WIRELESS BEST PRACTICES

A while ago, I mentioned I would make a separate blog post for recurring situations in wireless environments. So here I will go over some common points to help improve wireless connections.

The standards

Wireless currently uses the standards 802.11a, 802.11b, 802.11g and 802.11n. The first to standards are rarely used but often present in wireless access points (which I will call WAPs for the rest of the article) for backwards compatibility.

Wireless-g is still the most deployed standard these days, with a theoretical throughput of 54 Mbps, with a range of 40 meters. Note the word 'theoretical': in practice, it's about half of each value, about 25 Mbps and 20 meters indoors. Outdoors, with no obstacles, you can get past 20 meters.

Wireless-n is the newest standard, 150 Mbps throughput and 70 meters range indoors. In practice, it's certainly not 70 meters, and it seems to stop at the same 20 meters as the g-standard, but within those 20 meters the signal is remarkably better. That's just my personal experience. Throughput is also halved, but 75 Mbps peaks can be reached which allow for the streaming of HD video.

Collision domain and channels

Wireless is a half-duplex medium, which means only one host on a channel can transmit a frame at the same time. It uses the CDMA/CA algorithm to detect and avoid frame collisions. So the more devices are communicating wireless with one WAP, the slower the speed will be. One laptop copying files may reach 25 Mbps on a wireless-g connection, but two laptops copying a lot of data likely get about 11 Mbps each (25 divided by two, minus some increased collisions). For this, a WAP can be set to a different channel. There are 11-13 channels, depending on the country you're in. Most WAPs use channel 11 or channel 6 by default. If your neighbours use a WAP and haven't changed this, you can change the channel you're using to something else so there is less interference. Preferably choose a channel at 3 steps higher or lower: in most environments, channels 1,3 and 9 are less used and therefore have less interference.

Interference

A lot of objects can cause interference. First are humans. The human body consists of +50% water, which absorbs radio waves. One person is not such a problem, but when deploying wireless in a room filled with people, expect a weakened signal. Another important cause are

large electrical objects like refrigerators, washing machines and the like. They contain a thick layer of metal which blocks the signal. Though not often the case, some objects may form a Faraday cage, like microwave ovens (which are electrical on top of that, too) and aluminium window frames. The latter one can effectively block out +80% of the signal. Also, since the winter will start soon, a christmas tree can block signals because it contains electrical cables with lights in a spiral. Yes, I've had people complaining to me about poor signal strength, only to find out it started after setting up the tree.

Thick concrete walls can be problematic too, which is unfortunate because this is sometimes the reason people choose wireless instead of cables in the first place. In my personal experience, wireless-n seems to be somewhat better with concrete compared to wireless-g, but it's not a large difference. Wooden furniture, walls, ceilings seem to be no problem at all.

Echo

If wireless devices are placed too close to each other, echos may occur, and communication becomes slow. This is usually when there's less than 1 meter between the devices. I've seen it happen, but frankly I've always wondered why one would use wireless it there's just one meter of cable needed to solve the problem.

Orientation

Exactly above the antenna of a WAP, signal strength is very poor. So if your laptop is on the first floor and your WAP is exactly below it, it may not connect at all. Most WAPs have an external antenna that you can orientate freely: orientate it so that from the antenna's perspective, the wireless device is sideways. If you can orientate the antenna on the wireless device as well, do the same.

Wireless-n WAPs often have three antennas, and people usually set them like a fan in three directions (vendors even advertise them like that). This is not necessary, just put them in the orientation which is best for 'sideways' communication. The multiple antennas are not for a broader range, but for improved frame receiving: if the frame is not received properly on one antenna, it may be received correctly on another, decreasing the need for retransmissions. They're also used for multiple individual streams for better throughput.

Security

Leaving a wireless network unsecured these days is one of the most stupid things a network engineer can do. Anybody within range can connect and wreak havoc within the network. MAC address filtering is an option in most WAPs, but that alone is not enough. It's easy to capture a MAC source address and spoof it.

If you think WEP encryption will be good, try searching for WEP cracking on YouTube and think

again. Plenty of tutorials out there. The best option is using WPA2 or WPA-AES for home deployments. When configuring WPA2, try to choose a difficult key, with some randomisation. Some people suggest turning off SSID broadcast, but this is not always a good idea. Turning off SSID broadcast on the WAP will keep the network invisible to any new device doing a site survey, but the wireless devices already connected to it will start sending out probes when they can't find the wireless network. So: disabling SSID broadcast, using your laptop on it, then powering up your laptop in a public place away from home will make your laptop send out probes containing the information about your wireless network. So choose carefully, and personally, I wouldn't do it.

And last: of course never leave the SSID name default, it will allow for easy guessing the WAP vendor, and in turn exploit vulnerabilities or try default passwords (which you should also change).

Multiple WAPs

If the building where you're installing wireless is large enough, you may need multiple WAPs. In this case you can either use a central controller, or manage them all one by one. I'm not going to talk about the controller-based version, as this is beyond what most home users will need. For multiple standalone WAPs in a home environment, the best thing to do is to keep them all in the same subnet (so use access points, not routers!), use the same SSID (network name) and encryption, but use different channels. This will allow smooth roaming between WAPs when moving mobile wireless devices around the house.

Network card settings

There's little to change on most wireless network card driver settings. In case of problems, check the following settings:

- Mode: can be mixed, b-only, g-only, … Check if it's compatible with your WAP. Mixed is usually okay.
- Power saving mode: present on some laptop cards. Some models use this too aggressively, causing signal strength problems. Disabling it may help.
- Roaming aggressivity: when 'low' it tries to stay connected as long as possible before searching for a new WAP. Usually 'low' is the best choice, except when in areas with lots of WAPs, where 'high' will make it choose the closest WAP faster.

Also note that there's no general standard to express signal strength on laptops and mobile devices. If laptop A has 4 out of 5 bars signal strength, and laptop B has 2 out of 4 bars signal strength, that does not necessarily mean laptop A has a better signal at the moment. Some

network cards are more sensitive, and some vendors use another type of scale (e.g. logarithmic versus linear).

Source : http://reggle.wordpress.com/2011/11/21/wireless-best-practices/