Oxford University Hospitals NHS

NHS Trust

Wireless access for Oxford University Staff on Oxfordshire NHS sites

Oxon Health Informatics Service (OHIS) – Background and scope.

OHIS design, configure, install and maintain all the network (wired and wireless) for the Oxford University Hospitals NHS Trust (OUH) (previously the Oxford Radcliffe Hospitals – Churchill, John Radcliffe, and Horton General hospitals, and the Nuffield Orthopaedic Centre), Oxfordshire PCT, Oxfordshire Learning Disability Trust (OLDT) and Oxford Health Foundation Trust (previously Oxford and Bucks Mental Health) – with approximately 90 NHS sites spread across Oxfordshire, Buckinghamshire and Wiltshire.

On several of these sites, we have historically worked very closely with Oxford University and often share facilities such as comms rooms, fibre, etc. However we have always maintained a complete separation of the two networks to ensure network integrity\security.

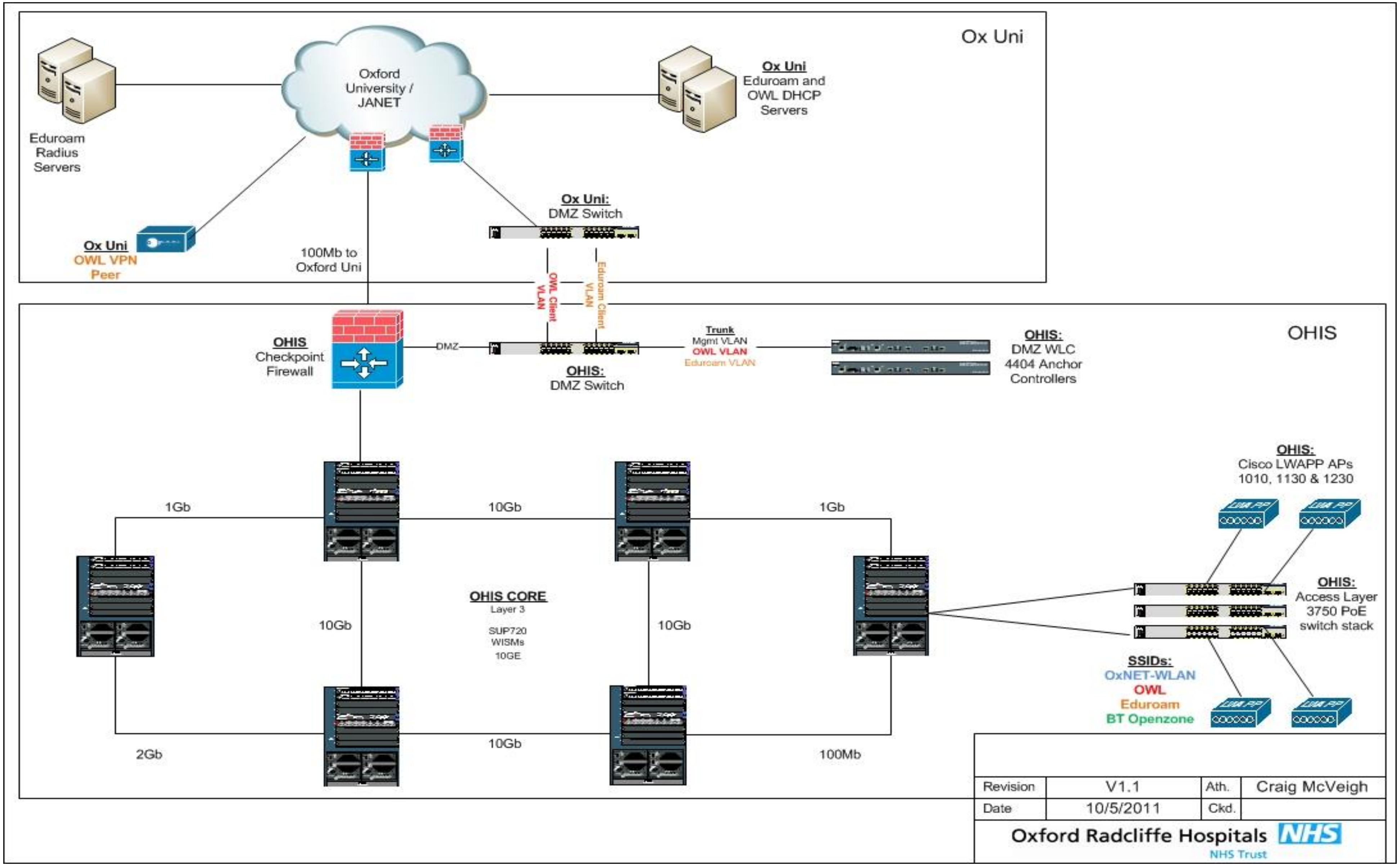
We also have several departments where NHS and University staff overlap\coexist, and so to provide access for University staff to network resources on their network (and vice versa) we have a direct private connection (which is firewalled to permit only required access) to the Oxford University network from one of our Core sites.

We began installing wireless in 2005/2006 at the John Radcliffe Hospital in Oxford using two Cisco 4404 WLCs and 25 Cisco 1200\1010 APs. The demand for wireless quickly grew and we redesigned our wireless infrastructure to allow for future expansion. We therefore installed two Cisco WISMs distributed across two of our Core 6509 switches and implemented Cisco WCS to allow for centralised management.

By 2009 we had installed wireless in every site we supported across Oxfordshire, and had in excess of 1,500 APs. With the increased growth of wireless usage and devices, and with wireless presence across the County, we saw an opportunity to provide better network access on NHS sites for Oxford University staff where Oxford University did not necessarily have a presence.

After discussing and agreeing with Oxford University the finer points such as authentication parameters etc, we designed and installed the below wireless topology (fig:1) so we could provide access to eduroam and Oxford Uni Wireless LAN (OWL) across all our sites.

As of April 1 2011, OHIS now also manage the network and wireless for Oxford Health Foundation Trust in Buckinghamshire and Wiltshire.



Ox Uni
Oxford University / JANET
Eduroam Radius Servers
Ox Uni Eduroam and OWL DHCP Servers
Ox Uni OWL VPN Peer
100Mb to Oxford Uni
Ox Uni: DMZ Switch
OWL Client VLAN
Eduroam Client VLAN
OHIS
OHIS Checkpoint Firewall
DMZ
OHIS: DMZ Switch
Trunk
Mgmt VLAN
OWL VLAN
Eduroam VLAN
OHIS: DMZ WLC 4404 Anchor Controllers
OHIS: Cisco LWAPP APs 1010, 1130 & 1230
1Gb
10Gb
1Gb
10Gb
10Gb
OHIS CORE
Layer 3
SUP720
WISMs
10GE
OHIS: Access Layer 3750 PoE switch stack
SSIDs:
OxNET-WLAN
OWL
Eduroam
BT Openzone
2Gb
10Gb
100Mb
Revision
V1.1
Ath.
Craig McVeigh
Date
10/5/2011
Ckd.
Oxford Radcliffe Hospitals NHS
NHS Trust

Fig: 1

Introduction to eduroam and OWL

Source: http://www.eduroam.org/

The eduroam initiative started in 2003 within TERENA's Task Force on Mobility, TF-Mobility. The task force created a test bed to demonstrate the feasibility of combining a RADIUS-based infrastructure with 802.1X standard technology to provide roaming network access across research and education networks. The initial test was conducted among five institutions located in the Netherlands, Finland, Portugal, Croatia and the UK. Later, other national research and education networking organisations in Europe embraced the idea and gradually started joining the infrastructure, which was then named eduroam.

eduroam allows any eduroam-enabled user to get network access at any institution connected to eduroam. Depending on local policies at the visited institutions, eduroam participants may also have additional resources (for example printers) at their disposal.

Today eduroam is a federation of federations (confederation); single federations are run at national level and they are all connected to a regional confederation.

eduroam technology is based on 802.1X standard and a hierarchy of RADIUS proxy servers.

The role of the RADIUS hierarchy is to forward the users' credentials to the users' home institution, where they can be verified and validated.

When a user requests authentication, the user's realm determines where the request is routed to. The realm is the suffix of the user-name, delimited with '@', and is derived from the organisation's DNS domain name.

Every institution (i.e. university or equivalent) that wants to participate in eduroam connects its institutional RADIUS-server to the national top-level RADIUS (NTLR) server of the country where the institution is located.

The NTLR is normally operated by the National Research and Education Network (NREN) of that country. These country-level servers have a complete list of the participating eduroam institutions in that country. This is sufficient to guarantee national roaming.

For international roaming, a regional top-level RADIUS server is needed in order to roam the users request to the right country. Currently there are two main regions where eduroam is deployed: Europe and Asia-Pacific.

Oxford Uni Wireless LAN (OWL) is an SSID for Oxford Uni staff to access resources on the Oxford University network. It is built upon using IPSEC VPN over wireless. They restrict clients to access only a VPN peer (on IPSEC ports) on their network so to gain full access a client must VPN in. the IPSEC VPN provides the encryption/authentication/security rather than relying on wireless security measures.

OHIS Wireless Infrastructure details:

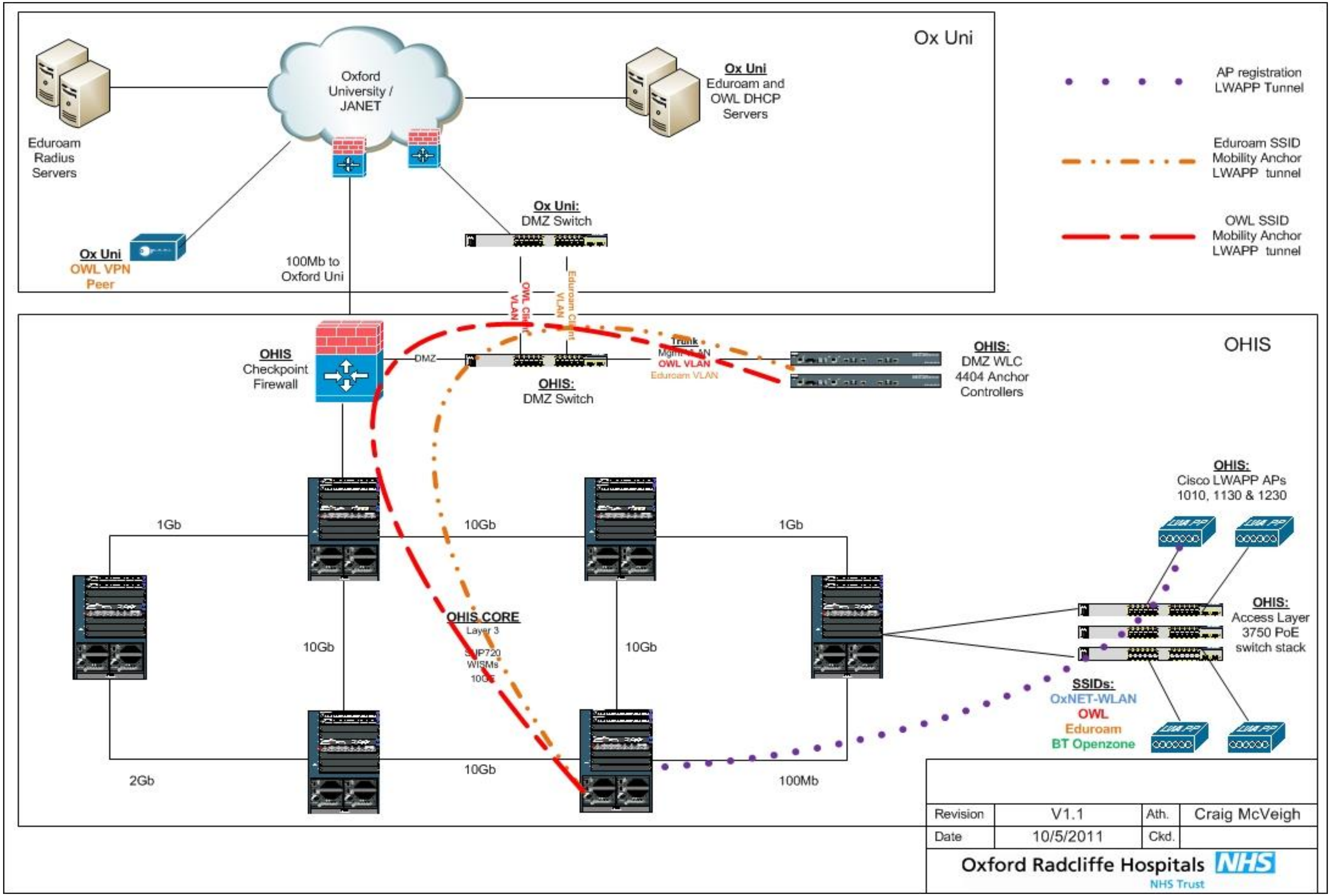
Currently, the components of our Cisco Unified Wireless Network are:

- 7 x Cisco Wireless Integrated Service Module (WISM)
- 4 x Cisco 4400 Wireless Lan Controller (WLC) for SSID mobility anchoring.
- 1,754 Lightweight Access Points (consisting of 1010, 1130 and 1200 models)
- 1 x Cisco Wireless Control System (WCS)
- Cisco 3750 PoE switches
- 4 x Cisco Secure Access Control Server (ACS) appliance for user/machine authentication via Microsoft AD.
- 1 x Cisco 3550 Mobility Services Engine (MSE) for location tracking (with Aeroscout MobileView RFID system)

With Cisco Lightweight APs, we can currently broadcast a maximum of 16 SSIDs out of each AP. We currently have 12 SSIDs being used, including corporate data WLAN, Voice over WLAN, clinical WLAN such as bloodtracking and public guest access via BT Openzone and access for Oxfordshire County Council staff.

These SSIDs are all tunnelled within the LWAPP tunnel back to WISM which the AP is controlled by. The WISM puts the SSID client traffic into the corresponding VLAN where it enters the network (ACLs are used on several of the SSIDs to secure\restrict access to only the resources they require.)

With regards to guest access (or hosting WLANs for external organisations such as Oxford Uni and BT Openzone) we chose to anchor the SSIDs from each WISM back to a WLC sitting in a DMZ outside of our network. By doing this, the guest client traffic is transported to the anchor WLC in the DMZ via a mobility LWAPP tunnel and therefore is logically and securely separated from the NHS network. It also means that no matter where in the county the guest user is, the traffic is presented at a single point outside of our network (see Fig 2: below)



Provided to the NHS-HE Connectivity Best Practice Working Group, May 2011

Eduroam/OWL provisioning for Oxford University on NHS Sites:

OHIS Responsibilities:

AP/WISM:
We created 2 new SSIDs for the Oxford University, namely OWL and eduroam. These were allowed to broadcast from every AP on our infrastructure to provide the best access possible for Ox University staff.

Encryption and authentication details for these SSIDs were provided to us by the Oxford University network team.

On each WISM these SSIDs are anchored back to a pair or Cisco 4400 WLCs in our DMZ off our Checkpoint Firewall (between NHS and University networks). The 4400 WLCs are in their own Mobility Group separate to the WISMs.

On the Checkpoint firewall, we only permitted the WISMs to access the DMZ anchor WLCs on LWAPP and mobility ports.

DMZ Anchor WLCs/DMZ switch:
On the DMZ anchor WLCs, we create the SSIDs as per the WISMs config, but with the addition of assigning the SSID a VLAN for client traffic to enter the Ox Uni network. Eduroam was assigned VLAN ID 382 and OWL was assigned VLAN ID 381.
The WLCs are connected to our 3750 DMZ switch via 1Gb Trunk, allowing only VLANs 381, 382 and VLAN 100 for management of the WLCs.

The DMZ WLCs were permitted to access the eduroam Radius servers to authenticate the clients onto the SSID. As Oxford University\JANET do not route 10.x.x.x addressing, we had to NAT our WLCs onto a University routable 163.1.46.x address. The authentication process is handled out of band (i.e. not via the client access)

The DMZ switch then has two access ports connected to an Ox Uni DMZ switch: one port in VLAN 381 for OWL client traffic, and a separate port for eduroam client traffic. We chose to use two access ports instead of a single trunk port to the Ox Uni DMZ switch for clarity rather than a technical reason. This was also an Ox Uni preference to not use trunks on their edge.

Oxford University responsibilities:

On the Oxford University network, they configured their edge switch to connect to our OHIS DMZ switch with matching VLAN IDs. The used QinQ to transport the client traffic across their Layer 2 infrastructure and presented the traffic on their network.

The WLC NAT addresses (163.1.46.x) were registered on to the eduroam radius servers as AAA clients with a shared secret. This secret password was provided to OHIS by Oxford University

Oxford University are responsible for both DHCP assignment for clients of both eduroam and OWL, and restricting\permitting access to resources on the Oxford University network were at the discretion and control of Oxford University I.T.