

# 802.11 Wireless Operations

ITL

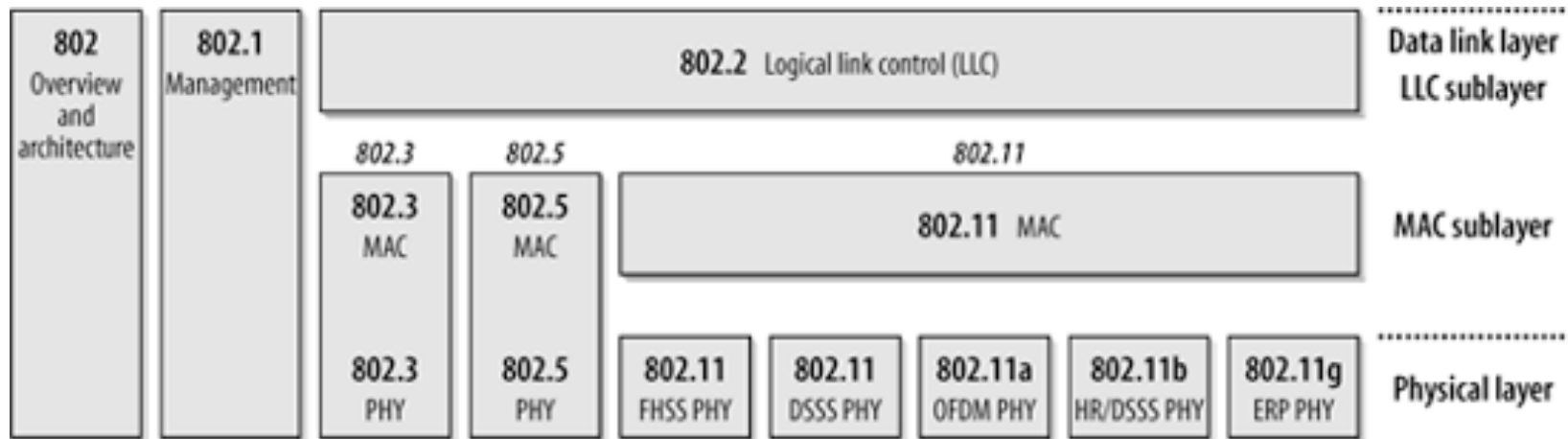
# Introduction

- Wireless networks are “different”
  - Errors are normal
  - Performance varies over time and space
- 802.11 is not “Ethernet over radiowaves”
  - The protocol and the frame format are different
- Wireless uses some unique terminology
- 802.11 Resource:
  - “802.11 Wireless Networks: The Definitive Guide”, by Matthew Gast, on Safari Online Books.

# 802.11 Basics

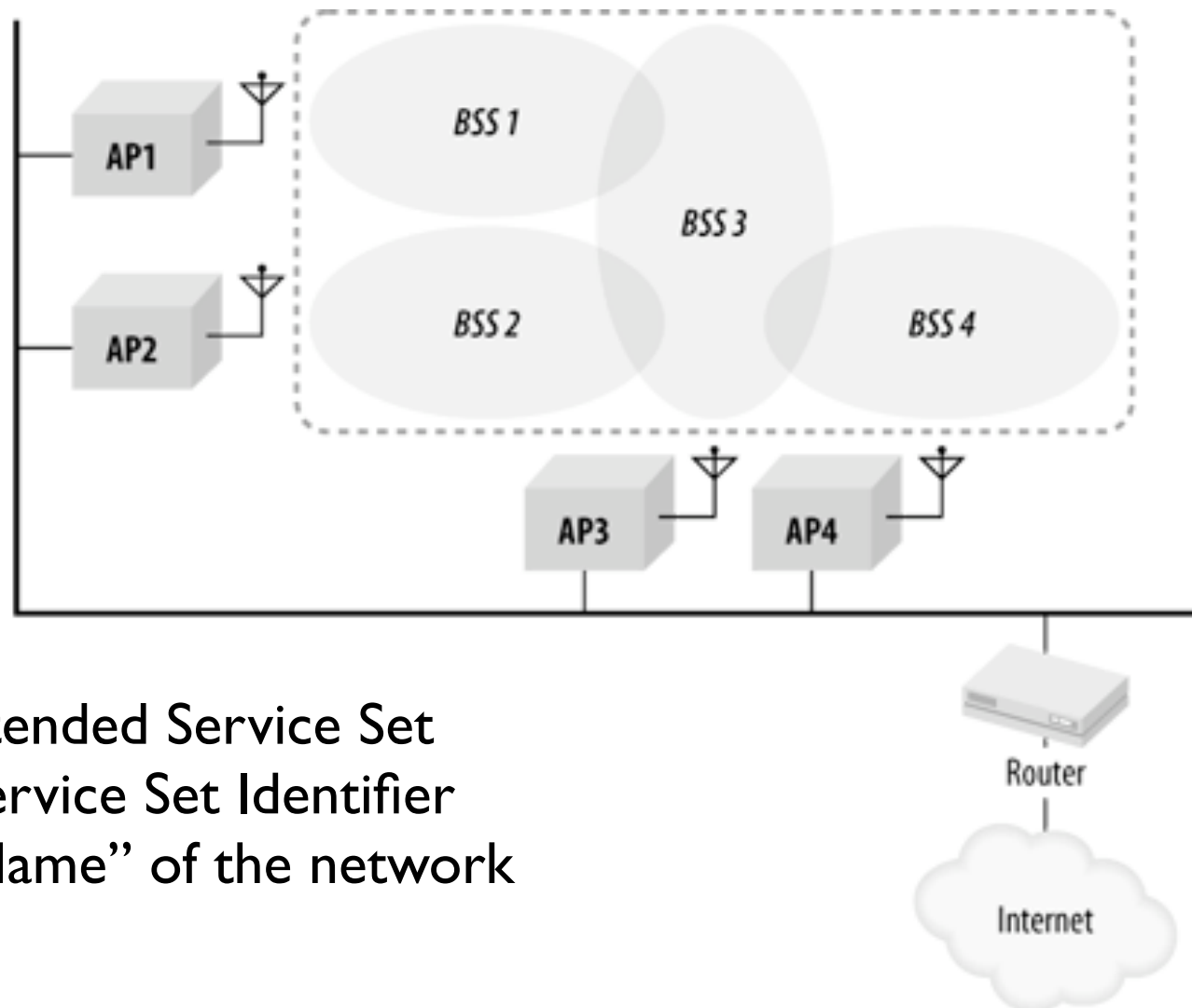
- 802.11 is a family of standards
  - Different frequency bands
  - Different encoding methods
  - Different range
- 802.11a (and 802.11n) operates in the 5GHz band, everything else is in the 2.5GHz band
- We are not alone..... (in the 2.5GHz band)
  - Cordless Phones
  - Bluetooth
  - Baby Monitors

# The 802 Family



From "802.11 Wireless Networks: The Definitive Guide", by Matthew Gast

# 802.11 Infrastructure Mode



- ESS - Extended Service Set
- SSID - Service Set Identifier
  - The “Name” of the network

From “802.11 Wireless Networks: The Definitive Guide”, by Matthew Gast

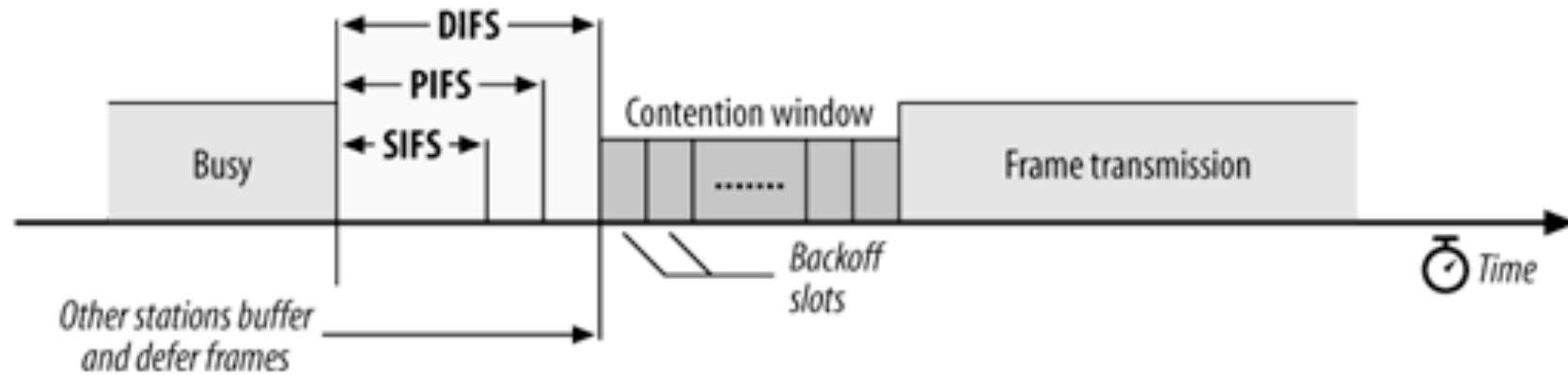
# Ad-Hoc Network Mode

- Direct communication station to station
- With Zeroconf, mDNS, and Service Discovery (stay tuned)
  - Create small peer-to-peer networks automatically
  - Exchange information among laptops, PDAs, printers, etc.
- Most operating systems allow the user to select the network mode
- A bad choice by the user means misery for everyone.....

# Basic MAC Operation

- CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
  - Also called DCF - Distributed Coordination Function
    - Listen for a current transmission
    - After transmissions stop, wait for the DIFS (DCF Inter-Frame Spacing) plus a random additional time
    - First transmitter “wins”
    - Next frame in a sequence is sent after a shorter SIFS (Short Inter-Frame Spacing), locking out other transmitters

# MAC Timing



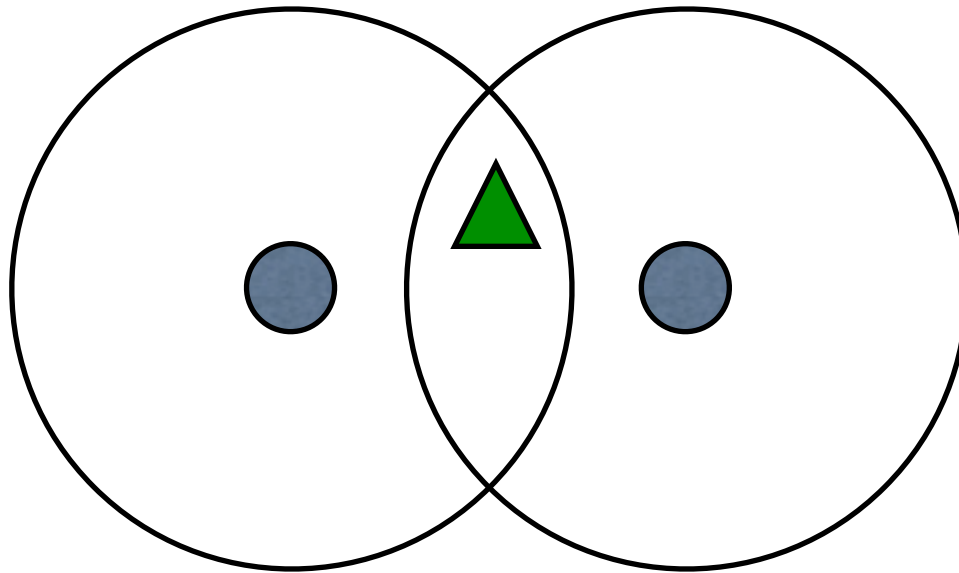
From "802.11 Wireless Networks: The Definitive Guide", by Matthew Gast

# What About Collisions?

- Non-broadcast packets are acknowledged
- Un-acknowledged frames are retransmitted
  - Retransmissions wait for a longer than normal back-off period
  - A configurable counter limits the number of re-transmissions for a frame

# Hidden Nodes

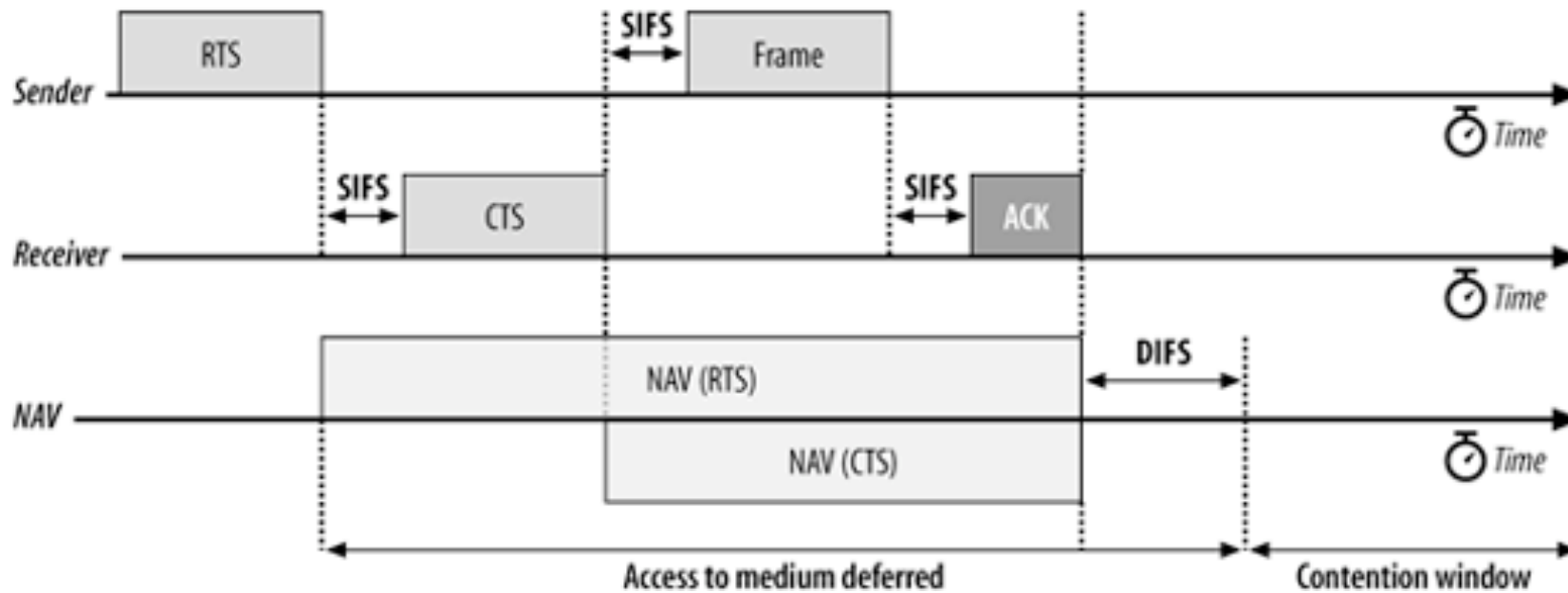
- Two stations can both see the AP, but not each other



# RTS/CTS and the NAV

- If hidden nodes exist, transmissions will collide
  - Both frames are lost
  - Random back-off before retransmit should fix the problem
  - Expensive if this happens a lot with large frames
- Stations can send a RTS frame
  - Include the Network Allocation Vector (NAV), essentially “I need the network for NAV amount of time”
  - AP responds with CTS including a NAV
    - The hidden station uses this as a “virtual carrier sense”

# NAV-based carrier sense



From "802.11 Wireless Networks: The Definitive Guide", by Matthew Gast

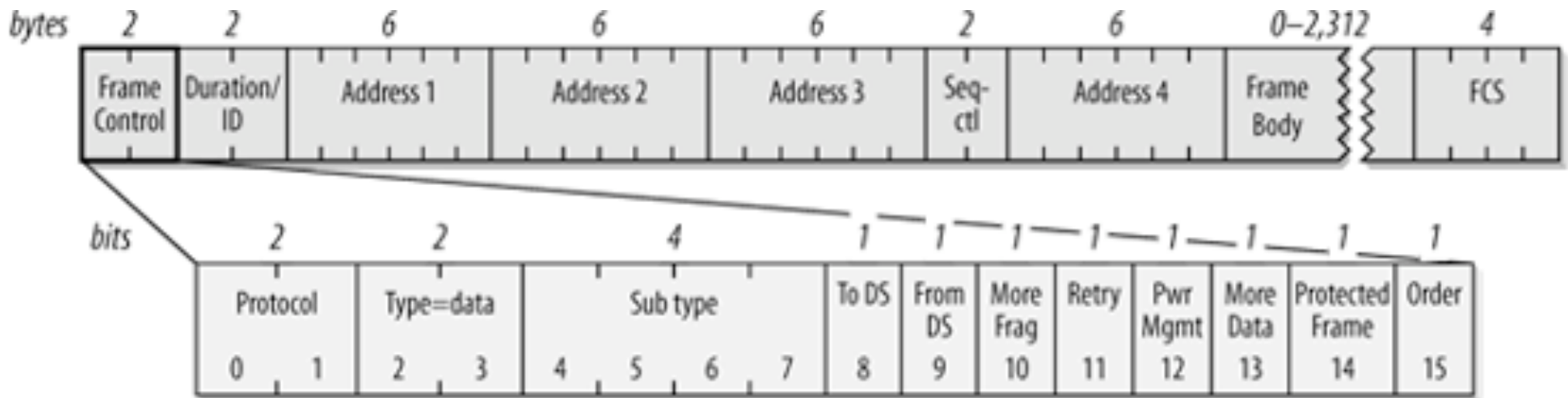
# Radio Overview

- 802.11 (DSSS)
  - 1 Mbps and 2 Mbps
- 802.11b (HR/DSSS)
  - 5.5 Mbps and 11 Mbps
- 802.11a (OFDM at 5GHz)
  - n-QAM/Convolutional Coding - 6 Mbps to 54 Mbps
- 802.11g (ERP)
  - Collection of standards
    - Compatible with 802.11 and 802.11b
    - OFDM, same rates as 802.11a, at 2.5 GHz

# 802.11

- 11 bit chipping sequence
  - **not** used for multiple access
- 5 MHz channels (1 through 14)
  - US uses channels 1-11
  - 11 MHz clock, 22 MHz spreading of the signal
  - 5 channel (25 MHz) spacing for non-interference
- Two speeds, using BPSK and QPSK

# 802.11 Frame



00=Management  
 01=Control  
 10=Data  
 11=Reserved

DS=Distribution System  
 aka Wired Ethernet

Duration/ID = (normally) 15-bit NAV value; highest order bit set. Also used for polling requests when a station wakes up from power save.

Power Management Bit = station will go to sleep after this frame

More Data Bit: transmitter has additional data for station that was dozing

# Management Frames

- Partial List
  - Beacon
  - Authentication/Deauthentication
  - Association Request/Response
  - Disassociation
  - Probe Request/Response

# Control Frames

- Partial List
  - RTS
  - CTS
  - Acknowledgement
  - Power Save Poll

# Beacon Frames

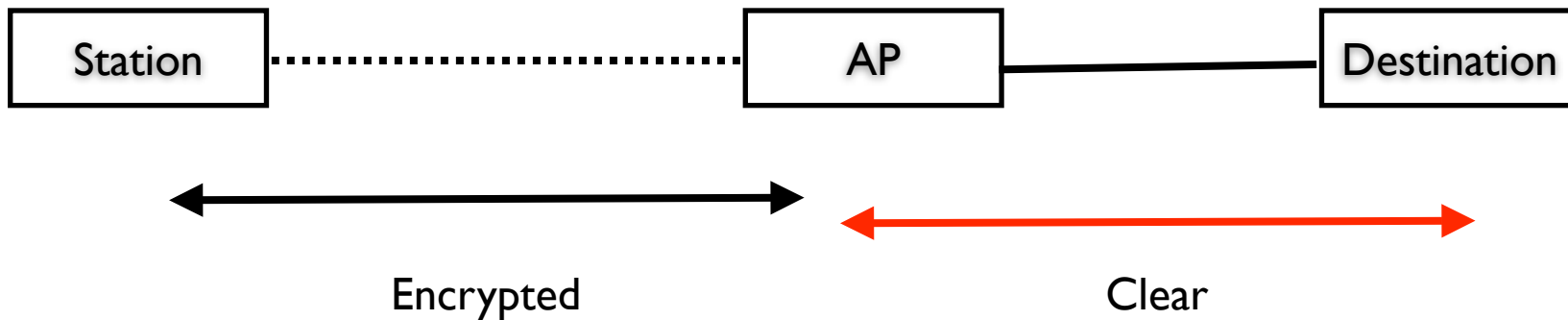
- Broadcast frames
  - By default sent about 10 times per second
    - Technically every 100 “Time Units”
    - A time unit is 1.024msec
  - Announce “Capabilities”
    - Ad-hoc or Infrastructure network?
    - SSID
    - Is encryption required?
    - Basic and Supported Data Rates
      - Stations must support all basic rates
      - Control frames use one of the basic rates

# Startup Sequence

- Station listens for beacons
- Station/user select a network to attach to
- Authenticate
  - “Open” -- just send me your MAC address
  - “Shared Key” -- original 802.11 standard is so weak that it should not be used
- Associate
  - Station sends request
  - AP accepts/rejects request, assigns ID

# Security 802.11

- Authentication
  - Station to Network
  - Network to Station **not** included
- Encryption



# Desirable

- Strong Encryption for the radio link
  - Still need to encrypt sensitive data end-to-end
- Mutual Authentication
- Ease of Management

# Options

- 802.1X
  - Enterprise solution
  - AP relays authentication to a back-end server
    - Usually RADIUS (Remote Authentication Dial In User Service)
  - Lots of options for authentication protocols
  - Open network
    - Possibly with gatekeeper as in OU's network.

# Security cont...

- WEP
  - Original standard, seriously flawed and ineffective
- 802.11i (TKIP and CCMP)
  - TKIP replaces WEP
    - Interim (draft) standard deployed as WPA
  - CCMP introduces new encryption type

# 802.11i - TKIP

- Replaces WEP while retaining the RC4 cipher
  - RC4 is often in hardware, so pre-802.11i devices may be able to do TKIP with a firmware upgrade
- Stations use a master key to derive a complete, unique RC4 key for each frame
- Master key may be pre-shared or distributed via 802.1X
- Includes key distribution schemes for dynamic, secure master key changes
- WPA is a pre-802.11i implementation, WPA-2 should be the same as TKIP

# Configuration

- Radio
  - “Channel” (frequency band) Selection
  - Power output
  - Supported speeds
  - Antenna selection (for APs with more than one antenna)
- IP Address
  - Only for administrative access, this is a layer 2 device
- SSID
  - Name for the network
    - Should the name be “announced”