

The Future of Network Monitoring

Some Thoughts

Stuart Parham
sparham@cisco.com
Cisco Systems
7.6.2005 Poznan

Some questions we need to answer

Cisco.com

- What do we want to monitor?
 - Data (content) ?
 - Usage (time) ?
 - Users (who) ?
- Why do we want to monitor it ?
 - Performance ?
 - Billing ?
- Where does the law stand on this ?
 - Depends on answers to above
 - For (requires) some
 - Against (forbids) others
- What CAN we monitor

Some interesting facts

- 40 Gigabit links are already here (being shipped !)
- 100 Gigabit links are not far away
- 40 Gigabit \simeq 4 Gigabyte per second \simeq 1 Terabyte every 250 Seconds
That is a Terabyte approx ever 4 Minutes
- 100 Gigabit \simeq 10 Gigabyte per second \simeq 1 Terabyte every 100 Seconds
That is a Terabyte approx ever 1.5 Minutes
- The industry already has Routers capable of switching in excess of 1 Terabit per second.
- This is increasing at a MUCH faster rate than processing power.

EVEN if we only capture the Header this is not going to be practical !

Some options

- We will need to use some kind of data SAMPLING
 - Number of experimental solutions are being worked on.
 - Studies into effect of sampling period etc. being carried out.
- IF network monitoring is necessary some form of hardware acceleration will need to be invented.
 - ASIC's are not fast or flexible enough
 - It will have to look for specific data not all
- “Legal Intercept” is going to pose problems. It is already causing the industry to look for “interesting” solutions for VOIP

Some more food for thought

Cisco.com

- How do we protect individual privacy (sampling can be good here)
- Ever more sophisticated attacks on our networks will require us to use new solutions for monitoring
- Will the need for privacy lead to a change in network usage patterns?.