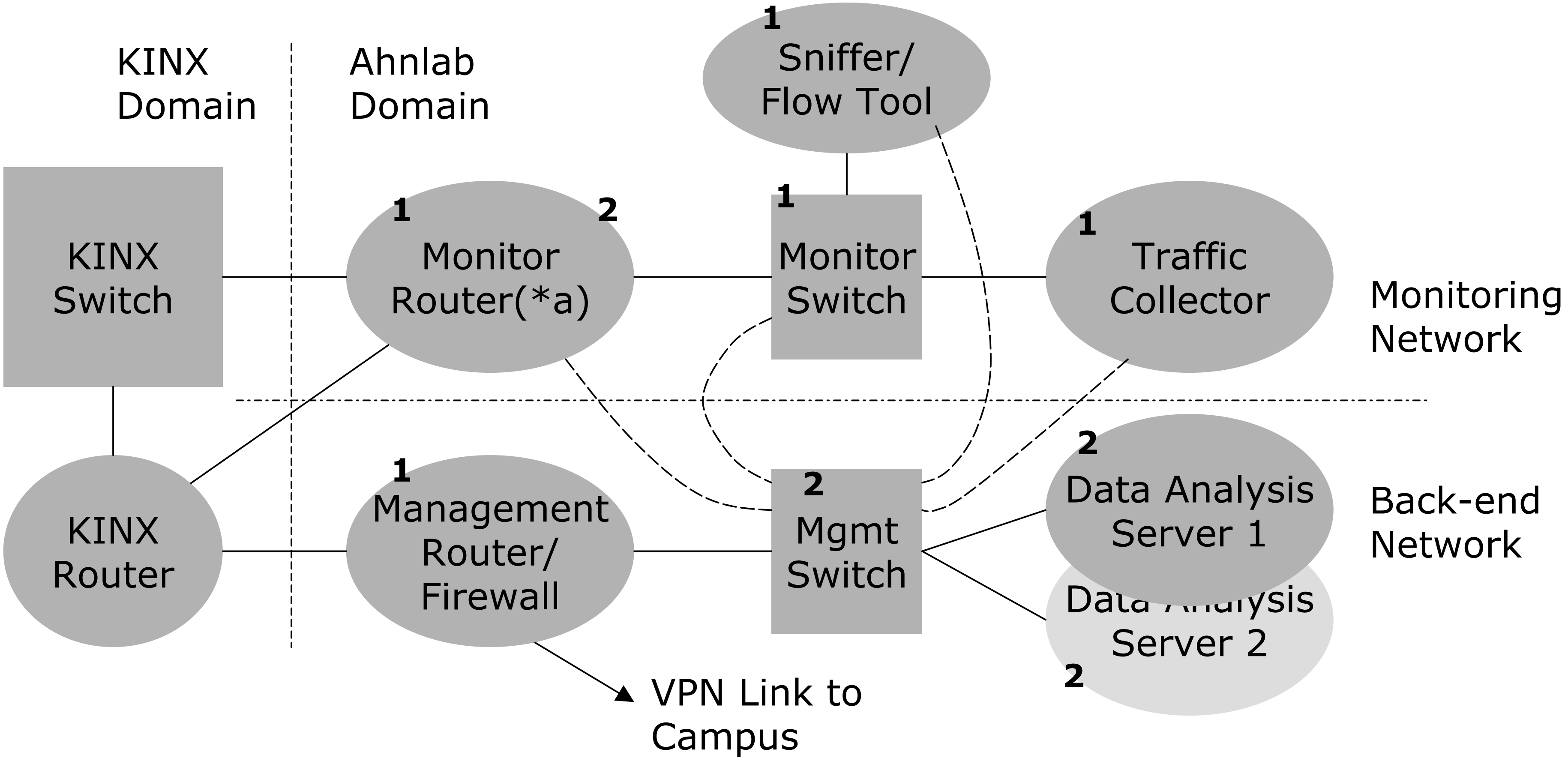
Sponsored by KINX, my employer and providers who peer with me

Monitoring Network



*may not be able to collect backscatter From dos attack generated from one of the exchange participants if providers are performing rpf check

How they are built?



Remarks: numbers denote priorities, (*a) Start with a PC router, then switch to a Cisco in the 2nd phase, all round objects in ahnlab domain are initially PCs, all square objects are layer 2 switches; all systems ntp synchronized

Expected Results

Statistics for

- Active Scans/Attacks from Spreading Worms
- Backscatter from DoS Attacks
- Route Stability

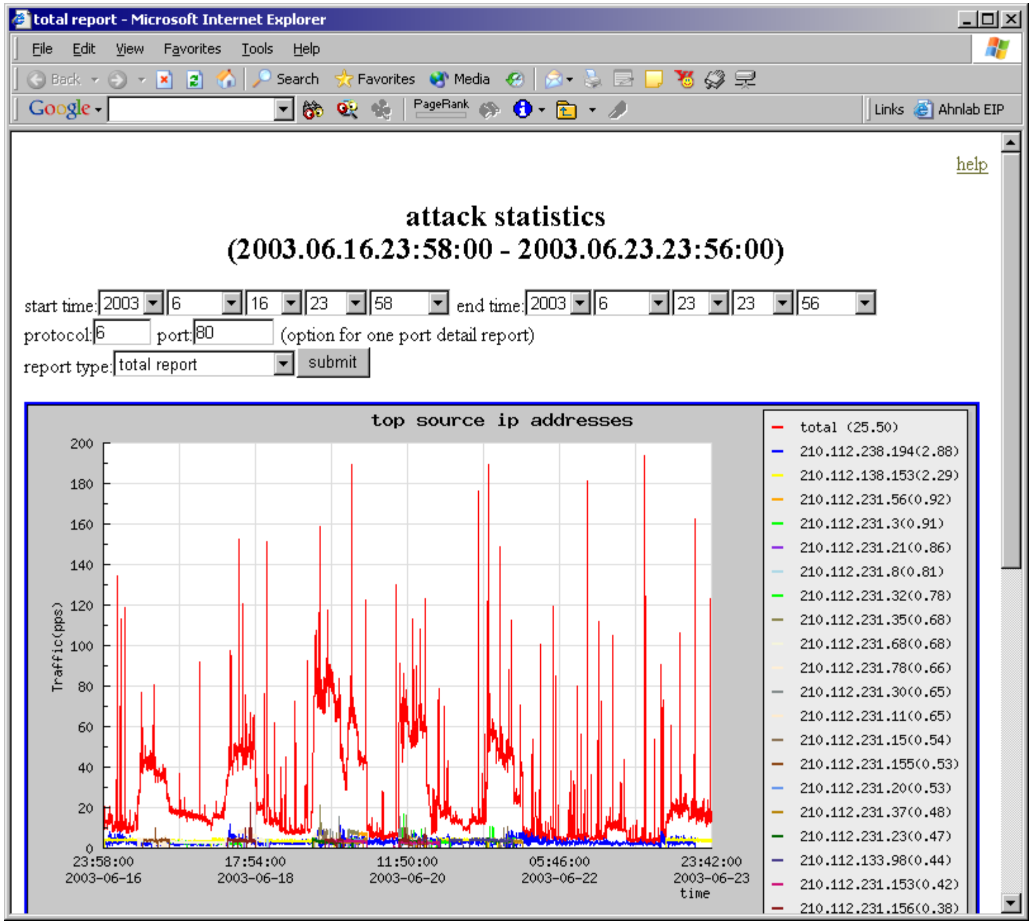
By

- Service Providers
- Origin Networks
- Attack Types
- Time Domain

Status

- Equipments installed in March
- Peering with 10 small/medium size providers
- Getting transit from one of the participants to get packets from largest providers
- Raw packets and summary records being archived
- User interface in development
  - Limited interface at http://kinx.bfbi.net/test/

Active Scanning

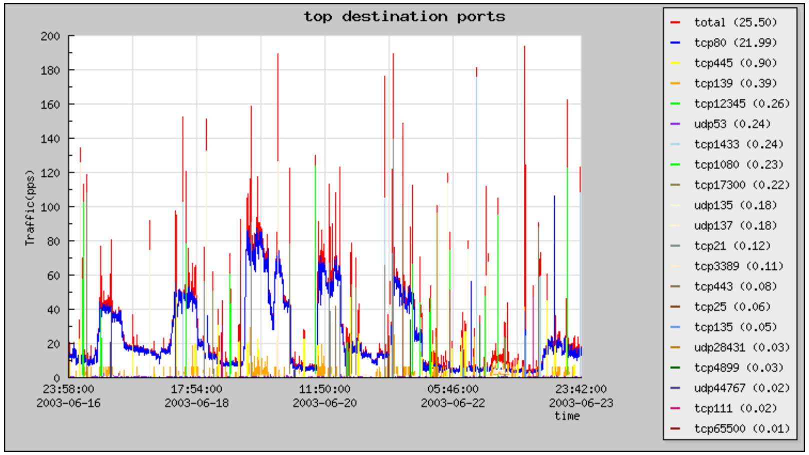


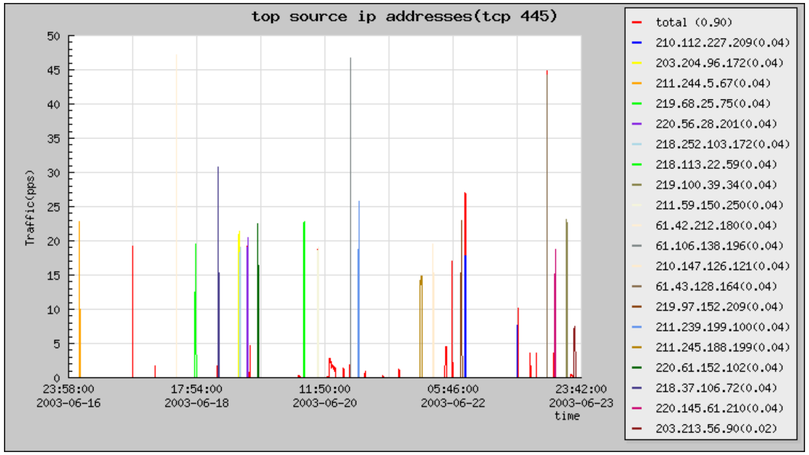
attack statistics
(2003.06.16.23:58:00 - 2003.06.23.23:56:00)

start time: 2003 | 6 | 16 | 23 | 58   end time: 2003 | 6 | 23 | 23 | 56

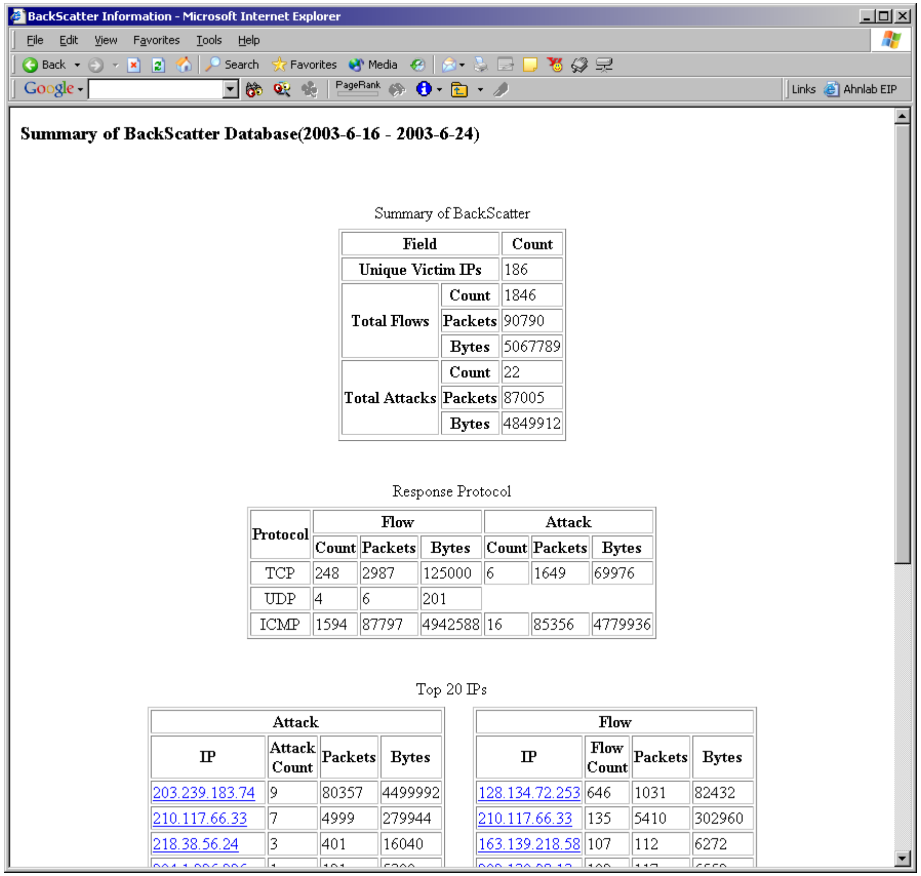
protocol: 6   port: 80   (option for one port detail report)

report type: total report   submit





Backscatter


File Edit View Favorites Tools Help
Back Search Favorites Media
Google PageRank
Links Ahnlab EIP

BackScatter Information - Microsoft Internet Explorer

Summary of BackScatter Database(2003-6-16 - 2003-6-24)

Summary of BackScatter

Field		Count
Unique Victim IPs		186
Total Flows	Count	1846
	Packets	90790
	Bytes	5067789
Total Attacks	Count	22
	Packets	87005
	Bytes	4849912

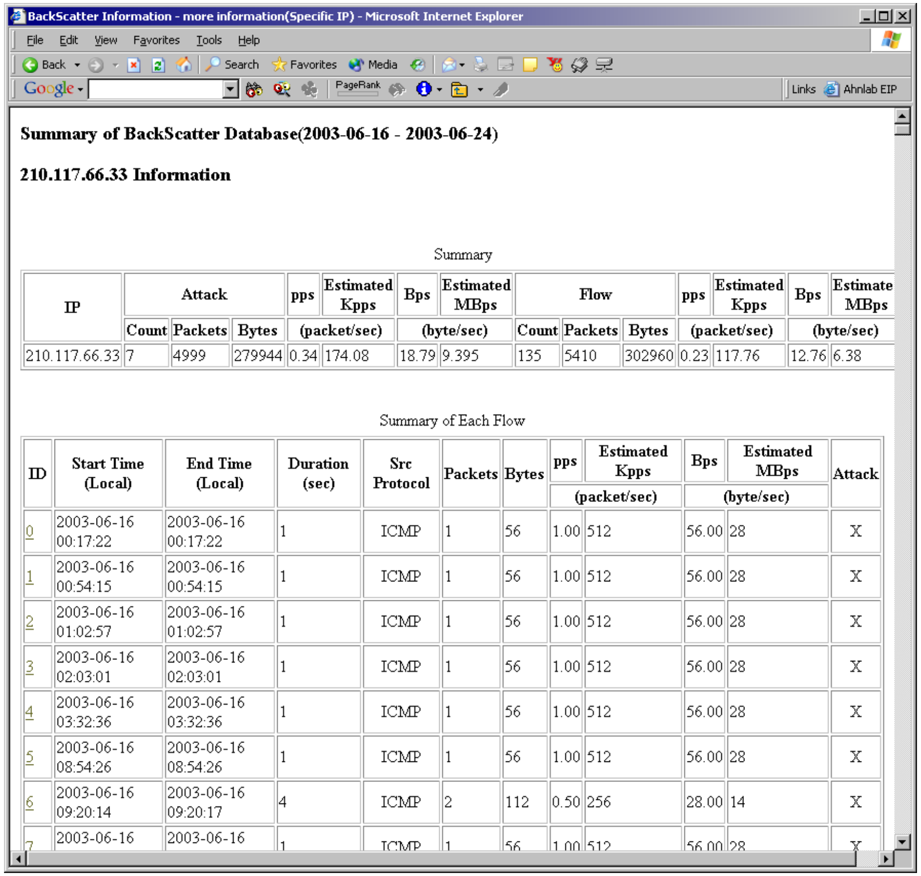
Response Protocol

Protocol	Flow			Attack		
	Count	Packets	Bytes	Count	Packets	Bytes
TCP	248	2987	125000	6	1649	69976
UDP	4	6	201			
ICMP	1594	87797	4942588	16	85356	4779936

Top 20 IPs

Attack			
IP	Attack Count	Packets	Bytes
203.239.183.74	9	80357	4499992
210.117.66.33	7	4999	279944
218.38.56.24	3	401	16040

Flow			
IP	Flow Count	Packets	Bytes
128.134.72.253	646	1031	82432
210.117.66.33	135	5410	302960
163.139.218.58	107	112	6272


File Edit View Favorites Tools Help
Back Search Favorites Media
Google PageRank
Links Ahnlab EIP

BackScatter Information - more information(Specific IP) - Microsoft Internet Explorer

Summary of BackScatter Database(2003-06-16 - 2003-06-24)

210.117.66.33 Information

Summary

IP	Attack			pps	Estimated Kpps	Bps	Estimated MBps	Flow			pps	Estimated Kpps	Bps	Estimate MBps
	Count	Packets	Bytes	(packet/sec)		(byte/sec)		Count	Packets	Bytes	(packet/sec)		(byte/sec)	
210.117.66.33	7	4999	279944	0.34	174.08	18.79	9.395	135	5410	302960	0.23	117.76	12.76	6.38

Summary of Each Flow

ID	Start Time (Local)	End Time (Local)	Duration (sec)	Src Protocol	Packets	Bytes	pps	Estimated Kpps	Bps	Estimated MBps	Attack
							(packet/sec)		(byte/sec)		
0	2003-06-16 00:17:22	2003-06-16 00:17:22	1	ICMP	1	56	1.00	512	56.00	28	X
1	2003-06-16 00:54:15	2003-06-16 00:54:15	1	ICMP	1	56	1.00	512	56.00	28	X
2	2003-06-16 01:02:57	2003-06-16 01:02:57	1	ICMP	1	56	1.00	512	56.00	28	X
3	2003-06-16 02:03:01	2003-06-16 02:03:01	1	ICMP	1	56	1.00	512	56.00	28	X
4	2003-06-16 03:32:36	2003-06-16 03:32:36	1	ICMP	1	56	1.00	512	56.00	28	X
5	2003-06-16 08:54:26	2003-06-16 08:54:26	1	ICMP	1	56	1.00	512	56.00	28	X
6	2003-06-16 09:20:14	2003-06-16 09:20:17	4	ICMP	2	112	0.50	256	28.00	14	X
7	2003-06-16	2003-06-16	1	ICMP	1	56	1.00	512	56.00	28	X

Remarks