Chapter 17

Testing a Wireless LAN

This chapter will introduce you to:

- Wireless LAN Testing Considerations
- Signal Coverage Testing
- Performance Testing
- In-Motion Testing
- Security Vulnerability Testing
- Acceptance/Verification Testing
- Simulation Testing
- Prototype Testing
- Pilot Testing
- Test Documentation

Because of the use of radio waves, it is important to fully test a wireless LAN (WLAN) before letting users start using it. Be certain to perform testing after installing a WLAN to ensure that the WLAN system satisfies requirements. In some cases, during operations and maintenance, it might be necessary to perform testing when troubleshooting problems. This chapter covers the types of testing that you should accomplish.

Wireless LAN Testing Considerations

When planning the testing of a WLAN, consider the following forms of testing:

- **Signal coverage testing:** Signal coverage testing determines where client devices are able to satisfy coverage requirements. This testing may be part of performing a WLAN site survey or done after the network is installed to determine the as-installed signal coverage.

- **Performance testing:** Performance testing determines whether the WLAN can satisfy user needs for using specific applications over the WLAN.
- **In-motion testing:** In-motion testing determines whether users can continue to make use of applications while roaming throughout the coverage areas, especially when the roaming requires handoffs between access points.
- **Security vulnerability testing:** Security vulnerability testing ensures that the WLAN implements required security mechanisms and offers sufficient protection to unauthorized access and passive monitoring.
- **Acceptance/verification testing:** After installing a WLAN, it is important to run a series of acceptance/verification tests to ensure that the WLAN satisfies all requirements. This is especially important if the organization is having a contractor install the WLAN.
- **Simulation testing:** In some cases, such as when implementing a very large WLAN, it may be beneficial to simulate the behavior of the WLAN before actually installing it. This can provide helpful feedback when designing the system, especially if the WLAN will have critical performance requirements.
- **Prototype testing:** Prototype testing involves implementing an individual function of the WLAN that is not well understood before deploying the complete system. For example, an organization may not be very familiar with 802.1X authentication systems and may benefit by implementing the 802.1X authentication in a lab environment with a limited number of test client devices.
- **Pilot testing:** Before installing the WLAN across the entire organization, which may include numerous buildings and different applications, it is strongly advisable to install the system in a limited number of facilities (ideally one) and make that one work effectively first. After you work out all the problems, you can install the WLAN at the remaining location without the need for extensive rework because the problems will likely have been solved during the pilot testing.

The remainder of this chapter explains the details of these forms of testing.

Signal Coverage Testing

Signal coverage testing involves using a signal coverage tester (sometimes referred to as a signal meter) to measure WLAN signals throughout the coverage areas. The main objective is to ensure that signal levels are high enough to support the levels of performance that the users need when using applications over the WLAN.

Wireless Site Survey Coverage Testing

Signal coverage testing is often part of performing a wireless site survey and should be done before installing the WLAN. This is done by positioning a test access point at various locations throughout the required coverage area and using a signal meter to measure

signal values in the vicinity of the test access point. The results of this propagation testing provide a basis for making decision on where to install access points. For more details on performing coverage testing during wireless site surveys, see Chapter 15, "Performing Wireless Site Surveys."

Note When performing wireless site survey coverage testing, set the signal-measuring tool to only record signal strength on the channel that the test access point is set to. This eliminates the possibility of the tool missing access point beacons and improves accuracy.

As-Installed Coverage Testing

After installing a WLAN, it is important to perform as-installed signal coverage testing. This ensures that the WLAN is providing signal coverage in all required coverage areas based on the final positioning of access points. As with coverage testing done during a wireless site survey, as-installed coverage testing involves using a signal meter to measure signal values throughout the required coverage areas. As-installed coverage testing, however, does not use a test access point. The actual installed access points that comprise the WLAN generate the signals that the signal meter measures. In addition, instead of only testing specific locations, you walk through the entire facility and measure the signal values. The goal with as-installed coverage testing is to ensure that the signal coverage requirements are fully met by the installed access points.

As with propagation testing done during a site survey, as-installed coverage testing requires you to determine minimum signals levels that constitute acceptable signal coverage. You can then utilize a signal meter to measure the signal values and generate coverage maps based on a minimum threshold. See Chapter 15 for more information about defining acceptable signal values for signal coverage.

It is generally advisable to generate signal coverage maps for the facility where the WLAN is installed. Many of the signal meters specialized for performing site surveys include this feature. You load in floor plans of the facility, and the signal meter indicates where there is acceptable coverage based on the signal values that you have recorded during the testing.

Note When performing as-installed coverage testing, set the signal measuring tool to record signals on all relevant that the installed access points are set to. This ensures that all signals are recorded properly. See Chapter 14, "Test Tools," for details on signal meters.

Consider Beacon Rates

When using survey tools to measure signal strength for generating signal coverage maps, be certain to take into account the 802.11 beacon intervals set in the access points or mesh nodes. The default beacon interval is generally 100 milliseconds, and the default setting for most survey tools is to measure signal strength on each radio frequency (RF) channel for 250 milliseconds (sometimes called the scan time). With these settings, you

are assured of the access points or mesh nodes transmitting a beacon while the survey tool is measuring the signals on a particular channel. In fact, at least two beacons will occur during that time, so the survey tool will not miss any of the beacons.

A possible problem may occur, however, if the beacon interval on the access points or mesh nodes is set to a longer value. For example, Tropos mesh nodes generally have default beacon intervals of 250 milliseconds. They do this to reduce overhead traffic (that is, beacons) on the network. In this case, if your survey tool is set to a scan time of 250 milliseconds or less, then there is a possibility that a beacon will not occur during the 250 milliseconds. In most cases, the scan time is adjustable. To ensure the survey tool you are using is measuring all possible signal data, it is a good idea to be certain that the scan time of the survey tool is greater than the beacon interval.

Citywide Indoor Signal Coverage Testing Considerations

To create a municipal wireless network that enables full public access to the Internet, the network must offer signal coverage inside businesses and homes. At some point, you will need to verify that sufficient signal coverage exists in the percentage (for example, 70 percent) of inside locations. This type of testing is easier said than done.

A major problem is that the majority of indoor areas are not open to the public. As a result, a system integrator completing system testing or the municipality performing acceptance testing does not have ready access to indoor places. Understandably, businesses and homeowners are usually reluctant to let strangers inside their private establishments. Therefore, it might be possible to test only a very small number of indoor areas, those that are accessible to the public, such as restaurants, grocery stores, and so on.

A municipality may be able to boost the number of indoor test locations, however, by soliciting volunteers that allow test teams to enter their private businesses and homes. For example, a municipality may setup a system that automatically calls utility customers, explains the need to perform the testing, and asks the customer to participate in the testing (possibly by having the customer press a specific numbered key on their phone). The municipality could then provide the volunteer list to the test team, which would greatly expand the umber of indoor test locations. This also gets the community involved in the deployment in a positive way, which based on my experiences is always a good thing.

Performance Testing

The WLAN must specific applications defined in the requirements, and to do so, it must be capable of passing a variety of tests.

Association Tests

Make sure that each of the client device types will associate with at least one or more access points that are part of the installed system. This is an initial test to see whether the client devices can establish a wireless connection, which primarily involves the 802.11

protocols and any vendor-specific enhancements. Confirm sufficient associations before moving on with other testing. This is important because sometimes client device radios are not fully compatible with the access points, even though they both comply with 802.11n. If you do not ensure that the client devices have stable associations, other performance tests may indicate erratic and inaccurate results.

Note A problem with using client radio devices from different manufacturers on the same network is that vendor-enhanced features may not be usable. In this case, the functionality of the network may be reduced to the least common denominator, which are the functions specified only by the 802.11 standard. Test the use of these enhanced features, such as network monitoring tools and performance enhancements.

For example, with a wireless IP phone implementation, the phone should have an indicator that confirms that association has been made. Power up the phone and check whether the phone indicates an association. If the phone will not associate with an access point, recheck the phone configuration, especially the service set identifier (SSID), authentication type, and security password. These parameters must match those configured on the access point for association to be successful. Also, ensure that you are operating the phone in an area where signal coverage exists. You can generally do this by observing the signal status on the phone.

When performing an association test, connect the client device to an access point and monitor the connection for at least 10 minutes. In some cases, the client device may initially associate with an access point without any issues, but it might inadvertently disassociate after a few minutes. If problems occur, research similar problems regarding the types of client radios and access points that you are using, and upgrade the firmware if necessary to fix the problem. Sometimes you must upgrade the firmware in the client device radios, access points, or both, for the association process to work effectively.

Registration Tests

After confirming that the client devices associate effectively with access points, the next step is to ensure that each of the client device types register successfully with the network and applicable applications. This involves protocols and processes that operate over the 802.11 protocols.

Network Connection Tests

As a basis for communications between the client devices and the application, most wireless systems implement either TCP or UDP. In either case, ensure that the client device successfully connects to the network and has a valid IP address. This can generally be done by observing the association table found in the access point. It is also a good idea to ensure that the client device is capable of responding to a ping generated from the same subnet where the application resides. The ping result should indicate that the client

device responds to the ping with acceptable delays and not time out. If network connection tests indicate a problem, ensure that the client device has a valid IP address and you might want to upgrade the firmware on the client device, access points, or both.

Authentication Tests

Many WLAN systems implement 802.1X security mechanisms. If this is the case, ensure that the client device is successfully authenticating with the network. You can do so by observing the access point authentication status table or RADIUS server administration.

If you are testing a wireless IP phone application, for example, be sure that each phone properly authenticates with the system. If only Wired Equivalent Privacy (WEP) security is in use, the phone will not authenticate with the access point if the WEP on the phone does not match the WEP key configured in the access point. In this case, the phone will not even associate with the access point. When using Lightweight Extensible Authentication Protocol (LEAP), the phone may associate with the access point but not authenticate with the LEAP authentication server. Therefore, verify that the phone is actually authenticating with the authentication server. To do this, you will probably need to access the authentication logs on the server. If the phone is not authenticating, check that the LEAP username and password entered in the phone are the same as those configured in the authentication server.

Application Connection Tests

Be certain to check whether each type of client device type properly connects to the actual application. With a wireless IP phone implementation, for example, ensure that the phone registers with the call manager software and receives the applicable phone number. If the phone does not register properly, which is usually identified as an indicator on the phone, recheck that the phone is actually configured in the call manager software. If the phone is configured in the call manager, recheck that the phone has the proper IP address, subnet mask, primary gateway, and DNS settings. Keep in mind that the phone may associate with an access point but not be able to obtain an IP address. The IP address should correspond with the address plan for the location where it is connecting to the network.

Application Tests

After you have verified that the client device is successfully connecting to the system, confirm that each type of client device is able to interface with the WLAN with acceptable performance. For example, if you are testing a wireless IP phone system, you are now ready to see whether you can actually place calls. The goal is to determine whether the phone can make a connection with another phone and that voice quality if acceptable. This testing will check to be sure that that the wireless network and supporting wired infrastructure is supporting the phone calls adequately.

Start by placing a call on each phone from a stationary location. Place a call to preferably someone on a wired phone, and talk for at least a minute while assessing voice quality. If you find that the quality is poor, check the signal coverage at that location. For instance,

you should only observe from the phone's location a single access point on a particular nonoverlapping channel (1, 6 or 11) with a signal level that is at least 15 dB higher than other access points set to the same nonoverlapping channel. The presence of more than one access point set to the same RF channel and having similar signal levels may cause significant interference that reduces voice quality. In addition to checking the wireless network, you might recheck the quality of service settings on the call manager software to be sure that it is set properly.

Note In mixed mode implementations, ensure that 802.11n devices are in deed operating at 802.11n rates by checking client association tables.

Load Tests

As final step when testing the performance of the WLAN, ensure that multiple users can use applications on the network. The goal here is to verify that the WLAN can continue to satisfy all requirements while a typical (and maximum) number of users are using the system. The best way to test load on the network is with actual users and client devices. In some cases, however, you may need to resort to simulation as explained later in this chapter.

For example, with a wireless IP phone system, make use of multiple wireless IP phones throughout the facility. Ideally, distribute and use the phones in a similar manner as they will actually be used when operational. Find volunteers or actual users to help you with these tests. You can give them each a phone, instruct them on how to use it, and have them initiate calls with others. To simplify testing, you can start by having the group of callers place calls from the same location, and then have them separate uniformly throughout the facility while continuing voice conversations and monitoring voice quality. If requirements in parts of the facility specify a need for higher capacity, have an appropriate number of test users make use of the phones from that area. Again, strive to test the system as users will use it.

While performing the load tests, monitor the system using network analyzers or system management tools, if available. Also, be sure to receive feedback from the users actually using the devices, and identify any related issues. If problems arise, note the applicable time and location in the facility where the problem occurred. Doing so makes it easier when looking through the results of the monitoring tools to identify the underlying problems.

Note Consider using load test tools, such as PureLoad, to simulate multiple user connections to the wireless network.

In-Motion Testing

Once stationary usage of the applications is working satisfactorily, run tests to verify that users moving throughout the coverage areas are able to continue operating the applications successfully. When testing, be certain to move about the coverage area at typical and maximum speeds that users will operate the applications. This is necessary because roaming tends to break down at higher speeds. Also, run a wireless packet sniffer to record packet transmissions between the client device and the network. This will help you better understand the underlying issues if you run into problems. For example, you might see significant delays when the system is reestablishing the flow of packets when the client device radio hands off from one access point to another. By looking at the packet trace, you may also see that a client device is experiencing significant retransmissions with a particular access point before handing off to another access point with better signal quality, which would point to issues with the client radio's ability to roam.

For wireless IP applications, place a call and walk through the facility while talking to someone on a wired phone. As you walk, monitor the voice quality. If everything is working okay, you should hear consistent quality as you traverse the facility and the phone roams from one access point to another. If you detect poor sound quality at any point, check the signal strength indicator on the phone. A reduction of sound quality may occur when the signal strength is low. To make roaming phone call tests easier to perform, wear an earpiece for listening to the voice quality and monitoring the signal strength indicator on the phone at the same time.

When performing the roaming tests, ensure that the phone can "see" at least two access points (each on nonoverlapping channels) from anywhere within the covered area. This can often be done by observing the phone's wireless connection utility. If two or more access points cannot be seen on nonoverlapping channels, a phone roaming from one access point to another may not be smooth enough to maintain good voice quality. To make voice quality consistent, you might need to reengineer the wireless network by moving access points or adding additional access point.

If the phone is connected to a particular access point and does not roam even if located directly under another access point, there may be more than one access point having relatively high signal strengths on overlapping RF channels. In this case, you may be able to fix the problem by adjusting the transmit power of one of the access points. Or, you might need to reengineer the WLAN. Another reason that the phone may not be roaming in this scenario is that the nearby access point is not operating. So, check the status of the access point.

Another problem with roaming is that the phone may roam from one access point to the other too slowly. In this case, check the phone wireless utility to ensure that there is indeed another acceptable access point to roam to. The problem could be that there are no other access points having strong enough signal strength for the phone to roam. If the phone appears to roaming promptly to the next access point, there might still be excessive delay problems on the wired network infrastructure.

Sometimes the phone may roam okay with regard to the network, but the phone loses connection with the call manager. In this case, check to be certain that the phone is not traversing different IP subnets, which can cause a Layer 3 connection loss and disconnection from the call manager. In addition, if using Cisco LEAP, make certain that some of the access points are not blocking TCP ports associated with the LEAP protocol.

Note If you find that moving throughout the facility causes the client device to drop connections or act erratically (and the wireless network is installed optimally), the wired infrastructure may not provide acceptable roaming delays. For example, the Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, and 2948G-GE-TX switches are known to introduce substantial roaming delays. Cisco does not recommend using these switches in a wireless voice network. Also, if a Cisco Catalyst 4000 series switch is used as the main Layer 3 switch in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The SUP1 or SUP2 module can cause roaming delays.

Security Vulnerability Testing

It is important to run a series of tests to verify the security of the wireless network. This is necessary to ensure that the network satisfies all security requirements. If possible, employ someone (an "ethical hacker") who has knowledge and experience regarding wireless security and hacking methods. In addition to verifying proper configuration of devices on the network, you should attempt to break into to the system.

Security Settings Verification

Start by reviewing the security configuration settings in client radios, controllers, and access points. This includes confirming that encryption and authentication functions are configured correctly in relation to design specifications. For example, if design specifications indicate use of Advanced Encryption Standard (AES) encryption, ensure that the access points are configured to require AES encryption. Do not assume that the WLAN has the proper configuration, be certain to look at the configuration of the actual equipment.

Once you are sure that the network's security settings are correct, determine whether authorized client devices can successfully connect to the network using the applicable security mechanisms, such as AES encryption and 802.1X authentication. In addition to ensuring that it is possible to connect, verify that the actual security mechanism is in use. You can do so by running a wireless packet sniffer, which will identify the applicable security mechanism that correspond to the client device being tested.

Penetration Testing

The ability of authorized client devices being able to connect to the network is only part of security testing. You also need to verify that unauthorized client devices cannot connect to the private side of the network or reach the protected network from the public side of the network.

Private-Side Testing

A good place to start with penetration testing is to attempt to connect unauthorized devices to the private side of the network, which should be configured with encryption and authentication mechanisms that only allows authorized client devices to successfully connect. Assume that you know the SSID of the private network because that can be easily found by monitoring 802.11 association requests from client device radios. Configure an unauthorized client device with this SSID and verify that you cannot connect to the network. Of course if it is possible to connect to the private side of the network without applicable encryption passwords, there are major problems with the security of the network. In this case, review the security settings on the access point.

Public-Side Testing

Of course some networks, such as public hotspots may not have any security mechanisms and encourage open connections, but the network may also include a private network as well. In this case, run tests to verify that client devices connecting to the public side of the network cannot access any sensitive resources.

As part of analyzing the security vulnerabilities of a wireless network, run a TCP port scanner, such as SuperScan or Retina, to find open TCP or UDP ports that may offer security holes. SuperScan runs on a Windows laptop and scans all ports via the wireless network. Most of the time, SuperScan returns information (for example, IP address) about open port 80 (HTTP) interfaces on access points and printers, but it also finds other open ports made available by the installation of various applications.

Note You can download a SuperScan, a free port scanner, from http://www.foundstone.com/us/resources/proddesc/superscan.htm.

Of course, you can place the found IP address of the node, such as a printer, in your web browser and reach the configuration screen for the associated device or application. Because most users do not implement an admin username and password on printers, for example, hackers could (on some printers) configure the printer to send all printed data to a capture file on their laptop, which of course is not good. Be sure that there are no ports available that will make the network vulnerable to a hacker. If open ports are found, consider redesigning the security of the network.

When running penetration tests, use a port scanner with a test computer, which should be the same as the target client device, connected to the network at various locations, as follows:

- **Scan test computer from within the same subnet:** This test determines the extent to which a public wireless user can access user devices that are in the same subnet as another user. This scenario is common with public hotspots, where the hacker is connecting to the network from the same area as a targeted user (for example, from the same coffee shop). With the port scanner connected to the same subnet as the test computer, initiate a scan of all applicable TCP/UDP ports of the IP address of the test computer.
- **Scan test computer from a different subnet:** This test determines the extent to which a public wireless user can access user devices that are in a different subnet. This scenario is common with public hotspots, where the hacker is connecting to the network from a different area than a targeted user (for example, from different parts of an airport). With the port scanner connected to a different subnet as the test computer, initiate a scan of all applicable TCP/UDP ports of the IP address of the test computer.
- **Scan test laptop located on a private subnet from a public subnet:** This test determines the extent to which a public wireless user located on a public subnet can access devices that are on a private subnet. This scenario is applicable where a hacker is trying to compromise the security of users connecting to the protected side of the network. With the port scanner connected to the public subnet and the test computer connected to the private network, initiate a scan of all applicable TCP/UDP ports of the IP address of the test computer.

In addition to scanning a test computer, perform a scan of all devices that connect to the network, such as access points, controllers, switches, and application servers. In addition to wireless components, be certain to include devices that are not part of the wireless network, such as printers. If scanning all ports, you will probably need to limit the number of devices (by IP address) or the scanned ports to a limited set. Otherwise, the scans may run for days. Be sure to hit the more vulnerable ports, such as port 80. Before running the tests, talk to your local network security manager to decide which ports are most important to scan.

Acceptance/Verification Testing

In cases where an organization hires a contractor to implement the WLAN, it is important for the organization to conduct acceptance/verification testing to ensure that all technical system requirements are met and that the overall system is functioning effectively. The tests verify that the overall system has adequate signal coverage, performance, capacity, and security, and that management systems are in place and operating properly. Therefore, acceptance/verification testing includes the testing explained previously in this

chapter, but it is a formalized process. In fact, it is a good idea to make acceptance/verification testing part of the contract with a system integrator and possibly stipulating successful completion of acceptance/verification testing as a requirement for part of the payment for the system.

The following are benefits of acceptance testing:

- Determines whether the system is fully operational prior to being given operational status, which avoids potential issues with usage and support
- For potential legal purposes, provides expert technical evidence of system elements that do not meet contracted requirements
- Provides a form of insurance to services providers that the system will support intended applications prior to them investing in the deployment of applications

In addition to the testing covered earlier in this chapter, acceptance/verification testing should address the following elements:

- **Installation practices:** Tour the facility and ensure that access points are installed properly, antennas are aligned correctly, and cabling is neat and organized. For more information about installation best practices, see Chapter 16, "Installing and Configuring a Wireless LAN."
- **System documentation:** Review all documentation, such as system design specifications, as-installed signal coverage maps, cabling diagrams, and operational support plans. The various chapters throughout this book explain what this documentation should include.
- **Operations and maintenance:** Look over operations and maintenance procedures and make sure that all applicable staff has proper training. Test the reaction time of the support staff by triggering a failure event, such as disabling one or more access points. This should be done without any notice to the support staff. Observe how long it takes the support staff to fix the problem and verify that this falls within required times.

Simulation Testing

Simulation uses software models that artificially represent the network's hardware, software, traffic flows, and use. You can run simulations that replay or generate various types of traffic or protocol streams to validate results quickly; days of network activity go by in minutes when simulating traffic using such tools. Currently available simulation tools can assist a designer in developing a simulation model. Most simulation tools represent the network using a combination of processing elements, transfer devices, and storage devices. Simulation tools are generally costly, with prices in the tens of thousands of dollars. You might be better off hiring a company that already owns a simulation tool.

The main attributes of using simulation to verify the technologies are the following:

- Results are only as accurate as the model; in many cases, you will need to estimate traffic flows and utilization.
- After building the initial model, you can easily make changes and rerun tests.
- Simulation does not require access to network hardware and software.
- It does not require much geographical space, just the space for the hardware running the simulation software.
- Simulation software is fairly expensive, making simulation not economically feasible for most one-time designs.
- The people working with the simulation program will probably need training.

Consider using simulation for the following situations:

- When developing a type of WLAN product that does not yet exist
- When it is not feasible or possible to obtain applicable WLAN hardware and associated software for testing purposes
- When testing performance requirements based on predicted user activity (because it is often not practical to do this with physical prototyping)
- When it is cost-effective to maintain a baseline model of a product or system to test changes to the baseline

Prototype Testing

A physical prototype is a part of the product or system you want to verify through construction and testing. It consists of the actual hardware and software you may eventually deploy. Prototyping generally takes place in a laboratory or testbed.

The main attributes of physical prototyping are as follows:

- Yields accurate (real) results because you are using the actual hardware and software, assuming you can include applicable user utilization loads
- Relatively inexpensive as part of a system installation because you can obtain components under evaluation from vendors
- Takes time to reconfigure the prototype to reflect changes in requirements
- Requires access to network components, which can be a problem if you do not have easy access to vendors
- Requires space to lay out the hardware and perform the testing

Consider using physical prototyping for the following situations:

- When initially testing the design of a new WLAN product before going into mass production
- When testing the system design of a WLAN solution before vendor selection, especially when the operating environment may have a high degree of signal impairment (such as multipath distortion and RF interference)

Typically, you do not need to physically prototype the entire system, especially those parts that other companies have implemented without encountering problems. Consider prototyping any solutions that have not been tested before, especially those elements dealing with performance and range.

Pilot Testing

Pilot testing involves installing a real version of the WLAN system that users actually operate. This testing enables the evaluation of realistic use and long-term performance issues. The results of this testing will also provide a blueprint for the installation of WLANs in other common facilities.

The main attributes of pilot testing are as follows:

- Yields the most accurate (real) results because you are using the actual hardware and software under realistic conditions.
- Involves the purchase of applicable hardware and software
- Depends on relatively firm requirements to minimize costly changes to the installed system
- Requires a live facility to install and use the system

Consider using pilot testing for the following situations:

- When testing the design of a new product before going into mass production
- When testing the system design of a WLAN solution before installing the system

The implementation of a WLAN pilot test generally involves the installation of multiple access points to cover a significant portion of the overall intended coverage area. Before installing the pilot system, perform a wireless site survey to determine the number and location of access points (see Chapter 15). This data will provide a warning of issues that you might need to consider before installing WLANs at other facilities.

Test Documentation

At the conclusion of testing, produce a test report that addresses the following elements:

- **Background:** Explain what is being tested and why the testing is being done.
- **Test team:** Identify all people who were involved with the testing and their roles.
- **Requirements summary:** Briefly describe the WLAN requirements and reference the requirements document for more details.
- **Test methods and tools:** Describe how the testing was accomplished and the tools that were used to collect the data.
- **Test results and analysis:** Include all applicable test data. Many test tools put data in a format that you can include in your test report. If this is too cumbersome for inclusion directly within the test report, reference applicable test files. Also, explain the results, including any underlying issues that might be causing problems.
- **Recommendations:** Explain what changes should be made to the network to counteract issues found during testing.

Test documentation becomes a vital part of a WLAN. Managers and support staff can refer back to test reports in the future to better understand why changes were made to the network and what might be useful to fix future problems. As a result, be certain to fully document any testing that you do.

Summary

Sooner or later, you will likely be involved with testing a WLAN. It is needed for testing signal coverage when performing a wireless site survey and after installing the access points (as-installed coverage testing). Performance testing is also important to complete. This includes a series of testing, which includes association tests, registration tests, application tests, and load tests. Performance testing should be done from stationary locations and while users are in motion and roaming throughout the facility (if applicable). To verify security of the network, perform a series of security tests, which includes security settings verification and thorough penetration testing. For many deployments, especially when an organization has hired a contractor to install the system, you should complete more formal acceptance/verification testing. At the conclusion of any testing, always produce a test report that fully documents the testing, such as what was tested, why the testing was performed, and results and recommendations.