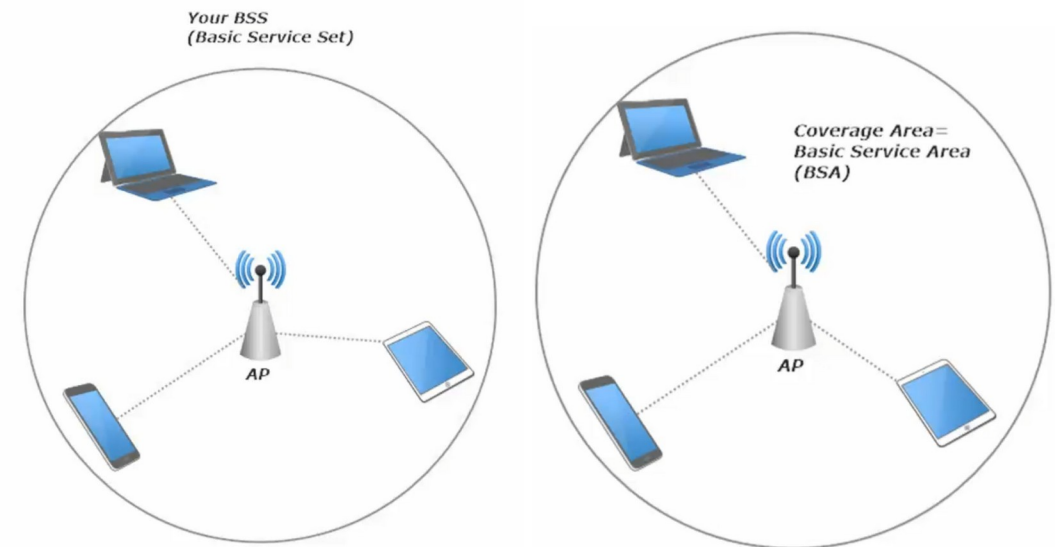
Wireless

Radio Frequency
Higher Frequencies of RF
higher data rates
shorter ranges, difficulty passing through objects, such as walls

Basic Services Set
The 802.11 standard define service sets as a logical group of wireless-capable devices that share the same Service Set Identifier (SSID).

BSS is a logical group of wireless-capable devices that are operating on the same radio freq and same security settings.

Wireless Access Point (AP / WAP)



Basic Service Area (BSA) is the coverage areas afforded to us by the BSS

Infrastructure mode BSS contains a single AP and multiple clients, who communicate directly with the AP and with each other – but not directly PC1 to PC2 is really PC1 > AP > PC2
Much like a hub-and-spoke network
Client to client communication goes thru the AP

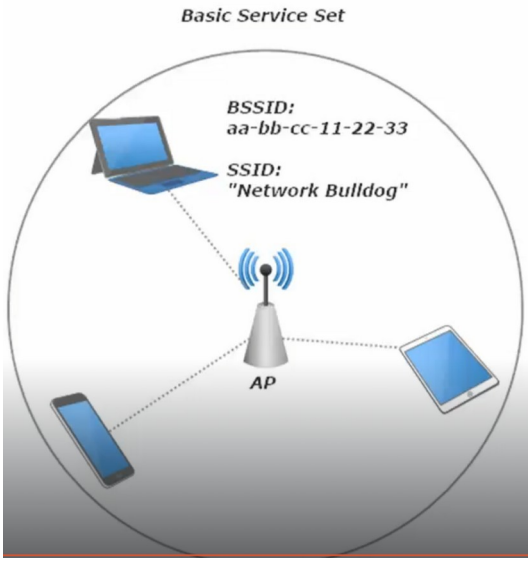
How clients connect to an AP
The potential client sends an *association request* to the AP, and then it's up to the AP whether to grant it. If granted, the client is said to be successfully associated with the BSS.

Every BSS has a BSSID – Basic Service Set Identifier
The BSSID is composed of a 24-bit OUI and a 24-bit serial number. The MAC address of the AP

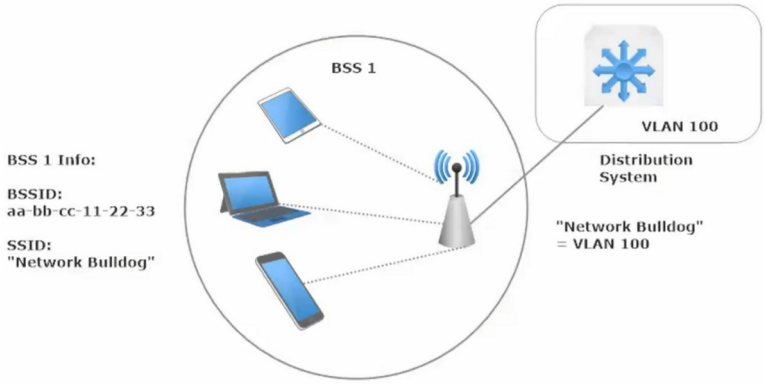
To let clients know a wireless network is available, the AP will advertise its existence, and part of that advertisement is the BSSID
Another part of that advertisement is the SSID, the Service Set Identifier.

SSID
A customizable value that is used to identify a wireless network

BSSID identifies the AP
SSID identifies the Wireless network

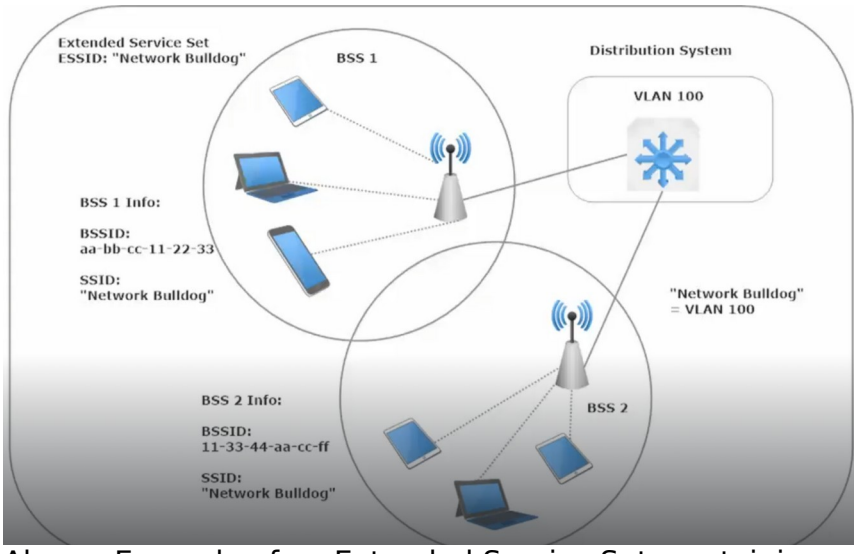


The Distribution System and the extended service set
Our Basic Service Set (BSS) allows clients in that same BSS to communicate, but we also need the ability to communicate with clients from another BSS or hosts on the wired network.



Above: By adding a multi-layer switch the BSS can communicate to other hosts on the network connected through the Distribution System (AKA L3 Switch)

The *Extended Service Set* is a collection of BSSes that allows for inter-BSS communication



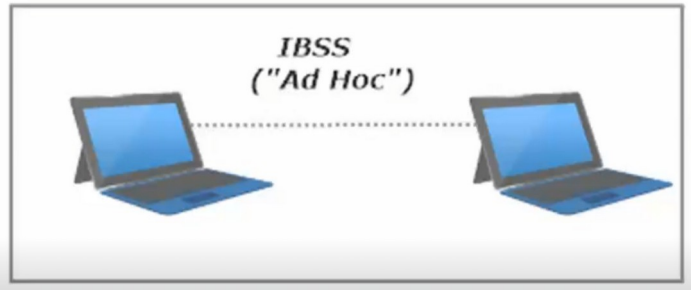
Above: Example of an Extended Service Set: containing a Distribution System and two BSSes

Each AP is an ESS will have its own individual BSSID , but will share the SSID
It wouldn't be much of a scalable solution if the SSIDs changed every time a client left the coverage zone of 1 AP and enters into another AP's coverage zone.

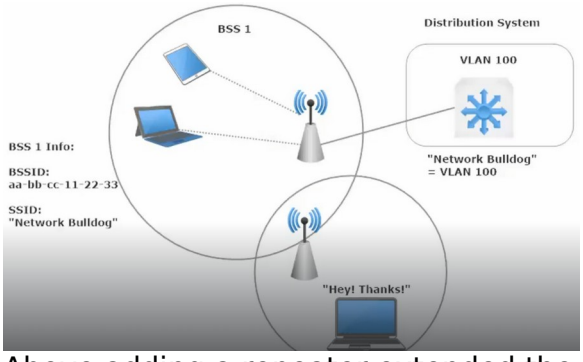
Roaming Client – a client who moves from the coverage of one AP in an ESS to the coverage of another AP in that same ESS.

An *Independent Basic Service Set* is independent because of its lack of an official AP.
I say “official” since one the wireless devices that wants to take part in an IBSS acts in some ways as an AP, including advertising the very existence of the IBSS.

IBSS is also known as an *ad hoc* network
Ad hoc = when necessary or needed, aka created or done for a particular purpose as necessary.



Bridges and Repeaters
Wireless Network Repeater – extends the initial range of a BSS
The repeater doesn’t have to be a dedicated device that can only serve as a repeater; it can an AP.
Can serve as a small bridge to extend a network past its current range, but is not a scalable solution.



Above adding a repeater extended the BSA

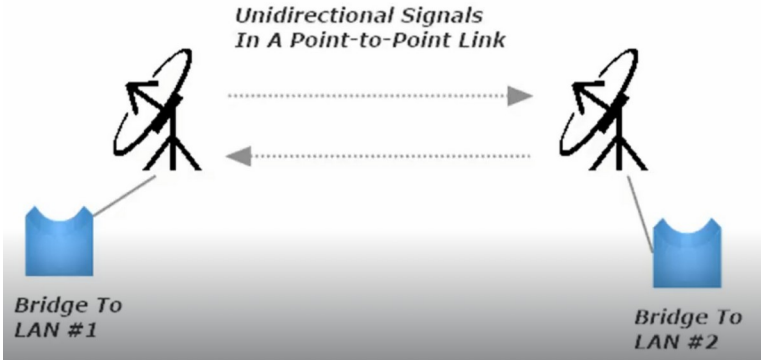
Why not use a bunch of repeaters on your network? They have issues
Wireless interference level is high since a single-transmitter / single-receiver repeater will need to be on the same channel as the AP in order to function as a repeater.

This can lead to “bounceback”, where an AP sends a signal, the repeater receives it and repeats it – and the AP ends up receiving a signal it just sent. As a result of this, wireless throughput drops by min 50%.

Downside 2: adding a repeater opens ip another point of vulnerability on your wireless network. Not every repeater will have a security suite as strong as your average Wireless AP, particularly older repeaters.

Workgroup Bridge (*WGB*) – generally used to connect a wired network client to a wireless network.
The WGB is the middleman of a wired-host-to-wireless-network connection.
The WGB is a client of the AP in a BSS, and the wired client is a client of the WGB

AP >> WGB >> ethernet >> ethernet port of Client
Outdoor Bridge – serves to bridge the gap between multiple LANs. The topology and capabilities are just a bit different when more than two LANs are involved.
When two LANs are to be connected, a point-to-point outdoor bridge consist of one unidirectional antenna at each end of the link.
Since each antenna can be pointed directly at the other end of the link, signal strength is kept at a maximum.



When there are more than 2 LANs, a point-to-multipoint bridge is necessary. Similar to a hub-and spoke wired network, in that there will be a central location that everyone points to (the hub). This central location must be able to communicate with every non-central location (the spokes).
The spokes can point a unidirectional signal at the hub (keeps connection as strong as possible)
Since the hub must be able to communicate with all spokes, it has to send out an omnidirectional signal.

Wireless Security

AAA – Authentication, Authorization, Accounting

Authentication – should I let User X in
Authorization – What are they allowed to do once in (admin priv?)
Accounting – keep track of who enters and what they access

Authentication
AP - Should I let this user/client in?
AP -Is this user even who I think they are / who they say they are?
Client – Is this AP a legit member of the network I am trying to join?
Rogue AP – under the control of a hacker, man-in-the-middle attack

WEP

- First wireless security was WEP (wired equivalent privacy)
- WEP – ratified in 1997, deprecated in 2004
- WEP can be put to work via open system authentication and shared key authentication
- WEP is easily compromised.

Open system authentication – no authentication needed, just as it is named.
During authentication, the client presents no actual Authentication info. The authentication process is simply the client sending an 802.11 authentication request

Shared key authentication – uses a challenge-response auth setup, where each party knows the auth key before the actual auth process begins.
The client uses the WEP key to encrypt the response to that challenge. The client then sends another auth request (AR) and this request will contain the encrypted challenge response.
The AP then decrypts the response using the same shared key.

WPA – Wifi Protected Access

- WPA available since 2003 – uses dynamic key management (built on EAP)
- WPA uses Temporal Key integrity Protocol (TKIP)
- TKIP had a separate 128 bit key for each packet
- Used with RADIUS in the enterprise
- Uses an encrypted hash
- Each packet has a unique encryption key
- WPA included a *Message Integrity Check (MIC)*, the MIC included the sender's MAC address, which helped with verifying who the sender actually was.

WPA2

- Based on 802.11i architecture
- Can integrate with 802.1x
- 802.1x with EAP (Extensible Authentication Protocol (EAP) (note: not limited to wireless networks.

- Allows users/devices to authenticate with EAP plus TACACS+/RADIUS
- 3 main roles in an 802.1x/EAP deployment
  1. Supplicant – the device that wants access
  2. Authenticator – the device providing access to the network
  3. Authentication Server = the device providing the authentication. (RADIUS / TACAS+ servers)
- RC4 replaced by AES (Advanced Encryption Standard) 256 bit and beyond
- TKIP replaced by CCMP (Computer Mode w/ Cypher Block Chaining)
- CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - Access control
  - Authentication
  - Data confidentiality
- Uses an encrypted hash
- Each packet has a unique encryption key

WPA3

- Replaced the Pre-Shared Key (PSK)
- Simultaneous Authentication of Equals (SAE) used instead
- WPA3-Enterprise offers optional 192-bit encryption
- Protection of management frames enforces
  (note: 3 types of wireless frames (Data, Management, and Control Frames)

Mac Address Filtering

- Make a whitelist/blacklist of allowed/disallowed MAC address.
- Should be used in tandem with other security as MAC addresses can be spoofed.

Extensible Authentication Protocol (EAP)
Authentication framework used in wireless networks (RFC 3748)
100+ Types available

EAP MD5 - uses a series of challenges and responses.
Uses the same MD5 hash as the Cisco router command (service password-encryption)
Easily broken (intro – Win 2000 exit Win Vista)

LEAP - Lightweight EAP (Cisco proprietary). Client and Auth server challenge each other
Challenge responses are encrypted
Uses dynamic WEP keys
Supported by some third party (non-cisco) vendors via the Cisco Compatible Extension Program
LEAP is easily cracked. Deprecated, but still an option on some clients and Aps

EAP-FAST (EAP Flexible Authentication by Secure Tunneling)
Cisco's replacement for LEAP
A secure tunnel between the endpoints is contructed via use of a PAC (Protected Access Credential) during a three-phase process, which begins with Phase Zero

Phase 0 – PAC Generation
Phase 1: A transport Layer Security (TLS) tunnel between the endpoints is constructed AFTER the Supplicant and AS perform mutual authentication.
Phase 2: Authentication of the peer takes place thru that TLS tunnel

Outer Authentication – made outside the TLS tunnel (not created yet). This auth has the AS and Supplicant perform mutual auth via that PAC (protected Access Credential)
Digital certificates can be used in an EAP-FAST deployment (optional)
Inner Authentication – Authentication that occurs within the TLS tunnel (encrypted)

PEAP Protected EAP

- Encapsulates EAP via a TLS Tunnel (increases the protection of authentication messages by creating a protected TLS tunnel)
- Within this protected tunnel, an authentication protocol such as MS-CHAPv2 can then be used.
- Major difference between PEAP and EAP-FAST is PEAP's use of a digital cert for the AS authentication
- Digital Cert is issued and Signed by a CA (Cert Authority)
- The Supplicant uses its copy of a CA Cert to compare to the AS's cert. If they match, the TLS tunnel is built between AS and client.
- The Client is then authenticated cia encrypted authentication info send thru the tunnel.
- Two PEAP types, both compatible with WPA2
- PEAPv0 / EAP-MSCHAP2, which use the Microsoft Challenge Auth Protocol version 2
- PEAPv1 / EAP-GTC (Generic Token Card)

EAP-TLS EAP Transport Layer Security

- The next logical step after PEAP, which requires a digital cert to be presented by the AS
- Requires a digital certificate to be presented by both the Supplicant and AS, giving us mutual authentication via digital certs
- Downside to EAP-TLS – depending on size of network, it can be difficult to get a DC to every single on of your clients, you usually end up setting up your own CA.
- Downside 2: Some devices don't support digital certs
- With a client-side certificate, a compromised password is not enough to break into EAP-TLS enabled systems because the intruder still needs a client-side cert. password is not even needed, as it is only used to encrypt the client-side certificate for storage.

EAP-TTLS - uses a secure TLS tunnel (also)

Pre-shared Key (PSK)
Secret data shared between devices before communication is allowed

- Used in WEP, WPA (WPA-PSK or WPA2-PSK) etc for wireless
- Also used in EAP
- Key is usually a password, a passphrase, or a hexadecimal string
- WPA2 Pre-shared Key (PSK), we can choose the encryption key format as either ASCII or Hex

Geofencing

- Feature inside software
- Uses GPS or radio to define geographical boundaries
- Defines triggers for devices entering/exiting network boundaries

CCMP