Campus Networking Best Practices

Session 5: Wireless LAN

Hervey Allen
NSRC & University of Oregon
hervey@nsrc.org

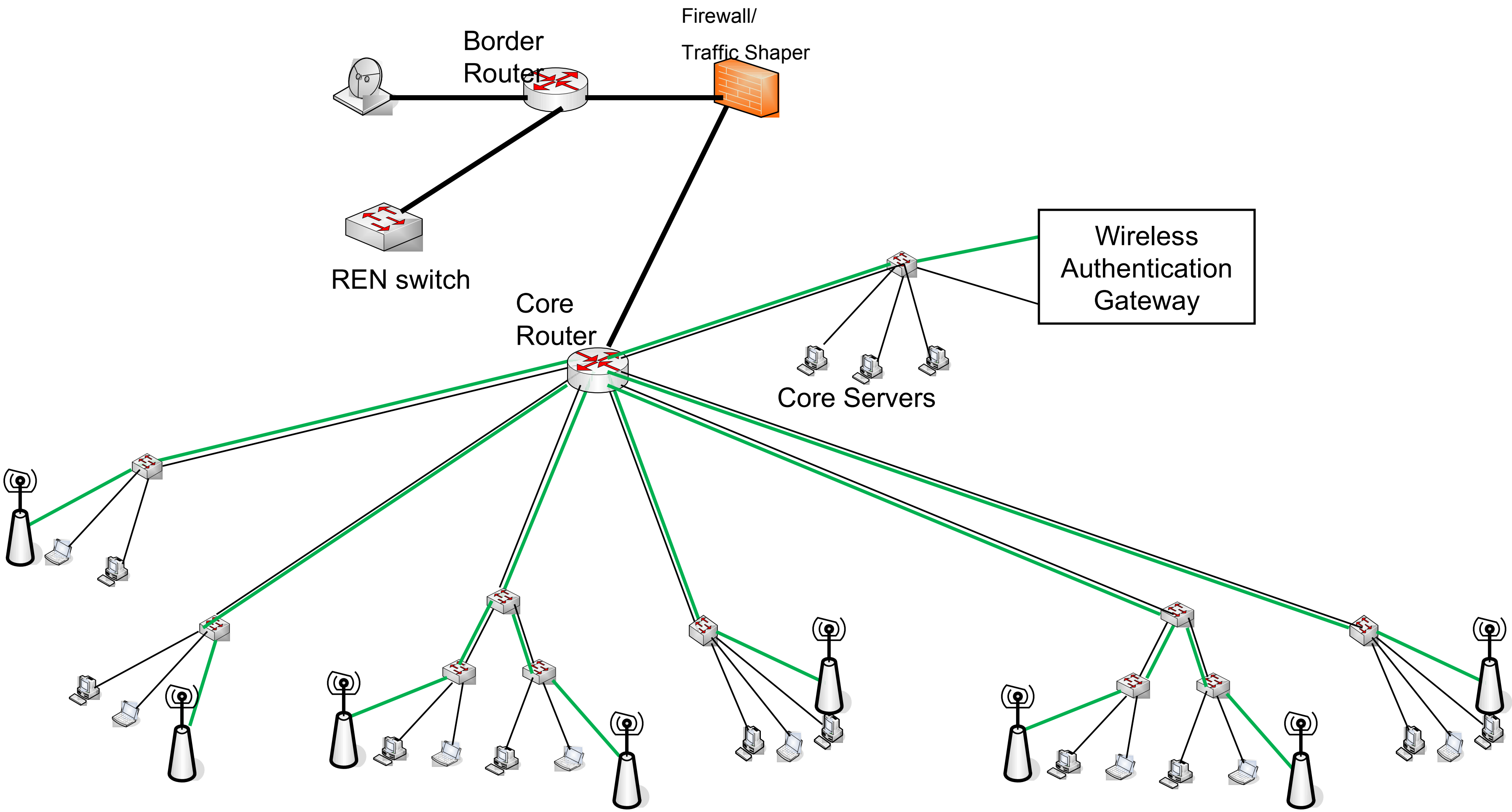
Dale Smith
University of Oregon & NSRC
dsmith@uoregon.edu

UNIVERSITY OF OREGON

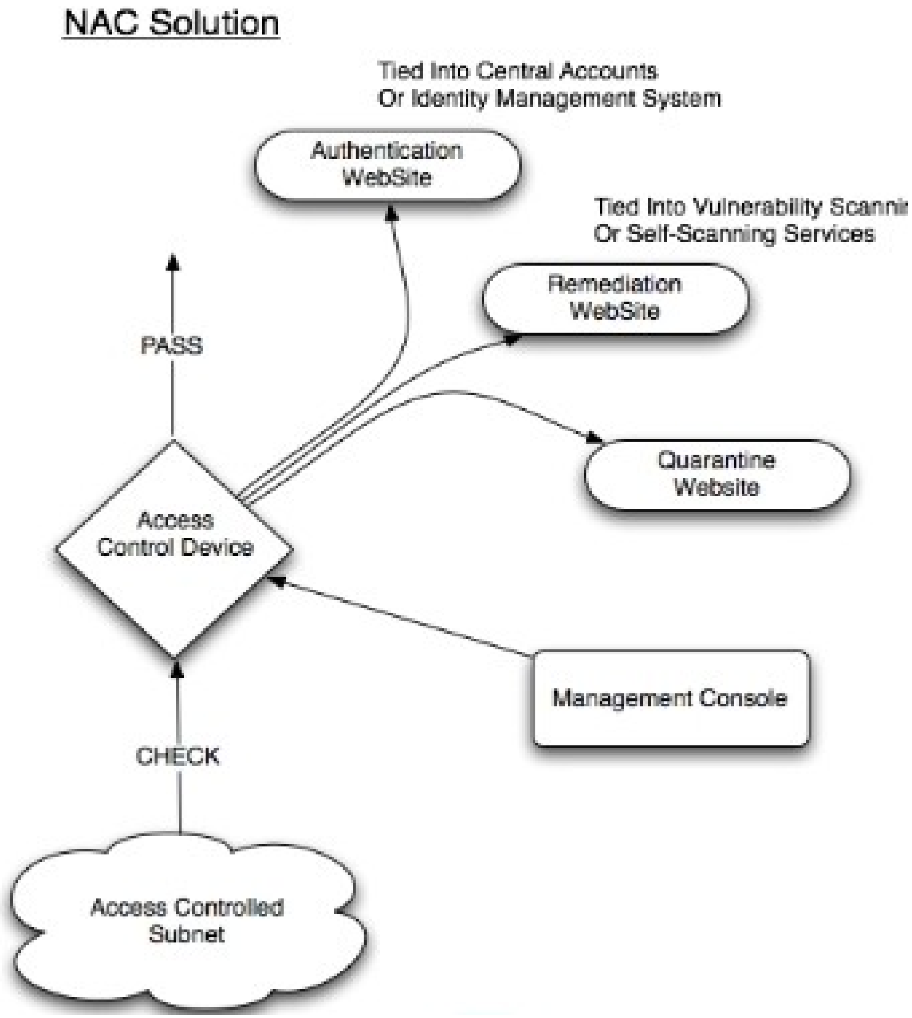
Network Startup Resource Center

Wireless LAN

- Provide wireless network across your campus that has the following characteristics:
  - Authentication – only allow your users
  - Roaming – allow users to start up in one section of your network, then move to another location
  - Runs on your campus network


Firewall/
Traffic Shaper
Border
Router
REN switch
Core
Router
Wireless
Authentication
Gateway
Core Servers

Network Access Control (NAC)



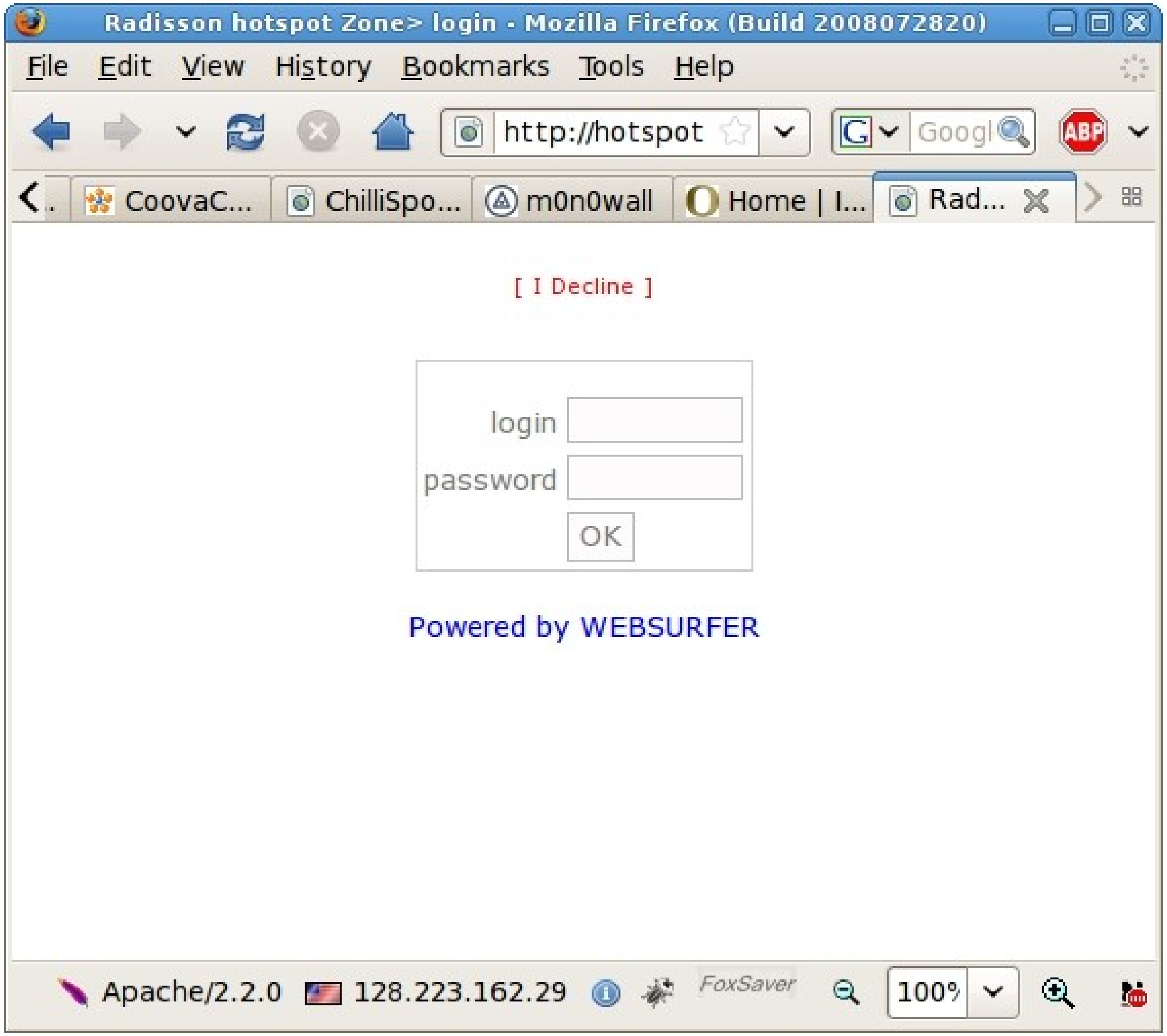
Enterprise Identity Management

- Processes and Documentation of users.
  - Now you must deal with this.
  - What to use as the back-end user store?
    - LDAP
    - Active Directory
    - Kerberos
    - Other?
  - Will this play nice with future use?
    - email, student/staff information, resource access, ...

Identity Management Cont.

- An example of such a project can be seen here:
  - http://ccadmin.uoregon.edu/idm/
- This is a retrofit on to an already retrofitted system.
- Learn from others and try to avoid this situation if possible.

A Wireless Captive Portal



Radisson hotspot Zone> login - Mozilla Firefox (Build 2008072820)

[I Decline]

login

password

OK

Powered by WEBSURFER

The Wireless Captive Portal

- Previous example was *very* simple.
- A Captive Portal is your chance to:
  - Explain your Acceptable Use Policies
  - Decide if you must authenticate, or
  - Allow users on your network and monitor for problems instead (alternate solution).
  - Anything else? Branding?

What's Happening?

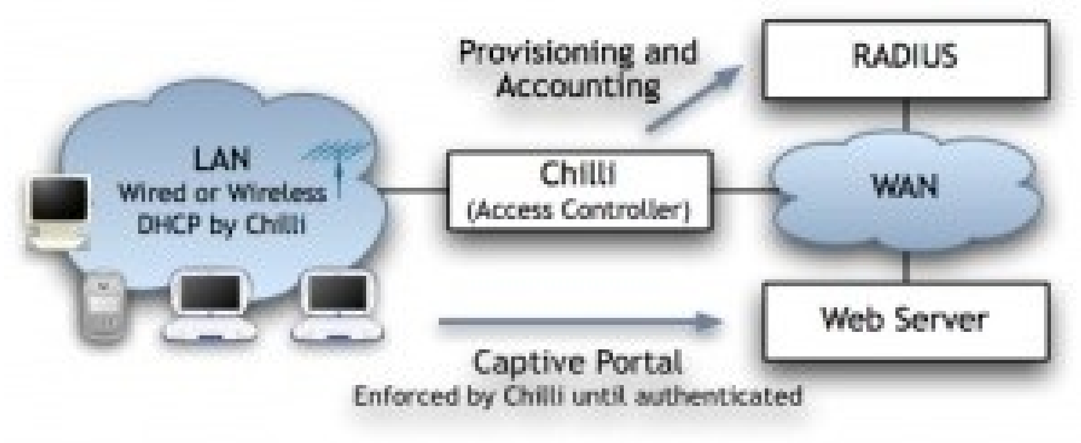
- remember our initial network diagrams...?
- Do you think our hotel built their own solution?
- Probably not...

Commercial Solutions

- **Aruba** http://www.arubanetworks.com/
- **Bradford Networks**
  - http://www.bradfordnetworks.com/
- **Cisco NAC Appliance (Clean Access)**
  - http://www.cisco.com/en/US/products/ps6128/
- **Cisco Wireless LAN Controllers**
  - http://www.cisco.com/en/US/products/hw/wireless/
- **Enterasys** http://www.enterasys.com/
- **Vernier** http://www.verniernetworks.com

Open Source Solutions

- **CoovaChilli** (morphed from Chillispot)
  - http://coova.org/wiki/index.php/CoovaChilli
  - Uses RADIUS for access and accounting.
  - CoovaAP openWRT-based firmware.



Open Source Solutions cont.

- **m0n0wall**
  - http://m0n0.ch/wall/
  - Embedded firewall appliance solution built on FreeBSD.
  - Entire configuration is stored in an xml file.
  - Sample Captive Portal Configuration Screen: http://m0n0.ch/wall/images/screens/services_captiveportal.png
  - Supported on low-end PC hardware, such as Soekris and ALIX platforms.

A Home-grown Solution

- **University of Oregon Captive Portal**
  - **NoCat** for Captive Portal
    http://nocat.net/
  - Access control mechanism:
    - **IP+Mac Address**
  - **IPTables+IPSets**
    http://www.shorewall.net/ipsets.html
    - IPSets are a high-speed matching module extension for IPTables.

A Home-grown Solution cont.

- Why this solution?
  - – Partially historical and timing related.
  - – Access control with IP+Mac Address allows for hashing on the IP address vs. a linear search on Mac addresses. At 4,000 addresses this became a problem.
  - – Some sample IPTables+IPSets rules are available with the tutorial materials on-line.

Other Considerations

Access Control Technology Possibilities

- DHCP control ==> *NetReg*
- MAC Address Filtering ==> Switches/Routers/Firewalls
- IP Address Filtering ==> Routers/Firewalls
- IP+Mac Address ==> software-based w/ IPTables+IPSets
- Cookie ==> *CAS*, *OpenID*/LDAP
- IP+Mac+Username(cookie) ==> some commercial solutions
- Port VLAN Assigment

Terminology/Projects

- **CAS**
  - Central Authentication System
  - http://www.ja-sig.org/products/cas/
- **NetReg**
  - Automated DHCP Registration System
  - http://netreg.sourceforge.net/
- **OpenID**
  - Single digital identity across multiple networks
  - http://openid.net/

What to Do?

- Review the options presented here, both commercial and Open Source.
- Review the various projects associated to understand how this all ties together.
- Devise a plan for your user identities, their storage and the processes around them.
- For sites under 3-4,000 users you might consider CoovaChilli or m0n0wall.

How it Ties Together

Wireless Captive Portals bring together a number of issues:

- **Network design** (VLANs to direct traffic to a single point – the captive portal solution).
- Longer-term **user identity** considerations.
- **Costs**, such as commercial software, hardware, Open Source solutions or even your own solution.
- **AUPs**, Acceptable Use Policies – you might need to decide what they are to present them to your users on your captive portal.

Resources

- Excellent Presentation on Network Access Control:
  - http://nsrc.org/workshops/2008/ait-wireless/kemp/network-security-nac-html.html
- Wireless Security Workshop at AIT:
  - http://nsrc.org/workshops/2008/ait-wireless/
  - Includes *lots* of presentations and exercises.

Questions?