Providing secure open-access networks

Oliver Gorwits

Oxford University Computing Services

Workshop Outline

- Review of the Problem Domain
- Designing secure open-access networks
    - Incl. software and hardware choices
- Implementing secure open-access networks
    - OUCS and Libraries
- Q & A

Problem Domain

- Summer 2003 : large-scale Internet worms
- Widespread laptop use
- Catch-22 for software updates
- Network security ⇔ University business

Statutes and Regulations

- ICTC Regulations
  - Monitoring (4)
  - Viruses (7.11)
  - Resources (13.2, 13.3)
- JANET Acceptable Use Policy
  - Non-member use

Designing the Network

Use Cases (1)

- Vital!
- Humans - Who
- Applications - What
- Computers - How
- Locations – Where & When

Use Cases (2)

- OUCS Helpcentre
  - MS, Antivirus updates
- Building visitors
  - Lectures, Conferences
- Larger scale non-full-member
  - Library Readers – odd services

Network Integration (1)

- Cabling and Switch-gear
  - Mix-in with existing infrastructure
  - New or refurbished facility
- Labelling and Identification
  - Distribution cables
  - Port faceplates

Network Integration (2)

- IP space
  - Address and port translation
- Hardware Configuration
  - Backup management
  - Avoid the replacement-exposure problem

Managing Users

- Controlled access
  - Physical, to the building
  - Virtual, to the network
- Accounting
  - Open-access means unknown user?
- Supervision

Network Access

- Firewall rules
  - Refer to the Use Case
- OUCS – restricted
  - Official service servers only
  - Transparent HTTP redirect
  - Default deny in both directions

Basic Topologies

- VLANs
  - Vendor support
- NAT
  - Software or Appliance
- DHCP
  - Client support (MacOS pre-X)

Hardware

- Off the shelf appliances
  - Cisco PIX – DHCP & NAT
- Open Source
  - Linux/*BSD with daemons
- Black box solutions
  - Bluesocket – Web interface

Software

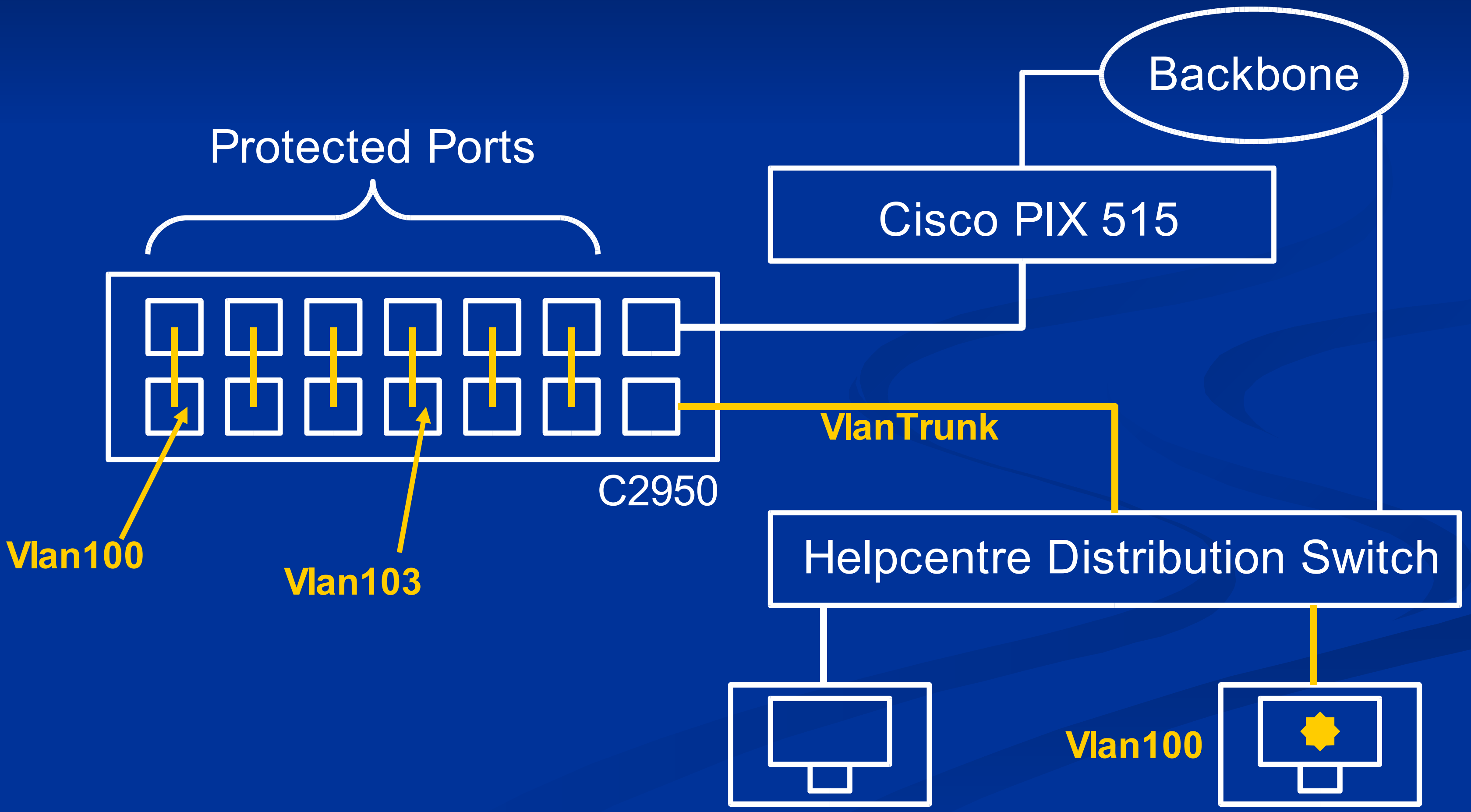
- Packet Filtering
  - iptables / ipfw
- Scanning
  - Commercial
    - Various - see Google
  - Non-commercial
    - nmap, nessus

Implementing the Network

OUCS Visitors Network (1)

- Mix-in with existing helpcentre network
- VLAN per user into managing devices
- Minimum ongoing maintenance
- No peer to peer communications
- Intended for MS/AV updates and teachers
- Restrictive service

OUCS Visitors Network (2)



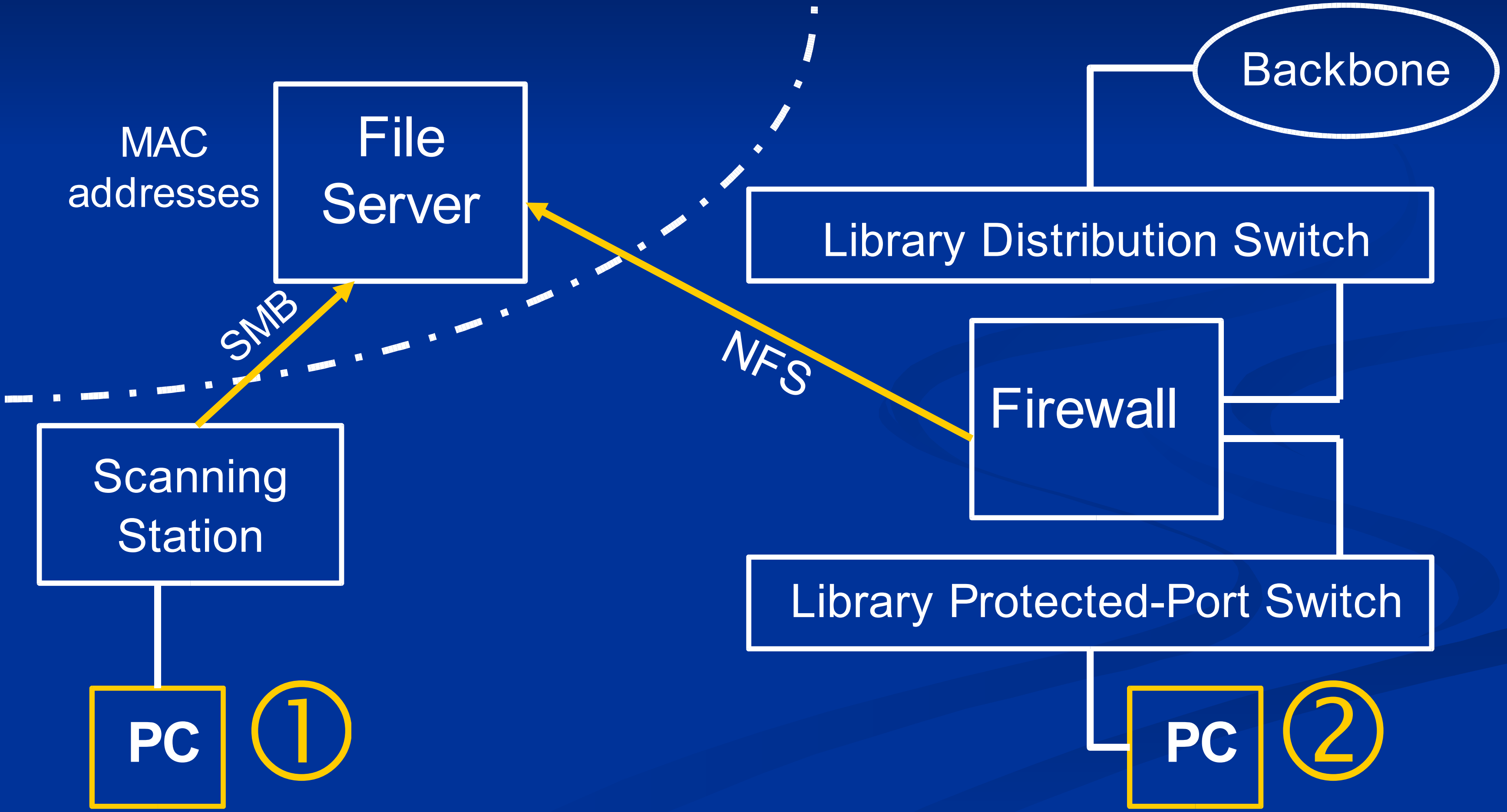
OUCS Visitors Network (3)

- Access Control List:
  - Default deny Incoming and Outgoing
  - OUCS : NTP, DNS, SMTP, HFS, NNTP, VPN
  - Also SSH, FTP, POP, IMAP to anywhere
  - OLIS on the telnet port
- Transparent HTTP redirect via OUCS proxy
- Minimal accounting; limited availability

Libraries Reader Network (1)

- Permissive service due to user requirements
  - Orthogonal to OUCS service
- Large number of (potential) users
  - Need to pre-register
- Multiple sites and networks
  - No site-local IT support

Libraries Reader Network (2)



Libraries Reader Network (3)

- Known limitations:
  - Possible post-registration infection
    - Annual registration expiry
  - Client ⇔ Scanning Station incompatibility

Q & A