CellStream, Inc.
Instruction. Knowledge. Skills.

Troubleshooting Wi-Fi / WLAN Networks

Presentation to Oklahoma Broadband Association – August 2024

CellStream, Inc. Copyright Notice

CellStream, Inc.

Instruction. Knowledge. Skills.

CellStream, Inc. was founded in March of 1998. We are a telecommunications consultancy, solving problems and educating our clients in the latest technologies. Our primary clients are the people that help bring all of us the Internet itself, and all its associated technologies. From network and computing equipment manufacturers, to service providers, and data networking companies, to technology experts themselves. We offer a broad set of Consulting Services. Our consulting strengths are in inter-networking, network design, network management, network protocols, computing, and engineering, with a focus on converged voice, video, and data services over large, complex, high bandwidth wired/wireless networks and network solutions. CellStream Consultants bring hundreds of years of cumulative, front-line experience across a range of specific technologies. From Optical to Wireless, and from hardware to software, our experience base can help in all aspects of our clients needs. We found that along with our skills in consulting, design, and collaboration, that our experience is often invaluable to our clients. This experience places us in a position of mentoring and educating our clients, and led to development of a training curriculum. Our enhanced Learning Services enable our clients to master technologies and processes in products and services anywhere/any time using Internet technology with minimized training lead times and cost control. We offer a number of technical training courses [see the Courses Listing page], and we also support e-learning: check out the Online School of Network Sciences. To contact us click here.

CellStream, Inc.

Main Web Site: www.cellstream.com Online School of Network Sciences: www.netscionline.com

Phone: +1 866-659-1014 toll free * Email: info@cellstream.com

Some initial points….

- Troubleshooting Wi-Fi network issues can be methodical and straightforward <u>if you follow a rigorous process to assessing and researching the problem</u>
- Troubleshooting WLAN Networks is <u>Not Easy</u>
- Troubleshooting WLAN's is First: <u>Evidence Gathering</u>

Unlike the picture, gathering digital evidence on WLAN's is dealing with things we can't see. Wireless signals are invisible. Connections come and go. Witnesses are difficult to find and sometimes understand. There is rarely a "smoking gun".

So you must be rigorous in gathering evidence – facts – and then assembling this information into a meaningful possible cause.

STOP DOING THIS →

"Your network is slow?"

"Can you unplug and restart the router?" or

"Can you unplug and restart the AP/modem?" or

"Can you reboot the computer?"

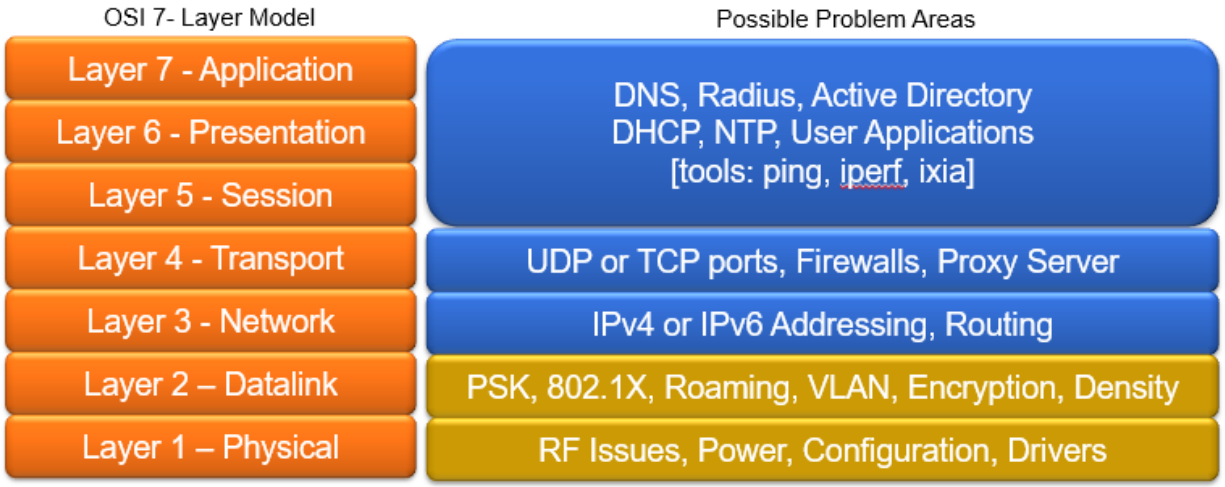
These are not "fixes".

These are not troubleshooting.

These practices may temporarily mask actual problems.

Troubleshooting WLAN Networks is Not Easy

- Follow a process – one that makes sense to you
- Always consider the Layered Model when initially thinking about the problem
- Before diving into WLAN issues:
  - Is the problem on the wired LAN or the Wireless LAN?
  - Is the problem client side or Access Point side?
  - Is the problem a WLAN issue – meaning Layer 2 and down?
  - If the problem is Layer 3 and up, may be better off troubleshooting using packet capture without Monitor Mode
    - Do not want to confuse WLAN retries and TCP re-transmissions
    - We may need decrypted traffic to do troubleshooting of user sessions



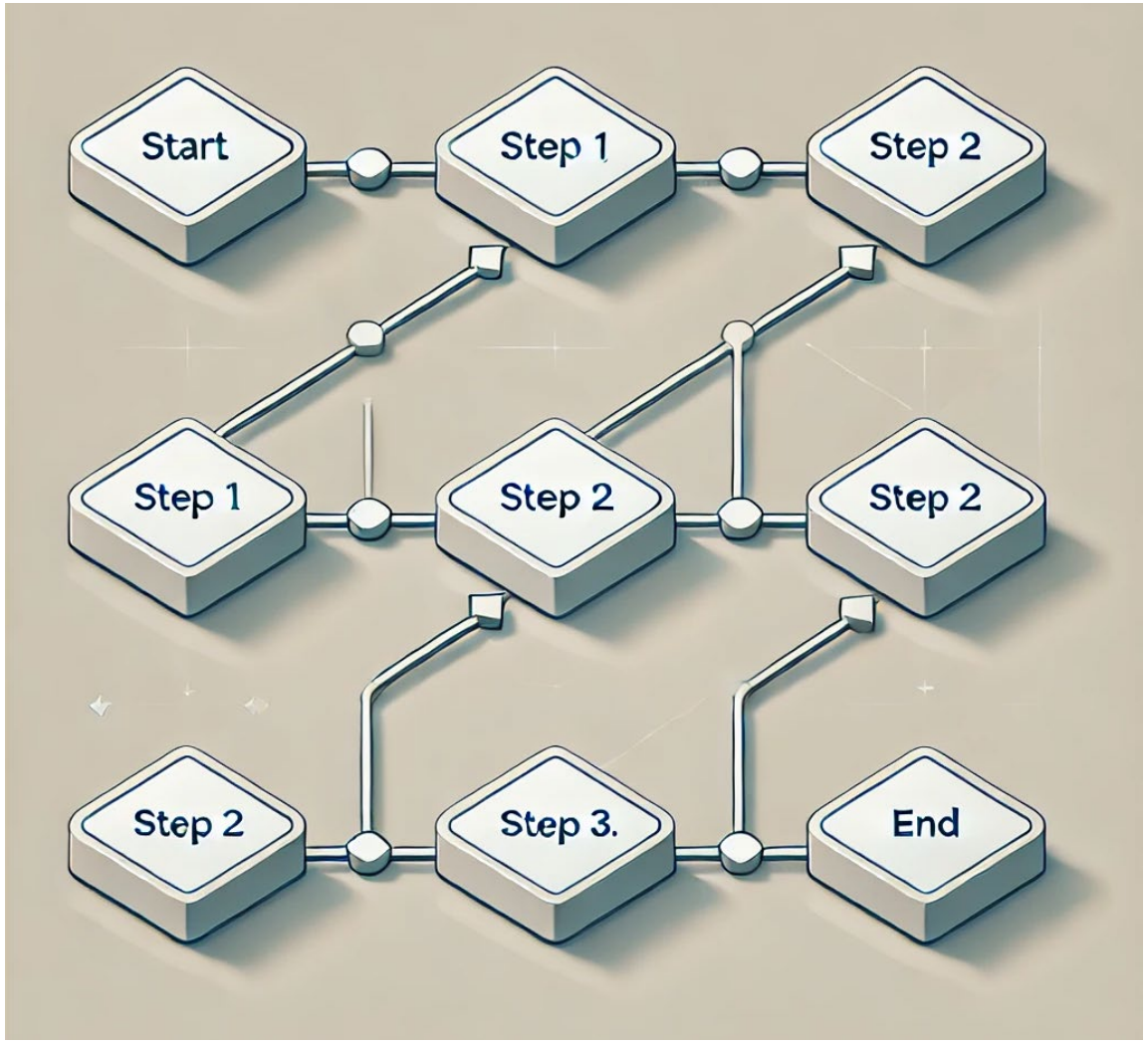
Anything above Layer 2 is not actually a WLAN issue

Keep the end goal in mind…

- What is the root cause of the issue?
- We don’t want to just fix the issue…
- You have to be able to justify why a corrective action was the ultimate cure

General Troubleshooting Workflow

- ❑ Identify and define the problem
- ❑ Checking Physical Connections
- ❑ Check the Wi-Fi Physical Layer Integrity
- ❑ Check Interference Types/Levels
- ❑ Check Wi-Fi Network Settings
- ❑ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



Further Defining the Problem – 1st Step

- Parse the problem statement/reported problem
- Define all terms used
- Expand and Explain
- Ensure the problem statement includes as many answers as possible to:
  - What?
  - When?
  - Where?
  - How?
  - Who?
  - How much? How Many?
  - Which?

- "When people on my network stream Netflix, my latency while gaming goes to a constant 500+ms, making any online game completely unplayable."

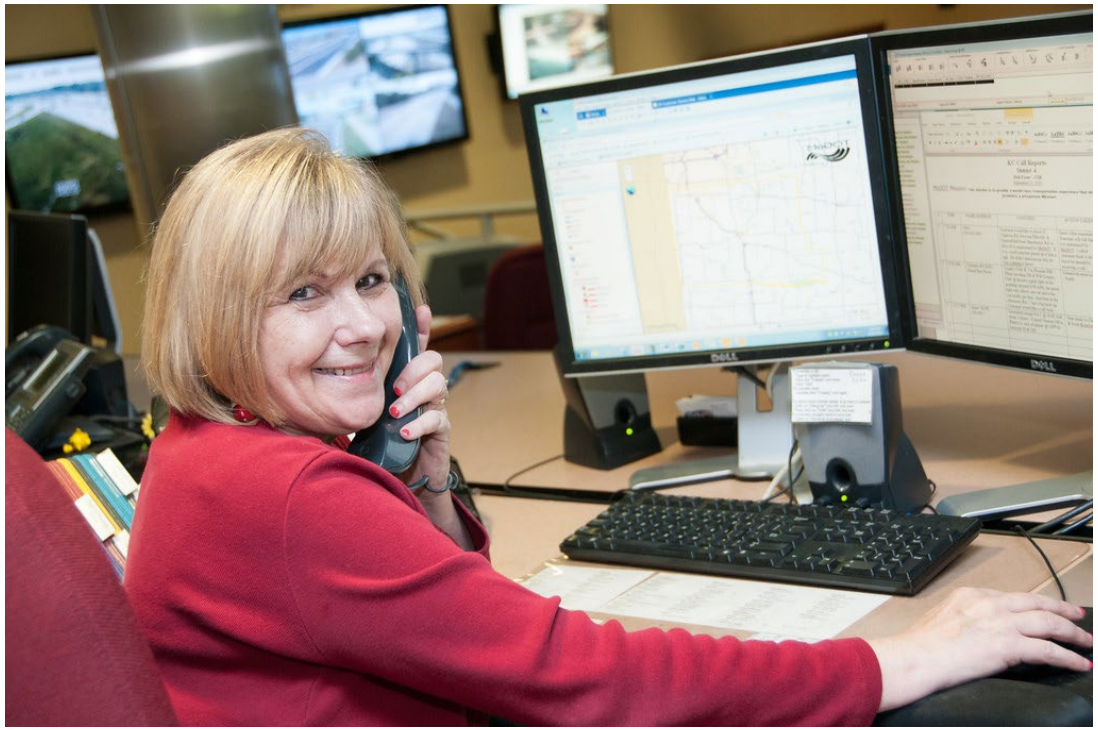
Further Defining the Problem

- Search for Possible Symptoms:
  - Slow speeds, intermittent connectivity, or no connection
- Identify Devices Affected:
  - Check if the issue is with one device or multiple devices
- Verify Service Status:
  - Check for outages or service issues
- Prior Support:
  - What steps have already been taken?

- Further Questions:
  - When does the problem occur?
  - Does the problem impact a single device/station or all stations?
  - How often does this problem occur? Is it constant?
  - Is the problem reproduceable? If so, how?
  - Did the problem emerge from recent changes?
  - Has this problem occurred previously? Is it new?
  - Did the problem change?
- Other questions…..

Hint for Success:

- Take a team effort to this first challenge to properly define the problem



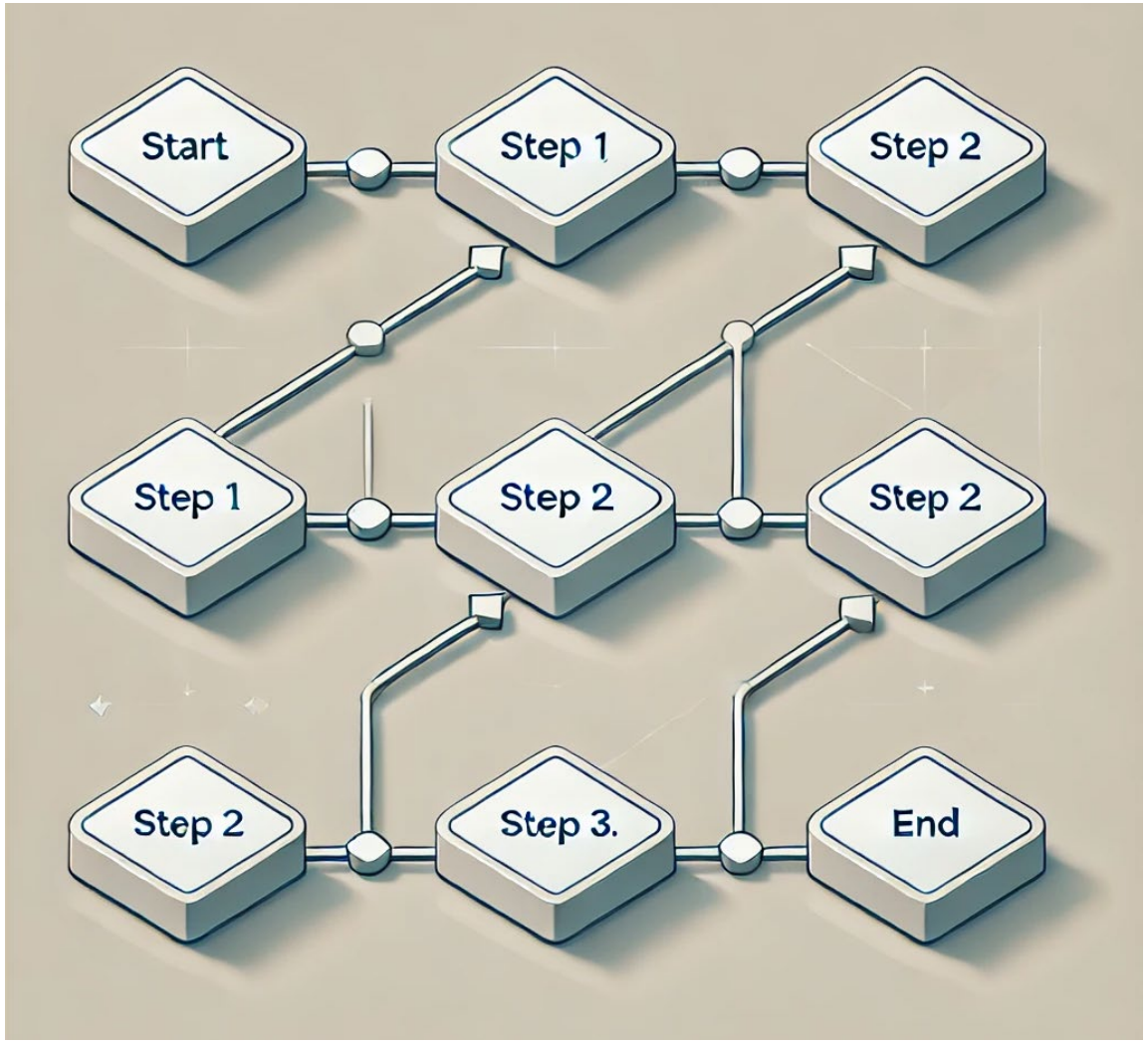
CSR – Customer Service Representative

+

FSR – Field Service Representative

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ❑ Checking Physical Connections
- ❑ Check the Wi-Fi Physical Layer Integrity
- ❑ Check Interference Types/Levels
- ❑ Check Wi-Fi Network Settings
- ❑ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document

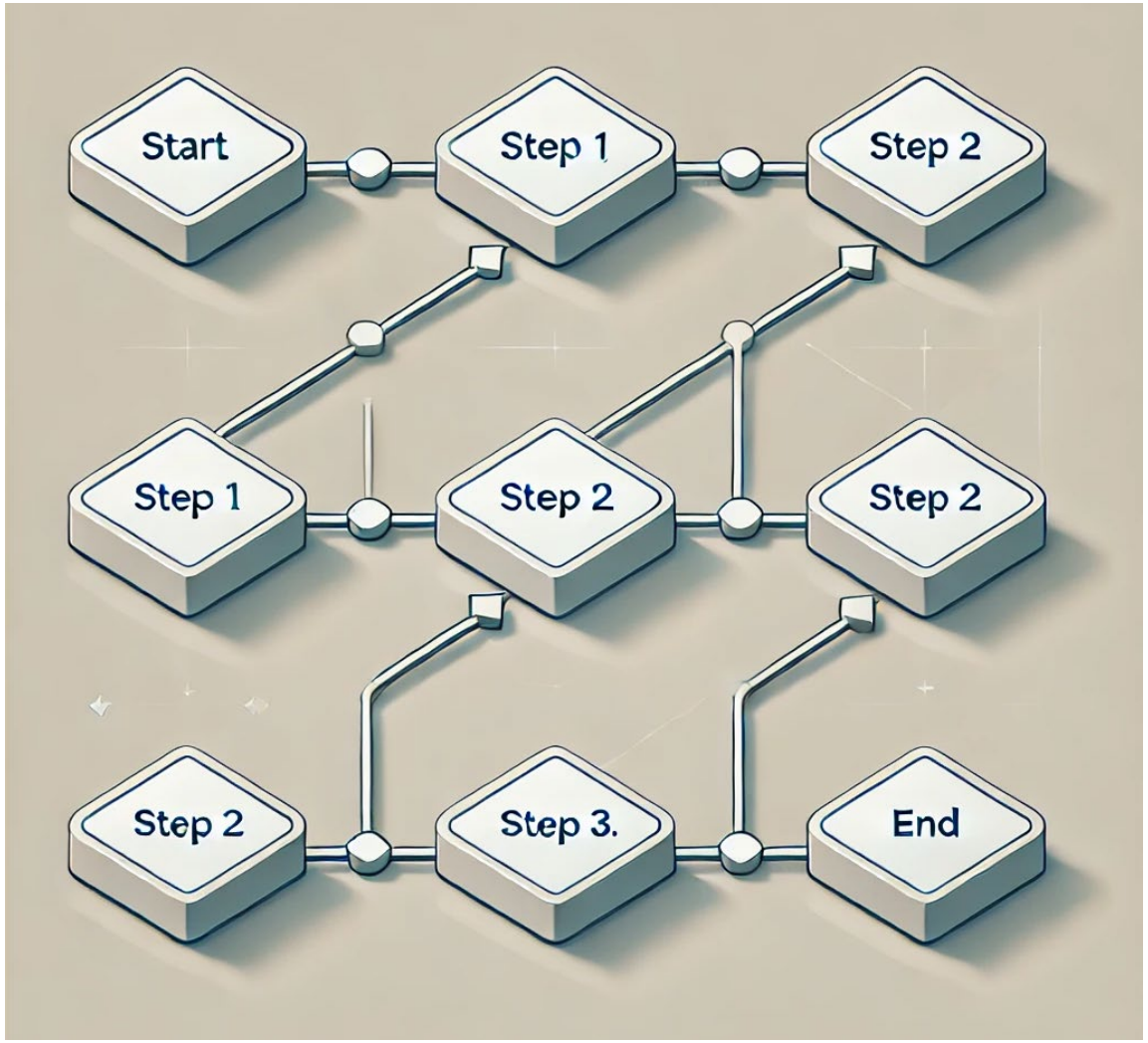


Check the Physical Connections

- Router/Modem:
  - Ensure the router and modem are plugged in and powered on
  - Is the power cable loose on either end?
- Cables:
  - Verify all Ethernet cables are securely connected
  - Do they fall out? Are they clicked in place?
- Antennas:
  - Are the antennas securely connected? Broken? Loose?
- Any other devices such as a switch connected? Are their connections good?

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ❑ Check the Wi-Fi Physical Layer Integrity
- ❑ Check Interference Types/Levels
- ❑ Check Wi-Fi Network Settings
- ❑ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



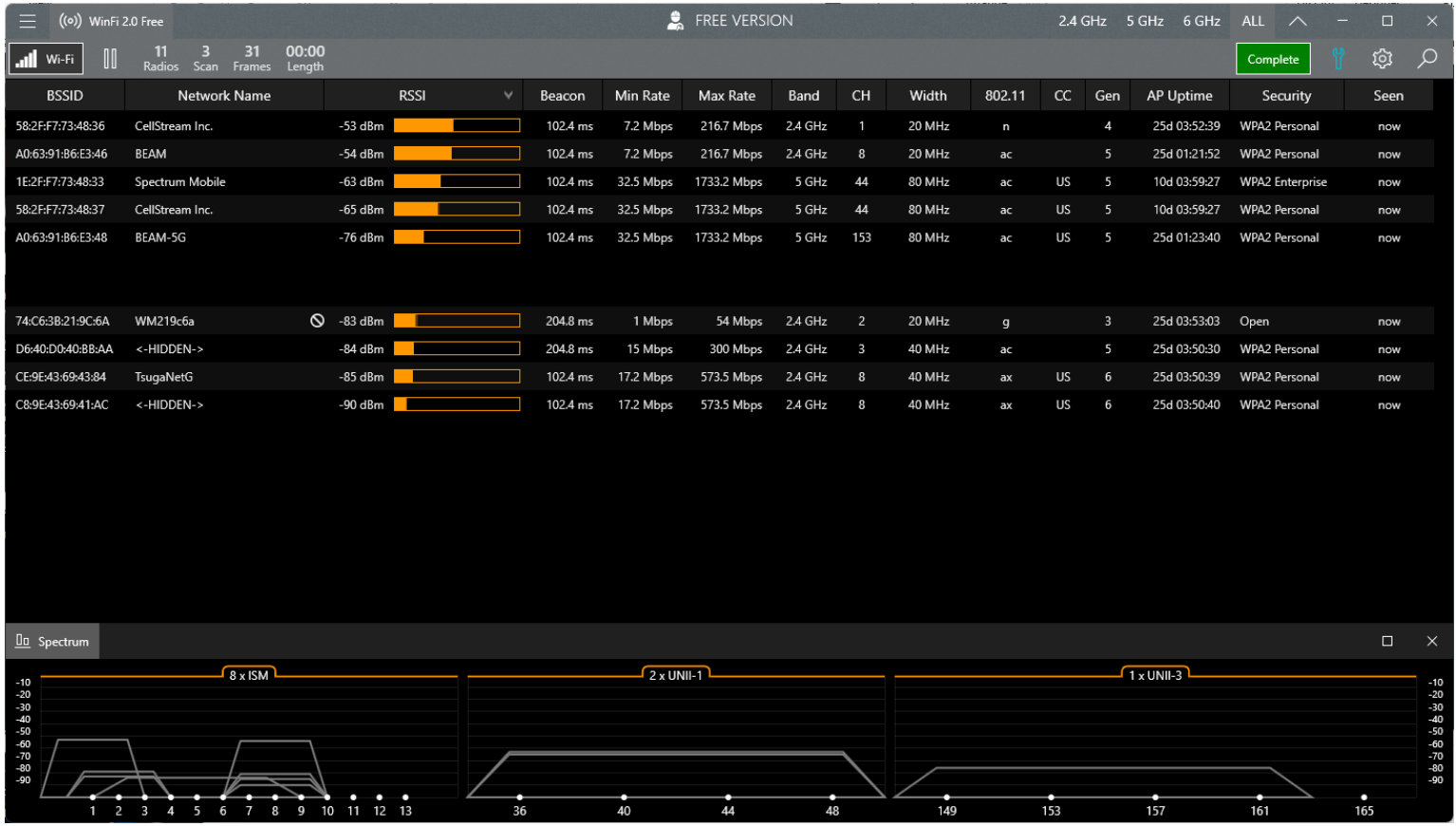
Check the Wi-Fi Physical Layer Integrity – Layer 1

- ❑ Evaluate Location: Ensure you are within range of the router
- ❑ Evaluate Obstructions: Consider any obstacles that might block the signal (walls, furniture)
- ❑ Evaluate possible sources of Interference: determine what frequencies are being used, what channels are being used

- Notes:
  - Checking Wi-Fi signal integrity involves using various tools and methods to measure how well the Wi-Fi signal is being transmitted/received by devices
  - The Personal Computer/Laptop is one of the best tools for the job

Mandatory – on every truck roll - A Quick Wi-Fi Scan/Survey

- Pick a GUI tool that you like
- Use your vendors' web interface/management tool
- Use the command line/terminal
- Get an understanding of the environment and the AP/STA players



Built-In Operating System Tools

On Windows Systems

- In a CMD window: `netsh wlan show networks mode=bssid`

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Andrew>netsh wlan show networks mode=bssid

Interface name : Wi-Fi
There are 7 networks currently visible.

SSID 1 : ATT9c9R495
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : b0:77:ac:ca:df:d0
         Signal             : 99%
         Radio type         : 802.11n
         Channel            : 1
         Basic rates (Mbps) : 6.5 16 19.5 117
         Other rates (Mbps) : 18 19.5 24 36 39 48 54 156

SSID 2 : A Rose in the city
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : dc:7f:a4:1b:18:86
         Signal             : 65%
         Radio type         : 802.11n
         Channel            : 9
         Basic rates (Mbps) : 6.5 16 19.5 117
         Other rates (Mbps) : 18 19.5 24 36 39 48 54 156

SSID 3 : ATTNzZju8s
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 64:55:b1:5f:d5:90
         Signal             : 93%
         Radio type         : 802.11n
         Channel            : 1
         Basic rates (Mbps) : 6.5 16 19.5 117
         Other rates (Mbps) : 18 19.5 24 36 39 48 54 156
```

On Mac Systems

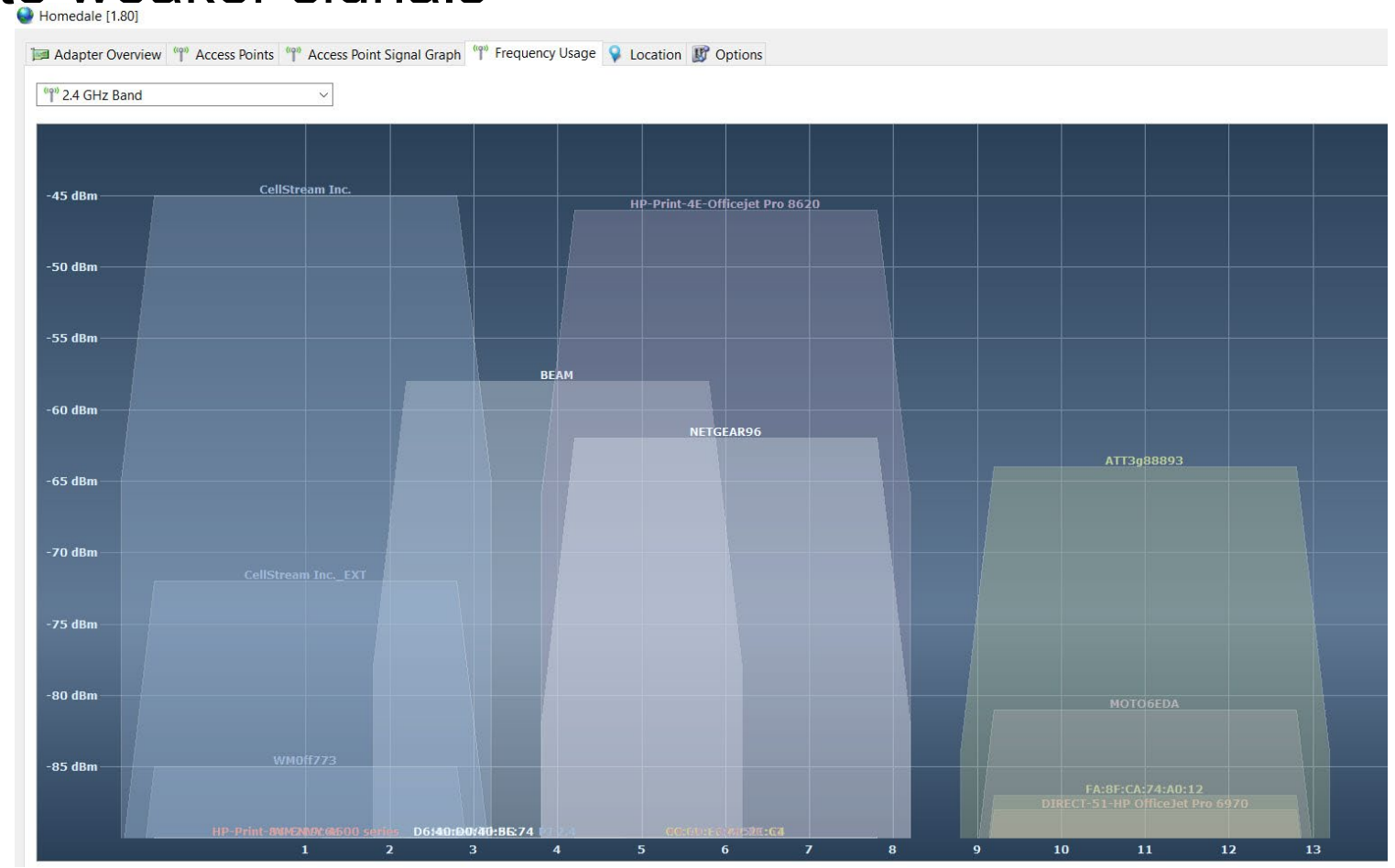
- Wi-Fi Menu: Hold down the Option key and click on the Wi-Fi icon in the menu bar to see detailed information including RSSI (Received Signal Strength Indicator) and noise

On Linux Systems

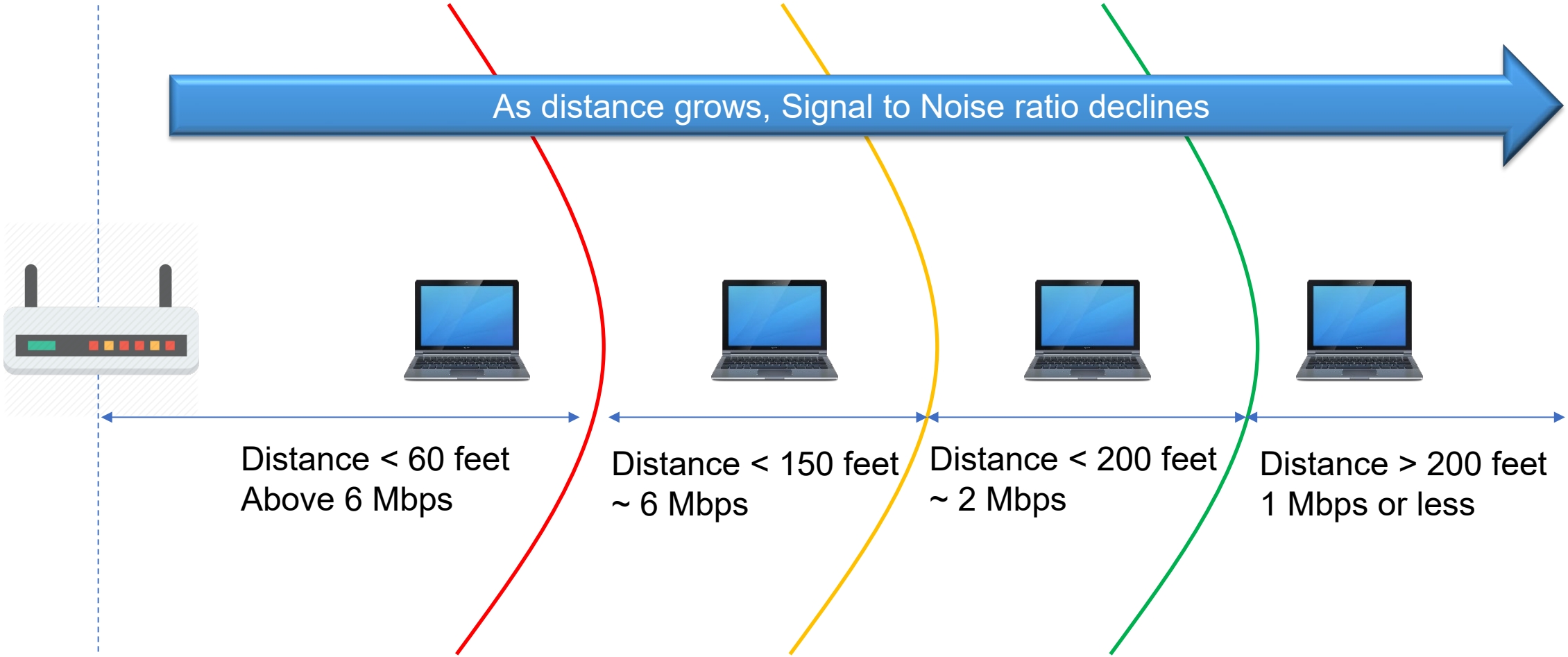
- Use the `nmcli dev wifi` command in the terminal to see a list of available networks with their signal strengths.

Interpreting Signal Strength

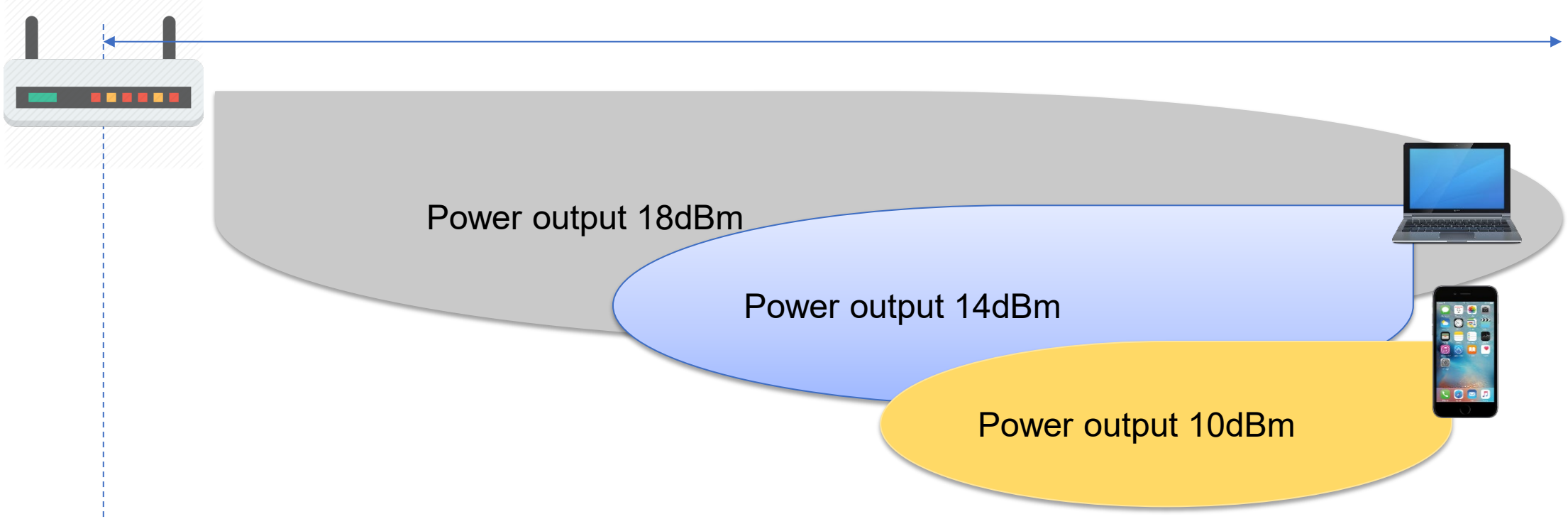
- RSSI (Received Signal Strength Indicator): Measured in dBm
- Higher negative values indicate weaker signals
  - -30 dBm: Excellent
  - -50 dBm: Very good
  - -60 dBm: Good
  - -70 dBm: Fair
  - -80 dBm: Poor
  - -90 dBm: Very poor



Distance and Speed in WLAN's



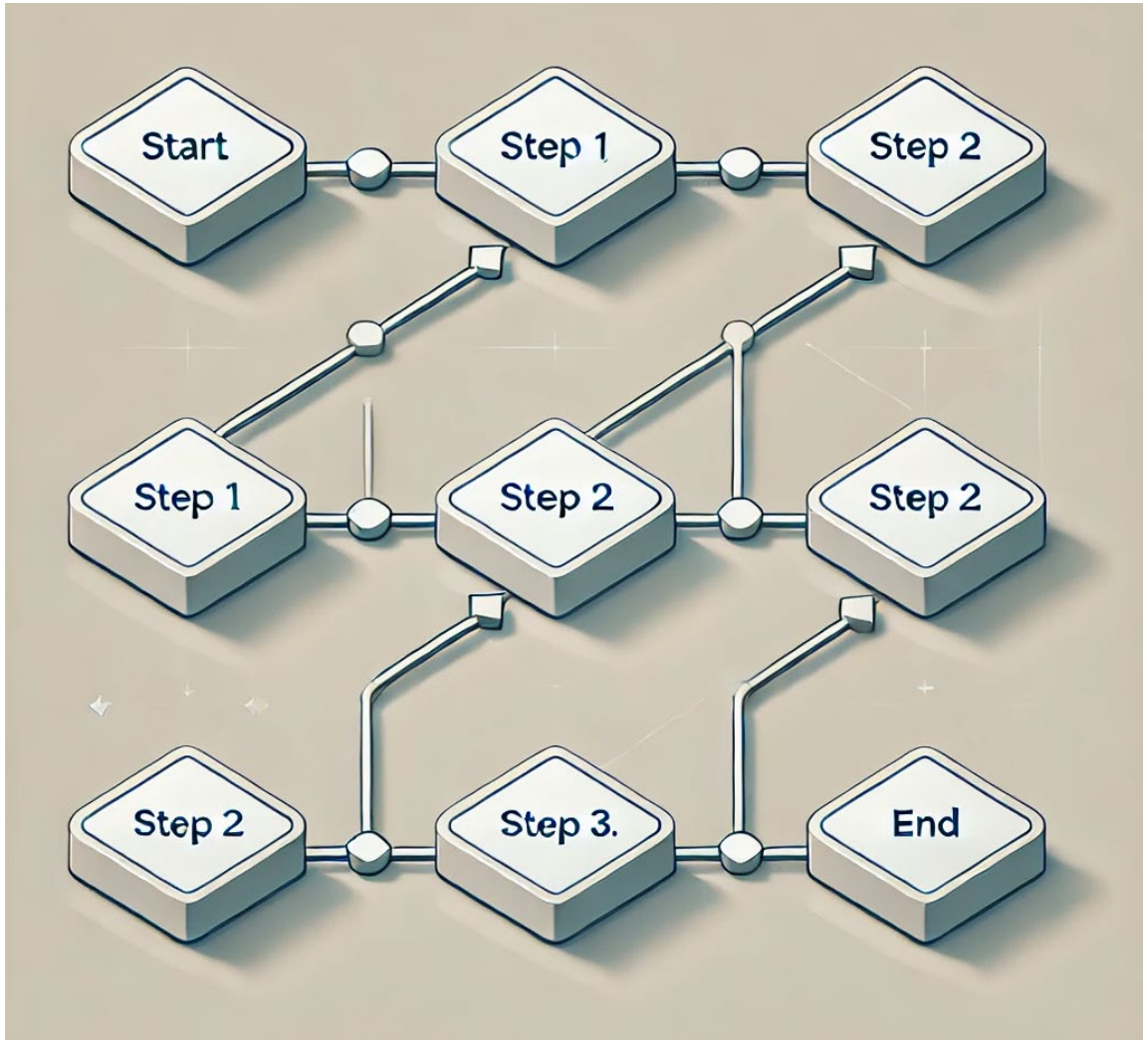
Consider the Problem of Asymmetric Tx Power



- Asymmetric power occurs because all WLAN communications is two-way
  - AP's can usually transmit further than clients
  - So client sees the AP, but the AP cannot see the client
- Therefore – we need to ask about device types, distances

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ❑ Check Interference Types/Levels
- ❑ Check Wi-Fi Network Settings
- ❑ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



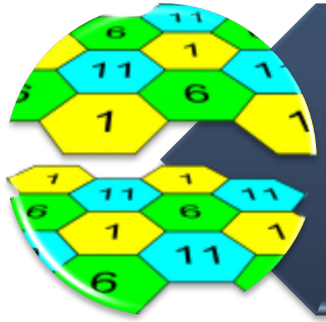
Is there Interference? Let's Define Interference Types!

Non Wi-Fi Noise

- These are non Wi-Fi devices emitting radio communications noise or competing for spectrum

Co-Channel

- Where every Wi-Fi device (AP's and Clients) compete for time to talk on the same channel

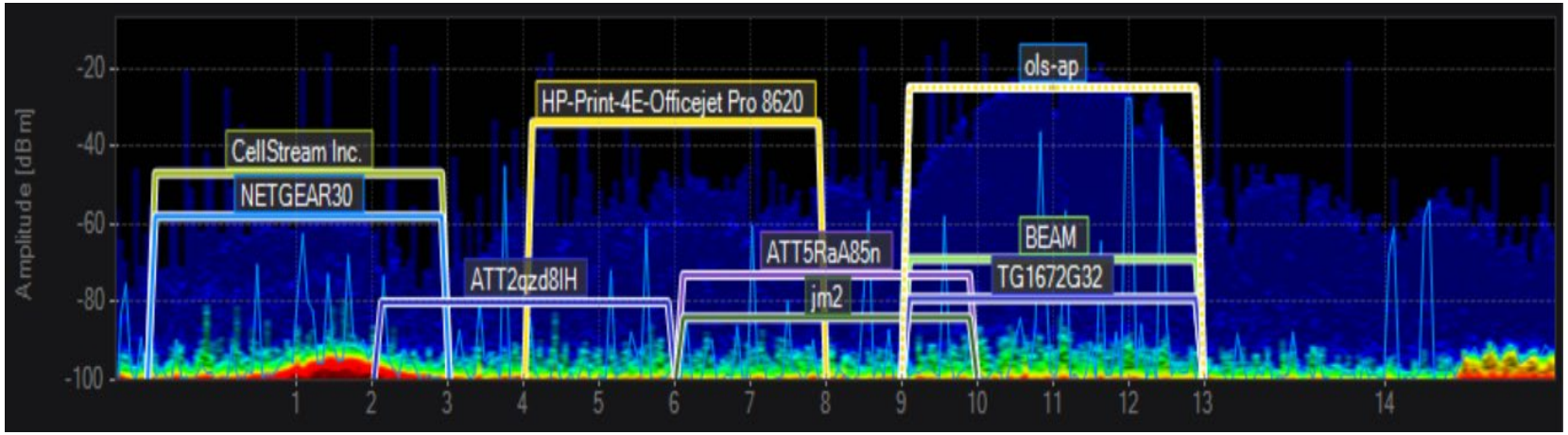


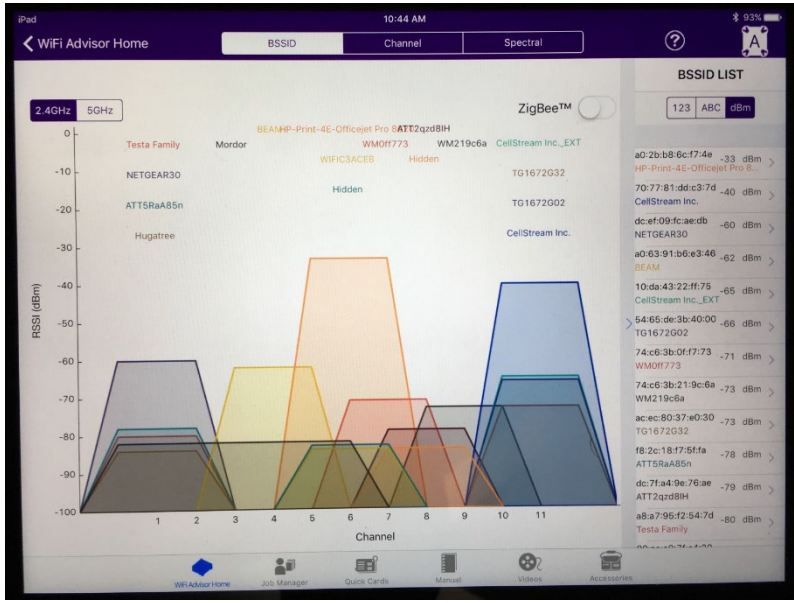
Adjacent Channel

- Where the Wi-Fi devices (AP's and Clients) are talking on overlapping channels, talking over each other

Necessary Tools: Wi-Fi Scanners vs. Spectrum Analyzers

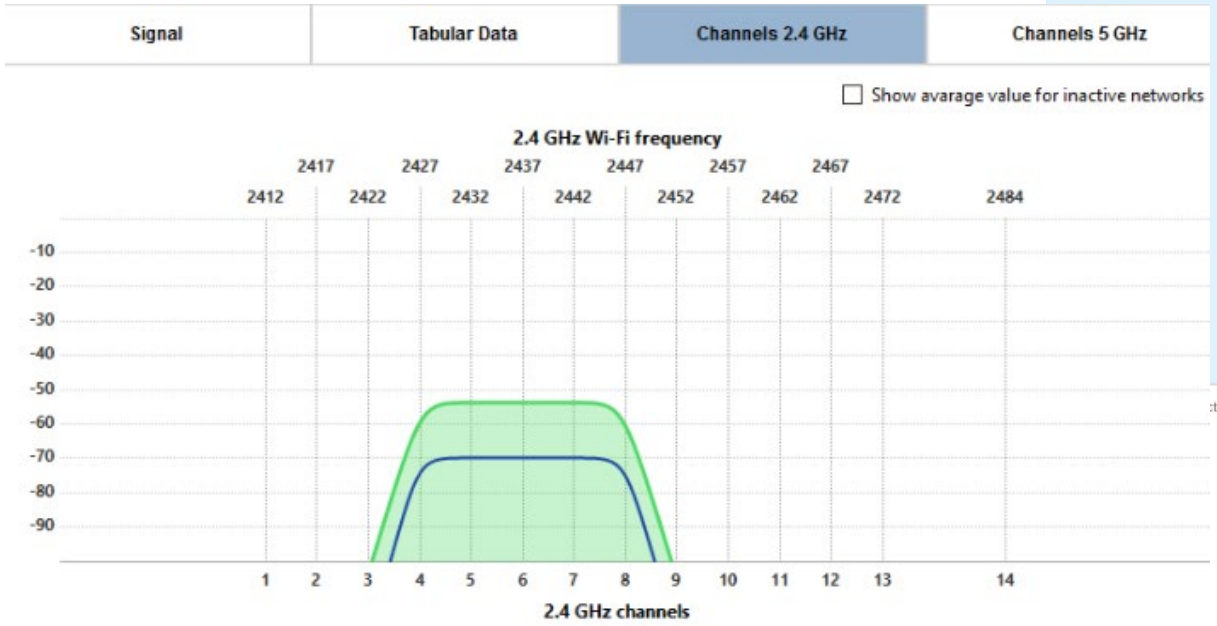
- Spectrum Analyzers listen to all frequencies in a particular range
  - We may see that there is outside interference from non-Wi-Fi devices
  - Need hardware and software
- Wi-Fi Scanners will use information from a Wi-Fi adapter to chart what frequencies and channels are being used
  - The problem is they do not show how much data exists on a given channel
  - Nor do they show interference from non-Wi-Fi devices
  - Usually just software
- Therefore, the technician may need both!

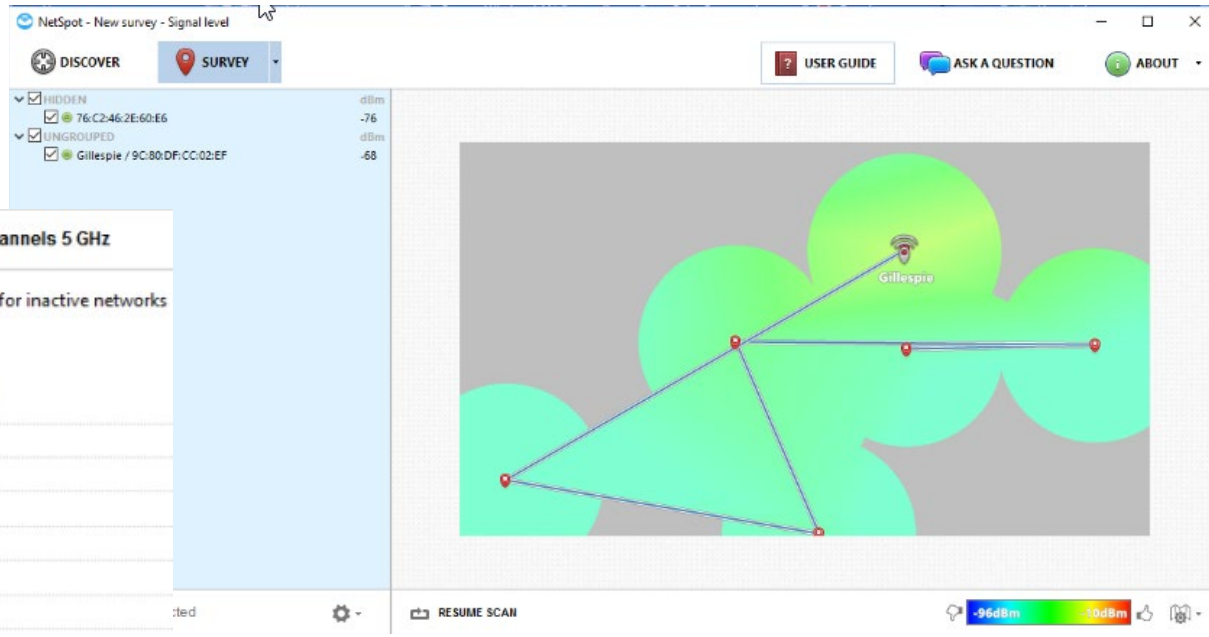




Where is that coming from?

- Using NetSpot – this is the survey:

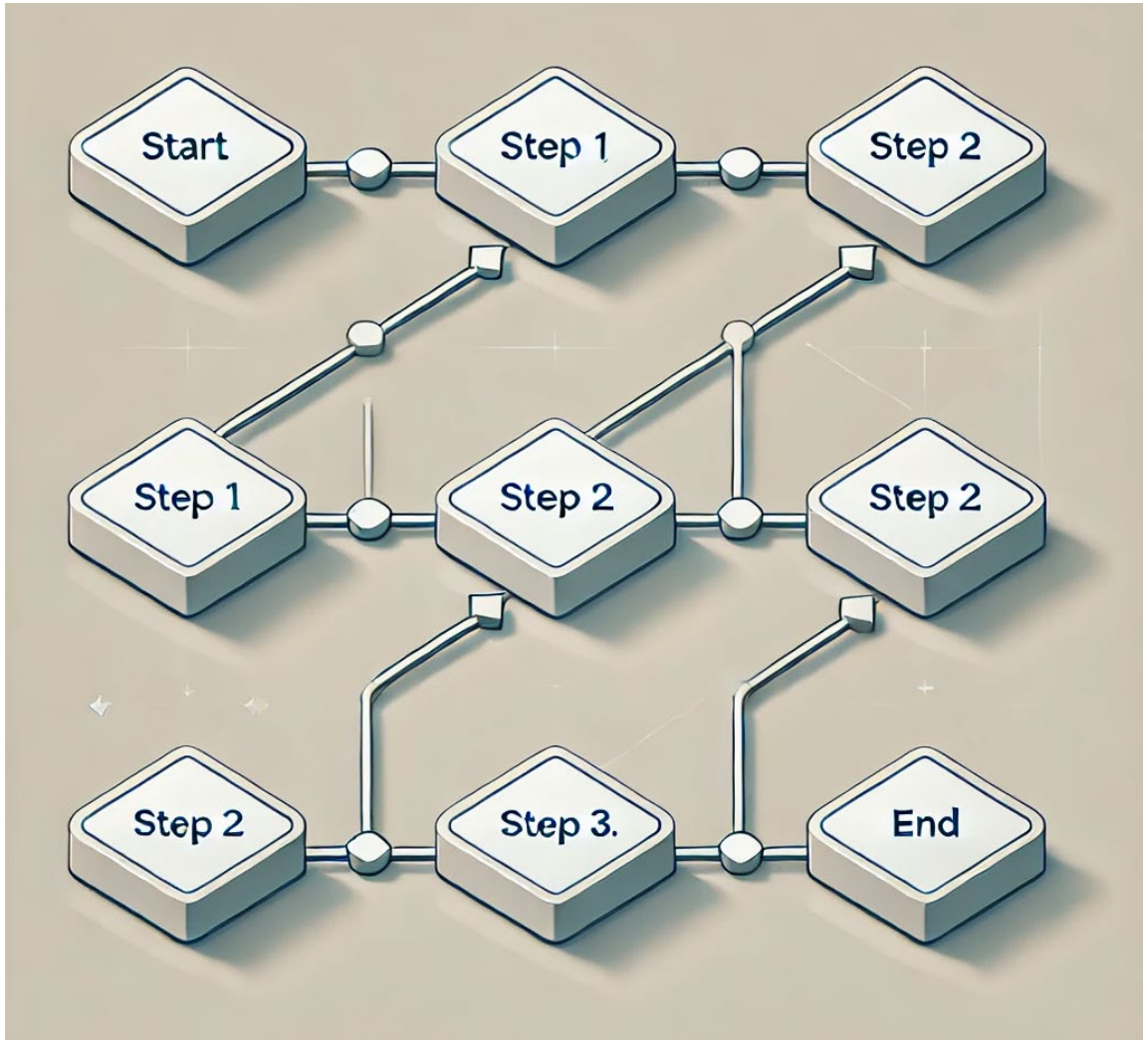




- Green signal is the AP, but what is the blue one?
- What could we do?

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ❑ Check Wi-Fi Network Settings
- ❑ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document

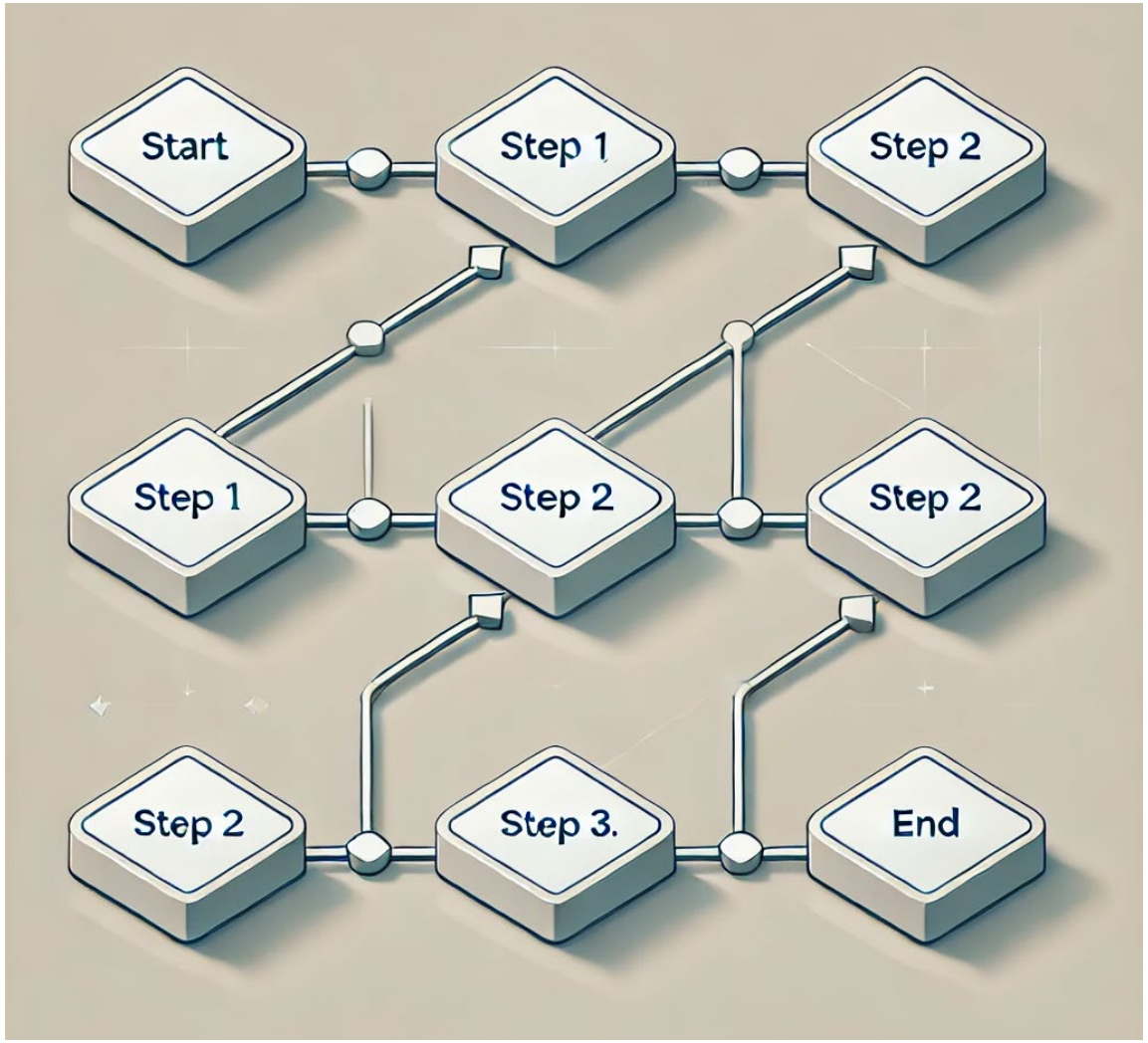


The Top Wi-Fi Settings to Watch Out For

- Channel Interference
  - **Channel Overlap**: Using a crowded or overlapping channel, especially in the 2.4 GHz band, can cause interference and slow speeds
  - **Auto Channel Selection**: Some routers may not effectively choose the best channel, leading to interference
- Incorrect SSID and Password Settings
  - **Wrong SSID**: Devices are trying to connect to a different network with a similar name – watch out for Extenders that use the same SSID as AP
  - **Incorrect Password**: Entering the wrong Wi-Fi password will prevent devices from connecting
- Advanced Wi-Fi Settings Misconfiguration
  - **Beamforming and MIMO**: Misconfigured advanced features like beamforming or MIMO (Multiple Input Multiple Output) can lead to connectivity issues
  - **QoS (Quality of Service):** Incorrect QoS settings can prioritize the wrong traffic, causing performance issues

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ❑ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



Making Sure Device Drivers are Up To Date

- There is an unfortunate problem in the industry: the rush to release products does not balance with the complexity of networking
- Never enough testing
- This leads to performance and security issues
- Result is a constant stream of software and driver updates
- A critical step in troubleshooting is to ensure all the latest firmware/drivers/software is in place
- That may eliminate problems – troubleshooting complete!

Router Firmware: Check for and install any available updates for your router.

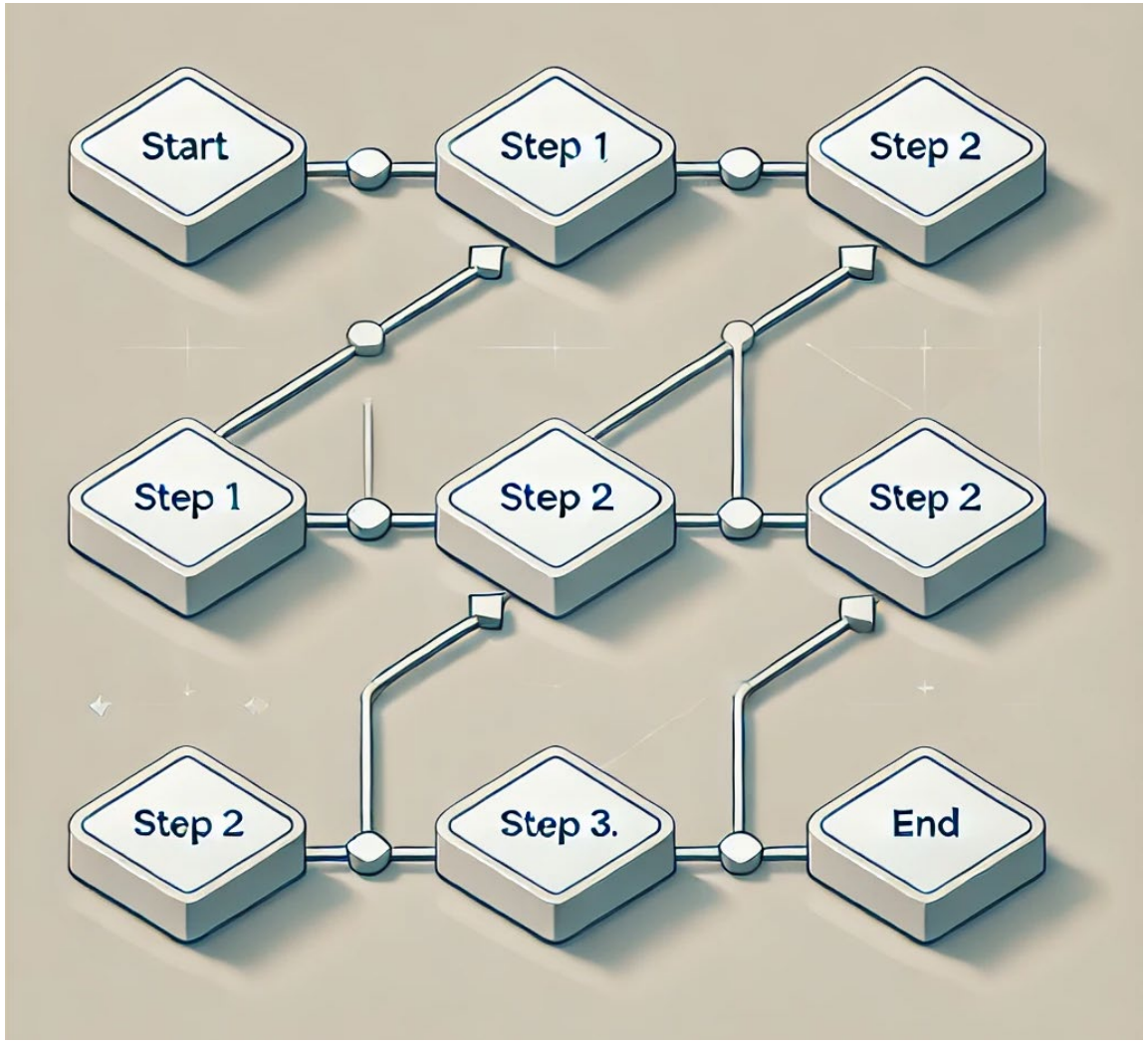
Device Drivers: Update the Wi-Fi drivers on your computer or other devices.

Drivers and Firmware

- Always check that the latest drivers and firmware are in use
- 802.11 amendments to the specifications lean heavily on backwards compatibility
- Legacy client-side drivers do not know how to handle new capability information/information elements/bits in the management frames
  - Be wary of issues that arise from new AP's and older client devices
  - Also update your own tools/sniffers so that they can process/dissect newer protocol formats

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ✓ Update any Firmware/Drivers
- ❑ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



General Network Settings – part 1

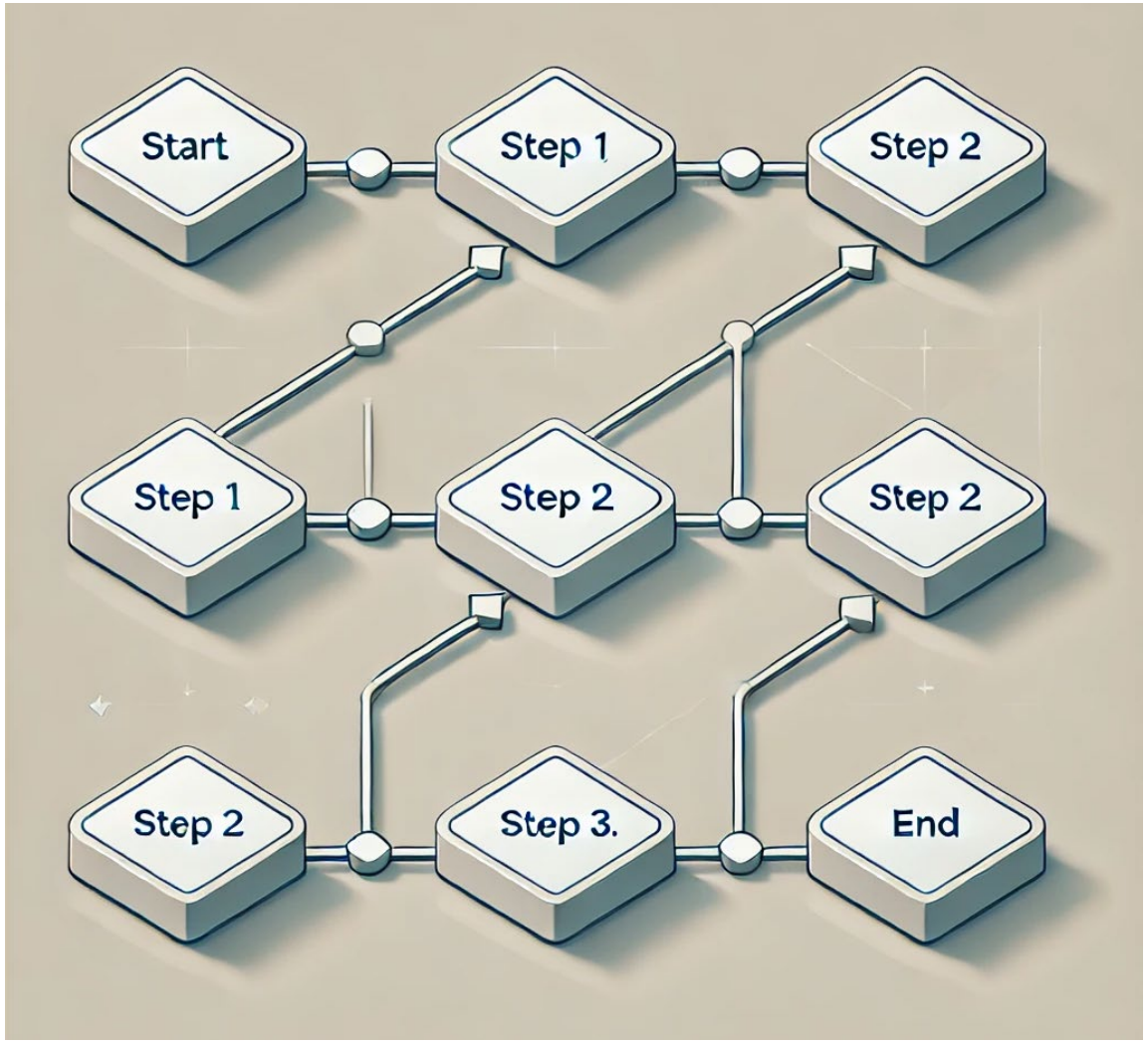
- Security Settings Issues
  - **Outdated Security Protocols**: Using outdated security protocols like WEP instead of WPA2/WPA3 can make the network vulnerable and may cause compatibility issues
  - **Incorrect Security Settings**: Mismatched security settings between the AP and client devices can prevent connections
- IP Addressing Problems
  - **DHCP Configuration**: Issues with the DHCP server can lead to IP address conflicts or devices not getting an IP address
  - **Static IP Conflicts**: Static IP addresses set on devices that conflict with the DHCP range can cause connectivity problems
  - **Network Address Translation**: Are the correct translation rules in place (look at addresses and ports)
- Network Mode Compatibility
  - **Mixed Mode Issues**: Using mixed mode (e.g., 802.11b/g/n) can cause performance degradation if older devices are connected
  - **Unsupported Modes**: Some devices may not support newer modes like 802.11ac or 802.11ax
- MAC Address Filtering
  - **Incorrect Filters**: Enabling MAC address filtering without properly configuring allowed devices can block access to the network
  - **Whitelist/Blacklist**: Misconfigured whitelists or blacklists can prevent devices from connecting

General Network Settings – part 2

- Roaming and Handoff Issues in Multi AP deployments
  - **Inconsistent Settings**: Inconsistent settings across multiple APs can cause roaming issues where devices don't seamlessly switch between APs
  - **Fast Roaming**: Misconfigured fast roaming settings (e.g., 802.11r) can cause connectivity issues
  - Is it easily possible to determine which AP or Extender the customer device is connected to?
- Bandwidth and Traffic Management
  - **Bandwidth Limiting**: Limiting bandwidth for certain devices can affect their performance
  - **Traffic Shaping**: Misconfigured traffic shaping settings can lead to poor network performance
- Guest Network Possible Issues
  - **Isolation Settings**: Guest networks with improper isolation settings can prevent access to necessary resources or the internet
  - **Limited Bandwidth**: Guest networks might have bandwidth limits that affect performance

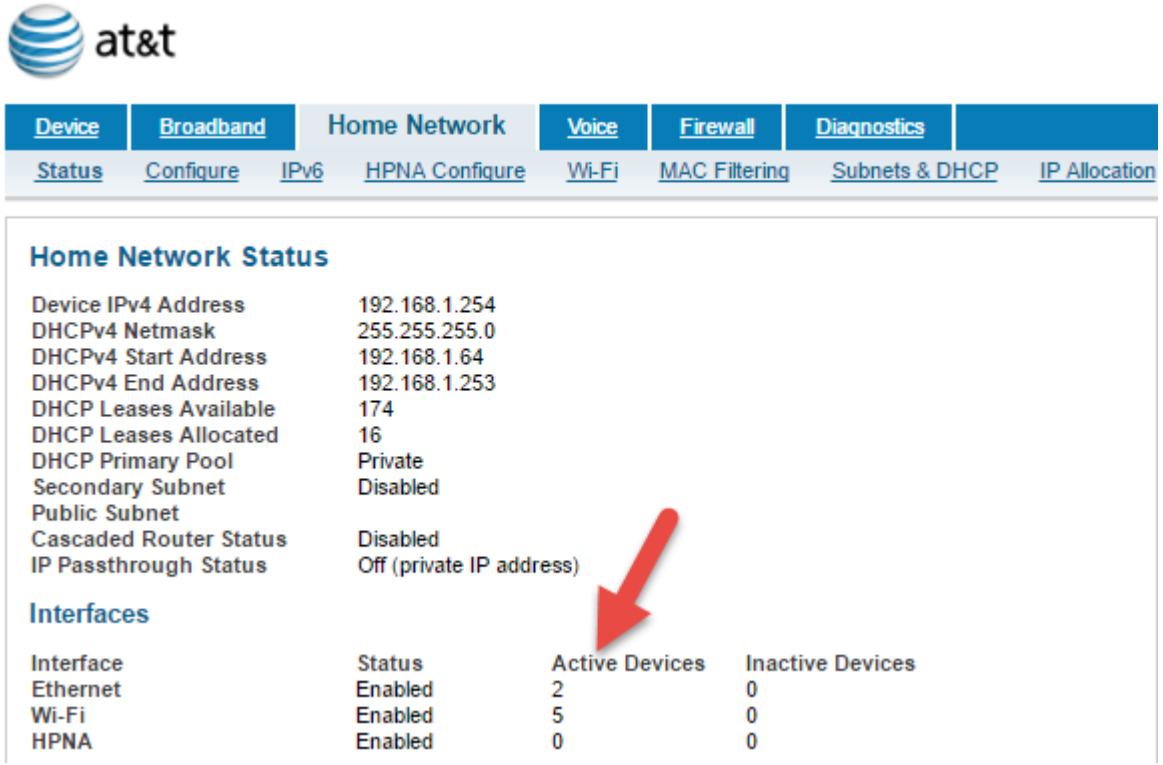
General Troubleshooting Workflow

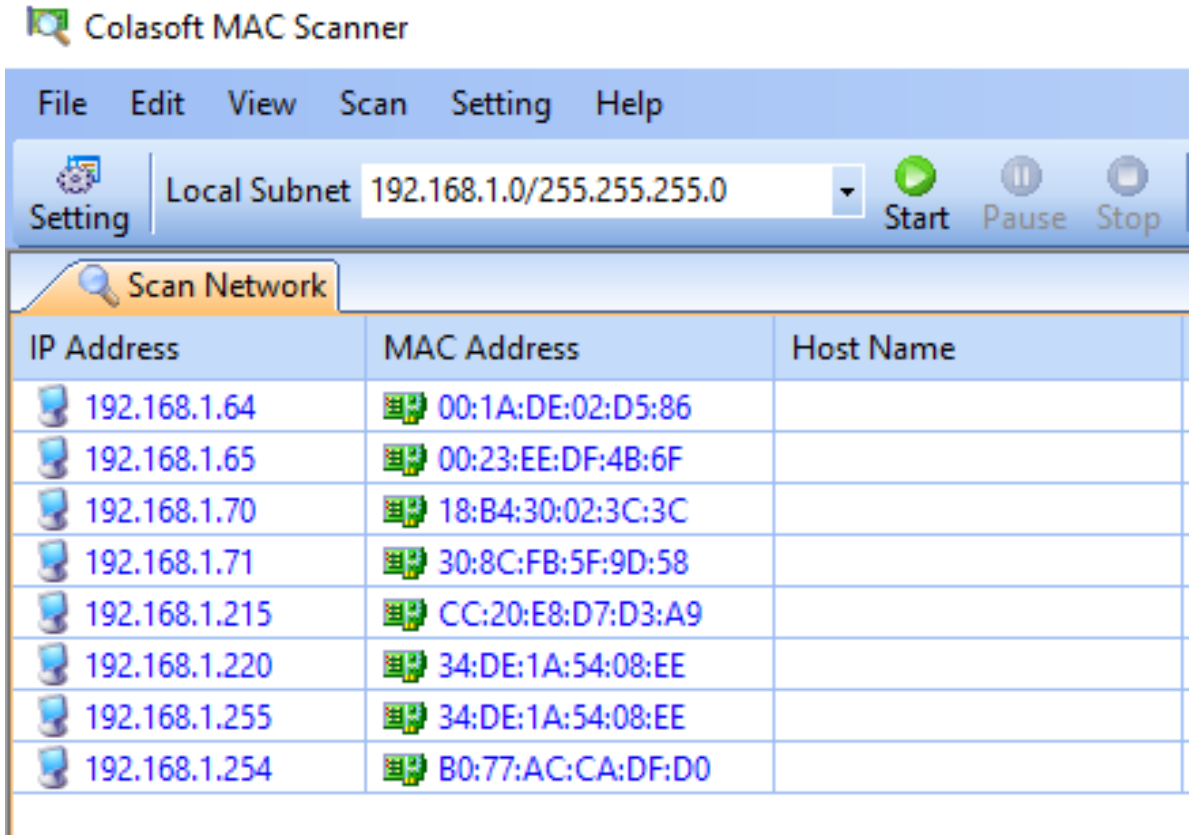
- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ✓ Update any Firmware/Drivers
- ✓ Check General Network Configuration
- ❑ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



How Many Connected Devices?

- Two answers:
  - 1: Look at the AP/Management ACS
  - 2: Use an ARP scan



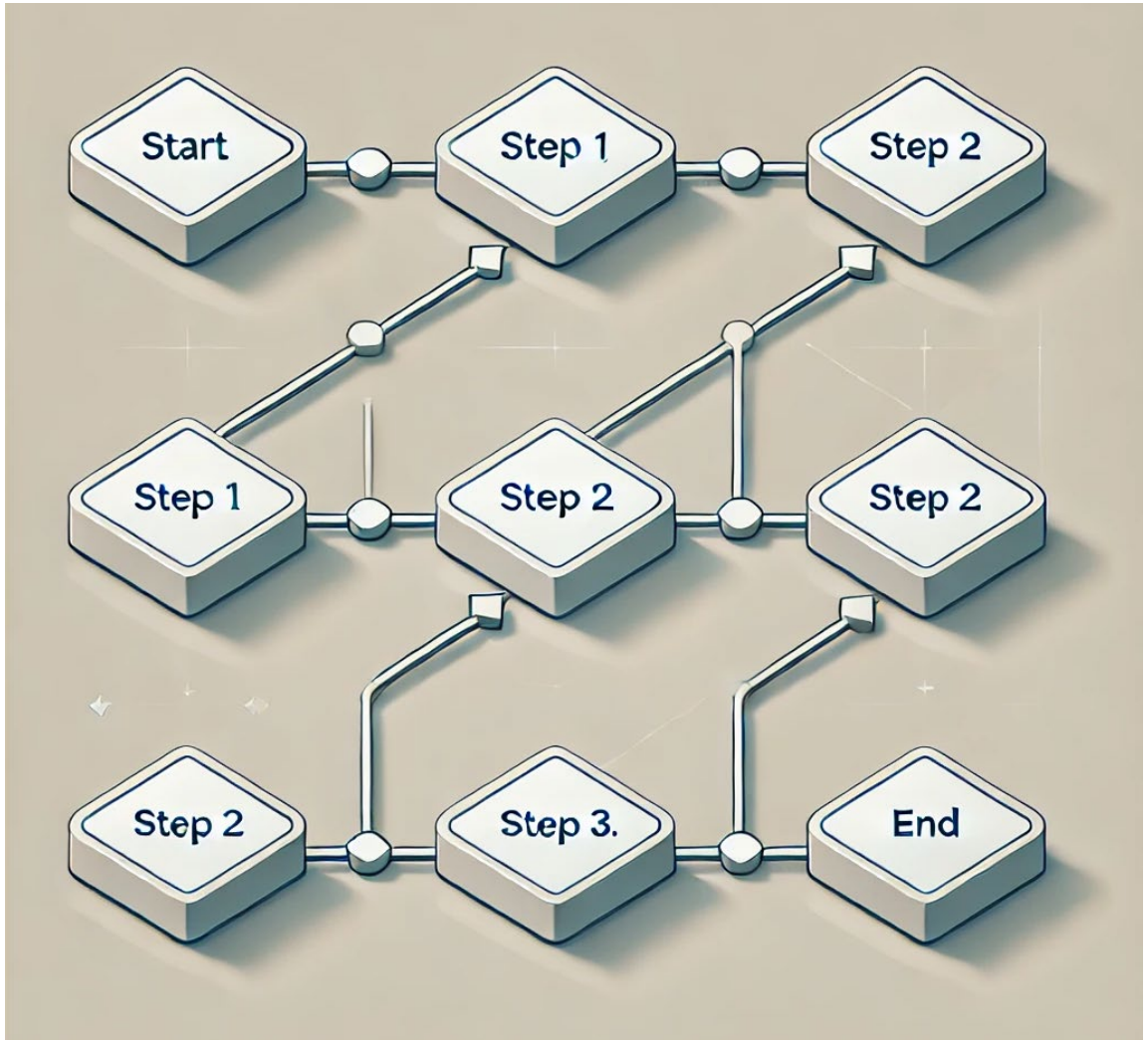


How busy is the WAN or WLAN Link?

- You can identify delays or lost packets by sending ping packets from your wireless client
- If there is more than 10ms of delay, there may be a problem such as:
  - Weak transmit signal from the client (the host does not reach the AP)
  - The AP could be saturated with connected clients)
  - Interference (a third party signal could degrade your AP or client's ability to detect signals between them)
  - Weak transmit power from the AP (the AP does not reach the host) — not common in a properly deployed network, unless the client is too far away
- Keep in mind that water will also cause a reduction in radio signal strength for those making use out of outdoor APs or wireless on a boat

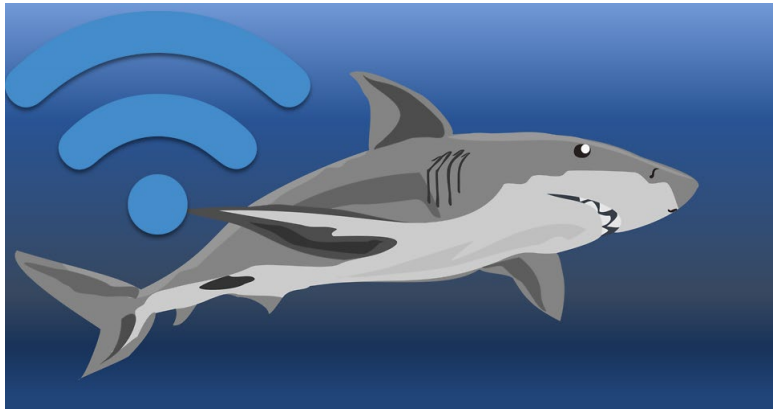
General Troubleshooting Workflow

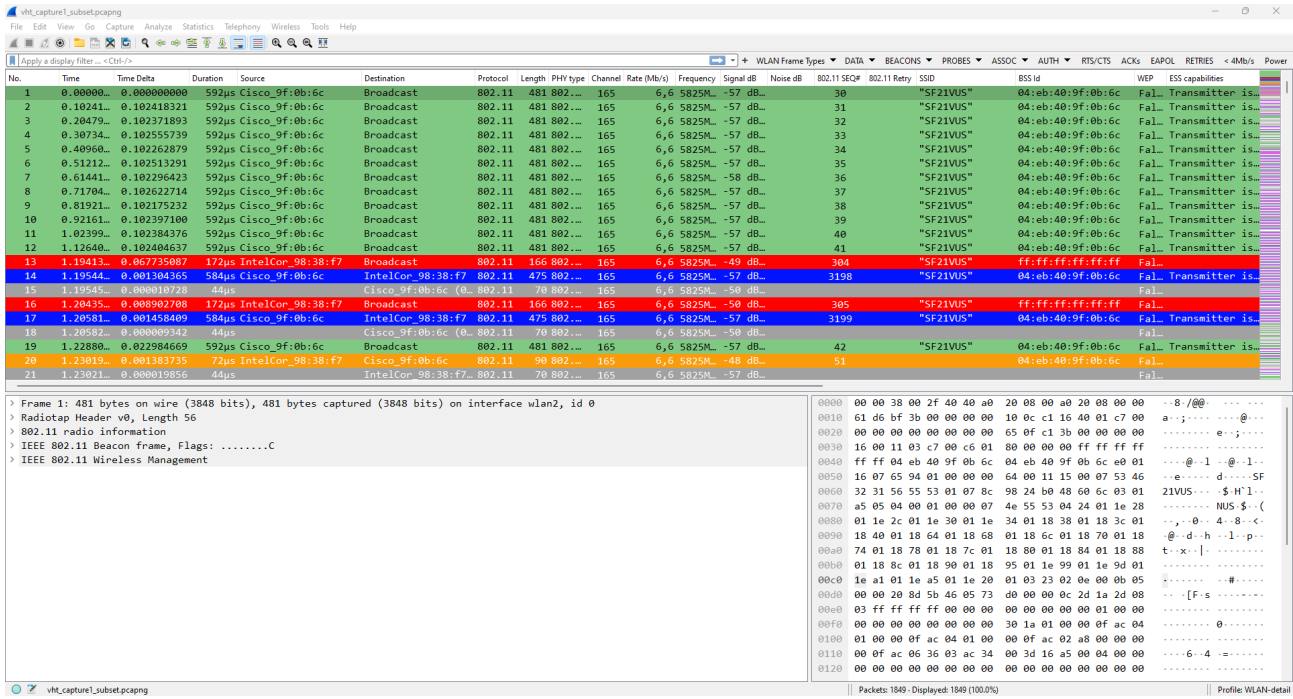
- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ✓ Update any Firmware/Drivers
- ✓ Check General Network Configuration
- ✓ Check for Network Overloading
- ❑ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



Do We Need to do Packet Capture?

- Generally, not for interference issues – Layer 1
  - Possibly for Co-channel interference
- Yes for:
  - Association
  - Authentication/Deauthentication
  - Roaming
  - Other Layer 2 MAC behavior issues
  - Delays
  - Retransmissions
  - Packet Loss
  - Sanity Checks





Insist on Windows? Here is what you need…

- My Windows Networking Tool
  - https://www.cellstream.com/download/windows-networking-toolkit/
- For accurate packet capture of Wi-Fi Traffic – you must be able to place the wireless interface in **MONITOR MODE**
- Windows can do this with a USB Wi-Fi interface, not the native one
  - https://www.cellstream.com/2024/03/25/a-list-of-usb-wi-fi-adapters-that-support-monitor-mode/
- You will need a free tool – WIRESHARK
  - www.wireshark.org
  - My WLAN Wireshark profiles https://www.cellstream.com/wireshark-profiles-repository/
- A good dose of skills and knowledge

Wireless Capture = Three Types of Frames

Data frames "wlan.fc.type==2"

Control frames "wlan.fc.type==1"

- Acknowledgement
- Request to Send
- Clear to Send

Management frames "wlan.fc.type==0"

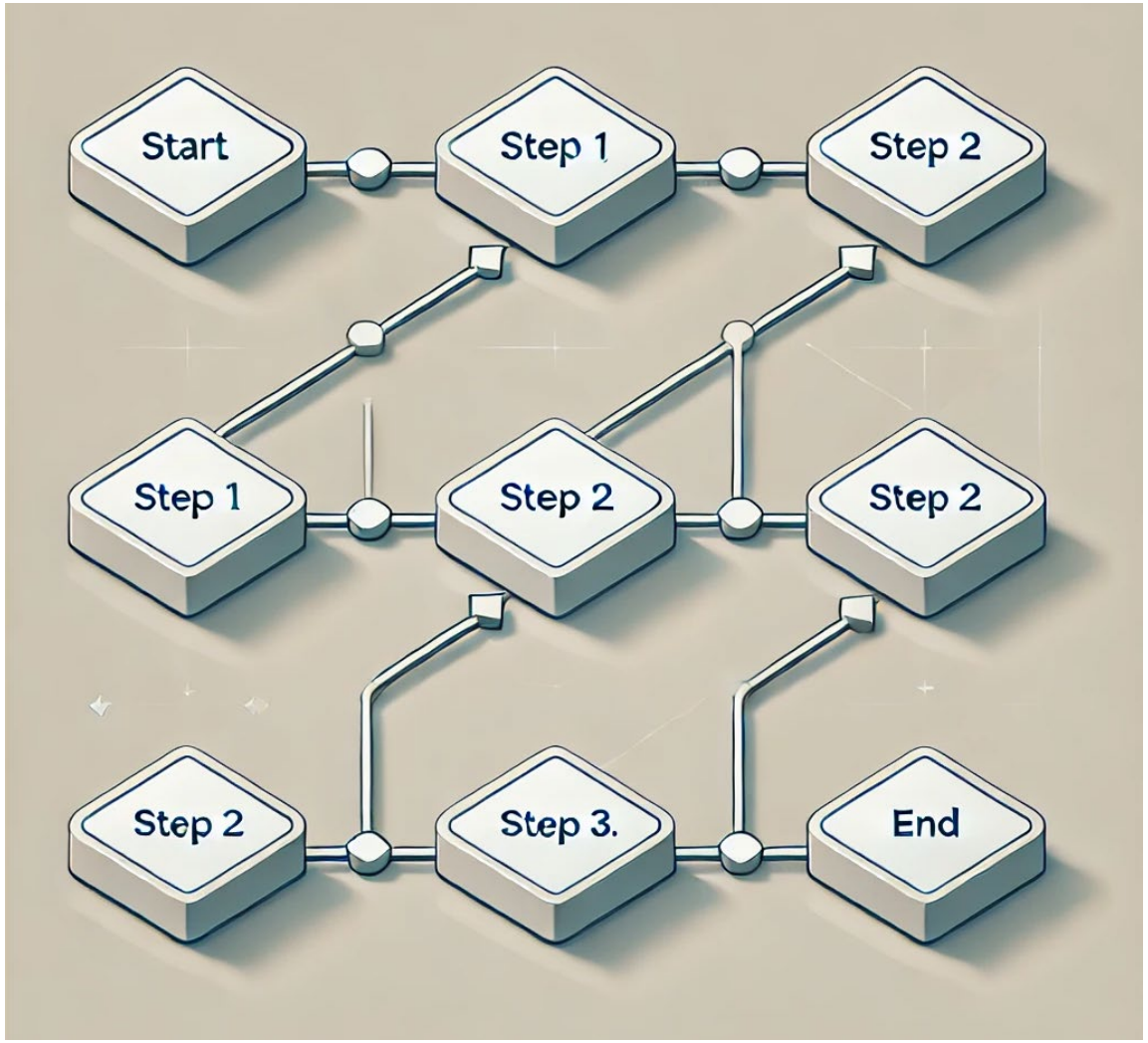
- Beacons
- Probe Requests / Probe Responses
- Association Requests / Association Responses
- Reassociation Requests / Reassociation Responses
- Disassociations
- Authentications / Deauthentications

Comparing AP and STA Capabilities

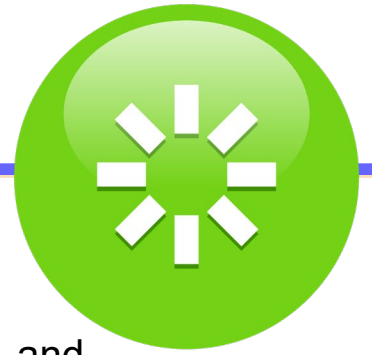
- Only discernable with a packet capture
- Step 1: Capture on the correct channel
- Step 2: Filter for Beacons from the SSID in question
  - wlan.fc.type_subtype == 0x0008 && wlan.ssid=="CellStream Inc."
- Step 3: Look for Associations from the STA in question
  - wlan.fc.type_subtype == 0x0000 && wlan.addr==de:ad:be:ef:ca:fe
- Step 4: Compare in Tagged Parameters of AP Beacon and the STA association requests:
  - HT, VHT, and HE capabilities
  - Inside HT capabilities:
    - Is LDPC supported?
    - Is SGI (Short Guard Interval) supported?
    - Under MCS in HT, VHT and HE – how many special streams are supported?

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ✓ Update any Firmware/Drivers
- ✓ Check General Network Configuration
- ✓ Check for Network Overloading
- ✓ Analyze Packet Data
- ❑ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document



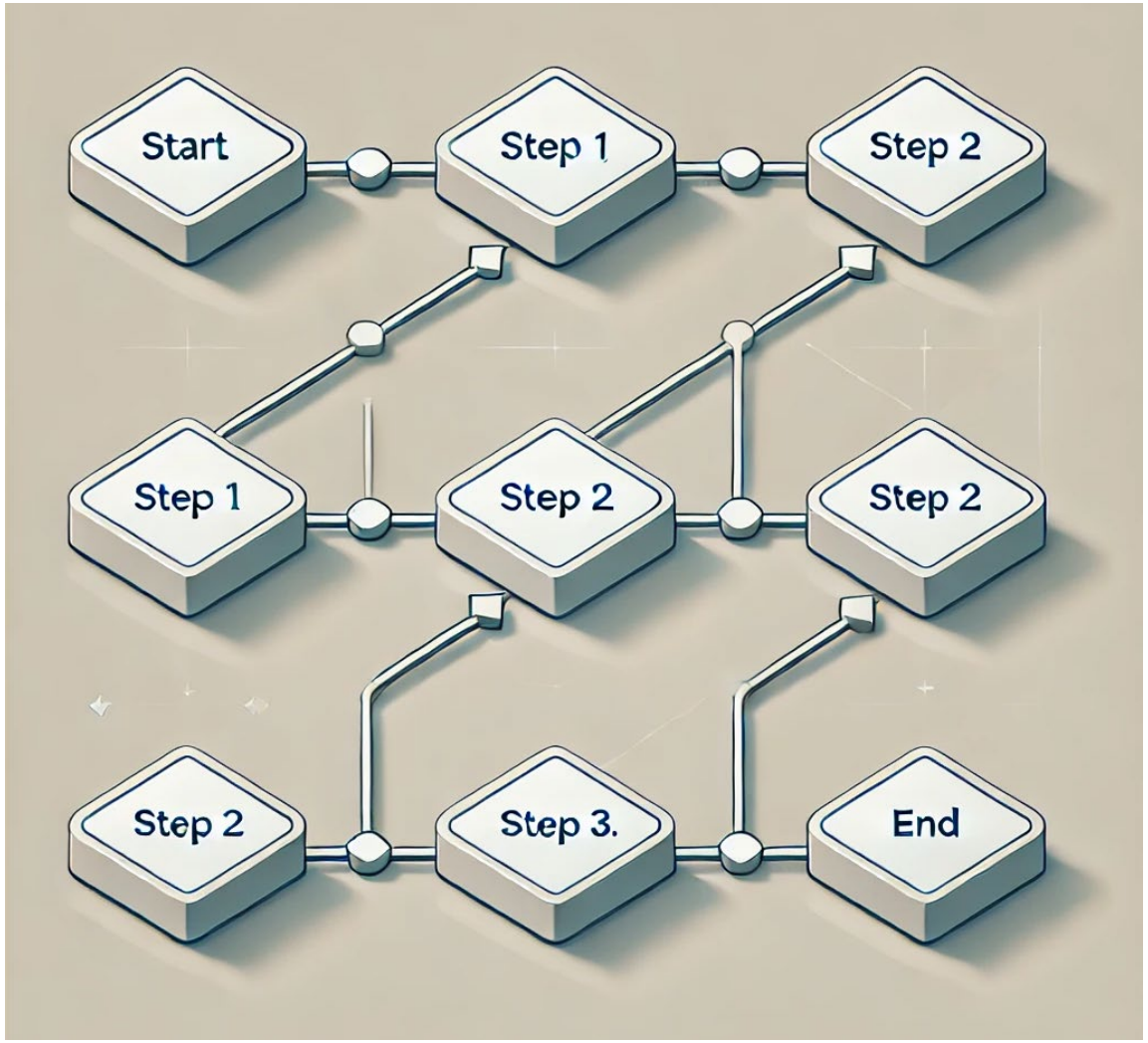
Factory Reset / Reboot



- **This is not a first step!**
- However, it can often be a final step once the issue is identified:
  - **Clearing Memory and Cache**: Over time, a router's memory can become cluttered with temporary data, cache, and processes that can slow down its performance. A reboot clears this memory, allowing the router to start fresh, which can improve performance
  - **Resolving Connectivity Issues**: Sometimes, devices may experience connectivity issues due to stale or corrupted network settings. Rebooting the router can reset the connections and resolve issues like dropped Wi-Fi, slow speeds, or devices not being able to connect
  - **IP Address Refresh**: If the router is having trouble assigning IP addresses to devices (DHCP Pool exhaustion), or if there's a conflict in the network, rebooting the router can force it to reassign IP addresses, which can resolve issues related to connectivity and access
  - **Clearing Network Congestion**: A reboot can help alleviate network congestion, especially in situations where multiple devices are competing for bandwidth, by resetting connections and reducing the load on the router
  - **Updating Configuration Settings**: If you've made changes to the router's settings, such as modifying the SSID, password, or security protocols, a reboot is often required to apply and activate these changes
  - **Fixing Software Glitches**: Like any electronic device, routers can occasionally experience software glitches or bugs. A reboot can resolve these temporary issues by restarting the router's firmware
  - **Improving Performance and Stability**: Regular reboots can maintain the overall performance and stability of the router, especially in environments with heavy usage or complex network setups
  - **Applying Firmware Updates**: After a firmware update, a reboot is usually necessary to complete the installation process and ensure that the router operates with the latest improvements and security patches

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ✓ Update any Firmware/Drivers
- ✓ Check General Network Configuration
- ✓ Check for Network Overloading
- ✓ Analyze Packet Data
- ✓ Factory Reset / Reboot
- ❑ Test and Verify the problem is corrected, document

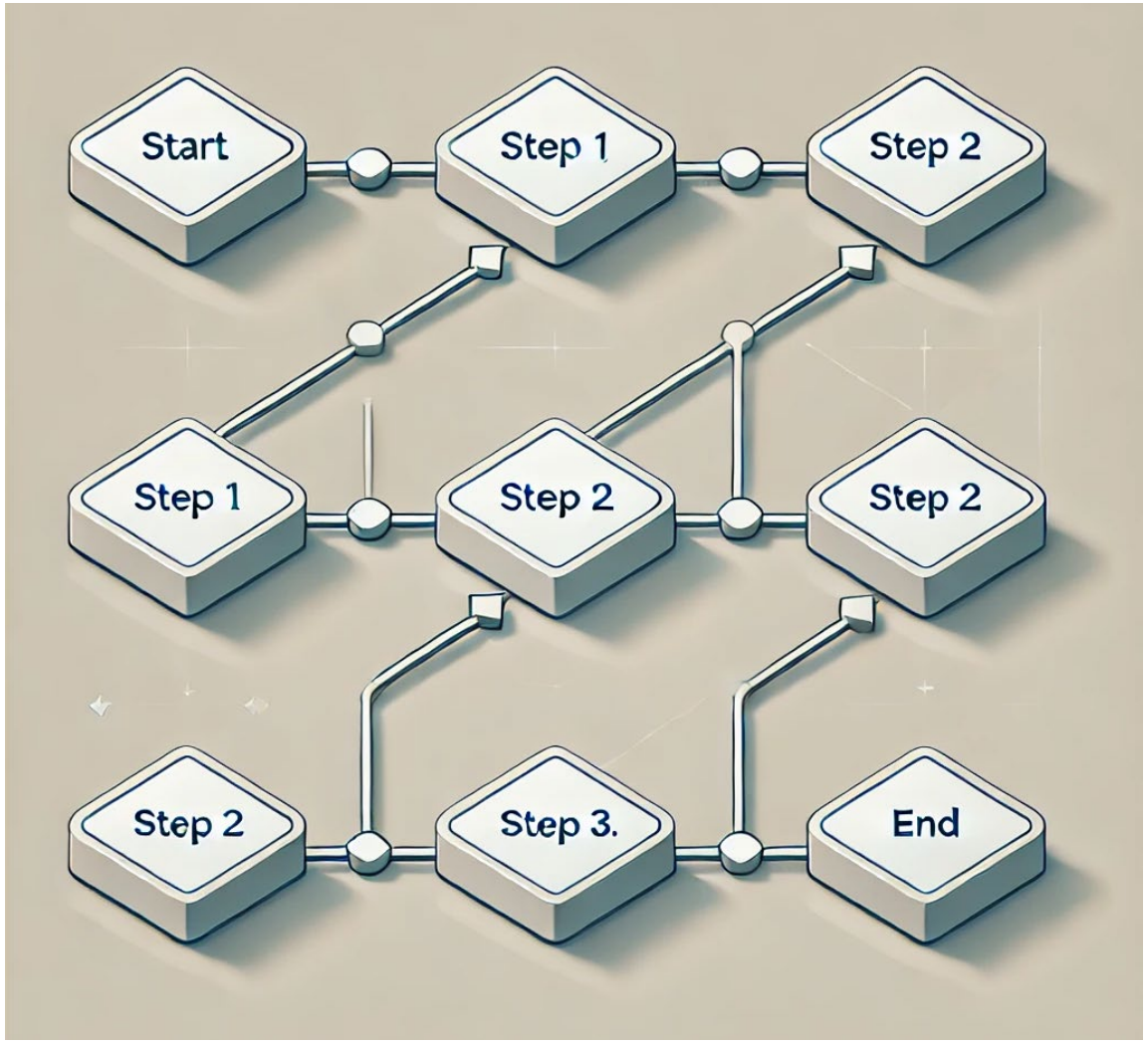


Testing and Verification

- **Ensure Functionality**: To confirm that the corrections or adjustments you made actually work as intended and do not introduce new issues
- **Optimize Performance**: To check if the changes have improved network performance, such as increased speed, better coverage, or reduced latency
- **Identify Hidden Issues**: Testing can reveal any unexpected problems that may arise from the changes, such as interference, signal dropouts, or compatibility issues with certain devices
- **Security Verification**: Ensuring that security settings, such as encryption or authentication methods, are correctly configured to protect the network from unauthorized access
- **User Experience**: To verify that the network provides a reliable and satisfactory experience for all users, including those with various types of devices
- **Compliance and Documentation**: Testing provides documentation and evidence that the network meets required standards or specifications, which can be important for compliance in certain environments, such as businesses or educational institutions
- **Avoid Downtime and Callbacks**: Verification helps prevent network outages or connectivity issues, which can be disruptive, especially in a critical environment

General Troubleshooting Workflow

- ✓ Identify and define the problem
- ✓ Checking Physical Connections
- ✓ Check the Wi-Fi Physical Layer Integrity
- ✓ Check Interference Types/Levels
- ✓ Check Wi-Fi Network Settings
- ✓ Update any Firmware/Drivers
- ✓ Check General Network Configuration
- ✓ Check for Network Overloading
- ✓ Analyze Packet Data
- ✓ Factory Reset / Reboot
- ✓ Test and Verify the problem is corrected, document



Some Examples of Wi-Fi Issues You are Likely to Find

- Interference
  - Co-channel & Adjacent channel
  - Narrowband – only on one channel
  - Wideband – several channels
  - All band – all channels in a frequency range
- Clients connecting at slow rates
- Misconfigured AP
- Too many AP's on a channel
  - Too many SSIDs broadcasting
  - Neighbor AP on the same channel
- Too many users on a channel
- Excessive Retries on a given channel
  - Channel Traffic congestion
  - Channel Device congestion
  - Poor Signal to Noise Ratio (SNR)
  - Range, RSSI
- Too many users on the same AP
- Client misconfiguration
- Legacy 802.11B clients present – ERP and 802.11N protection
- Beyond range, No secondary AP coverage
- Line of sight and antenna orientation for directional antennas

Thank you for your time…..Questions….

Author Biography and Details

Author: Andrew Walding

Biography of the Author

Mr. Walding is President of CellStream Inc., a global computing and telecommunications consulting group based in Texas. He holds multiple patents in telecommunications and has been in the industry since 1978. Additionally, Mr. Walding is an industry leading consultant, lecturer, author, instructor and course developer focusing on optical, packet switching, routing, and control protocols.

CellStream Inc. provides a diverse range of consulting services, serving the computing and telecommunications service providers and equipment manufacturers. CellStream has always been focused on emerging key technologies, enabling its clients to master new concepts in products and offerings with minimized lead times. CellStream consultants bring hundreds of years of front-line experience across a wide range of technologies and responsibilities. CellStream offers requirements/architecture definition, design support, RFP creation and response support, sales force enlightenment, solutions brainstorming, white paper and collateral creation/review services and much more.

Author contact information:
Email: andyw@cellstream.com
Web Sites:
CellStream Inc.: www.cellstream.com
Online School: www.netscionline.com

Tel: +1 866-659-1014
Fax: +1 866-659-1014