12. INDOOR INSTALLATION

1. Introduction

Previous editions of this book have focused on wide-area outdoor wireless as a means of connecting communities with each other and to the Internet. However, with the availability of WiFi access points for a low price and the proliferation of portable devices that are WiFi capable, WiFi has become the de facto standard for indoor network access in Enterprises and schools. This chapter introduces the main focus points in choosing and installing WiFi networks indoors.

2. Preparations

Before installing a wireless LAN it is a good idea to first think things through a bit:

- What is it that you are planning to do with the wireless network? Is it an addition to the wired network or a replacement for it? Are you going to run applications over the network that are not delay tolerant or sensitive to bandwidth variations (like voice and video conferencing).
- The main difference between indoor and outdoor wireless is the absorption and reflection of radio waves by the building itself. What building features do you need to take into account? Do the walls have metal, water or heavy concrete in them? Do windows have metal in them (e.g. metal coating or metal grids)? Is the building long and stretched or compact?
- Do you expect users to be mainly static, or will they move a lot? And when they move, is it important to have uninterrupted handover (this means, a handover so quick that you will not notice the interruption of a voice call)?
- Are there good places to hang the Access Points? Are wired sockets and electricity for the APs readily available? Is electricity stable? If not, even indoor APs might need stable solar/battery power supplies and/or UPS.
- Are there sources of interference, like ad-hoc APs brought in by users, bluetooth devices, microwaves?

3. Bandwidth requirements

Step one in designing an indoor wireless network is to determine the need in terms of the number of concurrent users to support, the number and type of devices and the type of applications they are running. It is also important to understand the distribution of the users. Lecture halls or meeting rooms have different usage patterns than corridors. A wireless network that is hardly used and that needs to support a low number of users is easy to deploy and will not run into trouble easily. The trouble starts when the number of users and their use of the network increases. This chapter therefore focuses on high-density wireless networks.
To give you an idea for the bandwidth requirement for some typical applications:

web surfing:	500 - 1000 kb/s
audio:	100 - 1000 kb/s
streaming video:	1 - 4 Mb/s
file sharing:	1 - 8 Mb/s
device backup:	10 - 50 Mb/s

Typical installations in an office environment are dimensioned to support 20-30 users per cell and have about 1 access point per 250-500 square metres, but as mentioned before, depending on characteristics of the environment this may not be sufficient. In a dense environment there may be up to 1 device per 20 square metres. Bottom line, you need to calculate the throughput needed per coverage area.
So if you have let's say 10 users in a 100 square metre area, of which 8 are surfing the web and 2 are watching online video you will need: 8 * 1000 kb/s + 2 * 4000 kb/s = 16000 kb/s for the 100 square metre area or 160 kb/s per square metre.

4. Frequencies and data rates

The 2.4 GHz and the 5 GHz solutions differ in a few key aspects. The 2.4 GHz band has a better range and less attenuation and is supported in most devices.
The main downside of the 2.4 GHz band is that there are only 3 non-overlapping channels, which severely limits the the number of access points that can be placed in a certain area.

This is unfortunate since making smaller cells (formed by having the APs broadcast with less power) is the easiest way of creating more throughput per area.
Note: sometimes 4 slightly overlapping channels are advised, but research shows that in fact this decreases performance. Performance in general, degrades fast with overlapping channels (co- channel interference). The 5 GHz band on the other hand has a worse range but has in most geographies around 20 channels which makes it much easier to deploy without interference from adjacent channels.
The other important element is the choice of WiFi standard, considering that average throughput in Mb/s for the most common technologies are:

11b:	7.2 Mb/s
11g:	25 Mb/s
11a:	25 Mb/s
11n:	25 - 160 Mb/s

It should be noted that performance drops when, for example, both 802.11b and 11g devices are served by the same AP. In a network where client devices are using a mix of 802.11g and 11b, the AP will shift down to lower speeds.
5 GHz is a preferred choice for high performance and high density networks. As you would like to limit the coverage of each AP to one small well defined area anyway, signal attenuation by walls etc is an advantage rather than a problem.
The deployment of 2.4 GHz for the majority of devices, combined with 5 GHz for the "important devices" is worth considering too.

5. Access Points choice and placement

When it comes to choosing Access Points (APs) for indoor wireless there are essentially 2 architectural choices: controller based and "fat clients". Fat clients are stand-alone APs that have all the intelligence on board to manage a WiFi network (choosing SSIDs, encryption method, routing/switching etc.). The controller-based solution on the other hand has APs that implement the minimal functionality to offer a wireless service along with a central controller that is common for all APs at a location.

The central controller also has all the intelligence and all traffic from the APs directed to it.
The choice between one of the two architectures is a trade-off between cost, ease of management and scalability. In general one can say that the more complex the environment and the larger the size the more attractive it becomes to run a controller-based solution.

Access Points should in general be placed in the areas with a high density of users, the signal will probably "leak" sufficiently to also serve the less dense areas. Unfortunately the overall performance of the system will mostly be determined by the clients, not the APs, so the placement of the APs, while important, can only do so much for the performance of the overall system. Other radio sources in the WiFi bands have a very strong influence on the performance of the WiFi network, so in general, if possible the APs should, as much as possible, be isolated from other radio sources, by using walls, ceilings and people as "shields".

In order to improve performance it is possible to use external antennas. Omni directional antennas are the most commonly used and they provide a coverage area roughly circular around the AP. In most indoor cases, however, APs will be installed on walls, ceilings, or columns, and omnidirectional antennas are a bad choice, if you look at where the radio waves are going, and where the users are.

So for these cases in which the AP is not at the centre of the area to be covered, directional antennas are an alternative. Some hotels and conference halls, for example, place small directional antennas at the corners of large, open areas or overhead to provide a "canopy" or "umbrella" of signal coverage in large spaces. Keep in mind that the many reflections typically encountered in an indoor environment make it difficult to try to fully control a specific coverage.

Access Points can be mounted on the ceiling, on the walls or in furniture, each with different characteristics. Ceiling mounting gives a good blanket coverage, wall mounting often gets the APs closer to the users and APs under tables or chairs or within furniture can use the natural isolation to create small cells with little interference from neighbouring APs, but there might be concerns about the possibility of harmful effects from the radiation emitted.

Lastly, for really demanding high performance networks, APs with smart adaptive antenna technology might be an option. They come at a price, but offer the advantage of adapting the radio signal to the locations of users dynamically - they will direct the radio waves to where they are needed, at each point in time.

6. SSID and Network Architecture

Indoor networks are likely to serve many concurrent users. Larger complexes like a university campus typically consist of many buildings, each with their own indoor network, and outdoor networks in between.

It is therefore important to make a good plan for your SSIDs.
Note that the SSID defines the broadcast domain on Layer 2 of the network. SSID planning needs to play together with your Layer 3 network architecture. If you would like users to roam seamlessly across your whole wireless network area, within or even beyond one building, then all APs should offer the same SSID, for example "UniversityWireless", or "eduroam" for a university that wants to participate in the global roaming service that eduroam offers.
However, users who stay within one SSID will not require or request a new DHCP lease, so you will have to accomodate all users within ONE Layer 3 subnet.
For a large campus, this might require a large flat subnet for all wireless users.
This is a trade-off situation - you can either have huge subnets with seamless roaming, or a more manageable subnet architecture with separate SSIDs such as "Library", "LectureHall", "Cafeteria", ...

7. Post Installation

Now that the infrastructure is in place it is important to make sure that everything works as expected and remains like that. This can be done in the form of a site survey, measuring signal strengths and throughput. But in the end the main reason to install a wireless network is to serve the users of it, so listening to users complaints or issues is equally important. Demand constantly changes and so does the state-of-the- art. It is important to keep up to date with user requirements and match that to planned upgrades of the technology you are deploying.