



---

# The Cybercafe

## User Authentication at Layer 2

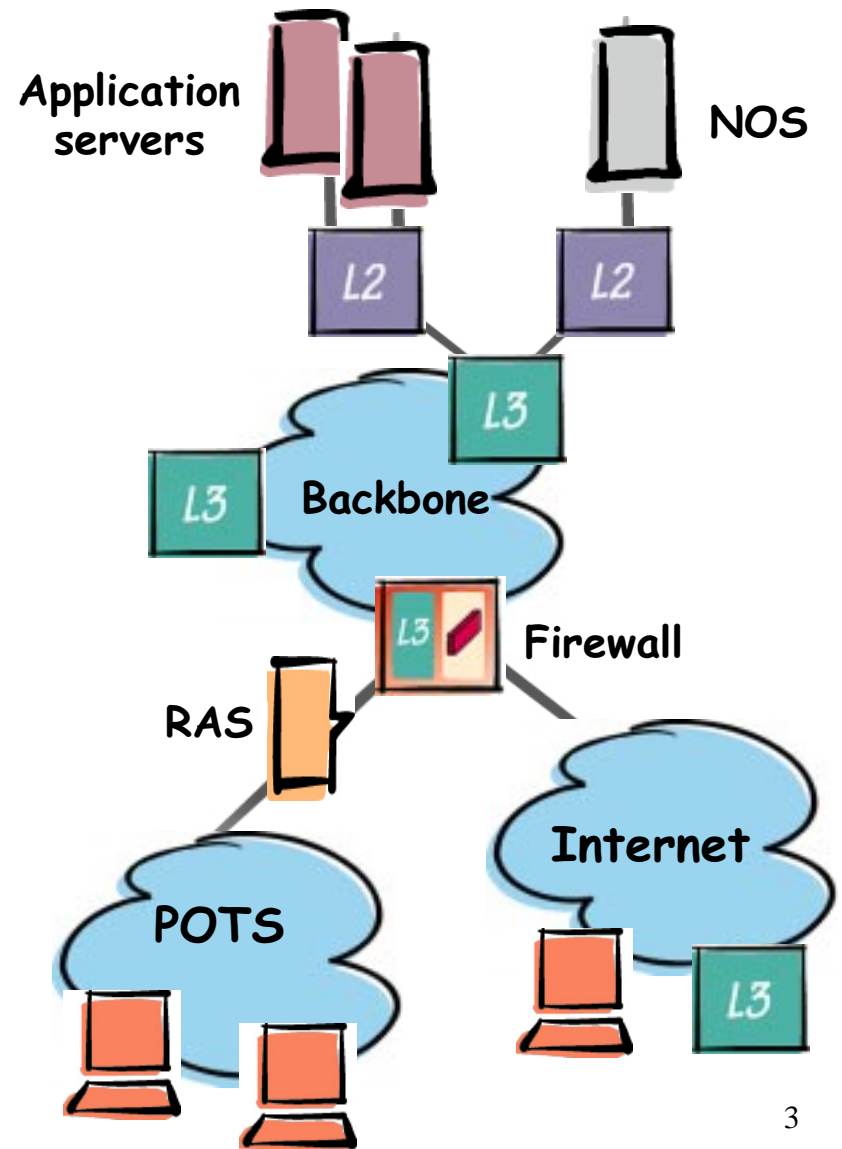
**Jeff Hayes, Product Manager**  
**[jeff.hayes@ind.alcatel.com](mailto:jeff.hayes@ind.alcatel.com)**

- ▼ User authentication
- ▼ Campus issues
- ▼ Cybercafe
- ▼ Access control
- ▼ Issues
- ▼ Cases studies



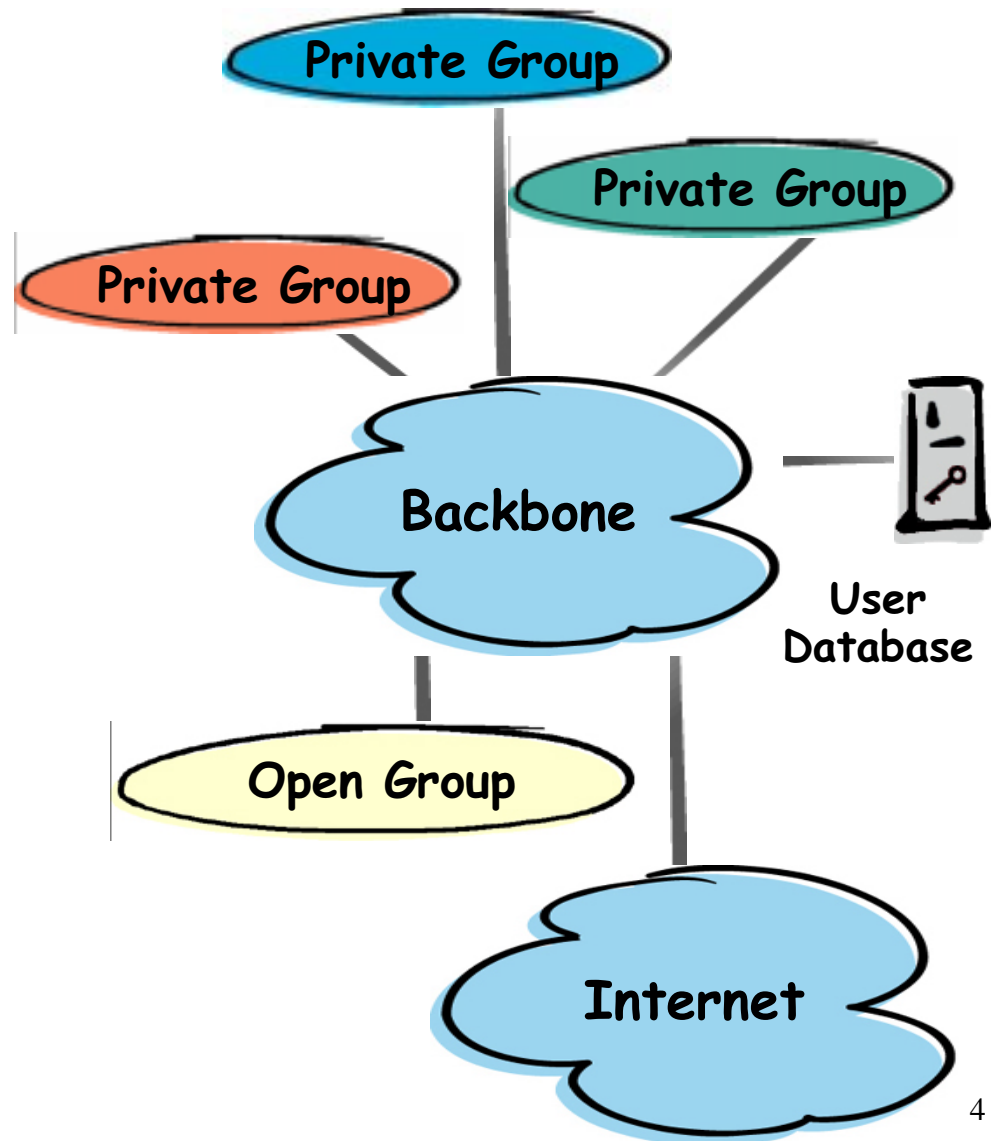
# User Authentication

- ▼ Remote Access
  - support for dial users
- ▼ Firewall authentication
  - user access from unknown IP sources
- ▼ Network Operating System authentication
  - NOS sign-on
- ▼ Application authentication
  - host and mainframe access



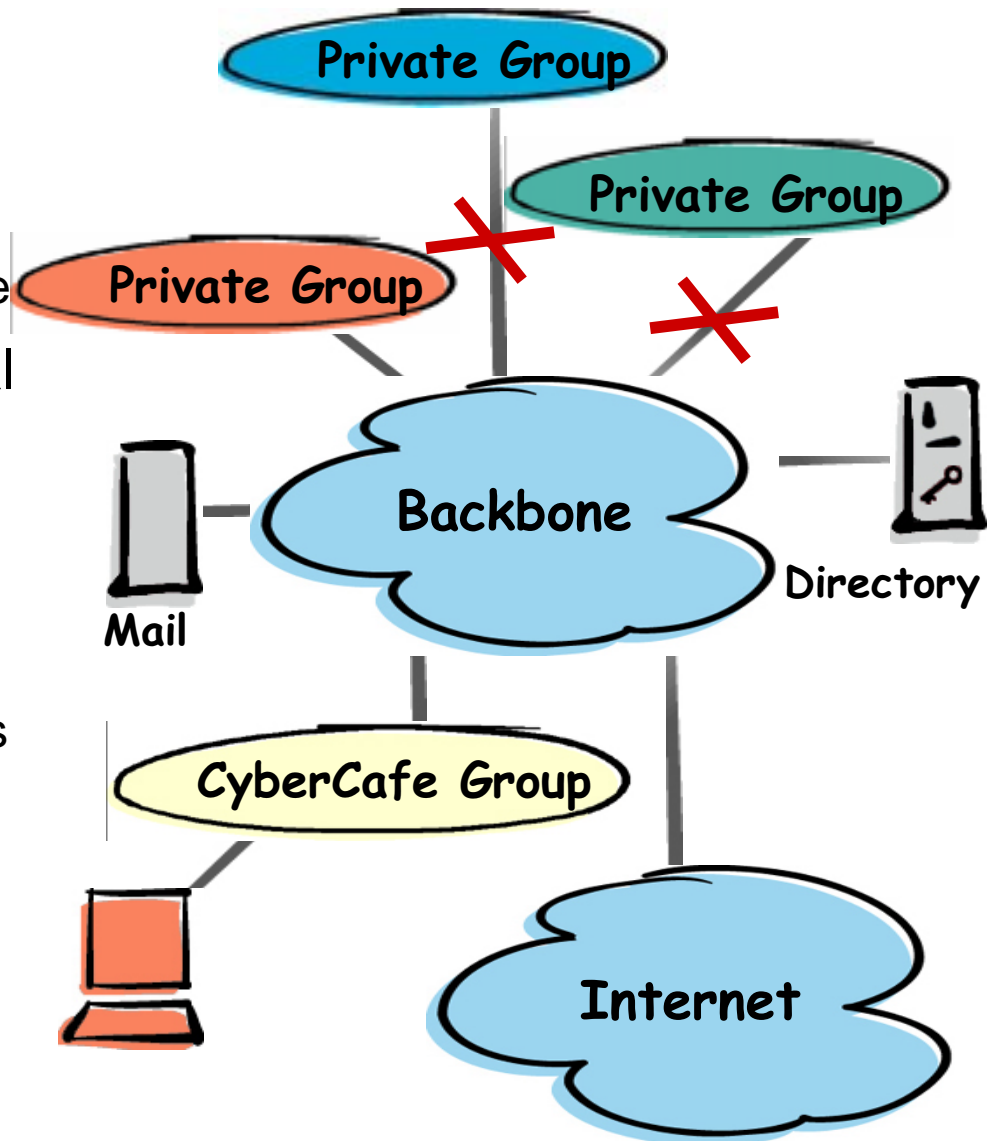
# Campus requirements

- ▼ provide open, internal communication
- ▼ provide Internet access
- ▼ provide access from anywhere on campus
- ▼ verify each user is authorized
- ▼ leverage common user database / directory



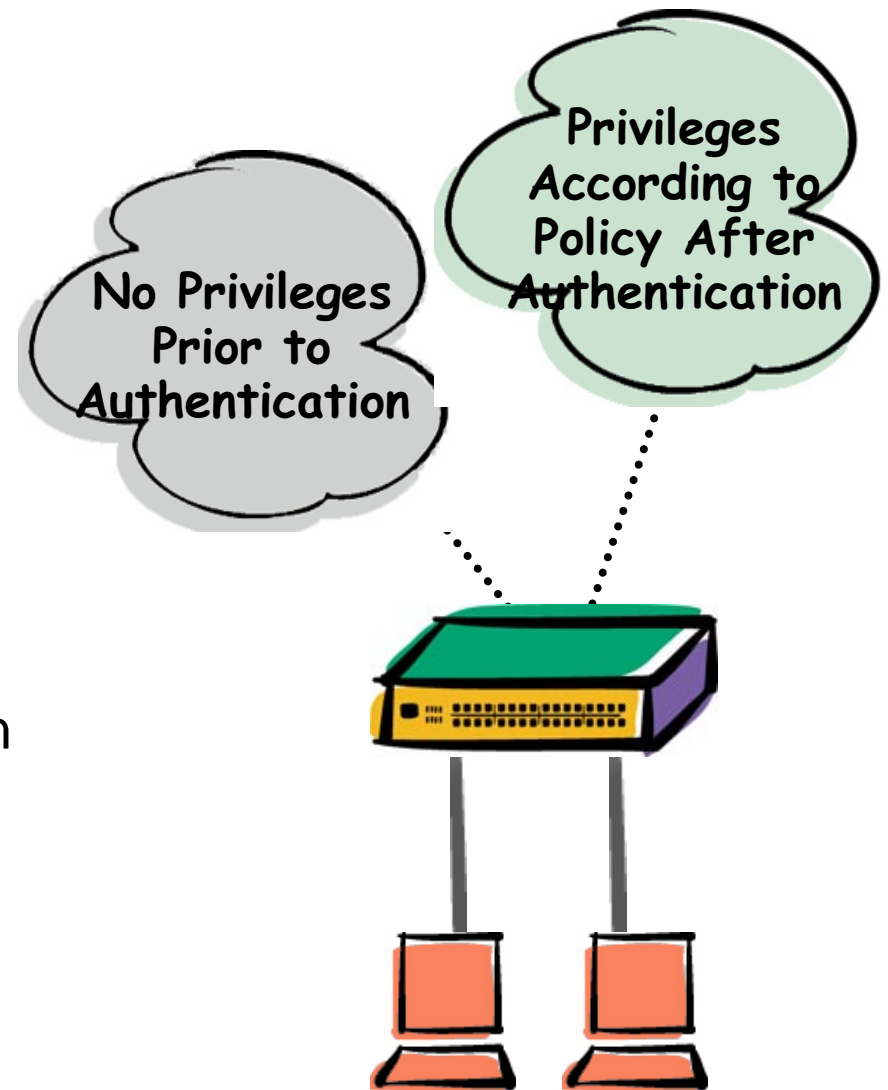
# The CyberCafe

- ▼ Perimeter security
  - Public access in a private environment
  - Access control at the edge
- ▼ Not all users created equal
  - trust all; really trust only a few
- ▼ Not all networks created equal
  - some require extra access control measures



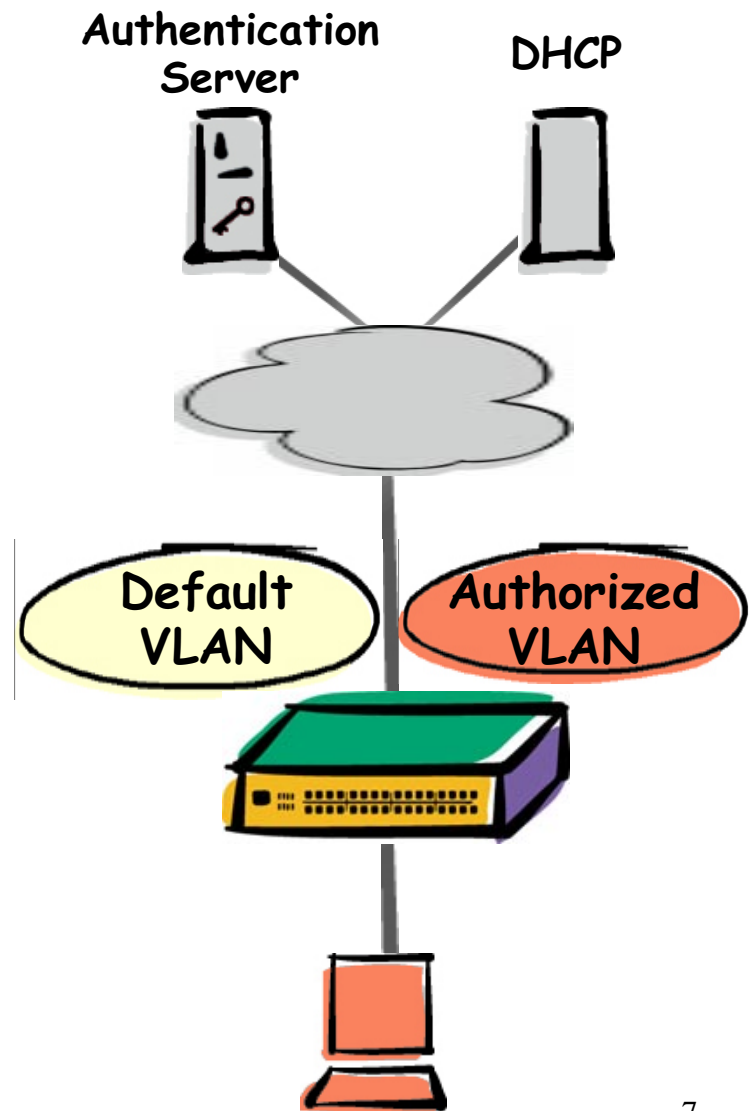
# CyberCafe - user perspective

- ▼ Sit down
- ▼ Plug into an Ethernet port
- ▼ Power on PC
- ▼ Obtain an IP address
- ▼ Activate browser
- ▼ Point at pre-configured authentication URL/address in switch
- ▼ Submit user name/password in Java applet
- ▼ Obtain authorization based on user profile
- ▼ Elapsed time = 30 seconds



# CyberCafe - the details

- ▼ Switch ports configured as authenticated ports
- ▼ These ports offer no initial privileges - default VLAN
- ▼ If dynamic address, request forwarded to DHCP server
- ▼ User login forwarded by switch to authentication server
- ▼ Auth server informs switch about user privileges
- ▼ User's MAC address virtually moved to authorized VLAN



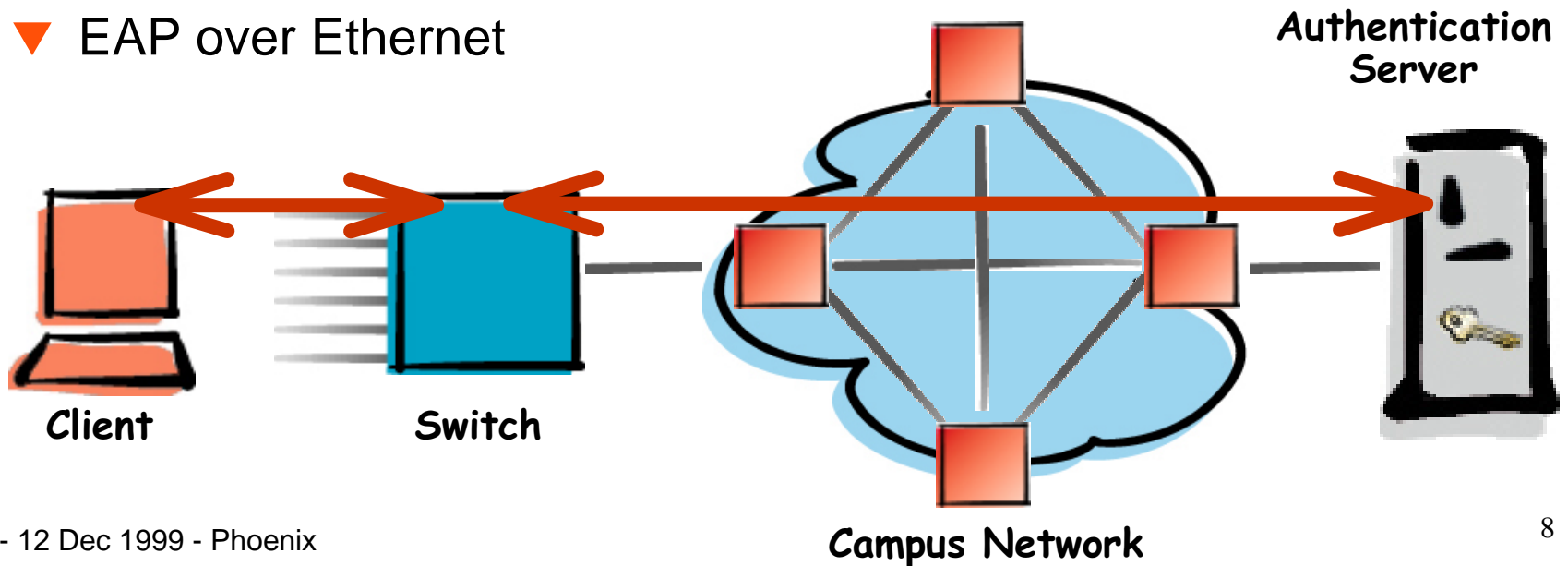
# Authentication mechanisms

## Client-to-Switch

- ▼ PC shim/executable
- ▼ TELNET
  - native
  - Browser/Java
- ▼ Secure Socket Layer (SSL)
- ▼ EAP over Ethernet

## Switch-to-Server

- ▼ RADIUS
- ▼ LDAP
- ▼ X.509 CA
- ▼ Kerberos v5



## ▼ RADIUS

- understood, deployed & affordable
- standard-based implementation that supports vendor-specific attributes

## ▼ LDAP Directory

- standardized & gaining momentum
- one directory, multiple functions
- major vendors supporting - Novell, AOL, MicroSoft

## ▼ Kerberos v5

- closest thing to SSO
- proven, in use in many environments

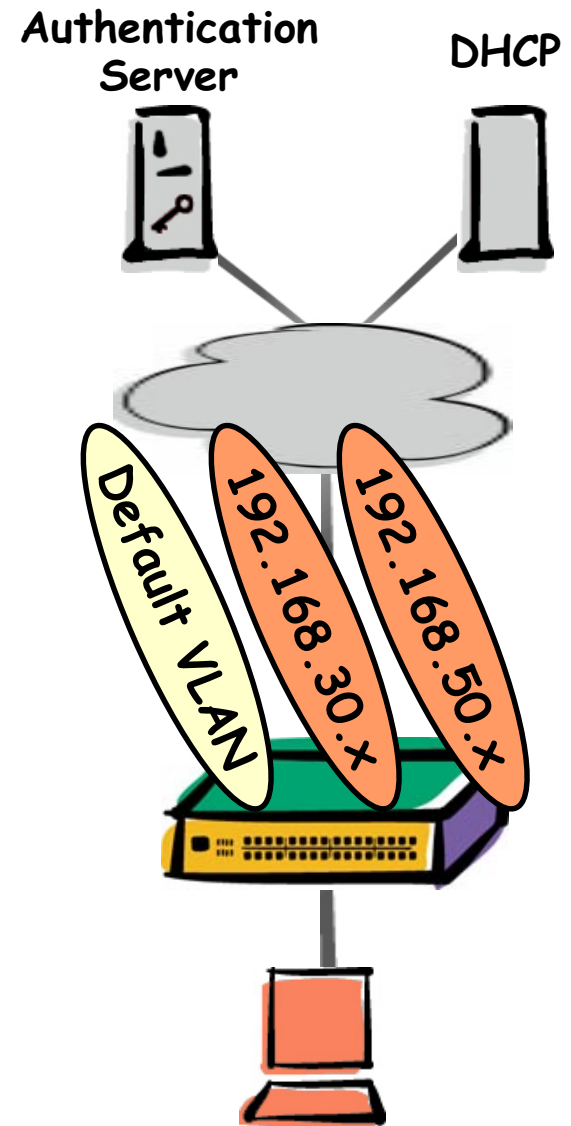
## ▼ Certificate Authority

- basis for e-commerce
- key deployments - Entrust, VeriSign, Baltimore



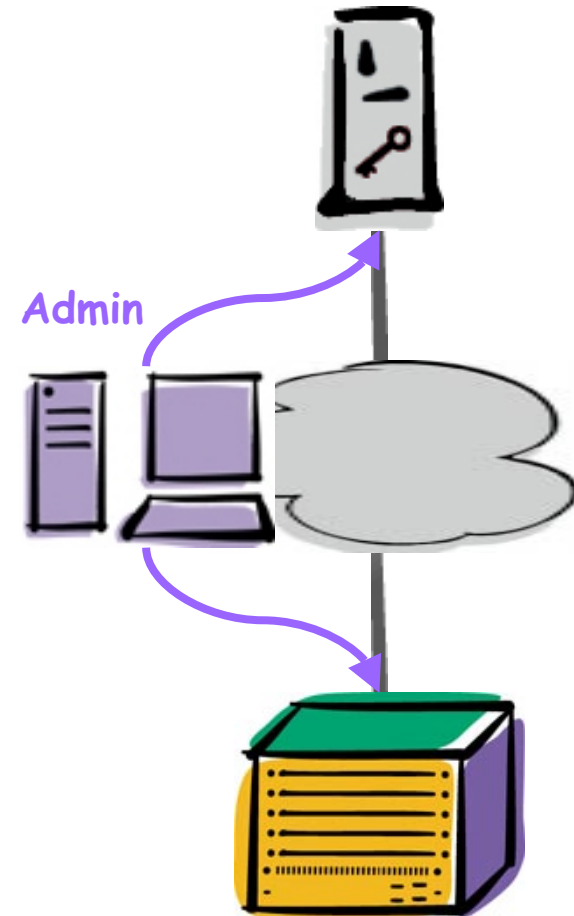
# CyberCafe Issues - DHCP

- ▼ If all users authenticated into the same group, not a problem
- ▼ If user get authenticated into different groups/subnets, there's an issue
  - Windows 95, 98 or NT do not relinquish a temp address after it expires
  - requires manual release and renew if one changes from one IP group to another
- ▼ Switch can force a release/renew when user's device moves from one group to another



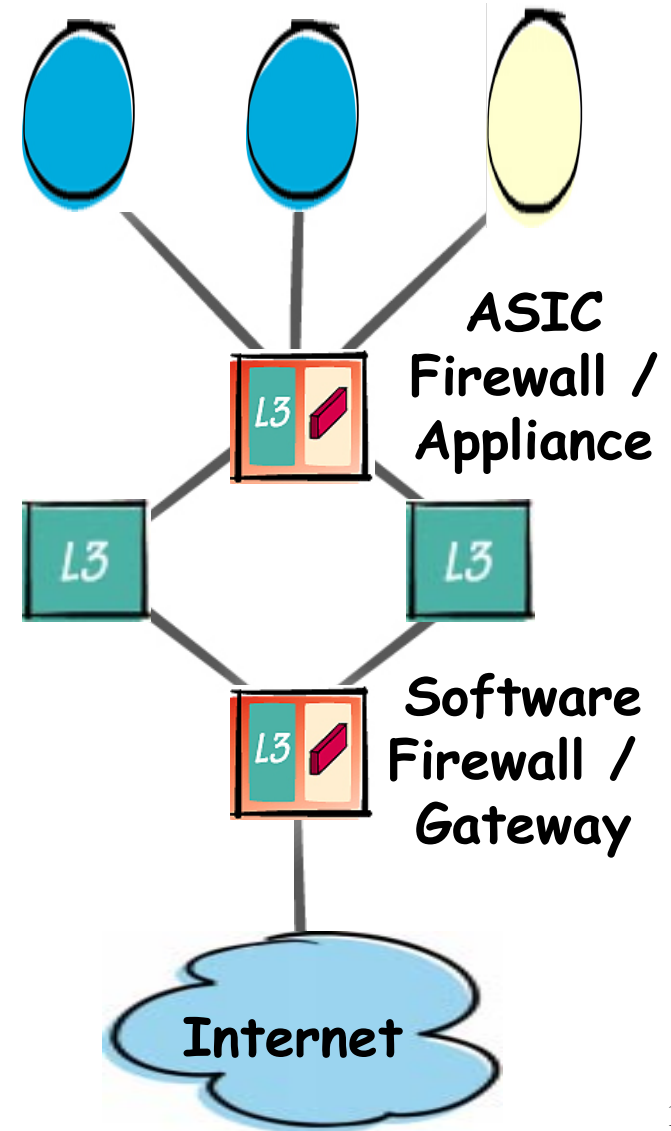
# CyberCafe - the administration

- ▼ Configure the switch
  - load correct authentication image
  - create required groups (default client and authenticated)
  - configure server related info (address, etc.)
- ▼ Configure the server
  - configure users with authentication group info (groups they can access)
  - configure switch related info (address, shared secret, skey, etc.)
  - activate accounting



# Controlling access

- ▼ Once authenticated, must isolate users
  - VLANs
  - Subnets
- ▼ Firewalls
  - software based
  - WAN oriented
  - moderate performance
  - very secure
- ▼ Access Lists
  - ASIC based
  - LAN oriented
  - wire-speed
  - moderate security



# Case Study - University

## Goal - open, secure computing

### ▼ Facilities

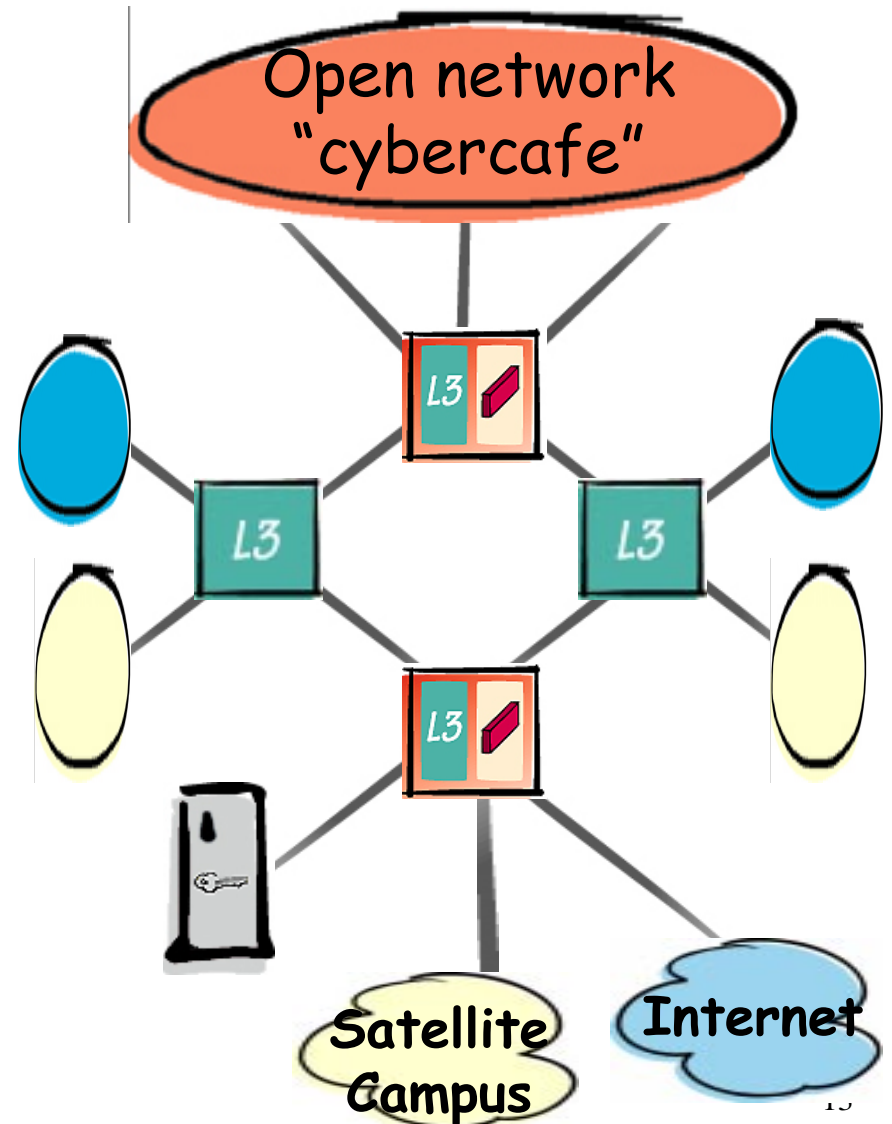
- large campus with satellites & dorms

### ▼ Users

- students - dorms, classrooms & library
- faculty - offices & classes
- admin - offices

### ▼ Policy

- DHCP & static addresses
- authenticate users
- filter between subnets

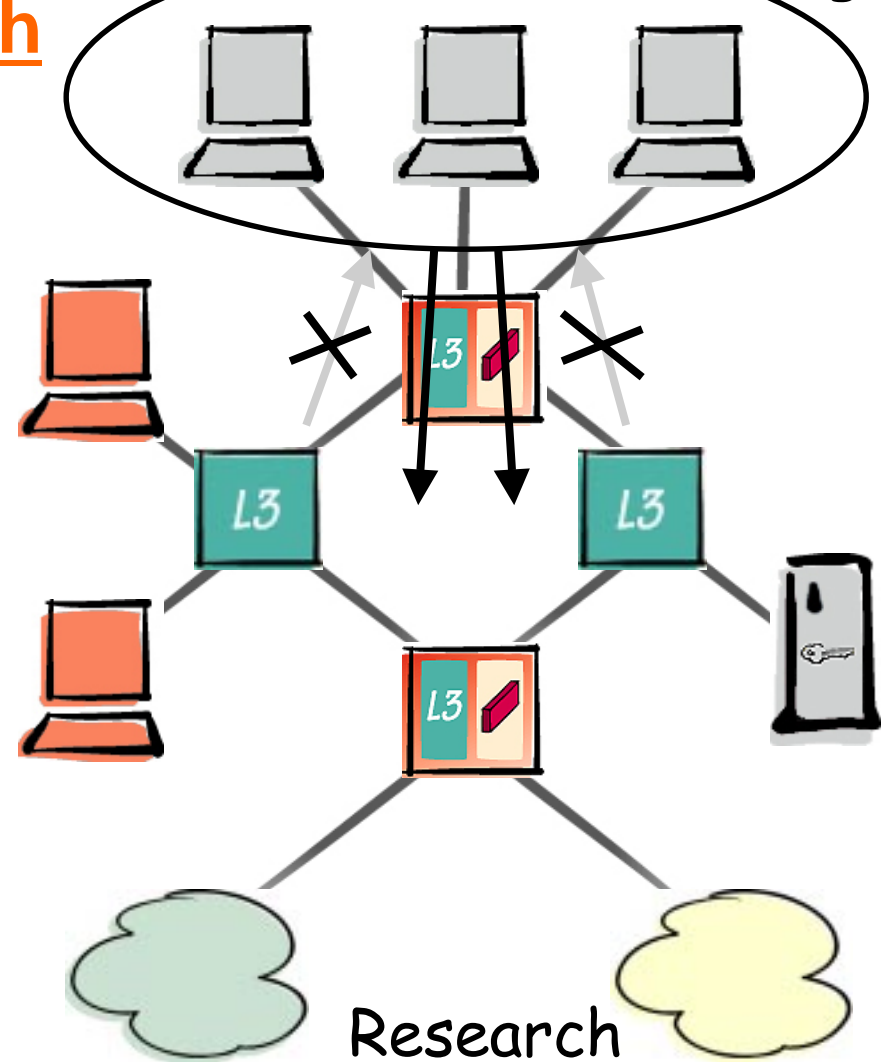


# Case Study - Medical

## Goal - patient & research confidentiality

- ▼ Facilities
  - 2500 bed hospital
  - large research labs
- ▼ Users
  - patient, research, MD, nurse, admin
- ▼ Policy
  - authenticate into key subnets
  - filter/firewall internal traffic

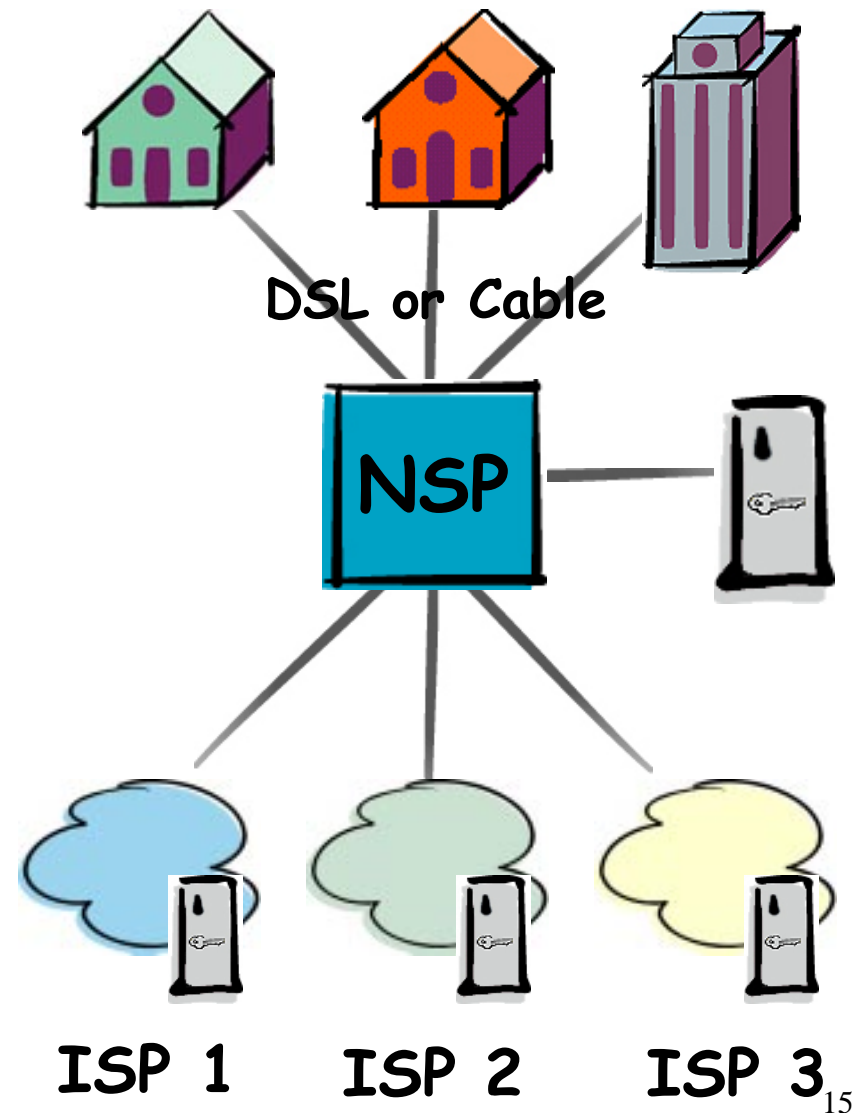
### Patient Records & Accounting



# Case Study - Carrier

## Goal - secure, multi-layer access

- ▼ Connect remote sites via high-speed LAN drop
- ▼ User informs NSP its target ISP
  - switch forwards accordingly
  - keeps usage info
- ▼ Each ISP handles its own authentication and billing



## ▼ IEEE 802.1x

- Port-based Network Access Control
- supplement to 802.1D
- draft 1 published 20 September 1999
- [ftp://p8021:-go\\_wildcats@p8021.hep.net/8021/x-drafts/d1/802-1x-d1.pdf](ftp://p8021:-go_wildcats@p8021.hep.net/8021/x-drafts/d1/802-1x-d1.pdf)
- will use EAP over Ethernet between client and switch
- authentication server can be RADIUS, LDAP, TACACS+, Kerberos, etc. -- not specified by spec

## ▼ Issues

- port based only
- easy for switch vendors to implement
- no authorizations like a layer 2 solution provides



# CyberCafe - Summary

---

- ▼ Most authentication occurs above L2
  - users' are already on the network
- ▼ Campus' needs distributed security
  - same privileges regardless of location
- ▼ Controlled, wire-speed performance
  - once authenticated at Layer 2, user operates at native wire speeds
  - firewalls control internal forwarding
- ▼ Leverages existing user databases
  - RADIUS, LDAP, CA, Kerberos
  - can be part of a single sign-on solution



---

**Thank You!**

**Questions?**