



# Networking in a Large Enterprise

**Matthew Cook**  
**Network & Security Manager**  
**Loughborough University**

## A bit about myself...

- Network & Security Manager at Loughborough University
- Team of ten IT Professionals
- Worked at Loughborough for 9+ years
- JANET(UK) Trainer
- Security Researcher

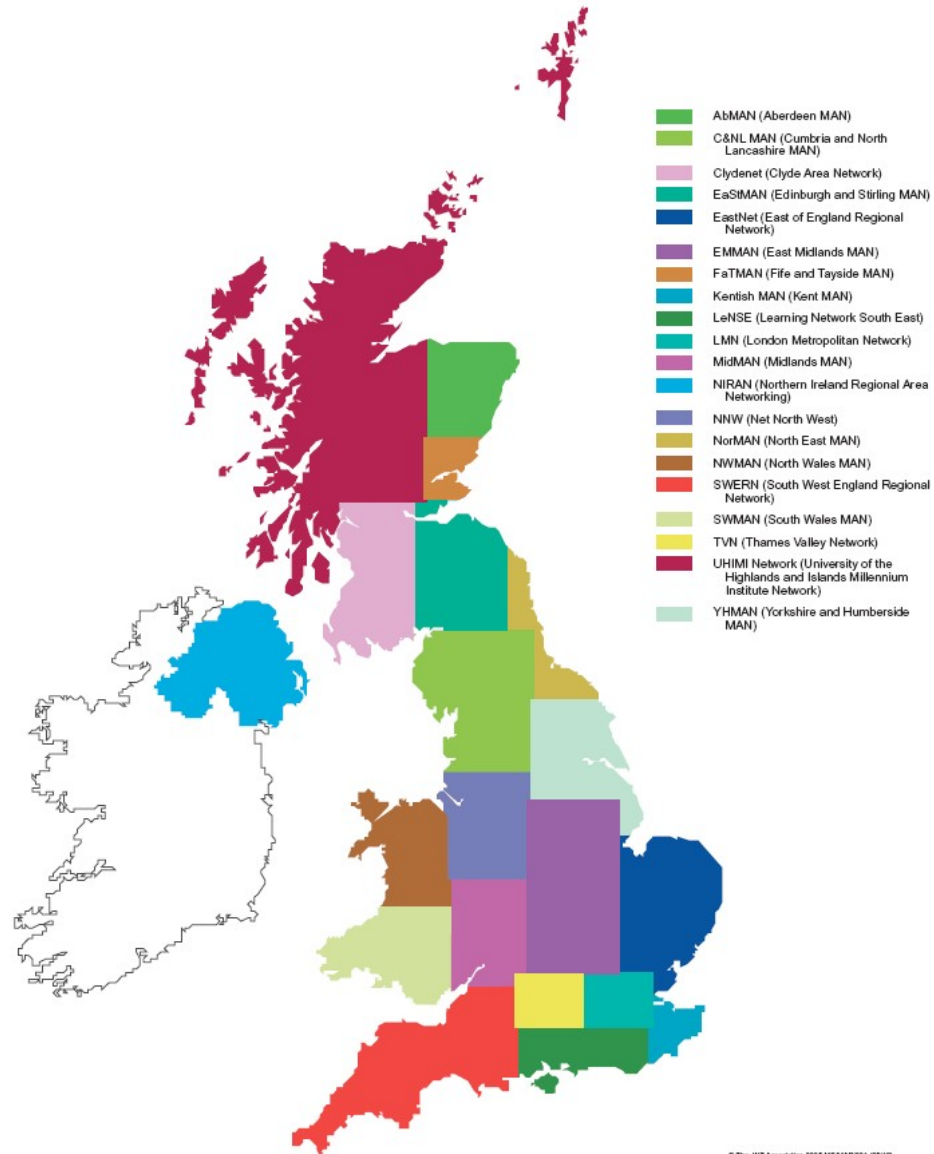


# Super JANET Backbone



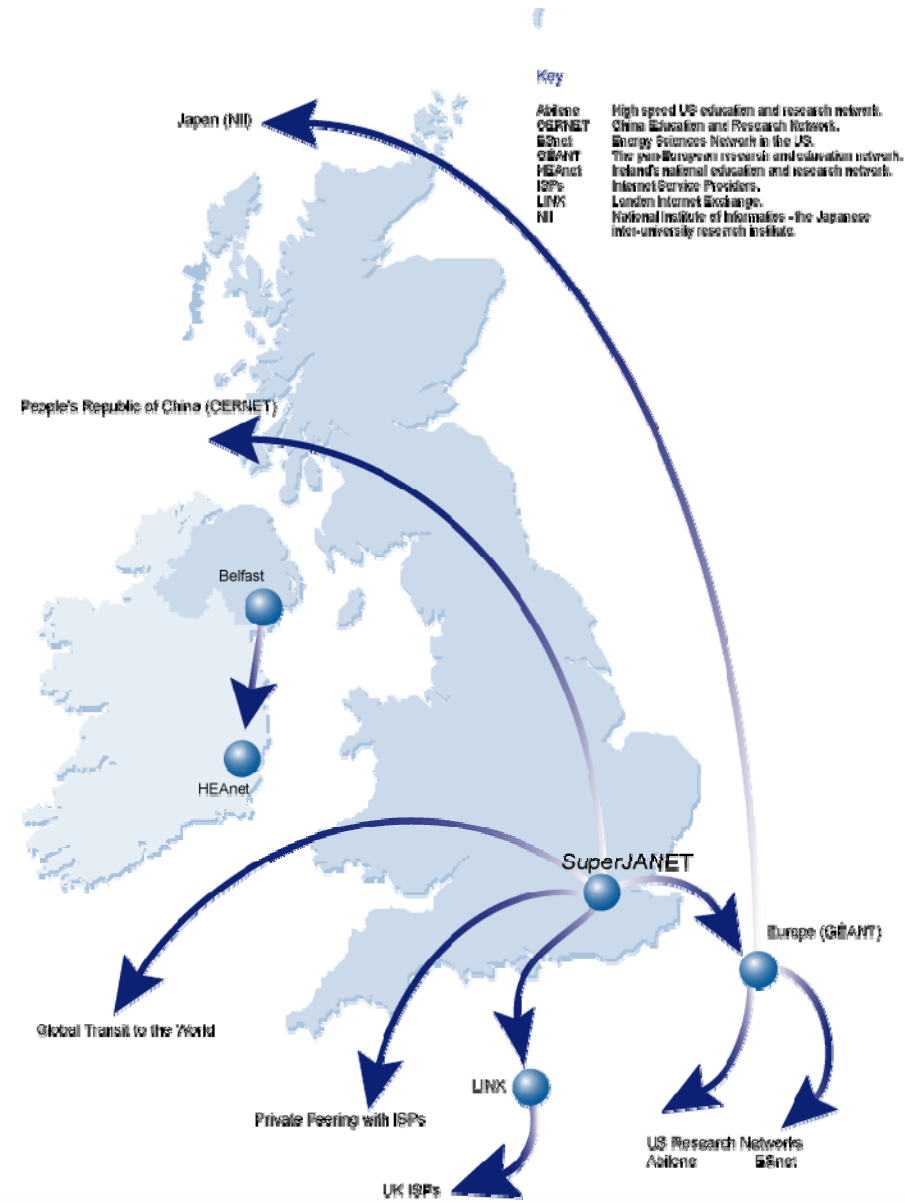
©The JTA Association 2005 (GSM/04/04/11)

# Regional Networks



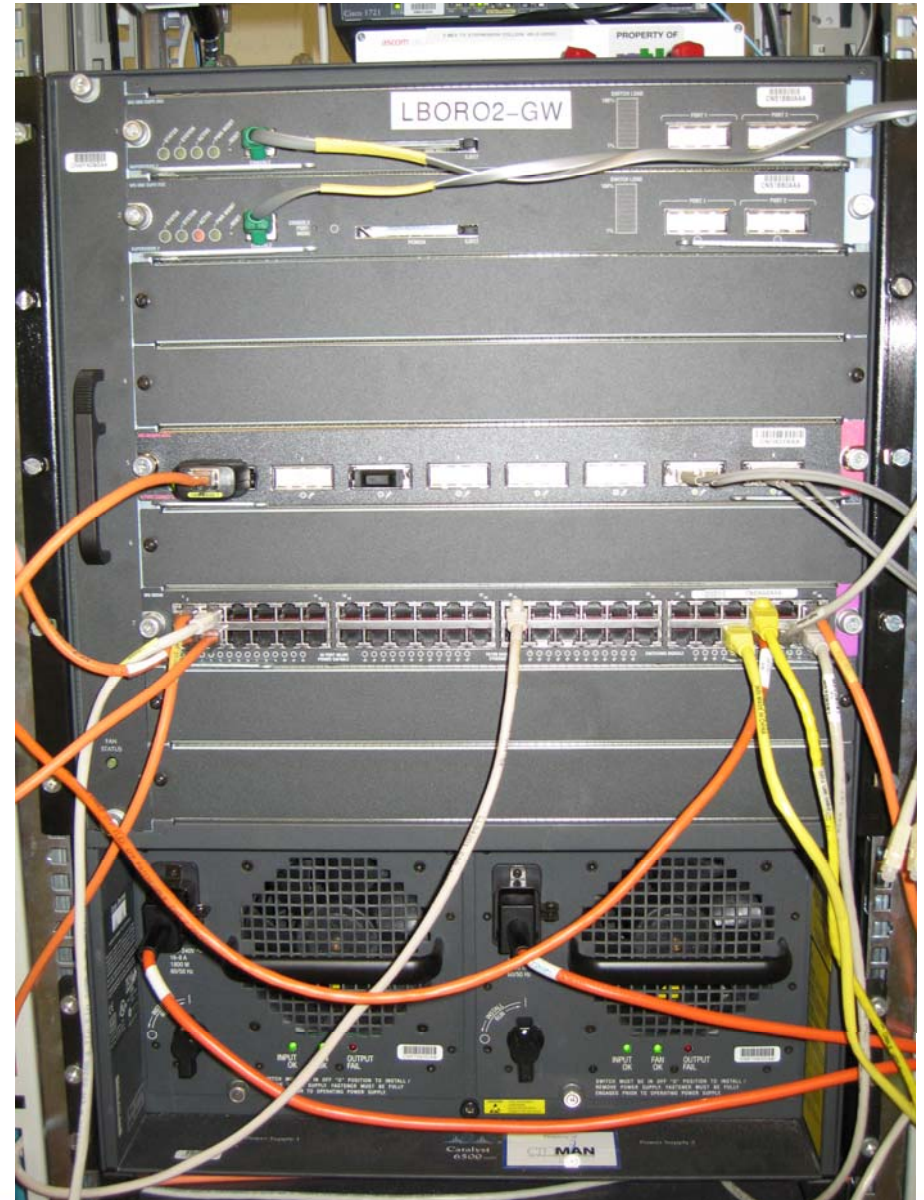
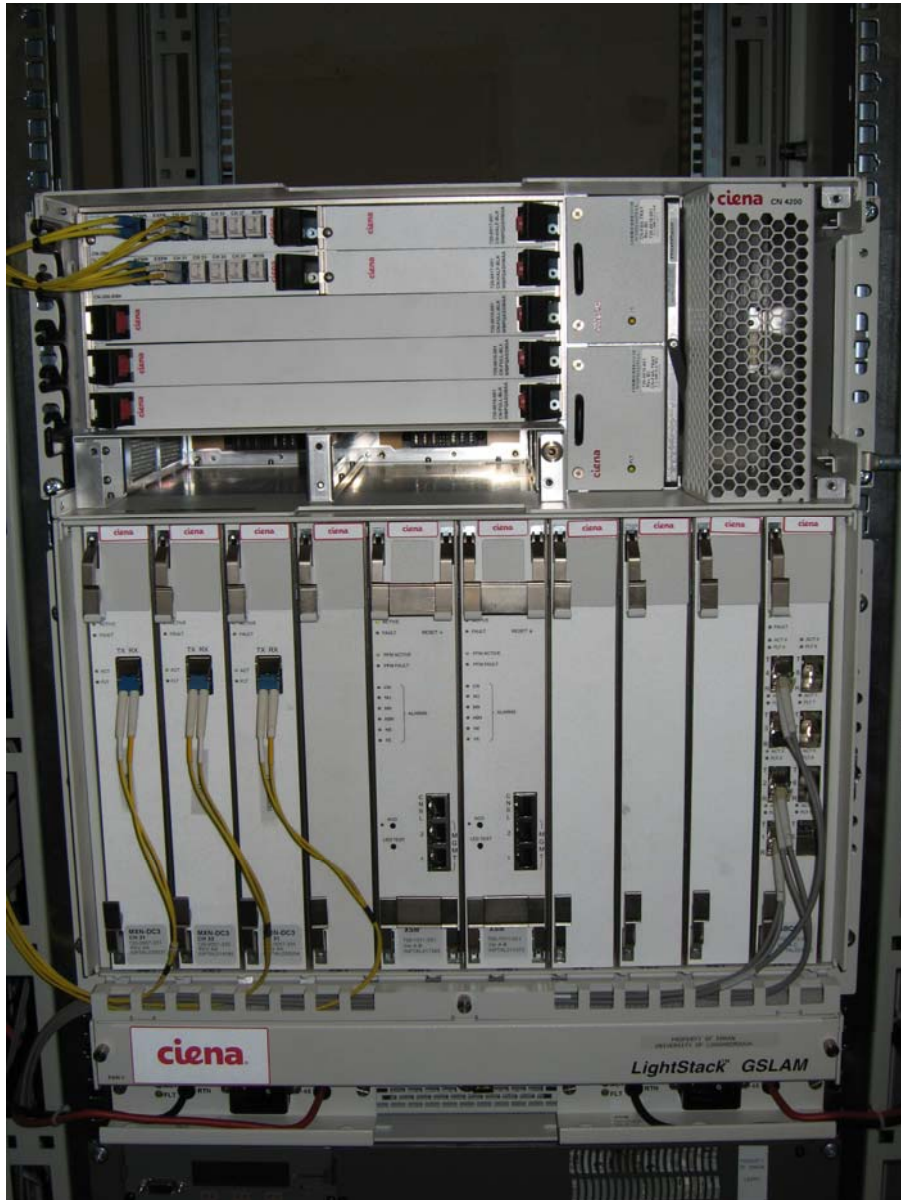
© The JNT Association 2005 MS000101 (05/10)

# The Wider Internet



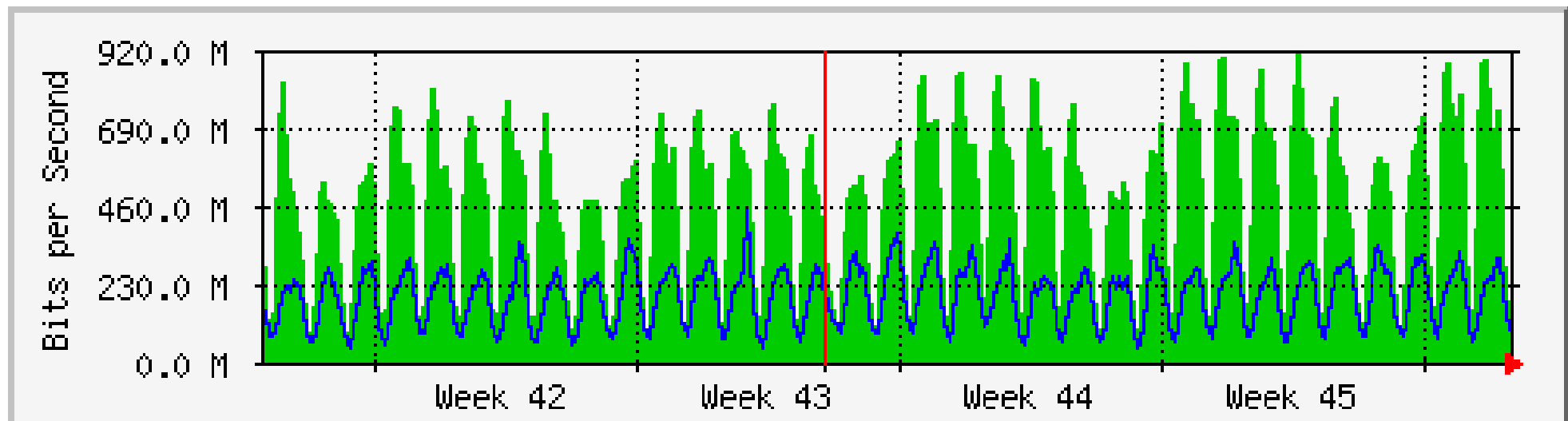


# In real life



# JANET Traffic

## 'Monthly' Graph (2 Hour Average)

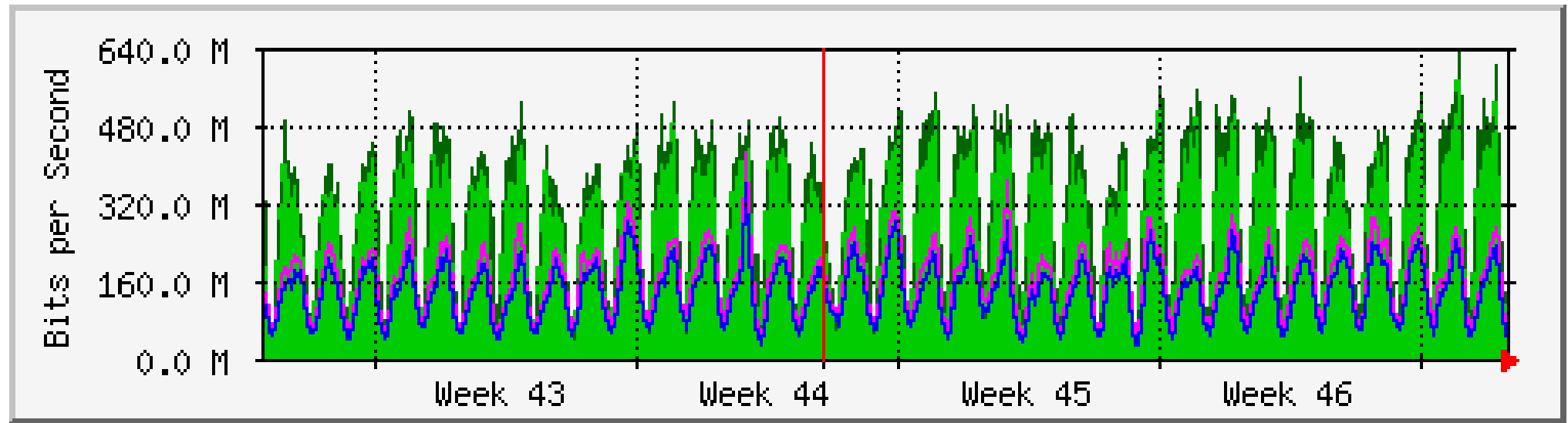


Max In: 916.2 Mb/s (9.2%)    Average In: 462.7 Mb/s (4.6%)    Current In: 133.1 Mb/s (1.3%)  
 Max Out: 451.7 Mb/s (4.5%)    Average Out: 196.0 Mb/s (2.0%)    Current Out: 99.8 Mb/s (1.0%)



# Lboro Traffic

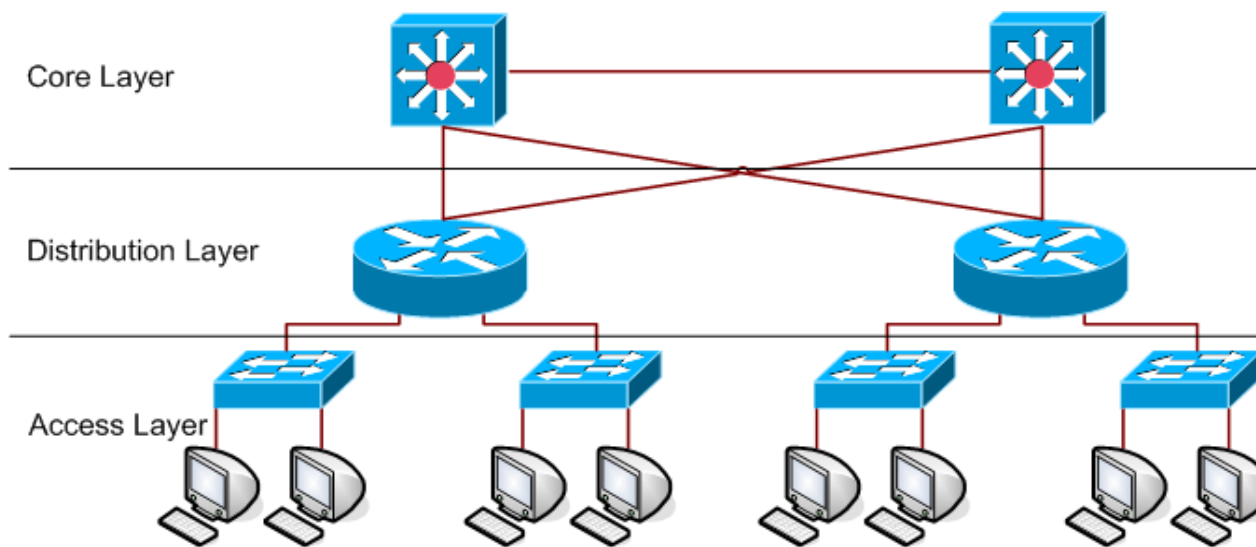
## 'Monthly' Graph (2 Hour Average)



	Max	Average	Current
<b>In</b>	637.0 Mb/s (63.7%)	279.2 Mb/s (27.9%)	73.8 Mb/s (7.4%)
<b>Out</b>	419.0 Mb/s (41.9%)	133.4 Mb/s (13.3%)	50.7 Mb/s (5.1%)

## Networking Models

- Most organisations use the three layer hierarchical network model or a model based on a merged core and distribution layer.



## Access Layer

- Traffic Sniffing
  - Shared Ethernet
  - Macof
  - Switches turned into hubs
- MAC Address filtering
  - Network Access
  - Prevention of MAC/CAM Table flooding
- DHCP Snooping
  - Rogue DHCP Servers
  - Wireless Base Stations
- Port Shutdown
  - Remote Disconnection
  - Multiple machines and hubs

## Fault Tolerance and Load Balancing

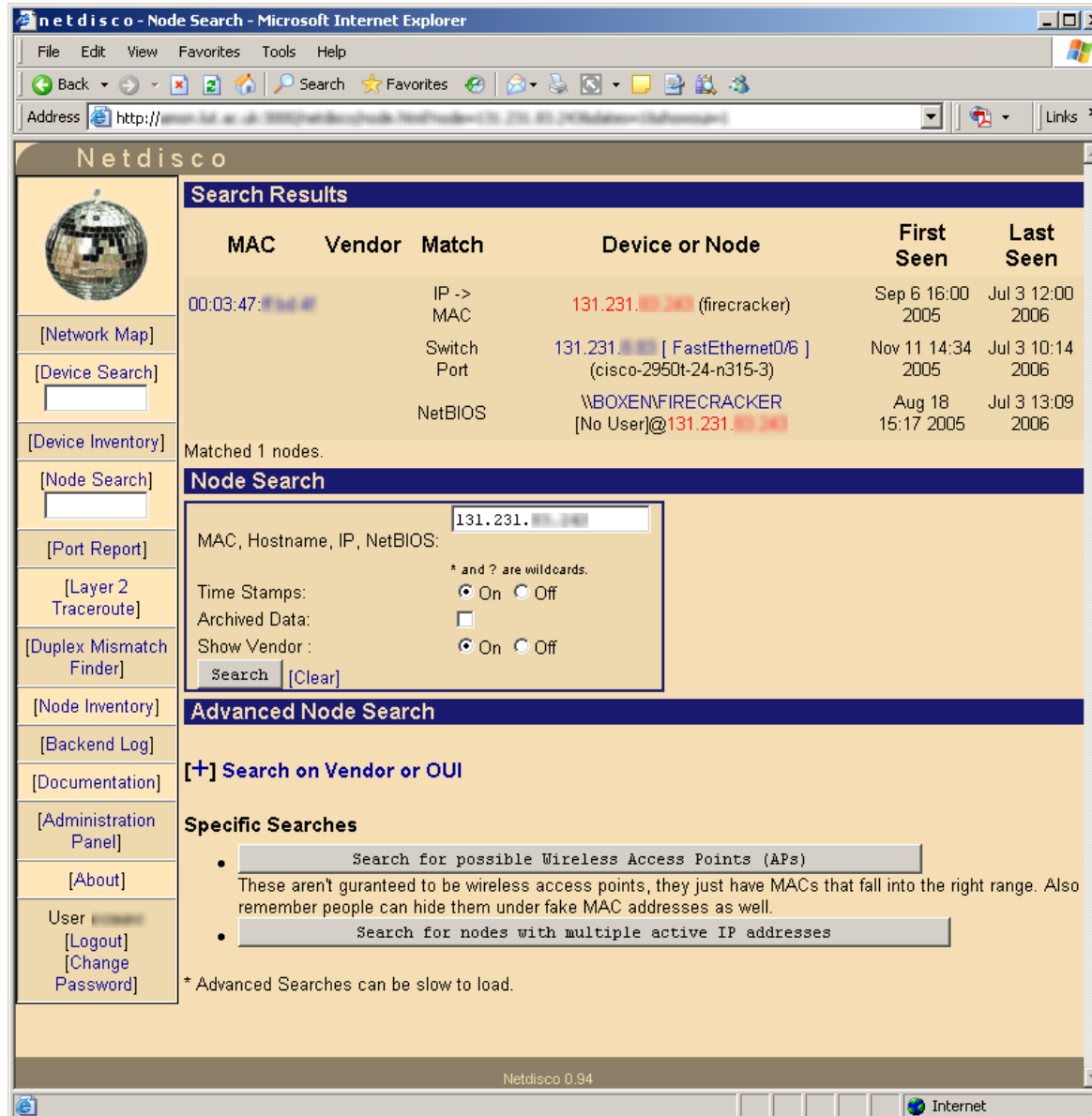
- Network Devices with 24/7 availability
  - Twin power supplies
  - Twin supervisor cards
  - Replaceable chassis components
- Network Level
  - Redundant devices
  - Spanning Tree
  - Hot Standby Routing Protocol
- Load Balancing
  - Less of an issue
  - Session Cookies

## Network Equipment Store

- Warranty
  - Limited Life Time
- Stock
  - One switch to every 40-50 switches
  - Interconnects
  - GBICS
  - Cables
- Wireless/IP over Power



# Network Management



**netdisco - Node Search - Microsoft Internet Explorer**

Address: http://www.131.231.100.100/netdisco/nodeSearch.html

**Netdisco**

**Search Results**

MAC	Vendor	Match	Device or Node	First Seen	Last Seen
00:03:47:12:34:56		IP -> MAC	131.231.100.100 (firecracker)	Sep 6 16:00 2005	Jul 3 12:00 2006
		Switch Port	131.231.100.100 [ FastEthernet0/6 ] (cisco-2950t-24-n315-3)	Nov 11 14:34 2005	Jul 3 10:14 2006
		NetBIOS	\\BOXEN\FIRECRACKER [No User]@131.231.100.100	Aug 18 15:17 2005	Jul 3 13:09 2006

Matched 1 nodes.

**Node Search**

MAC, Hostname, IP, NetBIOS:

\* and ? are wildcards.

Time Stamps:  On  Off

Archived Data:

Show Vendor:  On  Off

**Advanced Node Search**

**[+] Search on Vendor or OUI**

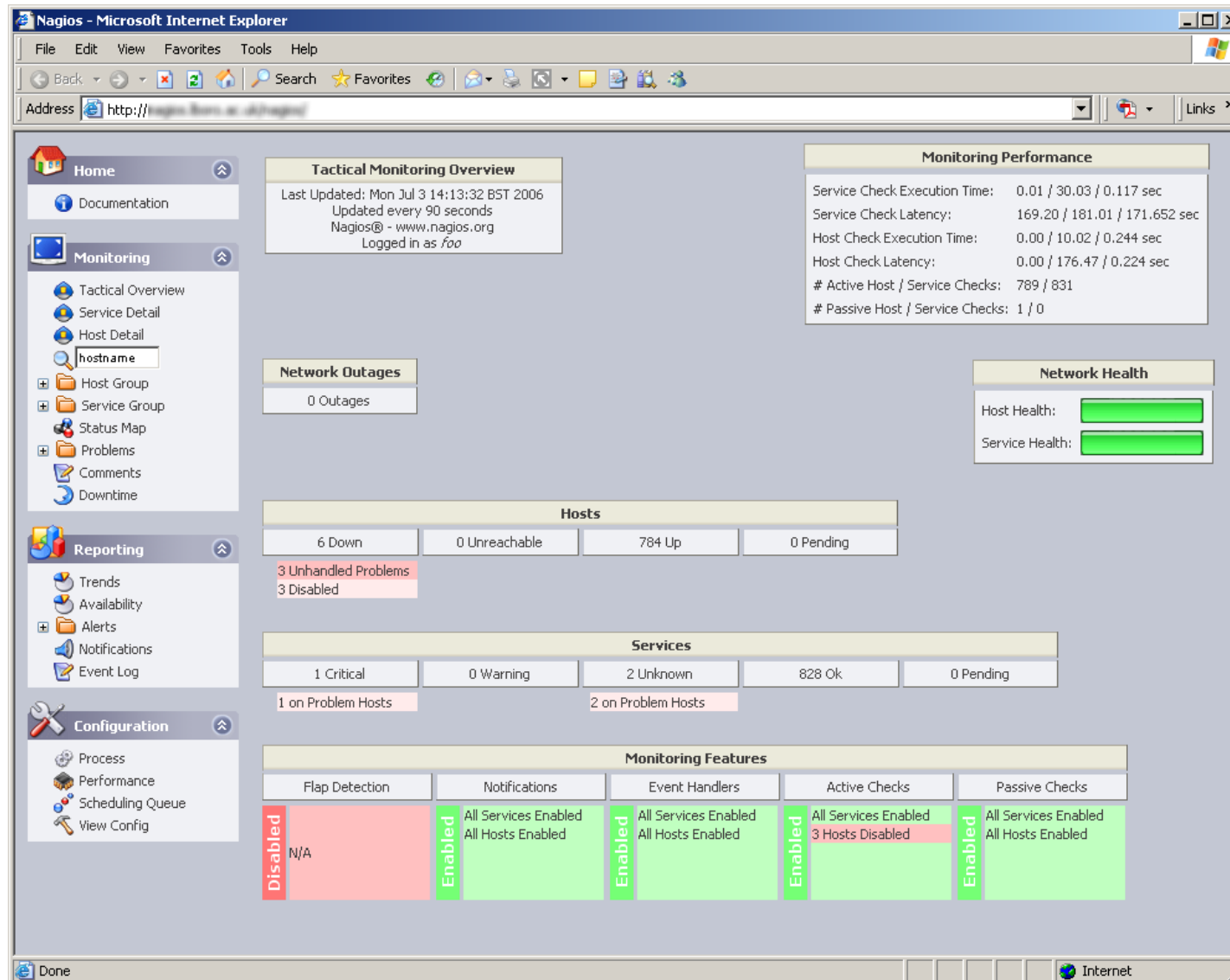
**Specific Searches**

- These aren't guaranteed to be wireless access points, they just have MACs that fall into the right range. Also remember people can hide them under fake MAC addresses as well.
- 

\* Advanced Searches can be slow to load.

Netdisco 0.94

# Network Management



**Nagios - Microsoft Internet Explorer**

Address: <http://nagios.fern.ac.uk/nagios/>

**Home**

- Documentation

**Monitoring**

- Tactical Overview
- Service Detail
- Host Detail
- hostname
- Host Group
- Service Group
- Status Map
- Problems
- Comments
- Downtime

**Reporting**

- Trends
- Availability
- Alerts
- Notifications
- Event Log

**Configuration**

- Process
- Performance
- Scheduling Queue
- View Config

**Tactical Monitoring Overview**

Last Updated: Mon Jul 3 14:13:32 BST 2006  
 Updated every 90 seconds  
 Nagios@ - www.nagios.org  
 Logged in as foo

**Monitoring Performance**

Service Check Execution Time: 0.01 / 30.03 / 0.117 sec  
 Service Check Latency: 169.20 / 181.01 / 171.652 sec  
 Host Check Execution Time: 0.00 / 10.02 / 0.244 sec  
 Host Check Latency: 0.00 / 176.47 / 0.224 sec  
 # Active Host / Service Checks: 789 / 831  
 # Passive Host / Service Checks: 1 / 0

**Network Outages**

0 Outages

**Network Health**

Host Health: ██████████  
 Service Health: ██████████

**Hosts**

6 Down	0 Unreachable	784 Up	0 Pending
--------	---------------	--------	-----------

3 Unhandled Problems  
3 Disabled

**Services**

1 Critical	0 Warning	2 Unknown	828 Ok	0 Pending
------------	-----------	-----------	--------	-----------

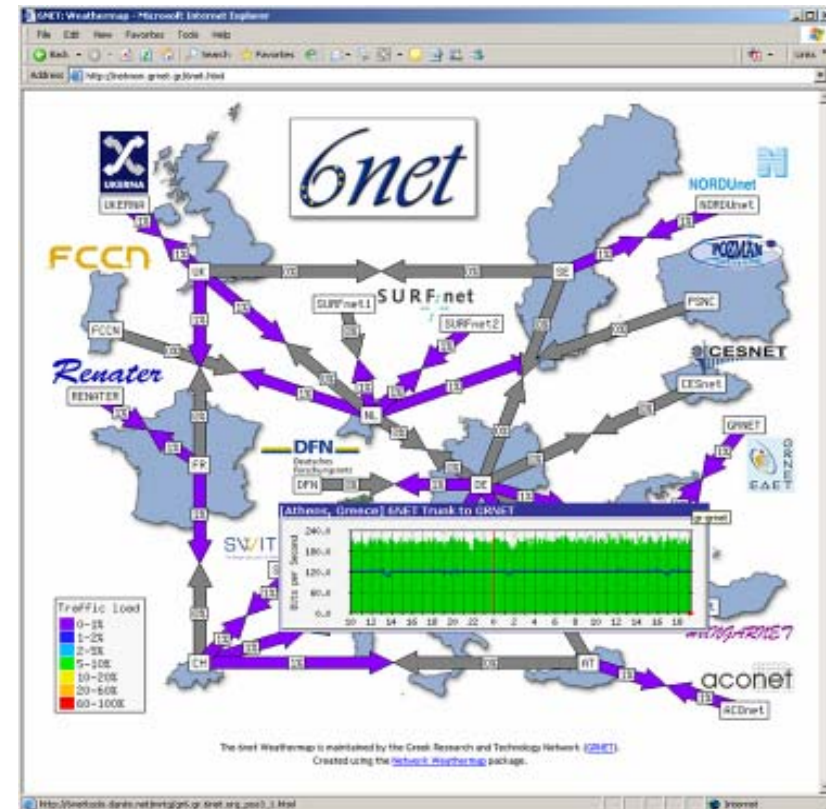
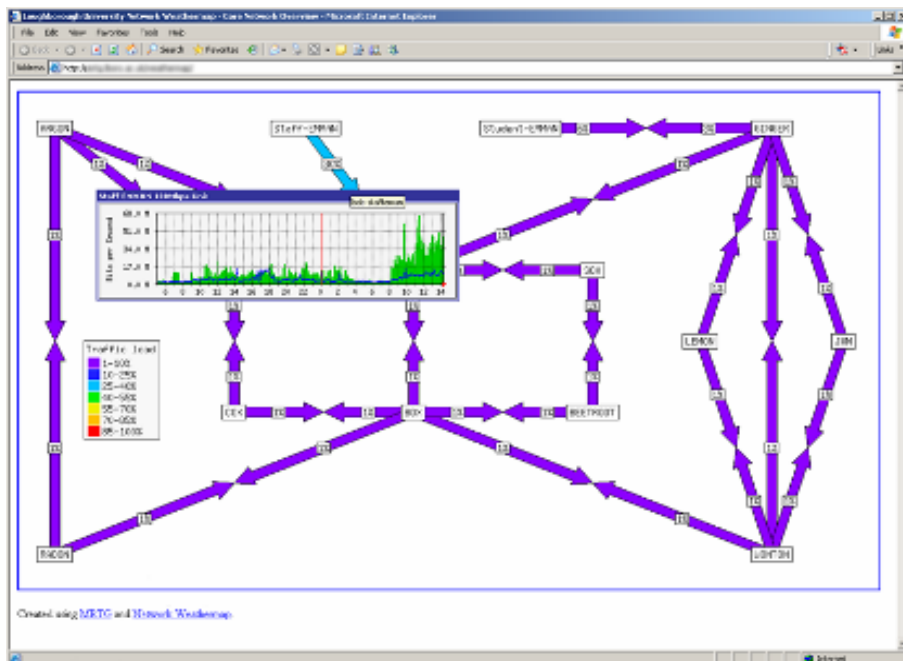
1 on Problem Hosts      2 on Problem Hosts

**Monitoring Features**

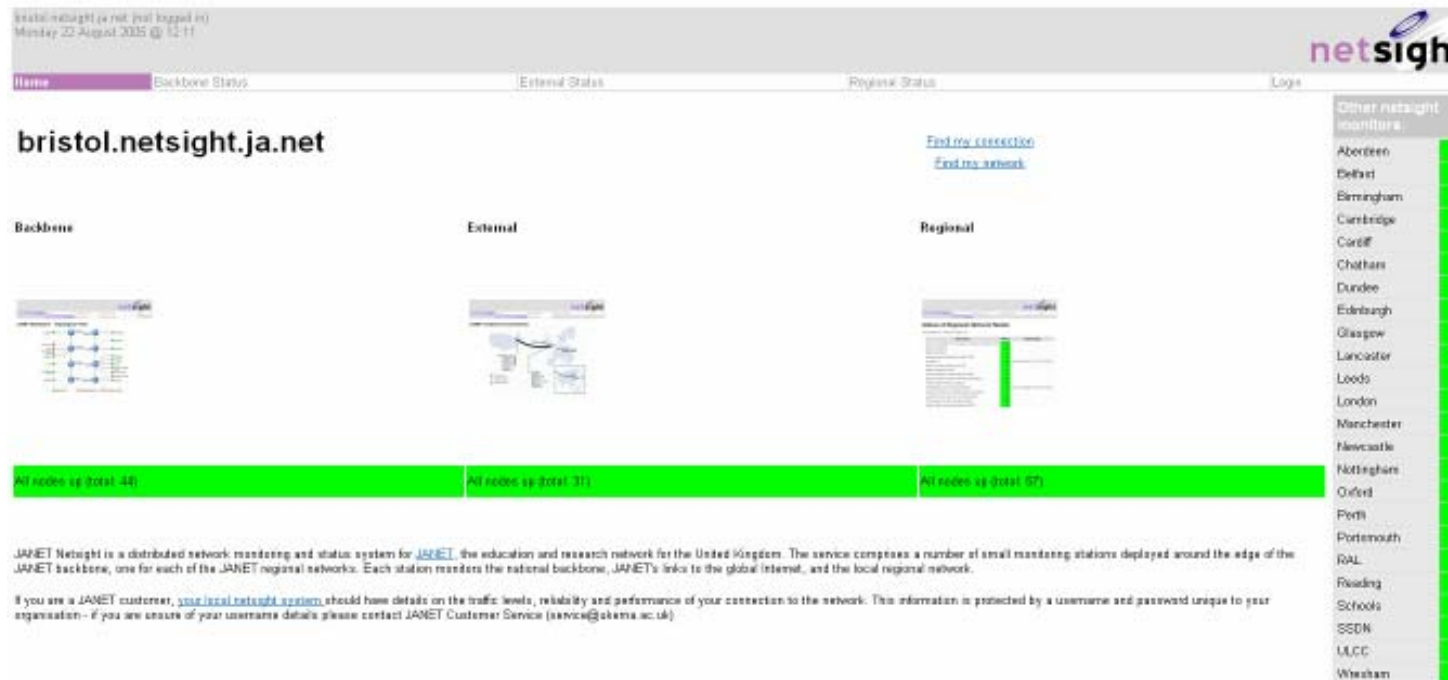
	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Disabled	N/A	Enabled	Enabled	Enabled	Enabled
		All Services Enabled All Hosts Enabled	All Services Enabled All Hosts Enabled	All Services Enabled 3 Hosts Disabled	All Services Enabled All Hosts Enabled

Done Internet

# Network Management



# JANET Netsight



bristol.netsight.ja.net

Backbone Status External Status Regional Status

Backbone External Regional

All nodes up (total 44) All nodes up (total 31) All nodes up (total 57)

JANET Netsight is a distributed network monitoring and status system for [JANET](#), the education and research network for the United Kingdom. The service comprises a number of small monitoring stations deployed around the edge of the JANET backbone, one for each of the JANET regional networks. Each station monitors the national backbone, JANET's links to the global internet, and the local regional network.

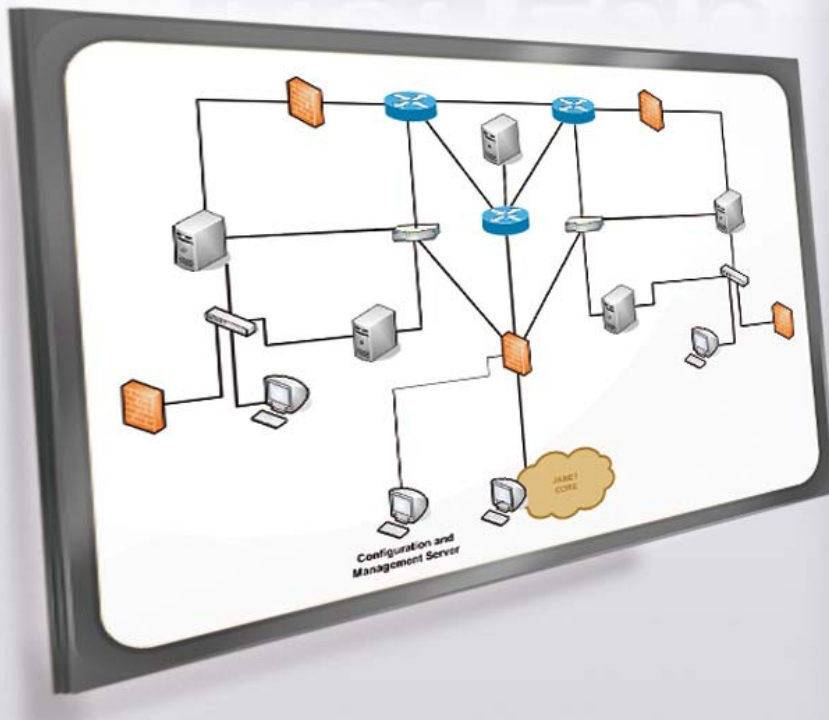
If you are a JANET customer, [your local netsight system](#) should have details on the traffic levels, reliability and performance of your connection to the network. This information is protected by a username and password unique to your organisation - if you are unsure of your username details please contact JANET Customer Service ([service@akema.ac.uk](mailto:service@akema.ac.uk)).

Provides an easy-to-understand view of the status and performance of the JANET network

# JANET NetLab



## Net Lab



- Core of JANET
- State of the art
- Industry standard
- Course support
- VMware ESX
- VPN connection
- Firewalls
- IPv6
- Multicast

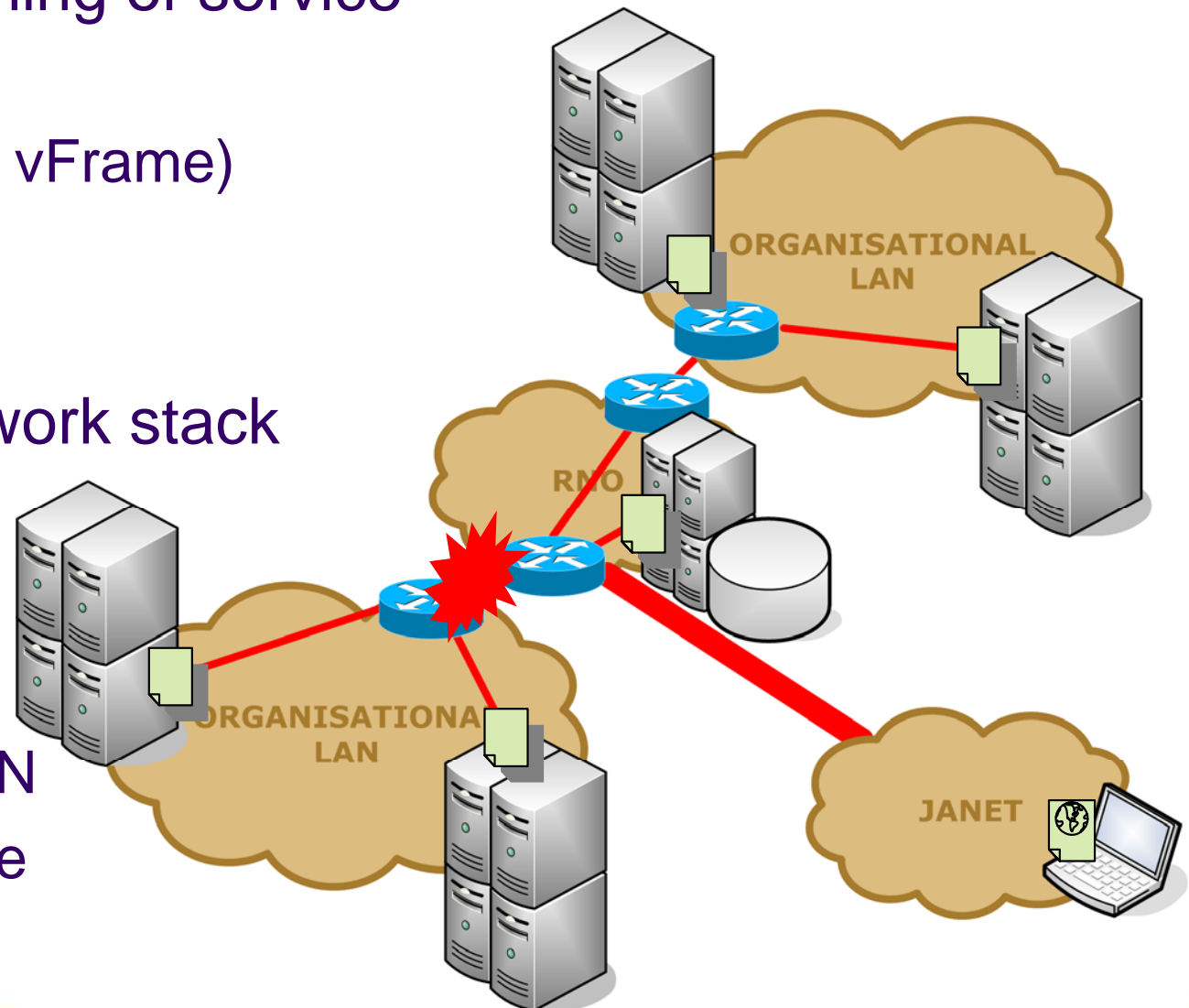
## Network Implications

- Is the virtual network secure?
  - Does your IDS/IPS have visibility of the virtual switch?
  - Network probe guest VM?
  - Increased frequency of SSL based attacks
  
- Expectation that the network can deliver:
  - Speed requirements, does it make sense to virtualise high bandwidth applications?
  - Same IP Everywhere (VMotion)
  - Automated VLAN changes
  - What is the virtual switch, or router?



# Futures

- Automated provisioning of service
  - Virtual Machine
  - Networking (Cisco vFrame)
  - Storage
  
- Complete IPv6 Network stack
  
- Pervasive Data Centres
  - Organisational SAN
  - Shared VM Service





**Questions?**

**Matthew Cook**  
**<http://escarpment.net/>**