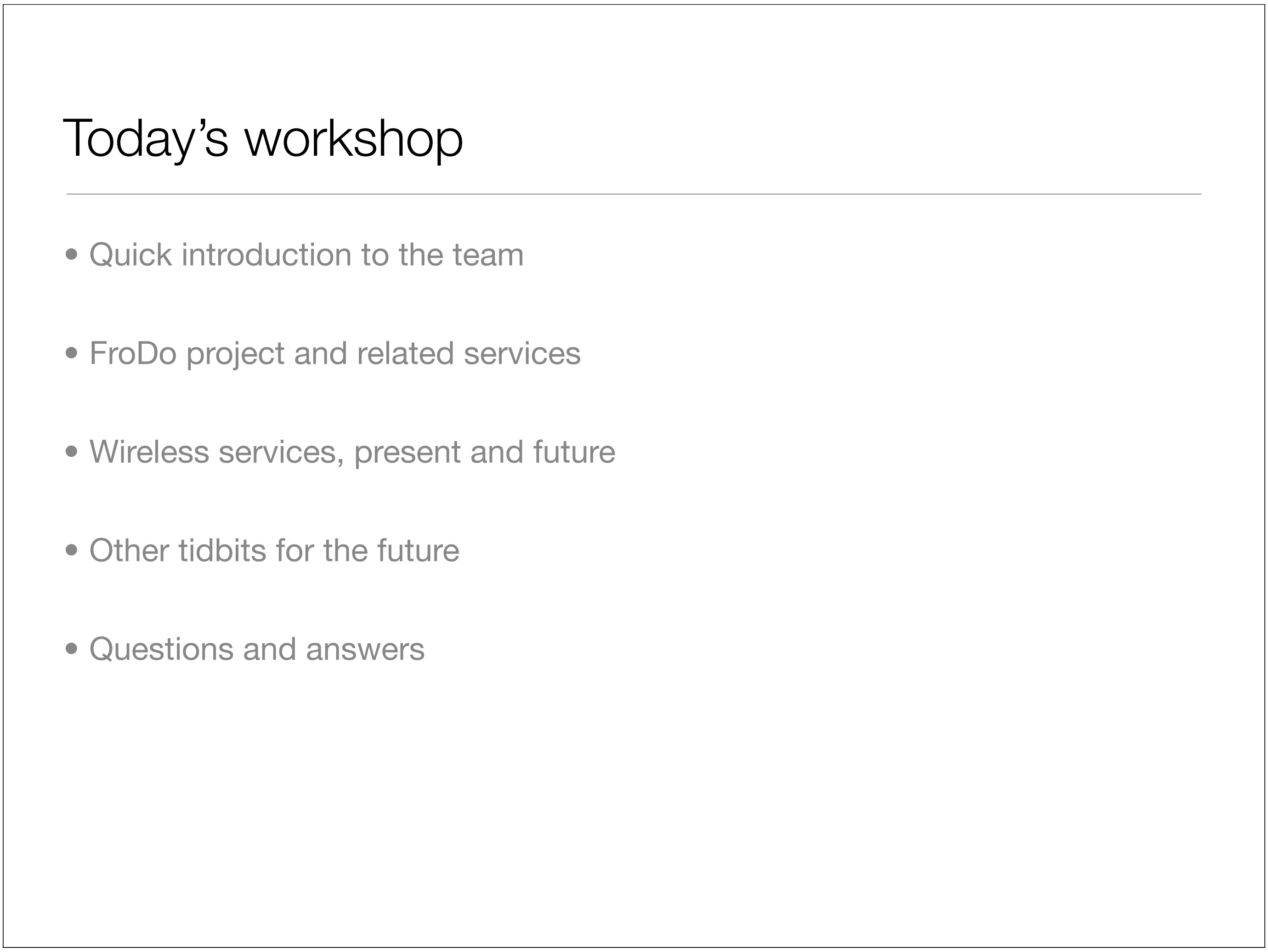
Network and Wireless Services Update, 2008

Oliver Gorwits
Senior Network Development and Support
Oxford University Computing Services

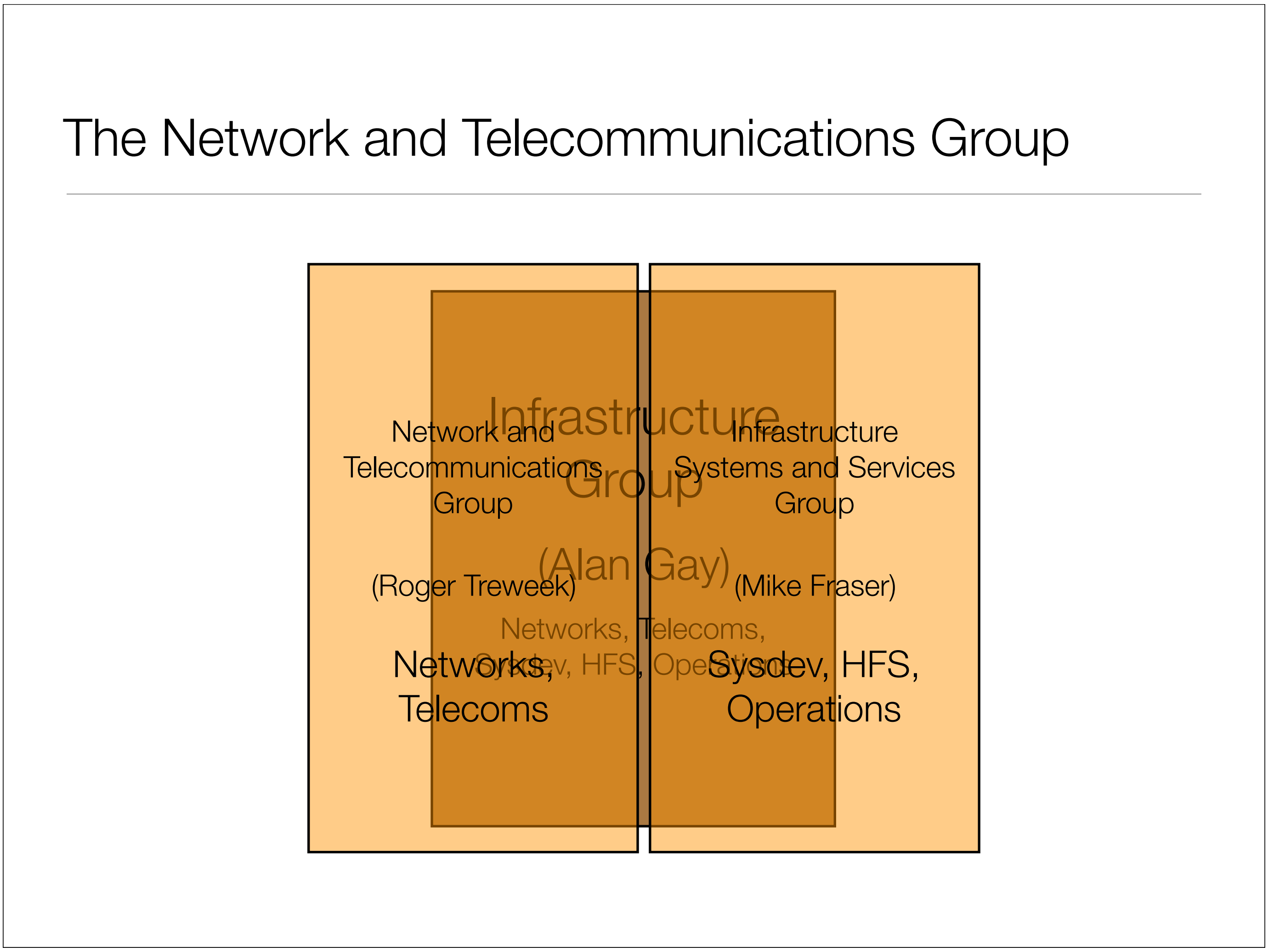
Delivered to the ICTF Conference on 16th July 2008.
If you are reading this version please note that information contained may be out of date.



Today’s workshop

- Quick introduction to the team
- FroDo project and related services
- Wireless services, present and future
- Other tidbits for the future
- Questions and answers

So today we’re going to cover quite a few topics to do with networking and wireless. To start with though I thought I’d just show you where my team lies within OUCS. Then I’m going to sum up on the FroDo project, and inform you of some additional new services you may be unaware of. Next comes what I imagine most of you are here to see, an explanation of our current and future wireless services, including the University’s new strategy for this. Then if we have time I’ll briefly talk about some new projects which are also proceeding in the next year.



The Network and Telecommunications Group

Infrastructure Group

(Alan Gay)

Networks, Telecoms, Sysdev, HFS, Operations

Network and Telecommunications Group

(Roger Treweek)

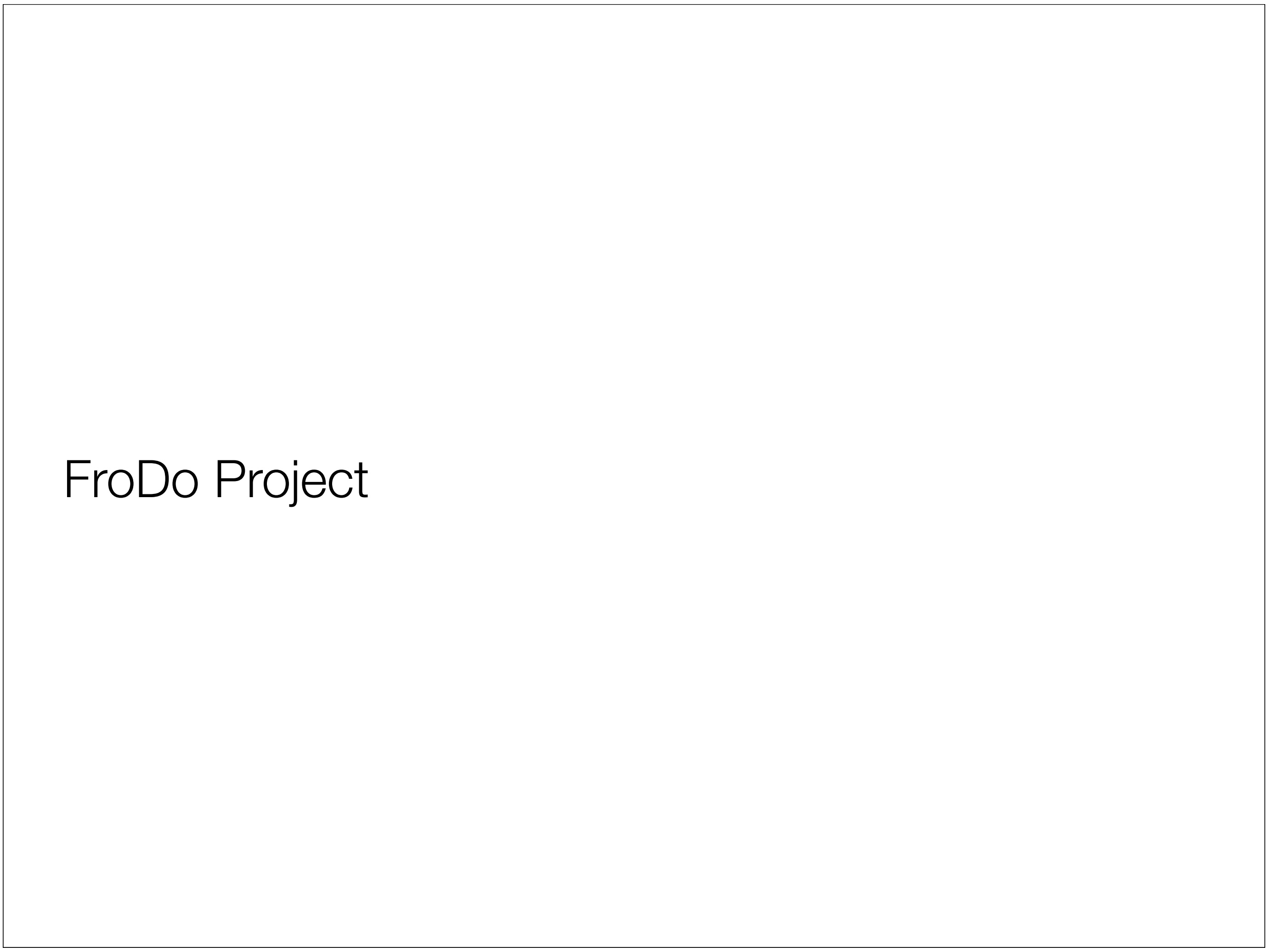
Networks, Telecoms

Infrastructure Systems and Services Group

(Mike Fraser)

Sysdev, HFS, Operations

Just one slide here as I’m sure many of you will not be aware of how things have changed in our part of OUCS. This is what you are probably familiar with, the Infrastructure Group headed by Alan Gay. Alan retired last year and following that the group was split as it had also grown quite large. We now have these two groups as you can see, headed by Roger and Mike. Of course we all still work closely together particularly on things like email relay between Oxmail and Herald.

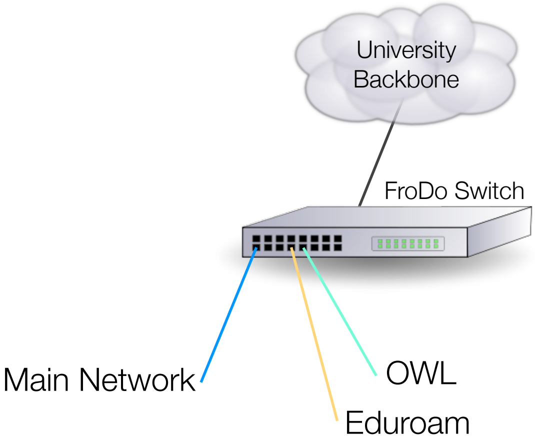


FroDo Project

The FroDo project ended this year so let’s just recap what that has brought us, especially the new services on offer.

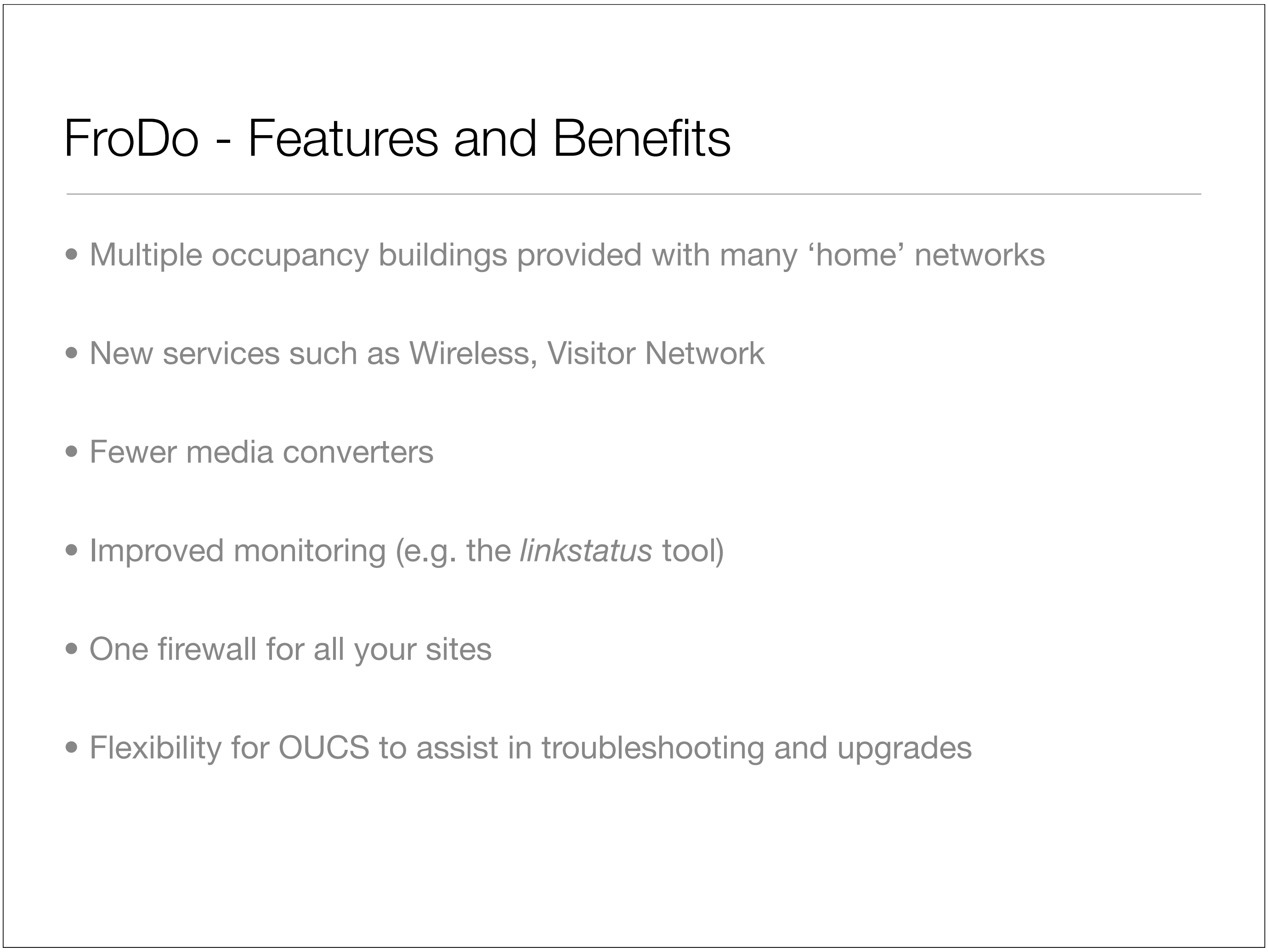
FroDo - Project Summary

- Adds a ‘distribution layer’ to the backbone network
- A switch, with UPS, in almost every building (239 so far...)



Briefly, we’re adding a layer to the onion, this time within the front door to your building. Usually it comprises a small cabinet, switch and UPS.

The diagram here shows that your college or department data connection comes off a port on the switch, as do other services such as wireless. This image will be the basis for most of the builds in this presentation.

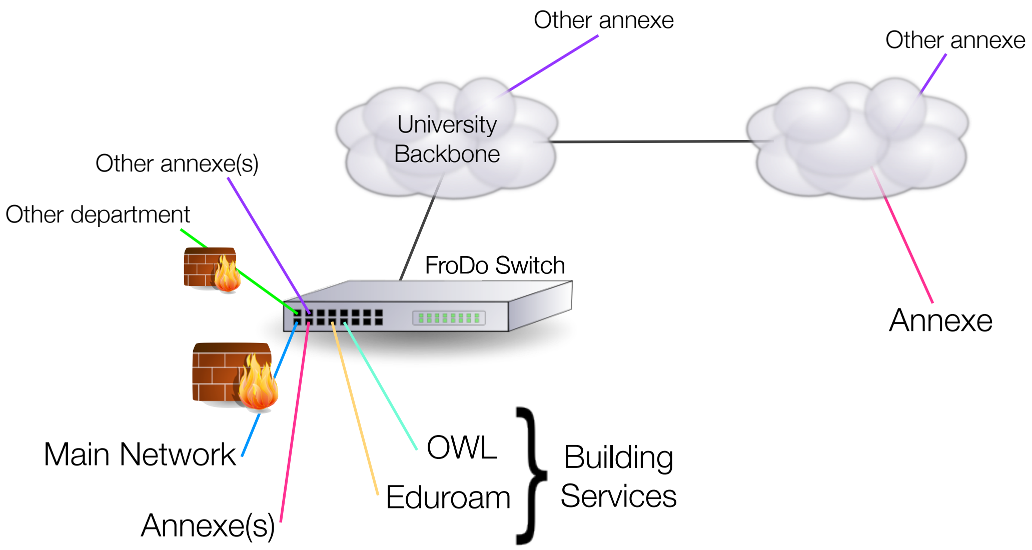


FroDo - Features and Benefits

- Multiple occupancy buildings provided with many ‘home’ networks
- New services such as Wireless, Visitor Network
- Fewer media converters
- Improved monitoring (e.g. the *linkstatus* tool)
- One firewall for all your sites
- Flexibility for OUCS to assist in troubleshooting and upgrades

This slide was skipped in the public presentation.

FroDo - Connection Scenario

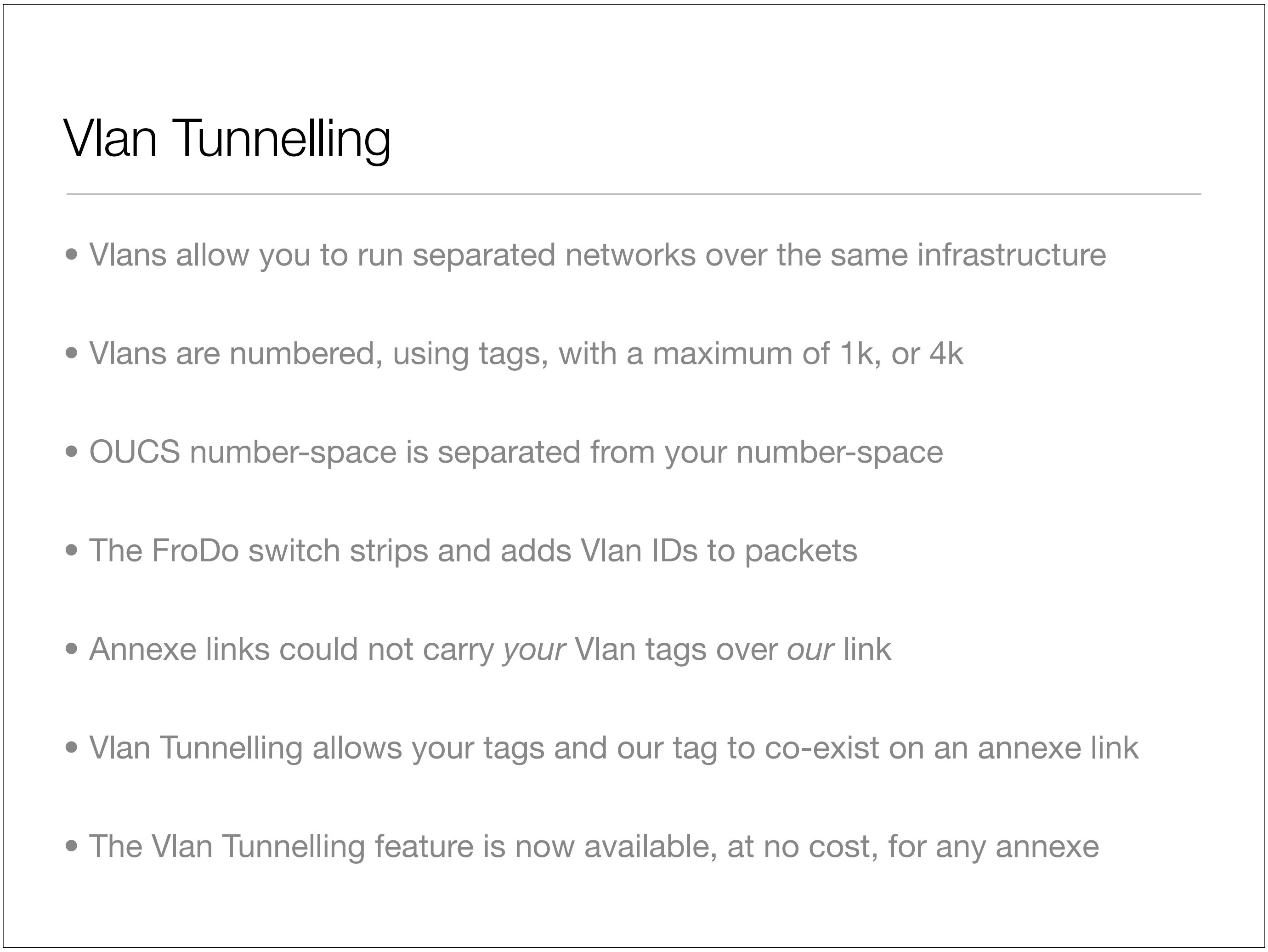


Let’s run through quickly some of the features FroDo brings.

We begin with a connected network as we saw on the previous slide. FroDo allows us to bring your annexe site connections into your main college or department site, regardless of the number of annexes. This puts those users directly on your in-house LAN, so they can share the same IP range and access the same servers directly. You can then have one firewall at the main site covering all sites, rather than the old system where you needed a firewall at each annexe a they connected directly to the Internet.

For multiple occupancy buildings FroDo allows us to deliver many separate networks rather than the old method of co-locating your systems on another department’s network. That unit as well can have its own annexes brought in separately.

One final note is that service ports such as OWL and Eduroam are provided for the building, on only one set of ports. It’s down to the occupants of the building to agree to share the wireless infrastructure and in practice we’ve not seen any problems with this.



Vlan Tunnelling

- Vlans allow you to run separated networks over the same infrastructure
- Vlans are numbered, using tags, with a maximum of 1k, or 4k
- OUCS number-space is separated from your number-space
- The FroDo switch strips and adds Vlan IDs to packets
- Annexe links could not carry *your* Vlan tags over *our* link
- Vlan Tunnelling allows your tags and our tag to co-exist on an annexe link
- The Vlan Tunnelling feature is now available, at no cost, for any annexe

A new feature we've just introduced in the last few weeks is vlan tunnelling. I'm going to give you a brief introduction to Vlans as I know this topic may be new to some of you, and then show why this feature is advantageous.

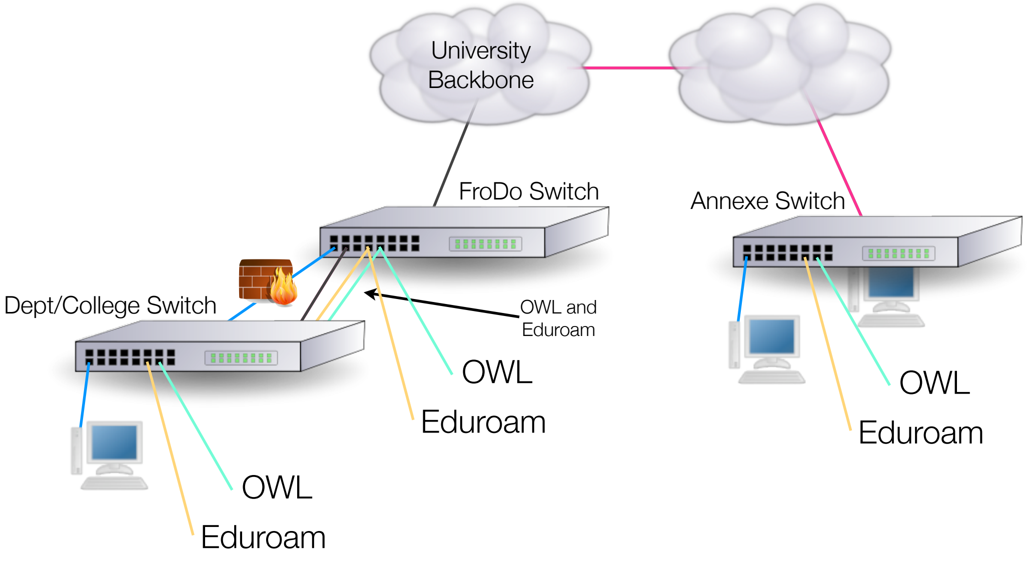
With a single physical infrastructure vlans allow you to have completely separate networks, which is great for management networks or wireless. There are a limited number of vlan tags so OUCS keeps a separate number space from your networks, and uses the FroDo to add and remove the tags.

The annexe link you saw on the previous slide used to be configured in such a way as to only carry one tag, the OUCS one, so you as a department or college could only pipe one Vlan across to your annexes.

This vlan tunnelling feature allows us to configure the links to support two levels of vlan tagging. So your tags are preserved between your sites, but our tag is used on the backbone network for switching.

This is now available. I should just note that it does require a reboot of your FroDo switch as part of the reconfiguration.

Vlan Tunnelling Diagram

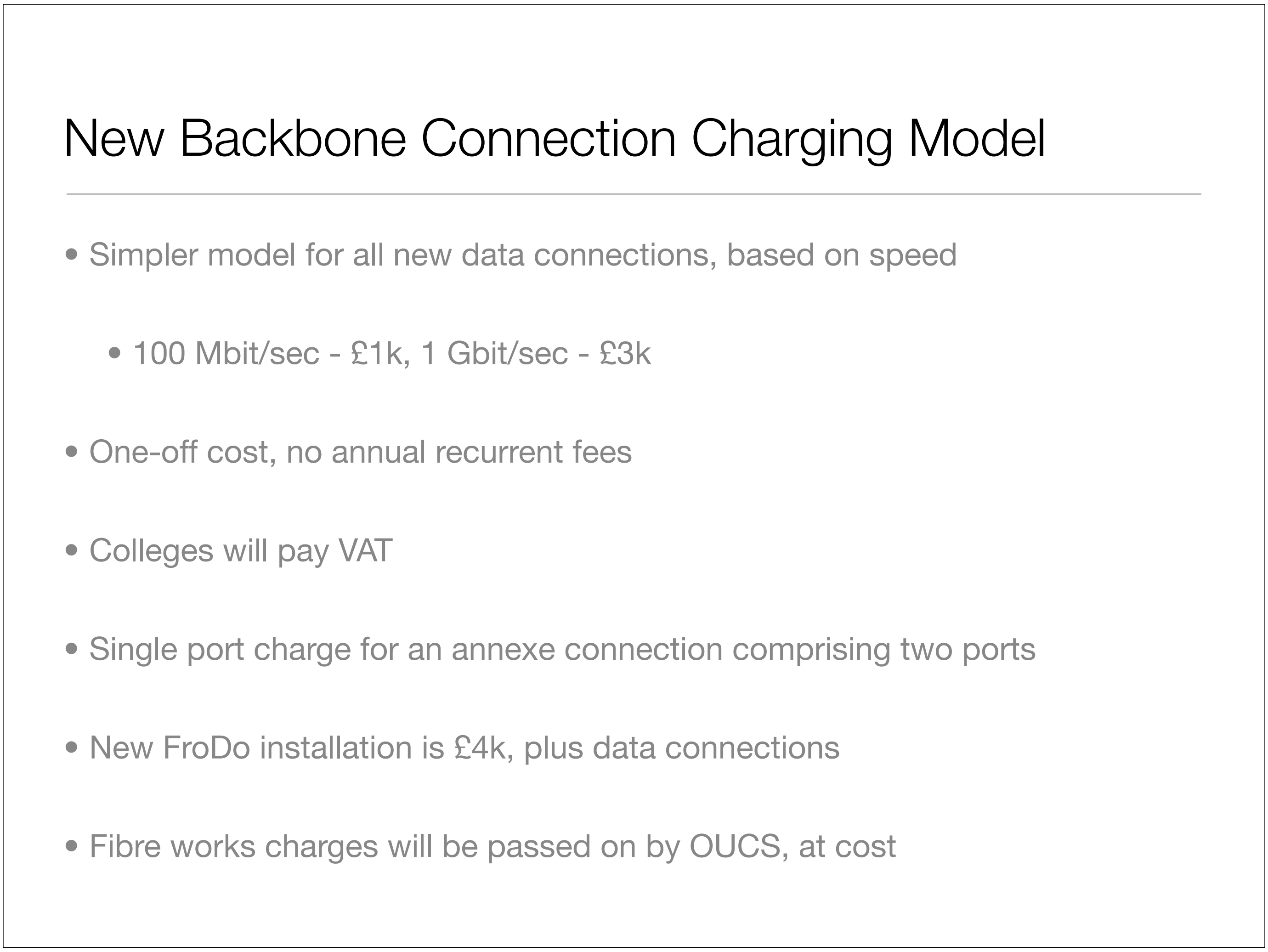


Friday, 18 July 2008

To put this in pictorial form. If we start with a regular main site feeding from the backbone. As expected the site has a switch and also uses OWL and Eduroam from the FroDo. Let’s also connect the annexe using the old system of a single Vlan connection, shown by the links in pink.

If the department takes OWL and Eduroam into its own switch infrastructure on separate Vlans, they’re still not available at the annexe site.

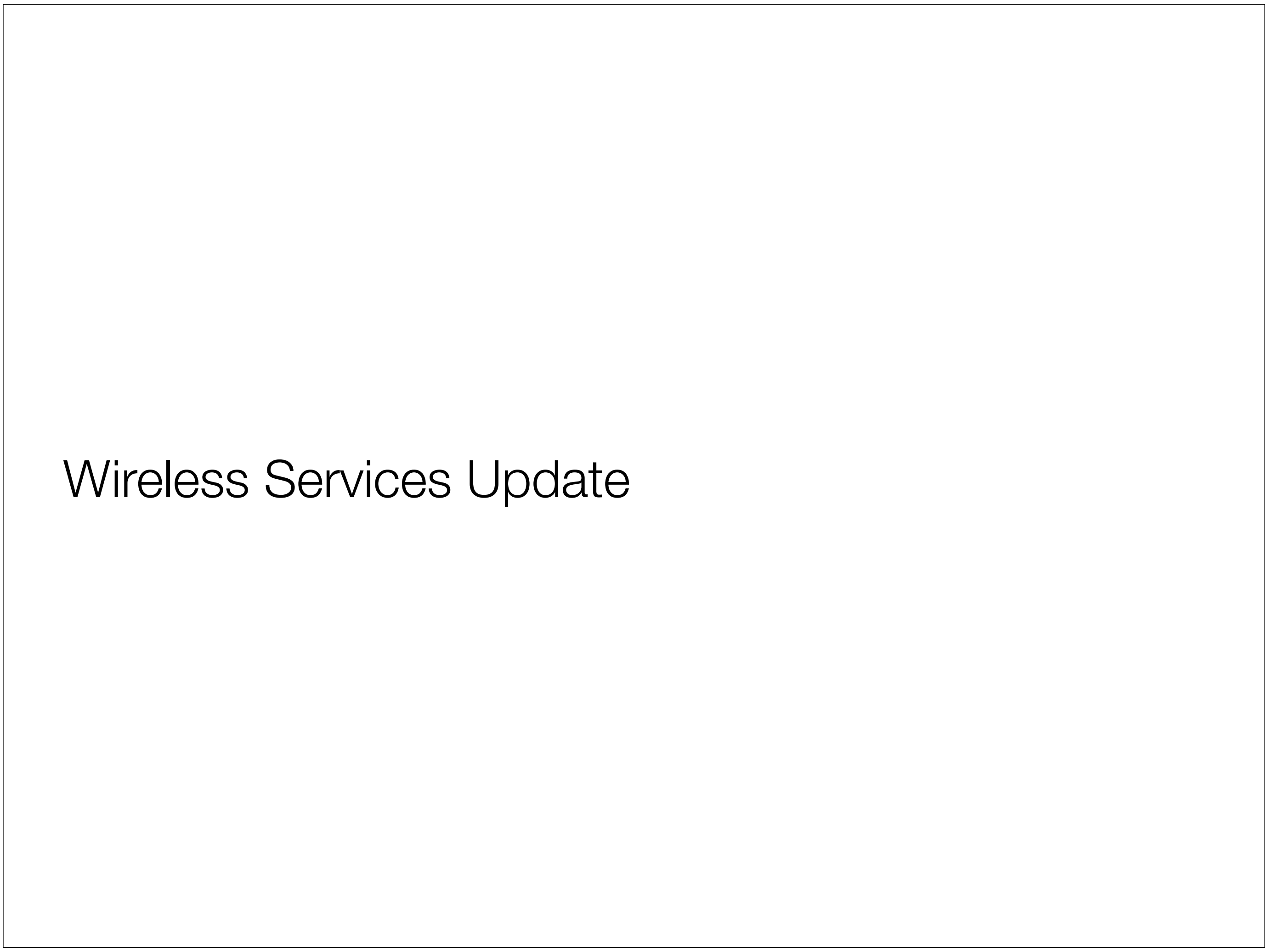
If we move to using a vlan tunnel between the main site and the annexe site, shown by the pink links changing to charcoal there, we can then attach a switch at the remote site to explode those Vlans and get all three networks at the annexe.



New Backbone Connection Charging Model

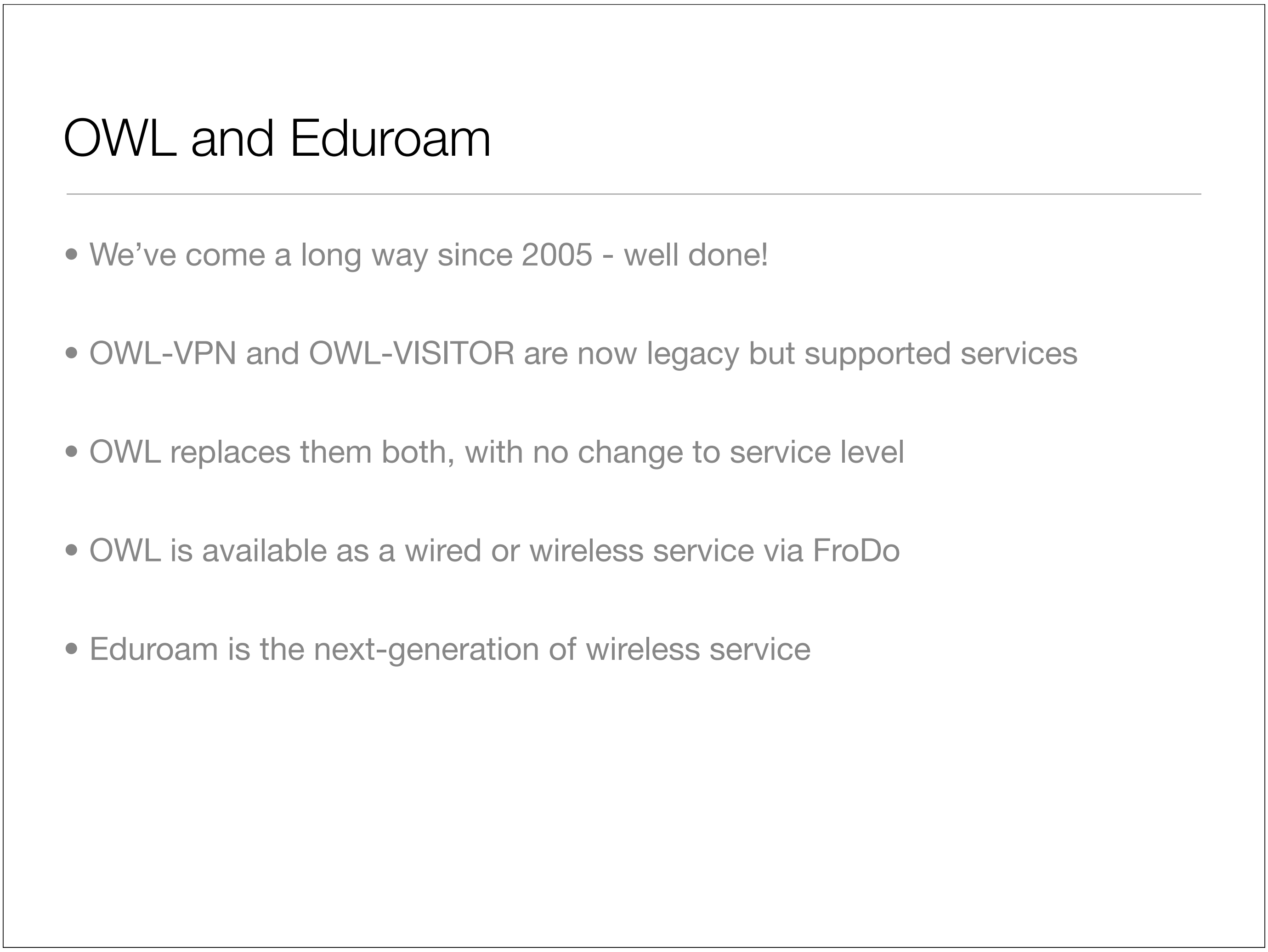
- Simpler model for all new data connections, based on speed
  - 100 Mbit/sec - £1k, 1 Gbit/sec - £3k
- One-off cost, no annual recurrent fees
- Colleges will pay VAT
- Single port charge for an annexe connection comprising two ports
- New FroDo installation is £4k, plus data connections
- Fibre works charges will be passed on by OUCS, at cost

This slide was skipped in the public presentation.



Wireless Services Update

So that wraps up the FroDo, let’s move onto wireless.



OWL and Eduroam

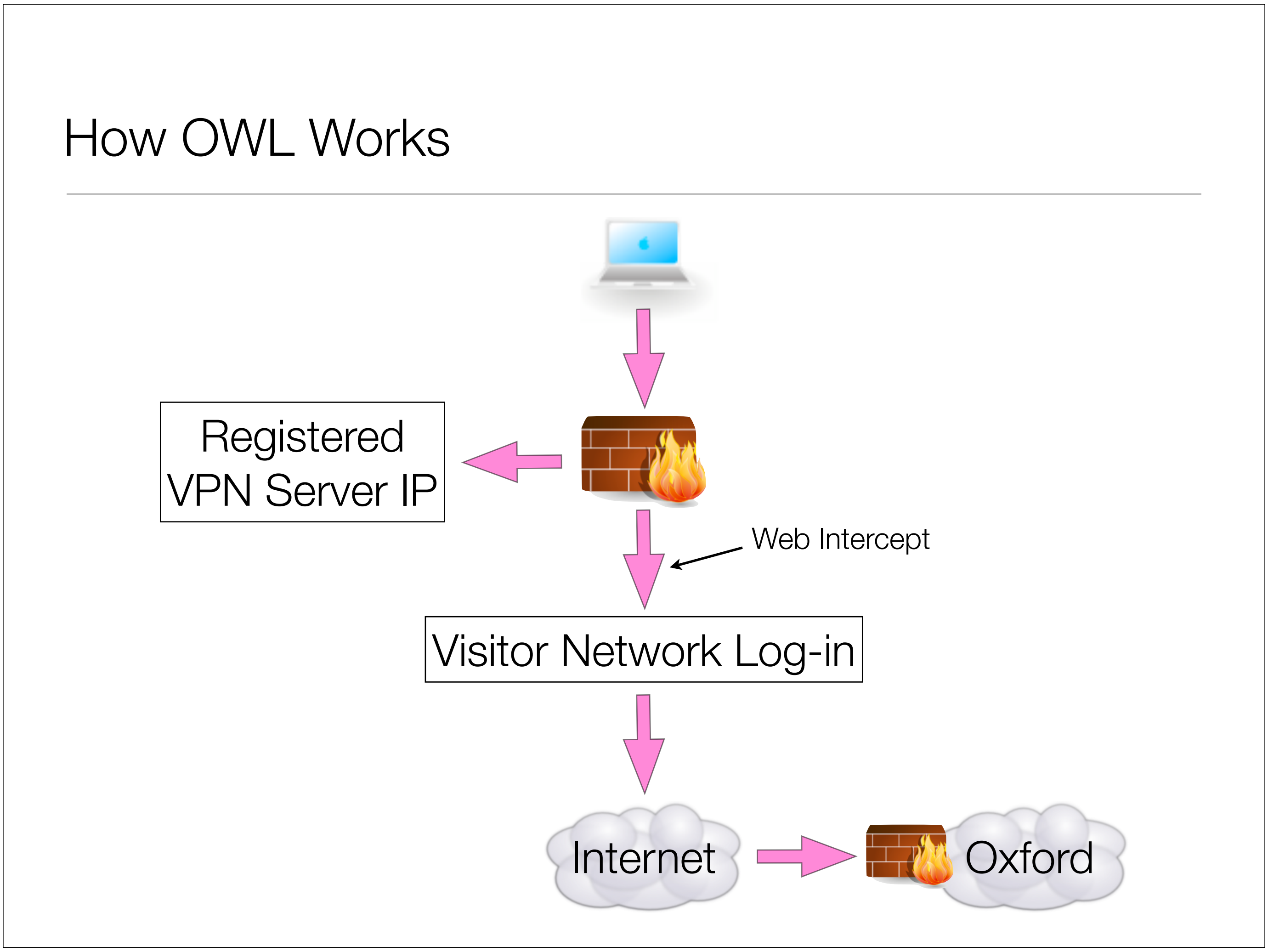
- We’ve come a long way since 2005 - well done!
- OWL-VPN and OWL-VISITOR are now legacy but supported services
- OWL replaces them both, with no change to service level
- OWL is available as a wired or wireless service via FroDo
- Eduroam is the next-generation of wireless service

I’m going to first explain what OWL and Eduroam are, before moving on to the new strategic developments in wireless.

I think the achievements in wireless so far are something to be proud of. From what I’ve seen at other UK Universities we’re doing very well; it’s more impressive here because of our federated IT model.

The Visitor and VPN variants of OWL are now deprecated, although they are of course still supported by OUCS. We’ve replaced them both with OWL, which serves the exact same services but in one SSID. You should also be aware that OWL is available over wired connections.

Eduroam is of course the next big thing. It’s a much improved wireless experience.



How OWL Works

Registered VPN Server IP

Web Intercept

Visitor Network Log-in

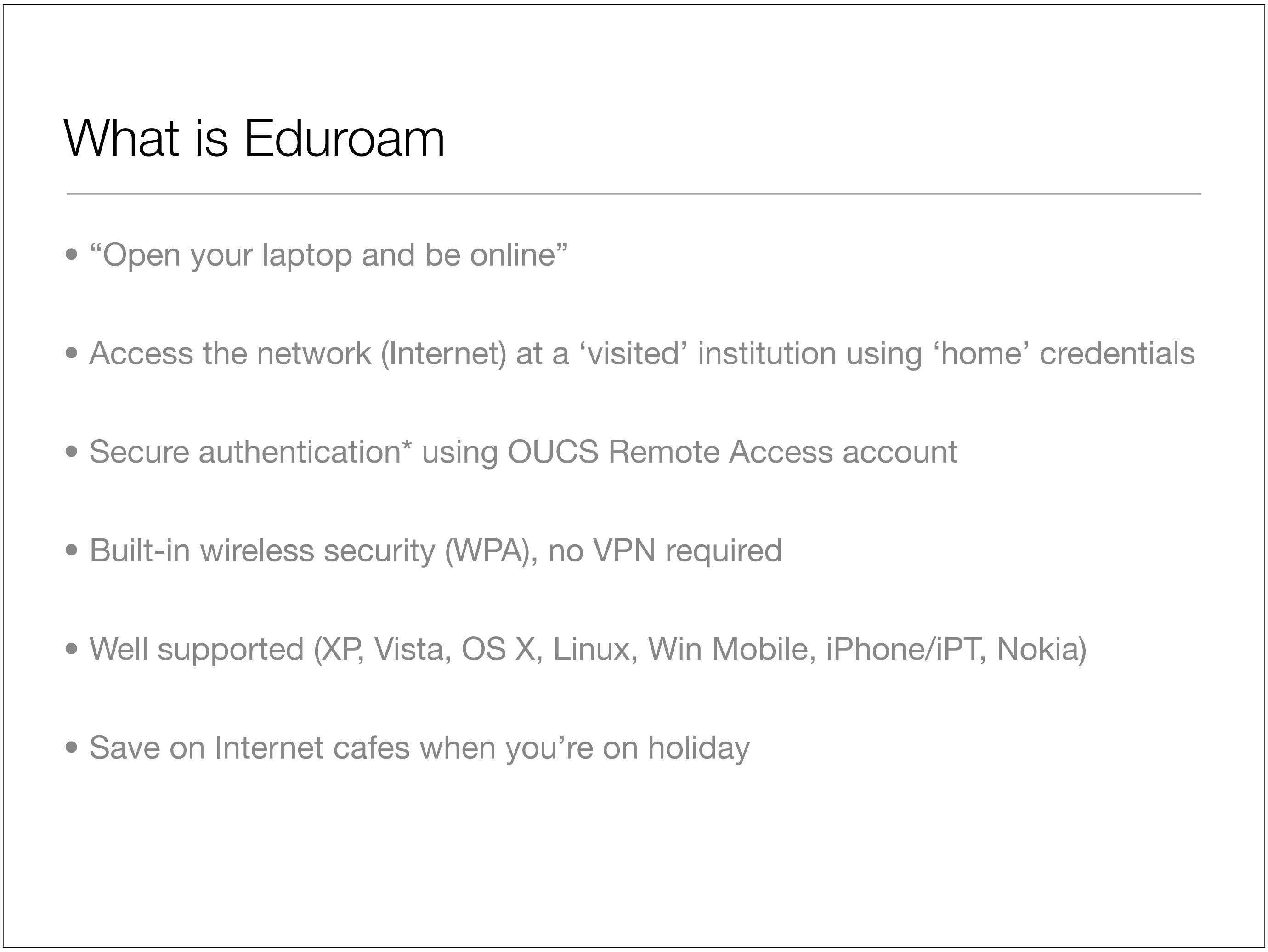
Internet

Oxford

Very briefly, this is what you get with OWL.

The user connects to the wireless network and then if they contact servers in our list of registered IPs then that traffic is immediately permitted. If you run a VPN service which you already expose to the Internet then feel free to send us an email asking to be added to the list. This means users don't first need to connect to the OUCS VPN before connecting on to your own VPN.

If not using that service, all users are presented with the Visitor Network log in page, and if they log in successfully then they're on the Internet. Note that they're outside of the Oxford network, so come back in as any other Internet user through the JANET connection firewall.



What is Eduroam

- “Open your laptop and be online”
- Access the network (Internet) at a ‘visited’ institution using ‘home’ credentials
- Secure authentication* using OUCS Remote Access account
- Built-in wireless security (WPA), no VPN required
- Well supported (XP, Vista, OS X, Linux, Win Mobile, iPhone/iPT, Nokia)
- Save on Internet cafes when you’re on holiday

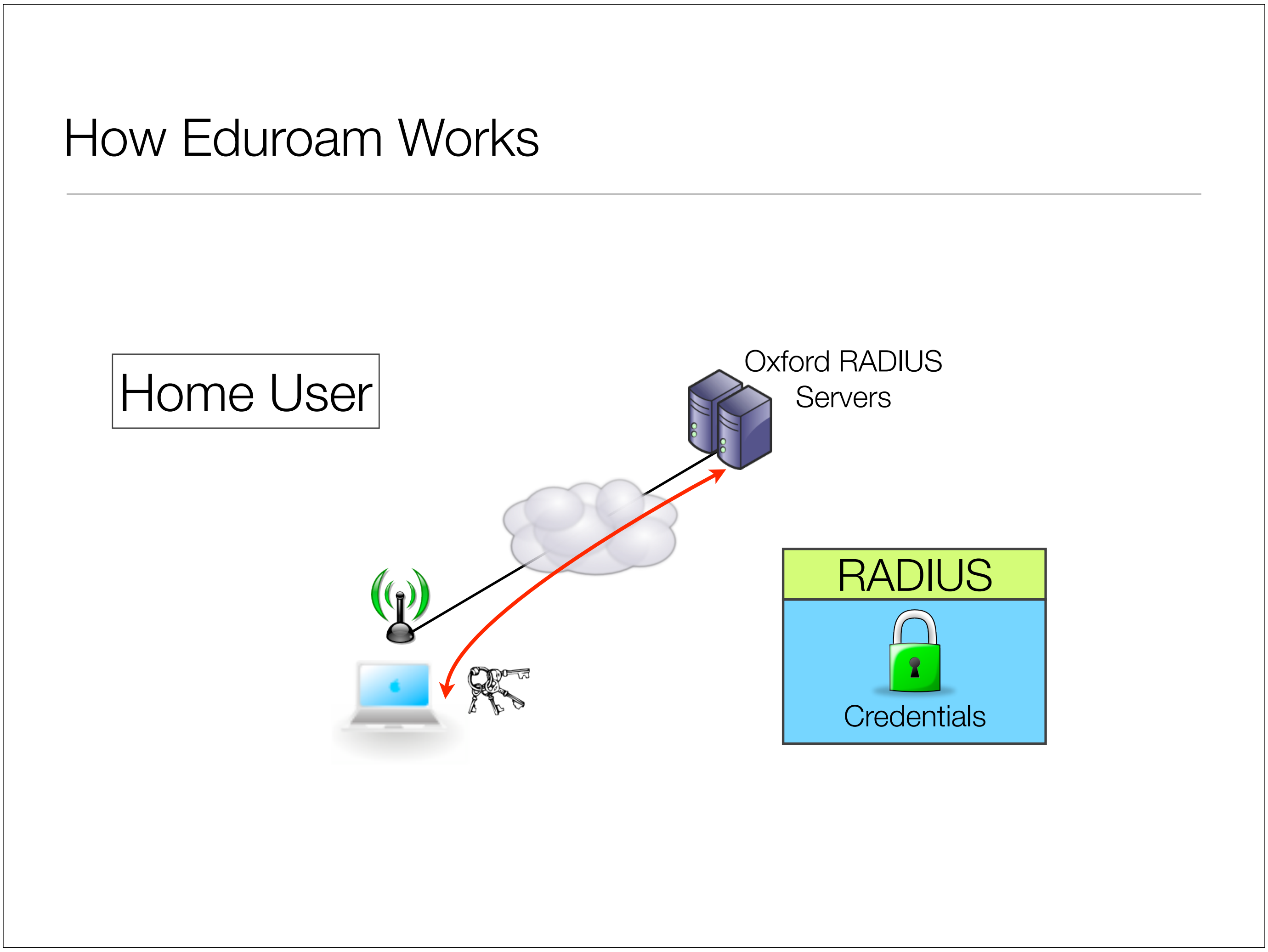
I think this phrase from the Eduroam web site sums it up. The idea is to make a secure connection to the network, but seamlessly.

Eduroam provides access for local users, and a better experience for Oxford members than OWL. For visitors it’s a way to access the network without having to make any contact with you as local ITSS.

Oxford users use the OUCS Remote Access Account.

No additional software is required, everything is built into most operating systems, including now the iPhone and iPod Touch I’m pleased to say!

And most people tell me they appreciate using local education networks for some free Internet access whilst on holiday.



How Eduroam Works

Home User

Oxford RADIUS Servers

RADIUS

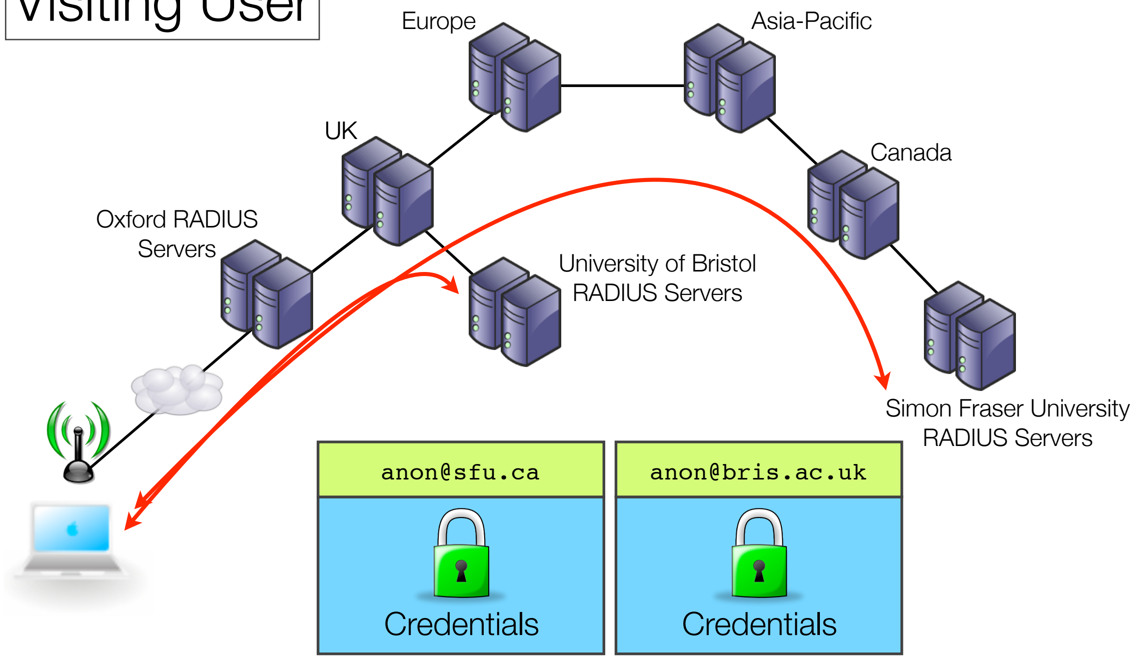
Credentials

Under eduroam the user’s credentials are not seen by the local access point. A secure tunnel is established between their system and the OUCS RADIUS servers. The authentication takes place over a secure channel.

However the packets sent do have an outer RADIUS part which the access point can read, so it knows whether to accept the client onto the network or not.

How Eduroam Works

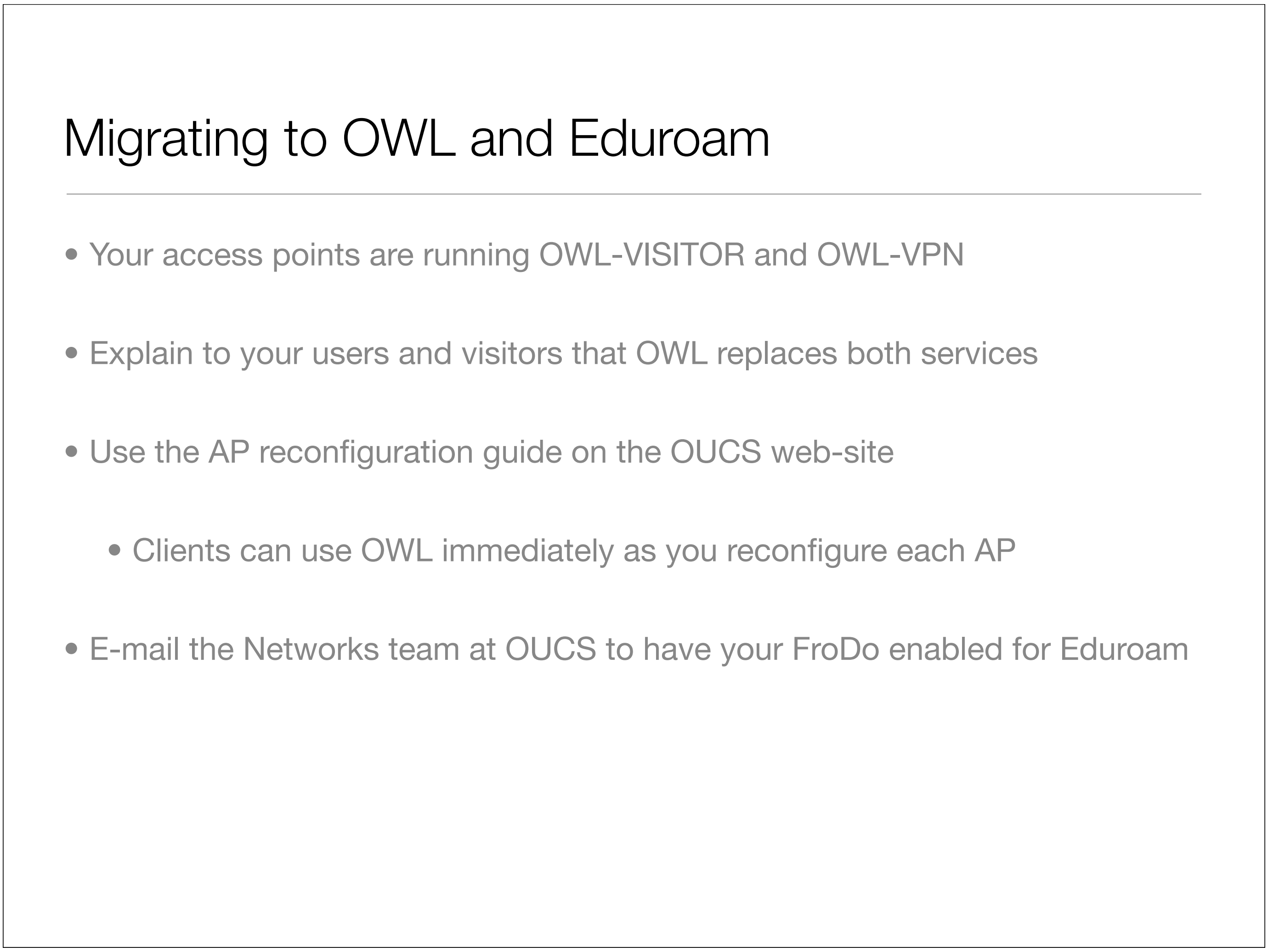
Visiting User



For users visiting Oxford or Oxford users visiting elsewhere the process is similar. For this you need to append the institution domain to the username, so for a Bristol user it would look like this.

The Oxford servers don’t know that institution domain, so they pass the authentication to the UK servers which pass it back to the Bristol servers. The client is still establishing a secure connection all the way to its home servers - none of the intermediate servers or systems can read the credentials.

For an internationally roaming user it’s much the same. Let’s whiz through how it looks for a user from Canada. This time the UK servers don’t know the domain so they pass it up to the European servers who do know, and punt it across to Asia-Pacific as there’s no North American continental server. Down it goes to SFU and again we see that it’s a secure connection end to end.



Migrating to OWL and Eduroam

- Your access points are running OWL-VISITOR and OWL-VPN
- Explain to your users and visitors that OWL replaces both services
- Use the AP reconfiguration guide on the OUCS web-site
    - Clients can use OWL immediately as you reconfigure each AP
- E-mail the Networks team at OUCS to have your FroDo enabled for Eduroam

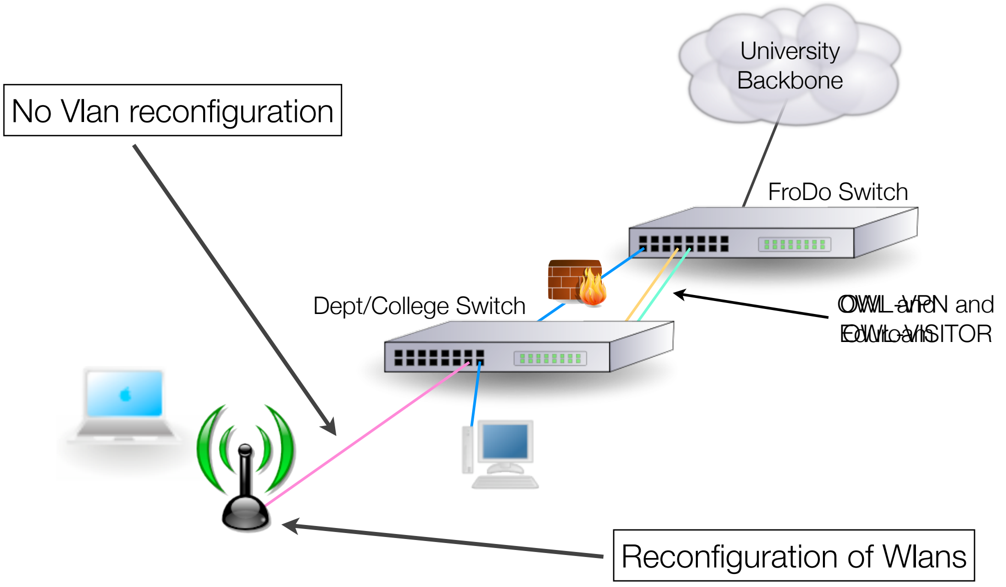
The steps for migrating from VPN and Visitor to OWL and Eduroam are not too involved.

Remember that the OWL service replaces both existing services so explain this to your users.

On the OUCS website we have a configuration guide PDF doc which talks you through a migration, and also a bare metal configuration of OWL and Eduroam.

Your users can use OWL immediately, and email my team to have Eduroam activated on your FroDo. We won’t do this in advance as it needs to be fully secured through having all access points reconfigured.

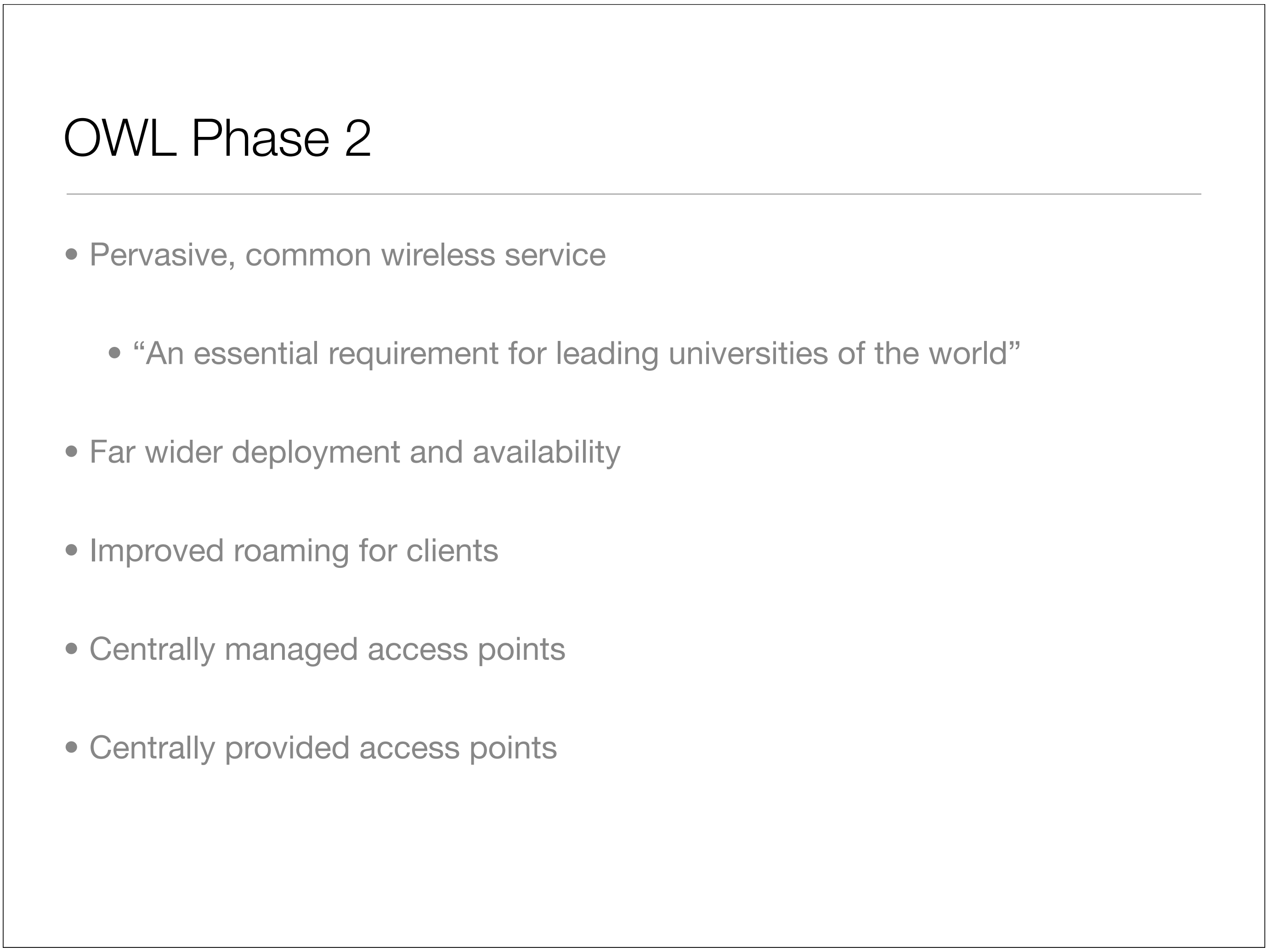
OWL and Eduroam - Before and After



No Vlan reconfiguration

Reconfiguration of Wlans

This slide was skipped in the public presentation.



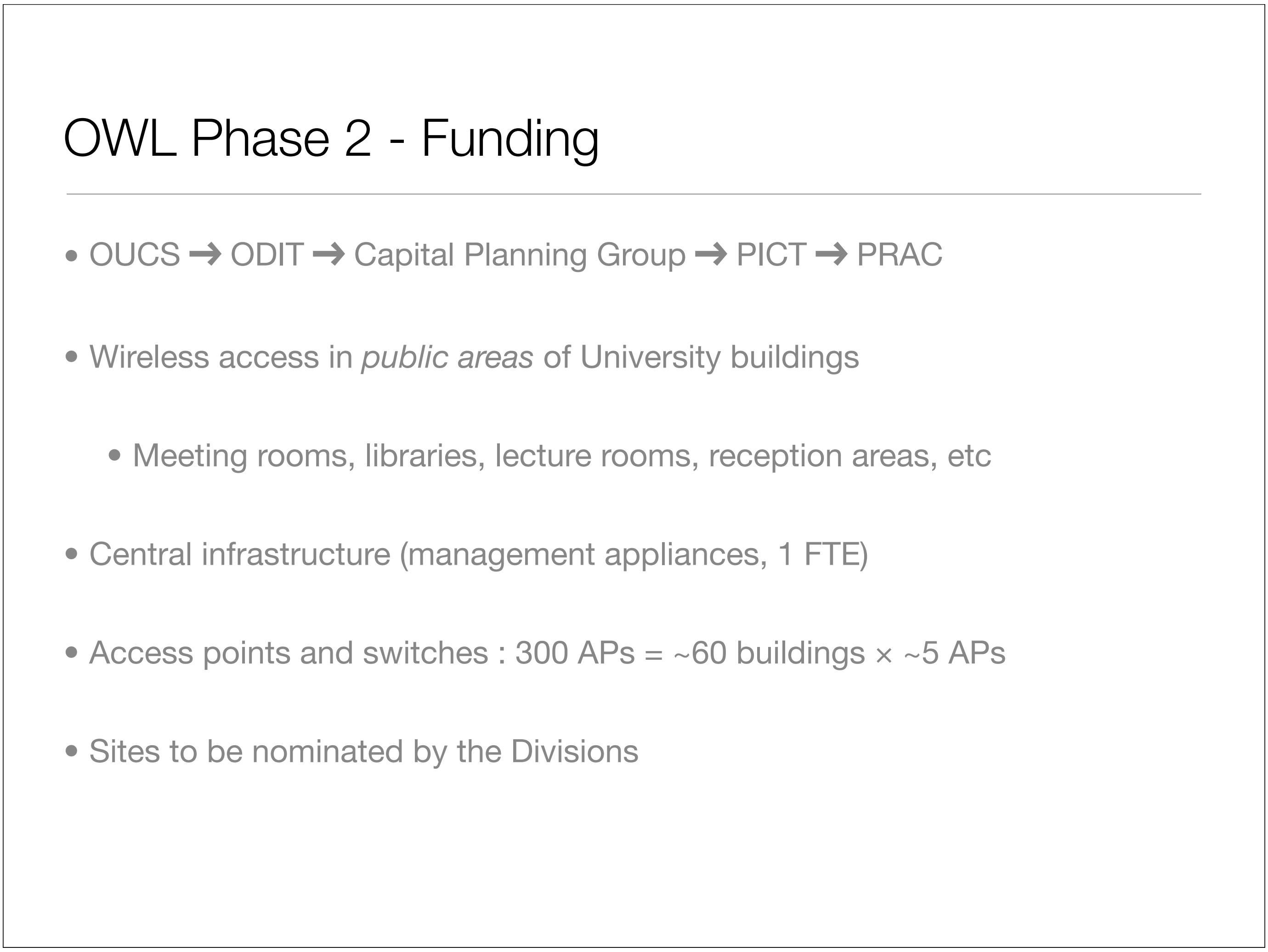
OWL Phase 2

- Pervasive, common wireless service
  - “An essential requirement for leading universities of the world”
- Far wider deployment and availability
- Improved roaming for clients
- Centrally managed access points
- Centrally provided access points

Understandably, pervasive wireless is expected in an institution of this type. But how does that differ from what we’re already doing?

Clearly, it means -more-, in particular more access points, more hotspots, and more services. Also it means an improved experience for users as they take on more demanding applications such as video and voice.

And to us as IT staff it can mean a saving in the management overheads of wireless. Centrally managed access points, and also centrally provided access points for selected areas.



OWL Phase 2 - Funding

- OUCS ➔ ODIT ➔ Capital Planning Group ➔ PICT ➔ PRAC
- Wireless access in *public areas* of University buildings
  - Meeting rooms, libraries, lecture rooms, reception areas, etc
- Central infrastructure (management appliances, 1 FTE)
- Access points and switches : 300 APs = ~60 buildings × ~5 APs
- Sites to be nominated by the Divisions

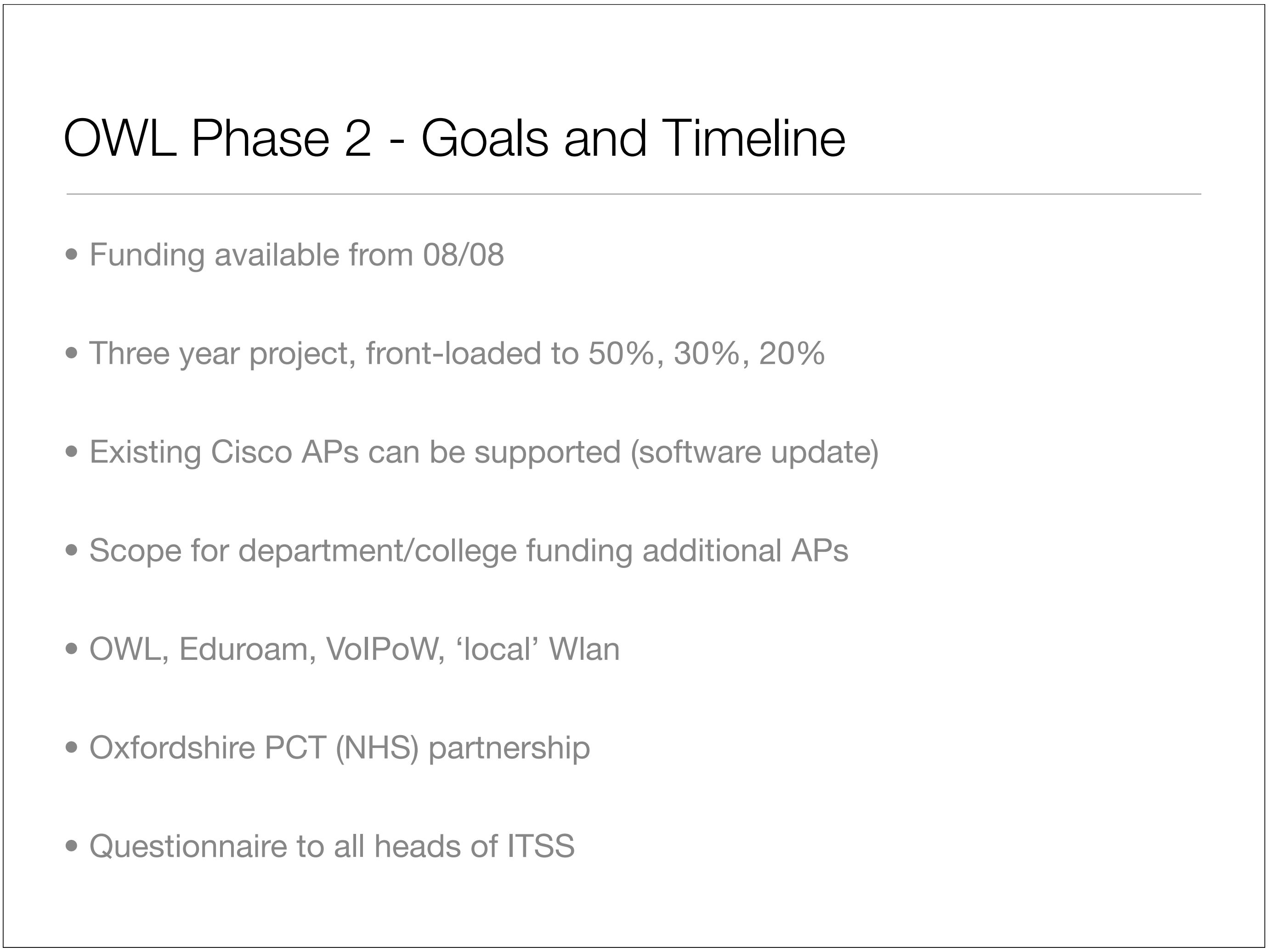
So let me explain how OUCS came by the funding to achieve this. The University director of IT, Paul Jeffreys, sent out a request for note of capital projects which could be considered by university committees. I assisted Roger Treweek in preparing a paper for Paul’s office, ODIT, which then submitted it to the Capital Planning Group. This is a committee charged with whittling down all the requests for capital funding to a handful of candidates. This then went to the PRAC ICT Sub Committee and then finally PRAC for approval.

The most important factor is that this funding covers public areas in the University. It really would be prohibitively expensive to centrally fund flood wireless in all the office spaces I’m afraid - however there’s scope for additional hotspots which I’ll cover shortly. Here are some examples of what are considered public areas - you might say they are shared workspaces as of course they might not be open to members of the public.

OUCS is funded to provide the central infrastructure required to support this, including one new post.

In the bid we had to detail the scale of the funded access point deployment. The figure arrived at was 300 access points, and the University has around 60 buildings which you might call significant, so that’s an average of 5 access points each, for the public areas.

None of us at OUCS believe we are in a good position to determine where there will be demand for wireless, so Stuart Lee last week I believe sent an email to the heads of each of the five Divisions asking for somebody to let us know where they would like the hotspots to be. If you, in your department, think there’s a shared space crying out for wireless then please as in your Division to have yourself put on the list.



OWL Phase 2 - Goals and Timeline

- Funding available from 08/08
- Three year project, front-loaded to 50%, 30%, 20%
- Existing Cisco APs can be supported (software update)
- Scope for department/college funding additional APs
- OWL, Eduroam, VoIPoW, ‘local’ Wlan
- Oxfordshire PCT (NHS) partnership
- Questionnaire to all heads of ITSS

My team will receive funding from August this year, and the design of the system is pretty much complete so we hope to get underway soon.

It’s a three year deployment, and these percentages refer to the number of access points we intend to deploy from our pool of 300 over the three years.

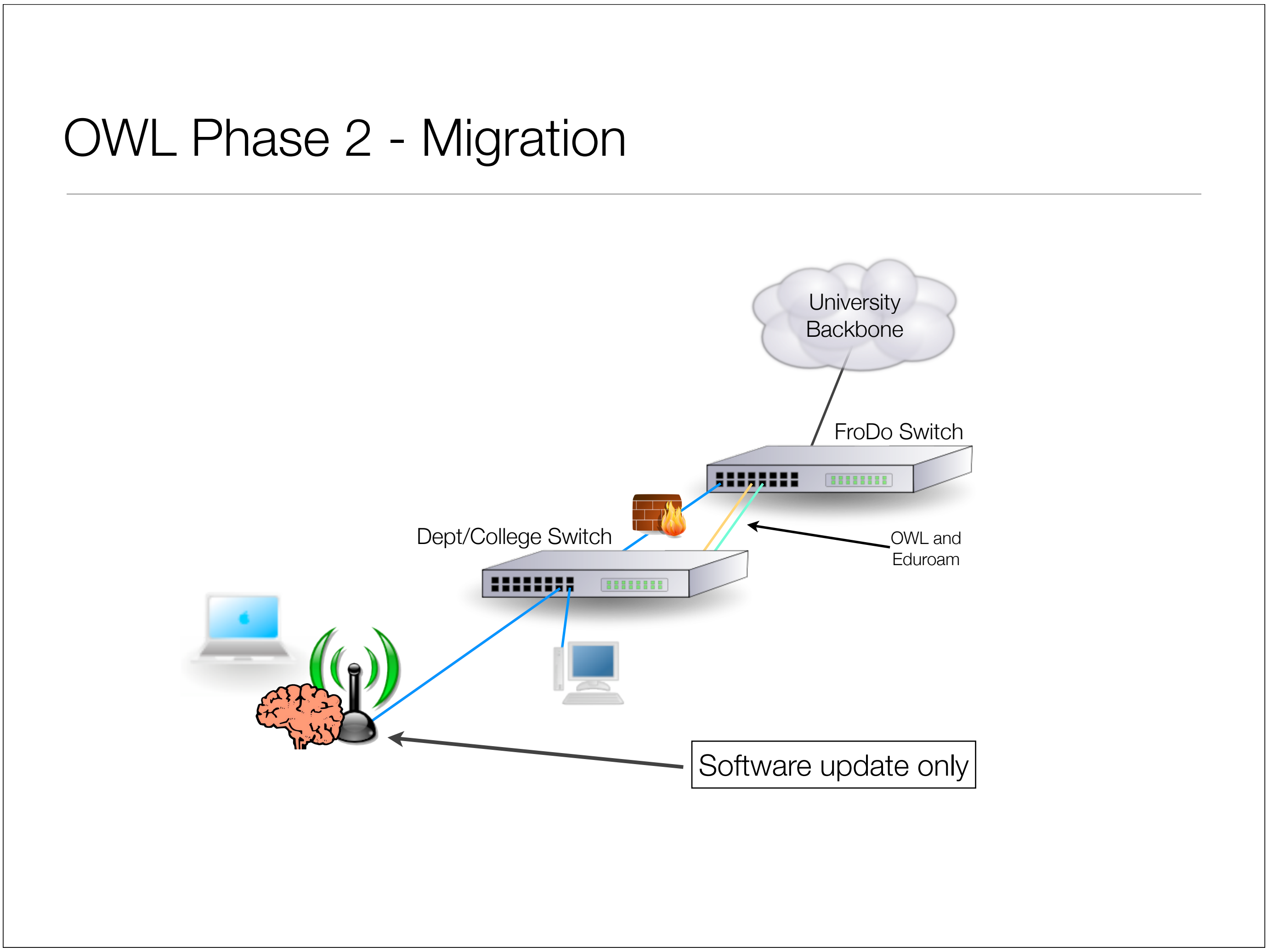
As you know we have been recommending the purchase of Cisco access points since the beginning of OWL, because we knew that they could all be reconfigured to support a central management system. That means your existing Cisco access points can be supported, if you wish for OUCS to manage them of course.

There will also be scope for you to purchase additional access points which might be for office spaces, or shared areas which did not make it onto the Divisional selection list. We will of course be specifying which access points are to be purchased but OUCS will also try to get good pricing through our work with Cisco, suppliers and the University purchasing officer.

The networks served by this will of course be OWL and Eduroam, plus we hope to push out wireless voice over IP services. This seems to be very popular with support personnel who roam around, or a helpdesk environment. Finally we also will aim to provide each department and college with a local wireless network which connects back to your site.

An interesting collaboration is with the Oxfordshire NHS who have a similar Cisco wireless system projected to have around 1,500 access points. We have an agreement with them to push OWL and Eduroam out over that network as well, which is good news for the medical sciences people working in Oxford hospitals.

Finally, but before any of this really goes ahead, my team will be sending you a questionnaire to help us refine all of these points. It’s really important to get your feedback on these plans before we get stuck in, to help us deliver the most useful service to you.



OWL Phase 2 - Migration

University Backbone

FroDo Switch

Dept/College Switch

OWL and Eduroam

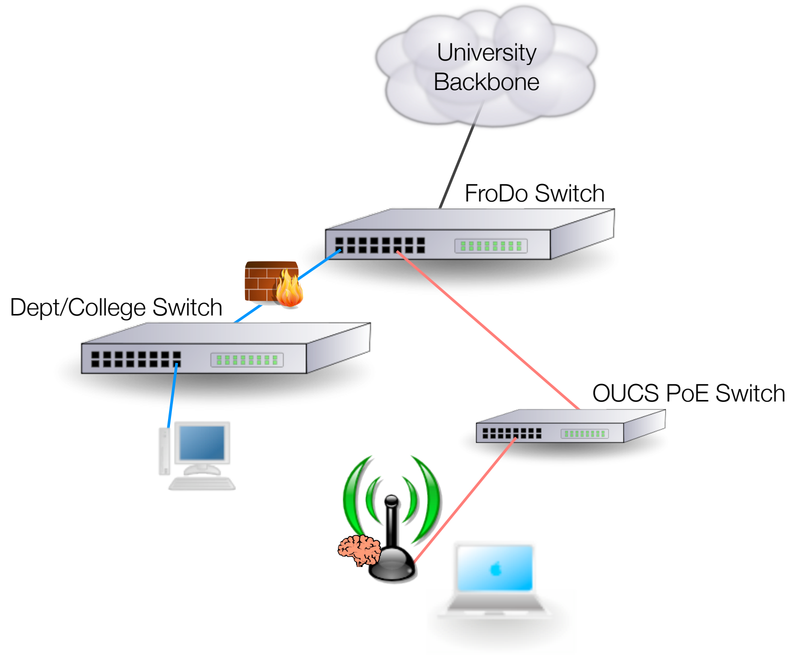
Software update only

Now for some more pictures. When you add wireless using our blueprint under the current scheme you end up with an autonomous access point connected via a trunk link into your switch, and you also take feeds from the OWL and Eduroam FroDo ports.

To migrate to the managed wireless system you would load a new software image onto the access point, and that’s probably going to be it. The link to the switch is now using your local in-house LAN, and you can dispense with the OWL and Eduroam feeds if you wish.

I’ll cover some of the technical points in a couple of slides but as you can see there’s little to do, and especially little configuration.

OWL Phase 2 - New Installation



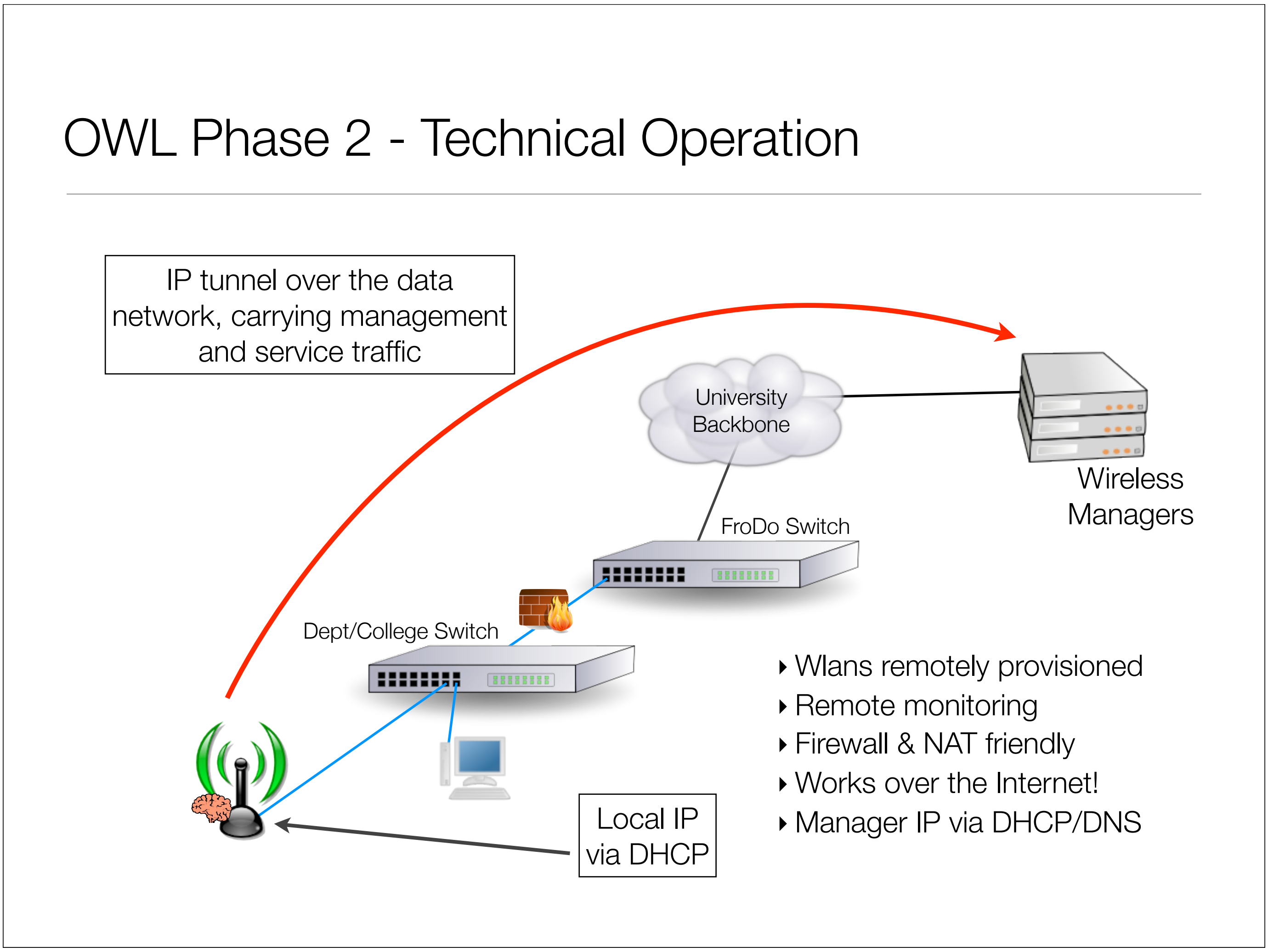
University Backbone

FroDo Switch

Dept/College Switch

OUCS PoE Switch

For a new installation of centrally provided access points we have support in the funding to provide our own managed switches. We expect these will be power over ethernet eight port switches, for simplicity.



OWL Phase 2 - Technical Operation

IP tunnel over the data network, carrying management and service traffic

University Backbone

Wireless Managers

FroDo Switch

Dept/College Switch

Local IP via DHCP

- Wlans remotely provisioned
- Remote monitoring
- Firewall & NAT friendly
- Works over the Internet!
- Manager IP via DHCP/DNS

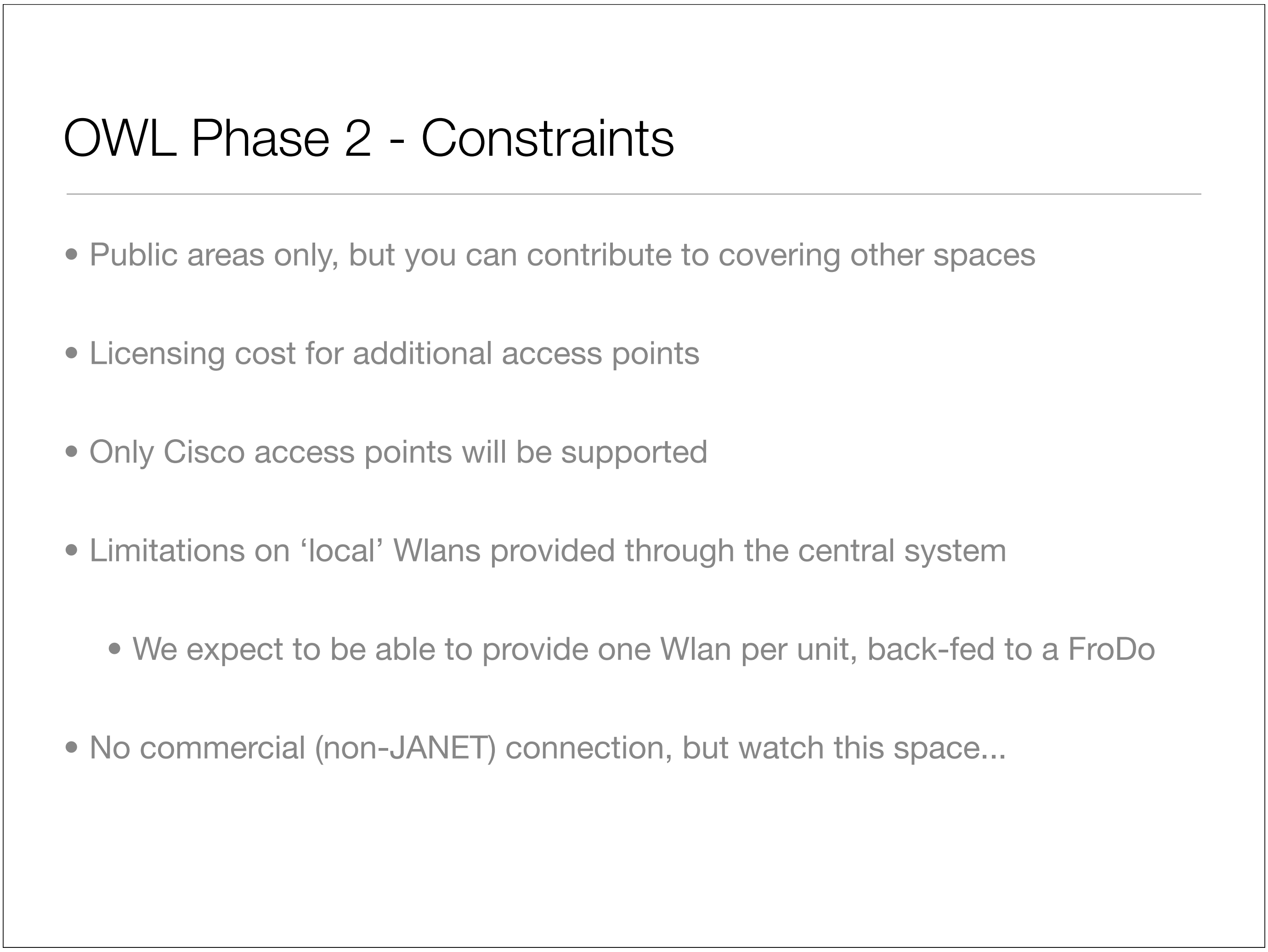
Now I’m going to show you a little more detail on how the managed access point system works.

We begin with an access point on your data network although it could also be on our infrastructure as I showed in the previous slide.

The access point has an IP address configured via DHCP from the local area network’s subnet. In the core of the network we have some management appliances. The access point establishes a tunnel back to its management appliance, the controller, and over this is sent all the management and service traffic.

This means the Wlans are provisioned remotely. We also monitor things centrally from the management appliances, as they can see if any access point goes offline and also track client status. The IP tunnel is NAT and Firewall friendly, even working across the Internet.

And you may ask how does the access point know where the controller is - well it gets that address either in a DHCP option field or via a predictable DNS entry in its local subdomain.



OWL Phase 2 - Constraints

- Public areas only, but you can contribute to covering other spaces
- Licensing cost for additional access points
- Only Cisco access points will be supported
- Limitations on ‘local’ Wlans provided through the central system
  - We expect to be able to provide one Wlan per unit, back-fed to a FroDo
- No commercial (non-JANET) connection, but watch this space...

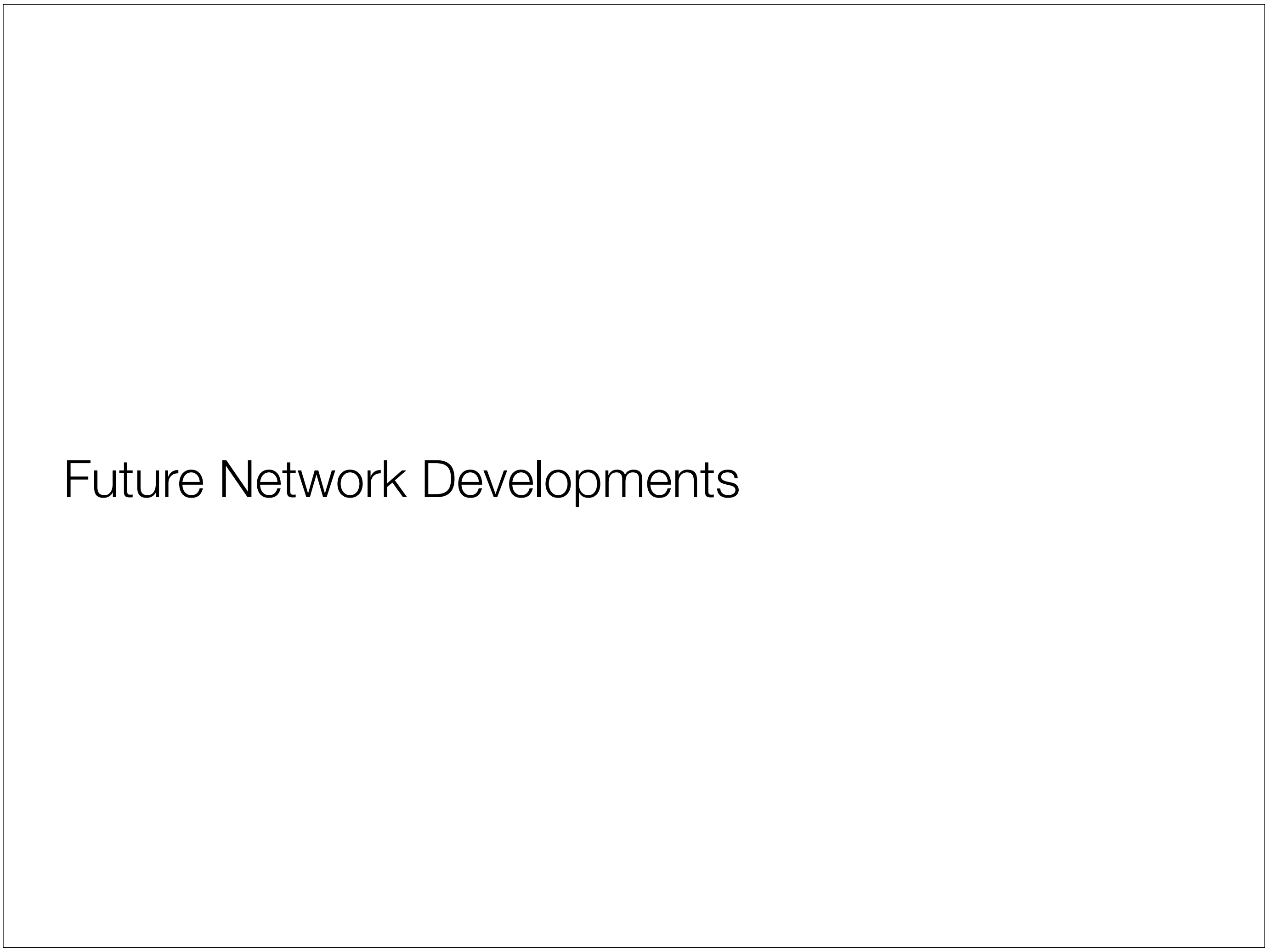
Remember that we can only fund access points in public areas, but you are able to contribute towards access points anywhere else.

There’s likely to be an up front cost to add these access points to the system, because we pay a license fee per access point on the central controllers, and also because we need to fund a portion of the cost of the controller which will be managing your supplied access point.

Naturally, we can only support Cisco access points.

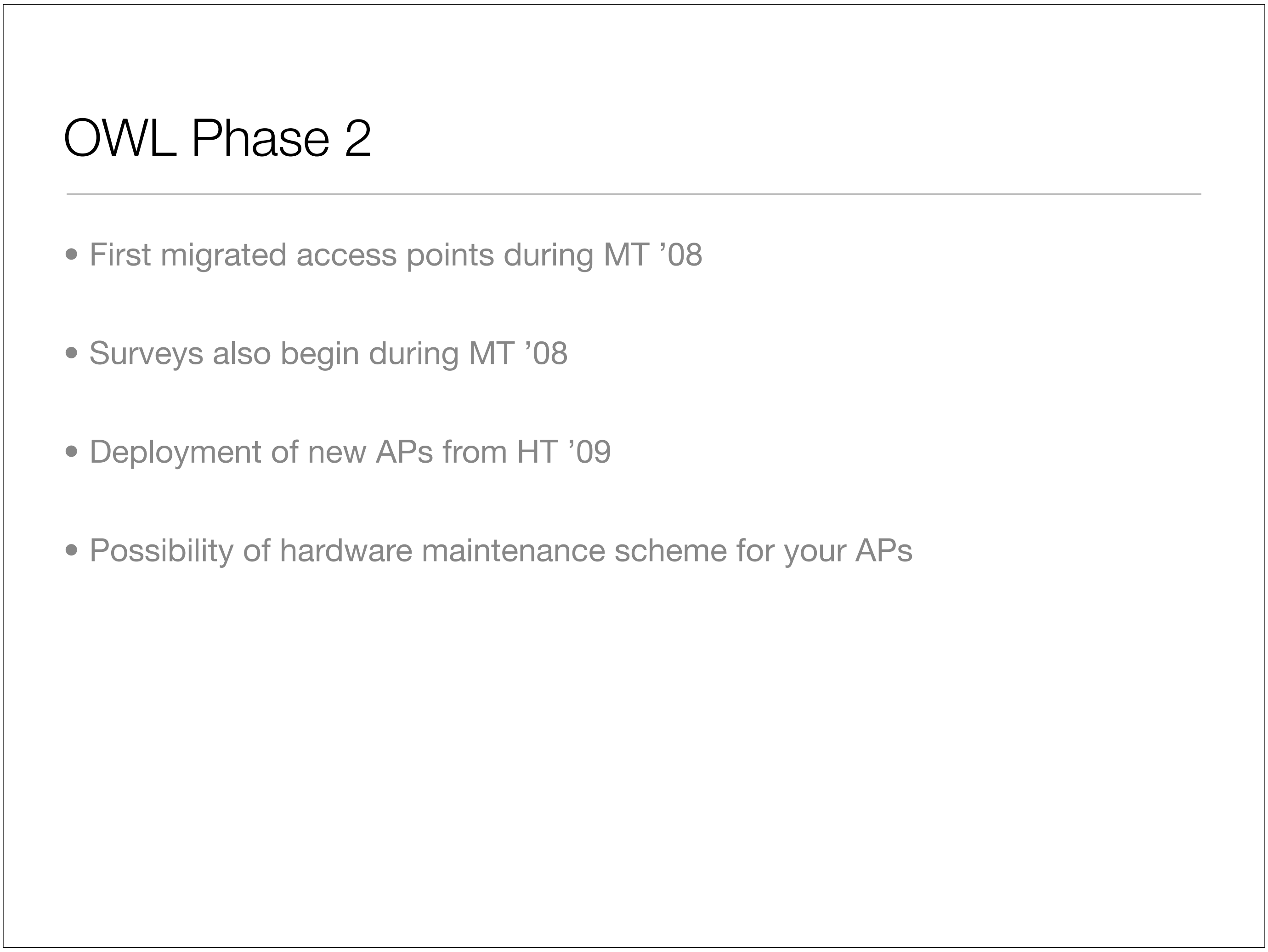
To expand a little on the local department and college Wireless Lan I mentioned before. In addition to centrally provisioned wireless services like OWL and Eduroam we expect to be able to provision additional services on a per-access point basis. Within the system we think it will be feasible to provide each department or college with one wireless network which can be piped back to a port on their main site FroDo switch.

One final thing which some has been asking about is whether there will be a service for commercial purposes separate to the Visitor Network which uses our JANET connection. We are looking into this in OUCS, and it will be asked about in the questionnaire so if you are interested in this please have a think about it and be prepared when the questionnaire comes.



Future Network Developments

The last few slides now will cover the projects we'll be working on over the next year.



OWL Phase 2

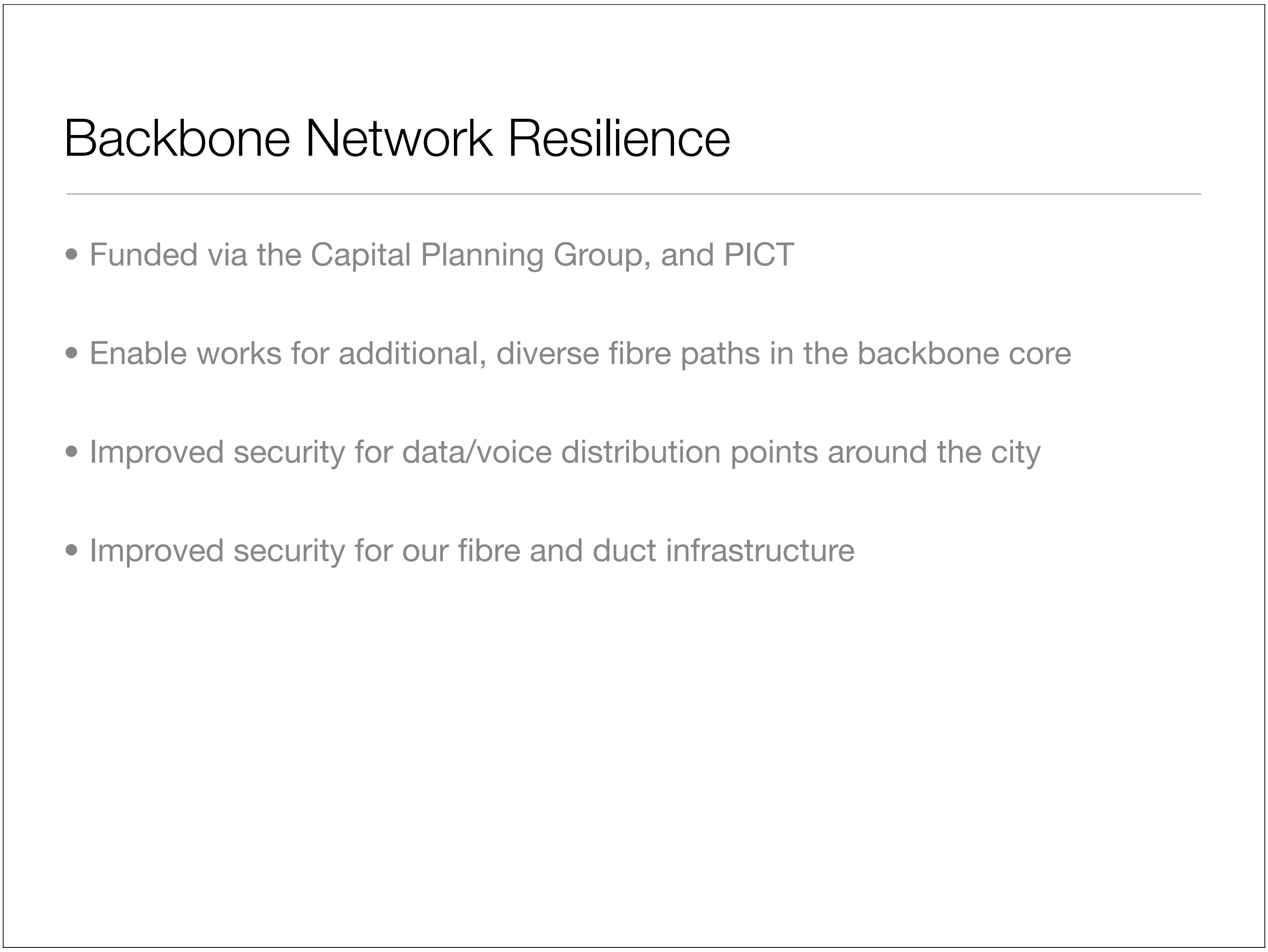
- First migrated access points during MT ’08
- Surveys also begin during MT ’08
- Deployment of new APs from HT ’09
- Possibility of hardware maintenance scheme for your APs

Of course OWL Phase 2 will be a major part of our work, and here are some reference points.

This coming term we hope to have the central management appliances installed, and can begin migrating any existing Cisco access points which you wish to have managed by us. We’ll also be surveying the list of sites nominated by the Divisions to assess how many access points will be required and where they will go, and so on.

We expect to begin field installations of new access points from the start of the next calendar year.

Another thing to be considered is whether to operate a hardware maintenance scheme much like the existing Network Control 3Com hardware support system. Again this will be in the questionnaire so please consider whether you want this.



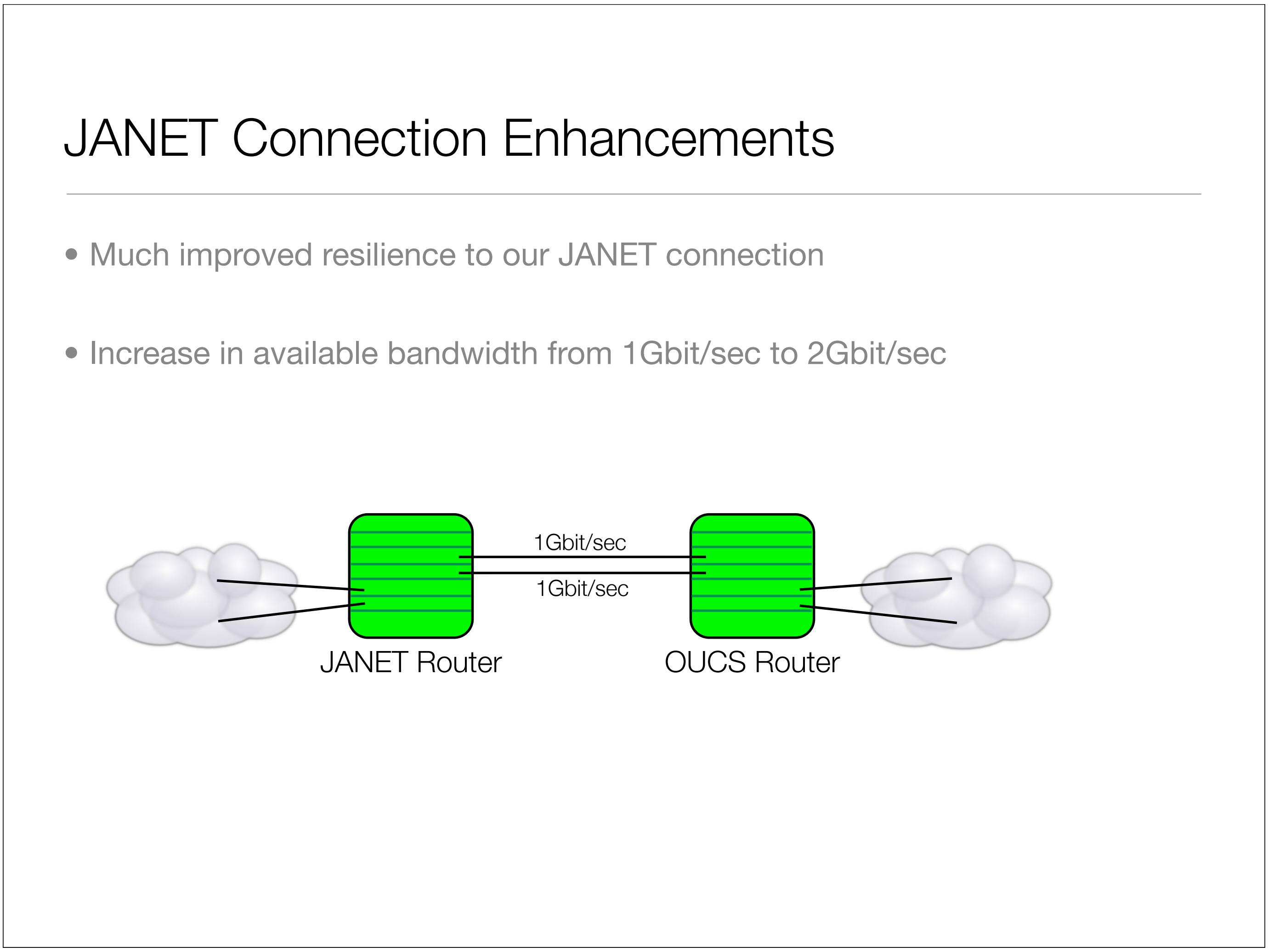
Backbone Network Resilience

- Funded via the Capital Planning Group, and PICT
- Enable works for additional, diverse fibre paths in the backbone core
- Improved security for data/voice distribution points around the city
- Improved security for our fibre and duct infrastructure

This is another project which has been funded through the same process as OWL Phase 2, via the University Capital Planning Group.

OUCS and the Internal Auditors identified that the backbone network required some capital investment over the next few years to improve its resilience and security.

The funding will enable additional resilience in the core of the backbone network. It will also allow us to improve the physical security of our data and voice distribution points around the city, and also the physical security of our fibre and duct infrastructure.



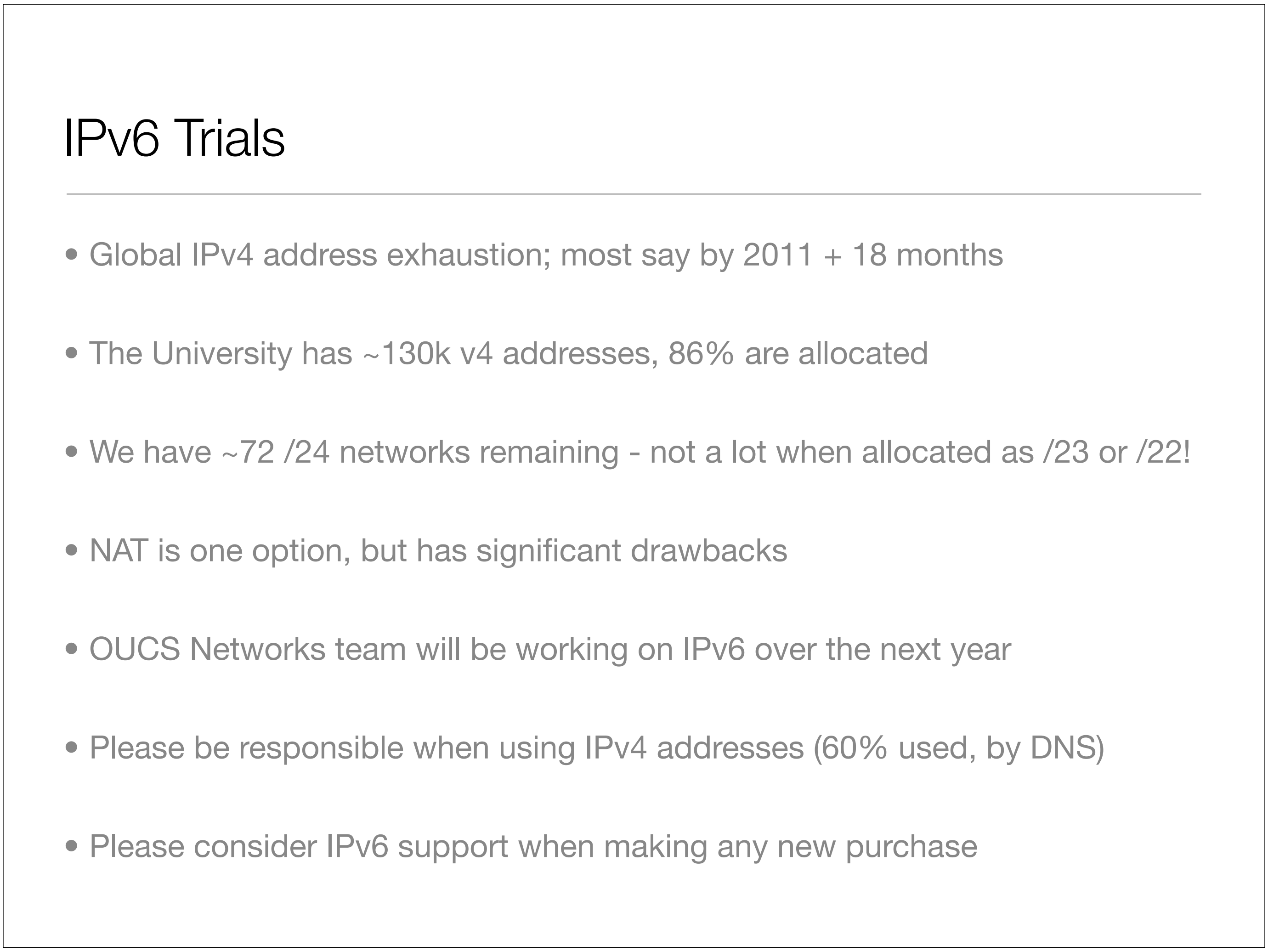
JANET Connection Enhancements

- Much improved resilience to our JANET connection
- Increase in available bandwidth from 1Gbit/sec to 2Gbit/sec

In a separate project I've worked with JANET-UK to improve the state of our connection to the Internet, with one of the key benefits being an increase in the available bandwidth.

As you can see from this diagram the old situation had a number of single points of failure, where if one line card in a router on either side failed we could suffer loss of connectivity.

Following improvements on both sides we now have much better redundancy and also an increase in available bandwidth so long as both links are running.



IPv6 Trials

- Global IPv4 address exhaustion; most say by 2011 + 18 months
- The University has ~130k v4 addresses, 86% are allocated
- We have ~72 /24 networks remaining - not a lot when allocated as /23 or /22!
- NAT is one option, but has significant drawbacks
- OUCS Networks team will be working on IPv6 over the next year
- Please be responsible when using IPv4 addresses (60% used, by DNS)
- Please consider IPv6 support when making any new purchase

Finally, I'd like to let you know that we are working on IPv6 deployment for the University, although this is really just a heads-up to you.

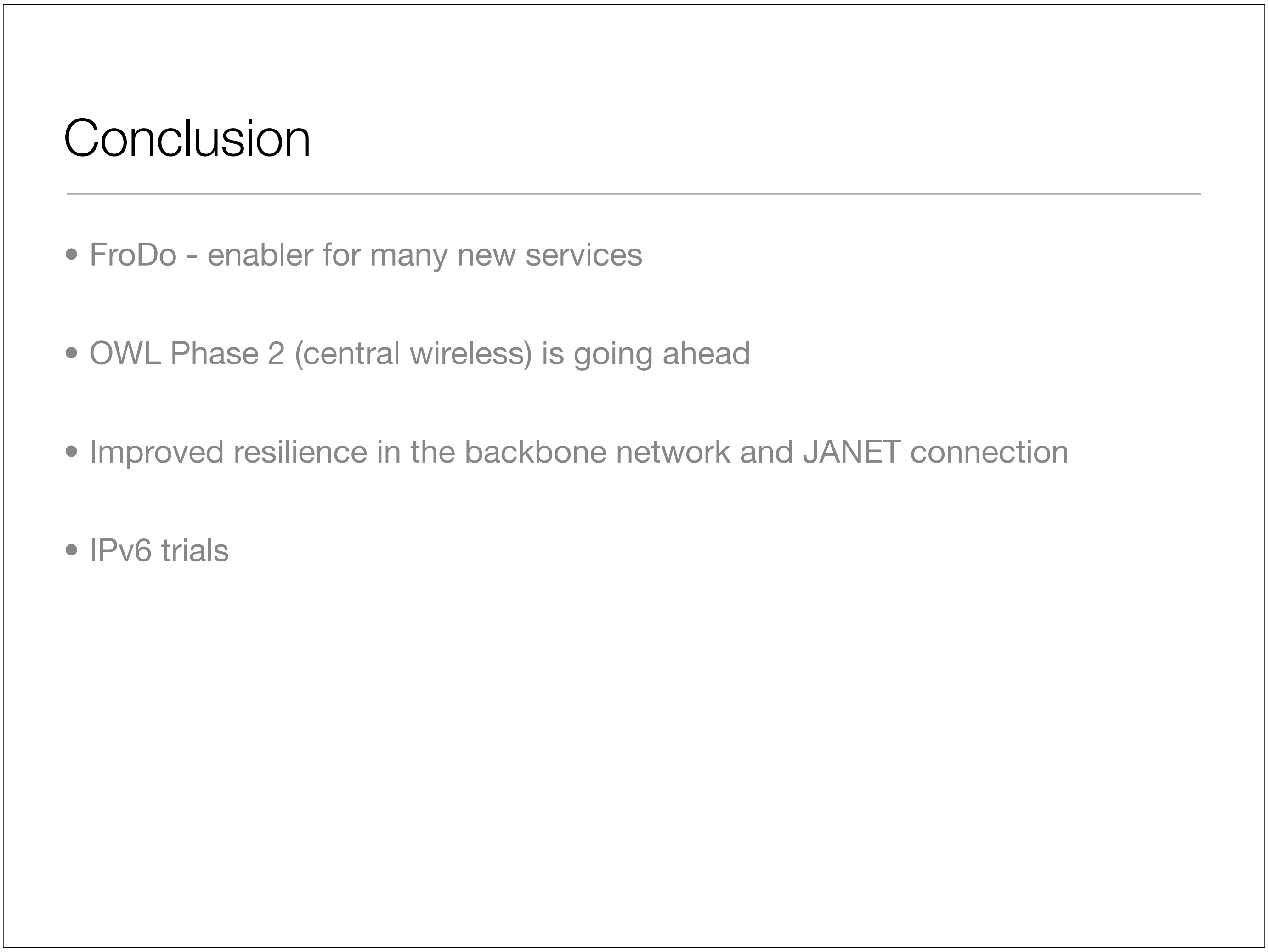
The most quoted statistic is that there'll be no more IPv4 addresses allocated after some time in 2013. It's unlikely the University would ever get allocated more IP addresses anyway, but this is still and interesting statistic as we reflect this, having already allocated 86 per cent of our space.

That leaves us with 72 class C networks, which will not last long as hostmaster receives around one request every few weeks, usually for something larger than a / 24.

It's desirable to avoid NAT, but of course sometimes it is unavoidable. So as I say we'll be testing systems on IPv6 connections over the next year.

We ask that you be responsible with your IPv4 usage, as by our reckoning only 60 per cent of that 86 per cent is in use, if you have all adhered to policy and registered all used systems in the DNS.

Also you'd do well to consider IPv6 support when making any purchase in the future.



Conclusion

- FroDo - enabler for many new services
- OWL Phase 2 (central wireless) is going ahead
- Improved resilience in the backbone network and JANET connection
- IPv6 trials

So in conclusion we’re please that so many of you are making best use of the FroDo switches at your site, and I’ve shown you some more features which are now available.

OWL Phase 2 is on its way. The University is funding improvements to the resilience of our network, and my team is looking into what to do after we run out of IPv4 addresses.

Questions and Answers