

Bradford Campus Manager

Installation at New College

James Dore (New College IT)

james.dore@new.ox.ac.uk

Rick LeClerc (Bradford Networks founder)

Matt Ashman & Andrew Brimson (Khipu Networks)

matt.ashman@khipu-networks.com

andrew.brimson@khipu-networks.com



What was the need?

- Lots of users requiring controlled access
- Authentication and audit trail
- Straightforward management
- Make use of existing infrastructure
- Tie in to future projects

Situation pre-BCM:

- Different registration methods for wired and wireless connection
- Many separate authentication sources and methods
- Tied to inflexible, aged, custom IPTABLES firewall.
- No consistency for users or admins.

User issues

- They don't sit still: using many devices from multiple locations.
- Access needs to be consistent and easy
- Security is generally a secondary concern

Security by default

- Security assessment as part of the registration process - unavoidable by the user.
- This means it must be as straightforward as possible.
- Easy = Happy Users = Secure Users = Happy admin

Audit trail

- Who's using which machine?
- Where are they using it from?
- Are they doing anything they shouldn't?

Our network

- Novell eDirectory managed workstations
- 3Com switching hardware
- Trapeze managed wireless system
- Home-brew Firewall registration
- All separate stores of user data

The Plan:

- One Username and password
- One login process for users
- One source of Identity data
- One management system

The Plan:

- One Username and password
- One login process for users
- One source of Identity data
- One management system

...to rule them all!

Blind Alleys

- 802.1x
 - Inflexible - couldn't reconfigure ports & VLANs dynamically
 - Requires client install on each pc.
Expensive or impossible for older OS
- Switch based RADIUS
 - Replace all our switches?!
 - Similarly inflexible

Bradford's Solution

- Manipulate the switch port by SSH and SNMP in real time.
- Settings based on progress through registration, and login credentials

The Process

- New machines
- Existing machines
- Miscreants

New machine


Network Registration - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://netauth.new.ox.ac.uk/registration/?client=firefox-a&rls=

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

New College Network Registration





Why have I arrived at this page?

You have arrived at this page because you have attached an unregistered computer to the network.

In order to connect to the network you need to authenticate and submit your computer to be vetted to ensure that it meets the required standards to be allowed on the network.

[Continue](#)

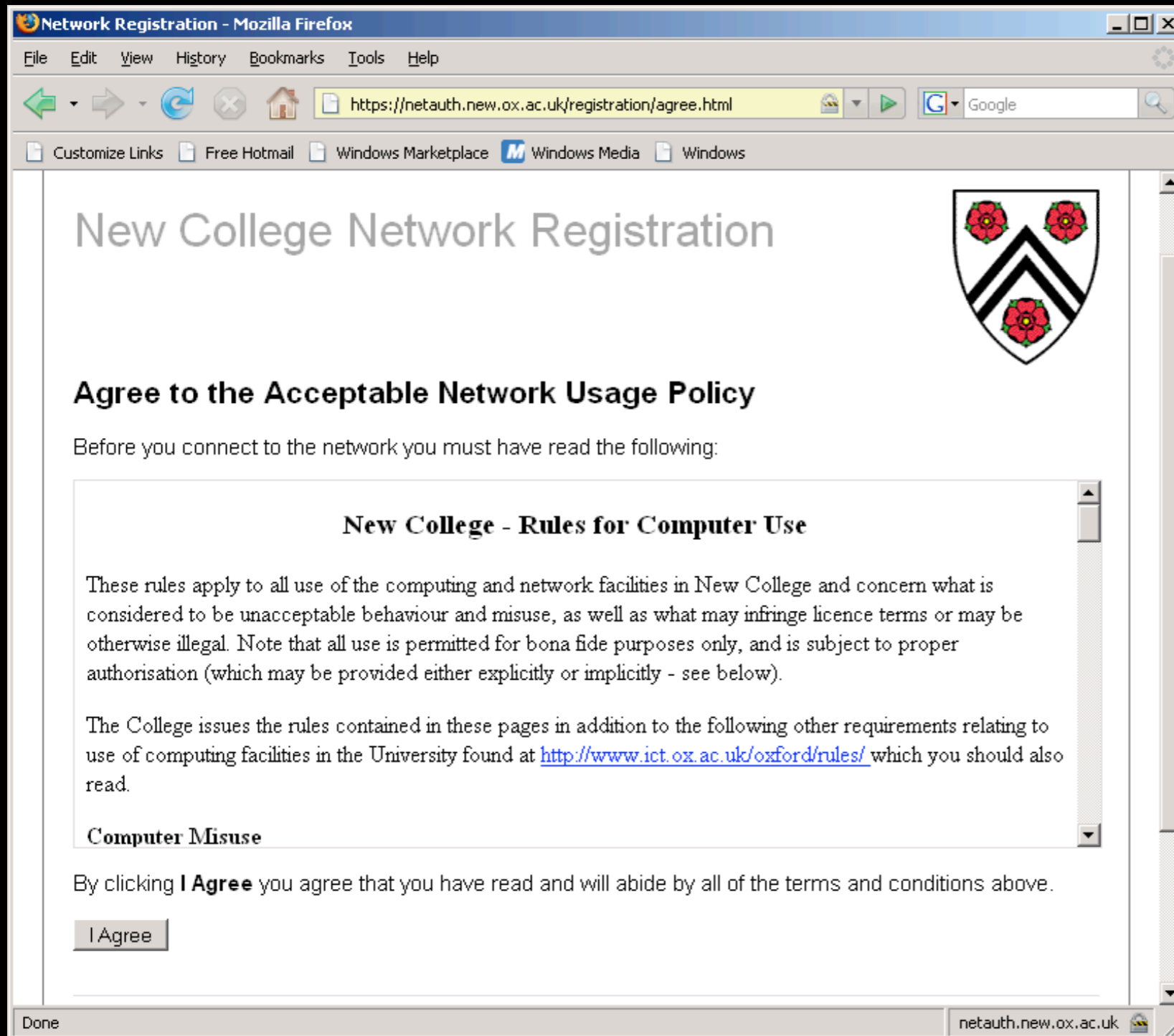
IT Helpdesk - it-support@new.ox.ac.uk - ext 89094, 89095 or 79252

Done netauth.new.ox.ac.uk

- Welcome to the network!

Accept the AUP




Network Registration - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://netauth.new.ox.ac.uk/registration/agree.html

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

New College Network Registration



Agree to the Acceptable Network Usage Policy

Before you connect to the network you must have read the following:

New College - Rules for Computer Use

These rules apply to all use of the computing and network facilities in New College and concern what is considered to be unacceptable behaviour and misuse, as well as what may infringe licence terms or may be otherwise illegal. Note that all use is permitted for bona fide purposes only, and is subject to proper authorisation (which may be provided either explicitly or implicitly - see below).

The College issues the rules contained in these pages in addition to the following other requirements relating to use of computing facilities in the University found at <http://www.ict.ox.ac.uk/oxford/rules/> which you should also read.

Computer Misuse

By clicking **I Agree** you agree that you have read and will abide by all of the terms and conditions above.

Done netauth.new.ox.ac.uk

- Once per new machine, or on a schedule

Health check

Registering Your Computer

Upon clicking on the **Logon** button below you will be asked to download the Client Security Agent (CSA) application. This application checks your computer against network security policies to ensure that your computer meets the minimum security level required for access to the Network.

If you have already downloaded the CSA application and saved it to your desktop please **delete this version** and redownload the CSA application using the button below.

It is a requirement that users must download this application and scan their computers in order to verify that your computer meets the network security policies.

Logon to the Network

Enter your New College Username and Password below to logon to the network.

By clicking on Logon you agree that you have read and will abide by the terms of the Acceptable Network Usage Policy.

Microsoft Windows CSA.exe Instructions

1. When prompted to download the CSA.exe file save it to your Desktop.
2. Double-click the CSA icon on the Desktop to run the CSA application.

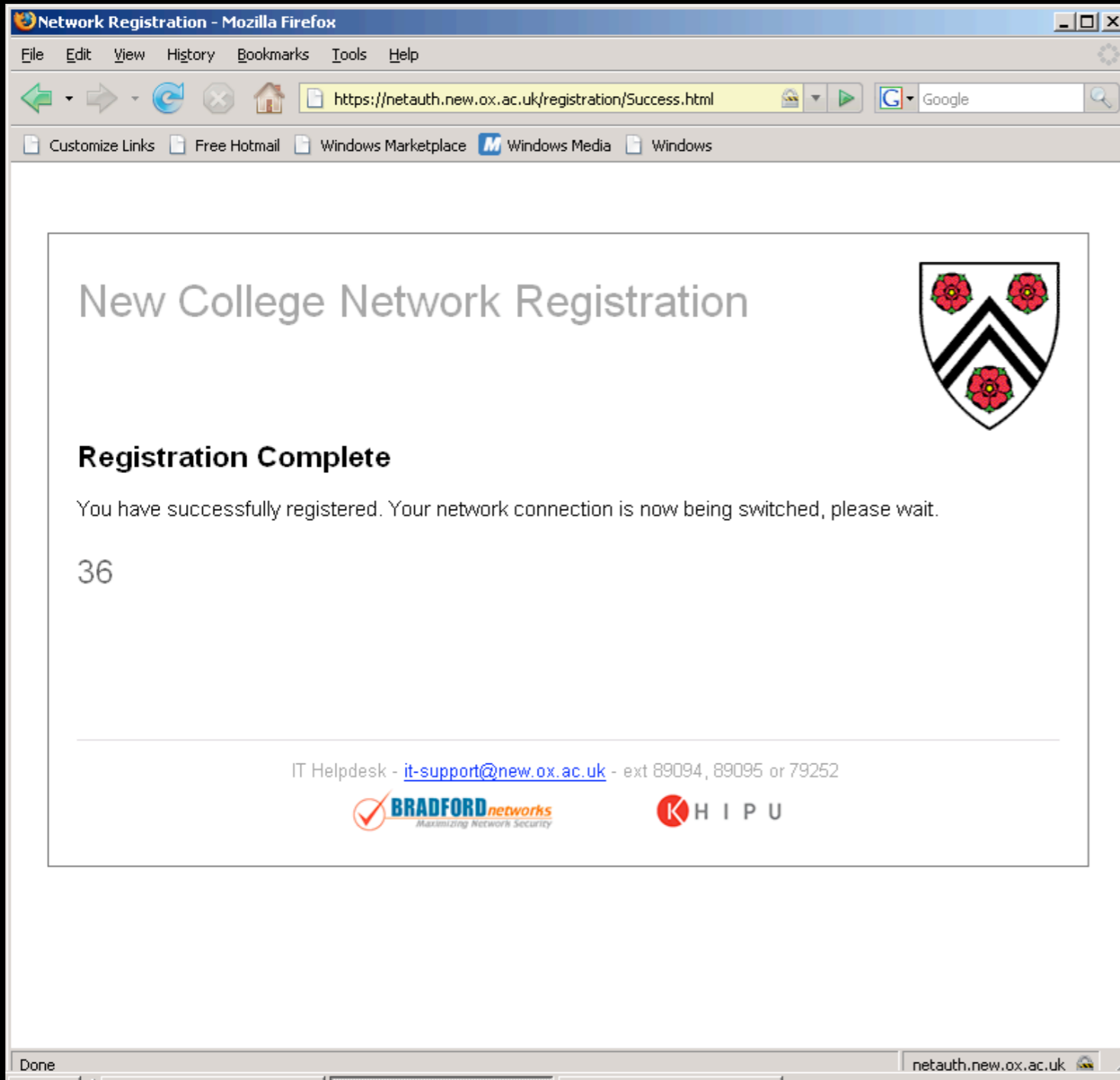
Username:
james

Password:
XXXXXXXXXX




Waiting for netauth.new.ox.ac.uk... netauth.new.ox.ac.uk

- Provide credentials
- Machine is scanned using soluble client

Done!



The screenshot shows a Mozilla Firefox browser window with the title "Network Registration - Mozilla Firefox". The address bar displays the URL "https://netauth.new.ox.ac.uk/registration/Success.html". The page content includes the following elements:

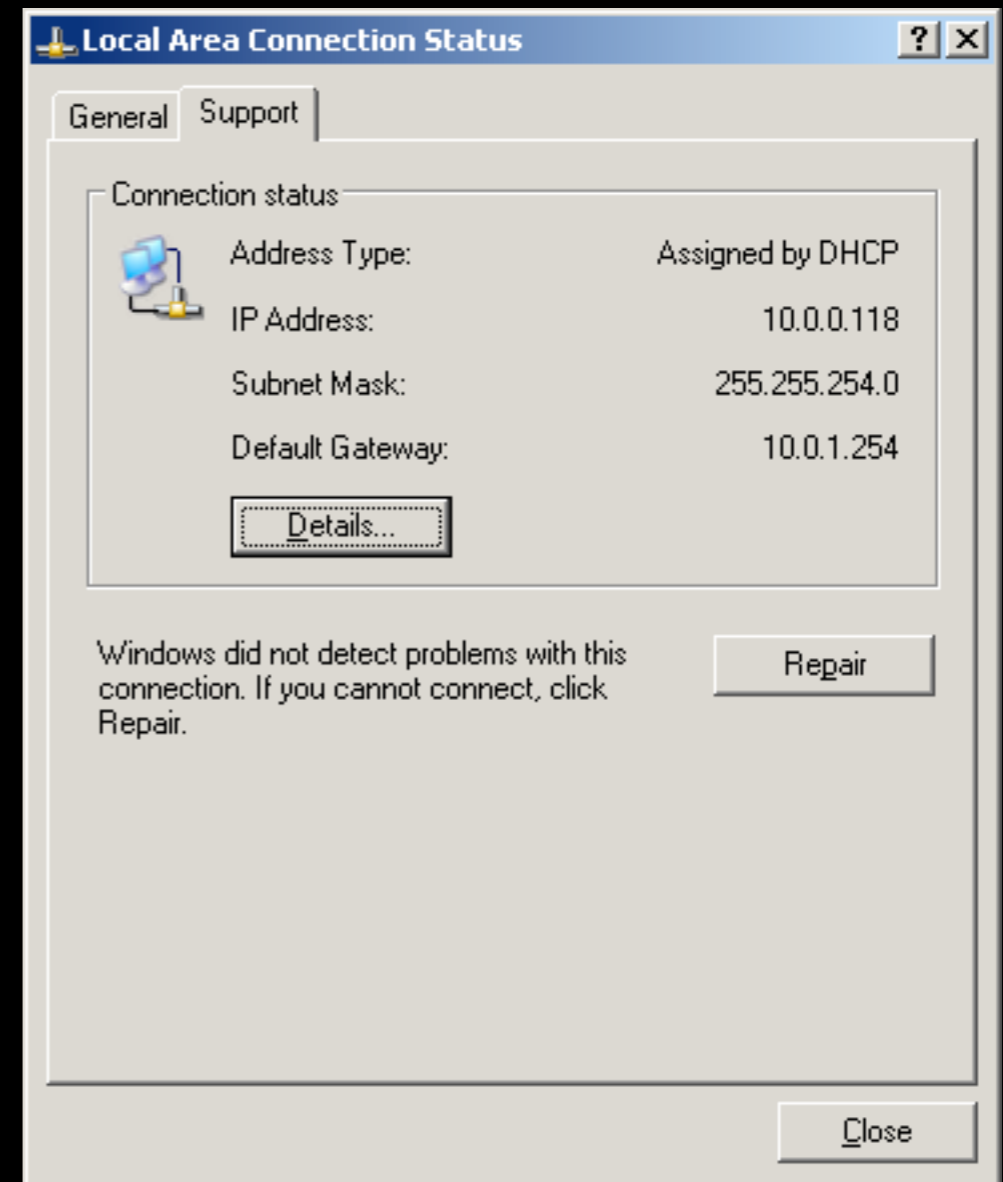
- New College Network Registration**: The main heading of the page.
- : The crest of New College, featuring three red roses on a shield.
- Registration Complete**: A sub-heading indicating the process is finished.
- You have successfully registered. Your network connection is now being switched, please wait.
- 36
- IT Helpdesk - it-support@new.ox.ac.uk - ext 89094, 89095 or 79252
- : Logo for BRADFORD networks, with the tagline "Maximizing Network Security".
- : Logo for K H I P U.

The browser's status bar at the bottom shows "Done" and the address "netauth.new.ox.ac.uk".

- All ok!

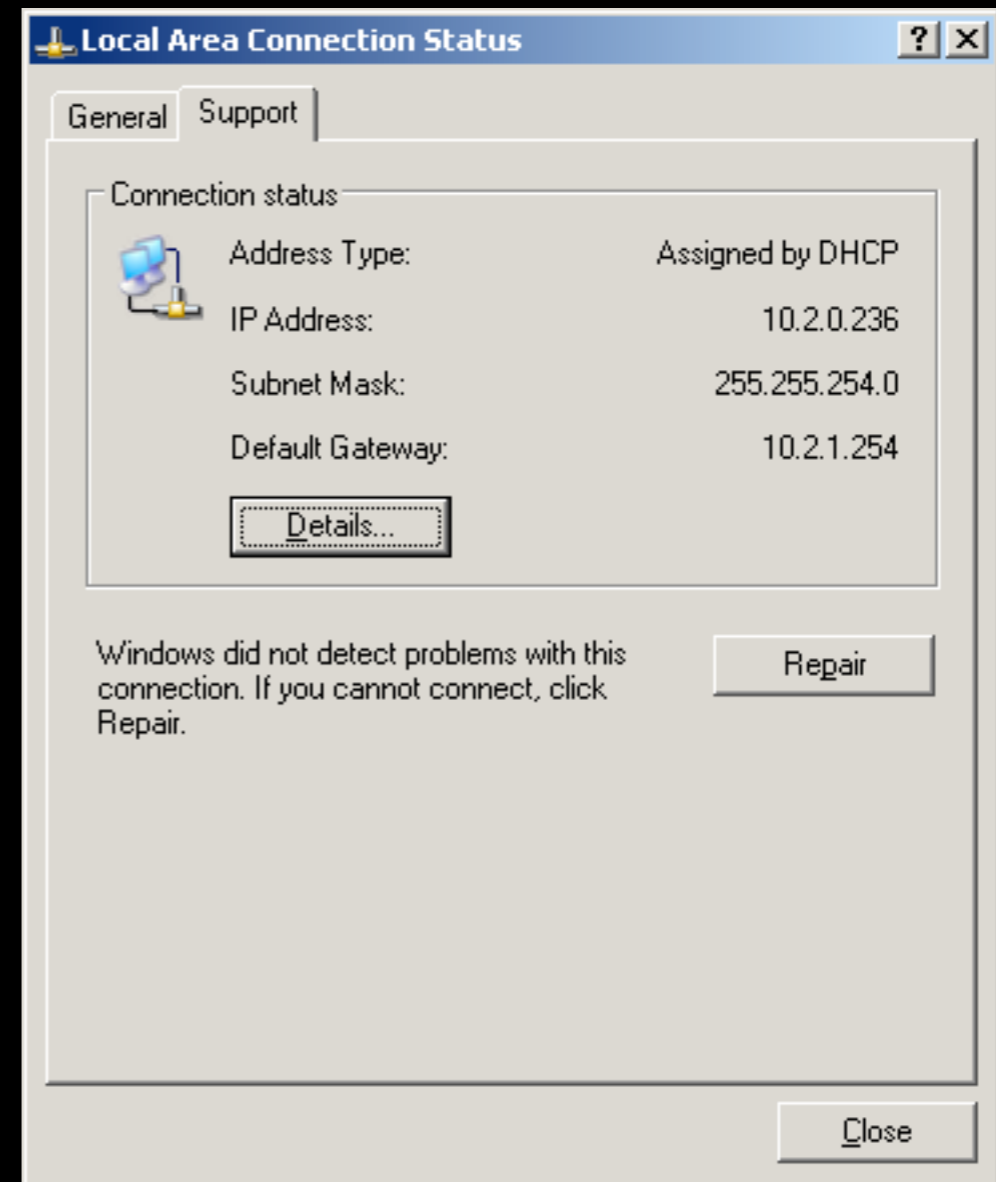
Behind the scenes I

- New machine appears, seen by BCM trapping SNMP port up.
- Placed in VLAN 100, with IP in range 10.0.0.0/254



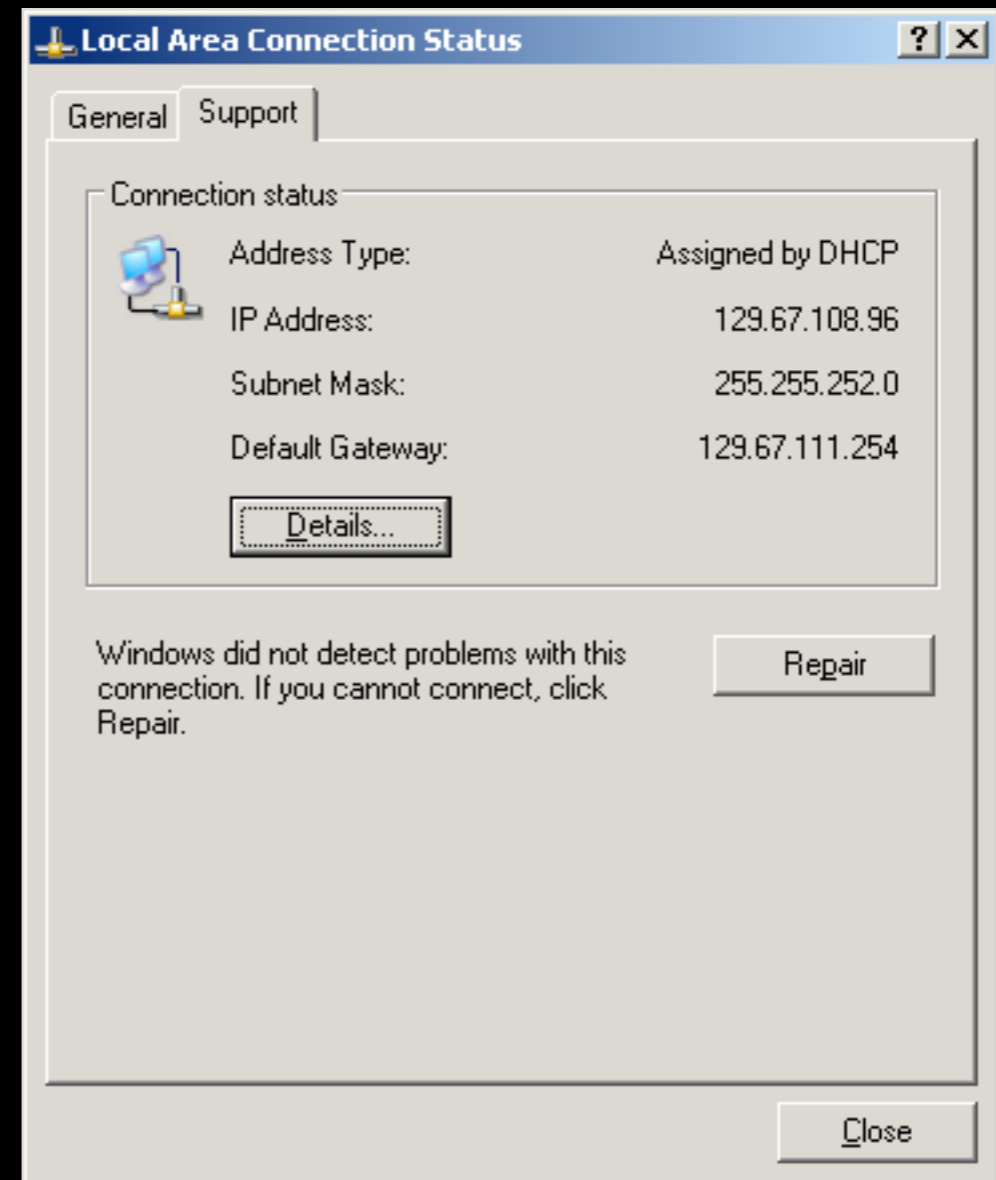
Behind the scenes 2

- After hardware is registered, BCM changes port to AUTH VLAN (10.2.0.0/24)
- Here is where user is asked for credentials



Behind the scenes 3

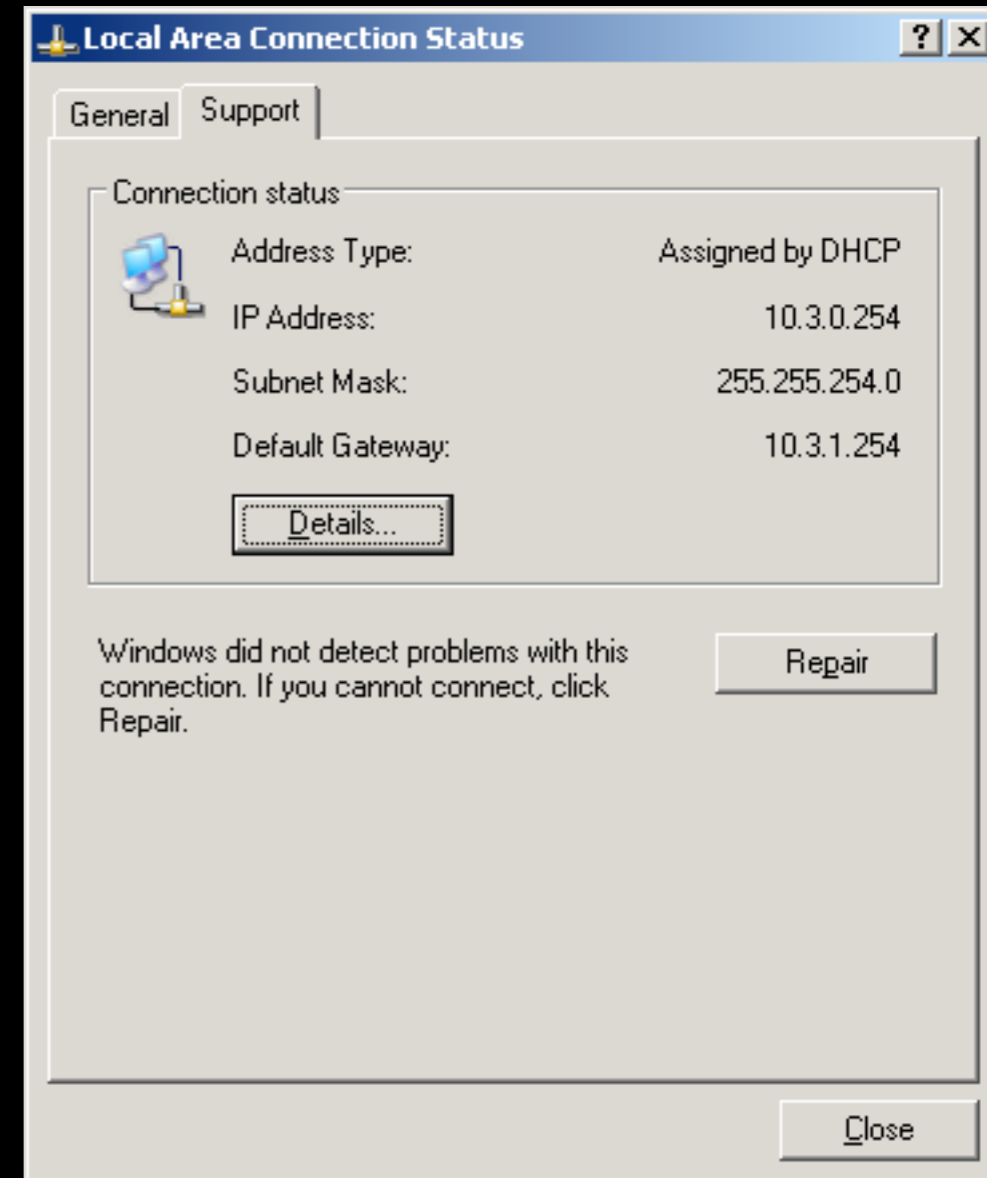
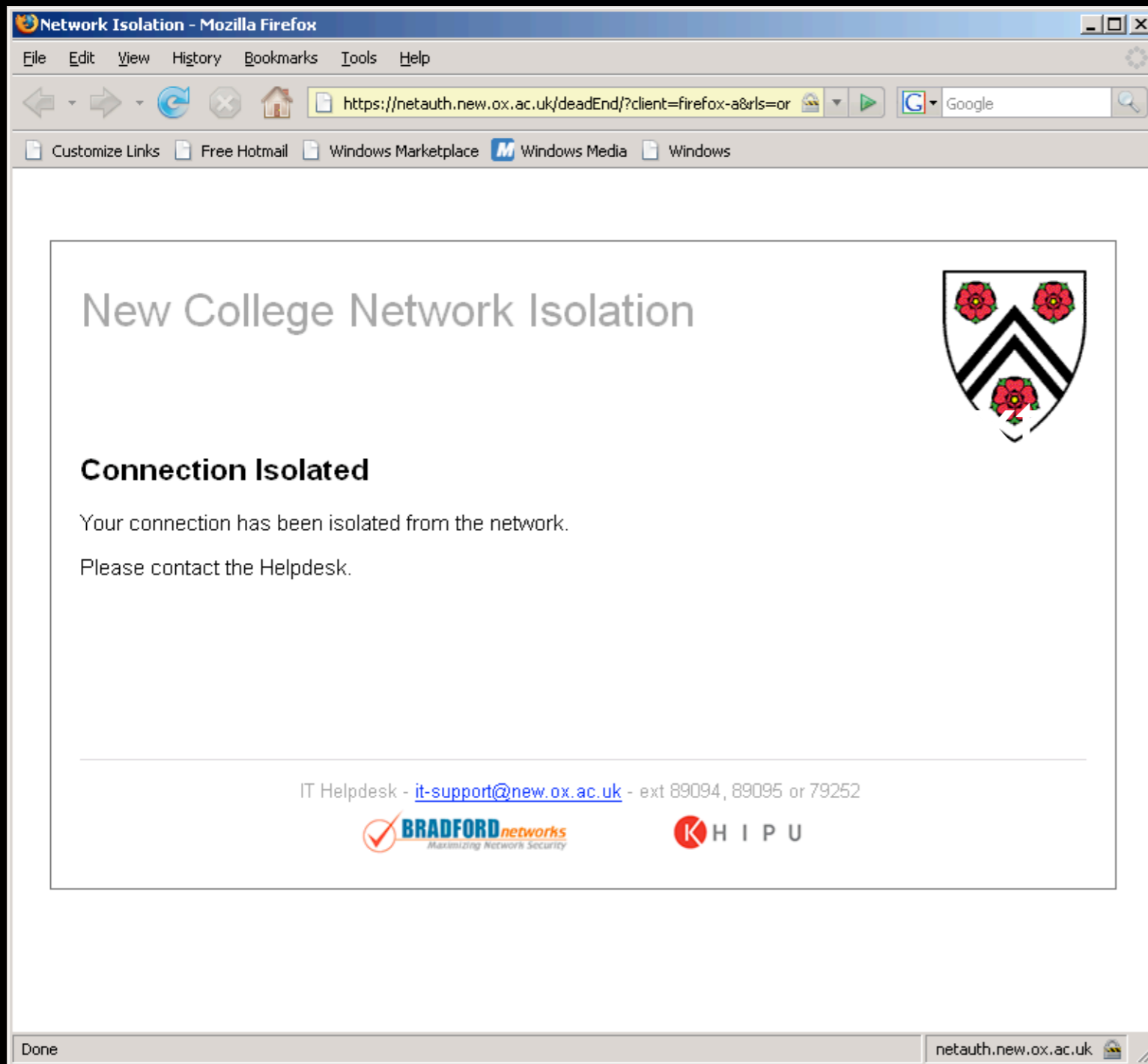
- Credentials and hardware are ok, Go To VLAN 1 to get a public IP.



Issues detected?

- Failed the security scan? Go to VLAN 102 (REM remediation) for limited access to Patches, Antivirus, Antispyware software.
- Miscreant? Firewall policy infringement? Go to VLAN 103 (DEAD) either automatically or by hand of Admin
- Blocking a user manually takes under 10 seconds

You're barred:



This follows the user *and* the workstation wherever they connect.

Still to do!

- Sort out remediation: Which sites and which software the policy should allow or deny.
- Should we force removal of P2P at registration stage, or let firewall detect and deny user automatically?
- Assign production VLAN based on eDirectory context

Fin?

- Live Demo of the Admin interface?
- Installation process?

Installing at New

- Purchase BCM units
- Place in rack at centre of network, on core switch
- Does not need to sit in-line

Configure the switches

- Add VLAN ID's and SNMP trap destination
- Ensure SNMP community strings are consistent (but not 'private' & 'public'!)
- Configure VLAN tagging on Uplink ports

Import the switches

- Using the BCM web console, add all your switches
- Decide on your policies
- Add the ports to be managed to the relevant Groups

Useful bits

- Inventory of machines - dhcpd.conf etc
- Compatible switches - see http://www.bradfordnetworks.com/products/network_access_control_interoperability.html
- An SSL certificate for the BCM units