Chapter 1 Networking Fundamentals

This chapter provides an overview of basic networking concepts, including network architecture, design, and project management.

Table of Contents

Figures

Table

Examples

Introduction to Networking Fundamentals

Overview

This manual provides an overview of concepts and technologies considered to be fundamental to organizational network design.

The contents of this manual are grouped into seven chapters, as follows:

- This chapter provides an overview of basic networking concepts, including network architecture, design, and project management.
- Chapter 2: Network Connectivity, describes cabling and wireless technologies used to link network devices in a single building or a multi-building campus.
- Chapter 3: Fundamental Network Components, provides an overview of the hardware components used to enable building, campus, and multi-site networks.
- Chapter 4: Network Communications, describes the communications protocols associated with networks, internetworks, storage, and telecommunications circuits.
- Chapter 5: Network Administration and Security, describes the concepts, technologies, and standards associated with network management and network security.
- Chapter 6: Commercial Building Networks, provides an overview of design guidelines for building, campus, and multi-site networks, including remote access connectivity for mobile users.
- Chapter 7: Data Center Networks, provides an overview of design guidelines for data centers, including the facilities, cabling topologies, and network equipment associated with data center deployment.

Appendix A: Codes, Standards, Regulations, and Organizations, details the sources of codes and standards and lists important international, multinational/regional, and country-specific codes and standards.

Appendix B: Legacy Technologies, provides an overview of network technologies used in the past but no longer considered for deployment within most organizations.

Appendix C: Numbering Conversions, provides a reference for numeric conversions.

Networking History and Evolution

Overview

This manual focuses on server-based networks as the standard form of organizational networking. However, it should be noted that other types of networks are also used for message exchange between users. The earliest form of electronic networking for the purpose of message transfer was the local telephone exchange, which has evolved to become a carrier network providing transport services for both voice and data traffic on a global scale.

Data networks designed exclusively for computing environments followed the introduction of business computing in the 1950s. Prior to that time, computers were used mostly for research and national defense purposes.

Milestones in the history of data networking include:

- 1960s—The first large-scale commercial computer network is created for an airline reservation application. Also, the Advanced Research Projects Agency Network (ARPANET) successfully links computers developed by different manufacturers, forming what is later described as the origin of today's Internet.
- 1970s—A networking technology for minicomputers called Ethernet is developed.
- 1980s—The increase in the number of stand-alone desktop microcomputers within organizations encourages widespread adoption of local area networks (LANs).
- 1990s—Web-based Internet resources are introduced on a global scale.
- 2000s—Improved mobile/wireless devices and networks provide the means to connect to an organizational network from nearly any location in the world.

The advances in computing and communications technologies, and the decline in costs, have made it possible to provide each user with multiple fixed or mobile processing devices (e.g., desktop, laptop, handheld, and home computers). Each of these devices is independently capable of storing data and connecting to an organizational network, a home network, or the Internet. This is in contrast to earlier times, when all users had to share the processing and storage capabilities of a single centralized computer using desktop terminals.

The evolution in computing can therefore be described as a migration from centralized to decentralized or distributed, with networks used to interconnect various types of computing and storage devices.

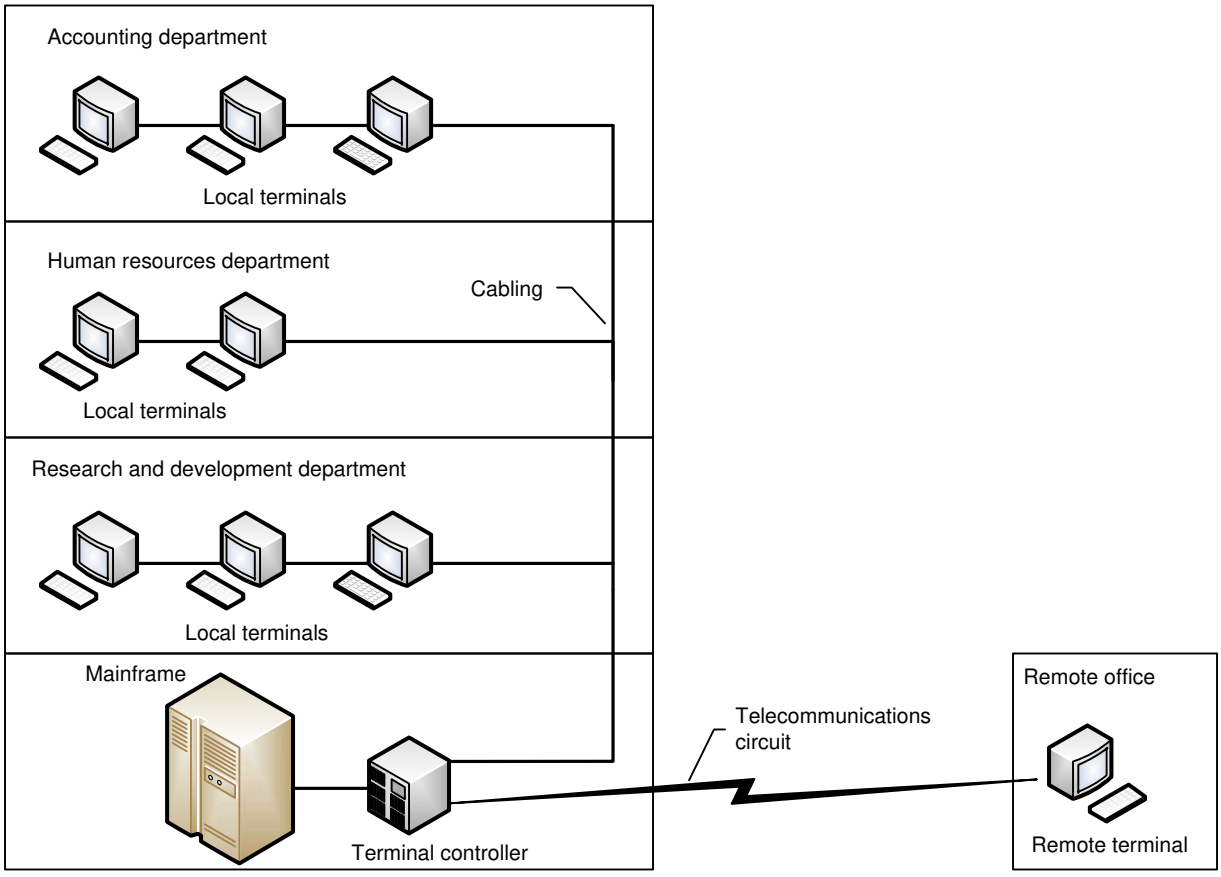
Mainframe Terminals

The first computers available to organizations were mainframes, introduced in the 1950s. A mainframe is characterized by its centralized approach to processing and storage where all computing and storage operations are controlled by a single device. Thousands of users can simultaneously issue commands or enter data from stations called terminals, which are a combination of a monitor and a keyboard connected to the mainframe.

At the time of their introduction, mainframes were affordable mostly to large organizations. In most cases, one mainframe was acquired and placed in a single room to serve the needs of the entire organization. This made it necessary to develop the means for both local staff and employees at other locations to access the mainframe.

The solution was to use two types of connectivity—cabling to link local terminals and telecommunications circuits to link terminals in remote offices as shown in Figure 1.1. These connections can be described as the original forms of local and wide area networking.

Figure 1.1
Mainframe environment

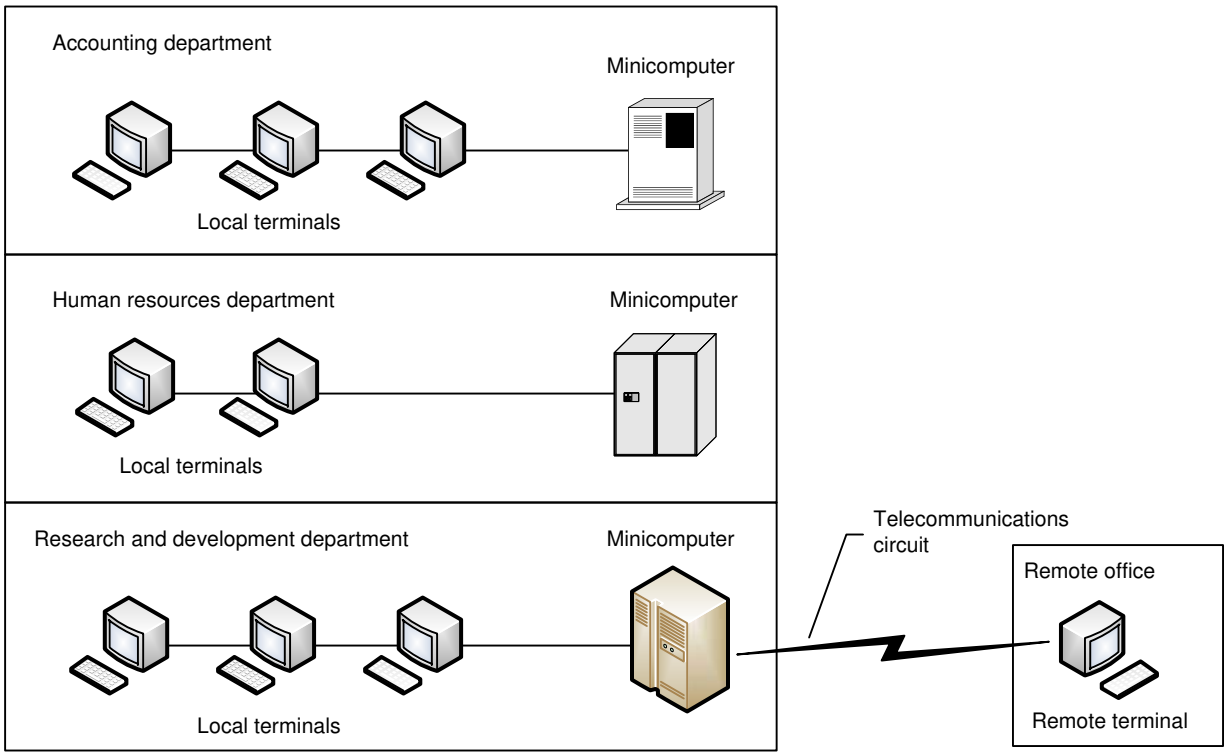


Minicomputer Terminals

In the 1970s, advances in computing made it possible to develop smaller versions of mainframes. These devices were called minicomputers and functioned in the same manner as mainframes, but on a smaller scale. The lower cost of minicomputers enabled smaller organizations and individual departments within large organizations to acquire a computer system.

From a networking perspective, minicomputers operate like mainframes. Terminals are connected to a centralized processing and storage unit using cabling or telecommunications circuits, as shown in Figure 1.2. Compared with mainframes, fewer simultaneous terminal connections (also called sessions) are possible, due to the relatively limited performance and storage capabilities of minicomputers.

Figure 1.2
Minicomputer environment



NOTE: Although this manual focuses on networking using current server and storage technologies, it should be noted that both mainframes and minicomputers can be configured as servers and connected to the networks described in this manual.

Personal Computing Devices

Due to their low cost and the availability of all types of software, personal computers (PCs) have been acquired in large volumes by organizations since the 1980s. At the time of their introduction, PCs provided a great deal of flexibility to users accustomed to requesting mainframe or minicomputer services from data processing departments.

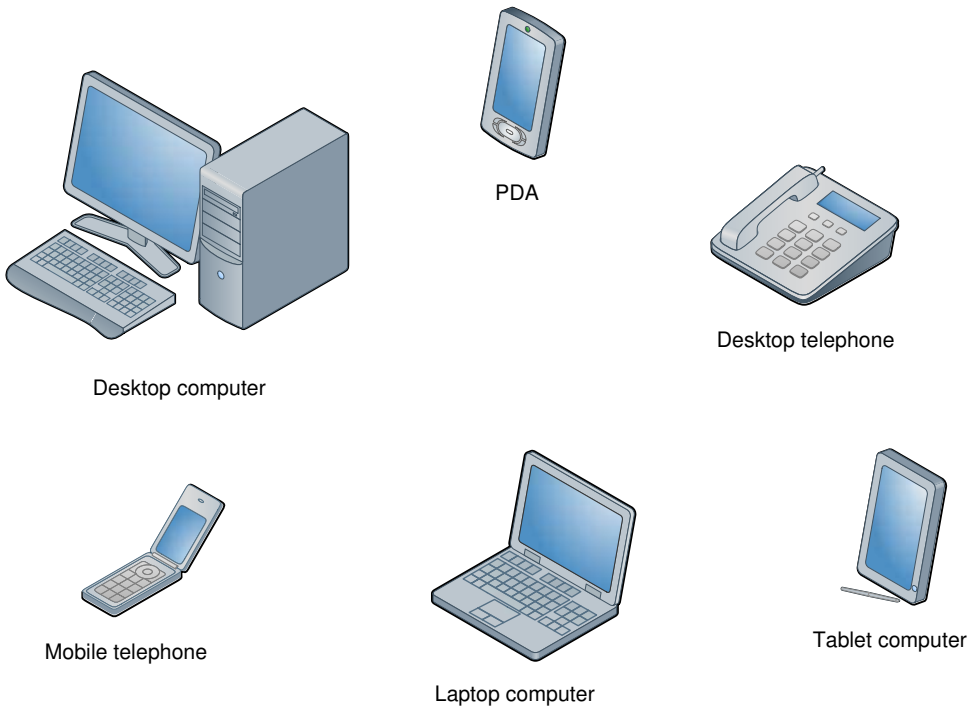
The PC made it possible for any individual or group to choose, purchase, install, and operate a computer without the involvement of programmers or other computing specialists. With the introduction of terminal emulation software, PCs could also access data on mainframes and minicomputers, eliminating the need for terminals.

NOTE: Terminal emulation software enables a PC to assume the operating characteristics of various types of terminals.

The progress in computing and manufacturing technologies has made it possible to incorporate the processing and storage capabilities of desktop computers into portable computing devices (e.g., laptops, tablets, personal digital assistants [PDAs]). Similarly, current desktop and mobile telephones are capable of connecting to the same data networks as computing devices, making them similar in capability to traditional PCs.

Examples of personal computing devices are shown in Figure 1.3.

Figure 1.3
Personal computing devices



Open Systems Interconnection (OSI) Reference Model

Overview

Communications on a network takes place at many levels (e.g., applications, diagnostics, device control). In 1978, the International Organization for Standardization (ISO) introduced a framework for classifying all of the processes associated with message exchange on a network. This framework is formally called the Open Systems Interconnection (OSI) Reference Model, but is commonly referred to as the OSI model.

The objective of the OSI model is to provide a structured approach for the development of all types of networks. The model specifies the sequence of processes required for network message transfer between applications running on different systems.

NOTE: In this context, a system can be defined as two or more computers and the associated software, peripherals, operators, physical processes, and media that form an autonomous unit capable of processing and transferring data.

Layers

The OSI model uses an approach called layering to illustrate and explain the message exchange process. This approach divides the various functions and services provided by a network into discrete groupings called layers, as illustrated in Figure 1.4.

Figure 1.4
Open Systems Interconnection Reference Model

Layer 7	Application layer
Layer 6	Presentation layer
Layer 5	Session layer
Layer 4	Transport layer
Layer 3	Network layer
Layer 2	Data Link layer
Layer 1	Physical layer

NOTE: A layer function can be described by number or by name. For example, the terms Layer 3 switching and Network layer switching refer to the same process.

Layers, continued

In the OSI model, each layer provides services to the layer above, while hiding from that layer the processes used to implement the services. Ideally, changes can be made to any layer without requiring changes to any of the other layers, as long as the inputs and outputs of the changed layer remain the same.

For example, specifications for transmission over optical fiber cabling can be incorporated into Layer 1 of an existing Layer 2 network technology (e.g., Ethernet) without modifying any of the existing Layer 2 specifications. This makes it possible to take advantage of new technologies within a given layer without sacrificing compatibility with existing networks.

The layers in the OSI model are commonly described as being connected to each other in vertical form, also called a stack or protocol stack. The stack defines how network hardware and software interact at various levels to transfer messages between devices on a network and between networks on an internetwork.

Protocol stacks have the following characteristics:

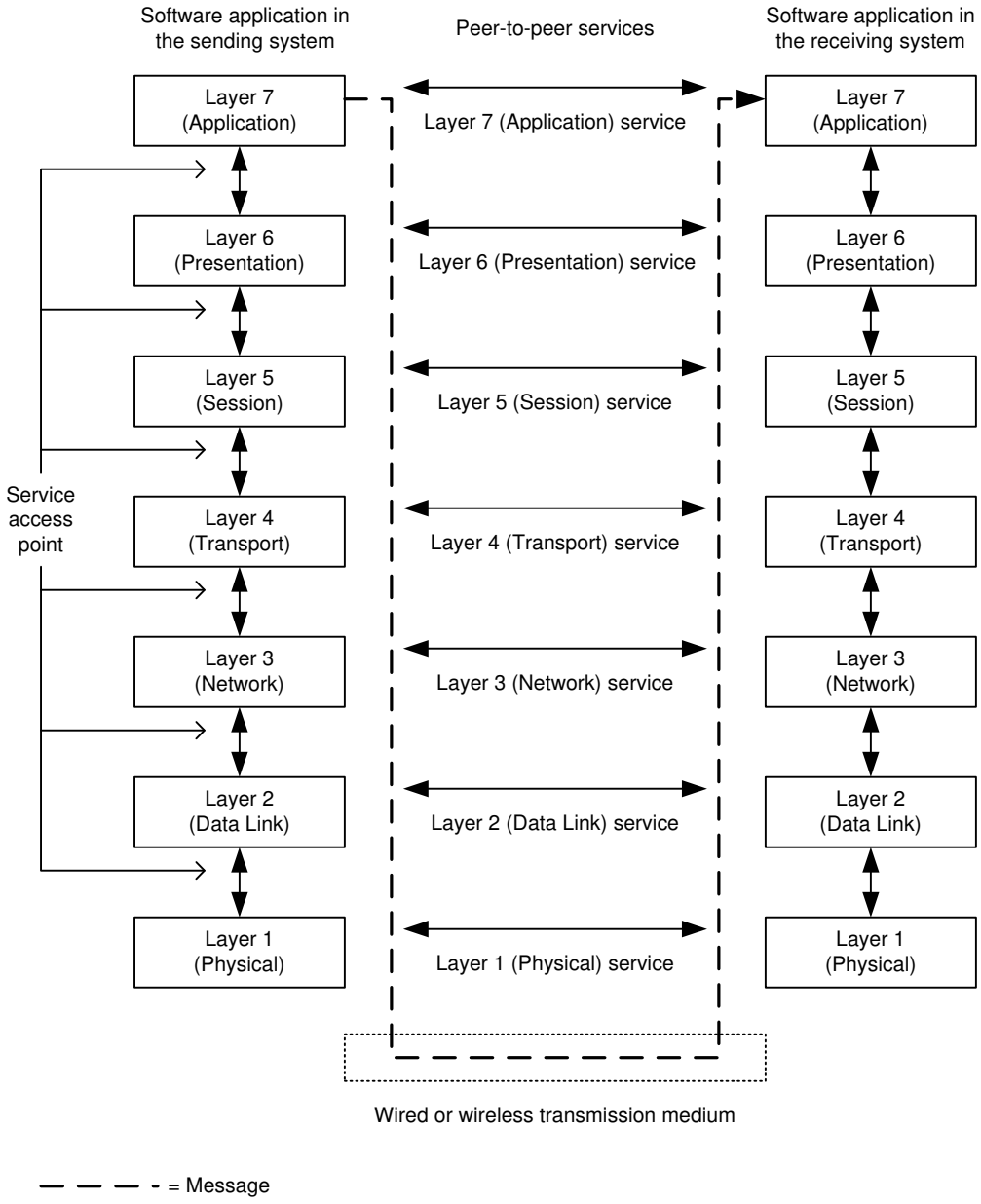
- Each layer provides a set of services.
- Services of each layer and the stack are defined by protocols.
- Lower layers provide services to upper layers.
- Service access points (SAPs) are the connection points between layers.

When a message needs to be transferred between two systems, a peer-to-peer relationship is established between the corresponding layers in the protocol stack of each system—a given layer at one end communicates with its counterpart at the other end over the network. The message, along with any control information, is passed down from the sending layer to the layer below.

This process continues until the lowest layer in the stack is reached. The data is then transmitted from the lowest layer of the sending system to the lowest layer in the receiving system, where it is passed up through the layers until it reaches the counterpart, or peer, of the sending layer, as shown in Figure 1.5.

Layers, continued

Figure 1.5
Message transfer described using the Open Systems Interconnection Reference Model



Layers, continued

Layer 7 (Application) Services

Layer 7 services make it possible for identical or non-identical applications running on different systems to use a network to exchange information. Services defined by this layer include file transfer, message handling, and remote management. For example, various types and versions of e-mail software can use the same Layer 7 protocols to exchange messages over the Internet.

Layer 6 (Presentation) Services

Layer 6 services are responsible for various forms of data conversion. This layer negotiates and establishes a common form for data representation, which includes character code translations, data compression, and message encryption.

Layer 5 (Session) Services

Layer 5 services are responsible for synchronizing and managing data transfer between network devices. For example, a Layer 5 protocol can direct a device to start, stop, restart, or abandon data transfer activity.

Layer 4 (Transport) Services

Layer 4 services make it possible to assign various levels of quality to the data transfer process. When a connection is being established between network devices, the Layer 4 protocol can be used to select a particular class of service. This layer can also monitor the transfer for billing purposes, ensure that the appropriate service quality is maintained, and generate an alert if this quality has been compromised.

Layer 3 (Network) Services

Layer 3 services are responsible for internetwork data transfer (e.g., between five Ethernet networks linked using the Internet). If multiple routes exist between the networks, a Layer 3 protocol can choose the most appropriate one, based on such criteria as message priority, route congestion, or route cost.

Layer 2 (Data Link) Services

Layer 2 services are responsible for intranetwork data transfer (e.g., between devices on an Ethernet network). Some of the functions of a Layer 2 protocol include device identification and managed access to a shared transmission channel.

Layer 1 (Physical) Services

Layer 1 services are responsible for the transfer of bits over various media.

NOTE: The OSI model does not explicitly define cabling or wireless transmission media.

Message Transfer Sequence

Any successful message transfer between two systems follows a four-step process:

Step	Message Transfer Between Two Systems
1	Preparation of the message to be transferred after a request is made by a software application running on the sending system.
2	Access to the network and transmission of the message.
3	Retrieval of the message by the receiving system.
4	Delivery of the message to the appropriate software application running on the receiving system.

Examples 1.1 and 1.2 illustrate the role of each layer in the message transfer process.

Example 1.1
Message output at the sending system

OUTGOING MESSAGE

A software application running in the sending system directs a message to Layer 7.

↓

Layer 7 (Application)

Layer 7 is responsible for:

- Organizing the message into blocks of data.

↓

[AH][DATA]

An application header (AH) is added to each block, forming an application protocol data unit (APDU). The AH is used to identify the:

- Sending application.
- Destination application.

↓

[APDU]

↓

Message Transfer Sequence, continued

Example 1.1
Message output at the sending system, continued

↓

Layer 6 (Presentation)

Layer 6 is responsible for:

- Translating the character code used by the sending system to that used by the receiving system, if necessary.
- Compressing the data to improve transfer efficiency, if necessary.
- Encrypting the data for security, if necessary.

↓

[PH][APDU]

↓

[PPDU]

A presentation header (PH) is added to each APDU received from Layer 7, forming a presentation protocol data unit (PPDU). The PH is used to:

- Provide details on any encoding, compression, or encryption used.

↓

Layer 5 (Session)

Layer 5 is responsible for:

- Marking the first and last block of data.
- Including a special marker with the last block of data to allow the destination system to send a reply (if necessary).

↓

[SH][PPDU]

↓

[SPDU]

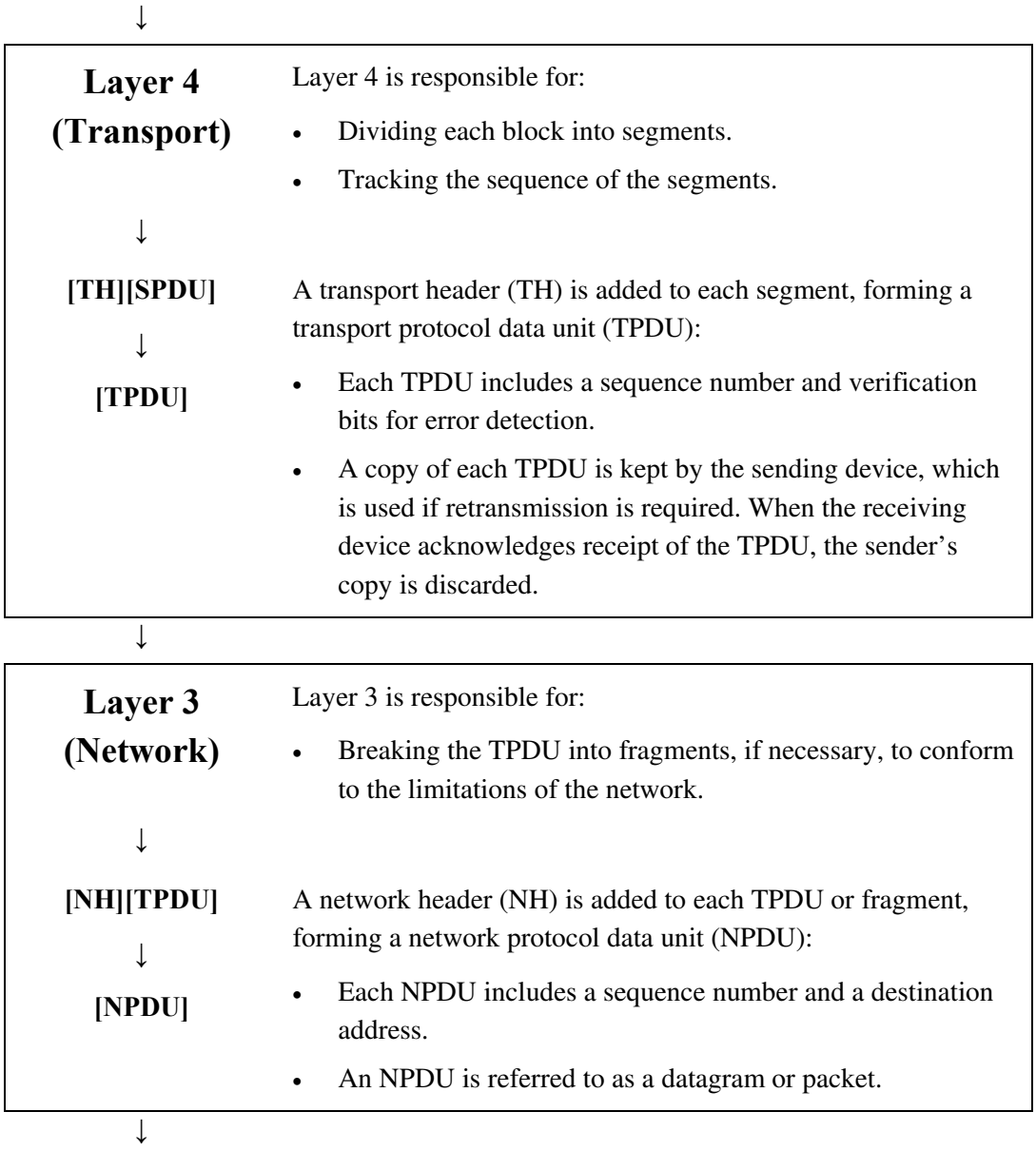
A session header (SH) is added to each PPDU received from Layer 6, forming a session protocol data unit (SPDU). The SH is used to:

- Indicate any markers accompanying the data blocks.

↓

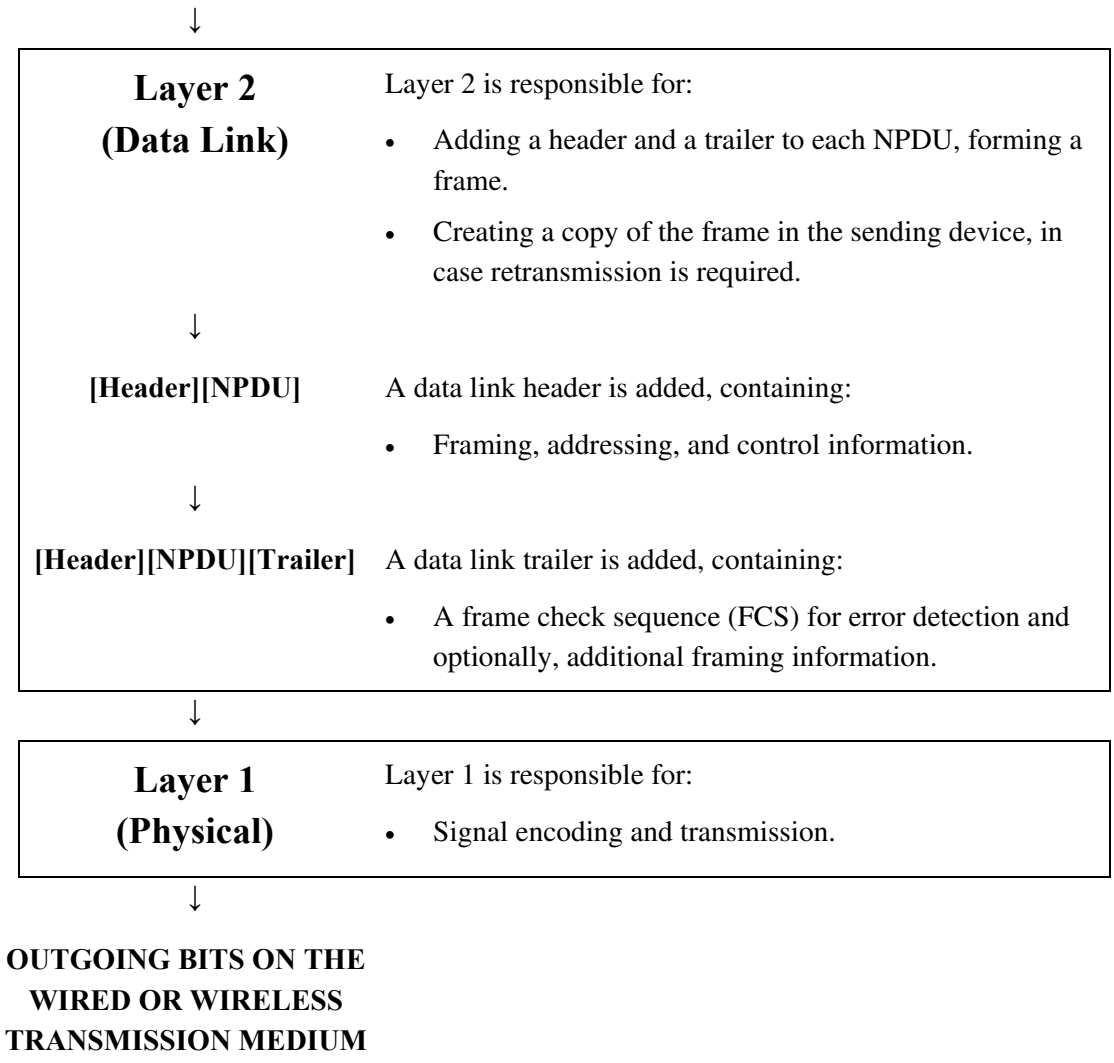
Message Transfer Sequence, continued

Example 1.1
Message output at the sending system, continued



Message Transfer Sequence, continued

Example 1.1
Message output at the sending system, continued



Message Transfer Sequence, continued

Example 1.2
Message input at the receiving system

INCOMING BITS ON THE WIRED OR WIRELESS TRANSMISSION MEDIUM

↓

Layer 1 (Physical)

Layer 1 is responsible for:

- Converting the incoming signal into a sequence of bits.

↓

[Header][NPDU][Trailer]

↓

Layer 2 (Data Link)

Layer 2 is responsible for:

- Removing the header and trailer information.
- Using the FCS to check if the contents were modified after transmission.

↓

[NPDU]

↓

[NH][TPDU]

↓

Layer 3 (Network)

Layer 3 is responsible for:

- Removing and inspecting the NH.
- Verifying that the values for destination address and sequence number are correct.
- Waiting for all the datagrams that form a TPDU to arrive and then assembling the TPDU.

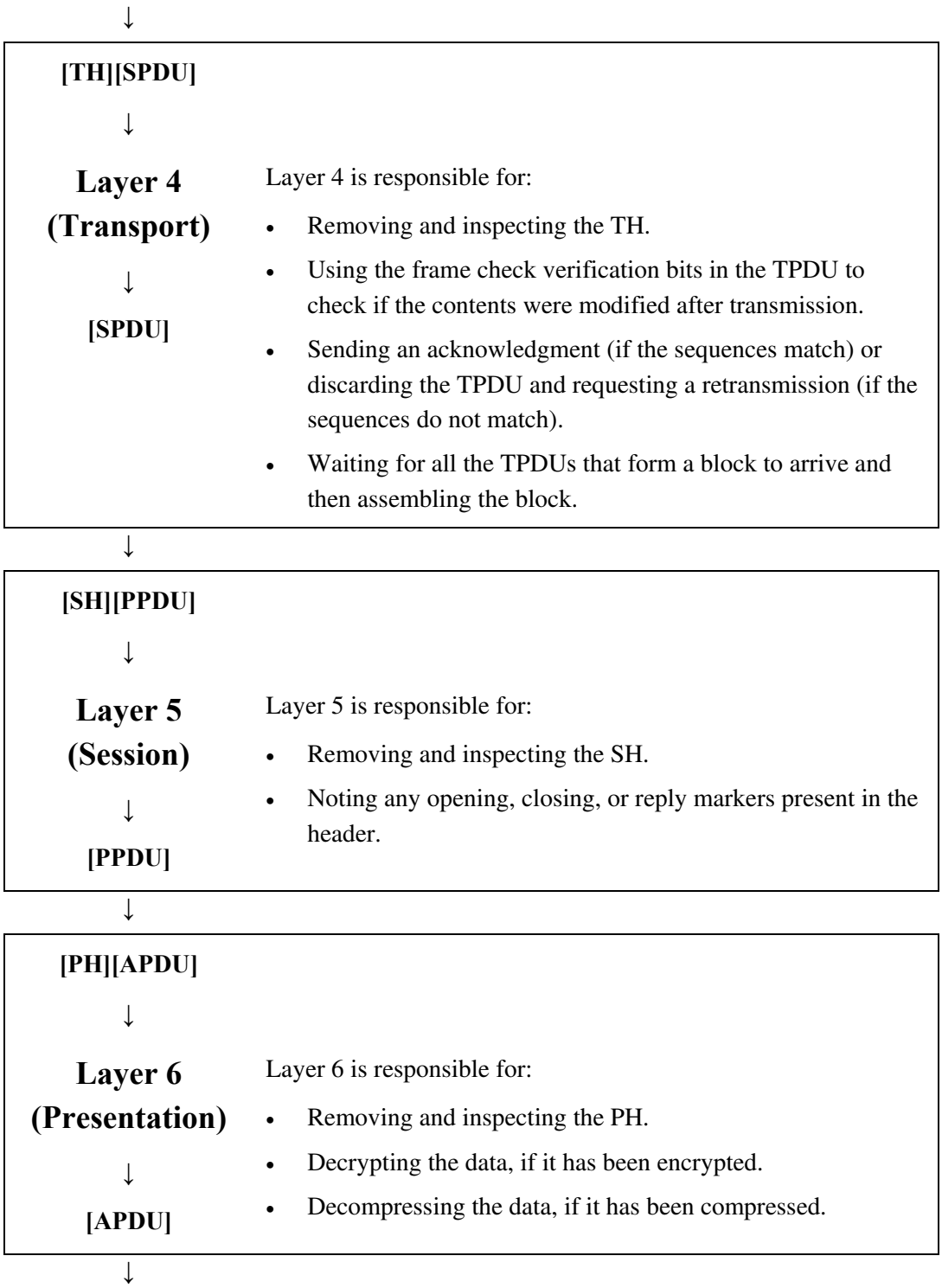
↓

[TPDU]

↓

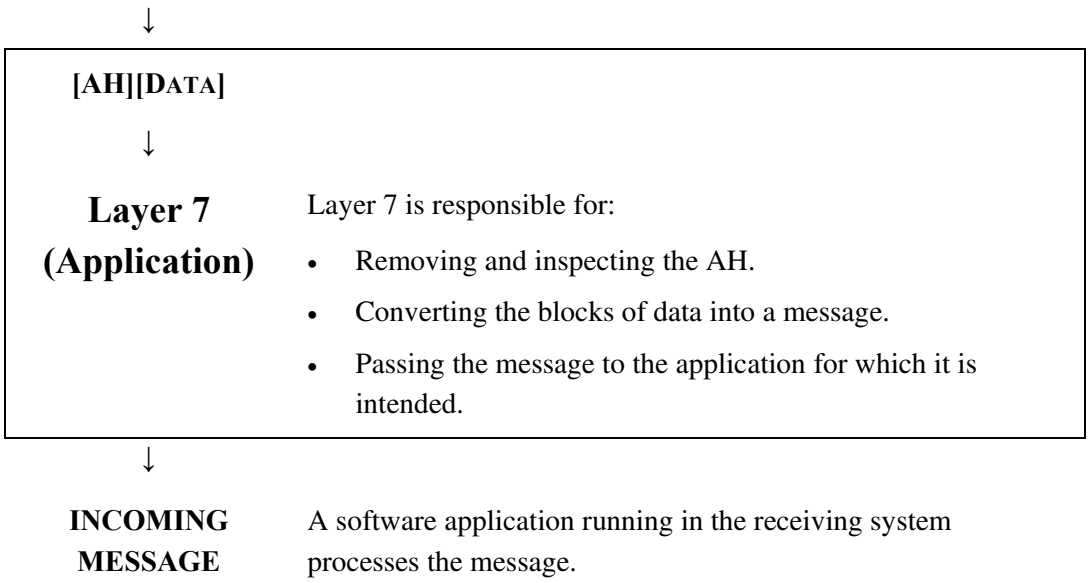
Message Transfer Sequence, continued

Example 1.2
Message input at the receiving system, continued



Message Transfer Sequence, continued

Example 1.2
Message input at the receiving system, continued



Introduction to Network Architecture and Design

Overview

Networks are implemented to enable the sharing of resources and the exchange of information between users. As the number of resources, users, and connections increases, most networks must be routinely modified to accommodate growth—ideally without any reduction in the features and performance levels users have come to expect. This makes network architecture and design a dynamic and continuous process within most organizations.

Network architecture can be described as the structured grouping of hardware, software, and applications. The successful integration of these three elements allows for the transfer of all types of messages between users, administrators, and devices.

Networking or LAN technologies for PCs were introduced in the 1980s to manage the rapid growth of desktop computing within many organizations.

Problems associated with stand-alone devices include the following:

- Each PC stores data locally, unlike mainframes or minicomputers, both of which use centralized storage. As a result, faulty reporting and decision-making can occur if the same data is updated on some PCs, but not on others.
- Security is a major concern, since every PC can potentially contain sensitive data, making it easier for unauthorized individuals to gain access to valuable organizational information.
- Backups may not exist for critical data if users do not duplicate their files on a regular basis. The failure of a single storage device can result in significant disruption and costs in terms of time, resources, and money.
- Various users or groups are free to install and use different software applications on their PCs, making file sharing difficult within the organization.
- It is more difficult to justify the purchase of expensive devices or services, since only one PC at a time can benefit. For example, a dedicated high-rate Internet connection is typically not economically feasible for every user in an organization with tens or hundreds of stand-alone PCs.

Overview, continued

Implementing a network makes it possible to solve these problems in the following ways:

- A network makes it possible to centralize data. All files shared by users are stored in a central location, which guarantees consistency and simplifies the update process.
- Multiple levels of security can be implemented on a network, making it more difficult to obtain unauthorized access to data.
- A network can be equipped with a backup system that runs at specific intervals, ensuring that critical data is available from a secondary source if needed.
- In addition to user-created files, software applications can be installed on centralized storage, accessible from any station connected to the network. This accelerates the deployment process, since any application or update needs to be installed only once on the network versus on each stand-alone PC.
- All users can access any resource connected to the network (e.g., high-speed copiers or Internet links).

Physically, a network can be as small as two connected PCs and the media used to enable the connections (i.e., cabling, a wireless link, or a telecommunications circuit).

In addition to wired or wireless connectivity, a network must be equipped with services designed for resource sharing, including:

- Access control, which is necessary in cases where two or more devices attempt to use a shared resource (e.g., telecommunications circuit between two sites, a printer) at the same time.
- Synchronization, which is necessary to ensure that a receiving device is listening when a sending device is transmitting to that device.
- Flow control, which is necessary to monitor and adjust the rate at which data is transferred from sender to receiver in order to minimize transfer time and data loss. For example, if a receiving device is occupied with other tasks, it will use flow control to ask the sending device to pause transmission.
- Error control, which is necessary to verify that a message was transferred successfully between a sender and a receiver (or to request a retransmission if the transfer was not successful).

Types of Networks

Networks can be characterized using one or more technical or operational attributes (e.g., type of technology or number of connected users and devices). One common attribute used to categorize networks is geographic area or span, where a network is labeled on the basis of the physical area it covers.

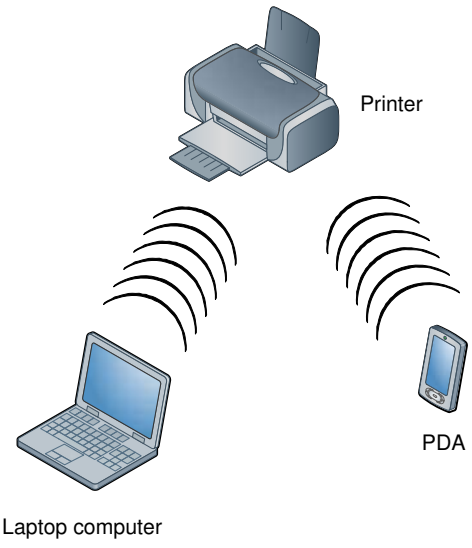
The five most common types of networks in terms of geographic area from the smallest to the largest are:

- Personal area networks (PANs).
- Local area networks (LANs).
- Campus area networks (CANs).
- Metropolitan area networks (MANs).
- Wide area networks (WANs).

Personal Area Networks (PANs)

PANs cover areas generally associated with individual workspaces (e.g., a home office or an office cubicle). Within these spaces, individual networks connecting two or more devices may be enabled using wireless technologies, as shown in Figure 1.6.

Figure 1.6
Personal area network



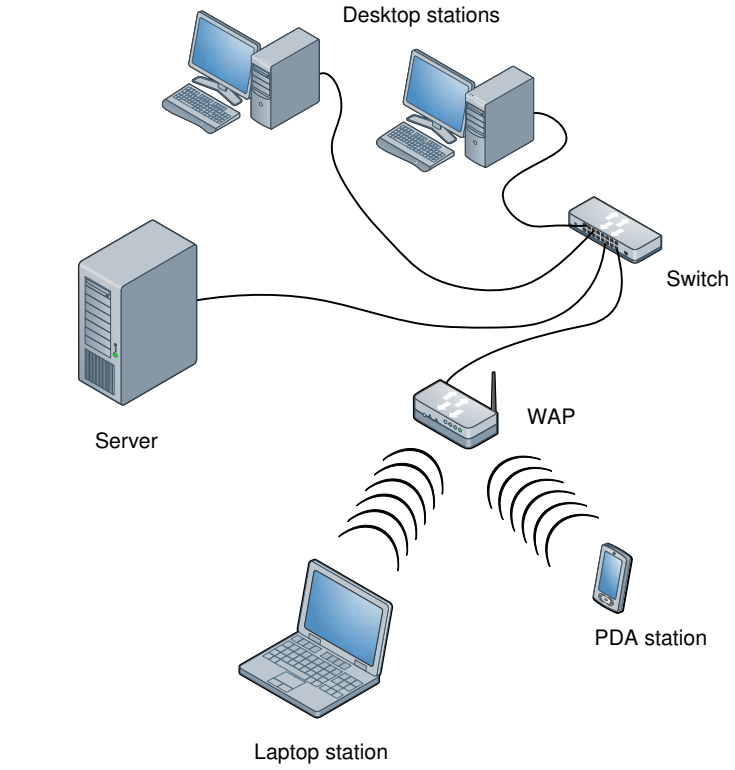
Types of Networks, continued

Local Area Networks (LANs)

LANs cover areas generally associated with some or all of the space within a building. In most cases, multiple workspace devices are connected to shared devices (e.g., switches, servers) to form a LAN.

One LAN can serve a single department, multiple groups, or all users within a building. Cabling, wireless, or a combination of both can be used to link LAN devices, as shown in Figure 1.7.

Figure 1.7
Local area network



PDA = Personal digital assistant
WAP = Wireless access point

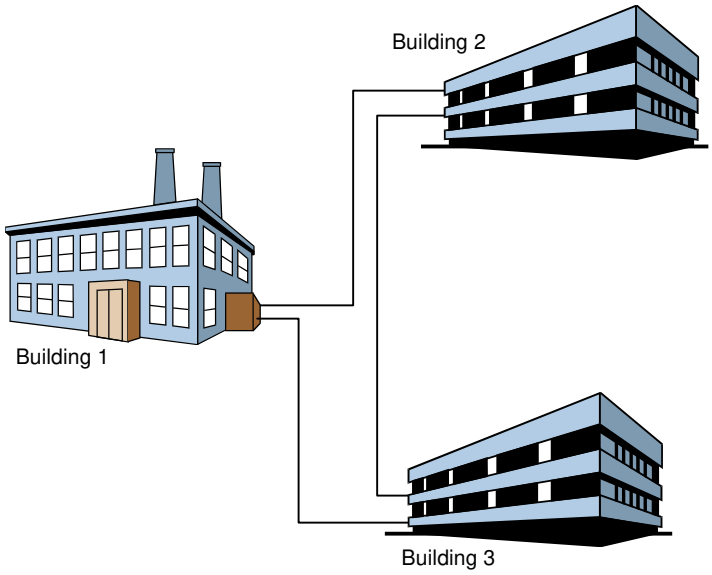
Types of Networks, continued

Campus Area Networks (CANs)

CANs are created by linking the LANs located in two or more buildings that are in close proximity to each other, as shown in Figure 1.8. Connections between the buildings can be made using cabling or wireless technologies.

NOTE: The term campus LAN is also used to describe a CAN.

Figure 1.8
Campus area network

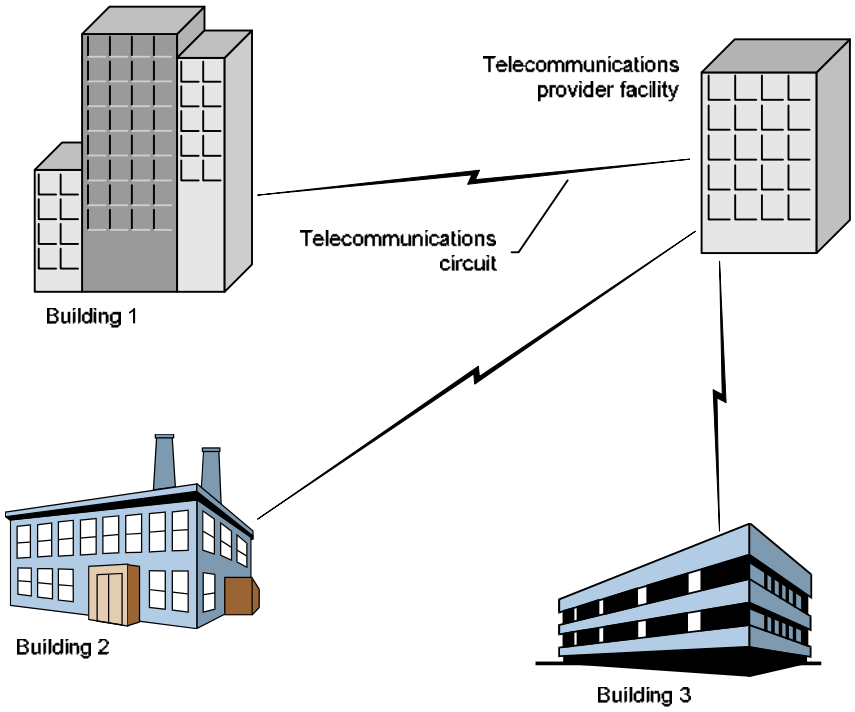


Types of Networks, continued

Metropolitan Area Networks (MANs)

MANs are created by linking the networks located at two or more sites within a city. Connections can be made using cabling or wireless technologies, with optical fiber cabling often used to link a customer's buildings to a facility operated by a telecommunications provider, as shown in Figure 1.9.

Figure 1.9
Metropolitan area network

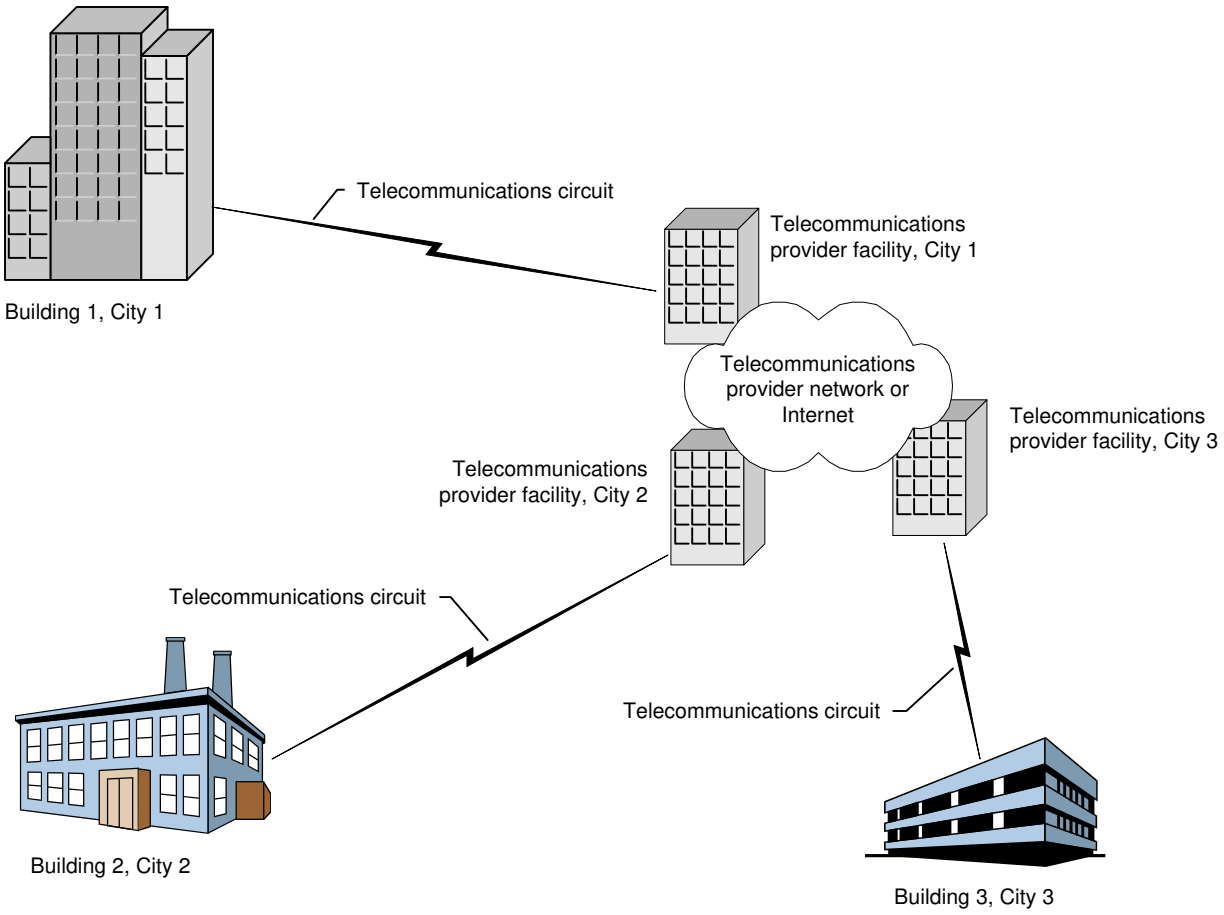


Types of Networks, continued

Wide Area Networks (WANs)

WANs are created by linking the networks located at two or more sites over geographic distances that extend beyond the span of a single metropolitan area. These include links between cities, countries, and in the case of global WANs, continents. Telecommunications circuits link each building to facilities operated by a telecommunications provider (same as MANs), as shown in Figure 1.10.

Figure 1.10
Wide area network



Types of Messaging

Most network messaging can be described as one-to-one communications, where the sending device addresses an outgoing message for delivery to a single receiver. In some cases, however, a message must be directed to a group of devices or all devices on the network. This is also referred to as one-to-many or one-to-all communications.

Most network devices are capable of issuing three types of messages:

- Unicast
- Broadcast
- Multicast

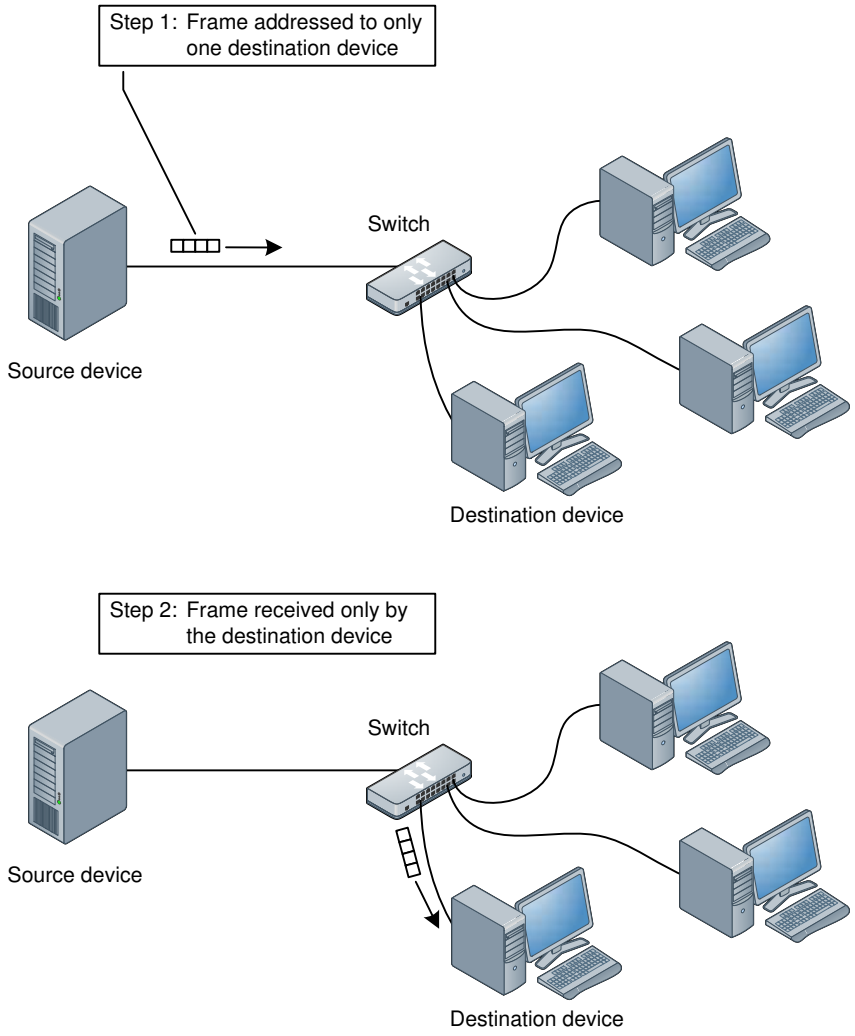
Unicast Messaging

In unicast messaging, or unicasting, each message is addressed to one recipient, as shown in Figure 1.11. If a device needs to send the same message to multiple destinations, it must perform a replicated unicast—the same transmission is repeated for each destination, as shown in Figure 1.12.

With unicasting there is no risk of sending a message to an unintended recipient, since the network directs each frame to the device corresponding to the unicast destination address. This process is also referred to as a point-to-point transfer. However, generating multiple frames containing identical data is an inefficient use of network resources and requires additional processing in the sending device.

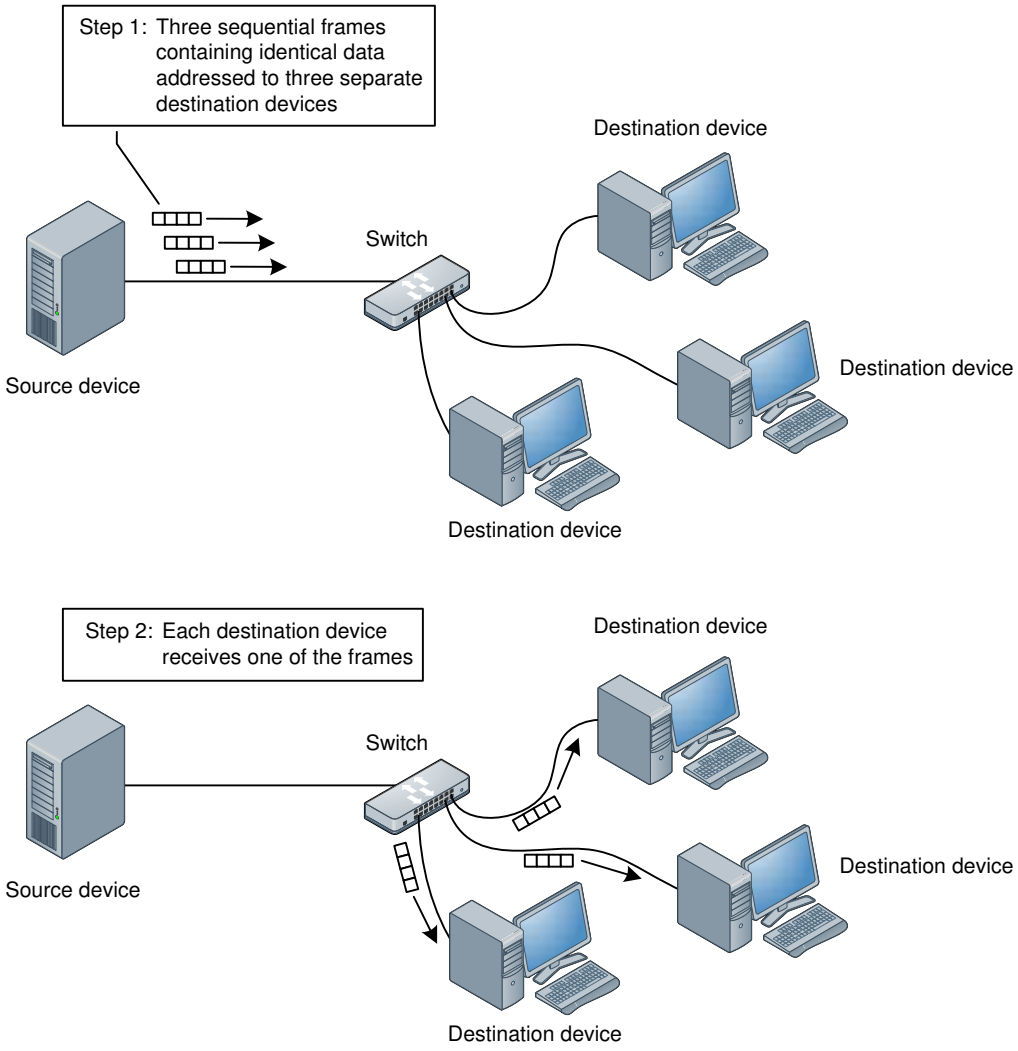
Types of Messaging, continued

Figure 1.11
Unicast messaging



Types of Messaging, continued

Figure 1.12
Replicated unicast messaging



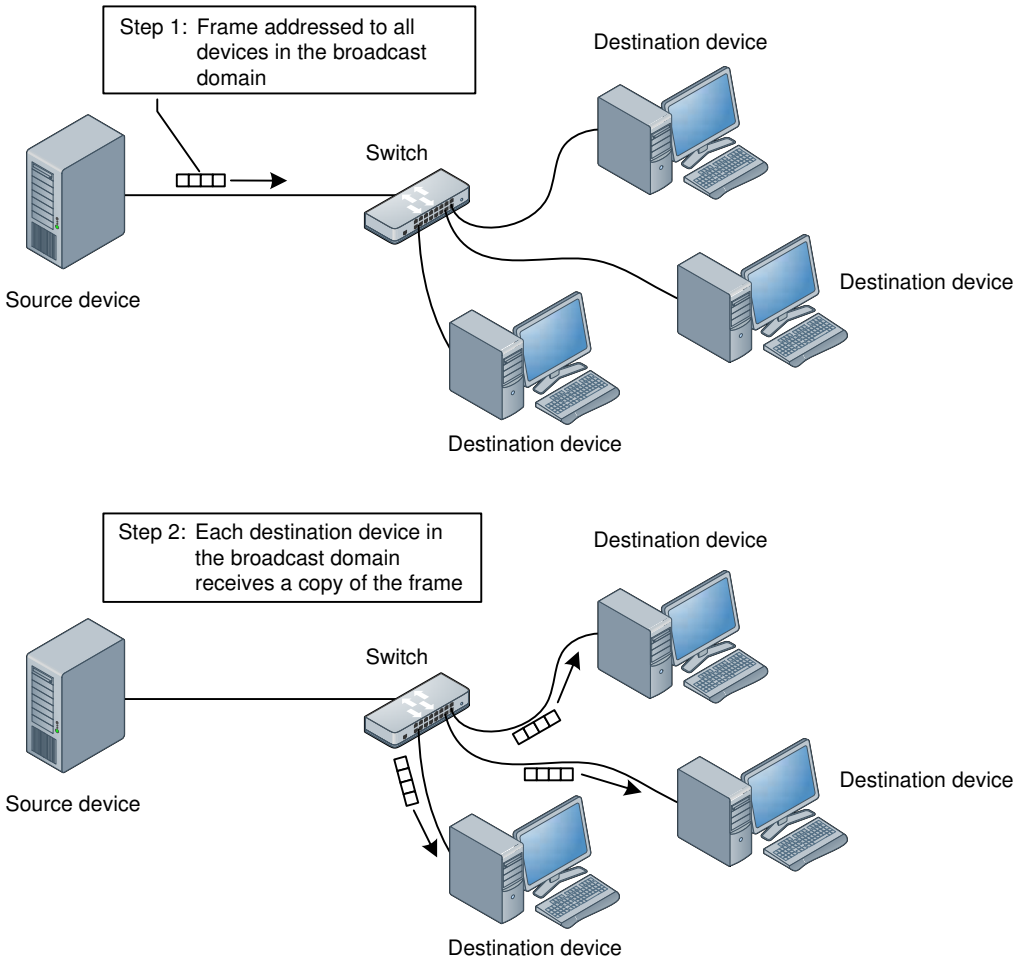
Types of Messaging, continued

Broadcast Messaging

In broadcast messaging, or broadcasting, each frame contains a special sequence of bits in the address to indicate that the destination is all devices (referred to as the broadcast domain) as shown in Figure 1.13. Such transfers are also referred to as point-to-multipoint—the sending device transmits a broadcast frame once and the network directs the frame to all other devices.

This method is most efficient in cases when all network devices require the message being broadcast. However, if this is not the case, a destination device not requiring the message wastes processing resources—it must read and subsequently discard the incoming frame. When the number of discarded frames exceeds the number required, the broadcast is considered to be an inefficient use of network resources.

Figure 1.13
Broadcast messaging



Types of Messaging, continued

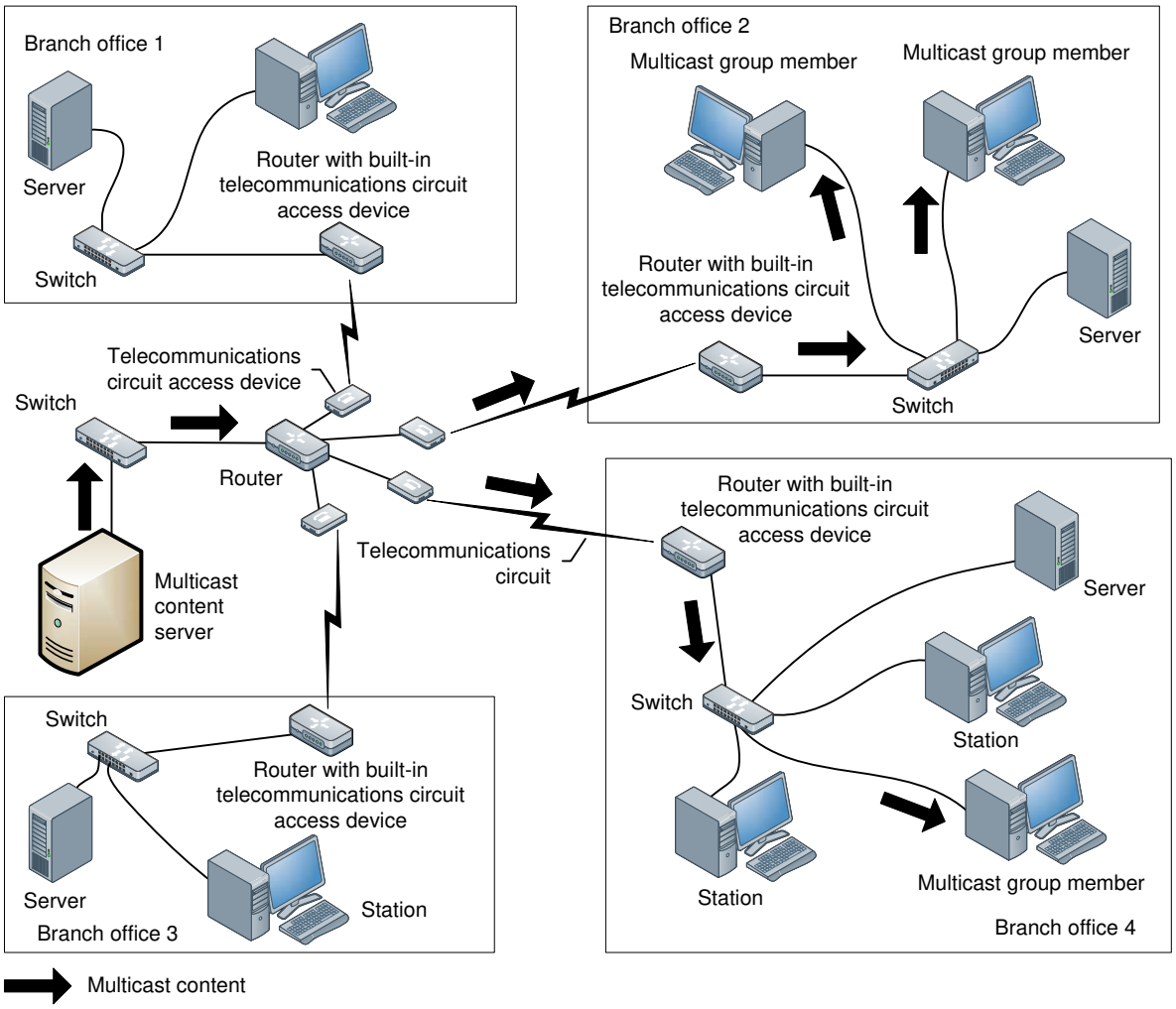
Multicast Messaging

In multicast messaging, or multicasting, the network delivers a transmitted message to a select number of devices—not all devices as in the case of a broadcast. The sending device transmits the message once to a special multicast group address and the network directs the message only to those devices that are listed as members of the group, as shown in Figure 1.14. Multicasting can be described as selective or directed broadcasting. It is the intelligent form of point-to-multipoint message transfer.

NOTES: In Figure 1.14, multicast content is selectively forwarded from the server to the two branch offices where multicast group members are located.

Network switches and routers must be enabled to process multicast messages, otherwise they will be broadcast.

Figure 1.14
Multicast messaging



Types of Addressing

A typical organizational network consisting of multiple interconnected LANs uses two types of addresses to transfer messages between all devices, as follows:

- Every device on a LAN must have a unique address for successful message delivery over the LAN's broadcast domain.
- Since there are multiple LANs connected to each other through an internetwork, each network must have a unique address for successful message delivery over the internetwork.

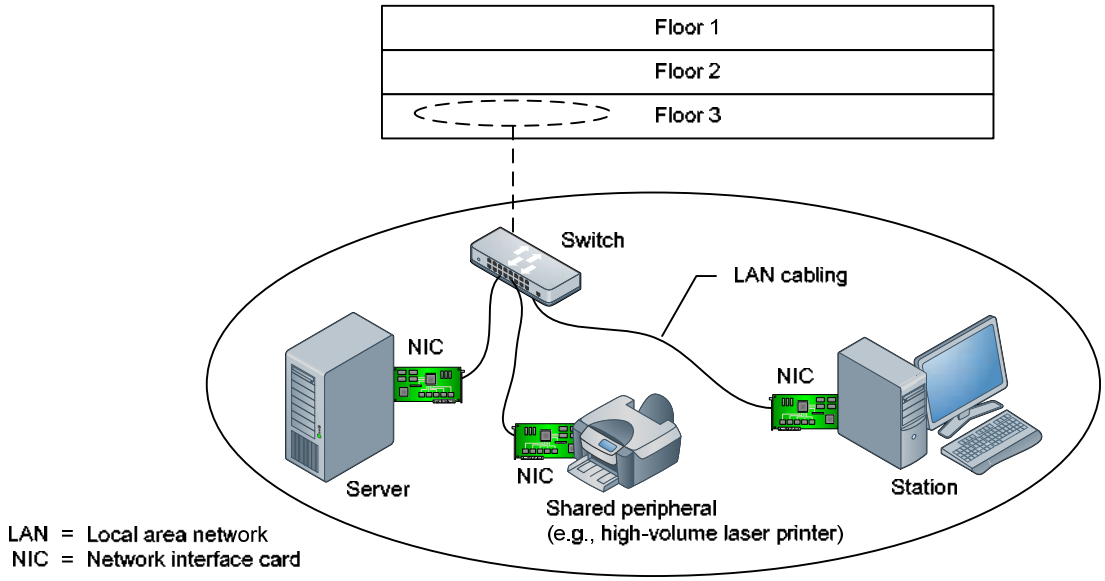
A comparison can be made between these two types of addresses and the addresses used to identify a building in a city. For example, 8610 Hidden River Parkway is the equivalent of a unique device address on a network, while 8610 Hidden River Parkway, Tampa is the equivalent of the combined device and network address on an internetwork.

NOTE: Other types of addresses are also used on networks to identify various resources (e.g., communications channels, protocols, application service ports).

Local Area Network (LAN) Addressing

As described previously, LANs are used to interconnect PCs and other network devices in a geographically limited area, typically not exceeding a single building, as shown in Figure 1.15. Devices are linked using any combination of cabling and wireless systems. The role of the LAN is to enable users to access resources (e.g., devices, software programs, data files) that are not directly connected to or stored on their stations.

Figure 1.15
Example of a local area network



Types of Addressing, continued

The size and complexity of an organizational network determines the number of times a message is processed by network access devices (e.g., switches, wireless access points [WAPs]) before reaching its destination. The endpoint of a message is a specific device, which can be uniquely identified by an address assigned to its network interface card (NIC).

The term medium access control (MAC) address is often used to describe the unique address of a device. Alternate terms used to describe MAC addresses include:

- Layer 2 address.
- Data Link layer address.
- NIC address.
- Hardware address.
- Device address.

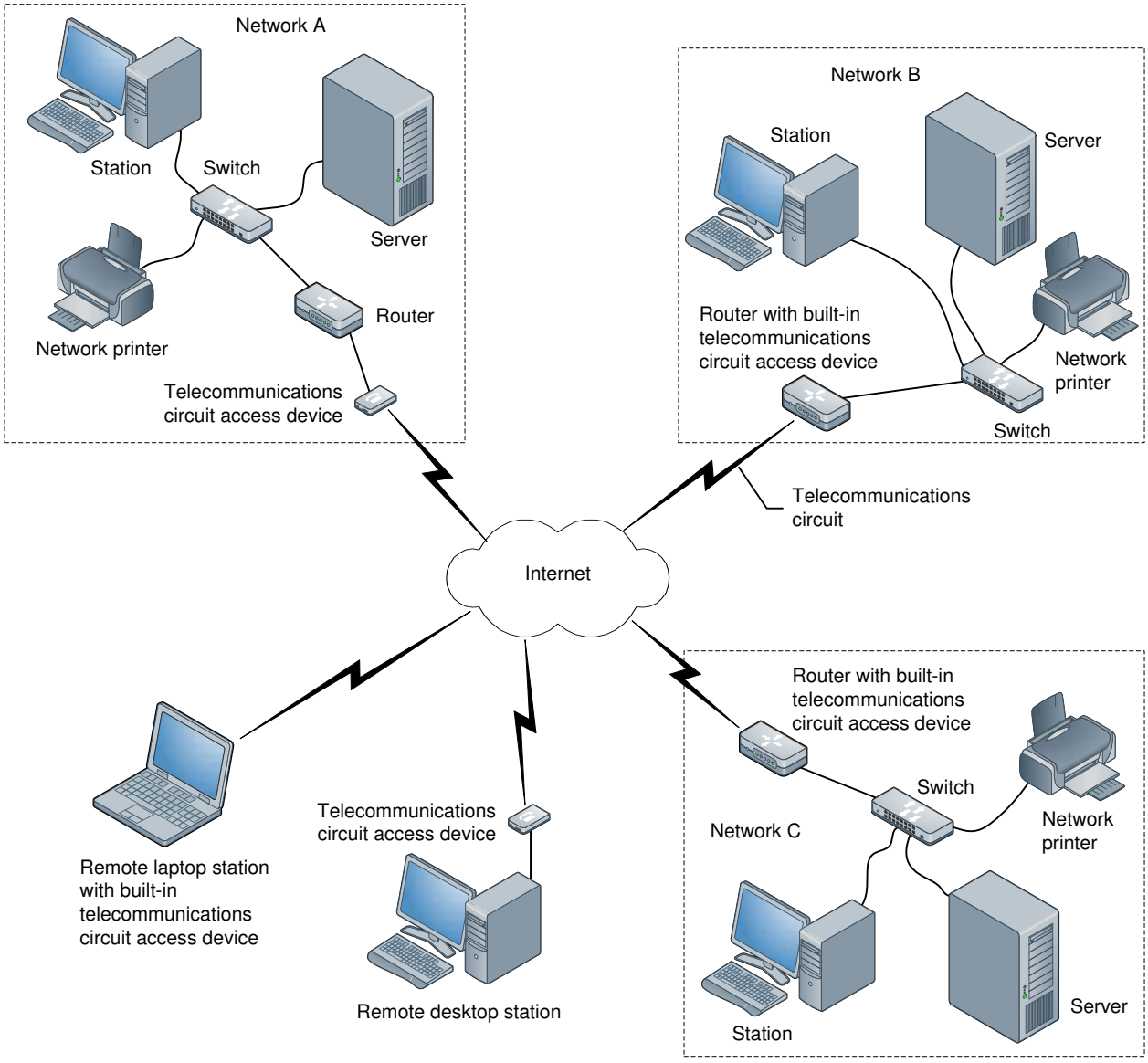
Internetwork Addressing

The role of an internetwork is to enable communications between devices connected to two or more separate networks. An internetwork can span a small or large geographic area, connecting LANs that belong to the same or different organizations.

A small internetwork can connect LANs on different floors of a building. The largest internetwork in existence is the Internet, which is global in scope and serves as a universal resource for message transfer between all types of networks (or between remote stations and networks, as shown in Figure 1.16).

Types of Addressing, continued

Figure 1.16
Example of an internetwork



Types of Addressing, continued

An internetwork like the Internet links all types of similar or dissimilar networks (e.g., Ethernet LANs, mobile telephone networks). In order to uniquely identify each device on any network connected to the Internet in a consistent manner, an address called the Internet protocol (IP) address is assigned to the network interface of each device. This public IP address uniquely identifies both the device and the network to which the device is connected.

NOTES: Non-unique private IP addresses may also be assigned to devices for internal use. Such addresses cannot be used to send messages over the Internet.

The terms network identification (netid) and host identification (hostid) can be used to describe the two parts of an IP address. In such cases, netid identifies the LAN broadcast domain and hostid identifies the device within the LAN broadcast domain.

Using the same format for all addresses on an internetwork makes it possible to link together all types of devices and networks. If necessary, any device can be reconfigured to take the place of any other (e.g., in the event of a breakdown or an upgrade) through a reassignment of the IP address.

The term IP address is often used to describe the internetwork address of a device, since IP is used globally to link to the Internet. Alternate terms used to describe IP addresses include:

- Internet address.
- Layer 3 address.
- Network layer address.
- Subnet address.
- Internetwork address.
- Routing address.

NOTE: IP addresses are the most common—but not the only—means of network/device identification. Other network address systems can also be used on non-IP internetworks.

Types of Addressing, continued

Message Transfer Using Addressing

MAC addresses are used to identify the source and destination of each message on LANs. The stations, servers, and shared peripherals in the LAN broadcast domain communicate with each other using MAC addressing.

When multiple LANs are connected to an internetwork using routers, both MAC and IP addresses are used as follows:

- All routers on an internetwork keep tables of the IP addresses of networks connected to the internetwork.
- A router connected to a network keeps a table of both the MAC address and the IP address of each device on that network.
- When a router receives a message intended for a device on a network connected to itself, it uses the information in its table to forward the message to the appropriate device, using the MAC address.
- When a router receives a message intended for a device on a network connected to another router, it uses the IP address to place the message on a path to that router.

NOTE: On large internetworks, multiple router hops may be required to send a message from one network to another.

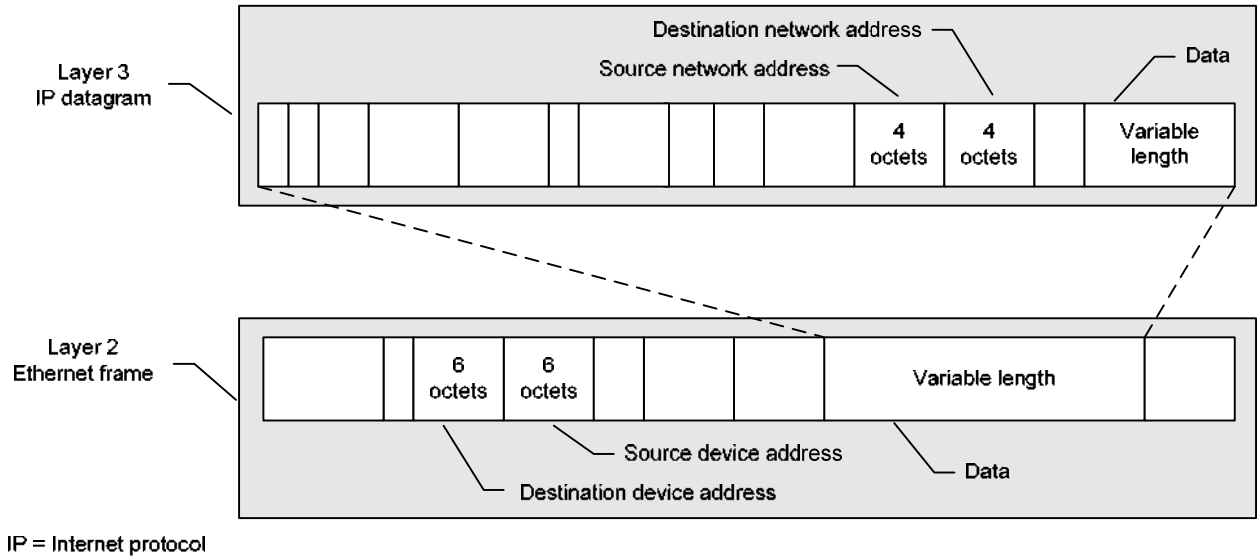
Different terms are used to distinguish between the message format used on a LAN and the message format processed by routers when directing traffic to and from an internetwork. The term:

- Frame is used to describe Layer 2 or LAN messaging units (e.g., Ethernet frames).
- Datagram or packet is used for Layer 3 or internetwork messaging units (e.g., IP datagrams or IP packets).

Types of Addressing, continued

Datagrams containing IP addresses are encapsulated (placed in frames containing MAC addresses), which is comparable to placing an envelope addressed to an individual inside a larger envelope addressed to an organization. Figure 1.17 illustrates this process using a Layer 3 IP datagram within a Layer 2 Ethernet frame.

Figure 1.17
Relationship between an Internet protocol datagram and an Ethernet frame



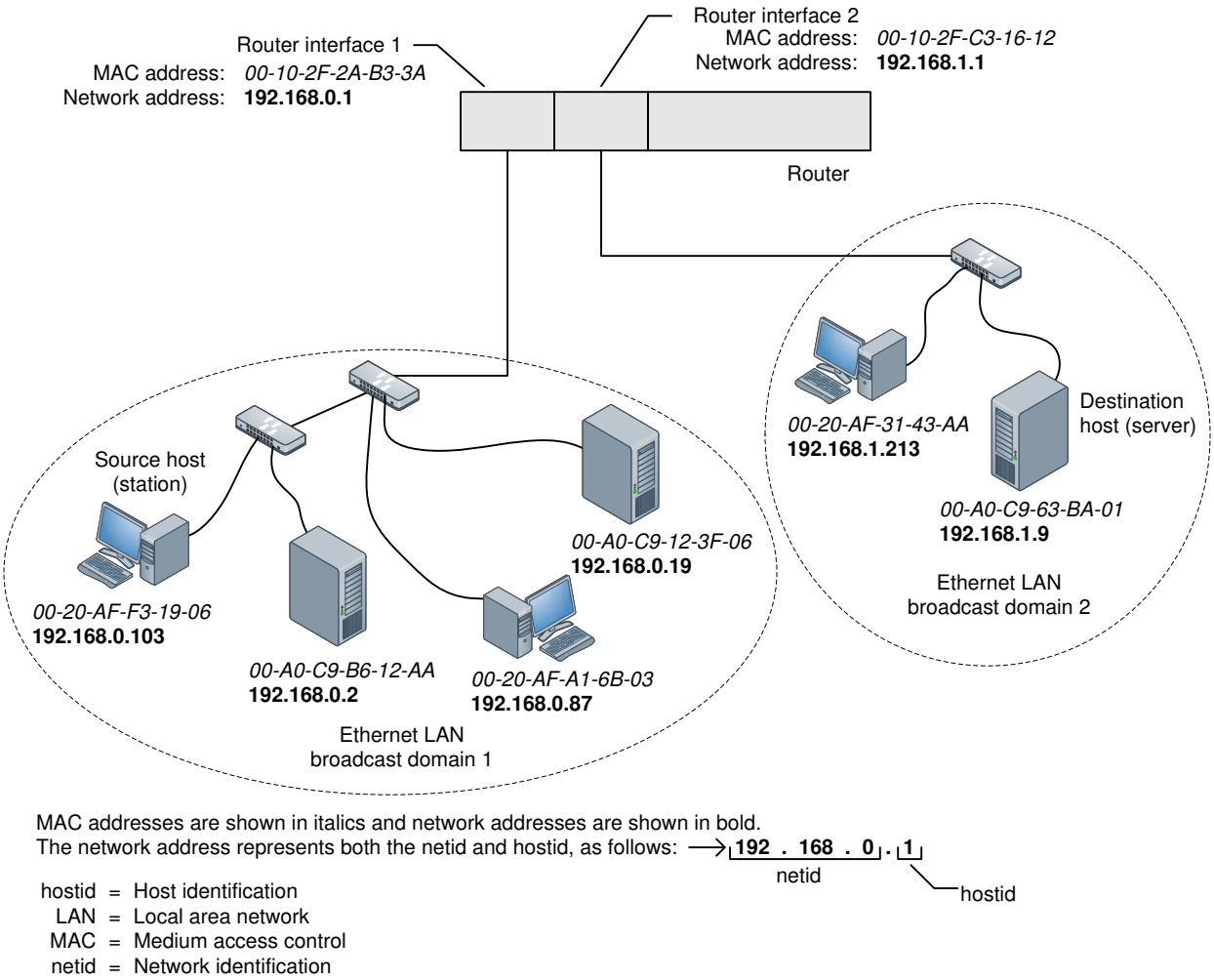
NOTE: An octet is a grouping of eight bits and is commonly referred to as a byte.

Types of Addressing, continued

Figure 1.18 illustrates an internetwork message transfer using Layer 2 Ethernet and Layer 3 IP addressing. In this figure, a router links two Ethernet LAN broadcast domains. Each device on the network, including each router interface, has both a MAC and an IP address, as shown.

NOTE: It is common to express MAC addresses using hexadecimal (hex) notation and IP addresses using dotted decimal notation instead of a sequence of zeros and ones. Each 2-digit grouping in a hex address (e.g., A0) represents eight bits. Each decimal value in a dotted decimal address (e.g., 192) also represents eight bits. MAC addresses are 48 bits in length (12 hex digits) and IPv4 network addresses are 32 bits in length (4 decimal values).

Figure 1.18
Internetwork message transfer



Types of Addressing, continued

In Figure 1.18, the message transfer process occurs as follows:

Step	Message Transfer Process
1	The source host (station) in broadcast domain 1 has an IP datagram to send to the destination host (server) in broadcast domain 2.
2	Since the netid of the destination host (192.168.1) is different from the netid of the source host (192.168.0), the source host places the datagram in an Ethernet frame and sends the frame to the router, using the router interface 1 MAC address as the destination address (00-10-2F-2A-B3-3A).
3	The router receives the frame on interface 1, removes and discards the MAC addressing and control information, and reads the network address.
4	Since the destination host is on a LAN connected to the same router, the router places the datagram in a new Ethernet frame and sends this frame out of interface 2 to the server, using the server's MAC address as the destination address (00-A0-C9-63-BA-01).

The four steps described above illustrate how MAC addresses of the frames are discarded and replaced as many times as necessary to transfer a datagram from its source network to its destination network. At all times, however, the IP datagram and the addresses it contains remain unchanged.

This illustration can also be used to describe the function of IP addressing and routers to reduce broadcast traffic on a network. Routers confine broadcast traffic to the broadcast domain where they originate.

In Figure 1.18 any datagram addressed to all devices is sent to only those devices with the same netid as the source of the datagram. For example, a broadcast frame, containing a datagram issued by host 192.168.0.87 in broadcast domain 1 is prevented by the router from distribution to devices in broadcast domain 2 with netid equal to 192.168.1—only the hosts 192.168.0.19, 192.168.0.2, and 192.168.0.103 receive the broadcast.

NOTE: Because the datagram is broadcast, the host 192.168.0.1 (router interface 1) also receives the message but it is not forwarded.

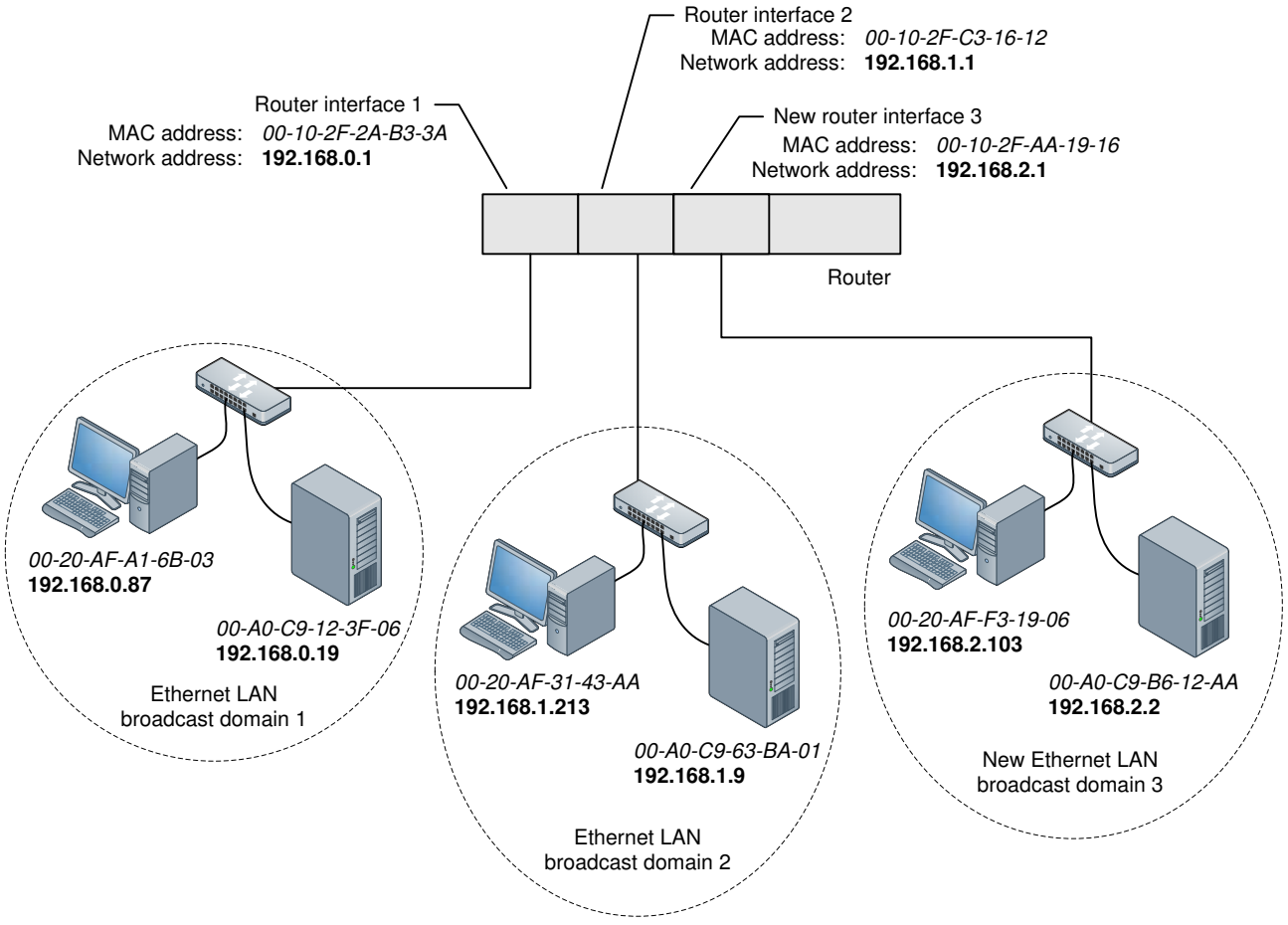
If the level of broadcast traffic becomes excessive and results in delayed network response time, an existing broadcast domain can be split into two by changing the network address of some of the devices and using an additional router interface. This modification is shown in Figure 1.19 where the Ethernet LAN broadcast domain 1 shown in Figure 1.18 has been split into two broadcast domains (broadcast domain 1 and new broadcast domain 3).

Types of Addressing, continued

From an addressing point of view, all that is required is to change the network addresses of the devices transferred to the new broadcast domain. The netid for the new broadcast domain is 192.168.2, which is applied to all devices in this domain, as shown in Figure 1.19.

After this modification is made, any broadcast datagram issued by host 192.168.0.87 in broadcast domain 1 is prevented by the router from distribution to devices in broadcast domains 2 and 3 with netid equal to 192.168.1 or 192.168.2—only the host 192.168.0.19 receives the broadcast.

Figure 1.19
Creating a new broadcast domain



MAC addresses are shown in italics and network addresses are shown in bold.
The network address represents both the netid and hostid, as follows: → **192 . 168 . 0** . **1**
netid
hostid

hostid = Host identification
LAN = Local area network
MAC = Medium access control
netid = Network identification

Network Architecture Standards

Networking-related standards are issued by:

- Standards organizations.
- Industry forums.
- Interest groups.
- Influential vendors.

Standards compliance can be voluntary or mandatory depending on governmental regulations in a given country or economic zone.

Two standards organizations with global influence on networking standards are the:

- IEEE® (formerly known as Institute of Electrical and Electronics Engineers, Inc.®)
- Internet Engineering Task Force (IETF)

IEEE Standards

IEEE is the organization responsible for the standardization of most Layer 2 networking technologies. Specifically, IEEE 802 Local and Metropolitan Area Network Standards Committee (LMSC) guides the development of networking technologies that enable the same services and applications to operate over a variety of Layer 2 networks. An example is Internet connectivity, which can be enabled on any type of wireless or wired LAN.

The objective of IEEE 802 LMSC is to publish standards that are supported by both vendors and buyers of networking products. The greater the level of acceptance of a given standard, the higher the level of assurance of interoperability among products described as standards-compliant.

Many of the standards published by IEEE have subsequently been adopted by the:

- American National Standards Institute (ANSI) as U.S. standards.
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) as global standards.

IEEE 802 LMSC has a number of Working Groups (WGs) and Technical Advisory Groups (TAGs). Each focuses on a specific set of topics and technologies. Since its inception in 1980, IEEE LMSC has formed a total of 21 WGs and TAGs, some of which have been disbanded or are no longer active.

Network Architecture Standards, continued

At the time of this writing, the active IEEE 802 WGs and TAGs are:

- IEEE 802.1—Higher Layer LAN Protocols Working Group
- IEEE 802.3—Ethernet Working Group
- IEEE 802.11—Wireless LAN (WLAN) Working Group
- IEEE 802.15—Wireless Personal Area Network (WPAN) Working Group
- IEEE 802.16—Broadband Wireless Access Working Group
- IEEE 802.17—Resilient Packet Ring (RPR) Working Group
- IEEE 802.18—Radio Regulatory Technical Advisory Group
- IEEE 802.19—Coexistence Technical Advisory Group
- IEEE 802.20—Mobile Broadband Wireless Access (MBWA) Working Group
- IEEE 802.21—Media Independent Handover Services Working Group
- IEEE 802.22—Wireless Regional Area Networks (WRANs) Working Group

The inactive IEEE 802 WGs are:

- IEEE 802.2—Logical Link Control (LLC) Working Group
- IEEE 802.5—Token Ring Working Group

The disbanded IEEE 802 WGs and TAGs are:

- IEEE 802.4—Token Bus Working Group
- IEEE 802.6—Metropolitan Area Network (MAN) Working Group
- IEEE 802.7—Broadband Technical Advisory Group
- IEEE 802.8—Fiber Optic Technical Advisory Group
- IEEE 802.9—Integrated Services LAN Working Group
- IEEE 802.10—Security Working Group
- IEEE 802.12—Demand Priority Working Group
- IEEE 802.14—Cable Modem Working Group

NOTES: There is no IEEE 802.13 group.

The IEEE 802 Working Group home page at http://grouper.ieee.org/groups/802/dots.html provides information and links to additional resources for each WG and TAG.

Network Architecture Standards, continued

Internet Engineering Task Force (IETF) Standards

IETF is one of a group of organizations responsible for the overall development of the Internet and the standardization of internetworking technologies. The influence of IETF on Layer 3 internetworking standards can be compared to the influence of IEEE on Layer 2 LAN standards.

In addition to IETF, the following organizations contribute to the overall development of the Internet:

- Internet Society™ (ISOC), which oversees overall development on the Internet.
- Internet Architecture Board (IAB), whose members are appointed by ISOC, serves as ISOC's technical advisory group. IAB is responsible for the overall development of the protocols and architecture associated with the Internet.
- Internet Engineering Steering Group (IESG), whose members are approved by IAB, oversees the activities of IETF and manages the process used to introduce or update Internet standards.
- Internet Research Task Force (IRTF), which is the research counterpart of IETF. Technical topics considered theoretical or experimental in nature are explored by IRTF. When a technology is judged suitable for practical use on the Internet, it is forwarded to IETF for consideration.
- Internet Research Steering Group (IRSG), which oversees the activities of IRTF in the same way IESG manages IETF.
- Internet Corporation for Assigned Names and Numbers (ICANN), which replaced the Internet Assigned Numbers Authority (IANA) in 1998. ICANN oversees Internet naming and addressing.

Each Internet standard is published and updated with the title request for comments (RFC) and all are freely available on the Internet. A protocol under consideration for eventual adoption as an Internet standard is first published as a proposed standard. After additional study, the protocol may be promoted to the draft standard stage. The final step in the standardization process is the promotion of a draft standard to the status of standard.

NOTES: Additional classifications include informational standard, experimental standard, and historic standard. Such standards are excluded from consideration as operational Internet standards or best current practices (BCPs).

The RFC Search page at http://www.rfc-editor.org/rfcsearch.html provides listings and contents of all past and current RFCs.

Network Design

An organizational network requires many types of design, each focusing on a specific characteristic of the network. For example, one design can detail network traffic flows, while another illustrates the physical location of each network device.

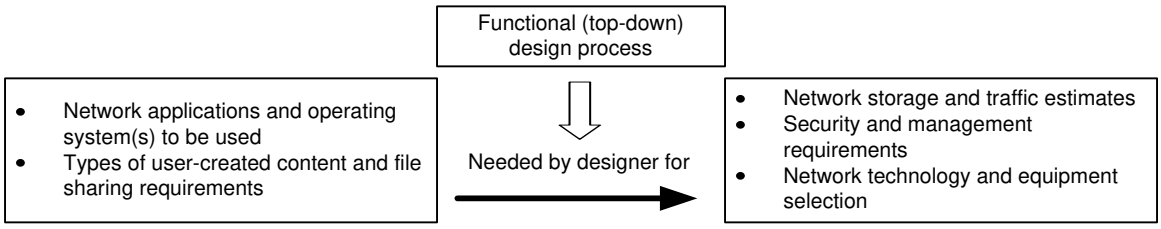
Functional Design Process

Functional design is also referred to as top-down design. In this process, the network designer begins with an assessment of the types of users and applications likely to be supported by the proposed network.

Other factors, including the proposed network operating system (NOS) and the expected volume of data to be generated by users, are also evaluated.

Upon analysis of the information gathered, the designer can generate preliminary requirements for network processing and storage, expected traffic patterns and levels, and the administrative infrastructure, as shown in Figure 1.20. This information is then used to select the appropriate network technologies and products.

Figure 1.20
Functional (top-down) design



Network Design, continued

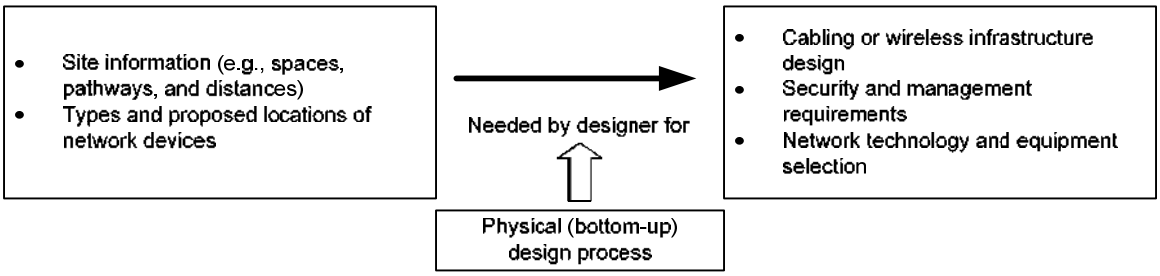
Physical Design Process

Physical design is also referred to as bottom-up design. In this process, the network designer begins with an assessment of the site(s) where the proposed network is to be deployed. Details such as the physical characteristics of the premises, security requirements, and expected distances between network devices are assessed, as shown in Figure 1.21.

Upon analysis of the information gathered, appropriate selections can be made for the types of network connectivity and products required at the site(s).

NOTE: The physical design process is used in cases where detailed network characteristics are not available (e.g., new multi-tenant commercial buildings).

Figure 1.21
Physical (bottom-up) design



Project Management

Overview

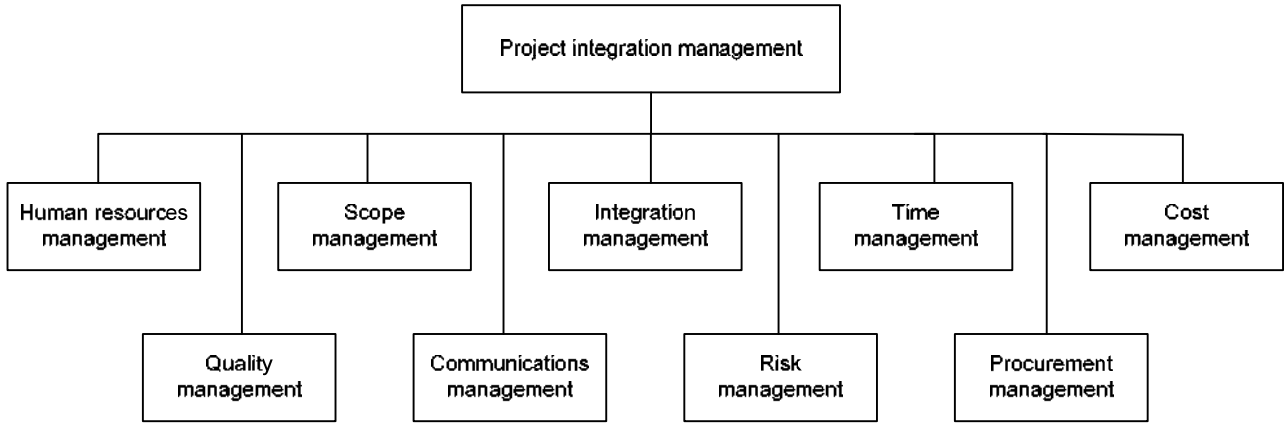
In general terms, a project can be described as an activity of limited duration, where human, physical, and financial resources are deployed to produce a well-defined output.

The goal of project management is to ensure that all resources are optimally used to deliver the expected output, on-time and on-budget. Project managers use a variety of tools and techniques to schedule and coordinate all necessary activities, including specialized software.

The Project Management Institute (PMI) is a not-for-profit association with worldwide membership that has developed a library of standards consisting of best practices for project management professionals. One of its publications is *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)-4th Edition*, issued in 2008.

The PMBOK defines nine types of management knowledge areas considered to be universally applicable to all projects, as shown in Figure 1.22.

Figure 1.22
Project management knowledge areas



Overview, continued

Human Resources Management

The human resource area of project management covers personnel issues, which involves engaging the right people to do the job and ensuring they are properly trained, equipped, and motivated. In addition, project safety, an area where the PM may have the greatest personal liability, also is covered by this area.

Scope Management

Scope management of a project involves development of a scope statement approved by both the customer and the company. The scope can include and go beyond the detailed specifications for the job.

NOTE: The scope may be understood as the fence around a project and includes a list of assumptions about the project.

Integration Management

Integration management of a project covers the breakup of a large project into multiple small projects or the reverse, running several small projects as one large one. It involves the integration of various subteams (e.g., electrical contractor, private branch exchange/local area network [PBX/LAN] vendors) into a project organization with an integrated plan.

Time Management

Time management of a project covers time estimates and schedules. It includes the integration of time schedules from various subteams and calculation of the critical path of events on the project. During the project, a current schedule must be maintained and communicated to the team.

Cost Management

Cost management of a project includes development of a cost estimate and project budget. During the project, costs are tracked and budgets are adjusted and updated to reflect a change order or additional service activity.

Quality Management

Each project should have a quality management plan that includes detailed review of the design documentation throughout the project. In the event that the information transport systems (ITS) designer is also responsible for the build portion of the project, then physical quality (i.e., workmanship) and test results would also be a part of this area. Finally, customer value items (e.g., punctuality, appearance, and professionalism of the cabling installers) are included in this area.

Overview, continued

Communications Management

Communications management of a project does not just happen—it is planned. A communications plan includes scheduled meetings and the use of electronic media. In certain situations, it may be a good idea to establish a "war room" for the project, where the schedule and actual results can be posted on a whiteboard.

Risk Management

Each project and project element carry various types of risks. Depending on the nature of the project, it could include injury, professional damage, scheduling conflicts, errors and omissions, and cost risk. If possible, a risk assessment should be completed before a company submits a proposal on the project. A risk plan should then be developed with a focus on mitigating the risk.

Procurement Management

This area of project management covers procurement of resources outside the team, including materials and subcontractors. It includes the transport and storage cost of bulk purchases versus just-in-time procurement on a construction-type project.

Specifications Writing

Overview

Specifications are one of the elements produced during the design phase of a construction project.

The four main types of specifications that can be used to define the requirements are:

- Performance—The focus is on results. Contractors can choose the materials and installation methods to provide the desired results.
- Proprietary—Specifications call out brand names and models.
- Descriptive—The focus is on exact properties and installation methods.
- Reference—Requirements are based on an established standard.

Construction documents in North America use a standardized format jointly produced by the Construction Specifications Institute (CSI) and Construction Specifications Canada (CSC).

These standards are currently being harmonized worldwide. The SectionFormat™ / PageFormat™ document standardizes how the text on each page in a specification is presented and organizes the information in each section and then organizes each section into three parts:

- Part 1—General
- Part 2—Products
- Part 3—Execution

The MasterFormat™ is a list of numbers and titles compiled to organize the activities and requirements of a construction project. Before the 2004 edition, the MasterFormat™ included 16 divisions, as well as a summary of the front-end requirements. Telecommunications scope of work was included within the electrical scope of Division 16 and work areas were found on the "E" drawings. This format is still prevalent within the North American design and construction industry.

The MasterFormat™ structure was developed by CSI because construction projects can use many different delivery methods, products, and installation methods. Successful completion of these large and complex projects requires effective communication among the people involved. Information retrieval is nearly impossible without a standard filing system familiar to each user. The MasterFormat™ serves as this standard filing system.

MasterFormat™ numbers and titles are suitable for use in project manuals, for organizing cost data, placing reference keynotes on drawings, for filing project information and other technical data, for identifying drawing objects, and for presenting construction market data.

Overview, continued

When combined with the WBS numbering for task assignments, and tracked in a visual information system (VIS) or geographic information system (GIS), the end user will be able to track what was installed, who installed it, and when the installation was completed. The system also will link to test records, pictures, drawings, and other project information in the end customer computer aided cable management (CAFAM) system.

MasterFormat™ 2004—Numbering Revision

In 2004, the CSI published a new format for the organization of project information within the construction industry. Adaptation of this format continues today. One of the most significant changes in the MasterFormat™ 2004 revision is the adoption of a six-digit numbering system in place of a five-digit system for organizing various subcategories.

Table 1.1
MasterFormat™ 2004—numbering revision

Division	Title
PROCUREMENT AND CONTRACTING REQUIREMENTS GROUP	
Division 00	Procurement and Contracting Requirements
SPECIFICATIONS GROUP	
General Requirements Subgroup:	
Division 01	General Requirements
Facility Construction Subgroup:	
Division 02	Existing Conditions
Division 03	Concrete
Division 04	Masonry
Division 05	Metals
Division 06	Wood, Plastics, and Composites
Division 07	Thermal and Moisture Protection
Division 08	Openings
Division 09	Finishes
Division 10	Specialties
Division 11	Equipment
Division 12	Furnishings
Division 13	Special Construction
Division 14	Conveying Equipment
Division 15	Reserved for future expansion
Division 16	Reserved for future expansion
Division 17	Reserved for future expansion
Division 18	Reserved for future expansion
Division 19	Reserved for future expansion

MasterFormat™ 2004—Numbering Revision, continued

Table 1.1, continued
MasterFormat™ 2004—numbering revision

Division	Title
Facility Services Subgroup:	
Division 20	Reserved for future expansion
Division 21	Fire Suppression
Division 22	Plumbing
Division 23	Heating Ventilating and Air Conditioning
Division 24	Reserved for future expansion
Division 25	Integrated Automation
Division 26	Electrical
Division 27	Communications
Division 28	Electronic Safety and Security
Division 29	Reserved for future expansion
Site and Infrastructure Subgroup:	
Division 30	Reserved for future expansion
Division 31	Earthwork
Division 32	Exterior Improvements
Division 33	Utilities
Division 34	Transportation
Division 35	Waterway and Marine
Division 36	Reserved for future expansion
Division 37	Reserved for future expansion
Division 38	Reserved for future expansion
Division 39	Reserved for future expansion
Process Equipment Subgroup:	
Division 40	Process Integration
Division 41	Material Processing and Handling Equipment
Division 42	Process Heating, Cooling, and Drying Equipment
Division 43	Process Gas and Liquid Handling, Purification and Storage Equipment
Division 44	Pollution Control Equipment
Division 45	Industry-Specific Manufacturing Equipment
Division 46	Reserved for future expansion
Division 47	Reserved for future expansion
Division 48	Electrical Power Generation
Division 49	Reserved for future expansion

MasterFormat™ 2004—Numbering Revision, continued

An example of the new six-digit format is:

27 13 00 Communications Backbone Cabling

As was the case with the old system, the first two digits, in this case "27," still represent the division number, also known as "level one." The next pair of numbers, in this case "13," and the third pair "00," represents level three. Generally, level four numbers are not defined, but when they are, an additional pair of digits is attached to the end, preceded by a "dot."

An example is:

27 13 43.33 DSL Services Cabling

Additional recommendations for the use of level four and level five is included in the MasterFormat™ 2004 application guide and throughout the full publication, preserving the level of user modifiable numbers for flexibility.

More importantly, because each level of classification is represented by a pair of digits, there is room to address over 10 times as many subjects at each level, providing flexibility and room for expansion that the five-digit numbers could not provide, and addressing future needs for expansion for new subject matter.

MasterFormat™ 2004 Division Number Changes Affecting Information Transport

Division 16 has been reserved for future expansion and material has been relocated to Divisions 26—Electrical, and 27—Communications in the facility services subgroup.

- Division 21—Fire Suppression: Fire suppression subjects relocated from Division 13.
- Division 25—Integrated Automation: Expanded integrated automation subjects relocated from Division 13.
- Division 26—Electrical: Electrical and lighting subjects relocated from Division 16.
- Division 27—Communications: Expanded communications subjects relocated from Division 16.
- Division 28—Electronic Safety and Security: Expanded electronic safety and security subjects relocated from Division 13.
- Division 31—Earthwork: Site construction subjects, chiefly below grade, from Division 2.
- Division 33—Utilities: Expanded utility subjects relocated from Division 2.

References

BICSI®. *Telecommunications Distribution Methods Manual,* 12th ed. Tampa, FL: BICSI, 2009.

Construction Specifications Institute and Construction Specifications Canada. *MasterFormat™.* Alexandria, VA and Toronto, ON: Construction Specifications Institute and Construction Specifications Canada, 2004.

Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) - 4th Edition.* Newtown Square, PA: Project Management Institute, 2008.

