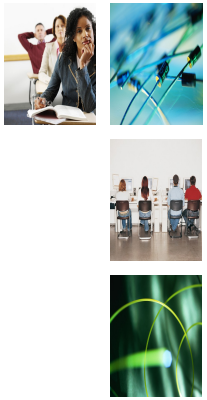


Security of Service

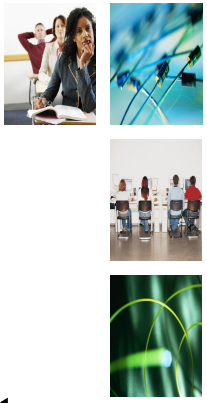
Rob Evans

JANET(UK)



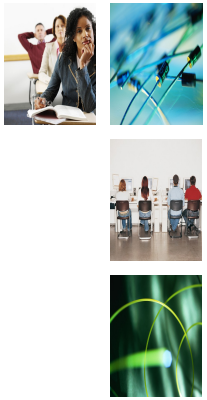

What this talk is about

- Our experiences of building a resilient network.
- Securing the supply of a service.



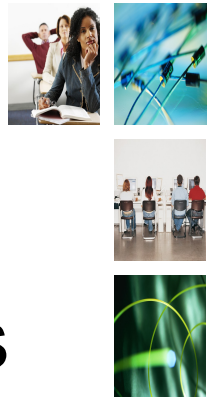
What this talk isn't about

- Title is a legacy from the conference it was first presented at. This isn't about:
  - Privacy
  - Intrusion Detection
  - CSIRT-type “Stuff”
- There's more than one way to skin a cat
  - Your network may be bigger and more resilient than ours.



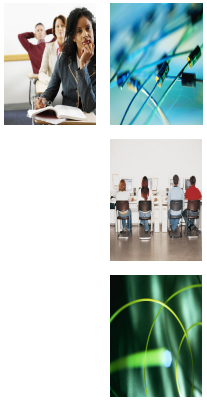
What we had

- SuperJANET4, launched in 2001
- Succeeded in breaking out of the cycle of bandwidth-limited backbones of previous years
- Good capacity
- Resilient
- ...but had some weak spots



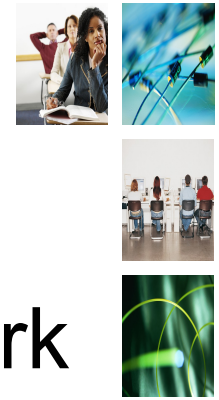
What we had

- Sites connected to Regional Networks
- Regional Networks connected to backbone
  - From 622Mbit/s to 2.5Gbit/s
  - Mainly protected SDH
  - Some Gigabit Ethernet (intra-room)
- Backbone highly resilient
- RN links less so



RN link resilience

- Protected SDH links.
  - Good, yes?
- Better than unprotected bits of fibre.
- But:
  - Single router on the backbone
  - Single router at the RN
  - Lots of scope for the telco to reroute and lose resilience.
  - You only find out the protect path isn't working when you need it.



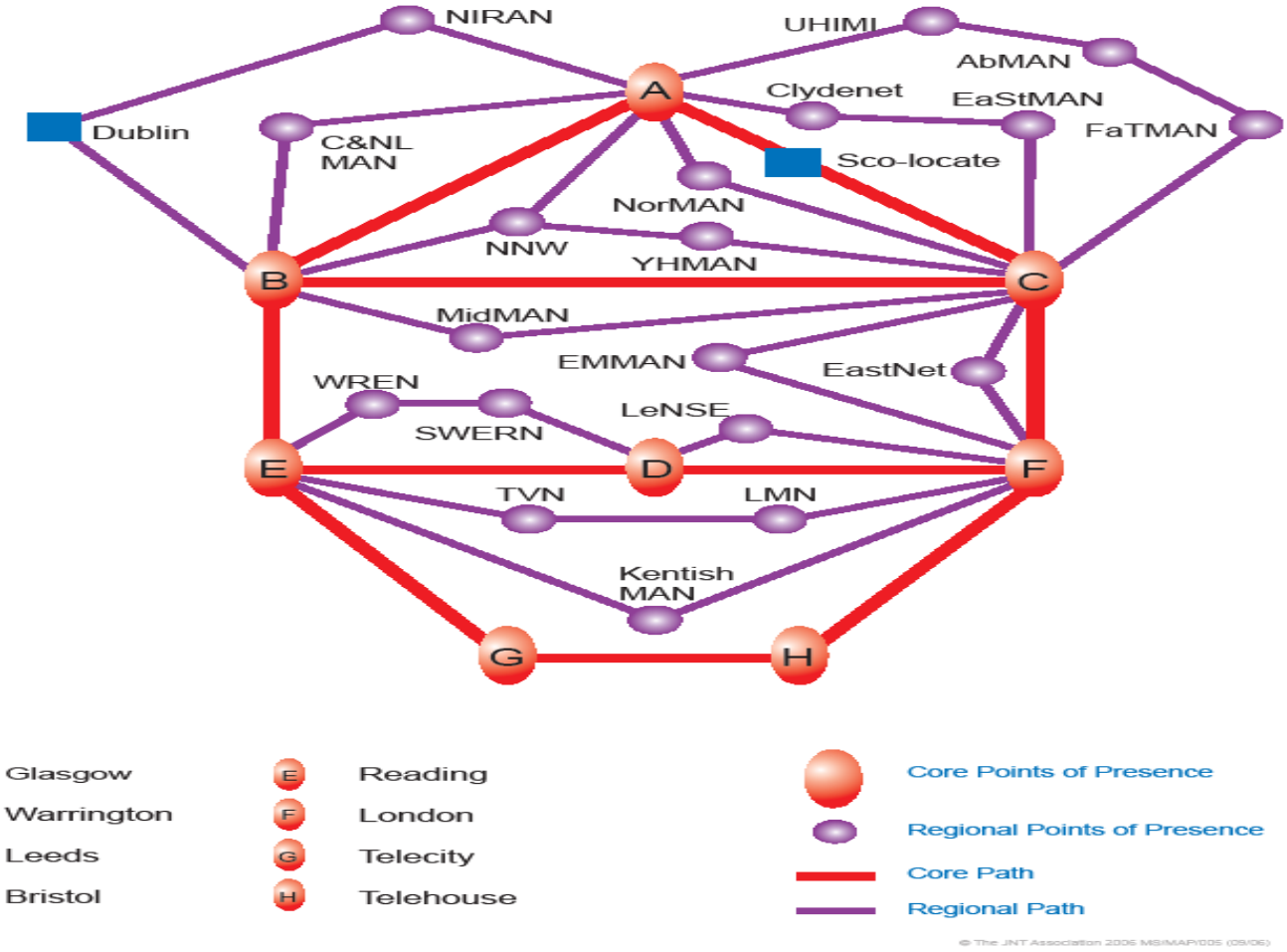
What we wanted

- Greater resilience for Regional Network links
  - Link failure takes off many sites.
- Increased agility for bringing extra circuits up
  - Capacity
  - Bandwidth channels for research work

Security against...

Photo courtesy of HEAnet

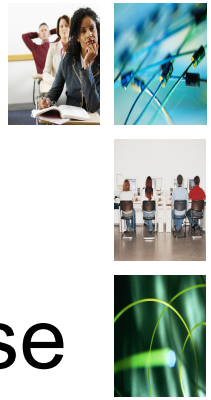
SJ5 Architecture






Basics

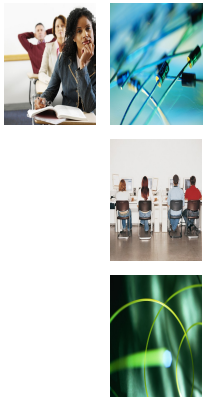
- Dedicated fibre and DWDM equipment
  - Not subject to requirements of other customers
- Ciena CoreStream at the core PoPs
- Ciena 4200 for the “collector arcs”

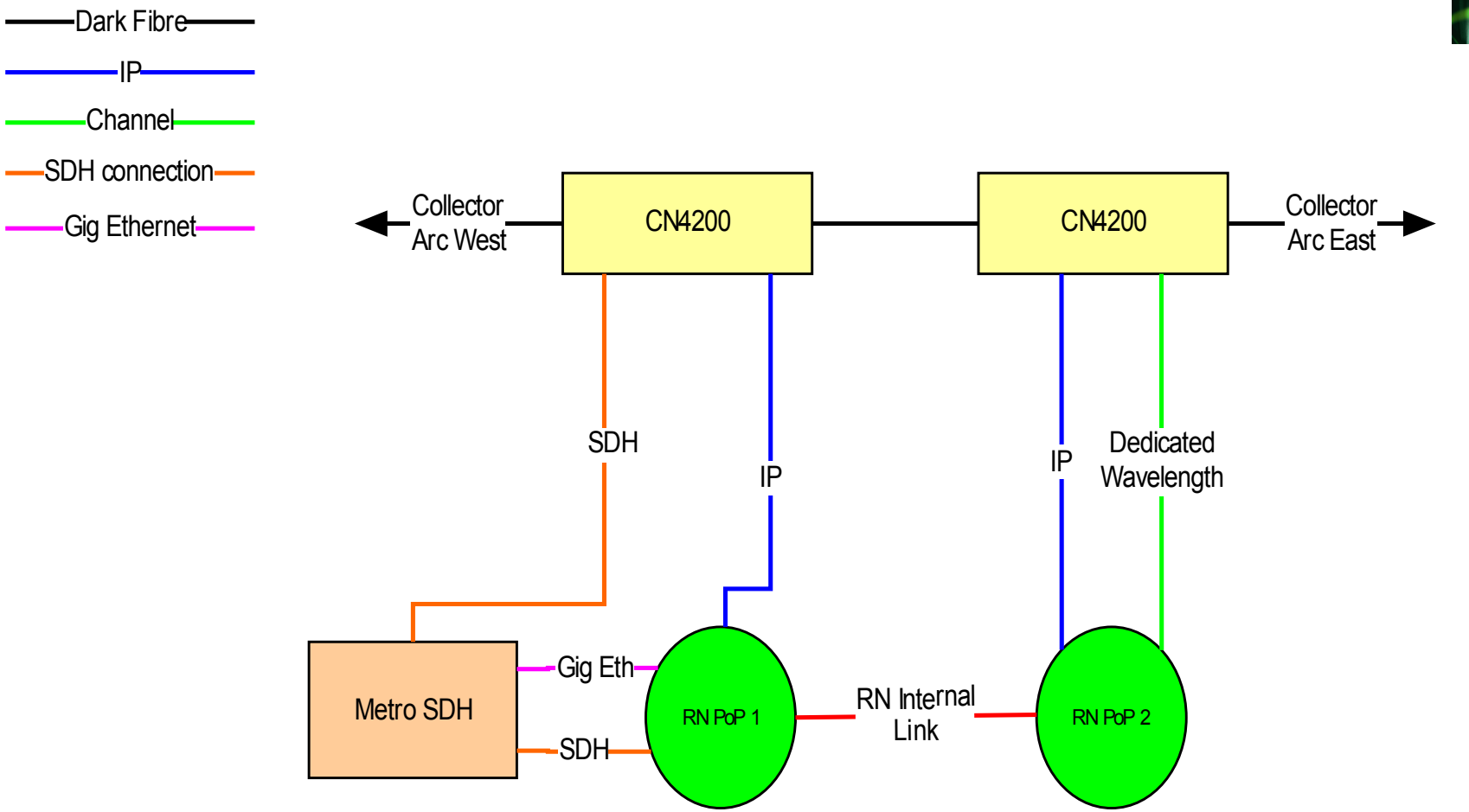


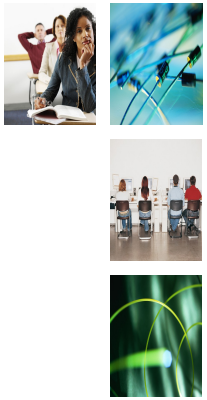
Regional Connections

- All Regional Networks have two diverse fibre connections to the backbone
  - Same capacity to ensure full resilience
  - Two different regional network PoPs
  - Two different Core PoPs

Regional Connections







Problems

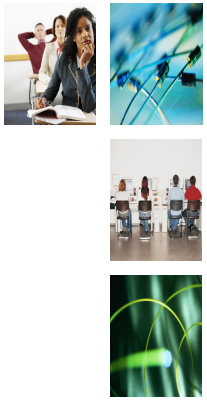
- Finding truly diverse fibre
  - Even in metro areas
- Are two fibres in the same duct diverse?
  - How about the same trench?
  - Opposite sides of the road?
  - Parallel roads?
- Is the information accurate...

Fibre Routing

Photo from http://www.flickr.com/photos/samjudson/

Fibre Routing

Photo from http://www.flickr.com/photos/samjudson/



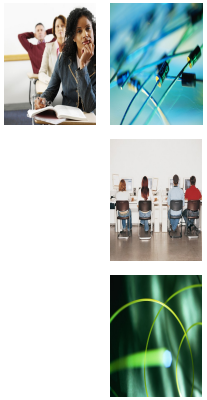
Design Choices

- Mandated SDH for Regional Network connections to the backbone
  - SDH notices faults, brings down interface, triggers IP routing changes
  - BFD not mature and widely deployed
  - Ethernet OAM not yet available
  - No SDH “ring” for optical protection
  - Quick failover essential for streaming media
- Complaints about cost required central funding for RN interfaces.



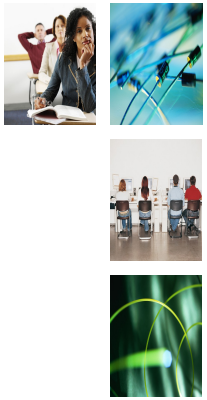

Core and Regional

- Regional Networks have previously had great autonomy in designing their own networks
  - Mismatch between services offered on core and on RN.
  - Difficult to roll out new services
    - Backbone has been IPv4/IPv6 dual stack since 2003.
    - Some RNs still aren't (but will be soon as it is coming into the SLA)



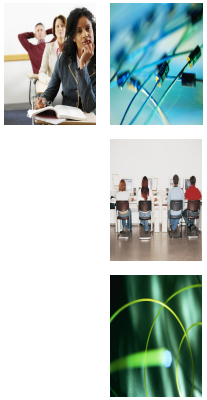
Core and Regional

- Introducing a “Technical Design Authority”
- Works with all the Regional Networks on their design and procurement.
- Ensure consistent access to new services
  - IPv6
  - Lightpaths



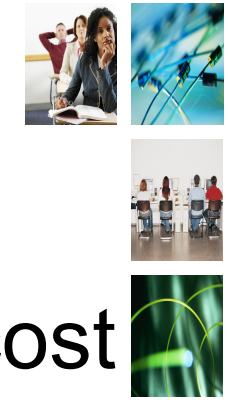
Core: Bandwidth

- Single large pipes rather than load-sharing over smaller circuits.
  - Simpler
  - Currently still 10Gbit/s
  - One trial link at 40Gbit/s
  - Backbone-wide within a couple of years
    - Hopefully.
    - PMD is SEP (sorta)



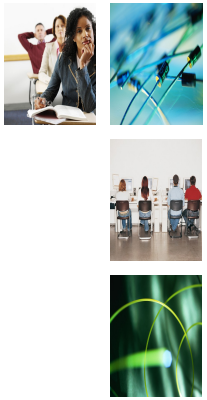
Core: Bandwidth

- Separate large or disruptive flows out onto dedicated channels
  - "Lightpaths"
  - Not only high bandwidth, but also specialist requirements
    - Large Hadron Collider, CERN
  - Separate the requirements of a research network from the need to run a highly available IP service for the rest of the customers



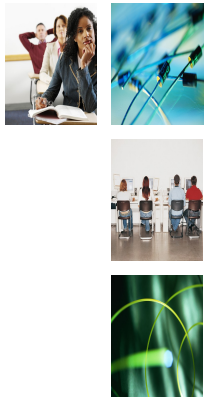
Core: Bandwidth

- Add additional channels at marginal cost
  - Fixed price between any two core PoPs
  - Proven useful for external connectivity
  - Also being used to provide GEANT (network linking R&E networks across Europe) with additional capacity to Dublin



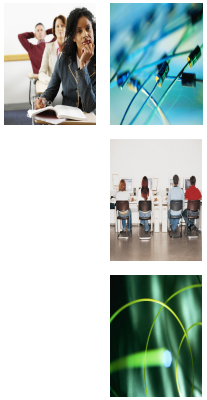
Core: Routers

- Reduced number of routers on core
  - SJ4 differentiated between “core” and “access” routers
  - Required due to functionality of routing equipment when it was designed
    - Difficult to do filtering and high-speed routing at the same time
  - Also useful for link monitoring. JANET router at the remote end of each link.



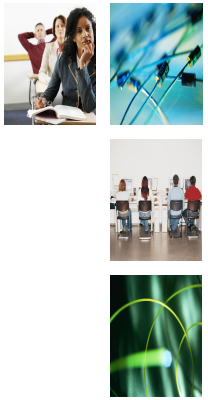
Core: Routers

- SJ5 collapses both functions onto the backbone routers
  - Fewer boxes to manage and upgrade
  - More than 20 fewer routers in SJ5
- Use optical equipment for link monitoring
- Still a few wrinkles
  - Sampled netflow (1/10) on 10Gbit/s+ hard to do with current equipment



External connectivity

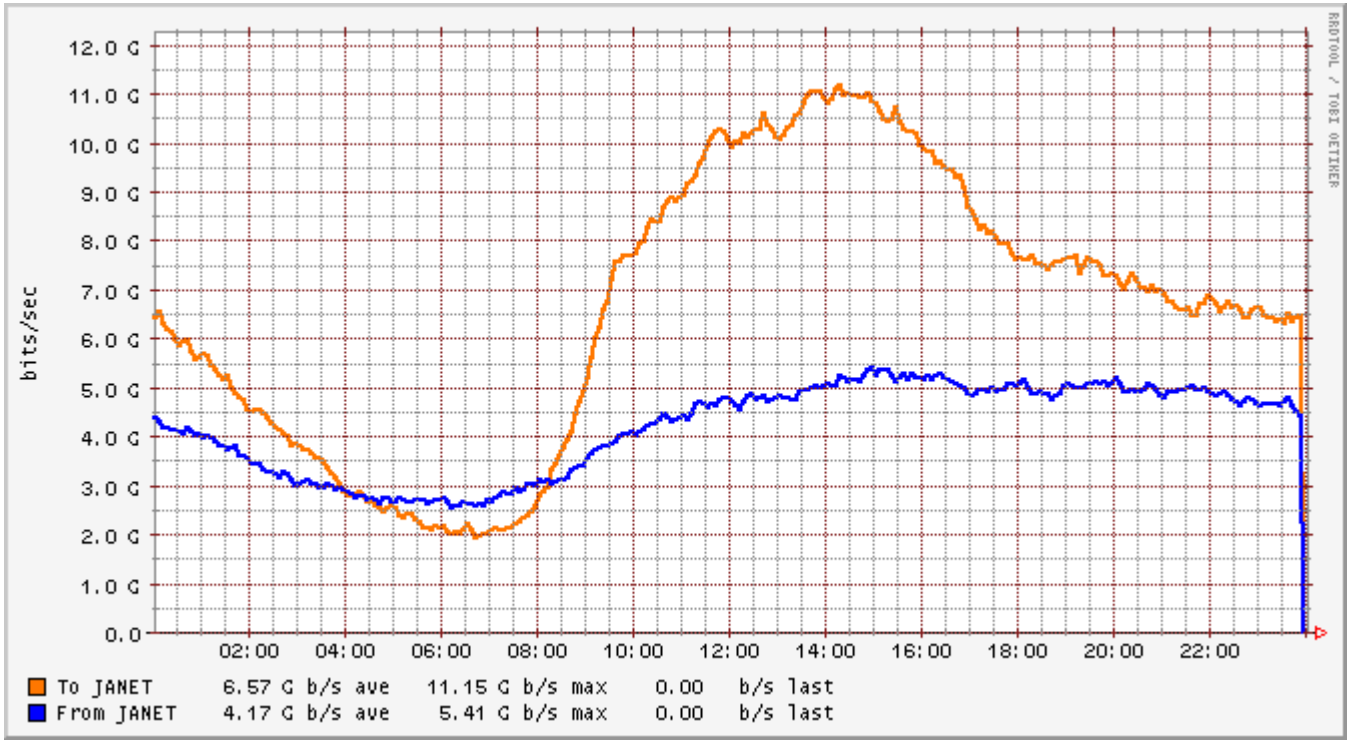
- Two locations in London's Docklands
  - Difficult to get high-speed transit elsewhere
  - Even if you do, it is usually long-lined from Docklands
- Each site has 10Gbit/s to two backbone nodes
- Required bandwidth growing ahead of 40Gbit/s availability
- In process of upgrading each site with 10G to four backbone nodes.



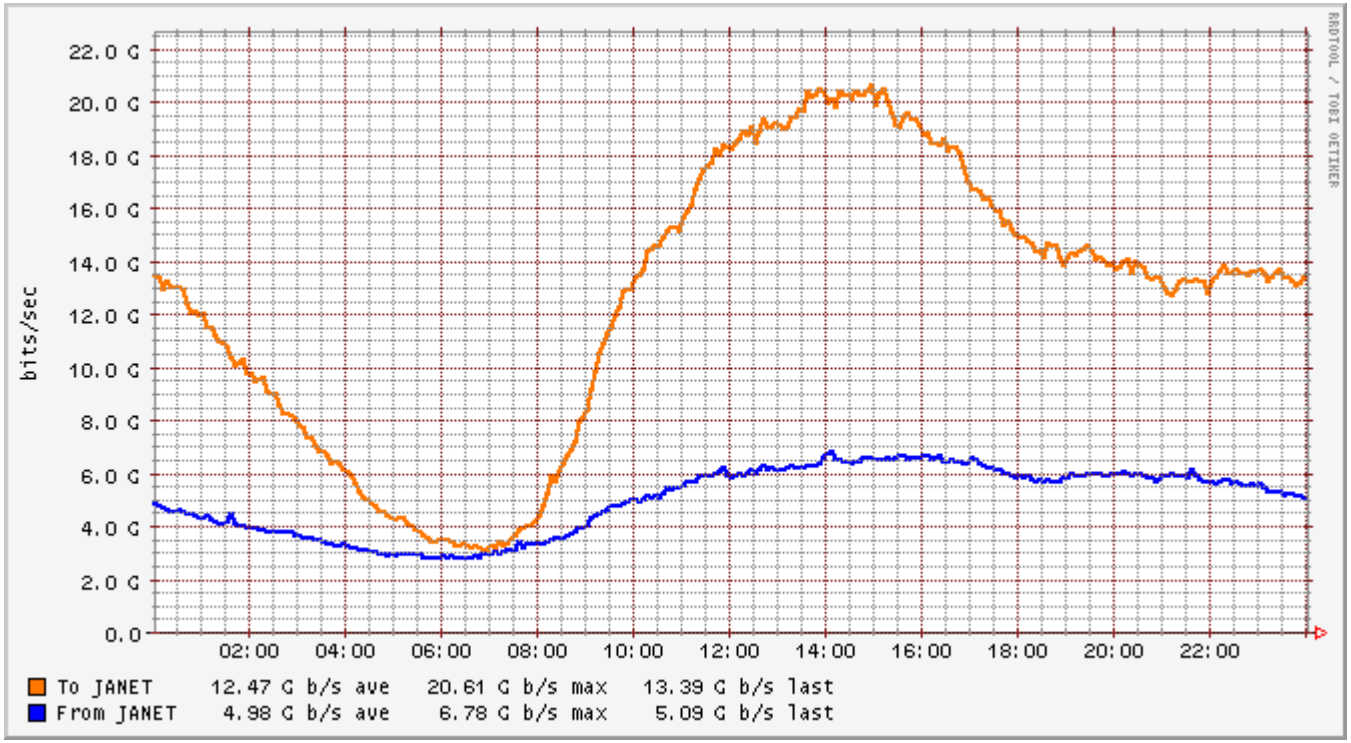
External Connectivity

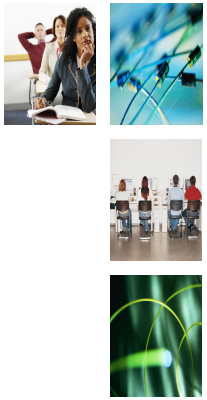
- Multiple transit providers in each location
- Different IXP LANs
- Private peerings in both locations
- Primary and backup GEANT connections spread over the two sites

Thursday, May 18th, 2006



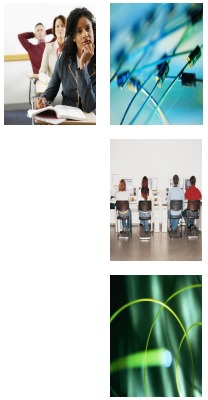
Thursday, May 17th, 2007





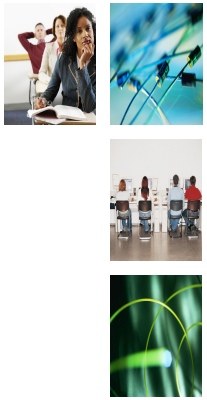
Operations

- Historically subcontracted to external party
  - University of London Computer Centre
    - If you look out the window on the left-hand side...
- In-house as of January 1st, 2007.
  - Reduce risk
- Still based in London
  - Main JANET office is near Oxford
  - but...



Operations

- Just built a new Network Operations Centre
  - Redundant access circuits to diverse backbone PoPs
  - UPS & Diesel generator
    - >20 hours before refuelling
- Second emergency NOC across river
  - Different electrical supplies, access circuits, etc.
- Service Desk phone number can be directed to Oxford or London as needed



Some statistics

- 5,851 Km of dark fibre
- 90 circuits (60 at 10Gbit/s)
- 112 sites housing optical equipment
- Longest unregenerated link: 554 Km
- Longest single span: 243.6 Km, 51.2 dB loss




Still one problem to solve

- Operator error
- ...but we have a solution for that too...




- Questions?