Indoor WLAN Design

Part II: Practical Experience

Kjell Jørgen Hole
UiB

Last updated 13.01.09

Mail: Kjell.Hole@ii.uib.no
URL: www.kjhole.com

Outline

- Why you need a good understanding of the wired network
- What to do and what not to do
- Experimental network
- Some simple diagnostic tools
- Antenna characteristics and placement
- Performance tuning
- The interference threat

Wired Network

- Most 802.11b networks extend existing wired networks

- The wired network may be quite complex, especially if it spans several buildings

- An 802.11b network depends on having a solid, stable, well-designed wired network in place

- A good understanding of the wired network structure is needed to successfully deploy an 802.11b network because the wireless network depends on services from the wired network

Single IP Subnet Needed

- Because network-layer mobility is not generally available on IP (layer 3) networks, mobility must be limited to the link layer

- To allow users to roam between BSs, all BSs must be on the same IP subnet serviced by a *single* (layer 3) router. In this case, it doesn't matter which BS an MS is connected to because the MS is reachable through the IP router

- An MS can move between the BSs and keep its IP address. As far as the outside world can tell, the MS might as well be a workstation connected to the wired network

Spanning Multiple Physical Locations

- BSs that cooperate in providing mobility must be connected to each other at the link layer (layer 2). However, the wireless network may still span multiple physical locations, e.g., different buildings

- It is possible to connect (layer 2) switches to join multiple physical locations into a single *logical* network. Roaming between the different locations is then possible by making the logical network a single IP subnet

Address Assignment Through DHCP

- To make life easy for users, MSs should automatically configure themselves with IP network information. DHCP is the best way to do this

- BSs often include DHCP servers. These servers should *not* be used. It is recommended using the existing DHCP server on the wireline network
  - note that two active DHCP servers on the same network will create havoc

- DHCP server may be placed on IP subnet for BSs, or at some central location using DHCP relay through router

What to Do

- Be nice to the network administrators (you'll need all the help you can get)

- Get blueprints or floor plans and take a tour of installation site

- Get map of wired network, if one exists

- Carry out a throughput analysis to estimate

  – peak throughputs required

  – maximum density of users

More to Do

- Take some time to work with "power users" to ensure that application performance is adequate
- Do a site survey using the devices with the poorest coverage characteristics
- If possible, turn off VPN while installing WLAN
- Make sure the BS software is properly updated
- Test the BSs before installation

What Not to Do

- It may be necessary to hide BSs and external antennas to maintain the physical security of the network. If possible, try not to put BSs up in the ceiling or any place that takes ladders and keys to get at it

- Do not select BSs with fixed antennas and no inputs for external antennas

- Amplifiers are available for increasing transmit power. However, it may be preferable to use more low-power BSs since this will provide better service to a larger number of users

More You Should Not Do

- Avoid using many different types of BSs. This complicates
  - the estimation of the cell sizes because the BSs may have different antennas and/or transmit powers
  - the updating of the BS software since it is necessary to learn multiple BS configuration programs
  - the optimization of the network throughput since some of the BS configuration programs may not give the user access to the necessary protocol parameters

Experimental Network (1)

We built an experimental network at the Department of Informatics consisting of

- 2 BSs on fourth floor
- 4 BSs on third floor
- 3 BSs on second floor
- 1 BS on first floor

Experimental Network (2)

- The BSs utilized channels 1, 4, 7, and 11
- All BSs were set up as bridges with the same network name "Laptop net"
- Roaming was possible even though we used both Apple AirPort and AmbiCom BSs
- WEP was turned off. We used VPN or NoCat for authentication

Diagnostic Tools (1)

- Affordable and good diagnostic tools were not available. The lights on the BSs often gave the best indication that something was wrong

- The *AirPort Admin* utility (from Apple) may be used to determine the IP addresses of the BSs connected to the wireline network

- Can use the Unix command "ping" to determine whether or not a BS is active

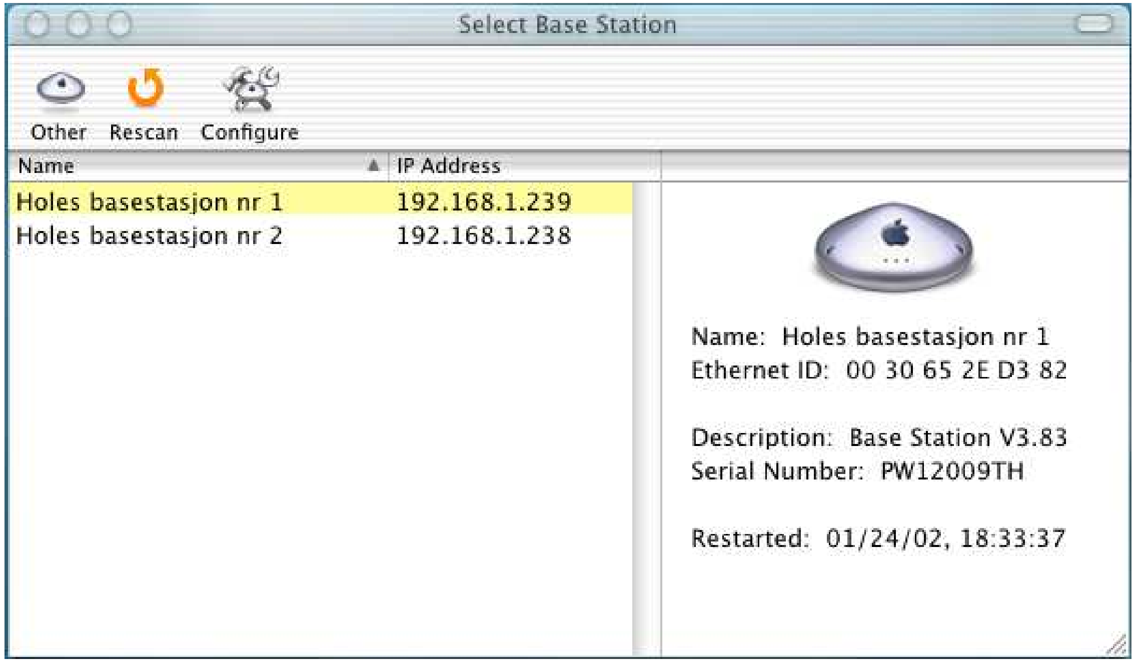

Figure 1 AirPort Admin displays list of AirPort BSs on network

Ping

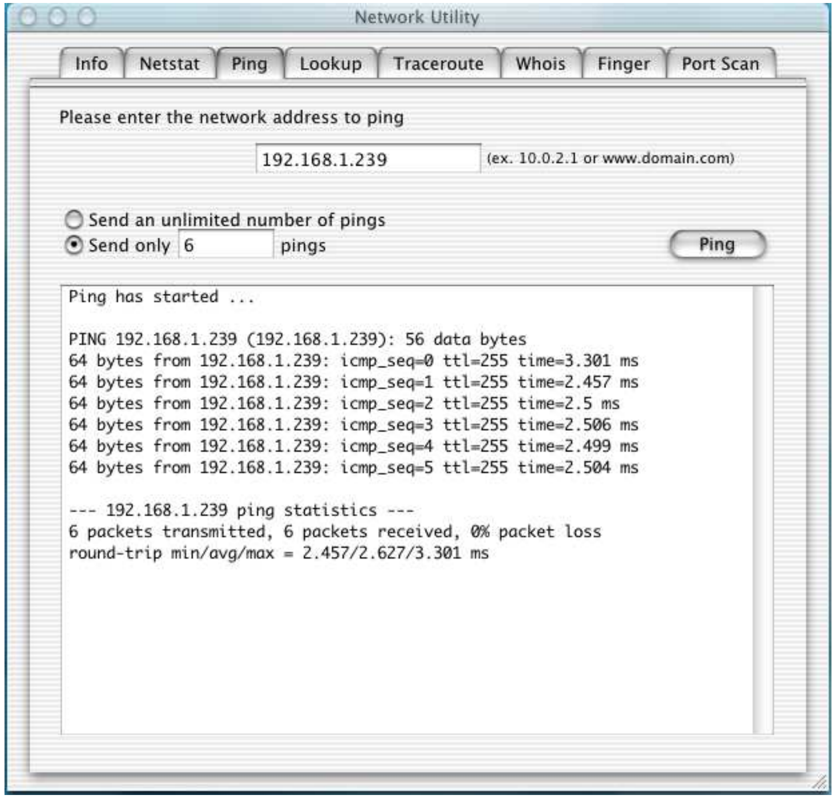

Figure 2 Unix command Ping

Diagnostic Tools (2)

- We utilized *Orinoco Client Manager* to measure signal strength

Receiver sensitivity matrix for Orinoco Silver cards

11Mbits/s	5.5 Mbits/s	2 Mbits/s	1 Mbits/s
-82 dBm	-87 dBm	-91 dBm	-94 dBm

Orinoco Client Manager Test 1

MS: Dell Latitude with Orinoco Silver Card

BS: Apple AirPort graphite

Signal path: about 6m, one wall

Measurements

	MS	BS
11Mbits/s:	100%	100%
Signal:	−60dBm	−65dBm
Lost:	0	0

Orinoco Client Manager Test 2

Signals from four different BSs measured

Measurements

BS	Channel	SNR (dB)	Signal (dBm)
3	4	33	-61
1	1	24	-69
2	7	11	-84
4	11	7	-88

This may be an example of **bad** network planning. User “sees” two good channels 1 and 4 with interchannel interference

Antenna

Antenna Device that converts electrical signals on wires to radio waves and vice versa

- made of conducting material
- radio waves hitting antenna cause electrons to flow in the conductor and create a current
- applying current to antenna creates electric field around antenna
  - as current to antenna changes, so does the electric field
  - a change in the electric field causes a magnetic field, i.e., a radio wave

Antenna Types

Omnidirectional antenna sends and receives signal from any direction

Directional antenna radiates and receives on a narrow portion of the field

- Bidirectional antenna is used to cover corridors
- Unidirectional antenna is used for point-to-point link

Omnidirectional Antenna

Figure 3 In a standard office/home environment ExtendAIR Omni antenna increases the effective range of AirPort to approximately 75m

Directional Antenna

Figure 4 In typical use, ExtendAIR Direct antenna increases the effective range of AirPort to approximately 150m with a 70° beam width of coverage. Optimal performance will be achieved through positioning of the antenna in line-of-sight of the target clients or coverage area

Antenna cabling

- A cable connects an external antenna to the BS
- Most vendors sell two kinds of antenna cable:
  - expensive thick “low-loss” cable
  - inexpensive thin cable
- The signal strength decreases with the length of any cable
- A thin cable can result in a large reduction in signal strength
- It is important to keep the antenna cable as short as possible

Antenna Characteristics

- A good understanding of antenna characteristics is needed to successfully build large wireless networks

- Antenna selection has a large impact on the range and usability of the wireless network

- Almost every *external* 802.11b card puts the antenna in the worst possible orientation: sideways and very close to the laptop (or desktop)

Antenna Characteristics and Placement

- Laptops with built-in antennas have much larger range. Many laptops have multiple antennas in the lid

- An even better range may be obtained by attaching a small omnidirectional external antenna to the client card and orienting it properly
  - use shortest possible cable to minimize signal loss

- Place antennas such that nearly all users have signal strength at least equal to -82 dBm. This ensures that most users are able to communicate at 11 Mbits/s

Performance Tuning

- Since a *wired* LAN is still the primary network for many users, the wireless network is often seen as less critical

- However, the number of wireless network users is growing, putting more strain on wireless networks

- It may therefore be necessary to tune administrative parameters to achieve the required network performance

Radio Management (1)

The most precious resource on an 802.11b network is radio bandwidth. Several parameters allow you to optimize a network's use of the radio resource:

Beacon interval Beacon frames are used to announce the existence of an 802.11b network. Decreasing the beacon interval makes scanning more reliable and faster. Increasing the beacon interval may add an incremental amount of throughput

RTS threshold Any frame larger than the RTS threshold must be cleared for departure by the RTS/CTS procedure. If network throughput is slow or there are high numbers of frame retransmissions, enable RTS clearing by decreasing the RTS threshold

Radio Management (2)

Fragmentation threshold Any frames longer than the fragmentation threshold are sliced into smaller units for transmission. In environments with severe interference, encouraging fragmentation by decreasing this threshold may improve the effective throughput

Retry limits Number of times a station will attempt to retransmit a frame before discarding it. There are two retry limits, one for frames larger than the RTS threshold and one for frames shorter than the threshold. When TCP segments are lost, TCP performs a slow start. Longer retry limits may increase the time it takes to declare a segment lost

Other Parameters

There are also other parameters that may be adjusted to optimize

- Power management
- Timing operations

The Wi-Fi Interference Threat

- If a *Wireless Internet Service Provider* (**WISP**) does not plan the **placement** and **channel assignments** of its wireless network, then the interference from other networks may cause serious problems

- Since more and more WISPs are popping up all over, the ISM band is becoming more and more crowded. Hence, the interference problem is getting worse

- Everyone has the same right to access the ISM band. Clearly, a WISP must accept interference as a part of doing business in this band

Harmful Interference

Harmful interference Interfering signals of such magnitude that the desired signals, carrying telecommunication services, are disrupted

- As an example, assume that the WISPs `ABC.com` and `XYZ.com` have networks up and running in the same area. Both experience some interference, but the WISPs are not losing connections or customers
- Then `ABC.com` decides to expand its service area by adding an amplifier on one of its omni antennas. `ABC.com` knocks out `XYZ.com`'s signals. In this case, `XYZ.com` is experiencing harmful interference

Mistakes Made by WISP

- What did ABC.com do wrong?
  - *They failed to engineer a sustainable network*: Rather than amplifying its signal strength, ABC.com should have considered adding a new BS or tried to utilize a directional antenna to broaden its service area
  - ABC.com *failed to accommodate other operators in the area*: They did not realize that the poorly planned network extension would bring down another network
  - ABC.com *failed to coordinate and communicate its plan*: ABC.com should have informed other operators in its shared service area about its planned network change

Wi-Fi Discipline

- *Knowledge*: Learn as much as possible about Wi-Fi equipment before deploying a network
- *Say hello*: Before deploying the network, send a letter of introduction to other wireless operators in your service area utilizing the ISM band
- *Join or establish a local wireless group*: Use the group to resolve frequency disputes in the area
- *Phone list*: Build a Web based phone directory for all wireless operators in the area.

Interference from Cordless Phones

- Many households and businesses use cordless phones. Most cordless phones operate at 2.4GHz, i.e., in the ISM band

- Most 2.4GHz phones use *Frequency Hopping Spread Spectrum* (FHSS) technology. FHSS hops from frequency-to-frequency across the entire 2.4GHz spectrum

- Since an 802.11b BS transmits within approximately one third of the 2.4GHz spectrum, a FHSS 2.4GHz cordless phone will clobber an 802.11b network, causing interference or even failure

What to Do

- Try changing the channel of the BS
- Maximize the distance between the BS and the cordless phone base
- Use an *remote* external antenna on your computer

Bluetooth Interference (1)

- Bluetooth radios may be found in many laptops, cell phones and PDAs
- Bluetooth devices use frequency hopping to hop over the entire 2.4GHz band
- Because 802.11b and Bluetooth devices may transmit at the same time, causing packet collisions, 802.11 networks can suffer lower performance

Bluetooth Interference (2)

- Since the transmit power of a Bluetooth device is much smaller than an 802.11 device, the distance between the two devices must be relatively small ($\approx 1m$) for significant interference to occur

- The biggest impacts are when a company implements a large-scale Bluetooth network

Many BSs May Cause Interference

- Many BSs were deployed at the CeBIT exhibition in Hanover (2003). With 76 BSs in one exhibition hall, the Internet access essentially stopped working altogether
  - The effective range of each BS was reduced to a few meters with data rates barely into the tens of Kbps
- **Remark**: Strategy for frequency planning not known

Conclusions

- Building wireless networks may not be as easy as some vendors claim. However, it is possible for "amateurs" to build small indoor WLANs

- The building of large WLANs, perhaps with point-to-point bridges to link buildings, should be left to the experts

- It is important to explain the performance limitations of WLANs to "power users"