Wireless Networking

2008 Update on Wi-Fi Technologies

Lewis Rosenthal, CNA, CLE, CLP
Chief Network Architect, Hautspot, LLC

Who Am I?

- Principal, Rosenthal & Rosenthal, LLC
- Network consultant since 1987
- Novell certified since 1998
- Certifications include CNA, CLE, and CLP
- Presented at Warpstock 2003-2007

Overview

- 802.11a/b/g and 802.11n
- available architectures for wireless hardware (Mini-PCI, mPCI-Express, CardBUS, PCMCIA, USB, and PCI)
- available encryption methods

802.11*x*

- Set of standards for wireless network communications over ethernet
- 802.11a: first to be ratified; 5GHz band
- 802.11b: next to be ratified: 2.4GHz band
- 802.11g: builds on 802.11b; up to 54Mbps
- 802.11i: encryption standard (WPA2)
- 802.11n: latest generation; MIMO for wide bandwidths; 2.4 & 5GHz; 20 & 40MHz channels; backward compatible

802.11

- The IEEE standard for wireless Local Area Networks.
- Encompasses several different layers of the OSI model
- 802.11a, 802.11b, and 802.11g are most common for small networks
- 802.11n not yet ratified, but "Pre-N" equipment is available, and ratification is getting close

802.11b

- Operates in the 2.4GHz band
- Employs 11 channels (US); 14 in Europe
- Subject to interference from cell phones, microwaves, remote controls, cordless phones, etc.
- Able to implement standard security protocols (security is independent of physical layer) – WEP, WPA, EAP, etc.
- Max theoretical throughput is 11Mbps
- Still the hotspot "standard"

802.11g

- Operates in the 2.4GHz band
- Employs 11 channels (US); 14 in Europe
- Subject to interference from cell phones, microwaves, remote controls, cordless phones, etc.
- Able to implement standard security protocols (security is independent of physical layer) – WEP, WPA, EAP, etc.
- Max theoretical throughput is 54Mbps
- 802.11b generally travels farther

802.11a

- Operates in the 5 GHz band
- Maximum theoretical data rate is 54 Mbps, but more realistically 20 Mbps to 25 Mbps
- In a typical office environment, its maximum range is 50 meters (150 feet) at the lowest bandwidth
- At higher bandwidth, the range is less than 25 meters (75 feet)
- 802.11a has three channel ranges, lower, middle, and upper, specified for indoor, indoor/outdoor, and outdoor use
- WLAN products now often include 802.11a technology as well as 802.11b/g (tri-mode)

802.11n

- Current draft allows for theoretical bandwidth of ~600Mbps (70-100Mbps is more realistic)
- Using MIMO, multiple antennas are employed
- Hardware is to be backward compatible to a/b/g
- 20MHz or 40MHz channel widths; 40MHz can be logically “split” to allow legacy connections
- Range several times that of 802.11b

MIMO

- My-Moe, not Me-Moe
- Multiple-Input; Multiple-Output
- Employs multiple antennas, breaking data stream into different parallel segments
- Less frequent data retries
- Minimum of 2, typically 3 or 4 antennas; 16 possible
- 1x1 = 1 Tx / 1 Rx; 4x4 = 4 Tx / 4 Rx
- STBC, SDM, TxBF, ASEL, SGI, MRC, more subcarriers, new mod rates, FEC, MORE!!!!

ENCRYPTION

- WEP
- WPA
- WPA2

WEP

- 40 or 104-bit + 24-bit IV (Initialization Vector)
- Four key strings (ASCII or hex)
- RC4 encryption algorithm
- Weak, even with 104-bit keys, due to repetition of IV in the clear (capture & crack)

WPA

- Wi-Fi Protected Access
- 128 & 256-bit keys
- Subset of 802.11i
- TKIP (Temporal Key Integrity Protocol; time-based, auto-rotation of keys)
- Uses concept of “passphrase” (WPA-Personal or WPA-PSK)
- Not implemented in all drivers (but most modern ones)

WPA2

- True, 802.11i implementation
- 128 or 256-bit keys
- AES encryption algorithm (much tighter than RC4)
- Utilizes TKIP+RC4 or TKIP+AES
- Allows for both to be used simultaneously
- Passphrase used for WPA2-Personal or WPA2-PSK
- Not implemented in all drivers

WPA Supplicant

- Necessary “shim” to provide support for WPA and/or WPA2
- Implemented in software, “above” the driver (upper layers of the OSI model)
- Responds to requests passed up the OSI chain from the driver (authenticate, disconnect, etc.)

QUESTIONS?