A Distributed, Robust Network Architecture Built on an Ensemble of Open-Source Firewall-Routers

Dr Simon A. Boggis
<s.a.boggis@qmul.ac.uk>

IT Services,
Queen Mary, University of London

JANET Networkshop 38, Manchester, 2010

Queen Mary
University of London

Outline

Queen Mary University of London

Queen Mary, University of London

- Research-focused higher education institution.
- Four main campuses in London.
- 21 academic departments.
- 15000 post- and undergraduate students.
- 3000 staff.

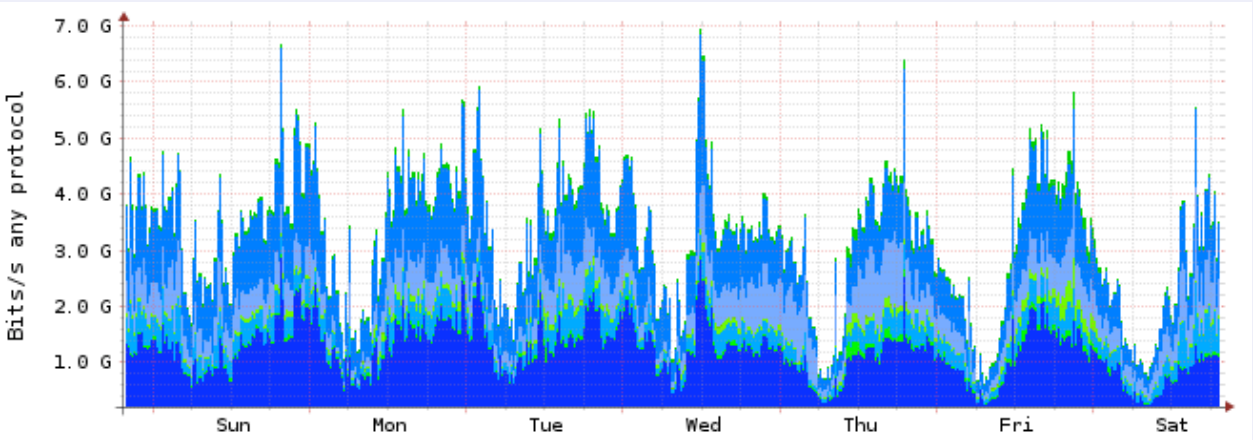
<http://www.qmul.ac.uk>

Queen Mary
University of London

Traffic (March 2010)

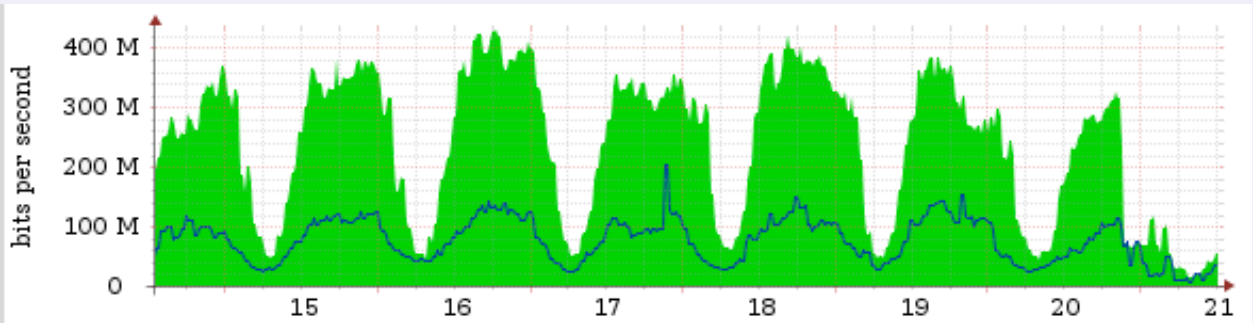
Peak Internal Traffic

- 7Gbit/s
- 1.1M packet/s.



Peak External Traffic

- 500Mbit/s in.
- 200Mbit/s out.
- 100k packet/s.



Queen Mary University of London

Philosophy

IT Environment

- IT highly devolved to departments:
  - Variable levels of provision and support.
  - Diverse, heterogeneous clients and systems.
- College network was segmented and distributed:
  - Many logical/administrative boundaries (ca. 350 IP networks).
  - Logical units span physical locations.
  - Desire to avoid constraining planners (+ 802.1x benefit).

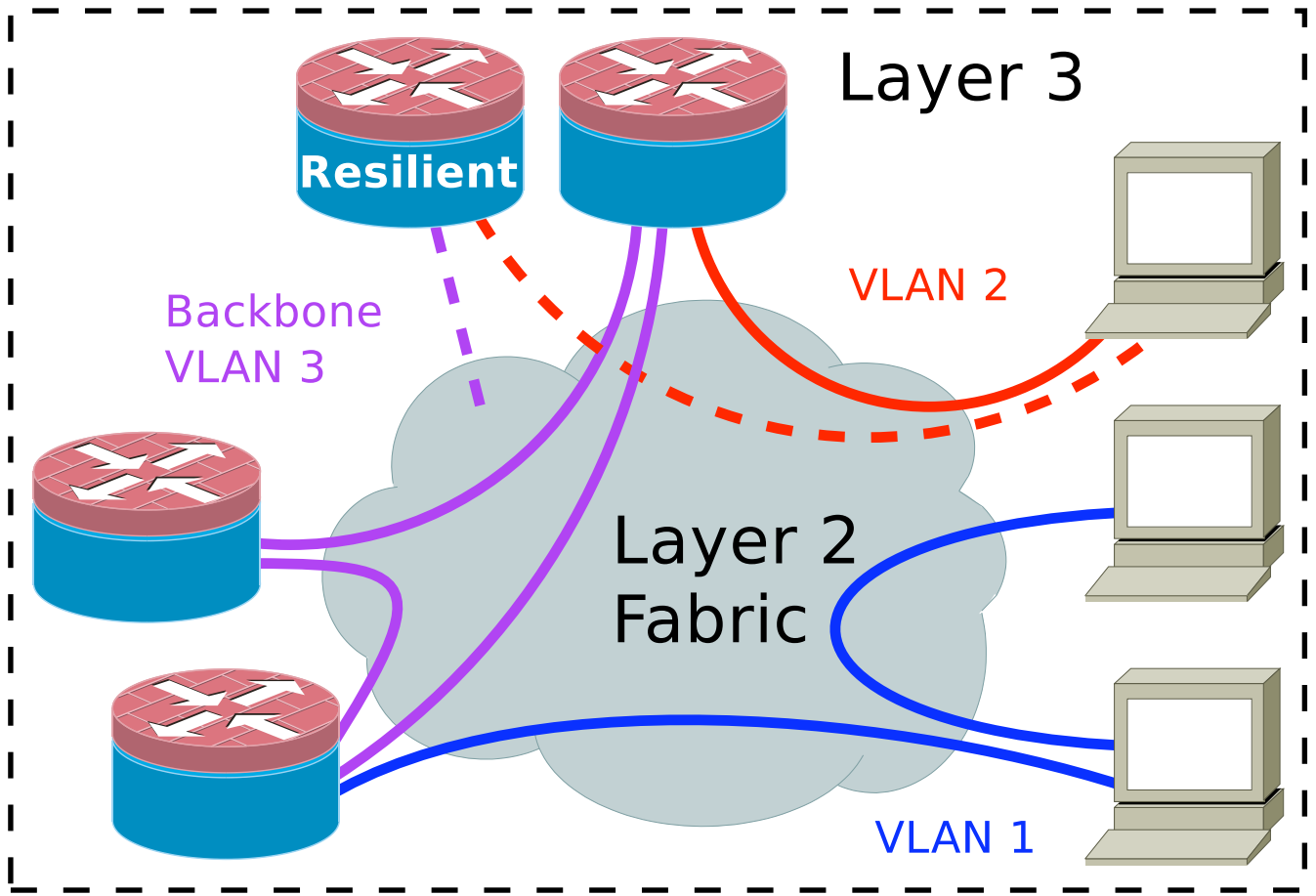
Requirements

- Avoid being forced into unwanted centralisation.
- Scalable, high-performance, robust, resilient and modest cost.

Queen Mary University of London

Factorised, Distributed Network

- Resilient layer 2 fabric: *switches and links*.
- Parallel layer 3 *firewall/routers*.



Queen Mary
University of London

Distributed, Resilient Layer 2 Fabric

Distributed

- Core switches distributed across sites.
- Workload distributed over multiple switches.
- High performance.

Resilient

- Modular switches with internal redundancy.
- Resilient physical links with diverse routing.
- "Instant" link/node failover (IP telephony!).
- Distribution layer LACP trunks.

Queen Mary University of London

Distributed, Parallel Firewall-Routers

Distributed

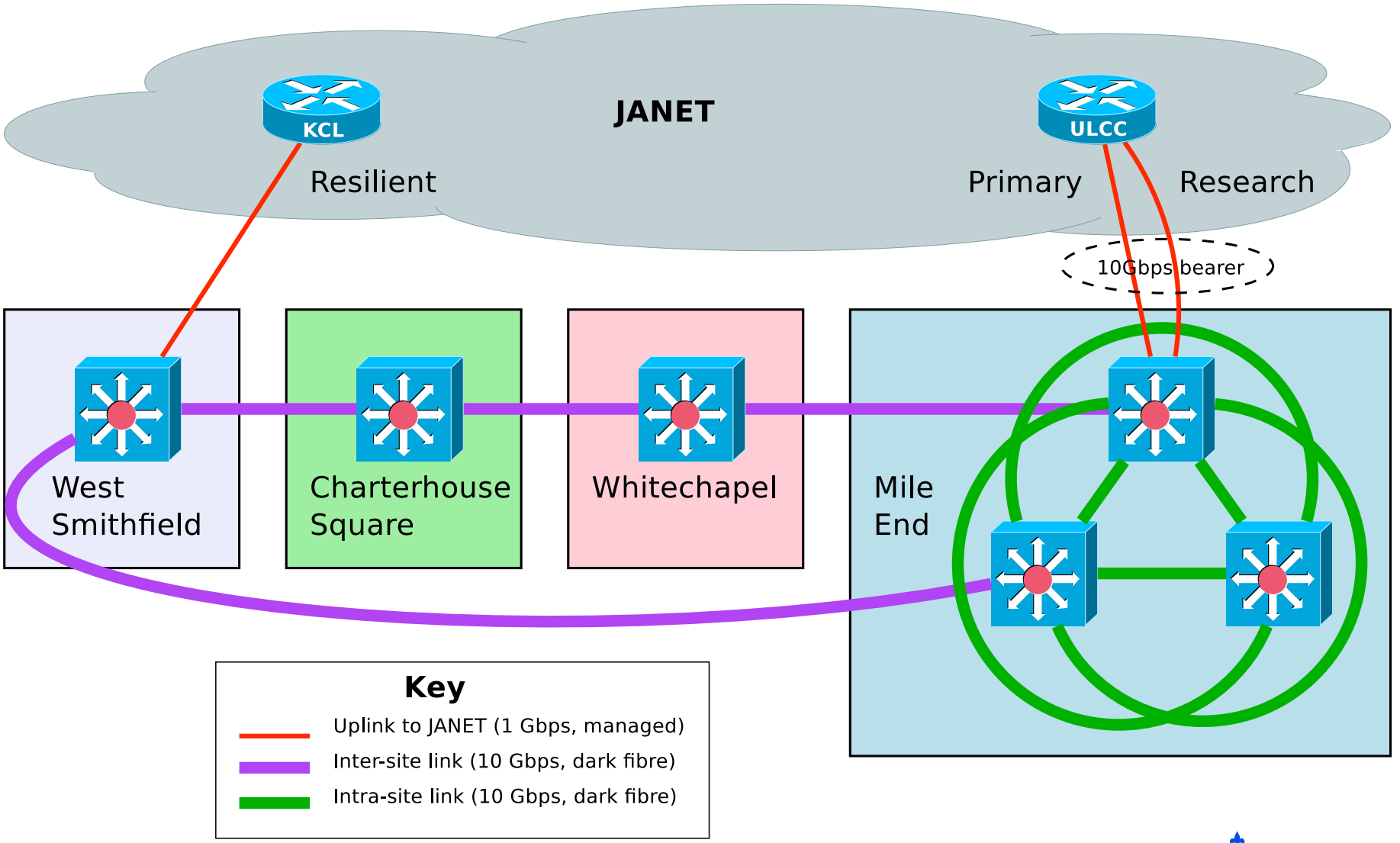
- No single points of failure.
- Workload division = problem isolation.
- Self-contained, independent and robust: graceful failure modes.
- Efficient: filter and traffic-shape near edge.
- More traffic on switches, but bandwidth cheap.

Parallel

- High performance, low cost.
- Easy to scale - just add more.
- Resilience: multiple identical, redundant routers.

Queen Mary University of London

Layer 2 Fabric



Queen Mary University of London

Open-Source PC Firewall-Router Platform

Commodity Hardware:

- Commodity 2U server class PCs.
- 8 Core 3GHz Intel CPU, 4GiB RAM.
- 4 x 1Gbit/s Intel E1000 NIC.
- Remote OOB management (IPMI).
- Redundant power supplies, fans, disks.

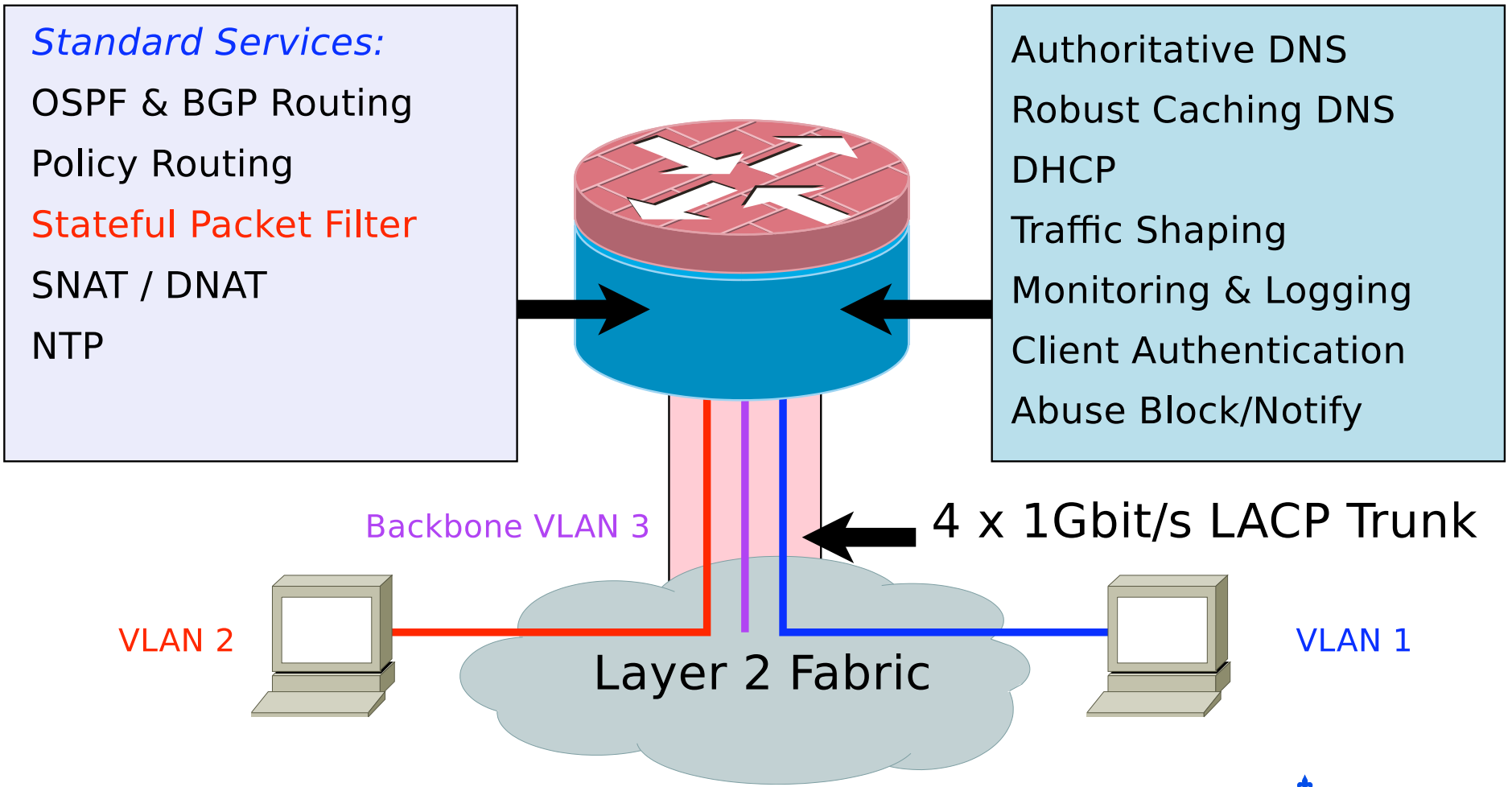
Open-Source Operating System and Software:

- OS: Debian GNU/Linux 5.0 "Lenny".
- Quagga Routing Suite, Netfilter and iproute2.
- DJB DNS, ISC dhcpd, NTPv4 and apache.

Queen Mary University of London

An Open-Source PC Firewall-Router

Self-contained, independent and robust.



Queen Mary University of London

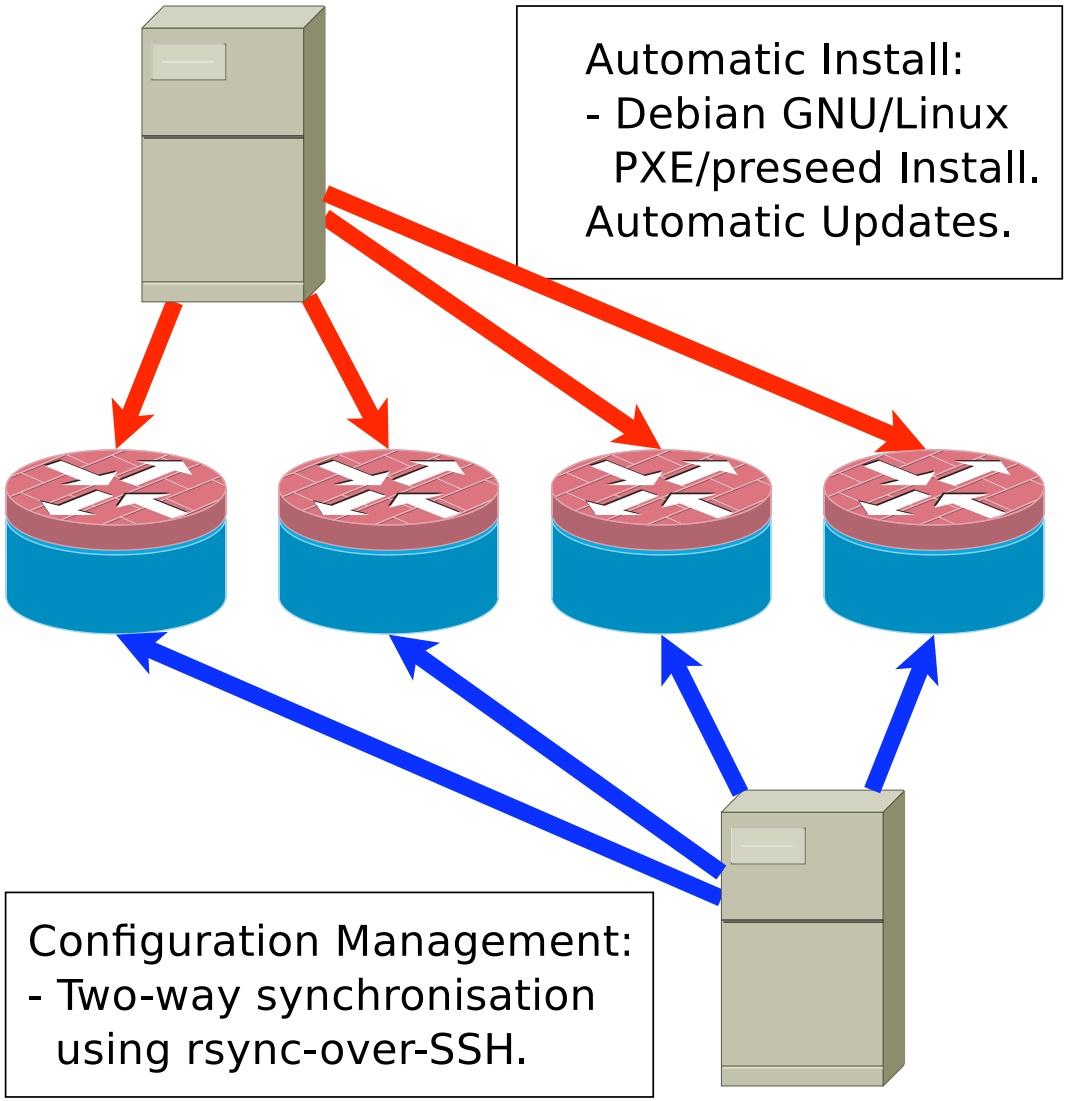
Self-Contained Firewall-Router Services

- *Full* state-tracking firewall.
- Authoritative DNS, Robust Caching DNS:
  - nearest answer, short-circuit delegation.
- DHCP, radvd or DHCPv6 (if you prefer).
- Traffic shaping (xmit), scheduling, policing (recv):
  - Linux tc (HTB + SFQ).
- Monitoring & Logging:
  - libpcap, state-tracking, ARP, IPv6 ND.
- Client Authentication, Abuse block/notify:
  - Netfilter DNAT + ipt_recent and apache mod_rewrite.

All of the above benefit from:
Flexible central control/configuration mechanisms.

Queen Mary University of London

Firewall-Router Management



Installation System

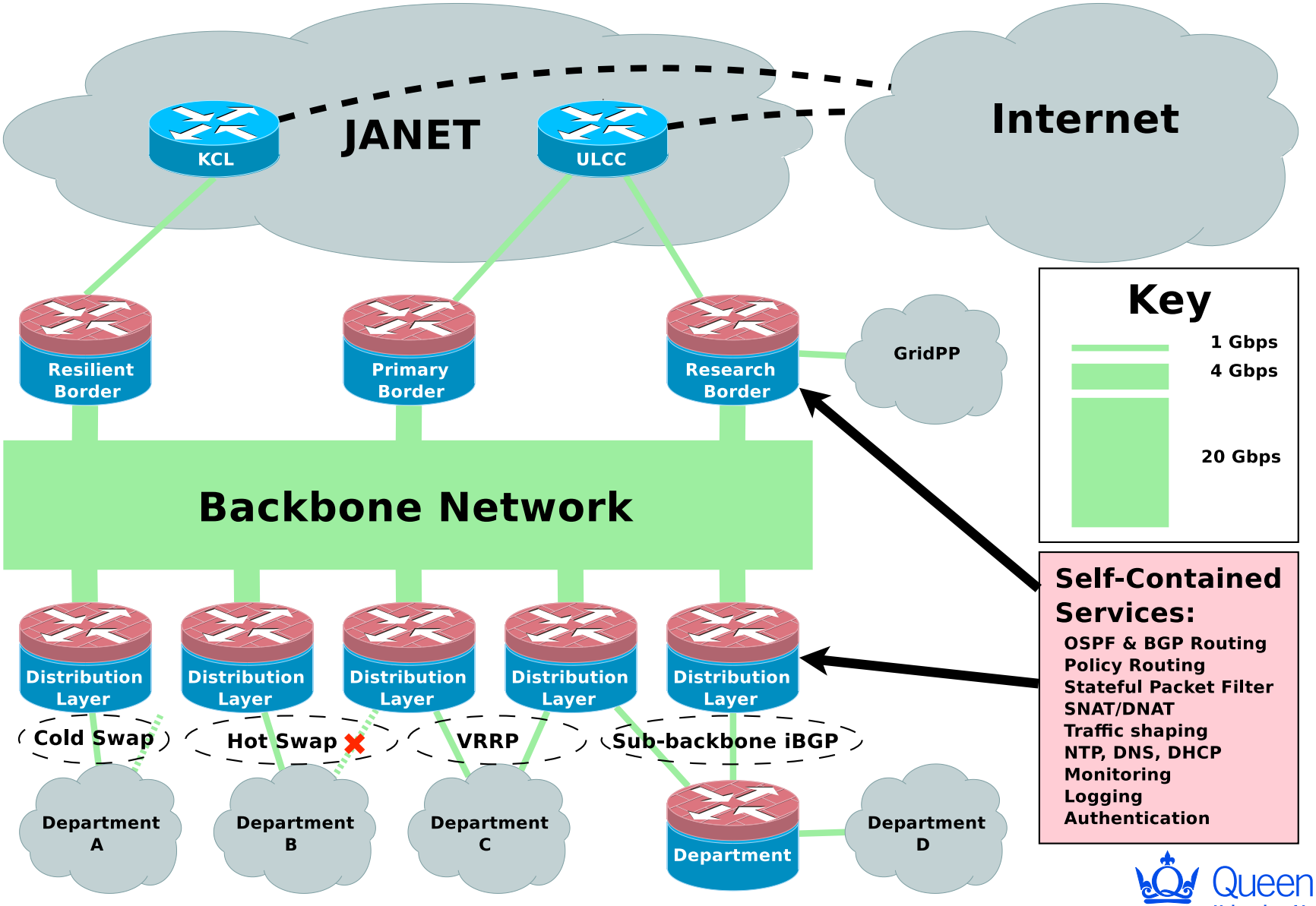
- Interchangeable Hardware.
- Easy "canned" setups.
- Remote operation.
- Automatic - 5 minutes.

Configuration System

- Shared, hierarchical.
- Autogeneration.
- Two-way sync.
- Versioned (subversion).

Queen Mary University of London

Implementation Overview



Queen Mary University of London

Firewall-Router Performance

- Intel E1000 NIC: in theory 800k packets/s, seen ca. 650k packet/s.

NIC Interrupt Mitigation is Essential:

- Operating system support for intelligent interrupt handling.
- Transition from interrupt to polling operation as load increases.
  - Linux kernel newer than 2.6.18.
  - "New" API network driver to support autotuning.

Linux System Configuration:

- Increase RX/TX ring buffers to maximum (256 $\Rightarrow$ 4096).
- CPU affinity helps - dedicated CPU per NIC.

Queen Mary University of London

Open-Source vs. Proprietary Software

Features

- Leading/bleeding-edge functionality: earlier (e.g. state-tracking).
- Usually wider, richer range of features.
- Excellent documentation and support: can talk to developers.

Flexible and Adaptable

- Sophisticated, flexible control mechanisms.
- Interoperability: open-standards.
- Easy to modify to deal with changing requirements.
- Ability to fully investigate and fix problems yourself:
  - Commercial big names can be unresponsive to small customers.
  - Highly skilled staff required to take full advantage.

Queen Mary University of London

Firewall-Router: PC vs. Commercial Appliance

Open-Source PC Firewall-Router

- Low-cost incremental upgrades (£2k).
- Advanced facilities at low performance overhead.
- Network services self-contained on router.
- Sophisticated diagnosis capabilities.
- Frequent small updates (fewer than desktop system).
- Easy to automate.

Commercial Appliance

- Upgrades in larger chunks (£40k).
- Use of advanced facilities can degrade performance.
- Additional network service appliances required.
- Limited diagnosis capabilities.
- Infrequent, large updates.
- Harder to automate effectively.

Queen Mary University of London

Whole Solution: PC vs. Commercial Appliances

Open-Source PC Firewall-Routers

- Modest cost: <£20k for 10 (non-resilient).
- Model matches distributed nature of network.
- Install/management system: economies of scale.
- Specialist skilled staff required.
- Can be harder to buy-in services: this is changing.

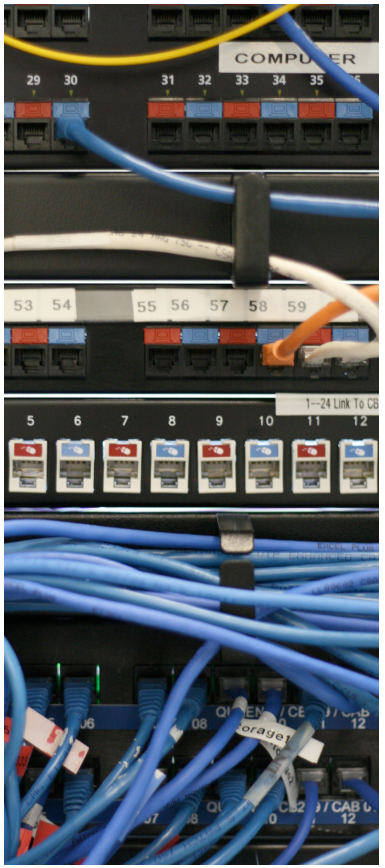
Commercial Appliances

- Expensive: £160k for 4 routers (non-resilient) + support appliances.
- High unit-cost drives artificial centralisation.
- Discrete functions on multiple appliances (management?).
- Can be "run" by more general staff . . . + consultants.

Conclusion

Open-source PC Firewall-Routers

- Good match for the nature of the network and requirements of a medium-large institution.
- Valuable flexibility and adaptability.
- Performance and resilience at modest cost.



Queen Mary University of London

Current and Future Developments

Roll-out of automatic failover to Departments:

- VRRP / keepalived / CARP.
- BGP routing.

Split multi-link trunking (IEEE 802.3ad):

Servers and distribution-layer switches not dependent upon single uplink switch.

Queen Mary University of London

Acknowledgements

IT Services Colleagues:

- John Cobb
- David Pick
- Tavinder Jandu
- Jeff Fern
- Jaspal Sura

Queen Mary University of London

Questions?

Queen Mary
University of London