Sponsored by:

PANDUIT™

Appendix A

The Physical Layer

Cisco Networking Academy Program

Fundamentals of Wireless LANs v1.2

Table of Contents

A.1 The Physical Layer

A.1.1 Introduction

In the networking environment, almost any task or function is assigned to a layer of the seven-layer model published by the International Standards Organization (ISO). This model, called the OSI (Open Systems Interconnect) model, breaks the complex process of network communications into pieces that are easier to understand.

Each layer of the model has a standard defined input and a standard defined output, starting with the personal computer or other communicating device, and continuing to the cables that all the data travels along.

These are the seven Layers of the OSI model:

1. **Physical Layer or Bottom Layer -** The wire itself, or in the case of Wireless LANs, radio waves
2. **Data Link Layer -** Addressing each device that transmits on the network
3. **Network Layer -** Addressing individual networks to which one communicates
4. **Transport Layer -** Segmenting long files into more practical pieces, and controlling the flow of data
5. **Session Layer -** Keeping up with multiple conversations between various computers and servers
6. **Presentation Layer -** Reformatting, encoding, and compressing as required
7. **Application Layer -** The tools a computer program uses to talk to the network

It may at first seem strange to speak of a physical layer that includes cabling for a wireless network. If the physical layer is wireless, then why speak of copper or fiber? Cables are an important part of the wireless infrastructure.

There are several reasons for relying on cables that connect wireless basic service sets (BSSs). One of the biggest is security. By definition, wireless signals can be picked up by any antenna that can receive them. Whether or not the eavesdropper can decode the intercepted signals depends upon the experience, knowledge, and tools of the interceptor. Over time, the odds are with the eavesdropper, especially if recordings are made and the captured data can be subject to cracking over time.

Another security risk to wireless is that unauthorized users may attempt to attach themselves to the network, stealing bandwidth, and sometimes accessing confidential network resources.

Another reason to depend on a wired backbone between wireless LANs (WLANs) is that of frequency conservation. The wireless bands are divided into many channels, but these channels overlap to a certain degree. Several plans exist to maximize the use of these panels of channels, and they depend on isolating each use of a channel from other uses of that channel in the same network. Occupying a channel with a backbone wireless signal when a wired backbone is available may seriously restrict the allocation of the remaining channels in the panel.

A.1.2 Wireless Topologies

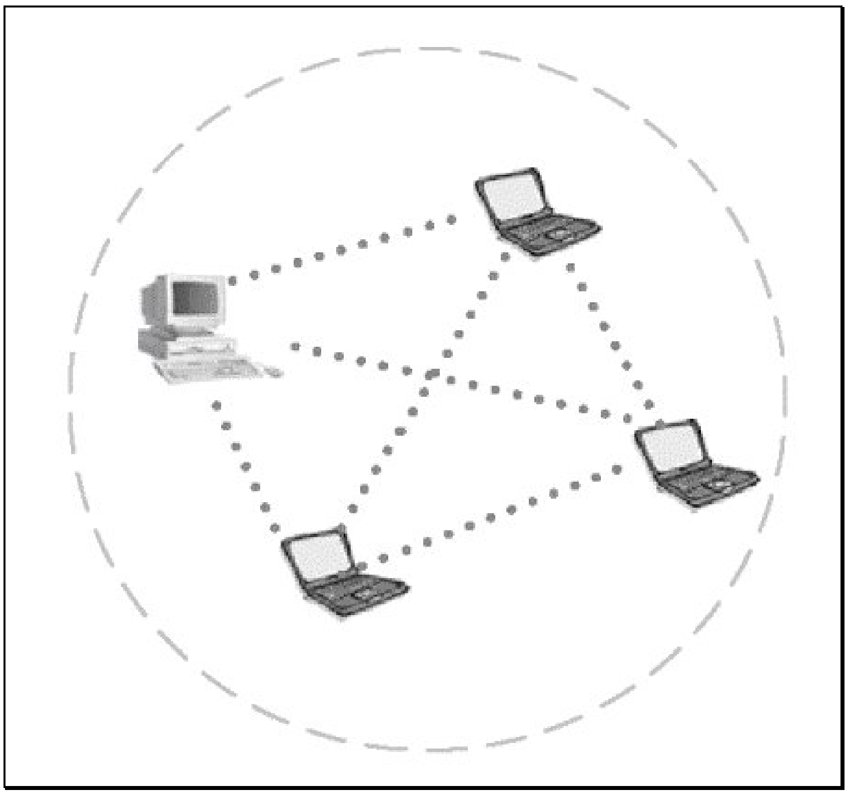

Figure [1]: An independent basic service set using no cables

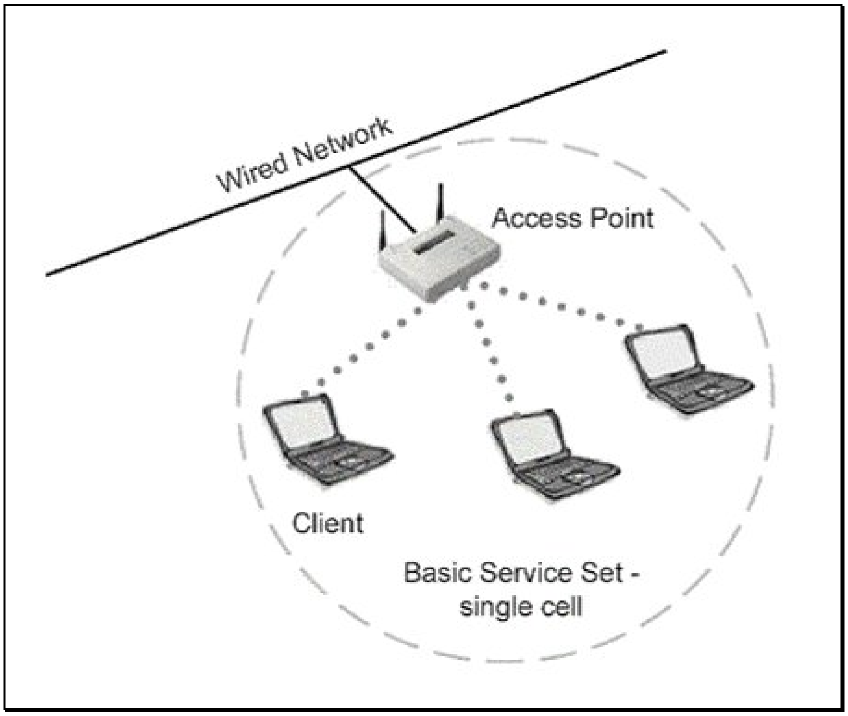

Figure [2]: A basic service set (BBS) that uses an access point to connect to the wired network

The independent basic service set (IBSS) shown in Figure 1 allows several wireless elements to connect in an ad hoc arrangement. The strong advantage to this is that users can join and leave the network at will with no need to adjust the cabling. Network moves, adds, and changes take place almost transparently.

Complications can arise once there is a need to connect to services outside of those provided by members of the group. A wired connection shown in Figure 2 is required. The special terminal that connects the wireless network-to-network cables is called an access point.

A.1.3 Wireless and Structured Cabling Systems of Today

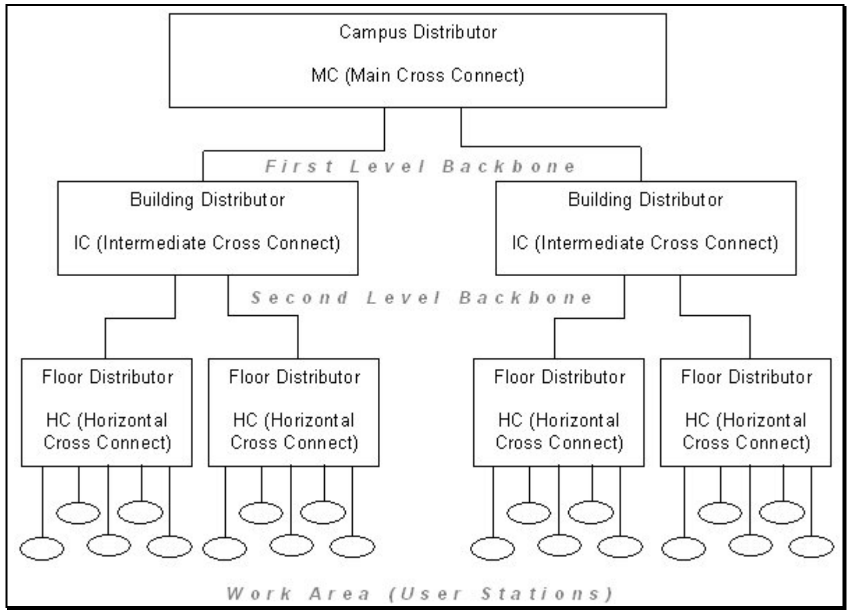

Figure [3]: The ANSI/TIA/EIA-568-B, 569-A, 606-A standard diagram

In a proper structured cabling system, all of the cables follow a star topology. The topology starts with the trunk lines from the core radiating out to intermediate distribution facilities, which cross connect to horizontal cabling which feeds end users and the work areas. Wireless access points are installed near the floor distributors as horizontal cross connects.

A.1.4 Wireless Zone Cabling

Figure [4]: A ceiling-mounted consolidation point. (Photo courtesy of Panduit Corp)

Figure [5]: A wireless access point

There is a concept in cabled networks that may be particularly useful in wireless situations. The concept is called zone cabling, and the two elements it depends on are called Multiple User Telecommunications Outlet Assemblies (MUTOAs) and Consolidation Points (CP). There are differences between these items but they can be overlooked for this discussion.

The purpose of zone cabling is to limit changes in network wiring to the areas where the changes occur rather than to disturb other portions of the network that are still functional. This is done by running horizontal cables from the telecommunications rooms to central points near each work area, and then by running work area cables to these same points. If later, there is a shuffle in the work area that requires moves, adds, or changes, these changes are made at the central point. The cables back to the telecommunications room are undisturbed. This is shown in Figure 4.

Wireless local-area networks (WLANs) can use a similar approach. Set an access point at the end of a trunk cable that extends from the telecommunications room. This access point allows users to form temporary connections, or permanent connections for which wiring is not available. This is shown in Figure 5.

If the wireless access point is to be useful, it must be mounted in a place that it can serve the users. The positioning of access points involves many factors, among them the ability to transmit along a path free of obstructions and reflections. The specialized tools required to position an access point are covered in the course. This supplement will focus on the wired network to which the access point attaches, and on the cabling required to power it.

A.2 Securing Cables

A.2.1 Cable Hanging

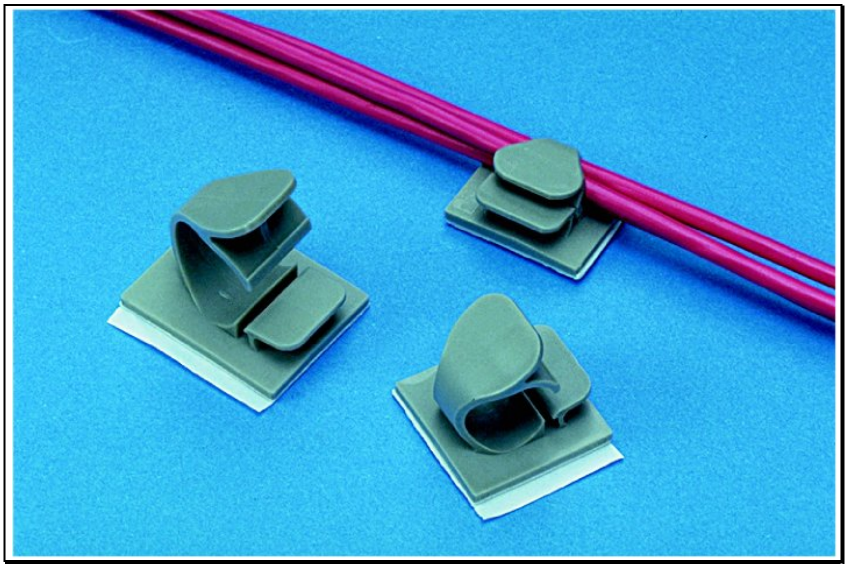

Figure [6]: Wiring management devices can secure cables leading to an access point. (Photo courtesy of Panduit Corp)

Most of the access points and bridges installers will be placing will be mounted in the area above a suspended ceiling. The American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), and Electronic Industries Alliance (EIA) standards, and to a certain extent electrical codes, require that data cables never be laid across the top of a suspended ceiling. All cables must be properly secured in dedicated cable management devices.

There is more than one reason for this. In the first place, the system is likely to perform better. Second, it may protect cabling from persons in other crafts whom regard carelessly installed data cabling as a nuisance, and who have been known to cut cables in order to move them out of their way. The major reason to use the proper cable suspension apparatus is that the standards require it. Appropriate and useful cable management and routing devices are shown in Figure 6.

A.2.2 Power and Conduit

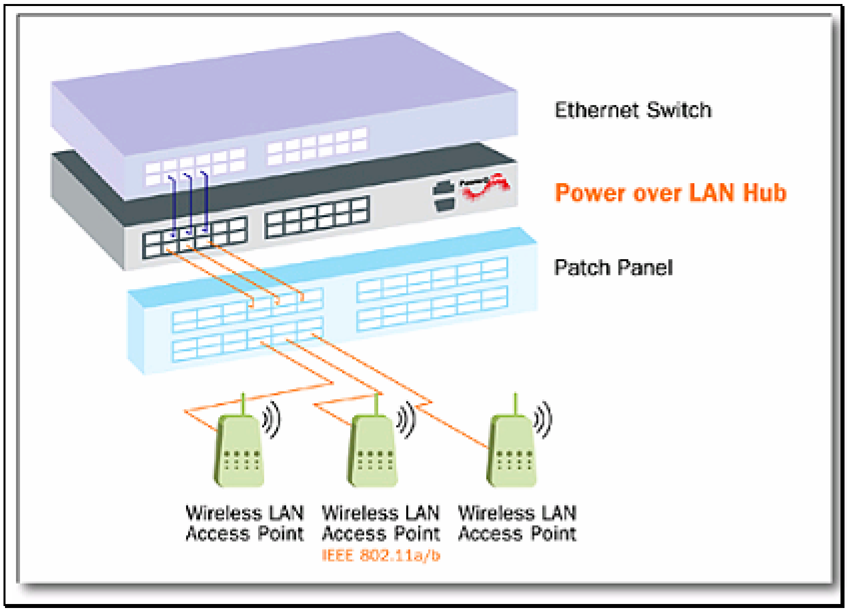

Figure [7]: Power over Ethernet devices and devices that follow the IEEE 802.3af standard power remote access points using Ethernet cabling

Figure [8]: A dual-channel surface mount raceway. (Photo courtesy of Panduit Corp)

Figure [9]: Multichannel raceway. (Photo courtesy of Panduit Corp)

Wireless access points and bridges obtain their electrical power from two sources:

- An alternating current (AC) power line that feeds a battery eliminator type power supply, which feeds the access point.
- Pairs in the Ethernet cables that carry power from IEEE 802.3af compatible power insertion units or switches with specialized interfaces, or other Power over Ethernet (PoE) injectors and taps.

To the wireless installer or network designer, it may be difficult to know which of these methods will be used. Both methods have advantages.

At this time, IEEE 802.3af systems are thought to be ideal for wireless access points, digital cameras, Internet protocol (IP) telephones, and other devices located where it would be inconvenient to obtain AC power. IEEE 802.3af systems are also used in cases where it is more convenient to use the Ethernet cable for power. One power over LAN adapter is shown in Figure 7. Network hardware equipped with such devices is often expensive.

In cases where AC power is available or easily run, a surface mount raceway can make it possible to provide both power and data cables. Electrical codes allow the same raceway to share data and power cabling, provided there is an insulating barrier between the power and data portions. This is shown in Figure 8.

As shown in Figure 9, the resulting raceway assembly can serve both power and data needs for the access point with ease.

A.2.3 Indoor Antennas

Figure [10]: A double dipole antenna

Figure [11]: The Cisco 2.2-dBi Ceiling Mount Omni

Although most access points have built-in antennas, most also provide the opportunity to plug in external antennas. These allow a more precise shaping of the antenna pattern to the work area.

The same wiring devices that apply to the cables feeding access points and bridges can be beneficial to external antennas as well. In fact, they may be more important. Many antennas use special connectors that ensure that antennas and transmitters remain properly matched so as to stay within the U.S. Federal Communications Commission (FCC) acceptance rules. This can increase the cost of the cables that attach to them. Damage to a cable may shut down an access point until a replacement can be obtained, because repairing the specialized connectors may not be possible in the field.

A.2.4 Specialized Cable Protection

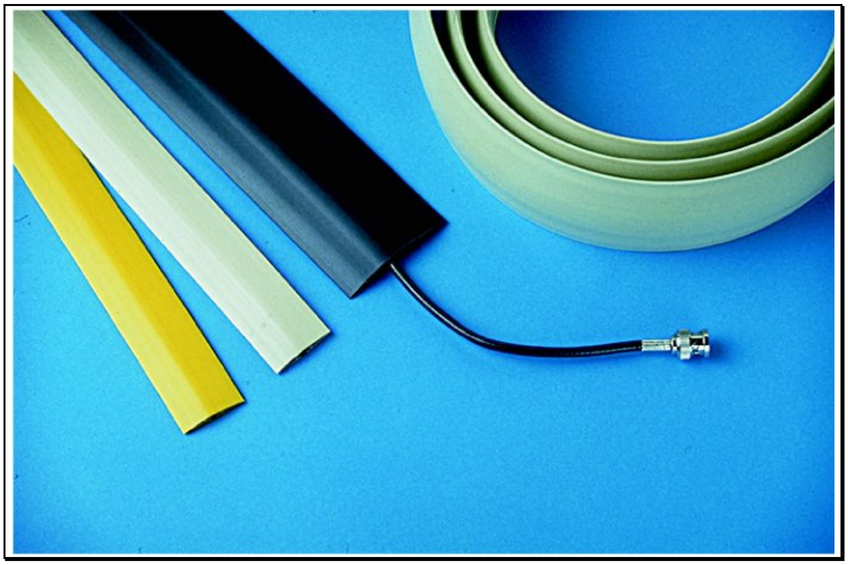

Figure [12]: Floor guard allows installers to route cables across floors (Photo courtesy of Panduit Corp)

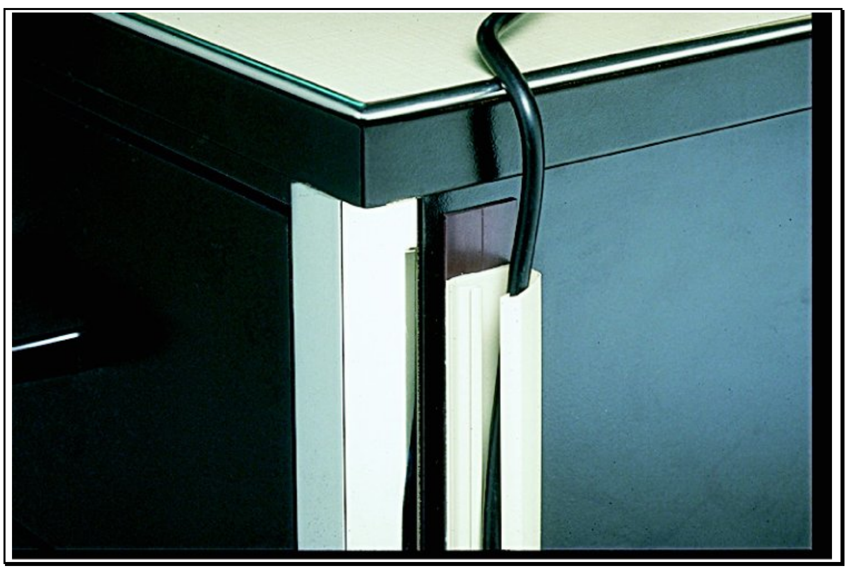

Figure [13]: Magnetic strips mount adhesive-backed raceway to metal surfaces (Photo courtesy of Panduit Corp)

People, as well as equipment, benefit from proper cable protection. Cables are a trip hazard that can harm people and equipment. Floor guards and magnetic strips can help to route cables safely when other alternatives are not easily available. This is shown in Figure 12 and Figure 13.

A.3 Cable Administration

A.3.1 Cable Organization and Administration

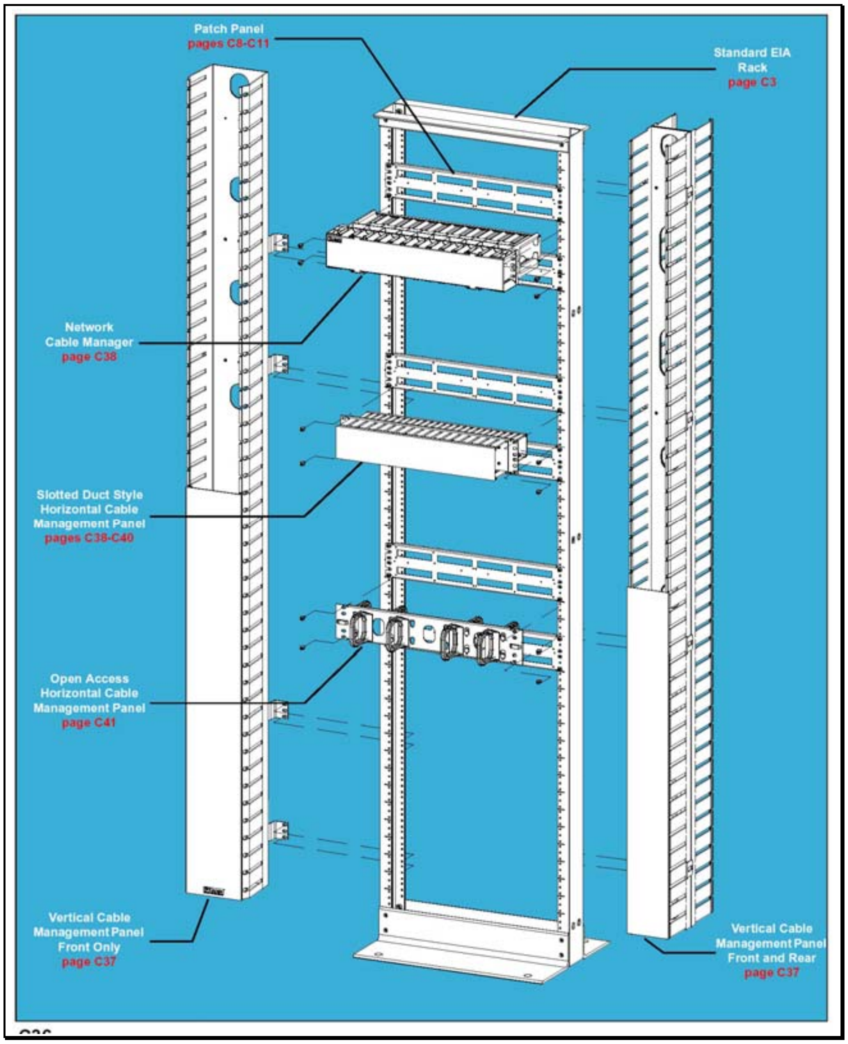

Figure [14]: Wire management trays on equipment racks (Photo courtesy of Panduit Corp)

Every cable that appears in the telecommunications room is identified according to the requirements of TIA/EIA-606-A standard for cable administration.

Keeping all of the incoming and outgoing cabling organized is a serious challenge. For this reason, wire management products, shown in Figure 14, have been developed.

A.3.2 Cable Labeling

Figure [15]: Cable label printer (Photo courtesy of Panduit Corp)

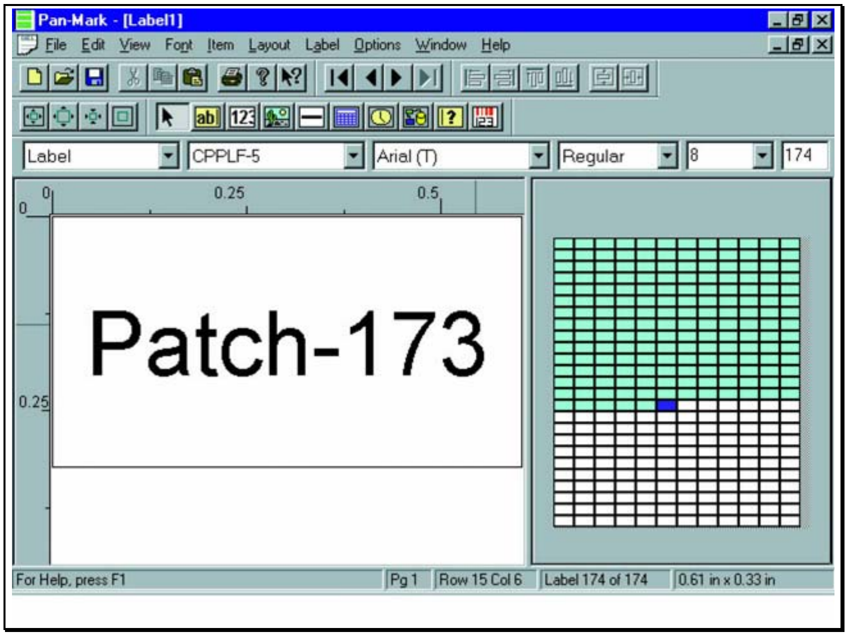

Figure [16]: An automated label printing program (Photo courtesy of Panduit Corp)

One key to identifying individual cables, as required by TIA/EIA-606-A is an efficient method of labeling and organizing. One very useful tool is a printer that will make multiple copies of a label. This makes it easy to mark a cable in more than one place, and most importantly, at both ends. Such a system is shown in Figure 15.

Another significant part of the labeling process is to develop a database that tracks which cables go where, and allows the facility to keep up with moves, adds, and changes. This program can output label data directly to a labeling software program, as shown in Figure 16.

A.3.3 Hand Cable Labeling

Figure [17]: Write-on labels (Photo courtesy of Panduit Corp)

The cable or wireless link that interconnects two BSSs is called the distribution system (DS). While TIA/EIA standards such as TIA/EIA-606-A require that every cable be labeled, wireless systems may evade such requirements if the installer is not careful. This happens when two distribution systems that connect two access points are wired together in such a way that neither of them passes through a telecommunications room, and the wires are not cataloged by the labeling scheme used by the network.

Situations such as this must be avoided. However, if the cable is installed and there is no one to authorize more appropriate routing, the installer should at least label it clearly so that the situation can be modified at a later time. A handy manual labeling tool is shown in Figure 17. This will allow the installer to create permanent, readable labels without having to locate automated labeling equipment.

A.4 External Antennas

A.4.1 External feed lines

Figure [18]: Fiber-optic labels (Photo courtesy of Panduit Corp)

Figure [19]: A rack grounding kit (Photo courtesy of Panduit Corp)

Many antennas are designed for external mounting. This creates three specific challenges for the installer:

- Weather protection
- Lightning protection
- Grounding considerations

Weather protection is a matter of keeping the coaxial cable sealed. If water gets in, it may not work, even after it dries.

Lightning protection is required because the metal portion of an external antenna can be a good lightning target. Lightning or static electricity can travel down the coaxial feed line and endanger internal equipment. Therefore, special care must be taken to ensure that coaxial cables are always properly grounded, and that lightning arrestors are used to dissipate harmful voltages. Some administrators attempt to isolate their equipment from harmful voltages by inserting a fiber-optic link in such a manner that the antenna and associated terminal equipment are isolated from each other. This fiber link can be marked as in Figure 18.

Grounding is always an important part of any telecommunications system. The equipment racks in a system should be bonded to ground, so as to avoid them becoming part of any ground loops that may form between equipment. A rack grounding kit is shown in Figure 19. This will contain all of the pieces required to electrically bond racks to each other and to the building ground.

Grounding and bonding for electrical and lightning protection is discussed in sections 100, 250, and 800 of the National Electrical Code (NEC) and similar documents in various countries. Grounding to address telecommunications performance issues are discussed in TIA/EIA-607-A, *Commercial Building Grounding and Bonding Requirements for Telecommunications*. Comparable standards documents exist for the ISO and CENELEC organizations.

Summary

Cable management, cable labeling, and bonding and grounding are necessary for WLANs. It is a requirement of the TIA/EIA standards that all cabling adhere to established guidelines.

Fortunately, there are suppliers who can make this task easier. Careful selection of the appropriate products will ensure standards compliance, provide a high degree of reliability, and minimize installation and maintenance effort.