A case study in complying with the technical specification

Table of Figures

1. Introduction

All organisations participating in the eduroam must comply with the eduroam Technical Specification [1]. This case study illustrates how the University of Bristol (UoB) has implemented the necessary infrastructure to do this. The requirements of the technical specification can be split into three categories:

- Common requirements - for all participating organisations
- Home organisation requirements - for organisations whose home users visit other eduroam participants

- Visited organisation requirements – for participants receiving visitors

1.1 Preamble

1.1.1 The RADIUS Servers

The University operates two RADIUS (Remote Authentication Dial In User Service) servers for use with eduroam. These are standard x86 based rack mount machines running Red Hat Enterprise Linux version 4. The software used to provide RADIUS services is FreeRADIUS. The servers also provide RADIUS services for the University's other wireless services, a VPN remote access system, and authentication of users logging in to network devices and for network switches providing wired 802.1x authenticated connections to various office PCs.

1.1.2 The Network

The University of Bristol has a large network spread across multiple sites around the city. Each site generally has its own router, which in turn is connected to the routed backbone. The result of this is that a single VLAN (virtual LAN) for the eduroam would not be suitable for its network; hence multiple VLANs have been set up, one for each router. Using policy based routing, all the traffic from these VLANs is sent back to the University's gateway firewall (Cisco® PIX) which then NATs the traffic from all the VLANs on to public IP address space (eduroam clients are given private IPv4 IPs). The University does not currently route IPv6, hence IPv6 can be used by eduroam clients only via a tunnelling method such as Teredo.

1.1.3 The Authentication Database

The University's primary user database is a Microsoft Active Directory Domain (the UoB domain). For the purposes of the eduroam, the RADIUS servers are configured to authenticate against the domain via a utility called ntlm_auth. ntlm_ auth. This uses a UNIX® pipe provided by the winbindd daemon to access the ADS:

```
[root@custard [2] ~]# ls -lah /var/lib/samba/winbindd_privileged/
drwxr-x--- 2 root radiusd 4.0K Mar 25 12:09 .
srwxrwxrwx 1 root root         0 Mar 25 12:09 pipe
```

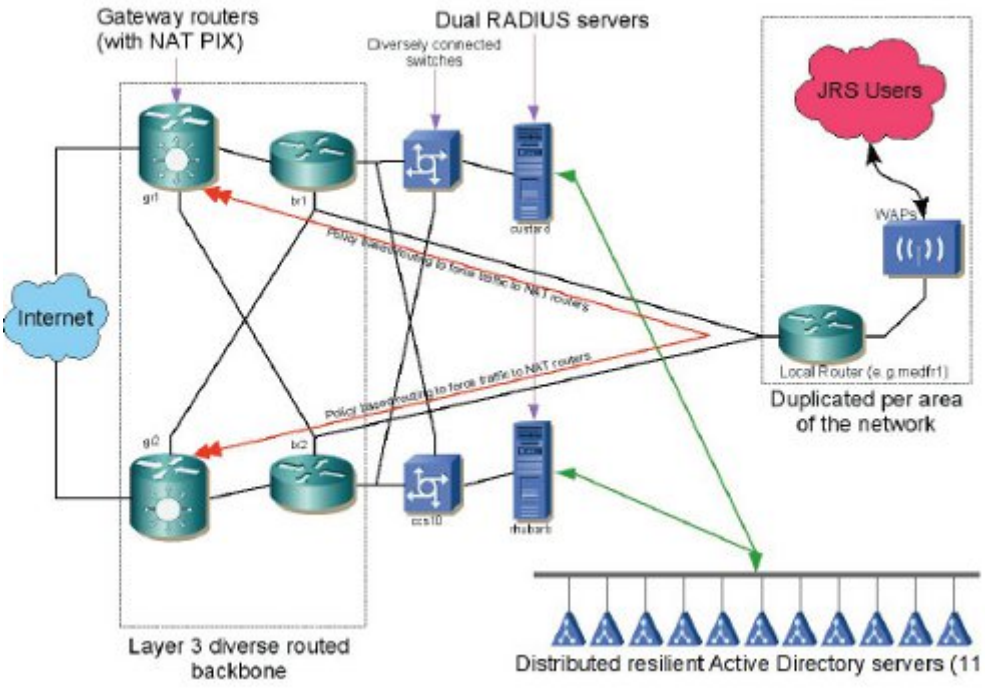
An example use of ntlm_auth is shown below:

```
[root@custard [2] ~]# ntlm_auth --request-nt-key --username=iser-linauth --
challenge=17ed657f0f546466 \
--nt-response=47d8d0302b953022f8988e90a16615206a9aebe0330d0177
NT_KEY: 7BE059BDE970E9A5D81720C7CF742283
```

In the command line can be seen the MS-CHAP challenge, the NT response and the corresponding NT key, indicating that authentication was successful.

Both ntlm_auth and winbindd are part of the Samba Suite.

Figure 1 shows a diagram of system topology.



[3]

2. eduroam Technical Specification Requirements

This section refers to the requirements listed in the eduroam Technical Specification, together with the way in which the requirement has been satisfied at Bristol.

2.1 Common Requirements

> *p 5, RQ 1. Participants must observe the requirements set out in sections 2 and 3 of the eduroam Technical Specification.*

Sections 2 & 3 of the Technical Specification are the Common Requirements, covered by this section of the case study, and the Home Organisation Requirements, covered by the next section.

> *p 5, RQ 2. Participants that choose to implement a visitor VLAN must observe the requirements set out in section 4 of the eduroam(UK) Service Technical Specification.*

UoB has implemented a visitor VLAN. Please refer to Section 2.3 of this document, Visited Organisation Requirements.

> *p 5, RQ 3. Participants must designate a technical contact who can be contacted using e-mail and telephone during normal business hours. The contact may be either a named individual or an organisational unit. Arrangements must be made to cover for absence owing to eventualities such as illness and holidays.*

James J.J. Hooper is the designated technical contact. Cover during absence is provided by the NetComms Team (part of Information Services).

p 5, RQ 4. Every log entry must state the date and time it was logged.

Please refer to Appendix 1: Logging of this document for details of logging mechanisms used.

p 5, RQ 5. Logs must be kept for a minimum of three months.

Please refer to Appendix 1: Logging for details of logging mechanisms used.

p 6, RQ 6. Participants' RADIUS clients and servers must comply with RFC 2865 and RFC 2866.

RFC 2865 is regarding the RADIUS protocol and RFC 2866 is regarding RADIUS Accounting. The UoB implementation uses FreeRADIUS as the RADIUS server and Cisco® wireless access points as the RADIUS clients.

p 6, RQ 7. Participants' RADIUS clients' and servers' clocks must be configured to synchronise regularly with a reliable time source.

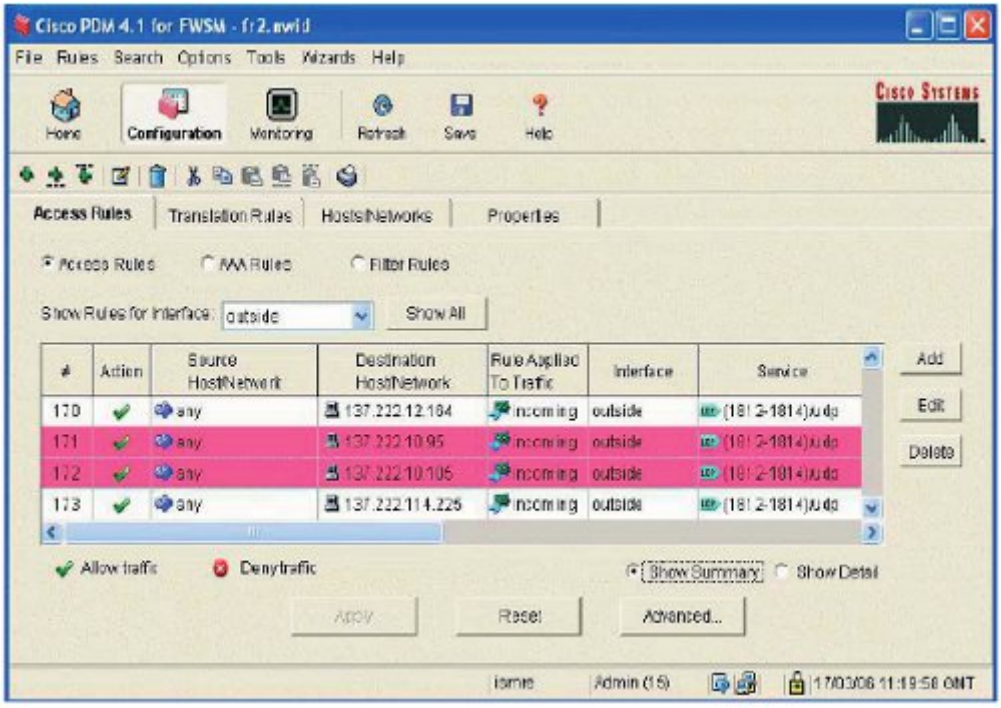
The RADIUS servers and clients are configured to synchronise against the NTP (RFC 1305) servers ntp0.bris.ac.uk and ntp1.bris.ac.uk. These servers synchronise with the Janet time servers.

p 6, RQ 8. Participants must deploy at least one ORPS (organisational RADIUS proxy server).

UoB has two RADIUS servers – rhubarb.bris.ac.uk and custard.bris.ac.uk.

p 6, RQ 9. Participants' ORPSs must be reachable from the eduroam(UK) Service NRPS (National RADIUS Proxy Servers) on either UDP/1812 and UDP/1813 (recommended), or UDP/1645 and UDP/ 1646 (if required by the participating Organisation).

The RADIUS servers are configured to accept requests from roaming1.ja.net and roaming2.ja.net and a suitable hole for UDP/1812 and UDP/1813 has been created in the perimeter firewall, as illustrated in Figure 2. More information is available about the UoB firewall from the Cisco® FWSM website.



[4]

The firewalls (iptables) on each of the RADIUS servers have also been configured with similar rules. This was done using the following iptables rules:

```
-A INPUT -m udp -p udp --dport 1812 -j ACCEPT
-A INPUT -m udp -p udp --dport 1813 -j ACCEPT
-A INPUT -m udp -p udp --dport 1814 -j ACCEPT
```

p 6, RQ 10. Participants' ORPSs must respond to ICMP (Internet Control Message Protocol) Echo Requests sent by the NRPS.

The RADIUS servers are configured to respond to ICMP echo requests and suitable holes have been made in the perimeter firewall to allow this.

p 6, RQ 11. Participants' ORPSs must log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded:

p 6, RQ 11.1 The value of the user name attribute in the request.

p 6, RQ 11.2 The value of the Calling-Station-Id attribute in the request.

Please refer to Appendix 1: Logging for details of logging mechanisms used.

p 6, RQ 12 Participants must log all RADIUS accounting requests exchanged with the NRPS; the following information must be recorded:

p 6, RQ 12.1 The value of the user name attribute in the request.

p 6, RQ 12.2 The value of the accounting session identifier.

p 6, RQ 12.3 The value of the request's accounting status type.

Please refer to Appendix 1: Logging for details of logging mechanisms used.!!!

2.2 Home Organisation Requirements

> *p 8, RQ 13. Home organisations' eduroam user names must conform to the NAI (Network Access Identifier) specification (RFC 4282).*

UoB usernames are between four and six characters and comply with RFC 4282.

> *p 8, RQ 14. The realm component must conclude with participant's realm name, which must be a domain name in the global DNS (Domain Name System) that the recipient organisation administers, either directly or by delegation.*

The UoB's realms are bris.ac.uk and bristol.ac.uk. These are DNS registered on a system administered by the University.

> *p 8, RQ 15. Home organisations must log all authentication attempts; the following information must be recorded:*

> *p 8, RQ 15.1. The time that the authentication request was received.*

> *p 8, RQ 15.2. The authentication result returned by the authentication database.*

> *p 8, RQ 15.3. The reason given, if any, if the authentication was denied or failed.*

Please refer to Appendix 1: Logging for details of logging mechanisms used.

> *p 9, RQ 16. Home organisations must configure their RADIUS server to authenticate one or more EAP (Extensible Authentication Protocol) types.*

The RADIUS servers are configured to authenticate EAP-TTLS and EAP-PEAP (with an inner method of MS-CHAPv2). The RADIUS servers are configured to do this with the following entries in the FreeRADIUS eap.conf file

```
eap {
    default_eap_type = ttls
    timer_expire = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no

    md5 {
    }
    tls {
        private_key_file = ${raddbdir}/certs/custard.key
        certificate_file = ${raddbdir}/certs/custard-cert.pem
        CA_file = ${raddbdir}/certs/is-cacert.crt
        dh_file = ${raddbdir}/certs/dh
        random_file = /dev/urandom
        fragment_size = 1024
        include_length = yes
```

```
    }

    ttls {
    }

    peap {
        default_eap_type = mschapv2
    }

    mschapv2 {

    }
}
```

> *p 9, RQ 16.1. Home organisations must select a type, or types, for which their RADIUS server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580 within RADIUS Access-Accept packets.*

The RADIUS servers are configured to authenticate EAP-TTLS and EAP-PEAP (both with an inner method of MS-CHAPv2). Keying material is generated and transferred in the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes.

> *p 9, RQ 17. Home organisations must create an authenticable test account.*

Such an account has been configured and a test authentication completed successfully.

> *p 10, RQ 17.1. The test account must be able to authenticate PAP and the EAP type(s) selected by the participant.*

This has been verified.

> *p 10, RQ 17.2. eduroam(UK) Support (jrssupport@ja.net [5]) must always be informed immediately if the password for this account is changed. However, if it is believed that the password has been compromised then the password must be changed immediately and eduroam(UK) Support informed as soon as possible.*

This will be done!

> *p 10, RQ 18. Home organisations must educate their users to validate the certificate presented by a WRD NAS (Network Access Server).*

The UoB eduroam service information website contains guidelines for users visiting organisations that are using WRD. Bristol has not implemented a WRD system.

2.3 Visited Organisation Requirements – Common to All eduroam(UK) Service Tiers

> *p 11, RQ 19. Visited organisations must implement at least one of the JRS1, JRS2 or JRS3 tiers.*

UoB is presently running a JRS2 tier.

p 11, RQ 20. Visited organisations must ensure that a non-Janet service cannot be mistaken by visitors for the participant's eduroam service.

No other services are known or advertised as 'eduroam'. The Information Services Communications Officer ensures that no two services have conflicting names. On the network, all wireless devices are managed by the Networking and Digital Communications Team who only use the 'eduroam' SSID for the eduroam.

p 11, RQ 21. The 'eduroam' prefix is reserved for SSIDs used with the eduroam service tiers.

SSIDs containing 'eduroam' are used solely for eduroam purposes.

p 11, RQ 22. Visited organisations must implement a separate VLAN for each tier that they choose to implement. A tier's VLAN must not be shared with any other tier or network service.

The eduroam network has its own VLANs which are used solely for JRS2 tier. More information about the UoB's network is available in the Preamble.

p 11, RQ 23. Visited organisations that provide access to a eduroam(UK) Service tier for local users, or visitors from organisations not participating in the eduroam, must ensure that the user has read and agreed to both the eduroam Policy and the local AUP.

All relevant AUPs are displayed or linked to from UoB's eduroam website (**http://www.bristol.ac.uk/jrs** [6])

p 11, RQ 24. Visited organisations must not offer visitors any wireless media other than IEEE 802.11.

Only IEEE 802.11 media is offered.

p 12, RQ 25. Visited organisations must forward RADIUS requests originating from eduroam NASs and containing user names with unknown realms via an ORPS to an NRPS.

The RADIUS servers are configured to do this with the following entries in the FreeRADIUS proxy.conf file

```
realm DEFAULT {
        type          = RADIUS authhost = roaming1.ja.net:1812 accthost =
roaming1.ja.net:1813
        secret        = bigSecret
        nostrip
        dead_time = 0
}
realm DEFAULT {
        type          = RADIUS authhost = roaming2.ja.net:1812 accthost =
roaming2.ja.net:1813
        secret        = isAsecret
```

```
        nostrip
        dead_time = 0
}
```

p 12, RQ 25.1. RADIUS Access-Requests must be addressed to UDP/1812.

The RADIUS servers are configured to do this with entries as per RQ25 (previous page) in the FreeRADIUS proxy.conf file.

p 12, RQ 25.2. RADIUS Accounting-Requests must be addressed to UDP/1813.

The RADIUS servers are configured to do this with entries as per RQ25 (previous page) in the FreeRADIUS proxy.conf file.

p 12, RQ 26. Visited organisations may configure additional realms to forward requests to other internal RADIUS servers, but these realms must not be derived from any domain in the global DNS that the participant does not administer.

UoB has not configured additional realms to forward requests to other internal RADIUS servers.

p 12, RQ 27. Visited organisations may configure additional realms to forward requests to external RADIUS servers in other organisations, but these realms must be derived from domains in the global DNS that the recipient organisation administers (either directly, or by delegation).

UoB has not configured additional realms to forward requests to external RADIUS servers in other organisations.

p 12, RQ 28. Visited organisations must not otherwise forward requests to other eduroam participants.

All requests destined for other participants' RADIUS servers are proxied via the eduroam NRPS.

p 13, RQ 29. Visited organisations must deploy NASs that include the following RADIUS attributes within Access-Request packets.

p 13, RQ 29.1. The supplicant's MAC address within the Caller-Station-ID attribute.

p 13, RQ 29.2. The NAS's IP address within the NAS-IP-Address attribute.

All NASs are configured to put the supplicant's MAC address within the Caller-Station-ID attribute (preferably in IETF format e.g. 00-00-40-96-3e-4a). All NASs are configured to put their IP addresses (in dotted decimal format) in the NAS-IPAddress attribute.

p 14, RQ 30. Visited organisations may implement IPv4 and IPv6 filtering between the visitor VLAN and other external networks, providing that this permits the forwarding of the following protocols:

p 14, RQ 30.1. IPv6 Tunnel Broker NAT traversal: UDP/3653 and TCP/3653 egress and established.

p 14, RQ 30.2. IPSec NAT traversal: UDP/4500 egress and established.

p 14, RQ 30.3. Cisco® IPSec NAT traversal: TCP/10000 egress and established.

p 14, RQ 30.4. PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.

p 14, RQ 30.5. OpenVPN: TCP/5000 egress and established.

p 14, RQ 30.6. SSH: TCP/22 egress and established.

p 14, RQ 30.7. HTTP: TCP/80 egress and established.

p 14, RQ 30.8. HTTPS: TCP/443 egress and established.

p 14, RQ 30.9. LDAP: TCP/389 egress and established.

p 14, RQ 30.10. LDAPS: TCP/636 egress and established.

p 14, RQ 30.11. IMSP: TCP/406 egress and established.

p 14, RQ 30.12. IMAP4: TCP/143 egress and established.

p 14, RQ 30.13. IMAP3: TCP/220 egress and established.

p 14, RQ 30.14. IMAPS: TCP/993 egress and established.

p 14, RQ 30.15. POP: TCP/110 egress and established.

p 14, RQ 30.16. POP3S: TCP/995 egress and established.

p 14, RQ 30.17. Passive (S)FTP: TCP/21 egress and established.

p 14, RQ 30.18. SMTPS: TCP/465 egress and established.

p 14, RQ 30.19. Message submission: TCP/587 egress and established.

p 14, RQ 30.20. RDP: TCP/3389 egress and established.

p 14, RQ 30.21. VNC: TCP/5900 egress and established.

p 14, RQ 30.22. Citrix: TCP/1494 egress and established.

All router ACLs & firewalls have been configured to allow the protocols listed in RQ 30.

p 15, RQ 31. Visited organisations deploying application or ‘interception’ proxies on the visitor LAN must publish this fact on their eduroam website.

UoB does not use application or ‘interception’ proxies on the visitor LAN.

p 15, RQ 32. If an application proxy is not transparent, the visited organisation must also provide documentation on the configuration of applications to use the proxy.

UoB does not use application or ‘interception’ proxies on the visitor LAN.

p 15, RQ 33. Visited organisations must publish a eduroam service information website which must be generally accessible from the Internet and within the organisation to allow visitors to access it easily. The website must include the following information at a minimum.

p 15, RQ 33.1. The participant’s AUP (Acceptable Use Policy).

p 15, RQ 33.2. Sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered, the eduroam Tier(s), and SSIDs.

Please see **http://www.bristol.ac.uk/jrs** [6]

p 15, RQ 33.3. Where applicable, the information specified in section 4.6 regarding application and interception proxies.

UoB does not use application or ‘interception’ proxies on the visitor LAN.

p 16, RQ 34. A broadcast SSID of ‘eduroam’ must always be used for eduroam wireless services, except in the following circumstances.

A broadcast SSID of ‘eduroam’ is used for eduroam wireless services.

p 16, RQ 34.1. A broadcast SSID of ‘eduroam-wep’ may be used with WEP but only where the ‘eduroam’ SSID is required by another eduroam wireless service.

UoB does not currently offer a WEP service.

p 16, RQ 34.2. A broadcast SSID of ‘eduroam-web’ may be used with WRD but only where the ‘eduroam’ SSID is required by another eduroam wireless service.

UoB has not implemented a WRD service.

p 18, RQ 43. Visited organisations must allocate IPv4 addresses to visitors using DHCP.

DHCP is configured on the eduroam VLAN. The ISC DHCPd is used as the DHCP server. An example of the DHCP configuration file is below:

server-identifier dhcp-srv.bris.ac.uk;

ddns-update-style none; authoritative;

log-facility local6;

```
# This is because we use DHCP in a failover & load balancing
# configuration between multiple DHCP server machines
failover peer ‘dhcpcluster’ {

        #primary;
        secondary; address 137.222.253.66;
        port 647;
        peer address 137.222.253.65;
        peer port 847;
        max-response-delay 30;
        mclt 600;
        #split 128;
        load balance max seconds 3;
}

# option definitions common to all bristol networks...
option domain-name ‘bris.ac.uk’;

option domain-name-servers dns0.bris.ac.uk, dns1.bris.ac.uk;

# Subnet declaration for the local interface on the
# DHCP server box (required)
subnet 137.222.253.64 netmask 255.255.255.192 {
  option routers 137.222.253.126;
  option subnet-mask 255.255.255.192;
}

# Declaration for the eduroam network
shared-network ‘eduroam-A’ {
        subnet 172.21.130.0 netmask 255.255.254.0 {
          pool {
                        failover peer ‘dhcpcluster’;
                        deny dynamic bootp clients;
                        option routers 172.21.131.254;
                        range 172.21.130.1 172.21.131.248;
                        default-lease-time 360;
                        option subnet-mask 255.255.254.0;
                        max-lease-time 1000;
            }
          }
}
```

p 18, RQ 44. Visited organisations must log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.

All DHCP leases are logged.

p 18, RQ 45. Visited organisations must log NAT address mappings, if used.

The Cisco® PIX that does the NAT for UoB’s eduroam VLANs is configured to log address

mappings.

> *p 18, RQ 48. Visited organisations that choose to deploy WEP must configure their WAPs to require the use of 128-bit keys, and to rotate these keys every five minutes.*

UoB has not currently deployed WEP.

2.4 Visited Organisation Requirements – JRS2 Specific

> *p 17, RQ 38. The JRS2 and JRS3 tiers must only implement IEEE 802.1X; no form of WRD is permitted.*

UoB does not offer a WRD service.

> *p 17, RQ 39. IEEE 802.1X NASs must support symmetric keying using keys provided by the home organisation within the RADIUS Access-Accept packet, in accordance with section 3.16 of RFC 3580.*

> *p 17, RQ 40. Only a single user is permitted per NAS port.*

This is the default setting on the Cisco NAS equipment in use at UoB. Devices are not configured to differ from this default.

> *p 18, RQ 46. The JRS2 tier may implement WEP; if it does not, it must implement WPA.*

UoB has implemented WPA.

> *p 18, RQ 49. The JRS2 tier should implement WPA; if not, it must implement WEP.*

UOB has implemented WPA.

Appendix 1: Logging

Logs are produced with the following format:

> DATE<tab>TIME<tab>RadiusPacketType
>
> <tab>AttributeName<tab>AttributeValue
> <tab>AttributeName<tab>AttributeValue
> <tab>AttributeName<tab>AttributeValue
> <blankLine>

e.g.

> 2006-03-17 10:57:37 acct
>
> SERVICE_TYPE Framed-User
>
> CISCO_NAS_PORT ‘6735’
> ACCT_STATUS_TYPE Start
> CALLED_STATION_ID ‘00-16-C7-71-A2-61’
>
> NAS_PORT_TYPE Wireless-802.11

```
ACCT_SESSION_ID ‘00001AA0’
NAS_PORT 6735
CALLING_STATION_ID ‘00-0E-35-DD-CA-22’
ACCT_DELAY_TIME 0
CLIENT_IP_ADDRESS 172.17.49.103
ACCT_AUTHENTIC RADIUS
USER_NAME ‘jh1761’
CISCO_AVPAIR ‘connect-progress=Call Up’
NAS_IP_ADDRESS 172.17.49.103
```

The logs are created like this using a perl script:

```
#!/usr/bin/perl

use strict;
my $tag = $ARGV[0];
if ($tag =~ m/^([a-zA-Z0-9\-\_]*)/) { $tag = $1;}
my $log = ‘/var/log/radius/radius-log-’ . $tag . ‘.log’;
my ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
open(f,’>>$log’);
print f sprintf(‘%04u-%02u-%02u\t%02u:%02u:%02u\t$tag\n’ ,$year+1900, $mon+1,

$mday, $hour, $min, $sec);
foreach my $v (keys %ENV) {
        if (($v ne ‘USER_PASSWORD’) && ($v ne ‘EAP_MESSAGE’)) { print f ‘\t$v\t’
. substr($ENV{$v},0,255) .’\n’; }
}

print f ‘\n’;
close(f);
exit 0;
```

The perl script is instantiated in /etc/raddb/radiusd.conf as shown below:

```
...

modules {
        ...
        exec log-auth {
                wait = no
                input_pairs = request
                #output_pairs = none
                program = ‘/etc/raddb/bin/log-script.pl auth’
}
```

```
exec log-auth-reply {
        wait = no
        input_pairs = reply
        #output_pairs = none
        program = '/etc/raddb/bin/log-script.pl auth'
}

...
}
...
```

Logs are kept both on the RADIUS servers and on a remote syslog host. Each is configured to rotate the logs weekly and to keep 26 weeks (6 months) of logs. This is done with the following entries in /etc/logrotate.conf

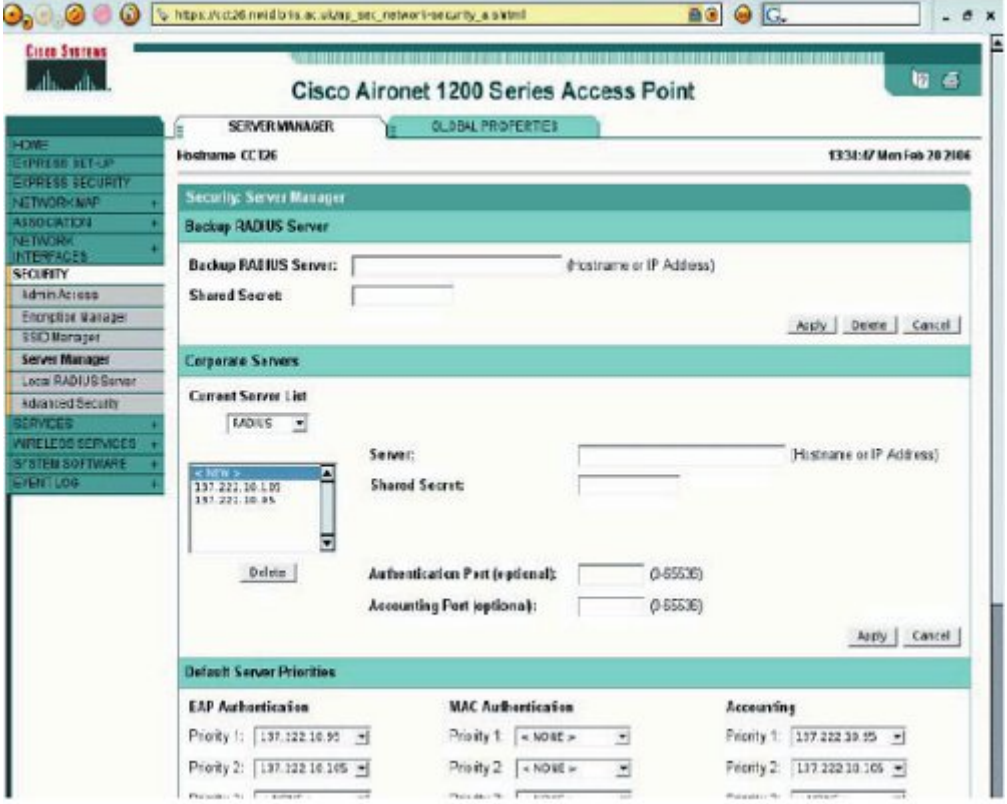
```
# Rotate logs weekly
weekly

# keep 26 weeks worth of backlogs
rotate 26
# create new (empty) log files after rotating old ones
create
# compress log files with gzip
compress
```

Appendix 2: Wireless Access Points (WAPs)

The following details the precise steps used to configure the eduroam SSID on a Cisco® 1200 series WAP. The configuration method is largely web-based, as this is what was found to be easiest. Large numbers of WAPs can be bulk configured in a similar web-based method via the use of a Cisco® Wireless LAN Solution Engine (WLSE), which the university has purchased.

1. Go to the web interface of the WAP (e.g. **`https://cct26.nwid.bris.ac.uk`**).
2. Login.
3. Select the 'SECURITY' menu, and then select 'Server Manager' (Figure 3).



[7]

4. In the ‘Corporate Servers’ section, set the ‘Current Server List’ to ‘RADIUS’.

5. Enter the address of the RADIUS server in the ‘Server’ box (137.222.10.95 and 137.222.10.105).

6. Enter server secret in the ‘Shared Secret’ box.

7. Enter the address of the RADIUS server in the ‘Server’ box.

8. In the ‘Authentication Port’ box enter 1812.

9. In the ‘Accounting Port’ box enter 1813.

10. Click ‘Apply’

11. Select ‘Global Properties’ (Figure 4).

[8]

12. In the ‘RADIUS Server Timeout’ box enter 3.

13. In the ‘RADIUS Server Retransmit Retries’ box enter 4.

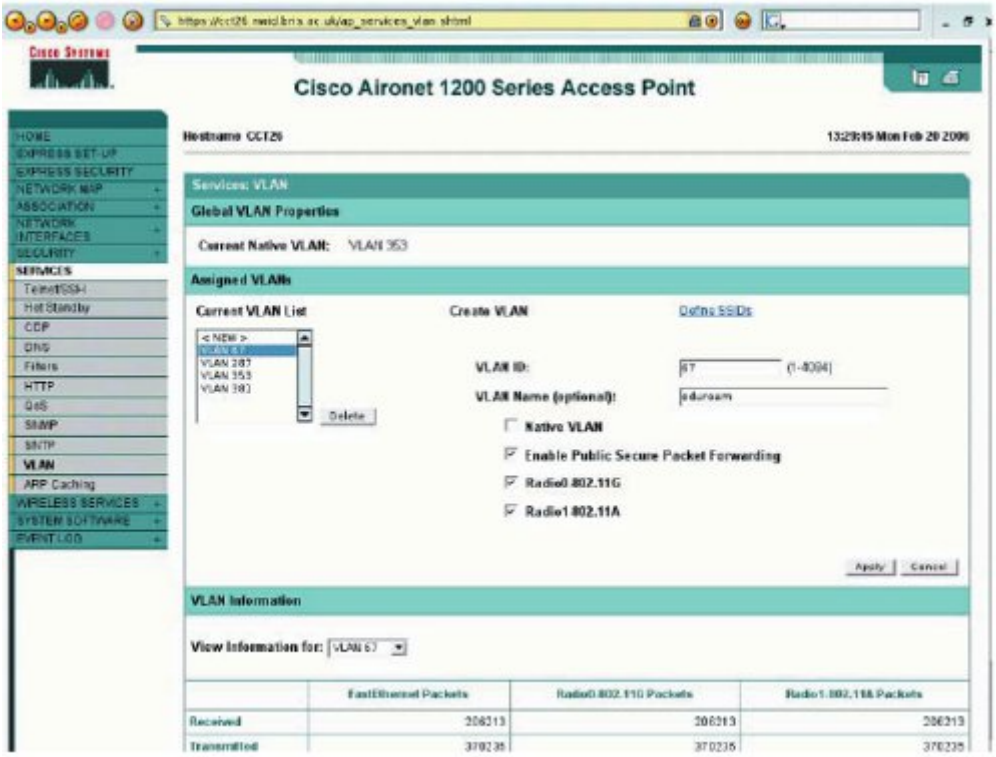
14. Select the ‘Enable’ radio button for the ‘Dead RADIUS Server List’ option.

15. Enter 2 in the ‘Server remains on list for’ box.

16. Select the ‘ITEF’ radio button for the option ‘RADIUS Calling/Called Station ID Format’.

17. Click ‘Apply’

18. Select the ‘SERVICES’ menu, and then select ‘VLAN’ (figure 5).



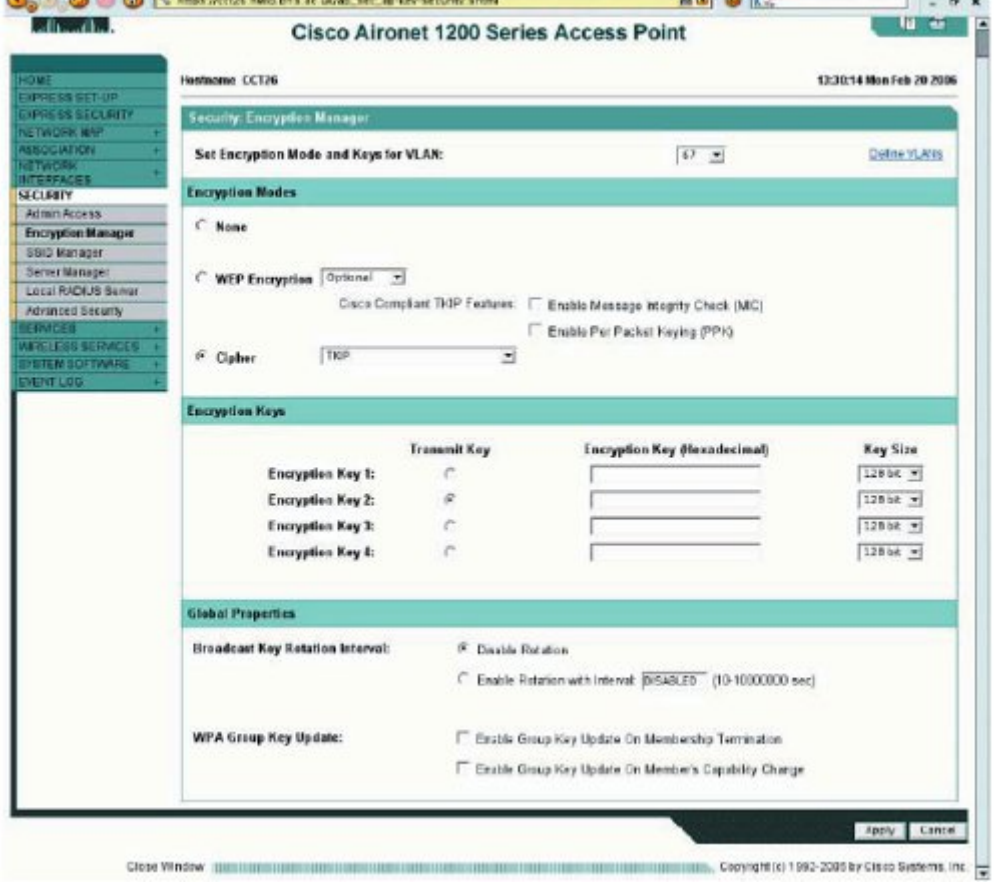
[9]

19. Enter the ‘VLAN ID’ e.g. 67.

20. Tick the boxes: ‘Enable Public Secure Packet Forwarding’, ‘Radio0-802.11G’, ‘Radio1-802.11A’.

21. Click ‘Apply’.

22. Select the ‘SECURITY’ menu, and then select ‘Encryption Manager’ (figure 6).



[10]

23. Change the ‘Set Encryption Mode and Keys for VLAN:’ drop-down option to the appropriate VLAN.

24. Select the ‘Cipher’ radio button as the ‘Encryption Mode’.

25. Select ‘TKIP’ from the ‘Cipher’ drop-down list.

26. Click ‘Apply’ at the bottom of the page.

27. From the ‘SECURITY’ menu, select ‘SSID Manager’ (figure 7).

[11]

28. Enter the new SSID in the ‘SSID’ box.

29. Select the appropriate VLAN from the ‘VLAN’ drop-down list.

30. Tick both the ‘Radio0-802.11G’ and ‘Radio1-802.11A’ interfaces.

31. In the ‘Authentication Settings’ section of the page, for ‘Methods Accepted’, tick ‘Open Authentication’ and ‘Network EAP’.

32. In the ‘Open Authentication’ drop-down list, select ‘with EAP’.

33. In the ‘Authenticated Key Management’ section of the page, select ‘Mandatory’ in the ‘Key Management’ drop-down list.

34. Tick the ‘WPA’ box.

35. In the ‘Accounting settings’ section of the page, tick the box ‘Enable Accounting’.

36. In the ‘Multiple BSSID Beacon Settings’ section of the page, tick the box ‘SetSSID as Guest Mode’ (under the heading ‘Multiple BSSID Beacon’).

37. Click ‘Apply’.

38. Scroll down to the bottom of the ‘SSID Manager’ and find the ‘Guest [12]

39. For both radios, select the ‘Multiple BSSID’ radio button’.

40. Ensure the ‘Set Single Guest Mode SSID’ and ‘Set Infrastructure SSID’ drop-down options are set to ‘<NONE>‘ for both radios.

41. Click ‘Apply’ (the one right at the bottom of the page).

42. The last section of the configuration can be done via the command line or the web interface. Open a terminal to the WAP or navigate to the command line web interface, e.g. **`https://cct26.nwid.bris.ac.uk/level/15/exec/-/configure/http`**

43. Then execute the following commands (you will need to be ‘enabled’):

```
configure terminal
radius-server vsa send authentication
radius-server vsa send accounting
exit
write mem
```

The equivalent commands can be executed via the web interface by going to the following URLs:

```
https://cct26.nwid.bris.ac.uk/level/15/configure/-
/radiusserver/vsa/send/authentication/CR

https://cct26.nwid.bris.ac.uk/level/15/configure/-
/radiusserver/vsa/send/accounting/CR
```

44. Test the configuration with a client!

Appendix 3: RADIUS Attribute Filtering

A user's credentials are always proxied via the NRPS to their home organisation's RADIUS server when the user is not at their home organisation. Therefore the RADIUS attributes present in the reply packet sent to the local NAS are set by the remote RADIUS server. If this server was compromised or mis-configured, it could be set to return attributes that could cause the local NAS to give the user a higher level of network access than desired.

For example, returning the attributes below could make the NAS put the user into an arbitrary VLAN (in this case VLAN 1):

```
Tunnel-Type := 'VLAN',
Tunnel-Medium-Type := 'IEEE-802',
Tunnel-Private-Group-Id := 'VLAN0001'
```

To prevent this the attributes contained in packets received from foreign RADIUS servers are filtered. Using FreeRADIUS, this is done using the module rlm_attr_filter. The module is instantiated in radiusd.conf as shown below:

```
...
modules {
    ...
    attr_fi lter {
        attrsfile = ${confdir}/attrs
    }
    ...
}
...
```

The file ${confdir}/attrs contains the following lines – any attribute not matching one of the lines is discarded.

```
DEFAULT
    Reply-Message =* ANY,
    Proxy-State =* ANY
```

This filtering prevents UoB's NASs receiving unwanted attributes.

Links
[1] https://community.jisc.ac.uk/case-study-complying-technical-specification/janet-eduroam-technical-specification
[2] mailto:root@custard
[3] http://community.ja.net/sites/default/files/compliance-cs-fig01.jpg
[4] http://community.ja.net/sites/default/files/compliance-cs-fig02.jpg
[5] mailto:jrssupport@ja.net
[6] http://www.bristol.ac.uk/jrs
[7] http://community.ja.net/sites/default/files/compliance-cs-fig03.jpg
[8] http://community.ja.net/sites/default/files/compliance-cs-fig04.jpg
[9] http://community.ja.net/sites/default/files/compliance-cs-fig05.jpg

[10] http://community.ja.net/sites/default/files/compliance-cs-fig06.jpg
[11] http://community.ja.net/sites/default/files/compliance-cs-fig07.jpg
[12] http://community.ja.net/sites/default/files/compliance-cs-fig08.jpg