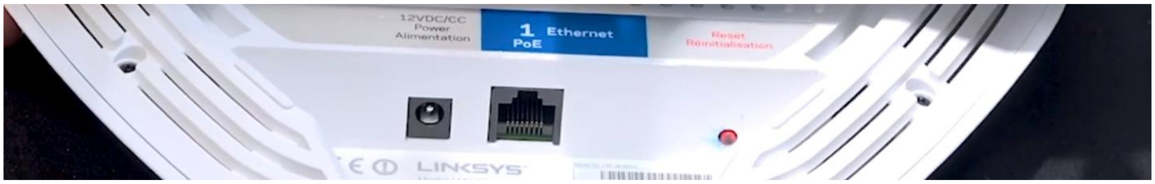
Ch 20 - Wireless Networking

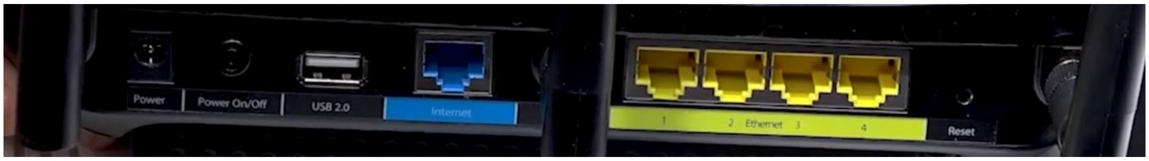
Wireless Network Hardware

- A wireless access point (WAP) bridges 802.11 and Ethernet networks
- Wireless clients connect to WAPs
- 802.11 works in one of two modes: infrastructure mode or ad hoc mode
- Use correct antenna for the job

IEEE 802.11 - King Standard. Primary way all of our Wireless Devices talk.

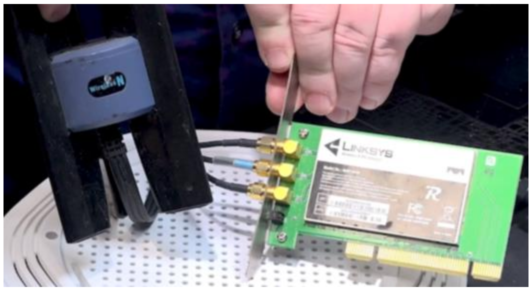


WAP (Wireless Access Point) - acts as a bridge between an Ethernet Network
and a Wireless 802.11 Network
Only will have 1 Ethernet Connection



Antennas on a Router are a big clue that it's Wireless
This Router has a built in Router, a built in Switch, and it's a WAP!

2 Different Modes we work in the 802.11 world.
1) If we have a WAP, or multiple of WAP's, we're in Infrastructure Mode
Most common way we do 802.11
Look around at the walls/ceilings of a building. You'll probably notice WAP's



Another thing we'll need is a Wireless Network Interface Card (a NIC) (plus Antenna).
Mobo's could have a built in NIC, which could have an Antenna attachment.
Laptops have a NIC, and the Antenna is almost always built into the Monitor
You're always going to have a WAP and a NIC

The WAP will be configured to have an SSID (Service Set Identifier)
On your phone, the different Wireless Networks are the SSID’s to connect to
and the NIC’s will connect to it through your client’s software

2) Ad Hoc Mode - this is not as common
There is no WAP. You just have a bunch of NIC’s.

If there’s a bunch of Laptops, and someone tries to set up a Wireless Network,
the other computers will treat your computer like a WAP!

This is a nice trick to use on airplanes

Antennas - absolutely critical for how we get the signal around

3 Types of Antennas
1) Omni-Directional - 1 Piece of Metal that sticks up.
Radiation pattern looks like a big fuzzy ball.
The more power you put into the antenna, the larger the fuzzy ball gets.

Dipole Antenna - 2 Omni-Directional Antennas
that point exactly opposite of each other.
Antenna pointing Up, and another pointing Down.

The signal propagates outward like a large disc-shape,
not up, or down, just outward.

2) Patch - Looks very Flat
Radiation pattern looks like a big fuzzy ball, but only half of one!

So, if you’re up against a wall and you want to
propagate outward one way, but not the other, use a Patch!

3) Highly Directional - Yagi Antenna (looks like a hedge clipper)
Radiation pattern looks like a Long Stretched out Football

Another type of Highly Directional Antenna is a Parabolic Antenna

Wi-Fi Standards

- 802.11 uses the 2.4- and 5-GHz ISM bands
- 802.11 uses premade channels
- Memorize the band usage and relative speeds of the 802.11 extensions

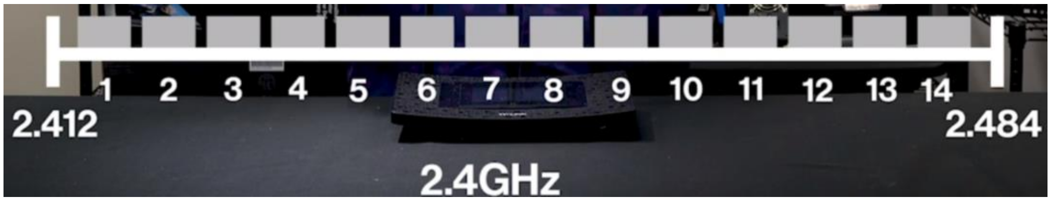
802.11 Standard - based on the unlicensed
ISM (Industrial, Scientific, and Medical) Radio Bands

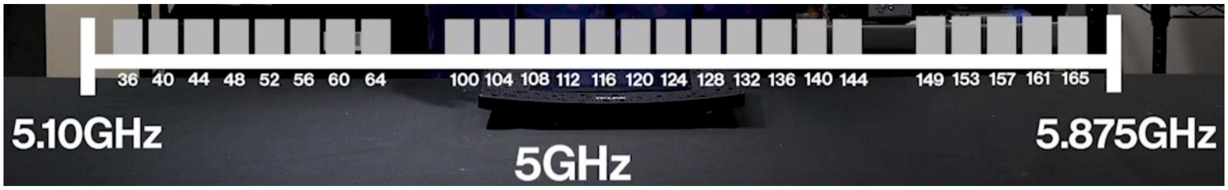
Band - Range of Radio Frequencies. 802.11 Standard uses both these Bands….
2.4 GHz Band - 2.412 - 2.4884 GHz
5 GHz Band - 5.150 - 5.875 GHz

We have this range of frequencies to work with
so different WAP's can use different ranges.

Channels - in the 802.11 2.4 GHz band, there are multiple channels.
Each channel takes a piece of this band.
You can tune your WAP to use a specific channel

# of Channels - Japan 14 - Europe 13 - USA 11





802.11 Extensions - 802.11 Standard needs to be upgraded with the times & technology
These upgrades are called Extensions

802.11a - 54 Mbps; 5 GHz Range
802.11b - 11 Mbps; 2.4 GHz
802.11g - 54 Mbps; 2.4 GHz ← Backwards compatible with 802.11b!! but not 802.11a
802.11n - 100Mbps; 2.4GHz & 5 GHz ← Backwards compatible with any Wireless NIC!!

WAP is a Radio, either a 2.4 GHz, or 5 GHz, Radio

802.11n also introduced….
MIMO (Multiple In/Multiple Out) - allows a WAP to use multiple Antennas
to change its radiation signal to really “zero in on”/converge to a device.

There’s nothing to configure! Just make sure you have a 802.11n WAP,
and a 802.11n Wireless NIC, and you’re set!

802.11ac - This is what we have today
Incredibly fast.
It splits the Channels, and improves the concept of MIMO from 802.11n,
and creates Multi-User (Mu-MIMO) which can converge the signal to
multiple clients at a time, depending on the number of radios it has put in it.

These WAP’s will have a 2.4 GHz radio in the device,
but this is only used for backwards compatibility.
This radio has nothing to do with the ac standard

802.11n - Wi-Fi 4
802.11ac - Wi-Fi 5

If you get a 802.11ac WAP, you won’t receive the benefits from this
without having a 802.11ac Wireless NIC!!!!

Make sure your NIC matches your WAP!

It’s a Huge Mesh

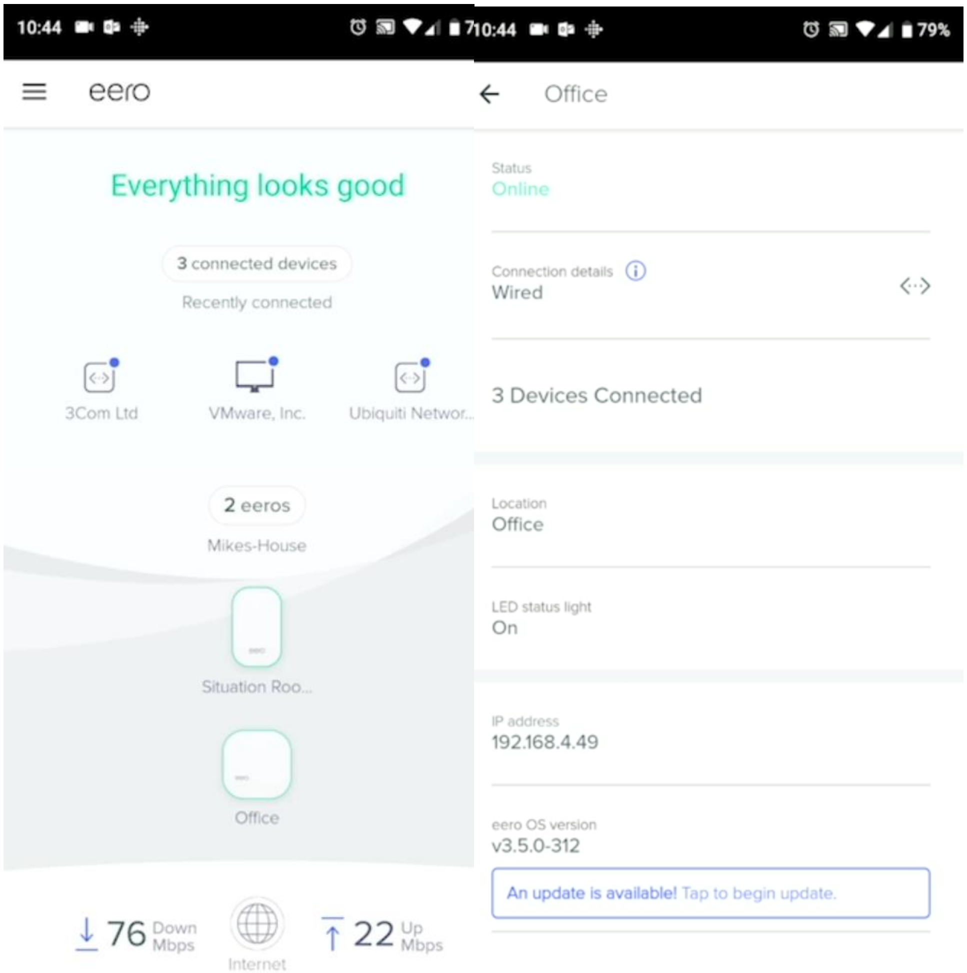
- Mesh networks are often a great wireless solution for SOHO environments
- Mesh networks have a base station and beacon devices that connect to the base station
- Mesh networks use their own encryption
- Mesh networks are universally easy to configure

Full Infrastructure Network is often overkill for Small Offices (2-50 computers) & Home Offices which would be better suited with a WMN

WMN (Wireless Mesh Network) - this is Ad Hoc Mode on Steroids
Very easy to set up.

We have 1 Base Station (Device #3 in the image), connected to the Network (cable modem, or whatever you have), and Configure an SSID

Then, place your External Stations (Devices #1 & #2) - plug into a Surge Protector in areas where you want to connect your devices



Everything looks good

3 connected devices

Recently connected

2 eeros

Mikes-House

Status
Online

Connection details
Wired

3 Devices Connected

Location
Office

LED status light
On

IP address
192.168.4.49

eero OS version
v3.5.0-312

An update is available! Tap to begin update.

Phone App shows 2 eeros (Situation Room & Office). Clicking these will give more details

These devices use 3rd Party Encryption that’s robust & already ready to go out of the box!
Only need to set up an SSID & SSID Password

Eero aka Beacon

You can run a Placement Test to see if it has really good coverage & good Wireless Service

Mesh Networks are becoming more Popular

They won’t have the big Throughput with a robust Infrastructure Network with lots of WAP’s but their ease of Configuration and ability to support what people have in Small Offices and Home Offices is absolutely great!

Enterprise Wireless

- Enterprise WAPs often use Power over Ethernet (POE)
- Use powerful wireless analysis tools to determine WAP location
- Enterprise networks often use RADIUS or TACACS+ protocols for authentication
- Two or more WAPs sharing the same SSID are known as ESSIDS

Small Office/Home Office vs Enterprise Wireless setups
are very similar, but with some differences.

You still have SSID's, and Encryption (WPA/WPA2)
The Bands are there. The versions of 802.11 are there.
But, it just gets a little bigger for Enterprise.

Tend to use dedicated lots of WAP's. These are real WAP's.
They're not also Routers, or Switches.

WAP's are PoE (Power over Ethernet) Devices
They get the electricity from the Ethernet cable they connect to!

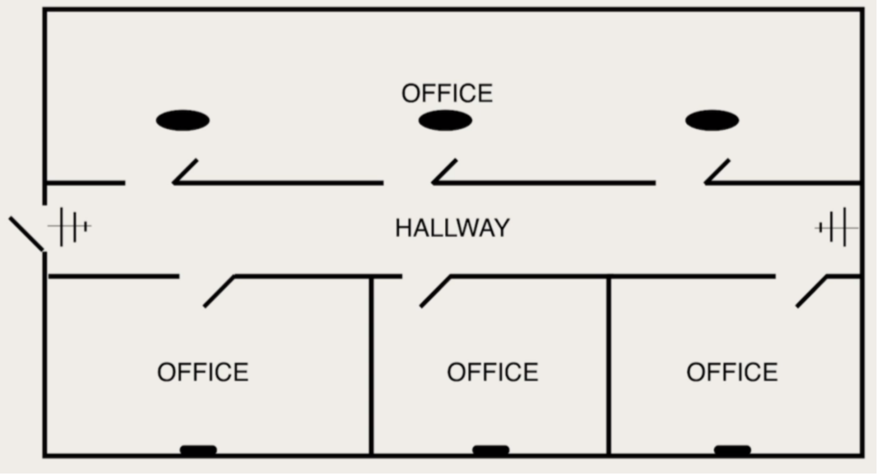
To take advantage of PoE, you need to have devices that are PoE capable.

There are 2 versions of PoE
PoE (1st Generation) - rare these days
PoE+ ("P-o-E Plus") - Supplies a lot more electricity to Devices

You need to have a PoE Switch
Switch is designed to send out all the communication & the electricity
The convenient thing about PoE is that
you don't have to plug your WAP's into a wall!

If you don't have a PoE Switch, you can use a PoE Injector
which basically is an adapter.
Switch connects to Injector, and Injector connects to WAP.

In an Enterprise, need to think about location of WAP's and the Antennas

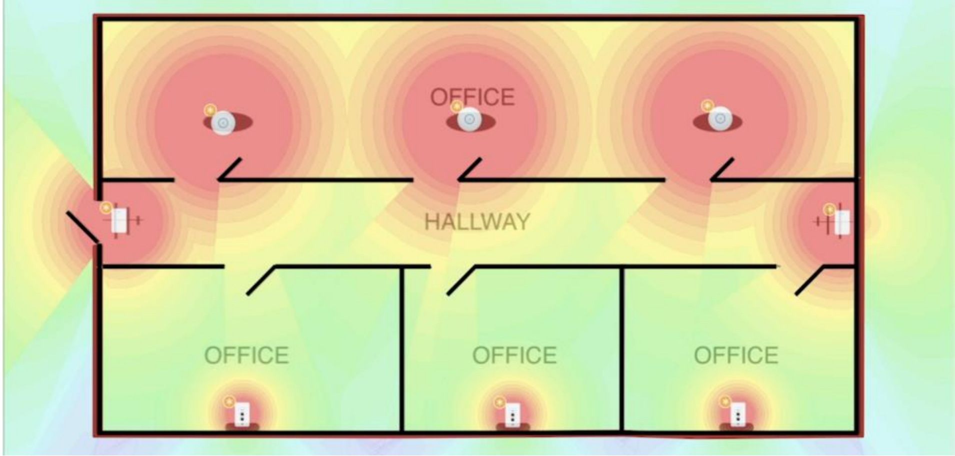


If we want coverage in the Hallway, use Directional Antennas on 1 or both ends.

(Directional = Long Football Shape)

In the Small Offices, use Patches (Half of a Sphere Shape)

In Larger Areas, use Dipoles or Omni's



You can place WAP's and they'll show a Heat Map (Red indicates highest coverage)

Gives you an idea where you might have dead spots

This analysis is Not Free.

Another big change going from SOHO Wireless to Enterprise Wireless is AAA.

AAA (Authorization, Authentication, Accounting) - you're going to be using WPA2,
but you're not going to be using Personal Shared Key (PSK)

You're going to be using RADIUS or TACACS+ boxes,
that will provide authentication you need.

When signing into a Network, they're not going to know the PSK,
their Client is going to make the sign in with a Username and Password,
then they'll be assigned WPA2 Information,
and then they connect to the Network.

This is very aggressive authentication & authorization.
You can add Smart Cards, but usually it's just a Username & Password

Configuring your WAP's - First thing you have to do is find out each ones IP Addresses

Video 84 at 5 min 55 sec (1002) shows how to configure these WAP's

What we'd be setting up in an Enterprise Environment is Not an SSID,
but instead an ESSID (Extended SSID). It's the same SSID on all of the WAP's!
Moving from one room to another, you change from one WAP to another,
and this is possible with no hesitation with an ESSID!!

The secret to an ESSID is to make the same SSID on all the WAP's,
and make sure they're all a member of the same LAN.

Wireless Isolation - the only computer on the Network your client is able to talk to
is the WAP. No file/folder sharing allowed. Great feature for a coffee shop.

Rogue AP Detection - Very frustrating when somebody enters the room
with their own WAP. This happens all the time! All of these WAP's
have a MAC Address and they all know each other's MAC Address.
If any other device tries to act like a WAP that's not on the list of known
MAC Addresses, this Rogue Detection can simply block it!
ALWAYS know your Network ID, so when weird things happen!
Rate Limit - you can Throttle the Speed that SSID might be doing
either Upstream, or Downstream.

Captive Portal - Login screen where you need to type in a Username & Password

For all of these WAP’s, they all need to be same name & same password.

Wireless LAN Switches - Switch with PoE, but instead of configuring a bunch of WAP’s, we go into the Switch, and we set up 1 ESSID, which is then propagated out to all the other WAP’s

Or, if we want to setup a Captive Portal, we setup 1 Captive Portal, and all the Usernames are propagated out to all the other WAP’s.

Cost of a WAP is below $100 for a good one. A couple 100 for a very good one.

Specialty Wireless LAN Switches (with PoE) designed to work with WAP’s are very expensive, powerful, and the only place you’ll see them is in an Enterprise Network.

Beyond Wi-Fi

- RFID uses tiny radios activated by the energy of the scanning device
- NFC requires extremely close proximity to function
- Bluetooth is like 802.11 but pairs with devices to function as point-to-point

802.11 most dominant Standard today, but there are others….

RFID (Radio Frequency Identification) - Very popular in Industrial Warehouses
Manifests as a Tiny Sticker, which is actually a Radio and stores a few 100 bits

Put this sticker on a box, and you have these Readers
which use the Radio Frequency Energy to Power these Stickers,
and the Stickers transmit back to the Reader.

This gives you the information about the box/product.

NFC (Near Field Communication) - Laser Printer has a feature “Tap-to-Print”
Smart phones have an RFID Reader in it NFC is a type of RFID!!!!
Tap-to-Print means you literally have to tap your cell phone
to the sticker to get it to print!

Another NFC is “Tap-to-Pay” -very popular with Mac & Google Devices

Bluetooth - looks a lot like 802.11 on a signal level, but Bluetooth is designed
to be able to only connect/Pair 2 devices together at the same time
in a PAN (Personal Area Network)

Class	Power	Range
Class 1	100 mW	100 m
Class 2	2.5 mW	10 m
Class 3	1 mW	1 m

Troubleshooting Wireless Connections

- The CompTIA A+ exams list specific wireless errors
- Wi-Fi analyzers are very helpful to diagnose wireless problems
- Memorize Mike's fixes for the wireless problems

Anytime you're having an issue with Wireless is some kind of Wi-Fi Analyzer
WiFiman - benefits in being able to see the Network

If one device (computer) can't see the Wireless Network,
and another device (phone) can't see it either,
you shouldn't be worrying about the Devices,
you should worry about the SSID!

No Connectivity -

Maybe you're trying to get to an SSID that doesn't exist
They might've changed the SSID, or the Password

Low RF (Radio Frequency) Signal - if it's too low, you won't have Connectivity

It may show that you're connected to the SSID, but turning on/off,
because you just don't have enough signal.
Get Closer to the SSID.
Take a look at your WAP Antennas.
The way that these External Antennas are pointing
will make a big difference in the way the Radio Radiation shape.

Limited Connectivity -

A lot of situations that happen with No Connectivity, Low Connectivity,
are also the same for Limited Connectivity.
Recent built walls, or Baby Monitors next to the WAP
can really Slow Down Transfer Speeds.
These analyzers are designed to find anything in any ISM Band
to find things like Baby Monitors, and Microwaves

Intermittent Connectivity - Running Great, and then No Connection, or Stalling

- Result of Low RF Signals.
- Too many people on your Wireless Network.
  - You need to get more WAP’s! There’s no way around this!
  - QoS will help too