

Chapter 1 - Networks

Cisco Networking Essentials

by Troy McMillan

Sybex © 2012 *Citation*

Recommend?

[< Previous](#)



[Next >](#)

Chapter 1: Networks

Computer networks are everywhere. It's impossible to escape them in the modern world in which we live and work. We use them at work, at home, and even in between, in places like our cars, the park, and the coffee shop. We have come to take them for granted in the same way we treat electricity and hot water.

But a lot is going on behind the scenes when we use these networks. Cisco routers and switches play a critical role in networks' successful operation.

This opening chapter lays the foundation required to understand all the details that make networks function. Specifically, this chapter covers the following topics:

- Describing network components
- Classifying networks by function
- Defining network architectures

Describing Network Components

To understand how networks work, it helps to have an appreciation of why they exist in the first place. As incredible as it may seem now, for a number of years, when computers first came into use, very few computers were networked. They operated as little islands of information with no connection to one another. Data had to be transferred between computers by copying it to a floppy disk, physically taking that floppy disk to the other computer, and copying the data to the destination machine. This process is now sometimes jokingly referred to as the *sneakernet*.

Modern networks can include many components. Some of the most basic components are computers, routers, and switches. [Figure 1.1](#) shows some Cisco routers and switches. *Routers* are used in a network to transfer information between computers that are not on the same network. Routers are capable of doing this by maintaining a table of all networks and the routes (directions) used to locate those networks. *Switches* come in two varieties. Layer 2 switches simply connect computers or devices that are in the same network. Layer 3 switches can do that but are capable of acting as routers as well. Two models of routers are depicted in [Figure 1.1](#), with a switch in the middle of the stack. Routers and switches are covered in depth in [Chapter 10, "Network Devices."](#)



Figure 1.1: Cisco routers and switches

In this section, the benefits of networking are covered as well as the components required to constitute a network.

Defining the Benefits of Networks

There are many benefits to networks, one of which was touched on in the introduction to this section: using a network makes sharing resources possible (without putting on your sneakers and leaving your seat). When connected by networks, users can share files, folders, printers, music, movies, you name it! If it can be put on a hard drive, it can be shared. Additional benefits are included in the following list:

Resource Sharing Resource sharing is less earthshaking at home, but in the workplace it was a key element that drove the adoption of PCs. Other computer types such as mainframe computers and dumb terminals were already in use, but were seen as specialized pieces of equipment to be used only by guys in lab coats and some other geeky types. There were other reasons for the PC revolution, but resource sharing helped to increase productivity. As an example, 10 coworkers could access a file on the network at the same time, which eliminated the time and effort spent burning, labeling, transporting, and storing 10 floppies.

Note The term *resource* is used extensively when discussing networking and simply refers to anything that a user on one computer may want to access on a different computer. Examples include files, folders, printers, and scanners.

Reduced Cost and Easier Installation of Software Another advantage for business that didn't become apparent as quickly as resource sharing was a reduced cost of software. Many software products are sold to organizations on a network basis. For example, instead of buying 25 retail versions of word processing software, a single copy can be purchased for the network and then a number of seat licenses can be added to the bundle. The result is a significant savings to the company.

Taking that idea a step further, the network also makes it possible to place the installation files (from the CD containing the software) on a server and to then install the software over the network (as shown in [Figure 1.2](#)). This capability relieves IT staff from having to physically visit each machine with CD in hand to perform the installation. Moreover, the software could be installed on all five machines at once over the network by using those same files.

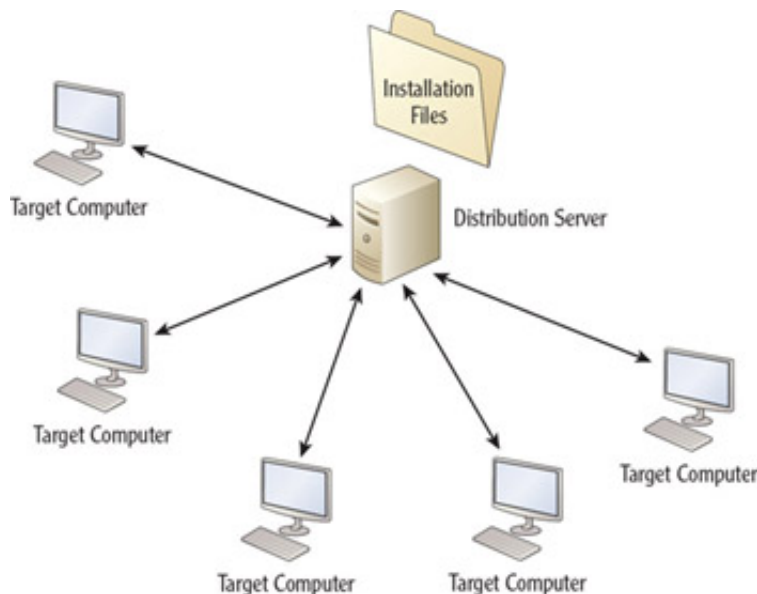


Figure 1.2: Network installation

Improved Security All this peace, love, and sharing doesn't mean that everything is available to everyone. Shared resources can be secured with restrictions on who can access them and what exact access each individual possesses. So you can share a file on your computer but share it with only two of your coworkers, and not all of them. Moreover, you could allow one coworker to only read the document while the other could be allowed to edit or even delete the document.

This type of control was difficult when files were shared on floppies. After the floppy left your hand, it was out of your control. Computer networks can enforce security controls among the computers and users.

Improved Communications It's hard to even imagine today's workplace without email, instant messaging, video chatting, and conferencing, but 25 years ago, these tools did not exist. In today's world, almost *no* communication can wait for regular postal mail (this service that we once depended on is now often called *snail mail*). Even more impressive is that distance is no obstacle. You can chat online with someone in India or China as easily as with a fellow worker sitting in the next cubical!

Now think of all the paper that is being saved that used to be consumed by companies sending regular mail to one another. The problem was multiplied by the need to keep multiple copies of the documents sent through the regular mail. Email systems can be configured to maintain a copy of every email sent, and documents that used to exist in multiple physical copies now reside as a single digital copy on a server (and probably also on a backup tape).

Meetings that used to require plane trips and hotel stays can now be held online with all participants able to see one another, share documents, view slides or documents from the presenter, and even hold votes and surveys. The only consideration is time zones!

More Workplace Flexibility Users are no longer physically tied to the same computer. If resources are stored on servers, as they are in most organizations, a computer problem no longer renders a user unable to work. In a domain-based network (more on that later in this chapter in the section "Understanding Client-Server Networks"), the user can move to any other computer that is a member of the domain, access his files on the server, and continue to work while his computer is repaired or replaced.

Building on this idea, workers are increasingly telecommuting as they can use the Internet to connect to the work network and operate as if physically present in the office.

Note *Telecommuting* means working from another physical location, usually from home. It saves gas, time, and in many cases results in more productivity on the part of the worker.

Reduced Cost of Peripherals When users can share printers, scanners, and fax machines,

usually fewer devices are needed. This reduces costs for the organization. Sharing these devices also offloads the responsibility for managing and maintaining these shared devices.

Note *Peripherals* are any devices that operate in conjunction with the computer yet reside outside the computer's box. Examples include the display, mouse, keyboard, printer, camera, speakers, and scanners.

Centralized Administration Although not possible in a peer-to-peer network, in a domain-based network, all computer administration is centralized. This means that the LAN administrator is responsible for maintaining the security of the network, and this work is done from a special type of server called a *domain controller*. Domain controllers do more than provide security. They also serve as the directory of the resources available on the network. This is why these services are called *directory services*. (Peer-to-peer networks, domain-based networks, and LANs are explained throughout the rest of this chapter.)

Directory Assistance, Please!

Directory services, such as Active Directory by Microsoft, help users to locate files, folders, and other resources in the network.

Identifying the Requirements for a Network

A network cannot be called a network if it does not meet certain requirements. At their simplest, those requirements include the following:

- At least two computers
- A resource that needs to be shared
- A transmission medium
- A communications agreement

Each requirement is detailed in the following list. The coverage of the last two bullet points is somewhat brief as transmission mediums are discussed in [Chapter 9, "Cabling,"](#) and protocols (communications agreements) are covered in detail in [Chapter 4, "Protocols."](#)

At Least Two Computers It seems obvious, but if there are not at least two computers, there is no need for a network. A single computer doesn't need a network to access the information on its own hard drive. Getting information from computer A to computer B without using the sneaker net is what drove the development of networks.

A Resource That Can Be Shared You already know from our earlier discussion that resources are anything that needs to be shared. This can include physical entities such as printers and scanners, or it can be files and folders located on another computer, as shown in [Figure 1.3](#). If it can be shared and moved from one computer to another, it can be considered a resource.

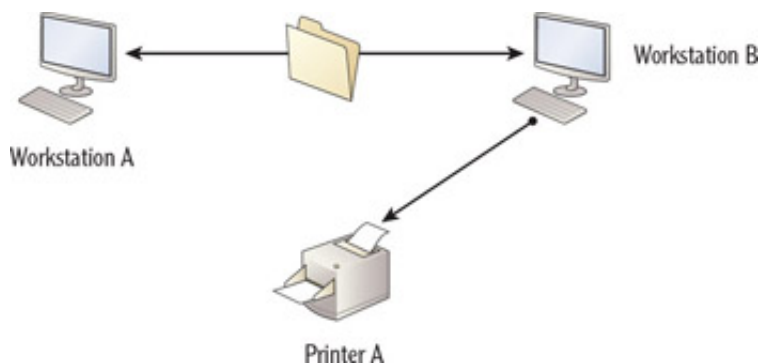


Figure 1.3: Sharing resources

A Transmission Medium Some form of communications medium is also required. The most common form is a cable, but wireless communications are becoming increasingly widespread because of certain advantages to this approach. Both methods are shown in [Figure 1.4](#).

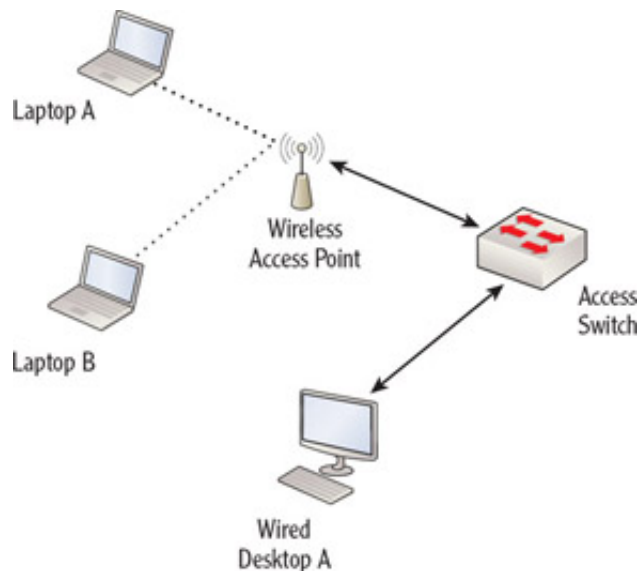


Figure 1.4: Transmission mediums

Medium? Do I Need a Ouija Board?

A communications *medium* is any process that can be used by two computers to transfer data. It can be bounded (via a cable) or boundless (wireless).

A Communications Agreement One of the main stumbling blocks present when computers were first being networked was a language problem. As you know, two people who need to converse cannot do so unless they speak a common language. Likewise, computers have to be speaking the same language in order to have a communications agreement. Networking languages are called *protocols*. In [Figure 1.5](#), workstation 2 is able to communicate with workstation 3 because they are both using TCP/IP, but cannot communicate with workstation 1 because it is using IPX/SPX, a different networking protocol.

Note Protocols are discussed in [Chapter 4](#).

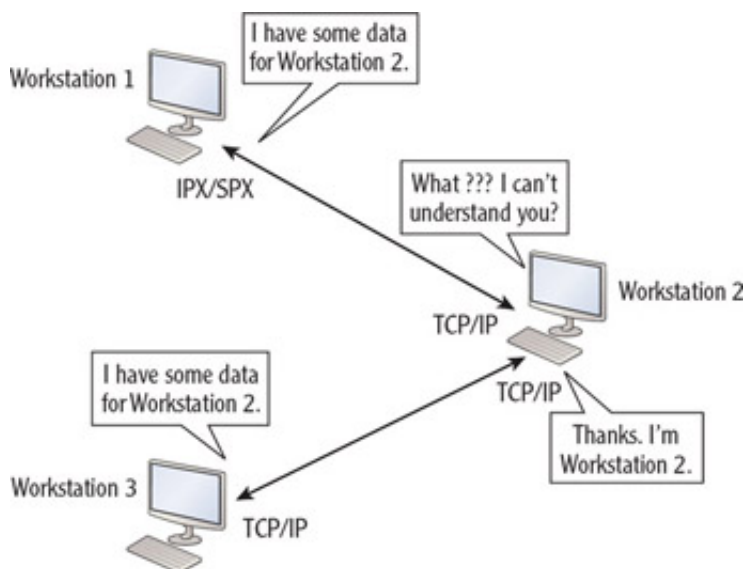


Figure 1.5: Protocol agreement

Before the standardization of network protocols, brought about by the explosion of the Internet and the introduction of reference models such as the OSI and the DoD models, computers from different vendors could not be networked together because they used proprietary and dissimilar network protocols.

Note The OSI and DoD network models are covered in [Chapter 2, "The OSI Model."](#)

In addition to the minimum requirements for a network, additional components are usually present in varying


combinations. *Repeaters* are devices designed to regenerate or strengthen transmission signals to avoid attenuation or weakening of the signal, which leads to data corruption. *Hubs* are junction boxes with no intelligence that are used to connect devices together on the same physical network. Switches can act as hubs but provide vastly improved performance and offer additional functions not available in hubs. Routers, as discussed earlier, are used to connect networks and allow computers located on different networks to communicate. Cisco routers and switches are intelligent because of the Cisco Internetwork Operating System (IOS), which is included in and is used to manage the functions of these products. The Cisco IOS is discussed in [Chapter 12, "Managing the Cisco IOS."](#) Routers, switches, and hubs are covered in detail in [Chapter 10](#).

Proprietary vs. Standard

The term *proprietary*, used often in the IT world, refers to any process or way of doing something that works only on a single vendor's equipment. The opposite of this is a *standard*, which is any way of carrying out a function that the industry has agreed upon. An everyday example of a standard is the ubiquitous wall socket. A standard was developed so that consumers could be assured that any electrical device would match this standard outlet type.

As the next few chapters unfold, you will gain new perspectives about these requirements as you learn more about the details of each. Now let's look at some characteristics of various types of networks.

 [Previous](#)

[Next](#) 

Use of content on this site is subject to the restrictions set forth in the [Terms of Use](#).

Page Layout and Design ©2016 Skillsoft Ireland Limited - All rights reserved, individual content is owned by respective copyright holder.

[Feedback](#) | [Privacy and Cookie Policy \(Updated 12/2014\)](#) | v.4.0.78.153

