**KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**CHEMICAL ENGINEERING DEPARTMENT**

**CHE 158: INTRODUCTION TO INFORMATION TECHNOLOGY**

**INSTRUCTOR:** Dr. (Mrs.) Mizpah A. D. Rockson

LECTURE 9: **COMMUNICATIONS AND NETWORKS**

**Learning Objectives**

At the end of the lecture the student is expected to be able to do the following:

1. Explain connectivity, the wireless revolution, and communication systems.
2. Describe physical and wireless communication channels.
3. Differentiate between connection devices and services including dial-up, DSL, cable, satellite, and cellular.
4. Describe data transmission factors, including bandwidth and protocols.
5. Define networks and key network terminology including network interface cards and network operating systems.
6. Describe different types of networks, including local, home, wireless, personal, metropolitan, and wide area networks.
7. Describe network architectures, including topologies and strategies.
8. Explain the organization issues related to Internet technologies and network security.

**9.0 Introduction**

We can communicate almost instantaneously with others worldwide; changing events from the smallest of countries and places are immediately broadcast to the world; our e-mail messages are delivered to handheld devices; cars access the Internet to provide driving instructions and solve mechanical problems. Even household appliances can connect to the Internet and be remotely controlled. The communications and information options we have at our fingertips have changed how we react and relate to the world around us.

As the power and flexibility of our communication systems have expanded, the sophistication of the networks that support these systems has become increasingly critical and complex. The network technologies that handle our cellular, business, and Internet communications come in many different forms. Satellites, broadcast towers, telephone lines, even buried cables and fiber optics carry our telephone messages, e-mail, and text messages. These different networks must be able to efficiently and effectively integrate with one another.

**9.1 Communications**

Computer communications is the process of sharing data, programs, and information between two or more computers. We have discussed numerous applications that depend on communication systems, including

* **E-mail** —provides a fast, efficient alternative to traditional mail by sending and receiving electronic documents.
* **Instant messaging** —supports direct, “live” electronic communication between two or more friends or buddies.
* **Internet telephone** —provides a very low-cost alternative to long-distance telephone calls using electronic voice and video delivery.
* **Electronic commerce** —buying and selling goods electronically.

In this chapter, we will focus on the communication systems that support these and many other applications. Connectivity, the wireless revolution, and communication systems are key concepts and technologies for the 21st century.

**9.1.1 Connectivity**

**Connectivity** is a concept related to using computer networks to link people and resources. For example, connectivity means that you can connect your microcomputer to other computers and information sources almost anywhere. With this connection, you are linked to the world of larger computers and the Internet.

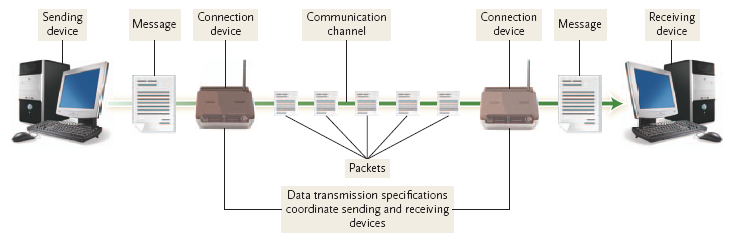
**9.1.2 Wireless communication**

The single most dramatic change in connectivity and communications in the past few years has been the widespread use of mobile telephones with wireless Internet connectivity. Students, parents, teachers, businesspeople, and others routinely talk and communicate with these devices. It is estimated that over 3 billion mobile telephones are in use worldwide. This wireless technology allows individuals to stay connected with one another from almost anywhere at any time.

**So what’s the revolution**? While wireless technology was originally used primarily for voice communications, today’s cell phones support e-mail, Web access, and a variety of Internet applications. In addition, wireless technology allows a wide variety of nearby devices to communicate with one another without any physical connection. You can share a high-speed printer, share data files, and collaborate on working documents with a nearby co-worker without having your computers connected by cables or telephone—wireless communication. High speed Internet wireless technology allows individuals to connect to the Internet and share information from almost anywhere in the world. **Is this revolution**? Yes and it is just the beginning!

**9.1.3 Communication systems**

**Communication systems** are electronic systems that transmit data from one location to another. Whether wired or wireless, every communication system has four basic elements.



**Figure 9.1: Basic elements of a communication system**

* **Sending and receiving devices.** These are often a computer or specialized communication device. They originate (send) as well as accept (receive) messages in the form of data, information, and/or instructions.
* **Communication channel.** This is the actual connecting or transmission medium that carries the message. This medium can be a physical wire or cable, or it can be wireless.
* **Connection devices.** These devices act as an interface between the sending and receiving devices and the communication channel. They convert outgoing messages into packets that can travel across the communication channel. They also reverse the process for incoming messages.
* **Data transmission specifications.** These are rules and procedures that coordinate the sending and receiving devices by precisely defining how the message will be sent across the communication channel.

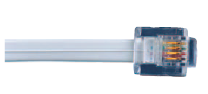
**9.2 Communication channels**

**Communication channels** are an essential element of every communication system. These channels actually carry the data from one computer to another. There are two categories of communication channels. One category connects sending and receiving devices by providing a physical connection, such as a wire or cable. The other category is wireless.

**9.2.1 Physical connection**

Physical connections use a solid medium to connect sending and receiving devices. These connections include telephone lines (twisted pair), coaxial cable, and fiber-optic cable.

* **Twisted-pair cable** consists of pairs of copper wire that are twisted together. Both standard **telephone lines** and **Ethernet cables** use twisted pair. Ethernet cables are often used in networks and to connect a variety of components to the system unit.

**Figure 9.2: Twisted-pair cable Figure 9.3: Coaxial cable**

* **Coaxial cable,** a high-frequency transmission cable, replaces the multiple wires of telephone lines with a single solid-copper core. In terms of the number of telephone connections, a coaxial cable has over 80 times the transmission capacity of twisted pair. Coaxial cable is used to deliver television signals as well as to connect computers in a network.
* **Fiber-optic cable** transmits data as pulses of light through tiny tubes of glass. In terms of the number of telephone connections, fiber-optic cable has over 26,000 times the transmission capacity of twisted-pair cable. Compared to coaxial cable, it is lighter, faster, and more reliable at transmitting data. Fiber-optic cable is rapidly replacing twisted-pair cable telephone lines.



**Figure 9.4: Fiber-optic cable**

**9.2.2 Wireless connection**

Wireless connections do not use a solid substance to connect sending and receiving devices. Rather, they move data through the air. Primary technologies used for wireless connections are radio frequency, microwave, satellite, and infrared.

* **Radio frequency (RF)** uses radio signals to communicate between wireless devices. For example, smartphones and many Internet-enabled devices use RF to place telephone calls and/or to connect to the Internet. Most home or business wireless networks are based on a technology called **Wi-Fi (wireless fidelity)** to communicate over short distances. A number of standards for Wi-Fi exist, and each can send and receive data at a different speed.

**Bluetooth** is a short-range radio communication standard that transmits data over short

distances of up to approximately 33 feet (about 10 meters). Bluetooth is widely used for

wireless headsets, printer connections, and handheld devices. The range of Wi-Fi networks

is being extended over greater distances using a new technology known as **WiMax**

**(Worldwide Interoperability for Microwave Access).** WiMax is commonly used by

universities and others to extend the capability of existing Wi-Fi networks.

* **Microwave** communication uses high-frequency radio waves. Like infrared, microwave communication provides line-of-sight communication because microwaves travel in a straight line. Because the waves cannot bend with the curvature of the earth, they can be transmitted only over relatively short distances. Thus, microwave is a good medium for sending data between buildings in a city or on a large college campus. For longer distances, the waves must be relayed by means of microwave stations with microwave dishes or antennas.



**Figure 9. 5: Microwave dish**

* **Satellite** communication uses satellites orbiting about 22,000 miles above the earth as microwave relay stations. Many of these are offered by Intelsat, the International Telecommunications Satellite Consortium, which is owned by 114 governments and forms a worldwide communication system. Satellites rotate at a precise point and speed above the earth. They can amplify and relay microwave signals from one transmitter on the ground to another. Satellites can be used to send and receive large volumes of data. **Uplink** is a term relating to sending data to a satellite. **Downlink** refers to receiving data from a satellite. The major drawback to satellite communication is that bad weather can sometimes interrupt the flow of data.

One of the most interesting applications of satellite communications is for global positioning. A network of 24 satellites owned and managed by the Defense Department continuously sends location information to earth. **Global positioning system (GPS)** devices use that information to uniquely determine the geographical location of the device.

* **Infrared** uses infrared light waves to communicate over short distances. It is sometimes referred to as line-of-sight communication because the light waves can only travel in a straight line. This requires that sending and receiving devices must be in clear view of one another without any obstructions blocking that view. One of the most common applications is to transfer data and information from a portable device such as a notebook computer or PDA to a desktop computer.

**9.3 Connection devices**

At one time nearly all computer communication used telephone lines. However, because the telephone was originally designed for voice transmission, telephones typically send and receive **analog signals,** which are continuous electronic waves. Computers, in contrast, send and receive **digital** **signals.** These represent the presence or absence of an electronic pulse—the on/off binary signals. To convert the digital signals to analog signals and vice versa, you need a modem.

Analog signal Digital signal

**9.3.1 Modem**

The word **modem** is short for *modulator-demodulator.* **Modulation** is the name of the process of converting from digital to analog. **Demodulation** is the process of converting from analog to digital. The modem enables digital microcomputers to communicate across different media, including telephone wires, cable lines, and radio waves.

The speed with which modems transmit data varies. This speed, called **transfer rate,** is typically measured in **thousands of bits (kilobits)** **per second (Kbps).** The higher the speed, the faster you can send and receive information.

There are four commonly used types of modems: telephone, DSL, cable, and wireless.

* A **telephone modem** is used to connect a computer directly to a telephone line. These modems can be either internal or external. Internal modems are on an expansion card that plugs into a slot on the system board. An external modem is typically connected to the system unit through a serial or USB port.
* A **DSL (digital subscriber line)** modem uses standard phone lines to create a high-speed connection directly to your phone company’s offices. These devices are usually external and connect to the system unit using either USB or Ethernet ports.
* A **cable modem** uses the same coaxial cable as your television. Like a DSL modem, a cable modem creates high-speed connections using the system unit’s USB or Ethernet port.
* A **wireless modem** is also known as a **WWAN (wireless wide area network) modem.** It is usually a small plug-in USB or ExpressCard device that provides very portable high-speed connectivity from virtually anywhere.

**9.3.2 Connection service**

While the special high-speed lines are too costly for most individuals, Internet service providers do provide affordable connections. For years, individuals relied on **dial-up services** using existing telephones and telephone modems to connect to the Internet. This type of service has been replaced by higher-speed connection services including DSL, cable, satellite, and cellular services.

* **Digital subscriber line (DSL) service** is provided by telephone companies using existing telephone lines to provide high-speed connections. **ADSL (asymmetric digital subscriber line)** is one of the most widely used types of DSL. DSL is much faster than dial-up.
* **Cable service** is provided by cable television companies using their existing television cables. These connections are faster than DSL.
* **Satellite connection services** use satellites to provide wireless connections. While slower than DSL and cable modem, satellite connections are available almost anywhere using a satellite-receiving disk.
* **Cellular services** use **3G** and **4G cellular networks** to provide wireless connectivity to the Internet. Although not as fast as the other services, cellular services are rapidly growing in popularity for mobile devices such as cell phones and other portable devices.

**9.4 Data transmission**

Several factors affect how data is transmitted. These factors include bandwidth and protocols.

**9.4.1 Bandwidth**

**Bandwidth** is a measurement of the width or capacity of the communication channel. Effectively, it means how much information can move across the communication channel in a given amount of time. For example, to transmit text documents, a slow bandwidth would be acceptable. However, to effectively transmit video and audio, a wider bandwidth is required. There are four categories of bandwidth.

* **Voiceband,** also known as **low bandwidth,** is used for standard telephone communication. Microcomputers with telephone modems and dial-up service use this bandwidth. While effective for transmitting text documents, it is too slow for many types of transmission, including high-quality audio and video.
* **Medium band** is used in special leased lines to connect minicomputers and mainframes as well as to transmit data over long distances. This bandwidth is capable of very high-speed data transfer.
* **Broadband** is widely used for DSL, cable, and satellite connections to the Internet. Several users can simultaneously use a single broadband connection for high-speed data transfer.
* **Baseband** is widely used to connect individual computers that are located close to one another. Like broadband, it is able to support high-speed transmission. Unlike broadband, however, baseband can only carry a single signal at one time.

**9.4.2 Protocols**

For data transmission to be successful, sending and receiving devices must follow a set of communication rules for the exchange of information. These rules for exchanging data between computers are known as **protocols.**

The standard protocol for the Internet is **TCP/IP (transmission control protocol/Internet protocol).** The essential features of this protocol involve

(1) identifying sending and receiving devices and (2) breaking information into small parts for transmission across the Internet.

* **Identification:** Every computer on the Internet has a unique numeric address called an **IP address (Internet protocol address).** Similar to the way a postal service uses addresses to deliver mail, the Internet uses IP addresses to deliver e-mail and to locate Web sites. Because these numeric addresses are difficult for people to remember and use, a system was developed to automatically convert text-based addresses to numeric IP addresses. This system uses a **domain name server (DNS)** that converts text-based addresses to IP addresses. For example, whenever you enter a URL, say www.computing-2012.com, a DNS converts this to an IP address before a connection can be made.



**Figure 9.6: DNS converts text-based addresses to numeric IP addresses**

* **Packetization:** Information sent or transmitted across the Internet usually travels through numerous interconnected networks. Before the message is sent, it is reformatted or broken down into small parts called **packets.** Each packet is then sent separately over the Internet, possibly traveling different routes to one common destination. At the receiving end, the packets are reassembled into the correct order.

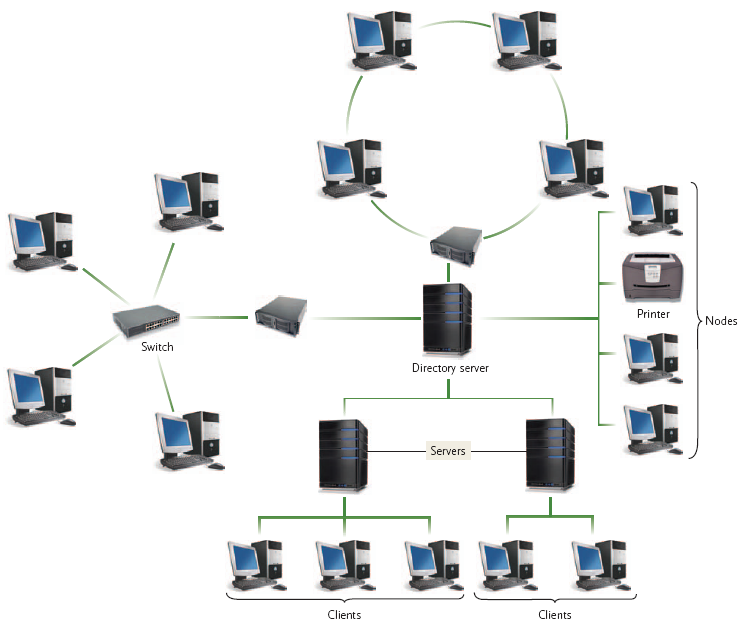
**9.5 Network**

A **computer network** is a communication system that connects two or more computers so that they can exchange information and share resources. Networks can be set up in different arrangements to suit users’ needs.

**9.5.1 Terms**

There are a number of specialized terms that describe computer networks. These terms include

* **Node** —any device that is connected to a network. It could be a computer, printer, or data storage device.
* **Client** —a node that requests and uses resources available from other nodes. Typically, a client is a user’s microcomputer.
* **Server** —a node that shares resources with other nodes. Dedicated servers specialize in performing specific tasks. Depending on the specific task, they may be called an application server, communication server, database server, file server, printer server, or Web server.
* **Directory server** —a specialized server that manages resources, such as user accounts, for an entire network.
* **Host** —any computer system that can be accessed over a network.
* **Switch** —central node that coordinates the flow of data by sending messages directly between sender and receiver nodes. A **hub** previously filled this purpose by sending a received message to all connected nodes, rather than just the intended node.



**Figure 9.7: Computer network**

* **Network interface cards (NIC)** —these are expansion cards located within the system unit that connect the computer to a network. Sometimes, they are referred to as LAN adapter.
* **Network operating systems (NOS)** —control and coordinate the activities of all computers and other devices on a network. These activities include electronic communication and the sharing of information and resources.
* **Network administrator** —a computer specialist responsible for efficient network operations and implementation of new networks.

A network may consist only of microcomputers, or it may integrate microcomputers or other devices with larger computers. Networks can be controlled by all nodes working together equally or by specialized nodes coordinating and supplying all resources. Networks may be simple or complex, self-contained or dispersed over a large geographical area.

**9.6 Network types**

Networks also may be citywide and even international, using both cable and wireless connections. Local area, metropolitan area, and wide area networks are distinguished by the geographical area they serve.

**9.6.1 Local area network**

Networks with nodes that are in close physical proximity—within the same building, for instance—are called **local area networks (LANs).** Typically, LANs span distances less than a mile and are owned and operated by individual organizations. LANs are widely used by colleges, universities, and other types of organizations to link microcomputers and to share printers and other

resources.

The LAN provides two benefits: economy and flexibility. People can share costly equipment. For instance, the four microcomputers share the laser printer and the file server, which are expensive pieces of hardware. Other equipment or nodes also may be added to the LAN—for instance, more microcomputers, a mainframe computer, or optical disc storage devices. Additionally, the **network gateway** is a device that allows one LAN to be linked to other LANs or to larger networks.

There are a variety of different standards or ways in which nodes can be connected to one another and ways in which their communications are controlled in a LAN. The most common standard is known as **Ethernet.** LANs using this standard are sometimes referred to as Ethernet LANs.

**9.6.2 Home network**

While LANs have been widely used within organizations for years, they are now being commonly used by individuals in their homes and apartments. These LANs, called **home networks,** allow different computers to share resources, including a common Internet connection. Computers can be connected in a variety of ways, including electrical wiring, telephone wiring, and special cables. One of the simplest ways, however, is without cables, or wireless.

**9.6.3 Wireless LAN**

A wireless local area network is typically referred to as a **wireless LAN (WLAN).** It uses radio frequencies to connect computers and other devices. All communications pass through the network’s centrally located **wireless access point** or **base station.** This access point interprets incoming radio frequencies and routes communications to the appropriate devices.

**9.6.4 Personal area network**

A **personal area network (PAN)** is a type of wireless network that works within a very small area—your immediate surroundings. PANs connect cell phones to headsets, PDAs to other PDAs, keyboards to cell phones, and so on. These tiny, self-configuring networks make it possible for all of our gadgets to interact wirelessly with each other. The most popular PAN technology is Bluetooth, with a maximum range of around 30 feet (10 m).

**9.6.5 Metropolitan area network**

The next step up from the LAN is the **MAN** —the **metropolitan area network.** MANs span distances up to 100 miles. These networks are frequently used aslinks between office buildings that are located throughout a city.Unlike a LAN, a MAN is typically not owned by a single organization.Rather, it is either owned by a group of organizations who jointly own andoperate the network or by a single network service provider who provides networkservices for a fee.

**9.6.6 Wide area network**

**Wide area networks (WANs)** are countrywide and worldwide networks. These networks provide access to regional service (MAN) providers and typically span distances greater than 100 miles. They use microwave relays and satellites to reach users over long distances. Of course, the widest of all WANs is the Internet, which spans the entire globe.

**9.7 Network architecture**

**Network architecture** describes how a network is arranged and how resources are coordinated and shared. It encompasses a variety of different network specifics, including network topologies and strategies. Network topology describes the physical arrangement of the network. Network strategies define how information and resources are shared.

**9.7.1 Topologies**

A network can be arranged or configured in several different ways. This arrangement is called the network’s **topology.** While many different topologies can be used for networks, six basic categories represent the past and present.

The past is represented by two network topologies that can still be found today. They are:

* **Bus network** —each device is connected to a common cable called a **bus** or backbone and all communications travel along this bus.
* **Ring network** —each device is connected to two other devices, forming a ring. When a message is sent, it is passed around the ring until it reaches the intended destination.

The present is represented by four network topologies that are widely used today. These current network topologies are:

* **Star network** —each device is connected directly to a central network switch. Whenever a node sends a message, it is routed to the switch, which then passes the message along to the intended recipient. The star network is the most widely used network topology today.
* **Tree network** —each device is connected to a central node, either directly or through one or more other devices. The central node is connected to two or more subordinate nodes that in turn are connected to other sub ordinate nodes, and so forth, forming a treelike structure. This network, also known as a **hierarchical network,** is often used to share corporate wide data.
* **Hybrid network** —is a combination of different topologies. For example, large organizations today typically have a complex network of smaller networks. These smaller networks have been created over time and use a variety of different topologies. Connected together, these smaller networks form a hybrid network.
* **Mesh network** —this topology is the newest type and does not use a specific physical layout (such as a star or a tree). Rather, the mesh network requires that each node have more than one connection to the other nodes. The resulting pattern forms the appearance of a mesh. If a path between two nodes is somehow disrupted, data can be automatically rerouted around the failure using another path. Wireless technologies are frequently used to build mesh networks.

**9.7.2 Strategies**

Every network has a **strategy,** or way of coordinating the sharing of information and resources. The most common network strategies are terminal, client/server, peer-to-peer, and distributed. In a **terminal server network,** processing power is centralized in one large computer, with the capacity to handle a large number of connections. The nodes connected to this host computer are either terminals with little or no processing capabilities or microcomputers running special terminal emulation software such as Windows Remote Desktop.

**Client/server networks** use central computers to coordinate and supply services to other nodes on the network. The server provides access to resources such as Web pages, databases, application software, and hardware. This strategy is based on specialization. Server nodes coordinate and supply specialized services, and client nodes request the services. Commonly used server operating systems are Windows Server, Mac OS X Server, Linux, and Solaris. Client/server networks are widely used on the Internet.

In a **peer-to-peer (P2P) network,** nodes have equal authority and can act as both clients and servers. The most common way to share games, movies, and music over the Internet is to use a P2P network. For example, special file-sharing software such as eDonkey or BitTorrent can be used to obtain files located on another microcomputer and also can provide files to other microcomputers.

P2P networks are rapidly growing in popularity as people continue to share information with others around the world. The primary advantage is that they are easy and inexpensive (often free) to set up and use. One disadvantage of P2P networks is the lack of security controls or other common management functions. For this reason, few businesses use this type of network to communicate sensitive information.

In a **distributed processing network,** processing capability is located and shared at different nodes or locations. This type of strategy is common for decentralized organizations where divisional offices have their own computer systems. The computer systems in the divisional offices are networked to the organizations’s main or centralized computer.

**9.8 Organizational Networks**

Computer networks in organizations have evolved over time. Most large organizations have a complex and wide range of different network configurations, operating systems, and strategies. These organizations face the challenge of making these networks work together effectively and securely.

**9.8.1 Internet technologies**

Many organizations today employ Internet technologies to support effective communication within and between organizations using intranets and extranets.

* An **intranet** is a *private* network within an organization that resembles the Internet. Like the *public* Internet, intranets use browsers, Web sites, and Web pages. Typical applications include electronic telephone directories, e-mail addresses, employee benefit information, internal job openings, and much more. Employees find surfing their organizational intranets to be as easy and as intuitive as surfing the Internet.
* An **extranet** is a *private* network that connects *more than one* organization. Many organizations use Internet technologies to allow suppliers and others limited access to their networks. The purpose is to increase efficiency and reduce costs. For example, an automobile manufacturer has hundreds of suppliers for the parts that go into making a car. By having access to the car production schedules, suppliers can schedule and deliver parts as they are needed at the assembly plants. In this way, operational efficiency is maintained by both the manufacturer and the suppliers.

**9.8.2 Network security**

Large organizations face the challenge of ensuring that only authorized users have access to network resources, sometimes from multiple geographic locations or across the Internet. Securing large computer networks requires specialized technology. Three technologies commonly used to ensure network security are firewalls, intrusion detection systems, and virtual private networks.

* A **firewall** consists of hardware and software that control access to a company’s intranet and other internal networks. Most use a special computer or software called a **proxy server.** All communications between the company’s internal networks and the outside world pass through this server. By evaluating the source and the content of each communication, the proxy server decides whether it is safe to let a particular message or file pass into or out of the organizations’ network.
* **Intrusion detection systems (IDS)** work with firewalls to protect an organization’s network. These systems use sophisticated statistical techniques to analyze all incoming and outgoing network traffic. Using advanced pattern matching and heuristics, an IDS system can recognize signs of a network attack and disable access before an intruder can do damage.

**Virtual private networks (VPN)** create a secure private connection between a remote user and an organization’s internal network. Special VPN protocols create the equivalent of a dedicated line between a user’s home or laptop computer and a company server. The connection is heavily encrypted and, from the perspective of the user, it appears that their workstation is actually located on the corporate network.