ECE 435 – Network Engineering
Lecture 32

Vince Weaver

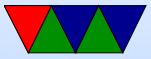
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

17 April 2026

Announcements

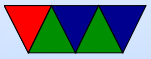
- HW#10 was due
- HW#11 will be posted
- Project status reports due
  - One e-mail per group
  - One-line summary of project topic
  - Brief update on how it is going
  - Whether you're willing to present on Monday / Wednesday / Friday



Wireless Services

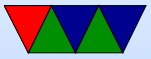
Must provide 9 services

- Intracell for dealing with things outside of a cell
  - Association – allow stations to connect to base stations. When arriving announce its identity and capability
  - Disassociation – either side may break the association, should do it before shutting down
  - Reassociation – can change preferred base station, useful for handover (but best-effort)



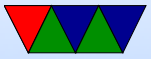
- Distribution – determines best way to route frames
- Integration – in case frame needs to be sent through a non-802.11 network

- Intercell
  - Authentication – check password
  - Deauthentication – to leave network
  - Privacy – encryption
  - Data delivery – modeled on Ethernet, no guarantees frames will get in



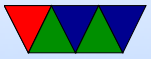
Encryption

- Important as anyone can eavesdrop, even from a distance
- https://arstechnica.com/gadgets/2019/03/802-eleventy-who-goes-there-wpa3-wi-fi-security-and-what-



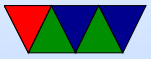
Authentication

- Three states: not authenticated, authenticated but not associated, authenticated and associated
- device sends probe requests. Advertise data rates and what version of 802.11 supported. BSSID of ff:ff:ff:ff:ff:ff so all access points that hear it will respond
- if an access point (AP) supports a common data rate, it will respond with SSID, data rate, encryption mode, etc
- device chooses an access point and authenticates.

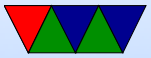


Originally this would have been WEP, but deprecated so often happens in open and usually succeeds. Device sends a 802.11 open authentication frame, seq 0x01

- AP responds saying open with seq 0x02
- if AP receives frames other than auth or probe from device, responds with a deauth to make it start over
- A device can be authenticated to multiple APs but only associated with one
- device determines who to associate with and requests

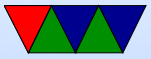


- AP responds and creates association ID
- once associated then WPA/WPA2 has to happen still before data can flow



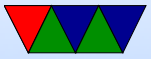
WEP (obsolete)

- WEP – Wired Equivalent Privacy
  - Used RC4 and CRC32
  - Deprecated 2004
  - Meant to be 64 bit originally, but 40 due to export limitations
  - Later 128-bit. Can enter in hex or ASCII chars
  - Can be cracked fairly quickly these days (10 mins on a laptop)



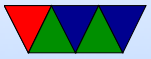
WPA (Wi-Fi Protected Access)

- Also broken, obsolete in 2008
- 802.11i – Temporal Key Integrity Protocol (TKIP)
- 64 or 128 bit encryption key
- TKIP replace CRC, harder to crack, RC4
- Generate new key each packet



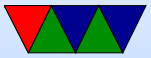
WPA Personal vs Enterprise

- WPA-personal
  - Pre-shared key (PSK), AKA the password
  - 128 bits derived from 256 bits
  - If ASCII, PBKDF2 applied and then SSID used as salt (to prevent rainbow tables)
- WPA-enterprise
  - Like eduroam
  - more complicated key setup
  - Authentication via 802.1X server, RADIUS, PEAP



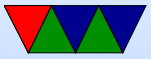
WPA2 (Wi-Fi Protected Access II)

- Key exchange Broken in 2017
- IEEE 802.11i-2004
- Uses AES
- 4-way handshake
  - AP sends random number (ANonce)
  - Client sends own (SNonce)
  - AP calculates PTK from that, encrypts
  - Client decrypts with PTK. If works, good
- PTK key for unicast, GTK for broadcast



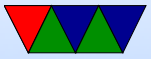
WPA3 (2018)

- 802.11-2016
- Replaces PSK (pre-shared key exchange) with SAE
- Simultaneous Authentication of Equals instead of pre-shared key
- Supposed to help with weak passwords, and also configuring devices without displays
- 802.11w – protection of management frame



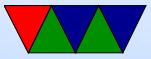
WPA Password Issues

- Rainbow tables possible (pre-compiled tables that can speed breaking encryption, made with common passwords and SSIDs)
- WPA/WPA2 can try to crack weak passwords offline
- WPA3 need active connection to network to do it
- WPA/WPA2 lack of forward secrecy, once password broke can decrypt all future and past traffic
- Possibly if you share WPA password then anyone who knows password can decrypt

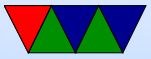


Encryption Issues

- Past security issues with WiFI:
- KRACK attack (key reinstallation attack)
  - Issue on Linux machines, Ironically had issues for too closely following IEEE standard
  - 4-way WPA2 handshake
  - You can resend 3rd way of handshake with the key, and other side will accept it (in case it was lost) and re-start encryption from beginning
  - This leads to same key being used to encrypt multiple

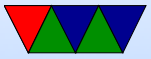


frames
  - That makes reversing the key trivial
- Frag attack
  - `https://lwn.net/Articles/856044/`
  - (fragmentation bit is outside of the encrypted/protected, so by messing with that you can get rogue chunks of encrypted data inserted into frames)

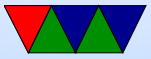


Other Security Issues

- Packet sniffing
- Easier to tap into a network undetected. Long range antennas
- Malicious association – go into an area with own access point that machines will connect to
- MAC spoofing, set your MAC to an existing machines
- Denial of Service – flood the router so it can't respond

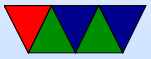


- Deauthentication attack– continually spoof an "I'm leaving" packet from all MAC addresses on network
- Hide you SSID? How effective is that?
- Encryption breaking, see long list of issues on WPA Wikipedia page



Wifi network setup

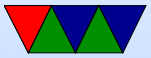
- Simple like at home, you have a password and share it with people you trust
- Automated, like at airport. Connect with no password, but stuck on private 10.0.0.x network with DNS pointing only to own server. You have to make account / pay money / etc which will then add your MAC address. Then re-connect and then it lets you through
- Enterprise. Have to set up key file and maybe authenticate with username/password



Transmission Power

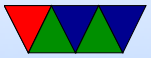
- 802.11b signal typically around 32mW
- Often use dBmW (often shorted dBm) where 0dBm=1mW
- 1dBm = 0.001258925W
- Convert -68 dBm to Watts
  - $P = 1W * 10^{P_{dBm}/10}/1000$
  - -68 dBm = 160pW

- Convert 1W to dBm



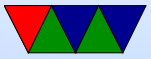
- $P_{dBm} = 10 * log_{10}(1000 * P_W/1W)$
- 1W = 30dBm

- Juno space probe (13 Oct 2016)
  - 8.4GHz, received -135.75dBm (2.7e-20kW) 18kb/s (math is right. why report kW not W though?)



Channels

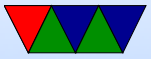
- 802.11b, DSSS 2.4GHz, 2412MHz as first channel, 14 channels 5MHz apart 1-14.
- 802.11g same as 802.11b when talking to b, but a modes when talking to other g
- 802.11a 5GHz band, channels 1-199 starting at 5005MHz 5MHz apart
- CMSA/CA – uses RTS/CTS. 802.11g needs to do this if 802.11b present, slowing things down 20-50%



Linux Interface

- In old days “iwconfig” or “iwlist”, deprecated
- On debian at least, install “iw” package
- /usr/sbin/iw dev – show devices
- sudo /usr/sbin/iw wlp1s0f0 scan

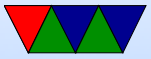
```
wlan0     IEEE 802.11abg  ESSID:"Whatever"
          Mode:Managed  Frequency:2.452 GHz
                        Access Point: 00:1C:10:11:B4:C6
          Bit Rate=54 Mb/s   Tx-Power=200 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:XXXXX
          Power Management:off
          Link Quality=42/70  Signal level=-68 dBm
```



```
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

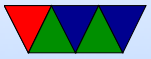
What does some of this mean? RTS threshold: can old do CTS/RTS if file is too big

same with Fragment threshold



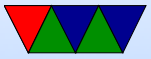
Capturing 802.11 packets

- Is it possible to gather raw 802.11 packets, like you can with ethernet/tcpdump?
- Tricky. Often wireless networks restrict raw access to the transmitter/receiver for regulatory issues (don't want random code on computer able to blast out radio signals that could interfere with shared network)
- There is a special "monitor" mode you can put some wifi cards into
- Only some of my machines support it



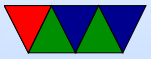
- For pi3/pi4 there are custom firmware replacements (nexmon) that in theory enable it plus other hacking

```
# Find out name of wifi device
sudo /usr/sbin/iw dev
# Replace wlan0 here with what the previous command reports
# Device must be down
sudo /usr/sbin/iw wlan0 set type monitor
then use wireshark
# Return to managed mode
sudo /usr/sbin/iw wlan0 set type managed
```



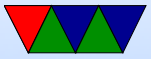
Bridging

- How do you connect together multiple groups of machines into one big LAN?
- An interconnection at the link layer is called a MAC bridge, or bridge. Also a Layer-2 switch
- IEEE 802.1D
- Transparent bridge, as users are not aware of them
- Bridge acts in promiscuous mode (receives every frame on the LAN) so it can find ones that need to forward on across the bridge



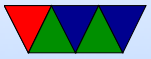
Terminology Review

- repeater – purely electronic, resends voltages (original Ethernet allowed four)
- hubs – frames coming in one port sent to all others
  creates a collision domain
- bridge – connects two or more LANs. Each line own collision domain
  can maybe bridge different types of networks (Ethernet/token, wired/wireless)
- switch – point-to-point frame routing, sort of like one



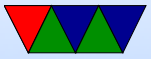
bridge per port

- router – higher layer, strips off frame headers and looks at packets, then generates new frame headers when it routes to other network



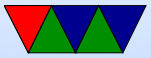
Bridging Diagram

- Some switches are just a bunch of ethernet cards, bridged together, possibly just running an embedded OS like Linux
- TODO: diagram
- Can also bridge in software, can bridge emulator/VM to external network port
- Linux `br0` device

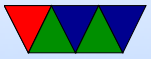


Backward/Self Learning

- Want switches to be able to find any ethernet device on network automatically without having to configure it
- How does bridge learn the MAC addresses?
- It watches for frames coming in and their source address. Puts in table.
- How does it learn where destination is? It broadcasts to all. Once the destination also sends a frame (so its source is known) then the switch updates its table and no longer broadcasts.

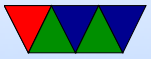


- How do you handle machines that are moved? Aging mechanism. If not heard from for a while, expire the table
- Multicast or Broadcast, can follow GMRP or GARP to limit how far it is broadcast



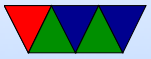
Bridge vs Switch

- Before 1991 a switch was a bridge (in the standard)
- In 1991 Kalpana made a "switch" and differentiated it by cut-through instead of store and forward
- Store and forward – whole frame received before resent larger latency, no problem with broadcast, can check FCS
- cut-through – can start transmitting before receiving completely (destination MAC at beginning). Slightly better latency, broadcast not possible, too late to check



FCS

- These day most are store and forward



Switch Implementation

- Can implement in software with an OS like Linux
- Multiple ethernet cards
- Use operating system bridge support to bridge the interfaces together