CONNECTING TO THE COLLEGE NETWORK

Document Id	Connecting to the College Network
Sponsor	Laura Gibbs
Author	Nigel Rata
Date	May 2014

Version Control Log

Version	Date	Change
1.0	25/05/10	Initial draft for review
1.1	6/10/10	Updated
1.2	15/05/2014	Updated

Document Approval

Name	Approval Date
Laura Gibbs	27.5.14
ITUAG	27.5.14

Introduction

The College depends heavily upon its IT network for Research, Teaching and Administrative activities. It is essential that the stability, integrity and security of the College IT network be safeguarded for use by all members of College.

To assist in ensuring the availability of an effective, highly available network and to facilitate the rapid tracking down and resolution of any problems by the IT department, the following policy has constructed.

User Responsibilities

- All users of the network must be aware that they are bound by the RHUL Security Policy, the Conditions of Use of IT Facilities Policy and the JANET Acceptable Use Policy as operated by Janet and JISC.
- All systems connected to the College network must be accurately registered with IT under the terms of IP Allocation and Management Policy. Registrations can be arranged via the IT Service Desk.
- All systems directly connected to the College network must comply with the current technical networking requirements defined in appendix A.
- Custodians must ensure that only authorised College users or properly registered guests have access to the College network from their systems.
- All systems connected to the College network must be configured in accordance with the Information Security Policy.

IT Responsibilities

- All network addresses, including IP addresses, will be allocated and administered under the terms of the IP Allocation and Management Policy.
- Physical connections to the College backbone (central core network) may be made only by IT. No extensions or modifications to the physical infrastructure of the RHUL network, including wireless, may be made without first consulting IT. This includes the addition of network switches, hubs, wireless access points and router devices and cabling other than patch cable to a provided network wall socket. Any network infrastructure equipment or wiring is managed and controlled by IT unless an exemption has been agreed with an individual or department. Staff and students are free to connect computing equipment (e.g. laptops, desktops and printers) to any live network port. Request to make network sockets live should be made via ITservicedesk@rhul.ac.uk.

- IT may, on behalf of the College, and subject to appropriate consultations, restrict excessive use of the backbone bandwidth.

- In the event of unacceptable network events occurring on a LAN, IT may request access to and inspect the configuration of devices or equipment on that network and to request the immediate removal of any devices or equipment that it believes could be the source of the problem.

- In the event of unacceptable events on a LAN causing problems on another part of the College network or on an external network, IT may need to disable any part of the LAN, as necessary, in order to remove the source of the problem. While every effort will be made to contact the system custodian, Head of Department and/or other appropriate persons, this may not always be possible. All services will be reconnected at the first opportunity.

- Failure to comply with the rules for connection to the College network may result in immediate disconnection from the network.

- To proactively protect the security and operation of the network and the systems thereon, IT may carry out both manual and automated systematic vulnerability scans on computer systems connected to the College network. Best efforts will be undertaken to minimize any disruption, but in the unlikely event of such a scan causing problems, IT does not accept responsibility for any loss of availability or data. Where possible, advanced warning will be given. Individuals or departments may request from IT that certain computer equipment be exempt from these scans, this should be done in conjunction with appropriate evidence that the device is secure.

Appendix A – Guidelines and Rules for connection to the RHUL network.

This document presents a set of rules of operation that must be obeyed and limitations of service provision that must be accepted when a device is connected to the RHUL network. Failure to comply will result in disconnection or other form of restriction of the device by IT without warning.

The "RHUL network" is the data communications network in RHUL that is owned by RHUL and maintained on its behalf by IT. A device is considered to be connected when it is able to transmit packets to or receive them from the RHUL network, or cause them to be transmitted or received on its behalf by any sort of proxy (including a NAT system (Network Address Translation)). A device is not connected when it is isolated from the RHUL network, either by a gap in the transmission medium or by an intervening device that completely prevents packets being transmitted to the RHUL network or received from it.

1. The RHUL network is owned by RHUL. It is maintained by IT.
2. A device connected to the RHUL network must be accurately registered with IT. Where appropriates DHCP (Dynamic Host Configuration Protocol) should be used to set the IP address and other address-related parameters.
3. No extensions or modifications to the physical infrastructure of the RHUL network, including wireless, may be made without first consulting with and obtaining permission from IT. This includes the addition of switch, hub, wireless access point and router devices and cabling other than a patch cable to a provided RHUL network wall socket.
4. Installation of a modem on a device connected to the RHUL network, or the establishing of any other means of access from external networks, is not permitted. This presents a security risk, providing an uncontrolled access path to the RHUL network. A connected device must not transmit or receive network traffic that, by its rate or type, is illegal, disruptive or has a serious adverse impact on users of the RHUL network or other, external networks. IP multicast traffic must not be transmitted on parts of the RHUL network that have not been enabled by IT to support it because it may be flooded to all devices on the local network. A requirement for the use of IP multicast should be discussed with IT.
5. If a device is connected to more than one part of the RHUL network at the same time it must not forward packets (or perform bridging) between its network interfaces, unless it has been agreed wit IT that it can perform this function.
6. Using the source IP address of an IP packet on the RHUL network, IT must be able to quickly and easily identify and locate the connected device that initiated the traffic.

7. Use of NAT (Network Address Translation) is discouraged. If devices are connected using a NAT system the NAT scheme must be one-to-one, i.e. a particular outside (public) IP address must always map uniquely to the same inside (private) IP address so that the true origin of traffic through the NAT system can be identified. The maintainer of the NAT system must be able to provide this mapping information to IT.

8. A device connected to the RHUL network must not provide a DHCP server. The only DHCP servers available to hosts on the RHUL network must be those of the central IT DHCP service.

9. The only network layer protocol supported is IP.

10. IP addresses should not be regarded as immutable and on occasion a device may be required to change IP address. Hostnames rather than IP addresses should be used in applications to avoid the operational impact of such changes.

11. RHUL network equipment will not perform proxy-arp or other techniques to transparently compensate for the misconfiguration of IP address and related parameters. A device must have the correct configuration of IP address, netmask, broadcast address and default gateway.

12. The RHUL network routers do not supply or accept routing information (including the default route), in any routing protocol, to devices other than themselves. A device connected to the RHUL network should not rely on a routing protocol, or a router discovery protocol, to learn the default gateway. It should use DHCP to acquire the default gateway automatically.

13. The IEEE 802.11 wireless component of the RHUL network can only be provided reliably in areas where it is free from radio interference.