WLAN Technologies

News

https://blog.lastpass.com/2024/02/warning-fraudulent-app-impersonating-lastpass-currently-available-in-apple-app-store/?is=6fa78154dbea9fd6a29caa59a8a9433f63d310cc0d643f0f38e7e9ff5be35bf6

Overview

- Describe common WLAN topologies and 802.11 standards
- Explain the basic functionality of access points
- Explain the difference between an access point and a wireless bridge
- Identify the different types of antennas, along with their uses
- Explain the reasons for, and steps behind site surveys
- Explain why wireless is vulnerable to packet analysis and describe how hackers exploit this vulnerability

How WiFi Works

- https://web.archive.org/web/20171226072425/https://www.verizoninternet.com/bookmark/how-wifi-works/

WLAN Topologies

- Radio card
  - 802.11 standards refer to as a station (STA)
  - A station can be any 802.11-capable device
    - Laptop, smartphone, tablet, plug-in card
  - If endpoint, called a client station
- Access point (AP)
  - Also a station
  - Serves as central hub that communicates with all client stations within range

Wireless Client Devices

- Any device that meets the following criteria can act as a wireless client:
  - It contains a radio card or integrated transmit (TX) and receive (RX), noted as TX/RX.
  - It contains an antenna.
  - It operates under 802.11 protocol standards.
- A client station is configured to associate with an access point by creating a Layer 2 connection

Wireless Client Devices (Cont.)

- Every access point is identified by a **service set identifier (SSID)**
  - SSID is a configurable name or alphanumeric code
- If multiple access points configured with the same SSID, and if the correct security credentials supplied, client will be handed over to the strongest signal
  - Access points must use different channels to avoid interference

Wireless Client Devices (Cont.)

- Before a client can connect to an access point, it must detect presence of access point
- A client does this by:
  - **Passive scanning:** Client listens for a beacon, which an access point continually emits. When client "hears" a beacon advertising an SSID for which it has been preconfigured, it selects that access point.
  - **Active scanning:** Client proactively scans the network by sending out probe pulse requests
  - **View client-probe-mapping pcap**

Wireshark Exploration of Beacons and Probes

Demonstration

Files: WifiOSA.pcap

802.11 Service Sets

- 802.11 standards define four topologies, called **service sets:**
  - Basic service set (BSS)
    - With the BSS, all communication goes through the access point. That is, in a BSS, client stations cannot communicate with each other directly.

802.11 Service Sets

- Extended service set (ESS)
  - An ESS is a combination of two or more BSSes connected via a distribution system medium such as an Ethernet network.
    - Seamless roaming: uses a 15 to 20 percent overlap in coverage areas
    - Nomadic roaming there is no overlap, with coverage areas remaining autonomous
    - Collocation model: there is 100-percent overlap between the two access point service areas Used to address client capacity issues

802.11 Service Sets

- Independent basic service set (IBSS)
  - No access point is used. Instead, client stations form peer-to-peer relationships with other client stations
- Mesh basic service set (MBSS)
  - Clients, access points, and gateways are all meshed together, enabling client-to-client and AP-to-AP communication.

Historic 802.11 Standards

- **802.11b (Wi-Fi 1):** Uses the unregulated 2.4 GHz band, with a throughput of 11 Mbps
- **802.11a (Wi-Fi 2):** Operates at 5 GHz and provides data rates between 1.5 Mbps to 54 Mbps
- **802.11g (Wi-Fi 3):** Supports bandwidths of up to 54 Mbps, utilizes the 2.4 GHz frequency band, allowing greater range than 802.11a; backward-compatible with 802.11b
- **802.11n(Wi-Fi 4):** Operates on 2.4 GHz and 5 GHz bands with speeds up to 600 Mbps

Source: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/

802.11 Standards (Cont.)

- **802.11ac(Wi-Fi 5):** Extension of 802.11n, offers more channels and streams up to 1.3 Gbps of throughput on the 5 GHz band
- **802.11ax(Wi-Fi 6):** uses the TV white-space spectrum and handles higher density by segregating channels
  - The main goal of this standard is enhancing throughput-per-area in high-density scenarios, such as corporate offices
  - **Wi-FI 6e:** Extends the standard to use the 6 Ghz band
- **Wi-Fi 7** https://spectrum.ieee.org/wi-fi-7-stomps-on-the-gas
- Other niche standards exist

WiFi 6 Improvements

- Orthogonal Frequency Division Multiple Access (OFDMA)
  - Allows the AP to transmit multiple signals at the same time, instead of sequentially
- Overlapping Basic Service Sets (OBSS)
  - Allows the use of "colors" to uniquely identify traffic and distinguish from noise.
- Beamforming
  - Detects direction of target devices and focuses transmission in that direction, rather than broadcasting

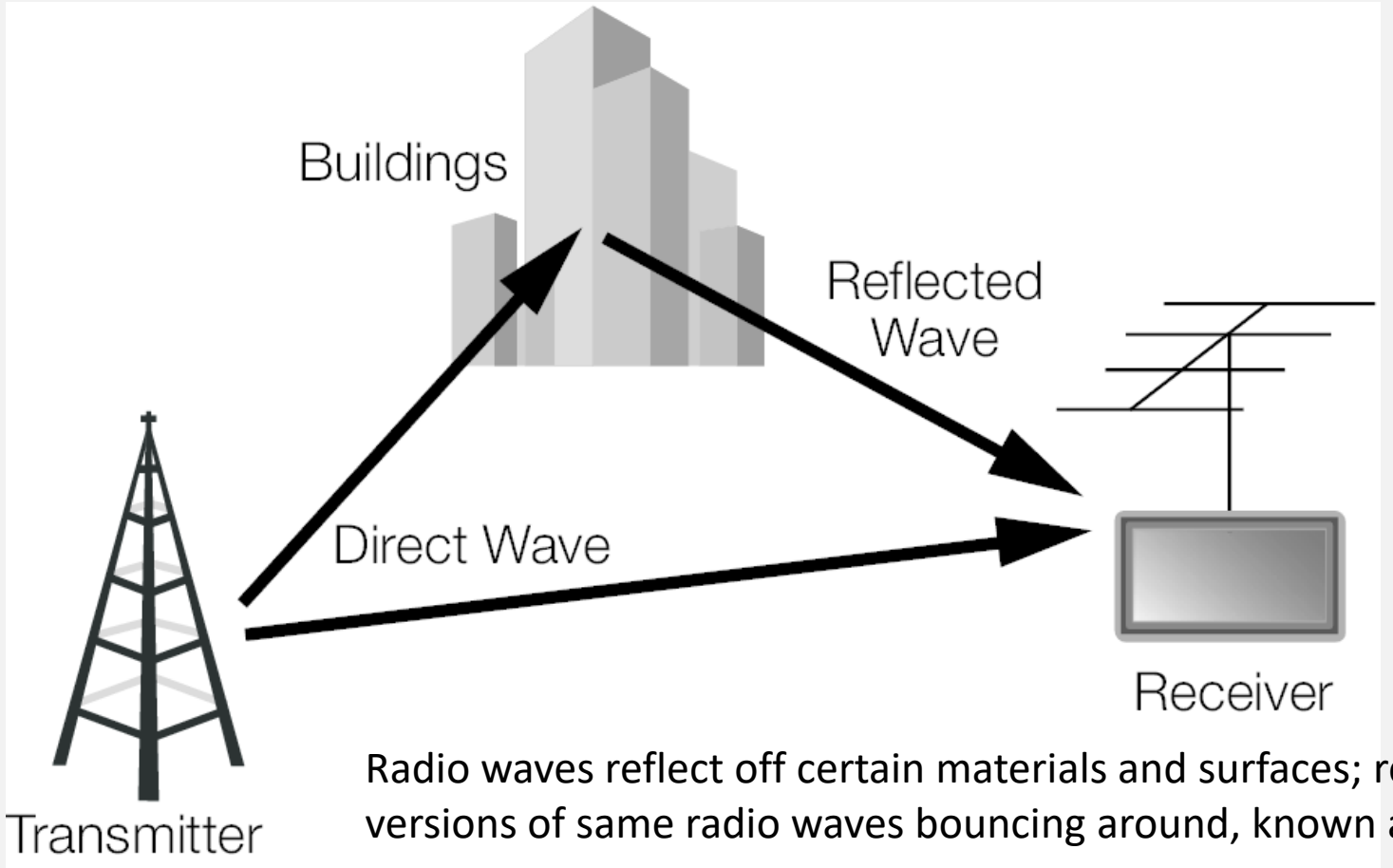
802.11 Unlicensed Bands

- **Unlicensed bands:** Users can operate without an FCC license
  - Must still use certified equipment and comply with power limitations
  - Unlicensed bands are subject to interference
- **Narrowband:** Uses little bandwidth by transmitting over a narrow beam of frequency with high power (for example, a 2 MHz wide channel at 80 watts)

802.11 Unlicensed Bands

- **Spread spectrum:** Transmission is spread across entire frequency space available (for example, over a 22 MHz band at 100 mW. 11 times the channel width but a nearly 1,000 times lower power). No license required less susceptible to multipath.
- **Frequency hopping spread spectrum (FHSS):** Transmits data using a small carrier space in short bursts and then continuously changing to another frequency during transmission.
- **Direct sequence spread spectrum (DSSS):** Stays a fixed channel, hopping within the frequency space on that channel. Using a technique called data encoding.

Multipath Problem

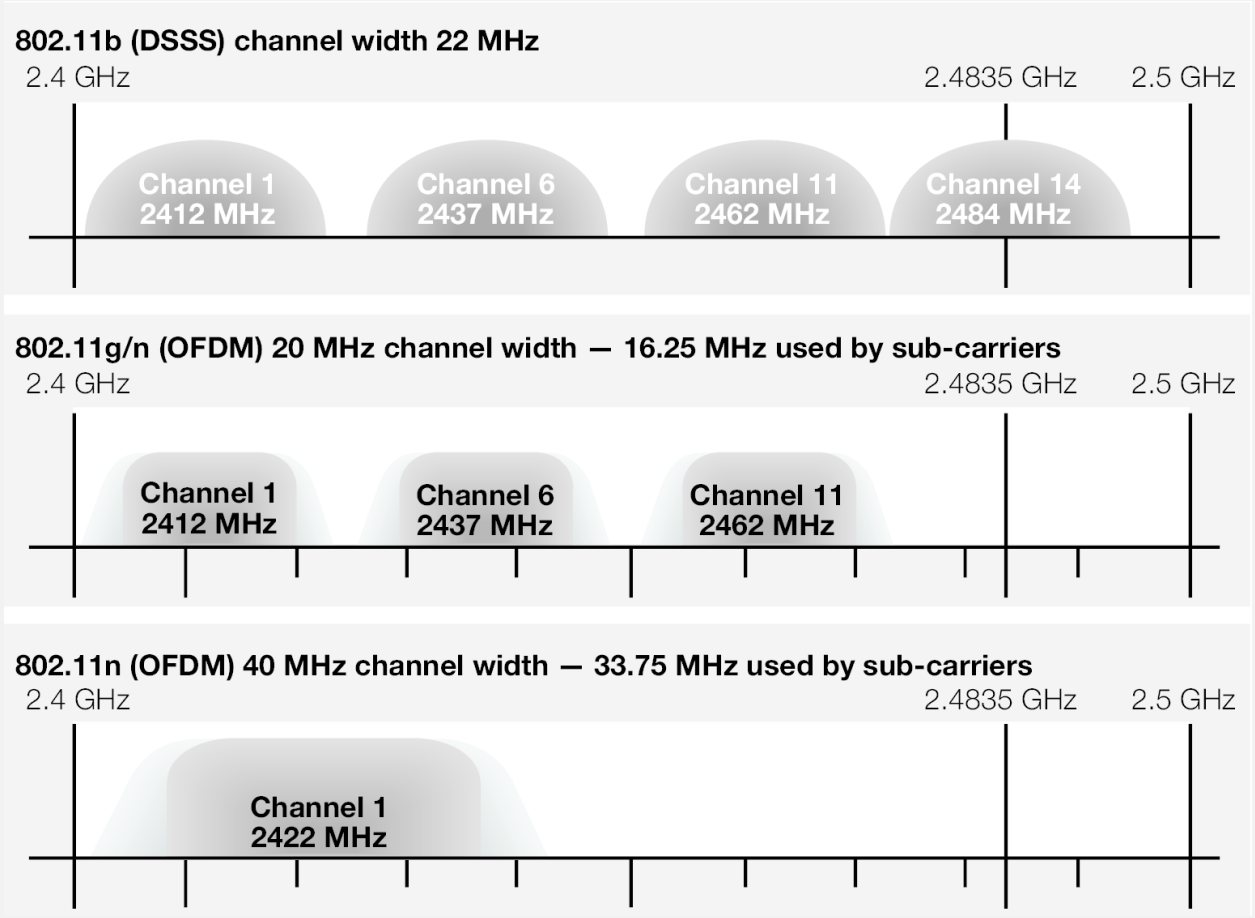


Radio waves reflect off certain materials and surfaces; results in multiple versions of same radio waves bouncing around, known as multipath

Wireless Access Points

- Wireless access point (WAP)
  - A half-duplex switch that contains a radio card and an antenna that can be tuned to one or more unlicensed radio frequencies
    - Specifically, the 2.4 GHz and/or the 5 GHz bands
- Different WAPs can operate on several channels within each frequency
- Network designers configure WAPs to ensure that non-overlapping channel plans are used to avoid interference

Wireless Access Points (Cont.)



https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php

Install and Start WiFi on Windows

Tools

- A variety of tools are available and free versions change frequently
- Windows
  - Inssider
  - NetSpot - https://www.netspotapp.com/
    - Also works on Android
  - Acrylic Suite
- Linux
  - Kismet

Using Netspot to view networks and signal strength and channels

Demonstration

How Does a WAP Work?

- Acts as a portal for another network, typically on another physical medium such as wired Ethernet
- Uses RF signals as a carrier band frequency
- Frequencies assigned to 802.11 are the unlicensed bands at 2.4 GHz and 5 GHz
- WAP radio cards are configured to work on one of the two unlicensed bands and on several channels

WAP Architecture

- Two types of WAPs:
  - **Autonomous access points:** Able to operate at the control and data layers, autonomous access points have switch-like intelligence.
  - **Thin access points:** Switch-like intelligence is stripped out and relocated in a WLAN controller device. The WLAN controller acts as a central administrator and controller for several thin access points.
    - Considerably eases the administrative burden of managing many WAPs on a WLAN

Wireless Bridges: Introduction

- Distribution system service (DSS) translates traffic between an 802.11 device and the distribution medium used for backhaul
- If backhaul medium is wireless, WAP can also serve as a wireless bridge
- 802.11 standard describes a mechanism called wireless distribution system (WDS) whereby the frame format can handle four MAC addresses
- Real-world deployments for WDS are in bridges, repeaters, and mesh networks

Wireless Workgroup Bridge

- Often used when there are several non-wireless devices, such as Ethernet-networked PCs, in a workgroup or in an office that require backup wireless connectivity to the network
- If the wired network goes down, devices with wireless access can continue to communicate

Residential Gateway

- A home wireless router that acts as a gateway to the Internet through a DSL or cable broadband connection
- Typically has a built-in hub supporting four Ethernet connections and a built-in WAP to create a WLAN

Enterprise Gateway

- Difference between a residential and an enterprise wireless gateway is a matter of capabilities
- Enterprise gateway typically has a WLAN and a LAN interface, which enables it to act as a translational bridge between the two mediums
- Is typically deployed as a guest point of access to the Internet, with no direct access to the corporate network

Wireless Antennas

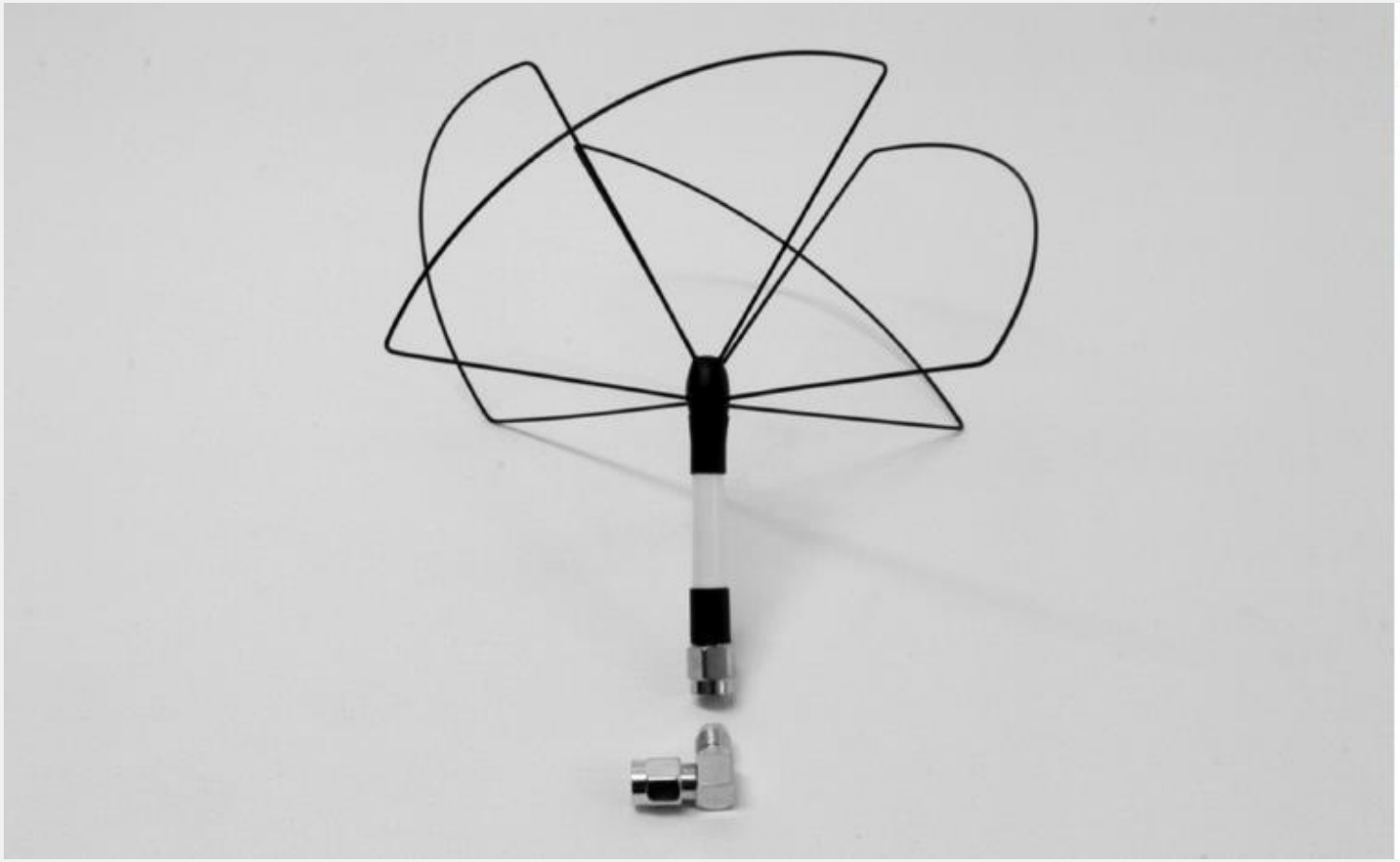
- **Omnidirectional**
- General-purpose antennas typically installed by default on WAPs; radiate radio waves equally in all directions, theoretically providing 360-degree coverage
- **Semi-directional**
- Are used when coverage is required in a specific direction
  - RF radiance tends to be limited to 180 degrees

Start Access Points

Configure names and channels 2.4 Ghz only

Semi-directional Yagi Antenna

Semi-directional Planar Antenna



Courtesy of Circular Wireless

Wireless Antennas (Cont.)

- **Highly directional**
- Are very specific; comparable to a flashlight with a very focused beam
  - Typically used in point-to-point situations, where a very exact, high-gain beam is required
  - Examples: Grid antennas and parabolic antennas

Highly Directional Grid Antenna

Highly Directional Parabolic Antenna

Wireless Antennas (Cont.)

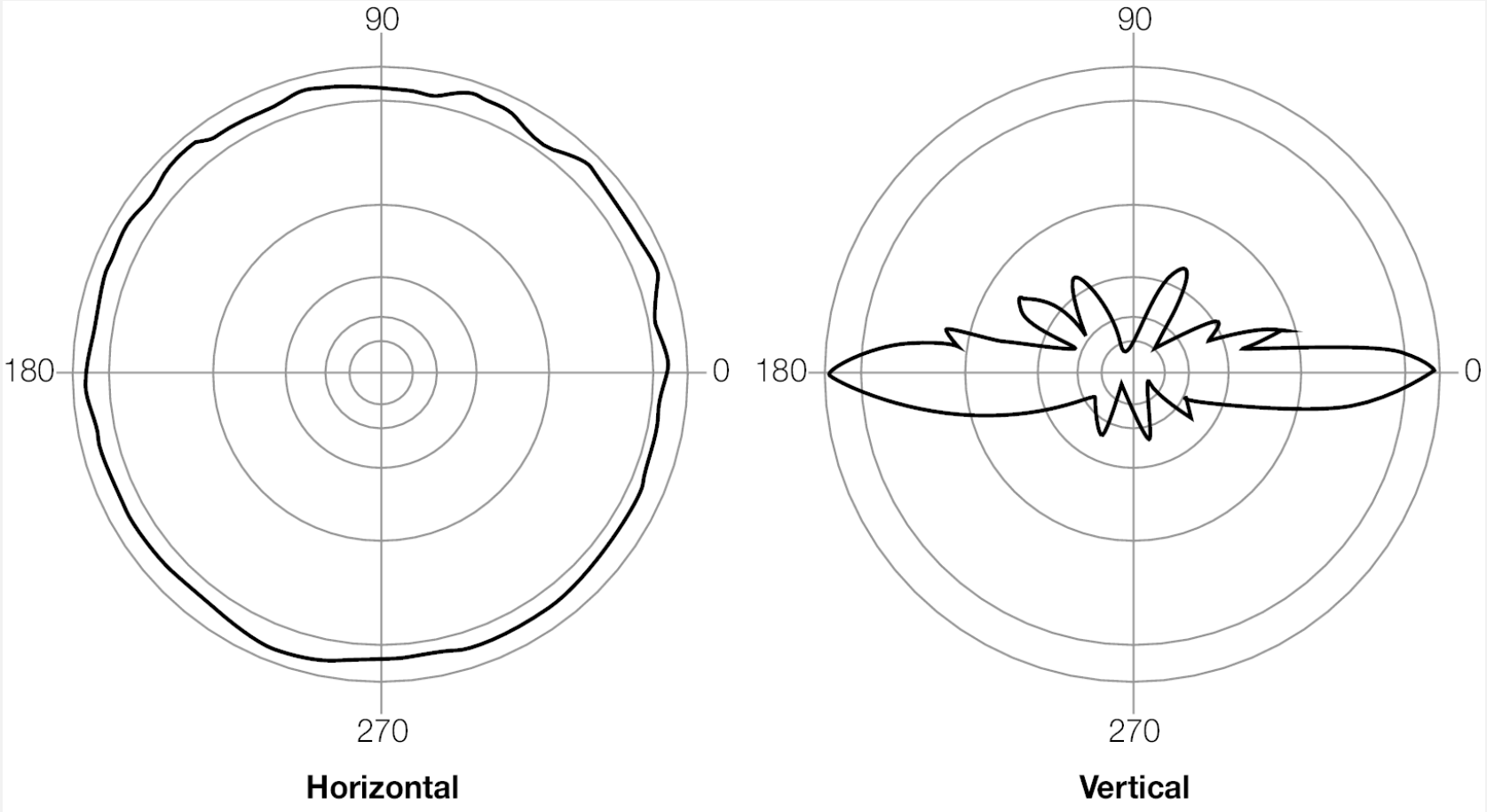
- **Multiple input/multiple output (MIMO) antennas**
- Architecture allows multiple antennas to transmit and receive concurrently
- MIMO technology allows complex signal-processing techniques, provides enhanced range, throughput, and reliability
- Key components in mobile 3G and 4G handsets, but also included in the 802.11n standard

Wi-Fi Router with MIMO Antennas

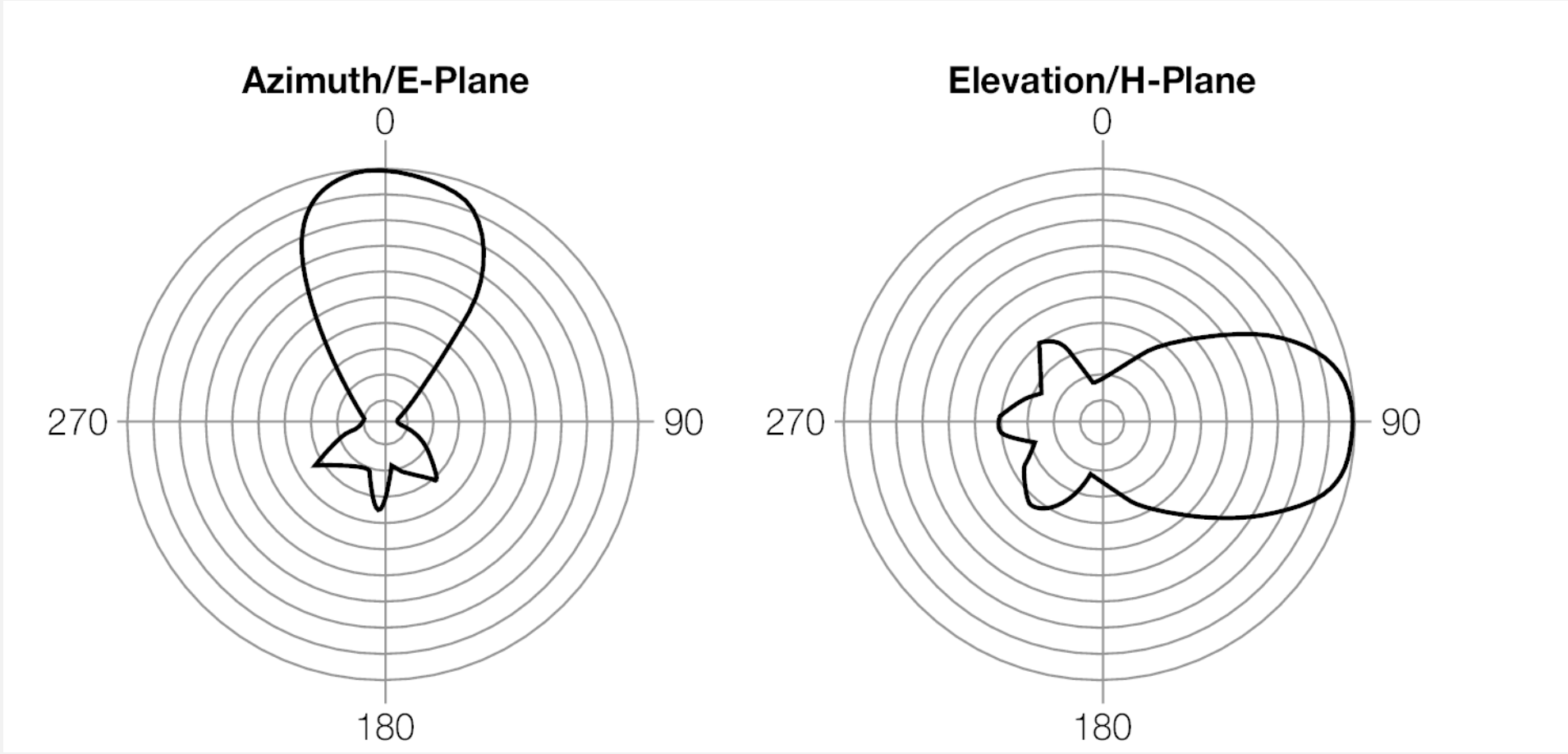
Determining Coverage Area

- When dealing with antennas, is important to understand antenna coverage charts from vendors
  - Often called planar charts or radiation envelopes
- Each antenna type has specific characteristics
- Shown in coverage charts from two perspectives: a heads-down azimuth or horizontal aspect, and a side-on elevation or vertical aspect

Omnidirectional Coverage Map



Semi-directional Coverage Map



Coverage Area and Wi-Fi Roaming

- Common design is overlapping coverage areas so network can support **seamless roaming**
  - Designer specifies overlapping access point coverage of at least 15 to 25 percent
- **Nomadic roaming**
- Coverage driven by need to ensure segregation and minimal overlap in coverage
- User's connection is lost and then re-established when crossing access point boundaries

Coverage Area and Wi-Fi Roaming (Cont.)

- **Collocation**
- A fully overlapping access point used to increase capacity
- **Mesh basic service set (MBSS)**
- Access points act as bridged trunks that link with other mesh mode access points to backhaul traffic from network to a distribution medium portal or gateway
- Common design in larger networks with areas inaccessible to wired connectivity

Improving Wi-Fi Signal

- Repeater (Amplifier)
  - Repeats signals to and from access point
  - Must be close enough to AP to have good signal
  - Still affected by obstacles
- Extenders
  - Wired connection to AP
  - Full power signal, but requires wiring
- Power Line Communications (PLC) Devices
  - Get signal from AP over electrical outlets
  - Outlets must be in same phase to work

Self-organizing WLANs

- Controller-based access points provide ability to dynamically reconfigure lightweight thin access points based on changing RF conditions
- Network can adjust signals, channels, power levels, and patterns to maintain optimal operating characteristics and network performance

Determining Wi-Fi Coverage

Site Survey

- Important to ensure proper coverage and detect signal leakage or pollution.
- Locate and map radio frequency (RF) footprint for each discovered access point against a default grid or an imported floor plan
- Should include capacity planning and identify possible areas of interference
- Example programs:
  - Ekahau HeatMapper
  - Netspot paid editions https://www.netspotapp.com/
  - Acrylic Wi-Fi Heatmaps – offers a free education version

Spectrum Analysis

- Helps detect RF interference that might conflict with WLAN
- Spectrum analyzer is used
  - A test device that measures the amplitude and frequency of electromagnetic signals (radio waves)
- Spectrum analysis enables you to visualize and map what RF activity already exists within the 2.4 and 5.0 GHz spectrums
- If background noise (unwanted radiation on those channels) exceeds 85 dBm, wireless network performance suffers

Sources of Noise and Interference

- Microwave ovens
- Cordless phones
- Fluorescent bulbs
- Elevator motors
- Bluetooth radios
- Other 802.11 wireless networks
- Malicious transmitters (jammers)

Coverage Analysis

- Conduct site coverage and capacity-planning interviews
  - Information-gathering exercises to establish the capacity and coverage requirements based on the population density in certain areas, which may determine the need for smaller or larger cells or even collocation
- No special tools are required other than the RF signal strength indicator on a laptop or other 802.11-enabled device

Access Point Placement

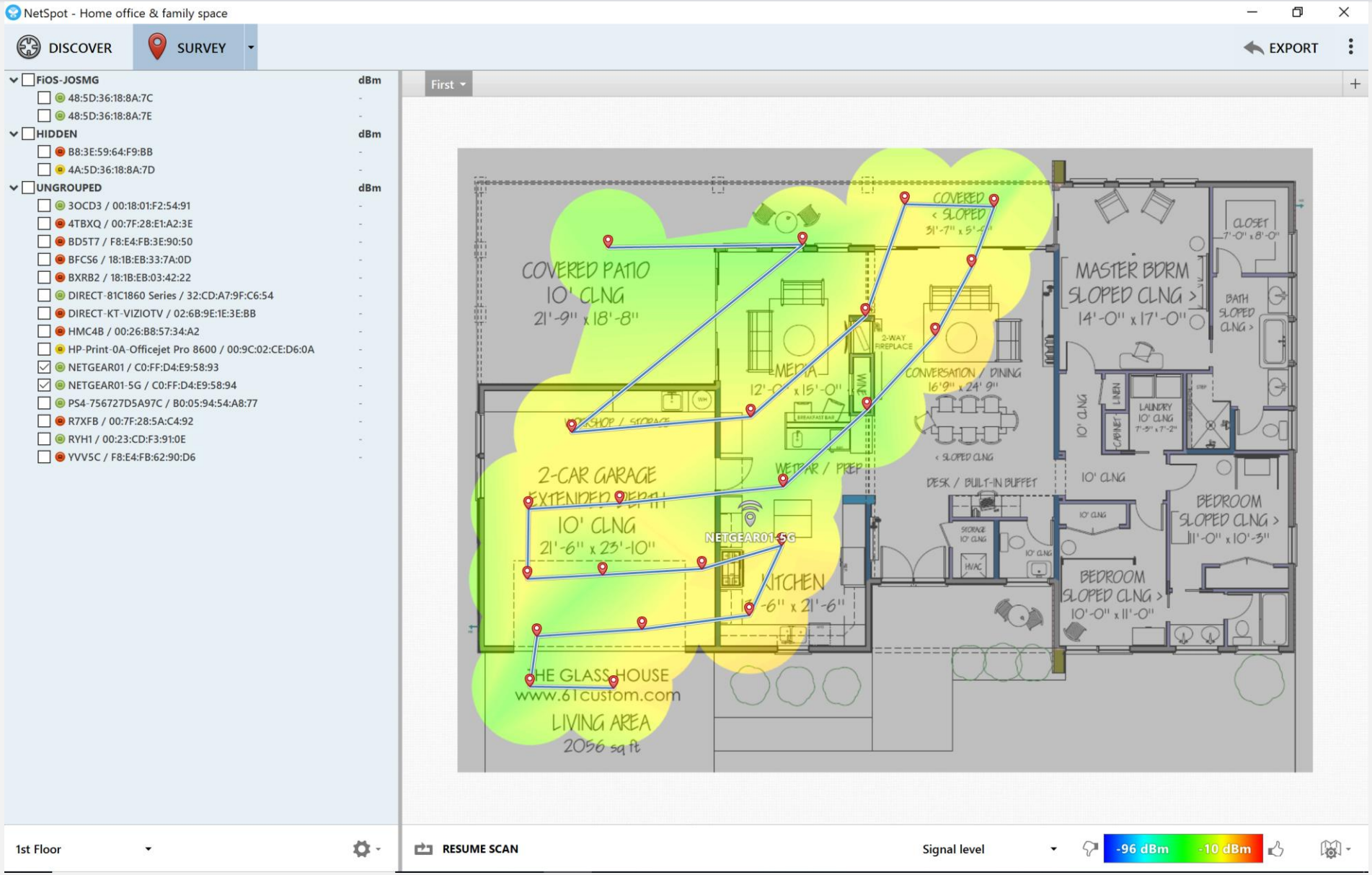
- Site survey dictates location and boundaries of access points
- Position of each access point must be checked to ensure it is within reach of a wiring closet
  - Ethernet has a distance restriction of 100 meters with Cat 5 cabling
- Use mixture of omnidirectional and semi-directional antennas

Coverage Assessment

- After access points are placed and enabled, assess coverage:
  - Manually
  - Through use of predictive analytics

Coverage Assessment (Cont.)

- Example tool: https://www.netspotapp.com/
- Another example: Ekahau heat mapper
- Manual method
  - **Passive mode:** A client card is used to collect the RF measurement of receive signal levels, signal noise, and signal-to-noise ratios
  - **Active mode:** Client station authenticates and associates with access points, working at Layer 1, Layer 2, and Layer 3
- Predictive method
  - Uses predictive modeling applications and simulation software to create visual models of RF cell coverage



University of Nevada, Reno