www.howtonetwork.net

CCNA: Wireless Local Area Nework (WLAN)

What is a WLAN?

WLAN allows a set of computers to communicate and share information without the need of physical media. WLAN uses Air as the transport medium

WLAN Standards and Governing Bodies

IEEE: Standardization of wireless LANs (802.11). IEEE has rectified the 5 major WLAN standards: 802.11, 802.11b, 802.11a, 802.11g, 802.11n

Wi-Fi Alliance: An industry consortium that encourages interoperability of products that implement WLAN standards through their Wi-Fi certified program

Service Set

Service Set: is a logical grouping of (wireless) devices. WLANs provide network access by broadcasting a signal across a wireless radio frequency (RF) carrier

Service Set Identifier: A receiving station can be within range of a number of transmitters. The transmitter prefaces its transmissions with a service set identifier (SSID). The receiver uses the SSID to filter through the received signals and locate the one it wants to listen to

Independent Basic Service Set (IBSS): An IBSS consists of a group of 802.11 stations communicating directly with one another. An IBSS is also referred to as an ad-hoc network because it is essentially a simple peer-to-peer WLAN

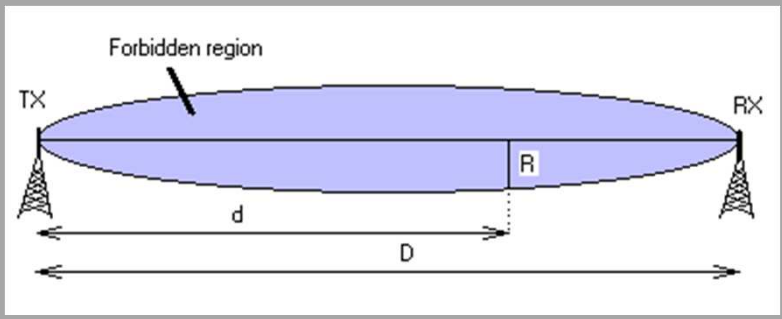
Basic Service Set (BSS): requires a specialized station known as an access point (AP). The AP is the central point of communications for all stations in a BSS. The client stations do not communicate directly with other client stations. Rather, they communicate with the AP, and the AP forwards the frames to the destination stations

Extended Service Set (ESS): Multiple infrastructure BSSs can be connected with a distribution system (DS). The collection of BSSs interconnected via the DS is known as the ESS. The DS does not have to be via a wired connection. The 802.11 specification leaves the potential for this link to be wireless. However, DS is usually a wired network. ESS also allows the facility of roaming to wireless clients

Radio Frequency (RF) Terminologies

RF Propagation: movement of RF signal through a medium.

Fresnel Zone: to maximize the receiver strength, one needs to minimize the effect of the out-of-phase signal by eliminating obstacles from the RF line of sight (LoS) or forbidden region because an obstacle will disturb the RF signal



Fresnel Zone (FZ): “D” is the distance between transmitter (TX) and receiver (RX). “d” is the radius of the FZ

Diffraction: the phenomenon when RF waves bent around sharp object creating new wave fronts. The higher the frequency of transmission, the higher the loss will be

Reflection: RF waves reflect from uniformly smooth non-absorbing obstacles they meet

Scattering: RF energy is reflected out of a non-uniform surface in multiple directions

Absorption: the RF energy is absorbed when it hits objects like water, wood and even people

Attenuation: the loss of radio signal strength, it limits the range of radio signals and is affected by the materials a signal must travel through (e.g. air, wood, concrete,). Free space loss is a type of attenuation that is the natural loss of the radio signal when propagating through the air without obstructions, the signal gets weaker and weaker when traveling away from the AP.

Diversity: use two or more antennas to improve the quality and reliability of a wireless link. Used especially in indoor environments, where there is not a clear line-of-sight (LOS) between transmitter and receiver

Radio Frequency (RF) Terminologies

WLAN Modes

There are two WLAN mode:

1. Ad-hoc Mode: wireless clients communicate directly. Ad-hoc mode only supports the IBSS
2. Infrastructure Mode: requires an AP. Supports BSS and ESS

WLAN Frequencies

WLAN uses the Industrial, Scientific, Mechanical (ISM) band. The ISM band consists of the following frequency ranges:

1. 2.4GHz: 802.11b/g/n WLANs
2. 5GHz: 802.11a/n

Media Access

WLAN control the media access with CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) algorithm. The CSMA/CD can be summarized in the following key points:

1. Listen to ensure that the medium (space) is not busy (no radio waves currently are being received at the frequencies to be used)
2. Set a random wait timer before sending a frame to statistically reduce the chance of devices all trying to send at the same time
3. When the random timer has passed, listen again to ensure that the medium is not busy. If it isn't, send the frame
4. After the entire frame has been sent, wait for an acknowledgment
5. If no acknowledgment is received, resend the frame, using CSMA/CA logic to wait for the appropriate time to send again

Deployment Guidelines

The following is checklist or a basic guideline for wireless LAN deployment:

1. Decide if an Ad-hoc mode or Infrastructure mode deployment is required
2. In case of infrastructure mode, make sure availability of basic network services including DHCP, DNS, VLAN and internet (if required)
3. Configuration/Verification of AP settings including SSID and clients can connect to the specified SSID
4. Configure Security for Wireless LAN and verify if the client can connect

Security

Wired Equivalent Privacy (WEP): uses static (64-bit) pre-shared keys. Keys had to be exchanged manually and cannot be changed without human intervention. Only 40-bit were actually used for derivation of key therefore, it was easily crackable

Wi-Fi Protected Access (WPA): WPA includes the option to use dynamic key exchange, using the Temporal Key Integrity Protocol (TKIP). WPA allows for the use of either IEEE 802.1X user authentication or simple device authentication using pre-shared keys. And the encryption algorithm uses the Message Integrity Check (MIC) algorithm

WPA2: includes dynamic key exchanges and stronger encryption (the AES algorithm) and user authentication. WAP2- is not backward compatible with WPA

Troubleshooting WLANs

RF Interference: occupies the (air) medium causing delay in sending and receiving data, collisions and resulting retransmission. RF interference is usually caused by high noise level. Noise level should be less then -85dBm for the band users are operating in

Coverage Black Holes: if the wireless survey is not conducted properly, this could result in limited or no RF signal coverage causing decrease wireless performance and service interruption. If the signal strength is less than -75dBm and high retries are greater than 10 percent, this is an indication of RF coverage issue

High Utilization: is caused by larger number of simultaneous active users or application such as wireless IP telephony may cause the access point (AP) to reach it maximum capacity. This result is lower throughput per user even signal strength is excellent due to additional overhead of re-transmitted data frames. This problem can be solved by increasing the number of AP and creating smaller radio cells (also called the micro-cells). Another approach is to move applications like IP telephony to different band. For example: IP telephony using 802.11a (5GHz) and data using 802.11b/g (2.4GHz)