eduroam Solution Briefing Note – Technical

eduroam was developed in partnership with Health Authorities (HAs) to meet the Faculty of Medicine's (FoM) needs by leveraging HA wireless infrastructure.

Solution Selection

Based on functional requirements gathered from UBC FoM-affiliated users and current HA wireless infrastructure three potential technical solutions were identified:

- **Cisco Auto-Anchor Mobility:** Cisco feature that tunnels traffic back to UBC, allowing users to roam between HA networks (e.g. VCH/PHSA) yet still be authenticated and receive an IP address by UBC at these different locations.
- **RADIUS Authentication:** Allow users to be authenticated by UBC servers with internet access provided by the HA.
- **RADIUS Federation:** Allow users to connect to an existing HA network but authentication is passed between HA and UBC servers. Internet access would be determined by the local HA network.

UBC and HA technical representatives selected the **Cisco Auto-Anchor Mobility** solution as the best fit from both FoM and HA perspectives.

Cisco Auto-Anchor Mobility

Clients connect to a HA wireless access point (WAP) and, based on the service set identifier (SSID), the local wireless LAN controller (WLC) forwards traffic to a UBC-based anchor controller for authentication and network access (see Figure 1).

Connectivity to the 3rd Generation E-Health Network Gateway (3NG) extranet creates a consolidated link to allow any HA WLC to communicate with UBC's anchor controller. In the short term, the primary path will be shared with the FoM distributed medical program's videoconference (VC) service (see Figure 2). This path is considered an interim solution; a more sustainable path will need to be established for future expansion.
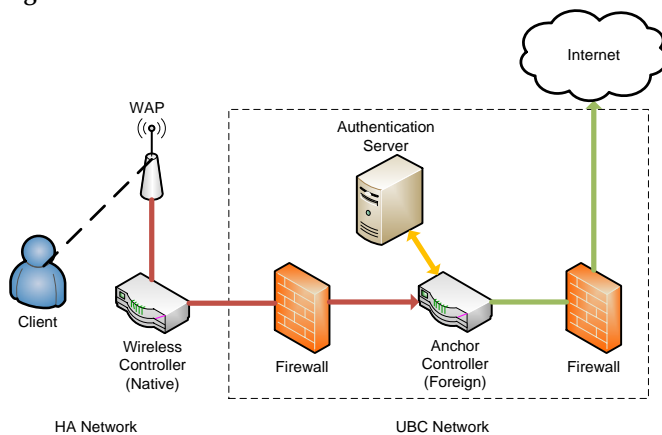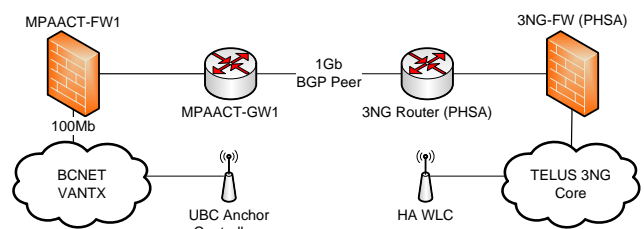
Figure 1 - Solution Overview

Figure 2 - Transport Route

The following major benefits of this solution are:

- Users are authenticated using their UBC credentials.
- Users receive a UBC IP address allowing them to access UBC IP-licensed resources without a VPN.
- Users receive same IP address and have the same experience, regardless of which HA location they connect from.
- Internet access is controlled and provisioned by UBC, with traffic kept separate from HA networks.

UBC

FACULTY OF MEDICINE

eduroam Solution Briefing Note – Technical

SSID - eduroam

eduroam (**edu**cation **roam**ing) is the secure, world-wide roaming access service developed for the international research and education community. This allows students, researchers, and staff from participating educational institutions to obtain Internet connectivity when visiting HA locations. Although this solution has been developed to support the needs of the UBC FoM, allowing other users that are affiliated with health education institutions to leverage this solution will only enhance the collaboration between the FoM and other health education institutions.

UBC's authentications servers will determine which network (i.e.: UBC VLAN) to assign the user based on their login credentials. UBC FoM users will be provided a UBC IP address to enable access to UBC licensed resources while a participating *eduroam* user with credentials from another educational institution will receive a commercial IP for internet access, provisioned by UBC.

Bandwidth

Based on Cisco's Wireless LAN Design Guide for High Density Client Environments in Higher Education, and UBC FoM use cases, the recommended bandwidth that HA WAPs should allow for is an average bandwidth of 1Mbps per connection (i.e.: user device) in a given area. Assume each FoM user will use a minimum of two devices on this network at a time.

A 1Gb link will be shared between this service and the FoM VC service (see Figure 2). Bandwidth from a hospital site to the 3NG will be determined by the link established by that HA. Quality of Service (QoS) has been enabled for VC traffic which will have priority over all other traffic via the MPAACT-GW1 router.

Security and Privacy

WPA2 and AES encryption will be used for traffic between the WAP and client device. 802.1X will be used for authentication between user and RADIUS server. An Ethernet over IP (EoIP) tunnel is established between the HA WLC and UBC IT anchor controller. This tunnel isolates the traffic from HA data traffic. This ensures that security and QoS policies can be separate and differentiated between UBC traffic and internal HA traffic. Firewall policies (e.g. 3NG extranet, MPAACT, UBC edge) govern the connectivity between the HA WLC and UBC IT anchor controller.

This service is intended for enabling access to educational resources and is not intended to accommodate personal information flow. Proper use requirements and education strategies are being developed and implemented by UBC.

Service Level

Following is a summary of support responsiblities for the UBC wireless service at HA locations:

- **UBC IT Help Desk:** Point of contact for FoM users of UBC wireless at HA locations. Responsible for assisting FoM users to resolve non-network issues and escalating to the UBC IT network team for network-related issues.
- **UBC IT Network Team:** Responsible for ensuring that the wireless anchor controller is operational and escalating any issues that seem to be HA network-related to the appropriate HA Service Desk.
- **Local HA Service Desk:** Triage between UBC IT and HA network teams. Not responsible for assisting FoM users with the UBC *eduroam* wireless service.
- **Local HA Network Team:** Responsible for ensuring local WLCs are operational and WAPs are properly broadcasting this wireless service.

Contact

Contact the Wireless Access to Educational Resources team at ubc.eduroam@ubc.ca

FACULTY OF MEDICINE