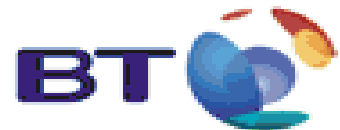


Traffic Analysis with Netflow (the short version)

Dave Burke, BT Ireland
IEnog Meeting 29/06/05



Scope of presentation

- Only covering Cisco Equipment
- Only 12.0S for this talk
- Flow-tools (<http://www.splintered.net/sw/flow-tools/>)
- Flowscan (<http://dave.plonka.us/FlowScan/>)

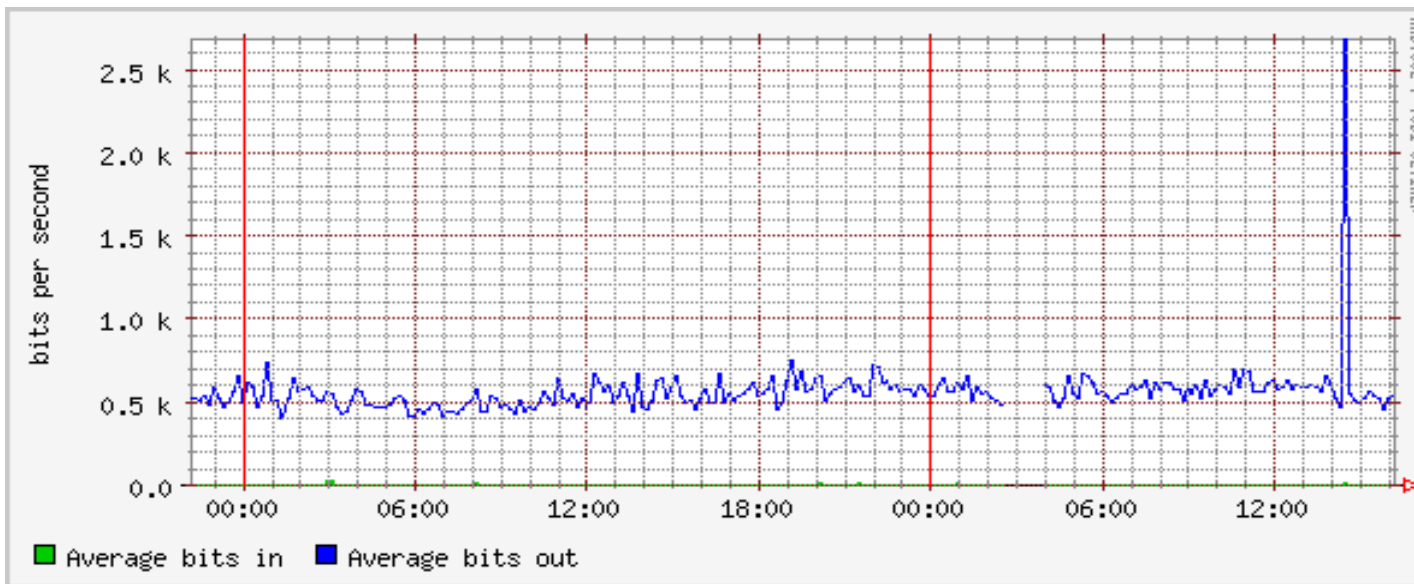
What is netflow ?

- From cisco.com "A flow is a unidirectional set of packets that arrive at the router on the same subinterface, have the same source and destination IP addresses, Layer 4 protocol, TCP/UDP source and destination ports, and the same ToS (type of service) byte in the IP headers"

Why Bother?

- Historical record of what happened on your network
- Independent record of traffic into and out of the network
- Traffic Accounting

Netflow records can help to explain unusual traffic patterns



Turning on netflow

```
core01.lab(config)#ip flow-export source loopback 0
```

```
core01.lab(config)#ip flow-export version 5 origin-as
```

```
core01.lab(config)#ip flow-export destination 192.168.1.25  
2055
```

```
core01.lab(config)#ip flow-sampling-mode packet-interval  
100
```

```
core01.lab(config)#int fa 0/0
```

```
core01.lab(config-if)#ip route-cache flow sampled
```

Accepting the exported flow traffic

- With Deb/Sarge:
 - apt-get install flow-tools
 - edit /etc/flow-tools/flow-capture.conf
 - Sample line:
 - -w /usr/local/netflow/flows 0/0/2055 -V5 -E10G -N 3
- With FreeBSD:
 - cd /usr/ports/net-mgmt/flow-tools && make install

Using flow-tools

```
daveb@netflow01:2005-06-29$ flow-cat ft-v05.2005-06-29.150617+0100 |  
flow-print -f 5 | grep 193.95.134
```

Start	End	Sif	SrcIPaddress	SrcP	Dif	DstIPaddress	DstP	P	F1	Pkts
15:01:51	15:02:02	5	81.178.117.23	6881	1	193.95.134.83	2205	6		
0	2	80								
15:01:35	15:02:02	672	62.21.105.239	6881	1	193.95.134.83	3383			
6	0	4	195							
15:01:18	15:02:13	5	82.82.201.138	6881	1	193.95.134.83	2971	6		
0	7	306								

Sample Traffic ACL

```
daveb@netflow01:~$ cat flow.acl  
ip access-list standard badguy permit 10.0.0.0 0.0.0.255  
ip access-list standard badguy permit 192.168.0.0 0.0.255.255  
ip access-list standard badguy permit 172.16.0.0 0.0.224.255
```

Output of 'badguy'

```
daveb@netflow01:~$ flow-cat * | flow-filter -f ~/flow.acl -S badguy | flow-print -f  
5
```

Start	End	Sif	SrcIPaddress	SrcP	Dif	DstIPaddress	DstP	P	Fl	Pkts	
23:54:55	23:54:55	5	192.168.1.10	0	0	194.125.x.231	0	6	4	1	40
23:56:03	23:56:03	5	192.168.0.210	3783	0	192.x.21.36	139	6	4	1	40
23:56:03	23:56:03	5	192.168.0.210	3791	0	192.x.21.36	139	6	4	1	40

Matching 2 or more fields

- For this we use flow-filter...

```
filter-primitive portirc
```

```
    type ip-port
```

```
    permit 6667
```

```
filter-primitive pagh.compsoc.com
```

```
    type ip-address
```

```
    permit 193.120.123.132
```

```
filter-definition irc-and-pagh
```

```
    match ip-destination-address pagh.compsoc.com
```

```
    match ip-source-port portirc
```

Show me all traffic from ASN#

```
daveb@analyse02:2005-06-23$ flow-cat * | flow-filter -a 109 | flow-print -f 5
```

Start	End	Sif	SrcIPaddress	SrcP	Dif	DstIPaddress	DstP	P
Fl Pkts	Octets							
00:04:54 1500	00:04:54	2	198.133.219.25	80	3	194.165.180.x	1298	6 0 1
00:05:10 1472	00:05:10	2	198.133.219.25	80	3	194.165.180.x	1302	6 0 1

Output of flow-nfilter

```
daveb@analyse02:2005-06-11$ flow-cat * | flow-nfilter -f ~/nflow.acl -F  
irc-and-pagh | flow-print -f 5
```

Start	End	Sif	SrcIPaddress	SrcP	DIf	DstIPaddress	
DstP	P	Fl	Pkts	Octets			
05:48:38	05:48:38	12	193.1.31.98	6667	2	193.120.123.132	49141 6
0	1	114					

I can't show my manager that!

- Managers don't want to see raw data, so need to present it nicely for them.
 - Flowscan comes in handy here.
 - Uses's rrd for dynamic graphs
 - Gives the top talkers every 5 minutes

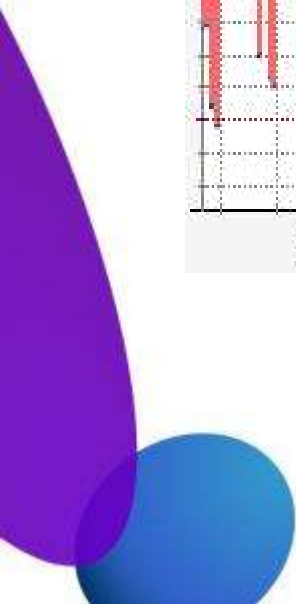
Top 40 by **bytes in**
for five minute flow sample ending Mon Jun 27 14:20:00 2005

rank	in Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1	bas003.bmt.esat.net 193.95.142.244	8.0 M (8.3%)	1.1 (0.0%)	1.5 k (6.3%)	3.3 m (0.0%)	40.0 m (0.0%)	3.3 m (0.0%)
#2	newsfeed.esat.net 193.95.141.36	4.2 M (4.4%)	95.9 k (4.0%)	1.2 k (5.2%)	10.2 (1.8%)	970.0 m (0.0%)	693.3 m (0.2%)
#3	deathstar.esat.net 193.95.134.145	2.2 M (2.3%)	8.5 (0.0%)	199.7 (0.9%)	20.0 m (0.0%)	216.7 m (0.0%)	16.7 m (0.0%)

Top 40 by **pkts in**
for five minute flow sample ending Mon Jun 27 14:20:00 2005

rank	in Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1	bas003.bmt.esat.net 193.95.142.244	8.0 M (8.3%)	1.1 (0.0%)	1.5 k (6.3%)	3.3 m (0.0%)	40.0 m (0.0%)	3.3 m (0.0%)
#2	newsfeed.esat.net 193.95.141.36	4.2 M (4.4%)	95.9 k (4.0%)	1.2 k (5.2%)	10.2 (1.8%)	970.0 m (0.0%)	693.3 m (0.2%)
#3	193.95.154.80	2.2 M (2.3%)	76.8 k (3.2%)	1.2 k (5.1%)	9.6 (1.7%)	131.8 (6.0%)	8.0 (2.5%)
#4	193.95.160.196	681.8 k (0.7%)	102.2 k (4.3%)	779.2 (3.3%)	21.2 (3.7%)	122.7 (5.5%)	19.0 (5.8%)
#5	193.95.154.104	1.1 M (1.1%)	16.5 k (0.7%)	603.1 (2.6%)	3.1 (0.5%)	97.4 (4.4%)	3.0 (0.9%)

EsatBT (AS2110) Well Known Protocols/Services, Bits, +out/-in



Thanks

