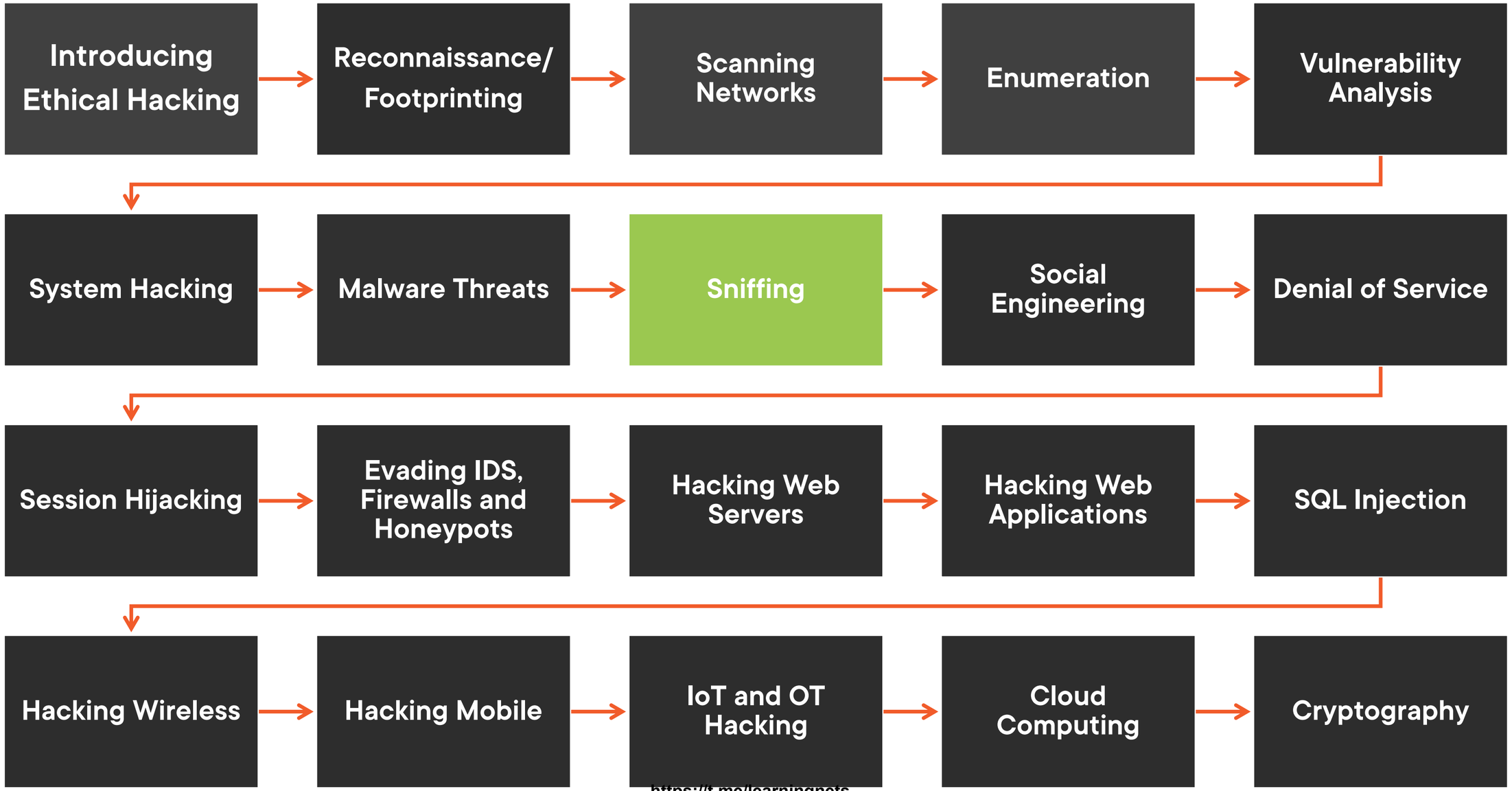
Ethical Hacking: Wireless

Comparing Wireless Terminologies

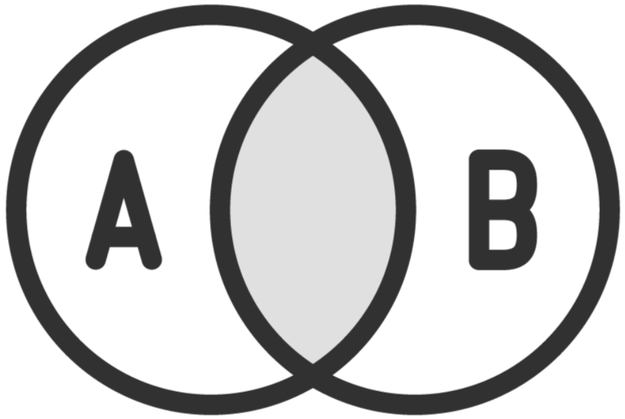
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

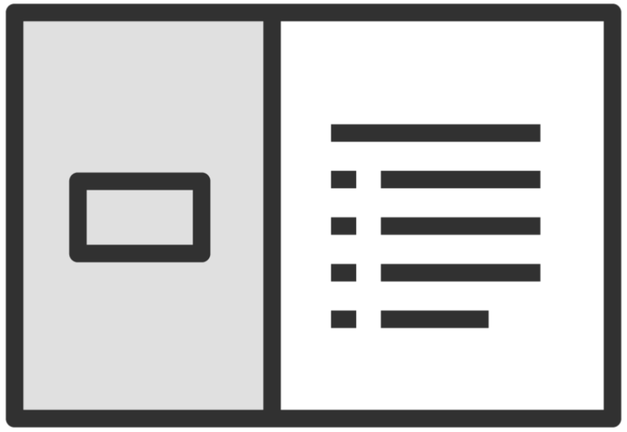
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Ethical Hacking Series

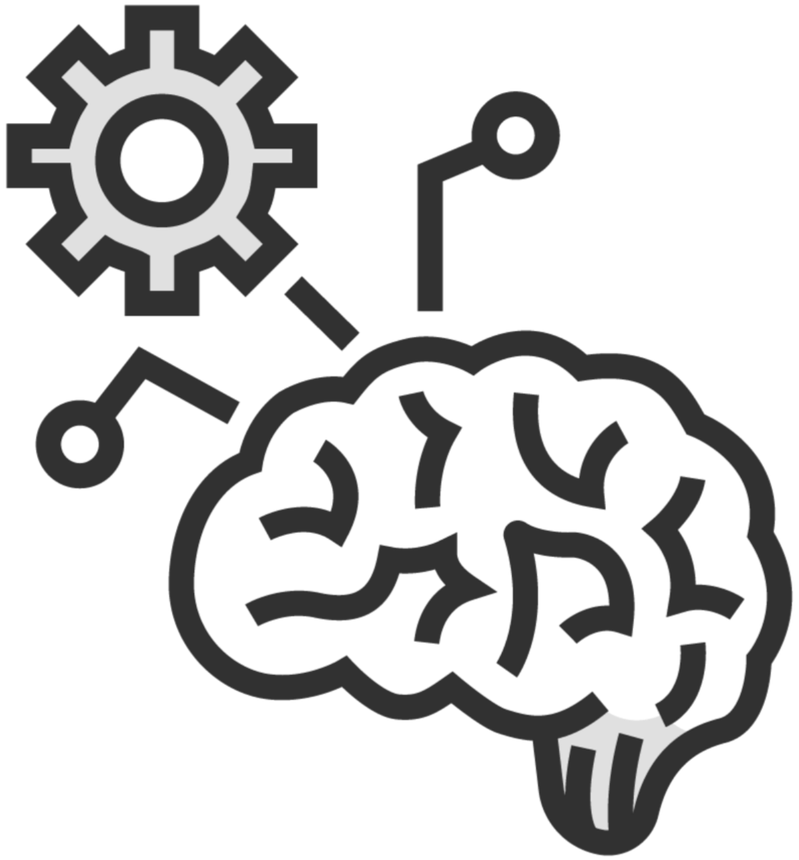


The Method behind My Madness





The Method behind My Madness

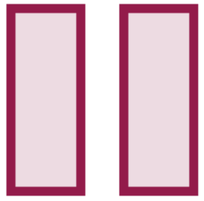


CEH Exam Study Tips

Dale's Study Tips

Study space

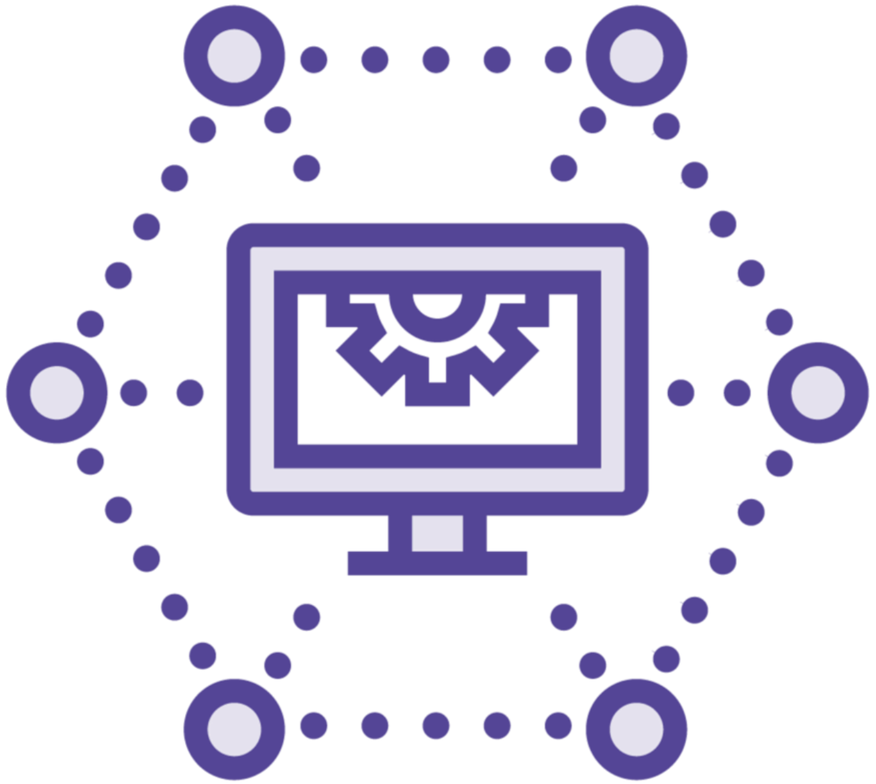
Take notes

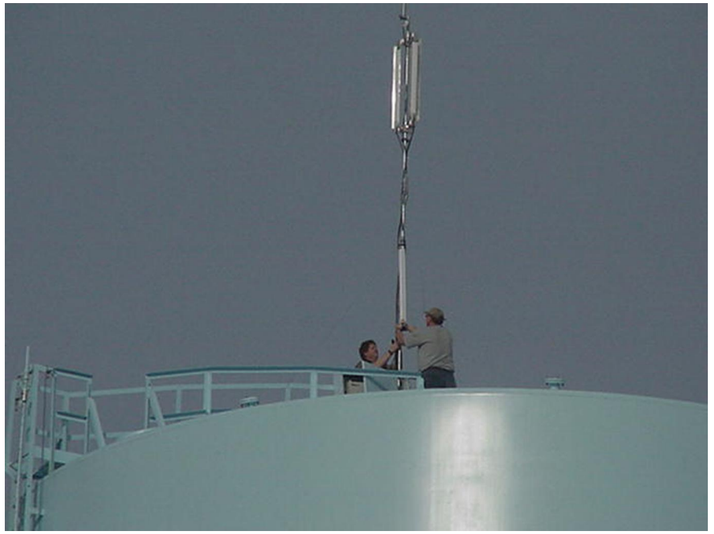


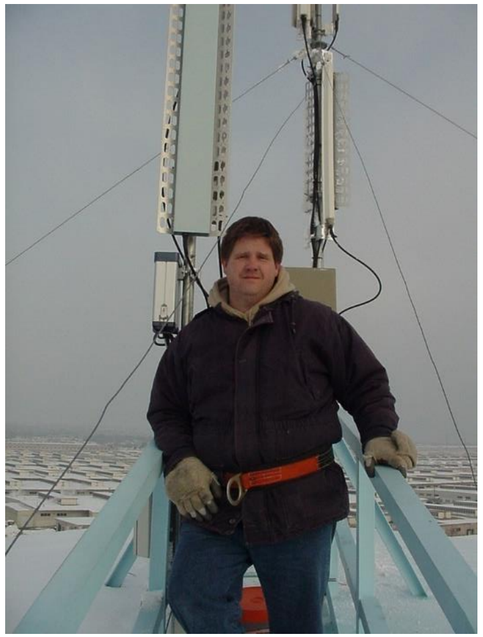
Pause, think, repeat

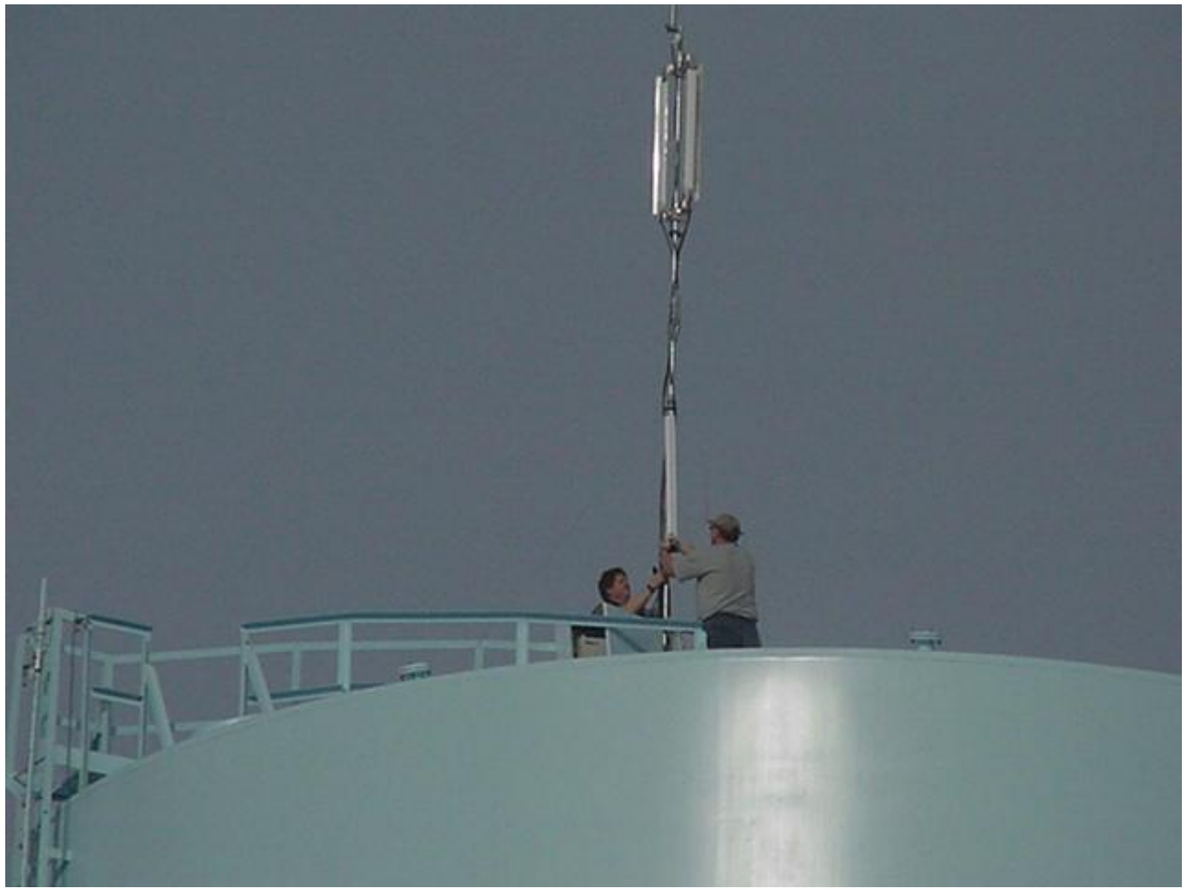
Be kind and rewind

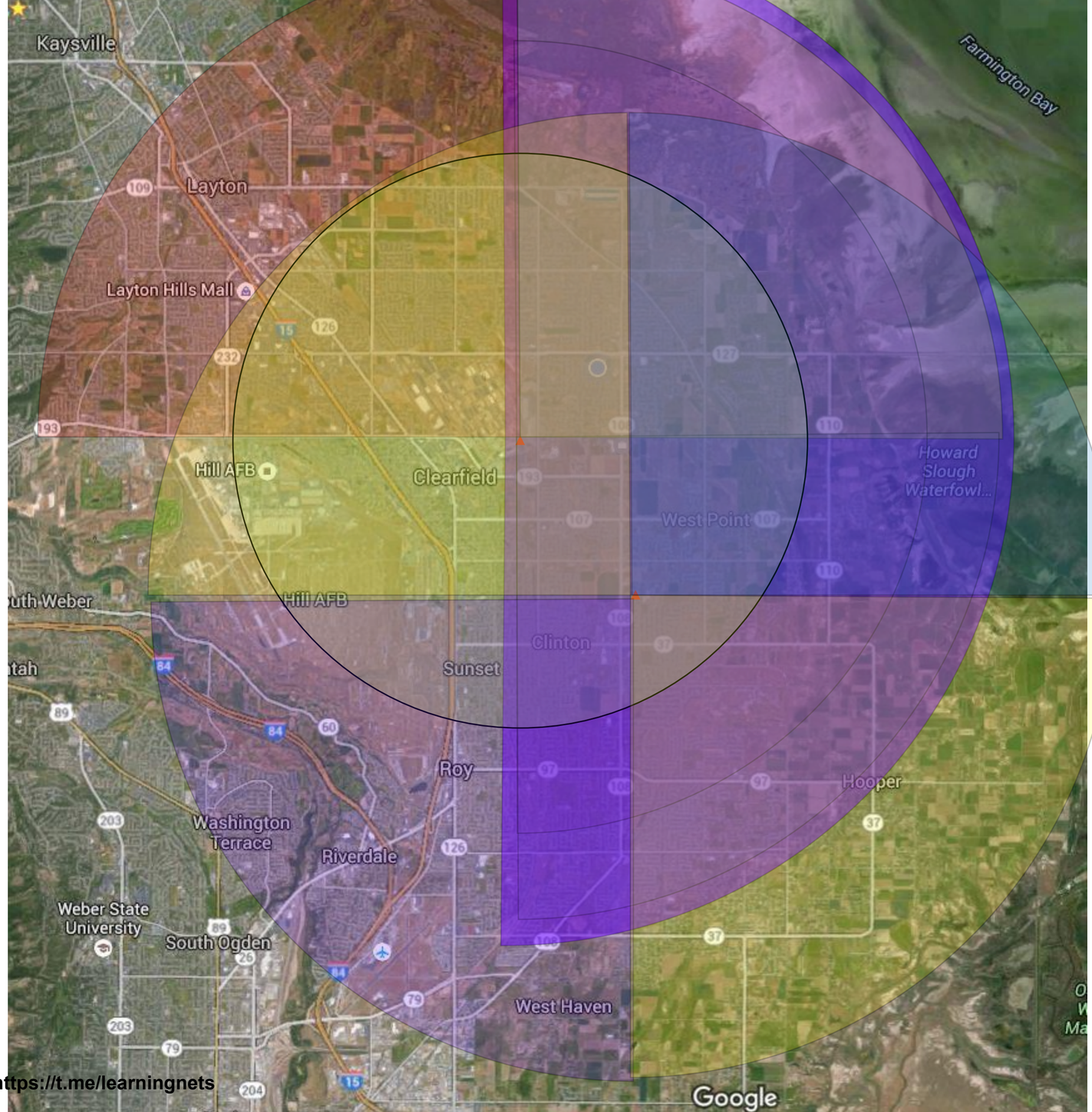
Dale's Study Tips











New security loopholes are consistently popping up because of wireless networking.

Kevin Mitnick

Some notes about the demos/labs

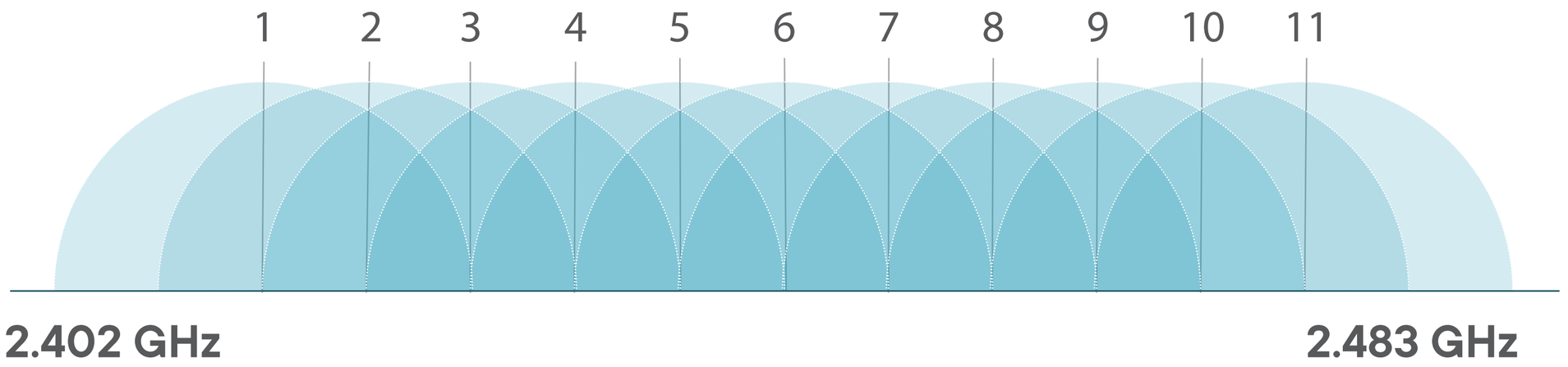
Key Terms

DSSS

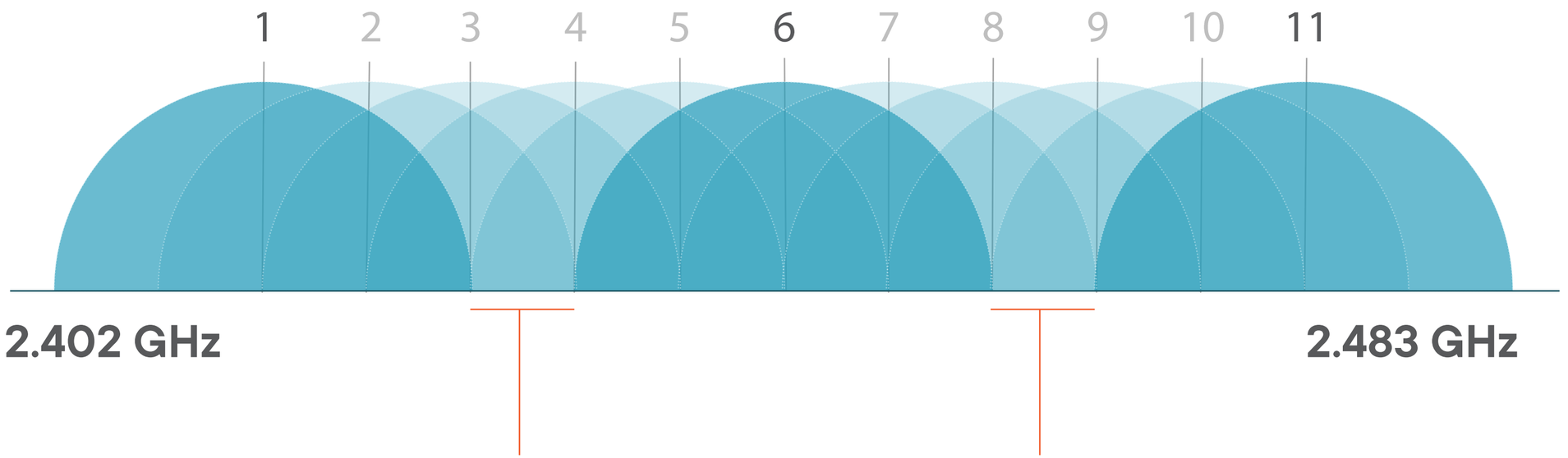
Key Terms

Direct-sequence spread spectrum

DSSS



DSSS



FHSS

Key Terms

Frequency-hopping spread spectrum

Hedy Lamarr

Silver screen actress

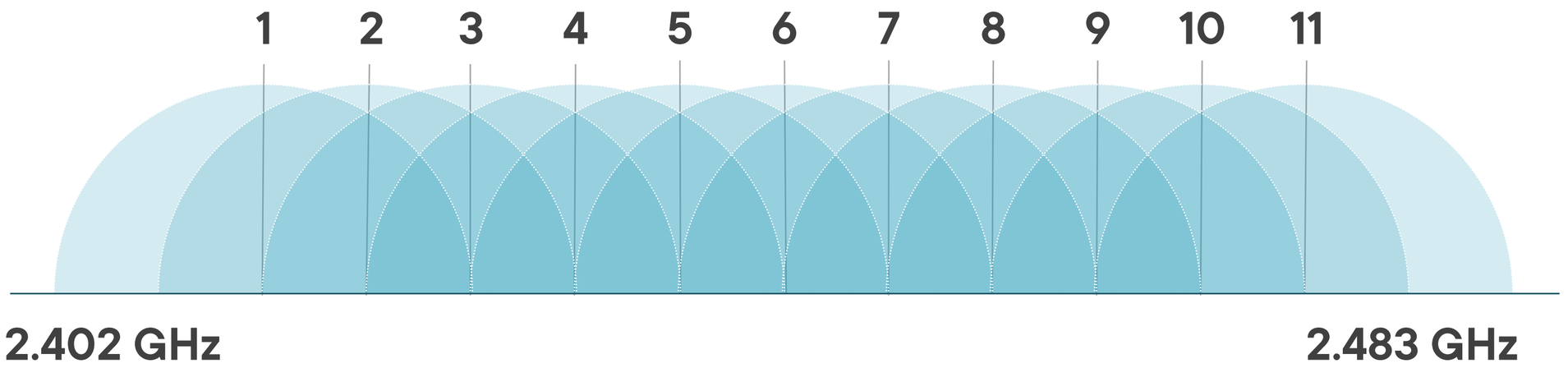
Inventor

Secret communication system

Unbreakable code by hopping frequencies

Adaptive FH(AFH) = Bluetooth

FHSS



Access Point

Key Terms

Access Point

Access Point

Enables wireless devices to connect to a wired network

BSSID

Key Terms

Basic service set identifier

BSSID

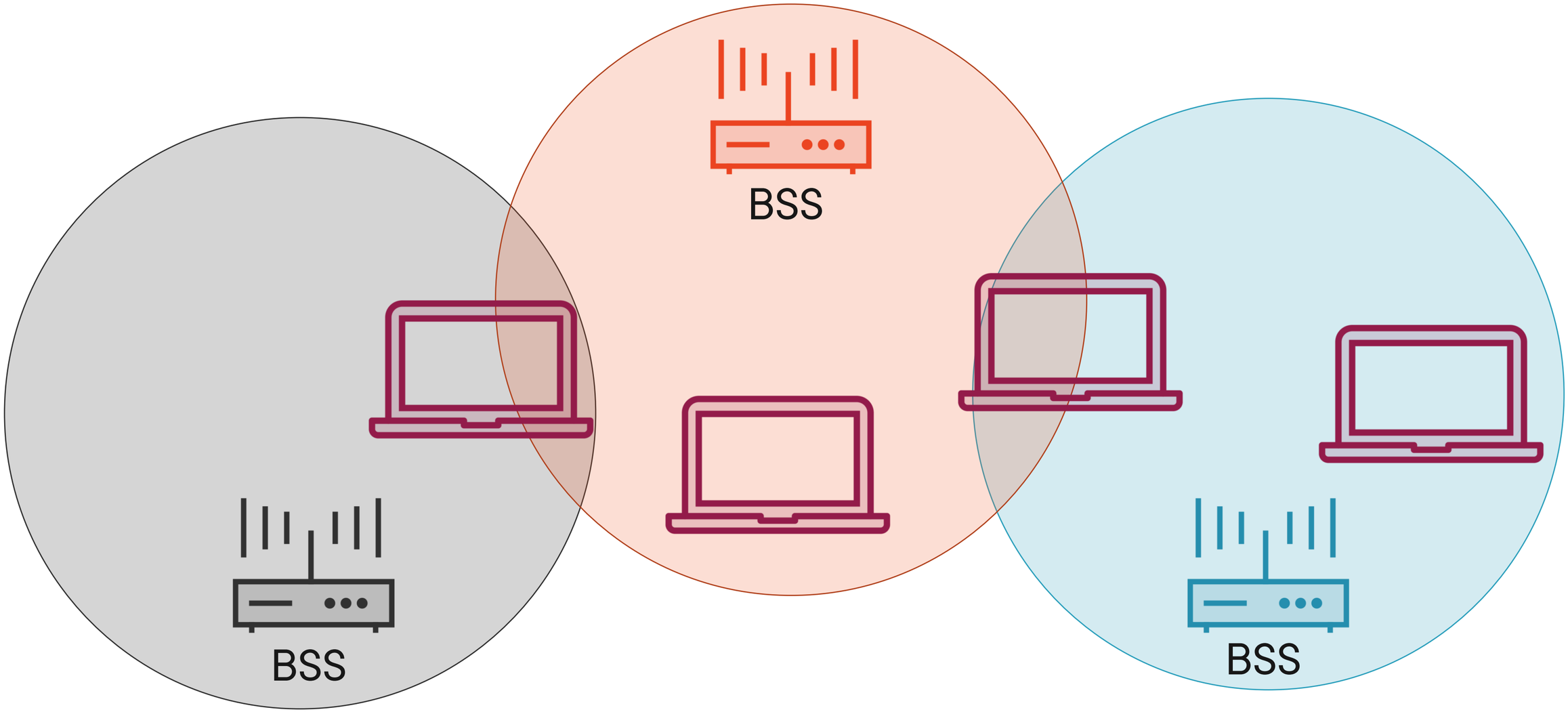
Don’t confuse with SSID

Basic Service Set (BSS)

Changes due to variation of range

Associated to the MAC address

AA:BB:CC:DD:EE:FF



BSSID

Don’t confuse with SSID

Basic Service Set (BSS)

Changes due to variation of range

Associated to the MAC address

Capturing tool identifies MAC address

AA:BB:CC:DD:EE:FF

SSID

Key Terms

Service set identifier

SSID

32 characters in length

Attached to every wireless packet

Allows multiple access points

Similar to wired ethernet

More Key Terms

Global System for Mobile Communications (GSM)

Hotspot

Association

MIMO-OFDM

Advantages and Disadvantages

Advantages and Disadvantages

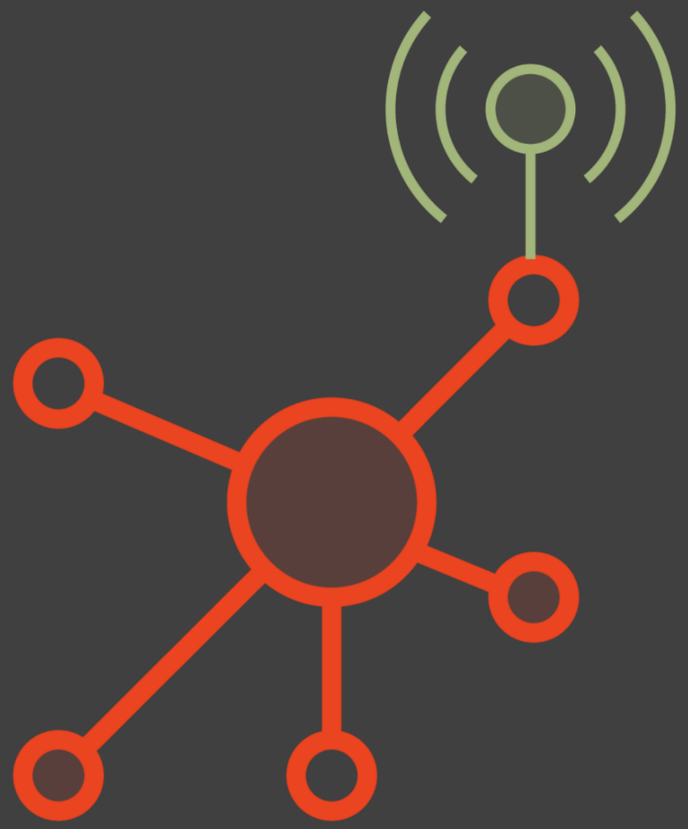
Disadvantages	Advantages
Security	Installation
Bandwidth	Connectivity
Upgrades	Mobility
Interference	

Advantages and Disadvantages

Disadvantages	Advantages
Security	Installation
Bandwidth	Connectivity
Upgrades	Mobility
Interference	Public Access

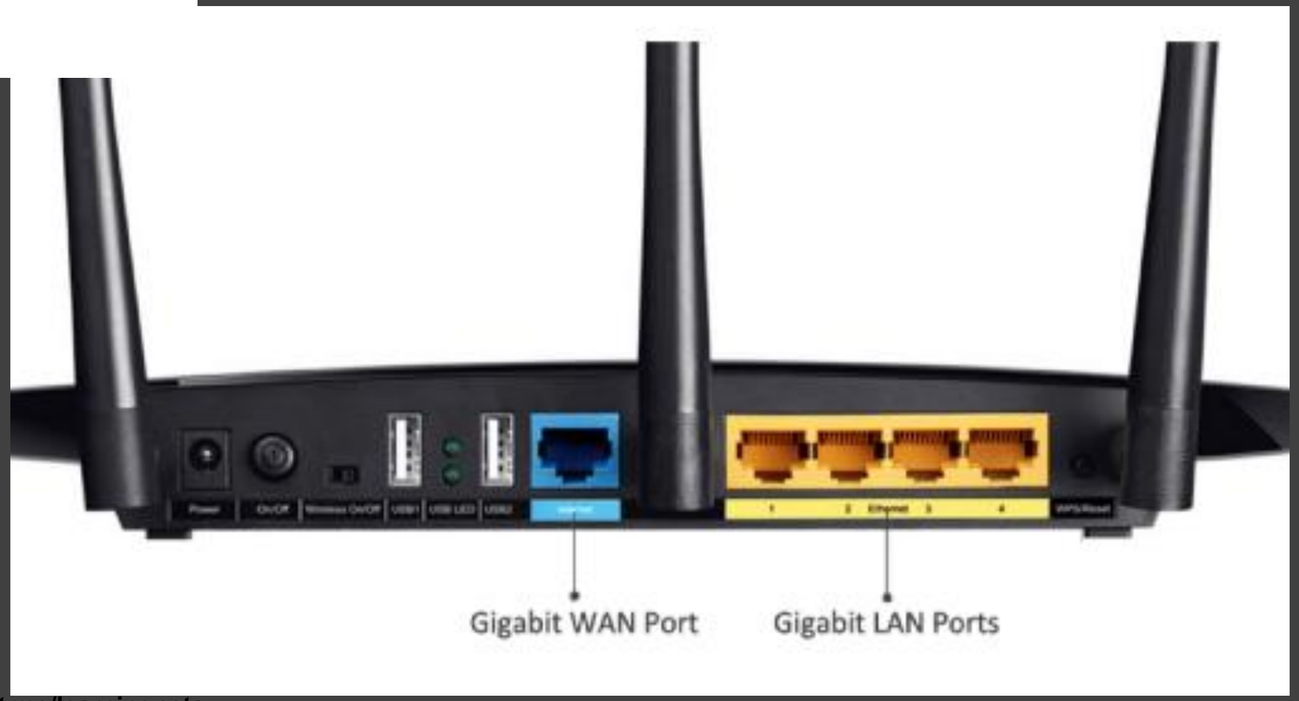
Types of Wi-Fi Networks

Types of Wireless Networks

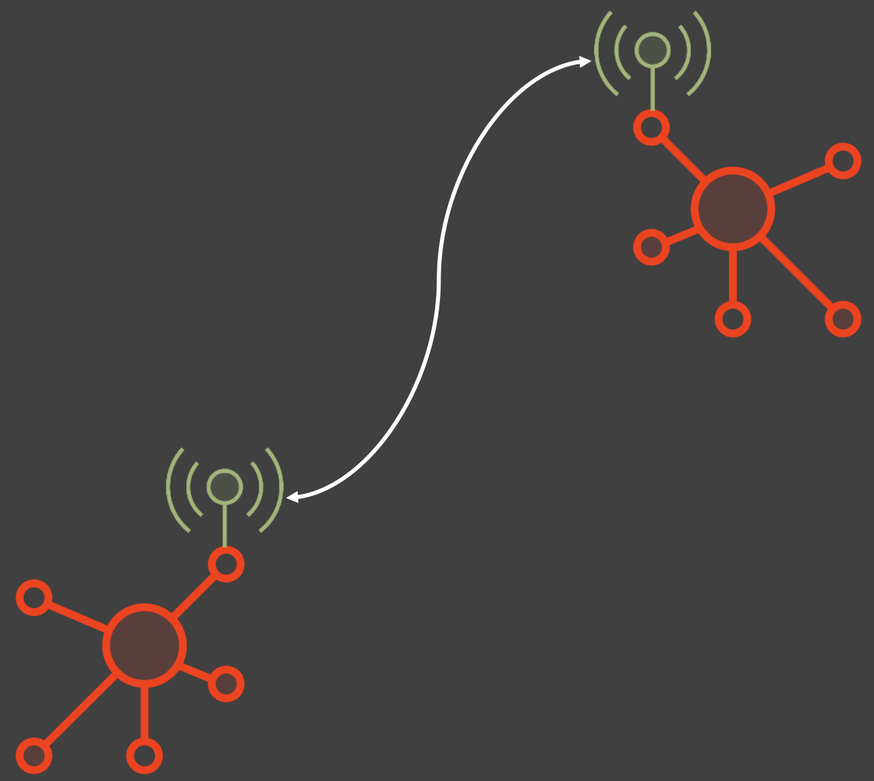


Extensions

Access Points*



Types of Wireless Networks

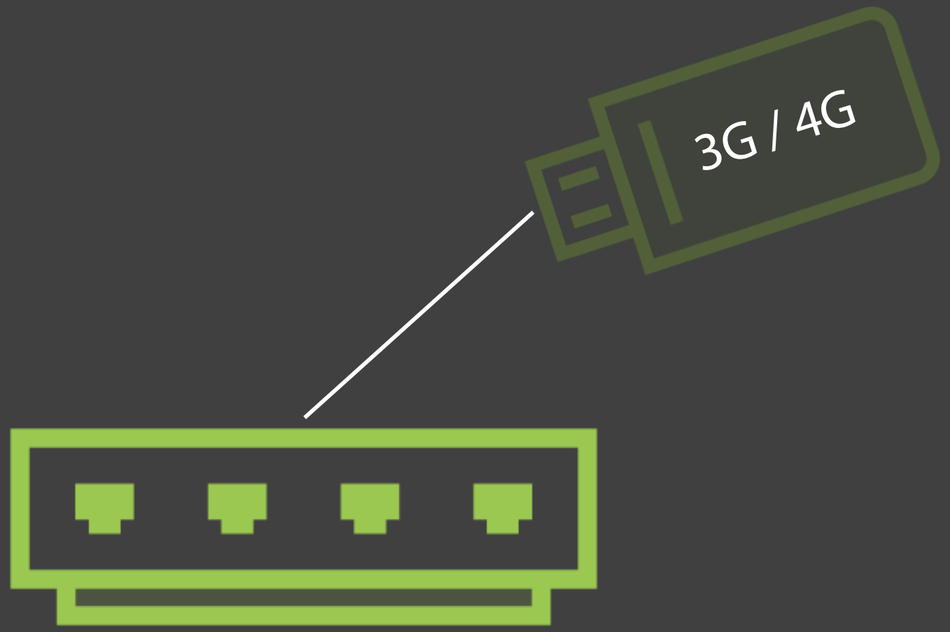


- **Extensions**
- **Access Points**
- **LAN-2-LAN Networks**

Types of Wireless Networks

- **Extensions**
- **Access Points**
- **LAN-2-LAN Networks**
- **Multiple AP Networks**

Types of Wireless Networks

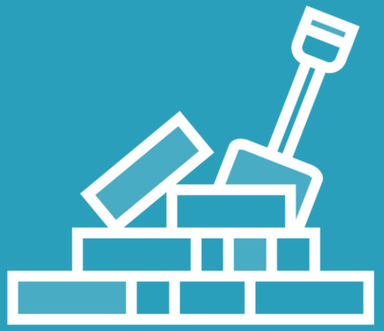


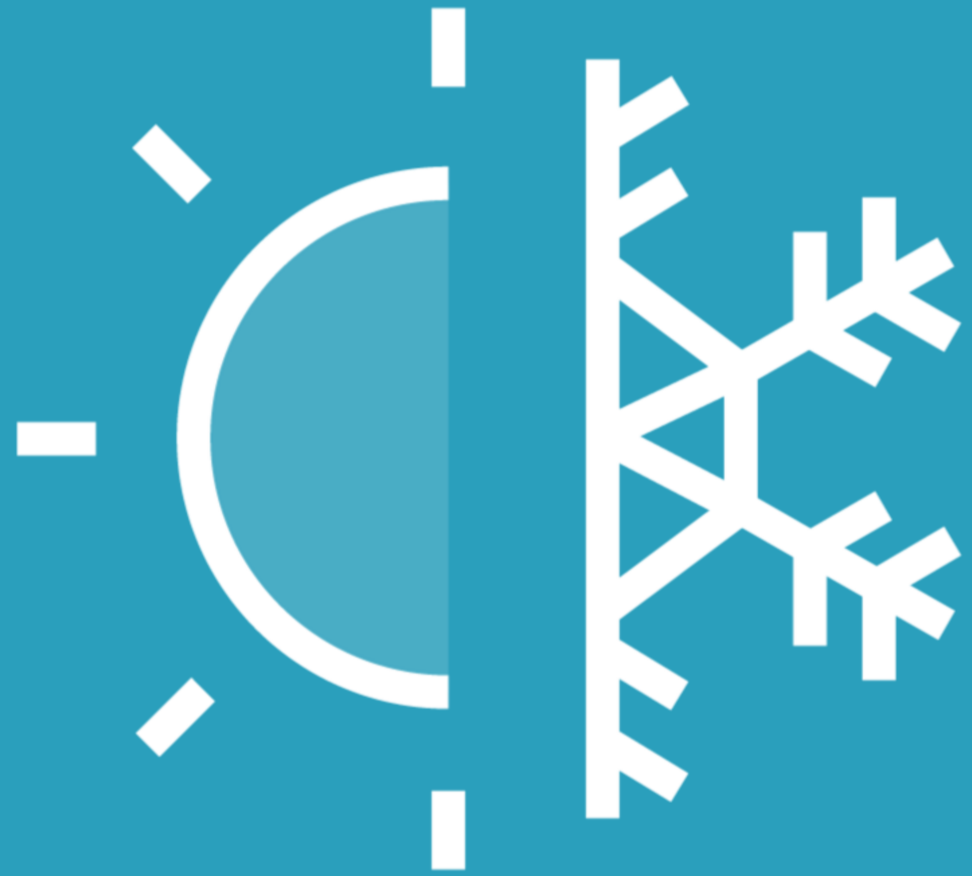
- **Extensions**
- **Access Points**
- **LAN-2-LAN Networks**
- **Multiple AP Networks**
- **Cellular Access Networks**

Standards

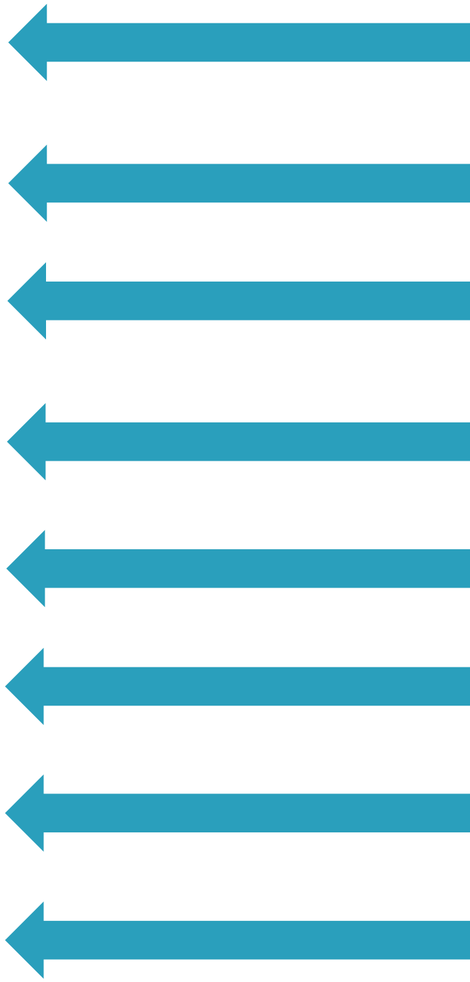




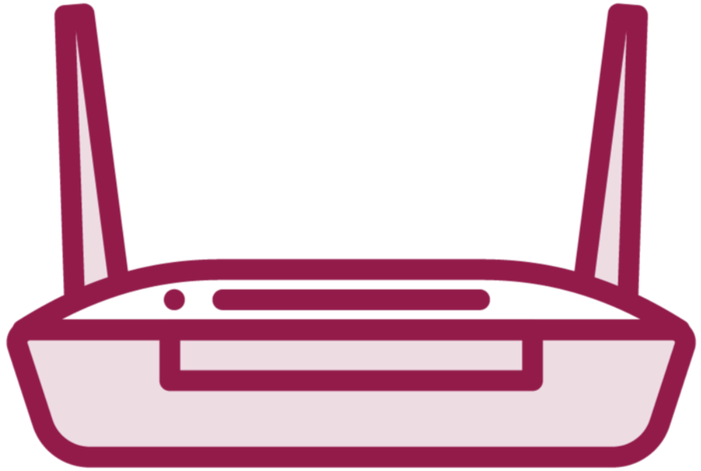





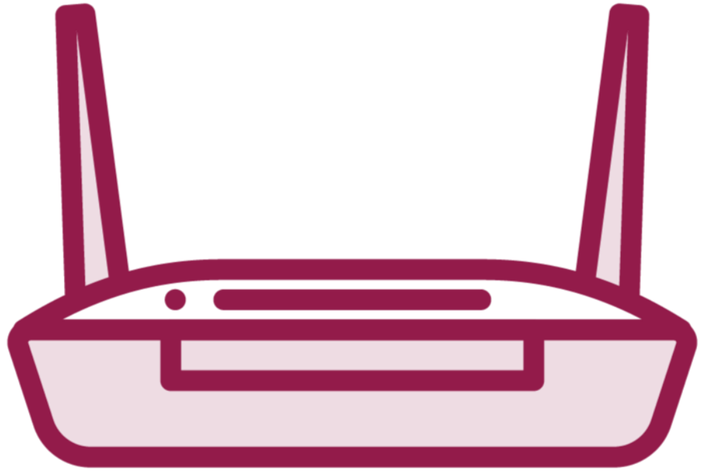
IEEE Standard	Frequency	Speed	Modulation
802.11	900Mhz & 2.4Ghz	3 Mbps	FSSS/DSSS
802.11a	5Ghz	54 Mbps	OFDM
802.11b	2.4Ghz	11 Mbps	DSSS
802.11g	2.4Ghz	54 Mbps	OFDM/DSSS
802.11n	2.4/5Ghz	54 -600 Mbps	OFDM
802.11ac	2.4/5GHz	1.3 Gbps	MIMO-OFDM
802.11ax	1-7.25GHz	13Gbps	MU-OFDM
Bluetooth	2.4Ghz	1-3Mbps	GFSK



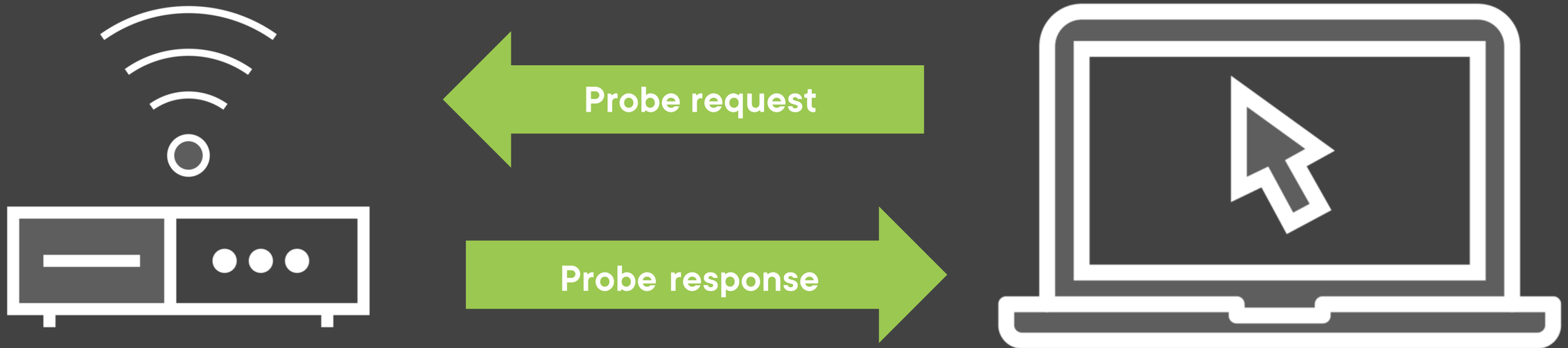
Wi-Fi Authentication Modes



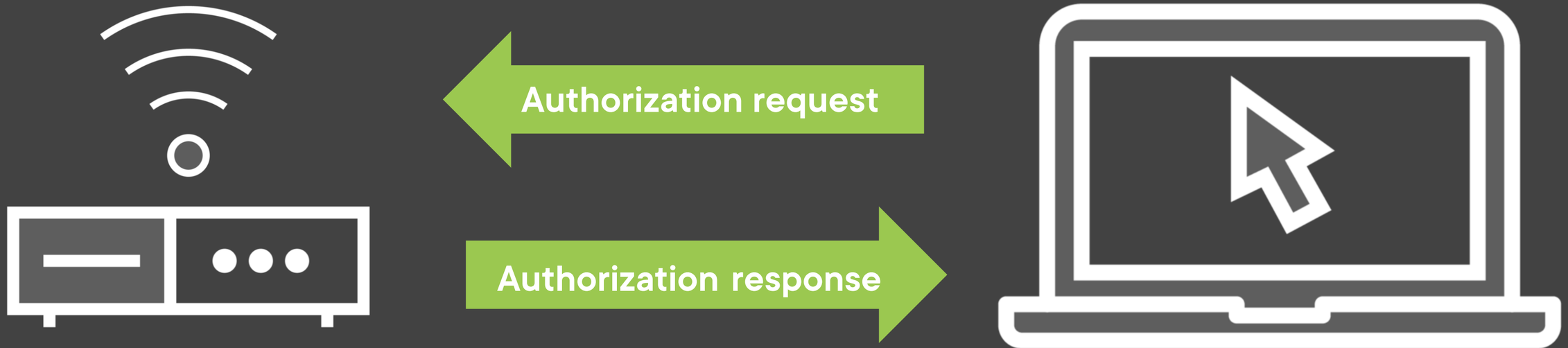
Two Methods



Open vs. Shared Method

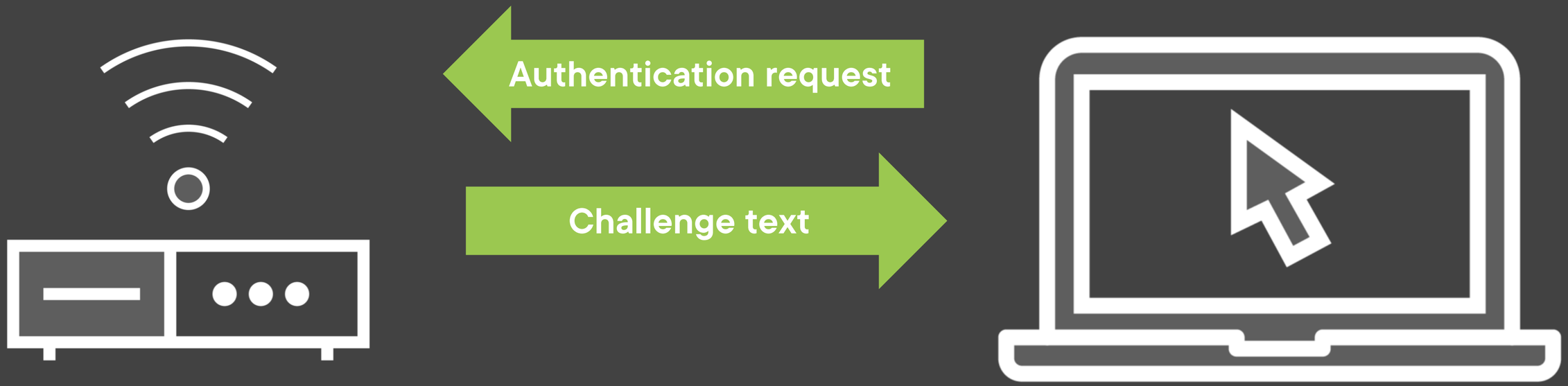


Open System Authentication

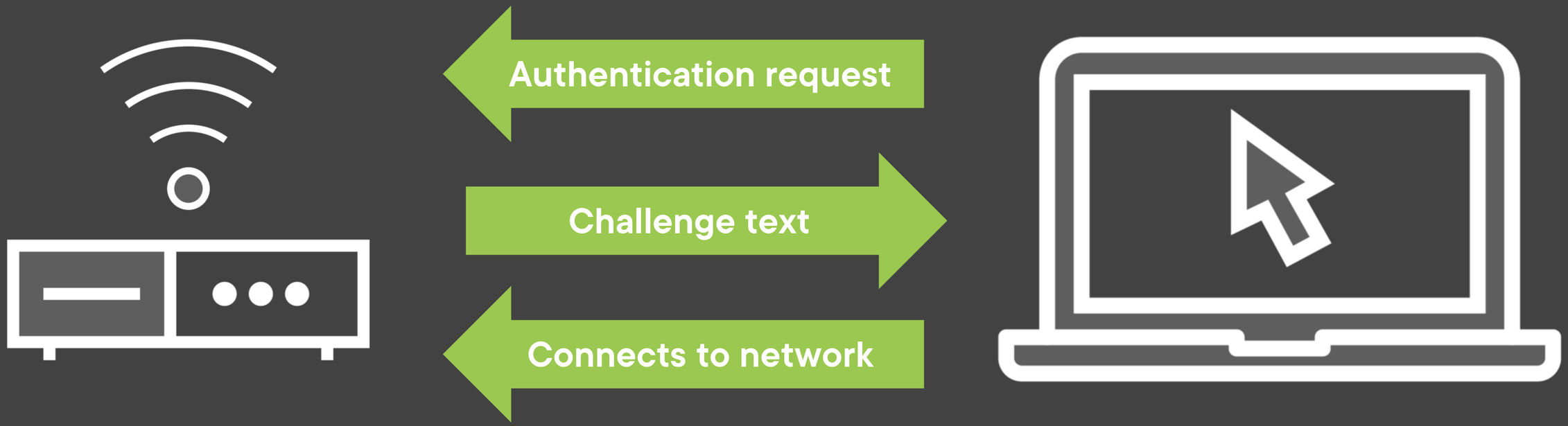


Open System Authentication

Open System Authentication

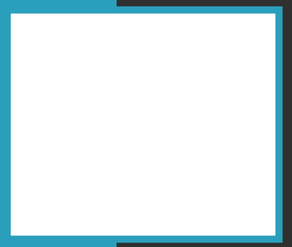


Shared Key

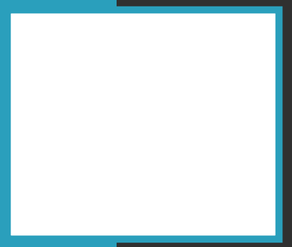


Shared Key

Quiz Time

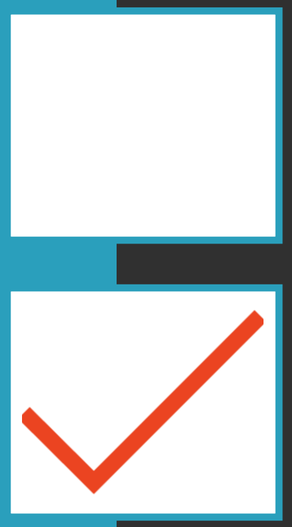


Share key



Open System Authentication

Quiz Time

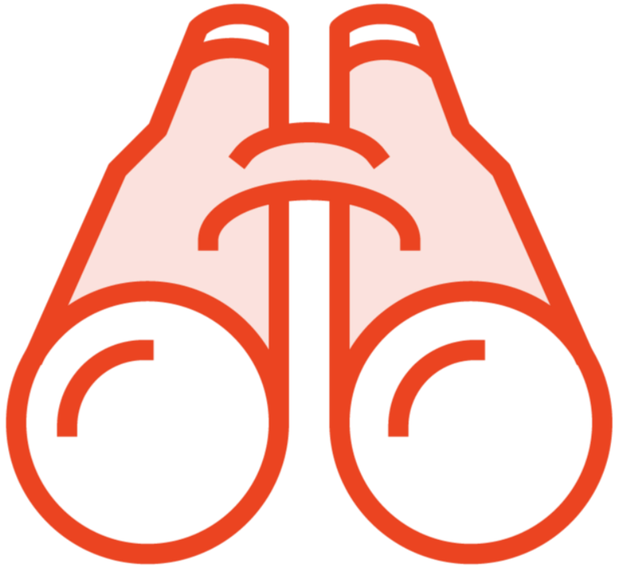


Share key

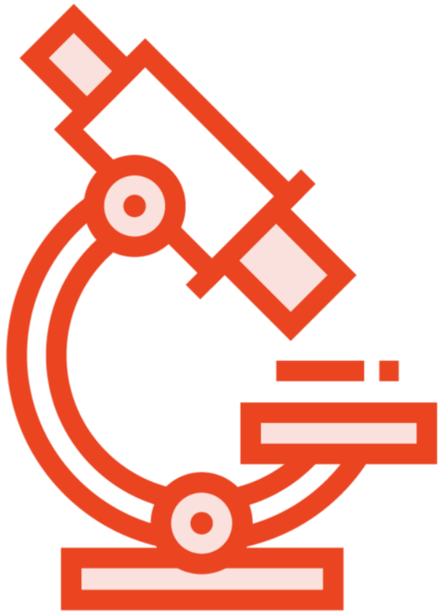
Open System Authentication

Chalking

Identifying Networks



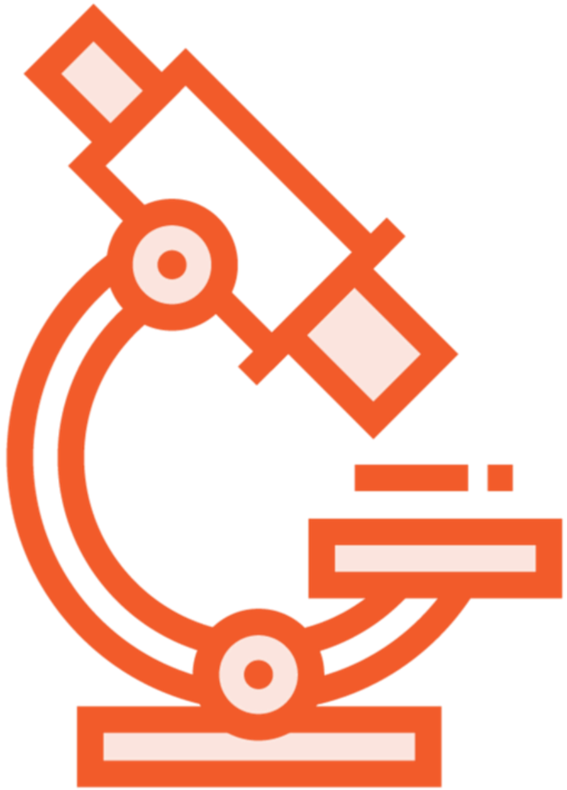
Find



Discover

Leave behind

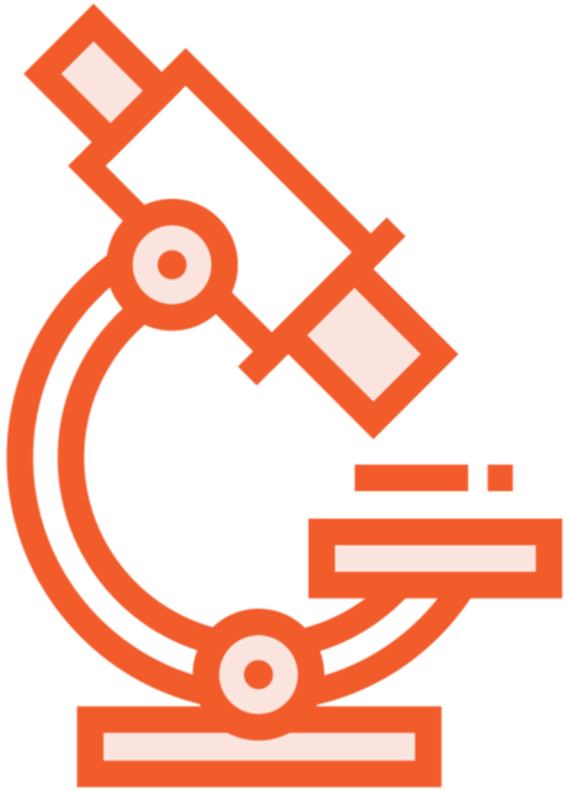
Discover



WarWalking

WarFlying

Discover



WarWalking

WarFlying

WarDriving

How It Began

Matt Jones

Marks or symbols

I8 I Ate	Allright (Ok)	Easy mark	Tell Pitiful Story	Work Available	M Tell a Hard luck story here
Fake illness here	Anything Goes	Sleep in barn	Can sleep in barn	Good Chance to get money here	Here is the place
Help if sick	Doctor	Telephone	Poor Man	Bad tempered owner	Dishonest Man
Man with a gun	Dog	Bad Dog	Officer	Police Officer Lives Here	Judge
Nothing doing here	Doubtful	Owner Home	Owner Out	No One Home	Someone Home

How It Began

Matt Jones

Marks or symbols

Homeless

How It Began

Matt Jones

Marks or symbols

Homeless

Safe to sleep

Help was nearby

Looks different today

Symbols

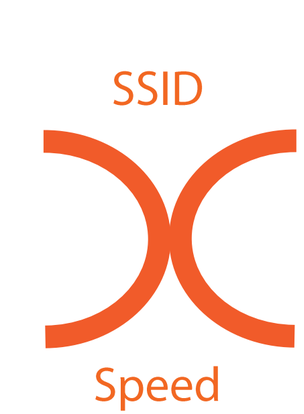
Node (open or closed)

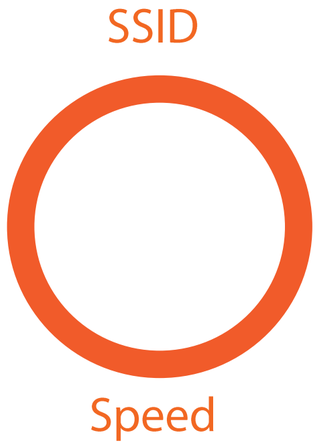
Encryption used

Speeds

SSID

Filtering





=

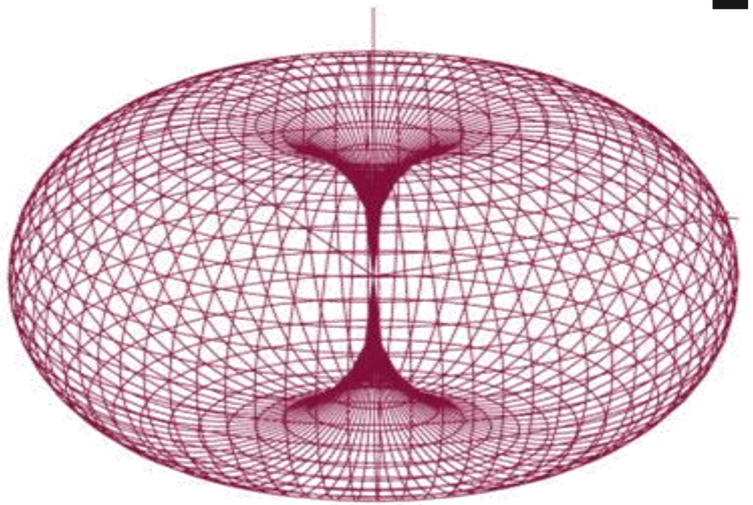
Dale might just be nearby

Antenna Types

Add b roll of someone driving around to match script

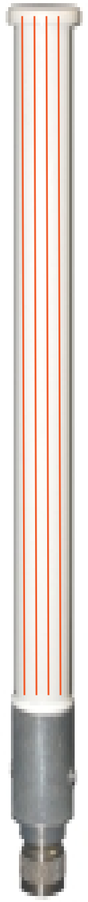
It's kind of funny, after you study wireless, it's amazing, you'll start looking around as you drive and you'll start to see antennas that you never realized were there before, and they pop up in the strangest of places. When it comes to antennas, the type will be determined by how you want to use it.

Omnidirectional

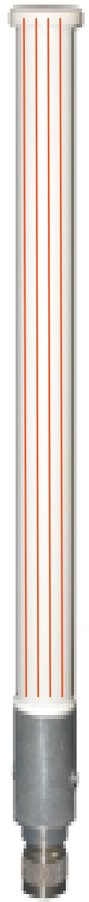


Broadcasts 360 degrees vertically

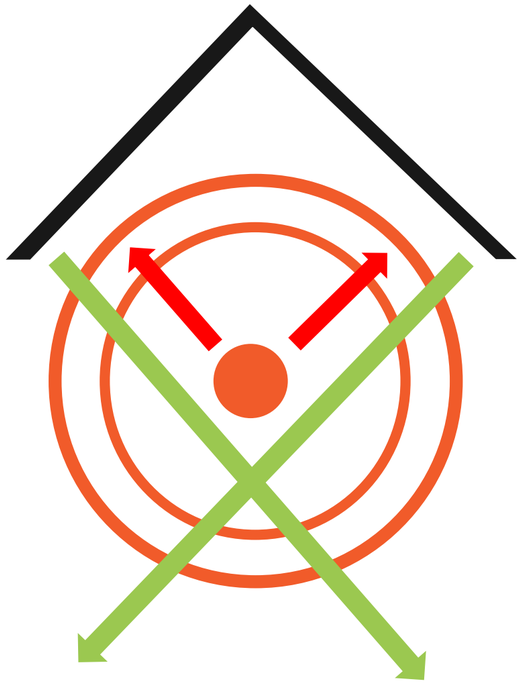
Less powerful



Horizontal vs Vertical



Directional Antenna



Various degrees
(45/90/180)

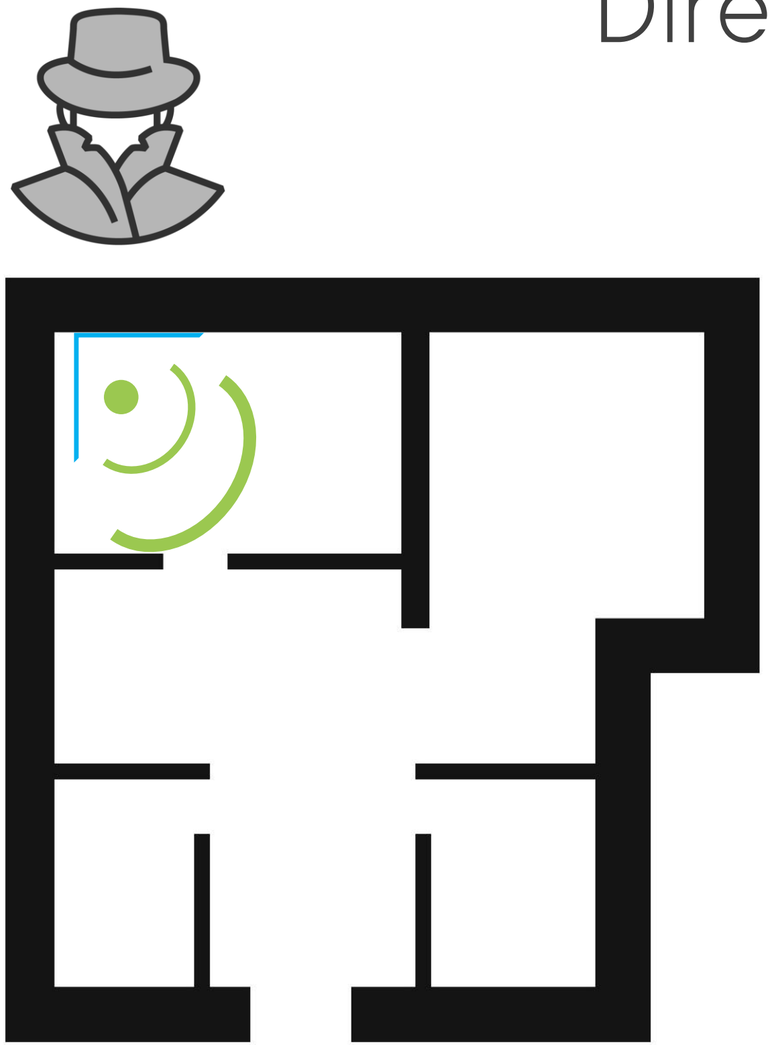
More powerful than Omni's

Directional Antenna

Various degrees
(45/90/180)

More powerful than Omni's

Directional Antenna



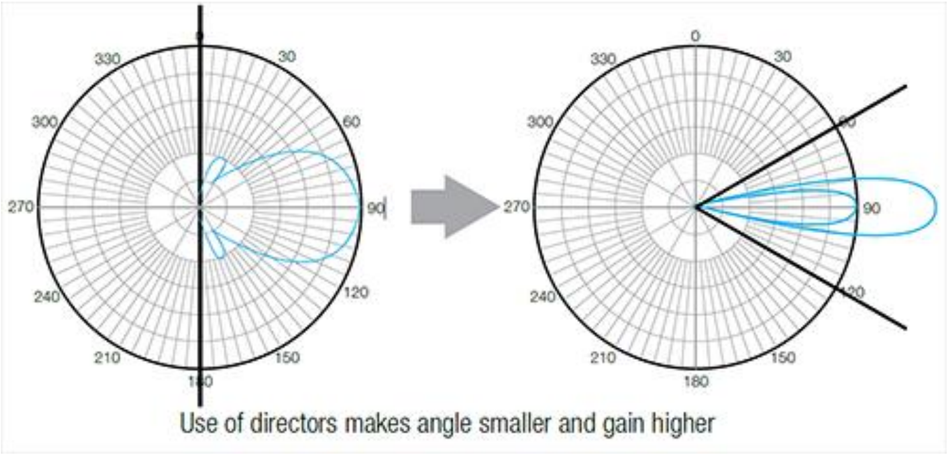
Various degrees
(45/90/180)

More powerful than Omni's

Parabolic Grid

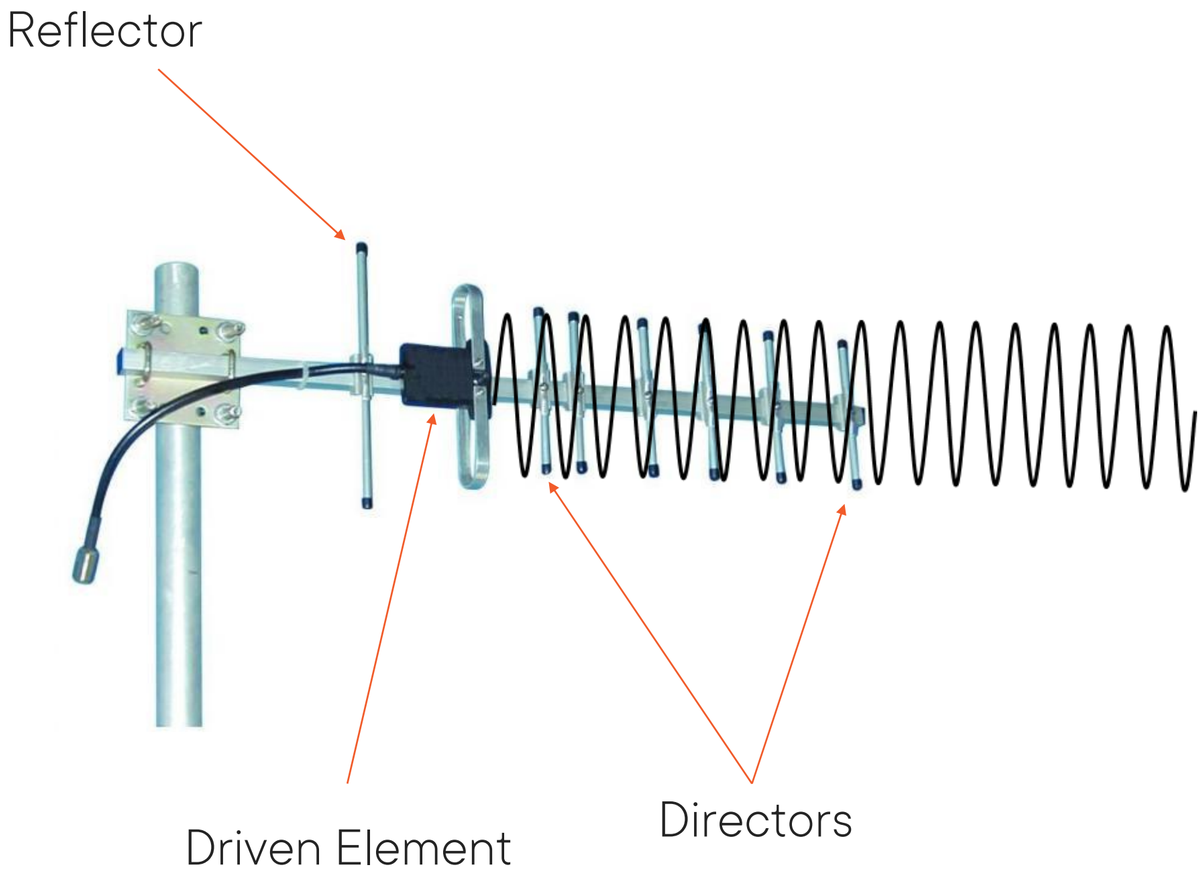
Like a satellite dish with a long distance reach

More powerful than Omni's



Use of directors makes angle smaller and gain higher

Yagi



Focused with a long distance reach

Learning Check

Learning Check

- **Open System Authentication**
- **Warwalking**
- **LAN-to-LAN**
- **BSSID**
- **SSID**

Up Next:
Summarizing Wireless Encryption