CHAPTER 8

Installing a Physical Network

The Network+ Certification exam expects you to know how to

- 3.3 Identify the appropriate tool for a given wiring task (for example: wire crimper, media tester/certifier, punchdown tool, or tone generator)
- 4.3 Given a network scenario, interpret visual indicators (for example: link LEDs and collision LEDs) to determine the nature of a stated problem
- 4.7 Given a troubleshooting scenario involving a network with a particular physical topology (for example: bus, star, mesh, or ring) and including a network diagram, identify the network area affected and the cause of the stated failure

To achieve these goals, you must be able to

- Recognize and describe the functions of basic components in a structured cabling system
- Explain the process of installing structured cable
- Install a network interface card
- Perform basic troubleshooting on a structured cable network

In previous chapters, you toured the most common network technologies used in today's (and yesterday's) networks. At this point, you should be able to visualize a basic network setup. For bus topologies like 10Base2, visualize a cable running in a ceiling or along the floor with each PC connected somewhere along the bus. For star bus or star ring topologies like 10BaseT or Token Ring, visualize some type of box (hub, MSAU, or switch—whatever you like) with a number of cables snaking out to all of the PCs on the network (see Figure 8-1).

On the surface, such a network setup is absolutely correct, but if you tried to run a network using only a hub and cables running to each system, you'd have some serious practical issues. In the real world, you need to deal with physical obstacles like walls and ceilings. You also need to deal with those annoying things called *people*. People are incredibly adept at destroying physical networks! They can unplug hubs, trip over cables, and rip connectors out of NICs with incredible skill unless you protect the network from their destructive ways. Although the simplified hub-and-a-bunch-of-cables type of network we currently know would work in the real world, this simple network

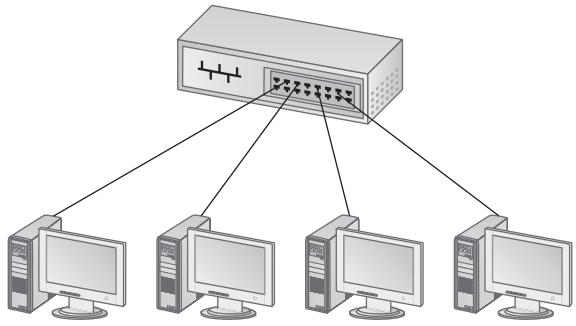


Figure 8-1 What an orderly looking network!

clearly has some problems that need addressing before it can work safely and efficiently (see Figure 8-2).

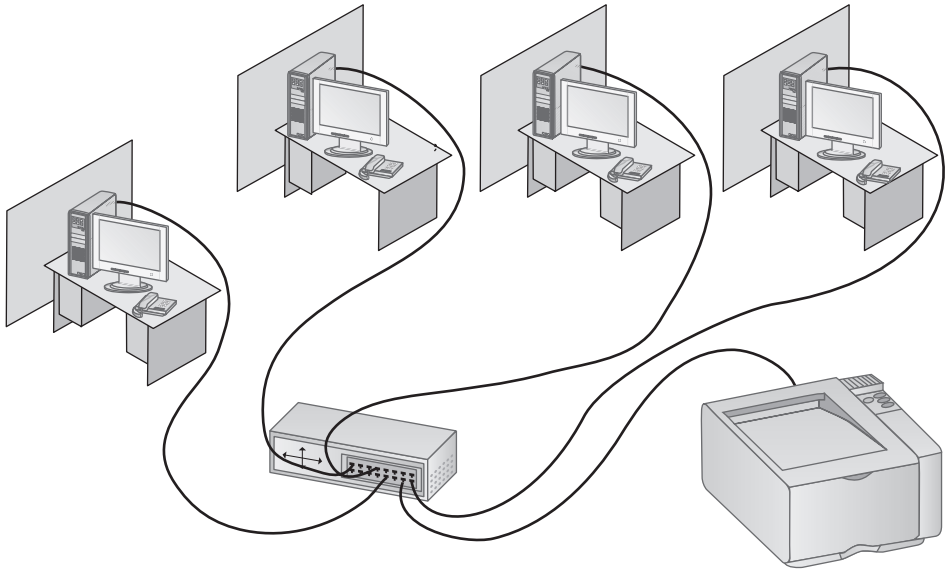


Figure 8-2 A real-world network

This chapter will take the abstract discussion of network technologies from previous chapters into the concrete reality of real networks. To achieve this goal, we'll be marching through the process of installing an entire network system from the beginning. To start, I'll introduce you to the magical world of *structured cabling*: the critical set of standards used all over the world to install physical cabling in a safe and orderly fashion. We'll then delve into the world of larger networks—those with more than a single hub—and see some typical methods used to organize them for peak efficiency and reliability.

Next, we'll take a quick tour of the most common NICs used in PCs, and see what it takes to install them. Finally, we'll look at how to troubleshoot cabling and other network devices—including an introduction to some fun diagnostic tools!

Historical/Conceptual

Structured Cabling

If you want a functioning, dependable, real-world network, you need a solid under standing of a set of standards, collectively called *structured cabling*. These standards, defined by the EIA/TIA (yup, the same folks who tell you how to crimp an RJ-45 onto the end of a UTP cable) give professional cable installers detailed standards on every aspect of a cabled network, from the type of cabling to use to the position of wall outlets. The Network+ exam requires you to understand the basic concepts involved in designing a network and installing network cabling, and to recognize the components used in a real network. Network+ does not, however, expect you to be as knowledgeable as a professional network designer or cable installer. Your goal is to understand enough about real-world cabling systems to support basic troubleshooting. Granted, by the end of this chapter, you'll have enough of an understanding to try running your own cable (I certainly run my own cable!), but consider that knowledge a handy bit of extra credit!

Cable Basics—A Star Is Born

With that goal in mind, let's explore the world of connectivity hardware, starting with the most basic of all networks: a hub, some UTP cable, and a few PCs—in other words, a typical physical star network (see Figure 8-3).

Okay, pop quiz! Is the network in Figure 8-3 a star bus or a star ring? Is it Token Ring, 100BaseT, or Gigabit Ethernet? Gotcha! It's a trick question—you can't tell from this picture. In fact, it could be any of these network technologies. If you have a 10BaseT network using CAT 5e cabling and you want to turn it into a Token Ring network, you simply replace the 10BaseT NICs in the PCs with RJ-45-equipped Token Ring NICs, and

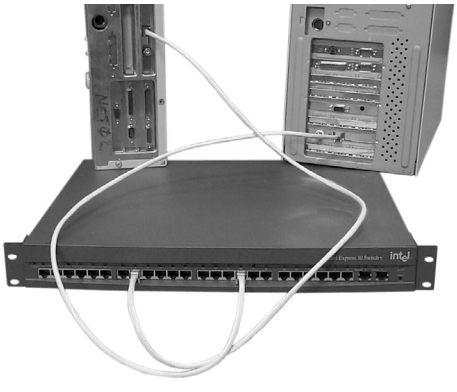


Figure 8-3
A hub connected by UTP cable to two PCs

the 10BaseT hub with a Token Ring MSAU. The cable would stay the same, because as far as the cabling is concerned, there is no difference between these topologies. The physical star does not need to change; only the logical portion—bus or ring—needs to change.

Does this ability to switch network technologies completely, yet keep the same cabling, surprise you? Many people find the idea of totally different network technologies like 10BaseT and Token Ring using the same cables somehow just not right. They think that because the network technology is different, the cabling should also be different. To those people I say, "Open your mind to the idea of cabling options!" If you went back in time 15 years, you'd find that pretty much every networking technology had its own type of cabling. Ethernet used RG-8 or RG-58, and Token Ring used Type 1 STP. Today, that is no longer the case. Over the years, UTP has edged out other cabling options to become the leading type of cabling used today. If an organization already has UTP cabling installed, they're not going to be interested in deploying a network technology that doesn't use UTP. If a network technology wants to thrive today, it must work with UTP. All new network technologies employ UTP, even the new Gigabit Ethernet standards!

NOTE The one exception to the use of UTP is fiber. It's not that much of an exception—almost all fiber network technologies from 10BaseFL to fiber-based Gigabit Ethernet use a star topology and the same type of fiber cable: 62.5/125 multimode.

Not only does UTP reign supreme, but all of today's network technologies run UTP in a physical star. This means that in today's networking world, you're almost always going to run into the same cabling situation: UTP in a physical star topology. Let's discuss the ramifications of the standard networking cabling scenario—the basic star—and see how the network technology industry evolved a bunch of cables running from the hub/switch to each computer into something more realistic.

NOTE Anyone who makes a trip to a local computer store sees plenty of devices that adhere to the 802.11 (wireless networking) standard. There's little doubt about the popularity of wireless. This popularity, however, is giving too many people the impression that 802.11 is pushing wired networks into oblivion. While this may take place one day in the future, wireless networks' unreliability and relatively slow speed (as compared to 100BaseT and Gigabit Ethernet) make it challenging to use in a network that requires high reliability and speed. Wireless makes great sense in homes, your local coffeehouse, and offices that don't need high speed or reliability, but any network that can't afford downtime or slow speeds still uses wires!

The Basic Star

No law of physics prevents you from installing a hub in the middle of your office and running cables on the floor to all the computers in your network. This setup will work, but it falls apart spectacularly when applied to the real-world environment. Three problems present themselves to the real-world network tech. First, the exposed cables run-

ning along the floor are just waiting for someone to trip over them, causing damage to the network and giving that person a wonderful lawsuit opportunity. Possible accidents aside, simply moving and stepping on the cabling will, over time, cause a cable to fail due to wires breaking or RJ-45 connectors ripping off cable ends. Second, the presence of other electrical devices close to the cable can create interference that confuses the signals going through the wire. Third, this type of setup limits your ability to make any changes to the network. Before you can change anything, you have to figure out which cables in the huge rat's nest of cables connected to the hub go to which machines. Imagine *that* troubleshooting nightmare!

"Gosh," you're thinking (okay, I'm thinking it, but you should be), "there must be a better way to install a physical network." A better installation would provide safety, protecting the star from vacuum cleaners, clumsy co-workers, and electrical interference. It would have extra hardware to organize and protect the cabling. Finally, the new and improved star network installation would feature a cabling standard with the flexibility to enable the network to grow according to its needs, and then to upgrade when the next great network technology comes along.

As you have no doubt guessed, I'm not just theorizing here. In the real world, the people who most wanted improved installation standards were the ones who installed cable for a living. In response to this demand for standards, the EIA/TIA developed standards for cable installation. The EIA/TIA 568 standards you saw in earlier chapters are only part of a larger set of EIA/TIA standards, all lumped together under the umbrella of structured cabling.

NOTE Installing structured cabling properly takes a startlingly high degree of skill. Thousands of pitfalls await inexperienced network people who think they can install their own network cabling. Pulling cable requires expensive equipment, a lot of hands, and the ability to react to problems quickly. Network techs can lose millions of dollars—not to mention their good jobs—by imagining they can do it themselves without the proper knowledge. If you are interested in learning more details about structured cabling, an organization called BICSI (www.bicsi.org) provides a series of widely recognized certifications for the cabling industry.

Structured Cable Network Components

Successful implementation of a basic structured cabling network requires three essential ingredients: an equipment room, horizontal cabling, and a work area. All the cabling runs from individual PCs to a central location, the *equipment room* (see Figure 8-4). What equipment goes in there—a hub, MSAU, or even a telephone system—is not the important thing. What matters is that all the cables concentrate in this one area.

All cables run horizontally (for the most part) from the equipment room to the PCs. This cabling is called, appropriately, *horizontal cabling* (see Figure 8-5). A single piece of installed horizontal cabling is called a *run*. At the opposite end of the horizontal cabling from the equipment room is the work area. The *work area* is often simply an office or cubicle that potentially contains a PC you want on the network (see Figure 8-6).

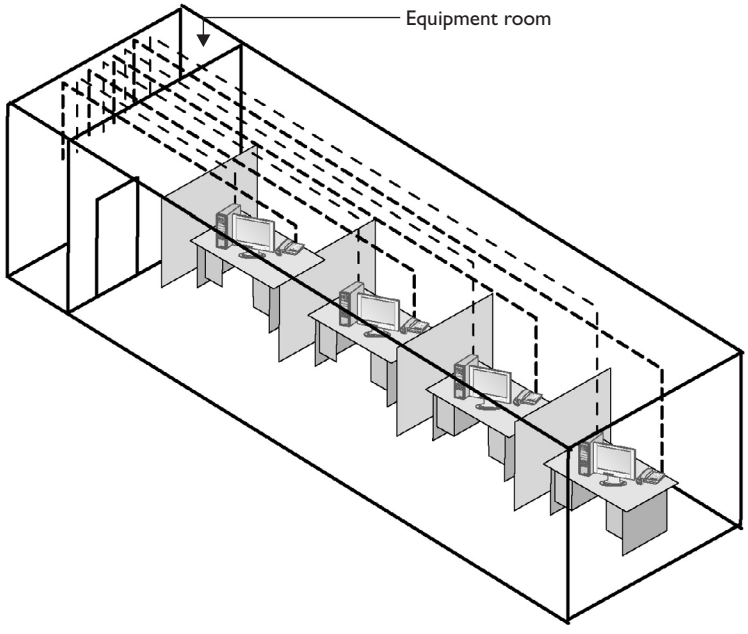


Figure 8-4 An equipment room

Each of the three parts of a basic star network—the horizontal cabling, the equipment room, and the work area(s)—must follow a series of strict standards designed to

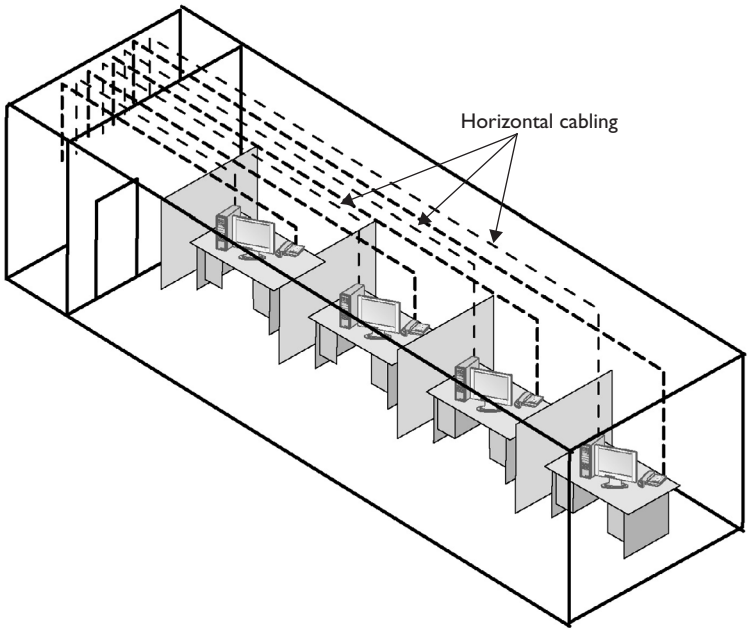


Figure 8-5 Horizontal cabling

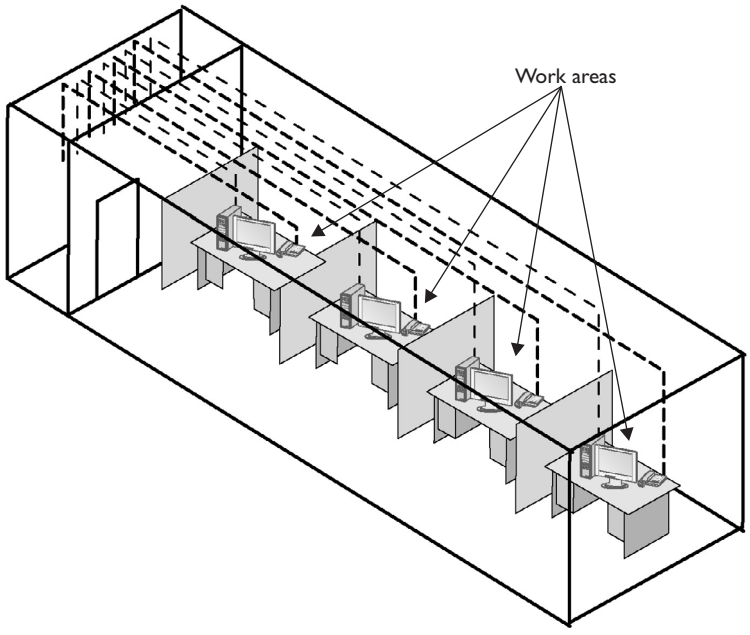


Figure 8-6
The work area

ensure that the cabling system is reliable and easy to manage. Let's look at each of the parts individually, starting with the horizontal cabling.

Horizontal Cabling

A horizontal cabling run is the cabling that goes more or less horizontally from a work area to the equipment room. In most networks, this is a CAT 5e or better UTP cable, but when we move into the world of structured cabling, the EIA/TIA standards require a number of other aspects to the cable, such as the type of wires, number of pairs of wires, and fire ratings.

TIP A single piece of cable that runs from a work area to an equipment room is called a run.

Solid Core vs. Stranded Core All UTP cable comes in one of two types: stranded core or solid core. Each wire in *solid core* UTP uses a single solid wire. With *stranded core*, each wire is a bundle of tiny wire strands. Each of these cable types has its benefits and downsides. Solid core is a better conductor, but it is stiff and will break if handled too often or too roughly. Stranded core is not quite as good a conductor, but it will stand up to substantial handling without breaking. Figure 8-7 shows a close-up of stranded and solid core UTP.

EIA/TIA specifies that horizontal cabling should always be solid core. Remember, this cabling is going into your walls and ceilings, safe from the harmful effects of shoes and

Figure 8-7 Stranded and solid core UTP

vacuum cleaners. The ceilings and walls enable us to take advantage of the better conductivity of solid core without risk of cable damage. Stranded cable also has an important function in a structured cabling network, but we need to discuss a few more parts of the network before we see where to use stranded UTP cable.

Number of Pairs Pulling horizontal cables into your walls and ceilings is a time-consuming and messy business, and not a process you want to repeat, if at all possible. For this reason, most cable installers recommend using the highest CAT rating you can afford. A few years ago, we would also mention that you should use four-pair UTP, but today, four-pair is assumed. Four-pair UTP is so common that it's difficult, if not impossible, to find two-pair UTP.

NOTE Unlike previous CAT standards, EIA/TIA defines CAT 5e and CAT 6 as four-pair-only cables.

Fire Ratings Did you ever see the movie *The Towering Inferno*? Don't worry if you missed it—*The Towering Inferno* was one of the better infamous disaster movies of the 1970s, but it was no *Airplane!* Anyway, Steve McQueen stars as the fireman who saves the day when a skyscraper goes up in flames because of poor-quality electrical cabling. The burning insulation on the wires ultimately spreads the fire to every part of the building. Although no cables made today contain truly flammable insulation, the insulation is made from plastic, and if you get any plastic hot enough, it will create smoke and noxious fumes. The risk of burning insulation isn't fire—it's smoke and fumes.

To reduce the risk of your network cables burning and creating noxious fumes and smoke, Underwriters Laboratories and the National Electrical Code (NEC) joined forces to develop cabling *fire ratings*. The two most common fire ratings are PVC and plenum. Cable with a *PVC (polyvinyl chloride)* rating has no significant fire protection. If you burn a PVC cable, it creates lots of smoke and noxious fumes. Burning *plenum*-rated cable creates much less smoke and fumes, but plenum-rated cable—often referred to simply as "plenum"—costs about three to five times as much as PVC-rated cable. Most city ordinances require the use of plenum cable for network installations. Bottom line? Get plenum!

The space between the acoustical tile ceiling in an office building and the actual concrete ceiling above is called the plenum—hence the name for the proper fire rating of cabling to use in that space. A third type of fire rating, known as *riser*, designates the proper cabling to use for vertical runs between floors of a building. Riser-rated cable provides less protection than plenum cable, though, so most installations today use plenum for runs between floors.

Choosing Your Horizontal Cabling In the real world, network people only install CAT 5e or CAT 6 UTP, even if they can get away with a lower CAT level. Installing rated cabling is done primarily as a hedge against new network technologies that may require a more advanced cable. Networking *caveat emptor* warning: many network installers take advantage of the fact that a lower CAT level will work on most networks, and bid a network installation using the lowest grade cable possible, so be sure to specify CAT 5e or even CAT 6 when soliciting bids for cable installation!

The Equipment Room

The equipment room is the heart of the basic star. This is where all the horizontal runs from all the work areas come together. The concentration of all this gear in one place makes the equipment room potentially one of the messiest parts of the basic star. Even if you do a nice, neat job of organizing the cables when they are first installed, networks change over time. People move computers, new work areas are added, network topologies are added or improved, and so on. Unless you impose some type of organization, this conglomeration of equipment and cables is bound to decay into a nightmarish mess.

Fortunately, the EIA/TIA's structured cabling standards define the use of specialized components in the equipment room that make organizing a snap. In fact, it might be fair to say that there are too many options! To keep it simple, we're going to stay with the most common equipment room setup, and then take a short peek at some other fairly common options.

Equipment Racks The central component of every equipment room is one or more equipment racks. *Equipment racks* provide a safe, stable platform for all the different hardware components. All equipment racks are 19 inches wide, but they vary in height. You'll see two- to three-foot-high models that bolt onto a wall, as well as to the more popular floor-to-ceiling models (see Figure 8-8).

You can mount almost any network hardware component into a rack. All manufacturers make rack-mounted hubs and switches that mount into a rack with a few screws. These hubs and switches are available with a wide assortment of ports and capabilities. There are even rack-mounted servers, complete with slide-out keyboards, and rack-mounted uninterruptible power supplies (UPSs) to power the equipment (see Figure 8-9).

Patch Panels and Cables Ideally, once you install horizontal cabling, it should never be moved. As you know, UTP horizontal cabling has a solid core, making it pretty stiff. Solid core cables can handle some rearranging, but if you insert a wad of solid core cables directly into your hubs, every time you move a cable to a different port on the hub, or move the hub itself, you will jostle the cable. You don't have to move a solid core

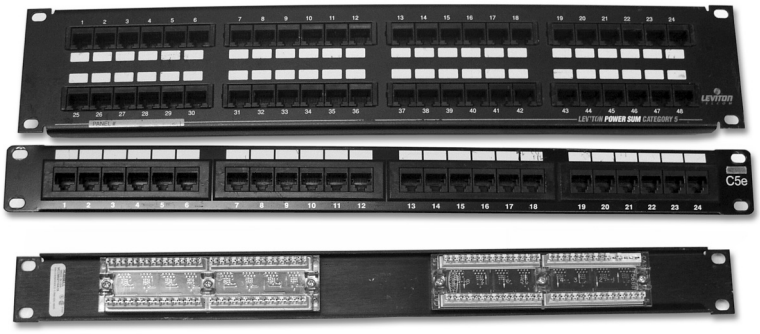
Figure 8-8 A bare equipment rack

Figure 8-9 A rack-mounted UPS

cable many times before one of the solid copper wires breaks, and there goes your network! Luckily for you, you can easily avoid this problem by using a patch panel. A *patch panel* is simply a box with a row of female connectors (ports) in the front and permanent connections in the back, to which you connect the horizontal cables (see Figure 8-10).

Not only do patch panels prevent the horizontal cabling from being moved, they are also your first line of defense in organizing the cables. All patch panels have space in the front for labels, and these labels are the network tech's best friend! Simply place a tiny label on the patch panel identifying each cable, and you will never have to experience that sinking feeling of standing in the equipment room of your nonfunctioning network, wondering which cable is which. If you want to be a purist, there is an official, and

Figure 8-10
Sample patch panels



rather confusing, EIA/TIA labeling methodology you can use; but most real-world network techs simply use their own internal codes (see Figure 8-11).

Figure 8-11
A labeled patch panel

NOTE The EIA/TIA 606 standard covers proper labeling and documentation of cabling, patch panels, and wall outlets. If you want to know how the pros label and document a structured cabling system, check out the EIA/TIA 606 standard.

Patch panels are available in a wide variety of configurations that include different types of ports and numbers of ports. You can get UTP, STP, or fiber ports, and some manufacturers combine several different types on the same patch panel. Panels are available with 8, 12, 24, 48, or even more ports. UTP patch panels, like UTP cables, come with CAT ratings, which you should be sure to check. Don't blow a good CAT 6 cable installation by buying a cheap patch panel—get a CAT 6 patch panel! Most manufacturers proudly display the CAT level right on the patch panel (see Figure 8-12).

Once you have installed the patch panel, you need to connect the ports to the hub through *patch cables*. Patch cables are short (two- to five-foot) UTP cables, similar to horizontal cabling (see Figure 8-13). Unlike horizontal cabling, patch cables use stranded rather than solid cable, so they can tolerate much more handling. Patch cables also differ from horizontal cables in their wiring scheme. EIA/TIA defines a straight-through

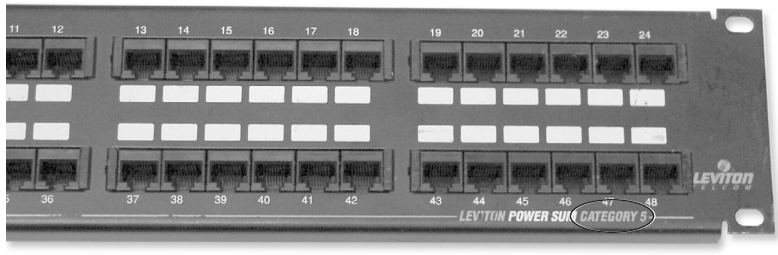


Figure 8-12 CAT level on patch panel

wiring for patch cables: Pin 1 on one connector goes to Pin 1 on the other; Pin 2 to Pin 2, and so on. Even though you can make your own patch cables, most people buy premade ones. Buying patch cables enables you to use different-colored cables to facilitate organization (yellow for accounting, blue for sales, or whatever scheme works for you). Most prefabricated patch cables also come with reinforced RJ-45 connectors specially designed to handle multiple insertions and removals.

Figure 8-13 Typical patch cables

An equipment room doesn't have to be a special room dedicated to computer equipment. You can use specially made cabinets with their own little built-in equipment racks that sit on the floor or attach to a wall, or use a storage room, as long as the equipment can be protected from the other items stored there. Fortunately, the demand for equipment rooms has been around for so long that most large office spaces come equipped with them.

At this point, our basic star installation is taking shape (Figure 8-14). We've installed the EIA/TIA horizontal cabling and configured the equipment room. Now it's time to address the last part of the structured cabling system: the work area.

The Work Area

What is a work area? From a cabling standpoint, a work area is nothing more than a wall outlet that serves as the termination point for horizontal network cables: a convenient insertion point for a PC. A wall outlet itself consists of a female jack to accept the cable, a mounting bracket, and a faceplate. You connect the PC to the wall outlet with a patch cable (Figure 8-15).

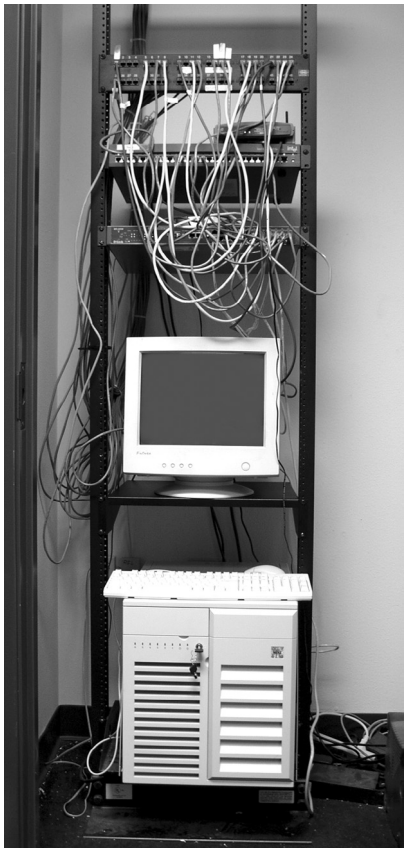


Figure 8-14
Complete medium-sized equipment room

Figure 8-15
A patch cable connecting a PC to an outlet

The female RJ-45 jacks in these wall outlets also have CAT ratings. You must buy CAT-rated jacks for wall outlets to go along with the CAT rating of the cabling in your network. In fact, many network connector manufacturers use the same connectors in the wall outlets that they use on the patch panels. These modular outlets significantly increase ease of installation. Make sure you label the outlet to show the job of each connector (see Figure 8-16). A good outlet will also have some form of label that identifies its position on the patch panel. Proper documentation of your outlets will save you an incredible amount of work later.

Figure 8-16 A typical wall outlet

The last step is connecting the PC to the wall outlet. Here again, most folks use a patch cable. Its stranded cabling stands up to the abuse caused by moving PCs, not to mention the occasional kick.

Now, my young apprentice, let us return to the question of why the EIA/TIA 568 specification only allows UTP cable lengths of 90 meters, even though most UTP networking technologies allow cables to be 100 meters long. Have you figured it out? Hint: the answer lies in the discussion we've just been having. Ding! Time's up! The answer is…the patch cables! Patch cables add extra distance between the hub and the PC, so EIA/TIA compensates by reducing the horizontal cabling length.

TIP Watch out for the word *drop*, as it has more than one meaning. A single run of cable from the equipment room to a wall outlet is often referred to as a drop. The word *drop* is also used to define a new run coming through a wall outlet that does not yet have a jack installed.

The work area may be the simplest part of the structured cabling system, but it is also the source of most network failures. When a user can't access the network and you suspect a broken cable, the first place to look is the work area!

Structured Cabling—Use It!

As you can see, EIA/TIA structured cabling methods transform the basic star from the cabling nightmare shown at the beginning of this discussion into an orderly and robust network. Sure, you don't have to do any of this to make a network function; you only have to do it if you want the network to run reliably and change easily with the demands of your organization. The extra cost and effort of installing a properly structured cabling

system pays huge dividends: you can avoid the nightmare scenario of having to find one bad cable in a haystack of unlabeled CAT 5, and you can protect the network from clumsy and/or clueless users.

Planning the Installation

A professional installer will begin a structured cabling installation by assessing your site and planning the installation in detail before a single piece of cable is pulled. As the customer, your job is to work closely with the installer. That means putting on old clothes and crawling along with the installer as he or she combs through your ceilings, walls, and closets. Even though you're not the actual installer, you must understand the installation process, so you can help the installer make the right decisions for your network.

Structured cabling requires a lot of planning. You need to know if the cables from the work areas can reach the equipment room—is the distance less than the 90-meter limit dictated by the EIA/TIA standard? How will you route the cable? What path should each run take to get to the wall outlets? Don't forget that just because a cable looks like it will reach, there's no guarantee that it will! Ceilings and walls often include nasty hidden surprises like firewalls—big, thick, concrete walls designed into buildings that require a masonry drill or a jackhammer to punch through. Let's look at the steps that go into proper planning.

Get a Floor Plan

First, you need a blueprint of the area. If you ever contract an installer and they don't start by asking for a floor plan, fire them immediately and get one who does! The floor plan is the key to proper planning; a good floor plan shows you the location of closets that could serve as equipment rooms, alerts you to any firewalls in your way, and gives you a good overall feel for the scope of the job ahead.

If you don't have a floor plan—and this is often the case with homes or older buildings—you'll need to create your own. Go get a ladder and a flashlight—you'll need them to poke around in ceilings, closets, and crawl spaces as you map out the location of rooms, walls, and anything else of interest to the installation. Figure 8-17 shows a typical do-it-yourself floor plan, drawn out by hand.

Map the Runs

Now that you have your floor plan, it's time to map the cable runs. Here's where you run around the work areas, noting the locations of existing or planned systems to determine where to place each cable drop. A *cable drop* is the location where the cable comes out of the wall. You should also talk to users, management, and other interested parties to try and understand their plans for the future. It's much easier to install a few extra drops now than to do it a year from now when those two unused offices suddenly find themselves with users who immediately need networked computers!

This is also the point where the nasty word "cost" first raises its ugly head. Face it: cables, drops, and the people who install them cost money! The typical price for a network

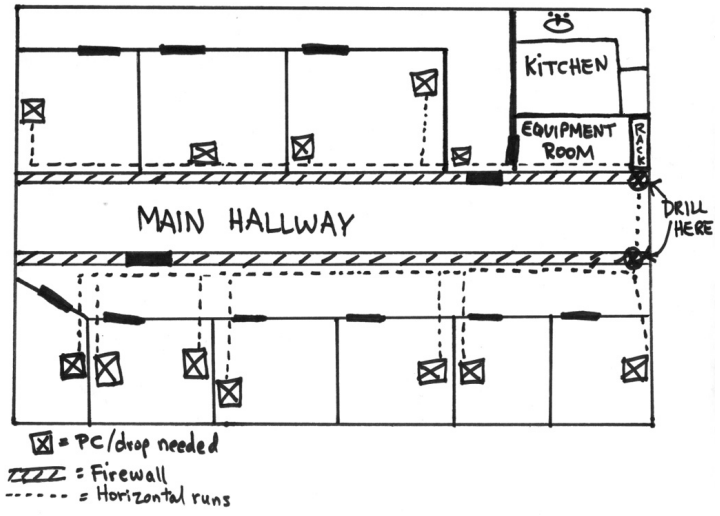


Figure 8-17 Hand-drawn network floor plan

installation is around US $150 per drop. Find out how much you want to spend and make some calls. Most network installers price their network jobs by quoting a "per drop" cost.

Inside or Outside the Walls?

While you're mapping your runs, you have to make another big decision: Do you want to run the cables in the walls or outside them? Many companies sell wonderful external raceway products that adhere to your walls, making for a much simpler, though less neat, installation than running cables in the walls (see Figure 8-18). Raceways make good sense in older buildings, or when you don't have the guts or the rights to go into the walls.

Figure 8-18 A typical raceway

Even though I said you can run cables through a raceway, let's face it: most of us prefer the nice little outlets with the wires running in the walls. Once we finish mapping the runs, we'll see just what that takes.

The Equipment Room While mapping the runs, you should decide on the location of your equipment room. When deciding on this location, keep five issues in mind: distance, power, dryness, coolness, and access.

- **Distance** The equipment room must be located in a spot that won't require cable runs longer than 90 meters. In most locations, keeping runs under 90 meters requires little effort, as long as the equipment room is placed in a central location.
- **Power** Many of the components in your equipment room need power. Make sure you provide enough! If possible, put the equipment room on its own dedicated circuit; that way, when someone blows a circuit in the kitchen, it doesn't take out the entire network.
- **Dryness** I imagine this one is obvious. Electrical components and water don't mix well. (Remind me to tell you about the time I installed a rack in an abandoned bathroom, and the toilet that later exploded.) Remember that dryness also means low humidity. Avoid areas with the potential for high humidity, such as a closet near a pool or the room where the cleaning people leave mop buckets full of water. Of course, any well air-conditioned room should be fine—which leads to the next big issue….
- **Coolness** Equipment rooms tend to get warm, especially if you add a couple of server systems and a UPS. Make sure your equipment room has an air-conditioning outlet or some other method of keeping the room cool. Figure 8-19 shows how I installed an air-conditioning duct in my small equipment closet. Of course, I did this only after I discovered that the server was repeatedly rebooting due to overheating!

Figure 8-19 An A/C duct cooling an equipment closet

- **Access** Access involves two different issues. First, it means preventing unauthorized access. Think about the people you do and don't want messing around with your network, and act accordingly. In my small office, the equipment closet literally sits eight feet from me, so I don't concern myself too much with unauthorized access. You, on the other hand, may want to consider placing a lock on the door of your equipment room if you're concerned that unscrupulous or unqualified people might try to access it. Figure 8-20 shows what happened to my equipment room when I allowed access to it!

Figure 8-20 Equipment room taken over by mops, brooms, and trash

The second access consideration is making sure the people who need to get at your equipment to maintain and troubleshoot it can do so. Take a look at my equipment room in Figure 8-21. Here's a classic case of not providing good access. Note how difficult it would be for me to get to the back of the server—I would literally need to pull the server out to check cables and NICs!

Figure 8-21 A server wedged into a closet

One other issue to keep in mind when choosing your equipment room is expandability. Will this equipment room be able to grow with your network? Is it close enough to be able to service any additional office space your company may acquire nearby? If your company decides to take over the floor above you, can you easily access another equipment room on that floor from this room? While the specific issues will be unique to each installation, keep thinking "expansion" as you design—your network will grow, whether or not you think so now!

Most equipment rooms require a floor-mounted equipment rack, but you do have other options. One option is a shorter rack, like the wall-mounted one shown in Figure 8-22.

Figure 8-22
A wall-mounted short rack

Serious equipment racks such as these must be mounted to the floor or the wall, usually with big concrete fasteners or other heavy-duty hardware. Installing a rack properly is a big job, and one I never do myself. A small network can dispense with a rack altogether and use a simple wall-mounted patch panel like the one shown in Figure 8-23.

NOTE All racks use a unique height measurement called units, or U. One U equals 1.75 inches. When you purchase a rack, its height will be listed in terms of U, for example 44U. All rack-mounted equipment uses the U measurement; it's common to see rack-mounted servers, hubs, and patch panels with U dimensions, such as 2U (3.5 inches) or 4U (7 inches).

So, you've mapped your cable runs and established your equipment room—now you're ready to start pulling cable!

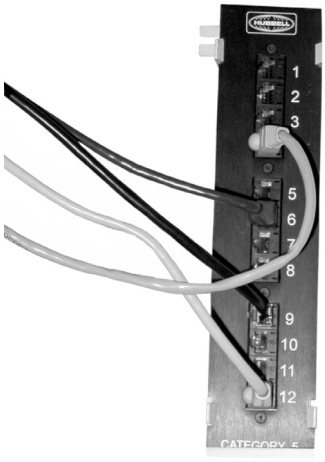


Figure 8-23
A wall-mounted patch panel

Installing the Cable

Pulling cable is easily one of the most thankless and unpleasant jobs in the entire networking world. It may not look that hard from a distance, but the devil is in the details. First of all, pulling cable requires two people if you want to get the job done quickly; three people are even better. Most pullers like to start from the equipment room and pull toward the drops. The pullers draw cable from a reel—many using a handy reel spindle to help the reel turn easily. In an office area with a drop ceiling, pullers will often feed the cabling along the run by opening ceiling tiles and stringing the cable along the top of the ceiling. Professional cable pullers have an arsenal of interesting tools to help them move the cable horizontally, including telescoping poles, special nylon pull ropes, and even nifty little crossbows and pistols that can fire a pull rope long distances! Figure 8-24 shows a tech pulling cable.

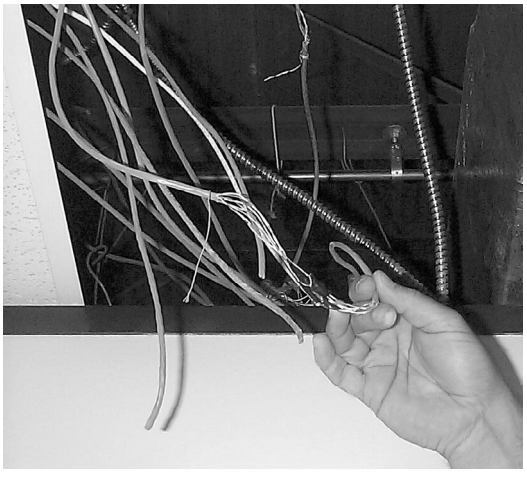


Figure 8-24
A tech pulling cable

Professional installers no longer simply dump cabling onto the top of a drop ceiling. A previous lack of codes or standards for handling cables led to a nightmare of disorganized cables in drop ceilings all over the world. Any cable puller will tell you that the hardest part of installing cables is the need to work around all the old cable installations in the ceiling! (See Figure 8-25.)

Figure 8-25
My buddy Roger Conrad working in a messy ceiling

Local codes, the EIA/TIA, and the NEC all have strict rules about how you pull cable in a ceiling. A good installer will use either hooks or trays, which provide better cable management, safety, and protection from electrical interference (see Figure 8-26). The faster the network, the more critical good cable management becomes. You probably won't have a problem laying UTP directly on top of a drop ceiling if you just want a 10BaseT network, and you might even get away with this for 100BaseT—but forget about doing this with Gigabit. Cable installation companies are making a mint from all the CAT 5 and earlier network cabling installations that need to be redone to support Gigabit Ethernet.

Figure 8-26
Cable trays above a drop ceiling

Running cable horizontally requires relatively little effort, compared to running the cable down from the ceiling to a pretty faceplate at the work area, which often takes a lot of skill. In a typical office area with sheetrock walls, the installer first decides on the position for the outlet, usually using a stud finder to avoid cutting on top of a stud. Once the worker cuts the hole (see Figure 8-27), most installers drop a line to the hole using a weight tied to the end of a nylon pull rope (see Figure 8-28). They can then attach the network cable to the pull rope and pull it down to the hole. Once the cable is pulled through the new hole, the installer puts in an outlet box or a low-voltage *mounting bracket* (see Figure 8-29). This bracket acts as a holder for the faceplate.

Figure 8-27
Cutting a hole

Figure 8-28
Dropping a weight

Figure 8-29
Installing a low-voltage mounting bracket

Back in the equipment room, the many cables leading to each work area are consolidated and organized in preparation for the next stage: making connections. A truly professional installer takes great care in organizing the equipment closet. Figure 8-30 shows a typical installation using special cable guides to bring the cables down to the equipment rack.

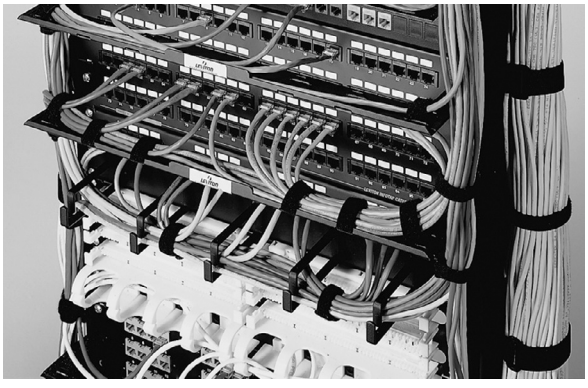


Figure 8-30 Cable guides help organize the equipment closet.

Making Connections

As the name implies, making connections consists of connecting both ends of each cable to the proper jacks. This step also includes the most important step in the entire process: testing each cable run to ensure that every connection meets the requirements of the network that will use it. Installers also use this step to document and label each cable run—a critical step too often forgotten by inexperienced installers, and one you need to verify takes place!

Connecting the Work Areas

Let's begin by watching an installer connect a cable run. In the work area, that means the cable installer will now crimp a jack onto the end of the wire and mount the faceplate to complete the installation (see Figures 8-31 and 8-32).

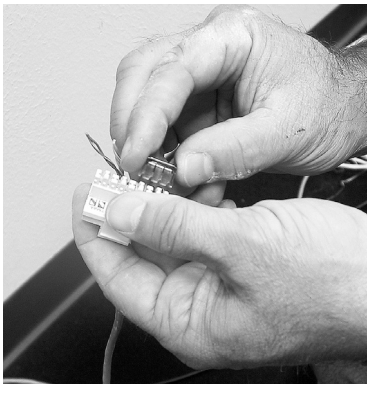


Figure 8-31 Attaching a jack to the wire

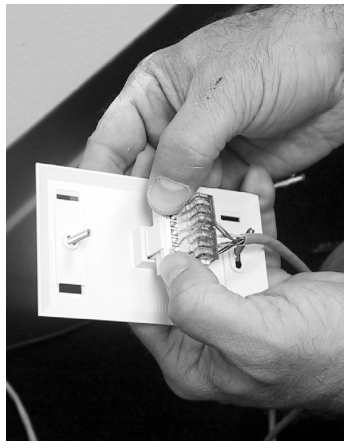


Figure 8-32 Fitting the jack into a faceplate

Note the back of the jack shown in Figure 8-31. This jack uses the popular *110-punchdown* connection. Other jack makers may use different types, but the 110 is the most common. Most 110 connections have a color code that tells you which wire to punch into which connection on the back of the jack. We use a special 110-punchdown tool to make these connections (see Figure 8-33).

Figure 8-33 The 110-punchdown tool

Connecting the Patch Panels

Connecting the cables to patch panels requires you to deal with two issues. The first is patch cable management. Figure 8-34 shows the front of a small network's equipment rack—note the complete lack of cable management! This one is so messy, I challenge you to find the patch panels and the hubs. (Hint: The hubs are in the center of the picture.) Managing patch cables means using the proper cable management hardware. Plastic D-rings guide the patch cables neatly along the sides and front of the patch panel. Finger boxes are rectangular cylinders with slots in the front; the patch cables run into the open ends of the box, and individual cables are threaded through the fingers on their way to the patch panel, keeping them neatly organized. Creativity and variety abound in the world of cable-management hardware—there are as many different

solutions to cable management as there are ways to screw up organizing them. Figure 8-35 shows a rack using good cable management—these patch cables are well secured using cable-management hardware, making them much less susceptible to damage from mishandling. Plus, it looks much nicer!

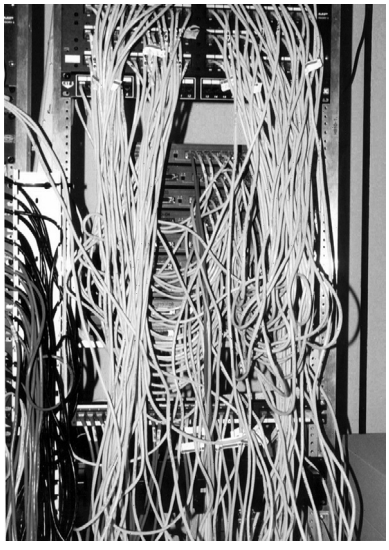


Figure 8-34 Bad cable management

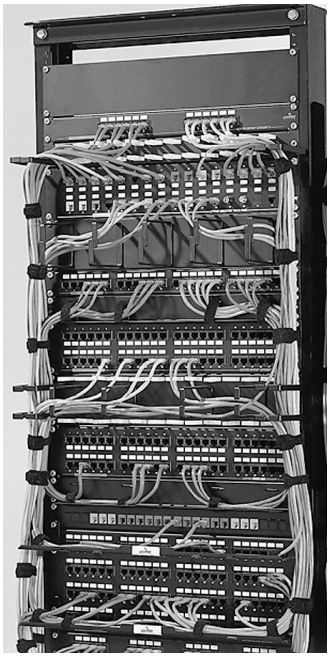


Figure 8-35 Good cable management

The second issue to consider when connecting cables is the overall organization of the patch panel as it relates to the organization of your network. Organize your patch panel so that it mirrors the layout of your network. You can organize according to the physical layout, so the different parts of the patch panel correspond to different parts of your office space—for example, the north and south sides of the hallway. Another popular way to organize patch panels is to make sure they match the logical layout of the network, so the different user groups or company organizations have their own sections of the patch panel.

Labeling the Cable

Even if your installer doesn't use an official EIA/TIA 606 labeling scheme, you still must label your runs. Design a labeling scheme that matches your network's organization—for example, you could have all the connections on the north side of the building start with the letter *N* followed by a three-digit number starting with 001. After you have a labeling scheme—this part is critical!—you must *use it*. When you make a network connection, label the outlet at the work area and the jack on the patch panel with the same number. Figure 8-36 shows a typical equipment rack with a number of patch panels—a common setup for a small network. In this case, both the color of the patch cables and their placement on the panels tell you where they belong in the network.

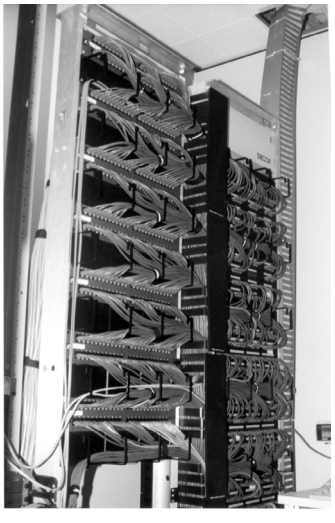


Figure 8-36 Well-organized patch panels

You must label, but you don't have to organize to this degree. In fact, many network installers choose not to, because they feel it wastes ports on the patch panel. What happens if one side of the network grows beyond the number of assigned ports, while the other side gets smaller? My answer: Get another patch panel. Other techs prefer to fill up the existing patch panels, even if it muddies their organizational scheme. This is a matter of personal choice, of course. Whatever the labeling scheme, only one thing matters. The

most important part of labeling is that both ends of a given cable say the same thing. Figure 8-37 shows some labels on a typical patch panel.

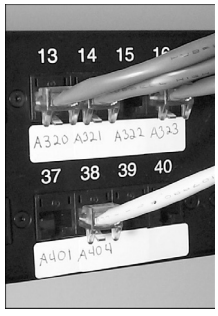


Figure 8-37
Labels on a patch panel

Take a look at the wall outlet in Figure 8-38. Note that the label on the outlet corresponds to the label on the patch panel in Figure 8-37. Failure to include this one simple step creates more problems than you can imagine. Good network installers always label the runs in this manner, not to mention a lot of other labeling that users do not see, such as labeling on the cable inside the wall. Proper labeling can save you from many potential disasters. Here's a classic example: John wants to install a second networked system in the unused office next door. He sees that the unused office has a network outlet, but he wants to make sure the wall outlet connects to the network hub. His problem: he can't determine which port on the patch panel he needs to use. Sure, he could guess, or use a special tool called a toner (we'll get to that later), but think how much faster it would be if all he had to do was read the label on the outlet and find the corresponding label on the patch panel! Make your life simpler than John's—label your patch panels and outlets.

Figure 8-38
Label on an outlet

Test Specific

Testing the Cable Runs

Well, in theory, your cabling system is now installed and ready for a hub and some systems. Before you do this, though, you must test each cable run. Someone new to testing cable might think that all you need to do is verify that each jack has been properly connected. While this is an important and necessary step, the interesting problem comes after that: verifying that your cable run can handle the speed of your network.

Before we go further, let me be clear: a typical network admin/tech cannot properly test a new cable run. The EIA/TIA provides a series of incredibly complex and important standards for testing cable. Unless you want to get into a 75-page discussion of things like near-end crosstalk and the attenuation-to-crosstalk ratio, this is an area where employing a professional cable installer makes sense. The testing equipment alone totally surpasses the cost of most smaller network installations! Advanced network testing tools easily cost over $5000, and some are well over $10,000! Never fear, though—a number of lower-end tools work just fine for basic network testing. Let's look at some of them.

NOTE These tools are also used to diagnose network problems.

The best tool to start with is the cable tester. *Cable testers* perform a wide variety of functions, and can diagnose all manner of problems with the cabling. Most network admin types staring at a potentially bad cable want to know the following:

- How long is this cable?
- Are any of the wires broken?
- If there is a break, where is it?
- Are any of the wires shorted together?
- Are any of the wires not in proper order (in other words, are there split or crossed pairs)?
- Is there electrical or radio interference?

Various models of cable testers are designed to answer some or all of these questions, depending on the amount of money you are willing to pay. At the low end of the cable tester market are devices that only test for broken wires. A wire that can conduct electricity is said to have *continuity*; thus, a broken wire lacks continuity. These cheap (under $100) testers are often called continuity testers (see Figure 8-39). Some cheaper cable testers will also test for split or crossed pairs and for shorts. These cheap testers usually require you to insert both ends of the cable into the tester. Of course, this can be a bit of a problem if the cable is already installed in the wall!

Medium price testers (≈ $400) have the additional capability to determine the length of a cable, and can even tell you where a break is located. This type of cable tester (see Figure 8-40) is generically called a *Time Domain Reflectometer (TDR)*. A medium-priced tester will have a small loopback device that gets inserted into the far end of the cable, enabling the tester to work with installed cables. This is the type of tester you want to have around!

If you want a device that can test the electrical characteristics of a cable, the price shoots up fast. These professional devices test critical EIA/TIA electrical characteristics, and are used by professional installers to verify installations. These are generally known

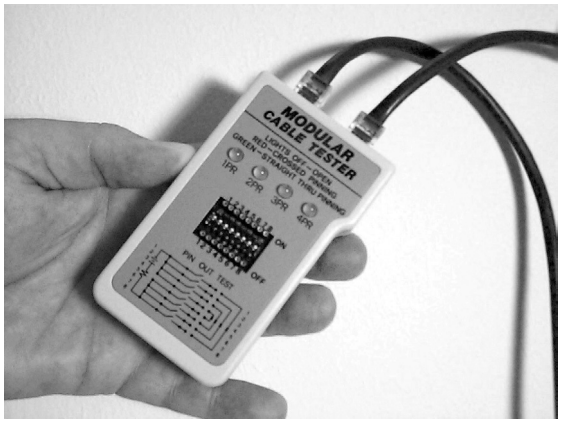


Figure 8-39
A simple cable tester

Figure 8-40
A typical medium-priced TDR—a Microtest Microscanner

as *media certifier tools*, as they generate a report that the installer can then print and hand to you as certification to prove that your cable runs pass EIA/TIA standards. Some of these high-end devices have powerful added features, such as the capability to plug into a network and literally draw a schematic of the entire network for you, including neat information like the MAC addresses of the systems, IP or IPX addresses, and even the operating system for each computer. Figure 8-41 shows an example of this type of scanner made by Microtest (www.microtest.com). These advanced testers are more than most network techs need, so unless you have some deep pockets or find yourself doing serious cable testing, stick to the medium-priced testers.

Getting Physical

The process of installing a structured cabling system is rather involved, requires a great degree of skill, and should be left to professionals. However, by understanding the

Figure 8-41 A typical media certifier—a Microtest OMNIScanner

process, you'll find you're able to tackle most of the problems that come up in an installed structured cabling system. Make sure you're comfortable with the components of structured cabling!

Beyond the Basic Star

The basic single hub with star configuration only works acceptably in the simplest networks. In the real world, networks tend to have many hubs, and often span floors, buildings, states, and even countries. Starting with the basic star, and using structured cabling where applicable, you can progress beyond that rudimentary configuration using certain equipment and strategies designed for larger, more advanced, and more efficient networks.

To see the many ways we can progress beyond the basic star, let's look at an example. The Bayland Widget Corporation's network has three 10BaseT hubs. Each hub serves a different department: hub *A* is for accounting, hub *B* is for sales, and hub *C* is for manufacturing. Bayland's clever network tech has connected the three hubs, enabling any system on any of the three hubs to communicate with any other system on any of the three hubs (see Figure 8-42).

Switched Networks

As you add PCs to a 10BaseT network, your network traffic will increase. As network traffic increases, your users will begin to experience a perceptible slowdown in network

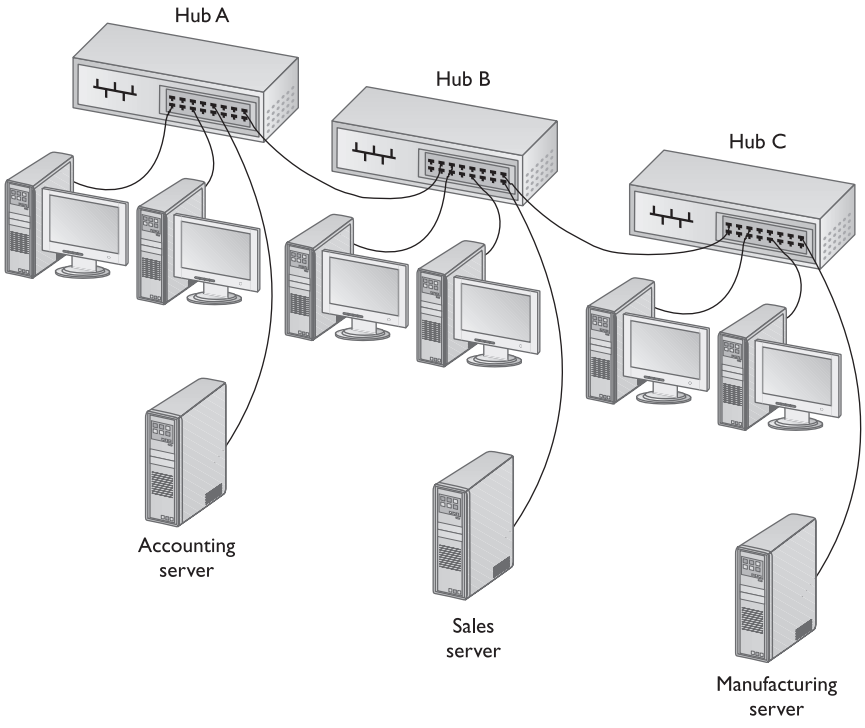


Figure 8-42 Bayland Widget Corporation's three cascaded 10BaseT hubs

performance. One of the fastest and cheapest hardware solutions for too much traffic on any star-bus Ethernet network is the addition of a switch. To switch (sorry, the pun was just hanging there!) to a switched 10BaseT network, simply remove a hub and replace it with a switch. You don't have to do anything to the cards or the cabling.

Like hubs, switches come in a dizzying variety of shapes and sizes. As you might have guessed, companies that make hubs tend to make switches, too, most of which use the same casing for equivalent hubs and switches. In fact, from 20 feet away, an equivalent hub and switch look identical. Figure 8-43 shows an Intel small office hub next to a small office switch; note that they are virtually identical.

In the past, switches were tremendously more expensive than hubs, but in the last few years, the price of switches has dropped immensely—from thousands of dollars to mere hundreds. Small eight-node switches are available at your local computer store for under $100. With the dramatic price drop, the switch has moved from a luxury technology to a standard part of all networks.

So, now you can buy a switch without selling your house to pay for it, but what do you do with it once you have it? You have many possibilities, depending on the type of network you have, but odds are you'll want to choose between two common implementation

Figure 8-43 Switches and hubs look the same.

strategies. The first option is to switch everything—forget about plain hubs and connect everything to a switch. The second option is to use the switch as a bridge between hubs. Let's look at both of these options, using Bayland Widget as the example.

Bayland's network has three hubs, each of which you can replace with a switch. This eliminates the collision domain problem: with three cascaded hubs, the packets sent from any PC go to all the other PCs on all three hubs, raising the likelihood of collisions. Because switches direct each packet only to the specified recipient PC, no collisions occur (after the switch determines the MAC addresses and creates a direct connection between the two computers). This is wonderful because it means that every connection runs at the full potential speed of the network—in this case, the full 10 Mbps of a 10BaseT network. Remember, the moment you start using switches, you can throw the 5-4-3 rule out the window!

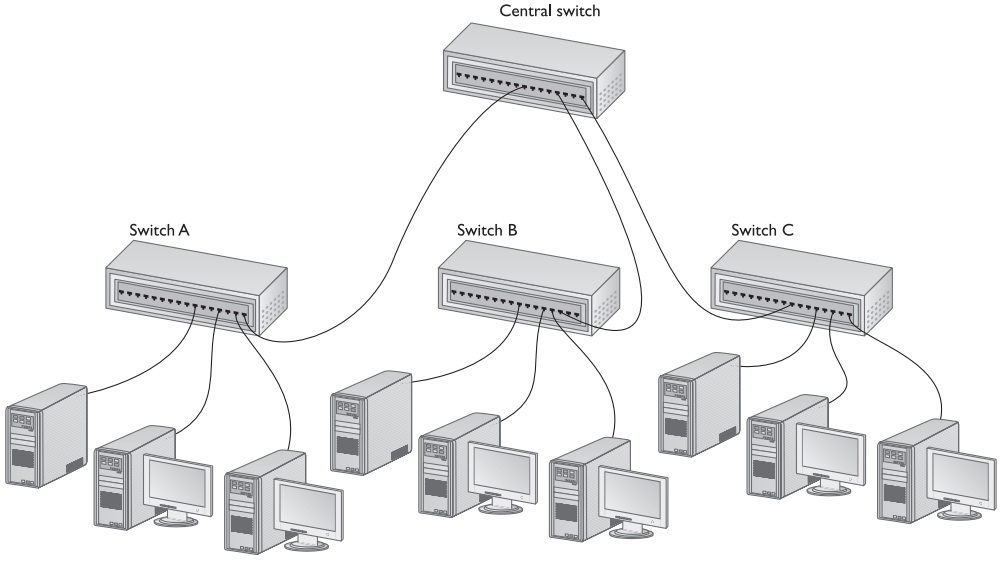


Figure 8-44 Bayland's network with three switches installed

Multispeed Networks

In the networking world, the fastest technology isn't always the best. My office uses a 100BaseT network. Even though Gigabit Ethernet is available with relatively inexpensive switches and NICs, the CAT 5 cable in our network simply was installed too poorly to handle it. The RJ-45 jacks were poorly crimped at the wall outlets and the horizontal cabling was laid too close to my fluorescent lights, so I'd need to replace all my structured cabling. The work we do is such that the vast majority of the users on the network wouldn't even notice the extra speed of Gigabit Ethernet. Computers that cruise the Web, pull down e-mail, and transfer an occasional Word document barely make use of 100-megabit connections, let alone gigabit! On the other hand, my hard-working servers handle almost 50 times as much traffic as my workstations, so they would benefit dramatically from a speed increase. How can I make my servers run at Gigabit Ethernet speeds, while my regular PCs run on 100BaseT?

The secret lies in a class of switches called *multispeed* switches. Multispeed switches come in two types. One type is a switch with some number of—for example—100BaseT ports. To the side of those ports lie one or two Gigabit ports. I can snap Gigabit Ethernet cards into my servers, and then plug those servers directly into the Gigabit ports (Figure 8-45).

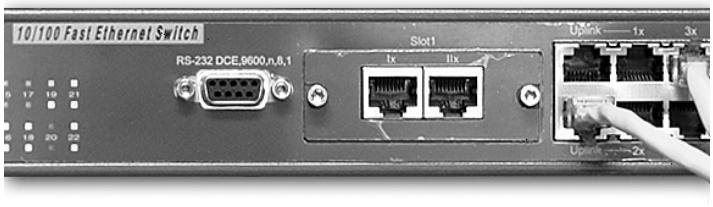


Figure 8-45 High-speed ports on a multispeed switch

With the second type of multispeed switch, every port is capable of running at more than one speed. Figure 8-46 shows the link lights for the primary switch in my office. Every port on the switch can run at either 10 or 100 Mbps. These ports are *autosensing*; this means that when you connect a cable into any port, the port will detect the speed of the NIC on the other end of the cable and run at that speed. An autosensing port that runs at either 10 or 100 Mbps is referred to as a 10/100 port. A port that runs at 10, 100, or Gigabit is often referred to as a 10/100/1000 port.

Figure 8-46 Multispeed port lights on a multispeed switch

You'll also find switches that combine both of the types just described. For example, I have a switch with 24 multispeed 10/100 ports and two Gigabit ports.

NOTE Is there such a thing as a multispeed hub? Sure, there have been multispeed hubs, but today they're so rare that we consider them obsolete.

Multispeed networks are incredibly common, as they provide an easy way to support a few systems that need a high-speed connection, while also supporting lower-speed systems. Another big benefit to multispeed networks is that you can use the high-speed ports on one switch to interconnect other high-speed ports on other multispeed switches. This creates a special, separate, high-speed segment called a *backbone* that acts as the primary interconnection for the entire network. Backbones are popular in larger networks where systems are separated by floors and buildings. Let's talk about larger networks and see how backbones fit into this picture.

Multiple Floors, Multiple Buildings

Once you begin to expand a network beyond the basic star configuration by adding more hubs and switches, new demands arise. These can be summarized in a single statement: as networks grow, they take up more space! Adding significantly more PCs to a network usually implies adding more offices, cubicles, and other work areas. Adding work areas means adding more switches and hubs in more equipment rooms.

As a general rule, networks use one equipment room per floor. If the room is centrally located in the building, cabling within the 90-meter limit will completely cover the floor space in most buildings. If your office has work areas on more than one floor, you essentially now have multiple networks on multiple floors. This is a classic example of the need for a backbone network. Backbones tie all the floors together with a robust, high-speed network fast enough to support the demands of combined networks.

Enlarging a network usually also means adding more servers to handle the increased demand. As more servers are added to the network, the administrators who tend to them will find it more efficient to group mission-critical servers together in a single computer room. A computer room not only provides enhanced safety and security for expensive hardware, it also enables administrators to handle daily support chores like backups more efficiently. Bottom line: the larger the network, the larger the space needed to support it, and the more complex your network infrastructure will be.

The concept of structured cabling extends beyond the basic star. EIA/TIA provides a number of standards, centered on EIA/TIA 568 and another important EIA/TIA standard, EIA/TIA 569. These standards address cabling configuration and performance specifications (568), and cable pathways and installation areas (569) involving multiple equipment rooms, floors, and buildings. Slightly simplified, EIA/TIA's view of structured cabling in larger networks breaks down into six main components: the equipment room, the horizontal cabling, the work areas, the backbone, the building entrance, and the telecommunication closets. The first three were discussed earlier and perform the same roles in a more complex network as in a basic star, so I'll concentrate on the last three.

NOTE Don't bother memorizing these terms. Network+ is not going to quiz you on naming the six components of structured cabling. Do make it a point to understand the equipment required for each of these components, and how the different parts interrelate.

Backbones and Building Entrances

When you split a network into multiple floors or buildings, a common practice is to interconnect those floors or buildings with a single high-speed segment—a classic example of a backbone. EIA/TIA specifies using UTP or fiber-optic cable for backbones. While any cable that meets the criteria for a backbone can certainly serve as a backbone cable, EIA/TIA conceives of backbones more as cables that vertically connect equipment rooms (often called risers) or horizontally connect buildings (interbuilding cables).

EIA/TIA provides some guidelines for backbone cable distances, but the ultimate criterion for determining cable length is the networking technology used. Most riser backbones use either copper or fiber-optic cables. Because of its imperviousness to electrical interference, fiber-optic is the only cabling you should use for interbuilding connections (see Figure 8-47).

Figure 8-47 Fiber-optic backbone cables connecting into hubs

The *building entrance* is where all the cables from the outside world (telephone lines, cables from other buildings, and so on) come into a building (see Figure 8-48). EIA/TIA specifies exactly how the building entrance should be configured, but we're not interested in the building entrance beyond knowing that fiber-optic cable should be used between buildings.

Complexity Is Cool!

As networks grow beyond the basic star, they will also grow in complexity. A large network that is switched, multispeed, and multifloored requires a substantial time investment for proper management and support. Those who take the time to understand their large networks find a beauty—or as Bill Gates would say, an *elegance*—that stems from a well-running large network. Complexity is definitely cool!

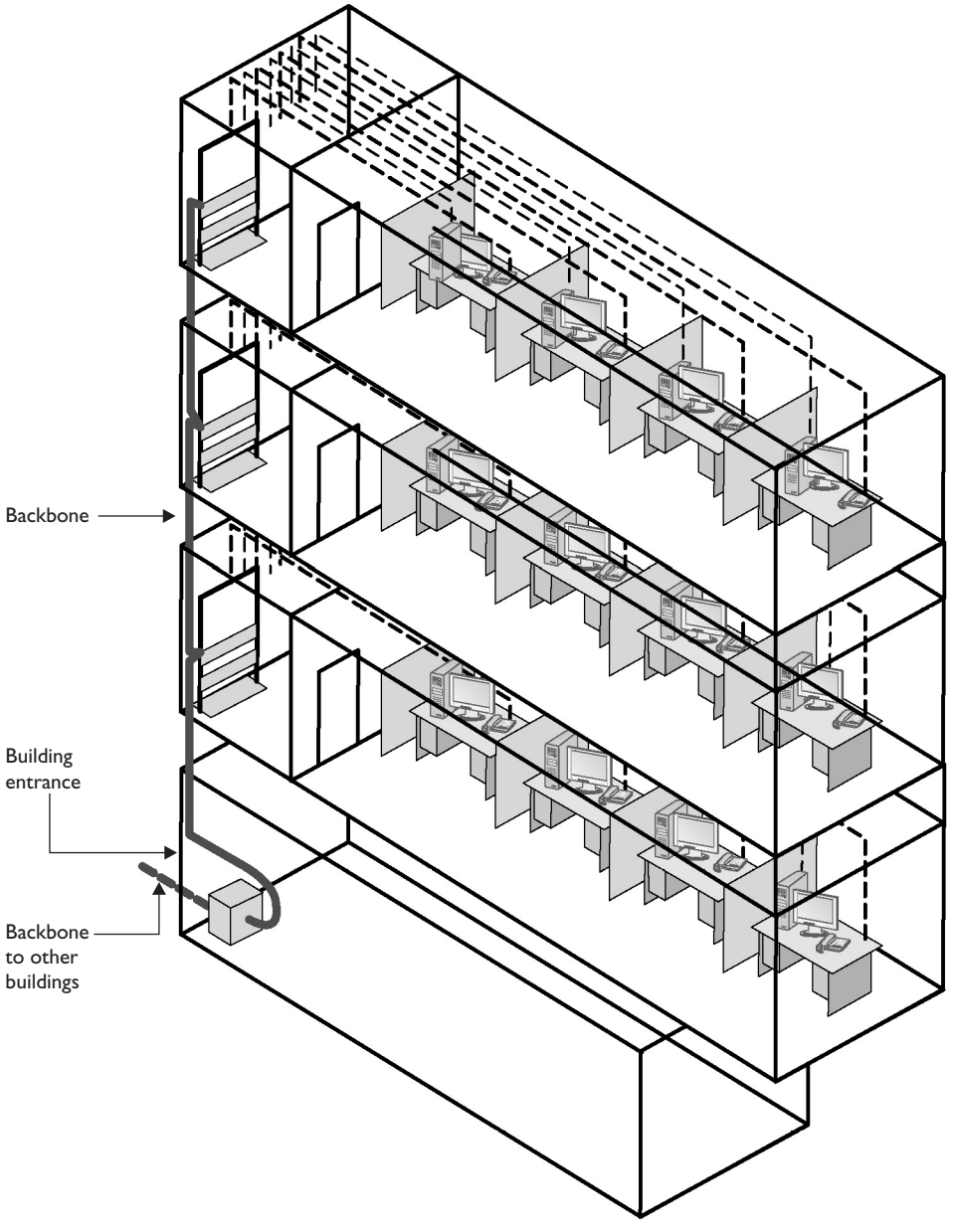


Figure 8-48 Backbone and building entrance

NICs

Now that the network's completely in place, it's time to turn to the final part of any physical network: the NICs. NICs are nearly as common as mice on today's PCs! A good network tech must recognize different types of NICs by sight and know how to install and troubleshoot them. Let's begin by reviewing the most common NICs.

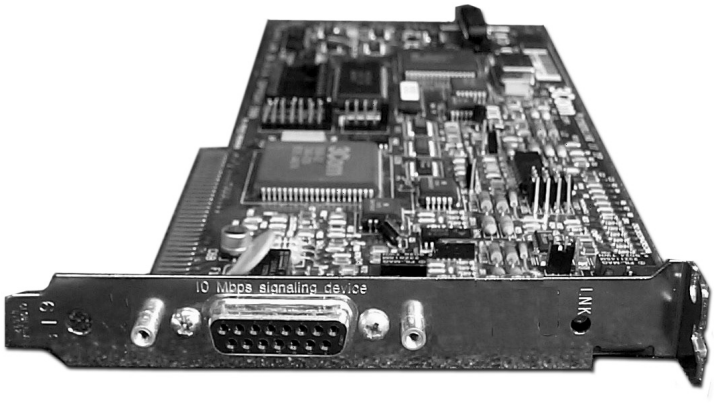
Ethernet NICs

Ethernet NICs are by far the most common type of NIC used today. It's tough to get an absolutely dependable statistic, but it's probably safe to say that most of all new installations use Ethernet in one way or another. Ethernet installations are also the most complicated, because of the vast variety of cable types and speeds.

10Base5 (Thicknet)

As you've seen, 10Base5 (Thicknet) NICs use a female, 15-pin DB DIX connector, as shown in Figure 8-49. The Ethernet drop cable runs from the DIX connector on the NIC to the AUI, which also happens to have a DIX connector. Many techs erroneously refer to the DIX connector as the AUI, as in, "Hey, plug in that AUI before the coffee gets cold!"

Figure 8-49
A DIX connector



10Base2

10Base2 (Thinnet) NICs have a BNC connector (as shown in Figure 8-50) that attaches to the network cable via a T-connector.

10BaseT

10BaseT, 100BaseT, and Gigabit Ethernet NICs all use the RJ-45 connector. The cable runs from the NIC to a hub or a switch (see Figure 8-51). It is impossible to tell one from the other simply by looking at the connection.

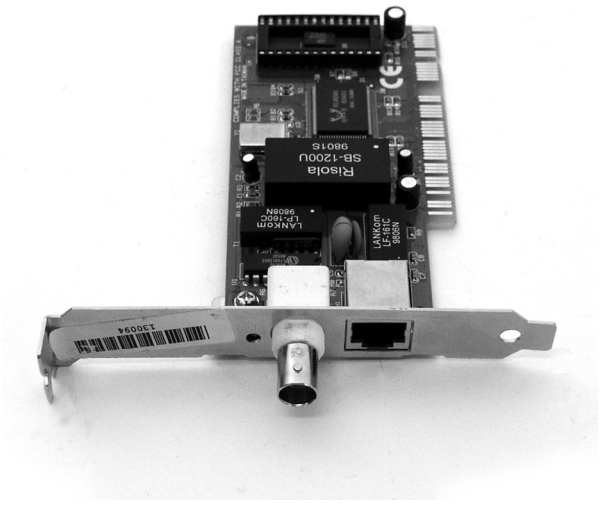


Figure 8-50 A combo Ethernet card with BNC (left) and RJ-45 (right) connectors

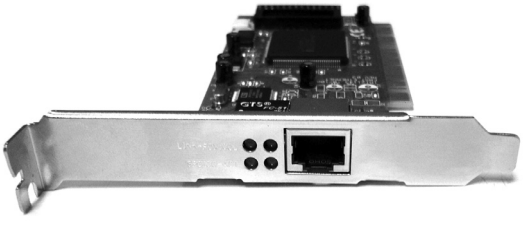


Figure 8-51 A NIC with an RJ-45 connector

Fiber-optic

Fiber-optic NICs are the most challenging. Most fiber networking standards allow cards to use either SC or ST connections on these NICs, so be alert to variations, even among cards from the same manufacturer (see Figure 8-52).

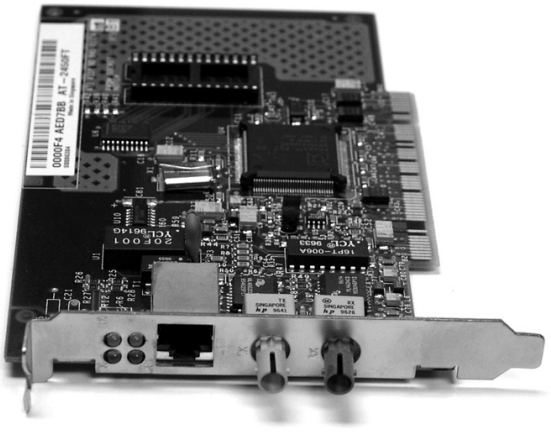


Figure 8-52 Combination ST fiber and RJ-45 NIC

Token Ring NICs

In this Ethernet-centric world, many network folks tend to look at IBM's Token Ring as yesterday's news. This is a mistake. Granted, finding a *new* Token Ring installation is about as easy as getting 50-yard-line seats at the Super Bowl, but Token Ring continues to enjoy a huge installed base. If you need proof that Token Ring is alive and well, simply browse any of the leading NIC manufacturers' web sites. Notice that they all continue to sell Token Ring cards, because the demand still exists, suggesting that Token Ring is doing just fine.

Token Ring NIC connectors come in only two types. The older and much more rare connector is a female DB-9. The newer, and far more common, connector is an RJ-45. (See Figure 8-53.)

Figure 8-53
A combo Token Ring NIC with RJ-45 and DB-9 connectors

Gee, this Token Ring card suddenly looks a lot like a 10BaseT card, doesn't it? The problem of figuring out what type of connector goes with what NIC is complicated by the fact that lots of networking technologies use the same connector—in particular the RJ-45. How can you tell whether the NIC in your hand with an RJ-45 connection is for 10BaseT, 100BaseTX, or Token Ring? The bad news is that you can't always tell; the good news is that there are some clues. If you see an RJ-45/BNC combo card, for example, you can be pretty sure that the RJ-45 is for 10BaseT. In addition, most cards will have some information printed on them that can provide clues. Everybody who makes Token Ring cards gives them a Token Ring-sounding name. So, if you see a word like TokenLink printed on a card, you should at least start with the theory that it's a Token Ring card. Finally, there's the small factoid that the NICs you're examining are probably part of a Token Ring or an Ethernet network—a big clue indeed, wouldn't you say?

Distinguishing between Token Ring and Ethernet is usually fairly easy. But supposing you know you have an Ethernet RJ-45 NIC, how do you know if it is 10BaseT, 100BaseT, or something else altogether? This is tougher. First of all, know your network and the cards you buy. Second, know your model numbers. Every NIC has a manufacturer's model number you can use to determine its exact capabilities. The model number is

nearly always printed on the card. Finally, pray that the NIC is Plug and Play (PnP) and stick it in a Windows 98/Me or Windows 2000/XP system. If you're lucky, the PnP application will recognize the card and give you some text clue as to what type of card it is (see Figure 8-54).

Figure 8-54 Windows 98 Plug and Play

The model number is the real key to knowing your NICs. As you will soon see, if you have the model number of a NIC, you also know the right driver for that NIC. You need to deal with this issue before you drop the NIC into a system, though, because once the NIC is installed in a PC, it's difficult to determine the model number from a Windows screen. Many network techs use one of two methods for remembering the types of cards used in their systems. The best way is simply to ensure that the model number of the NIC is printed on the card. If the manufacturer chose not to put the model number on the NIC, a good network admin takes the time to attach the model number or some other number physically to the NIC, as shown in Figure 8-55.

Granted, some folks will complain, "What good is having the model number on the card once you close the PC?" Well, in the real world, NICs tend not to stay in PCs, and you will be glad you put the model number on the NIC when you have to swap it out later and no longer have any clue what it is. Sometimes PnP doesn't work, and the model number will tell you which driver you need—so slap that number on a label and save yourself some hassle later! The other method—one used for many years, but increasingly difficult to do—is to buy only certain models of NICs. Buying only one model of NIC makes knowing what you have trivially easy. For years, the predominance of 10BaseT gave certain models of NICs a multi-year lifespan, which made it easy for NIC purchasers to pursue this method; it also generally made dealing with NICs much easier. The recent influx of new technologies such as 100BaseT and even Gigabit, however, has caused most purchasers to move into newer models, especially 10/100 Ethernet cards—making this strategy less convenient.

Figure 8-55
A NIC with model number label added to outside

Installing NICs

Now that you have a basic understanding of the different types of NICs, let's march through the process of installing a NIC in a PC. Installing a NIC involves three distinct steps. First, you must physically install the NIC. Second, the NIC must be assigned unused system resources—either by PnP or manually. Third, you (or PnP) must install the proper drivers for the card.

NOTE Remember that manufacturers update their drivers often. Even if Windows loads a driver for you, get the latest from the manufacturer's web site or use the Windows Update tool.

Buying NICs

Some folks may disagree with this, but I always purchase name-brand NICs. For NICs, stick with big names, such as 3COM or Intel. The NICs are better made, have extra features, and are easy to return if they turn out to be defective. Plus, it's easy to replace a missing driver on a name-brand NIC, and to be sure that the drivers work well. The type of NIC you purchase depends on your network. Try to think about the future and go for multispeed cards if your wallet can handle the extra cost. Also, where possible, try to stick with the same model of NIC. Every different model you buy means another set of driver disks you need to haul around in your tech bag. Using the same model of NIC makes driver updates easier, too.

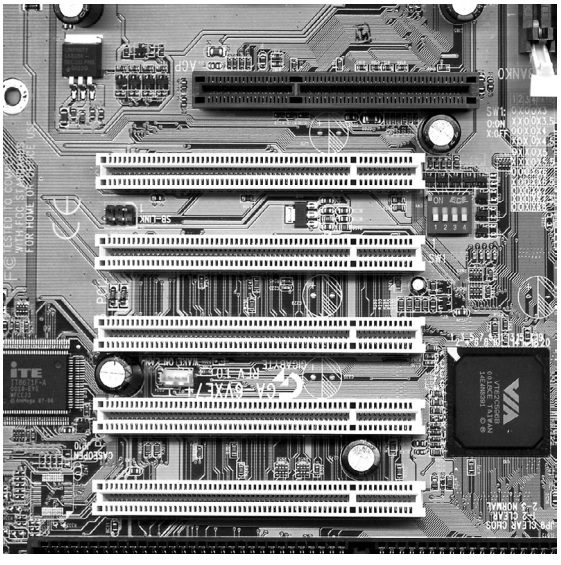
Many desktop systems and almost all laptops come with built-in Ethernet NICs with RJ-45 ports. Nothing is wrong with built-in NICs, as long as you know they will work with your network. Virtually all built-in NICs are autosensing and multispeed, so this is almost never an issue anymore—unless your network is all fiber-optic, or you're still running Token Ring!

NOTE Many people order desktop PCs with NICs simply because they don't take the time to ask if the system has a built-in NIC. Take a moment and ask about this!

Physical Connections

I'll state the obvious here: If you don't plug the NIC into the computer, it just isn't going to work! Many users happily assume some sort of quantum magic when it comes to computer communications, but as a tech, you know better. Fortunately, physically inserting the NIC into the PC is the easiest part of the job. Most PCs today have two types of expansion slots. The most common expansion slot is the Peripheral Component Interconnect (PCI) type (see Figure 8-56). PCI slots are fast, 32-bit, self-configuring expansion slots; virtually all new NICs sold today are of the PCI type, and with good reason: PCI's speed enables the system to take full advantage of the NIC.

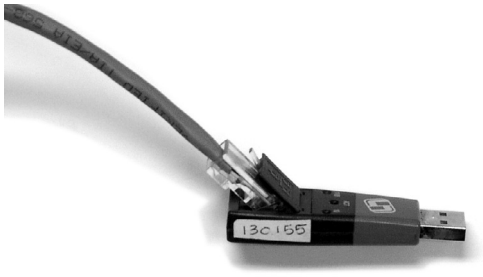
Figure 8-56
PCI slots



Another type of slot used for NICs is PCI-X. PCI-X is simply a faster PCI with a slightly longer (and brightly colored) slot. PCI-X is popular with Gigabit Ethernet due to its high speed, but it requires a motherboard with a PCI-X slot. Many higher-end motherboards now come with at least one PCI-X slot.

If you're not willing to open a PC case, you can get NICs with USB or PC Card connections. USB is convenient, but slow, and PC Card is only a laptop solution (see Figure 8-57). USB NICs are handy to keep in your toolkit. If you walk up to a machine that might have a bad NIC, test your suspicions by inserting a USB NIC and moving the network cable from the potentially bad NIC to the USB one. (Don't forget to bring your driver disc along!)

Figure 8-57
USB NIC



Drivers

Installing a NIC's driver into a Windows system is easy: just insert the driver CD when prompted by the system. The only problem is that this process is sometimes *too* automated! Windows will probably already have the driver if you use a more common model of NIC, but there are benefits to using the driver on the manufacturer's CD. The CDs that come with many NICs, especially the brand-name ones, include extra goodies such as enhanced drivers and handy utilities, but you'll only be able to access them if you install the driver that comes with the NIC!

Windows 2000 and XP give you the ability to show the status of the network connections in the taskbar. By default, only disconnected networks show up, but it's handy to have Windows always show the connection. To change this, go into Network Connections (in Windows 2000, it's called Network And Dial-Up Connections) in the Control Panel. Select the Properties for the network connection and check the "Show icon in notification area when connected" check box; note that this box is called "Show icon in taskbar when connected" in Windows 2000.

Lights

Most NICs made today have some type of lights, which are actually light-emitting diodes (LEDs—see Figure 8-58). Now that you know they are LEDs, call them "lights," just like all the other network techs. NICs with lights are mostly those for Ethernet network technologies that use RJ-45 (10BaseT, 100BaseT, and so on), and Token Ring cards. Don't be surprised if an old 10Base2 card has no lights. There is no guarantee that a NIC will have lights. In most cases, NICs with lights will have two of them. Sometimes there's only one, and they can be any color. More advanced cards might have four lights. These lights give you clues about what's happening, making troubleshooting a NIC much easier.

A *link light* tells you that the NIC is connected to a hub or switch. Hubs and switches also have link lights, enabling you to check the connectivity at both ends of the cable. If a PC can't access a network, look in the back to be sure the cleaning person didn't accidentally unplug the cable while vacuuming around the PC. Multispeed switches will also usually have an LED that tells you the speed of the connection (see Figure 8-59).

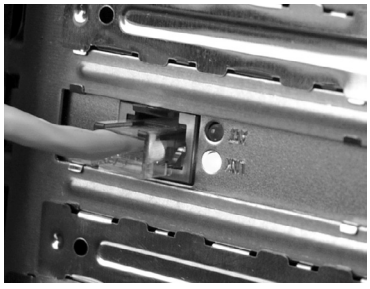


Figure 8-58
Typical lights on a 10BaseT NIC

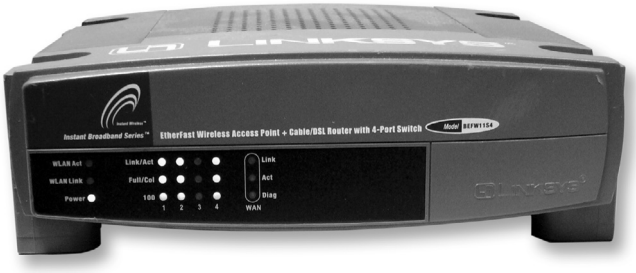


Figure 8-59
Link lights on a hub

The second light is the *activity light*. This little guy will flicker when the card detects network traffic. The activity light is a lifesaver for detecting problems, because in the real world, the connection light will sometimes lie to you. If the connection light says the connection is good, the next step is to try to copy a file or do something else to create network traffic. If the activity light does not flicker, there's a problem.

Another LED you will often find on multispeed NICs tells you the speed of the connection. This "speed" LED works in different ways depending on the NIC. On my 10/100 NICs, a single light is on when they run at 100 Mbps and off when they run at 10 Mbps. Some Gigabit Ethernet NICs have a single LED that glows in different colors, depending on the speed.

You might run into a fourth light on some much older NICs, called a collision light. As you might suspect from the name, the *collision light* flickers when it detects collisions on the network. Modern NICs don't have these, but you might run into the phrase on some test.

No standard governs how NIC manufacturers use their lights. When you encounter a NIC with a number of LEDs, take a moment and try to figure out what each one means. Although different NICs have different ways of arranging and using their LEDs, the functions are always the same.

Fiber-optic NICs rarely have lights, making diagnosis of problems a bit more challenging. Nevertheless, most physical connection issues for fiber can be traced to the ST or SC connection on the NIC itself. Fiber-optic cabling is incredibly delicate; the connectors that go into NICs are among the few places that anyone can touch fiber optics, so the connectors are the first thing to check when problems arise. Those who work with fiber always keep around a handy optical tester to enable them to inspect the quality of

the connections. Only a trained eye can use such a device to judge a good fiber connection from a bad one—but once you learn how to do it, this kind of tester is extremely handy (Figure 8-60).

Figure 8-60
Optical tester

Direct Cable Connections

Without doubt, NICs and modems are overwhelmingly the most common method of connecting PCs. But there is one other method—called *direct cable connection*—that should be addressed for completeness. All recent versions of Windows come with software to enable direct serial-to-serial, parallel-to-parallel, or infrared-to-infrared port connections between two PCs. Parallel connections require a special IEEE 1284-rated bidirectional parallel cable.

To connect two PCs using their serial ports, you need to string a special cable called a *null modem cable* between the two PCs. They can then share hard drives, but nothing else. Serial direct cable connections are slow—a maximum of 115,600 bps—but they are a cheap and dirty network option when you don't have a pair of NICs handy.

Diagnostics and Repair of Physical Cabling

"The network's down!" is easily the most terrifying phrase a network tech will ever hear. Networks fail for many reasons, and the first thing to know is that good quality, professionally installed cabling rarely goes bad. Chapter 20, "Zen and the Art of Network Support," covers principles of network diagnostics and support that apply to all networking situations, but let's take a moment now to discuss what to do when you think you've got a problem with your physical network. The first question to ask yourself is, "Do I have a physical problem?"

Diagnosing Physical Problems

Look for errors that point to physical disconnection. A key clue that you may have a physical problem is that a user gets a "No server is found" error, or goes into My Network

Places and doesn't see any systems besides his own. In general, look for errors implying that some network device is not there. If one particular application fails, try another. If the user can't browse the Internet, but can get his e-mail, odds are good that the problem is with software, not hardware—unless someone unplugged the e-mail server! If possible, try the problem user's logon name and password on another system, to make sure that account can access the shared resource.

Multiple system failures often point to hardware problems. This is where knowledge of your network cabling helps. If all the systems connected to one switch can suddenly no longer see the network, but all the other systems in your network still function, you not only have a probable hardware problem, you also have a suspect—the switch.

Check Your Lights

If you suspect a hardware problem, first check the link lights on the NIC and hub or switch. If they're not lit, you know the cable isn't connected somewhere. If you're not physically at the system, the Windows network connection icon on your System Tray is helpful. A user who's unfamiliar with link lights (or who may not want to crawl under her desk in a skirt) will have no problem telling you if the "Network cable unplugged" error shows up (Figure 8-61).

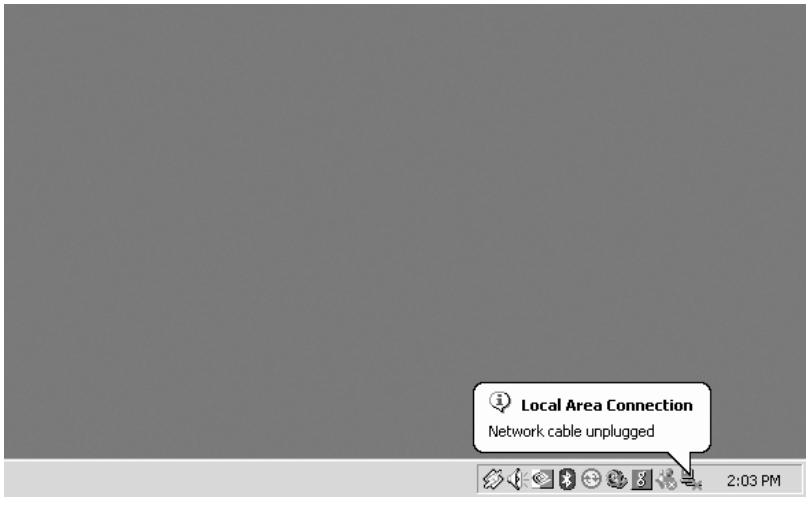


Figure 8-61 Disconnected cable

If your problem system is clearly not connecting, eliminate the possibility of a failed switch or other larger problem by checking to make sure other people can access the network, and that other systems can access the shared resource (server) that the problem system can't see. Make a quick visual inspection of the cable running from the back of the PC to the outlet. Finally, if you can, plug the system into a known good outlet and

see if it works. A good network tech always keeps a long patch cable for just this reason! If you get connectivity with the second outlet, you should begin to suspect the structured cable running from the first outlet to the hub or switch. Assuming the cable was installed properly and had been working correctly before this event, a simple continuity test will confirm your suspicion in most cases.

Check the NIC

Be warned that a bad NIC can also generate this "can't see the network" problem. Go into Device Manager and verify that the NIC is working. If you've got a NIC with diagnostic software, run it—this software will check the NIC's circuitry. The NIC's female connector is a common failure point, so NICs that do come with diagnostic software often include a special test called a *loopback test*. A loopback test sends data out of the NIC and checks to see if it comes back. Some NICs perform only an internal loopback, which tests the circuitry that sends and receives, but not the actual connecting pins. A true external loopback requires a loopback plug inserted into the NIC's port. If a NIC is bad, replace it—preferably with an identical NIC so you don't have to reinstall drivers!

Despite many claims by many software makers, there is no such thing as a single utility program that will test any NIC. The programs that make these claims try to communicate with the NIC via the NIC's drivers to send packets. If the NIC is physically bad or if the driver isn't working, you get a failure. You don't need a special program to do this for you—not when you can come to the same conclusion just by trying to access a web page using your browser! If you want to test your NIC, you'll need a diagnostic program that was designed for that NIC; if you don't have the CD-ROM that came with the hardware, check the manufacturer's web site for a program that you can download.

Cable Testing

With the right equipment, diagnosing a bad horizontal cabling run is easy. Anyone with a network should own a midrange tester with TDR like the Microtest Microscanner. With a little practice, you can easily determine not only whether a cable is disconnected, but also where the disconnection takes place. Sometimes patience is required, especially if you've failed to label your cable runs, but you will find the problem.

In general, a broken cable must be replaced. A bad patch cable is easy, but what happens if the horizontal cable is to blame? In these cases, I get on the phone and call my local installer—if a cable's bad in one spot, the risk of it being bad in another is simply too great to try anything other than total replacement.

Ah, if only broken cables were the network tech's worst problem! The rarity of this situation, combined with the relative ease of cable diagnostics, makes the problem of bad cables both uncommon and easily fixed. Far more problematic than broken cables is an issue that comes up in every network installation: tracking cable. When you're faced with an "I don't know where this cable goes" problem, you need a special tool called a toner.

Toners

It would be nice to say that all cable installations are perfect, and that over the years, they won't grow into horrific piles of spaghetti-like, unlabeled cables. In the real world, though, you will eventually find yourself having to locate ("trace" is the term installers use) cables. Even in the best-planned networks, labels fall off ports and outlets, mystery cables appear behind walls, new cable runs are added, and mistakes are made counting rows and columns on patch panels. Sooner or later, most network techs will have to be able to pick out one particular cable or port from a stack.

When the time comes to trace cables, network techs turn to a device called a toner for help. *Toner* is the generic term for two separate devices that are used together: a tone generator and a tone probe. The *tone generator* connects to the cable using alligator clips, tiny hooks, or a network jack, and it sends an electrical signal along the wire at a certain frequency. The *tone probe* emits a sound when it is placed near a cable connected to the tone generator (see Figure 8-62). These two devices are often referred to by the brand name Fox and Hound, a popular model of toner made by the Triplett Corporation.

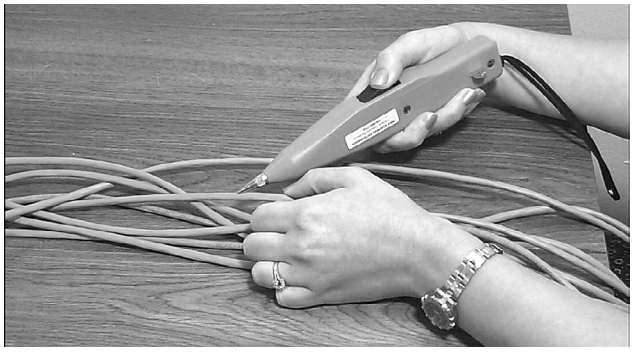


Figure 8-62 A tone probe at work

To trace a cable, connect the tone generator to the known end of the cable in question, and then position the tone probe next to the other end of each of the cables that might be the right one. The tone probe will make a sound when it's placed next to the right cable. More advanced toners include phone jacks, enabling the person manipulating the tone generator to communicate with the person manipulating the tone probe: "Jim, move the tone generator to the next port!" Some toners have one tone probe that works with multiple tone generators. Each generator emits a separate frequency, and the probe sounds a different tone for each one. Even good toners are relatively inexpensive (≈ $75); although cheapo toners can cost less than $25, they don't tend to work well, so it's worth spending a little more. Just keep in mind that if you have to support a network, you'd do best to own a decent toner.

A good, medium-priced cable tester and a good toner are the most important tools used by folks who must support, but not install, networks. A final tip: be sure to bring along a few extra batteries—there's nothing worse than sitting on the top of a ladder holding a cable tester or toner that has just run out of juice!

Chapter Review

Questions

1. Which of the following cables should never be used in a structured cabling installation?
   - **A.** UTP
   - **B.** STP
   - **C.** Fiber-optic
   - **D.** Coax
2. Which type of fire rating should horizontal cabling have?
   - **A.** Mil Spec
   - **B.** Plenum
   - **C.** PVC
   - **D.** UTP
3. The CAT 5e rating defines how many pairs of wires in the cable?
   - **A.** 2
   - **B.** 4
   - **C.** 8
   - **D.** It doesn't specify.
4. The best type of cabling to use for interbuilding connections is
   - **A.** UTP
   - **B.** Coax
   - **C.** Fiber-optic
   - **D.** STP
5. A _____ organizes and protects the horizontal cabling in the equipment room.
   - **A.** Rack
   - **B.** Patch panel
   - **C.** Outlet
   - **D.** 110 jack
6. Which of the following would never be seen in an equipment rack?
   - **A.** Patch panel
   - **B.** UPS or SPS

C. PC

D. All of the above can be seen in an equipment rack.

7. What are patch cables used for? (Select all that apply.)

A. To connect different equipment rooms.

B. To connect the patch panel to the hub.

C. They are used as crossover cables.

D. To connect PCs to outlet boxes.

8. Which of the following network technologies use UTP cabling in a star topology? (Select all that apply.)

A. 10Base2

B. Fiber optics

C. 10BaseT

D. 100BaseT

9. Jane needs to increase network throughput on a 10BaseT network that consists of 1 hub and 30 users. Which of the following hardware solutions would achieve this most inexpensively?

A. Add a fiber backbone.

B. Upgrade the network to 100BaseT.

C. Replace the hub with a switch.

D. Add a router.

10. Which standard addresses cable pathways and installation areas involving multiple rooms, floors, and buildings?

A. EIA/TIA 586

B. EIA/TIA 587

C. EIA/TIA 568

D. EIA/TIA 569

Answers

1. **D.** Coax cable should not be used in structured cabling networks.
2. **B.** Plenum cabling should be used in horizontal cabling.
3. **B.** The CAT 5e rating requires four pairs of wires.
4. **C.** EIA/TIA specifies fiber-optic cabling as the preferred interbuilding cabling.
5. **B.** The patch panel organizes and protects the horizontal cabling in the equipment room.

6. **D.** All these devices can be found in equipment racks.
7. **B, D.** Patch cables are used to connect the hub to the patch panel and the PCs to the outlet boxes.
8. **C, D.** 10BaseT and 100BaseT use UTP cabling in a star topology. 10Base2 is an older, dying technology that doesn't use UTP in a star. Fiber-optic networking uses a star topology, but the name is a dead giveaway that it doesn't use UTP!
9. **C.** Upgrading to 100BaseT will work, but replacing the hub with a switch is much cheaper.
10. **D.** EIA/TIA 569 addresses cable pathways and installation areas involving multiple rooms, floors, and buildings. The EIA/TIA 568 standard defines acceptable cable types, the organization of the cabling system, guidelines for installation of the cable, and proper testing methods. The other two choices were made up to confuse you!