RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: TECH-R11

What Every Security Professional Needs to Know About Wi-Fi 6

Dr. Avril Salter, CCNP-Wireless, CCNA-Security

IT training: wireless, network security, packet analysis
Salter & Associates
@AvrilSalterUSA

Session Outline

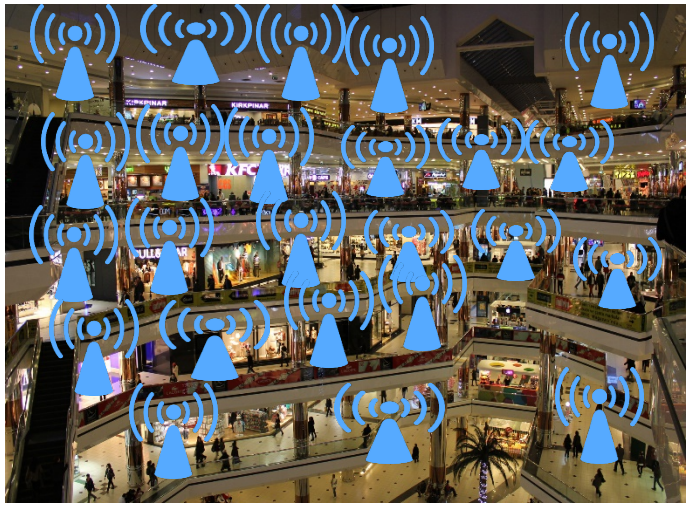
What I am Going to Talk About

- Wi-Fi 6 ~ 802.11ax certification
  - Compare and contrast with
    - 802.11n,ac
    - 5G
- Security considerations
  - WPA3

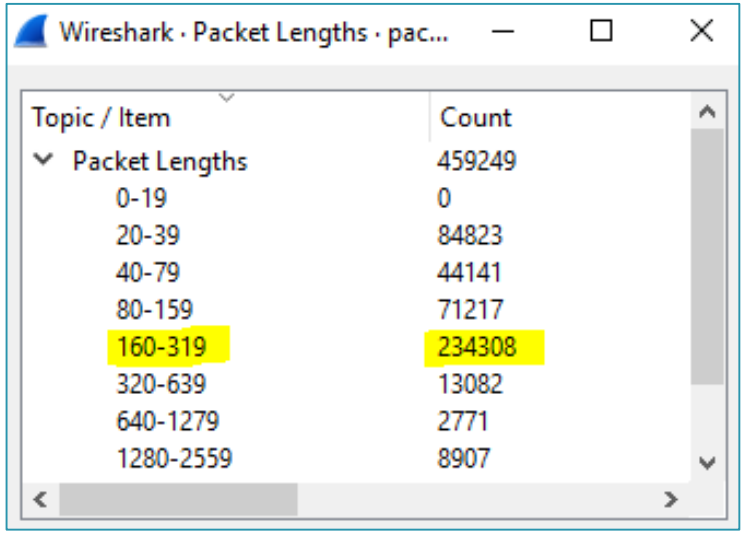
Why You Should Care

- Help you make decisions regarding your deployment or usage of these technologies
- You cannot secure what you do not understand

Where Wi-Fi is Particularly Problematic



Unplanned deployments



IoT traffic

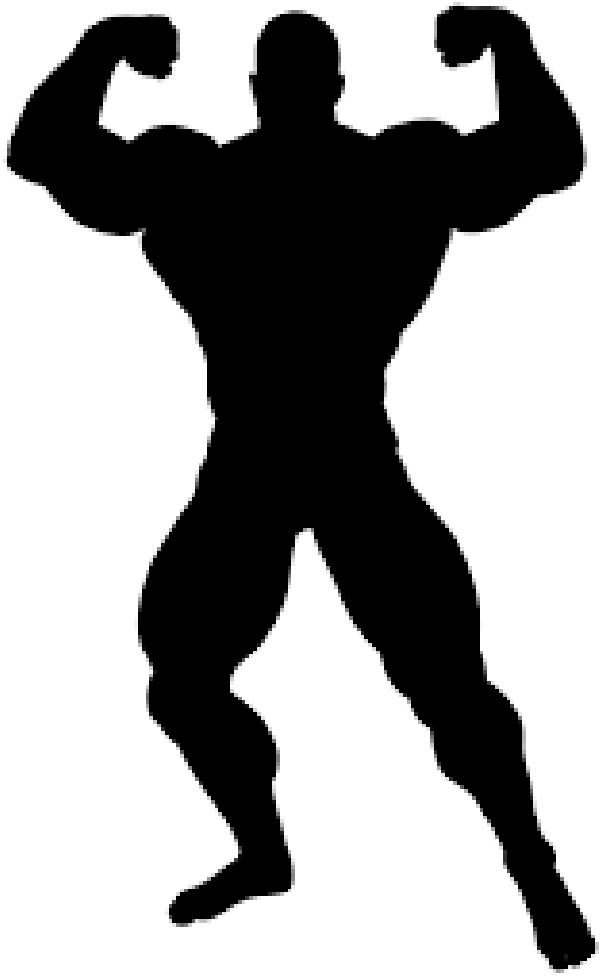
High density of users

802.11ax Builds on 802.11ac

Spectrum efficiency

Power efficiency

Operational efficiency



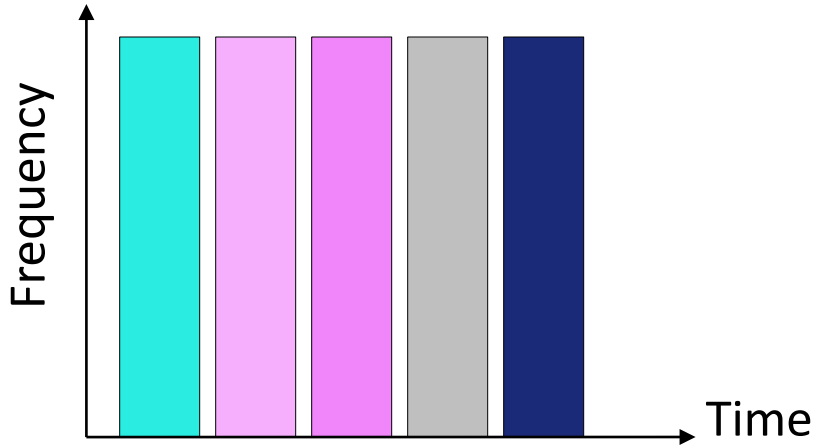
More Spectrum

- 2.4 GHz
  - 20 and 40 MHz channels
- 6 GHz band
  - FCC proposed new rules
  - Significant increase in unlicensed spectrum
  - Over 1 GHz

Multiple Simultaneous Users

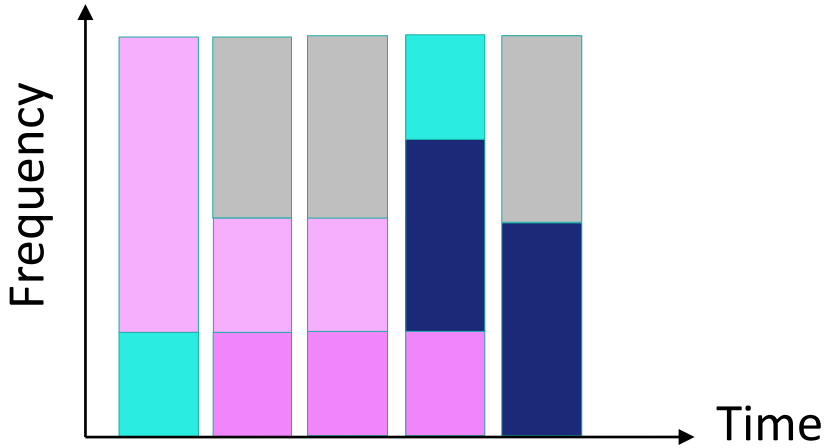
802.11ac
Orthogonal Frequency Division Multiplexing

- Single user transmission
- Collision avoidance mechanisms



802.11ax
Orthogonal Frequency Division Multiple Access

- Multiple simultaneous transmissions
- AP acts as a central controller
  - Allocation of subcarriers



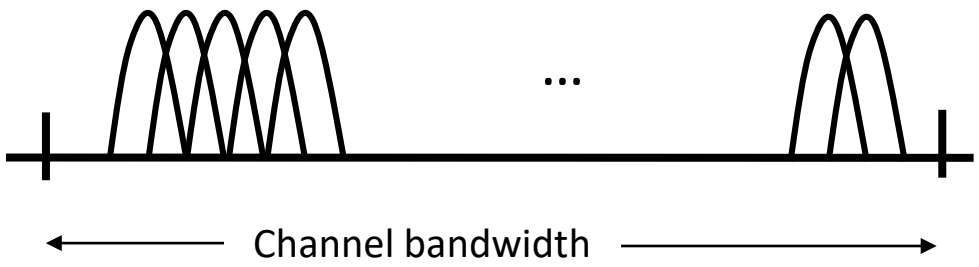
Reduces risk of collisions

Dr. Nril

Smaller Subcarriers

802.11ac

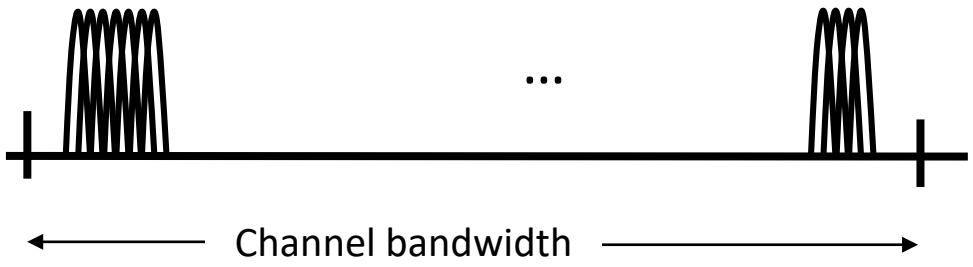
- Subcarrier spacing 312.5 kHz
- 256 subcarriers in 80 MHz channel



802.11ax

- Subcarriers spacing 78.125 kHz
- 1024 subcarriers in 80 MHz band

4X



Devices are Allocated Resource Units (RU)

- Smallest RU is 26 subcarriers

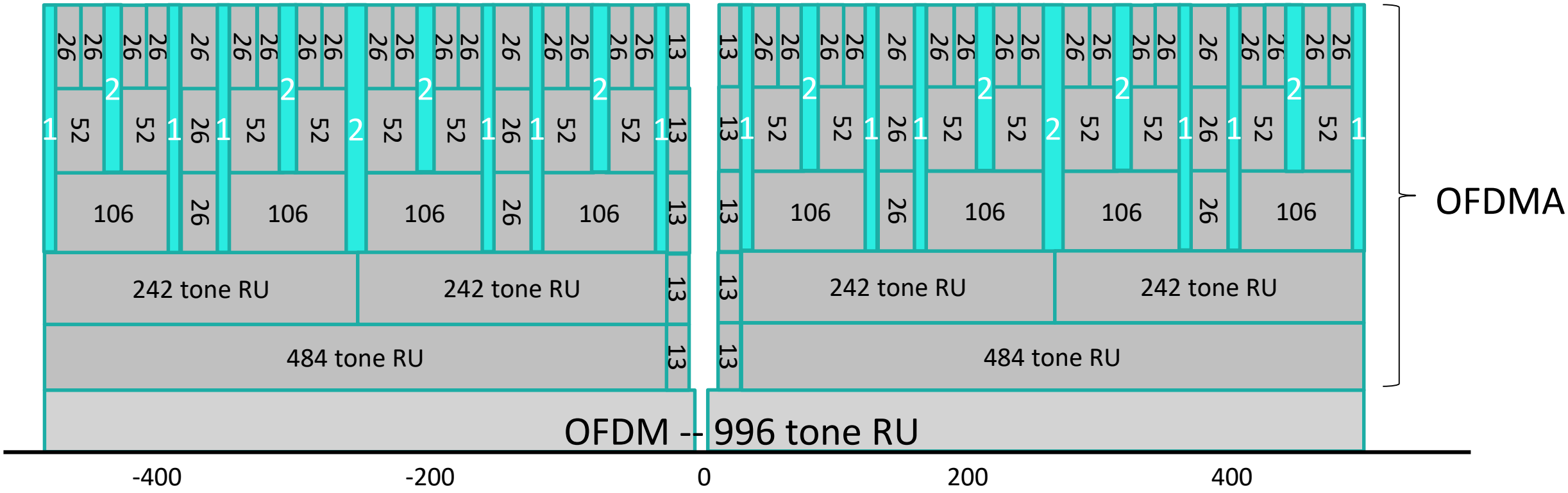


Illustration shows a 80 MHz Channel

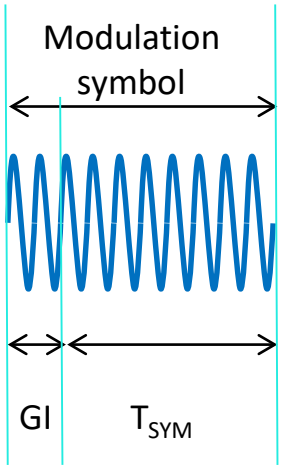
Efficient for different services types

Longer Modulation Symbol Period

4X

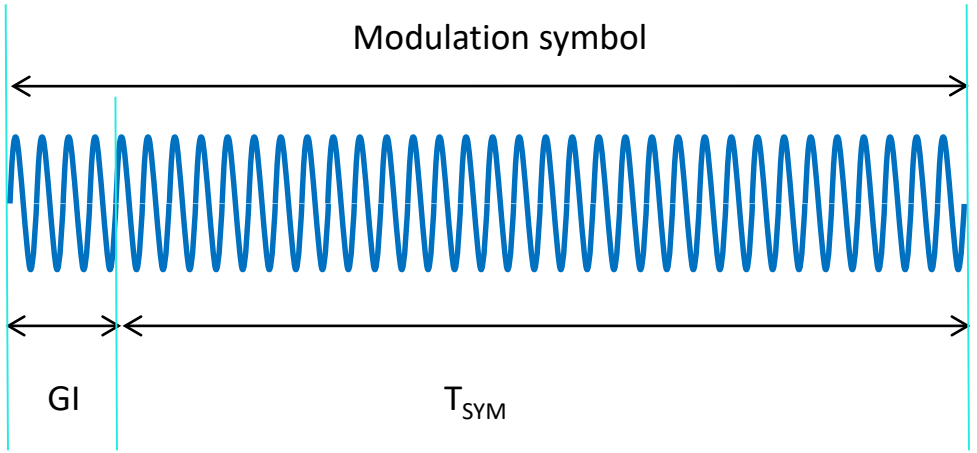
802.11ac

- 3.2 µs symbol duration (T_{SYM})
  - 0.8 or 0.4 µs Guard Interval (GI)



802.11ax

- 12.8 µs symbol duration (T_{SYM})
  - 3.2, 1.6, 0.8 µs Guard Interval



Improves probability of signal reception

Dr. Nril

Data Rate Efficiency

Spectral Efficiency for broadband clients

- More bits per Hertz
- Increases from 433 to 600 Mb/s

Assumes a 80 MHz channel

$$\frac{5}{6}\ \text{FEC} \times \frac{980\ \text{SC}^1 \times 10\ \text{bits per SC}}{12.8\ \mu\text{s IFFT/FFT period} + 0.8\ \mu\text{s GI}}$$

$$= 600\ \text{Mb/s}$$

Robustness and power efficiency for IoT Devices

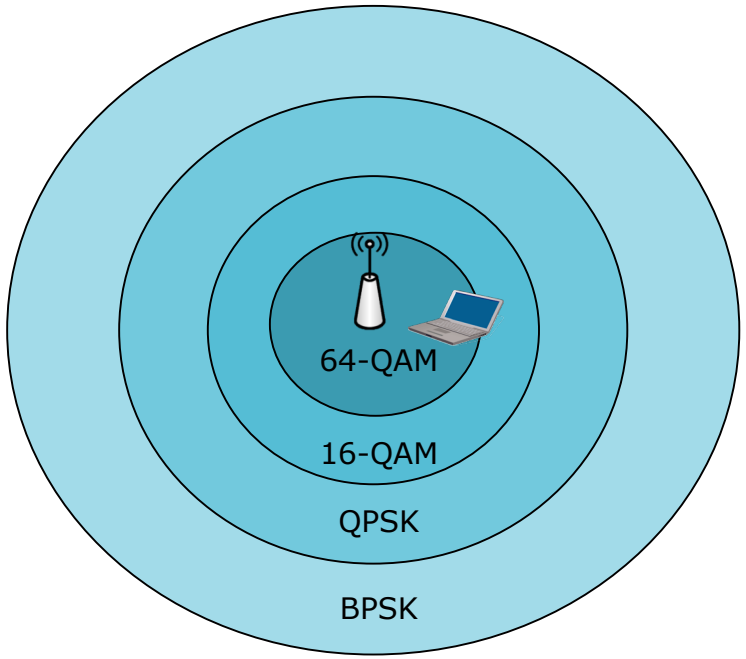
- Allows clients to operate in 20 MHz only mode
- Dual Subcarrier Modulation (DCM)

$$\frac{1}{2}\ \text{FEC} \times \frac{1}{2}\ \text{Rep} \times \frac{24\ \text{SC}^1 \times 1\ \text{bits per SC}}{12.8\ \mu\text{s IFFT/FFT period} + 3.2\ \mu\text{s GI}}$$

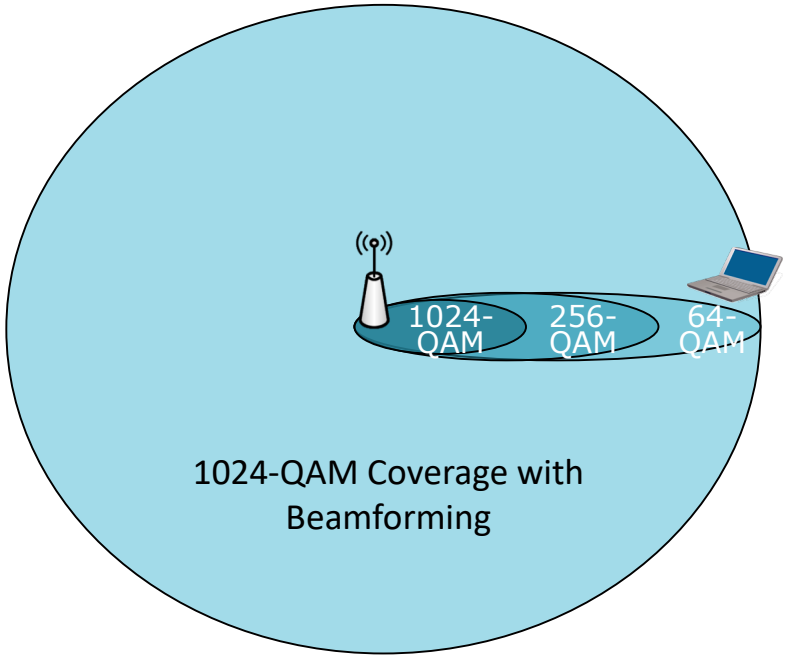
$$= 375\ \text{kb/s}$$

Beamforming Enables Higher Level of Modulation

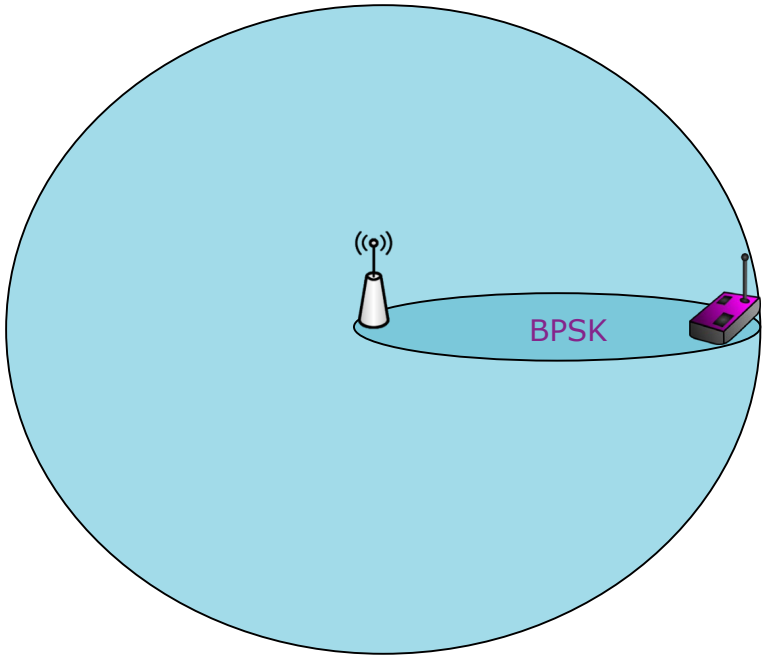
Omni directional antennas



Higher data rates at greater distances



Better battery performance for IoT devices

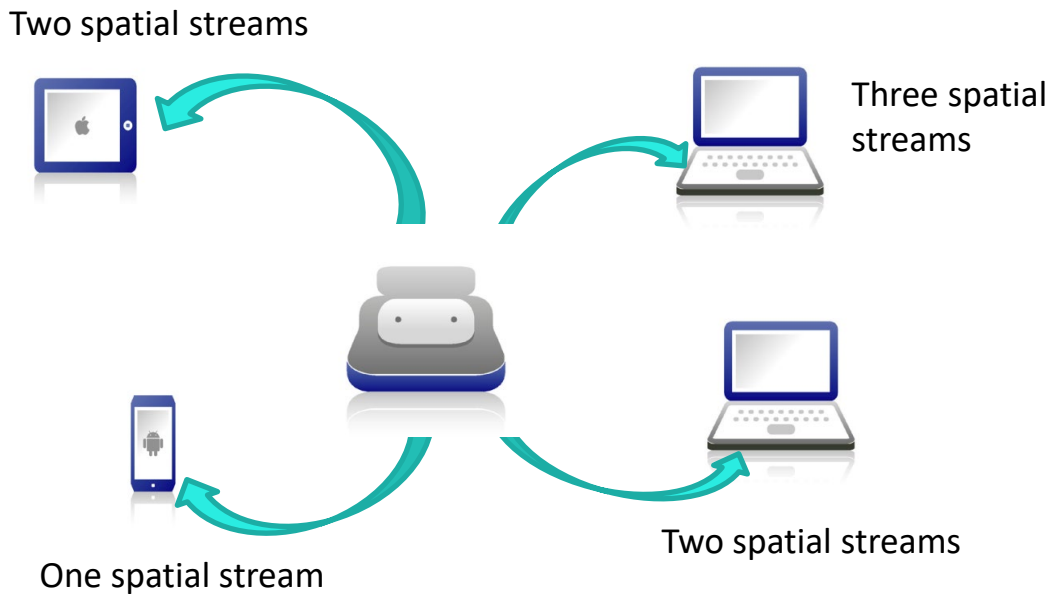


Actual coverage varies with RF conditions

Advances in MIMO Technologies

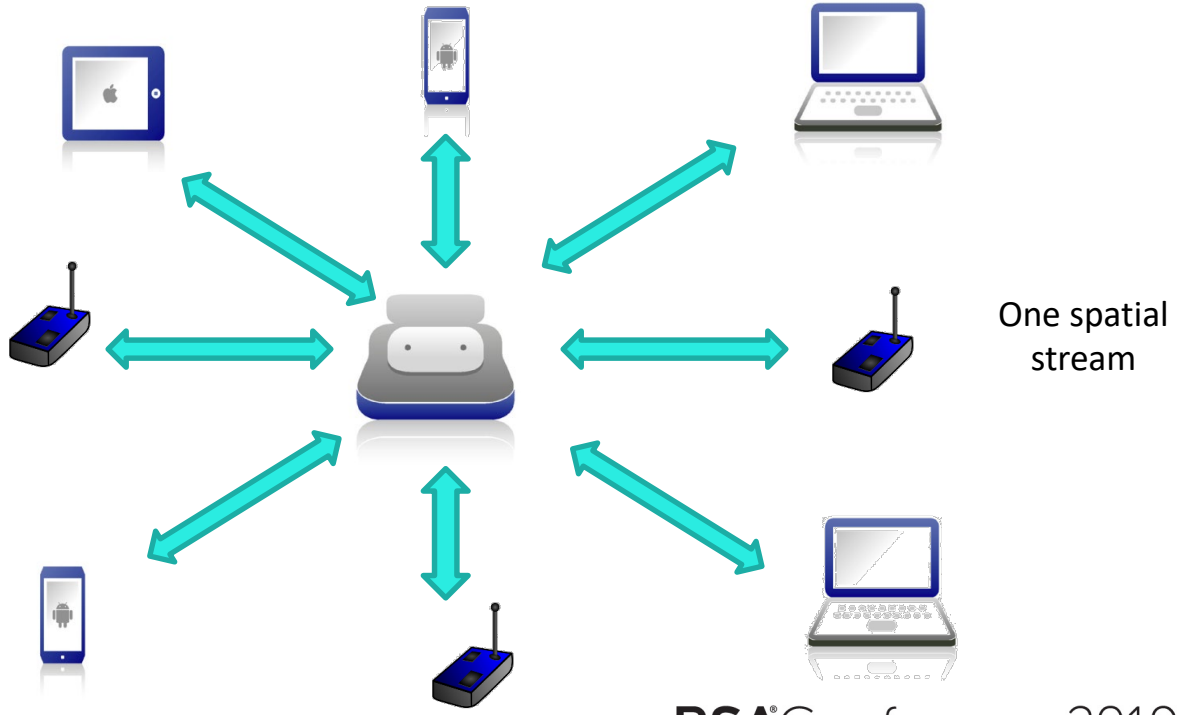
802.11ac

- DL MU-MIMO
  - 8x8 MIMO
  - Maximum of 4 stations



802.11ax

- DL and UL MU-MIMO
  - 8x8 MIMO
  - Maximum of 8 station



Number of Simultaneous Multiplexed Users

- MU-MIMO is supported on allocations sizes ≥ 106 subcarriers

RU size	20 MHz	40 MHz	80 MHz	160, 80+80 MHz
26	9	18	37	74
52	4	8	16	32
106	16	32	64	128
242	8	16	32	64
484	--	8	16	32
996	--	--	8	16
2x996	--	--	--	8

128

Assumes 8x8 MU-MIMO

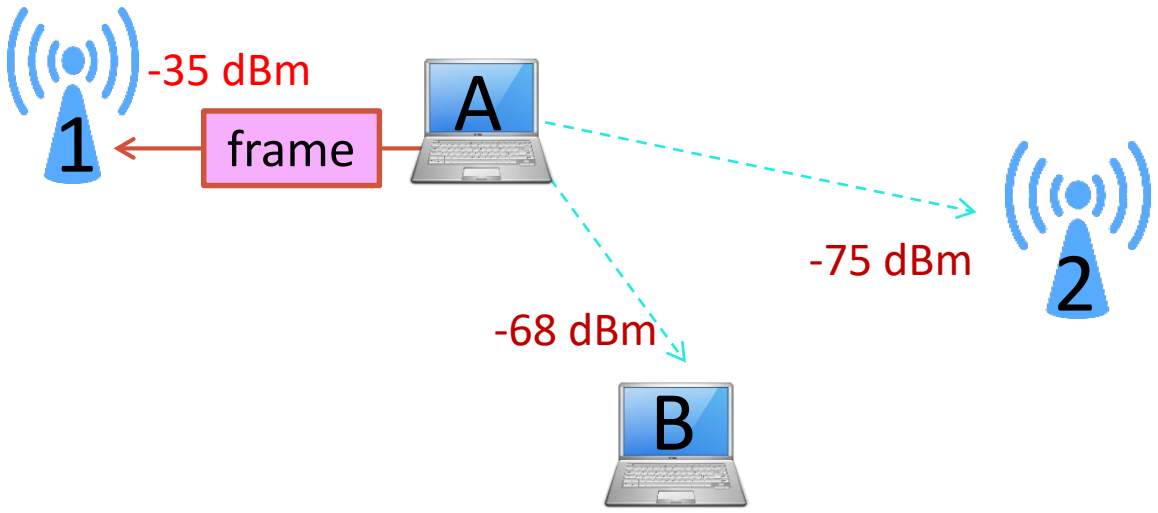
Support dense environments

Dr. Nril

Operational Efficiency

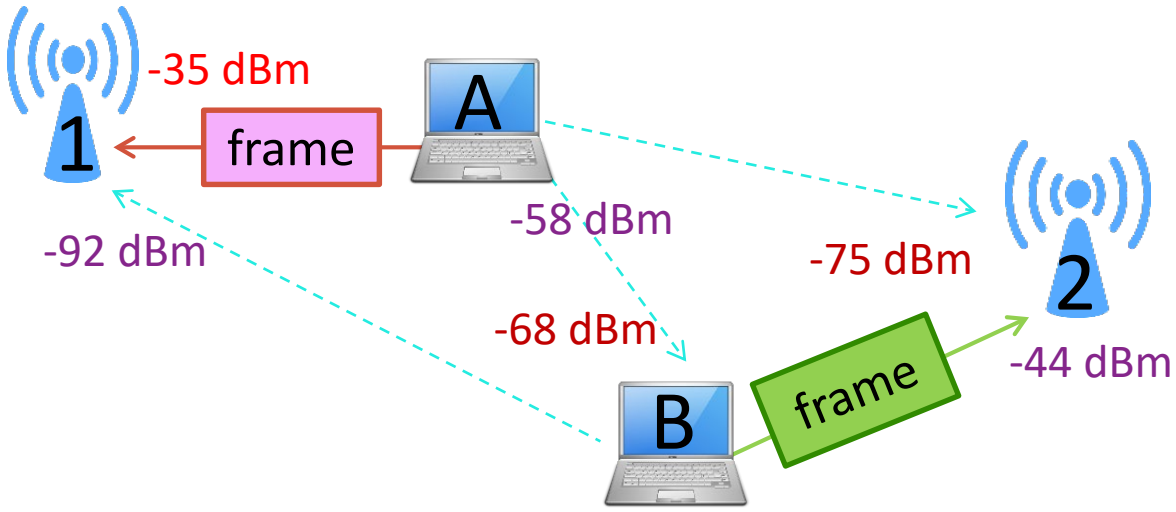
Legacy Collision Avoidance

- STA A transmits to AP
- STA B detects channel busy
- Compares to CS threshold
- Defers transmission



802.11ax Collision Avoidance

- STA A transmits to AP 1
- STA B detects channel busy
- Compares to OBSS CS threshold
- STA B initiated transmissions to AP 2
- At reduce transmit power

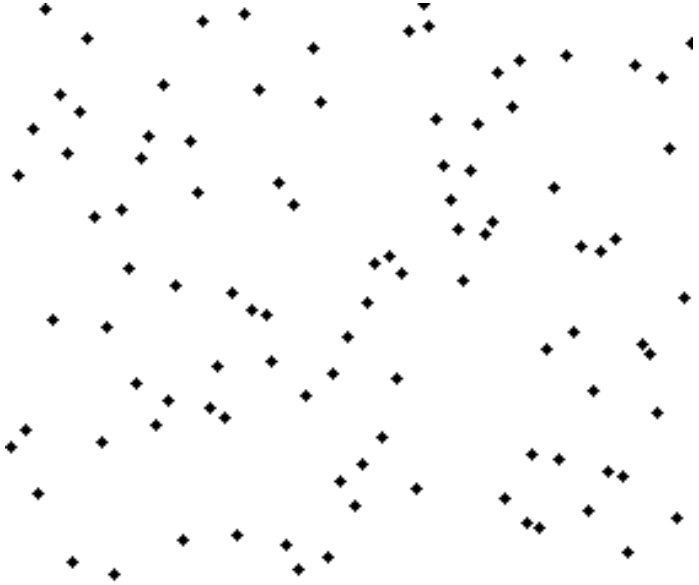


Wi-Fi 6

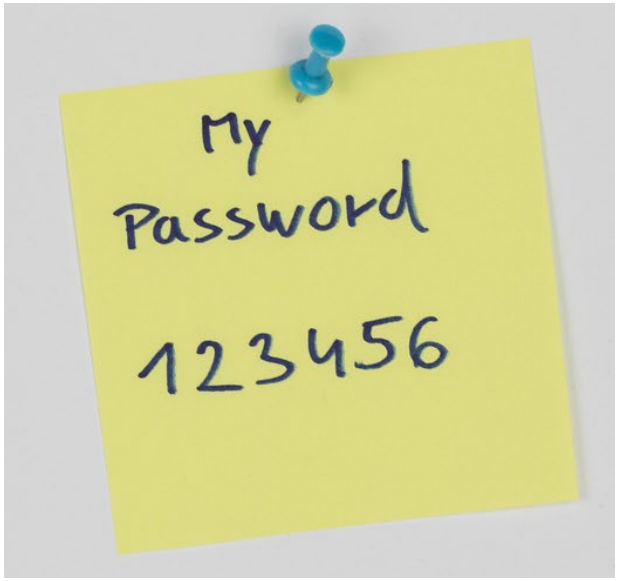
802.11ax
High efficiency
WLAN

Dr. Wireless

Where Security is Particularly Problematic



Variety of cryptographic algorithms



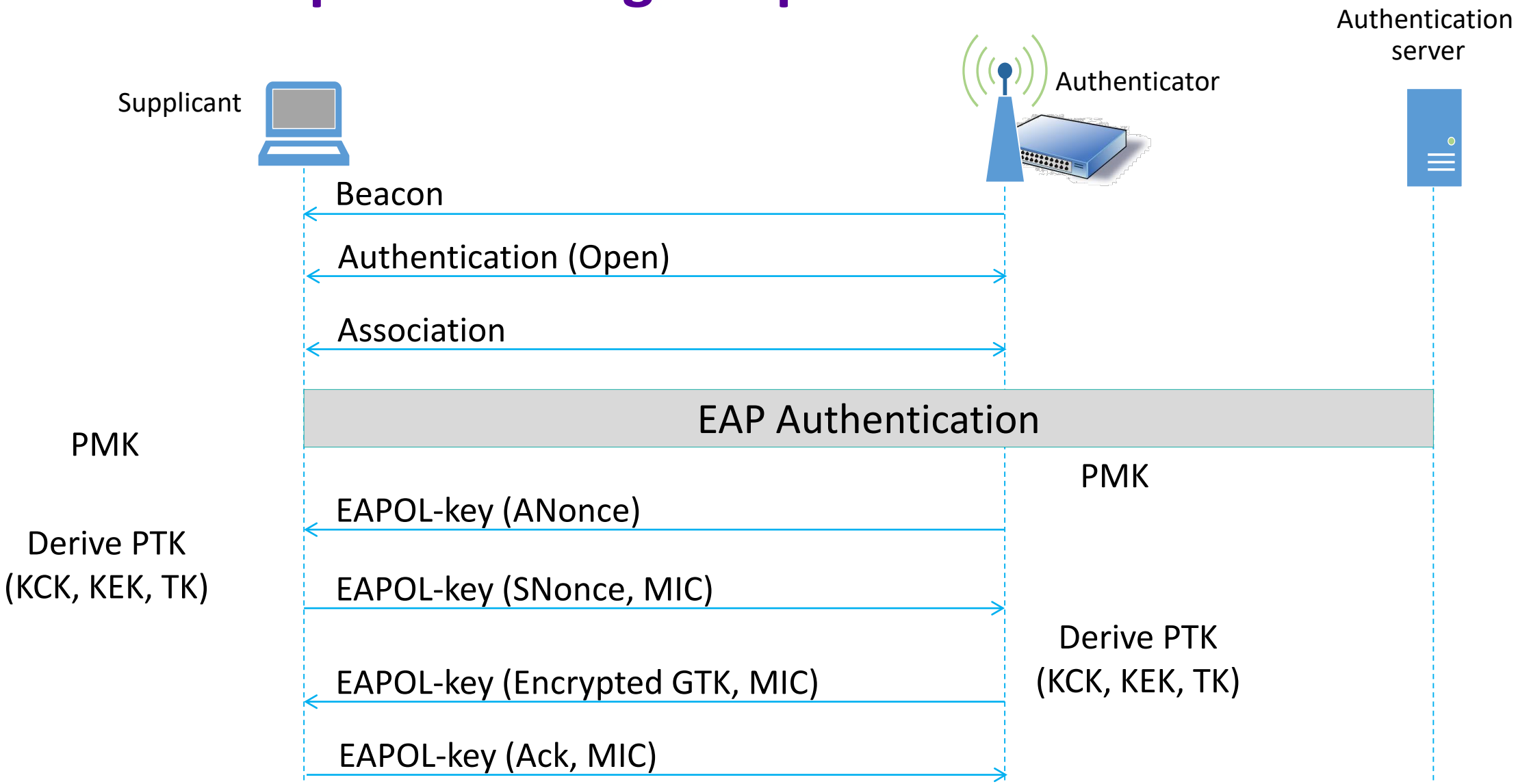
Weak passwords

Open networks

WPA3: An Upgrade to WPA2

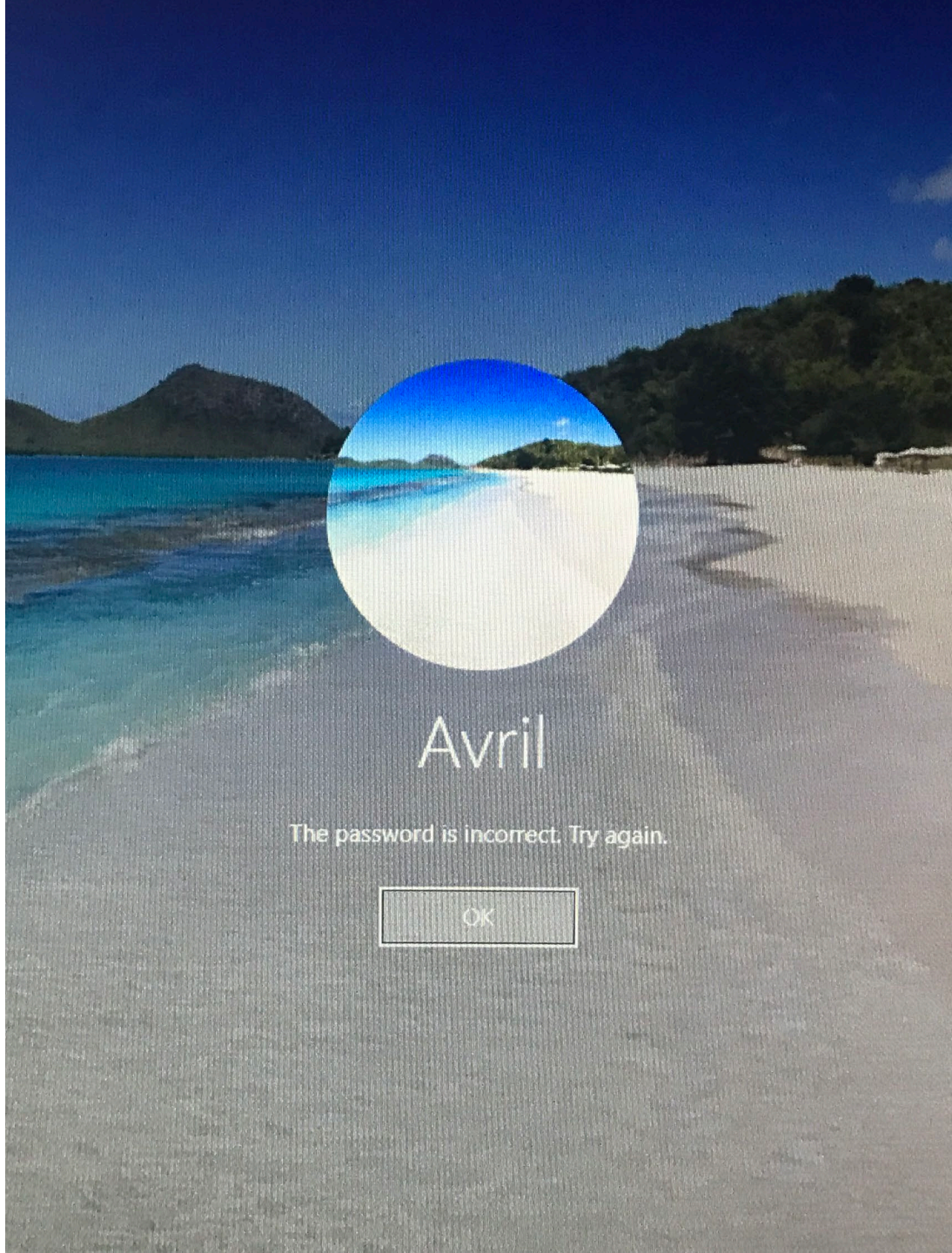
	WPA2		WPA3	
	Personal	Enterprise	Personal	Enterprise
Encryption	128 AES	128 AES	128 AES	192 AES
Authentication	PSK	802.1X	SAE	802.1X
Protected mgmt. frames (PMF)	Not required	Not required	Mandatory	Mandatory

WPA3 Enterprise: Stronger Cipher Suites



I changed all my passwords to
“incorrect”

Now when I forget,
it tells me my
password is “incorrect”.



Overcoming the Impact of Weak Passwords

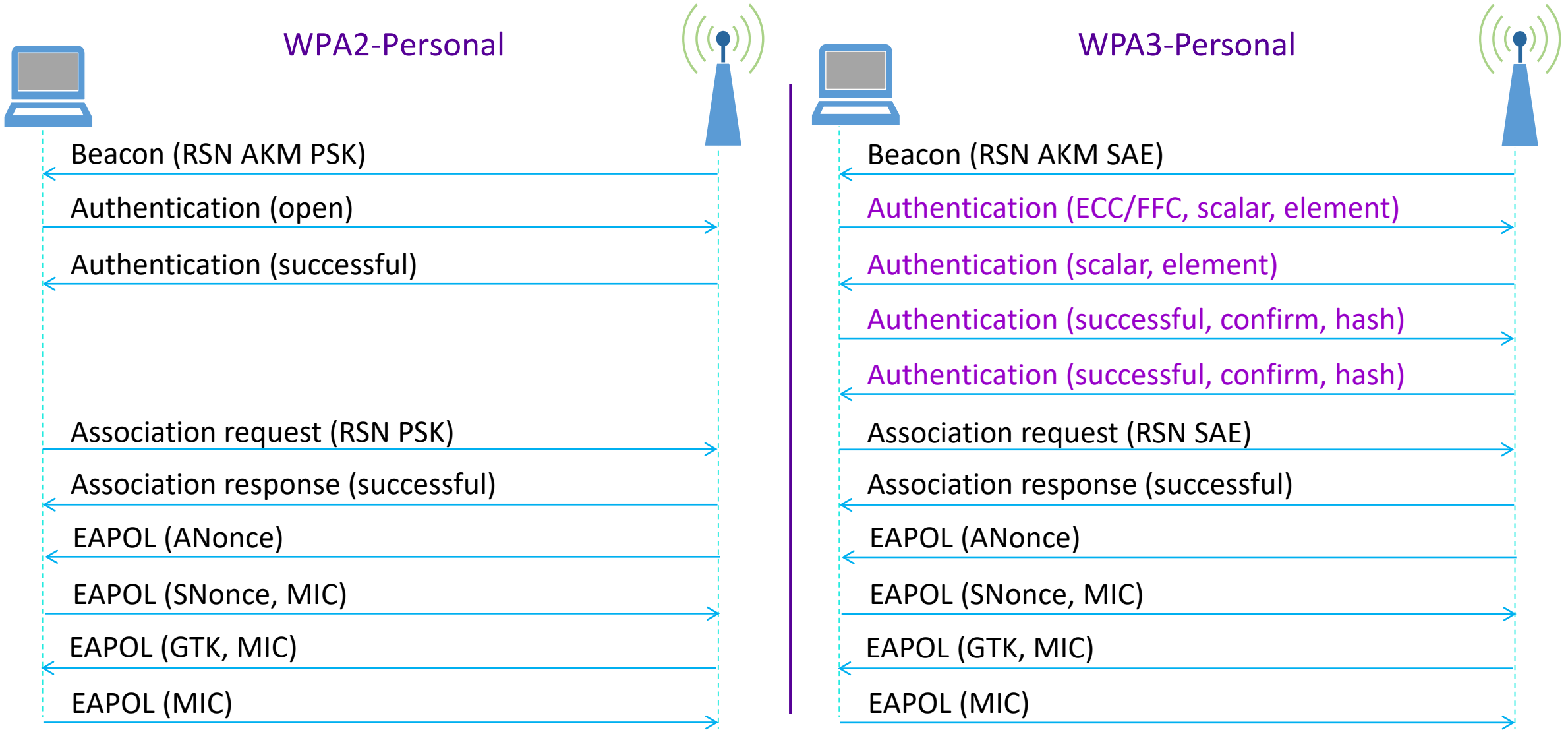


Illustration shows STA initiating SAE

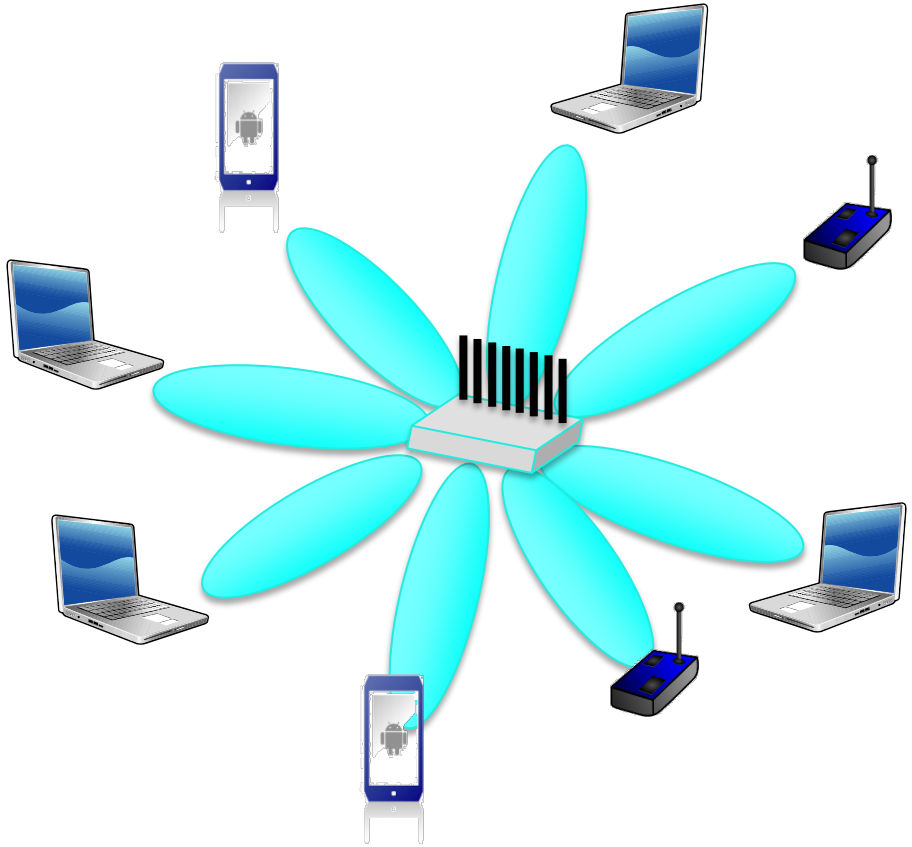
Wi-Fi CERTIFIED™ WPA3™

- Released June 2018
  - Initially optional
  - Expected to become mandatory in future
- WPA3 products
  - Certified products shipping 4Q 2018
  - Broad adoption late 2019
    - In conjunction 802.11ax products
- Probably requires new hardware
  - Not a firmware or software upgrade

Early 802.11ax products lack WPA3

Capture Traffic Transmitted on a Beam

- MU-MIMO makes over-the-air captures of data traffic significantly more complex
  - Transmissions to multiple users
  - On same frequency channel
  - At the same time
- Arguably more secure
- Possible attacks
  - Minimize use of MU-MIMO
    - E.g. Disruptive interference
  - Listen on partial beam



Apply What You Have Learned Today

Now	In a week	In 3 months	In 6 months
Wi-Fi 6 and WPA3 dense and IoT environments	Wi-Fi 6 and WPA3 evolutionary upgrades	Wi-Fi 6 and WPA 3 products starting to ship	Capturing wireless traffic increasingly difficult
Write down 2 or 3 things in this presentation most relevant to you	Assess if Wi-Fi 6 and WPA 3 are important to your organization	Check availability of Wi-Fi 6 and WPA3 certified equipment	Evaluate security impact of legacy devices

Thank you for listening ☺

www.**linkedin**.com/in/**avrilsalter**
Avril@dravril.com
@avrilsalterUSA

WPA3-Enterprise TLS Cipher Suites

Reference Slide

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - ECDHE and ECDSA using the 384-bit prime modulus curve P-384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - ECDHE using the 384-bit prime modulus curve P-384
  - RSA ≥ 3072-bit modulus
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - RSA ≥ 3072-bit modulus
  - DHE ≥ 3072-bit modulus

Encryption for Open Wi-Fi Networks

Back-up Slide

Not part of WPA3

Opportunistic Wireless Encryption (OWE)