



Enterprise Wireless Mobility RF Troubleshooting

by Ken Chipps

Introduction

[Sources of Problems](#)

Interference-Related Problems

[Common Manifestations of Interference](#)

[*Narrowband Interference*](#)

[*All Band Interference*](#)

[*Adjacent Channel Interference*](#)

[*Co-channel Interference*](#)

[*Multipath Interference*](#)

[*Association/Disassociation/Reassociation*](#)

[*Desensitization*](#)

[*Electrical Power Interference*](#)

[*Ethernet Interference*](#)

[900 MHz Interference](#)

[2.4 GHz Interference](#)

[5 GHz Interference](#)

[Detecting Interference](#)

[Water](#)

[*VSWR*](#)

[Isolating the Problem Domain](#)

Technology-Related Problems

[Configuration Problems](#)

[Connectors](#)

[Cable](#)

[Polarization](#)

[Antenna Types](#)

[Distance](#)

[Line of Sight](#)

[Fresnel Zone](#)

[Earth Bulge](#)

[Antenna Alignment](#)

[Hidden Node](#)

[Near/Far](#)

[Low Throughput](#)

[Fragmentation](#)

[Sensitivity](#)

[Harmonics](#)

[Intermodulation Products](#)

[Cisco Specific Problems](#)

[Tools](#)

[Coax Tester](#)

[Spectrum Analyzer](#)

[Network Analyzer](#)

[Hotspots](#)

[Conclusion](#)

Introduction

This tutorial covers the last two subjects in the wireless section of the CCIE test outline: RF troubleshooting and hotspots (PWLANS, as Cisco calls them).

As with most of the material on wireless that Cisco lists as sources of test questions for the CCIE test, currently, there is little on the Cisco web site on these subjects. For example, a search for "RF troubleshooting" turns up eight hits. None of these are specific to troubleshooting problems related to radio frequency. Two of the eight are just announcements of the topic being on the test. Searching again in the Technical Support & Documentation section, using only "RF" and "troubleshooting" as the keywords, turns up 1,090 hits. Only one of these has RF troubleshooting in the article title. Most of the information on this subject that Cisco provides is in the various product installation and troubleshooting guides.

To remedy this problem, this tutorial addresses the topic of RF troubleshooting in two main sections. First is a discussion of the nature of the radio frequency environment and the sources of the problems inherent in this type of environment. After that, technology specific issues are covered.

Sources of Problems

There are many sources for the problems seen in wireless networks. They are all due to two reasons. First is the unbounded nature of a wireless network, which makes it subject to interference in all its forms. The second is the nature of the technology itself. The standards on which the current technology is based produce several interesting problems.

Interference-Related Problems

Common Manifestations of Interference

Interference is seen as noise. When you measure the signal and the noise to determine the signal-to-noise

ratio, everything the radio cannot decipher is considered noise. Keep in mind that much of this noise is actually someone other signal, just as your signal is noise to another wireless network. The way to think of the signal-to-noise ratio is to envision that you are standing in a swimming pool. The water is the noise. It is your job to keep the radio, your head, as far above the water as possible. The gap between your head and the top of the water is the signal-to-noise ratio.

Noise is made up of many things. Some is naturally occurring, some is human created, and the rest is someone else's signals. To make life easier in the unlicensed world, keep your signal as contained as possible so that it will not become noise to someone else. Cooperation is the key to effective use of the unlicensed frequencies. Wireless networks see the following types of interference:

- Narrowband
- All band
- Adjacent channel
- Co-channel
- Multipath
- Disassociation
- Desensitization
- Electrical Power
- Ethernet

Narrowband Interference

Narrowband interference is basically another signal at a single or narrow range of frequencies. It blocks out part of the spread spectrum signal. An advantage to spread spectrum technology is its ability to work around limited narrowband interference. To see narrowband interference, use a spectrum analyzer as discussed below. To get rid of the narrowband interference:

- Shield it
- Turn it off
- Change channels on the wireless network equipment

All Band Interference

All band interference is from one end of the band to the other. A microwave oven is an example of this type of interference. In the 5 GHz range, high-power radar units used around airports and military installations will wipe out any other use of this range. All band interference is seen on a spectrum analyzer as discussed below. About the only solution to all band interference other than getting rid of the source is to change bands, such as from the 2.4 GHz 802.11b to the 5 GHz 802.11a.

Adjacent Channel Interference

Adjacent channel interference is produced by co-locating access points where the channels overlap somewhat. Recall that the only useable channels in 802.11b are 1, 6, and 11. To see this, use a program like NetStumbler. This program is discussed in [the "Enterprise Wireless Mobility" Study Guide](#) at CertificationZone. To prevent adjacent channel interference:

- Do not use channels that overlap
- Move the access points far enough apart that the cells do not overlap
- Turn the power down to reduce the cell size

Co-channel Interference

With co-channel interference, there is direct overlap of the channels. An example might be two different organizations using the same channels where one is on floor 1 and the other on floor 2 or in an adjacent office. To detect this, a tool like NetStumbler is required.

To prevent this:

- Do not use channels that overlap
- Move the access points far enough apart that the cells do not overlap or turn the power down to achieve the same effect
- Change the orientation of the antennas, with one network using horizontal polarization and the other vertical polarization

Multipath Interference

Another type of interference is multipath. When a radio frequency wave leaves an antenna and encounters objects off which it is reflected, this creates multiple wave fronts, one for each reflection point. Some of these waves go off in space, but others reach the receiving antenna along with the original wave front. Since the reflected waves cover the distance from the transmitter to the receiver over a different time interval than the original wave, there is a delay between the original wave front arrival and the reflected wave's arrival. The time between the arrival of the original wave and the last reflected wave is the delay spread. The value for delay spread will vary. For an 802.11b or g network, the delay spread is less than 50 nanoseconds (ns) for a typical home, 100 ns for office environments, and 200 to 300 ns for a manufacturing floor. Multipath causes several problems:

- Decreased signal amplitude or downfade
- Corruption
- Nulling
- Increased signal amplitude or upfade

With decreased signal amplitude, the reflected waves are added to the original wave. If the reflected waves are out of phase with the original wave, then a decrease in amplitude is seen. If a reflected signal is even more out of phase, then the reduction may be so great that the received signal cannot be read at all or only partially due to corruption. This is seen in a low signal-to-noise ratio. In nulling, the phase of the

reflected signal entirely cancels the original signal. When a reflected signal is in phase with the original signal, the total signal may be larger in amplitude. This causes higher signal strength than would normally be expected at the antenna, but still lower than the transmitted signal strength. Detecting multipath interference is difficult. Multipath cannot be measured directly; only its effects can be seen and from this multipath deduced. For example, if a link budget calculation is performed but the signal as measured is less, then multipath can be a reason. Holes, areas of no signal, detected when doing a site survey may be caused by multipath. Solutions for multipath interference include:

- Moving objects that reflect the signal
- Moving the antennas so as to avoid the multipath path
- Antenna diversity

Antenna diversity is the use of multiple antennas, inputs, or receivers. There are several types of antenna diversity that are commonly used. First is non-active diversity, which uses multiple antennas and a single receiver input. This is common in LANs. Active diversity utilizes multiple antennas and multiple inputs to a single receiver. It reads the signal from one antenna at a time. Switching diversity uses multiple antennas and multiple receivers. It switches receivers based on the signal strength at each antenna. Transmission diversity transmits out the last antenna used for reception. It can alternate antennas for retransmissions.

Association/Disassociation/Reassociation

If a client associates, then disassociates, then reassociates over and over, this may be due to a nearby strong foreign signal. Use the spectrum analyzer to look for a signal in the range of the channel being used or change channels to check on this. To solve this, change channels or move the device that is generating the strong signal.

Desensitization

Desensitization occurs when a nearby high-power transmitter overwhelms your receiver. This signal comes from a licensed radio operating as designed. It is just generating so much power that your receiver cannot deal with it. This legal signal overpowers the rejection capability of the front-end RF filter. When this high power signal comes into the receiver, the automatic gain control of the receiver reduces its amplification. This means the gain required for proper signal-to-noise processing is reduced to a level where the desired signal cannot be read. The only solution to this is to abandon the location as the licensed radio has the right of way. An unlicensed radio should not generate enough power to cause this. If it does, suspect that the other network is operating illegally. In that case, the FCC or other regulatory body can be called in.

Electrical Power Interference

Electromagnetic interference can be generated by poor quality electrical power delivered to the radio. To prevent this, supply conditioned power. This can be done by plugging the radio into a UPS or, even better, using a proper electrical circuit for the radios. A proper electrical circuit for computer equipment is a dedicated circuit with an isolated ground. This type of circuit is designated by an orange outlet with a small green triangle.

Ethernet Interference

It has been reported on a wireless newsgroup, although I have never seen it, that wireless equipment that connects back to the site using 100 Mbps Ethernet can cause interference on channels 4, 5, and 7 of an 802.11b network. The solution is to back the speed down to 10 Mbps. This may or may not be a real problem. You might want to try it if nothing else works.

900 MHz Interference

Most equipment used for wireless LANs and CANs operates in either the 2.4 or 5 GHz ranges. For metropolitan area networks (MAN) that operate in areas of dense foliage, 900 MHz is sometimes used. The unlicensed 900 MHz range is from 902 to 928 MHz. This may also be a solution for CAN links that do not have a clear line of sight. 900 MHz systems experience their own peculiar types of interference.

Common sources of interference in the 900 MHz band include:

- Older cordless telephones
- Paging systems at 929 to 932 MHz that bleed over
- Analog cellular phone systems stop at 896 MHz, but have been known to cause crosstalk all the way up to 914 MHz
- FEMA and ESMR high-powered emergency service and dispatch equipment that can bleed as high as 904 MHz
- SCADA used for telemetry and equipment monitoring uses this range
- The 940 to 960 MHz part of the 900 MHz range is licensed. High power licensed links in this range can be a problem.
- 900 MHz near a TV antenna can cause interference on the television channels around 5 and 6

2.4 GHz Interference

Common sources of interference in the 2.4 GHz band include:

- Bluetooth devices
- New cordless telephones
- Amateur radio operations
- Lights that use 2.4 GHz signals to excite the gas in the tube
- Satellite radio services that use 2.3 and 2.4 GHz
- Cellular phone sites, which do not use the unlicensed frequencies for cell phone service, but they do use them for backhaul from site to site
- Medical devices
- Elevator motors
- Television station transmission from remote vehicles back to the studio

Bluetooth is widely discussed as a cause of interference for 2.4 GHz systems. Supposedly, the new version of Bluetooth, 1.2, does not do this. Reports in the trade press suggest a 15 percent throughput loss when older Bluetooth equipment is in operation near a wireless 802.11b/g LAN. Unlike the DSSS signal used by 802.11 systems, Bluetooth uses frequency hopping. It hops from frequency to frequency using the entire 2.4 GHz unlicensed range. This hopping pattern is 1,600 hops per second.

5 GHz Interference

Some interference sources that affect the 5 GHz range are the same as for the 2.4 band such as:

- The newest cordless telephones
- Amateur radio operations from 5.650 to 5.925 GHz
- Cellular phone sites, which do not use the unlicensed frequencies for cell phone service, but they do use them for backhaul from site to site
- Television station transmission from remote vehicles back to the studio

Others are peculiar to 5 GHz.

Radar and navigation aids are interference sources peculiar to 5 GHz signals. These are not an issue unless the link is near a military installation, airport, or some areas of the coast. The frequencies used by these devices include:

- 4.990-5.000 meteorology and radio astronomy
- 5.250-5.650 radar
- 5.460-5.470 radio navigation
- 5.470-5.650 maritime radio navigation
- 5.600-5.650 meteorological radar

Older analog cordless phones pretty much wipe out any other use of the channel they are operating on. The solution is to get rid of the phones, change the phones to another frequency, or change the wireless LAN to another channel. The newer digital phones use the same spread spectrum technology as wireless LANs. They are still a problem, but less so. Reported throughput loss is around 10 percent for these.

Detecting Interference

In 802.11-based networks, interference will show up as increased fragmentation, decreased transmission rates, and increased retransmission. These can be seen using a network analyzer such as Sniffer Wireless by Network General or AiroPeek NX by Wild Packets.

Water

In addition to the interference caused by airborne radio waves, outdoor radio equipment is subject to damage from water infiltration. Water is always bad for a wireless connection. In general there is no way to remove all the water from a part, so just replace it. This type of problem typically occurs in connections,

where the water works through the waterproofing. Coax cable, as discussed below, commonly has a foam dielectric. This acts like a sponge to absorb and wick the water along the cable. Just cutting off the connector and reterminating the cable may not work, as you will not know how far down the cable the water has gone.

One way to check for water is to measure the Voltage Standing Wave Ratio (VSWR). This test is done with a device designed for this purpose. The Anritsu Site Master line of products is commonly used. As Anritsu says, "Covering the 625 MHz to 2500 MHz frequency band, the Site Master S251C site management tool is designed to accurately locate and identify cable and antenna system faults and conduct isolation and gain measurements. This model is ideally suited for users working in cellular, PCS/GSM and ISM applications. Measurement capability includes return loss, VSWR, cable loss and distance-to-Fault (DTF) analysis." The only problem with this marvelous tool is the cost, which is around \$10,000 to \$15,000. One can be rented for about \$600 per month. Another tool that can do this at a lower cost is a power meter such as the Praxsym PM-2458. This tool can measure the line loss in a coax cable, test connector termination, and verify antenna operation. A VSWR of 1.2:1 is desired with the cable between the test unit and the antenna and 1.5:1 when the test unit is next to the antenna.

VSWR

What exactly is VSWR? It occurs when there is an impedance (the resistance to current flow) mismatch between devices. A mismatch occurs when one piece of equipment has different impedance from the device it is connected to. The VSWR is produced when the RF signal is reflected at that junction where the impedance mismatch occurs. The result is return loss. Return loss is the forward energy that is reflected back toward the source. Too much VSWR causes a decrease in the signal that arrives at the antenna for transmission. This decrease may be constant or variable. If too much power is reflected back to the transmitter, it can damage the transmitter. In reference to the discussion of water just above, water in a connector changes the impedance of the part the water infiltrates.

Isolating the Problem Domain

It is always difficult to know where to begin looking for the source of a problem with a wireless connection. In general, loss at both ends of the link, symmetrical signal loss, is due to antenna, connector, or cable problems. The received signal level will drop at both ends of the connection. This requires you to examine both ends of the connection.

Asymmetrical signal loss is due to local interference or improper configuration of one of the radios. Look first at the end where the signal is weakest.

Technology-Related Problems

Configuration Problems

In a radio-based system such as a wireless LAN, both radios must be configured to talk to each other. Types of configuration problems include:

- SSID
- Frequency
- Data Rate
- Root Bridge

Both units in a wireless LAN must use the same Service Set Identifier (SSID). Cisco bridge units must also use the same SSID. Most other vendors use the MAC address of the other end of the bridge link. Both units must use the same channel or frequency to communicate. In the case of a bridge link, both radios must transmit data at the same rate for communication to take place. Bridges do not typically use adaptive data rates as do wireless LANs. For Cisco radios, one end of a point-to-point bridge link must be set to root bridge mode, but only one end. It does not matter which end is so set. A root bridge cannot talk to another root bridge.

Connectors

The connectors and cables used for CAN links are not at all like those used in LANs. Besides the correct connector type, the cable itself must be the correct type. In the case of coax cable there are many different types all with different characteristics. Cables are used to connect the antenna to the radio when they cannot be collocated. This is seen sometimes in wireless LANs and often in wireless CANs. Cisco also uses a coax cable to provide electrical power to some of the bridge units.

In general, Cisco radios use either the RP-TNC connector, which is a reverse polarity TNC or an N connector for the antenna connection, when the antenna is not internal. The RP-TNC looks like this.



[IE-RFT-WP1-01]

Figure 1. Reverse Polarity TNC Jack

Photo Courtesy of Amphenol



[IE-RFT-WP1-02]

Figure 2. Reverse Polarity TNC Plug

Photo Courtesy of Amphenol

If not, the RP-TNC then the radio uses the N connector for the antenna connection. The N connector looks like this.



[IE-RFT-WP1-03]

Figure 3. N Jack

Photo Courtesy of Amphenol



[IE-RFT-WP1-04]

Figure 4. N Plug

Photo Courtesy of Amphenol

The F connector is used on the coax power cables.



[IE-RFT-WP1-05]

Figure 5. F Connector on a cable

Photo Courtesy of Amphenol

Cable

The type of cable used is coax, such as this.

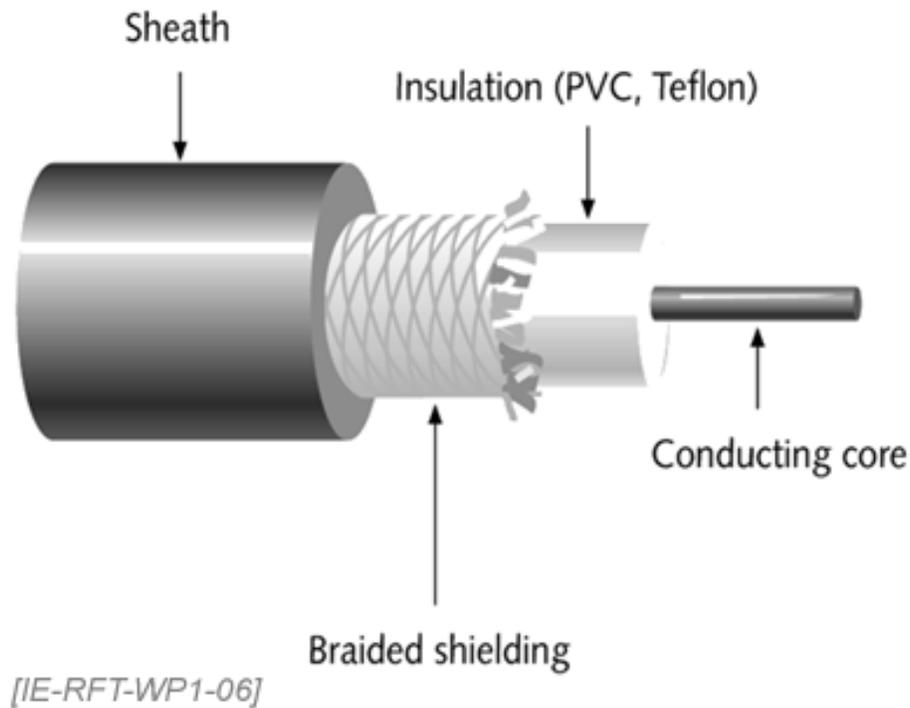


Figure 6.

Cisco says this type of coax cable is RG-213 with 50-ohm impedance. Be sure all components are rated the same impedance.

Cable runs from the radio to the antenna must be kept as short as possible. Signal loss in cable is high. Even the expensive low-loss cables lose significant signal strength for every foot of cable run. Here are the values quoted by Cisco for their standard cables.

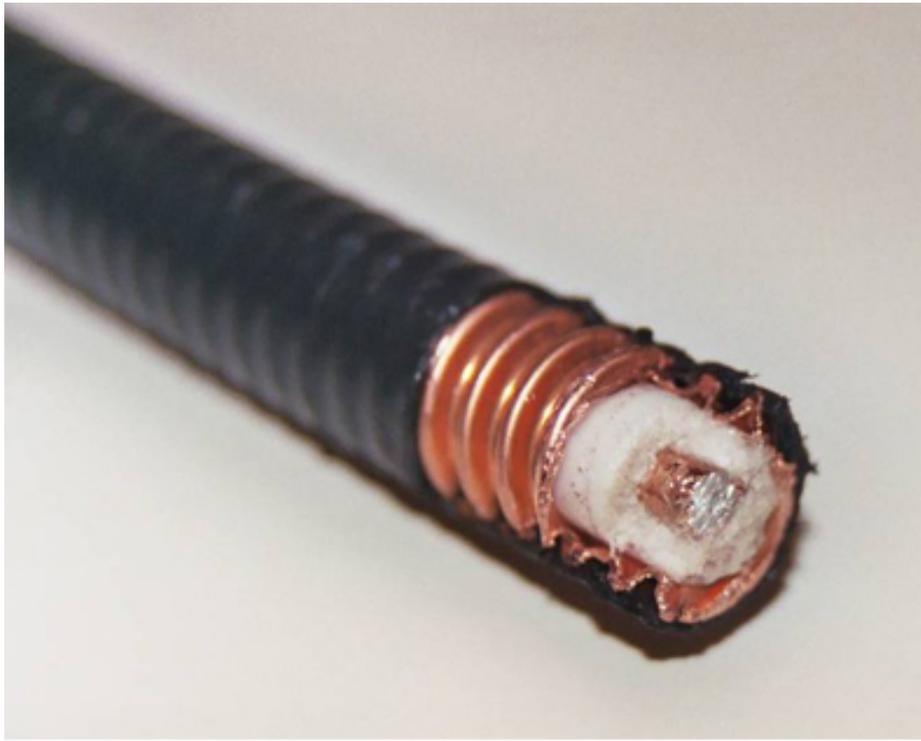
	AIR-CAB020LL-R	AIR-CAB050LL-R	AIR-CAB0100LL-R	AIR-CAB0150LL-R
Length	20 ft (6 m)	50 ft (15 m)	100 ft (30 m)	150 ft (46 m)
Loss	1.3 dB	3.4 dB	4.4 dB	6.6 dB

These cables are basically the same as the more common ones from Times Microwave and Andrew. The Times Microwave LMR cable and the Andrews Helix line are widely used to connect radios to antennas. Here are the loss figures quoted by Cisco for these cables.

Cable	2.5 GHz Loss (dB) per 100 ft	5.8 GHz Loss (dB) per 100 ft
LMR-400	6.8	10.8
LMR-600	4.45	7.25
Helix	5.7	10.5

Notice that the loss is higher as the frequency goes higher.

LMR cable looks like this.



[IE-RFT-WP1-07]

Figure 7.

Heliac looks like this.



[IE-RFT-WP1-08]

Figure 8.

Photo Courtesy of Andrew

Bridge power cables are RG6 or RG59 75-ohm coax cable. This is a common cable. There is a 100-foot limit to this cable. Running it farther may work, but the unit will not receive sufficient power, which will lead to premature failure of the radio.

The point of all of this discussion of connectors and cabling in a tutorial on RF troubleshooting is that the coverage area will be less -- sometimes much less -- than expected if the wrong type of cable or connector is used. For example, Figure 9 is a graphic to illustrate this. It shows that separating the antenna from the radio creates a smaller coverage area due to the loss of signal strength in the cable. This same thing will happen if the wrong type of cable is used or if water gets in the cable.

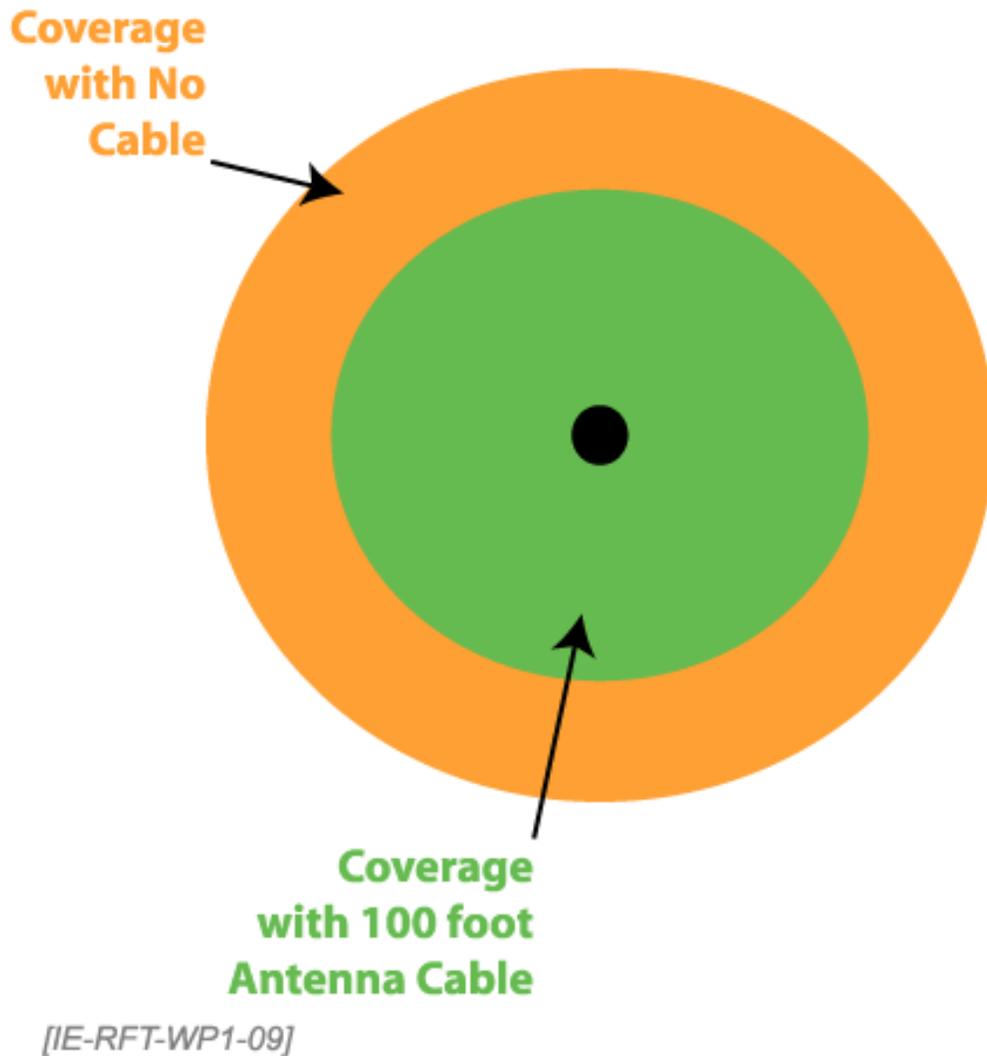


Figure 9.

Attaching connectors to low loss cable requires special tools and some training. The tools from Times Microwave cost several hundred dollars. Failure to properly install the connector will lead to unexpected signal loss. The best method is to use preassembled cables with the connectors already installed.

Once the cable is assembled, if it goes outside, some method of sealing the connection where the cable attaches to the connector and then the connector to the radio must be used. As stated above, moisture is very, very bad for connections carrying RF signals. You must keep moisture out of the connections. If water gets in, forget getting it out, just replace the part. To keep it out in the first place, seal connections using one of the methods discussed below. Recheck these connections on a regular basis. Unexpected signal loss over time is often due to water infiltration.

No one can agree on the best way to keep moisture out. Everyone does agree that it must be done. Listed next are some of the methods that have been suggested. No one method is any better than any other. Try them and use the one that works for you. The basic method is to wrap the connection with a layer of 3M Scotch 33+ tape. Then a layer of 3M Scotch 2210 vinyl mastic tape. The final layer is another one of 3M Scotch 33+. Each layer is laid on from bottom to top to produce a shingling effect. Also be sure the tape lays down nice and flat with no bubbles or bulges. The first layer of electrical tape adds a protective layer between the connector and the mastic, which is sticky. The next layer of the vinyl tape covers the mastic and keeps the gooey stuff from sticking to something it should not, as well as keeping out the water. The mastic is basically a thick sticky tape. It is sticky on one side. The stick is covered with a peel off cover. This substance is about 1/8" thick. The three layer combination also allows the tape to be removed by slicing down to the bottom layer and peeling the tape off like you peel a banana. In some places, Cisco

recommends 3M Scotch 88 tape. 3M says this tape:

...offers better mechanical/abrasion resistance, and is thicker for quicker build-up. For professional use, this tape combines the flexibility of a PVC backing with excellent electrical insulating properties to provide primary electrical insulation for splices up to 600V and protective jacketing. UL Listed and CSA Certified. Excellent resistance to UV rays, abrasion, moisture, copper corrosion, alkalis and acids. Excellent all-weather performance in cold to 0°F (-18°C) or hot to 220°F (105°C).

3M says the 33+ tape is:

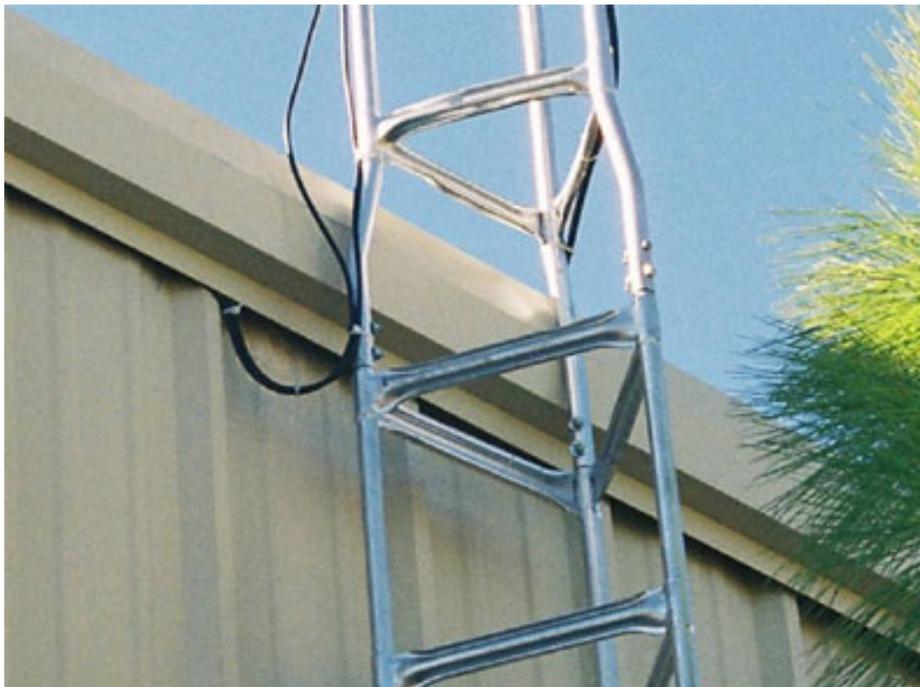
...highly conformable and super stretchy in all weather applications. This tape provides flexibility and easy handling for all around performance. It combines PVC backing with excellent electrical insulating properties to provide primary electrical insulation for splices up to 600V and protective jacketing. UL Listed and CSA Certified. Excellent resistance to UV rays, abrasion, moisture, copper corrosion, alkalis and acids, and is flame-retardant. Excellent all-weather performance in cold to 0°F (-18°C) and is designed to perform in a continuous temperature environment up to 220°F (105°C).

Use either one.

In addition to this basic method, some first spray the inside of the connector with non-dielectric Bull Frog protectant. Others apply a liberal (about 3 mm) coat of Scotch Coat liquid, not spray to this top. Others say forget the sprays and liquids, as they just make a mess.

Another idea is Coax-Seal. This is recommended by Cisco in several places. It is a form of the vinyl mastic. This is applied as a single layer. An example of how this is applied is shown on the [Coax-Seal web site](#).

Always use a drip loop, such as shown in Figure 10, to keep the water from riding along the cable to the connector.



[IE-RFT-WP1-14]

Figure 10.

This is quite a lot of information on water infiltration protection, but this is an important topic for preventing trouble. A link will work for a while, but gradually fail if these protective measures are not applied.

Water in another form can also cause problems for outdoor point-to-point links. When water freezes into ice on an antenna, the result can be a dramatic change in the antenna's radiation pattern according to Til-Tek. The higher the frequency, the worse is the problem. Til-Tek's research has found ice buildup to be a problem because the dipole elements of an antenna radiate radio waves into free space. The impedance of free space is 377 ohms. If the air surrounding the elements is replaced by ice, which has lower impedance, the impedance match and radiation pattern of the antenna will change. Ice has the same effect as if the directors were lengthened. As the electrical length of the directors becomes greater than one-half wavelength, they stop being directors and start acting like reflectors. To prevent this problem, antenna elements are usually encased in a plastic protective housing or radome.

For example, for a 10-element Yagi antenna at 502 MHz, the normal radiation pattern looks like this.

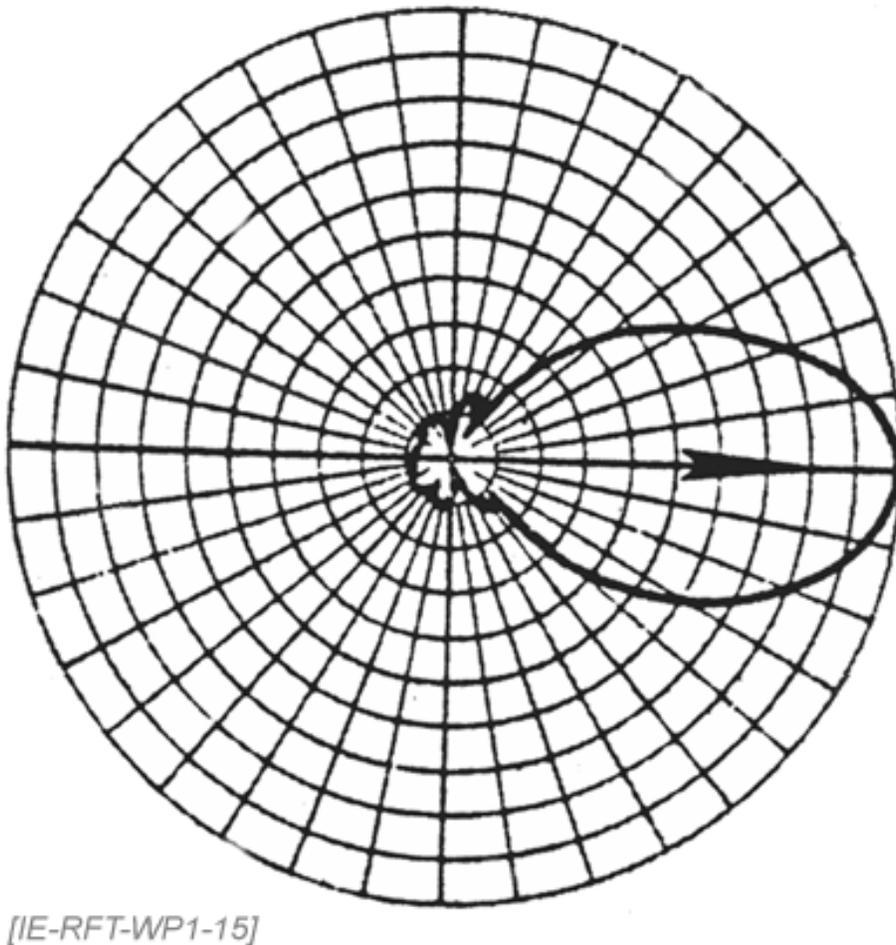


Figure 11.

Graphic from Til-Tek

With 0.20 inches of ice, the same antenna has a radiation pattern like this.

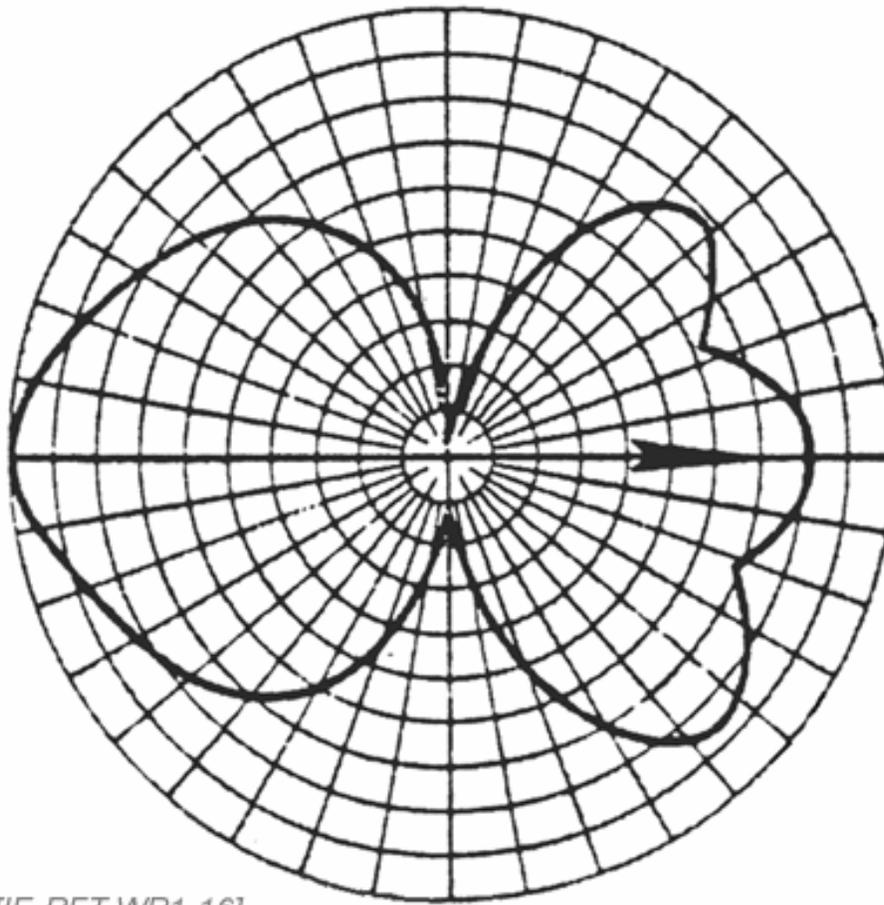


Figure 12.

Graphic from Til-Tek

Here's an example of ice buildup on an outside antenna.



[IE-RFT-WP1-17]

Figure 13.

Photo Courtesy of Alvarion

Polarization

Another source of problems for point-to-point links is cross polarization of the two antennas. Care must be taken to ensure that both ends of the link use either horizontal or vertical polarization. Using one type on one end and the other type on the other end will cause signal loss up to 20 dB. This can be enough loss to prevent the link from working at all. Just looking at a unit will not tell you which way to mount it. Look for a label or other mark.

Antenna Types

It is not necessary to use the same model or even style of antenna at each end of a point-to-point link. Both antennas must use the same polarization. For example, a wireless metropolitan area network, such as a wireless ISP, will use an omnidirectional antenna at the base station and directional antennas at the customer ends. Using a different style antenna will not cause a problem. Using an antenna designed for one frequency with a radio for another frequency will not work. The connectors are the same regardless of the frequency used.

Distance

For an outdoor bridge connection, distance is always an issue due to the dynamic nature of the radio frequency environment. Cisco states that a 25-mile link is possible. Establishing and maintaining such a link while using an unlicensed frequency can be tricky. To evaluate this, the first thing that should be done is a link budget calculation. Cisco provides an Excel spreadsheet for this purpose.

Cisco Systems		For Cisco Aironet 5GHz Outdoor Links ONLY!	
Models Supported - Cisco Aironet BR1410 ONLY!			
Regulatory Domain	United States/Canada	Select this from Power Regulatory Domain page	
Site 1		Site 2	
BR1410 Model number	AIR-CT5514-A-K3-H	BR1410 Model number	AIR-CT5514-A-E8-N
Select Power level	15mW/22dBm	Select Power level	15mW/22dBm
Select Data rate	96Mbps		
Select Antenna 1 here	Dish 20dBi	Select Antenna 2 here	Dish 20dBi
Note: When using 20dBi dish, power level must be set to 22dbm or lower		Note: When using 21dBi dish, power level must be set to 22dbm or lower	
For other Antenna- Enter Gain Here	0.00	For other Antenna- Enter Gain Here	0.00
Enter Cable Loss dB/100 ft here	0.00	Enter Cable Loss dB/100 ft here	0.00
Enter in Length Here	0	Enter in Length Here	0
Effective Isotropic Radiated Power	50	Effective Isotropic Radiated Power	50
Environmental Conditions			
Terrain	Average terrain with some roughness		
Atmosphere	Normal, interior, continent, temperate or sub-arctic		
Max Distance	13.19 Miles	21.21 Kilometers	

[IE-RFT-WP1-18]

Figure 14.

Graphic Courtesy of Cisco

For an inside wireless LAN, the material the building is made of affects the ability of the signal to penetrate over the expected distance. Radio signal obstructions commonly found in buildings include:

- Steel studs in walls
- Steel doors
- Large structures inside the building such as elevator shafts and stairwells
- Steel reinforced floors

In an office environment the furniture itself may also have an effect, for example:

- Metal filing cabinets
- Metal mesh furniture

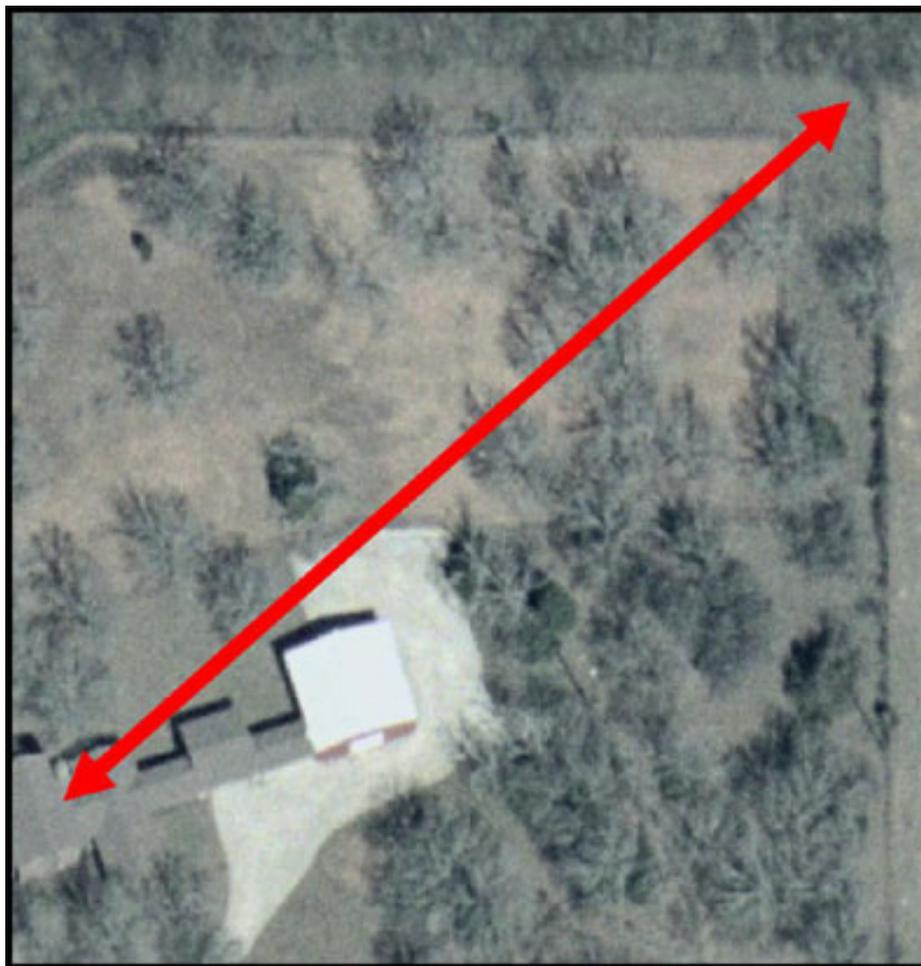
In a warehouse environment other elements may come into play, such as:

- Metal racks
- The products on the metal racks with high water content will block the signal. This is true of both the product and the packaging. Paper and cardboard can have high water content.

Although the structure of the building may not change, the contents certainly can. When a link that has worked fails, this is something to look at.

Line of Sight

Due to the low power levels that unlicensed equipment are limited to an unobstructed line of sight is highly desirable. Depending on the distance some obstructions can be penetrated. For example, I have a bridge link that punches through several trees as this aerial photograph shows.



[IE-RFT-WP1-19]

Figure 15.

For reference, the white square toward the bottom of the photograph is the roof of a 36 ft by 36 ft building. The antennas are at 18 feet. At this height, the signal must punch through several trees, but the distance is only about 500 feet. A common problem at longer distances is a signal that works when installed in the winter, but fails in the spring when the leaves come out.

Fresnel Zone

The Fresnel zone is an ellipsoid around the direct line of sight between two antennas. The first Fresnel zone is a surface containing all points for which the sum of the distances from that point to the ends is exactly $1/2$ wavelength longer than the direct path. Each subsequent Fresnel zone surrounding this first zone is some multiple of $1/2$ wavelength either in phase or out of phase with the direct wave, thereby producing constructive or destructive multipath signals. Anything that extends into the first Fresnel zone, such as trees, hills, and buildings can diffract, reflect, or degrade the signal. This zone is three dimensional. Therefore account for objects that protrude in from the sides as well as those that stick up. The higher the frequency, the shorter is the Fresnel zone. Also the longer the path, the broader the zone is. Usually up to 20% to 40% blockage of the Fresnel zone will not cause a problem. Envision this as a slightly elongated football with a string running through the middle of it connecting the two points. The football is the Fresnel zone and the string is the visual line of sight

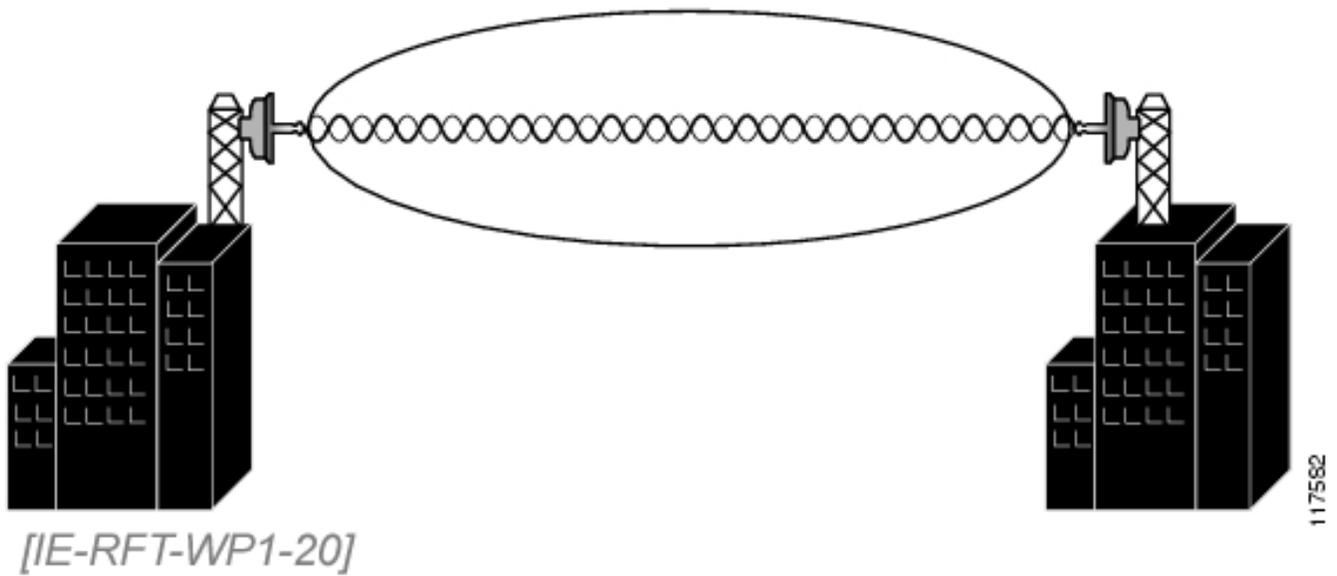


Figure 16.

Graphic Courtesy of Cisco



Figure 17.

Graphic Courtesy of Cisco

The formula Cisco likes for this is

$$0.60 F1 = 43 \times \text{SQR}(\text{Distance}/4 \times \text{Frequency})$$

Where $F1$ is the first Fresnel Zone radius in feet, $Distance$ is the total path length in feet, and $Frequency$ is in GHz. This is the size of the 60 percent clear zone, not the entire zone size.

This formula assumes the obstacle has a fairly sharp point at the top, such as a single tree. If the obstacle is more like a wide, flat top hill; then the loss is much higher. Further, this also assumes there is just one thing in the way. Many times there are several obstacles along the way. It is very difficult to model such a thing. This is why a fade margin is used. It attempts to account for all of these things for which exact calculations cannot be done.

Earth Bulge

For distances of over about seven miles, the curvature of the earth must be accounted for. The formula for this is

$$h = d^2/8$$

Where h is additional height required in feet and d is the distance between the antennas in miles.

This formula yields the additional antenna height required to account for the bulge. Not the total height, just the additional height.

Antenna Alignment

Over long distances, antenna alignment is critical and difficult. Keep in mind that as gain increases the radiation pattern tightens and narrows. Once the alignment is made, it is critical that the antennas remain stable. Poles that allow the antenna to sway back and forth are not a good idea. It may work when installed on a calm day, only to fail as the wind picks up. For example, I have a customer with his antenna on a 50-foot high 2-inch diameter pole. This pole uses three guy wires to keep it in place. As the temperature changes, the customer must go outside to adjust the guy wires to align the antenna. This link is only 1.5 miles long. At five or 10 miles, this will not do. No, this pole was not my idea.

Antennas can also be mounted inside behind a window. This eliminates many potential problems such as water infiltration, weather damage, and antenna movement. This assumes the window does not use a metallic tint or conductive gas of some type. This can be easily tested before installation.

Hidden Node

The hidden node problem occurs in wireless LANs when one node cannot hear another node transmitting. This occurs when they are separated by an obstruction or when they are too far apart. Both nodes can see the access point, but not each other. This causes excessive collisions on the network, retransmissions, and therefore reduced throughput. Detecting hidden node is difficult. Degraded throughput on the network is the common sign of hidden node. Examining the layout of the network may show hidden nodes. Moving or disconnecting possible hidden nodes and then examining the throughput may show these as well. This is a trial and error process.

The solutions for hidden node depend on the type of network. For a LAN, solutions include:

- Use RTS/CTS
- Adjust the point where the wireless packets are fragmented
- Increase the power used by the far nodes and decrease the power used by the nearby nodes
- Remove the obstacle
- Move the node closer
- Use a polling mechanism to control access

RTS/CTS does not solve the hidden node problem, but it may be a way to improve the throughput if the

node or obstacle cannot be moved. If network throughput is slow or if there are a large number of retransmissions, enable RTS by lowering the RTS threshold. On systems where a polling mode is not supported, Cisco recommends adjusting the RTS/CTS parameter by reducing the packet size from its default of 2048 to a value where CRC errors become acceptable.

When 802.11b is used as an outside network solution, such as creating a CAN or MAN to provide campus-wide access to a LAN or the Internet, the use of RTS/CTS is different. The correct approach to take in this type of network is to set RTS threshold very low on each client device and above the average packet size for each access point. The maximum sized packet typically seen is 1500 bytes. The minimum is 64 bytes. By setting the access point's RTS threshold to something higher than 1500, such as 1600 bytes, the access point will never have to ask permission to transmit. To maintain collision control on the network, the RTS threshold setting for every client is set to 60 bytes. Keeping in mind that all conversations in a MAN network should be between clients and access points, never client to client, this forces the client to always ask the access point for permission to transmit, while the access point can transmit anytime.

In a CAN, either the LAN or the MAN settings just discussed can be used depending on whether clients need to talk to each other by going through the access point or just talk to only the access point and devices behind it on the wired network.

Near/Far

The near/far problem occurs when there are nodes near the access point that have high power settings and other nodes far from the access point with low power settings. The near, high-power nodes overwhelm the far, low-power nodes. To detect this, check the network design. Look at the power output level of the nodes. Possible solutions to the near/far problem include:

- Reduce the power of the nearby nodes
- Increase the power of the far off nodes
- Move the far off nodes closer to the access point
- Move the access point to a more central location

Low Throughput

The throughput of a wireless system is dependent on:

- Amount of interference
- Type of interference
- Security solutions that add overhead
- Distance, since the data rate falls off as distance increases
- Older, slower computers
- Fragmentation
- Use of RTS/CTS

- Use of PCF - Polling mode

The most common solution to low throughput is the co-location of access points in a single area. For 802.11b, for example, three non-overlapping channels are possible. A single AP will provide from 4.5 to 5.5 Mbps in practice. In theory, three APs should provide 15 Mbps or so. In reality they will produce slightly less. The reason is that there is actually some overlap even among these sets of channels. Of course, it is possible to use fewer than three APs, two may be used on channels 1 and 11. This may make sense if the cost of three access points each producing 4 Mbps is compared to two producing 5.5 Mbps each. It may also make sense to force fragmentation so as to produce smaller frames. This means that the lost frames when retransmitted are smaller. When a packet must be fragmented this adds overhead as each fragment requires an ACK.

Fragmentation

As mentioned, fragmentation can be adjusted to improve efficiency on the network. If the network is experiencing high packet error rates, increase the fragmentation threshold. As Priscilla Oppenheimer and Joseph Bardwell discuss in *Troubleshooting Campus Networks*, this is done by starting with the maximum size and gradually dropping the threshold until an improvement is seen. As the frame size is increased, there is less overhead, but increased chance of collision. As the frame size decreases there is more overhead, but less chance of collision. Start with a setting of 1024 bytes. In a network where the average packet size is greater than 800 bytes, it may benefit the network to lower the fragmentation setting to see if performance improves. This can be determined by transferring a large file, such as 1 GB, as the test data must be larger than the fragmentation threshold, and timing how long it takes. Adjust the value in 100 byte increments above and below 1024 bytes and see when the most improvement occurs.

Sensitivity

In environments with high noise levels, it may help to reduce the sensitivity of the radio. By doing this, the radios will not see the noise if it is no longer sensitive enough to pick it up.

Harmonics

Interference can appear from odd locations, such as the result of harmonics and intermodulation products. Harmonics are exact multiples of a fundamental frequency, starting with two times the fundamental frequency. For example, a common source of interference for 2.4 GHz mounted on the same tower as paging equipment that operates in the 800 MHz range is a second harmonic from the paging transmitter. For a fundamental frequency of 800 MHz, the first harmonic is 1600 MHz and the second is 2400 MHz. This harmonic appears as interference in the unlicensed 2.4 GHz range. As the order of the harmonic goes up, the strength of its signal goes down. The most likely to create problems are the low order harmonics as the filtering in the receiver may not be able to keep these out. Harmonics are generated by almost all amplifiers. When a harmonic is produced by a transmitter, it is normally the result of insufficient transmitter filtering.

Intermodulation Products

At a site with multiple transmitters, the harmonics from two different ones can combine to form an intermodulation product. For example, if the second harmonic from one transmitter combines with the third harmonic from another transmitter, a fifth order intermodulation product is produced.

This new frequency can be the result of either adding or subtracting the two harmonics. The intermodulation can occur at the transmitter itself, in the receivers, or even be the result of poor connections on a tower.

Harmonics and intermodulation products are the result of nonlinear processes. In a radio, it is best if the amplifier amplifies without distortion, the mixer produces a perfect signal, and the radio receives perfectly. This does not happen. Everything is nonlinear. The output does not follow the input perfectly. In other words, distortion is created. Prevention of harmonics and intermodulation products is done with good radio design, filtering, and sound construction practices.

Cisco Specific Problems

Cisco has an article titled "Wireless Point-to-Point Troubleshooting Guide" on their web site that details conditions seen on the bridge radios along with suggested solutions. This is summarized here.

Radio Up Line Protocol Down is caused by interference, weak signal, a loopback enabled, wrong throughput setting, or a bad cable. Radio Down and Line Protocol Down is due to interface shutdown, interference, bad wireless line card, mismatched frequencies, ARQ incorrectly configured, incorrect throughput setting, privacy settings mismatched, transmit power incorrectly set, no power, bad cable, antenna problems, and incorrect or bad duplexer.

Tools

There are several tools the network administrator needs to diagnose these problems.

Coax Tester

Basic continuity in a coax cable can be tested with a multimeter or a coax test unit such as this.



[IE-RFT-WP1-22]

Figure 18.

Be sure that the unit has adaptors for the type of connector used as these usually only come with a BNC connector.

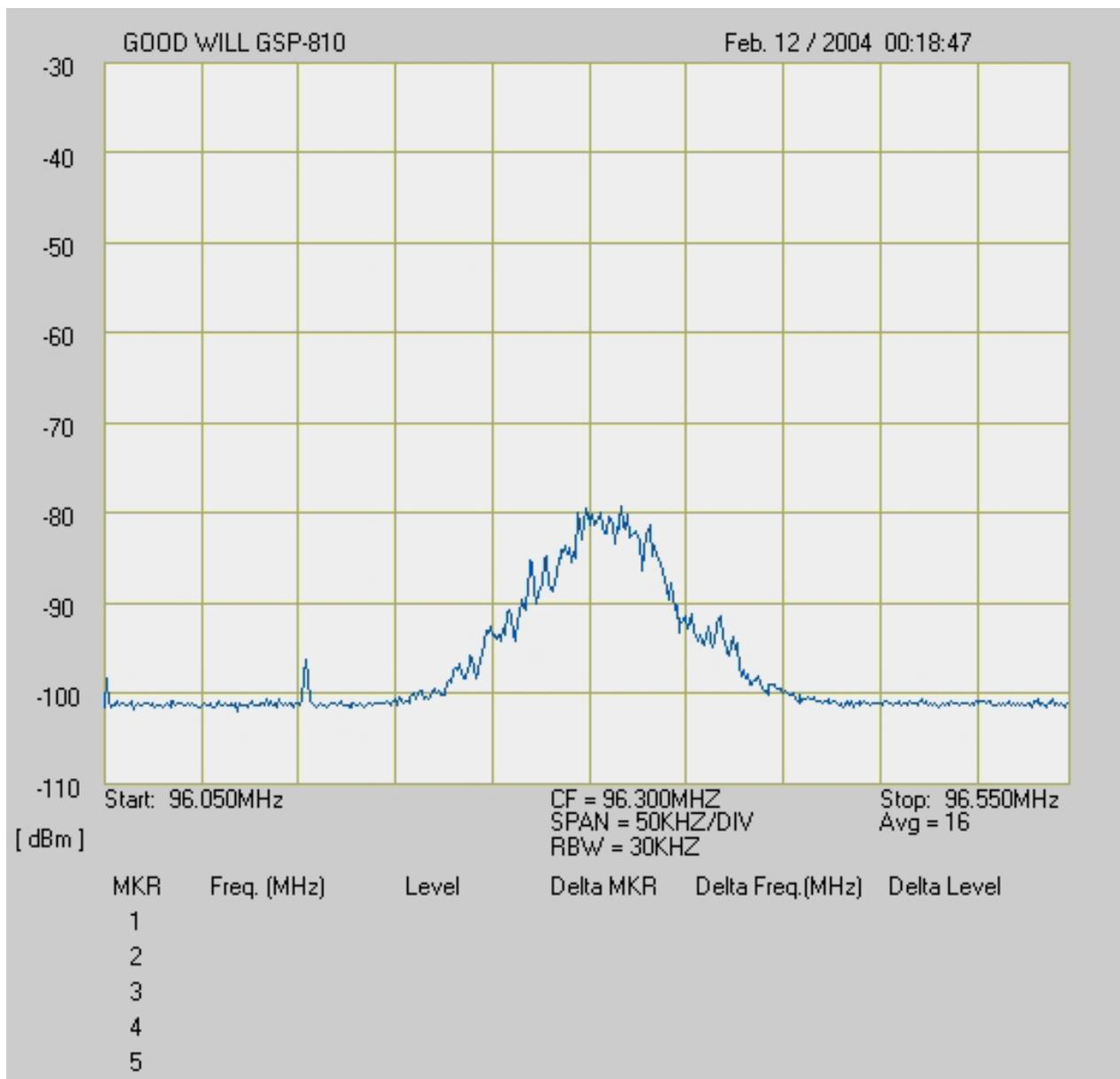
More advanced coax cable testing is done with a power meter such as the Praxsymb PA-2458 used to measure cable loss.

Spectrum Analyzer

As discussed in [the "How to Implement Wireless Networks" Study Guide](#) at CertificationZone, a spectrum analyzer is used to examine the actual waveform of RF signals. The use of this device is discussed in that tutorial.

For troubleshooting purposes, the antenna used with the spectrum analyzer can be the survey type antenna supplied with the unit or the antenna actually used by the affected system. The cable can be removed from the radio and attached to the spectrum analyzer. An adaptor may have to be used to match the connectors.

A consideration when looking at interfering signals on a spectrum analyzer is the nature of the dB. As also discussed in "How to Implement Wireless Networks" a dB is a logarithmic measure. This means a major change in signal level shows as a small change on the waveform display. On the typical vertical scale of a spectrum analyzer a 3 dB change in the signal which is double or half of the original signal is hard to see as this display shows.



[IE-RFT-WP1-23]

Figure 19.

See how a change from -80 to -83 would be difficult to spot.

Network Analyzer

A useful troubleshooting tool for wireless networks is a network analyzer that can read the information from the wireless NIC. Sniffer Wireless and AiroPeek NX can both be used for this purpose. Here is an example of the use of AiroPeek NX Version 2

Here is the opening screen.

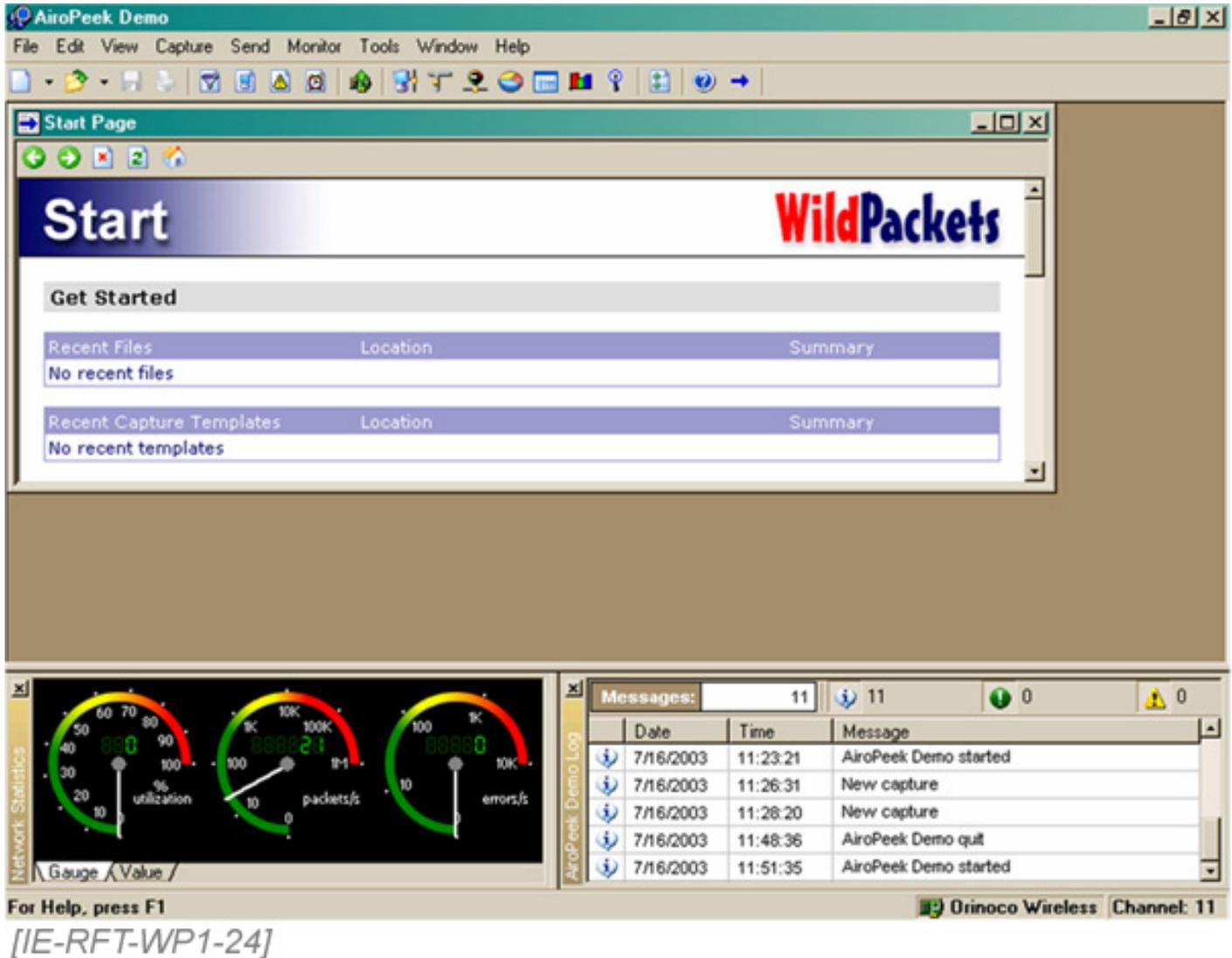


Figure 20.

The main point of interest on this screen is seen in the Network Statistics in the bottom left corner. This shows the real time:

- Utilization
- Packets

- Errors

This window has two views: Gauges and Values.

These look like this up close.

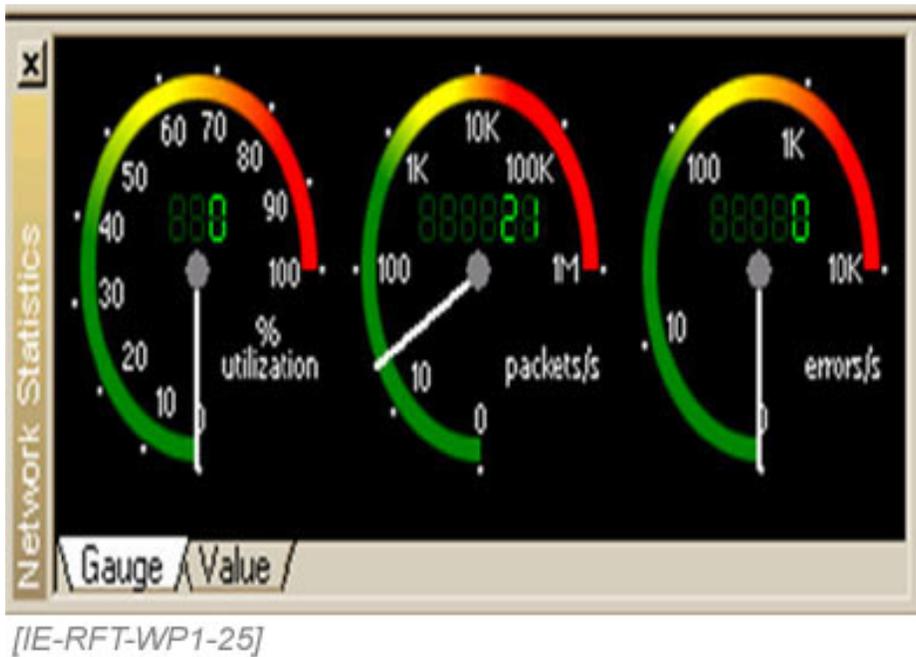


Figure 21.

and

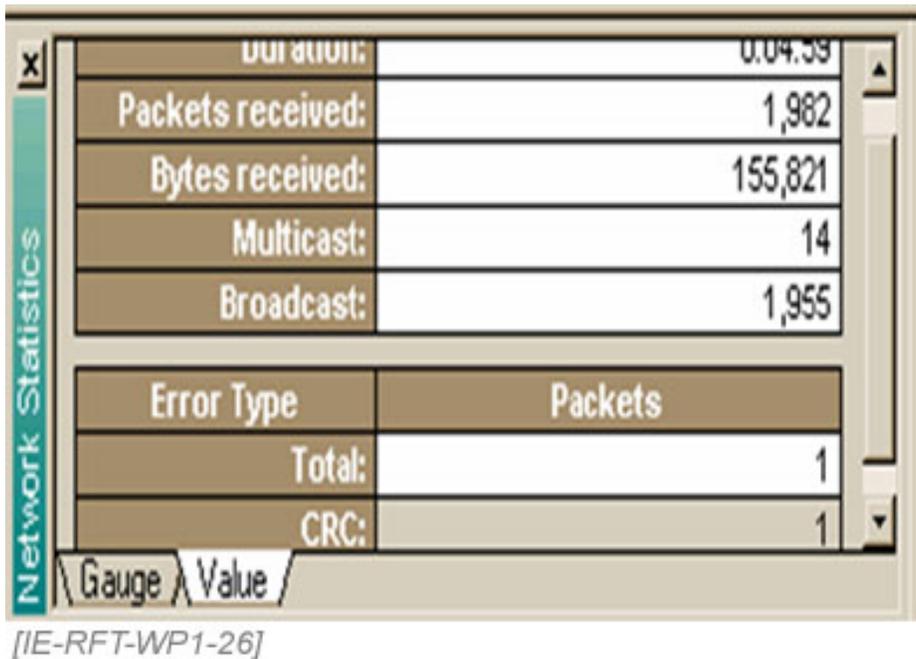


Figure 22.

In the Node Statistics display, accessible by clicking on its toolbar button, useful troubleshooting

information can be seen.

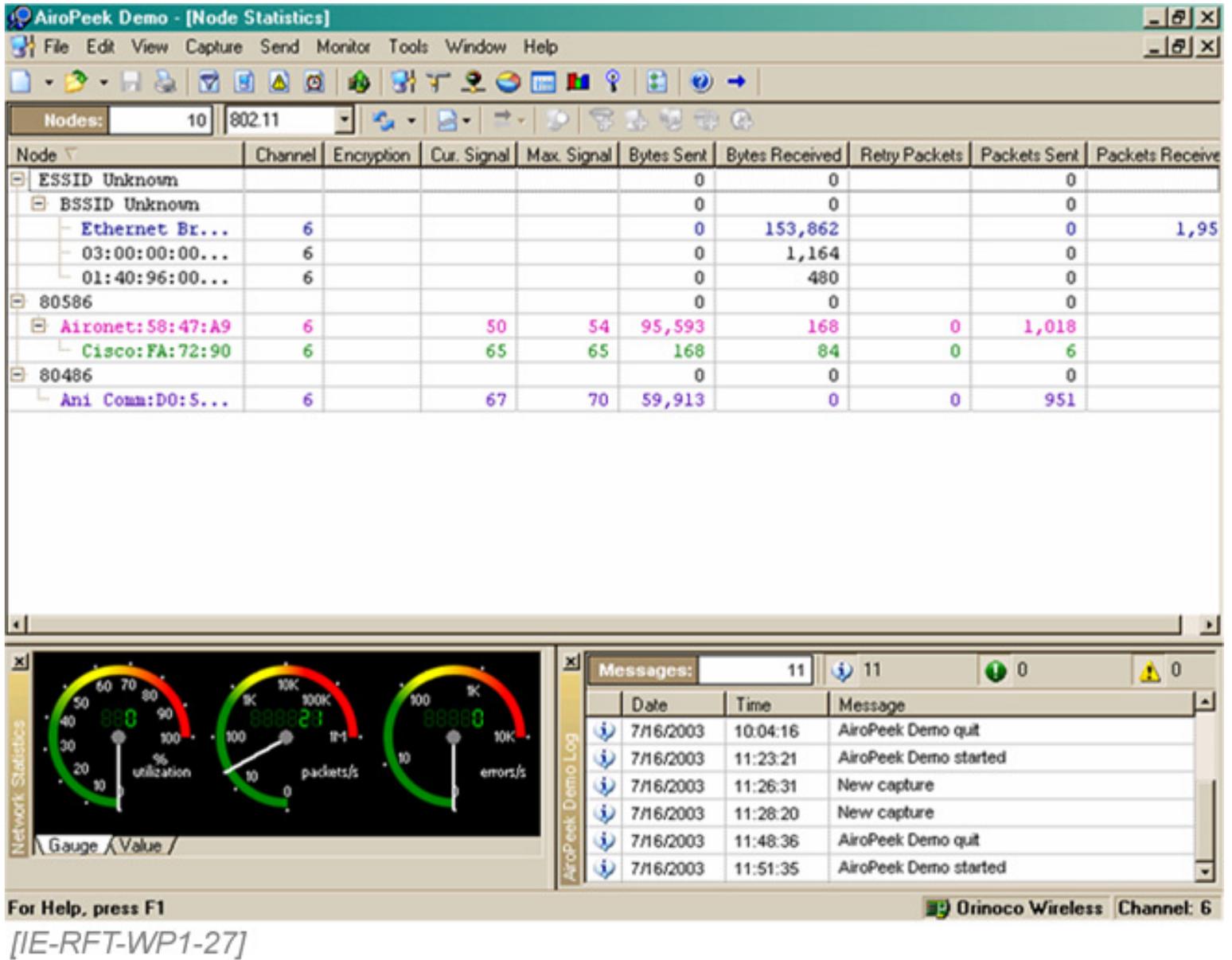


Figure 23.

This display shows the number of Retry packets. The Summary Statistics display shows some interesting information once it is expanded by clicking on the plus signs.

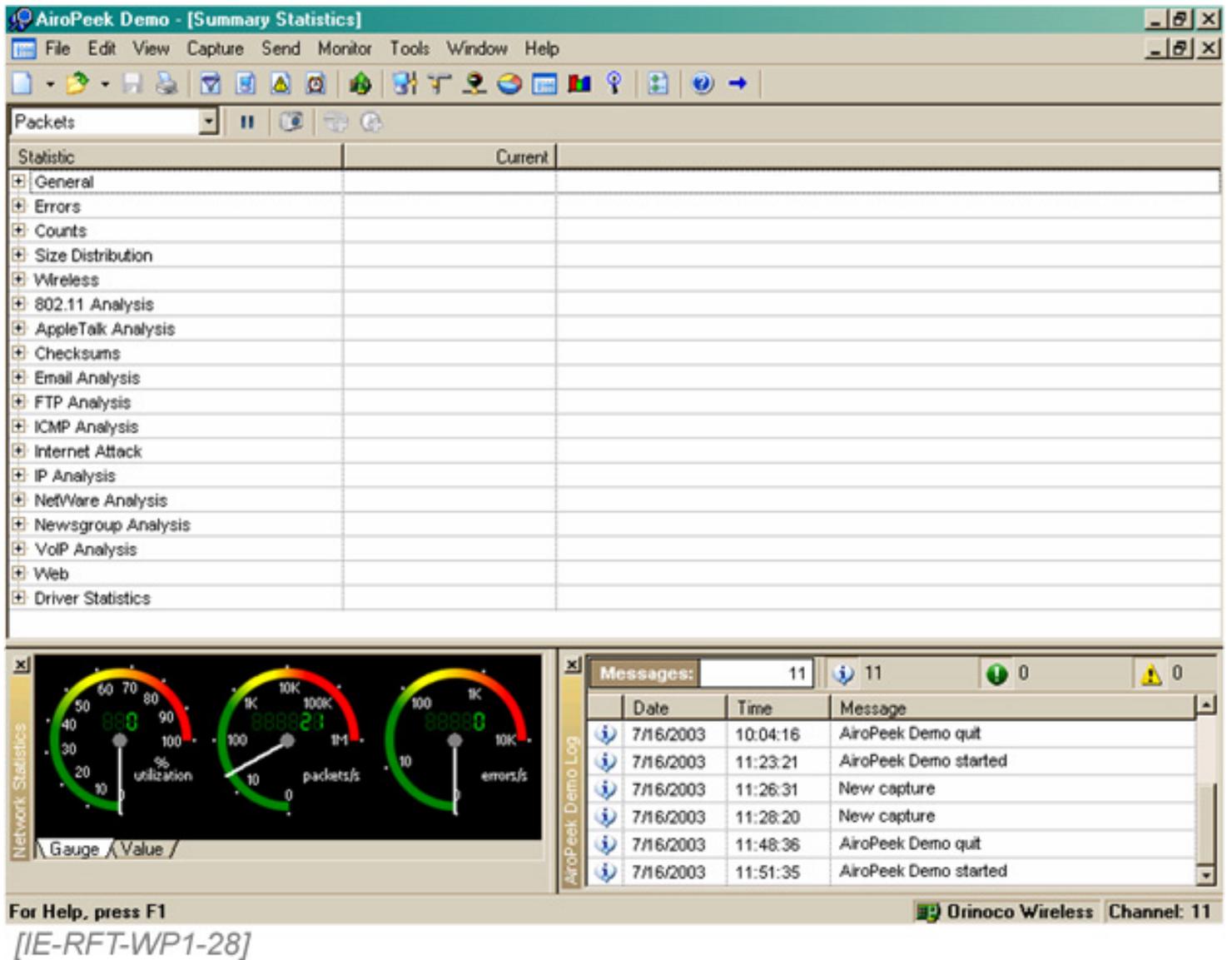


Figure 24.

In this case, the "+" beside Errors is clicked. This shows the number of CRC errors.

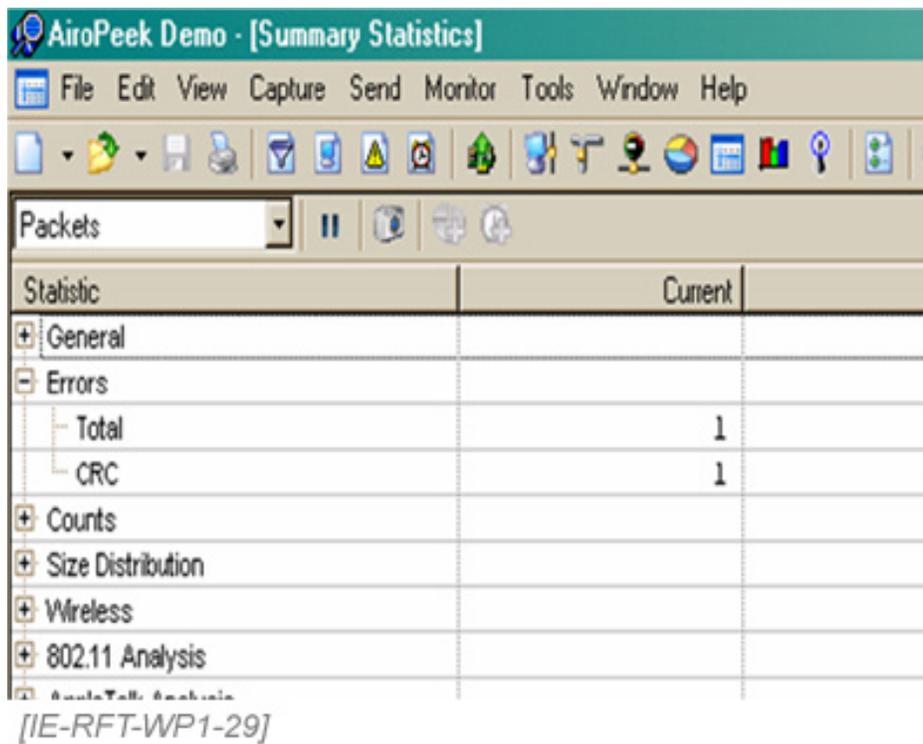


Figure 24a.

There is much more to this tool, but this gives you a basic idea of its functions.

Hotspots

A hotspot, or PWLAN as Cisco prefers to call it, is a place where Internet access is provided to a small area. While examining the material on the Cisco site related to this topic, I was reminded of the time I went to change a fuel filter on a Mercedes-Benz. I expected to find a small plastic filter held onto a rubber fuel line with a couple of 10 cent hose clamps. Instead I found a spun aluminum canister secured by two metal bands that was accessed by first removing the stainless steel fuel line and the fuel pressure dampener. All of this was suspended under the car by a shock absorbing system. A fascinating and effective system no doubt, but somewhat over engineered for the application. This is the case with the Cisco PWLAN (Public Wireless LAN) solution. This is an elaborate system relying on several hardware and software components. In contrast, most hotspot deployments today can be accomplished with a single box costing from nothing to a couple of hundred dollars. Much of the Cisco initiative on this is aimed at providing fine grained control of access, usage, and billing. Clearly, the hotspot model is quickly moving to one of open free access. Just as a restaurant must supply a glass of water and a restroom, many businesses are learning that providing free Internet access is just another cost of doing business. Enough opinion, let's see how the Cisco method works.

The Cisco PWLAN solution is illustrated in Figure 25.

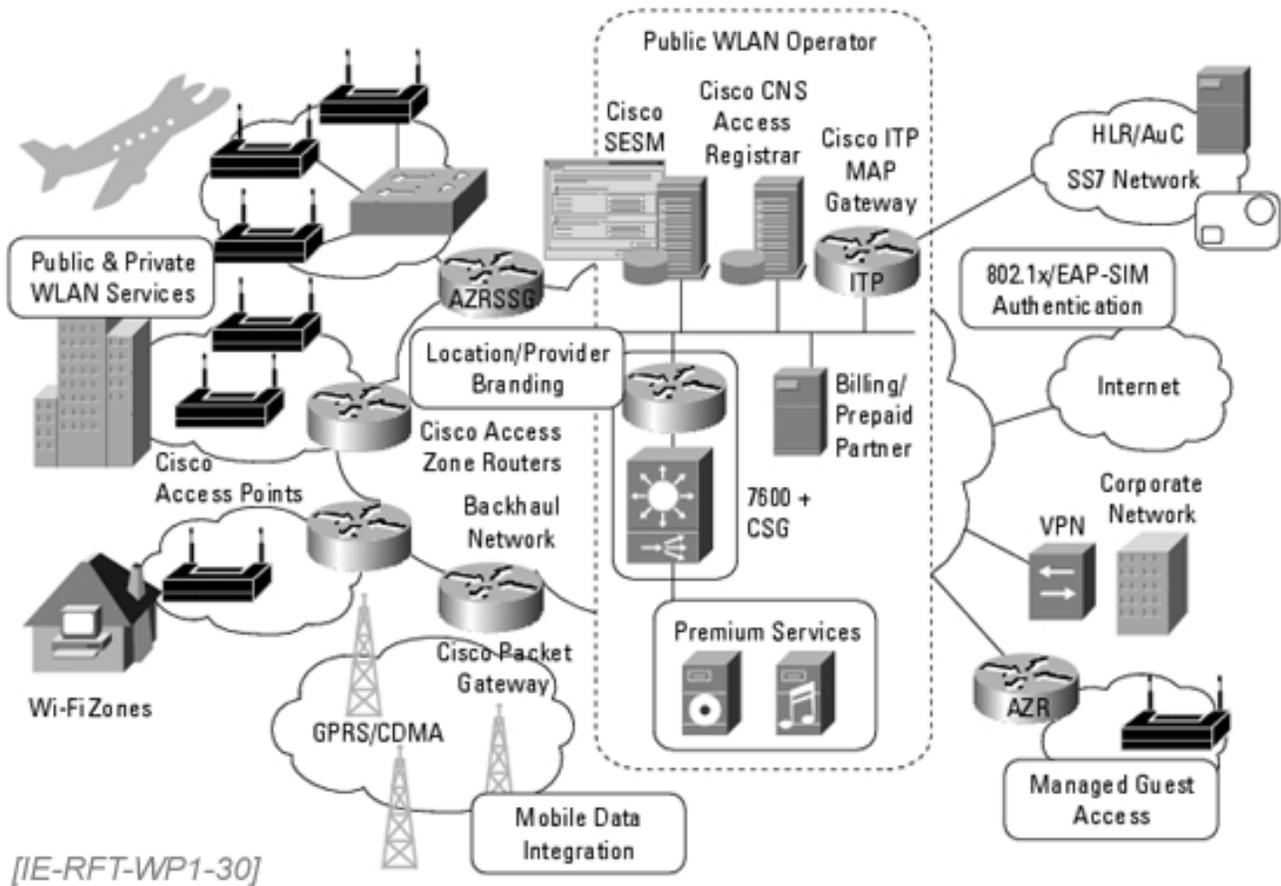


Figure 25.

Graphic Courtesy of Cisco

The key PWLAN related components in the Cisco solution are:

- Access Point
- Access Zone Router
- SSG
- SESM
- AR Server
- ITP

What do these things do within this framework? At the client location, the clients connect to the system through the access point. This needs to be from the Cisco 1100 or 1200 series. They do the usual access point function of connecting wireless clients to the wired network. Also at the client location is the Access Zone Router (AZR). This is a standard Cisco router from the 800 series up running PWLAN features. The AZR provides connectivity, client address management, security, and routing from the access point to the network infrastructure. At the core edge, access control is provided by the Service Selection Gateway (SSG) and the Subscriber Edge Services Manager (SESM). The SSG can be in the AZR or at the core. This is part of the Cisco IOS. The SSG router needs to be from the upper end of the router range. In a remote

core scenario, the AZR and SSG devices are separate routers. The AZR is at the client site and the SSG is at the core. In a centralized setup, they can both run on a single router from the higher end series. Access control functions provided by these two modules are control of access to the network, portal presentation, billing services, and branding. Behind the SSG and SESM is the AR (Access Registrar) server. This is an AAA server designed for this application that holds the user database, service profiles, and proxy connections to other providers. The ITP is the IP Transfer Point. This provides access to an SS7 network. This is a software feature module. If required, a billing server can supplement the AAA server functions by handling any prepaid services and the like delivered by third party providers. A Cisco switch with the Content Services Gateway (CSG) provides the ability to differentiate services by port or service. The CSG is a card that fits the Catalyst 6500 and 7600.

These components can be deployed in a centralized or distributed form. In the centralized PWLAN, the AZR is at the hotspot site as are the access points. The SSG is at the network core. This requires a high speed data connection between the two sites, such as a T1. In the distributed model, the AZR and SSG are one router at the hotspot site. This deployment is appropriate when there are multiple service providers for the location or for sites that already have Internet access.

The centralized approach

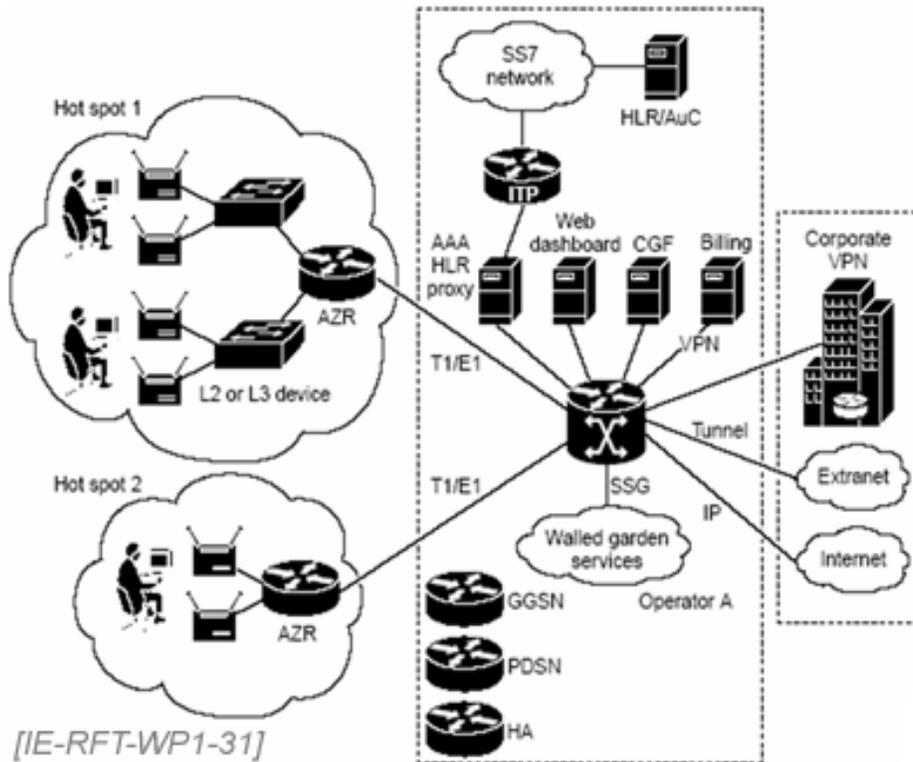


Figure 26.

Graphic Courtesy of Cisco

The distributed approach

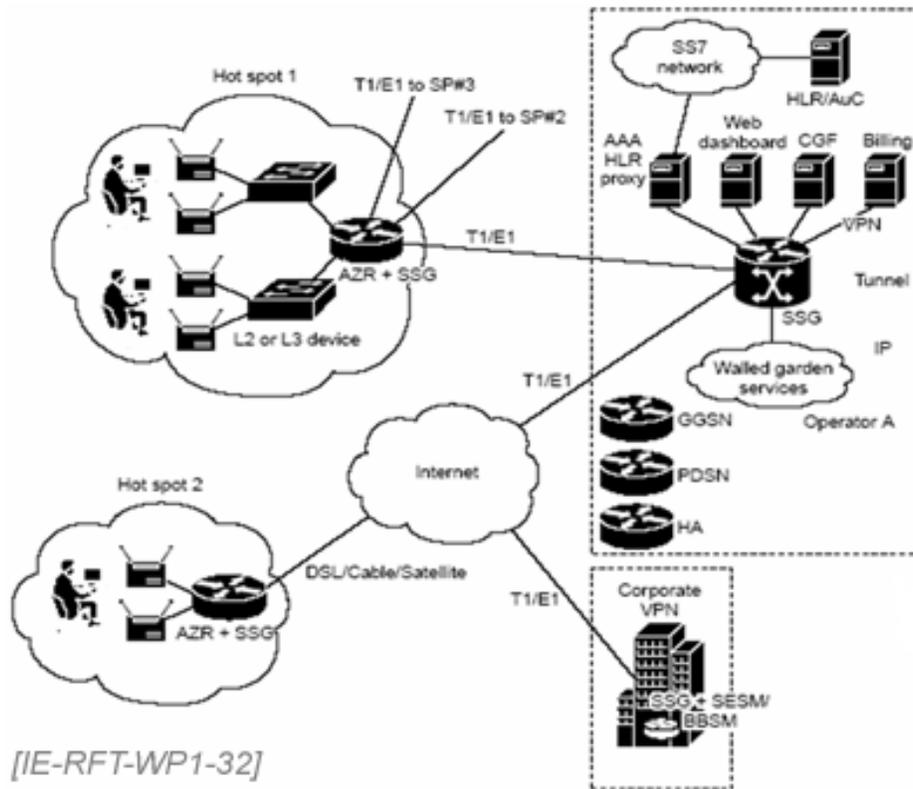
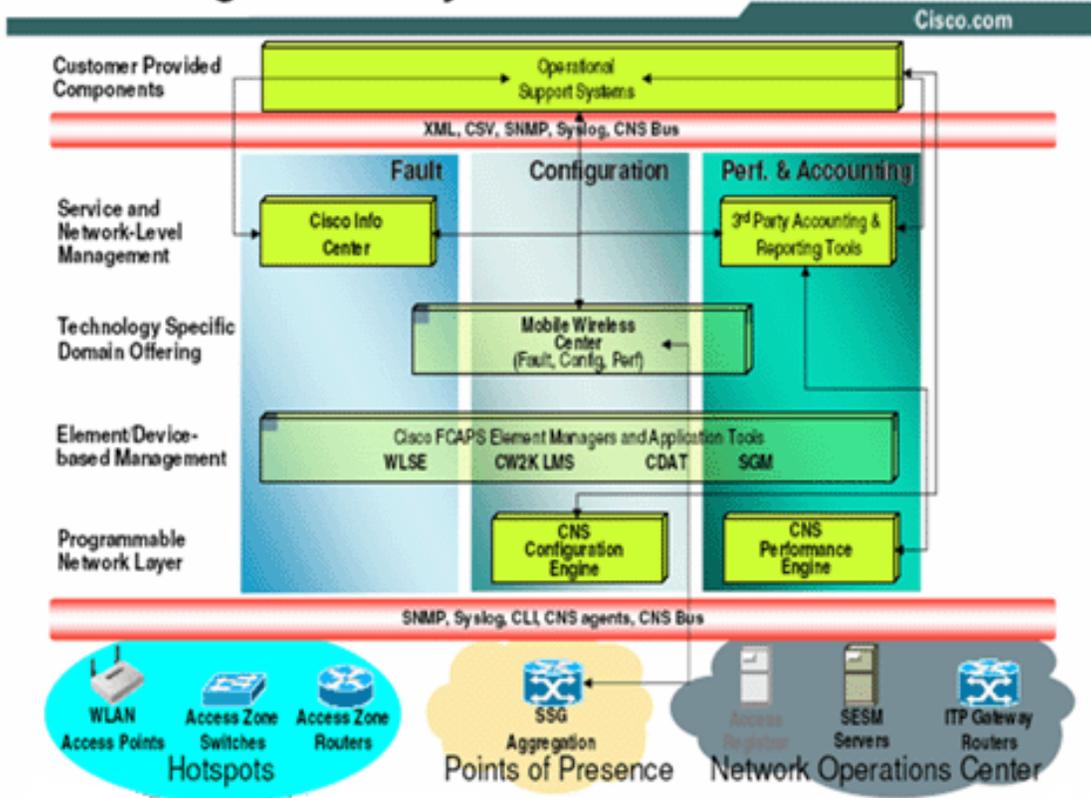


Figure 27.

Graphic Courtesy of Cisco

Within these various devices there are several management layers running.

Management Layers in PWLAN



[IE-RFT-WP1-33]

Figure 28.

Graphic Courtesy of Cisco

Conclusion

At this point, you should have an understanding of common problems and their solutions in relation to wireless data networks. This tutorial has also covered Cisco's approach to hotspots or PWLANs.