Network Equipment and Interconnectivity Guide

Revision: 1.6a
Date: 12th March 2012
## Version Control

<table>
<thead>
<tr>
<th>Ver</th>
<th>Date</th>
<th>Who</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>14 December 2011</td>
<td>JRM</td>
<td>Document created</td>
</tr>
<tr>
<td>1.4</td>
<td>17 January 2012</td>
<td>JRM</td>
<td>Core/FM/Edge/Wifi specified</td>
</tr>
<tr>
<td>1.4</td>
<td>18 January 2012</td>
<td>JRM</td>
<td>PNT amendments</td>
</tr>
<tr>
<td>1.4</td>
<td>18 January 2012</td>
<td>PNT</td>
<td>PNT amendments</td>
</tr>
<tr>
<td>1.4</td>
<td>19 January 2012</td>
<td>JRM</td>
<td>Fix testing and documentation</td>
</tr>
<tr>
<td>1.5</td>
<td>02 February 2012</td>
<td>RPS</td>
<td>Added consultant’s comments</td>
</tr>
<tr>
<td>1.6</td>
<td>06 February 2012</td>
<td>PNT</td>
<td>Minor amendments and additions</td>
</tr>
<tr>
<td>1.6a</td>
<td>12 March 2012</td>
<td>PNT</td>
<td>Minor amendments</td>
</tr>
</tbody>
</table>
1 Networking Equipment Guide – Outline

1.1 Purpose of this document
This document forms the basis of the requirements specification to be used in all new projects where any aspects of IT networking are involved, including, but not limited to, provision of wiring centres, ducts, inter- and intra-building connectivity, active and passive equipment, security, authentication, and data-related services.

Within this document, the term Specification refers to the most recent version of the University of York IT Services Network Infrastructure Specification, which form a part of this requirement.

The basic principle is that sufficient provision will be made for a secure, pervasive, highly resilient and easily managed data network, capable of meeting all of the University’s requirements for a “converged” network system. This network system is required to carry CCTV, Access Control, Building and Energy Management (BEMS), IP Telephony (IPT, VoIP), and Electronic Point of Sale (EPoS) traffic in a secure and reliable fashion and in accordance with any statutory or industry requirements, separately from student traffic, and separately from research and administrative traffic. At present, this is achieved using separate OSPF routing meshes for the networks.

To this end, it is a requirement of any network infrastructure designed or installed for the University, whether including active components or not, that it be capable of management and monitoring in detail by the University of York IT Services / Information Directorate Network Group. In recent years the Network Group has made a large investment in developing management and monitoring systems, and any network provision must be fully compatible with these requirements.

One of the essential features of the University network is the combination of the “one port fits all” concept in conjunction with flood patching. This allows the deployment and movement of many types of network-attached device with minimal intervention, dramatically reducing the resource required to deal with moves, adds, and changes.

At the time of writing the University network has approximately 900 Ethernet switches of various ages, providing approximately 30,000 edge ports in over 200 wiring centres. As wiring centres have, on average, one switch that can only be half-utilised (due to the inevitable difference in numbers between installed data outlets and available ports on a switch), one would expect at least 4800 ports to be unused. In fact there are over 25,000 devices registered for use on the network, some of which have multiple interfaces, so it can be seen that there is only a small overprovision. The initial capital cost of flood patching is quickly offset by the reduction in the technical staff costs that would otherwise be required.

Any network solution must therefore adopt the same flood-patched universal “one port fits all” regime.

It is recommended that this document be read in conjunction with the latest version of the IT Services Network Infrastructure Specification, copies of which are available on request.
2 Network Infrastructure requirement for new builds

2.1 Ducting and Fibre

All new builds including Heslington East New Goodricke and Heslington East Cluster I have multiple ducting and fibre routes into every building allowing us to build a resilient Network architecture. Designed into each major build area e.g. Cluster I or Cluster II are at least two networking “distribution” points – typically part of a Data Centre, PABX telephone room or built onto an electrical substation. These distribution points will be the focal point for ducting and fibres within each area with onward connectivity to other areas e.g. in Cluster I, S2 PBX connects to the northern Heslington East combined utilities corridor, TFTA connects to the southern Heslington East combined utilities corridor, and these two locations connect eastwards to substations LTA/SUB and LBR/SUB.

The Combined Utilities Corridor (CUC) uses Em_telle’s heavy duty 14/10mm microducts (Product code 8506) tie-wrapped in a 7 way bundle as specified in the IT Services Network Infrastructure Specification, Appendix 4. Each microduct in the bundle has a different colour.

2.1.1 Example Fibre Interconnects – Cluster I

Illustrated here are all the major wiring centres for the Heslington East Cluster I buildings as well as Cluster I distribution points TFTA (Data Centre) and S2 PABX (GNU/SUB Telephone Exchange). Inter-building links on Cluster 1 will typically use the 7 way variant of Em_telle’s Direct Install product (Product code 6438) which uses 5/3.5mm microducts.

Figure 1: Example of blown-fibre interconnection
2.2  Network Topology

Any active network and ancillary equipment, including but not limited to Ethernet switches, routers, media converters, storage devices, firewalls and wireless equipment, shall be of a type approved by IT Services / Information Directorate as these devices must integrate with existing infrastructure. Ethernet routing devices, Ethernet switches, WAPs, firewalls, etc must be capable of management from a command line accessible by serial port, SSH and by the SNMP protocol, and must not rely on menu-driven or web-based methods. To avoid congestion, the industry-standard general principle that all feed ports shall be of several times (normally ten times) the capacity of the ports they feed shall be adhered to.

IP addresses, both “public” (owned by or allocated to the University of York or its partner organisations) and “private” (RFC 1918 and RFC 3330/5735) and VLAN IDs must be allocated by the IT Services / Information Directorate Network Group. Other IP addresses, ie any not controlled by IT Services / Information Directorate and not part of an allocated “private” range, are not permitted. Use of NAT (network address translation) is not permitted. All devices connected to the network must be registered in the Information Directorate LAN database before commissioning them on the network.

Contractors must request the registration of devices and allocation of IP addresses via a web form. The application form and explanatory notes are accessible at the “Information for Contractors” webpage at http://www.york.ac.uk/it-services/info/contractors/. The form requires a username and password, which is allocated on a one-per-company basis, and there is a link on the explanatory notes web page which may be used to request this.

The developer will allow for the University of York IT Services / Information Directorate to design the network architecture and to prepare suitable kits lists, fibre connectivity diagrams, rack layouts for provision as part of their contract. The IT Services department will also provide configuration files for approved devices ready for procurement from and installation by University preferred data equipment vendors with the final commissioning and connection to the campus Network by University of York IT Services staff. To be able to do this IT Services require data outlet port counts along with drawn up diagrams showing positions of data outlets – particularly showing the location of Wireless Access Points, Access Control, EPoS and BEMS devices.

Where rack space to house third-party equipment is required in IT Services data racks the space allocation will be carried out and documented by the University of York IT Services.

2.2.1 Edge Network

Any new developments edge network must utilise the latest type of the following device/devices.

The edge network is based around the HP Procurve 2620 range (or its successor) of 48 port 10/100 Power Over Ethernet (PoE) switches for most applications and the HP Procurve 2910 range (or its successor) of 48 port 10/100/1000 PoE switches where higher performance is required e.g. specialist labs. All wiring centre outlets should be flood patched whether required or not. The switches will be configured to support the Universities “One Port Fits All” architecture allowing simple, safe and seamless connection of devices, whether that be a door lock, till or a high performance user device.
Ethernet switches, including routing devices, must support, as a minimum, the following features and protocols:

- At least 48 x autosensing 10/100Mb/s RJ45 ports (this restriction may be relaxed for devices serving a purely Layer 3 routing function and equipped with more than 24 optical ports)
- RS232-compatible serial console port
- 802.1p Class of Service and traffic prioritisation with at least 4 queues
- 802.1Q VLANs, at least 64 per device
- multiple subnets
- CIDR
- LLDP
- LLDP-MED
- Voice VLANs
- 802.3af PoE or 802.3at PoE+
- pre-standard PoE support
- configurable Auto-MDIX
- At least two Gigabit optical ports using SX and LX SFP transceivers
- RADIUS authentication and accounting
- Multilink trunking (supporting both LACP and manual configuration)
- IGMP snooping
- 802.1X authentication, with multiple 802.1X users per port
- MAC address-based port authentication to RADIUS
- Multiple authentication methods per port
- VLAN allocation per port by RADIUS
- MAC address limiting
- MAC address lockout
- Source-port filtering
- Configurable logging using SYSLOG
- SNTP
- SNMP v3
- RMON
- SFLOW
- Availability of all relevant standard and proprietary MIBs
- Port monitoring, including remote port monitoring
- Port mirroring
- DHCP snooping with DHCP protection
- Broadcast limiting
- rate limiting
- 802.1s multiple (per-VLAN) Spanning Tree Protocol
- software/firmware updates available for a minimum of 5 years
- command line interface
- SSHv2
- TFTP file transfer
- Secure FTP (SFTP) file transfer
- Dual flash images for firmware and configuration files
- Flexible mounting options including standard 19" rack mounting

Switches supporting Gigabit RJ45 ports must additionally support:

- At least 24 x autosensing 10/100/1000Mb/s RJ45 ports
- At least two (and normally four) 10G optical ports using SR and LR SFP+ transceivers
2.2.2 The Core Data Network

Any new developments Core data network must utilise the latest type of the following device/devices.

The core/distribution data network will be configured as an OSPF mesh based around the 
**HP Procurve 5400zl range (or its successor)** of modular switch routers housed within Data Centres, Substations or major wiring centres with multiple 10Gbit/s diversely routed uplinks.

- Ethernet routing devices must support, in addition to all of the above, the following:
  - IPv4 Layer 3 routing
  - IPv6 Layer 3 routing
  - RIP, RIP2 and OSPF3 routing protocols
  - static routes
  - multinetting
  - per-VLAN DHCP forwarding to multiple destinations
  - flow control
  - ACLs (access control lists)
  - IP address lockout
  - VRRP (Virtual Router Redundancy Protocol)
  - IGMP
  - MLD (Multicast Listener Discovery)
  - PIM sparse and dense modes
  - At least four optical ports using SR and LR SFP+ transceivers

- In certain locations, Ethernet routing devices must also support:
  - MPLS

2.2.3 Core FM Network

Any new developments Core FM network must utilise the latest type of the following device/devices.

The FM network is also based around the **HP Procurve 5400zl (or its successor)** range of modular switch routers housed within distribution centres (substations/PABX etc). These separately feed into edge switches giving out-of-band, resilient and compliant Facilities Management networking to support an ever increasing list of FM devices (IP Telephony, CCTV, Access Control, EPoS, eSuds, Alarm panels, BEMS, ...). There are also separate fibre feeds from each relevant substation to support car park barriers & associated devices.

2.2.4 Wireless

All buildings should have an internal data infrastructure to support pervasive internal wireless coverage and additional outlets and ducting to facilitate external Wireless Access Points where appropriate. Currently the Wireless architecture used by the University is by Aruba and supports B, G & N dual-band high density technologies. Any wireless solution must be a centrally managed dual-band thin client wireless solution that does not require VLANs to be presented from the network core directly to individual Wireless Access Points.

- Wireless coverage shall be provided in all communal areas, seminar rooms, lecture theatres, and all study bedrooms.
o Additional provision for wireless coverage shall be made for all office and research areas.
o Provision shall be made for future coverage of outdoor spaces.
o Wireless bandwidth shall be provided using the 2.4GHz band to support 802.11g and 802.11n, and also in the 5GHz band to support 802.11n.
o All wireless connectivity shall be secured by WPA2-Enterprise.
o All wireless access point configuration and management shall be carried out on central controllers.
o All wireless traffic shall be carried on Network Access Service VLANs and subnets local to the access point.
o It shall not be necessary to carry specific VLANs or subnets from the network core to outlying wireless access points; APs shall use local addresses, subnets, and VLANs to communicate with central controllers.
o Wireless APs and their controllers must be capable of management and monitoring by SNMP.
o Wireless controllers (and APs if not “thin” APs) must be capable of management by automatically or semi-automatically run scripts without the use of proprietary software.
o Wireless controllers (and APs if not “thin” APs) must be capable of management from a command line accessible by serial port and by the SSHv2 protocol, and must not rely on menu-driven or web-based methods.
2.3 **Testing and Documentation**

- No part of the network cabling or fibre-optic infrastructure shall be deemed complete or fit for purpose until standards-based test results in the appropriate format are received by IT Services / Information Directorate Network Group.
- No powered device shall be deemed ready for use until it is issued with a PAT certificate provided to the University or has a readily-visible sticker showing the date of testing, renewal date, and the initials or signature of the tester.
- No active device or network segment installed by other than IT Services shall be deemed ready for use until it is capable of being monitored using SNMP by the IT Services / Information Directorate network monitoring system.
Figure 2: Example of network topology in different areas