Unit 3
Concepts of Internet & Networking

A **computer network** is a group of computers connected to each other electronically. This means that the computers can "talk" to each other and that every computer in the network can send information to the others. Usually, this means that the speed of the connection is fast - faster than a normal connection to the Internet.

Advantages of Network

The following are the distinct notes in favor of computer network.
a. The computers, staff and information can be well managed
b. A network provides the means to exchange data among the computers and to make programs and data available to people
c. It permits the sharing of the resources of the machine
d. Networking also provides the function of back-up.
e. Networking provides a flexible networking environment. Employees can work at home by using through networks ties through networks into the computer at office.

Types of Network: One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of area network. Common examples of area network types are:

- LAN - Local Area Network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network

LAN - Local Area Network

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings.
In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

MAN - Metropolitan Area Network

A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.

WAN - Wide Area Network

A WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth.

A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.
A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM.

- General Features & Working of Internet,
- Cyber Safety,
- Network Topologies,
- Transmission media,
- OSI Model,

Network Risks & Protection strategies

Network Topologies

In computer networking ,*topology* refers to the layout of connected devices.

Topology in Network Design

Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there.
Network topologies are categorized into the following basic types:

- bus
- ring
- star
- tree
- mesh

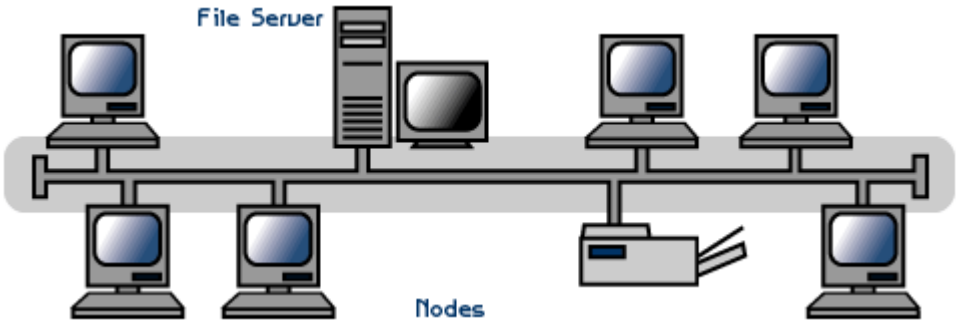
More complex networks can be built as hybrids of two or more of the above basic topologies.

Bus Topology

Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector.

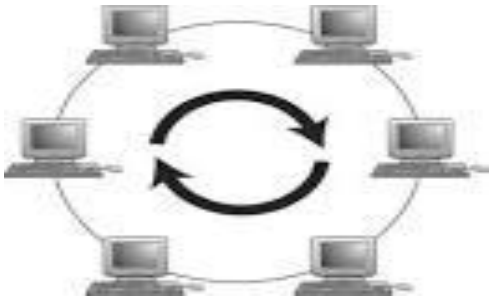
A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

Ethernet bus topologies are relatively easy to install and don't require much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies. However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable.



Ring Topology

In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network.
To implement a ring network, one typically uses FDDI, SONET, or Token Ringtechnology. Ring topologies are found in some office buildings or school campuses.



Star Topology

Many home networks use the star topology. A star network features a central connection point called a "hub node" that may be a network hub ,switch or router . Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. (If the hub fails, however, the entire network also fails.)

Tree Topology

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the root of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

Mesh Topology

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths

exist, messages can only travel in one direction.) Some WANs , most notably the Internet, employ mesh routing.
A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.

Summary

Topologies remain an important part of network design theory. You can probably build a home or small business computer network without understanding the difference between a bus design and a star design, but becoming familiar with the standard topologies gives you a better understanding of important networking concepts like hubs, broadcasts, and routes.

Computer network components

Computer network components include the major parts that are needed to install a network both at the office and home level. Before delving into the installation process, you should be familiar with each part so that you could choose and buy the right component that fits with your network system.

These hardware components include **cable**, **Hub**, **Switch**, **NIC** (network interface card), **modem** and **router**. Depending on the type of network you are going to install, some of the parts can be eliminated. For example, in a wireless network you don't need cables, hubs so on.

In this article we will discuss about the main computer network components required **to install simple computer network**, often called **LAN** (local area network).

Computer network is a group of two or more computers that connect with each other to share a resource. **Sharing of devices and resources is the purpose of computer network.** You can share printers, fax machines, scanners, network connection, local drives, copiers and other resources.

In computer network technology, there are several types of networks that range from simple to complex level. However, in any case in order to connect computers with each other or to the existing network or planning to install from scratch, **the required devices and rules (protocols) are mostly the same**.

Ok, let us go and see each component in detail…

Major computer network components

Computer network requires the following devices (some of them are optional):-

• Network Interface Card (NIC)

• Hub

• Switches

• Cables and connectors

• Router

• Modem

1. Network Interface Card

Network adapter is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)**encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.

There are **two types of network cards**: **wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

Network Card Speed

Network Interface card, one of the main computer network components, comes with different speeds, 10Mbps, 100Mbps, and 1000Mbps, so on. Recent standard **network cards built with Gigabit** (1000Mbps)

connection speed. It also supports to connect slower speeds such as 10Mbps and 100Mbps. However, the speed of the card depends on your LAN speed.

For example, if you have a switch that supports up to 100Mbps, your NIC will also transfer a data with this same speed even though your computer NIC has still the capability to transfer data at 1000Mbps (1Gbps). In modern computers, network adapter is integrated with a computer motherboard. However if you want advanced and fast Ethernet card, you may buy and install on your computer using the **PCI slot** found on the motherboard (desktop) and **ExpressCard slots** on laptop .

2. Hub

Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as **Switchs and Routers**.

3. Switch

Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses**physical device addresses** in each incoming messages so that it can deliver the message to the right destination or port.

Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

4. Cables and connectors

Cable is one way of transmission media which can transmit communication signals. The wired network typology uses special type of cable to connect computers on a network.

There are a number of solid transmission Media types, which are listed below. - **Twisted pair wire**

It is classified as Category 1, 2, 3, 4, 5, 5E, 6 and 7. Category 5E, 6 and 7 are high-speed cables that can transmit 1Gbps or more. -

Coaxial cable

Coaxial cable more resembles like TV installation cable. It is more expensive than twisted-pair cable but provide high data transmission speed.

Fiber-optic cable

It is a high-speed cable which transmits data using light beams through a glass bound fibers. Fiber-optic cable is high data transmission cable comparing to the other cable types. But the cost of fiber optics is very expensive which can only be purchased and installed on governmental level.

5. Router

When we talk about computer network components, the other device that used to **connect a LAN with an internet connection is called Router**. When you have **two distinct networks** (LANs) or want to share a single internet connection to multiple computers, we use a Router.

In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks.

There are two types of Router: **wired and wireless**. The choice depends on your physical office/home setting, **speed** and **cost**.

6. Modems

A modem enables you to connect your computer to the available internet connection over **the existing telephone line**. Like NIC, **Modem is not integrated with a computer motherboard**. It comes as separate part which can be installed on the PCI slots found on motherboard.

A modem is not necessary for LAN, but required for internet connection such as dial-up and DSL.

There are some types of modems, which differs in **speed and transmission rate**. Standard PC modem or Dial-up modems (56Kb data transmission speed), Cellular modem (used in a laptop that enables to connect while on the go),**cable modem (500 times faster than standard modem)** and DSL Modems are the most popular.

Introduction to Client Server Networks

The term *client-server*refers to a popular model for computer networking that utilizes client and server devices each designed for specific purposes. The client-server model can be used on the Internet as well aslocal area networks (LANs). Examples of client-server systems on the Internet include Web browsers and Web servers, FTP clients and servers, and the DNS.

Client and Server Devices

Client/server networking grew in popularity many years ago as personal computers (PCs) became the common alternative to older *mainframe* computers. Client devices are typically PCs with network software applications installed that request and receive information over the network. Mobile devices as well as desktop computers can both function as clients.
A server device typically stores files and databases including more complex applications like Web sites. Server devices often feature higher-powered central processors, more memory, and larger disk drives than clients.

Client-Server Applications

The client-server model organizes network traffic by application and also by sending device. Network clients make requests to a server by sending messages, and servers respond to their clients by acting on each request and returning results. One server generally supports numerous clients, and multiple servers can be networked together in a pool to handle the increased processing load as the number of clients grows.
A client computer and a server computer are usually two separate devices, each customized for their designed purpose. For example, a Web client works best with a large screen display, while a Web server does not need any display at all and can be located anywhere in the world. However, in some cases a given device can function both as a client and a server for the same application. Additionally, a device that is a server for one application can simultaneously act as a client to other servers, for different applications.

Some of the most popular applications on the Internet follow the client-server model including email, FTP and Web services. Each of these clients features a user interface (either graphic- or text-based) and a client application that allows the user to connect to servers. In the case of email and FTP, users enter a computer name (or sometimes an IP address) into the interface to set up connections to the server.

Local Client-Server Networks

Many home networks utilize client-server systems without even realizing it. Broadband routers , for example, contain DHCP servers that provide IP addresses to

the home computers (DHCP clients). Other types of network servers found in home include *print servers* and *backup servers* .

Client-Server vs Peer-to-Peer and Other Models

The client-server model was originally developed to allow more users to share access to database applications. Compared to the mainframe approach, client-server offers improved scalability because connections can be made as needed rather than being fixed. The client-server model also supports modular applications that can make the job of creating software easier. In so-called "two tier" and "three tier" types of client-server systems, software applications are separated into modular pieces, and each piece is installed on clients or servers specialized for that subsystem.
Client-server is just one approach to managing network applications. The primary alternative to client-server, *peer-to-peer* networking, treats all devices as having equivalent capability rather than specialized client or server roles. Compared to client-server, peer to peer networks offer some advantages such as better flexibility in expanding the network to handle large number of clients. Client-server networks generally offer advantages over peer-to-peer as well, such as in the ability to keep data protected from attackers.

OSI MODEL

The Open Systems Interconnect (OSI) model has seven layers. This article describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked this way:

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
    - What signal state represents a binary 1
    - How the receiving station knows when a "bit-time" starts

    - How the receiving station delimits a frame
- Physical medium attachment, accommodating various possibilities in the medium:
    - Will an external transceiver (MAU) be used to connect to the medium?
    - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
    - What physical medium options can be used
    - How many volts/db should be used to represent a given signal state, using a given physical medium

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

- Link establishment and termination: establishes and terminates the logical link between two nodes.
- Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- Frame delimiting: creates and recognizes frame boundaries.
- Frame error checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

- Routing: routes frames among networks.
- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

- Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
- Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

- Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
- Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
- Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

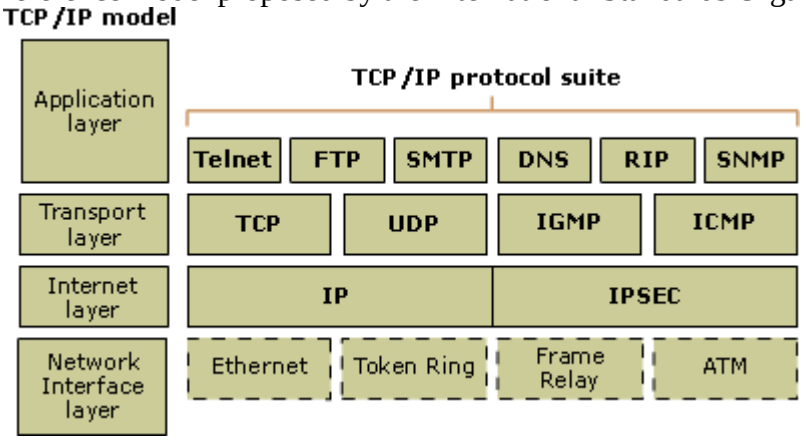
The application layer serves as the window for users and application processes to

access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

The TCP/IP model

The TCP/IP model
TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.
As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).



The types of services performed and protocols used at each layer within the TCP/IP model are described in more detail in the following table.

Layer	Description	Protocols
Application	Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other

		application protocols
Transport	Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data.	TCP, UDP, RTP
Internet	Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams.	IP, ICMP, ARP, RARP
Network interface	Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

Note

- The OSI reference model is not specific to TCP/IP. It was developed by the ISO in the late 1970s as a framework for describing all functions required of an open interconnected network. It is a widely known and accepted reference model in the data communications field and is used here only for comparison purposes.

***VoIP** is short for **V**oice **o**ver **I**nternet **P**rotocol.*

Voice over Internet Protocol is a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets usingIP rather than by traditional circuit transmissions of the PSTN.

One advantage of VoIP is that the telephone calls over the Internet do not incur a surcharge beyond what the user is paying for Internet access, much in the same way that the user doesn't pay for sending individual emails over the Internet.

There are many Internet telephony applications available. Some, like CoolTalk and NetMeeting, come bundled with popular Web browsers. Others are stand-alone products. VoIP also is referred to as *Internet telephony, IP telephony, or Voice over the Internet (VOI).*

What is network security? How does it protect you? How does network security work? What are the business benefits of network security?

You may think you know the answers to basic questions like, What is network security? Still, it's a good idea to ask them of your trusted IT partner. Why? Because small and medium-sized businesses (SMBs) often lack the IT resources of large companies. That means your network security may not be sufficient to protect your business from today's sophisticated Internet threats.

What Is Network Security?

In answering the question What is network security?, your IT partner should explain that network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

What Is Network Security and How Does It Protect You?

After asking What is network security?, you should ask, What are the threats to my network?

Many network security threats today are spread over the Internet. The most common include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

How Does Network Security Work?

To understand What is network security?, it helps to understand that no single solution protects you from a variety of threats. You need multiple layers of security. If one fails, others still stand.

Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats.

A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components often include:

- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks
- Virtual Private Networks (VPNs), to provide secure remote access

What are the Business Benefits of Network Security?

With network security in place, your company will experience many business benefits. Your company is protected against business disruption, which helps keep employees productive. Network security helps your company meet mandatory regulatory compliance. Because network security helps protect your customers' data, it reduces the risk of legal action from data theft.

Ultimately, network security helps protect a business's reputation, which is one of its most important assets.