

## **Automating the registration and configuration of network components for student residential networking**

### **Background**

Prior to the 2002/2003 session the arrangements at UCL for networking in Halls of Residence were ad-hoc. Old redundant networking equipment such as hubs was re-deployed in the Halls as and where necessary. A workflow system based on ARS (Action Remedy System) was developed and used to allow students to request to have their data point activated and to request assistance with connecting up. At best, the amount of effort available to help the students was approximately 1FTE.

In June 2002 as part of the income generation initiative it was decided to charge students for the use of data points in their study bedrooms. A complete review of the service was undertaken with the objective to minimise the amount of manual intervention between the receipt of funds and activation of the data point.

At the time less than two thirds of study bedrooms had a data point. A program was initiated to cable the remaining major Halls over the summer vacation. However, this was not straightforward as many of the rooms were either still occupied by postgraduate students or let to visitors. It was decided to connect every data point to a switch port, which required a huge rollout of ethernet switches.

Some of the Halls are geographically close to the main campus and are served by the extensive fibre network which covers a square mile around UCL. In order not to disadvantage the more distant Halls, 100Mbps leased lines were installed. The additional recurrent cost compared to a 2Mbps circuit was very often not much more than 50%. Each Hall has an IS managed desktop cluster and networked systems in the offices. Along with the study bedroom traffic the three constituencies are kept apart on separate LANs but share a common link to the main campus.

### **The System**

The 'system' comprises the following elements; HCMS (Halls Connection Management System), ARS (Action Remedy System), Cisco PIX 525 firewall, Cisco 3550 router, Cisco 3524 and 2950 LAN Switches, CiscoWorks2000 NMS. These components are connected as shown in fig 1.

The HCMS is a Dell system running Linux Slackware 8. The following software is installed;

DHCP, Apache Web Server, TCL, lib-cisco TCL library, 'expect' scripting language, Perl, ARS Perl module, CGI Perl module, MySQL database (client and server), mySQL Perl module, mySQL TCL library.

A firewall is positioned between the Halls and Campus networks. The policy employed on the firewall reflects the Service Definition for a Halls of Residence connection.

At the time of writing there are twelve Halls of Residence cabled with a mixture of Cisco LAN switches, which are either 3524s or 2950s.

### Halls of Residence Network

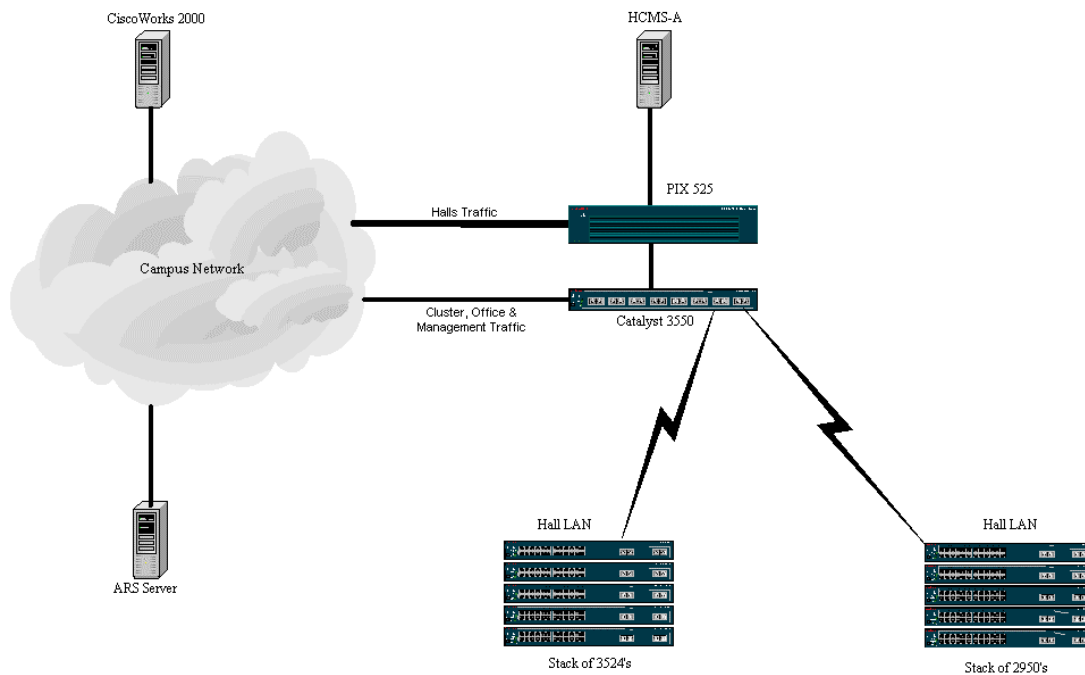


fig1

Each link to a Hall carries the following five trunked VLANs, cluster, offices, management, study bedroom registration and study bedroom data. The last two VLANs are terminated on the 3550, which handles the layer 3 routing for the Halls traffic.

CiscoWorks2000 is used to help manage the entire campus network and provides specific support for this project. In this context, it is employed to save switch configuration files, track configuration changes, field syslog messages generated by the switches and make common configuration changes across the entire Halls of Residence switched network.

Instead of allocating static IP addresses as in the old system, DHCP (Dynamic Host Configuration Protocol) is employed to allow “out of the box” configurations to work and hopefully minimise user intervention.

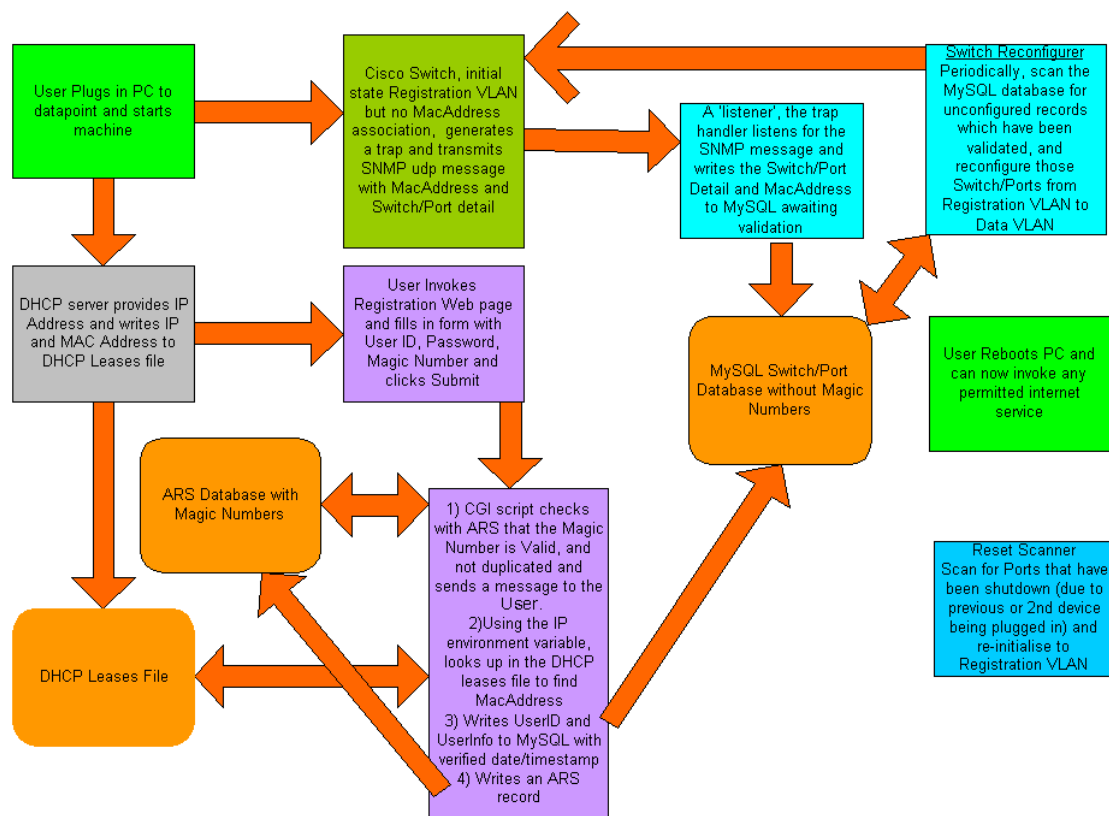
Initially all the data points are in the 'registration' VLAN. This only permits the student access to the WWW Halls Connection Registration page which is located on the HCMS.

After successful registration the student's data point is then reconfigured into the 'data' VLAN which allows access to all permitted computing services, resources and facilities in College, on JANET and the Internet.

### The Process

The student purchases a voucher from the College shop. This is in the style of 'payslip' folded stationary. Printed inside is a unique 12 digit random 'magic' number in the form of a 'top up style' similar to that used by the 'pay as you go' mobile operators.

Registration must be carried out from the student's study bedroom. Once the user plugs in and starts the machine the DHCP server (HCMS) provides an IP address and writes the IP and MAC addresses to the DHCP leases file. The switch port the user's data point is connected to is initially in the 'registration' VLAN.



Flow Diagram of New Connection Registration Process

fig2

Once the switch detects the connection it generates an SNMP trap. The trap handler script, running on HCMS, creates a record in a table in a MySQL database on receipt

of a valid Mac-Notification-Trap from a HoR switch. The format of the record appears in fig3. The trap gives the MAC address of the system which has now connected to the switch and an indication of the port to which it is connected (this is the ifindex value for a 2950 switch and a Bridge port table index for a 3524 switch which is then converted into an ifindex value). The traphandler uses SNMP to determine the type of switch, convert the Bridge Port table index to an ifindex if necessary and converts the ifindex to a port description.

***portConnTable***

Field	Type	Null	Key	Default	Extra
recordID	int(11)		PRI	NULL	auto_increment
createUTC	int(10)unsigned			0	
macAddress	char(17)				
switchAddress	char(15)				
switchPort	char(32)				
switchType	char(12)				
errorID	int(11)			0	
checkUTC	int(10)unsigned			0	
validUTC	int(10)unsigned			0	
userName	char(8)	YES		NULL	
userInfo	char(32)	YES		NULL	
arsTicket	char(10)	YES		NULL	
configUTC	int(10)unsigned			0	

fig3

Each newly created record is given a sequential recordID. The createUTC value is the time the trap was received. The traphandler fills in the following values in a new record entry;

createUTC	when the trap was received
macAddress	from the trap
switchAddress	IP source address of the trap message
switchPort	port description (eg. fa0/11)
switchType	type of switch (2950 or 3524)

Care is taken to ensure there is only one active record with a particular MAC address and only one active record for each switch address and port. The errorID field is set in any conflicting record.

The checkUTC field is set when it is confirmed that the MAC address given is actually configured on the port on the switch. This is done by a telnet connection to the switch which validates the switch configuration. The traphandler currently does this and the field is simply used to indicate that the check has taken place.

Whilst in the 'registration' VLAN the user can only access the web pages on the HCMS server which contain the registration form. The user must now complete the

form in order to register. Once authenticated with the standard UCL userid and password, the user is required to enter information about the connection to be activated. This data is used for tracking purposes only. It includes the room number, hall name and the data point number in their room. In addition the user will enter their 'magic' number which is used as an activation code. This is entered onto the webform and the user submits the data.

ARS is then used to check if the code has been previously used. If it has not then the user details are tagged to that record. If the code has been previously used by a different user the registration will fail. If the code has been used by the same user it will allow them to register, a maximum of three times. This is to permit the user up to two changes of MAC hardware.

Providing the data entered is valid the next process is to lookup the users MAC address based on the IP address used to submit the form. This is found in the DHCP leases file and is then used to update the MySQL table (fig3) that contains details of all connected devices on the network. ARS updates the last entry in this table with the same MAC address to include the users room, hall, userid and the internal tracking number used by ARS to correspond with the users registration. This allows support staff to lookup all details of the registration in ARS if required. Finally the validUTC timestamp is recorded to indicate that the port can be re-configured into the data VLAN.

The configure script runs periodically and for each record which has been validated as above, the port on the appropriate switch is reconfigured from the registration VLAN to the specific data VLAN for the switch.

Details of the Switches which comprise the Halls scheme are held in the swAuthTable in the MySQL database. The format of a record in this table is shown in fig 4.

***swAuthTable***

<b>Field</b>	<b>Type</b>	<b>Null</b>	<b>Key</b>	<b>Default</b>	<b>Extra</b>
swAddress	char(15)				
swName	char(64)	YES		NULL	
swLocation	char(32)	YES		NULL	
swRoCommunity	char(10)			****	
swTacAccess	char(44)			****	
hallVlan	int(10)unsigned			xxx	

fig4

Access to the switches is authenticated by a TACACS+ server. The swTacAccess field in this table contains a username, password and enable password for each switch. The swRoCommunity is the SNMP read community string (SNMP V2C) for each switch.

The effect of the configure script is to change the VLAN membership for the port concerned, and to disable the SNMP trap generation. This is relatively

straightforward. However, some enhancements are planned so as to better guarantee the self consistency of this process. These enhancements include;

- ensuring the port to be configured is not a trunk port
- including the Username and Date/Timestamp in the switch port interface description
- introducing a quarantine VLAN for systems deemed to be broken or hacked
- ensuring the MAC address to be configured is not already configured on a different port in the switched network
- ensuring that each username has only one configured port in the scheme.

### **Difficulties**

Around 95% of users have managed to register successfully without problems. The remaining 5% have principally had difficulties with the end system operating system or the network adaptor.

When users have had AOL software installed this causes the machine to use virtual MAC addresses. With a limit of one MAC address per port this generates a security violation and shuts the port down.

One major source of problems has been to ensure that a similar interface was given to a user regardless of the type of switch (Cisco 3524 or 2950) to which they attached. So in effect we have had to provide a service based on a common set of facilities in the switches. In fact this has been rather unfortunate; we may well have been able to have a simpler scheme based on just one type of switch.

Each switch is loaded with a template at the start of term; and great care needs to be taken to ensure it is correct. An initial problem was that due to an oversight a trunk port was reconfigured as a user port; which was disastrous!

Note that as designed, the MySQL database was simply a mechanism for enabling the registration process to complete, and as such was a historical record. However, as we have gained confidence in the scheme, the significance of the data in the Database has increased, and it is proposed that it be used for additional facilities, such as automating room moves and hardware changes via a re-registration process.

A major snag is allowing only one Mac Address per configured port. The switch action is to disable the port when anything untoward happens but this leaves the user in rather an indeterminate state. Initially this was solved on the 2950 switch by having the switch check the port every few minutes, and recovering the port if appropriate. This feature was not available on the 3524 switch, and so a small Perl script was used to try and recover disabled ports. However this did give a slightly different behavior to the user depending on the switch type.

Subsequently we have removed this automatic resetting on the 2950 switches, and have a Perl script which resets disabled ports on both types of switches back into the registration VLAN.

## **Conclusion**

The project began in June 2002 and had a deadline for completion of the beginning of session (mid September). Despite this constrained timetable and staff absences for the summer vacation the system was ready for the academic year.

The project has self evidently been a success given we have exceeded the target number of ports connected and revenue generated. With the exception of some refinements referred to earlier the system will run unchanged for next session.

Over 70 people were involved in the project. However, I would particularly like to highlight the contributions made by the following UCL IS staff; Robert Clark, Bob Lawrence, Michael Turpin, Rob Bradshaw, Colin Byelong, Nigel Hayward, Graham Newman and Mark Dixon.

Andrew Kerl  
Information Systems, University College London

March 2003