

Extending the IPFIX protocol for better QoS monitoring 24.07.07
Olav Kvittem, Arne Øslebø

Scampi/Lobster Software

- MAPI Measurement API in C
 - ◆ Interfaces passive measurement cards(DAG, Combo6)
 - Abstraction, sharing, branching, anonymization, efficiency(0-copy)
 - Functions filtering hw/sw, counters, flow analysis
- Applications
 - ◆ Service detection appmon
 - ◆ Polymorphic attack detector
 - ◆ Extended flow analysis Stager
 - * SubSecond Bandwidth measument(SSB)

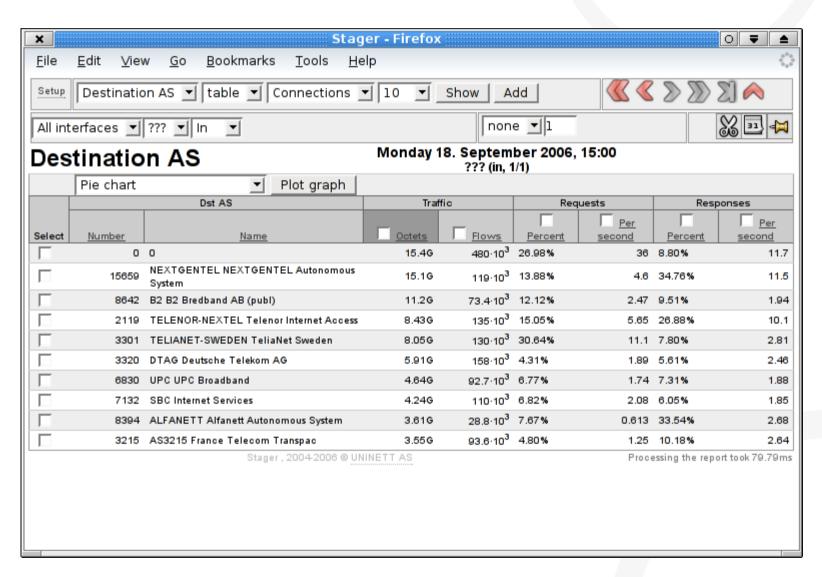


Extended flow parms.

- Compute cheap numbers : count, sum, sum of squares => standard deviation
- Packet size distribution
- Interarrival time distribution
- Bit rate vs time 1, 10, 100, 1000 ms (max/min)
- TCP properties : windows, retransmissions/out-of-seq, direction - initiator
- Service classification
- RTP time-stamps/payload-type



Destination AS report (2)





Most out of sequence dst-AS

```
• out 10ms 100ms eff win
```

```
• % Kbps Kbps Byte
```

- 1.5 5903 1007 8814
- •
- 11.9 1917 204 3081
- 13.6 1054 112 1650
- 15.1 1445 156 2467
- 21.4 1973 208 3120

summary

- We have demonstrated
 - ◆ MAPI passive probe IPFIX generator
 - ◆ Stager IPFIX flow reporting system
 - ◆ Enterprise IPFIX variables for performance
- Do you want to
 - standardize performance parameters?

