Monitoring – Knowing your network

By Nic Maurel

Why Monitor your network

- Many machines perform 'business critical' functions
- Network administrators need to know when these systems are down– Or running degraded
- Knowing your network is important
- Establishing baselines to recognise abnormal behaviour (Imagine yourself as bb)

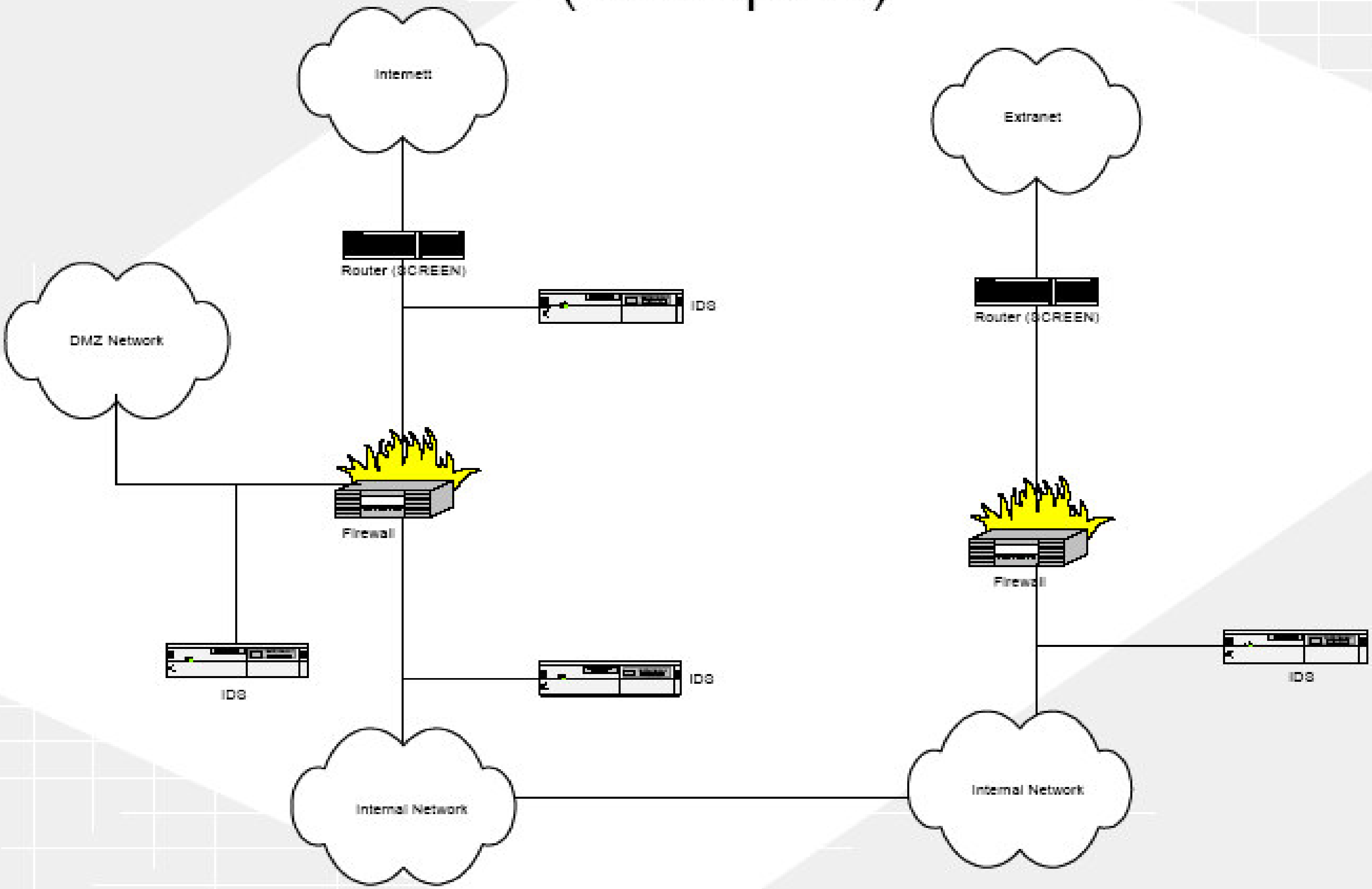
What can you do as a Network Administrator

- Combining tools helps to look at the network from different angles.
- Install an IDS – Monitor inside and outside of your network
- Monitoring software
- Install a central syslog server
- Customised scripts – for security and uptime purposes
- Graphing for Performance

What is an IDS?

- Intrusion detection system
- Network based IDS and Host based IDS
- Anomally Detection and Misuse based detection

IDS Placement (Conceptual)



Snort – www.snort.org

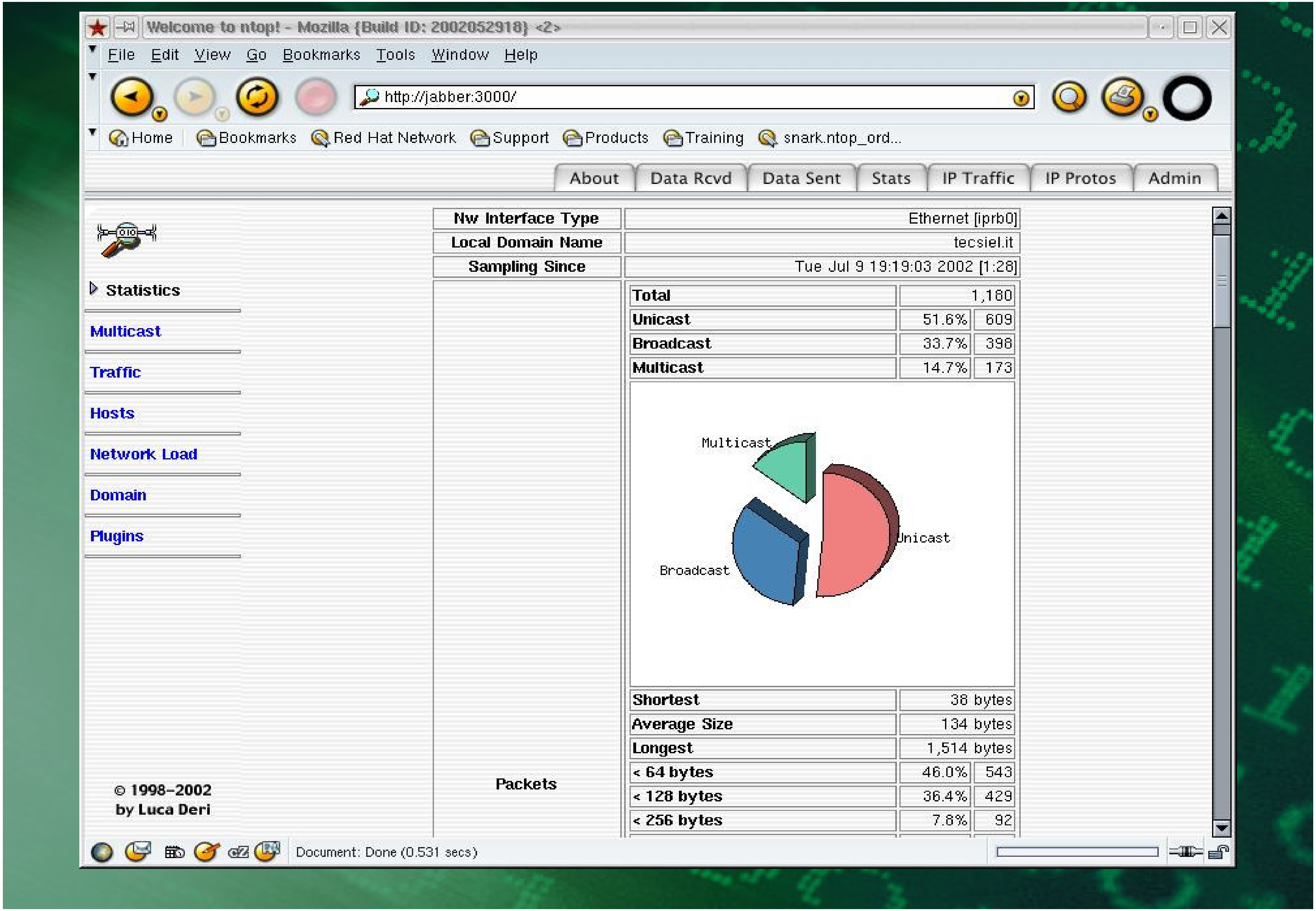
- OpenSource IDS – Windows and Linux
- Rules form “signatures”
- Anomalous activity detection is possible
  - stealth scans, OS fingerprinting, invalid ICMP codes, etc
- Rules system is very flexible, and creation of new rules is relatively simple

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 any (flags: SF; msg: “SYN-FIN Scan”;)
```

- Well integrated in community – Airsnort, snort-inline, snortsam

Ntop – www.ntop.org

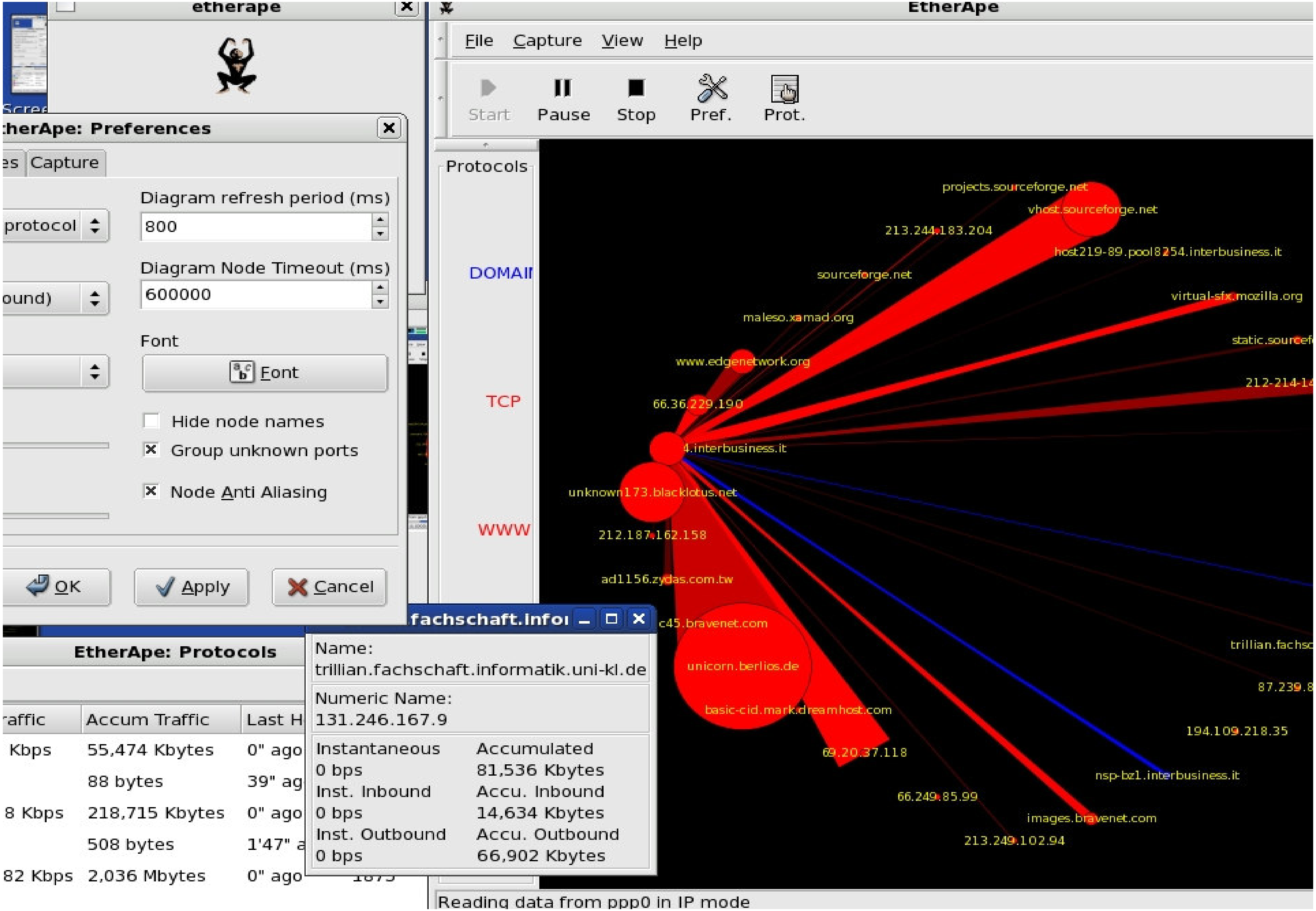
- Bandwidth Utilization
- Great for picking up realtime or historical trends
- Drill down Per Protocol – per session – per Host (passive detection)
- Web based interface – http or https
- Can Monitor Netflow Sflow and pcap hosts simultaneously
- Useful Graphs and pie charts



Nw Interface Type	Ethernet [iprb0]		
Local Domain Name	tecsiel.it		
Sampling Since	Tue Jul 9 19:19:03 2002 [1:28]		
Packets	Total	1,180	
	Unicast	51.6%	609
	Broadcast	33.7%	398
	Multicast	14.7%	173
	Shortest	38 bytes	
	Average Size	134 bytes	
	Longest	1,514 bytes	
	< 64 bytes	46.0%	543
	< 128 bytes	36.4%	429
	< 256 bytes	7.8%	92

Etherape – www.etherape.sourceforge.net

- Graphical representation
- Realtime statistics
- Can read
- Useful for actively monitoring network
- Only on Linux



therApe: Preferences

es | Capture

protocol

ound)

Diagram refresh period (ms): 800

Diagram Node Timeout (ms): 600000

Font: Font

□ Hide node names

☒ Group unknown ports

☒ Node Anti Aliasing

fachschaft.info

Name:
trillian.fachschaft.informatik.uni-kl.de

Numeric Name:
131.246.167.9

Instantaneous	Accumulated
0 bps	81,536 Kbytes
Inst. Inbound	Accu. Inbound
0 bps	14,634 Kbytes
Inst. Outbound	Accu. Outbound
0 bps	66,902 Kbytes

EtherApe: Protocols

raffic	Accum Traffic	Last H
Kbps	55,474 Kbytes	0" ago
	88 bytes	39" ag
8 Kbps	218,715 Kbytes	0" ago
	508 bytes	1'47" a
82 Kbps	2,036 Mbytes	0" ago

Reading data from ppp0 in IP mode

Awstats

http://awstats.sourceforge.net

- Web, ftp or mail server statistics graphically.
- Relatively easy to use
- Can do stats off IIS
- Has dependancies – perl and Apache
- Only linux

Syslog Server – shipped with OS

- Industry standard Centrally deployable
- Can encrypt the logs between servers
- Troubleshooting, Serve as early warnings and useful in reconstructing events
- Cisco logging by default ,Plugins for Windows – kiwi syslog daemon or Eventlog to Syslog Utility
- Configure log alert – logwatch,Tripwire, Swatch ect.

Scripts – using shell shipped with OS

- **Requires good technical knowledge**
- **Nmap :**

```
nmap –sP 192.168.1.0/24
nmap –sS -sV –O 192.168.1.1
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2006-02-08 10:14 SAST
Interesting ports on 192.168.4.65:
(The 1652 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 3.6.1p2 (protocol 1.99)
80/tcp   open  http        Apache httpd 2.0.55 ((Unix) PHP/4.3.10)
111/tcp  open  rpcbind     2 (rpc #100000)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.5.25 - 2.5.70 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 22.035 days (since Tue Jan 17 09:24:32 2006)

Nmap run completed -- 1 IP address (1 host up) scanned in 15.633 seconds
```

- **Netcat :**

```
Get.txt = GET / HTTP/1.1
nc –v www.google.co.za < get.txt > get.html
Connection to www.google.com 80 port [tcp/http] succeeded!
```

or

```
nc –v –z www.google.co.za 80
```

- **Tcpdump**

```
tcpdump –i eth0 “src 192.168.1.1 AND port 80”
```

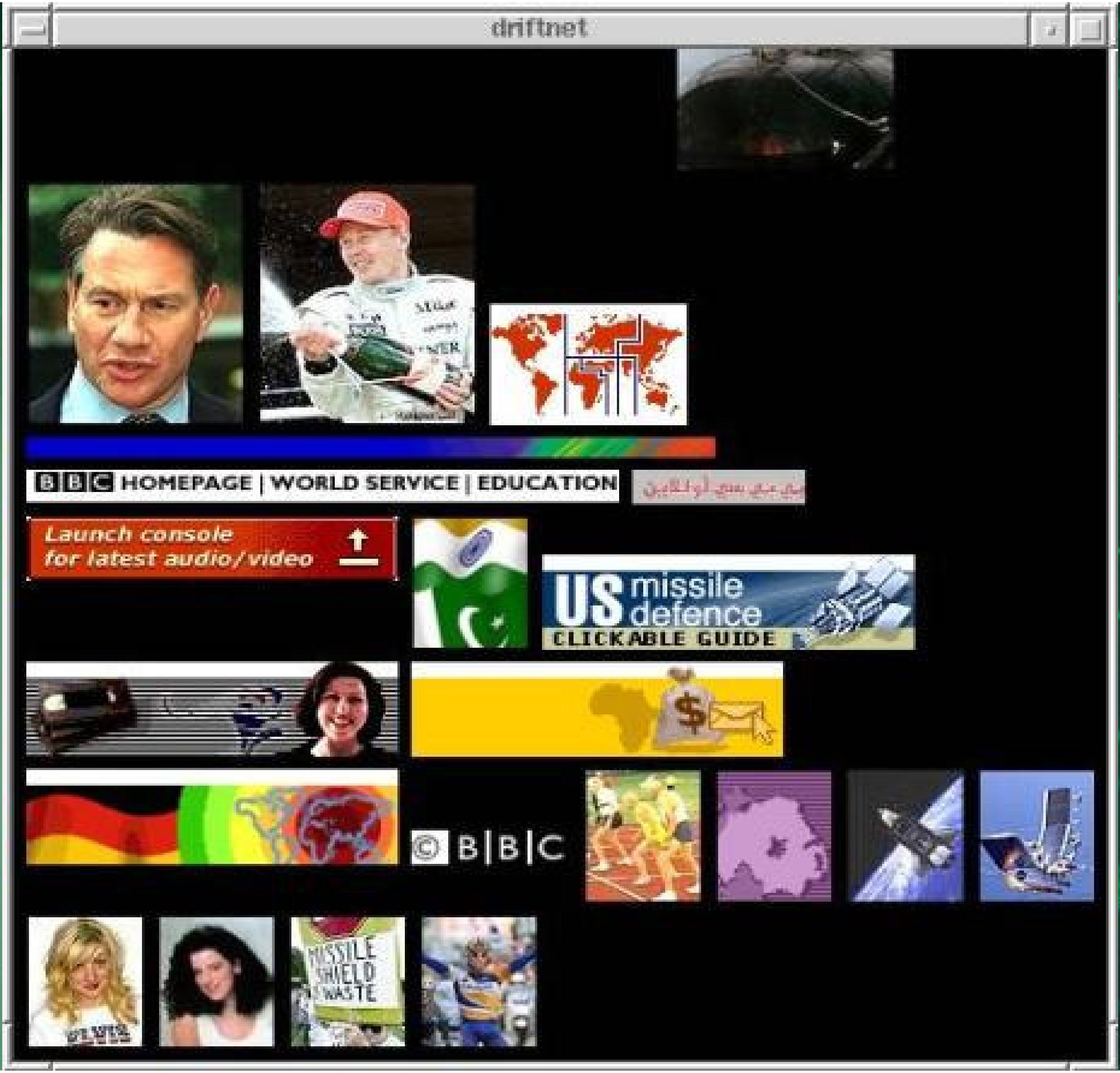
- **Ping**

Graphing

- MRTG
- **The first, open-source, easy to use performance monitoring tool**
- **Limitations : file oriented data storage, graphics continually generated and stored, unique graphic representation**
- RRDtool
- **Logging & Graphing**
- **Database oriented storage and on-demand enhanced graphics production. Include also a poller.**
- Cacti
- **A Web portal for monitoring, include RRDtool,and everything else**

Tools Worth Mentioning

- Driftnet – Picture Sniffer
- Honeyd - Honeypot
- Ethereal – Packet Sniffer
- Sarg – Squid Analysis Report Generator


driftnet
BBC HOMEPAGE | WORLD SERVICE | EDUCATION
بي بي سي أونلاين
Launch console
for latest audio/video
US missile defence
CLICKABLE GUIDE
© BBC
MISSILE SHIELD WASTE

Challenges Facing Monitoring

- Knowing what normal activity is crucial
- Gigabit networks will become increasing difficult to monitor because of the speed.
- Encrypted protocols
- Planning failure recovery strategies
- Zero Day attacks