Overview

- Last Lecture
  - Post installation
- This Lecture
  - Wireless networking
- Next Lecture
  - Scheduled tasks and log management

IEEE 802 Standards

- 802.1: Bridging and Management, e.g. 802.1X
- 802.3: Ethernet
- 802.11: Wireless (WiFi)
  - 802.11b, 802.11a, .11d, .11g, …, .11aj, .11ay
- 802.16 Broadband Wireless MAN (WiMAX)
- 802.15.4: Zigbee, wireless sensor networks
- 802.15.1: bluetooth, 802.15.6: WBAN
- http://standards.ieee.org/getieee802/

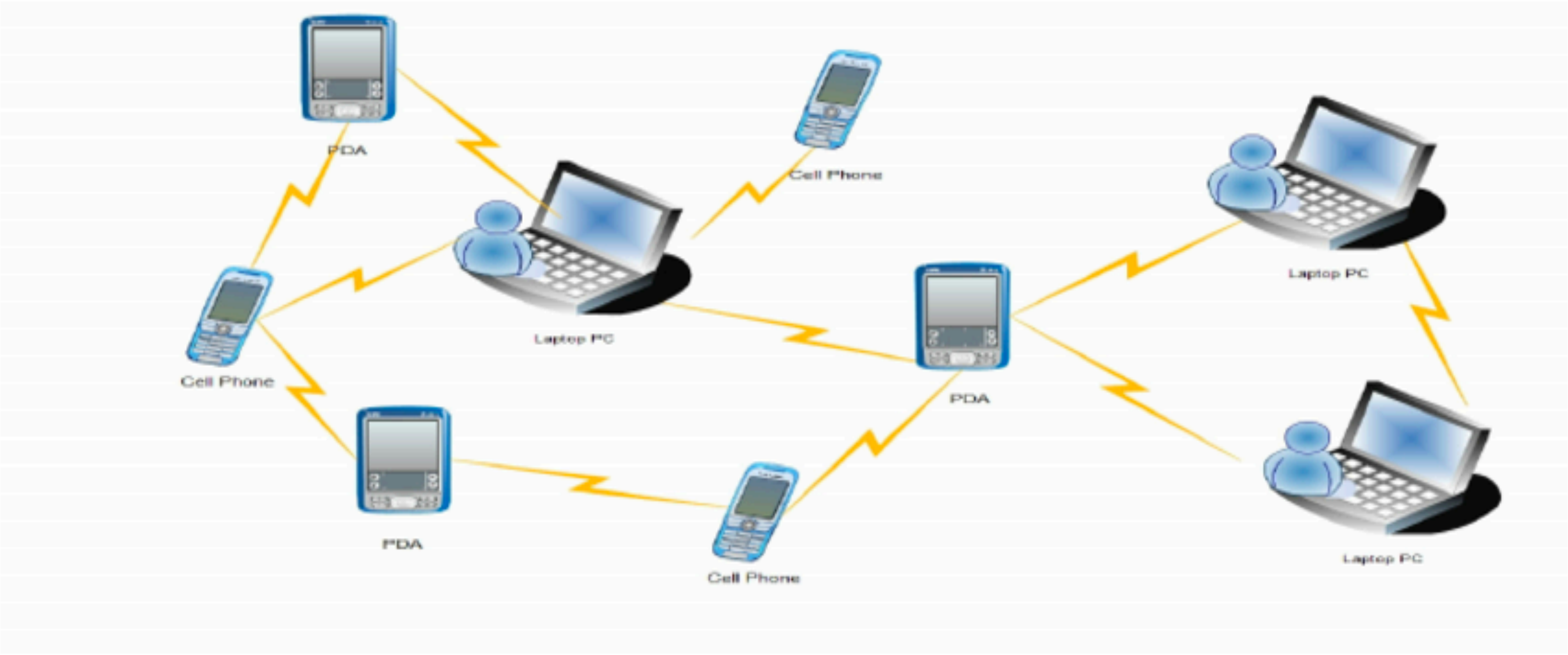
802.11 Family

- 802.11b
  - 11Mbps, 2.4GHz, Kick-started Wi-Fi technology, ~30m indoors.
- 802.11a
  - 54Mbps, 5GHz, technically superior to 11g, gradually common.
- 802.11g
  - 54Mbps, 2.4GHz, still very common. Compatible with 11b.
- 802.11n
  - 540Mbps (typ. 200Mbps), 2.4+5GHz, current choice
  - Max speed hard to determine, ~50m indoor, MIMO
  - Supports a/b/g or ‘Greenfield’ (exclusive).
  - Also supports extensions for priority, multimedia
- 802.11aj -- 15Gbps, mmWave
- 802.11ay -- 20Gbps, mmWave

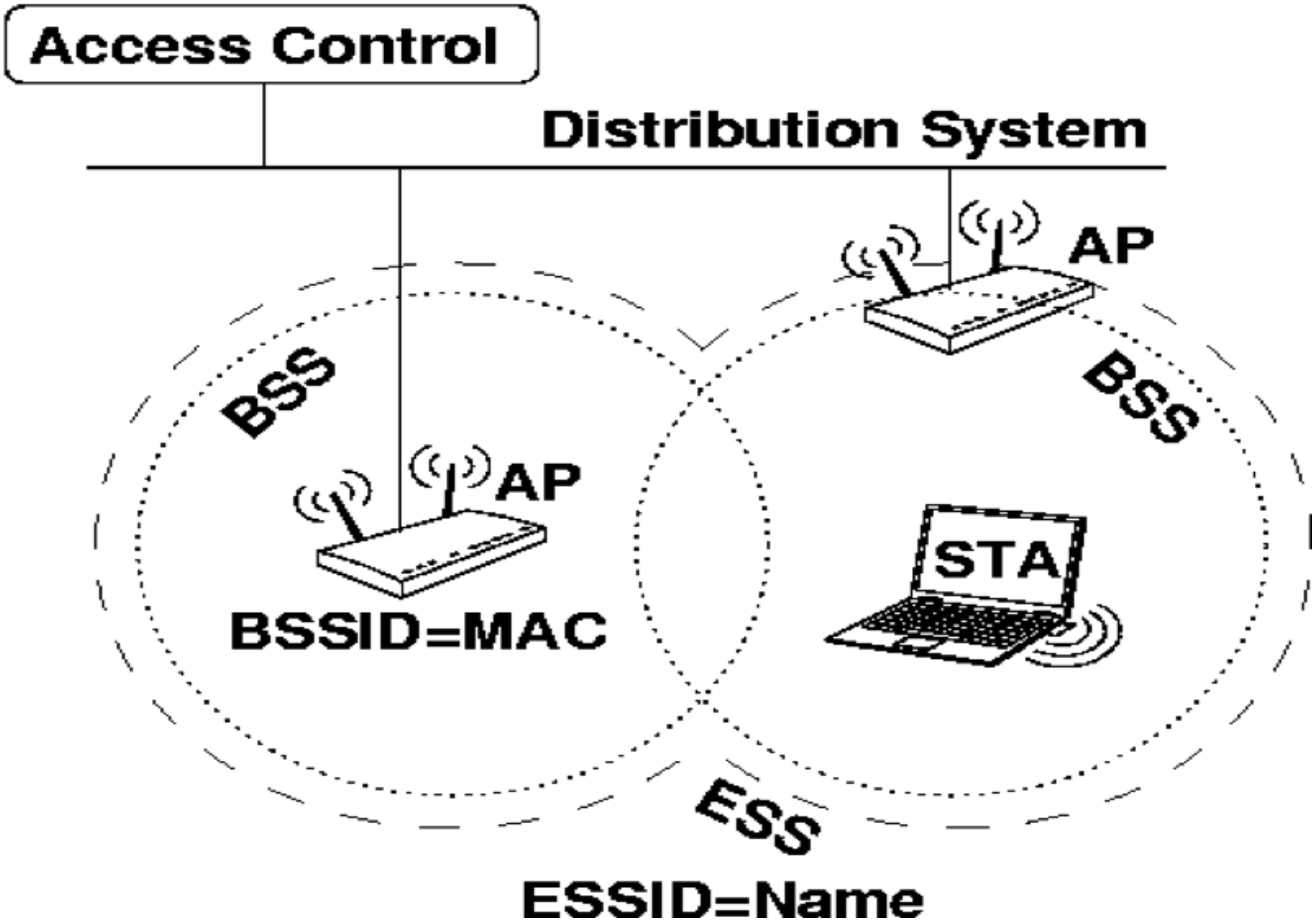
Operation Modes of 802.11

- Independent or ad-hoc mode
  - Nodes in an ad-hoc network communicate without any need for network infrastructure such as an AP, or network level services such as DHCP, DNS
  - ZeroConf protocols to manage IP addresses etc.
- Infrastructure or managed mode
  - Requires an access point (AP) to function
  - Higher network layers such as data link and IP are configured using the same methods as any wired Ethernet. Most commonly DHCP is used
  - Further security measures may be employed to manage security risks associated with wireless

Ad hoc Mode


PDA
Cell Phone
Laptop PC
Cell Phone
Laptop PC
PDA
PDA
Cell Phone
Laptop PC

Infrastructure Mode



Basic terminology

- AP: Access Point
- STA: Station/devices
- BSS: Basic Service Set
  - A group of stations that communicate with each other via an access point.
- ESS: Extended Service Set
  - Multiple BSSs can be linked using a distribution system to create an Extended Service Set
- SSID: Service Set Identifier
  - The MAC address of an AP
- ESSID: Extended Service Set Identifier
  - The name of the network

Wireless Distribution System (WDS)

- Backbone of multiple APs, and the inter-AP communication. Usually Ethernet, may be wireless.
- 802.11F defines the Inter Access-Point Protocol (IAPP)

Signal Strength

- Signal Level: Strength of the received signal
- Noise Level: Strength of the noise
- Link Quality: Signal to Noise Ratio (SNR)
- Transmit Power: How loud we speak
- Receive Sensitivity: How well we can hear
- Decibel: $10*\log_{10}(P/P_0)$, which shows the ratio of power of one signal over another.

Finding a Network

- Passive scanning listens for AP beacons
  - Listens on each channel for a certain dwell time
  - Won’t detect closed/hidden networks
- Active scanning sends Probe Requests
  - On each channel
  - Requests a particular ESSID or “any”
  - Produces a scan report with discovered ESSIDs

Security of WiFi

- MAC Filter List
  - Not a security protocol
  - Access Control by (changeable) MAC address
  - ACLs can be stored centrally using RADIUS
- WEP (Wired Equivalent Privacy)
  - Minimal protection
  - Not secure due to short key length
  - Pre-Shared Key (PSK)

WPA

- Wi-Fi Protected Access
  - Subset of 802.11i that was released when WEP flaws became a barrier to adoption
- WPA Personal
  - WEP with short-lived changing keys
  - Temporal Key Integrity Protocol (TKIP)
  - Different key per user/session/packet
  - Performance cost if not done in hardware

WPA Enterprise

- WPA Enterprise
  - 802.1X for user authentication
    - “Port” based authentication framework
    - Extensible Authentication Protocol (EAP)
  - Requires RADIUS backend
- 802.11i—WiFi Alliance calls it WPA2
  - Advanced Encryption Standard (AES) cryptography

Security Issues

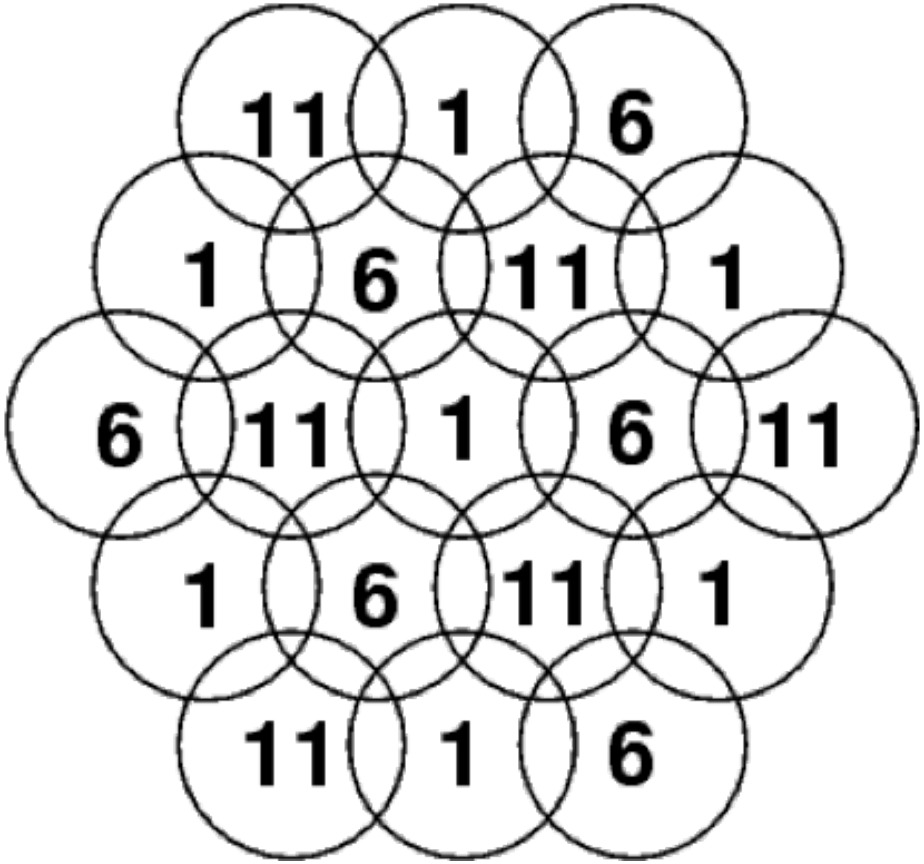
- Bandwidth stealing
  - You are responsible for their actions
- Access to wired network
  - and other wireless nodes
- ARP Poisoning
  - Man-in-the-middle attacks
- AP Spoofing

Uses of Wireless

- When cables are a hassle/liability ✔
- Transient networks ✔
- Hotspots ✔
- Backup links ✔
- Reliability ✗
- Security (can be managed) ✗
- Speed ✗

Channel Layout

- 13 channels (1, 2, …, 13)
- Hex-pattern layout for non-overlapping channels
  - But don’t forget that space is 3D
- Limit number of nodes to about 30 per AP



Antenna Types

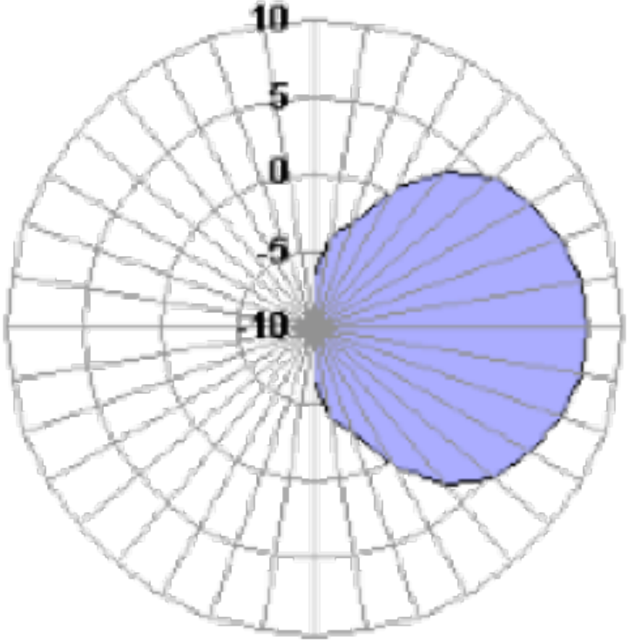
- Omni-directional
  - Diversity antennas
  - High-gain Omni

AP with antenna diversity

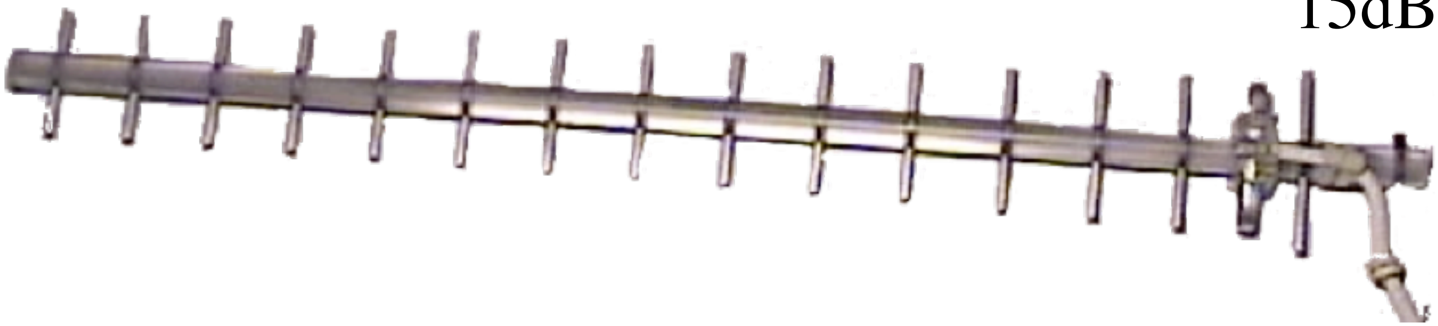
7dBi High-Gain Omni

Antenna Types

- Directional
  - Panel, Yagi, Parabolic
  - Shown is a Wave-Guide “cantenna”
  - Trade off polar coverage for distance
  - dBi is used to measure the gain: $10*\log_{10}(P_D/P_O)$, P_D is the power for directional, P_O is the power for standard omni-directional.

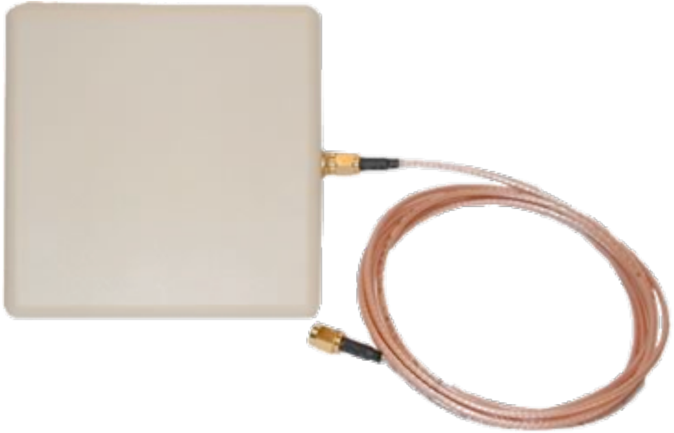


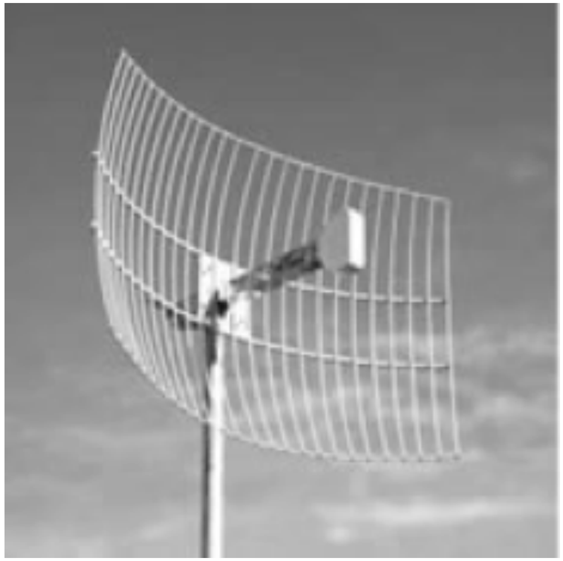
Directional Antennas



15dBi Yagi

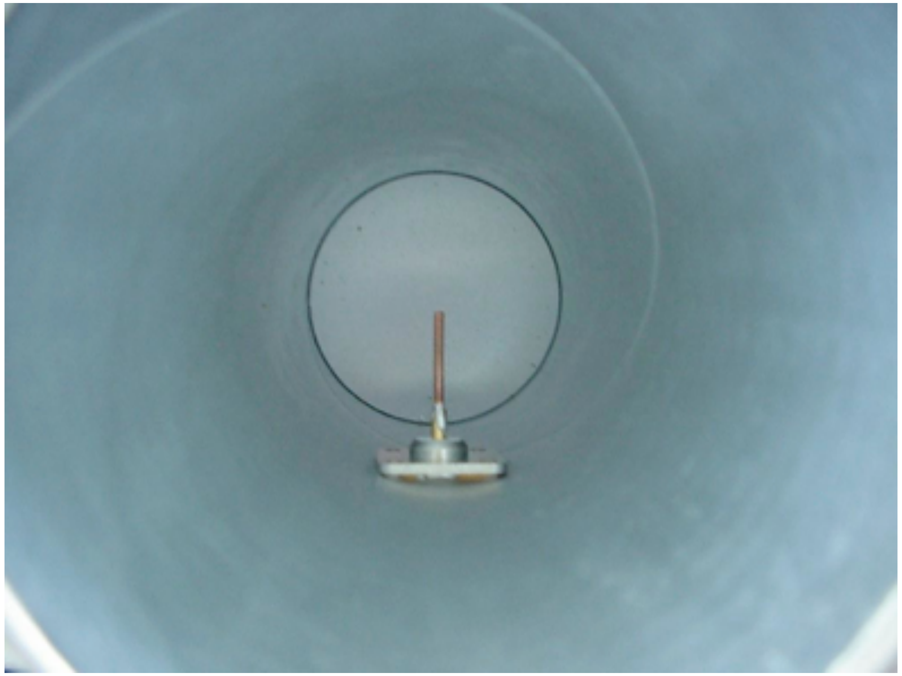
10dBi Panel

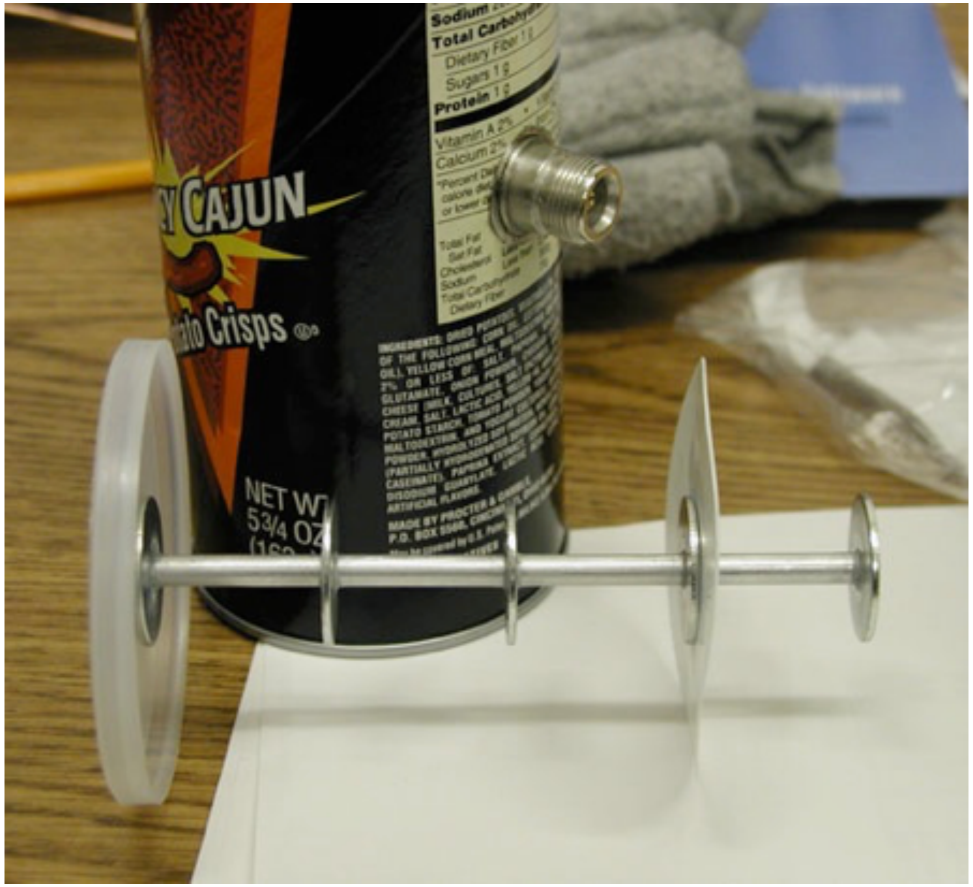




19dBi Parabolic

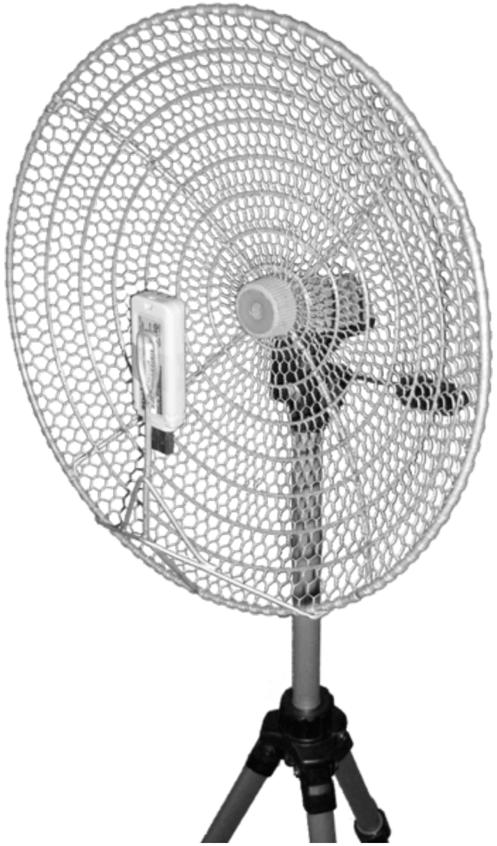
DIY Antennas





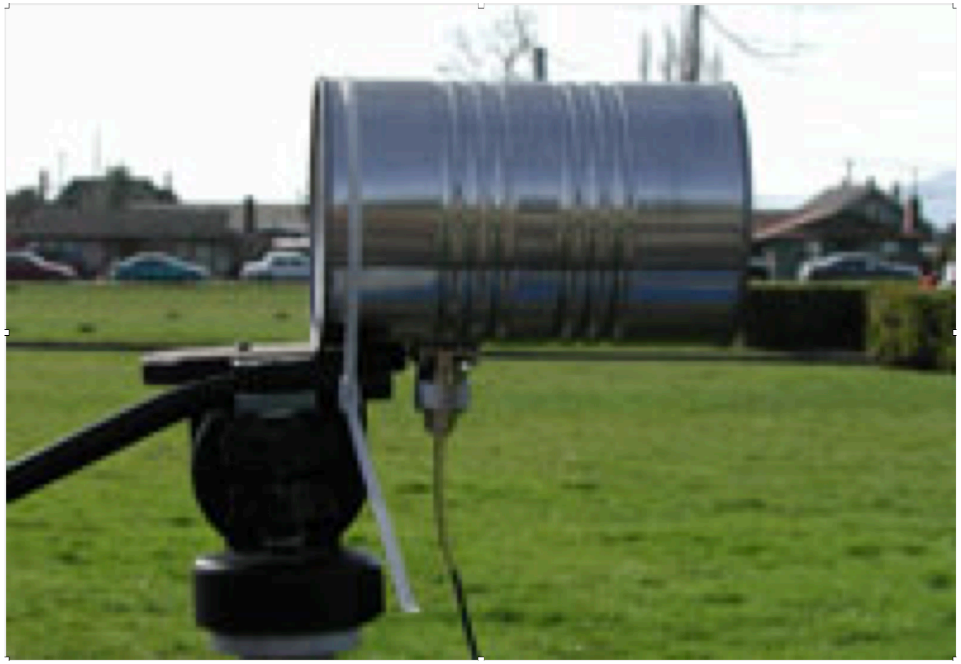
Frying scoop parabolic

- using a cheap USB Wi-Fi stick and a Chinese cook-ware
- ~12dBi



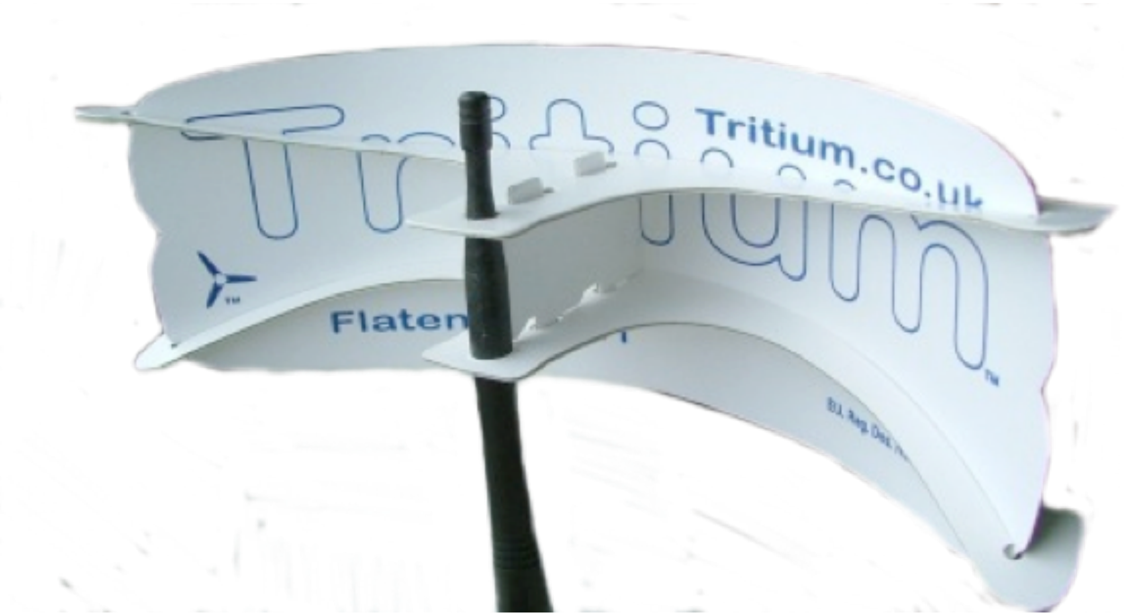
Coffee Can Waveguide

- The diameter is the important dimension, with enough length



Easy Parabolic

- Parabola from cardboard and foil.
- Can be used to boost signal for a simple dipole.



Summary

- Two modes of WiFi
  - infrastructure and ad hoc
- Two modes of authentication
  - key based and user code based
- Security issues
- Cases or conditions of using WiFi
- Two types of antennas