FreeRADIUS v2.02
at the University of Sussex

A JANET Roaming Service Case Study

Arran Cudbard-Bell

University of Sussex

025 (04/08)

Contents

1 Introduction

Organisations wishing to participate in JANET Roaming must first comply with the JANET Roaming Service Technical Specification, the latest version of which is available at **http://www.ja.net/documents/services/janet-roaming/techspec.pdf**. This case study complies with version 1.0 of the Technical Specification.

This case study assumes familiarity with FreeRADIUS, the preferred RADIUS solution for many JANET Roaming participants. Since the previous case study at the University of Bristol, FreeRADIUS has reached a new major revision. This new revision brings many new powerful features, including a new conditional language 'unlang' to aid in policy implementation, a much-improved proxying scheme, and a myriad of other improvements and fixes. This case study illustrates how the University of Sussex has implemented the necessary AAA infrastructure for participating in JANET Roaming, with particular focus on the configuration of FreeRADIUS v2.02 for compliance with JANET Roaming technical specifications.

1.1 Preamble

1.1.1 The FreeRADIUS Servers

The University operates a pair of RADIUS servers in a high availability configuration. These are dual processor Apple Xserves with PPC architecture, running OSX Server 10.4.11 and FreeRADIUS v2. Both servers operate two 'virtual' RADIUS servers. The first provides AAA services for the University's wireless-roaming, wired-residential and wired-roaming services, in addition to managing administrative logins for wired infrastructure devices (routers, switches etc.). The second adds one-time-password functionality, and provides access controls for the University's administrative network via a clustered VPN service.

1.1.2 The Network

The University of Sussex is spread over a large but self contained campus, and the network infrastructure reflects this. The core network consists of three Cisco Catalyst routers, with resilient bonded fibre interconnects; this forms the backbone of the Sussex network. The network is then divided into zones (each zone is typically a building) with HP ProCurve 5300XL series managed switches acting as the aggregation layer around the core. These aggregation switches are known locally as Zone point-of-presence switches, or just ZPoPs.[1]

A single VLAN exists for JANET Roaming/eduroam[2] users, which is carried over the core network to all ZPoPs. This VLAN does not present at layer 3 on the core, and all traffic instead flows through a single dedicated BSD routing firewall, which also provides DHCP and DNS-forwarding services. The firewall's public interface connects to a layer 2 network outside of the University's main perimeter firewall, and eduroam traffic flows to a LeNSE (the local regional area network) demarcation router in a single hop. Firewall policies are intentionally permissive, with no restrictions on outbound traffic and few restrictions on inbound traffic. IP addresses are allocated from a dedicated public IPv4 range

[1] See Glossary at end for expansion of all acronyms.

[2] The international RADIUS proxy server-based infrastructure that uses the 802.1X standard to allow any eduroam-enabled user to get network access at any connected organisation. See www.eduroam.org.

(192.33.16.0/24) with addresses resolvable to dy<int>.eduroam.sussex.ac.uk, where <int> is the fourth octet of the allocated IPv4 address.

JANET Roaming is available from any 802.1x enabled wireless access point, or 802.1x enabled wired infrastructure port; this includes 3,500 bedrooms in University managed residences.

1.1.3 The Authentication Database

The University’s primary user directory is a clustered OpenLDAP service. This consists of six LDAP slave nodes in a DNS round-robin, employing bi-directional synchronisation with an LDAP master node. LDAP based authentication attributes are extracted using the rlm_ldap module.

For user authentication at the University of Sussex, the RADIUS server performs an administrative bind to one of the LDAP slave nodes, and performs a search for the User Identifier present in the EAP tunnel. If the User Identifier is found in the directory, rlm_ldap then extracts the *NT-Password* and *UOSRADIUSAccountEnabled* attributes associated with the user.

The *NT-Hash* attribute is used by the FreeRADIUS *MS-CHAP* module, where *MS-CHAP*/*MS-CHAPv2* is the desired inner encryption method. *UOSRADIUSAccountEnabled* is interpreted as a Boolean attribute, where its presence enables the account for use with the RADIUS service and its absence disables it. This attribute is absent by default, and is only created after the user has accepted the University’s Acceptable Use Policy.

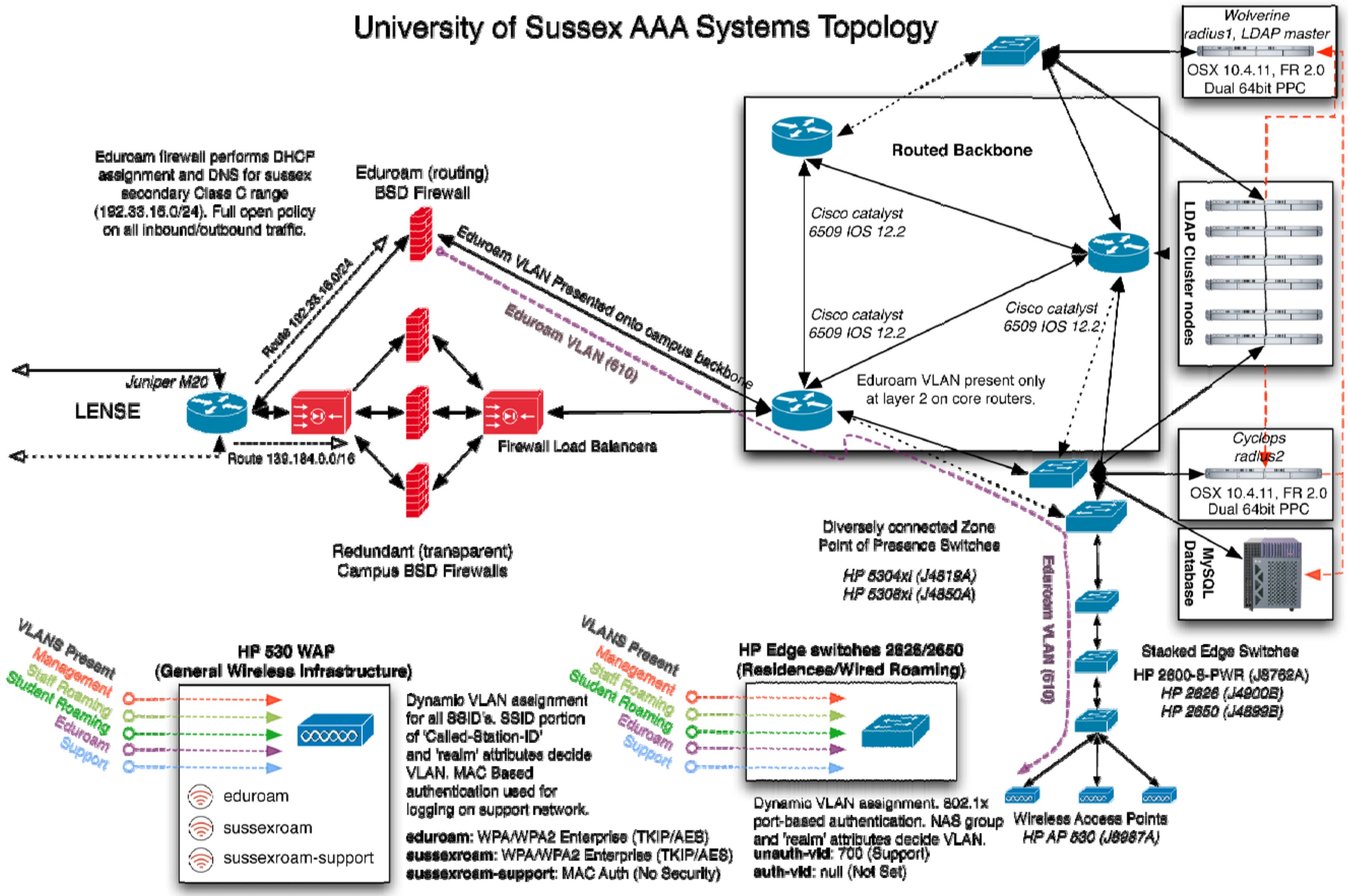

University of Sussex AAA Systems Topology
Eduroam firewall performs DHCP assignment and DNS for sussex secondary Class C range (192.33.16.0/24). Full open policy on all inbound/outbound traffic.
Eduroam (routing) BSD Firewall
Route 192.33.16.0/24
Juniper M20
LENSE
Route 139.184.0.0/16
Eduroam VLAN Presented onto campus backbone
Eduroam VLAN (610)
Firewall Load Balancers
Redundant (transparent) Campus BSD Firewalls
Routed Backbone
Cisco catalyst 6509 IOS 12.2
Cisco catalyst 6509 IOS 12.2
Cisco catalyst 6509 IOS 12.2
Eduroam VLAN present only at layer 2 on core routers.
Wolverine radius1, LDAP master
OSX 10.4.11, FR 2.0 Dual 64bit PPC
LDAP Cluster nodes
Cyclops radius2
OSX 10.4.11, FR 2.0 Dual 64bit PPC
MySQL Database
Diversely connected Zone Point of Presence Switches
HP 5304xl (J4819A)
HP 5308xl (J4850A)
Eduroam VLAN (610)
Stacked Edge Switches
HP 2600-8-PWR (J8762A)
HP 2626 (J4900B)
HP 2650 (J4899B)
Wireless Access Points
HP AP 530 (J8987A)
VLANS Present
Management
Staff Roaming
Student Roaming
Eduroam
Support
HP 530 WAP
(General Wireless Infrastructure)
eduroam
sussexroam
sussexroam-support
Dynamic VLAN assignment for all SSID's. SSID portion of 'Called-Station-ID' and 'realm' attributes decide VLAN. MAC Based authentication used for logging on support network.
eduroam: WPA/WPA2 Enterprise (TKIP/AES)
sussexroam: WPA/WPA2 Enterprise (TKIP/AES)
sussexroam-support: MAC Auth (No Security)
VLANS Present
Management
Staff Roaming
Student Roaming
Eduroam
Support
HP Edge switches 2626/2650
(Residences/Wired Roaming)
Dynamic VLAN assignment. 802.1x port-based authentication. NAS group and 'realm' attributes decide VLAN.
unauth-vid: 700 (Support)
auth-vid: null (Not Set)

Figure 1. Diagram of AAA systems topology.

2. The JANET Roaming Service Technical Specification Requirements

2.1 Common Requirements

From the JANET Roaming Service Technical Specification:

> ***P5,R01.*** *Participants must observe the requirements set out in sections 2 and 3 of this document.*

Section 2 ‘Common Requirements and Recommendations’ of the Technical Specification is covered by this section (2.1) and section 3 of the Technical Specification ‘Home Organisation Requirements and Recommendations’ is covered by section 2.2 of this document. Section 4 of the Technical Specification is covered by sections 2.3-2.4 of this document.

> ***P5,R02.*** *Participants that choose to implement a visitor VLAN must observe the requirements set out in section 4 of this document.*

The University of Sussex has implemented a visitor VLAN. See Section 2.3 and 2.4 of this document.

> ***P5,R03.*** *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.*

The University of Sussex has a designated contact. In their absence, cover is provided by various members of the ITS Infrastructure Services team, with a single point of contact being the IT Services Enquiries desk.

> ***P5,R04.*** *Every log entry must state the date and time it was logged.*

RADIUS packets are logged with a timestamp in the record header. Database entries have their creation time recorded in the *Date* and *AcctStartTime* fields. See Appendix 1 ‘Logging’ for details.

> ***P5,R05.*** *Logs must be kept for at least three months, and for no longer than six months.*

RADIUS packet logs are kept for 93 days and database records 180 days. Debugging logs, when captured, are retained for only 7 days. See Appendix 1 ‘Logging’ for details.

> ***P6,R06.*** *Participants’ RADIUS (Remote Authentication Dial In Service) clients and servers must comply with RFC 2865 and RFC 2866.*

The University of Sussex uses FreeRADIUS 2.02 as its RADIUS server, HP ProCurve 2600 series switches and HP ProCurve HP 530 Wireless Access Points, all of which claim compliance with RFC 2865 (Remote Authentication Dial In User Service (RADIUS)) and RFC 2866 (RADIUS Accounting).

> ***P6,R07.*** *Participants' RADIUS clients' and servers' clocks must be configured to synchronise regularly with a reliable time source.*

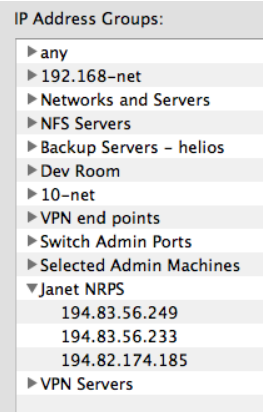
All RADIUS clients, RADIUS servers and any authentication sources used by the RADIUS servers synchronise with a stratum 2 server (ntp2.susx.ac.uk). This server is peered with ntp0.susx.ac.uk, ntp1.susx.ac.uk and ntp3.susx.ac.uk, with its time source taken from the JANET stratum 1 servers.

> ***P6,R08.*** *Participants must deploy at least one ORPS (organisational RADIUS proxy server).*

The University of Sussex has two RADIUS servers acting as ORPSs, *wolverine.uscs.susx.ac.uk (radius1.sussex.ac.uk)* and *cyclops.uscs.susx.ac.uk (radius2.sussex.ac.uk).*

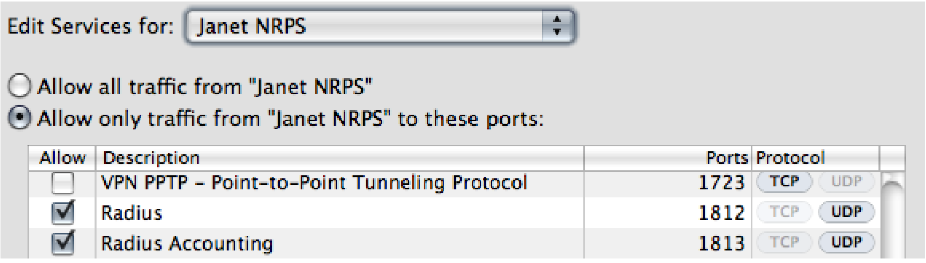
> ***P6,R09***. *Participants' ORPSs must be reachable from the JRS NRPS (National RADIUS Proxy Servers) on either UDP/1812 and UDP/1813 (recommended), or UDP/1645 and UDP/1646 (if required by the participating Organisation).*

University RADIUS servers listen on UDP/1812 (Authentication/Authorisation) and UDP/1813 (Accounting). Appropriate holes have been made in the ORPS OSX 10.4 Server Firewalls (see Figures 2.1 & 2.2) and the OpenBSD campus firewalls.



IP Address Groups:

- ▶ any
- ▶ 192.168-net
- ▶ Networks and Servers
- ▶ NFS Servers
- ▶ Backup Servers - helios
- ▶ Dev Room
- ▶ 10-net
- ▶ VPN end points
- ▶ Switch Admin Ports
- ▶ Selected Admin Machines
- ▼ Janet NRPS
  - 194.83.56.249
  - 194.83.56.233
  - 194.82.174.185
- ▶ VPN Servers



Edit Services for: Janet NRPS

○ Allow all traffic from "Janet NRPS"
● Allow only traffic from "Janet NRPS" to these ports:

Allow	Description	Ports	Protocol
□	VPN PPTP – Point-to-Point Tunneling Protocol	1723	TCP
☑	Radius	1812	UDP
☑	Radius Accounting	1813	UDP

Figure 2.1 (left) Figure 2.2 (right)

> ***P6,R10.*** *Participants' ORPSs must respond to ICMP (Internet Control Message Protocol) Echo Requests sent by the NRPS.*

ICMP Packets are allowed through the ORPS server firewalls and a hole has been created in the OpenBSD campus firewalls to allow ICMP packets from the NRPS to the ORPS.

These fragments from the OpenBSD PocketFilter (PF) configuration file on the campus firewalls permit inbound ICMP to the ORPSs:

```
# RADIUS servers that need to be pingable by JANET JRS
A_SUSSEX_RADIUS = "139.184.14.180/32, 139.184.14.181/32"

...

# Allow ICMP through to RADIUS servers (for JANET ROAMING)
pass in log quick on { $I_OUTSIDE } inet proto icmp \
    from any to { $A_SUSSEX_RADIUS } icmp-type echoreq keep state
pass in log quick on { $I_INSIDE } inet proto icmp \
    from { $A_SUSSEX_RADIUS } to any icmp-type echorep keep state
```

P6,R11. *Participants' ORPSs must log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded:*
R11.1. *The value of the user name attribute in the request.*
R11.2. *The value of the Calling-Station-Id attribute in the request.*

P6,12. *Participants must log all RADIUS accounting requests exchanged with the NRPS; the following information must be recorded:*
R12.1. *The value of the user name attribute in the request.*
R12.2. *The value of the accounting session identifier.*
R12.3. *The value of the request's accounting status type.*

University ORPSs keep logs of all RADIUS packets exchanged with NRPS. These include a list of all attributes and values present in the packet, and the type of packet. See Appendix 1 'Logging' for details.

2.2 Home Organisation Requirements

> ***P8,R13.*** *Home organisations' JRS user names must conform to the NAI (Network Access Identifier) specification (RFC 4282).*

University usernames are between 4 and 10 characters. *User-Name* strings follow the format [[:alnum:]]{3,8}@sussex.ac.uk, which conforms to RFC 4282.

> ***P8,R14.*** *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 University of Sussex realm is sussex.ac.uk. A parallel realm, susx.ac.uk, is also valid, but deprecated and does not appear in service documentation. These domains and all sub-domains are served by the University's DNS servers.

> ***P8,R15.*** *Home organisations must log all authentication attempts; the following information must be recorded.*
> ***R15.1.*** *The time that the authentication request was received.*
> ***R15.2.*** *The authentication result returned by the authentication database.*

All packets sent as responses to an NRPS request are logged. See Appendix 1 'Logging' for details.

> ***R15.3.*** *The reason given, if any, if the authentication was denied or failed.*

Simple diagnostic messages are returned in the *Reply-Message* attribute. These are logged both in the *postauth* database table and in packet logs. See Appendix 1 'Logging' for details.

> ***P9,R16.*** *Home organisations must configure their RADIUS server to authenticate one or more EAP (Extensible Authentication Protocol) types.*

Please see Appendix 4.1 'FreeRADIUS Configuration – EAP'.

> ***R16.1.*** *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 3580,11 within RADIUS Access-Accept packets.*

ORPSs are configured to authenticate supplicants using EAP-TTLS or EAP-PEAP (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, in compliance with RFC 2548.

> ***P9,R17.*** *Home organisations must create an authenticatable test account.*

A test account has been created in the University OpenLDAP directory service. All service authorisation attributes are null, apart from those used to allow RADIUS based authentication and access to the JANET Roaming service. This test account is also used in ‘ping’ checks to determine when NRPSs have come back online, as it tests the logical path to and from the NRPS.

> ***P10,R17.1.*** *The test account must be able to authenticate PAP and the EAP type(s) selected by the participant.*

NT-Hash and CRYPT passwords have been created for the test account, allowing authentication with PAP and any EAP type using PAP, MS-CHAP or MS-CHAPv2 as their inner method.

> ***P10,R17.2.*** *JRS Support (service@ja.net) 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 JRS Support informed as soon as possible.*

JANET Roaming Support will be informed by the designated JANET Roaming contact if any such situation arises.

> ***P10,R18.*** *Home organisations must educate their users to validate the certificate presented by a WRD NAS.*

The University of Sussex educates users not to use WRD NAS as they are inherently insecure and pose an unacceptable security risk. The University JANET Roaming website also advises users not to connect to networks bearing the eduroam-wep SSID for the same reason.

2.3 Visited Organisation Requirements

> ***P11,R19.*** *Visited organisations must implement at least one of the JRS1, JRS2 or JRS3 tiers.*

The University of Sussex has implemented the JRS2 tier.

> ***P11,R20.*** *Visited organisations must ensure that a non-JRS service cannot be mistaken by visitors for the participant's JRS service.*

No other services are advertised as 'JRS' (JANET Roaming Service) or 'eduroam'. All WAPs are managed by ITS Infrastructure Services, with naming conventions decided upon and documentation produced by ITS Client Services. ITS Client Services ensure that no other services could be mistaken for 'eduroam' in their documentation, and educate all visitors to the University on how they can utilise the different services available.

> ***P11,R21.*** *The 'eduroam' prefix is reserved for SSIDs used with the JRS service tiers.*

At the University of Sussex the WAPs only broadcast the 'eduroam' SSID, and central VLAN management performed by the ORPSs ensures that only 'eduroam' users will be placed on the Visitors' VLAN. The WAPs also scan for rogue stations broadcasting SSIDs conflicting with legitimate services; if any are found then immediate action is taken to disable the rogue station.

> ***P11,R22.*** *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 University of Sussex has implemented a separate VLAN for JANET Roaming users. Please see Figure 1 or section 1.1.2 for details.

> ***P11,R23.*** *Visited organisations that provide access to a JRS tier for local users, or visitors from organisations not participating in the JRS, must ensure that the user has read and agreed to both the JRS Policy and the local AUP.*

The ORPSs will only assign the Visitor VLAN to users authenticating via JANET Roaming. Local users are assigned a standard Roaming VLAN when connecting to the 'eduroam' SSID. This allows local users to configure their equipment to work with JANET Roaming, but not gain access to the Visitor VLAN.

> ***P11,R24.*** *Visited organisations must not offer visitors any wireless media other than IEEE 802.11.*

Only IEEE 802.11 wireless media is offered.

> ***P12,R25.*** *Visited organisations must forward RADIUS requests originating from JRS NASs and containing user names with unknown realms via an ORPS to an NRPS.*

Please see Appendix 4.3 ‘FreeRADIUS Configuration – Forwarding Configuration’.

> ***R25.1.*** *RADIUS Access-Requests must be addressed to UDP/1812.*
> ***R25.2.*** *RADIUS Accounting-Requests must be addressed to UDP/1813.*

The University of Sussex ORPSs are configured to do this. See R25 above for details.

> ***P12,R26.*** *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.*

The University of Sussex has only configured internal realms for global DNS domains that it administers.

> ***P12,R27.*** *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).*

The University of Sussex does not forward requests to external RADIUS servers other than the JANET Roaming NRPS.

> ***P12,R28.*** *Visited organisations must not otherwise forward requests to other JRS participants.*

The University of Sussex does not forward requests to external RADIUS servers other than the JANET Roaming NRPS.

> ***P13,R29.*** *Visited organisations must deploy NASs that include the following RADIUS attributes within Access-Request packets.*
> ***R29.1.*** *The supplicant’s MAC address within the Caller-Station-ID attribute.*
> ***R29.2.*** *The NAS’s IP address within the NAS-IP-Address attribute.*

All NASs used at the University of Sussex include this information in all accounting and access request packets.

> ***P14,R30.*** *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.*
> ***R30.1.*** *IPv6 Tunnel Broker NAT traversal: UDP/3653 and TCP/3653 egress and established.*
> ***R30.2.*** *IPSec NAT traversal: UDP/4500 egress and established.*
> ***R30.3.*** *Cisco IPSec NAT traversal: TCP/10000 egress and established.*
> ***R30.4.*** *PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.*
> ***R30.5.*** *OpenVPN: TCP/5000 egress and established.*

R30.6. *SSH: TCP/22 egress and established.*
R30.7. *HTTP: TCP/80 egress and established.*
R30.8. *HTTPS: TCP/443 egress and established.*
R30.9. *LDAP: TCP/389 egress and established.*
R30.10. *LDAPS: TCP/636 egress and established.*
R30.11. *IMSP: TCP/406 egress and established.*
R30.12. *IMAP4: TCP/143 egress and established.*
R30.13. *IMAP3: TCP/220 egress and established.*
R30.14. *IMAPS: TCP/993 egress and established.*
R30.15. *POP: TCP/110 egress and established.*
R30.16. *POP3S: TCP/995 egress and established.*
R30.17. *Passive (S)FTP: TCP/21 egress and established.*
R30.18. *SMTPS: TCP/465 egress and established.*
R30.19. *Message submission: TCP/587 egress and established.*
R30.20. *RDP: TCP/3389 egress and established.*
R30.21. *VNC: TCP/5900 egress and established.*
R30.22. *Citrix: TCP/1494 egress and established.*

No IP filtering that would restrict access to the protocols listed under R30 has been implemented.

P15,R31. *Visited organisations deploying application or 'interception' proxies on the visitor LAN must publish this fact on their JRS website.*
P15,R32. *If an application proxy is not transparent, the visited organisation must also provide documentation on the configuration of applications to use the proxy.*

No application or 'interception' proxies are present on the Visitor VLAN.

P15,R33. *Visited organisations must publish a JRS website which must be accessible from both the Internet and from within the organisation to allow visitors to access it easily. The website must include the following information as a minimum:*
R33.1. *The participant's AUP (Acceptable Use Policy).*

The standard University of Sussex AUP is available on the University JANET Roaming website.

R33.2. *Sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered, the JRS Tier(s), and SSIDs.*

A detailed list of locations where the visited service can be accessed is available on the University JANET Roaming website.

R33.3. *Where applicable, the information specified in section 4.6 regarding application and interception proxies.*

No application or interception proxies operate on the Visited VLAN.

> ***P16,R34.*** *A broadcast SSID of 'eduroam' must always be used for JRS wireless services, except in the following circumstances.*
>
> > ***R34.1.*** *A broadcast SSID of 'eduroam-wep' may be used with WEP but only where the 'eduroam' SSID is required by another JRS wireless service.*
> > ***R34.2.*** *A broadcast SSID of 'eduroam-web' may be used with WRD but only where the 'eduroam' SSID is required by another JRS wireless service.*

Only the 'eduroam' SSID is broadcast.

> ***P17,R43.*** *Visited organisations must allocate IPv4 addresses to visitors using DHCP.*

An instance of the ISC DHCP server, version 3.x, is used to allocate IPv4 addresses for eduroam users. The configuration file for this server is shown below:

```
ddns-update-style none;
authoritative;

shared-network EDUROAM {
  option domain-name "sussex.ac.uk";

  subnet 192.33.16.0 netmask 255.255.255.0 {
    option domain-name-servers 139.184.32.25, 139.184.32.26,
       139.184.32.27;
    option routers 192.33.16.1;
    option subnet-mask 255.255.255.0;
    default-lease-time 10800;
    max-lease-time 86400;

    pool {
      deny dynamic bootp clients;
      range 192.33.16.2 192.33.16.254;
      allow unknown clients;
    }
  }
}
```

> ***P17,R44.*** *Visited organisations must log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.*

ISC DHCP Servers log all leases allocated to visitors and their corresponding MAC addresses.

> ***P18,R45.*** *Visited organisations must log NAT address mappings, if used.*

No NAT operates on the Visitor VLAN.

2.4 Visited Organisation Requirements – JRS2 Specific

> ***P17,R38.*** *The JRS2 and JRS3 tiers must only implement IEEE 802.1X; no form of WRD is permitted.*

Only 802.1x has been implemented; no WRD services are in place.

> ***P17,R39.*** *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.*

All NASs operating with 802.11 media support this.

> ***P17,R40.*** *Only a single user is permitted per NAS port.*

WAPs will only allow one user per wireless station. Unfortunately due to compatibility issues with HP ProCurve switches and Windows Vista, it is possible to connect two clients to a single wired NAS port. This information is not published and the configuration will revert to one which enforces a single user per wired NAS port as soon as Windows Vista compatibility issues have been resolved.

> ***P17,R46.*** *The JRS2 tier may implement WEP; if it does not, it must implement WPA.*

The University of Sussex has implemented WPA and WPA2.

> ***P19,R49.*** *The JRS2 tier should implement WPA; if not, it must implement WEP.*

The University of Sussex has implemented WPA and WPA2.

Appendix 1: Logging

Appendix 1.1 File Based Logging

RADIUS packet logs are created using *rlm_detail*, a module included in all standard FreeRADIUS installations. *rlm_detail* creates copies of the incoming and outgoing packets with full attribute and value expansion, and may be instantiated multiple times to create separate files for packets passing through different sections of the server.

In addition to packet logs the University of Sussex also keeps full server logs, with the server running in the first level of debugging mode ***–x***.

Logs produced by *rlm_detail* will typically look like this:

```
      139.184.9.170 - Fri Feb  1 15:08:44 2008
            Packet-Type = Access-Accept
            Service-Type = Framed-User
            Framed-MTU = 1480
            Framed-Routing = None
            Framed-Protocol = PPP
            Framed-Compression = Van-Jacobson-TCP-IP
            Reply-Message = "User ac221 authenticated for Eduroam Service"
            User-Name = "ac221@loopback.sussex.ac.uk"
            Tunnel-Type:0 = VLAN
            Tunnel-Medium-Type:0 = IEEE-802
            Tunnel-Private-Group-Id:0 = "610"
            EAP-Message = 0x03090004
            Message-Authenticator = 0x00000000000000000000000000000000
```

Appendix 1.1.1 File Based Log Configuration

The University of Sussex configuration is similar to the default supplied with FreeRADIUS 2. The main differences are that the directory structure is organised by date as opposed to *Client-IP-Address*, and that the log files themselves are rotated every hour instead of every day. This allows easier deletion and archival of packet logs by date, and faster location of packet logs with information pertinent to a specific UID.

As the attribute *NAS-IP-Address* is generated by the NAS itself and can sometimes be inaccurate, the source address of the packet is logged above each entry. In the case of a request, *Packet-Src-IP-Address* reflects the IP address of the NAS or Proxy Server where the UDP packet originated. With a response packet, *Packet-Src-IP-Address* reflects the IP of the device that sent the request for which a response is being formulated.

The User-Password is suppressed in all relevant logging modules, since inclusion of cleartext passwords in logs is rarely desirable.

Accounting

The accounting log records the contents of any accounting request packets received by the UoS ORPS. This is to maintain compliance with JANET Roaming specifications.

```
detail accounting_log {
      detailfile = ${radacctdir}/%Y%m%d/accounting-detail-%H:00
      header = "%{Packet-Src-IP-Address} - %t"
      detailperm = 0600
}
accounting {
      accounting_log
}
```

Authorisation

The authorisation log records authentication requests received by the University's ORPS. This is primarily for debugging.

```
detail auth_log {
      detailfile = ${radacctdir}/%Y%m%d/request-detail-%H:00
      detailperm = 0600
      header = "%{Packet-Src-IP-Address} - %t"
      log_packet_header = yes
      suppress {
            User-Password
      }
}
authorize {
      …
      auth_log
}
```

Post Authentication

The post authentication log records the reply sent to the NAS. This is primarily used for debugging.

```
detail reply_log {
      detailfile = ${radacctdir}/%Y%m%d/reply-detail-%H:00
      header = "%{Packet-Src-IP-Address} - %t"
      detailperm = 0600
}
post-auth {
      ...
      reply_log
      Post-Auth-Type REJECT {
            ...
            reply_log
      }
}
```

Pre Proxy

The Pre Proxy log records requests sent to the JANET NRPS. This is to maintain compliance with JANET Roaming specifications.

```
detail pre_proxy_log {
      detailfile = ${radacctdir}/%Y%m%d/pre-proxy-detail-%H:00
      detailperm = 0600
      header = "%{Packet-Src-IP-Address} - %t"
      suppress {
            User-Password
      }
}
pre-proxy {
      ...
      pre_proxy_log
}
```

Post Proxy

The Post Proxy log records responses to requests sent to the JANET NRPS. This is to maintain compliance with JANET Roaming specifications.

```
detail post_proxy_log {
      detailfile = ${radacctdir}/%Y%m%d/post-proxy-detail-%H:00
      header = "%{Packet-Src-IP-Address} - %t"
      detailperm = 0600
}
post-proxy {
      ...
      post_proxy_log
}
```

Appendix 1.1.2 File Based Log Rotation

Packet logs are archived after two days (to allow easy access to recent logs), and rotated out of existence after 93 days. Server (debugging) logs are archived after 2 days and rotated out of existence after 7 days. Server log rotation is done using the UNIX *logrotate* utility, which in turn calls a bash script to move, archive, and delete packet logs. In addition to log rotation the *logrotate* utility also uses *launchctl*, the control utility for *launchd* (the Mac OS X service control daemon, similar to Solaris svcadm or Linux /etc/init.d) to restart the server and allow new NAS to be added to the ORPSs client list.

Logrotate configuration script

```
/var/log/radiusd/radius.log {
      daily
      rotate 7
      prerotate
            launchctl unload /Library/LaunchDaemons/org.freeradius
      endscript
      create 640 daemon admin
      compress
      delaycompress
      nomail
      postrotate
            launchctl load /Library/LaunchDaemons/org.freeradius
            /usr/local/etc/radiusd/rotate_pl.sh
      endscript
}
```

FreeRADIUS 2 launchd service

FreeRADIUS 2 by default will attempt to daemonise on startup (spawn a child and kill the foreground process), at which point *launchd* will note the death of the original foreground process and attempt to start a new instance of the daemon. The solution is to include the *–f* flag in the arguments list, which forces the FreeRADIUS daemon to remain in the foreground. The server is also run in the first level of debugging *–x* (additional *x*'s increase the debugging level), so that detailed information is generated in the server log about potential issues that may affect authentication.

Launchd FreeRADIUS service XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Debug</key>
        <true/>
        <key>Label</key>
        <string>org.freeradius</string>
        <key>OnDemand</key>
        <false/>
        <key>ProgramArguments</key>
        <array>
                <string>/usr/local/freeradius/sbin/radiusd</string>
                <string>-x</string>
                <string>-d</string>
                <string>/etc/raddb</string>
                <string>-f</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
        <key>ServiceDescription</key>
        <string>FreeRADIUS Daemon</string>
</dict>
</plist>
```

BASH archival script (/usr/local/etc/radiusd/rotate_pl.sh)

```
#!/bin/bash
# Daily packet log rotation and archiving script.

# Logging and archive paths
LOG_DIR='/var/log/radiusd'
ARCHIVE_DIR='/var/log/radiusd/archive'

# How many days do we keep logs for
LOG_R_DAYS=93
# How many days are logs exempt from archival or deletion
LOG_E_DAYS=2

# Output directory name $1 days ago.
# Work around featureless version of date in OSX 10.4
pastDate ()
{
if [ -z "$1" ] ; then
        date +%G%m%d
else
        date -r $(('date +%s' - $(($1 * 86400)))) +%G%m%d
fi
}
# Check existence of relevant directories
if [ -d "$LOG_DIR" -a -r "$LOG_DIR" ] ; then
      cd $LOG_DIR
      if [ ! -d "$ARCHIVE_DIR" ] ; then
            echo "Creating archive dir '$ARCHIVE_DIR'"
            mkdir $ARCHIVE_DIR
            if [ $? -ne 0 ] ; then
                  echo "Can't create archive dir '$ARCHIVE_DIR'"
                  exit 64
            fi
      fi
else
      echo "Can't read log directory '$LOG_DIR'"
      exit 64
fi

E_DATE='pastDate $LOG_E_DAYS' ; echo "Logs after $E_DATE will be ignored"
R_DATE='pastDate $LOG_R_DAYS' ; echo "Logs and archives prior to $R_DATE
will be deleted"

# Archive and remove directories
for LOGDD in 'ls $LOG_DIR | egrep '^[0-9]{4}[0-1][1-9][0-3][0-9]$''; do
      LOGFP="$LOG_DIR/$LOGDD"
      if [ "$E_DATE" -lt "$LOGDD" ] ; then
            echo "Ignoring '$LOGFP'"
      elif [ "$R_DATE" -gt "$LOGDD" ] ; then
            echo "Removing '$LOGFP'"
            rm -rf $LOGDD
      else
            echo "Archiving '$LOGFP'"
            ARCF="$LOGDD.tar.gz"
            tar -czf $ARCF $LOGDD
            if [ $? -ne 0 ] ; then
```

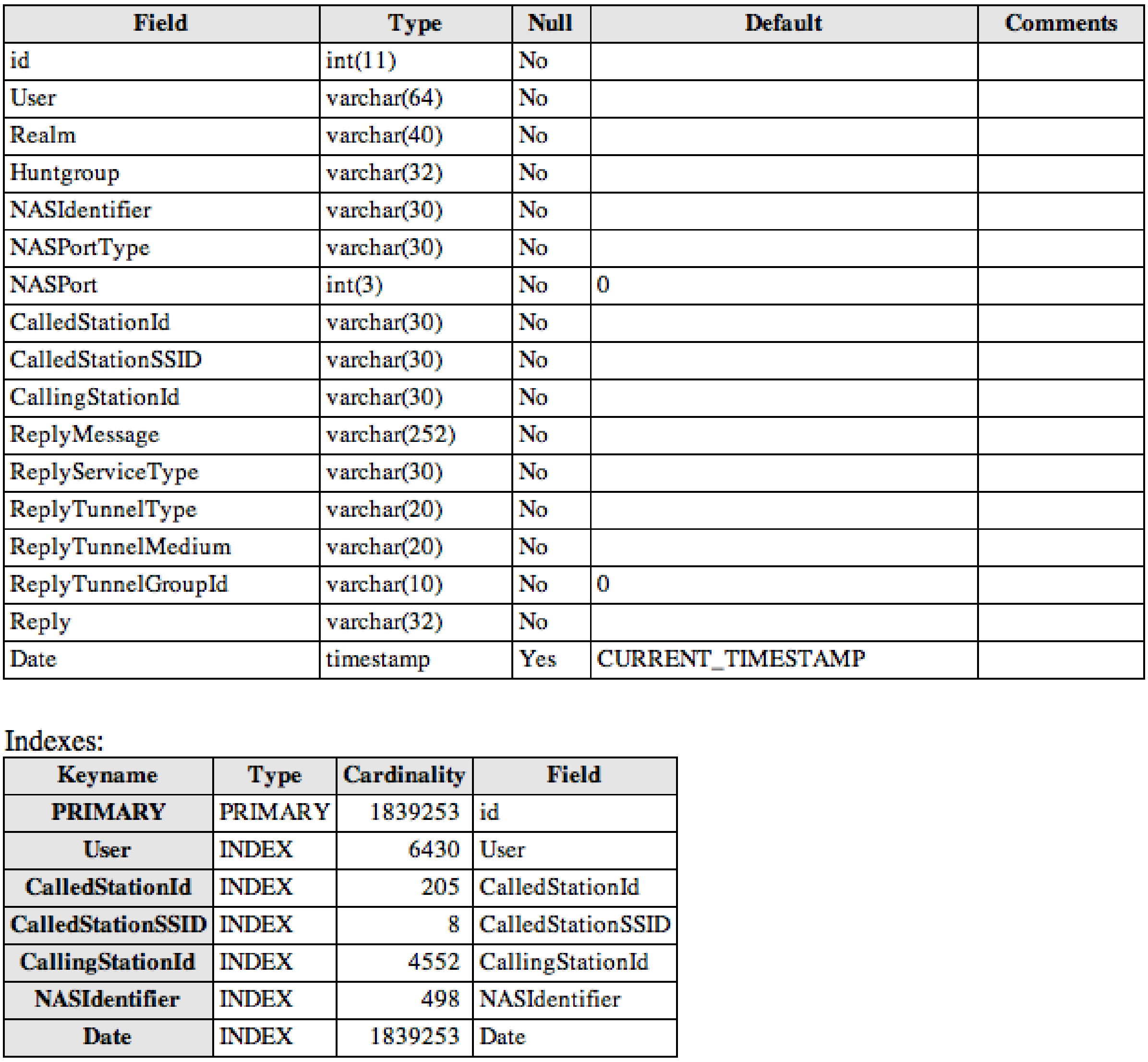
```
                  echo "Error creating archive for $LOGFP"
                  exit 65
            else
                  rm -rf $LOGDD
                  mv $ARCF $ARCHIVE_DIR
            fi
      fi
done

# Remove old archives
for ARCDD in 'ls $ARCHIVE_DIR | egrep -o '^[0-9]{4}[0-1][1-9][0-3][0-9]'';
do
      ARCFP="$ARCHIVE_DIR/$ARCDD.tar.gz"
      if [ "$R_DATE" -gt "$ARCDD" ] ; then
            echo "Removing '$ARCFP'"
            rm -rf "$ARCFP"
      else
            echo "Ignoring archive '$ARCFP'"
      fi
done
exit
```

Appendix 1.2 Database Logging

In addition to packet logs, post-auth records and accounting data are written to a MySQL (MyISAM) database. Records in this database pertaining to eduroam users are removed after 180 days, while local records generated by local users are kept in accordance with the University's data retention policy.

SQL Table Structure

Post Authentication (postauth)



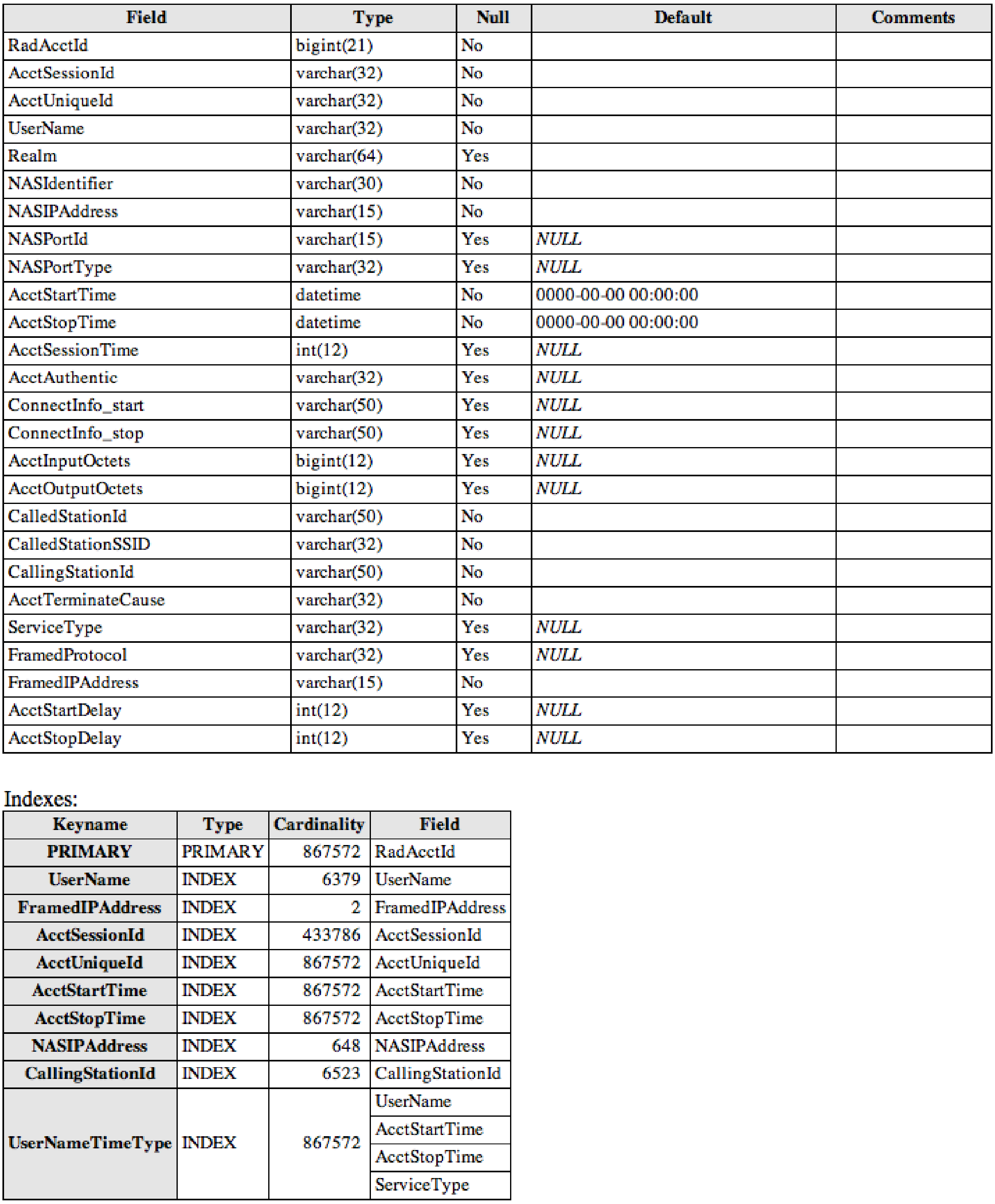
Field	Type	Null	Default	Comments
id	int(11)	No		
User	varchar(64)	No		
Realm	varchar(40)	No		
Huntgroup	varchar(32)	No		
NASIdentifier	varchar(30)	No		
NASPortType	varchar(30)	No		
NASPort	int(3)	No	0	
CalledStationId	varchar(30)	No		
CalledStationSSID	varchar(30)	No		
CallingStationId	varchar(30)	No		
ReplyMessage	varchar(252)	No		
ReplyServiceType	varchar(30)	No		
ReplyTunnelType	varchar(20)	No		
ReplyTunnelMedium	varchar(20)	No		
ReplyTunnelGroupId	varchar(10)	No	0	
Reply	varchar(32)	No		
Date	timestamp	Yes	CURRENT_TIMESTAMP	

Indexes:

Keyname	Type	Cardinality	Field
PRIMARY	PRIMARY	1839253	id
User	INDEX	6430	User
CalledStationId	INDEX	205	CalledStationId
CalledStationSSID	INDEX	8	CalledStationSSID
CallingStationId	INDEX	4552	CallingStationId
NASIdentifier	INDEX	498	NASIdentifier
Date	INDEX	1839253	Date

Figure 3.1 SQL Table Structure (Post Authentication logging table)

Accounting (radacct)



Field	Type	Null	Default	Comments
RadAcctId	bigint(21)	No		
AcctSessionId	varchar(32)	No		
AcctUniqueId	varchar(32)	No		
UserName	varchar(32)	No		
Realm	varchar(64)	Yes		
NASIdentifier	varchar(30)	No		
NASIPAddress	varchar(15)	No		
NASPortId	varchar(15)	Yes	*NULL*	
NASPortType	varchar(32)	Yes	*NULL*	
AcctStartTime	datetime	No	0000-00-00 00:00:00	
AcctStopTime	datetime	No	0000-00-00 00:00:00	
AcctSessionTime	int(12)	Yes	*NULL*	
AcctAuthentic	varchar(32)	Yes	*NULL*	
ConnectInfo_start	varchar(50)	Yes	*NULL*	
ConnectInfo_stop	varchar(50)	Yes	*NULL*	
AcctInputOctets	bigint(12)	Yes	*NULL*	
AcctOutputOctets	bigint(12)	Yes	*NULL*	
CalledStationId	varchar(50)	No		
CalledStationSSID	varchar(32)	No		
CallingStationId	varchar(50)	No		
AcctTerminateCause	varchar(32)	No		
ServiceType	varchar(32)	Yes	*NULL*	
FramedProtocol	varchar(32)	Yes	*NULL*	
FramedIPAddress	varchar(15)	No		
AcctStartDelay	int(12)	Yes	*NULL*	
AcctStopDelay	int(12)	Yes	*NULL*	

Indexes:

Keyname	Type	Cardinality	Field
PRIMARY	PRIMARY	867572	RadAcctId
UserName	INDEX	6379	UserName
FramedIPAddress	INDEX	2	FramedIPAddress
AcctSessionId	INDEX	433786	AcctSessionId
AcctUniqueId	INDEX	867572	AcctUniqueId
AcctStartTime	INDEX	867572	AcctStartTime
AcctStopTime	INDEX	867572	AcctStopTime
NASIPAddress	INDEX	648	NASIPAddress
CallingStationId	INDEX	6523	CallingStationId
UserNameTimeType	INDEX	867572	UserName AcctStartTime AcctStopTime ServiceType

Figure 3.2 SQL Table Structure (Post Authentication accounting table)

Simple record deletion queries

Because the University of Sussex RADIUS MySQL database uses MyISAM as its database engine, delete queries require the target table to be locked. Whilst the lock is in place, all FreeRADIUS modules attempting to run operations against the database will be blocked. If the table remains locked for more than the authentication timeout period on the NAS (typically 30 seconds) then authentication requests will start to fail. Additionally, every query waiting for the table lock to be lifted uses one MySQL connection and after the connection pool is exhausted, authentication attempts will either go unanswered or be rejected. It is therefore imperative that operations requiring table locks only run for a few seconds.

To mitigate the disruptive effect of delete queries, all fields used in delete conditions are indexed and queries are run hourly to reduce the number of rows to be deleted at any one time.

Eduroam accounting data removal query

Remove all accounting records over 180 days old, where authentication realm was an eduroam institution.

```
DELETE FROM 'radacct' WHERE 'AcctStartTime' <
FROM_DAYS((TO_DAYS(NOW()) - 180)) AND 'Realm' = 'jrs'
```

Eduroam post-authentication data removal query

Remove all post authentication records over 180 days old, where authentication realm was an eduroam institution.

```
DELETE FROM 'postauth' WHERE 'Date' < FROM_DAYS((TO_DAYS(NOW()) -
180)) AND 'Realm' = 'jrs'
```

Appendix 2: Wireless Access Points (WAPs)

Hewlett Packard AP 530 Wireless Access Points make up the bulk of the wireless infrastructure at the University of Sussex. The access points operate in a standalone configuration with no central management devices. This makes them extremely resilient to network outages and other issues which can impact negatively on centrally managed systems.

Appendix 2.1: Configuration of the eduroam BSSID (WAP 530 Access Point Firmware Revision W.A.2.10)

WAP 530s have both a graphical web interface (HTTP/HTTPS), and a Command Line Interface (SSH/Telnet/Console). As the CLI lends itself better to automated configuration, this method will be documented here.

1. Connect to the access point using either an ssh/telnet client:

   ```
   ssh –v2 admin@hp-w-engg1-hd-bodny.net.susx.ac.uk
   ```

   or by using a terminal with HP console cable and serial adaptor with the following settings:

   ```
   Baud-Rate: 9600 (Default)
   Data-Bits: 8
   Stop-Bits: 1
   Parity: None
   Flow-Control: None
   ```

2. Login

3. Enter configuration mode

   ```
   ProCurve Access Point 530# conf t
   ```

4. Choose an appropriate BSSID index (any integer from 1-16)

   ```
   ProCurve Access Point 530# radio 1
   wlan <BSSID-Index>
   ```

5. Set the SSID of the BSSID to ‘eduroam’ and give it a description.

   ```
   ssid eduroam
   description "Eduroam 802.1x auth wpa/wpa2 tkip/aes BSSID."
   ```

6. Select the basic security set. (N.B. `wpa-802.1x` is equivalent to WPA-Enterprise.) Enabling WPA2 is optional, since doing so may cause issues with certain broken wireless clients that, when given a choice between WPA/WPA2, fail to choose either!

   ```
   security wpa-8021x
   wpa-allowed
   wpa2-allowed
   ```

7. Select allowed ciphers; it’s best to have both TKIP and AES for compatibility reasons.

   ```
   wpa-cipher-aes
   wpa-cipher-tkip
   ```

8. RSN-Preauthentication is optional but recommended as it allows quick association when roaming between wireless cells. This feature will likely be superseded by 802.11r. N.B. RSN-Preauthentication is a feature of WPA2, so will only work with WPA2 enabled clients.
   ```
         rsn-preauthentication
   ```

9. Add RADIUS servers and shared secrets.
   ```
         radius primary key <shared_secret>
         radius primary ip <radius_server_ip2>
         radius primary port 1812
         radius secondary key <shared_secret>
         radius secondary ip <radius_server_ip1>
         radius secondary port 1812
         radius-accounting primary key <shared_secret>
         radius-accounting primary ip <radius_server_ip2>
         radius-accounting primary port 1813
         radius-accounting secondary key <shared_secret>
         radius-accounting secondary ip <radius_server_ip1>
         radius-accounting secondary port 1813
   ```

10. Enable the WLAN
    ```
          Enable
    ```

11. Exit and enable the radio (if not already enabled)
    ```
          exit
          enable
    ```

12. Save configuration changes
    ```
          write mem
    ```

13. Check everything works.

```
ProCurve Access Point 530# show stations
Station        On WLAN (radio index/WLAN index)       Auth.  Assoc.  Fwd.
---------------------------------------------------------------------------
00:14:a7:fa:9d:1a  eduroam (1/2)                       Yes    Yes     Yes
00:13:02:42:39:43  eduroam (1/2)                       Yes    Yes     Yes
```

Appendix 3: Wired Network

The majority of the edge network at the University comprises HP ProCurve 2600 series switches. These come in 26 and 50 port configurations, with two Dual Personality ports (SFP GBIC or 1000baseT) for uplinks, and 10/100 Auto MDIX Ethernet as edge ports. Most ports on campus are left at 10/100 Auto, with the exception of ports in residences which are set to operate at 10 Half-Duplex for compatibility reasons.

Unless there is the luxury of additional switch capacity and network outlets to create dedicated eduroam ports, the only sensible way to provide the eduroam service on wired infrastructure is via dynamic VLAN assignment. On HP ProCurve 2600 edge switches, VLANs assigned dynamically must be present on the switch as either statically configured VLANs or as VLANs learned via GVRP (a protocol for the dynamic distribution of VLANs).

Appendix 3.1: Configuration of Wired Infrastructure Switches for Use with the eduroam Service

ProCurve 2600 series have both a graphical web interface (HTTP/HTTPS), and a Command Line Interface (SSH/Telnet/Console). As the CLI lends itself better to automated configuration, this method will be documented here.

1. Connect to the access point using either an ssh/telnet client, e.g.:

   ```
   ssh –v 2 admin@hp-e-its-dev8021x-sw1.net.susx.ac.uk
   ```

   or by using a terminal with HP console cable and serial adaptor with the following parameters:

   ```
   Baud-Rate: 9600 (Default)
   Data-Bits: 8
   Stop-Bits: 1
   Parity: None
   Flow-Control: None
   ```

2. Having logged in, elevate to manager (if required) and enter configuration mode:

   ```
   hp-e-its-dev8021x-sw1# en
   hp-e-its-dev8021x-sw1# conf t
   ```

3. Add RADIUS servers:

   ```
   radius-server host <radius_server_ip1> auth-port 1812 acct-port 1813
   radius-server host <radius_server_ip2> auth-port 1812 acct-port 1813
   ```

4. Set the global shared secret (this can be set on a per server basis if required):

   ```
   radius-server key <shared_secret>
   ```

5. Set the port-access RADIUS type:

   ```
   aaa authentication port-access eap-radius
   ```

6. Enable the authenticator on select ports:

   ```
   aaa port-access authenticator <Port range>
   aaa port-access authenticator <Port range> control auto
   aaa port-access authenticator <Port range> client-limit 2
   ```

```
      aaa port-access authenticator <Port range> unauth-vid <Unauth
VID>
      aaa port-access authenticator active
```

7. Enable RADIUS accounting:

```
      aaa accounting exec start-stop radius
      aaa accounting network start-stop radius
      aaa accounting system start-stop radius
      aaa accounting update periodic 15
```

8. Save configuration:

```
      hp-e-its-dev8021x-sw1(config)# write mem
```

9. Confirm everything works:

```
hp-e-es-b01-f31-kit-sw1# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

             Current  Current        RADIUS ACL
 Port  Status VLAN ID  Port COS       Applied?
 ----  ------ -------- ----------- -----------
 5     Closed 1        No-override    No
 6     Open   610      No-override    No
 7     Closed 1        No-override    No
 8     Closed 1        No-override    No
 9     Closed 1        No-override    No
 10    Closed 1        No-override    No
 11    Closed 1        No-override    No
 12    Closed 1        No-override    No

hp-e-es-b01-f31-kit-sw1# show port-access authenticator 1-24 session-
counters

 Port Access Authenticator Session Counters

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

                               Session     Session
 Port  Frames In  Frames Out  Time(sec.)  Status      User
 ---- ---------- ---------- ---------- ---------- -------------
 5     10652      1293392     0
 6     31151      4981591     15303       in-progress ac221@loopback.sussex.ac.uk
 7     1336       997688      0
 12    5061       73777       0
```

Appendix 4: FreeRADIUS Configuration

Appendix 4.1: EAP

```
eap {
      default_eap_type = peap
      timer_expire = 60
      ignore_unknown_eap_types = no
      cisco_accounting_username_bug = no
      gtc {
            challenge = "Password: "
            auth_type = PAP
      }
      tls {
            certdir = ${raddbdir}/certs
            cadir = ${raddbdir}/certs
            private_key_password = whatever
            private_key_file = ${certdir}/radius.sussex.ac.uk.key
            certificate_file = ${certdir}/radius.sussex.ac.uk.crt
            CA_file = ${certdir}/sussexCA.pem
            dh_file = ${certdir}/dh
            random_file = /dev/urandom
            check_crl = no
            cipher_list = "DEFAULT"
      }
      ttls {
            default_eap_type = mschapv2
            copy_request_to_tunnel = yes
            use_tunneled_reply = yes
            virtual_server = "default-inner"
      }
      peap {
            default_eap_type = mschapv2
            copy_request_to_tunnel = yes
            use_tunneled_reply = yes
            proxy_tunneled_request_as_eap = no
            virtual_server = "default-inner"
      }
      mschapv2 {
      }
}
```

Appendix 4.2: Realm Configuration

ORPS specific configuration entries, such as shared secrets with the NRPSs, are stored in a separate directory to allow easy updating of global configuration files.

${raddbdir}/radiusd.conf

```
raddbdir-local = ${sysconfdir}/raddb.local
...
$INCLUDE  ${raddbdir-local}/proxy.conf
$INCLUDE  ${raddbdir}/proxy.conf
$INCLUDE  ${confdir}/clients.conf
```

${raddbdir-local}/proxy.conf

```
jrs_config {
      test_username = 'jrs-test@sussex.ac.uk'
      test_password = '<Test Account Password>'
      secret0 = '<NRPS0 Secret>'
      secret1 = '<NRPS1 Secret>'
      secret2 = '<NRPS2 Secret>'
}
```

${raddbdir}/proxy.conf

The JANET Roaming realm should be defined with the ‘nostrip’ option, else the server will strip off the domain component of the *User-Name* attribute prior to proxying.

```
# Realms
realm jrs {
      nostrip
      auth_pool = jrs_auth
      acct_pool = jrs_acct
}
```

Type can be set to either ‘client-balance’, ‘client-port-balance’ or ‘fail-over’. It is best practice not to use ‘load-balance’ with EAP requests.

```
# Server Pools
server_pool jrs_auth {
      type = client-port-balance
      home_server = jrs0
      home_server = jrs1
      home_server = jrs2
}
server_pool jrs_acct {
      type = client-port-balance
      home_server = jrs0
      home_server = jrs1
      home_server = jrs2
}
```

Setting status_check to request and specifying a local test account tests the ORPS’s ability to proxy packets to the NRPS, and the NRPS’s ability to forward on packets.

```
# Home Servers
home_server jrs0 {
      status_check = request
      username = ${jrs_config.test_username}
      password = ${jrs_config.test_password}
      ipaddr = roaming0.ja.net
      secret = ${jrs_config.secret0}
      port = 1812
      type = auth+acct
}
home_server jrs1 {
      status_check = request
      username = ${jrs_config.test_username}
      password = ${jrs_config.test_password}
      ipaddr = roaming1.ja.net
      port = 1812
      type = auth+acct
}
home_server jrs2 {
      status_check = request
      username = ${jrs_config.test_username}
      password = ${jrs_config.test_password}
      ipaddr = roaming2.ja.net
      secret = ${jrs_config.secret2}
      port = 1812
      type = auth+acct
}
```

${raddbdir}/clients.conf

```
client roaming0.ja.net {
      shortname = jrs0
      nastype = other
      secret = ${jrs_config.secret0}
}
client roaming1.ja.net {
      shortname = jrs1
      nastype = other
      secret = ${jrs_config.secret1}
}
client roaming2.ja.net {
      shortname = jrs2
      nastype = other
      secret = ${jrs_config.secret2}
}
```

Appendix 4.3: Forwarding Configuration

${raddbdir}/dictionary

```
#     Supposed domain of the user
ATTRIBUTE         Stripped-User-Domain                3009  string
```

${raddbdir}/unlangl/uidrewrite.conf

Because FreeRADIUS 2 uses the *libc* regular expression library, only POSIX 1003.2 compatible regular expressions can be used with ‘unlang’. Unfortunately this limits the feature set available for use with expressions.

The lack of support for conditional sub-expressions or atomic look-around means it is very difficult (if not impossible) to write an expression that is compliant with RFC 4282 Network Access Identifiers. The expression listed below will work for all NAIs except those which contain ‘@’ characters prefixed with a backslash.

Using the FreeRADIUS module *rlm_realm* is no better, as it runs the standard strrchr (suffix) and strchr (prefix) functions over the *User-Name* string and does not take into account backslash ‘escaped’ characters.

```
# USERNAME FORMATTING
# User-Name Formatting, extracts Realm, User.
if("%{User-Name}" =~ /^([^@]*)(@([-[:alnum:].]+))?$/){
      update request {
            Stripped-User-Name := "%{1}"
      }
      if("%{3}"){
            update request {
                  Stripped-User-Domain = "%{3}"
            }
      }else{
            update request {
                  Stripped-User-Domain = ‘sussex.ac.uk’
            }
      }
}
# Username in unrecognised format
else{
      reject
}
```

${raddbdir-local}/preproxy.conf

```
# PROXYING LOGIC
# Can't have null case statements, terminate null realms on this server
switch "%{Stripped-User-Domain}" {
      # Terminate requests from this domain as local realm
      case 'sussex.ac.uk'{
            update request {
                  Realm := 'local'
            }
      }
      # Terminate requests from this domain as local realm
      case 'susx.ac.uk' {
            update request {
                  Realm := 'local'
            }
      }
      # JRS Is the default realm
      case {
            update control {
                  Proxy-To-Realm := 'jrs'
            }
            update request {
                  Realm := 'jrs'
            }
      }
}
```

${raddbdir}/sites-available/default-outer

```
server default-outer {
      ...
      authorize {
            ...
            # Format incoming username string
            # * Username component extraction
            $INCLUDE  ${raddbdir}/unlang/uidrewrite.conf

            # Preproxy logic using V2 conditions
            # * Proxying logic
            $INCLUDE  ${raddbdir-local}/unlang/preproxy.conf
            ...
      }
      ...
      preacct {
            ...
            # Format incoming username string
            # * Username component extraction
            $INCLUDE  ${raddbdir}/unlang/uidrewrite.conf

            # Preproxy logic using V2 conditions
            # * Proxying logic
            $INCLUDE  ${raddbdir-local}/unlang/preproxy.conf
            ...
      }
}
```

Appendix 4.4: Inner/ Outer Identity Handling

In standard terminology the user identifier provided in the EAP-Identity packet from the supplicant is typically referred to as the *outer identity*, and the Identity provided with inner or phase 2 methods such as MSCHAPv2 is typically referred to as the *inner identity*.

As the outer identity is freely available for any intermediary proxy to use, it can be used to route requests through proxy chains such as the *eduroam* network. The Inner identity is known only by the Supplicant and the Authenticator, and is used for identifying the user attempting to authenticate. When the two identities differ, for example because the user wishes to preserve their privacy, it can cause issues in associating accounting information with a specific user.

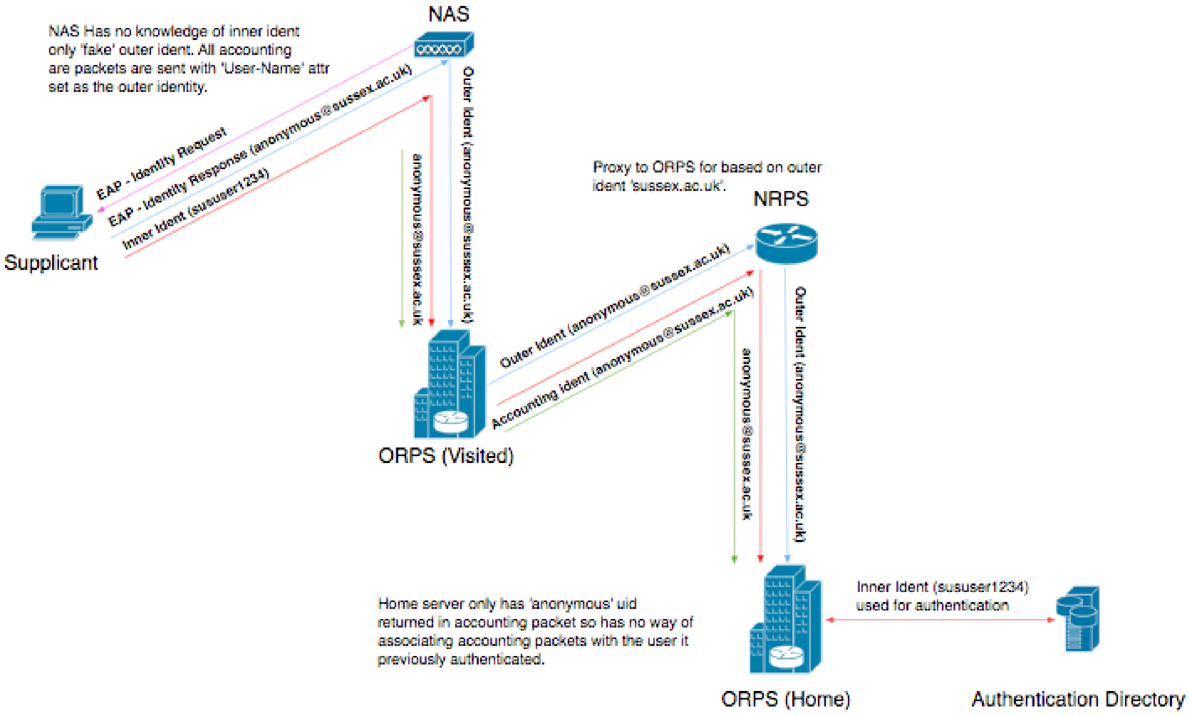

NAS Has no knowledge of inner ident
only 'fake' outer ident. All accounting
are packets are sent with 'User-Name' attr
set as the outer identity.
NAS
EAP - Identity Request
EAP - Identity Response (anonymous@sussex.ac.uk)
Inner Ident (sususer1234)
Supplicant
anonymous@sussex.ac.uk
Outer Ident (anonymous@sussex.ac.uk)
Proxy to ORPS for based on outer
ident 'sussex.ac.uk'.
NRPS
Outer Ident (anonymous@sussex.ac.uk)
Accounting ident (anonymous@sussex.ac.uk)
ORPS (Visited)
anonymous@sussex.ac.uk
Outer Ident (anonymous@sussex.ac.uk)
Home server only has 'anonymous' uid
returned in accounting packet so has no way of
associating accounting packets with the user it
previously authenticated.
Inner Ident (sususer1234)
used for authentication
ORPS (Home)
Authentication Directory

Figure 4.1. Identity transfer (anonymous)

These issues can be mitigated by returning the user's *inner identity* in the *Access-Accept* packet. NASs fully compliant with RFC 2865 will use the value of the *User-Name* attribute returned in the *Access-Accept* packet as the value of the *User-Name* attribute in all future accounting packets.

For this to work across proxy chains routing with the *outer identity*, all returned identities must contain a routable domain component. As there is no guarantee that the *inner identity* has a routable domain component, the University ORPSs are configured to insert the *User Identifier* component of the *inner identity* and the *realm* component of the *outer identity* into the *User-Name* attribute of the final *Access-Accept* packet.

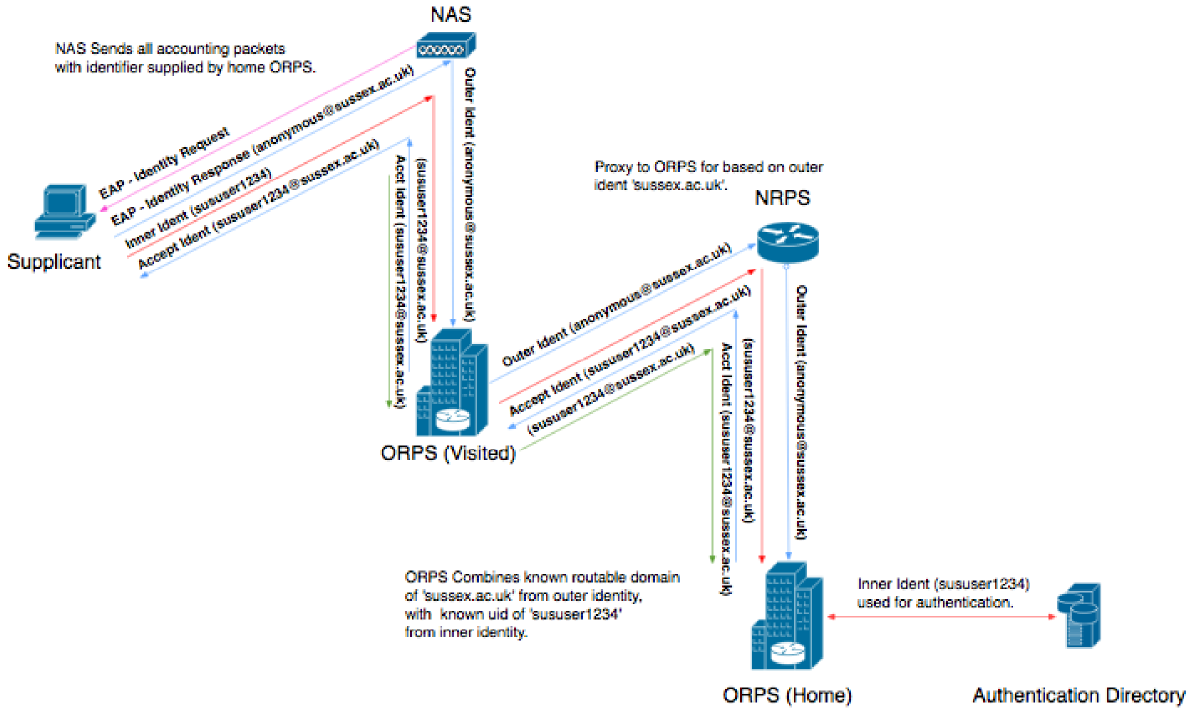

NAS
NAS Sends all accounting packets with identifier supplied by home ORPS.
EAP - Identity Request
EAP - Identity Response (anonymous@sussex.ac.uk)
Inner Ident (sususer1234)
Accept Ident (sususer1234@sussex.ac.uk)
Supplicant
Outer Ident (anonymous@sussex.ac.uk)
(sususer1234@sussex.ac.uk)
Acct Ident (sususer1234@sussex.ac.uk)
Proxy to ORPS for based on outer ident 'sussex.ac.uk'.
NRPS
Outer Ident (anonymous@sussex.ac.uk)
Accept Ident (sususer1234@sussex.ac.uk)
(sususer1234@sussex.ac.uk)
ORPS (Visited)
Outer Ident (anonymous@sussex.ac.uk)
(sususer1234@sussex.ac.uk)
Acct Ident (sususer1234@sussex.ac.uk)
ORPS Combines known routable domain of 'sussex.ac.uk' from outer identity, with known uid of 'sususer1234' from inner identity.
Inner Ident (sususer1234) used for authentication.
ORPS (Home)
Authentication Directory

Figure 4.2. Identity transfer (de-anonymised)

It is worth noting that a system implementing RFC4372 (Chargeable User Identity) would solve the issues mentioned above without compromising the user’s anonymity. Unfortunately the CUI attribute requires both NAS and RADIUS server support, and although it would be possible to support the use of CUIs with FreeRADIUS 2’s conditional language, at the time of writing NAS support is non-existent.

A more readily implementable solution to the problem of user anonymity is the use of the RADIUS *Class* attribute. The *Class* attribute (according to RFC 2865) should exhibit identical behavior to the *User-Name* attribute, in terms of Accounting-Packets. If a unique hash were inserted into the *Class* attribute of ORPS *Access-Accept* packets and recorded along with the user’s inner-identity then the value of the *Class* attribute included in accounting packets could be resolved to the user’s real identity without compromising anonymity. Administrators wishing to utilise the Class Attribute should be aware that some organisations may have their own local implementation and that the Class attribute sent may not be honoured.

Appendix 5: FreeRADIUS Attribute Filtering

Pre-Proxy

The pre-proxy filter is applied to all packets prior to proxying. The University of Sussex ORPS only filter attributes in packets being sent as part of an authentication attempt; Accounting packets are left unmodified. The *Service-Type* attribute in request packets is set to *Authenticate-Only*, as a hint to the Home Server that no authorisation attributes are required in the response. The first part of this filter complies with the current JANET Roaming service requirements for allowed attributes; the latter part contains optional attributes used primarily for accounting/debugging.

${raddbdir}/radiusd.conf

```
attr_filter attr_filter.pre-proxy {
      key = "%{Packet-Type}.%{Realm}"
      attrsfile = ${filterdir}/attrs.pre-proxy
}
```

${raddbdir}/sites-enabled/default-outer

```
pre-proxy {
      ...
      attr_filter.pre-proxy
}
```

${raddbdir}/filters/attrs.pre-proxy

```
Access-Request.jrs
      User-Name =* ANY,
      Reply-Message =* ANY,
      Service-Type := 'Authenticate-Only',
      State =* ANY,
      Class =* ANY,
      Message-Authenticator =* ANY,
      Calling-Station-ID =* ANY,
      Proxy-State =* ANY,
      EAP-Message =* ANY,
      MS-MPPE-Send-Key =* ANY,
      MS-MPPE-Recv-Key =* ANY,
      Fall-Through = yes
# Extra Identification attributes
Access-Request.jrs
      Chargeable-User-Identity =* ANY,
      Called-Station-ID =* ANY,
      NAS-IP-Address =* ANY,
      NAS-Identifier =* ANY,
      NAS-Port-Type =* ANY,
      NAS-Port-ID =* ANY,
      Acct-Session-Id =* ANY,
      Connect-Info =* ANY
```

Post-Proxy

The post-proxy filter is applied to all packets received resulting from a proxied request. By only allowing a limited subset of attributes, the ORPSs ensure no potentially dangerous attributes (e.g VLAN Assignment attributes) are sent to the NAS. The first part of this filter complies with the current JANET Roaming service requirements for allowed attributes, and the latter part contains optional attributes used primarily for accounting/debugging.

${raddbdir}/radiusd.conf

```
attr_filter attr_filter.post-proxy {
      key = "%{proxy-reply:Packet-Type}.%{Realm}"
      attrsfile = ${filterdir}/attrs.post-proxy
}
```

${raddbdir}/sites-enabled/default-outer

```
post-proxy {
      ...
      attr_filter.post-proxy
}
```

${raddbdir}/filters/attrs.post-proxy

```
Access-Accept.jrs
      User-Name =* ANY,
      Reply-Message =* ANY,
      State =* ANY,
      Class =* ANY,
      Message-Authenticator =* ANY,
      Calling-Station-ID =* ANY,
      Proxy-State =* ANY,
      EAP-Message =* ANY,
      MS-MPPE-Send-Key =* ANY,
      MS-MPPE-Recv-Key =* ANY,
      Fall-Through = yes
# Extra Identification attributes
Access-Accept.jrs
      Chargeable-User-Identity =* ANY
```

Accounting-Response

${raddbdir}/radiusd.conf

```
attr_filter attr_filter.accounting_response {
      key = %{User-Name}
      attrsfile = ${filterdir}/attrs.accounting_response
}
```

${raddbdir}/sites-enabled/default-outer

```
accounting {
      ...
      attr_filter.accounting_response
}
```

${raddbdir}/filters/attrs.accounting_response

```
DEFAULT
      Vendor-Specific =* ANY,
      Message-Authenticator =* ANY,
      Proxy-State =* ANY
```

Post-Authentication

${raddbdir}/radiusd.conf

```
attr_filter attr_filter.accounting_response {
      key = %{User-Name}
      attrsfile = ${filterdir}/attrs.accounting_response
}
```

${raddbdir}/sites-enabled/default-outer

```
post-auth {
      ...
      Post-Auth-Type REJECT {
            ...
            attr_filter.access_reject
      }
}
```

${raddbdir}/filters/attrs.access_reject

```
DEFAULT
      EAP-Message =* ANY,
      Message-Authenticator =* ANY,
      Proxy-State =* ANY,
      State =* ANY,
      Reply-Message =* ANY,
      Password-Retry := 3
```

Glossary

802.1x Authentication standard for wired and wireless LANs, used to identify users before allowing their traffic onto the network.

AAA Authentication, Authorisation and Accounting

AES Advanced Encryption Standard.

AUP Acceptable Use Policy.

BSSID Basic Service Set Identifier is the MAC Address of a single station within a WAP. Some modern enterprise level access points support multiple BSSIDs allowing for multiple service sets (SSIDs, encryption schemes etc) to exist on the same Access Point.

CBC-MAC Cipher Block Chaining Message Authentication Code.

CHAP Challenge-Handshake Authentication Protocol.

DHCP Dynamic Host Configuration Protocol.

DNS Domain Name System.

EAP Extensible Authentication Protocol.

EAPOL EAP over LAN.

EAP-PEAP An EAP type implementing TLS to secure a tunnel in which a second EAP type is used to provide authentication.

EAP-TLS An EAP type implementing authentication using certificates.

EAP-TTLS An EAP type implementing TLS to secure a tunnel in which an authentication protocol is used to provide authentication.

eduroam A federation, managed by TERENA, consisting of several NRENs, mainly European, that promotes inter-NREN roaming.

GVRP Generic VLAN Registration Protocol: advertises available VLANs and allows the creation of dynamic ‘on-demand’ VLAN paths across multiple pieces of connected infrastructure.

HTTPS Protocol for securing HTTP with either SSL or TLS.

IAS Internet Authentication Service, included with Microsoft Windows Server. Has become Network Policy Server in Windows Server 2008.

ICMP Internet Control Message Protocol.

ICV Integrity Check Value.

IEEE 802.1 A family of specifications for wired LANs.

IEEE 802.11 A family of specifications for wireless LANs.

IMAP Internet Message Access Protocol.

IP Internet Protocol.

IPSec Internet Protocol Security: a standard for security at the network or packet processing layer of network communication.

IPv4 current version of IP.

IPv6 expansion of IP.

IV initialization vector.

JRS1 with **JRS2** and **JRS3**, tiers of services within the JANET Roaming service.

LAN Local Area Network.

LDAP Lightweight Directory Access Protocol. A protocol used to access a directory listing.

LDAPS Secure LDAP.

MAC address Unique code assigned to most forms of networking hardware.

MIC Message Integrity Code.

MS-CHAP Microsoft Challenge Handshake Authentication Protocol.

MS-CHAPv2 MS-CHAP version 2.

NAI Network Access Identifier.

NAS Network Access Server.

NREN National Research & Education Network.

NRPS National RADIUS Proxy Service.

NTP Network Time Protocol.

OpenVPN VPN package providing the ability to create point-to-point encrypted tunnels between hosts.

ORPS Organisational RADIUS Proxy Servers.

PAP Password Authentication Protocol.

(S)FTP (Secure) File Transfer Protocol.

POE Power Over Ethernet.

POP Post Office Protocol.

POP3S Secure POP3.

PPP Point-to-Point Protocol.

RADIUS Remote Authentication Dial-In User Service.

RDP Reliable Datagram Protocol.

RFC Request for Comment: series of documents created to define accepted or proposed Internet standards or standards of practice.

RSN Preauthentication Allows opportunistic caching of encryption keys to allow fast association with neighbouring access points. Only available with WPA2.

SMTP Simple Mail Transfer Protocol.

SMTPS secure Simple Mail Transfer Protocol.

SSH Secure Shell: a standard for encrypted terminal Internet connections.

SSID Service Set Identifier: an identifier that a WAP and wireless stations use to communicate with each other.

syslog Server used by other hosts to record logging information remotely.

UDP User Datagram Protocol.

UID User ID

VLAN virtual LAN.

VNC Virtual Network Computing: desktop protocol to control another computer remotely.

VPN Virtual Private Network.

WAP Wireless Access Point.

WEP Wired Equivalent Privacy.

WLSE Wireless LAN Solution Engine.

WPA Wi-Fi Protected Access.

WPA2 The successor to WPA.

WRD Web Redirect.

ZPoP Zone point-of-presence switch.

Copyright notice

Extra copies of this document or any of these factsheets may be ordered from the JANET Service Desk, either by e-mail or in writing:

JANET Service Desk
JANET(UK)
Lumen House, Library Avenue
Harwell Science & Innovation Campus
Didcot
Oxfordshire
OX11 0SG

Tel: 0870 850 2212
Fax: 0870 850 2213
E-mail: service@ja.net

Alternatively it can be downloaded from the JANET website at:
http://www.ja.net/services/authentication-and-authorisation/janet-roaming/documentation.html#casestudies