Chapter 15 Computer Networks

Shambhavi Roy

Clinton Daniel
*University of South Florida, cedanie2@usf.edu*

Manish Agrawal
*University of South Florida, magrawal@usf.edu*

Follow this and additional works at: [https://digitalcommons.usf.edu/dit_tb_eng](https://digitalcommons.usf.edu/dit_tb_eng)

Scholar Commons Citation
[https://digitalcommons.usf.edu/dit_tb_eng/14](https://digitalcommons.usf.edu/dit_tb_eng/14)

This Book Chapter is brought to you for free and open access by the The Modernization of Digital Information Technology at Digital Commons @ University of South Florida. It has been accepted for inclusion in *FUNDAMENTALS OF INFORMATION TECHNOLOGY: Textbook – English* by an authorized administrator of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.
CHAPTER CONTENTS

Overview 324
  The Internet 325

TCP/IP Stack 326
  Physical Layer 327
  Data Link Layer 329
  Network Layer 331
  Transport Layer 332
  Application Layer 332

Networking Support Services 333

Computer Network Security 335

Chapter Terms and Definitions 337

Chapter Case: WHOIS Arianna’s Domain 338
Overview

The interconnection of information systems is an extremely important function in today’s personal, consumer, and business world. Many people stay connected with information available on the Internet by using virtual assistant technologies such as Amazon’s Alexa to purchase items online with their Amazon Prime account. Similarly, businesses are motivated to use interconnected devices to conduct daily tasks such as virtual meetings and email communication. In all these cases, computer networks are required to move information from one application operating on a computer to another. Computer networks can be defined as the interconnection of information systems through the use of components designed to communicate using standardized technologies.

Computers interact with networks by using specialized hardware components designed to communicate data in a very consistent way. In fact, today’s modern computer networks are the result of over 100 years of innovations engineered to communicate data. One of the earliest examples of using a network to communicate data from one device to another was the telegraph. Patented in 1840, the telegraph was a communications device used by Samuel Morse to send information to locations across great distances. To do this, the telegraph would connect and release a switch from a sender device that was designed to energize an electromagnet on a receiver device. Once the receiver’s electromagnet was energized, it would pull a marker to one side. The marker would then scratch a line on a paper at the receiver device. Morse then developed an encoding of the marks in the form of dots and dashes that today is known as Morse code. Morse code could be used to fully encode a message generated by energy that people can understand. For instance, the letter a is coded as a dot and a dash.

Since the invention of the telegraph, communication technologies have evolved considerably and eventually motivated the standardization of network architecture. In particular, when computers from different manufacturers in different countries needed to be networked together, the components had difficulty interoperating between the different networking equipment from the various vendors. It, therefore, became necessary to standardize computer networking technology. This problem motivated the standards organizations to develop models that could be adopted by the entire computer networking industry. The computer network industry could now innovate while complying with the standard model. For example, by developing components that offered standard interoperable functionality while consuming less power. We will learn more about these models and standards later in this chapter.
The Internet

Typically, when we talk about computer networks, we cannot escape a historical conversation about the Internet. What is the Internet and how did we get it? How does it help us today?

Put simply, the Internet can be defined as an interconnection of individual computers across the world through an interconnection of networks using a standardized set of communication protocols. The Internet allows people and systems to communicate in a consistent way as data moves across the multiple networks that are interconnected across the globe.

Consider a spiderweb, which has been spun by a spider. Each time the spider constructs a new direction in the web it is continuously connected to another portion of the web. You can trace multiple directions from any point within the spiderweb. The spiderweb design is similar to the concept of the Internet where computers are connected by specialized hardware, and you can trace their communication in multiple directions creating a web-like design.

When we think of the Internet, it's easy to relate it to what we know about the World Wide Web. The World Wide Web is what people use every day to do things like shop online, ask “Siri” (Apple’s digital assistant244) a question, or post videos to social media platforms such as Instagram.245 Historically, the World Wide Web grew in popularity through the use of web browser applications designed to enable people to navigate content in the form of webpages stored as documents on computers around the world. To navigate content and display it in a consistent way requires a standardized set of protocols. For instance, the Hypertext Transfer Protocol (HTTP) is an Internet protocol used by the World Wide Web that standardizes how documents such as webpages are transferred across systems.246 You can observe a secure version of HTTP called HTTPS if you type www.google.com in your Internet browser (Figure 240).

---


As seen in Figure 240, the browser navigation bar has applied the secure HTTPS protocol to communicate the Google home page document content to the screen. Internet browser applications, such as Google Chrome or Firefox, help keep us compliant with the HTTP protocol requirements of the Internet. This allows us to access content and documents across the World Wide Web without worrying about the complexities of the standardized communication.

**TCP/IP Stack**

As Internet technologies were standardized, they were eventually constructed as a stacked layer of technologies, specified as the Open Standards Interconnection (OSI) Model. Today, the OSI Model has been simplified using a core set of standardized technologies, which are described as the TCP/IP stack.

<table>
<thead>
<tr>
<th>Layer Number</th>
<th>Layer Name</th>
<th>Networking task</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Application</td>
<td>Specify the needs of users</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>Organize data for network transmission</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Identify and locate the destination network</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>Remove errors during transmission and label devices</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>Signals transmitted across a wire</td>
</tr>
</tbody>
</table>

The TCP/IP stack is a five-layered network architecture. The TCP/IP stack layers and their described functional networking tasks are described above, but includes some unfamiliar terms and technologies. Therefore, it makes sense to describe each layer in detail so that you can fully understand how the stack is used to support computer networks.
Physical Layer

The first thing needed for communication is the transmission of information over a distance. The physical layer of the TCP/IP stack does this and requires technology that can transmit signals across a physical medium. Different types of media include copper wire, optical fiber, or various forms of wireless communication (e.g., cellular and Wi-Fi). The signals are generated by capturing energy from an energy source and encoding the data using this energy for transmission over the physical medium.

Depending on the physical medium, signals are commonly transmitted as digital or analog. A digital signal is typically generated when an energy source transmitting the signal turns on and off. If the energy is present, we can measure the data as a 1. If the energy is absent, we can measure the data as a 0. Analog signals are generated by an energy source that applies continuous energy to the medium. This continuous signal changes in amplitude and frequency forming a sine wave as energy varies in intensity and time. Since an analog signal can be measured by amplitude and frequency, data can be encoded by varying the amplitude or frequency of the signal or both. Figure 241 illustrates the difference in how an analog versus a digital signal can be visualized.

![Figure 241](image)

The 1s and 0s data generated by signals traveling through a physical medium is commonly referred to as binary data. Binary data captured from signals can be encoded to represent characters that humans can understand. For instance, the American Standard Code for Information Interexchange (ASCII) includes numerical representations (decimals) that can be used to convert letters in the English language to binary data.247

---


---

**Hello**

The word “hello” can be represented as a binary number using the ASCII code.

<table>
<thead>
<tr>
<th>Character</th>
<th>ASCII Decimal</th>
<th>Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>104</td>
<td>01101000</td>
</tr>
<tr>
<td>e</td>
<td>101</td>
<td>01100101</td>
</tr>
<tr>
<td>l</td>
<td>108</td>
<td>01101100</td>
</tr>
<tr>
<td>l</td>
<td>108</td>
<td>01101100</td>
</tr>
<tr>
<td>o</td>
<td>111</td>
<td>01101111</td>
</tr>
</tbody>
</table>
Early physical media used in networks were made of copper wiring. In fact, today, copper wire exists in many office buildings and schools. You may have seen network plug outlets in your school walls with a cable plugged into it and attached on the other end to a teacher’s PC, laptop, or printer. Copper is an excellent conductor of electricity and can be used to carry signals across great distances. The most common type of network copper cable used today is called Cat5e, and it has a connector on its end called RJ45 (Figure 242).

As seen in Figure 242, Cat5e cable has four pairs of wires that are color coded. From left to right the pairs include White-Orange + Orange, White-Blue + Blue, White-Green + Green, and White-Brown + Brown. Each wire within the cable is carrying a different type of signal. Therefore, the color code sequence is important because it must match the signal sequence of receiving devices such as PCs, laptops, or printers.

Additionally, each of these colored wires is tightly twisted. The tight twisting of the copper wire improves the rate at which a signal can be transmitted through the cable. This also improves the speed of the data transfer on the network that the cable is connected to. Data transfer rate is measured in bits per second. For example, a Cat5e cable is capable of supporting network speeds up to 1000 Mbps (megabits per second). A bit is a small unit of data. A megabit represents a million bits. Therefore, Cat5e cable has tightly twisted copper wires capable of moving up to 1 million bits of data per second!

Another common physical medium used in networks is optical fiber. Optical fiber is typically bundled inside of fiber optic cable. Fiber optic cable is made up of a set of protected layers to prevent any damage to the inner glass fibers (Figure 243).

The inner glass fibers are typically the width of a human hair and designed to allow laser light to travel through the medium. Once an energy source generates a laser light it travels through the glass tube to its destination.

As the energized light signal is pulsed, or turned on and off, by a sending device (described in the “Data Link Layer” section below) it can be measured as data. Therefore, a light-sensitive receiver (also described in the “Data Link Layer” section) on the other end of the fiber optic cable can convert the pulses of light into a 1 or a 0. If light is present, the receiver can measure a 1 as data. If the light is absent, the receiver can measure a 0 as data.
Data Link Layer

Signals can get damaged while traveling through a medium. It is also necessary for devices to know if a signal is directed at them. Therefore, it is necessary to include a layer of technology that supports getting the signal to the desired destination without errors. The Data Link layer functions to provide both addressing and error detection.

Think about your home networks for a moment. You probably have devices such as PCs, smartphones, laptops, tablets, smart televisions, and network storage connected to the Internet on your home network. To make this network connection work, you will need a Router (described in the “Network Layer” section) between the devices, which is designed to connect to the Internet. We will talk more about what makes this possible later in this chapter.

We can use Figure 244 to imagine a scenario where you are using your laptop at home to complete a homework assignment that must be submitted online. I’m sure you would want your homework to find its way through the Internet to its final destination and arrive there in the exact state as you completed it, with no errors. This is where the Data Link layer is necessary.

Whether it is wireless or wired, you will have a connection between your home device and your home router. This connection is considered an instance of the Data Link layer. For example, your home laptop contains hardware that has a wireless network interface card (WNIC) built inside. The word interface is referenced in the WNIC hardware name because it describes the technology used to make the connection between the laptop and the home router or other networking device. Interface is a commonly used term in networking to describe the connection between devices.

Each WNIC, or any other type of network interface card (NIC), has what is called a Media Access Control (MAC) address, also called a physical address. The MAC address is a unique identifier assigned by the manufacturer of the hardware. If you were to open your laptop or other device, you may see the MAC address labeled on the hardware. But when you are connected to the Internet there are easier ways of discovering the MAC address you are currently using on a device. For instance, if you own a laptop with Microsoft Windows installed you can run a command within a command prompt that will output the MAC address actively being used by your WNIC. Here is an example of what some of the output would look like if you typed the command “ipconfig/ all” from a Microsoft Windows command prompt from a laptop that is actively connected to a wireless network:

```
C:\Users\clinton> ipconfig /all
```

Example of partial output from the above command (Note: your output will have different information than this one):
Wireless LAN adapter Wi-Fi:

Description: Intel® Wi-Fi AX200 160Hz

Physical Address: 6D-B1-00-5U-03-9R

DHCP Enabled: Yes

IPv4 Address: 192.168.1.26

In the above example of output from the “ipconfig /all” command, you can see that the Microsoft Windows operating system has identified that the active interface connection is using a WNIC described as “Intel Wi-Fi AX200 160Hz” with the physical address, or MAC address, of 6D-B1-00-5U-03-9R. In this case, the Data Link layer is implemented within the WNIC where the physical address can be used to uniquely identify a device connected to a network. Circling back to the homework example we mentioned earlier, the physical address plays an important role in making sure that your homework finds its way toward its final destination. Other technologies that support the Data Link layer and your homework finding its way also work similarly, as we will describe in detail later.

The Data Link layer not only functions to provide addressing, it also serves the function of error detection. There must be a technology within a layer of the TCP/IP stack that can detect if any errors were introduced during the transmission of a signal. Errors can occur when a signal is disrupted by events such as power outages or power spikes. When events like this occur, there must be a technology capable of detecting errors to improve the reliability of the network.

Errors are typically detected on a network using specialized algorithms. This is where mathematicians really get to use their skills. The algorithm used by networks to detect errors is known as a cyclic redundancy check (CRC). CRC uses Modulo 2 arithmetic to reliably calculate bit-level errors on binary (1s and 0s) data that may occur during network communication. These algorithms are always getting better and will keep mathematicians in business for many years to come.

Let’s look at a simple error-detection algorithm example that’s easy to understand, though not robust enough for industrial use. Recall that an algorithm is a set of steps used to accomplish a desired output. In this case we are constructing an algorithm designed to detect an error in the transmitted data.

Let’s say we want to send HELLO in a text message. We could code the letters in integer format as 8 5 12 12 15 based on their integer position in the English alphabet. In other words, the letter H is in the 8th position of the English alphabet while E is in the 5th position and so on. A simple algorithm first step would be to add all integers together to get the single integer value of 52.

\[ 8 + 5 + 12 + 12 + 15 = 52 \]

Now add 5 and 2.

\[ 5 + 2 = 7 \]

Now, the technology would send a text with the integer values of the letters HELLO as:

8 5 12 12 15 7

Where 7 is appended to the integer encoded version of HELLO.

Now, let’s try to detect an error when our technology receives the text message.
The receiver technology will get $8\ 5\ 12\ 12\ 15\ 7$

The receiver knows that the 7 is extra data, so it calculates:

$$8 + 5 + 12 + 12 + 15 = 52$$

Then it calculates: $5 + 2 = 7$

Now the receiver technology can interpret the HELLO text message, represented by integers in the data received, as having no errors because the calculated result 7 matches the extra data labeled as 7 on the end of the text message.

This simple algorithm is easy to understand but it certainly has flaws. For instance, what if the receiver technology received $8\ 5\ 11\ 13\ 15\ 7$ or $10\ 5\ 11\ 11\ 15\ 7$. Both integer combinations will sum to 52. But they are messages with errors. The first one would translate to HEKMO while the second one would translate to JEKKO. These text messages are certainly not HELLO, but our simple algorithm would not detect the error. If you can imagine the power of this simple algorithm example, you can then understand how mathematicians can improve the accuracy of the algorithm so that it can detect all possible errors. This is just one example of why math plays a critical role in technology.

**Network Layer**

While the Data Link layer is responsible for the connections between devices on a single network, the Network layer’s function is to transfer packets of data from a source computer, such as a laptop on your home network, to a destination computer through one or more networks. This task is also called routing and is performed by networking devices called routers. You may have a router in your home, that was supplied by your Internet service provider, which allows you to connect your home devices to resources across the global Internet (Figure 245).

As previously mentioned, the Network layer functions to transfer packets across multiple networks. A packet of data is a small segment of a larger piece of data sent over a network. For example, consider a scenario where you are using the Internet to research a topic on the World Wide Web for your homework assignment. As you open a webpage (described later in the “Application Layer” section of this chapter) with your browser, packets of data are being sent across the Internet from a webserver somewhere in the world to your laptop. All the content included on the website is not being sent as one large file. Instead, the website data would be broken into small packets of data prior to being transmitted over the Internet. Once the packets reach their destination, they will be reassembled into their original form so that the complete webpage can be viewed in your browser. This reassembly process is handled by the “Transport Layer,” which we will cover later in this chapter.

Communicating signals and data over networks involves the use of standard protocols. The most common protocol used at the Network layer is the Internet Protocol (IP). You may have noticed that this protocol is part of the name included in TCP/IP stack. This is because IP plays an essential role in the Network layer and is the standard responsible for routing packets across interconnected networks. IP is managed on networks by professionals who configure routers and facilitate routing by assigning IP addresses to devices.
addresses to devices. An IP address is a unique identifier that has been assigned to devices accessing a network. Unlike a MAC address, which is uniquely assigned by a hardware manufacturer, an IP address is automatically or manually assigned by technology designed to manage devices connecting to a local network or the Internet.

For example, in the “Data Link Layer” section of this chapter we reviewed the output of a Microsoft Windows command “ipconfig /all.” In the output of this command, you may have noticed:


The 192.168.1.26 is the unique IP address assigned to the device connected to the Internet.

Additionally, you will notice in the output of the command “IPv4.” This indicates IP version 4. This version contains 4 sections of integer values ranging from 0 to 255 and separated by periods. So, IP addresses range from 0.0.0.0 to 255.255.255.255. This version of the IP address was created in an early period where most experts thought that at most, the world would have one computer-connected device per person on the planet. IPv4 could support $2^{32}$ or about 4.29 billion devices. This was enough to assign one IP address per person at the time IPv4 was created. But today, many users have multiple devices, and we began running out of IPv4 addresses. So IPv6 was created that allows up to $2^{128}$ or approximately 340,282,366,920,938,463,463,374,607,431,768,211,456 devices! The IPv6 address is significantly longer and consists of integers and letters. Here is a sample of what an IPv6 address looks like:


Each of the four characters are separated by a colon. As you can see, it contains more information that can be used to support a lot more IP address combinations than IPv4.

**Transport Layer**

The Transport layer functions to ensure that data is reliably delivered to its destination over a network. To do this the Transport layer includes technology designed to track data as it is broken down into small segments. Segmentation is the process of breaking data down into smaller units to allow for a more compact transmission over a network using IP. This is useful because IP has a limitation on the size of packets it can transfer over a network. Once a receiving technology receives all the segmented data, the Transport layer is then responsible for reassembling these segmented packets of data back into their original form so that they can be used by an application such as a web browser.

The most common Transport layer protocol is the Transmission Control Protocol (TCP). Notice that TCP, just like IP, is part of the TCP/IP stack name. Applications like email can transfer data, such as an email message, to TCP so that the data can be broken into small segments before being transmitted to a destination on the Internet. These segments are assigned sequence numbers so that the receiving technology at the Internet destination knows how to logically reorder and reassemble to email message data back into its original format before handing it off to the receiving email application.

**Application Layer**

Since the Transport layer handles all details of transmitting data over a network, this opens tremendous potential for the development of applications. The Application layer functions to support the needs of technology users. If you want to send an email from your laptop or text a message to your friends
from your smartphone, you will need to use an application specialized for the task. TCP will make sure that the data is reliably sent across the Internet to your friends. This functional relationship between layers that support the Internet is why we call the technology stack TCP/IP.

With the support of the Application layer, the technology industry has invented many functional uses for the Internet to fit our daily lives. This table summarizes five common application protocols that have been developed to support a variety of applications.

### Common Application Layer Protocols

<table>
<thead>
<tr>
<th>Application Protocol</th>
<th>Functional Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP (Hyper Text Transfer Protocol)</td>
<td>Used in the World Wide Web to communicate data from webpages</td>
</tr>
<tr>
<td>SMTP (Simple Mail Transfer Protocol)</td>
<td>Used to send and receive email</td>
</tr>
<tr>
<td>FTP (File Transfer Protocol)</td>
<td>Used to communicate and transfer files between computers</td>
</tr>
<tr>
<td>SSH (Secure Shell)</td>
<td>Used to send commands between computers</td>
</tr>
<tr>
<td>IM (Instant Messaging)</td>
<td>Used to exchange text-based messages using computers or mobile devices</td>
</tr>
</tbody>
</table>

As you can see, the Application layer is the most practical layer that Internet users can relate to. These application protocols support many of our daily personal, professional, and academic uses for the Internet. So, whether you are using an app on your smartphone or working on an assignment using your school device, you are being supported by the Application layer of the TCP/IP stack.

### Networking Support Services

Services have been developed over time to support the use of Internet applications communicating on the TCP/IP stack. For instance, in order for an application to communicate on a network it needs to operate on a device that has been assigned an IP address. The Dynamic Host Configuration Protocol (DHCP) service was developed to manage the assignment of IP addresses on a network. This service is commonly used in places such as schools or businesses where people need to connect to the Internet.

Consider a scenario where you are at school, and you turn on your device to join the network so you can use the Internet. As soon as your device is turned on, the operating system is seeking an available network to connect to. If the network allows you to connect to it, a DHCP service assigns your device an IP address on the network. This assigned IP address is then used by your device so that you can operate applications capable of communicating on the Internet.

Another common service used on computer networks is the Domain Name Service (DNS). This service is used by the Domain Name System, which includes a set of databases responsible for translating IP addresses into domain names. To see DNS in action, you can execute a WHOIS query. A WHOIS query is used to check publicly available databases to identify who owns a domain. Additionally, you can check the DNS records to determine what IP addresses are owned and associated with the domain name.
To conduct a WHOIS query, open your browser and navigate to https://who.is/. Note, you can Google WHOIS and the search results will recommend many WHOIS query tools. Any of these will work just as well. Once you are on the who.is site, type usf.edu in the search bar and click the search button (Figure 246).

Your WHOIS query will result in lots of contact and other information about usf.edu. For instance, usf.edu was activated on September 29, 1986, and is registered by the University of South Florida Information Technology at 4202 E. Fowler Avenue, SVC 4010 Tampa, Florida 33620 USA. This information may be useful for anyone who is trying to investigate the owner and support for any specific domain.

Next, click on the “DNS Records” button to view a report on the records documented over time with the usf.edu domain. Make a special note of the entry next to www.usf.edu under the “Hostname” column (Figure 247).

As seen in Figure 247, www.usf.edu is used to respond to any Internet requests on the World Wide Web and it is assigned the IP address 52.149.184.58. If you were to navigate to www.usf.edu with your Internet browser, you would actually be navigating to the IP address 52.149.184.58. However, DNS translates this IP address into a domain name that humans can easily remember and understand.

Overall, many networking support services exist to promote the use of networks and their technologies. Information technology professionals make a career out of supporting, managing, and implementing these services in an enterprise business environment that supports people and business processes.
College degree programs and industry certifications have developed entire curriculums to support the knowledge and expertise needed to support the technologies of today and tomorrow. Therefore, it is a worthy investment to learn more about these services, if you are interested in a future career in technology.

**Computer Network Security**

Networks were originally motivated and designed around the concept of communication through technology. As you may have noticed throughout this chapter, these technologies were not designed to consider the risks of intentional harm to the systems or data as a result of a cyber-attack. You will learn more about cybersecurity in the “Cybersecurity” chapter of this textbook. For now, let’s consider a cyber-attack as an attempt by a malicious person or program to damage or destroy a computer network and the systems that support it. There are daily attacks on computer networks in our homes, schools, and business. Protecting networks using security technology is a necessity in today’s world.

One specific and important security technology that is designed to protect networks is a firewall. A firewall is a computer that is positioned on the network between the devices used inside a network and the outside world. The firewall computer keeps a careful eye on all the incoming network traffic and applies filters that can block any unwanted or malicious packets. The filters are configured by IT professionals who can assign a set of rules that are designed to identify known harmful network traffic.

Firewalls keep us all safe when we use our devices to communicate on the Internet. However, malicious people are always trying to get past these protective firewalls to cause harm to our systems. This is why for years to come cybersecurity professionals will continue to be in high demand.

There are some simple things that we can do to protect the security of our networks. Two such easy security practices include patching our systems and making sure that we communicate on our networks using secure methods. Patching systems basically involves keeping our software and operating systems up to date with the latest security updates. It is common among software and hardware vendors to discover weaknesses in their products that may expose vulnerabilities to a cyber-attack. To prevent these attacks from occurring, the vendors recommend that we update our systems by downloading and installing these patches.

Communicating on a network securely typically involves the use of encryption technologies. Put simply, encryption is the process where you use an algorithm to scramble data into a secret encoded message that can only be unlocked with a unique and guarded key. One such type of encryption uses a digital certificate. Digital certificates are issued by certificate authorities. You can use these digital certificates to encrypt data being transmitted over a network such as an email, text, or instant message.

To understand how encryption technologies work, consider the following simple example. You have a text message consisting of the word “hello” that you are about to send to your friend using your smartphone app.

Swap each letter with the one that holds its opposite position in the alphabet. For example, “a” would be swapped with “z” and “b” would be swapped with “y” and so on.

So, the encrypted version of “hello” would be “svool.”
The receiving technology would then need to have a key to unlock the algorithm. In other words, the receiver knows the algorithm used to scramble the letters and can execute the swap in reverse to translate “swool” back into “hello.”

This simple encryption example is useful to understand the concept. However, in practice the method to this algorithm could be leaked somewhere on the Internet and malicious people could write a simple program to decrypt all your network communication. This is why it is important to use strong algorithms that are so complex that it would be impractical for anyone to decrypt. You will learn more about the complexities of cybersecurity in the “Cybersecurity” chapter of the textbook.
**Encryption**: The use of an algorithm to scramble data into a secret encoded message that can only be unlocked with a unique and guarded key.

**Hypertext Transfer Protocol (HTTP)**: An Internet protocol used by the World Wide Web that standardizes how documents such as webpages are transferred across systems.

**Interface**: A networking term that describes the interconnection between a computing device, such as a laptop or smartphone, to a network.

**Internet**: An interconnection of individual computers across the world through an interconnection of networks using a standardized set of communication protocols.

**Internet Protocol (IP)**: A network layer protocol responsible for routing packets across interconnected networks.

**Media Access Control (MAC) Address**: Commonly known as a physical address; a unique identifier consisting of numbers and letters assigned to network interface hardware and used as the identity of a network address.

**Open Standards Interconnection (OSI) Model**: A conceptual stack of technologies that could be used to describe the various functions of a networked system.

**Packet**: A small segment of a larger piece of data sent over a network.

**Transmission Control Protocol (TCP)**: A reliable transport layer protocol that enables applications to exchange data over a network.

**World Wide Web**: An information system designed to display content in the form of documents, such as webpages, which are stored on computers across the world.
WHOIS Arianna’s Domain

Arianna has just learned about the World Wide Web and how it works. She was given an assignment by her teacher to come up with an online business idea. The online business should include a website that is available for her customers to use from any network across the world. Arianna knew this meant she had to purchase a domain and have it registered so that it is available to Domain Name Systems throughout the globe. To do this, Arianna needs to think of a unique domain name and complete a WHOIS query to see if it’s available. Basically, she must pick a domain name that nobody in the world has actively registered.

Question 1: Think of an online business idea. Now describe your online business in one or two sentences. Think of a unique domain name to use with your business and conduct a WHOIS query on the Internet to see if it’s available. If the domain name is already registered by someone else, think of another name. Continue to conduct WHOIS queries until you have identified a domain name that has not been registered by someone else. Write your domain name here.

Question 2: Now that you have explained your online business idea, use the Internet to conduct multiple WHOIS queries to identify at least one other company who has registered a domain name with a similar online business model idea. In other words, another company who may be a potential competitor. List all the information reported in that companies WHOIS query.