Installing a Wireless Network for University Members

Oliver Gorwits, Roger Treweek
Oxford University Computing Services
<wireless@oucs.ox.ac.uk>

Since Last Year…

- OUCS pilot completed
- A better idea of service requirements
  - Members and Visitors
- A better idea of user requirements
  - Public or Shared spaces
- Six co-operative deployments of OWL-VPN
- Tracking new vendors and initiatives (LIN)

Technology and Issues

Why Wireless?

- There are some obvious locations
  - Lecture rooms
  - Libraries, Study areas
  - Hard-to-wire areas
- Or for specific reasons
  - Conferences
  - Meetings
  - Mobility

Wireless Problems

- Security – products are not secure enough
- Privacy – snooping passwords, data
- 'Hub' style operation – anyone can see all traffic
- Hacker tools readily available
- Performance
- Propagation / Attenuation

Wireless Technology

- 802.11b
  - 2.4GHz, 11Mbps – basic common standard
- 802.11g
  - 2.4GHz, 54Mbps – popular but not without flaws
- 802.11a
  - 5GHz, 54Mbps – ideal, but not yet common

Site Survey

- Site survey is still recommended
- Use same make/model as it is intended to deploy
- Consider main coverage areas
- Number of access points and location
- Interference issues
  - Channel settings
  - Power settings

Security

Three areas to consider:

- Authorized users only
- Encrypted transmissions
- Accountability of usage

A Service for University Members

Cisco VPN

- 3000 series “concentrator”
- Redundant hardware
- >1000 concurrent users, 100 Mbit/s
- Special VPN IP address pool
- Client program for users, multi platform

VPN-assisted Wireless

Satisfies our requirements:

- Authorization:
  - Remote Access accounts
- Encrypted transmissions
- Accounting: RADIUS and logs

Site Requirements

- Separation from the main data network

- For the clients:
  - **DHCP** – unregistered
  - **DNS lookup → VPN concentrator**
- On the network:
  - **IP filter Clients → VPN concentrator**

Wireless Settings

Option	Value
SSID (Network Name)	**OWL-VPN**
Static WEP	**Disabled**
WEP Authentication	**Open** (not Shared)
Network Type	**Infrastructure** (not Ad Hoc)
Concentrator IP	**192.76.27.246**
VPN IP Filters	**UDP 500, 1500 both directions**

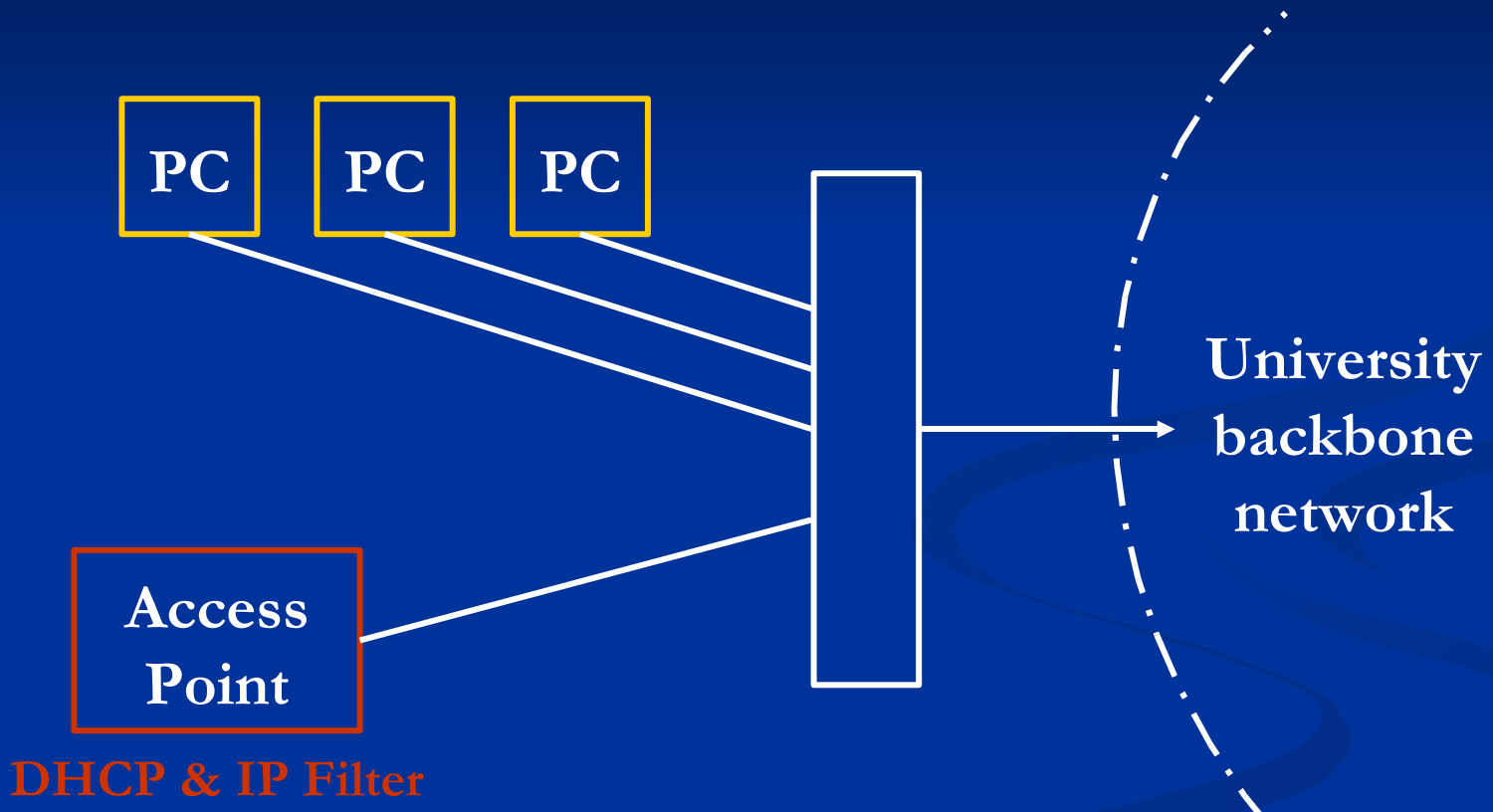
Access Points

- Cisco 1200 series AP
  - Combined 802.11b/g with 802.11a add-on module
  - IP Filters, DHCP server
  - Power over Ethernet (injector)
  - ~330GBP in 2004
- Alternatives from 3Com, etc
- Or use an integrated solution (Trapeze…)

Use Case 1

- Little additional equipment
  - Access Point and Power Injector
- No NAT
  - Small IP pool from unit for DHCP
- Simple configuration
  - Web Tool for Cisco 1200AP admin

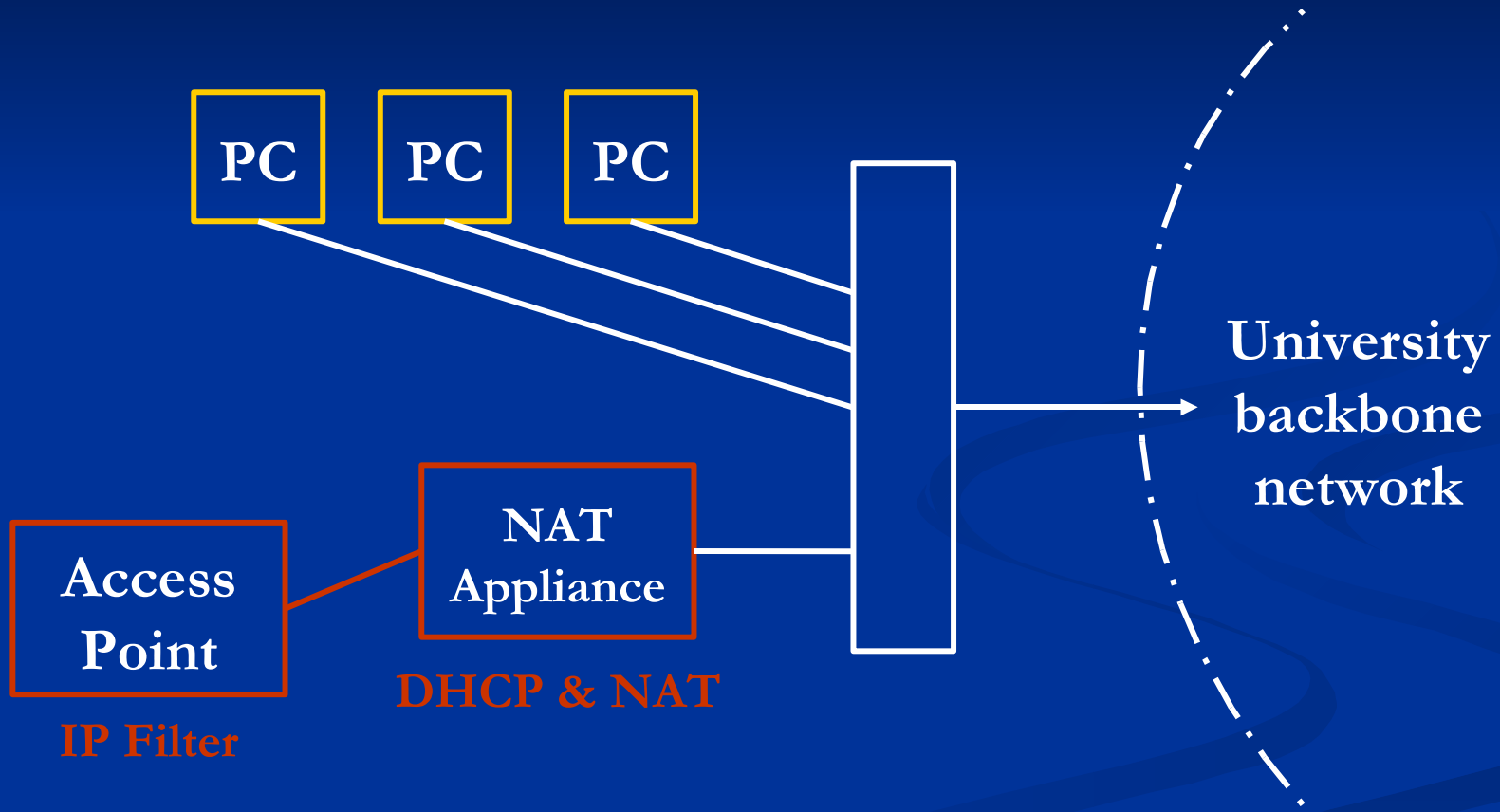
Use Case 1


PC
PC
PC
University backbone network
Access Point
DHCP & IP Filter

Use Case 2

- Less accommodating environment
  - Access Point and NAT Appliance
- NAT
  - IP filter on either appliance
- More hardware to configure
  - But mostly default configuration

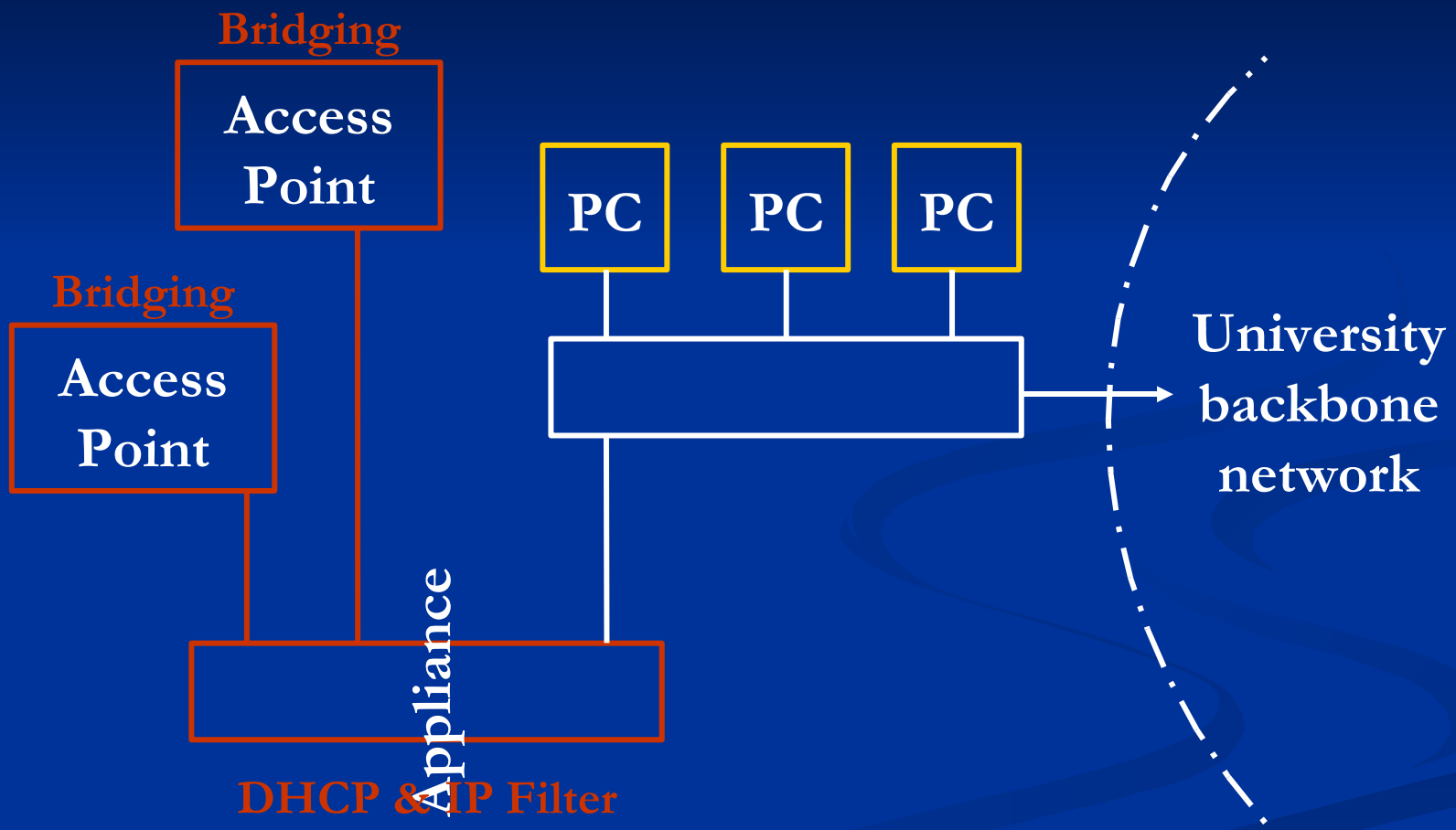
Use Case 2


PC
PC
PC
University backbone network
NAT Appliance
Access Point
DHCP & NAT
IP Filter

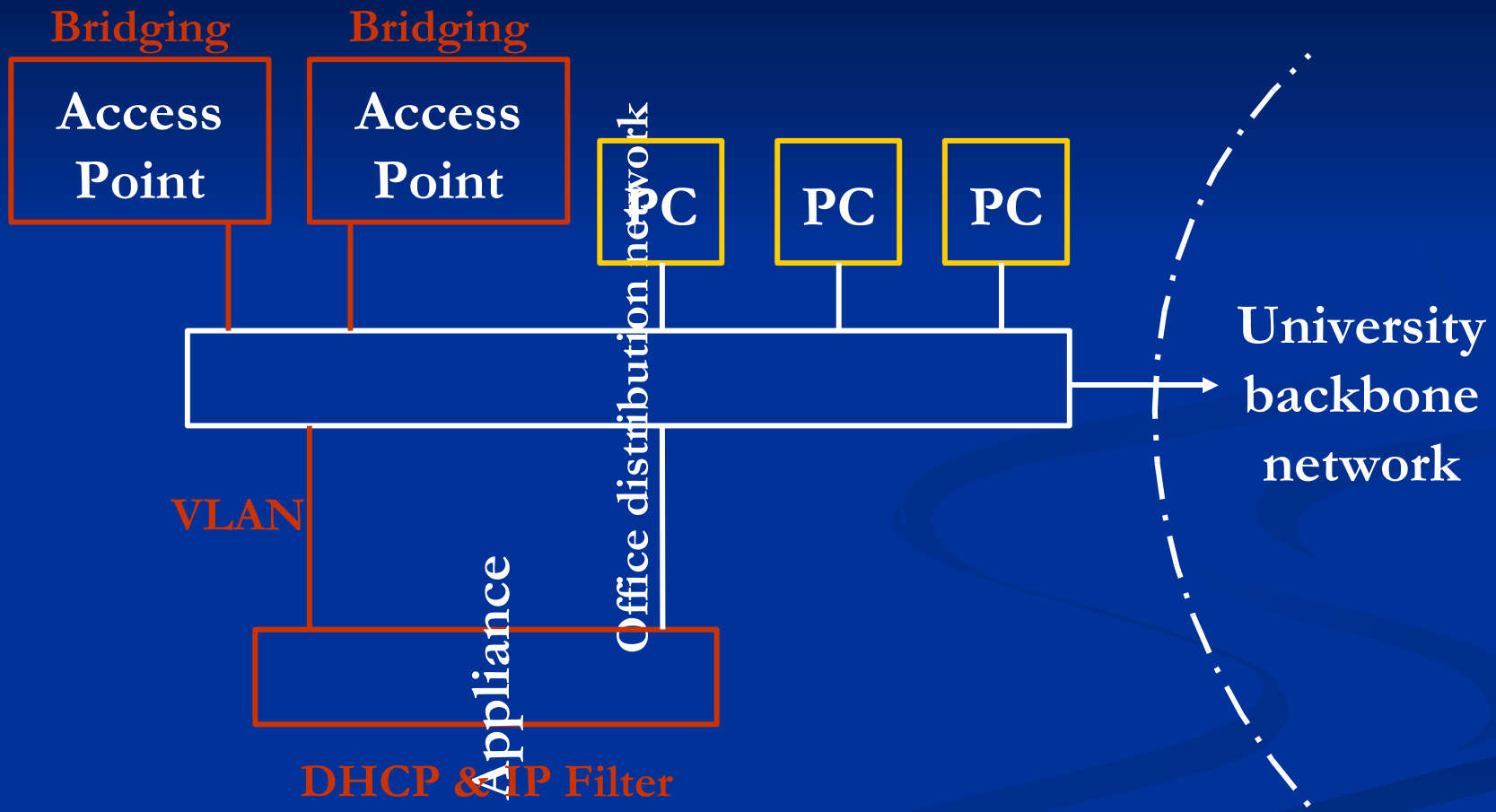
Use Case 3

- More substantial deployment
  - Fully switched network
  - Redundant cabling
  - or, VLAN-capable
- Access Points are bridging
- Single Appliance to IP Filter, DHCP, NAT
- Most flexible and future-proof

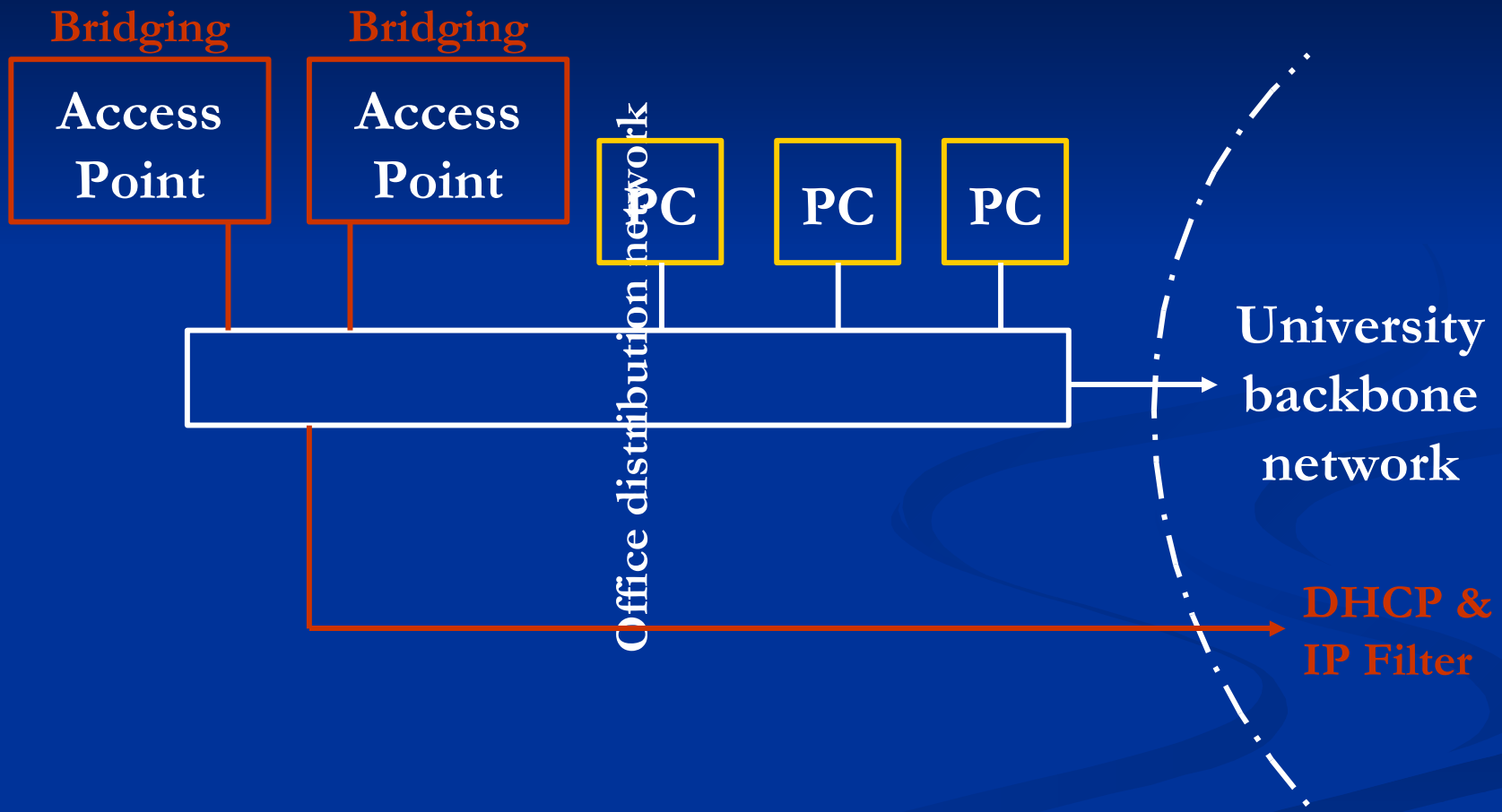
Use Case 3 - cabled



Use Case 3 - VLANs



Use Case 3


Bridging
Bridging
Access Point
Access Point
PC
PC
PC
Office distribution network
University backbone network
DHCP & IP Filter

Alternatives

- Bluesocket
  - Wireless / Wired “Captive Portal” appliances
  - Available from BTSkynet Systems
- Trapeze and Vernier
  - Full Integration solutions – edge to core
  - Available from QolCom

Networking Futures

FroDo

- A proposed upgrade to backbone connections
  - Single fibre becomes managed 24-port switch
  - UPS and Cabinet
  - One FroDo at main unit site
- Multiple services and Quality of Service
- Already deployed in a few locations
- Around 2kGBP depending on fibre work

FroDo (2)

- Many opportunities:
  - Shared occupancy
  - Simpler annexe management
    - Single Firewall
  - Bulk transit
  - “Dirty Network”
  - Wireless handoff…

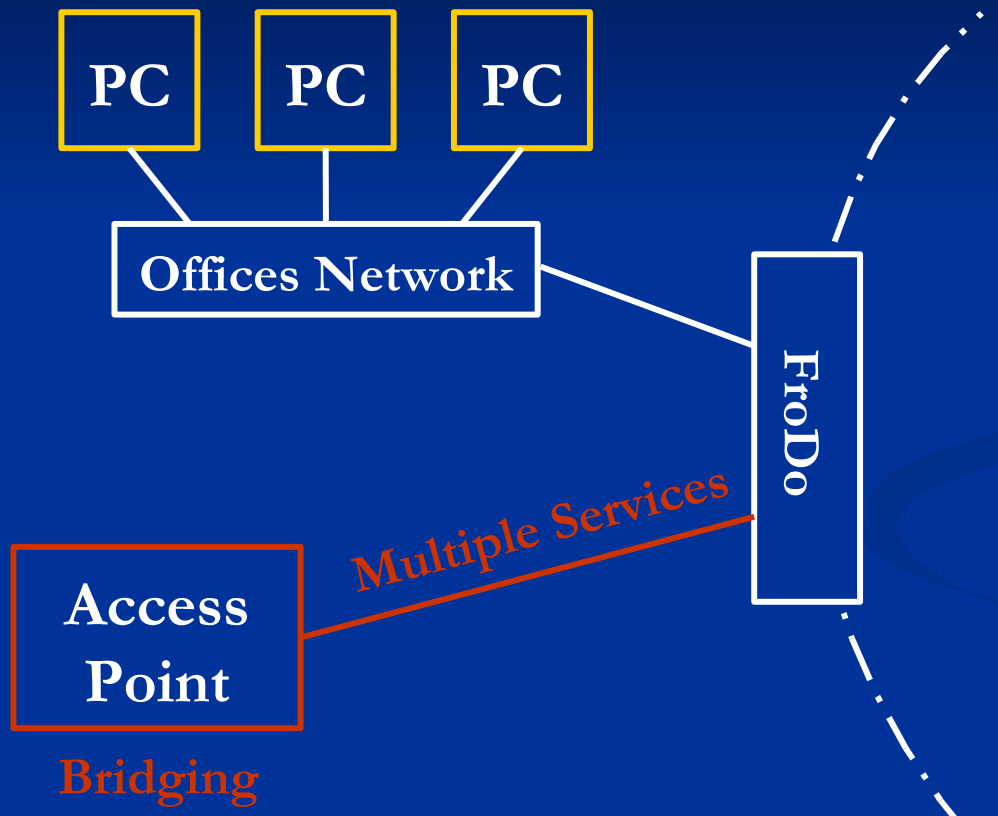
Guest Access

- Difficult to cater for
  - Various periods of attendance
  - Not University members
  - Might arrive at short notice
- Use a Gateway or “Captive Portal”
  - HTTP redirect to HTTPS login page
  - Successful login opens an IP Filter
  - Allow basic services, including visitor’s VPN

Deployment Requirements

- A FroDo
- Separation of your wireless network
  - Layer 1 : separate cabling
  - Layer 2 : VLANs
- Access Points that support multiple services
  - MBSSID
  - VLANs

Guest Access



University backbone network

Account Management

- Centrally organized, devolved administration
- Running from servers in OUCS
- Webauth'd
  1) Nominated users login with Oxford Username
  2) Create accounts singly or in bulk
  3) Set an expiry
  4) Set the sponsoring user or group

User Experience

1. Connect to an open, zero-config network
2. Attempt to browse web; redirected
3. Login with credentials
4. Cookie placed in their browser
   - Rapid reauthentication
5. IP Filter opened until account expiry or disassociation

Current Status

- Sadly no FroDo box at St. Catz, **yet**
- Will be running for a 200 delegate conference here in September 2005
- Login and network parts are complete
- Account Management nearing completion
- Still evaluating commercial alternatives
  - No suitable candidate so far

Q & A