Networks come in all sizes. They can range from simple networks consisting of two computers to networks connecting millions of devices.

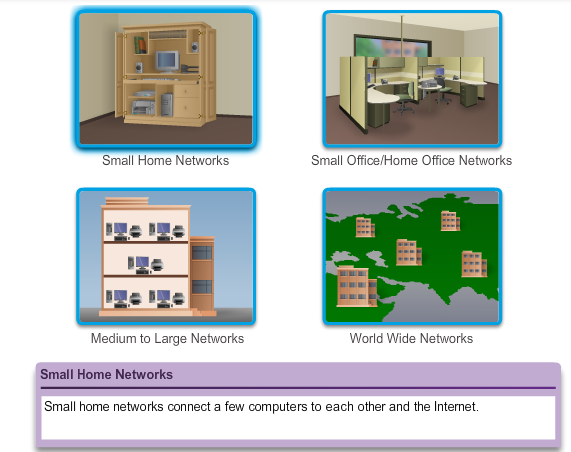
Simple networks installed in homes enable sharing of resources, such as printers, documents, pictures and music between a few local computers.

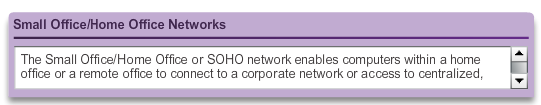
Home office networks and small office networks are often set up by individuals that work from a home or remote office and need to connect to a corporate network or other centralized resources. Additionally, many self-employed entrepreneurs use home office and small office networks to advertise and sell products, order supplies and communicate with customers. Communication over a network is usually more efficient and less expensive than traditional forms of communication, such as regular mail or long distance phone calls.

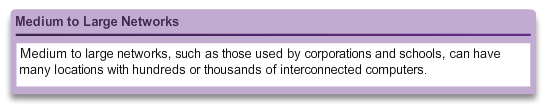
In businesses and large organizations, networks can be used on an even broader scale to allow employees to provide consolidation, storage, and access to information on network servers. Networks also allow for rapid communication such as email, instant messaging, and collaboration among employees. In addition to internal organizational benefits, many organizations use their networks to provide products and services to customers through their connection to the Internet.

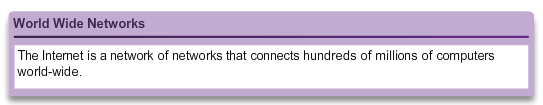
The Internet is the largest network in existence. In fact, the term Internet means a ‘network of networks’. The Internet is literally a collection of interconnected private and public networks, such as the ones described above. Businesses, small office networks, and even home networks usually provide a shared connection to the Internet.

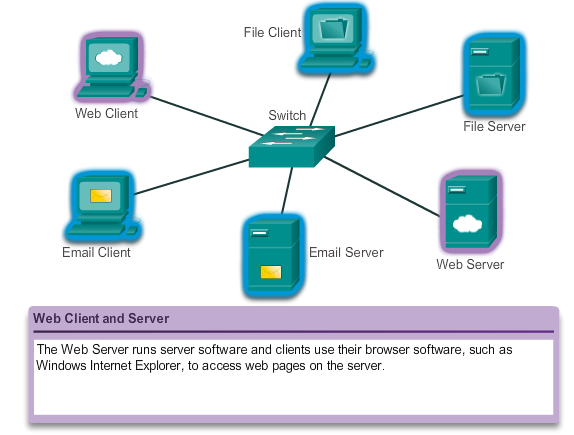
It is incredible how quickly the Internet has become an integral part of our daily routines.

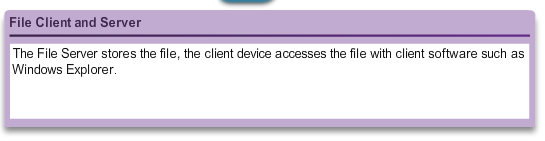


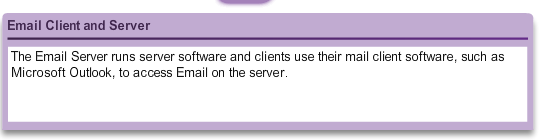








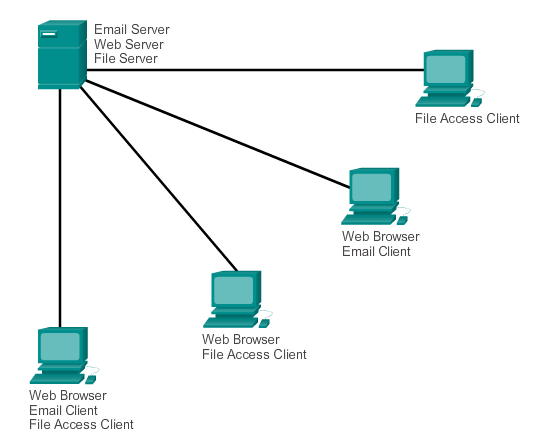




All computers connected to a network that participate directly in network communication are classified as hosts or end devices. Hosts can send and receive messages on the network. In modern networks, end devices can act as a client, a server, or both. The software installed on the computer determines which role the computer plays.

Servers are hosts that have software installed that enable them to provide information, like email or web pages, to other hosts on the network. Each service requires separate server software. For example, a host requires web server software in order to provide web services to the network.

Clients are computer hosts that have software installed that enable them to request and display the information obtained from the server. An example of client software is a web browser, like Internet Explorer.



A computer with server software can provide services simultaneously to one or many clients.

Additionally, a single computer can run multiple types of server software. In a home or small business, it may be necessary for one computer to act as a file server, a web server, and an email server.

A single computer can also run multiple types of client software. There must be client software for every service required. With multiple clients installed, a host can connect to multiple servers at the same time. For example, a user can check email and view a web page while instant messaging and listening to Internet radio.

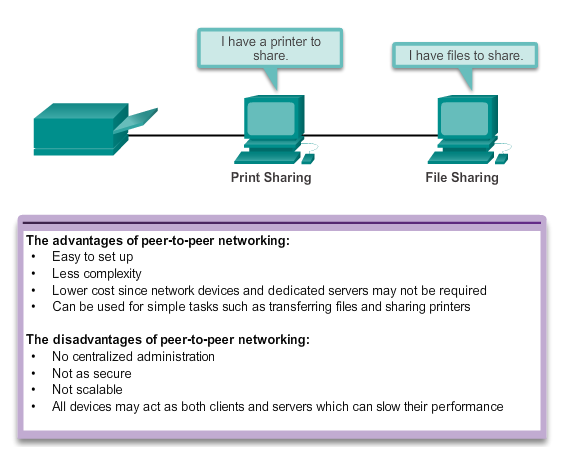
Client and server software usually runs on separate computers, but it is also possible for one computer to carry out both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network.

The simplest peer-to-peer network consists of two directly connected computers using a wired or wireless connection.

Multiple PCs can also be connected to create a larger peer-to-peer network but this requires a network device, such as a hub, to interconnect the computers.

The main disadvantage of a peer-to-peer environment is that the performance of a host can be slowed down if it is acting as both a client and a server at the same time.

In larger businesses, due to the potential for high amounts of network traffic, it is often necessary to have dedicated servers to support the number of service requests.



Components of a network

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

The network infrastructure contains three categories of network components:

* Devices
* Media
* Services

Click each button in the figure to highlight the corresponding network components.

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves.

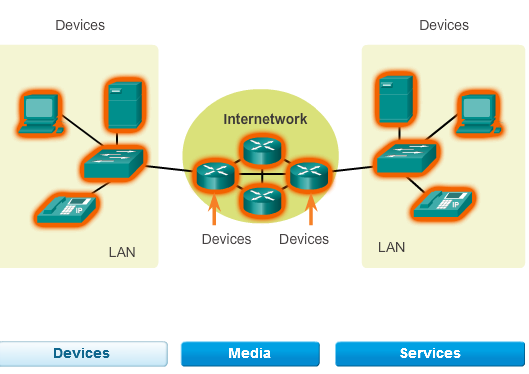
Network components are used to provide services and processes. These are the communication programs, called software, that run on the networked devices. A network service provides information in response to a request. Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

The network devices that people are most familiar with are called end devices, or hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are:

* Computers (work stations, laptops, file servers, web servers)
* Network printers
* VoIP phones
* TelePresence endpoint
* Security cameras
* Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

A host device is either the source or destination of a message transmitted over the network, as shown in the animation. In order to distinguish one host from another, each host on a network is identified by an address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.



Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network, as shown in the animation. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

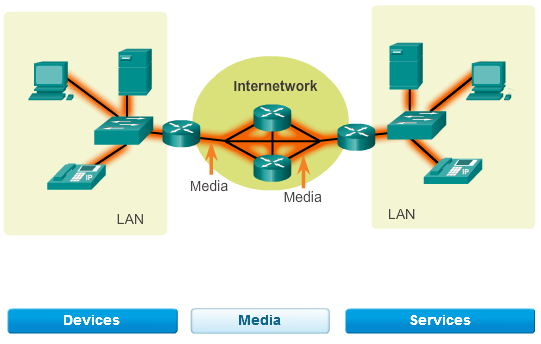
Examples of intermediary network devices are:

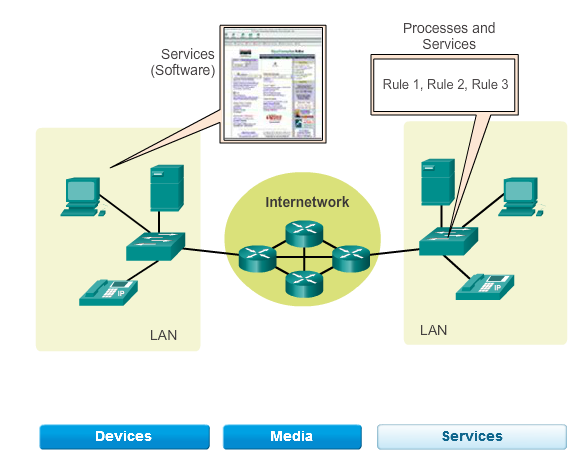
* Network Access (switches and wireless access points)
* Internetworking (routers)
* Security (firewalls)

The management of data as it flows through the network is also a role of the intermediary devices. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Processes running on the intermediary network devices perform these functions:

* Regenerate and retransmit data signals
* Maintain information about what pathways exist through the network and internetwork
* Notify other devices of errors and communication failures
* Direct data along alternate pathways when there is a link failure
* Classify and direct messages according to Quality of Service (QoS) priorities
* Permit or deny the flow of data, based on security settings





Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination.

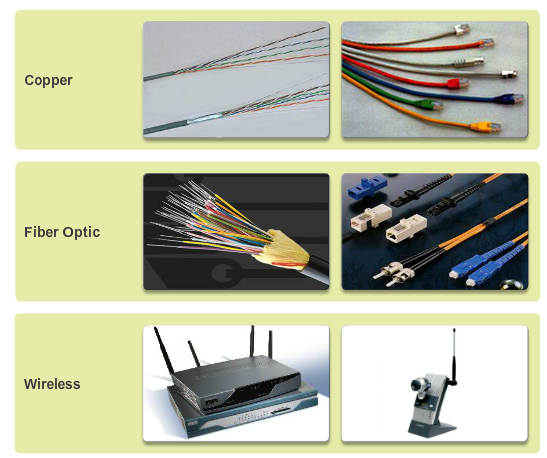
Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted. As shown in the figure, these media are:

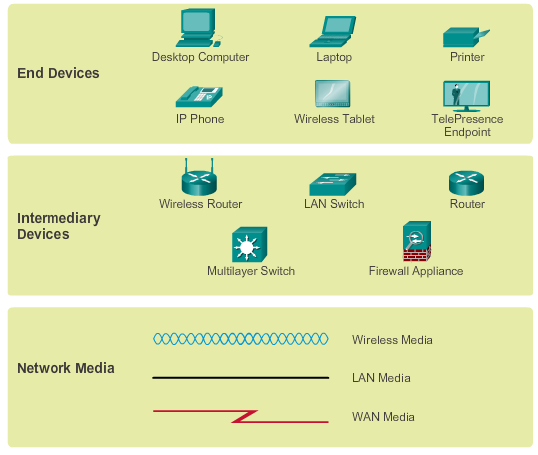
* Metallic wires within cables
* Glass or plastic fibers (fiber optic cable)
* Wireless transmission

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media has the same characteristics and is appropriate for the same purpose. The criteria for choosing network media are:

* The distance the media can successfully carry a signal
* The environment in which the media is to be installed
* The amount of data and the speed at which it must be transmitted
* The cost of the media and installation





When conveying complex information such as displaying all the devices and medium in a large internetwork, it is helpful to use visual representations. A diagram provides an easy way to understand the way the devices in a large network are connected. Such a diagram uses symbols to represent the different devices and connections that make up a network. This type of “picture” of a network is known as a topology diagram.

Like any other language, the language of networking uses a common set of symbols to represent the different end devices, network devices, and media, as shown in the figure. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network. Throughout this course and labs, you will learn both how these devices operate and how to perform basic configuration tasks on these devices.

In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are:

* **Network Interface Card** - A NIC, or LAN adapter, provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC.
* **Physical Port** - A connector or outlet on a networking device where the media is connected to a host or other networking device.
* **Interface** - Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to network interfaces.

Topology diagrams are mandatory for anyone working with a network. It provides a visual map of how the network is connected.

There are two types of topology diagrams including:

* **Physical topology diagrams** - Identify the physical location of intermediary devices, configured ports, and cable installation.
* **Logical topology diagrams** - Identify devices, ports, and IP addressing scheme.

