IT 609
Network and System Administration

Wireless

Thursday October 21, 2021

Wireless

Wireless Advantages

No wires!

Mobility

Low cost compared to running cable through existing buildings, labs, classrooms

Wireless Distribution System (WDS) can be setup to provide coverage of very large areas (e.g. UNH)

Excellent for home and small office networking - easy!

Wireless Disadvantages

Speed

- Any wireless technology will always be slower than a contemporary wired one

Reliability

- Interference and signal loss

Capacity

- Shared medium

Security

Radio vs...

Fiber optic

- Most secure, hardest to tap into
- Fastest
- Expensive

Copper cable

- More secure than radio
- Faster
- Costs vary depending on installation

Wi-Fi

Wireless LAN standards

aka IEEE 802.11

"Wi-Fi" is the marketing name

Radio transmission from a NIC to an access point that is attached to a wired network

Can also create ad hoc computer-to-computer networks

Wi-Fi vs. Ethernet

CSMA-CA instead of CSMA-CD

CA - Collision Avoidance = wait if the network is busy

Cannot do CD since a station cannot receive (listen for collision) at the same time it sends

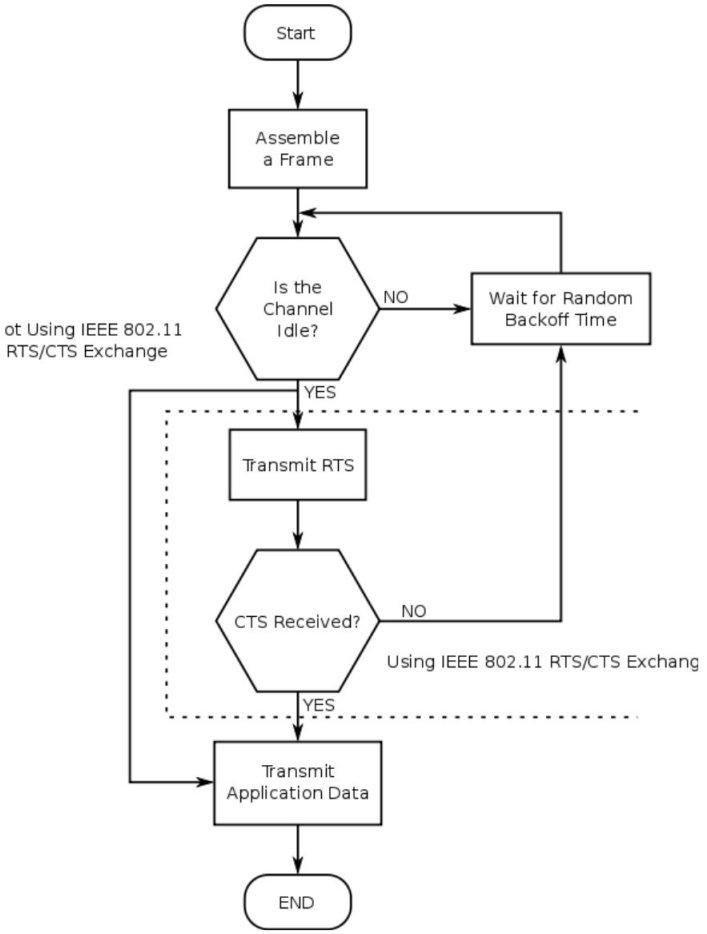
RTS/CTS - Ready to Send/Clear to Send

Acknowledgements - receiver acknowledges each frame received

CSMA/CA

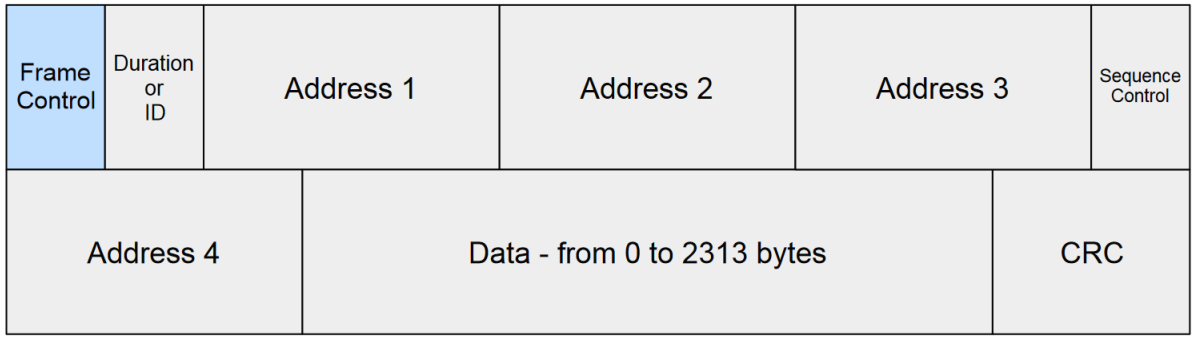
1. Wait for the network to be idle (CS).

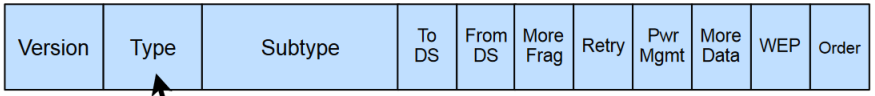
2. Send an RTS signal first and wait for a CTS back before sending actual data. (CA)



By jjgarcia.tsc [Attribution], via Wikimedia Commons http://upload.wikimedia.org/wikipedia/commons/1/1d/Csma_ca.svg

Wi-Fi Frame





Management, Control, or, Data

DS=Distribution System
Address values vary depending on DS bits

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	AP's Air Address	N/A
0	1	Destination	AP's Air Address	Source	N/A
1	0	AP's Air Address	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

~~802.11b~~ - Wi-Fi 1

1999

Transmits on 2.4 GHz frequency

Speed at 11 Mbps shared

Standard range of 300 feet

Speed decreases to 5.5, 2, and 1 Mbps as distance increases

~~802.11a & 802.11g~~
Wi-Fi 2 & Wi-Fi 3

Faster standards - both 54 Mbps shared max

1999

~~802.11a~~ - Wi-Fi 2

- Created at the same time as "b"
- Transmits at 5 GHz - less interference
- Theoretically shorter range (but faster!)

2003

~~802.11g~~ - Wi-Fi 3

- Ratified June 2003
- Same 2.4 GHz frequency as "b"
- Backwards compatible with "b"
- Equal or better theoretical range

~~802.11n~~ - Wi-Fi 4

Finally ratified
9/11/2009

2.4 GHz or 5 GHz

Speeds up to 540 Mbps

Based on MIMO

- Multiple input, multiple output
- More than 1 antenna, more than 1 channel
- 4 channels of 40 MHz each possible

Long time in development...2003 to 2009

- "Draft-N" equipment was sold based on Draft 2.0

~~802.11ac~~ - Wi-Fi 5

Approved
January 2014

5 GHz only

Speeds up to 1.3 Gbps (or better)

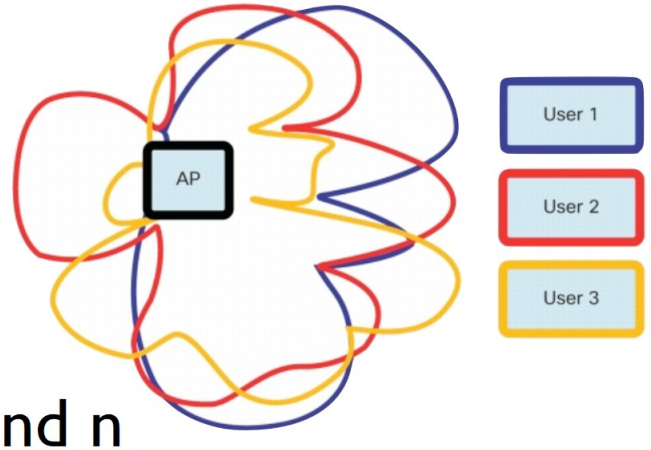
Wider channels

Up to 8 x 160 MHz channels

MIMO & Beamforming

Denser amplitude modulation

Backward compatible with g and n



http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/white_paper_c11-713103.html

~~802.11ac Wave 2~~ - Wi-Fi 5

Approved June 2016

5 GHz only

Speeds up to 2.34 Gbps

Multi-user MIMO = up to 4 devices at once

Up to 8 streams

Broader channels

Backward compatible with g and n

~~802.11ax~~ - Wi-Fi 6

Released 9/2019

2.4 GHz & 5 GHz initially, 1 GHz to 7 GHZ coming

Speeds up to 9.6 Gbps

Access by up to 8 devices (multiple channels) MU-MIMO

Improves device battery life with individualized Target Wake Time settings for each device

Comparison

Standard	Aka	Speed	Frequency
1	802.11b	11 Mbps	2.4 GHz
2	802.11a	54 Mbps	5 GHz
3	802.11g	54 Mbps	2.4 GHz
4	802.11n	540 Mbps	2.4/5
5	802.11ac	2.3 Gbps	5
6	802.11ax	9.6 Gbps	2.4/5/other

Wi-Fi Admin

SSID = Service Set Identifier

- Can be broadcast or hidden

Radio channels

- 2.4 GHz
  - 11 channels, 22 MHz wide, 5 MHz separation
  - Channels 1, 6, and 11 do not overlap
- 5 GHz
  - 19 (or 20) wider channels (=speed!)
  - Dynamic Frequency Selection

Wireless Pitfalls

Interference - especially at 2.4 GHz

- Cordless phones
- Bluetooth - has been improved on
- Wireless camera systems
- Microwave ovens - http://xkcd.com/654/

Wireless Pitfalls

- Blocked signals
  - Non-RF transparent materials
    - Metal construction
    - Water
  - Higher frequencies (e.g. 5 GHz) do not penetrate as well
- Shared bandwidth
  - More hosts = slower throughput
- Legacy support (802.11a/b) slows things down

Wireless Installation

One Access Point (AP) isn't enough in most cases

Wireless Distribution System (WDS)

- Links AP's together into a seamless network
- Clients are passed between AP's when moving

Access point positioning and quantity are key

Must also account for the number of users likely to be served in a space

Wireless Installation

Site survey

- Fancy test equipment or with just a Wi-Fi equipped computer that shows signal strength
- Check for signal strength, limits of range, dead spots
- Modeling software is also available to optimize placement based on building structure and materials

Add more access points, or relocate them as needed

UNH Wireless Upgrade

Summer 2014

- Added 1008 Access Points
- Goal of "ubiquitous" wireless coverage in academic buildings
- Need to blanket physical space plus accommodate the density of WiFi devices

2565 Access Points at UNH as of Oct. 2014

Additional 255 units monitoring airspace

Wireless Security

Radio communications

- Network medium is shared
- Radio doesn't stop at your wall!

Restrict access based on MAC address

- Can be defeated by sniffing and spoofing

Password protect network

- Password can be easily obtained

Wi-Fi Encryption - WEP

WEP- Wired Equivalency Protocol

Single encryption key can be obtained if enough traffic is captured

Now considered to be insufficient

https://www.youtube.com/watch?v=sJf1w7kosG8

Wi-Fi Encryption - WPA

WPA - Wi-Fi Protected Access

- Corrects WEP security holes
- Continually changing encryption keys and longer keys
- Current standard (WPA2) is aka 802.11i
- Only as good as the quality of the passwords
  - WPA-PSK - Pre-shared key, common for home/small business
  - WPA-802.1X - Enterprise authentication via RADIUS to validate usernames and passwords and/or certificates

WPA2 - KRACK

KRACK

- Key Reinstallation AttaCK
- Not a flaw in the encryption design like WEP
- Flaws in the implementation
  - Keys are exchanged in a 4-way handshake
  - An attacker can replay the 3rd step of this exchange leading to the receiver resetting a value and reusing a security nonce (number to be used only once)
- https://arstechnica.com/information-technology/2017/10/how-the-krack-attack-destroys-nearly-all-wi-fi-security/

WPA3

First releases in June 2018

Individualized encryption - public Wi-Fi

More secure handshake (see KRACK)

Automated setup

Stronger encryption standards

Still not perfect…https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/