Wireless Site Survey Guide

Site surveys are fundamental tools for those who deploy wireless local area networks (WLANs). Understanding the radio-frequency (RF) environment in which the WLAN will exist, and the level at which access points are "visible" throughout the facility is critical to a solid deployment. A well-executed site survey aids implementation, security, functionality and performance tasks. Correctly executing site surveys requires careful planning that takes key ideas into consideration: you must think in three dimensions, not two; you must plan beyond the walls of the installation; you must understand there is equipment other than what you will deploy, and that not all equipment will work together well; and you must keep in mind that a site survey is a temporary view that will need to be changed over time.

Physically executing a site survey requires adhering to key strategies including walking around, testing your assumptions, documenting the survey results and building continuous site reviews into your procedures.

Think in three dimensions

Radio Frequency (RF) waves move in three dimensions, so network planners and administrators who deploy WLANs need to think in three dimensions. An access point installed on one floor will most likely be visible on a floor above and below, as well as along the floor itself. Unlike the packets on a wired network, RF energy will keep going until it is either blocked or so weakened from distance that a receiver can no longer discriminate the signal from background noise. Think of the radio signals moving out from your access points as a balloon that slowly gets pushed out of shape as it encounters obstacles. Objects like metal file cabinets, metal stairs in the emergency exit, water filled plant leaves in a planter outside your office, or any of a thousand other items will affect the shape and intensity of the radio pattern by either reflecting or absorbing the signal.

Just to make matters more complicated, reflected signals may ultimately reach the intended receiver by taking a longer path from client to access point, arriving just a little later than the unreflected signal. When the same transmission is received several times after following different paths, it's called multipath reception. This multipath problem has plagued radio specialists since the days of Marconi's original radio experiments in the early years of the twentieth century. The results are similar in nature to the "ghost images" that plagued television before cable and satellite TV. Most current wireless networking access points have implemented twin antennas (sometimes hidden inside the plastic) that allow them to compare all signals received and differentiate the most direct from the many possible reflected signals. Access points, and some NICs, employ complex mathematical models that allow receivers to figure out which signal is the original and which signal has been bounced all over the building.

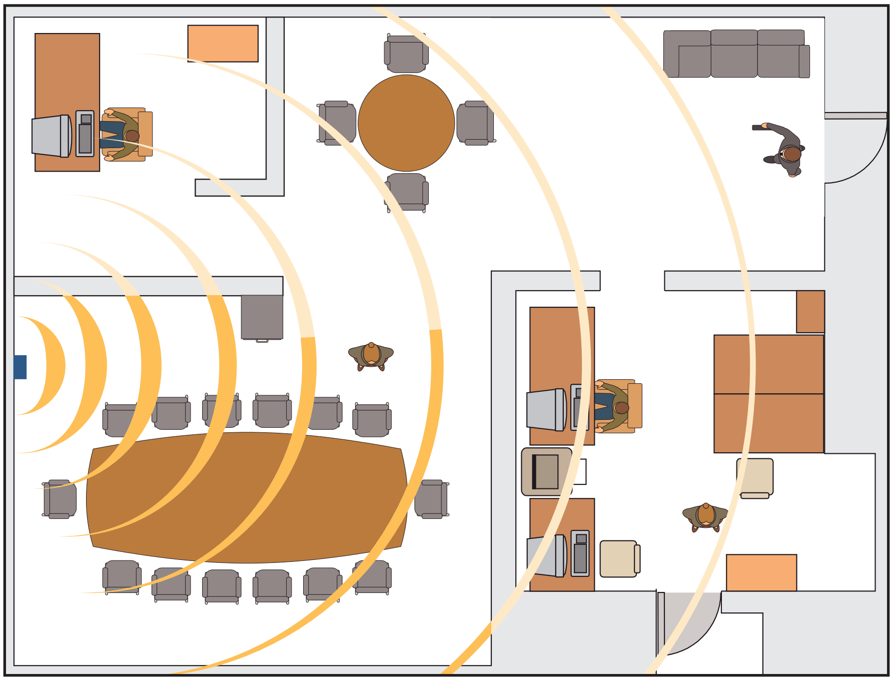


Figure 1. Signal strength from the access point will diminish due to obstructions as well as distance.

Don’t stop at the walls

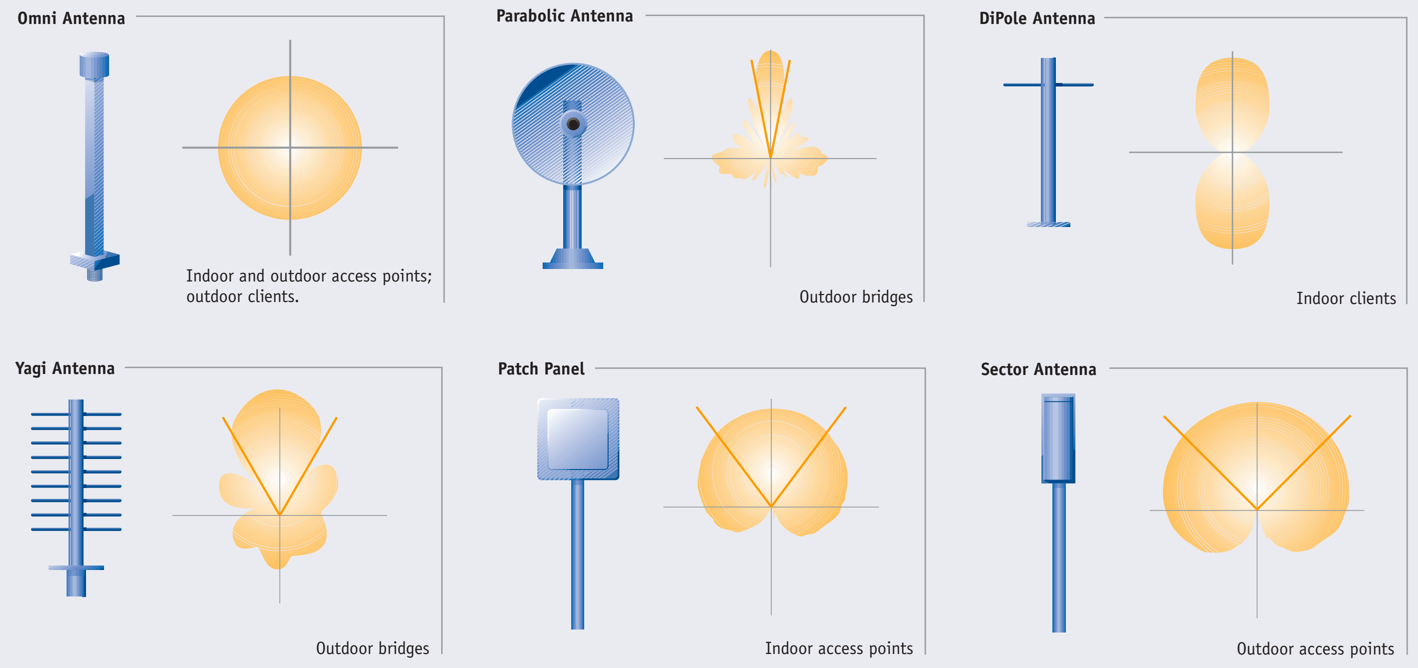
When you do your site survey, don’t stop your measurements when you get to the boundaries of your office/building/campus. Keep going and see how well your neighbor can receive your network signals. In your wired network, you can make sure you don’t wire up your neighbor, but keeping your network inside your building is not so easy in the case of WLANs. The rule is simple: if your neighbor can hear an unsecured wireless signal, then they can, with little effort, use it.

Figure 2: A small drop-ceiling antenna by HyperGain gives a 3db gain over the stub antennas that are standard equipment on access points.

There are always more sensitive antennas

The little stub antennas on your 802.11a/b/g card typically have almost no gain compared to the basic reference design. While they provide adequate reception for most applications, it doesn’t take much in the way of design and implementation to improve on the performance of the standard equipment. Many external antenna designs are available that can concentrate the radio signal through a process called “passive amplification” and improve received signal strength and quality. As an example, a 12db (decibel or db is the measurement of radio signal strength) potato chip can antenna

Antenna types and radiation patterns



	Client	Ceiling Mount	Patch Wall	Yagi	Parabolic	Sector
Type	DiPole	Omni	Directional	Directional	Directional	Directional
Gain	2 dBi	5 dBi	5 dBi	10 dBi	20 dBi	12 dBi
Beam Width	360° H	360° H	75° H	55° H	12.5° H	90° H

Figure 3: Transmission patterns that maximize useful distance in one direction will limit the breadth of the pattern.

will passively amplify the original signal 16 times. This is the equivalent of installing an amplifier that is many times the power of the low-power unit allowed in 802.11 applications. In experiments under ideal conditions, people have been able to detect signals several miles or kilometers away from the point where those little stub antennas have given up.

The same antenna variations that affect the strength of a transmitted signal also change the shape of the RF energy "balloon." Unidirectional antennas like Yagi or parabolic dish designs will stretch the RF balloon into a long narrow shape, concentrating the energy in a single direction.

Omnidirectional antennas, such as the stub antennas standard on most access points, are designed to transmit a pattern that is equally strong in all directions. Individuals setting up access points should be aware of an odd artifact created by most antennas; they will tend to focus most of their energy pattern in one direction, while smaller "side lobes" of weaker signals go in other directions. While the side lobes don't display the intensity of the main transmission lobe, users can connect perfectly well using these lobes, as long as they fall within the transmission pattern. Many wireless network administrators have been surprised by unauthorized users who have found one of these secondary lobes, parked in it, and happily connected to the network.

Not everyone is going to play nicely

The 802.11a, b and g wireless network standards are in radio frequency ranges designated by the Federal Communications Commission (U.S.) as available for unlicensed devices. (2.4 GHz band for 802.11b/g and 5 GHz band for 802.11a). Designated frequency ranges vary by country and region. The biggest issue in using an unlicensed range is that lots of different devices are allowed to operate in the same patch of radio spectrum. Cordless phones, microwaves, baby monitors, and many other devices all use or generate signals within this range, along with amateur radio operators (in portions of the range) and other, more powerful devices in other portions. Unlike heavily-regulated portions of the radio spectrum, there are no FCC inspectors ready to enforce non-interference rules. If your neighbor's cordless phone is interfering with your wireless network, you can't make him change phones. It's your responsibility to adapt to the circumstances, not theirs.

Things change – check more than once

Use "updating your wireless environment" as a good excuse to take a pleasant walk around your facilities. Finding out if your corporate neighbor has, for example, just added a Wi-Fi network would be a good thing to know about before you find that your access points and theirs are on the same channel. A bit of advanced information means you can respond with a tilt of an antenna or an addition of a new access point to strengthen the signal where your coverage may otherwise be overwhelmed by the "noisy neighbor."

Another benefit walking around brings to network management is the ability to document changes in your access point coverage pattern as employees move furniture around. Perhaps you'll find that your building manager has moved a metal lathe under the new wall, creating an impenetrable radio shield between the access point and a conference room. In some industrial settings, it's possible you'll stumble across a new arc welder and discover that an arc welder is perhaps the most effective radio-jamming device ever invented. Each enviromental change has the potential to generate a multitude of support calls that users will always attribute to your network instead of outside forces.

How paranoid do you want to be about access?

Do you really want to have a chalk mark on the sidewalk outside your building indicating that you're the new "wireless hotspot" for the neighborhood? If you don't, or if this is the first time you've thought about the question, the issue becomes one of where you want to spend your money. Do you stop the guerilla (unauthorized individuals trying to use your system) at the wireless access point or do you stop them just a bit further back in the network?

The easiest preventive measure is to simply turn on WEP (Wired Equivalent Privacy) and turn off ESSID broadcasting. While WEP has some well-publicized flaws, it's still much better than nothing. And, for the most part, WEP costs you nothing except a bit of time to set the keys on the various access points and NICs. Doing something as simple as turning off the ESSID broadcast and turning on WEP won't keep everyone out, but it will keep you off "hotspot maps" generated by "NetStumbler" and guerillas "WarDriving" your neighborhood.

Access control

With considerable debate raging over 802.1x and possible fixes for WEP, a large number of Wi-Fi installations have taken the attitude of stopping the guerillas after they associate with the access point, but before they get into your LAN. Popular because it's easy to deploy, the authenticated gateway method simply forces the wireless user to authenticate before any of their traffic can pass onto the LAN from the wireless world. This method, similar in concept to that used for dial-up access, is easy to understand. If you already have an authentication server such as RADIUS enabled for your modem pool, then implementing this method will be low-cost, reducing the total cost of ownership for your wireless network.

No peeking

There are a great many times that the data sent over your wireless network would be best kept away from prying eyes. In this case, a more aggressive approach would need to be taken. Available methods:

- VPN or encrypted mobile IP will fully encrypt the entire datastream from the client to the VPN server(s)
- Use encrypted clients like SSL or SSH
- Implement one of the emerging 802.1x wireless encryption clients
- Use a layered approach by combining some of the above

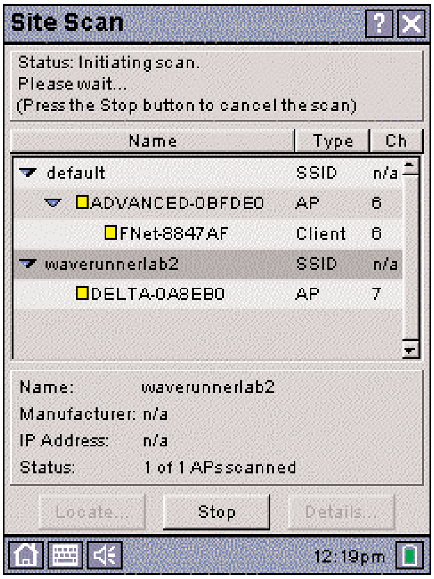
Whichever security technology you choose for your wireless network, keep in mind that the most important network security components are policies. Spend time working on acceptable use policies before you install the first hardware for your wireless network. Use the initial site survey to shape wireless access in your facilities so that you reduce the chance of accidentally sharing information or access with your neighbor. And, make sure you document every piece of hardware or software you install, and every change you make to either.

A successful installation begins with a site survey

Steps to a successful installation

What's already there?

Just because you didn't install an access point, doesn't mean there isn't one already there. Wireless LANs are one of the technologies that echo the original PC and handheld PDA in their corporate deployment – many are being installed by users before the IT department gets around to an official deployment. You should find out – before you begin your installation – whether the SOHO access point hidden under someone's desk is providing access to your network.



Site Scan

Status: Initiating scan.
Please wait...
(Press the Stop button to cancel the scan)

Name	Type	Ch
default	SSID	n/a
ADVANCED-0BFDE0	AP	6
FNet-8847AF	Client	6
waverunnerlab2	SSID	n/a
DELTA-0A8EB0	AP	7

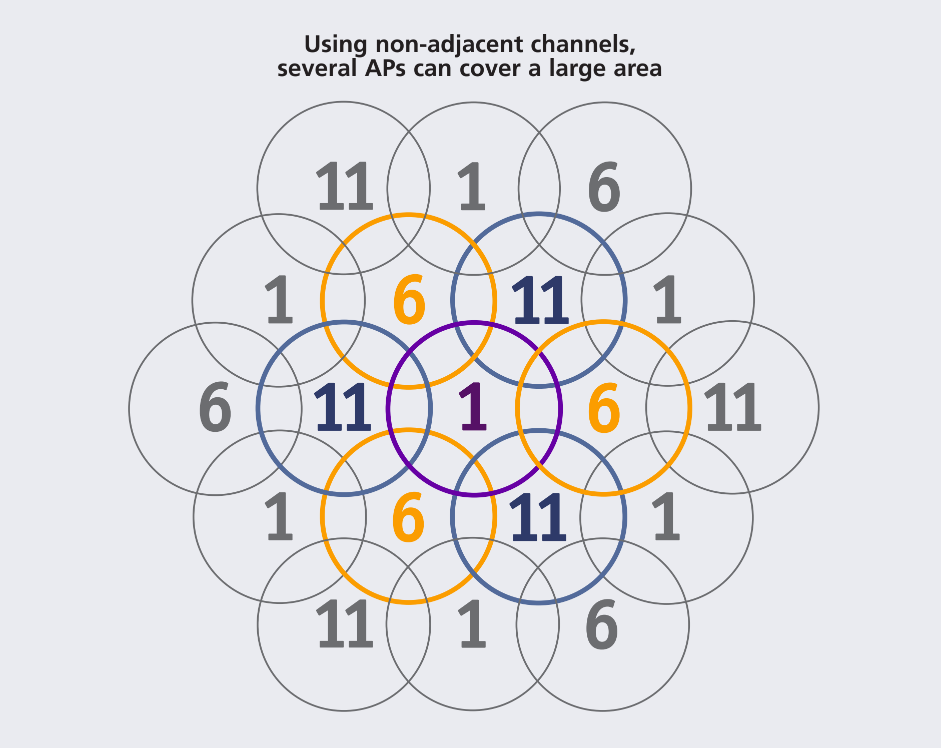
Name: waverunnerlab2
Manufacturer: n/a
IP Address: n/a
Status: 1 of 1 APs scanned

Figure 4: The Fluke Networks' WaveRunner site scan creates a list of any access points found during the initial walk around.

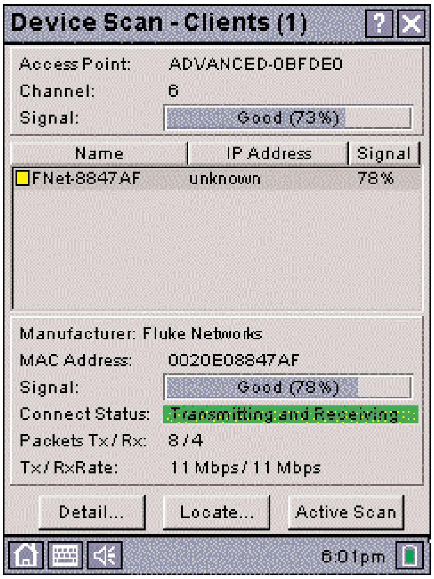
Knowing about the "extra APs" means they won't catch you unaware when your access point for that department starts getting a large number of errors.

Use Fluke Networks' WaveRunner device scan feature to find devices with strong signals that are on the same or adjacent channels. The issue here is to discover whether access points with overlapping coverage areas are broadcasting on the same channel, or on channels that have overlapping frequency ranges. Adjacent access points should be configured for different non-overlapping channels (channels 1, 6, and 11 in the USA). 802.11b is a direct-sequence spread-spectrum technology that uses adjacent channels in the 2.4 GHz frequency range. Lower cost access points have wider RF footprints that may bleed over into adjacent channels. In most default configurations, access points that find too much interference on the originally configured channel will attempt to move to another set of channels. In order to keep access points from spending too much effort avoiding one another, it's important for the network administrator to make sure they're configured on channels that appear to be clear of interference.

If access points can't find free channels, they may be forced to drop the wireless connection speed down to 5, 2 or even 1 Mbps. When you display the list of clients on an access point basis, you can easily see which clients are having problems by


Using non-adjacent channels,
several APs can cover a large area
11 1 6
1 6 11 1
6 11 1 6 11
1 6 11 1
11 1 6

looking at the error data shown by the WaveRunner Traffic and Top Talkers features. The connection speed information remains valuable because the connection speed information provided by most wireless NICs on the Windows task bar is woefully unreliable. Users who complain of poor application performance may simply, upon analysis, be found to be suffering from low AP connection speed.


Device Scan - Clients (1)

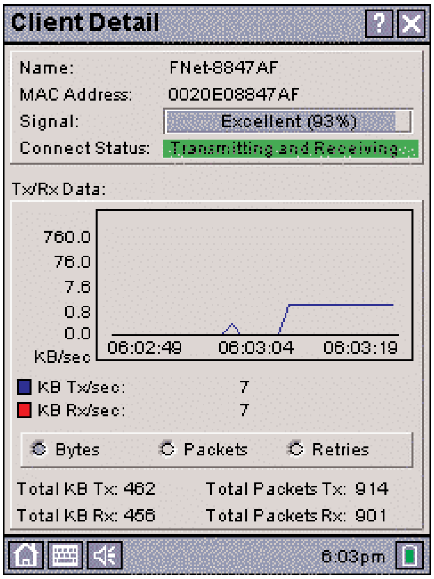
Access Point: ADVANCED-0BFDE0
Channel: 6
Signal: Good (73%)

Name	IP Address	Signal
FNet-8847AF	unknown	78%

Manufacturer: Fluke Networks
MAC Address: 0020E08847AF
Signal: Good (78%)
Connect Status: Transmitting and Receiving
Packets Tx/Rx: 8/4
Tx/RxRate: 11 Mbps/11 Mbps

Figure 5: Device scan from the WaveRunner gives you a quick run down on clients associated with each access point, their signal strength and transmit/receive rate.

A client consistently connecting at 2 Mbps in the corner office, but then having a full speed connection in the conference room, may indicate you need to consider another access point just for the office cluster, or perhaps shift an access point towards it.


Client Detail

Name: FNet-8847AF
MAC Address: 0020E08847AF
Signal: Excellent (93%)
Connect Status: Transmitting and Receiving

Tx/Rx Data:

🟦 KB Tx/sec: 7
🟥 KB Rx/sec: 7

○ Bytes ○ Packets ○ Retries

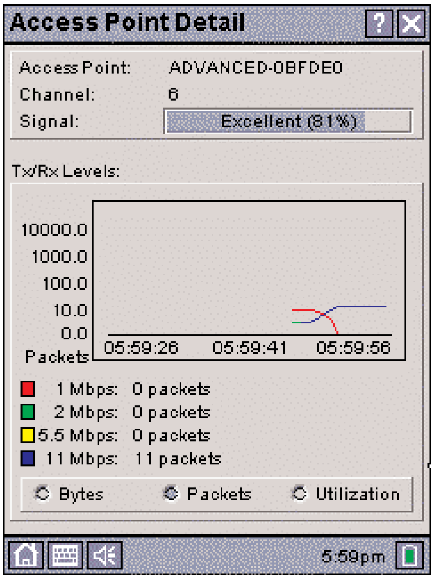
Total KB Tx: 462 Total Packets Tx: 914
Total KB Rx: 456 Total Packets Rx: 901

Figure 6: The client detail screen from the WaveRunner gives you a view of how each client is performing.

Do a walk around

Nothing can substitute for actually being there, and that's especially true for wireless networks. Take a Fluke Networks WaveRunner, and set up an actual access point in a likely location. Since antennas vary widely on different access points, it's a good plan to use an access point you're likely to deploy, rather than the cheapest access point from the discount store. Remember, the intent is to discover what the reception at various locations is likely to be during operation.

Verify you can actually talk to the access point, as seen in the following:


Access Point Detail

Access Point: ADVANCED-0BFDE0
Channel: 6
Signal: Excellent (81%)

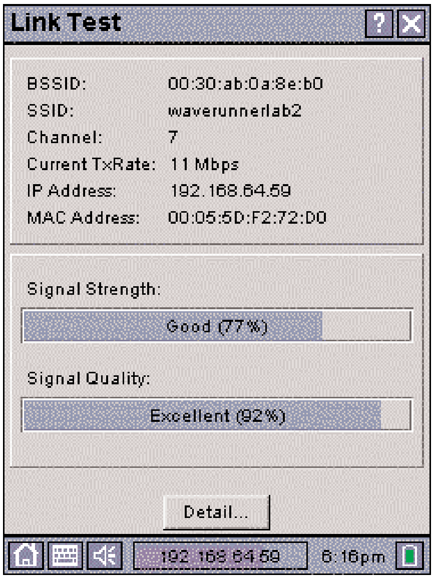
Tx/Rx Levels:

🟥 1 Mbps: 0 packets
🟩 2 Mbps: 0 packets
🟨 5.5 Mbps: 0 packets
🟦 11 Mbps: 11 packets

○ Bytes ○ Packets ○ Utilization

Figure 7: The Access Point Detail screen gives you a good idea of the overall health of the access point in question.

Walk around your facility, measuring signal strength in various locations.


Link Test

BSSID: 00:30:ab:0a:8e:b0
SSID: waverunnerlab2
Channel: 7
Current TxRate: 11 Mbps
IP Address: 192.168.64.59
MAC Address: 00:05:5D:F2:72:D0

Signal Strength: Good (77%)

Signal Quality: Excellent (92%)

Figure 8: Link Test gives you a fast, easy-to-read view of your expected signal strength and quality at any given point as you walk around your facility.

For more detailed information on WaveRunner, including user manuals and instructions on specific tests, go to **www.flukenetworks.com/waverunner**

Here is where a good map of your facility comes in handy. Documentation is the name of the game and on this first go around, you may just want to use pencil to mark up your map. One useful practice is writing a fraction notation in each place where workers might congregate. The top of the fraction is the signal strength and the bottom is the signal quality.

Don't set the installation in stone just yet

As you can see in Figure 9, we've marked the ratios of signal strength to signal quality. As either the strength or quality go down, you may want to consider deploying another access point on a temporary basis, then rerun your site survey. It is also a good idea to make all your AP placements temporary until you've had a chance to have your system under load for a while. Keep in mind the human body is 90% water and as a result, does a pretty good job of absorbing RF signals. While harmless to the humans involved, worker congregation points (water fountains, constrictions in traffic patterns or natural conversation points) have a tendency to create short outages if your signal strength at the location is already marginal. Let the wireless network and user patterns settle awhile before you start putting holes into your walls.

Fine tune

Keep that map around. Companies change and so will your wireless coverage. You may find it necessary to get just a little more distance in two different directions. In this case, perhaps a higher gain antenna or maybe a small shift in the direction the AP is pointed. *(See Figure 9: Each AP has a double headed antenna to indicate the general orientation of each access point.)*

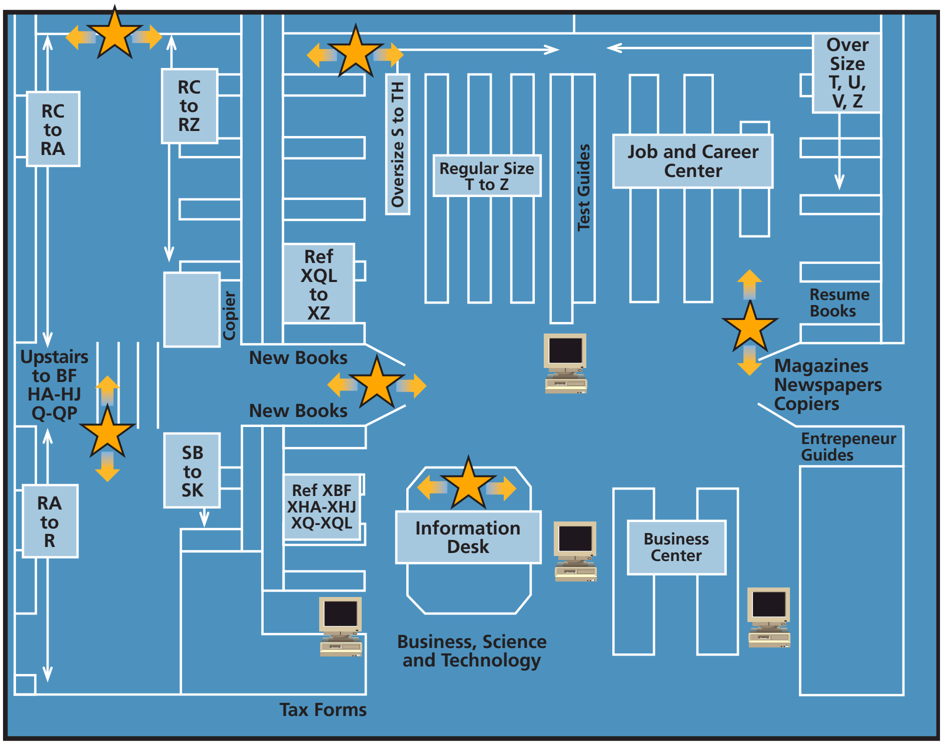


Figure 9: Many office building owners are willing to give tenants an electronic copy of your floor plans. Then using a diagramming application such as Microsoft® Visio, you can quickly and easily document your installation. Even a paper copy with pencil marks can give you a good idea of where your wireless resources will be available.

Test it

Keep a "typical" wireless rig available for testing, and use it to test whether your projections of coverage patterns and signal strength will match deployed reality. Install an access point and run a meeting in the lunchroom if that's where a lot of your users like to work. Go where your users go and do what your users do. Web connections, for example, have the ability to request a retransmission, and so can survive on a poor connection, but a video-on-demand application is immediately going to start looking choppy on even a mildly degraded link. When you know your applications and your in-place coverage patterns, you can begin to make accurate predictions about the performance users should see.

Fine tune again

Due to the "cell phone syndrome," many users are used to small glitches in wireless devices and therefore rarely report the "small stuff." However, small glitches have a bad habit of becoming large glitches if not attended to. Place a recurring appointment in your calendar to just walk around with your survey tool(s) to re-verify your initial numbers.

Document

You have to make the time to document your wireless network. This isn't like a wired network where you can follow the wires. Start off with that survey map shown in Figure 9 and add information like:

- Access point addresses: MAC and IP addresses
- Switch ports that feed your access points
- VLAN IDs if you've decided to separate your wireless traffic
- Information about APs surrounding your facility (APs that belong to other companies/organizations)
- A map of the surrounding area and how far your signal extends from each access point (this is a good excuse for a nice walk)
- A listing of the access point configurations and some sort of change log for those values including firmware and hardware revisions.
- A list of valid wireless card MAC addresses

Perform these steps on a regular basis to keep everything up to date. Remember, things change and it's not just your own approved access points you most consider – someone in accounting or your neighbors may have added something while you were not looking. Knowing the details of your environment is your first step towards keeping users happy with their wireless LAN installation.

Visit **www.flukenetworks.com/wireless** for additional wireless technical information and wireless network analysis solutions.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

©2003 Fluke Corporation. All rights reserved.

Printed in U.S.A. 9/2003 2105559 A-ENG-N Rev A