

SNAP & Wireless



Originally two projects:

- Student Network Access Project

Run by the Library to allow students to bring in the own laptop computer and connect to the University network

- Wireless networking project

Run by UCS as a pilot project to test out the usefulness of a generally accessible wireless network on campus.

Since a common interface for users was needed the projects were implemented as a single system.

Contents

- SNAP and Wireless projects
- SNAP requirements
- Plans 1 & 2
- Wireless security problems
- Plan 3
- How it's working
- Futures



SNAP Project



Benefits:

- Increased number of access points for students owning their own computers
- Access points available throughout extended library opening hours
- Reduction of pressure on University owned computer resources
- Wider access to flexible learning resources
- Provision of a facility for students to use their own software alongside other study facilities
- A working model for expanding in the libraries and elsewhere in the University

Wireless Project



Wireless to be installed at three locations on campus

- Library
- Guild
- Arts Lecture Theatre

Pilot project to test:

- Useability of wireless on campus
- Demand among staff and students

- IEEE 802.11b
 - 11Mb spread spectrum
 - 2.4GHz unlicensed
- Lucent access points

SNAP Requirements



Supported equipment:

- Support for wired and wireless connections
- Standard protocols to be used wherever possible to provide support for all laptop platforms

Protocols:

- Only TCP/IP supported
- All application protocols available by TCP/IP supported

Authentication:

- Authentication is required before access is given to the network
- Users to authenticate by username and password, preferably using the existing system

SNAP Requirements



Security:

- Wireless traffic should be protected by encryption
- (UCS) Privacy of user passwords protected
- It should be possible to track back to a user in the event unacceptable use problems
- The ability to restrict or block an Internet application is required

Charging:

- The cost of internet traffic should be charged back to users
- If their quota is exceeded internet access should be blocked but non-chargeable resources should still be accessible

SNAP requirements



Usability:

- Configuration and setup required on the clients machine should be minimised
- Interfaces for wired and wireless should be as similar as possible

UCS charging system

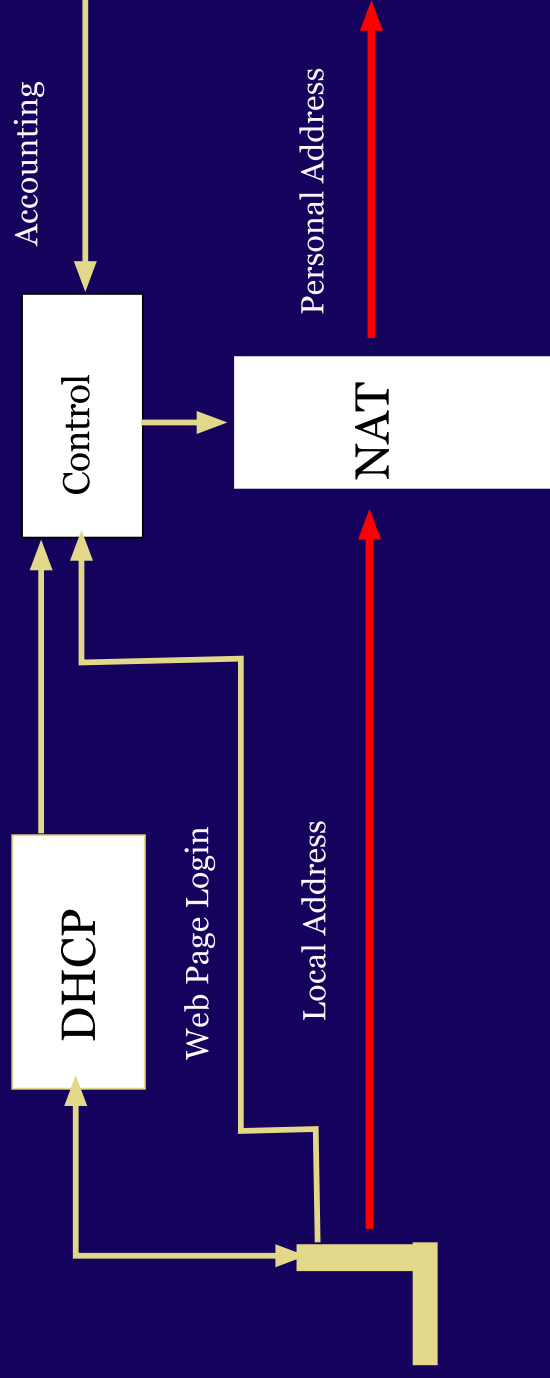


- The UCS validation database consists of username and unix encrypted password pairs, it exists in various formats such as password files and a radius server
- Each user is allocated an individual semi-permanent IP address for services such as dialin modems
- Students are allocated a small daily quota for traffic and can purchase extra traffic. Internet access for course work is the responsibility of the department.
- Charges are calculated daily using input from AARnet traffic logs and web cache logs etc

SNAP: Plan 1



NAT solution



SNAP: Plan 1



Advantages:

- Uses personal IP address
- No extra client software required

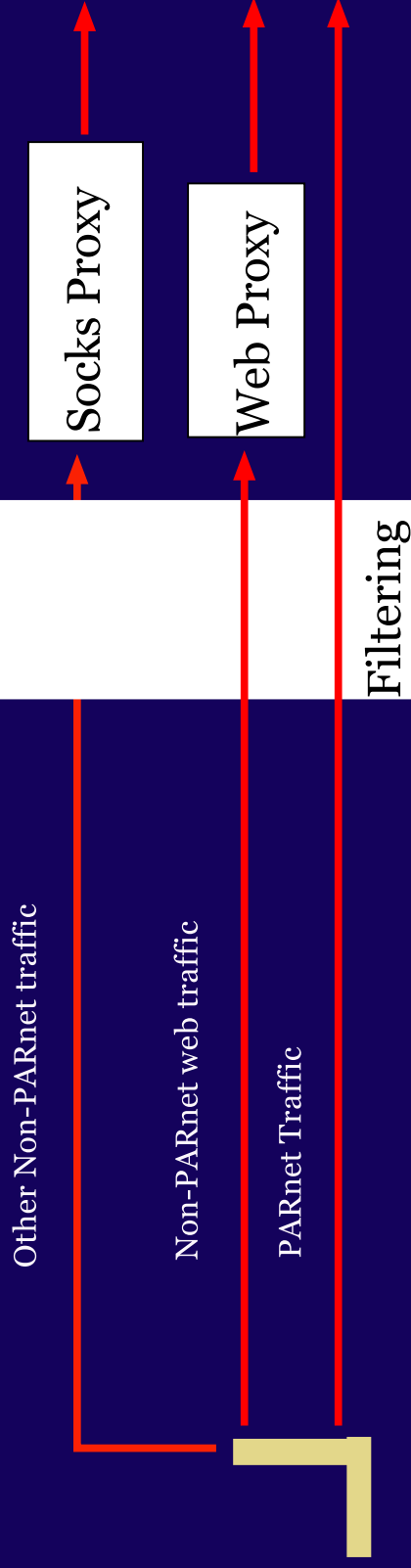
Disadvantages:

- What if they don't logout
 - DHCP doesn't keep a connection
 - Too short lease a problem with wireless
 - Lending of wireless cards, ethernet address not unique to a person
- WEP encryption

SNAP Plan 2



Proxy solution



SNAP Plan 2



Advantages:

- No problem if users don't logout
- No extra software for external web traffic

Disadvantages:

- Socks client software required for external non-web traffic and might not be totally transparent
- Access to PARnet would have to be controlled by registering MAC addresses
- Difficulty in tracing PARnet traffic back to user
- WEP encryption

Wireless Security



WEP

Wired Equivalent Security

Encryption shown to be weak

There exist programs that can derive the key in a few hours

Much more basic problem:

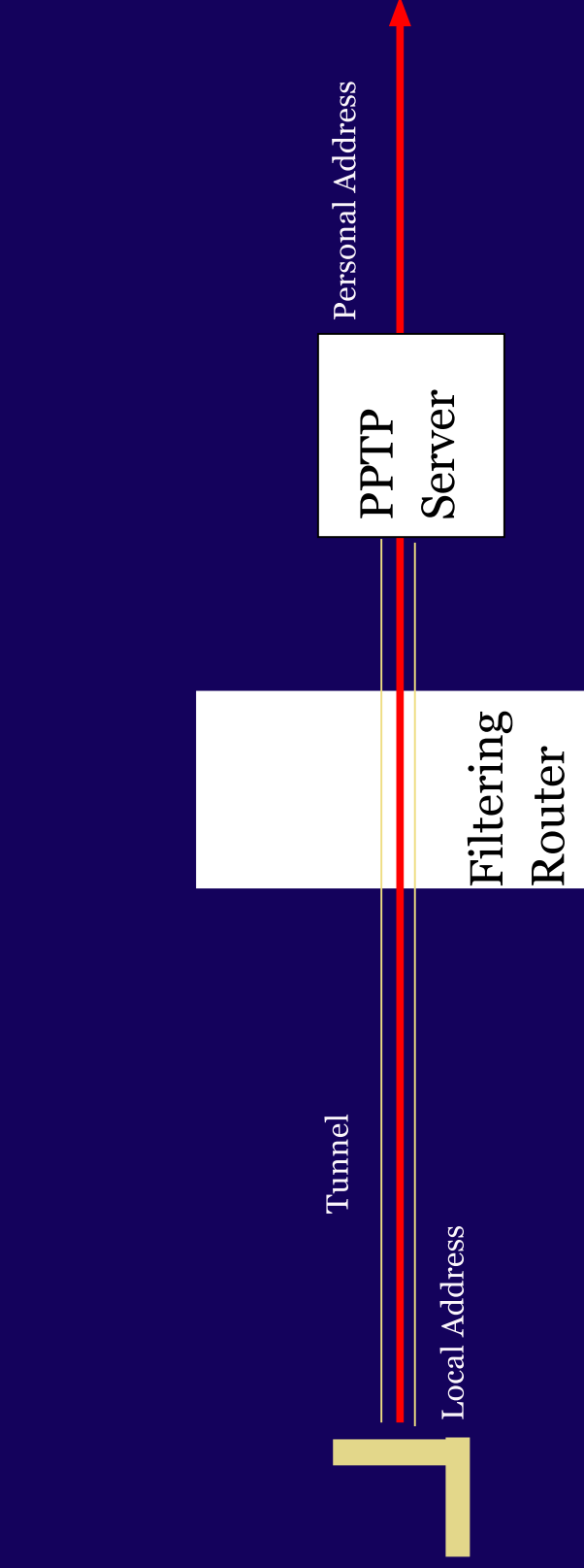
Single key shared between the access points and all the users.

With the key it is possible to see everyone's traffic

SNAP Plan 3



VPN solution



SNAP Plan 3



Advantages:

- Uses personal IP address
- Doesn't rely on WEP security
- Software comes with most windows systems

Disadvantages:

- Not available for Macs
- Encryption security not ideal

PPTP



Uses MS-CHAPv2 authentication, replacement for previous insecure MS-CHAP.

Security of MS-CHAPv2 is equivalent to the security of the NT has of the users password.

MS-CHAPv2 requires storing unencrypted passwords

- Can't use our password database
- Users set "pass-phrase" via web pages
- Has to be >8 characters

PPTP currently available for Mac doesn't support MS-CHAPv2
Support should be in next version of MAC OSX (Jaguar)

IP-SEC

- A more secure standards based alternative to PPTP
- Available for most platforms including MACs
- Comes with windows 2000 & XP

Why don't we use it:

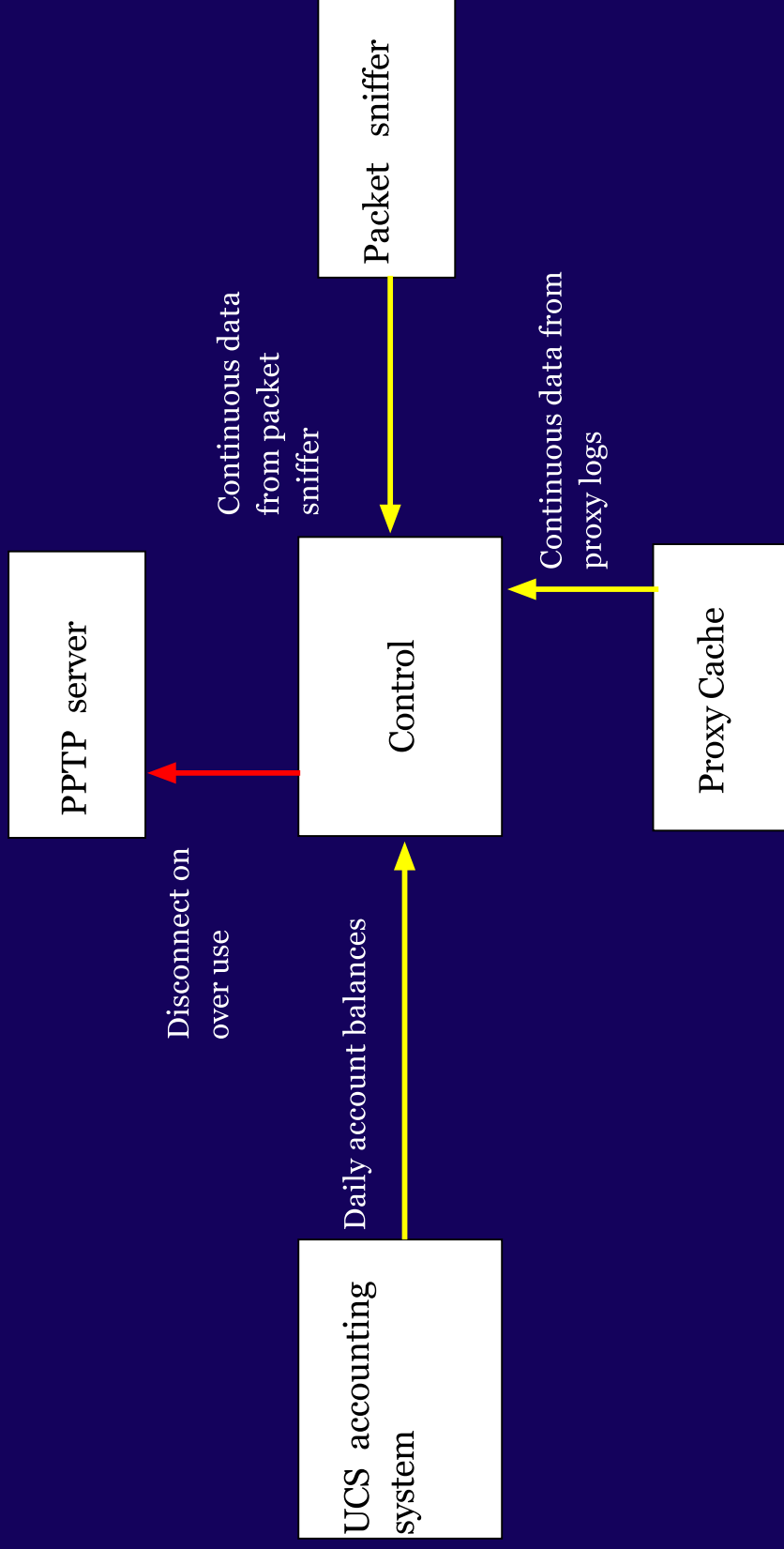
- Complex to setup (at least with free NA/PGP client)
- Linux implementation doesn't support "aggressive mode" for ideological reasons. Alternatives:
 - Use different platform
 - Use certificates
 - Use IKE key exchange daemon from BSD
- On the todo list



Accounting and Control



Block if excessive usage



Installation



Wireless access points:

- 2 in Arts lecture theatres
- 2 in Guild cafeteria area
- 1 in Library coffee shop area

Wired access

- 8 wired areas in 4 libraries

SNAP server is a rack mounted dual process Linux system

Support:

- SNAP support officer in Reid Library
- Web pages: <http://snap.uwa.edu.au>

Previous VPN system



Previous VPN system:

- The colleges are not part of UWA but the students there are
- The students wanted high speed access so we needed to charge them
- The solution:
 - Unencrypted PPTP VPNs into a UCS server that allowed them to use their personal IP address
 - The authentication used PAP and the UCS encrypted password database

Most non-MAC users have converted to SNAP

Usage

Number of different users per day:

- about 80 in colleges
- about 20 on SNAP wired and wireless

500 users have activated SNAP accounts

We need to generate exact statistics separating wired and wireless users, but currently most are wired users.



Immediate Plans



There are a number extra wireless stations being placed in the Libraries to cover the general study areas.

A survey is being carried out to see where staff and students would like wireless expanded to.

Wireless futures



Better security models that WEP exist but are proprietary.

The Lucent enhanced version was considered, but:

- We wanted users to be able to use cards from any manufacturer
- They didn't support handover

Desirable Properties:

- User based authentication
- Centralised management of user information
- Dynamic session based encryption keys
- Mutual authentication

Wireless futures



IEEE 802.11i

- Standard for authentication and encryption
- Still under development
- IEEE 802.1X "Network Port Authentication"
 - Authentication standard developed for ethernet ports
 - Being adapted to wireless
 - Uses IETF EAP (Extensible Authentication Protocol)
 - Uses Radius (also LDAP)
- Defines new cyphersuites TKIP (based on WEP) and AES

Wireless futures



IEEE 802.11a

- Approved standard
- 54Mb/s data rate
- 5GHz radio frequency
- Offers 8 channels

IEEE 802.11g

- Draft standard
- 54Mb/s data rate
- 2.4GHz (same as 802.11b)
- Backward compatible with 802.11b
- Offers 3 channels
- Interference from Bluetooth etc