Wireless Campus Network

Integrating Wireless into Campus Networks

Dale Smith
University of Oregon & NSRC
dsmith@nsrc.org

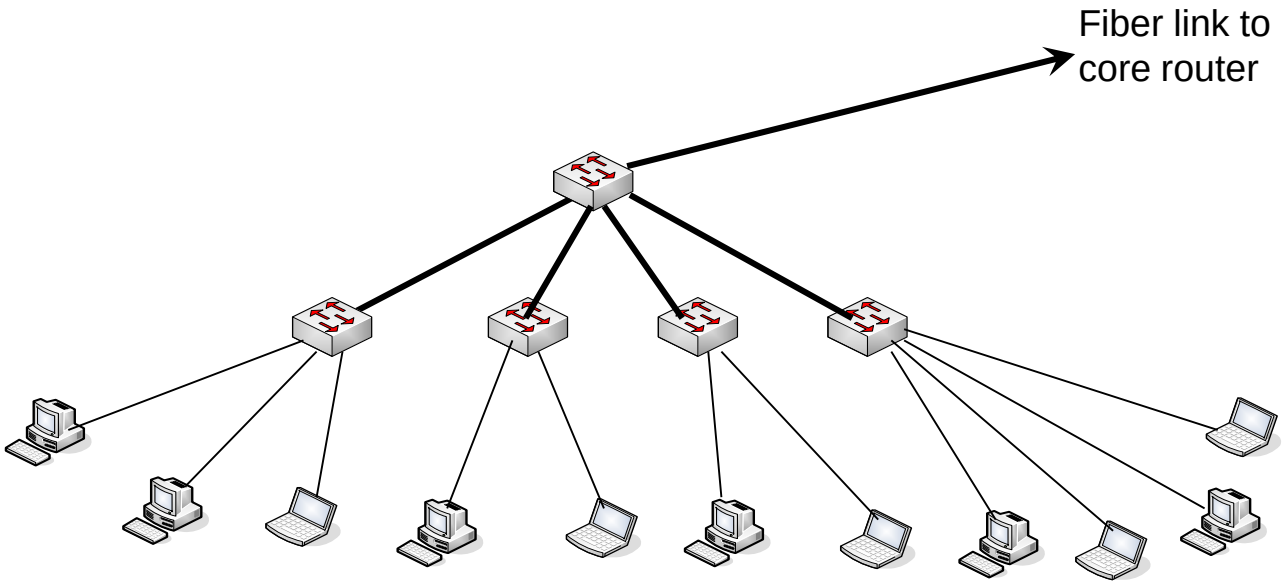
UNIVERSITY OF OREGON

Campus Network Overview

- Separate Edge Networks from Core
- Edge
  - Always switched
  - Serves one building
- Core
  - Always routed

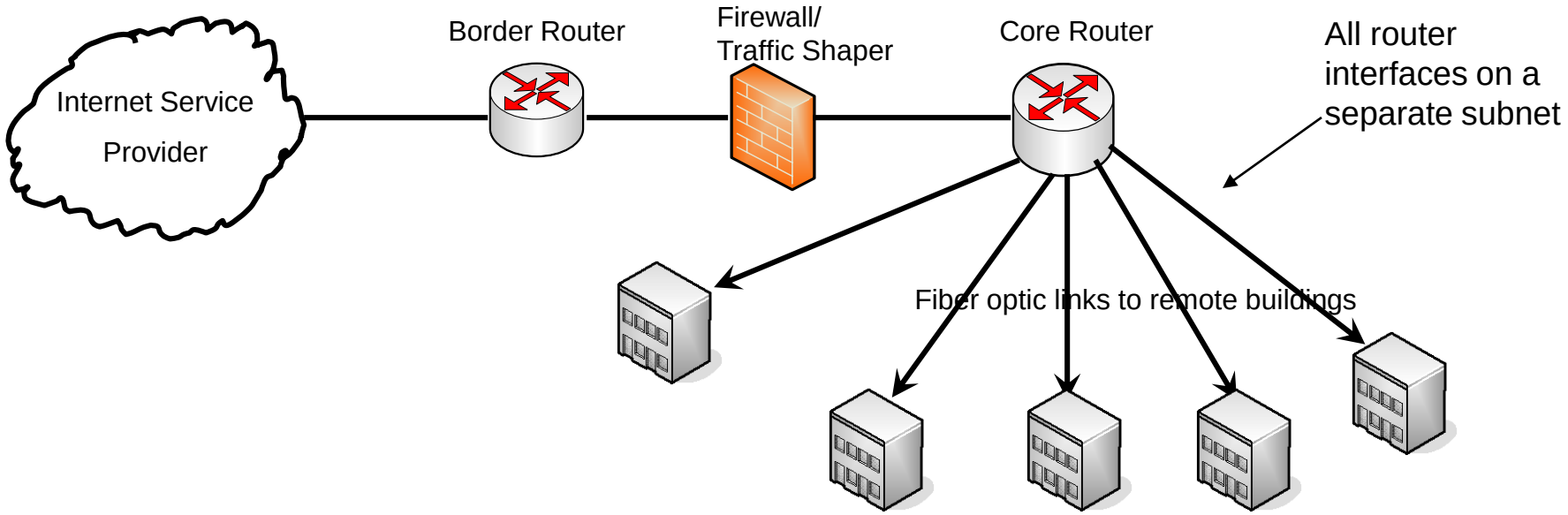
Edge Networks

- Make every network inside of every building look like this:



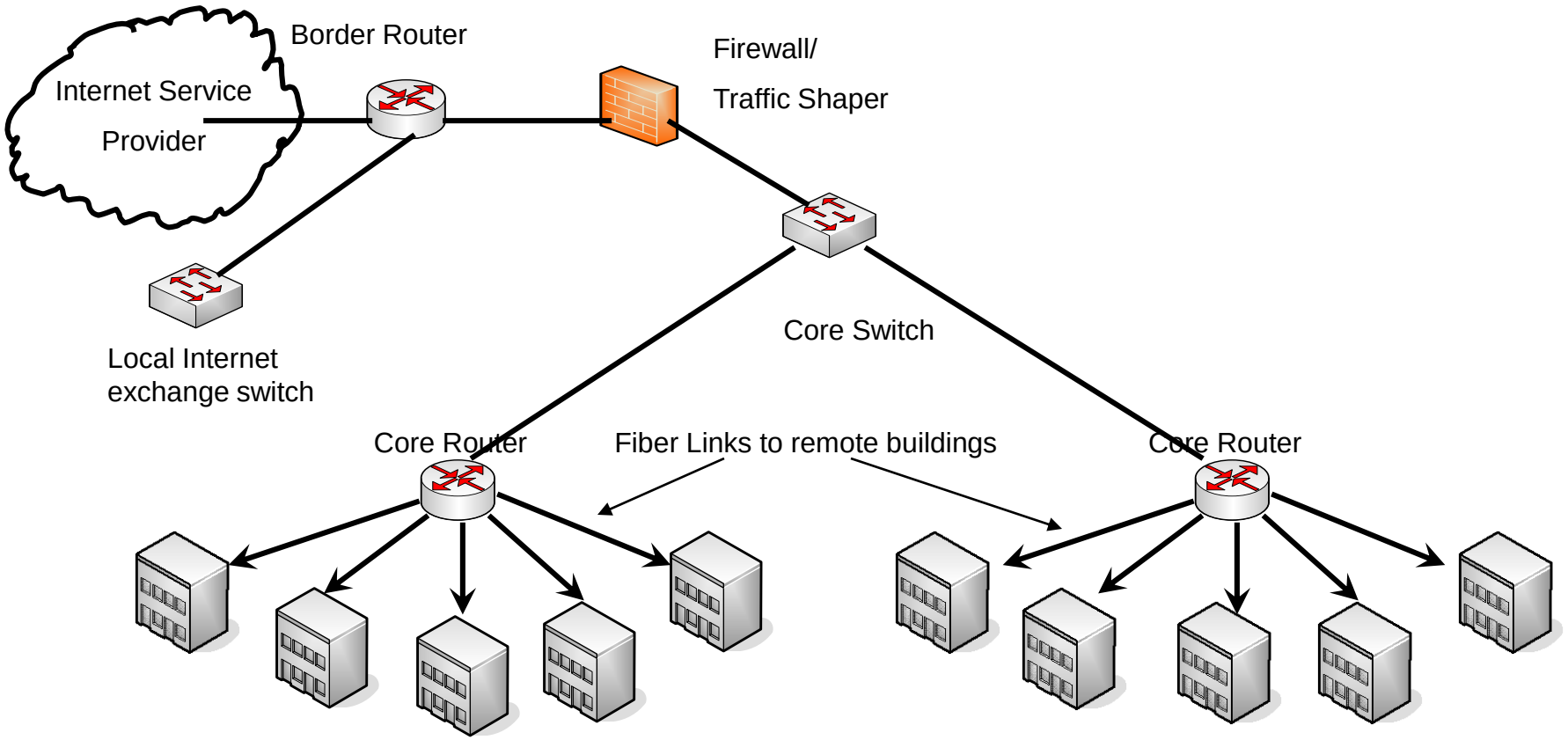
Core Networks

- You should be routing in the core of your network
- Routers give isolation between subnets
- This means that each building will be a different subnet

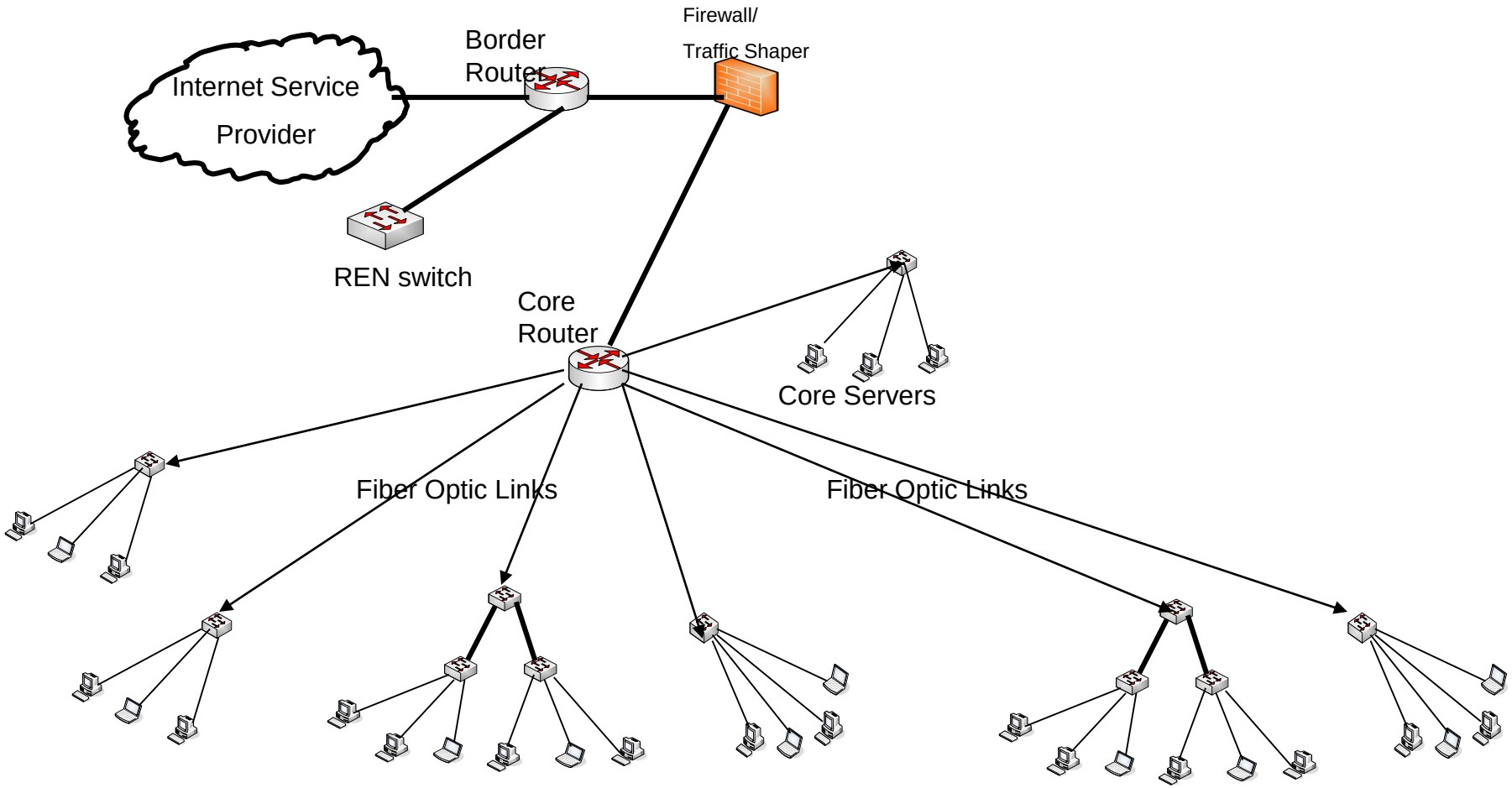


Complex Core Designs

- Multiple Core Routers



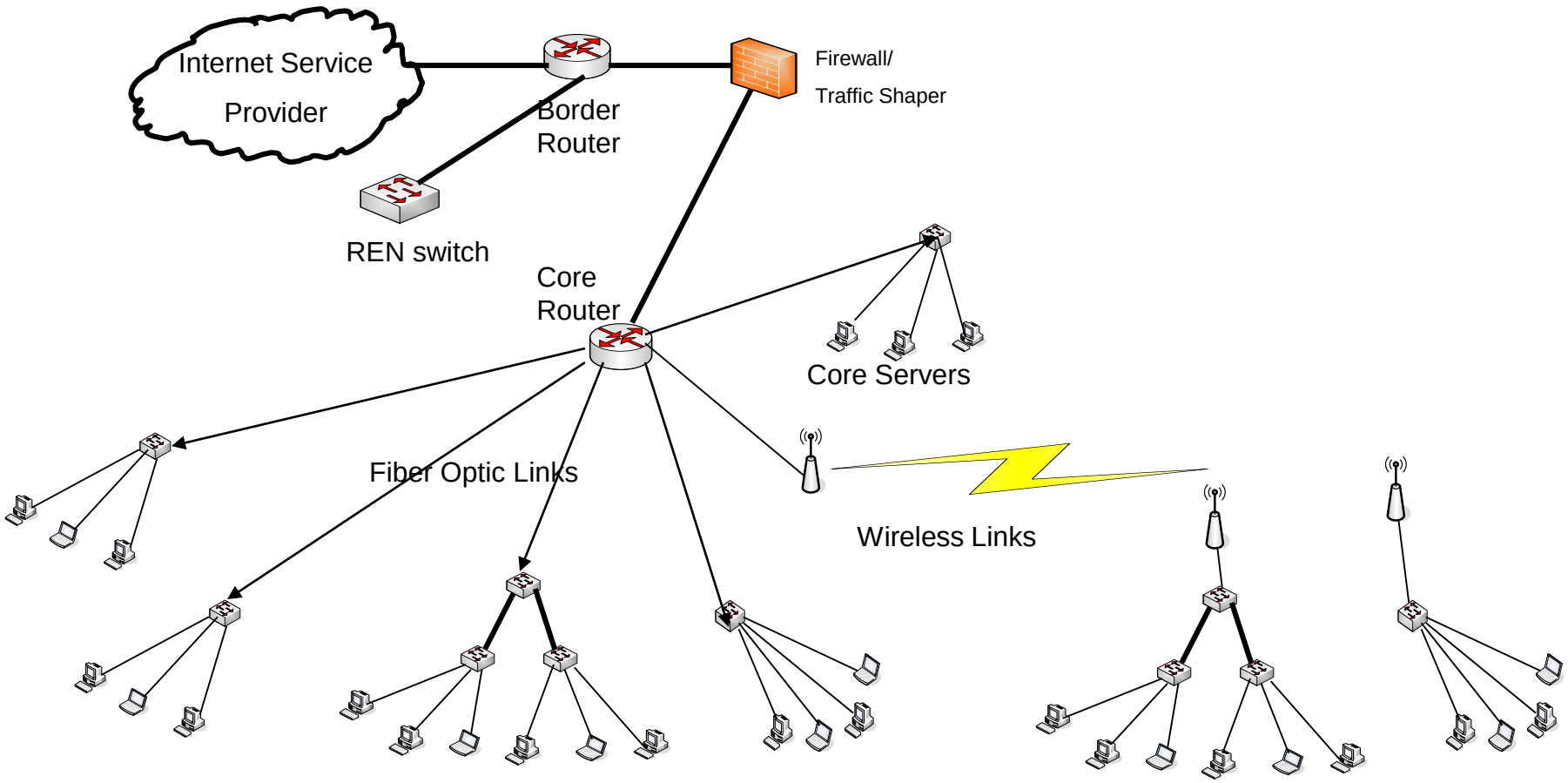
Putting it all Together



Integrating Wireless into the Network

- Wireless can play two different roles
  - Point to point links
    - Replaces fiber for service from core to aggregation switch in a building
  - Wireless LAN (hotspot)
    - Provides service to individual devices in a specific area

Point to Point



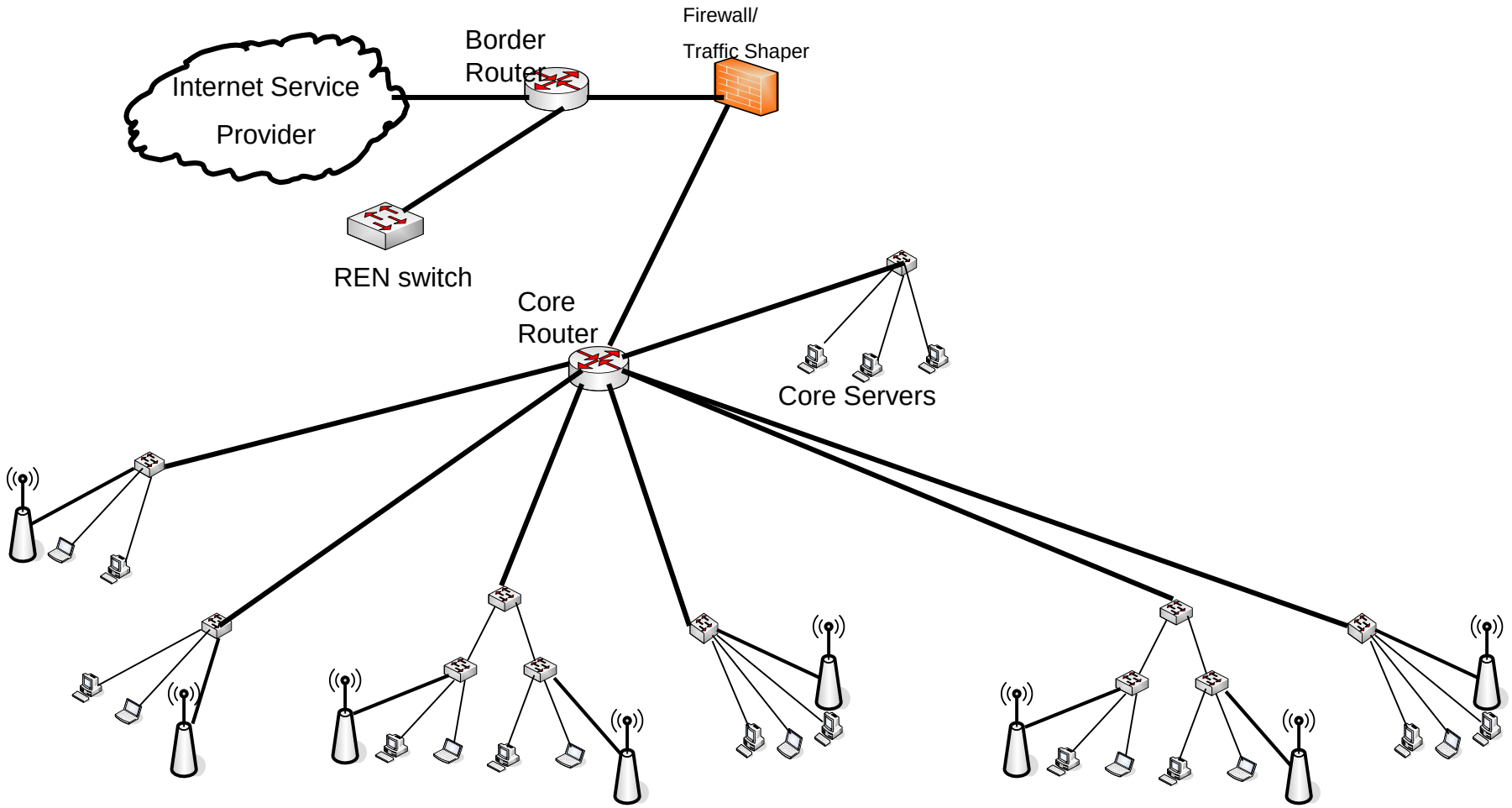
Point to Point

- Can replace fiber links
- Slower
- Less reliable
- Less costly
- Quicker to deploy
- Always put on a separate subnet – connect to a routed port in the core

Wireless LAN (Hotspot)

- Scope and Scale
  - Single Access points in Library, Coffee Shop, Classroom
  - Or more seamless coverage throughout public spaces – anywhere someone might study or work (roaming becomes an issue)
- Control who has access
  - Wide open
  - Authenticated

Wireless LAN – Use Campus Net



Routers versus Access Points

- Access points are like Ethernet switches.
  - They are just bridges
  - Allow for roaming if you plan right
- Routers
  - Typical consumer device meant for home or small office use
  - Typically will do NAT
  - Can’t roam between routers and keep sessions
- Must use DHCP for address assignment

Routers versus Access Points-2

Good to point out that **NAT** is not an essential function of an IP router

Small devices usually implement it, including most **access points,** which frequently can be configured to function in router mode

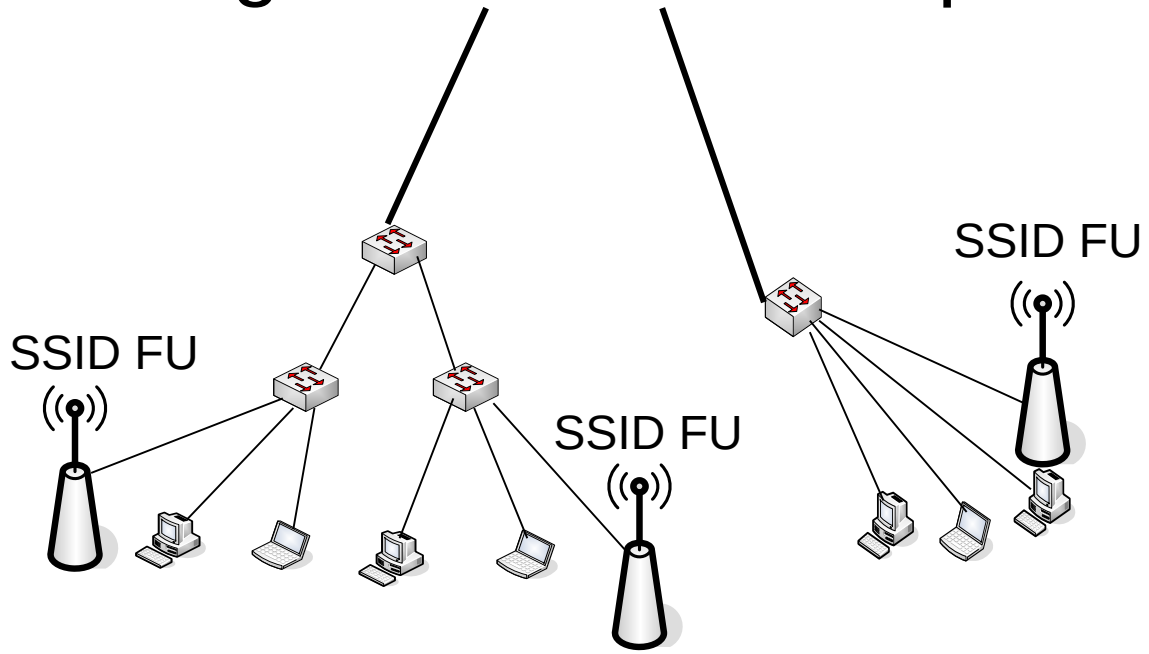
Probably not desirable in larger environments

Roaming and Client Behavior

- Wireless LANs use SSID for identification of network
- If a client moves from one access point/router to another that has the same SSID, it will not use DHCP to request a new IP address
  - This is why you can't roam with routers
  - And why you can with access points if you design your network appropriately

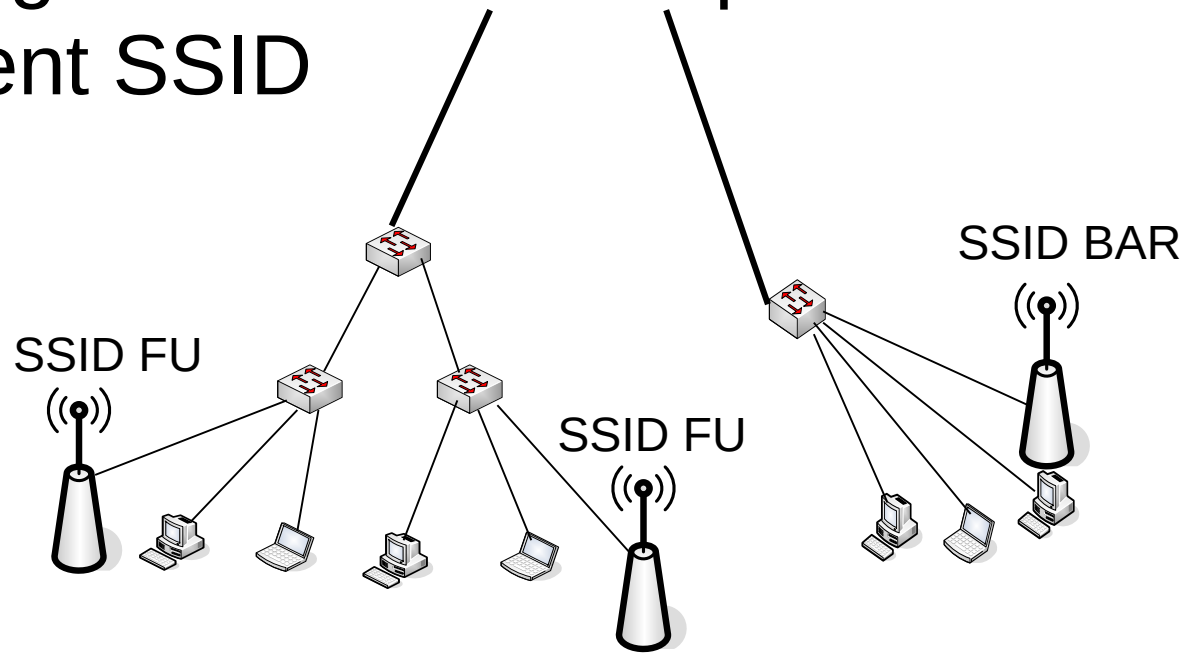
Roaming with same SSID

- Same SSID on access points
- Client will not request new IP address when moving between access points



Roaming with Different SSID

- Different SSID on some access points
- Client will request new IP address when moving between access points with different SSID

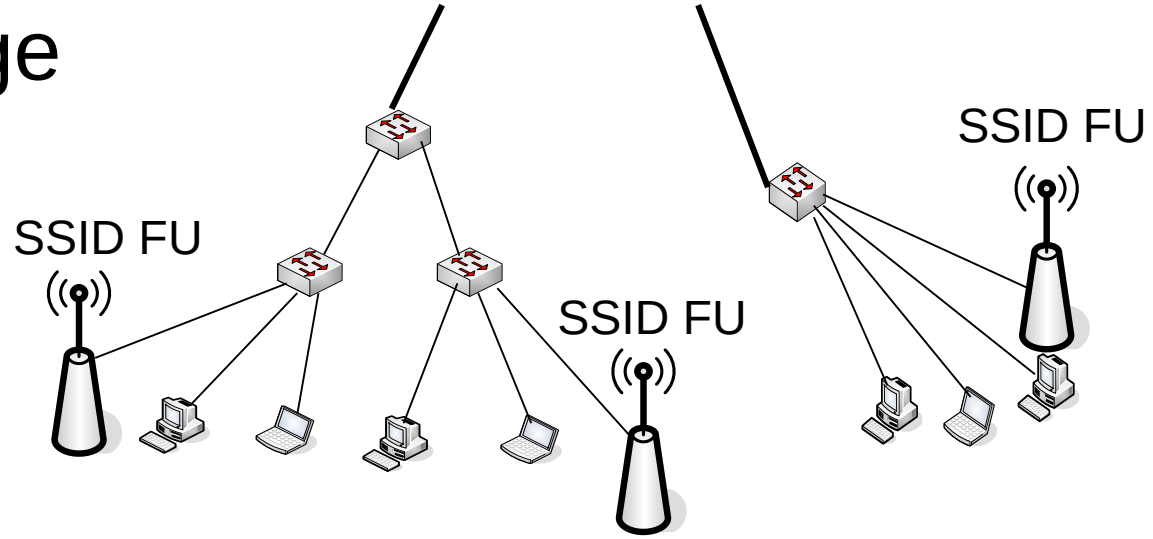


What happens when Roaming?

- Access points learn Ethernet (MAC) addresses
- Switches learn Ethernet (MAC) addresses
- Everything works fine from an Ethernet perspective because of dynamic learning of MAC addresses
- How about the IP layer?
  - If IP address changes with no change in SSID, it won't work

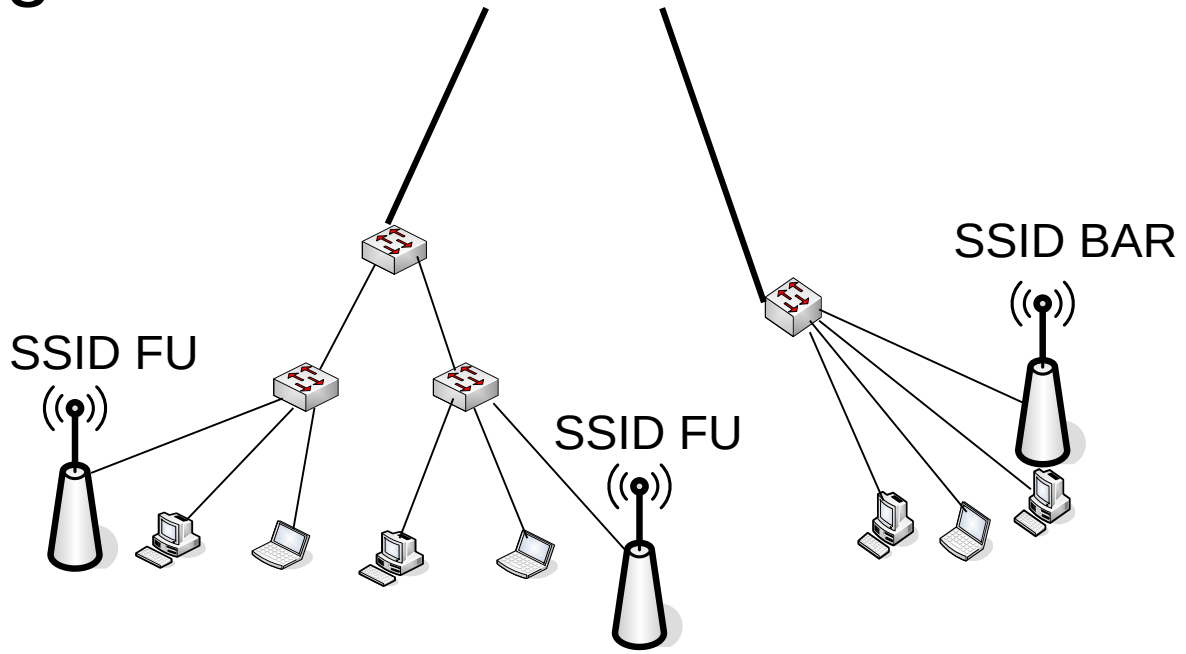
Roaming and IP – same SSID

- Unless we do something, this doesn't actually work
- Remember – different buildings are on different subnets, so IP address needs to change



IP and Roaming - Different SSID

- This actually works
- Client will request new IP address when moving between IP subnets



What about Authentication?

- Would like to protect your network from outside folks
- Would like to know who is using your network
- Would like to be able to deny admission to even known folks
- How might we do this?

Wireless Access Controls

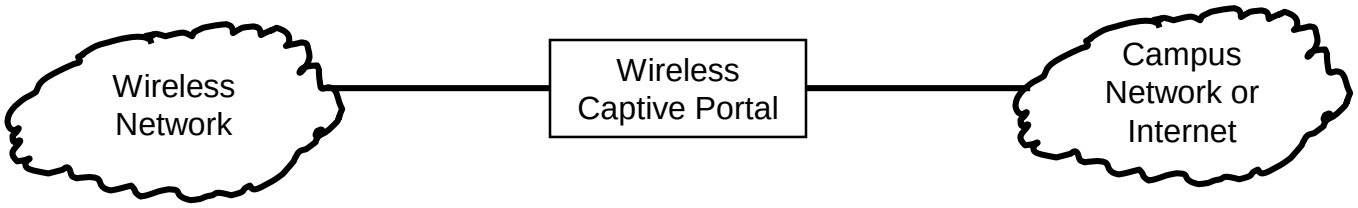
- Can use WPA with a pre-shared key
  - Common for hotels and home/office use
  - Hard to keep folks from sharing what the key is, so soon everyone has access
  - Doesn't provide you with identity of user
- Better to do something that requires authentication
  - Provides identity of user

Wireless Authentication

- Two basic techniques
  - Captive Portal
    - Intercepts web traffic and redirects to a “login” page
    - Typically an “in-line” device
    - Limitations on performance
    - Client only needs a web browser (that supports ssl)
  - 802.1X
    - IEEE standard for port-based access control
    - Enforced by access point (not in-line device)
    - Client must support 802.1X

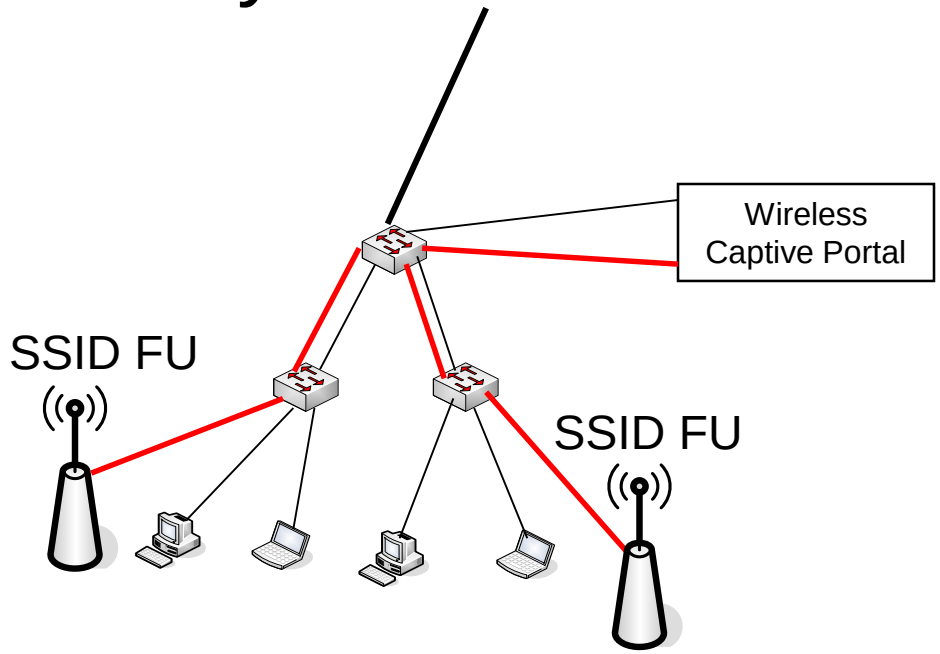
Captive Portal Network

- Portal is “in-line”
- Only allows traffic through after Authentication
- Becomes a performance bottleneck
- How do you do this on your campus network?

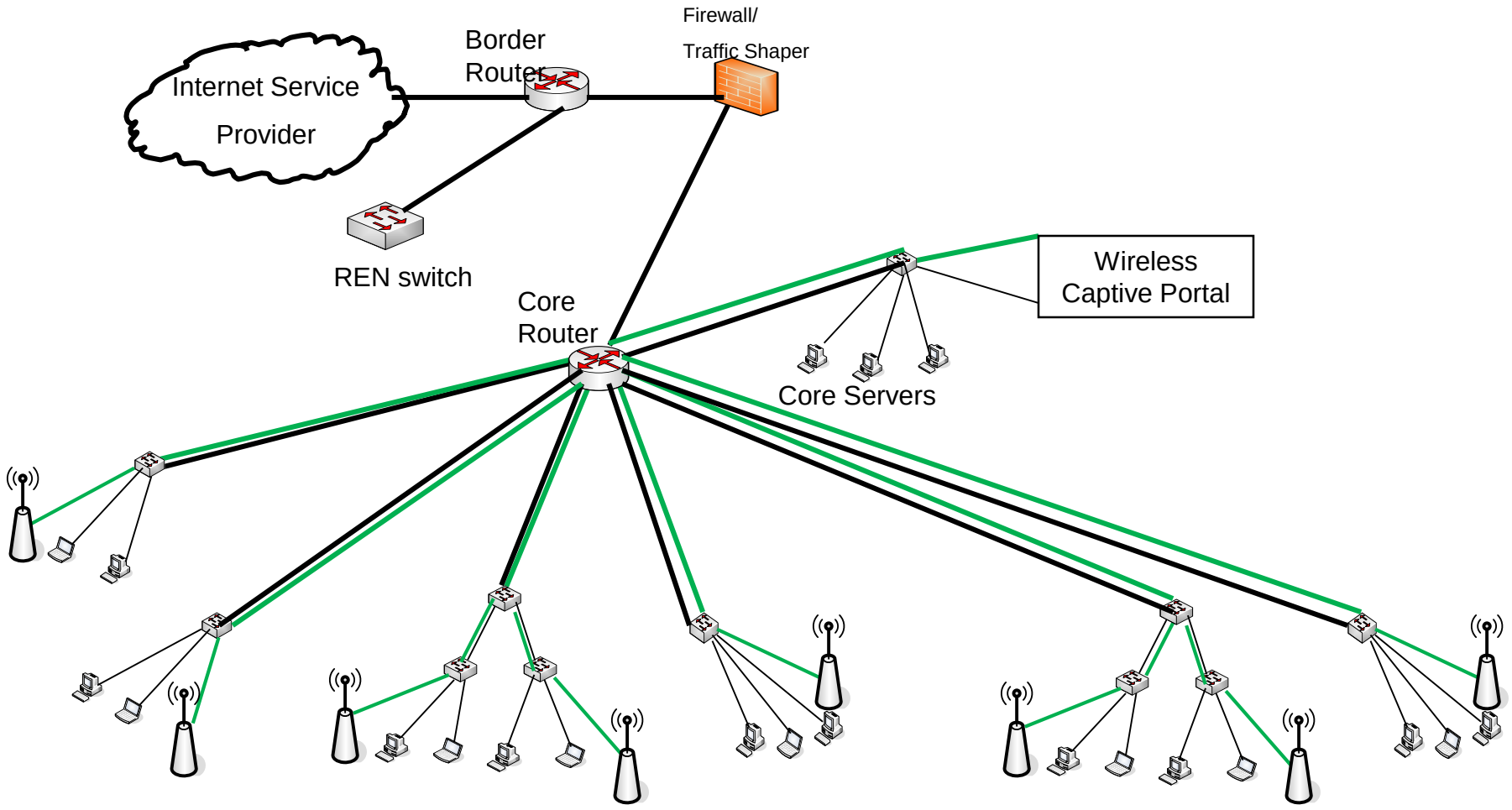


Captive Portal Network

- Trick is to deliver traffic from access point to portal
- Simplest way is to use VLANs



Single Campus VLAN for Portal

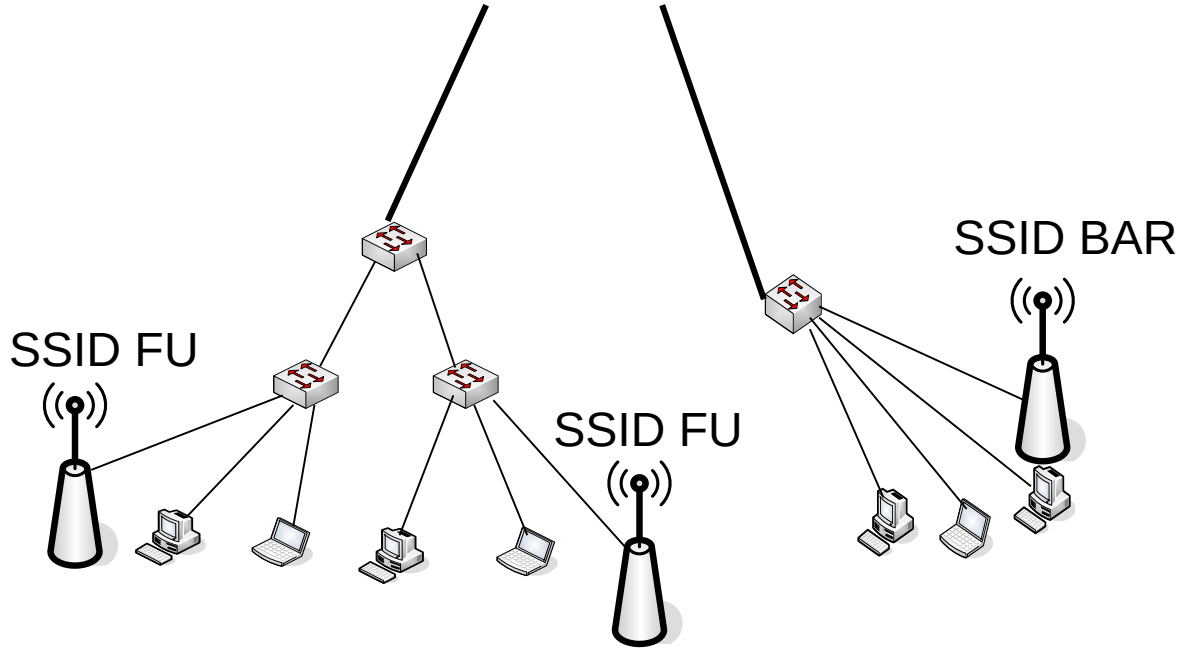


802.1X Authentication

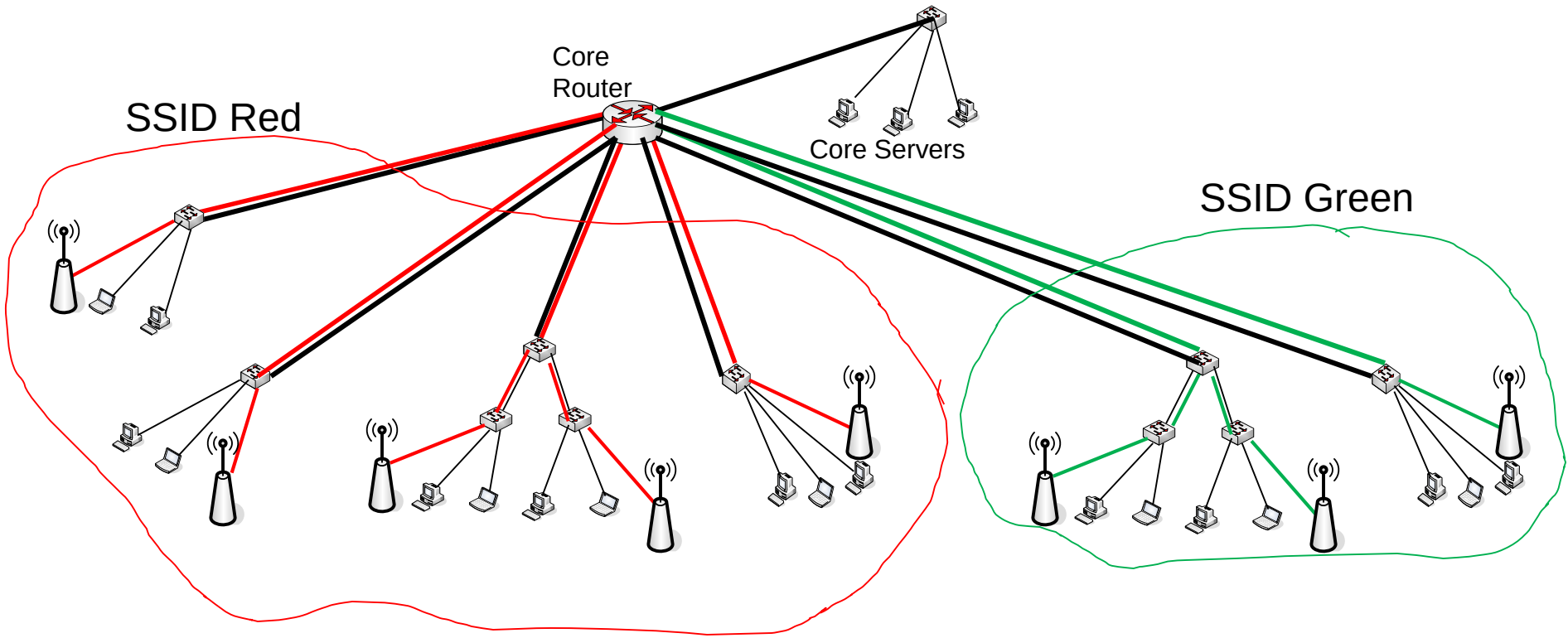
- Access control technique
- Requires 802.1X support in client
  - Windows XP, Vista, 7
  - MacOS and iOS
  - Android
  - Linux requires installation of drivers
- Networking for this is easier, but must worry about roaming across separate layer 3 networks (subnets)

802.1X and Roaming

- If you change subnets, you must use different SSID
- This is inconvenient, but works:



Can use VLANs for 802.1X



Key Issues

- Point to Point Links
  - Keep on separate subnet – broadcasts use bandwidth, so minimize them
- Wireless LAN
  - A single SSID means a single layer 2 network (broadcast domain)
  - Need to scope SSIDs to prevent problems

Thanks

Questions?

UNIVERSITY OF OREGON