Visualising Data
“Why do we need to Visualise Data?”

• Most straight data output is not intuitive

• Humans do well with graphical outputs

• Humans do pattern recognition well

• Visualising summarises data

• Visualising is easy for non-techies to understand

• Visualising is useful for trending or making a point
“Visualising Data - Trending”

- This example is for logging trends as graphs
- This can be done using MRTG/RRDTool/etc
- Useful to spot trends
- Shows management how something is doing in an easy to understand way
“Visualising - Custom”

- Creating visual representations is only limited by imagination and ability
- This example uses simple bash scripting
- Takes network data and colorizes it
- Makes it easy to see at a glance what traffic is flowing
- <demo>
“Visualising - Pictures”

- Are many tools for “alternate” data watching
- An interesting one is Driftnet
- Shows the actual pictures from web traffic flows
- Great fun to a party trick but use with caution
- <demo>
“Visualising - Flows”

• Another tool is Etherape

• Creates a “light show” based on length and bandwidth of a net flow

• Can apply filters

• Very useful as a graphical way to see what goes where

• <demo>
“Visualising - Relationships”

• Afterglow can be used to with Graphviz to create Relationship diagrams
• Any tuplet of data can be used
• Makes very pretty pictures
• Very useful to see relationships between traffic and hosts
• Very useful to see unrelated relationships
• <demo>
“Moving Forward...”

- All previous examples are only a small showing of what can be done
- Visualisation can be a small thing and can scale to a large solution (ie: Ntop)
- Any way to make large amounts of data easier to understand is useful
- Just look around and see what works for you
Thank you for your attention

-Appendix-

-MRTG - http://oss.oetiker.ch/mrtg/
-RRDTool - http://oss.oetiker.ch/rrdtool/
-Driftnet - http://ex-parrot.com/~chris/driftnet/
-Etherape - http://etherape.sourceforge.net/
-Afterglow - http://afterglow.sourceforge.net/
-Graphviz - http://www.graphviz.org/
-NTop - http://www.ntop.org