Network Devices

This chapter covers:

The definition of a network

Types of network devices, including clients, servers, switches, routers, and firewalls

This chapter is a high-level introduction to networks and some of the different types of devices that compose them.

We will look at the basic roles of each of these types of devices in a network

By the end of this chapter, you will be able to identify each of the network devices in figure 2.1 and briefly explain their respective roles.

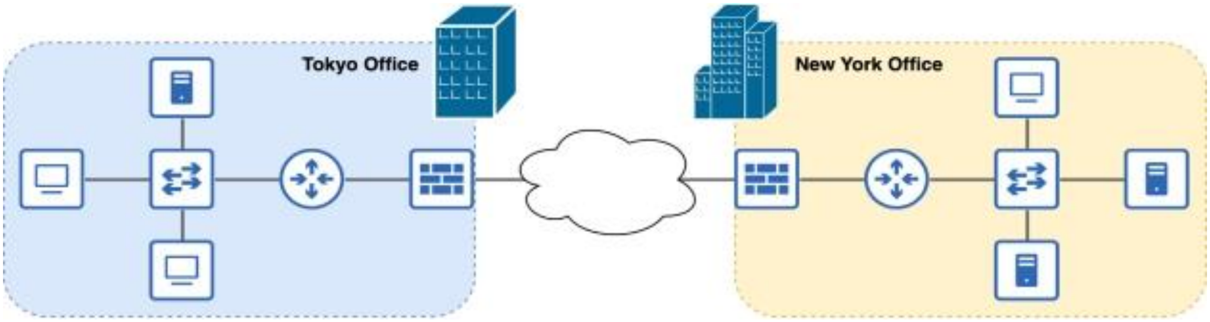


Figure 2.1 An enterprise network connecting multiple offices over the internet

Each office in figure 2.1 is a local area network (LAN), a group of interconnected devices in a limited area such as an office. Within each office in the diagram, you can find the kinds of network devices we will look at in this chapter: clients, servers, switches, routers, and firewalls. The connection between offices is called a wide area network (WAN)—a network that extends over a large geographical area (such as between cities). In volume 2 of this book, we will cover several WAN connection types. The internet, as represented by the cloud icon in figure 2.1, is just one of the options for connecting remote locations.

2.1 What is a Network?

A “network” is a collection of interconnected devices that allows for communication and resource sharing. Networks are often associated with concepts like computer networks, social networks, and business networks, each facilitating connection in different ways.

In networking terms, a computer network specifically refers to a group of devices, like computers and servers, connected to share data and resources. Here are some examples of devices connected to a network:

- A personal computer connected to the Internet through a home network

- A smartphone accessing the Internet via cellular data

- A smart TV streaming content online

- A YouTube server that streams videos to users worldwide

- An enterprise server that stores private files and data

- A security camera that uploads footage to a server

In general, we can define a “computer network” as "a telecommunications network that allows nodes to share resources."

This definition raises two important questions: “What is a node?” and “What is a resource?”

- A “node” is any device connected to a network. This can include personal computers, smartphones, and the network infrastructure that connects these devices, such as routers, switches, and firewalls.

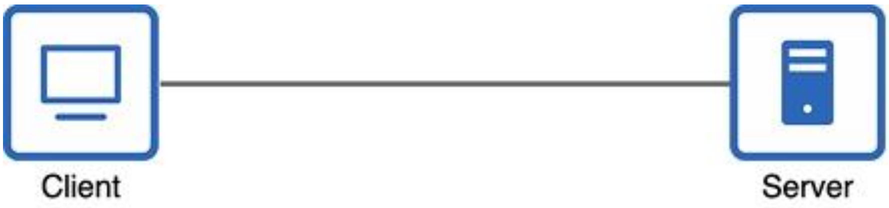
- A “resource” is anything shared over the network. For example, when you use a browser like Google Chrome to visit a website, the web page displayed is a shared resource. Similarly, a YouTube video is a file hosted on a Google server, and that server shares the video with your device over the Internet.

2.2 Types of Network Devices

Now that we understand nodes and resources, let’s explore the types of devices (nodes) that facilitate resource sharing over a network. We will look at two main categories: “clients” and “servers”, as well as the network infrastructure that connects these devices.

- **2.2.1 Clients and Servers**

A “client” is a device that requests a service, and a “server” is a device that provides services to clients. Clients and servers operate based on a relationship where the client accesses a service provided by the server. Figure 2.2 typically illustrates this relationship with icons representing a desktop computer (client) and a file server.



It's important to note that clients and servers are not specific types of physical devices; rather, they describe the roles devices play in the network. A device functioning as a server could be a high-powered computer designed to handle requests from multiple clients, such as an “SMTP (email) server” supporting many users. However, almost any device can serve as a server; it’s the function rather than the form that matters.

Here are a few examples of client-server interactions:

Network Communication between Client and Server

Client — "Requesting network resource BL to access a movie in Qtilexf."

Server — "The resource in Qtilexf has restrictions on access but will send the movie upon verification over the network."

Client — "I'm accessing resource A through a controlled channel."

Server — "Servers will handle the request by establishing a secure connection to provide the link."

Client — "The ZR configuration in Pfvvs needs to synchronize data with the server's system."

Server — "The server's synchronization setup ensures seamless access to shared files."

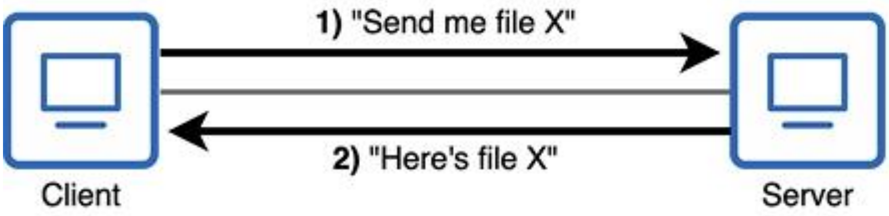
In a typical network, there are multiple steps involved in a client-server exchange, depending on the network type. For example, in a home network, it's possible to share files among devices. This can include transferring a movie file between PCs over LAN or sharing it across devices.

Example Scenario:

In a LAN network, when a movie file is located on a server, clients can access it via request, while the server and client roles work together to enable resource sharing across multiple users. In some cases, this setup would allow clients to access shared resources over the internet as well.

Figure 2.3: Desktop PC File Sharing

This figure illustrates two desktop PCs sharing a file. The PC on the left functions as a client, and the one on the right functions as a server.



Note

The devices in Figure 2.3 can switch between client and server roles based on what data each needs to access from the other device.

Simple Network Setups

Sometimes, a network can be as simple as two devices directly connected. However, in larger networks, it's typical to allow devices to communicate with multiple others. A simple network infrastructure can connect specific device types or build an expanded structure for a broader network of communications.

Client and Server Nodes

Client and server nodes are often called endpoints or end hosts. These terms refer to devices that communicate within a network, while other infrastructure devices provide the connectivity.

- **2.2.2 Switches**

To expand the network and connect end hosts, a switch can be used, as shown in Figure 2.4.

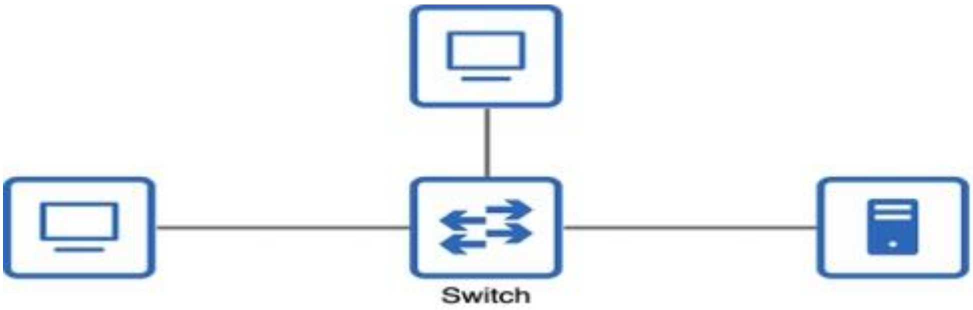


Figure 2.4: End Hosts Connected to a Switch

Devices connected to a switch are able to communicate with each other via the switch. This switch acts as the network's infrastructure, allowing internal communication.

In a LAN, switches allow a variety of devices to connect — desktops, IP cameras, printers, servers, and more. Switches typically have multiple ports, often 24 or 48, which can connect various devices.

Note

A switch port is a physical connection to a device. Devices are connected physically through cables, enabling them to communicate within the network. The port and interface are often interchangeable terms for this connection.

Switches use various technologies to facilitate communication among devices connected to them. In Chapter 6, we'll go deeper into switch technologies and their functionalities.

- **2.2.3 Routers**

End hosts can be connected through a switch to allow communication within a LAN. Switches provide connectivity within the LAN, but to communicate with external networks, such as the internet, a router is needed. Routers connect LANs to external networks, as shown in Figure 2.5.

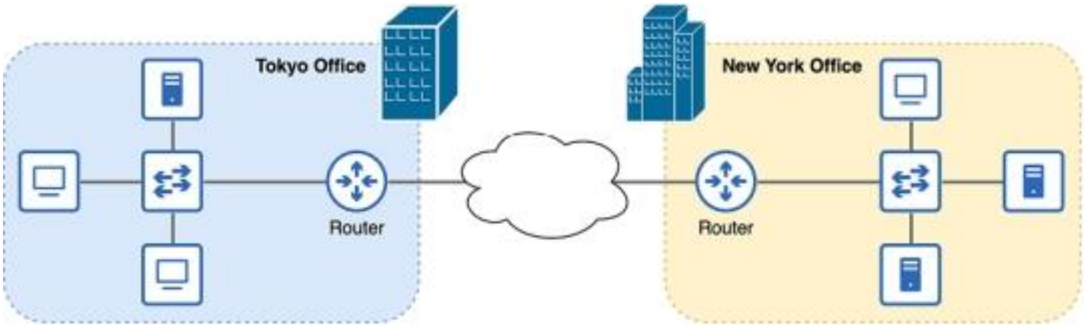


Figure 2.5: LANs Connected to the Internet via Routers

Note

The cloud symbol in network diagrams represents a larger network like the internet, which connects to LANs. Here, routers are used to enable communication between LANs and the internet.

Routers connect end hosts within a LAN, and they also facilitate communication between LANs and external networks, such as the internet.

Wireless routers often combine multiple networking functions into a single device, including routing, switching, wireless access points, and firewalls, making them ideal for small networks like home or small office setups.

- **2.2.4 Firewalls**

Firewalls protect networks by controlling communication between devices within the network and external networks like the internet. Firewalls are crucial in blocking unauthorized access and reducing security risks.

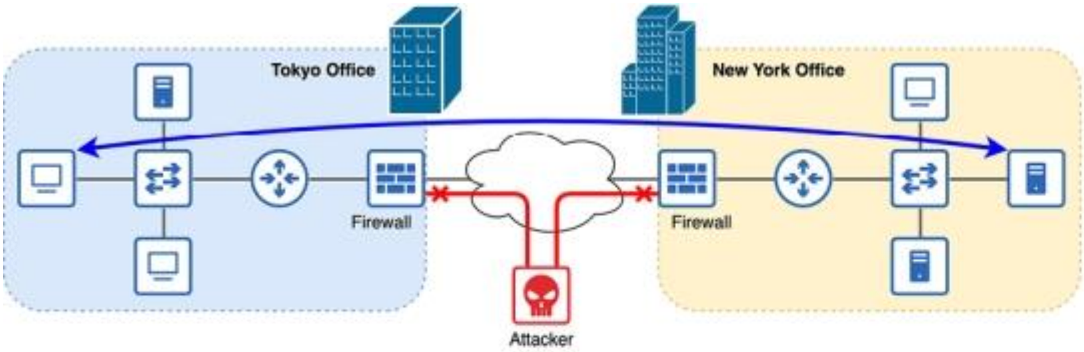


Figure 2.6: Firewalls Protecting Networks from Unauthorized Traffic

Firewalls act as security barriers, managing network traffic and blocking malicious traffic from entering the network.

There are two types of firewalls:

- Host-based Firewalls – Installed directly on individual devices, such as Windows Firewall, which filters traffic entering a single computer.
- Network Firewalls – Separate hardware devices used to protect larger networks. They inspect traffic entering and leaving the network and enforce rules to allow or block traffic accordingly.

Firewalls are essential for network security. In Chapter 11, we'll cover additional functionality and configurations of firewalls.

In Conclusion: Switches and routers form the backbone of network connectivity, while firewalls provide essential security. Understanding the basic roles of these components is fundamental for effective network management.

Summary

A local area network (LAN) is a group of interconnected devices in a limited area, such as an office.

A wide area network (WAN) is a network that extends over a large geographical area, such as between cities.

A computer network is a telecommunications network that allows nodes to share resources.

A node is any device that connects to a network: a personal computer, an iPhone, a router, etc.

A resource is anything that is shared over a network, such as a web page.

Various types of network devices are used to facilitate network communications.

Clients and servers are defined by their functions in relation to each other: clients access services provided by servers, and servers provide services for clients. Most types of devices can be both a client and a server.

Switches provide connectivity between devices in a LAN. They typically have many ports (24 to 48) for devices to connect to.

Routers provide connectivity between LANs and external networks, such as the internet.

A wireless router (Wi-Fi router/home router) is a multifunctional device that combines the roles of router, switch, wireless access point, and firewall.

Firewalls secure the network by inspecting traffic that enters or exits the network and allowing or denying it based on a set of configured rules.