CprE 530

Lecture 8

Topics

- Wireless Security
  - Vulnerabilities
  - Mitigation
- General Mitigation Methods
  - VLAN
  - NAC

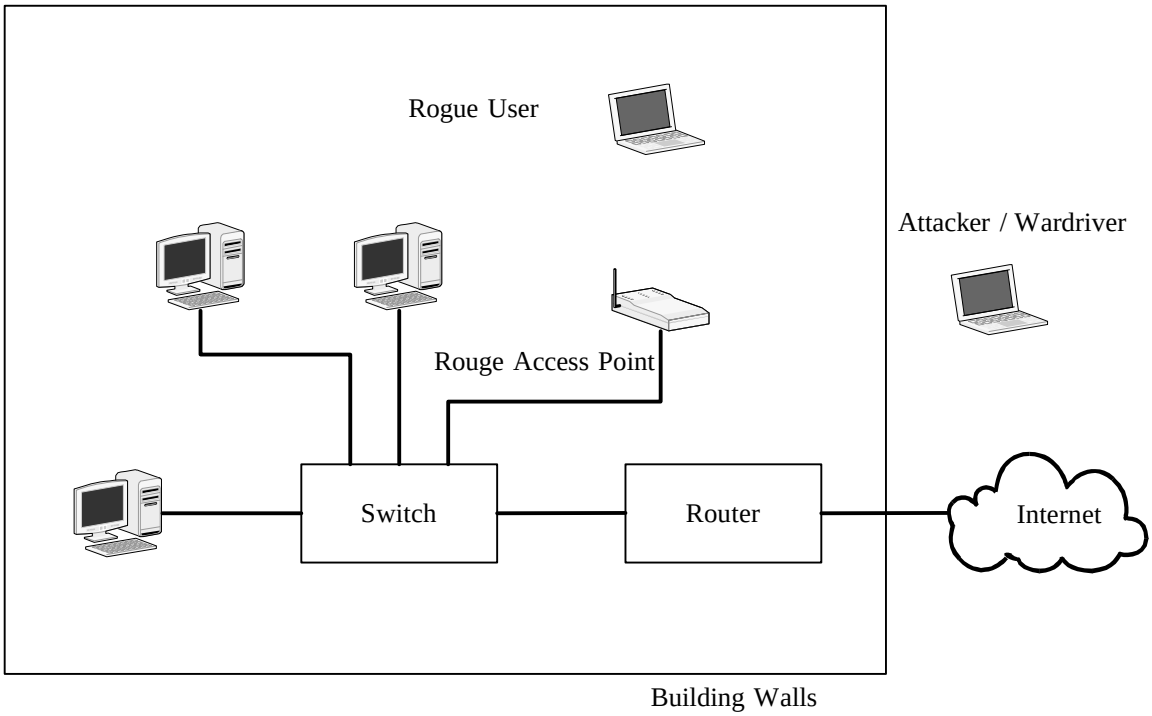
Authentication Based

- You can set the hardware address
- Hardware address is used as authentication in Access Points
- Device authentication
  - Access point authentication
  - Wireless device authentication
- Access point configuration authentication
  - Gaining access to the access point

Access point Authentication

- Rogue access point
  - Installed by valid user
- Fake Access point
  - Installed by attacker

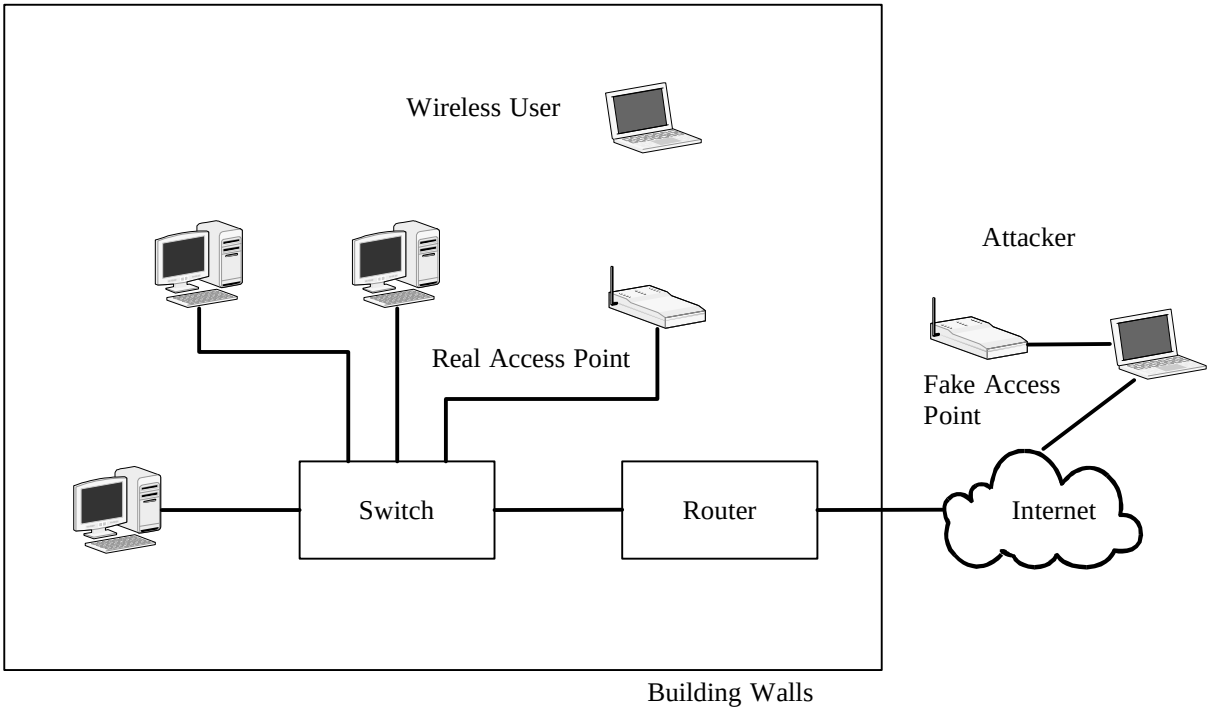
Rogue Access Point



Rogue Access Point

- Provides access to attacker
  - Intentional or unintentional
- Bypasses perimeter security mechanisms
- Hard to find and stop
  - Scan for SSID
  - Scan for wireless traffic
- NAC might provide some help.

Fake Access Point



Fake Access point

- Hard to fake an access point within an organization.
- Easier if the access point is a public access point with no encryption.
  - Not much to be gained by this

Access Point Configuration Authentication

- Access point are often configured over the network.
- They have default passwords
- An attacker could change security settings

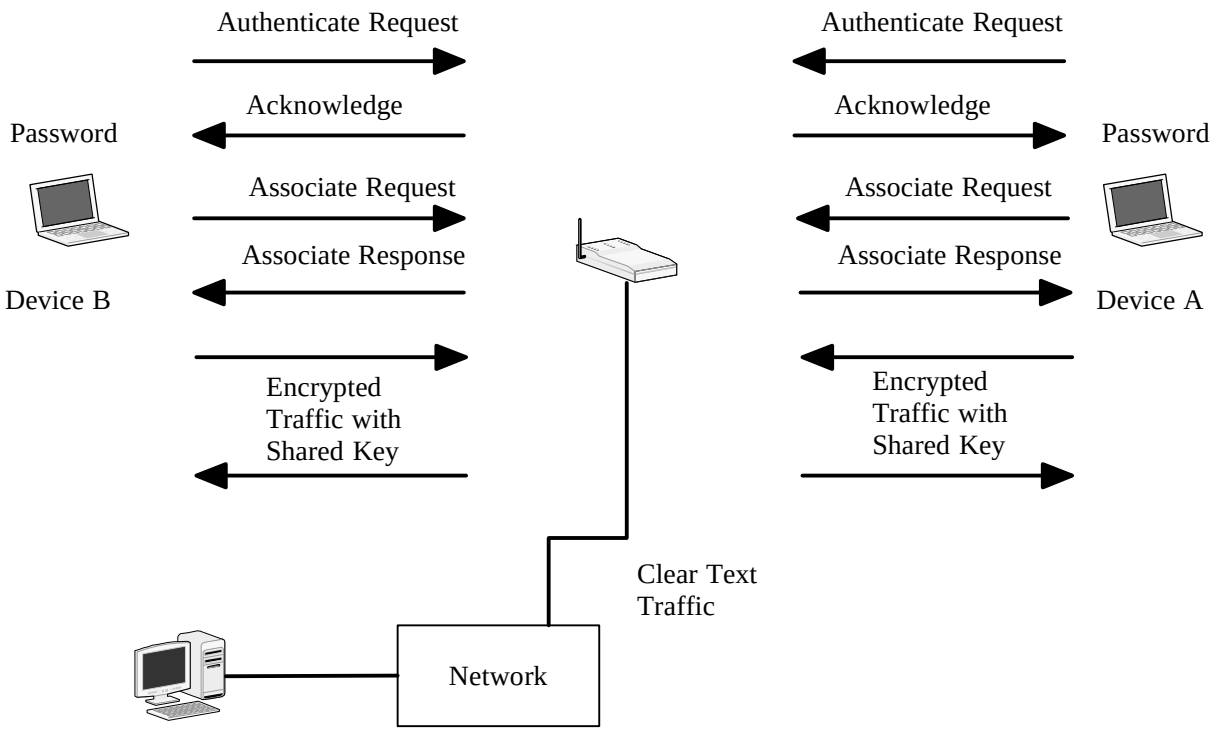
Traffic Based

- Ethernet controllers can be set in promiscuous mode which enables them to sniff traffic
- Broadcast traffic can cause flooding

Wired Equivalent Privacy (WEP)

- Shared keys
  - 40 bits
  - 128 bits
- Can be cracked if enough data is seen
- Aircrack will find a WEP key

WEP



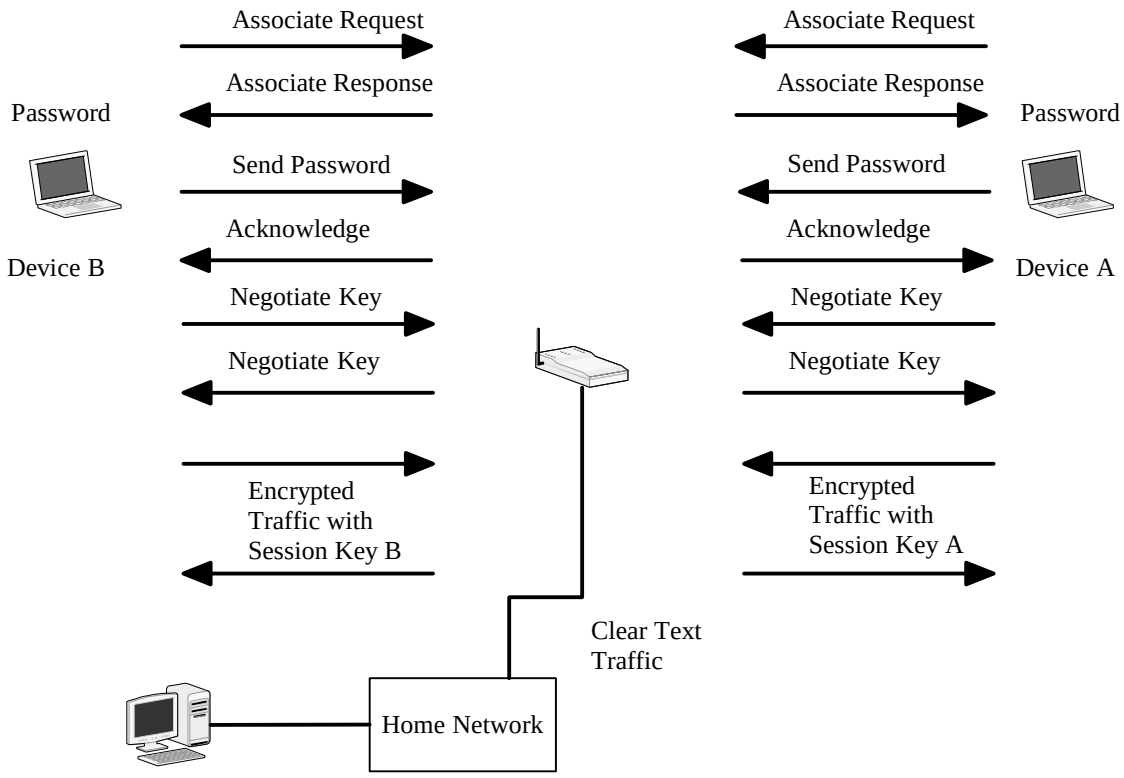
Wi-Fi Protected Access (WPA)

- Uses 802.1X + Extensible Authentication Protocol
  - Authentication with an auth server
- Encryption
  - Rc4
  - AES (WPA2)

WPA2 – Home use

- Uses a shared password for authentication
- If mobile password matches AP then encryption keys are exchanged
- New keys for each new association

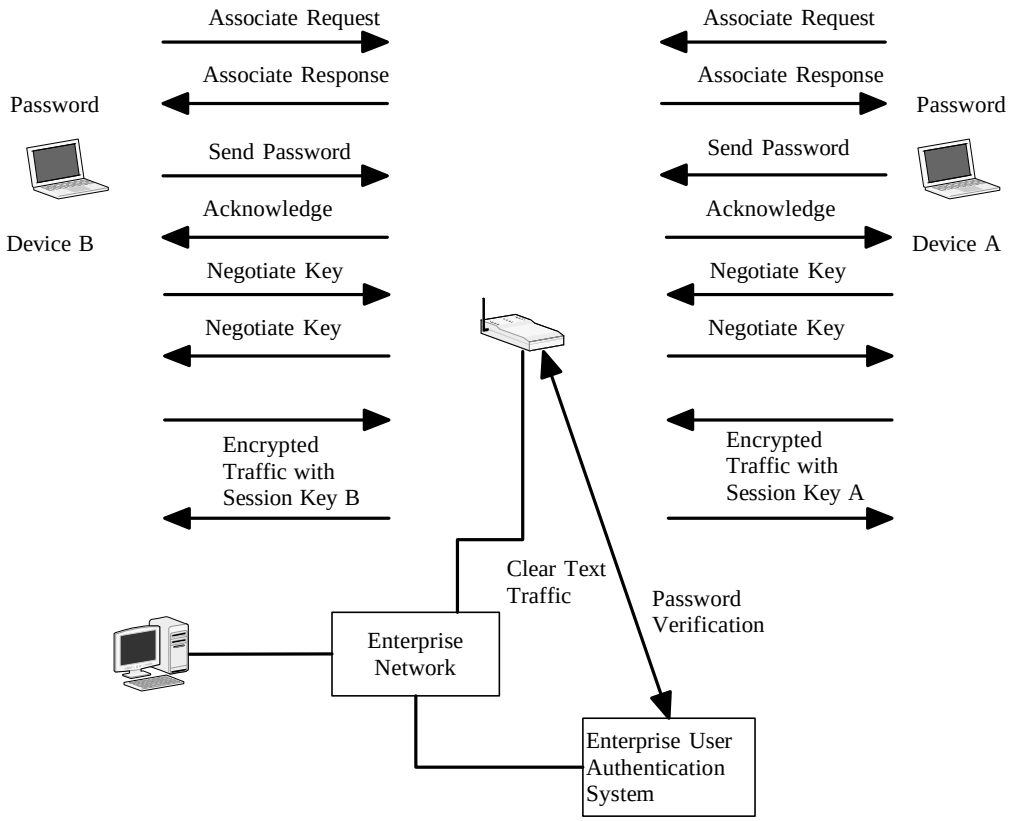
Home-Based WPA2



WPA2 – enterprise

- Mobile associates with AP
- Mobile authenticates with auth server (using 802.1X)
- Authentication server distributes keys to AP and mobile

Enterprise WPA2



Wireless (A world without perimeters)

- Wireless can create a new perimeter
  - Know access points
  - Unknown access points
- Treat your wireless access points the same as you would any remote access to your network.
  - Monitor it
  - Filter it
  - Protect it

Why is Wireless different?

- Most security models are based on a strong perimeter around an organization
- Wireless signals are not confined to the walls of an organization
- Wireless technology is plug and play
- Security makes wireless harder to use.

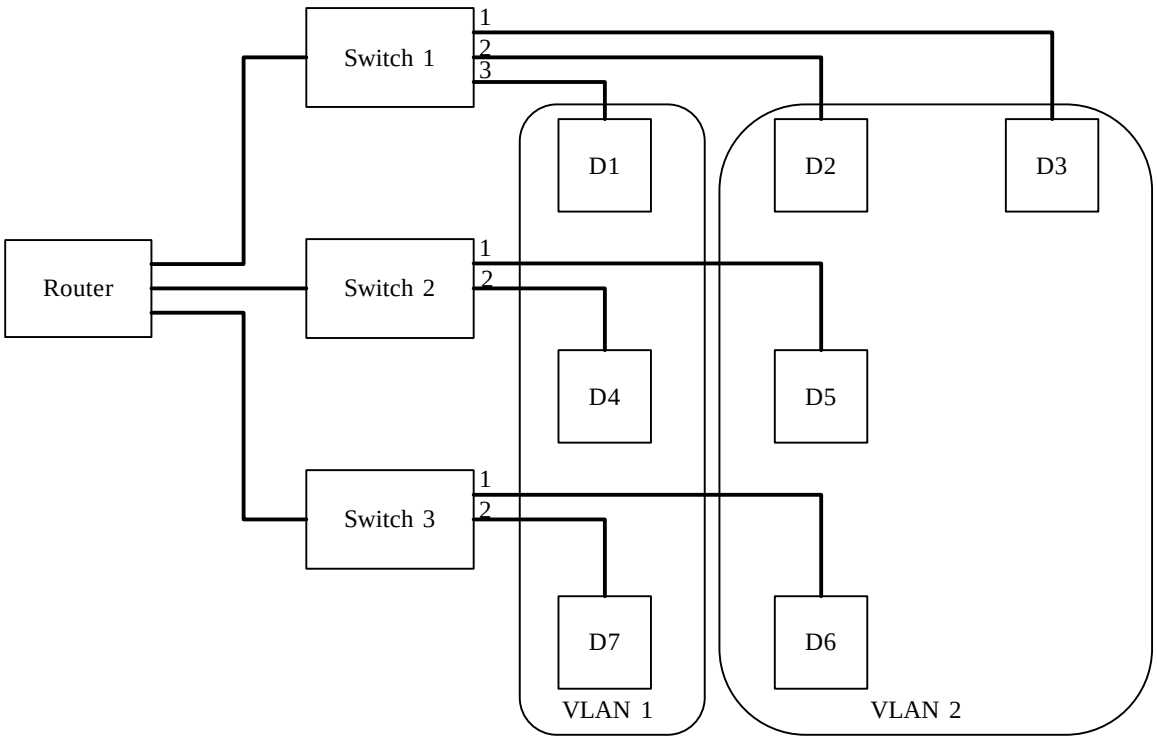
How to secure your wireless network

- Control your broadcast area
- Enable WEP, use WPA2 if possible
- Disable SSID Broadcast
  - More work to setup clients
- Change default AP settings
- Don’t choose descriptive SSID
- Restrict associations to MAC addresses

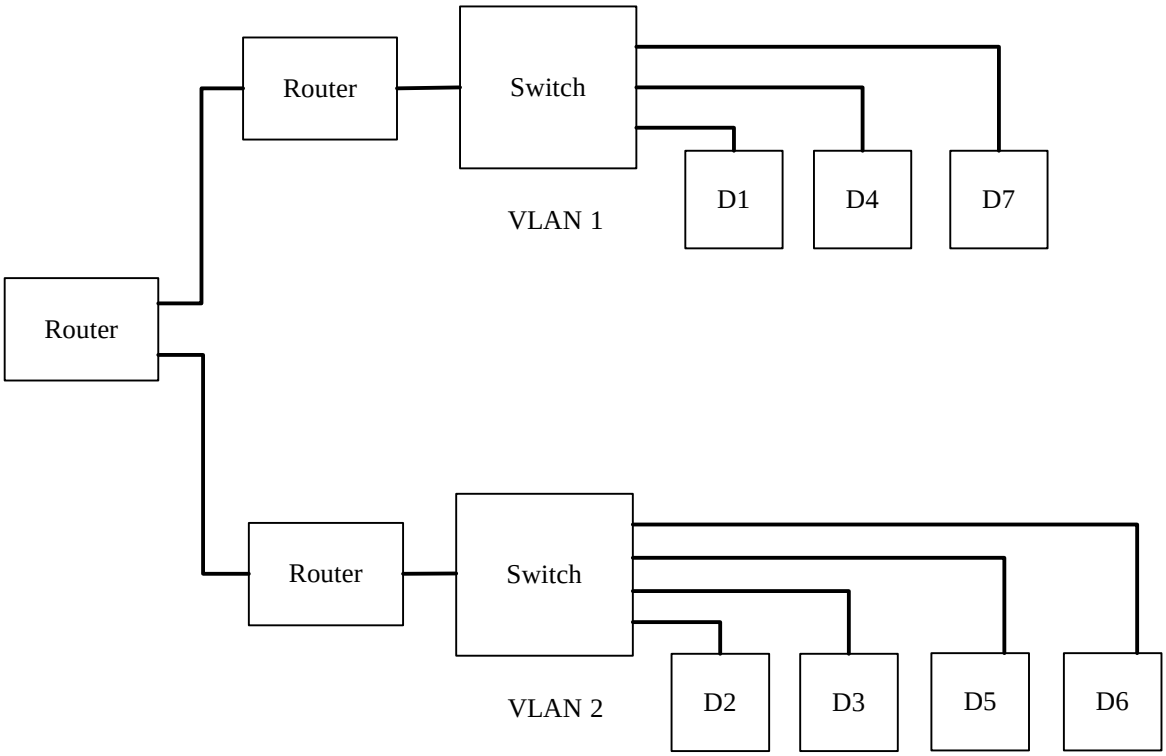
VLAN

- Virtual Local Area Network
  - Creates virtual networks where traffic is isolated between each VLAN based on the hardware address
- Two types
  - Static: each port on the switch is part of a VLAN
  - Dynamic: VLAN assignment is based on hardware address

VLAN



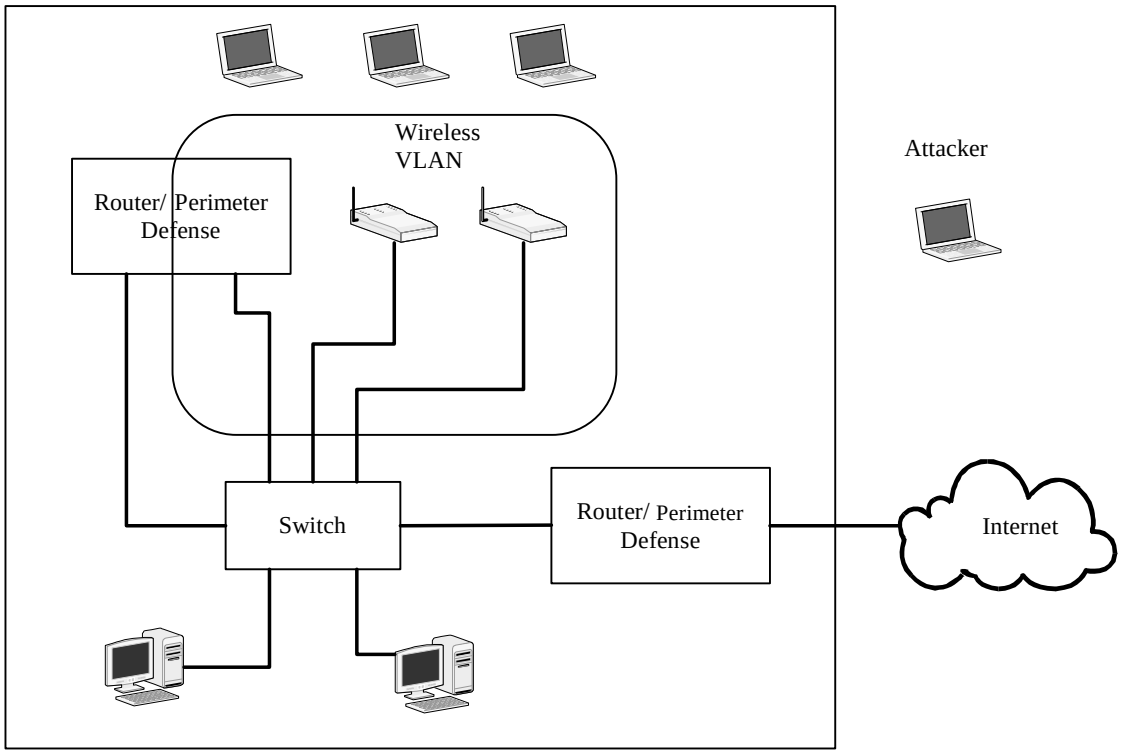
Logical View of VLAN



VLAN Security

- A VLAN will separate traffic, but will not protect devices inside a network from other devices in the same network
- Dynamic VLAN can be fooled by changing the MAC address
- Can help in wireless security

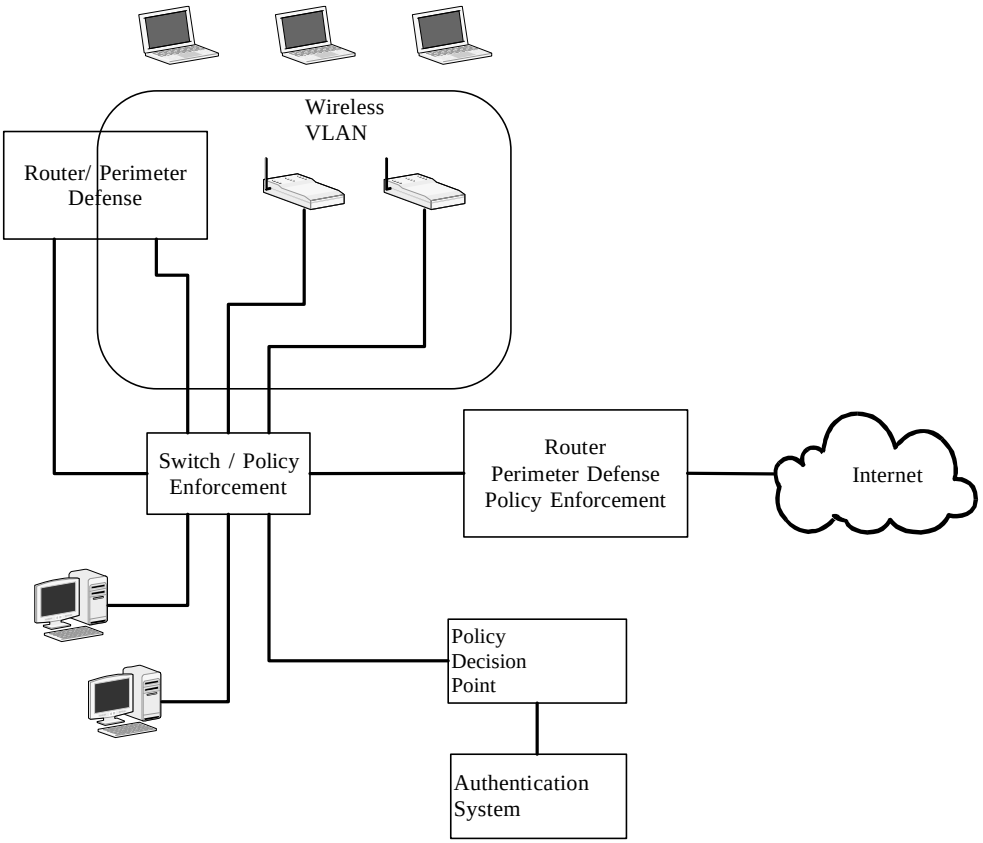
Wireless VLAN



Network Access Control

- Only allow trusted devices on the network
- A host has software that involves an assessment of the host (virus software, etc.)
- Hosts asks policy server if it can use the network
- Network will enforce the policy (limited or full access)

NAC Framework



NAC

- Limited use today
- Focuses on misconfigured or infected devices

Physical Network Security

- Protection methods are limited to local network
- Provides limited security