Integrating Wireless into Campus Networks

Terminology issues

- The networking and wireless worlds sometime use identical words or expressions that have a different meaning in their respective environments

- Since we are approaching wireless in the context of networking (or vice versa ? :), we need to agree on definitions, and thus avoid misunderstandings.

Confusion

Some of the terms that need clarifying:

– PoE (Power over Ethernet)
– Access point
  - Router
  - Roaming
  - Bridge
– Broadcast domain

PoE (Power over Ethernet)

- In the wireless world, PoE is referred to any time a category 5/5e/6 cable is used to carry both the Ethernet signal and the power. The power can be 12, 24, or 48 volts DC (or any voltage in between).
- In the Networking world, PoE refers to the IEEE 802.3af standard that provides 48 volts DC over the same cable that carriers the Ethernet signal.
- The conflict is in the DC voltage. Beware!

Access point

Reminder: in wireless, all equipment that can connect to a wireless network categoriezed into one of three categories:

- **Access Point, master,** sometimes referred to as **infrastructure.** These are typically boxes that we've been configuring and have a combination of radios and wired Ethernet ports.
- **Client.** This is typically your laptop.
- **Ad-hoc.** A special mode where two devices act as peers and talk to each other

Access Point continued

- When connected to wired networks, an **access point** can function as a **bridge** (L2), a **router** (L3), or even both.
- In the networking world, the term **access point** is almost always used to designate a device used to **bridge** traffic between a wireless network and a wired network, at Layer 2.

Bridge

A **bridge** is used to connect 2 or more Layer 2 **segments** together

A **segment** in this case may be:

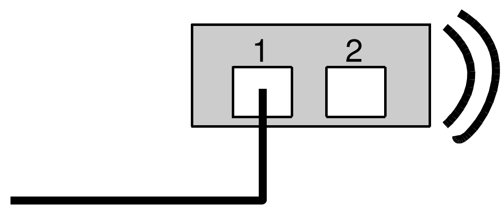
- a wired network
- a wireless network

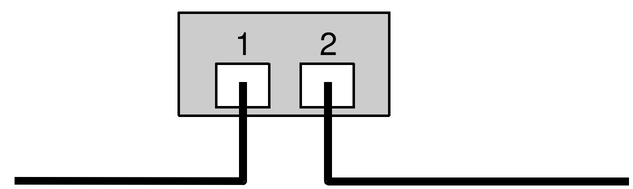
A **bridge** is essentially a 2 port **switch**

An access point which connects 2 interfaces: ...

- a wired interface (e.g.: 100/1000baseT)
- a wireless interface (e.g.: 802.1g)

… at Layer 2 is a **bridge**





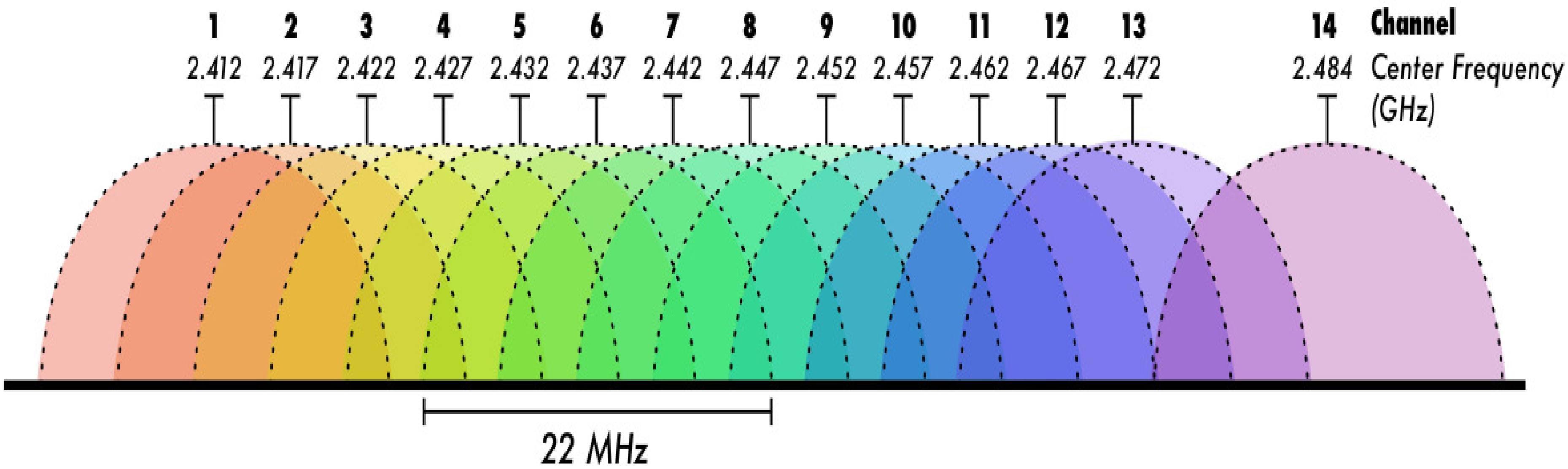
Router

- 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
- Can’t roam between routers and keep sessions. Hence not desirable in larger environments

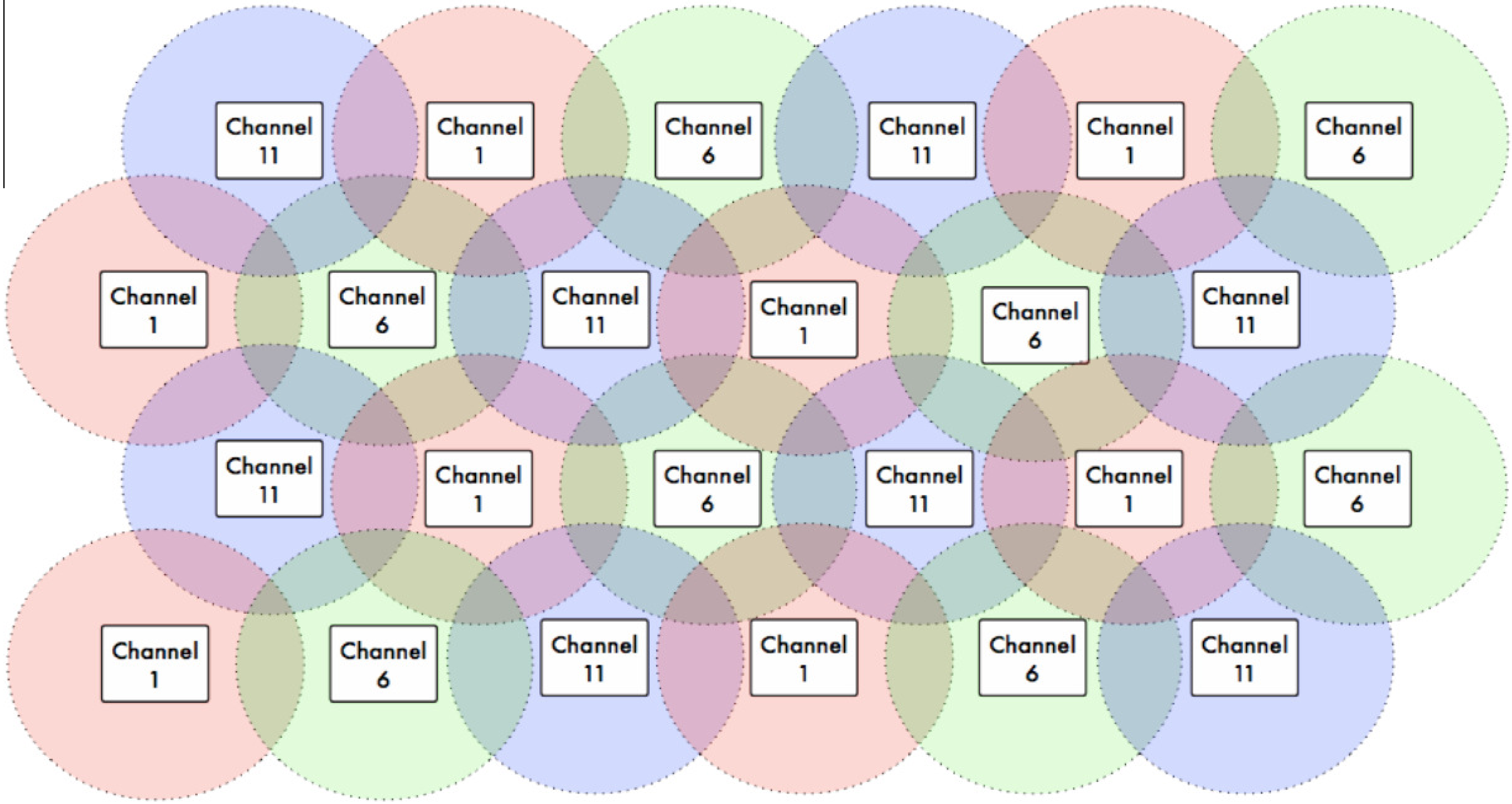
Broadcast domain

- In computer networking, a division of the network where all nodes (or hosts) within can reach each other by **broadcast** at L2
- **Broadcast** is, on ethernet, performed by sending traffic to MAC address ff:ff:ff:ff:ff:ff
- In the context of wireless, the equivalent of a **broadcast domain** from the networking world is implemented as SSIDs, so a single broadcast domain will be a single SSID

Frequency planning



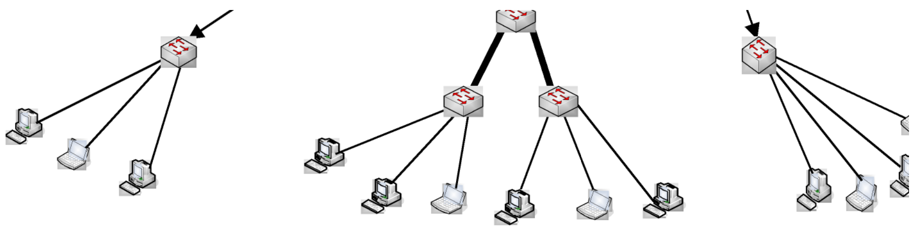
Frequency planning

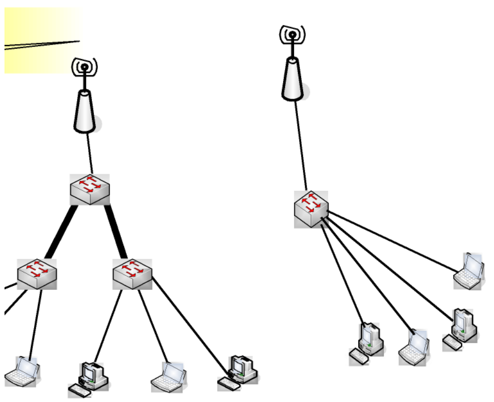


Integrating Wireless into the Network

- Wireless links (PtP) may replace fiber/wired links in the core network where distance or budget or security aspects suggest this
- Wireless "hotspot" access on the edges: offices, cafés, libraries, workspaces, ...
- Wireless mesh clouds on the edges, e.g. for compounds, housing, villages

Point to Point

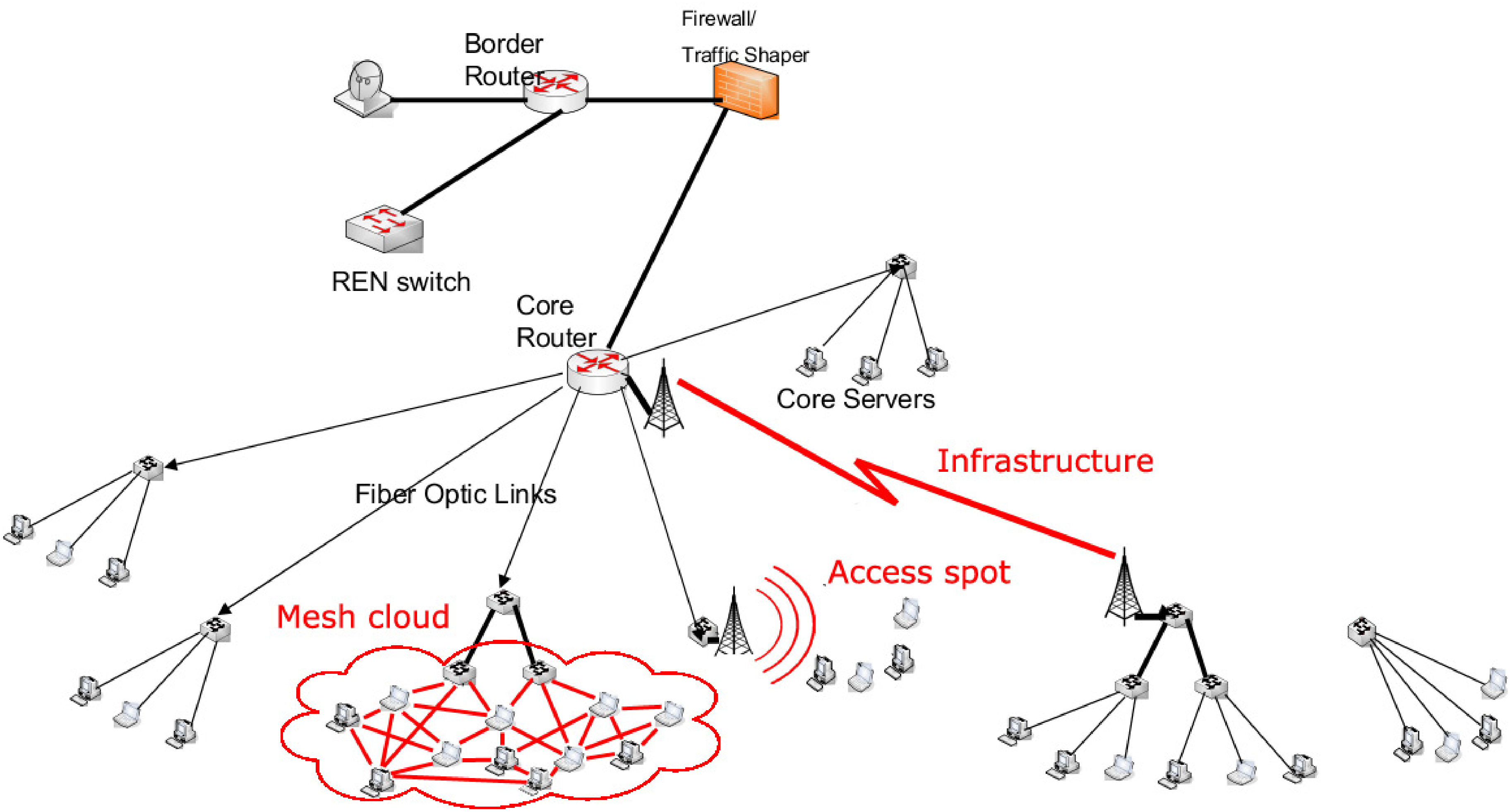




Point to Point

- 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

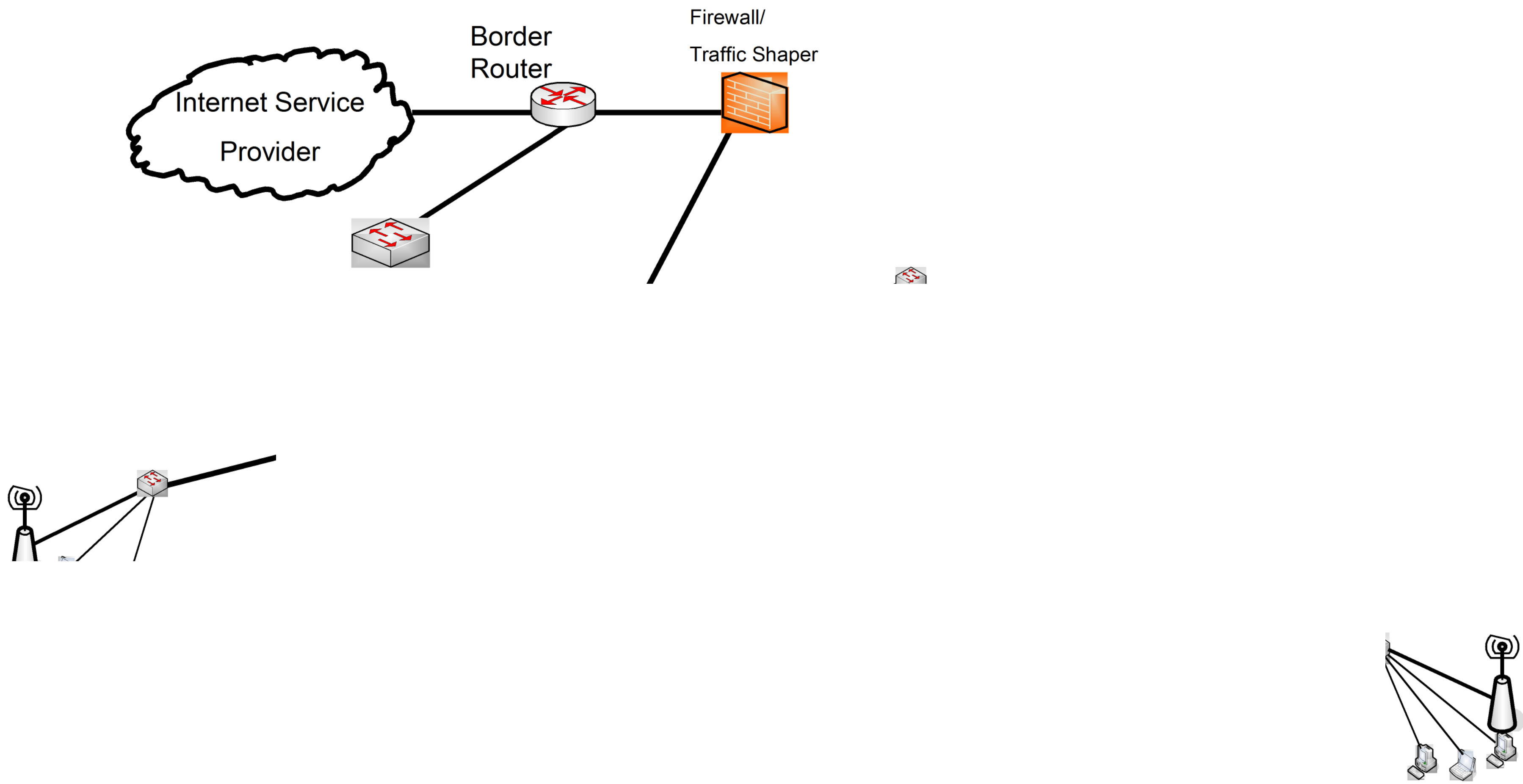
Wireless LAN – Use Campus Net



Wireless LAN (Hotspot)

- Scope and Scale
  - Single Access points in Library, Coffee Shop, Classroom, workplace
  - Or more seamless coverage throughout public spaces (outdoor) – anywhere someone might study or work
  - Large scale deployment will be complex

Wireless LAN – Use Campus Net



Problem to face

- Authentication
  - It depend on your campus AUP and/or your country laws.
- IP Address/subnet/VLAN
  - Use same data subnet/VLAN or separate.
  - Unifi subnet/VLAN
- Roaming
  - Your wireless smart phone/tablet mobility.
- APs administration
  - Install/upgrade/config APs firmware.

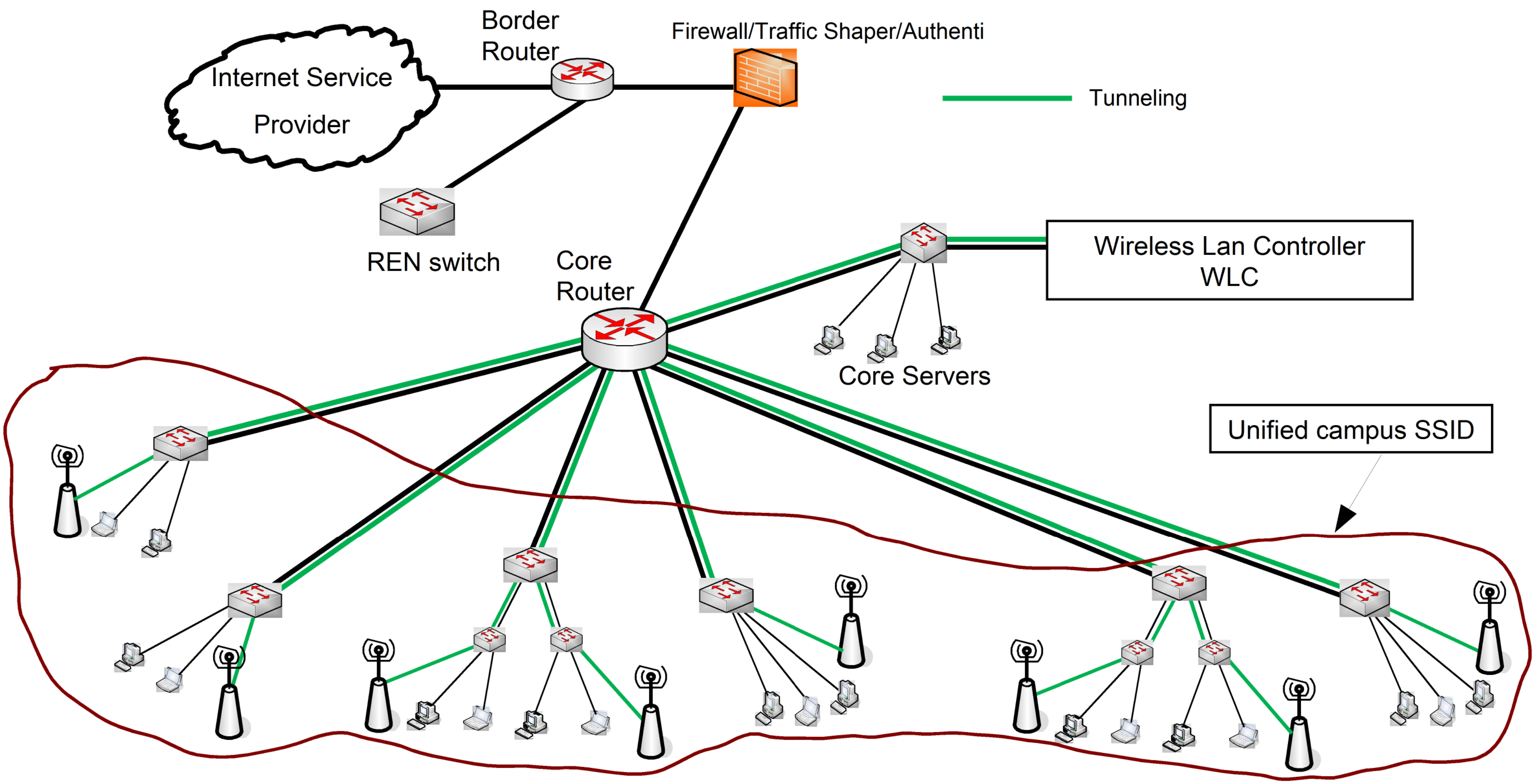
2 Solution

- Enterprise solution
  - Cisco
  - Aruba
- Low end solution (aka DIY)
  - Linksys, Mikrotik, ubiquit.
  - Need to prepare your campus network to support:
    - Campus-wide authentication (for wireless).
    - Roaming.
    - Administration (centralize tftp server to store firmware/config files/Log)

Enterprise Solution

- Cisco / Aruba
  - AP and controller
  - Can operate in L3 mode
  - APs can be installed anywhere in campus
  - APs automatically search and register itself to controller
  - APs establish tunnel to controller
  - All client traffics managed by controller
  - Roaming, Authentication, VLAN manage and APs configuration can be managed from centralize location

Enterprise Campus wireless solution



Low end solution

- Linksys (WRT54G[L])
  - A favorite platform for open source community
  - Numerous firmware available to flash with (DD-WRT, Tomato and OpenWrt.)
  - Feature rich
  - Can be integrated with campus net with some effort
- Mikrotik
  - Sell cheep hardware and software solution
  - Hude third party companies who make accessories specifically for MikroTik products

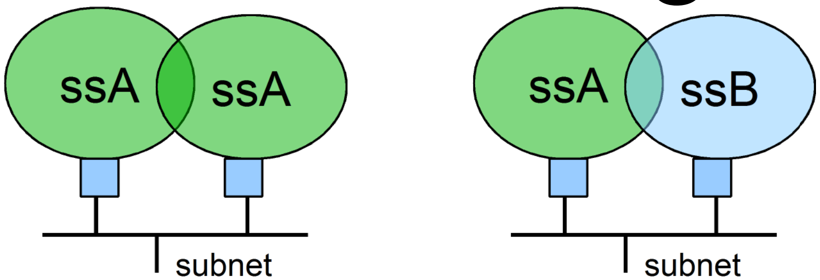
RouterBOARD_Selection_Guide.pdf

	411/711/SXT/Groove	411AR/711A/Groove A	411U	411AH	411UAHR	433	433AH	433UAH	435G	450/750	750UP	751U	450G/750GL	493	493AH	493G	800	1100/1200
Core Router																	✓	✓
Wireless Backbone									✓							✓	✓	
3G Device			✓		✓			✓	✓		✓	✓				✓		
Gigabit Eth									✓				✓			✓	✓	✓
Heavy Load Multi AP							✓	✓	✓						✓	✓	✓	
Heavy Load AP				✓	✓		✓	✓	✓						✓	✓		
Average Load AP				✓	✓	✓	✓	✓	✓			✓		✓	✓	✓		
Easy Load AP		✓	✓			✓						✓		✓				
Heavy Load Ethernet Router							✓	✓	✓				✓		✓	✓	✓	✓
Average Load Ethernet Router						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Easy Load Ethernet Router						✓				✓	✓	✓		✓				
Low Cost CPE, Point-to-Point	✓																	

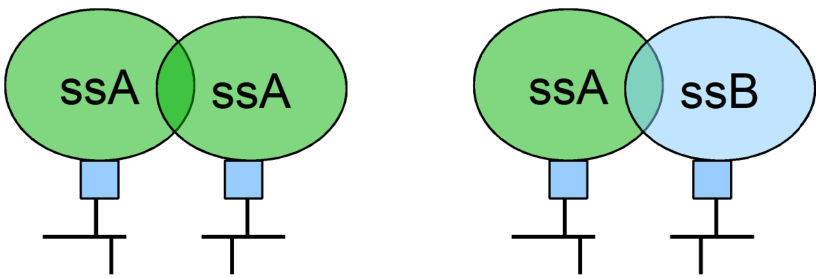
Low end solution

- Ubiquiti Unifi Wifi system
  - Free downloadable controller software
  - All APs can be managed centrally by controller.
  - Support CP on the controller
  - Cheep hardware.

Roaming matrix



same SSID	different SSID	
OK (1)	OK (2)	same IP subnet
NO (3)	OK (4)	different IP subnet

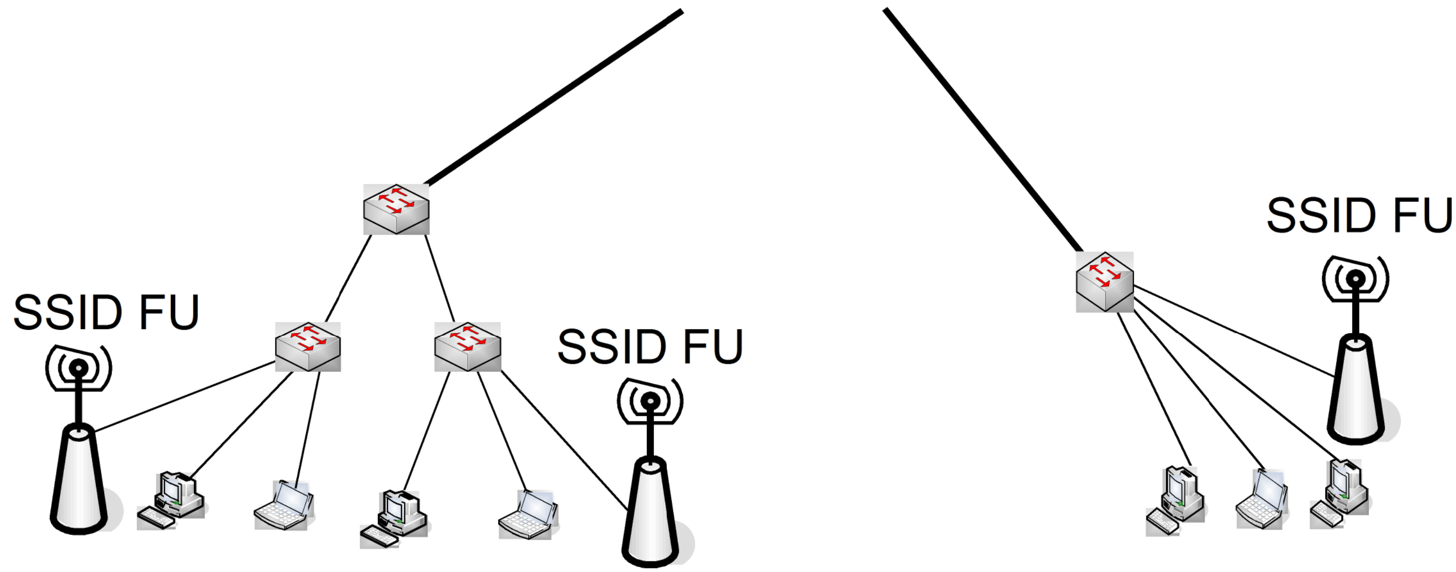


Roaming and Client Behavior

- 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

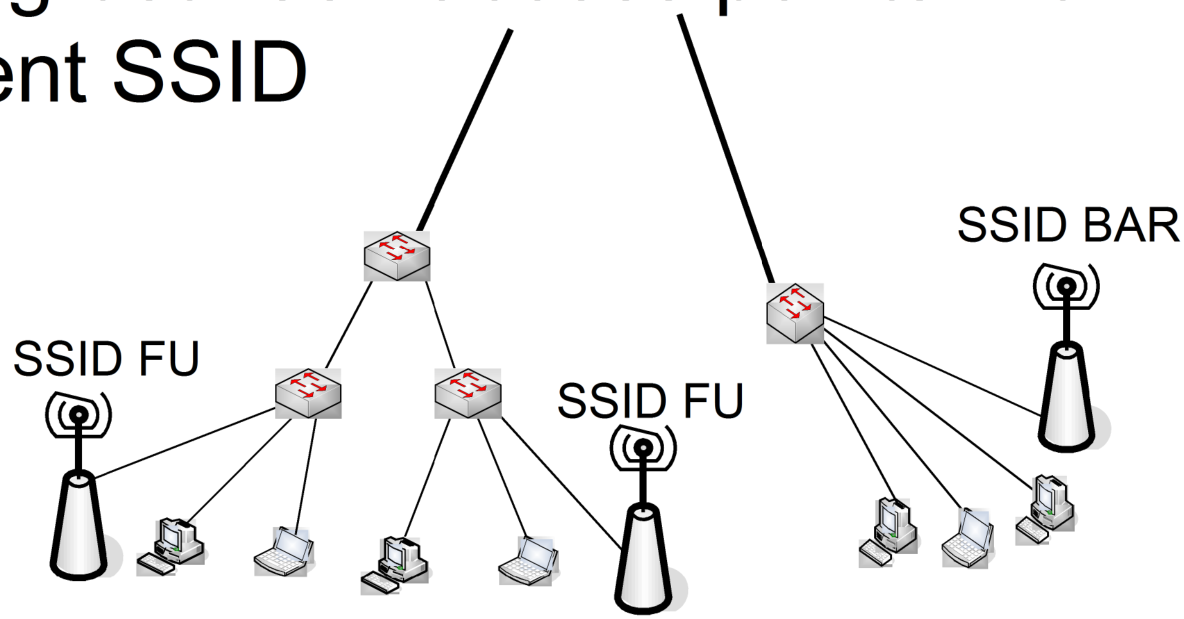
Roaming with same SSID

- 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

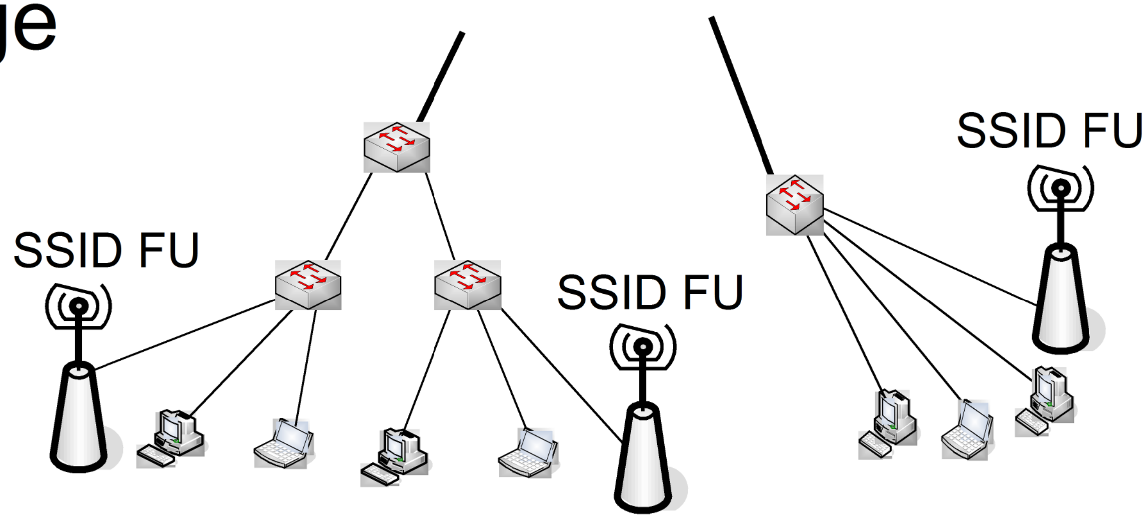


What happens when Roaming?

- 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

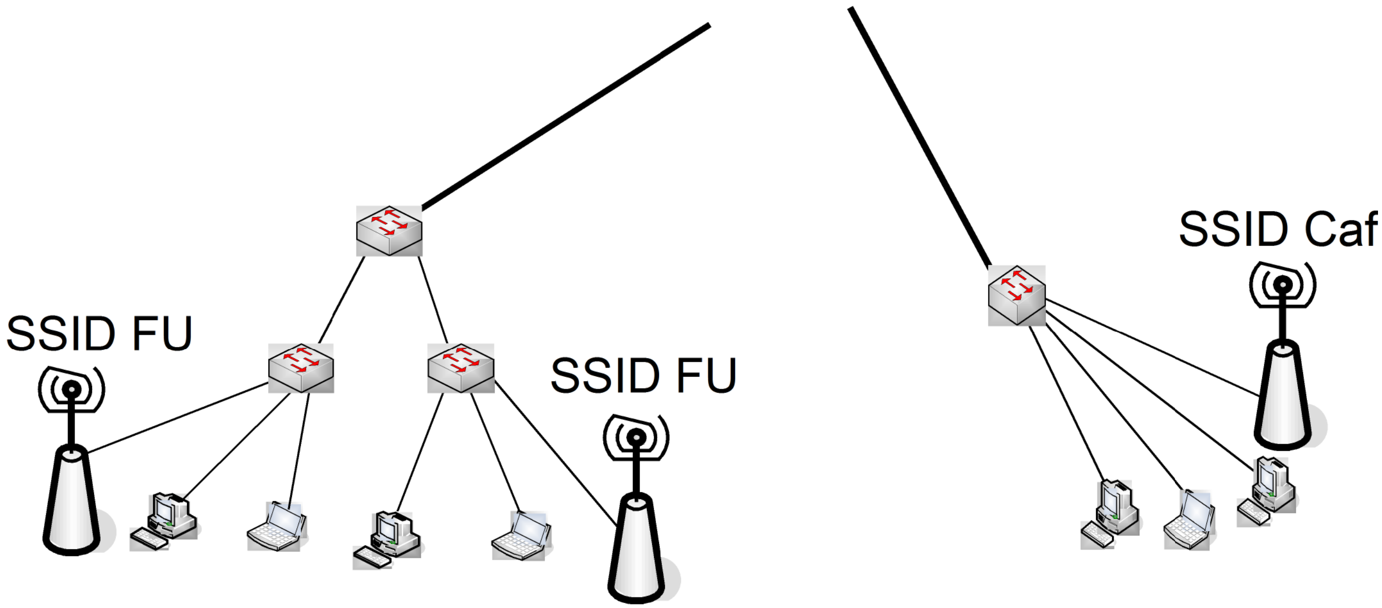
Roaming and IP – same SSID

- 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



Roaming

- On smaller networks, it's easy to do L2 roaming
- As networks get bigger, best to avoid large L2
- (broadcast) domains
- IP segmentation/subnetting
  - Why sacrifice this architectural principle when implementing wireless ?

Roaming cont.

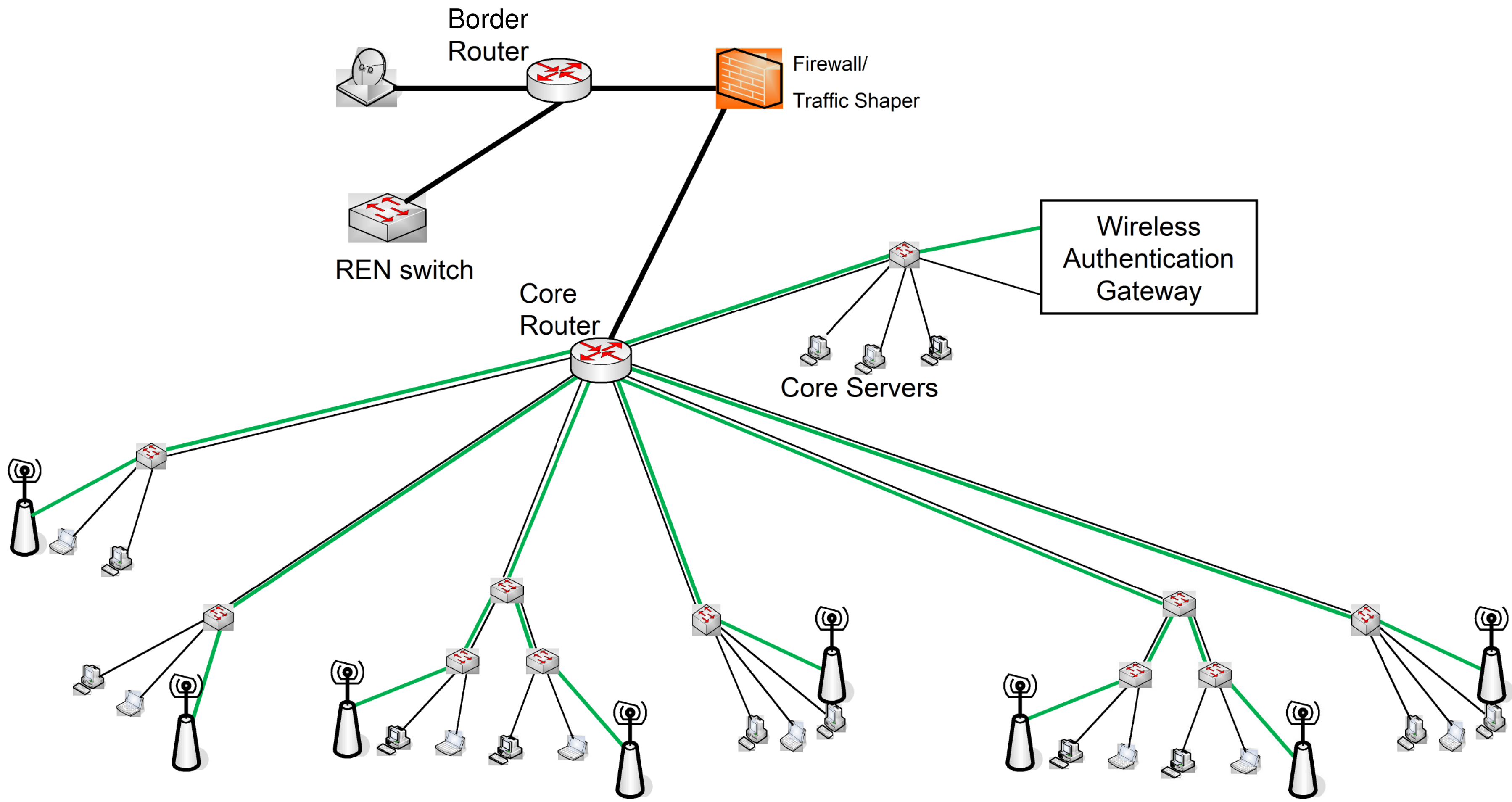
Necessary to find the right balance

- Groups of access points in same L2, same SSID, when closely located (same building, room, …)
- Different locations, different L3 (IP) networks, different SSIDs

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?

Simple Campus wide wireless solution



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

- Many techniques available:
  - 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

Wireless Authentication (cont.)

- Network Access Control (NAC)
  - Depend largely on your network equipments (switches)
  - Managed switch must be used across the campus
  - Provide authentication for both wired and wireless
  - Client needs a web browser (that supports SSL)
  - Netreg, Packetfence, bradford

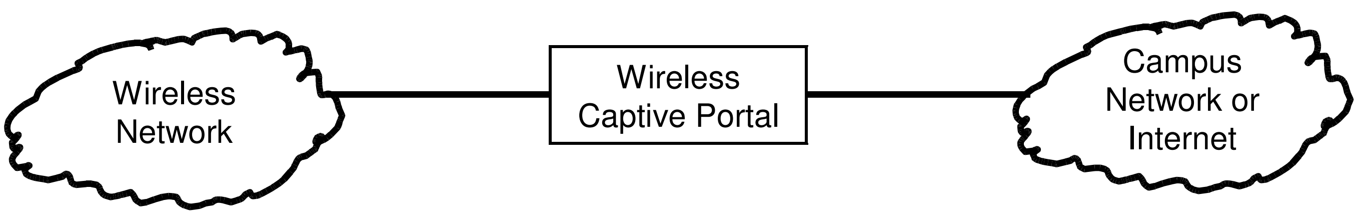
    http://netreg.sourceforge.net/

    http://www.packetfence.org

    http://www.bradfordnetworks.com/network_access_control

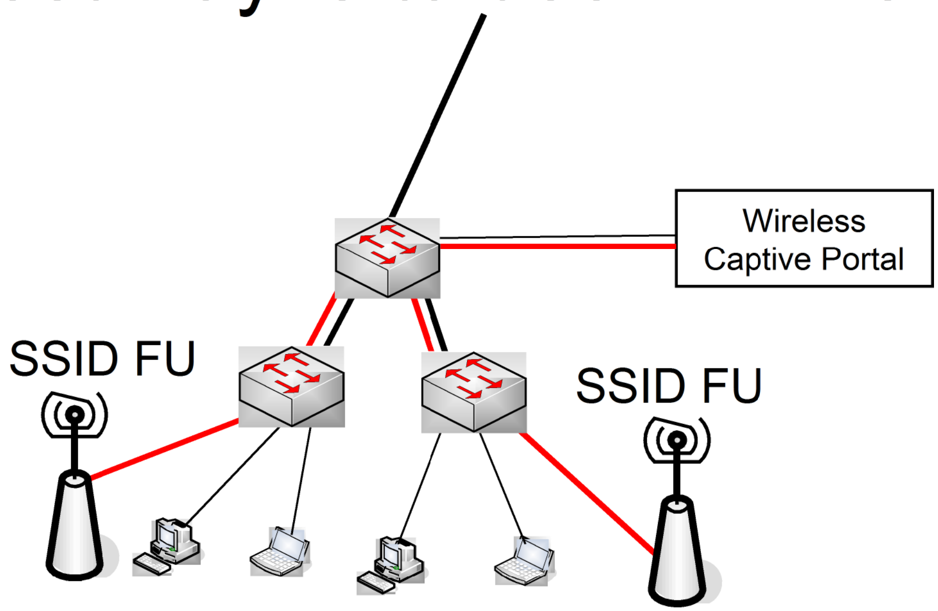
Captive Portal Network

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

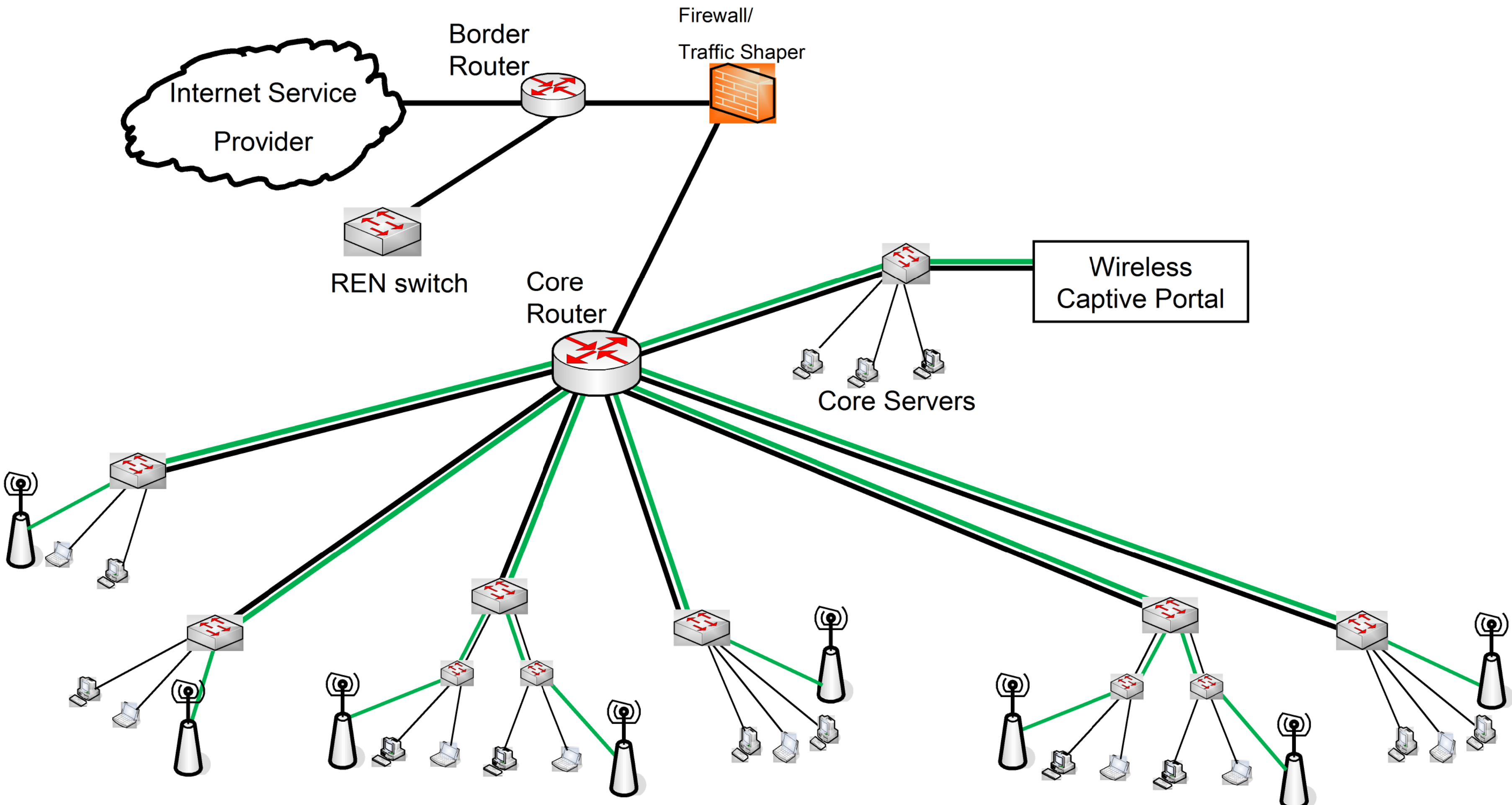


Captive Portal Network

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



Single Campus VLAN for Portal

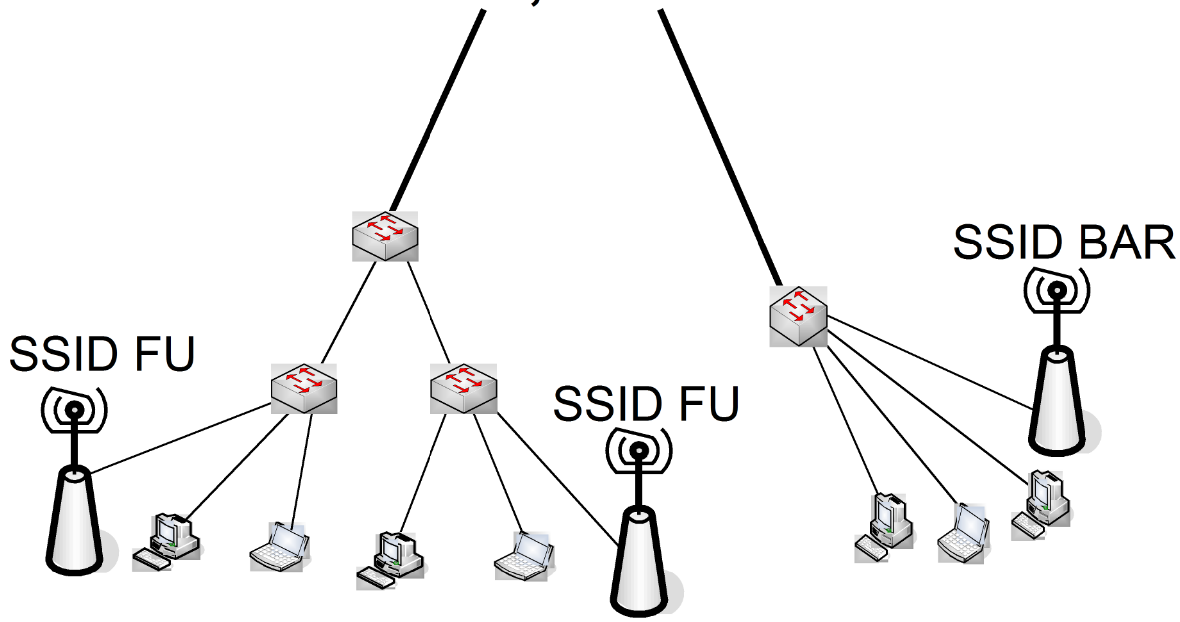


802.1X Authentication

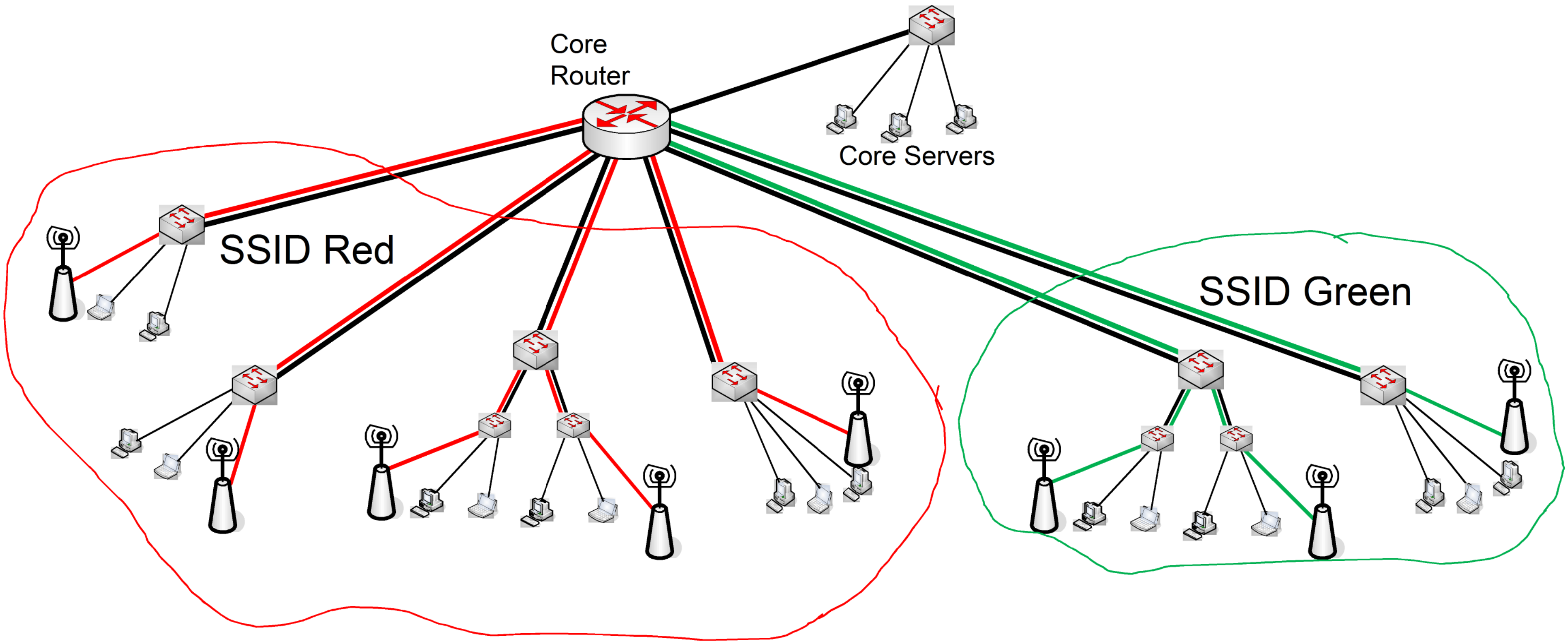
- Access control technique
- Requires 802.1X support in client
  - Windows XP, Vista, 7
  - MacOS and iOS
  - Android
  - Linux requires installation of drivers
- Networking for this is easier, but must worry about roaming across separate layer 3 networks (subnets)

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?

Symbols to use for diagrams