PU, RCHT CONNECTIVITY PROJECT – EDUROAM WIRELESS

1 Summary

eduroam (educational roaming) allows students, researchers and staff from participating institutions to obtain wireless internet connectivity across campus and when visiting other participating institutions. At the PU (Plymouth University) Cornwall campus we have extended the availability of the eduroam service to include the RCHT (Royal Cornwall Hospital Trust) buildings. This allows our staff, students and research staff to obtain wireless internet connectivity on laptop and mobile devices from anywhere on the RCHT site using their Plymouth University login credentials.

2 Product Description

To rollout eduroam Wireless internet across the RCHT (Royal Cornwall Hospital) site for PCMD (Peninsula College of Medicine and Dentistry) / FoH (Faculty of Health) PU staff, students and research staff.

3 Background - RCHT (Royal Cornwall Hospital Trust) University Campus

Plymouth University has an academic campus at RCHT contained within the KSPA (Knowledge Spa) building. Network connectivity to Plymouth University is provided via a wide area network circuit to the RCHT site, see fig 1.0 for a high level illustration of the network topology.

PCMD, FoH and Allied health professional students and staff are based across the RCHT site, the KSPA building is the academic base and clinical placements take place across the RCHT site and community hospitals. The RCHT IT department is called CITS, Cornwall IT Services.

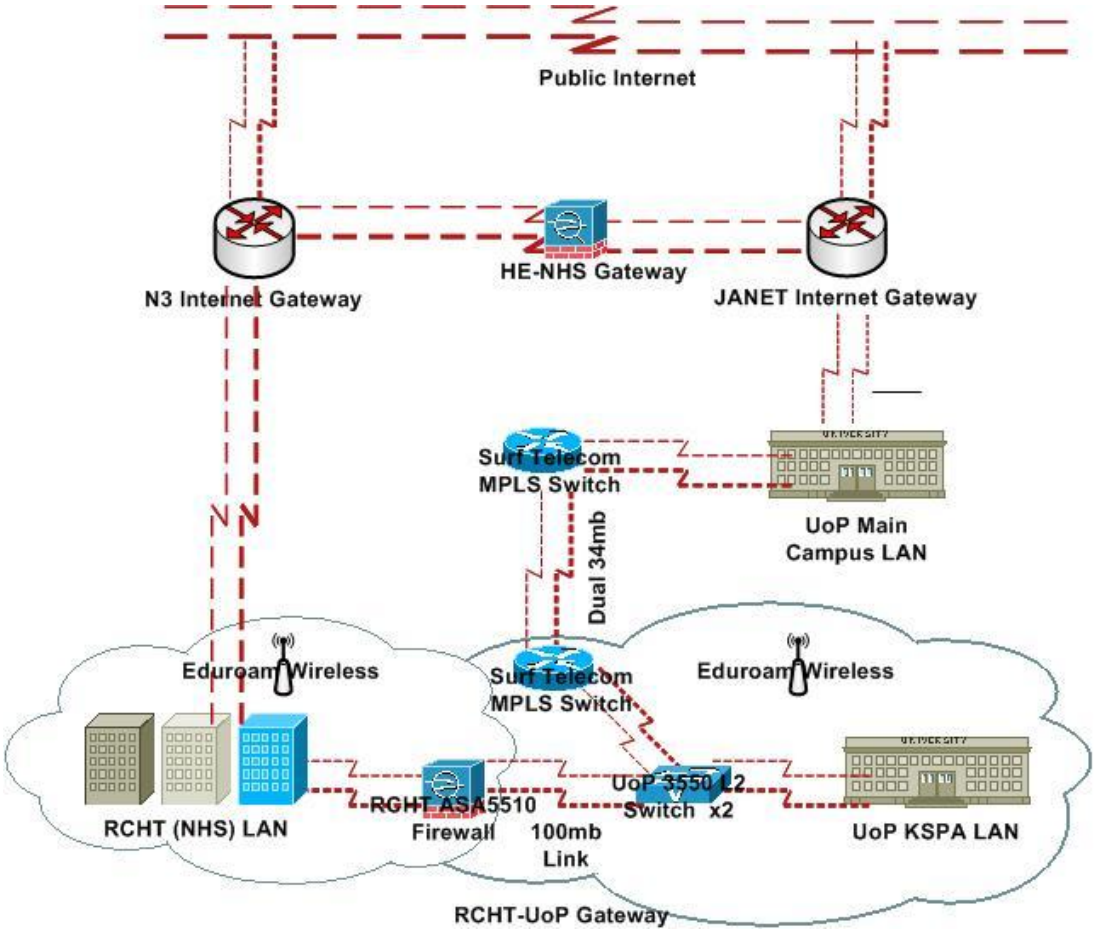

Figure 1.0 UoP & RCHT Connectivity

4 Introduction to eduroam

(ref: www.plymouth.ac.uk/eduroam)

Plymouth University is participating in the **eduroam** wi-fi service. eduroam is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming.

Being part of eduroam allows users visiting another institution connected to eduroam to log on to the wireless LAN using the same credentials(username and password) the user would use if he/she were at his/her home institution.

The **eduroam** federation (www.eduroam.org) spans the UK, 22 other European countries, Australia and Taiwan who have all collaborated to provide international RADIUS proxy authentication facilities.

Plymouth University eduroam service conforms to the JANET JRS Tier 2, as defined in their specification. Users of the eduroam service must connect to the wireless SSID 'eduroam'

In brief, these are the details you will need to use the service. A **laptop computer** or other **mobile device** with either an external or built-in wireless card suitable for use with 802.11g/n wireless networking, and which supports 802.1x authentication.

Setup instructions for connecting to the eduroam wireless network at Plymouth University can be found at http://www.plymouth.ac.uk/.eduroam .

Users of the Eduroam service must comply with Plymouth University's Computing Regulations, (along with some guidance notes), your home institution's Computing Regulations and by the JANET Acceptable Use Policy (to which your institution is a signatory).

5 RCHT Wireless Infrastructure

(ref: Chris Brunt CITS Network & Security IT Engineer)

CITS manage a Cisco Unified Wireless network at the main acute hospital site in Cornwall (Royal Cornwall Hospital) as well as outlying community hospitals and various administrative buildings. The wireless network currently consists of over 940 access points and 20 controllers on 16 sites countywide. It is used by hundreds of users every day.

This network is comprised of the following components:-

1121G, 1142N, 1231G, 1252N and 3502i series access points dependant on location.

3560G/3750G series power over ethernet (PoE) switches.

Wireless Integrated Service Module WLAN controllers (WiSM) in Catalyst 6500 series switches at RCH. Community sites may have integrated 3750G controllers or 5508 series controllers.

Mobility Appliance providing location services (triangulation and context awareness) as well as Wireless Intrusion Prevention/Protection.

Wireless Control System (WCS) Software running on a VMWare Virtual Machine providing centralised management of configuration, reporting, troubleshooting and mapping facilities.

ACS 5.2 Authentication, Authorization and Accounting (AAA) Radius and Tacacs access control servers.

Microsoft Active Directory back-end for user and machine accounts.

We have implemented multiple SSID networks across the network performing different functionality, such as Voice over Wireless LAN, standard data wifi access, Computers on Wheels and guest lobby services. These are tunnelled within the LWAPP (now CAPWAP) protocol back to the controllers, where each SSID has a vlan interface. At this point if required access control lists (ACLs) are applied to restrict traffic, or traffic goes through a firewall. At some remote sites where controllers are not required due to a small deployment of <5 access points. Hybrid Remote Access Point mode is utilised. This only tunnels WLAN control traffic across the WAN, local traffic joins the network at the local switchport. Only WPA2 / AES encryption is permitted.

5.1 EDUROAM SSID Rollout

5.1.1 RCHT Technical Description

eduroam was implemented at RCHT by creating a new SSID, mapping this to a new VLAN interface on the LAN. This vlan is non-routable on the CITS network and uses a private address range. This is connected to the edge firewall between a switchport on the CITS LAN and the UoP/PMS firewall by 100mb ethernet.

The firewall (Cisco ASA 5510) has a DMZ interface configured which connects the eduroam VLAN, and an outside interface connected to the UoP network (100mb), see Fig 1.0. The firewall issues IP addresses to the eduroam clients via a DHCP scope. DNS is provided by the UoP network. NAT is disabled to allow for the private address range to be routed appropriately on the PMS/UoP network.

Clients are authenticated by RADIUS servers on the UoP network, and routing and appropriate ACLs are in place on both sides to allow the wireless lan controllers on the CITS network to connect to the RADIUS servers. This happens via another interface on the firewall, separate to the eduroam traffic.

Wireless LAN clients should pick up the proxy server required for internet access provided 'Automatically detect settings' is enabled in the internet browser. This queries the UoP DNS servers for the wpad entry. Clients are prompted for authentication when using the proxy for internet access so traceability is there if required. See Fig 1.2 for an Illustration of the RCHT Eduroam infrastructure.

5.1.2 UOP Technical Description

(ref: Phil Stevens UoP Network Engineer)

The link between RCHT and UoP connects via ethernet into the UoP cisco 3550, this is a 100Mbps connection between the two organisations, see fig 1.0. The port is configured to be in a Vlan which is configured on two Cisco 4506 multi-layer switches which are located in the KSPA building. The vlan has a private address range, which is advertised into the UoP OSPF routing cloud. There are static routes configured on the two 4506's to route traffic to RCHT, as agreed between the two organisations.

The eduroam traffic, when passed from the NHS firewall, will be subject to an Access Control List (ACL) on the vlan which restricts the traffic passing to and from the vlan. As the traffic for eduroam is filtered by the NHS firewall, the ACL permits all traffic from the eduroam address range. There are also rules in place which permit the radius authentication to take place.

The eduroam address range is also advertised into the UoP OSPF routing cloud, so the traffic will be permitted to traverse Plymouth University network to gain access to internal resources as required.

The eduroam specification dictates the ports and protocols that are required to be permitted from the member institutions. These requirements are defined and permitted through the university firewalls at it's boundary to SWERN and Janet.

However, the addresses provided by the KSPA / RCHT eduroam are private and therefore not routable across the internet. Therefore, just prior to the boundary these private addresses are translated using NAT / PAT to use an address pool of just four addresses that can be routed across the internet.

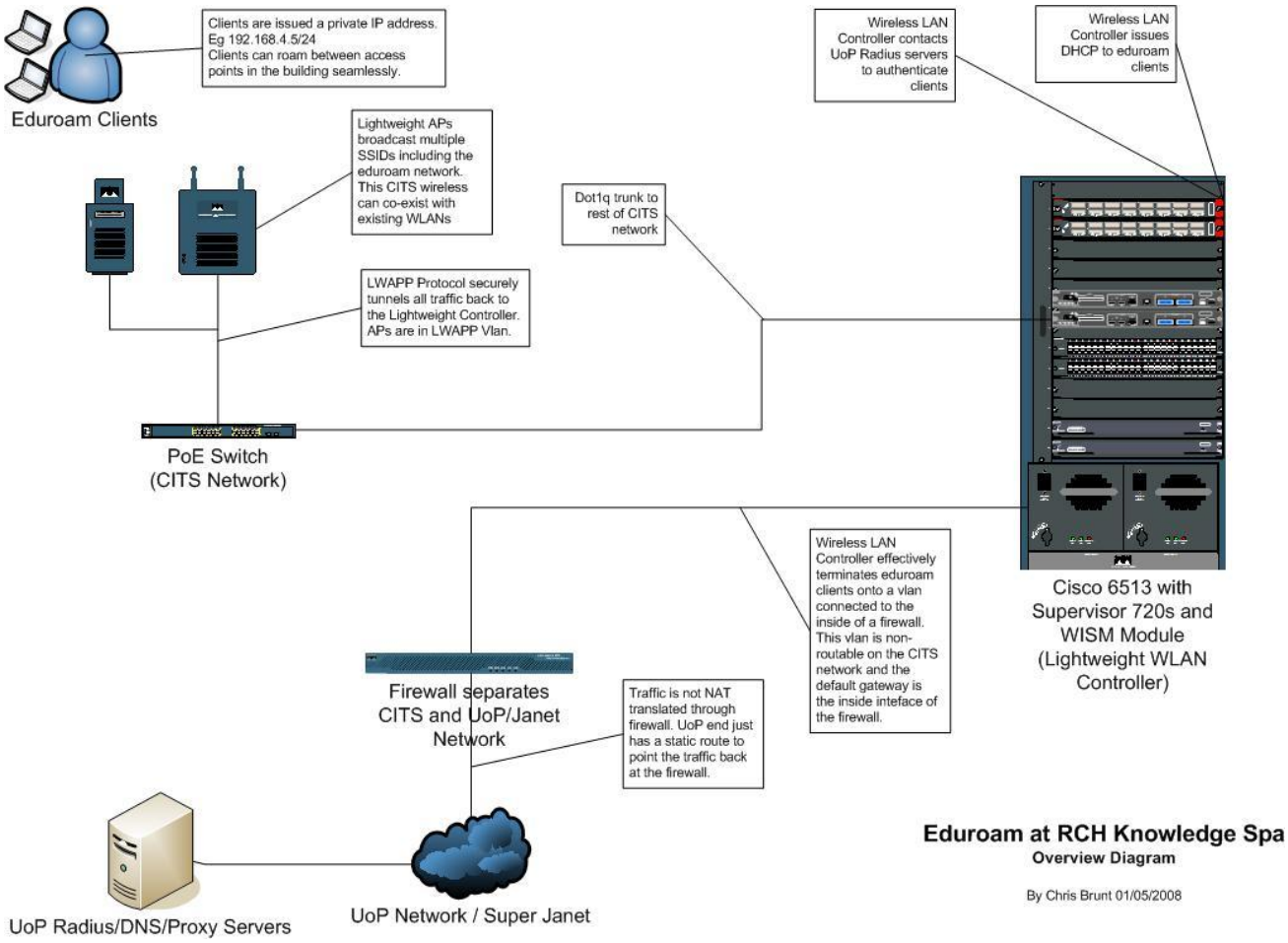

Figure 1.2 RCHT Eduroam Infrastructure

Document Management
Last Edit: 11/11/2011
Version: 0.3
Document author : Joe Grant. jjgrant@plymouth.ac.uk