COSC301 Lecture 5

802.11 Wireless Networking

Zhiyi Huang
Computer Science
University of Otago

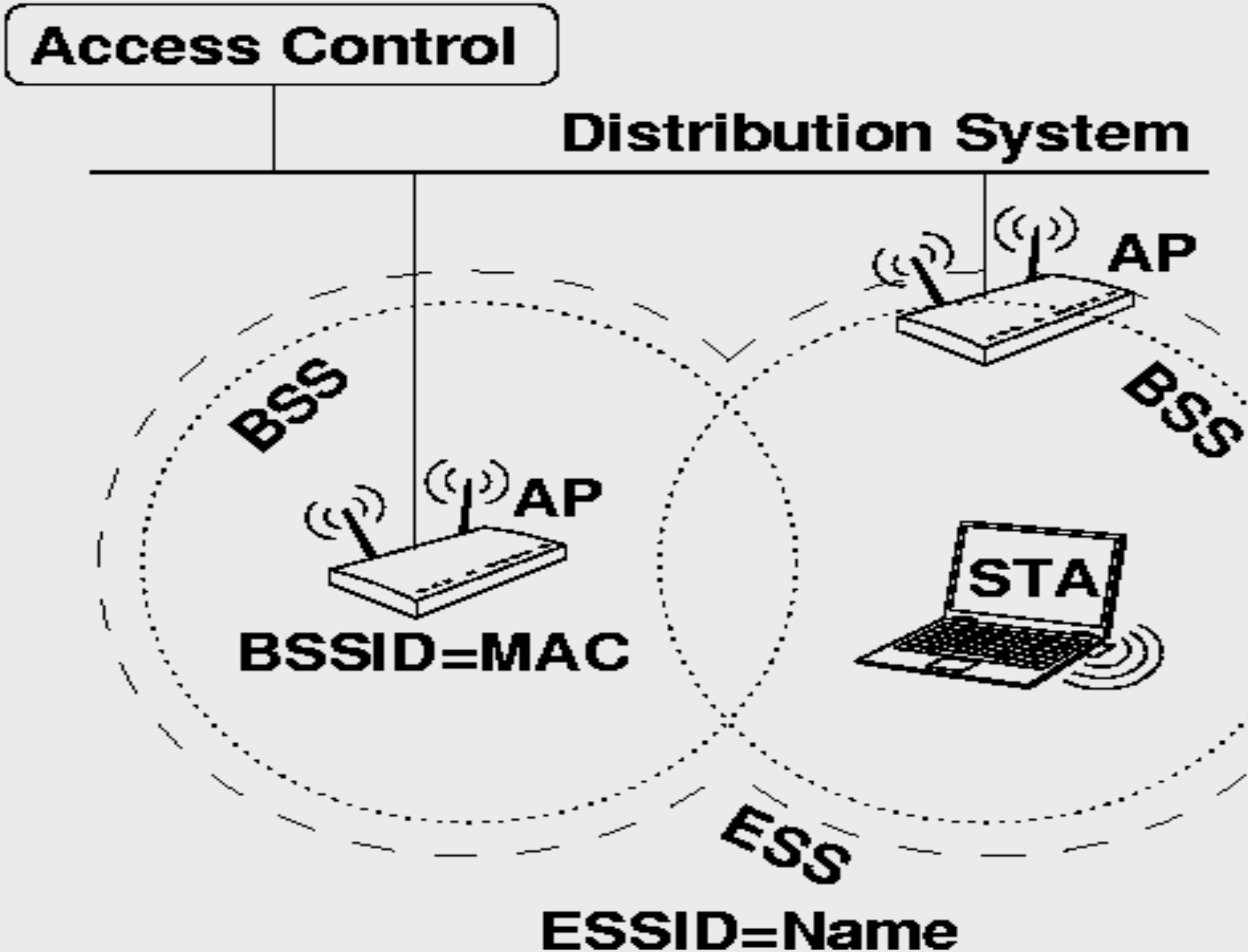
Some IEEE 802 Standards

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

802.11 Family

- 802.11b 11Mbps, 2.4GHz, Kick-started Wi-Fi technology,
  ~30m indoors.
- 802.11a 54Mbps, 5Ghz, Less common than 11g, but technically superior.
- 802.11g 54Mbps, 2.4GHz, still very very common
  Compatible with 11b. Mixed or exclusive...
- 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
- 802.11ac 1Gbps, 5GHz, ‘draft’ devices available now
- 802.11ad 7Gbps (typically less), 2.4+5+60GHz, “WiGig”

Structural Overview



802.11 Terminology

AP	Access Point
STA	Station
BSS	Basic Service Set

- A group of stations that communicate with each other and an access point, in an area called a basic service area.

802.11 Terms (cont.)

- 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

802.11 Terms. (cont.)

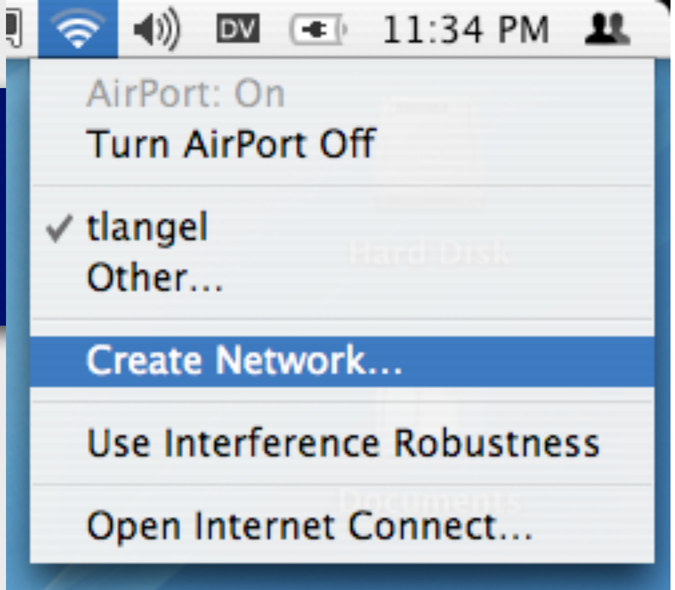
- Wireless Distribution System (WDS)
  - Backbone of multiple APs, and the inter-AP communication. Usually Ethernet, may be wireless.
  - 802.11F defines the Inter Access-Point Protocol (IAPP), but use is limited.
- Mode
  - Either Independent (Ad-Hoc) or Infrastructure (AKA Managed).
    - Ad-Hoc BSS is termed an IBSS.

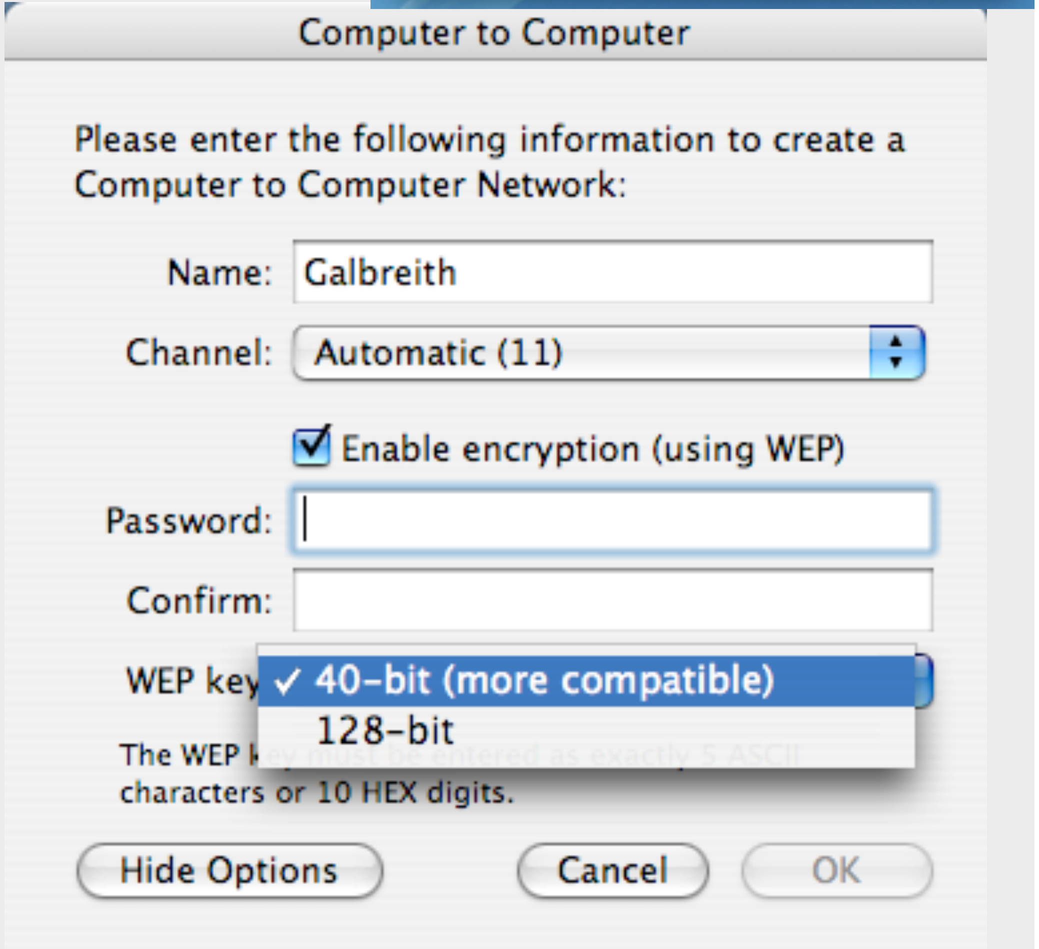
Infrastructure

- Requires an AP to associate to
- Higher layers of networking stack configured using the same methods as you would for any wired Ethernet station
  - Most commonly DHCP is used, as wireless nodes are generally mobile devices
  - Further security measures may be employed to manage security risks associated with wireless

Ad-Hoc

- 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.




Computer to Computer

Please enter the following information to create a Computer to Computer Network:

Name: Galbreith

Channel: Automatic (11)

☑ Enable encryption (using WEP)

Password:

Confirm:

WEP key: ✓ 40-bit (more compatible) / 128-bit

The WEP key must be entered as exactly 5 ASCII characters or 10 HEX digits.

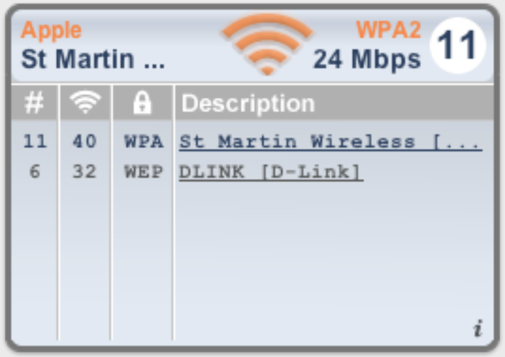
Signal Strength

Signal Level	Strength of the received signal
Noise Level	Strength of the noise
Link Quality	Signal to Noise ratio
Transmit Power	How loud we speak
Receive Sensitivity	How well we can hear

Decibels (dB)

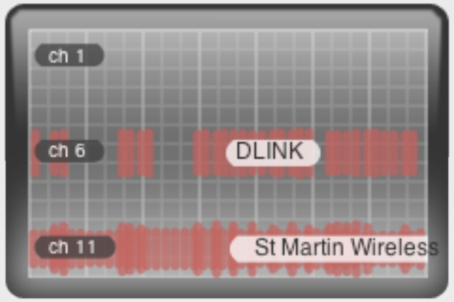
- A relative, logarithmic quantity used for easily working with antennas
- +3dB ≈ ×2
  - So a 10dB antenna would boost a signal a bit more than $2\times2\times2=2^3=8$ times
  - 32dB parabolic: $2^{10} < 32\text{dB} < 2^{11} = 1024–2048$ times
- dBi is dB relative to the isotropic radiator, used for rating antennas
  - A theoretical antenna that radiates equally well in all directions
- dBm (dB relative to 1 milliwatt) or just mW is often used for rating transmit power for transmitters

Finding a Network



Apple
St Martin ...
WPA2
24 Mbps
11

#	📶	🔒	Description
11	40	WPA	St Martin Wireless [...
6	32	WEP	DLINK [D-Link]



- 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

Finding a Network (cont.)

- …or passively scan in monitor mode
    - Some wireless NICs can allow the station to see all wireless frames on the channel
        - Getting hard to find, but Prism II chips can do this, as can others. Useful tool for wireless admins.
    - Used by products such as Kismet or AirSnort
    - Commonly used for Wardriving, etc.
    - Monitor mode is not needed for clients (stations).

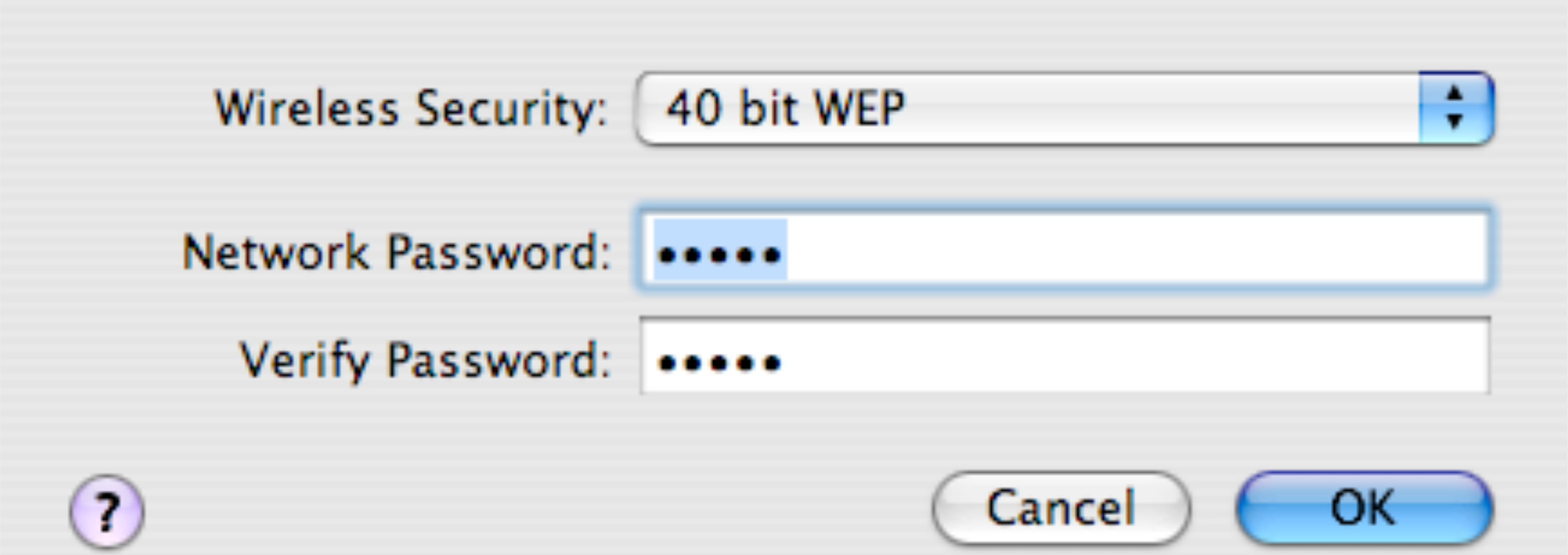
Authenticating

- Authenticates user or machine before being able to use the network
  - Consumer devices provide at least MAC filtering
    - Valid MAC addresses can be observed, and changed
  - Modern enterprise networks often have username/password (802.1X & RADIUS)
  - ... or there may be no authentication
  - You could perform authentication at a higher layer (replacing or supplementing wireless authentication)
    - e.g. requiring clients to connect and authenticate to a VPN

Security Prot. Overview

- MAC Filter List
  - Not a security protocol
  - Access Control by (changeable) MAC address
  - ACLs can be stored centrally using RADIUS
- WEP (Wired Equivalent Privacy)
  - Most common denominator
  - Minimal protection (it’s really quite broken)
  - Pre-Shared Key (PSK)
    - Large amount of work to change

WEP Configuration



Wireless Security: 40 bit WEP

Network Password: •••••

Verify Password: •••••

- WEP of *any* key-size is easily broken in under a second after 5-10 million packets [Aircrack]
- Can be given in either HEX or ASCII
- Note that “64bit”=40bit, and “128bit”=96bit
  - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

WPA

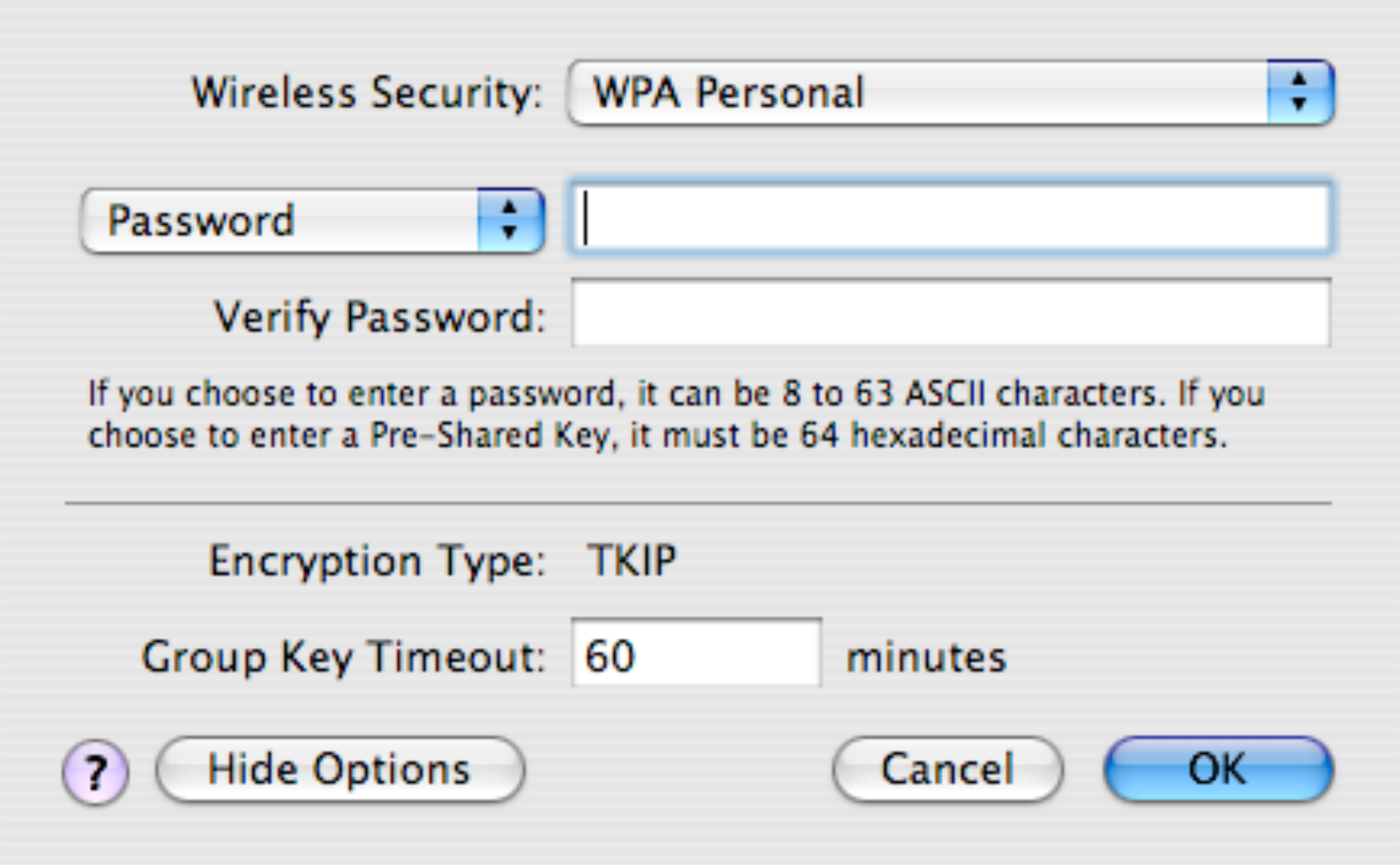
- Wi-Fi Protected Access
  - Subset of 802.11i that was released when WEP flaws became a barrier to adoption
- WPA Personal
  - WEP with short-lived changing keys
    - Temporal Key Integrity Protocol (TKIP)
    - Different key per user/session/packet
    - Performance cost if not done in hardware
 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

WPA Enterprise, 802.11i

- 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

WPA Personal

- The password or pre-shared key is the same for everyone
- How much effort would be required to change it?



Wireless Security: WPA Personal

Password:

Verify Password:

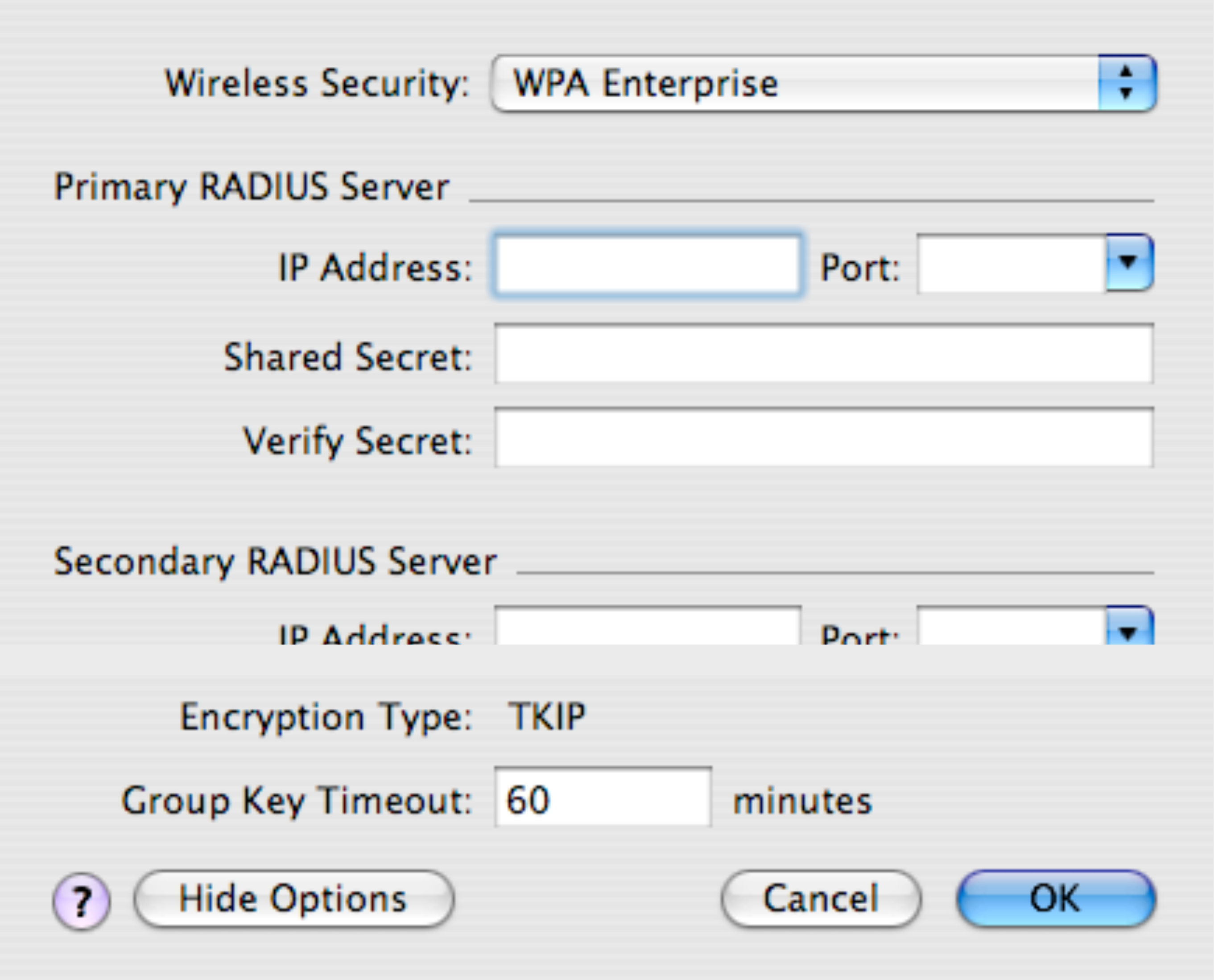
If you choose to enter a password, it can be 8 to 63 ASCII characters. If you choose to enter a Pre-Shared Key, it must be 64 hexadecimal characters.

Encryption Type: TKIP

Group Key Timeout: 60 minutes

WPA Enterprise

- Enterprise allows for username/ password authentication against a RADIUS server, such as FreeRADIUS



Wireless Security: WPA Enterprise

Primary RADIUS Server

IP Address:

Port:

Shared Secret:

Verify Secret:

Secondary RADIUS Server

IP Address:

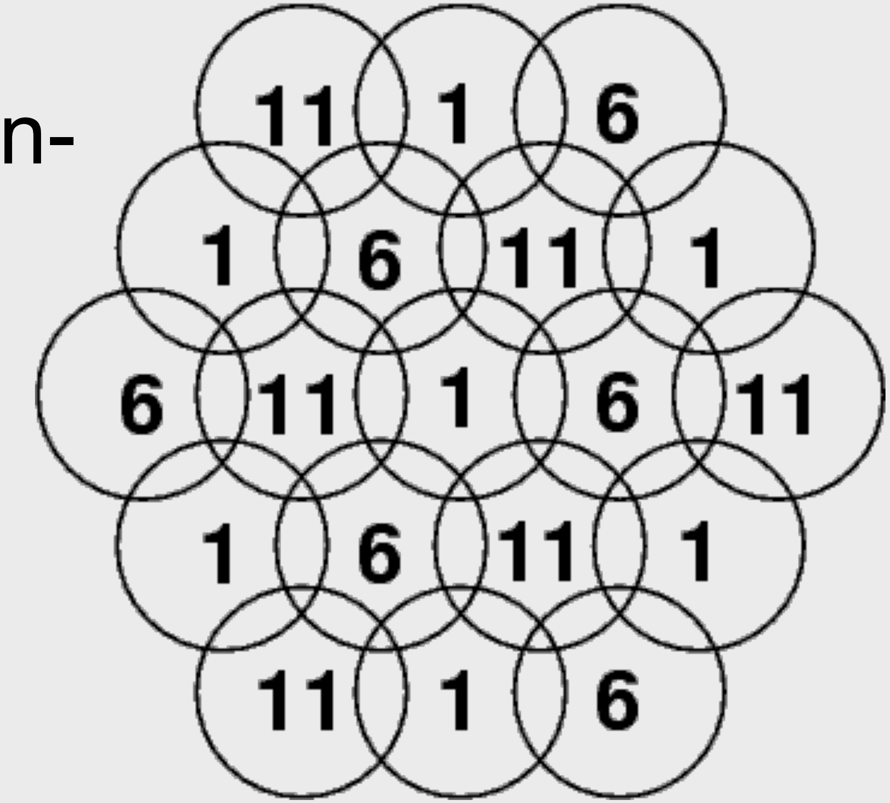
Port:

Encryption Type: TKIP

Group Key Timeout: 60 minutes

Channel Layout

- 13 channels in total (1, 2,…,13)
- Keep APs with overlapping coverage at least three channels apart
- Hex-pattern layout for non-overlapping channels
- But don't forget that space is 3D
- Limit number of nodes to about 30 per AP

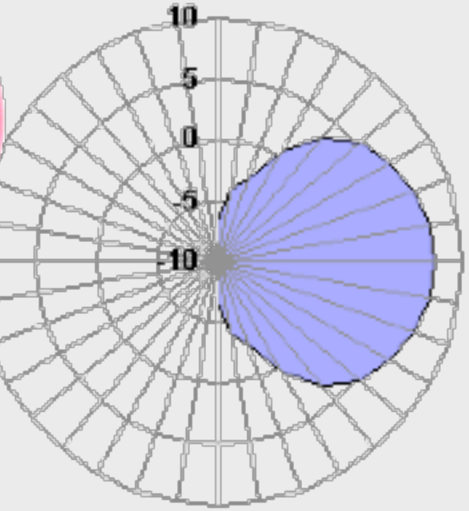


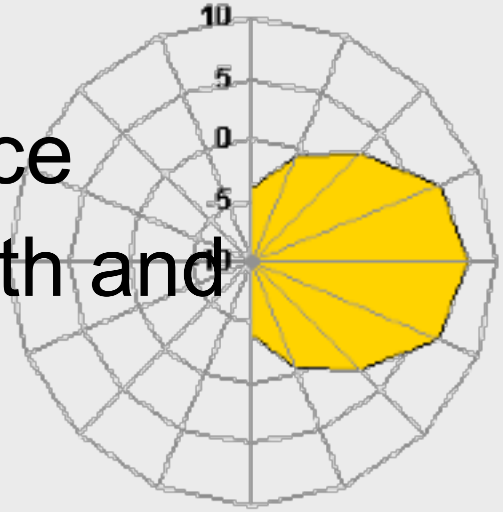
Locating Access Points

- Considerations
  - Backbone network connection
  - Power supply
    - AC supply
    - Power over Ethernet (PoE) modules or switch
  - Desired coverage area
  - AP-antenna distance (loss)
  - Environmental conditions
    - Wind disturbance; Rain; Sun (heat)

Antenna Types

- Omni-directional
  - High-gain Omni
  - Diversity antennas
- Directional
  - Panel, Yagi, Parabolic
  - Shown is a Wave-Guide “cantenna”
- Trade off polar coverage for distance
- Sometimes advertised with its azimuth and elevation to show coverage area





Omni-directional

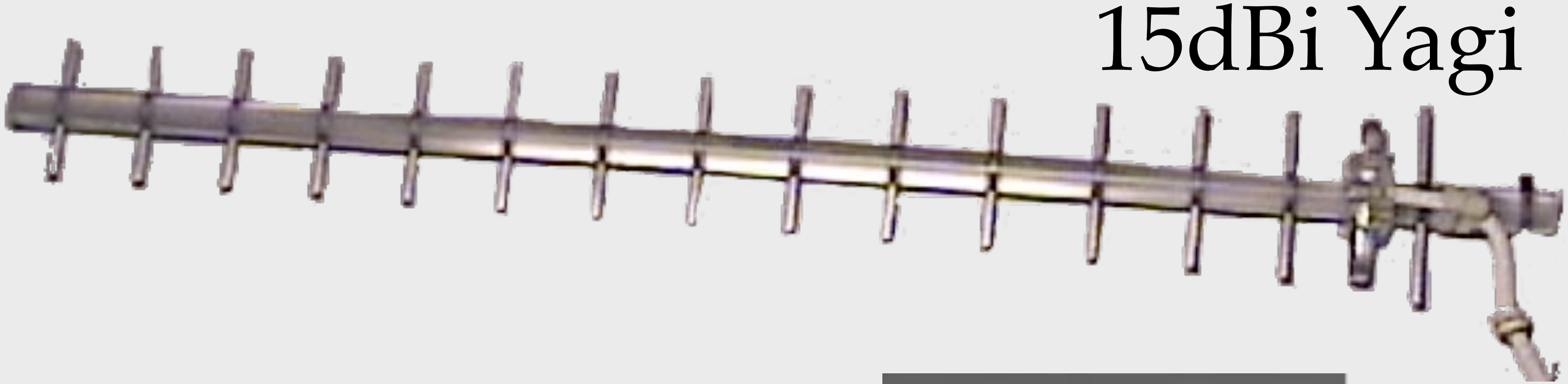
AP with antenna diversity

Linksys WRT54

7dBi High-Gain Omni

Directional Antennas

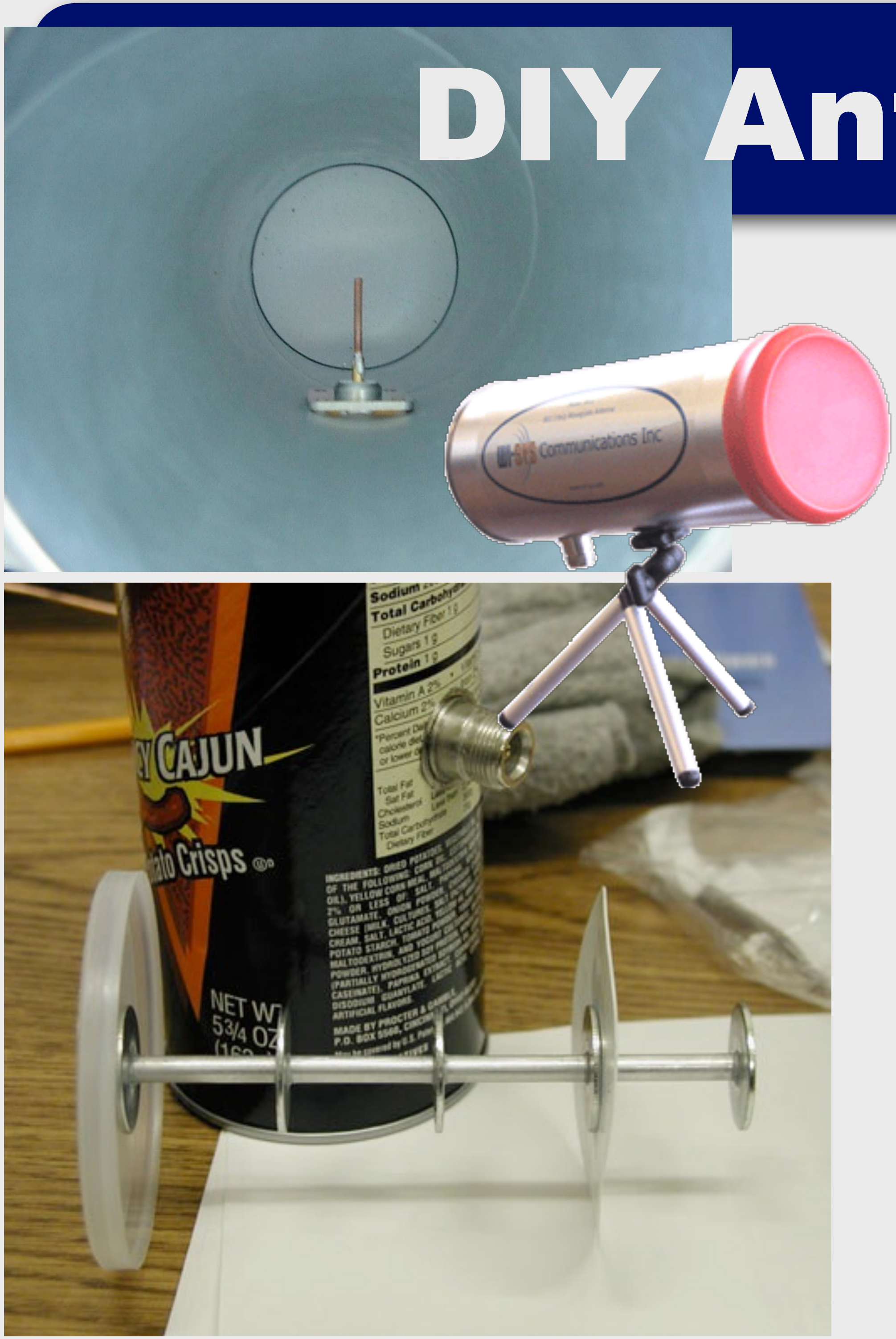
15dBi Yagi



10dBi Panel

19dBi Parabolic

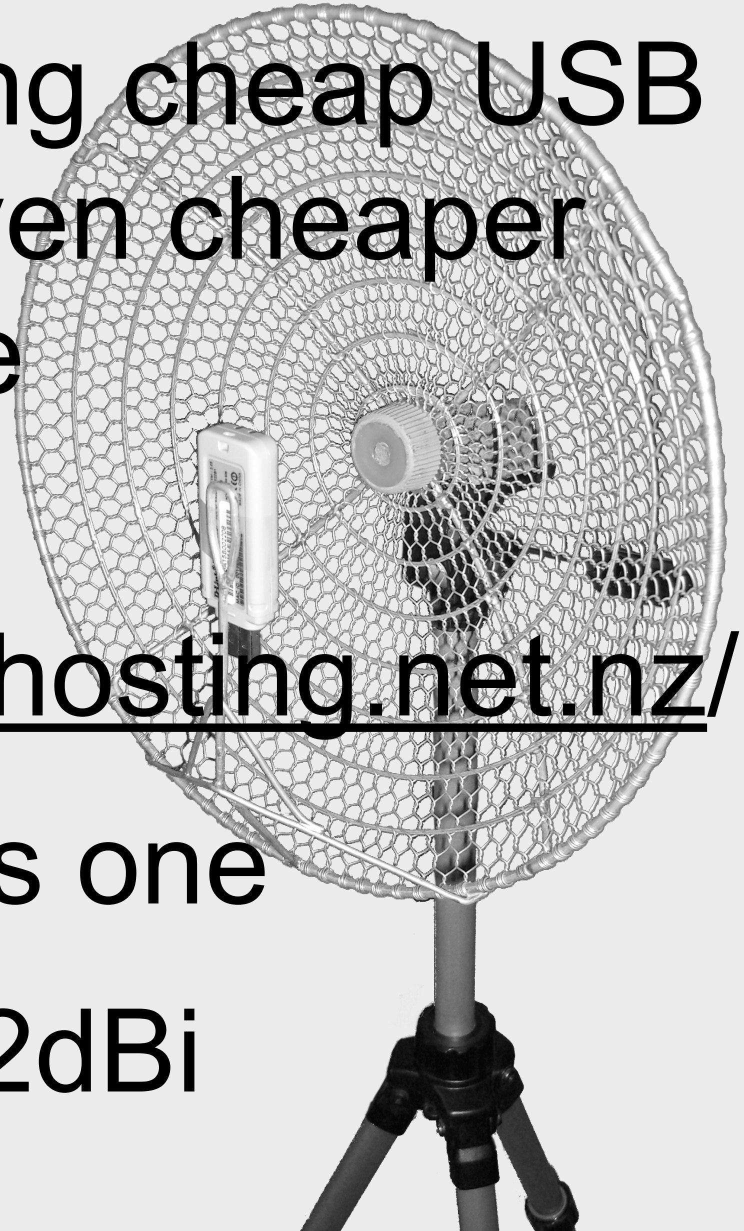
DIY Antennas



- Antennas are pretty simple, thus easy to make
- The Pringles can antenna that made DIY Wi-Fi popular

Frying scoop parabolic

- NZ innovation, using cheap USB Wi-Fi sticks and even cheaper Chinese cook-ware
- http://www.usbwifi.orconhosting.net.nz/
- Cameron made this one
- Intended to get ~12dBi

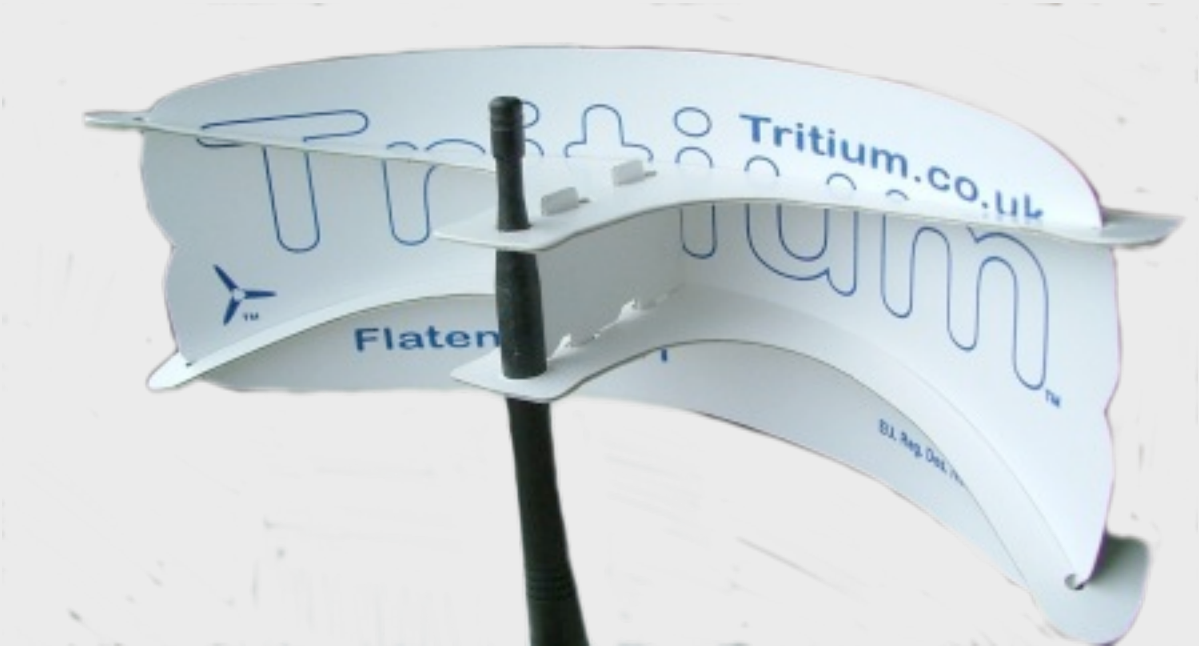


Coffee Can Waveguide

- 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.



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
  - also of wired network if not routed
- AP Spoofing

Uses of Wireless

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

References

- 802.11 Wireless: The Definitive Guide
  - Matthew S. Gast; O'Reilly & Associates
    ISBN: 0-596-00183-5
- 802.11 Security
  - Bruce Potter & Bob Fleck; O'Reilly & Associates
    ISBN: 0-596-00290-4