Computer Networks and Internet

Szu-Chi Chung

Department of Applied Mathematics, National Sun Yat-sen University

Introduction

- Internet is a system that interconnects billions of computers in the world, we think of the Internet not as a single network, but as an *internetwork*, a combination of networks
  - We start our journey by first defining a network
  - We then show how we can connect networks to create small internetworks
  - Finally, we show the structure of the Internet and open the gate to studying the Internet in the rest of this chapter

Networks

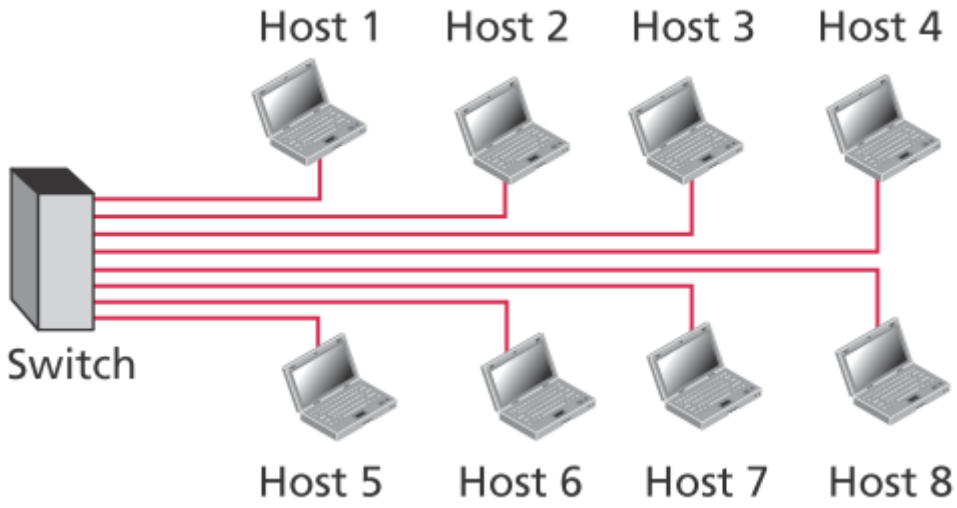
- A *network* is the interconnection of a set of devices capable of communication
  - A device can be a *host* (or an *end system* as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system
  - A device can also be a *connecting device* such as a *router* which connects the network to other networks, a *switch* which connects devices together, a modem (modulator-demodulator) that changes the form of data, and so on
- When we connect two computers at home using a plug-and-play router, we have created a network, although very small

https://zh.wikipedia.org/zh-tw/ADSL#/media/File:Alcatel_T07AW_of_Chunghwa_Telecom_2007-02-27.jpg

https://www.tp-link.com/tw/home-networking/wifi-router/archer-c1200/

Local area network

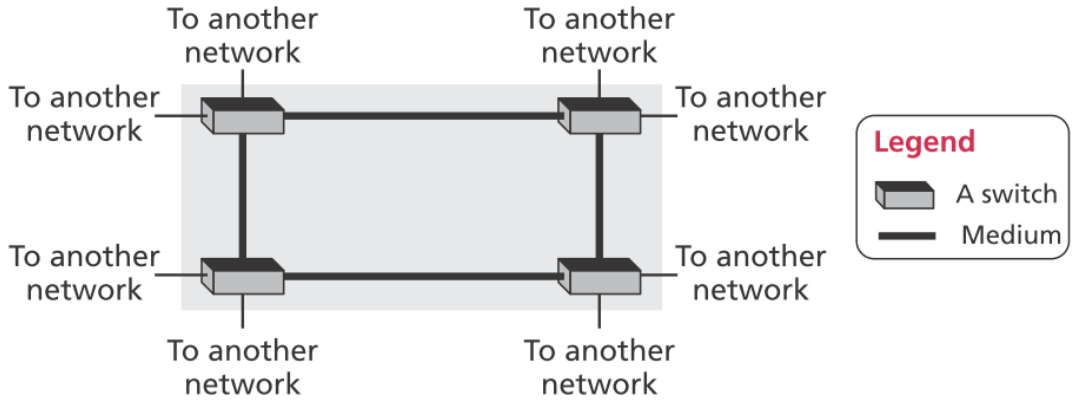
- A *local area network (LAN)* is usually privately owned and connects some hosts in a single office, building, or campus
  - Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN
  - A *packet* sent by a host to another host carries both the source host's and the destination host's addresses



Wide area network

- A wide area network (WAN) is also an interconnection of devices
  - Compared to LAN, a WAN has a wider geographical span, spanning a town, a state, a country, or even the world
  - A WAN usually interconnects connecting devices such as switches, routers, or modems and is normally created and run by communication companies
  - A *point-to-point WAN* is a network that connects two communicating devices through a transmission medium (cable or air)
  - A *switched WAN* is a network with more than two ends

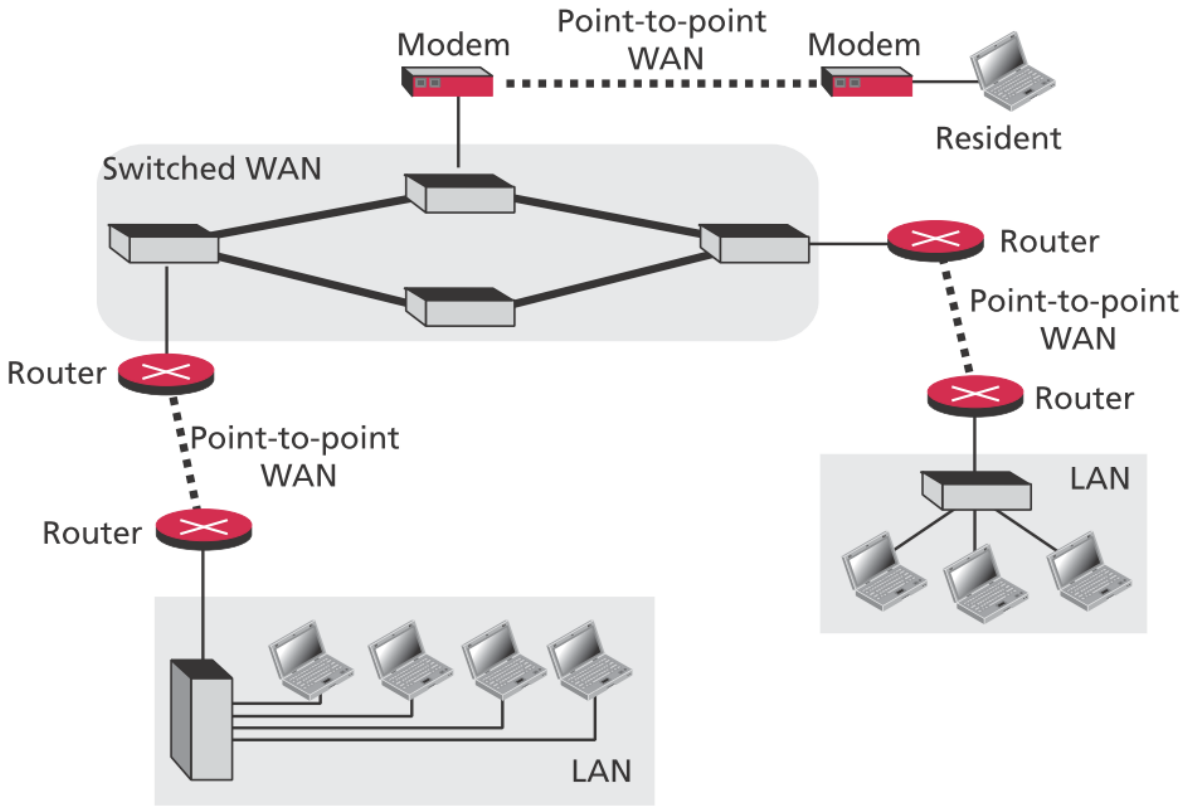
a. Point-to-point WAN



b. Switched WAN

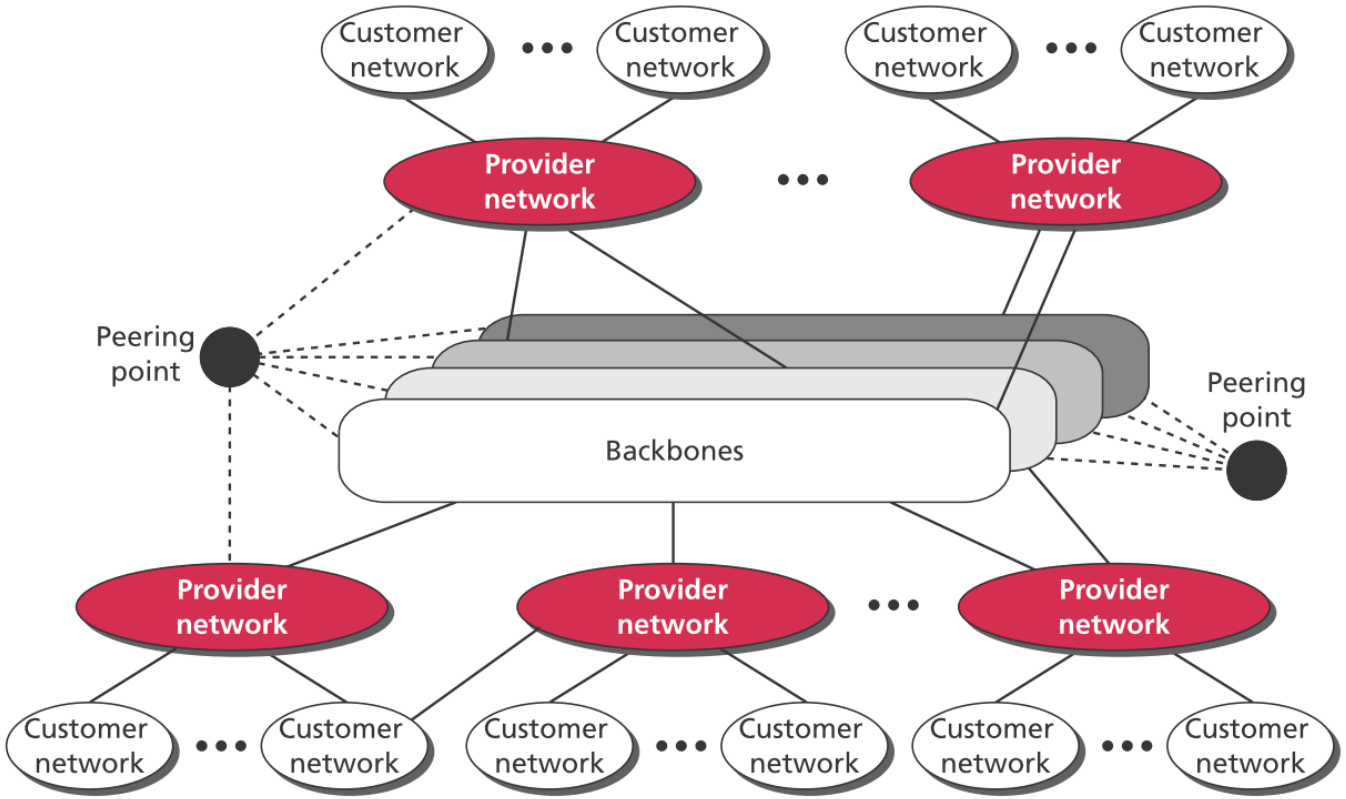
Internetwork

- When two or more networks are connected, they make an *internetwork,* or *internet*



The Internet

- The most notable internet is called the *Internet* (uppercase I), and is composed of thousands of interconnected networks
  - Backbones and provider networks are also called *internet service providers (ISPs)*
  - The backbones are often referred to as international ISPs
  - The provider networks are often referred to as national or regional ISPs

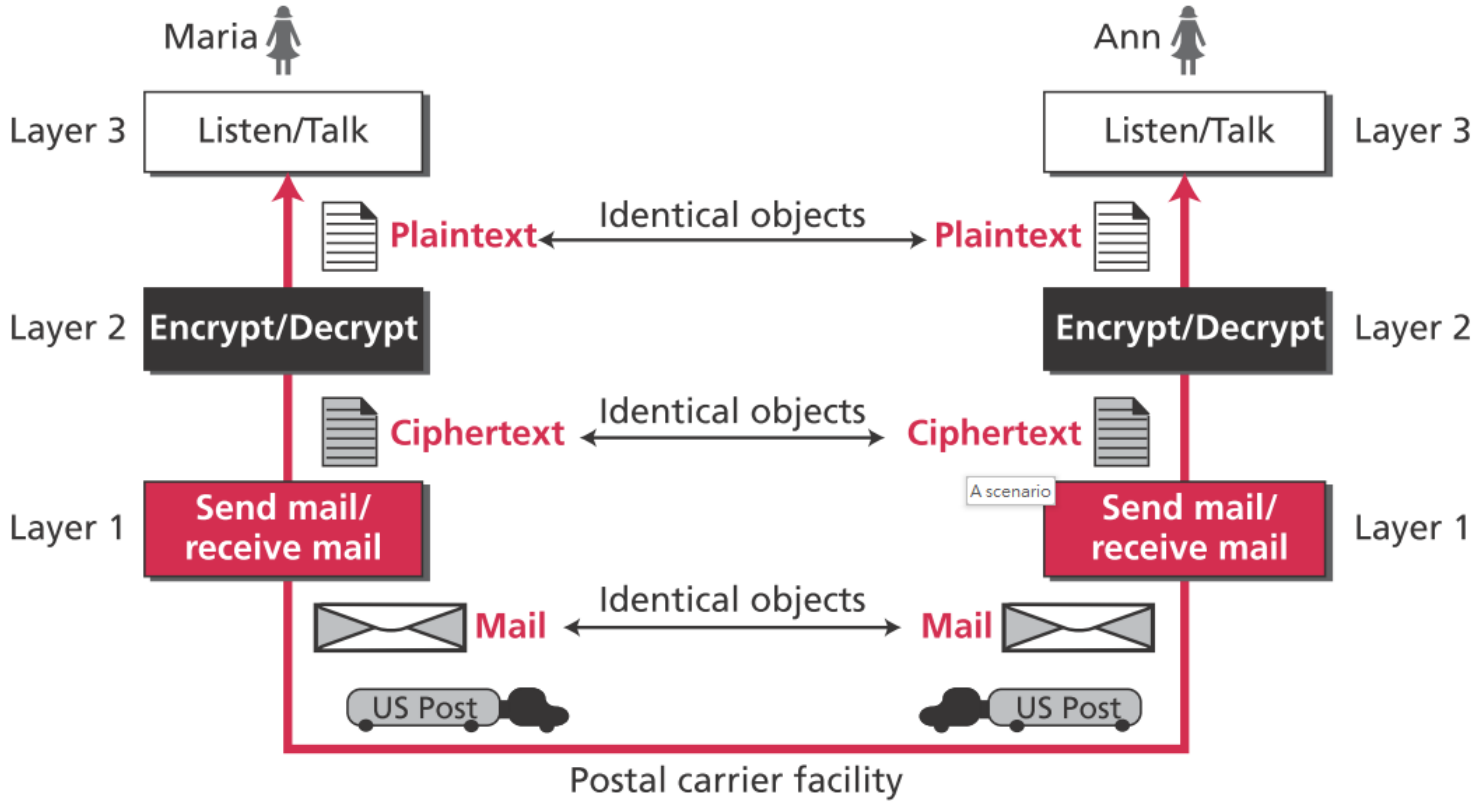


Protocol layering

- Similar to a computation in which we need both a computer and a program, we need both hardware and software for communication
- A word we hear all the time when we talk about the Internet is *protocol*
  - A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively
  - When communication is simple, we may need only one simple protocol
  - When communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or *protocol layering*

A scenario

- We assume that Ann and Maria are friends and they decide to continue their secret conversation using regular mail through the post office



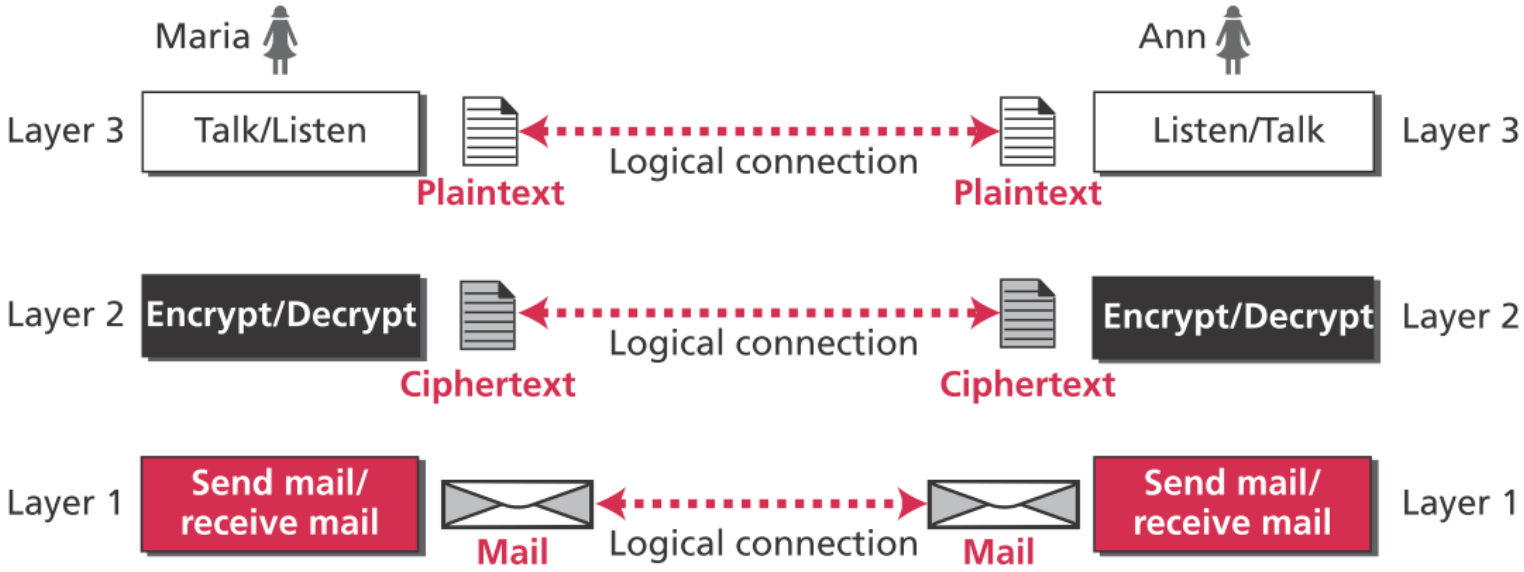
A scenario

- Protocol layering enables us to divide a complex task into several smaller and simpler tasks
  - If Maria and Ann decide that the encryption/decryption done by the machine is not enough to protect their secrecy, they need to change only the second-layer machine
    - This is referred to as *modularity* which means independent layers
  - A layer (*module*) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs
    - A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented
- In reality, communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers
  - If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive!

Principles of protocol layering

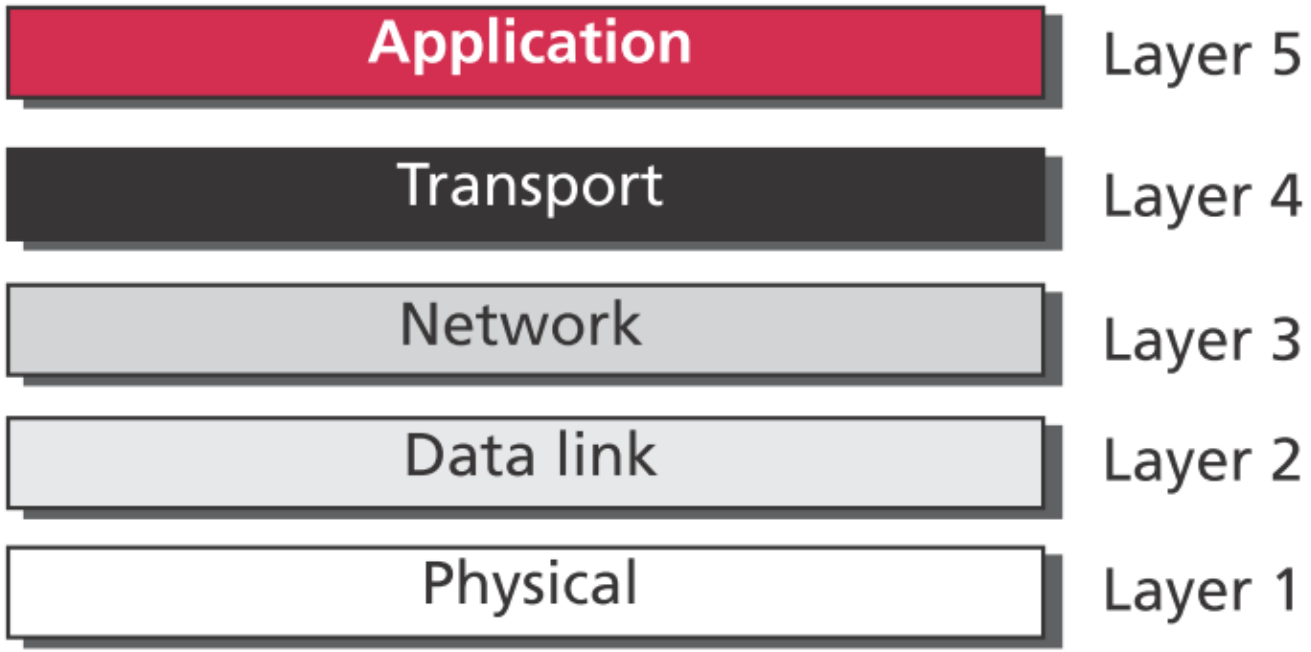
1. If we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction
2. Two objects under each layer at both sites should be identical

- After following the above two principles, we can think about *logical connection* between each layer!



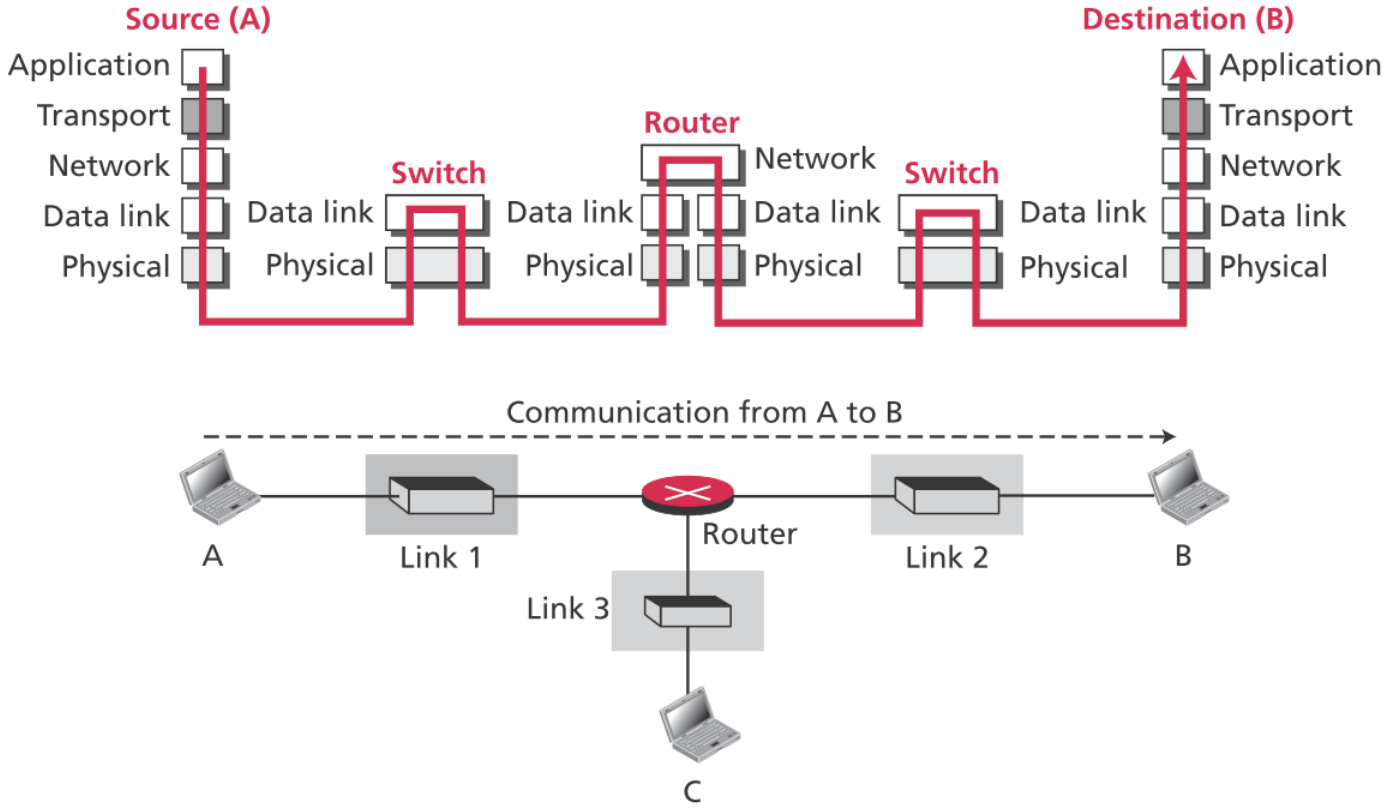
TCP/IP protocol suite

- *TCP/IP (Transmission Control Protocol/Internet Protocol)* is a protocol suite (a set of protocols organized in different layers) used in the Internet today
  - It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality



Layered architecture

- Assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch
  - The two hosts are involved in all five layers; the source host needs to create a message in the *application layer* and send it down so that it is physically sent to the destination host
  - The destination host needs to receive the communication at the *physical layer* and then deliver it through the other layers to the application layer

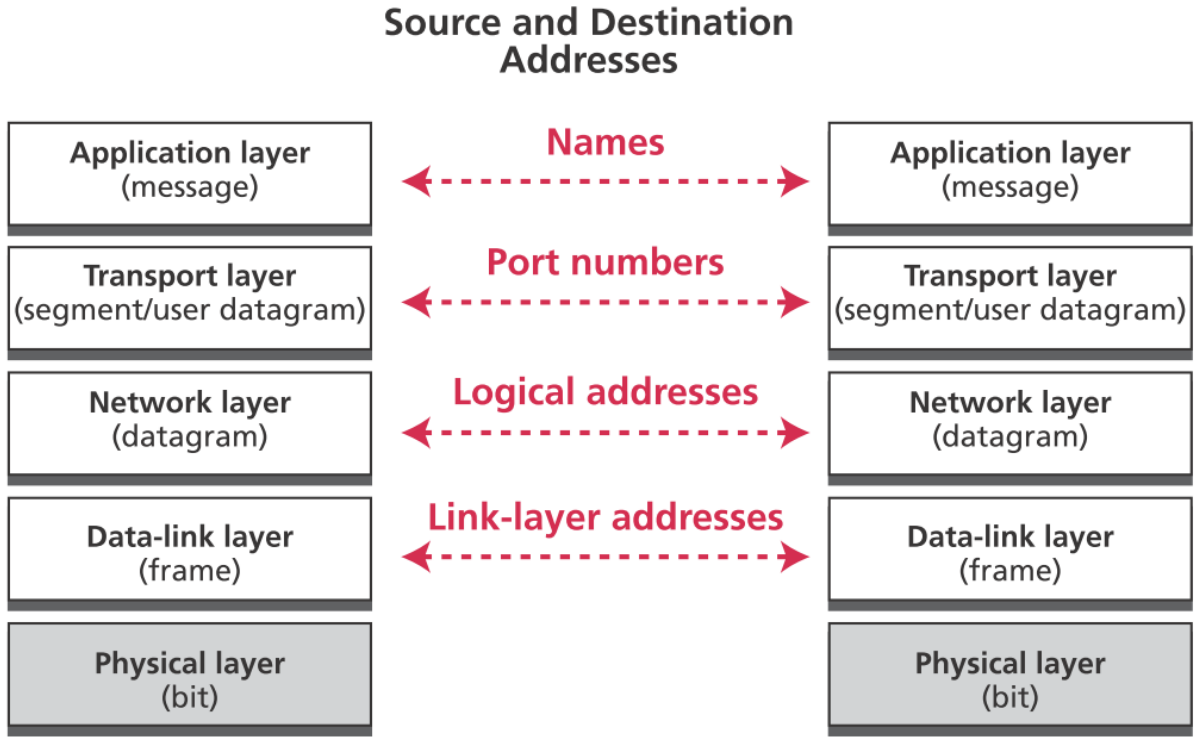


Layered architecture

- The router is involved only in three layers as the router is used only for routing
  - Each link may be using different link-layer and physical-layer protocols; the router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols
- A link-layer switch in a link, however, is involved only in two layers
  - The two connections are in the same link, which uses only one set of protocols

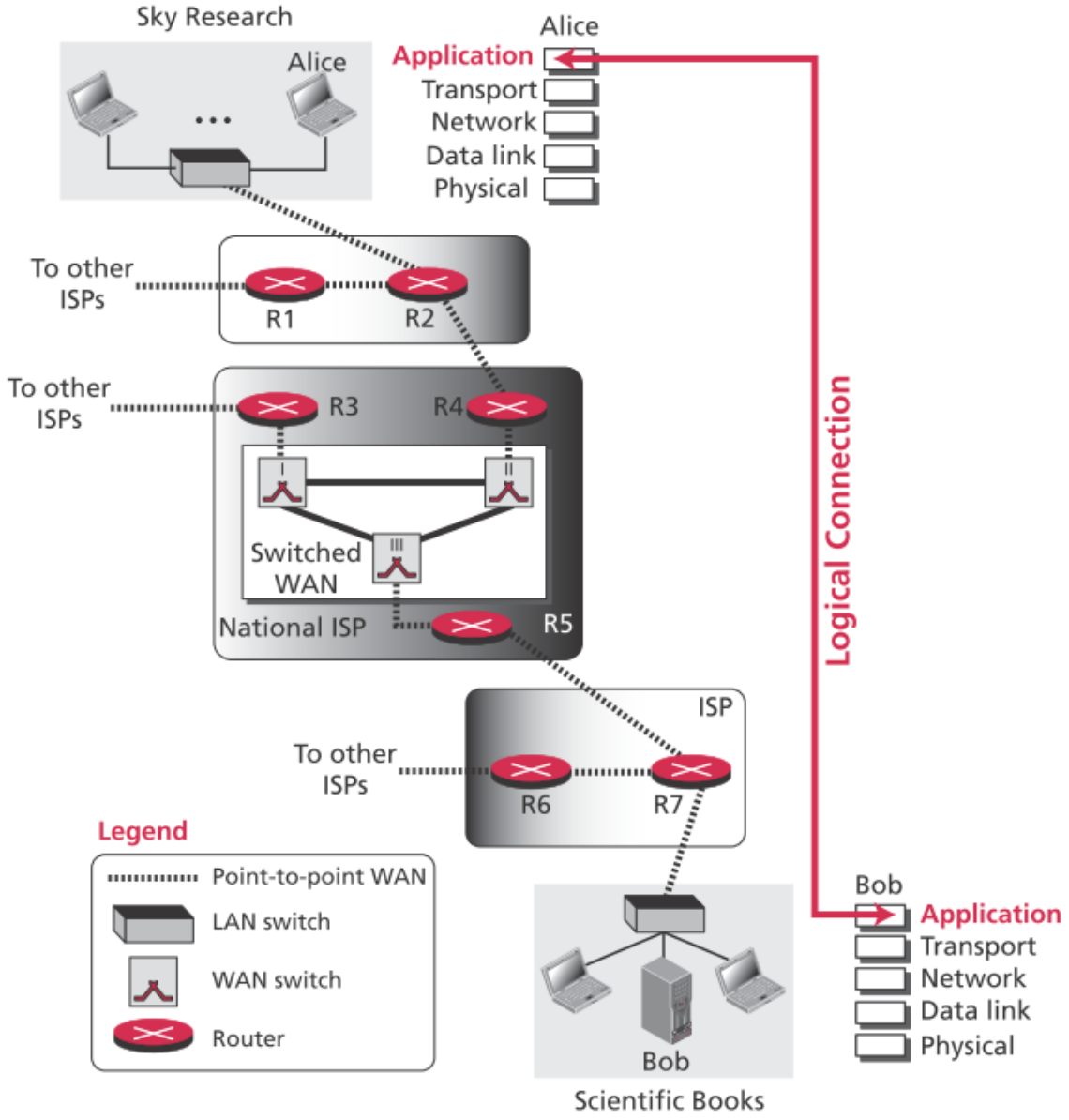
Addressing and packet names

- It is worth mentioning another two concepts related to protocol layering in the Internet: *addressing* and *packet names*
  - Any communication that involves two parties needs two addresses: source address and destination address
  - The link-layer addresses, sometimes called *MAC addresses*, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN)



Application layer

- The *application layer* provides services to the user
  - Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages
  - The actual communication, however, takes place through several devices (Alice, R2, R4, R5, R7, and Bob) and several physical channels

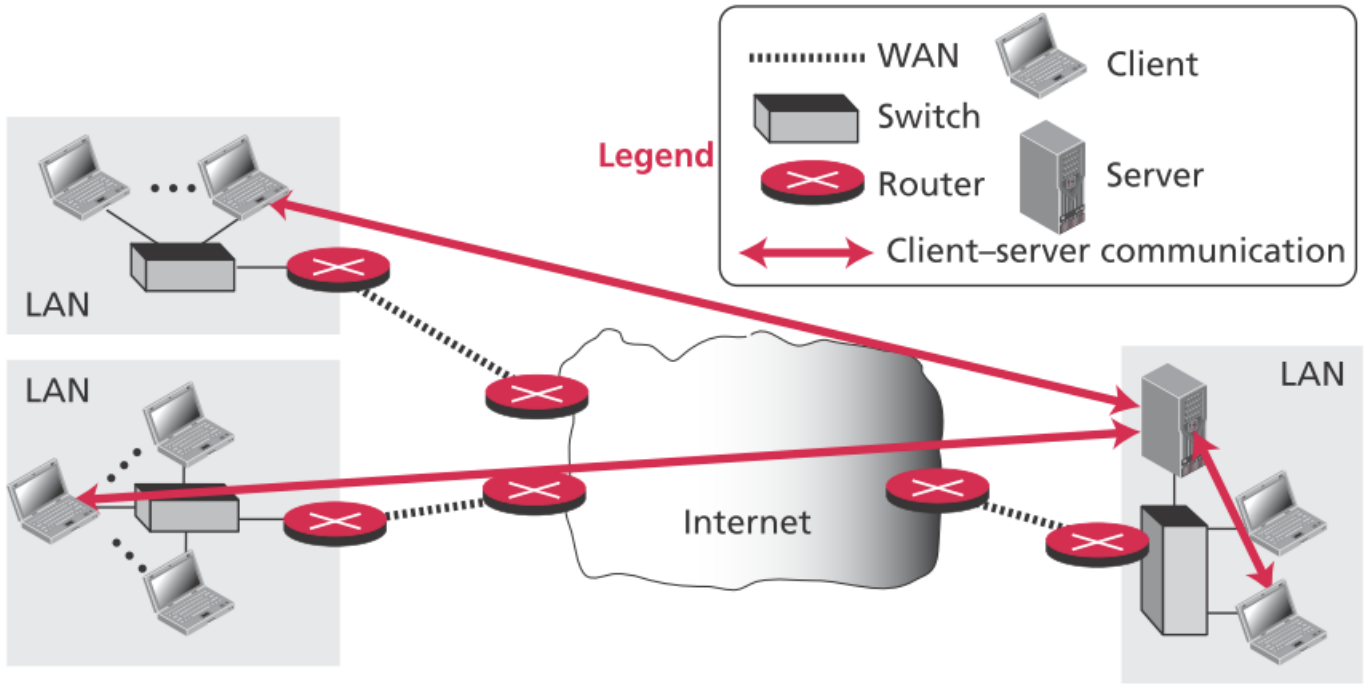


Application layer - Providing services

- The protocols in this layer do not provide services to any other protocol in the suite; they only receive services from the protocols in the transport layer
  - It is the only layer that provides services to the Internet user
    - The flexibility of the application layer allows new application protocols to be easily added to the Internet
  - What is the relationship should be between the two programs in the application layer?
    - Two paradigms have been developed: the *client–server paradigm* and the *peer-to-peer paradigm*

Traditional paradigm: client–server

- In this paradigm, the service provider is an application program, called the *server process*; it runs continuously, waiting for another application program, called the *client process* to make a connection and ask for service

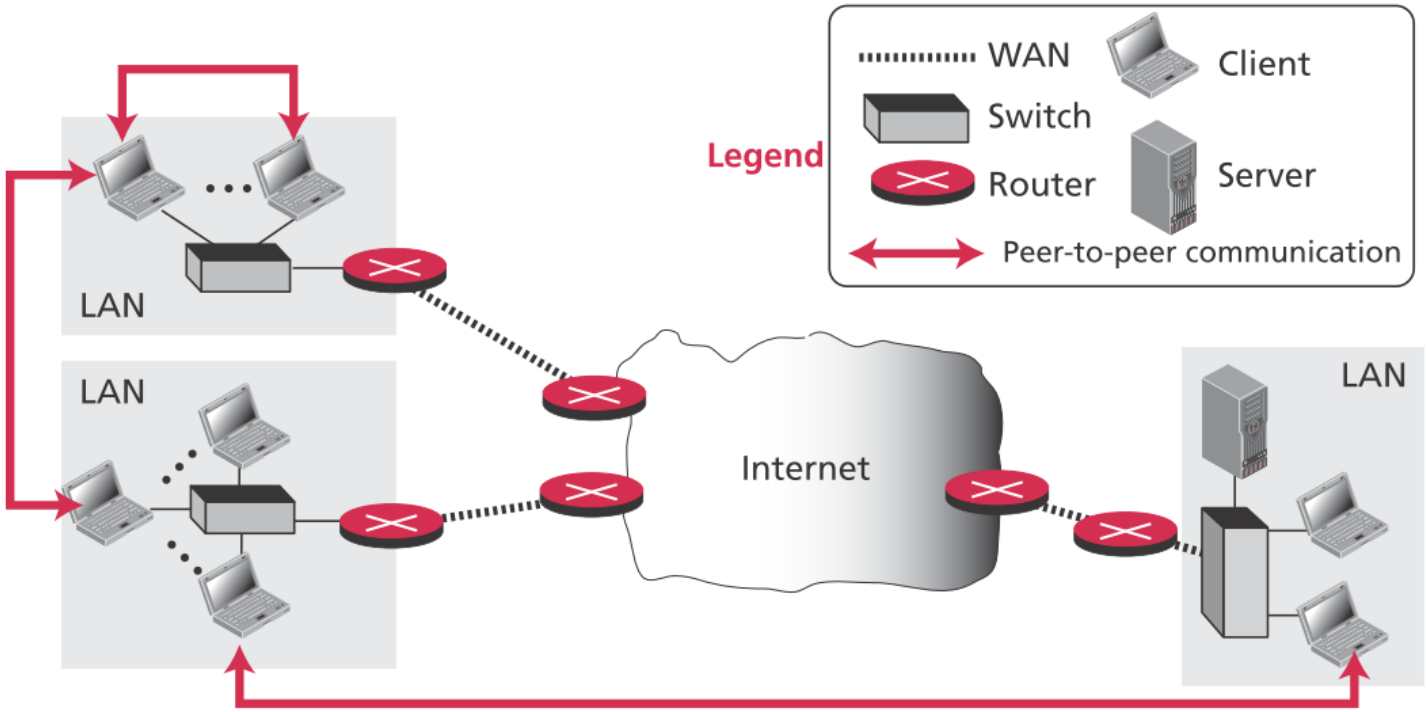


Traditional paradigm: client–server

- One problem with this paradigm is that the server should be a powerful computer to accept requests from a large number of clients
  - Several traditional services are still using this paradigm, including the World Wide Web (WWW), HyperText Transfer Protocol (HTTP), file transfer protocol (FTP), secure shell (SSH) and email

New paradigm: peer-to-peer

- In this paradigm, there is no need for a server process to be running all the time and waiting for the client processes to connect. The responsibility is shared between peers



New paradigm: peer-to-peer

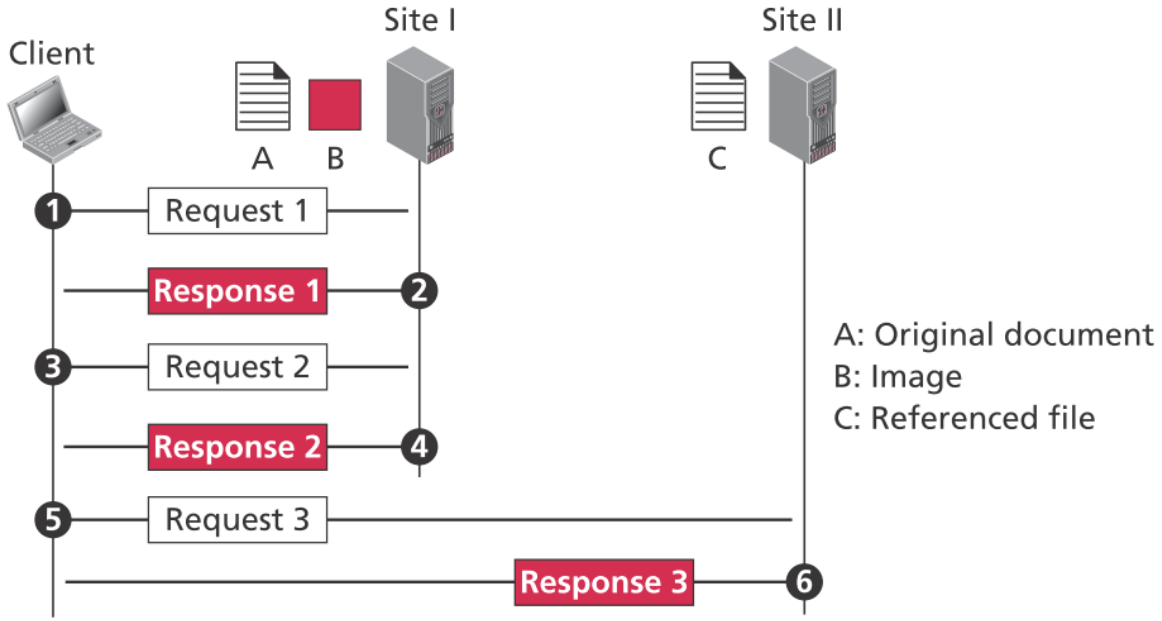
- One of the areas that really fit in this paradigm is Internet telephony
  - Communication by phone is indeed a peer-to-peer activity; no party needs to be running forever waiting for the other party to call
- Although it has been proven to be easily scalable and cost-effective in eliminating the need for expensive, there are also some challenges
  - The main challenge has been security; it is more difficult to create a secure communication between distributed services than between those controlled by some dedicated servers
  - The other is applicability; it appears that not all applications can use this new paradigm

World Wide Web (WWW)

- The Web is a repository of information in which documents (Web pages), are distributed all over the world and related documents are linked together
  - Distribution allows the growth of the Web. Each web server can add a new web page to the repository and announce it to all Internet users without overloading a few servers
  - Linking allows one web page to refer to another web page stored on another server. The linking of web pages was achieved using a concept called *hypertext*
    - The Web implemented this idea electronically: to allow the linked document to be retrieved when the link was clicked by the user
  - The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called *sites*. Each site holds one or more documents, referred to as *web pages*

Example

- Assume we need to retrieve a scientific document that contains one reference to another text file and one reference to a large image
  - Note that file A, file B, and file C are independent web pages, each with independent names and addresses



World Wide Web (WWW)

- The *browsers* that interpret and display a web page consist of three parts: a controller, client protocols, and interpreters
  - The controller receives input from the keyboard or the mouse and uses the client protocols to access the document and use the interpreter to display it
  - The client protocol can be one of the protocols described later, such as HTTP or FTP
  - The interpreter can be *HyperText Markup Language (HTML)*, Java, or JavaScript, depending on the type of document
- The web page is stored on the *web server*. Each time a request arrives, the corresponding document is sent to the client

Uniform resource locator (URL)

- To define a web page, we need three identifiers: *host, port* and *path* as well as which protocol we want to use
  - Protocol: The first identifier is the abbreviation for the client-server program that we need in order to access the web page
  - Host identifier: The host identifier can be the IP address of the server or the unique name given to the server
  - Port number: The port, a 16-bit integer, is normally predefined
  - Path: The path identifies the location and the name of the file in the operating system
- The *uniform resource locator (URL)* has been designed; it uses three different separators between the four pieces as shown below:

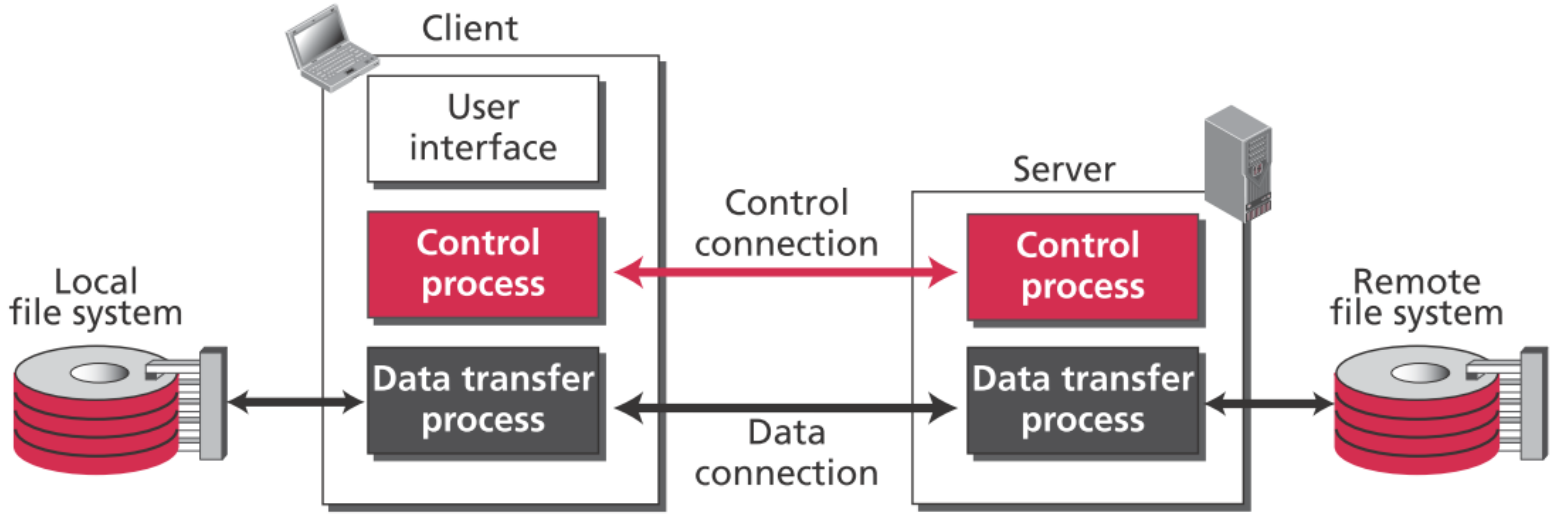
protocol://host/path	Used most of the time
protocol://host:port/path	Used when port number is needed

HyperText Transfer Protocol (HTTP)

- *HyperText Transfer Protocol (HTTP)* is a protocol that is used to define how the client–server programs can be written to retrieve web pages from the Web
  - An HTTP client sends a request; an HTTP server returns a response. The server uses the port number 80; the client uses a temporary port number

File Transfer Protocol (FTP)

- *File Transfer Protocol (FTP)* is the standard protocol provided by TCP/IP for copying a file from one host to another
  - Two systems may use different file name conventions, have different ways to represent data and have different directory structures
  - When a user starts an FTP session, the control connection opens. The data connection can be opened and closed multiple times if several files are transferred

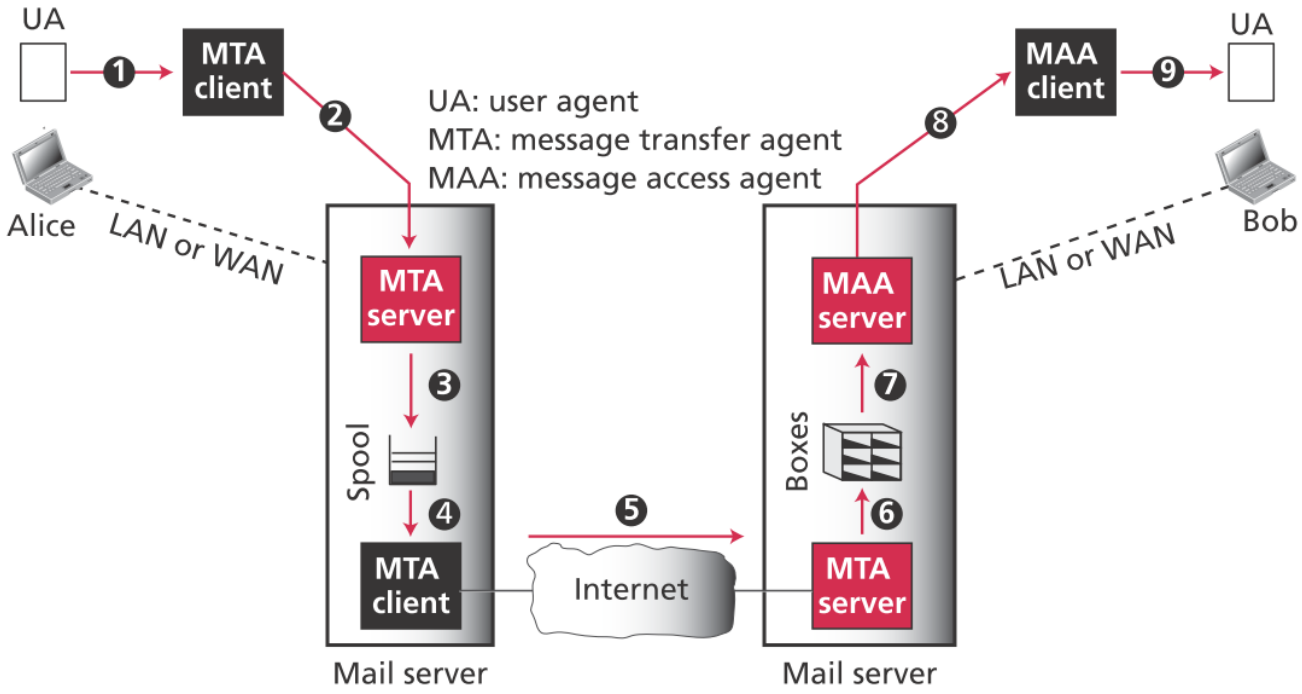


Electronic mail (email)

- Email is slightly different from the HTTP or FTP
  - It is considered a one-way transaction
  - This means that the idea of client/server programming should be implemented in another way: using some intermediate computers (servers)
    - The users run only client programs when they want and the intermediate servers apply the client/server paradigm

Electronic mail (email)

- Alice and Bob use three different agents: a *user agent (UA)*, a *Mail Transfer Agent (MTA)*, and a *Message Access Agent (MAA)*
  - Alice runs a UA program to prepare the message and send it to her mail server
  - The mail needs to be sent through the Internet from Alice's site to Bob's site using an MTA
  - Bob later uses an MAA client to retrieve the message from an MAA server running on the second server
    - Note that MTA client-server program is a *push* program. Bob needs a *pull program*. The client needs to pull the message from the server



TELNET

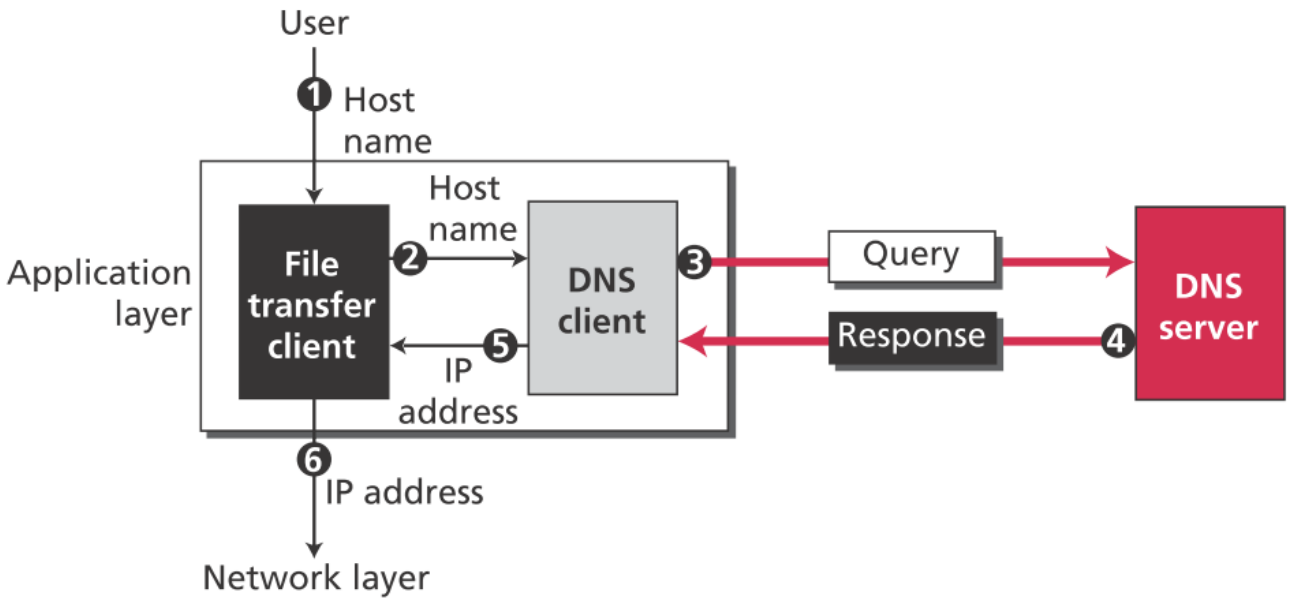
- It is impossible to have a client/server pair for each type of service we need; the number of servers soon becomes intractable
  - A solution is to have a *remote login* application that allows a user on the client site to log into the computer at the server site and use the services available there
    - For example, if a student needs to use the C compiler program at her university lab, there is no need for a C compiler client and a C compiler server. The student can use a client logging program to log into the university server and use the compiler program at the university
  - TErminaL NETwork (TELNET) is one of the original remote logging protocols
    - It has security issues because it sends all data including the password in plaintext (not encrypted)

Secure Shell (SSH)

- *Secure Shell (SSH)* is a secure application program that can be used for several purposes such as remote logging and file transfer
  - It was originally designed to replace TELNET

Domain Name System (DNS)

- TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet
  - However, people prefer to use names instead of numeric addresses. Therefore, a directory system that can map a name to an address has been proposed
  - For instance, if the user only the file transfer server name, the following procedure is conducted



Domain Name System (DNS) - Name space

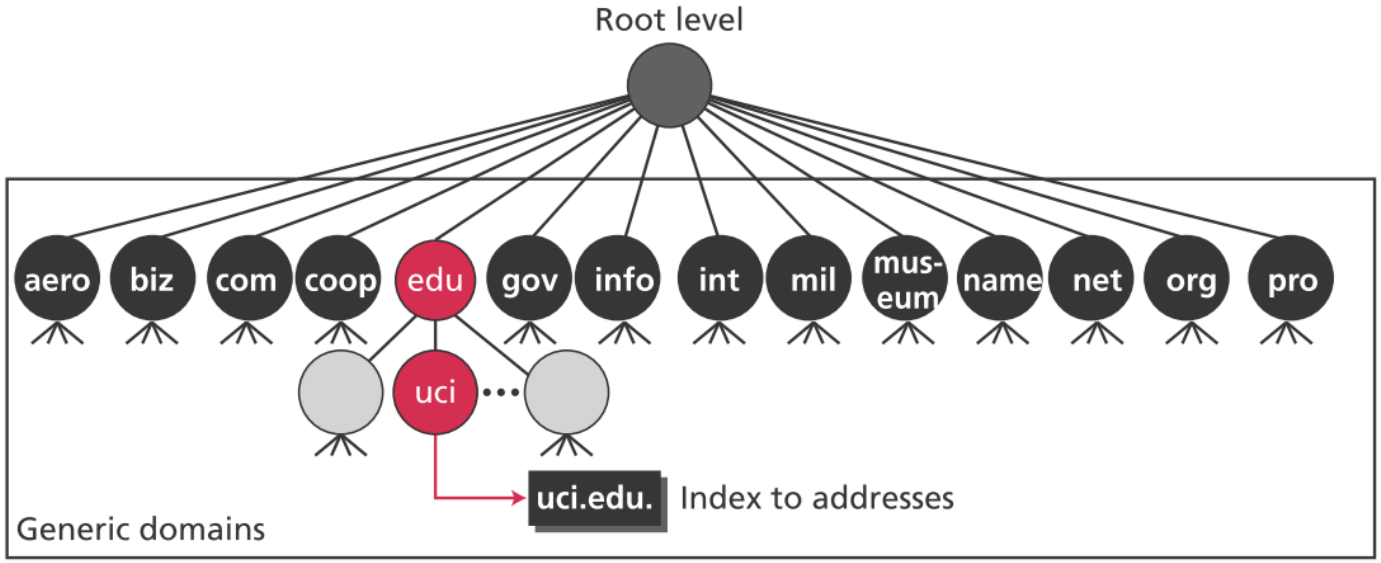
- A *name space* is used to map each address to a unique name and is normally organized hierarchically
  - In a hierarchical name space, each name is made of several parts
  - The first part can define the nature of the organization, the second part can define the name of an organization, the third part can define departments in the organization and so on

https://www.math.nsysu.edu.tw

http://www.math.ntu.edu.tw

DNS in the Internet

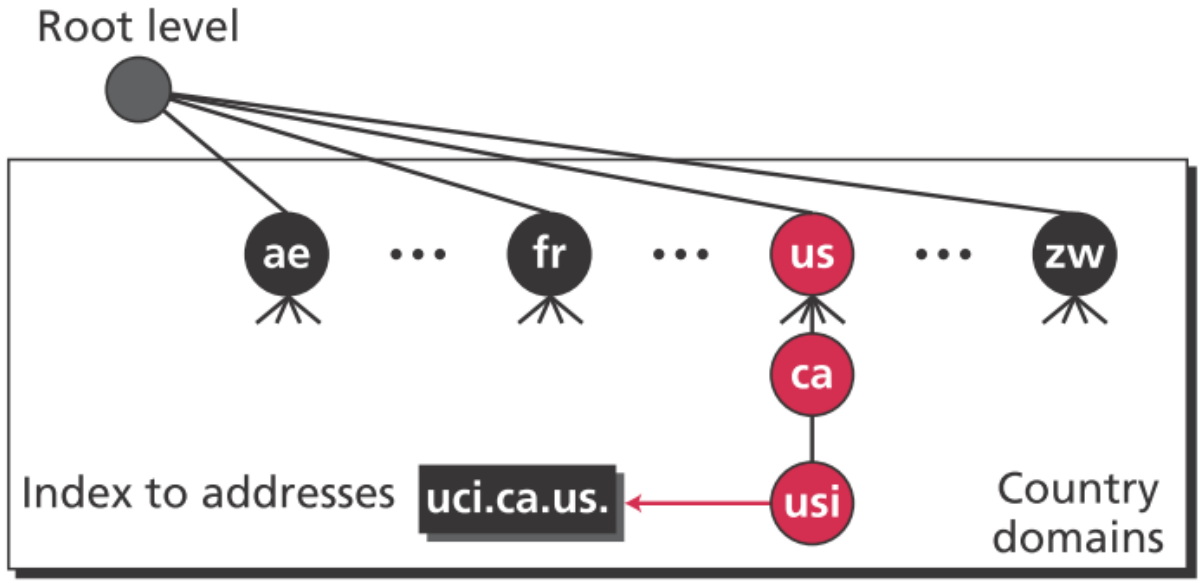
- The **domain name space** (tree) was originally divided into three different sections: generic domains, country domains, and the inverse domain
- The generic domains define registered hosts according to their generic behavior
  - Each node in the tree defines a domain, which is an index to the domain name space database



Label	*Description*	*Label*	*Description*
aero	Airlines and aerospace	int	International organizations
biz	Businesses or firms	mil	Military groups
com	Commercial organizations	museum	Museums
coop	Cooperative organizations	name	Personal names (individuals)
edu	Educational institutions	net	Network support centers
gov	Government institutions	org	Nonprofit organizations
info	Information service providers	pro	Professional organizations

DNS in the Internet

- The *country domains* section uses two-character country abbreviations (e.g., us for United States)
  - Second labels can be organizational, or they can be more specific, national designations
  - The United States, for example, uses state abbreviations as a subdivision of us (e.g., ca.us.)



Peer-to-peer (P2P) paradigm

- Peer-to-peer gained popularity with Napster (1999–2001), an online music file sharing service created by Shawn Fanning
- Gnutella had its first release in March 2000. It was followed by FastTrack (used by the Kazaa), Bit Torrent, WinMX, and GNUnet in March, April, May, and November of 2001 respectively
- When a peer in the network has a file (for example, an audio or video file) to share, it makes it available to the rest of the peers
  - An interested peer can connect itself to the computer where the file is stored and download it. As more peers join and download that file, more copies of the file become available to the group

Centralized networks

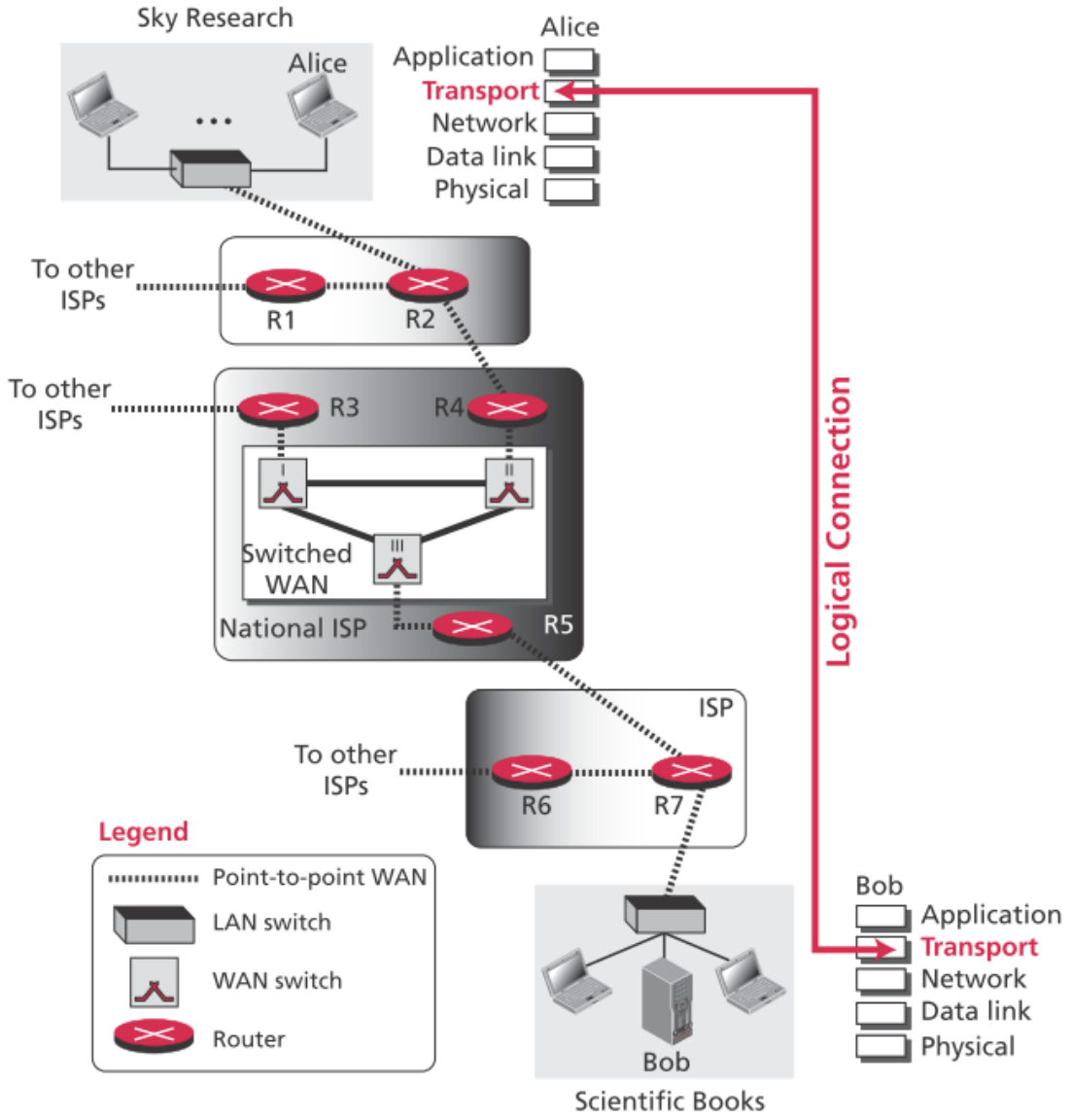
- In a *centralized P2P network (hybrid P2P network)*
  - The directory system listing of the peers and what they offer use a client-server paradigm
  - The storing and downloading of the files are done using the peer-to-peer paradigm
  - A peer first registers itself with a central server
    1. The peer then provides its IP address and a list of files it has to share
    2. A peer, looking for a particular file, sends a query to a central server
    3. The server searches its directory and responds with the IP addresses of nodes that have a copy of the file
    4. The peer contacts one of the nodes and downloads the file
- Centralized networks make the maintenance of the directory simple but have several drawbacks
  - Accessing the directory can generate huge traffic and slow down the system
  - The central servers are vulnerable to attack and whole system goes down if all servers fail

Decentralized network

- In a *decentralized P2P network*
  - Peers arrange themselves into an *overlay network*, which is a logical network made on top of the physical network
  - Depending on how the nodes in the overlay network are linked, a decentralized P2P network is classified as either unstructured or structured
  - In an *unstructured network*, the nodes are linked randomly. A search in an unstructured P2P is not very efficient because a query to find a file must be flooded through the network
    - Two examples of this type of network are Gnutella and Freenet
  - A *structured network* uses a predefined set of rules to link nodes so that a query can be effectively and efficiently resolved. The most common technique used for this purpose is the *Distributed Hash Table (DHT)*
    - One popular P2P file sharing protocol that uses the DHT is BitTorrent

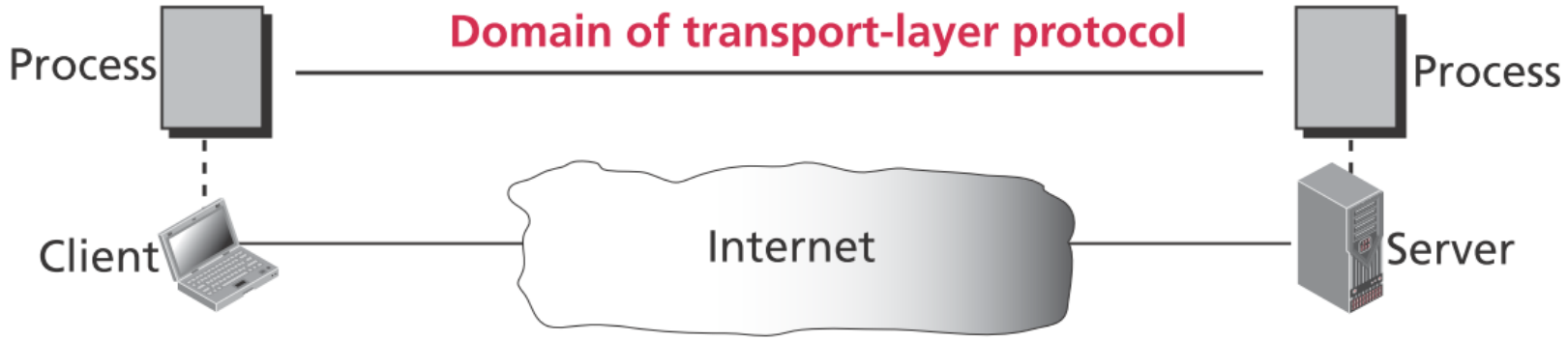
Transport layer

- It provides services to the application layer and receives services from the network layer
  - The transport layer is the heart of the TCP/IP protocol suite; it is the end-to-end logical vehicle for transferring data from one point to another on the Internet
  - Only the two end systems (Alice's and Bob's computers) use the service of the transport layer; all intermediate routers use only the first three layers



Transport-layer services

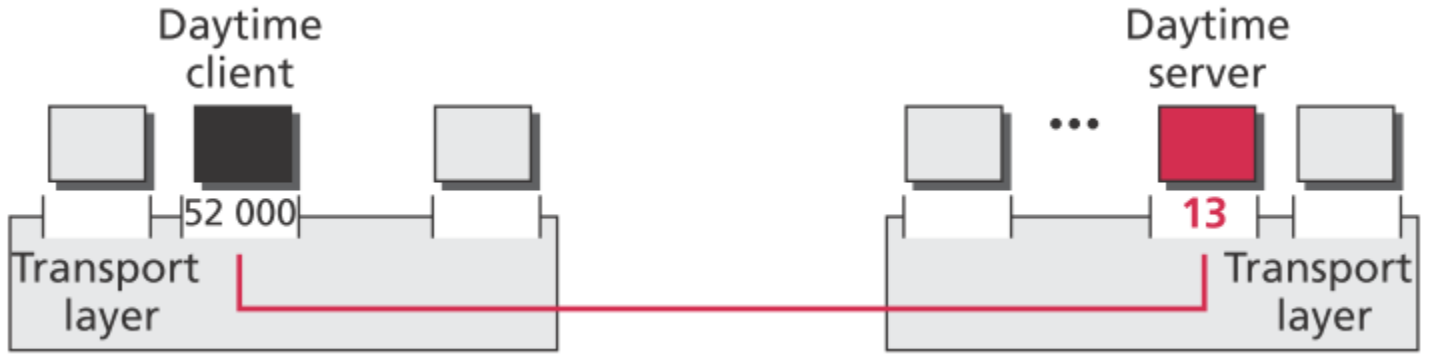
- The first duty of a transport-layer protocol is to provide *process-to-process communication*
  - A process is an application-layer entity (running program) that uses the services of the transport layer
  - The network layer (discussed later) is responsible for communication at the computer level (host-to-host communication)



Transport-layer services: port numbers

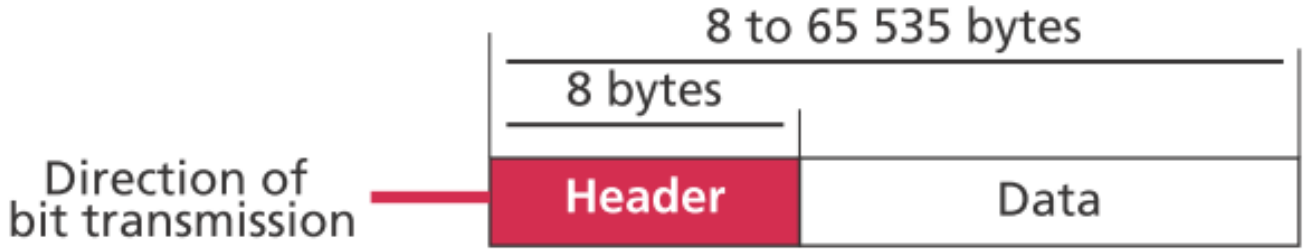
- The most common way to achieve process-to-process communication is through the client-server paradigm
  - For communication, we must define the local host and the remote host using IP addresses. To define the processes, we need second identifiers, called *port numbers*. In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535 (16 bits)
    - The client program defines itself with a port number, called the *ephemeral port number* which is recommended to be greater than 1,023
    - The server process must also define itself with a port number. TCP/IP has decided to use universal port numbers for servers; these are called *well-known port numbers*

FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80



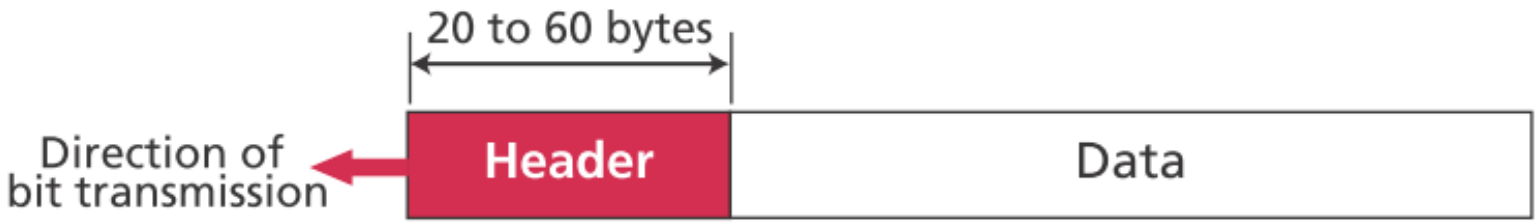
User Datagram Protocol (UDP)

- The *User Datagram Protocol (UDP)* is a connectionless, unreliable transport protocol
  - UDP is a very simple protocol using a minimum overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP
  - UDP packets, called *user datagrams*, have a fixed-size header of 8 bytes. However, the total length needs to be less because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes



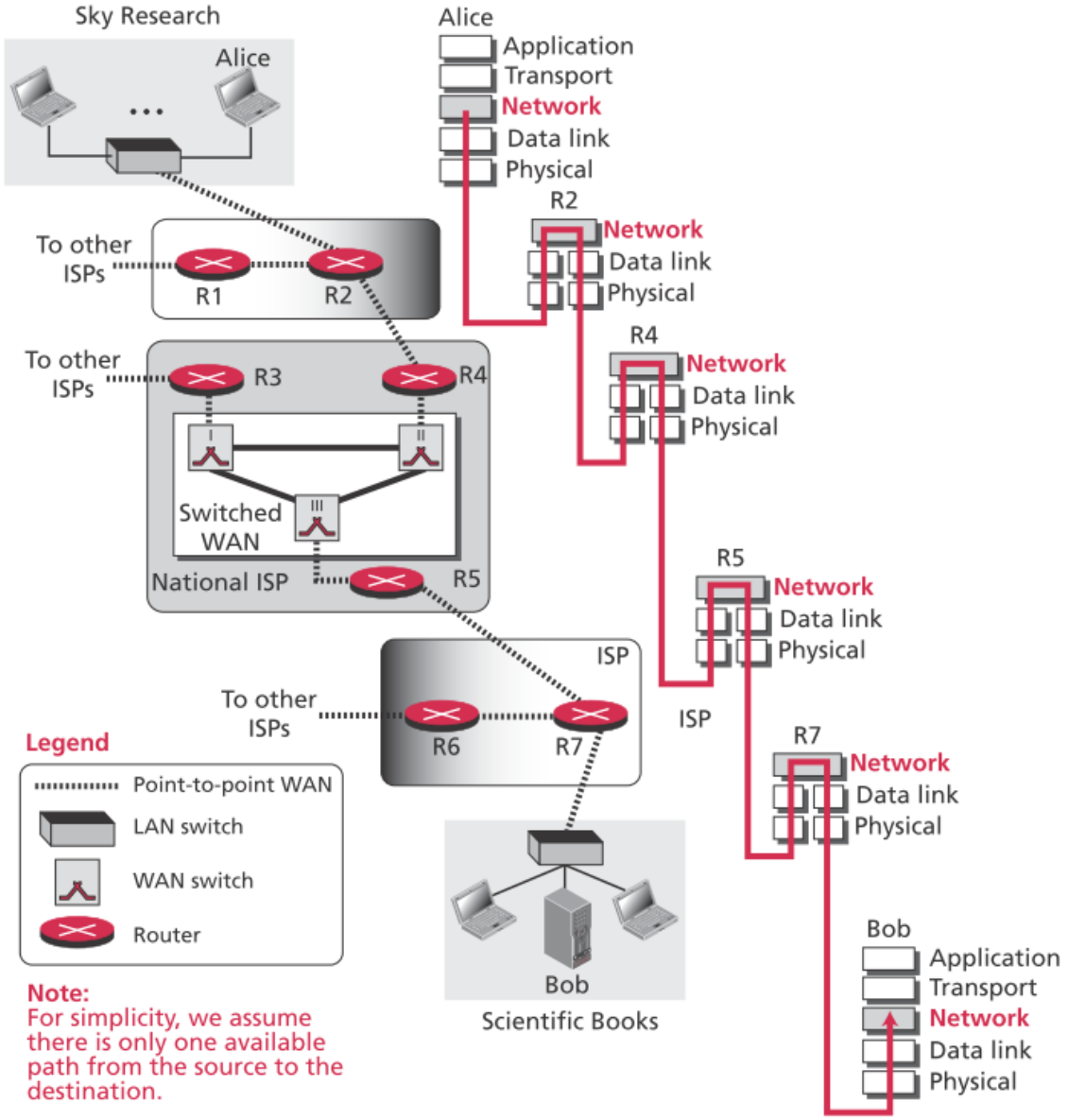
Transmission Control Protocol (TCP)

- *Transmission Control Protocol (TCP)* is a reliable protocol
  - TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service
  - It is a connection-oriented service since there is a connection (relationship) between all packets (segments) belonging to the same message (coming from the application layer)
  - TCP groups a number of bytes together into a packet called a *segment*. TCP adds a header to each segment (for control purposes) and delivers the segment to the network layer



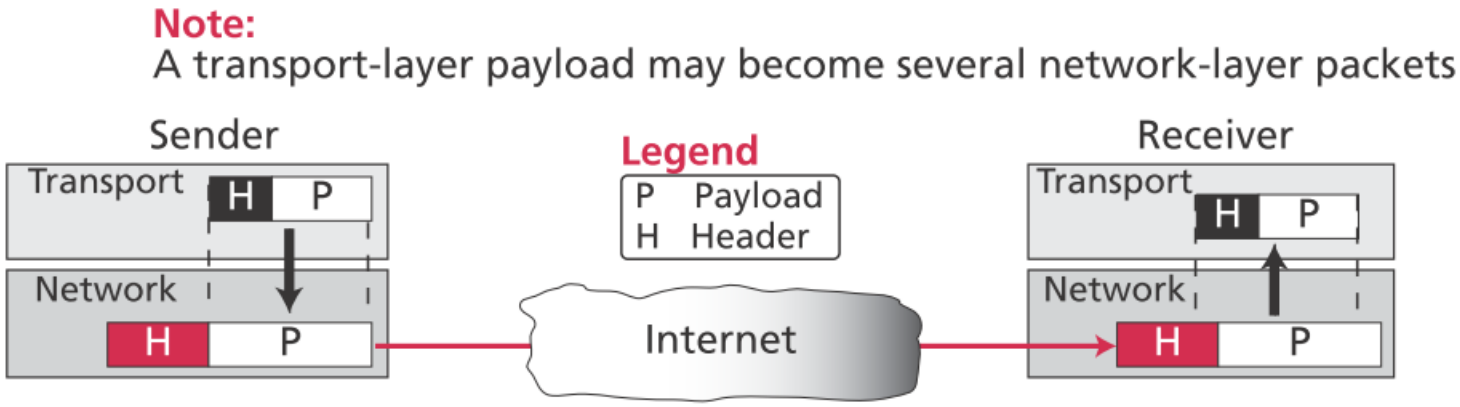
Network layer

- The *network layer* in the TCP/IP protocol suite is responsible for the host-to-host delivery of messages
  - The network layer is involved at the source host, destination host, and all routers in the path



Network layer services

- The first duty of the network layer is *packetizing*
  - Encapsulating the payload (data received from the upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination
    1. The source network-layer protocol receives a packet from upper layer, adds header that contains source/destination addresses and information that is required by the network-layer protocol
    2. Then it logically delivers the packet to the network-layer protocol at the destination
    3. The destination host receives the network-layer packet, decapsulates the payload and delivers it to the upper-layer protocol

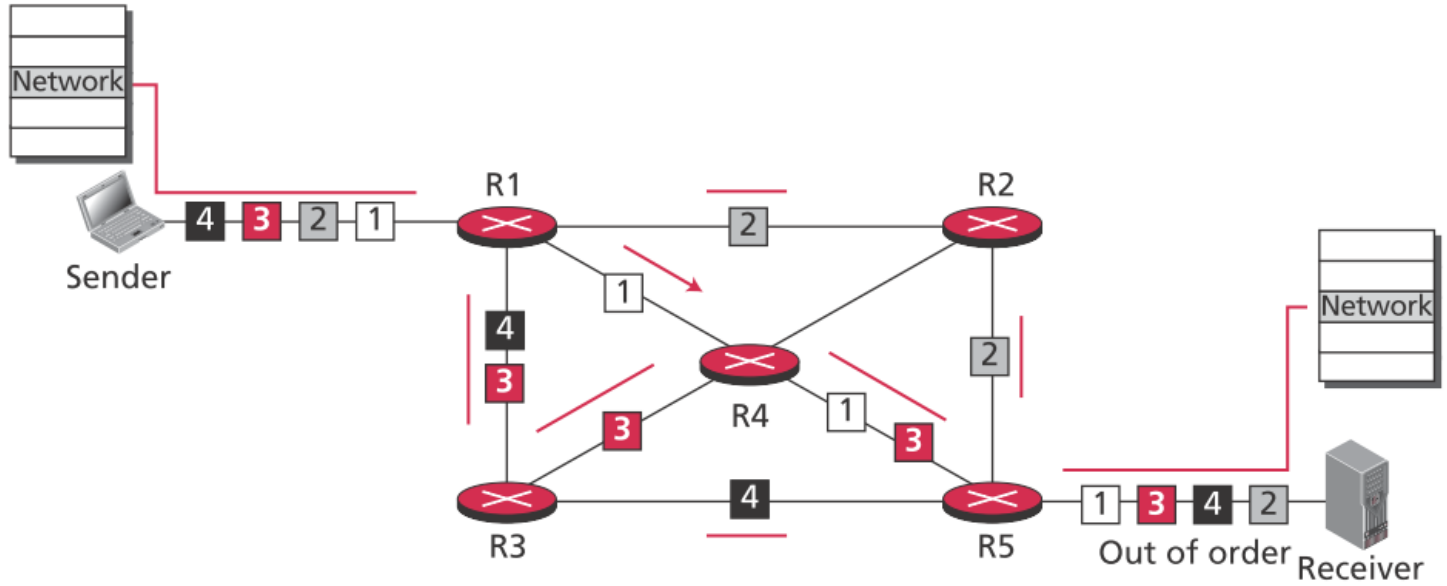


Network layer services

- The delivery of packets at the network layer is *unreliable*
  - This means that the packets can be corrupted, lost, duplicated
    - Since if we need a guarantee from the network layer, the delivery of packets will be delayed. Each packet needs to be checked at each router and destination and resent if corrupted
  - If we really want to guarantee that the messages are not corrupted, we need to use the TCP protocol at the transport layer
    - If a payload at the transport layer is corrupted, TCP drops the packet and requests the resending of the data

Network layer services

- The delivery at the network layer is also *connectionless*
  - It means that the network layer treats each packet independently
  - In other words, there is no relationship between packets belonging to the same transport-layer payload. If a transport-layer packet results in four network-layer packets, there is no guarantee that the packets arrive in the same order as sent because each packet may follow a different path to reach the destination

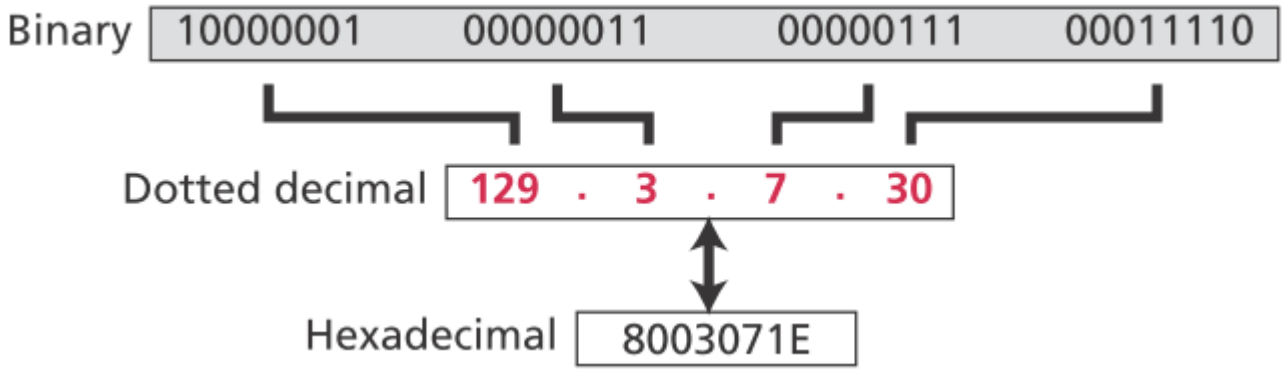


Network layer services

- The network layer is responsible for *routing* the packet from its source to the destination
  - There is more than one route from the source to the destination. The network layer is responsible for finding the best one among these possible routes
  - The network layer needs to have some specific strategies for defining the best route
    - This is done by running some routing protocols to help the routers coordinate their knowledge about the neighborhood and to come up with consistent tables to be used when a packet arrives

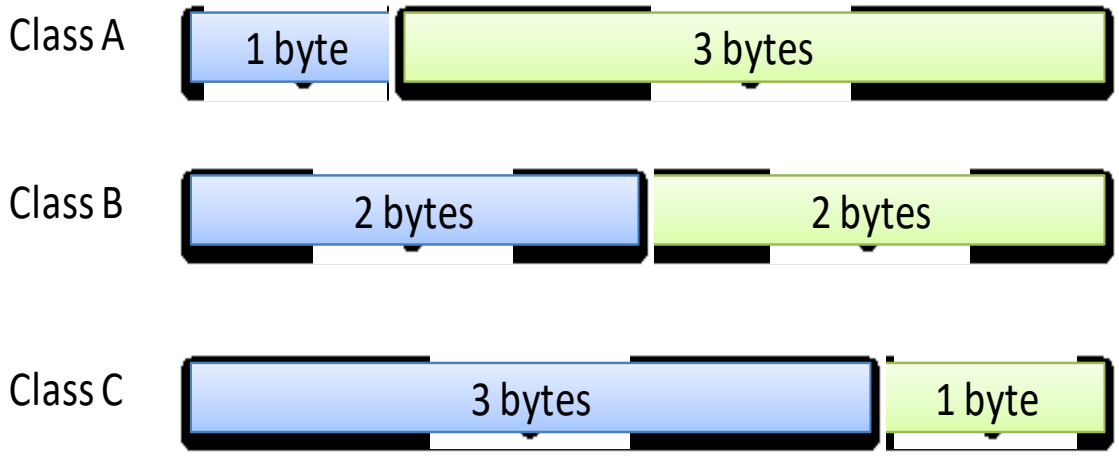
Network-layer protocols

- The main protocol is called the *Internet Protocol (IP)*
- The identifier used in the Internet Protocol Version 4 (IPv4) layer to identify the connection of each device to the Internet is called the Internet address (IP address)
  - An IPv4 address is a 32-bit address which is unique and universal
  - There are three common notations to show an IPv4 address
  - 192.168.0.0~192.168.255.255 are used as private IP address



Network-layer protocols

- A 32-bit IPv4 address is hierarchical and is divided into two parts
  - The first part of the address, called the prefix, defines the network (subnetwork)
  - The second part of the address, called the suffix, defines the node
  - With the mask, we can obtain the subnetwork



	Subnet mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

68.180.206.184/8 ⇨ 01000100101101001100111010111000

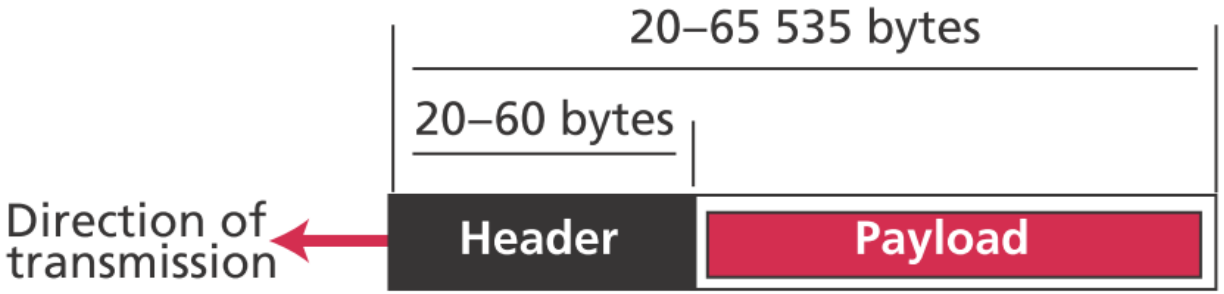
AND

255.0.0.0 ⇨ 11111111000000000000000000000000

68.0.0.0 ⇦ 01000100000000000000000000000000

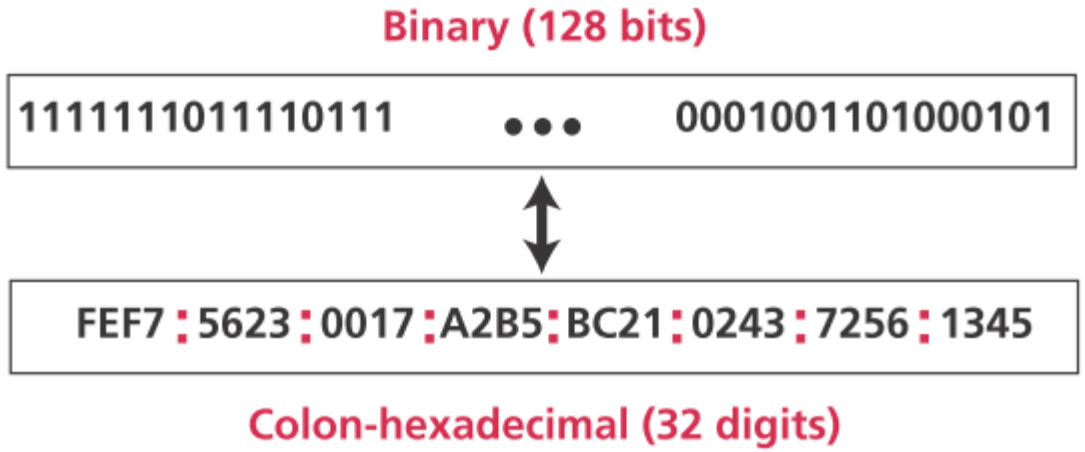
Network-layer protocols

- Packets used by the IP are called datagrams
  - A datagram is a variable-length packet consisting of two parts: header and payload (data).
  - The header is 20 to 60 bytes in length and contains information essential to routing and delivery
  - Some shortcomings of IPv4 such as address depletion prompted a new version of IP protocol in the early 1990s



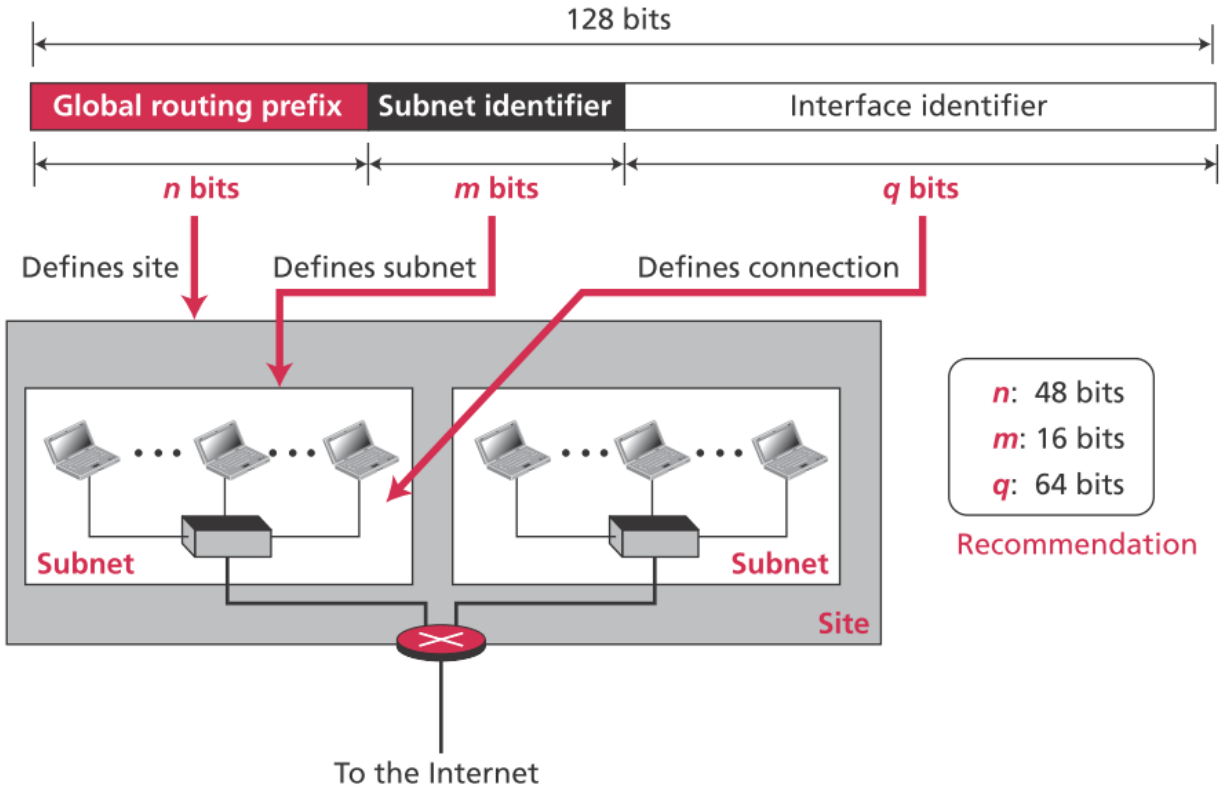
Network-layer protocols

- The new version is called *Internet Protocol version 6 (IPv6)* was a proposal to augment the address space of IPv4 and at the same time redesign the format of the IP packet and revise some auxiliary protocols
  - To prevent address depletion, IPv6 uses 128 bits to define any device connected to the Internet



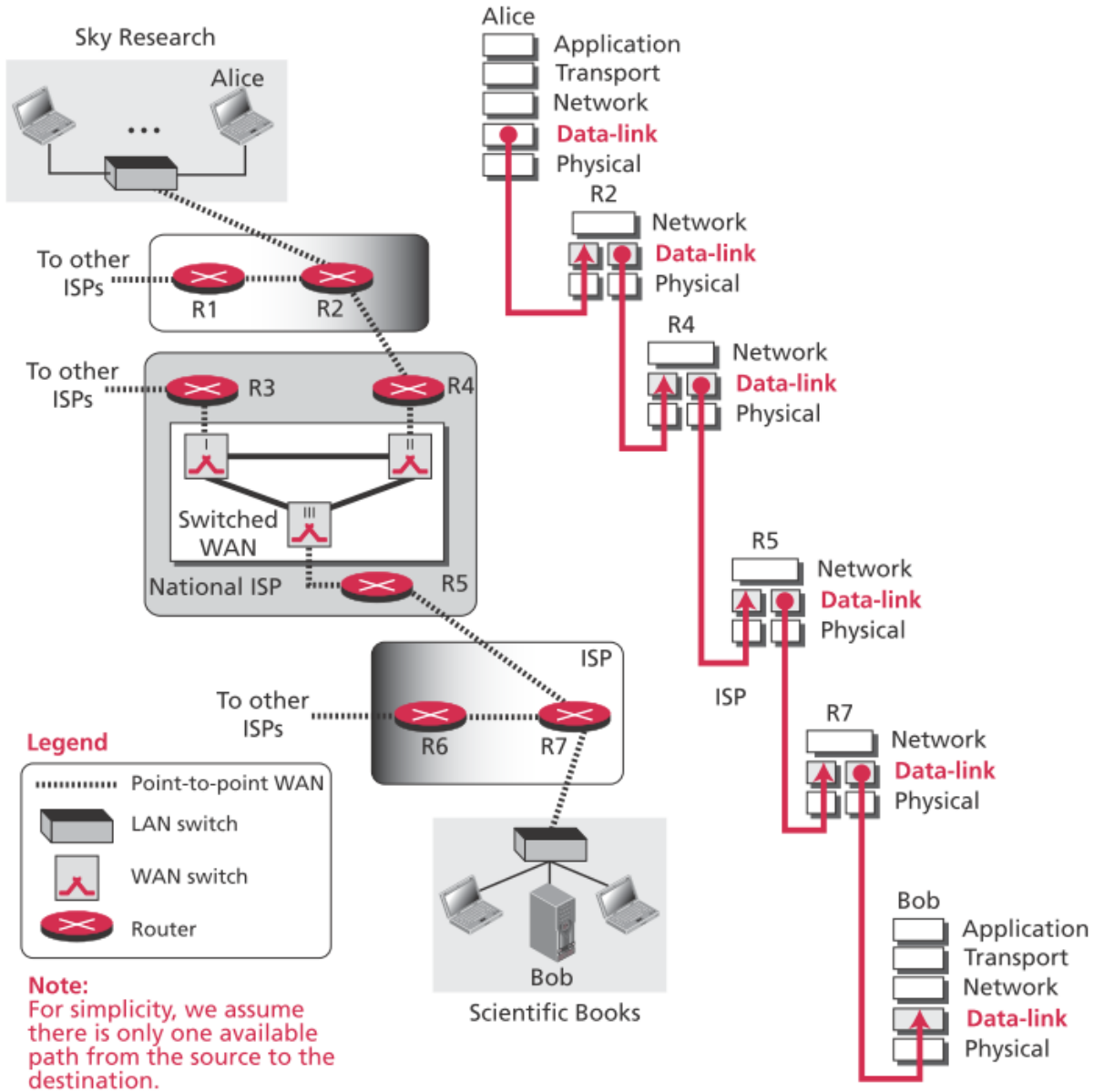
Network-layer protocols

- The address in IPv6 actually defines three levels of hierarchy: site (organization), subnetwork, and connection to the host
  - A datagram in this version is also a variable-length packet consisting of two parts: header and payload (data)



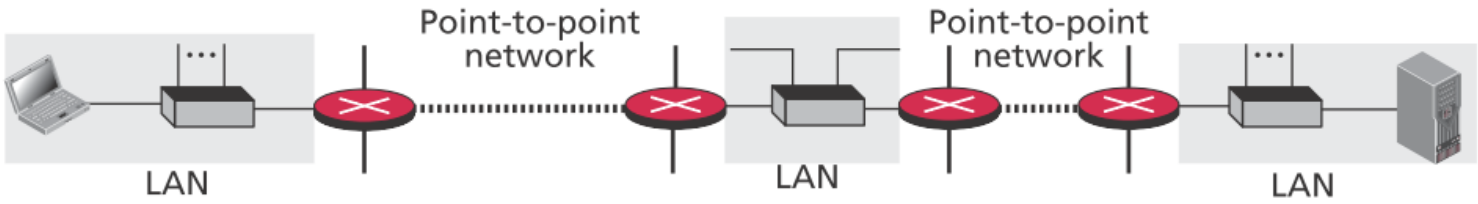
Data-link layer

- The TCP/IP suite does not define any protocol in the *data-link layer*
  - These networks, wired or wireless, receive services and provide services to the network layer
  - Communication at the data-link layer, however, is made up of five separate logical connections between the data-link layers in the path



Nodes and links

- While the communication at the application, transport, and network layers is end-to-end, communication at the data-link layer is *node-to-node*
  - It is customary to refer to the two end hosts and the routers as *nodes* and the networks in between as *links*
  - The link that connects the nodes are either LANs or WANs

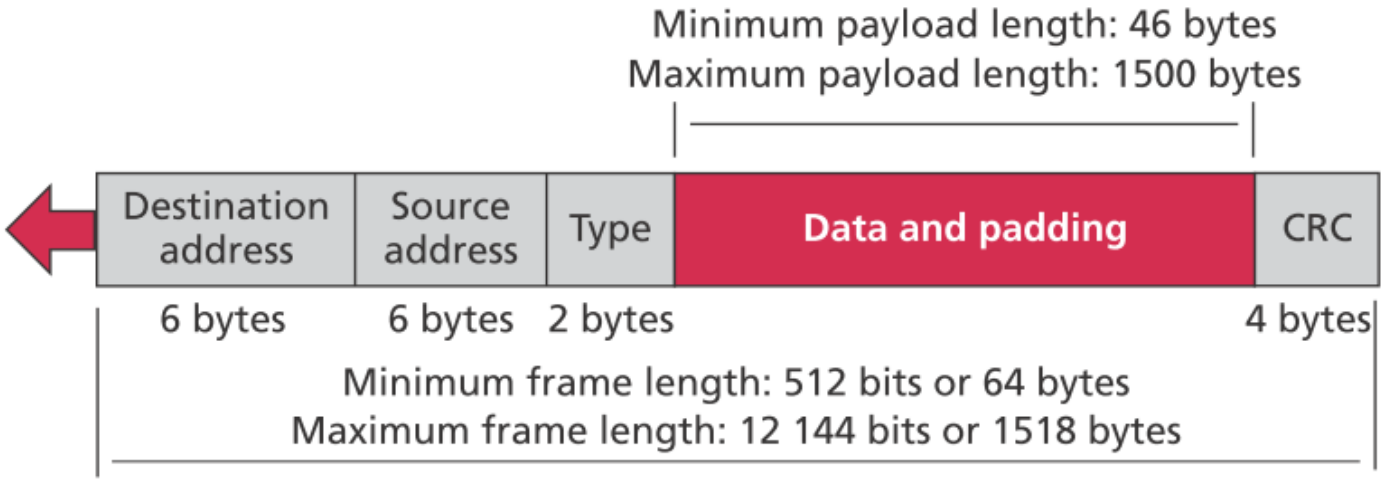


a. A small part of the Internet

b. Nodes and links

Local area networks (LANs) - Wired LANS

- Wired LANS: Ethernet
  - The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs
  - It has gone through four generations and the first was standard Ethernet (10 Mbps)
    - A group of bits are packaged together and referred to as a *frame*
    - A frame also carries some information such as the source/destination address (48 bits) which is known as *Media Access Control (MAC) Address*, the type of data, the actual data, and some other control bits as a guard to help check the integrity of data

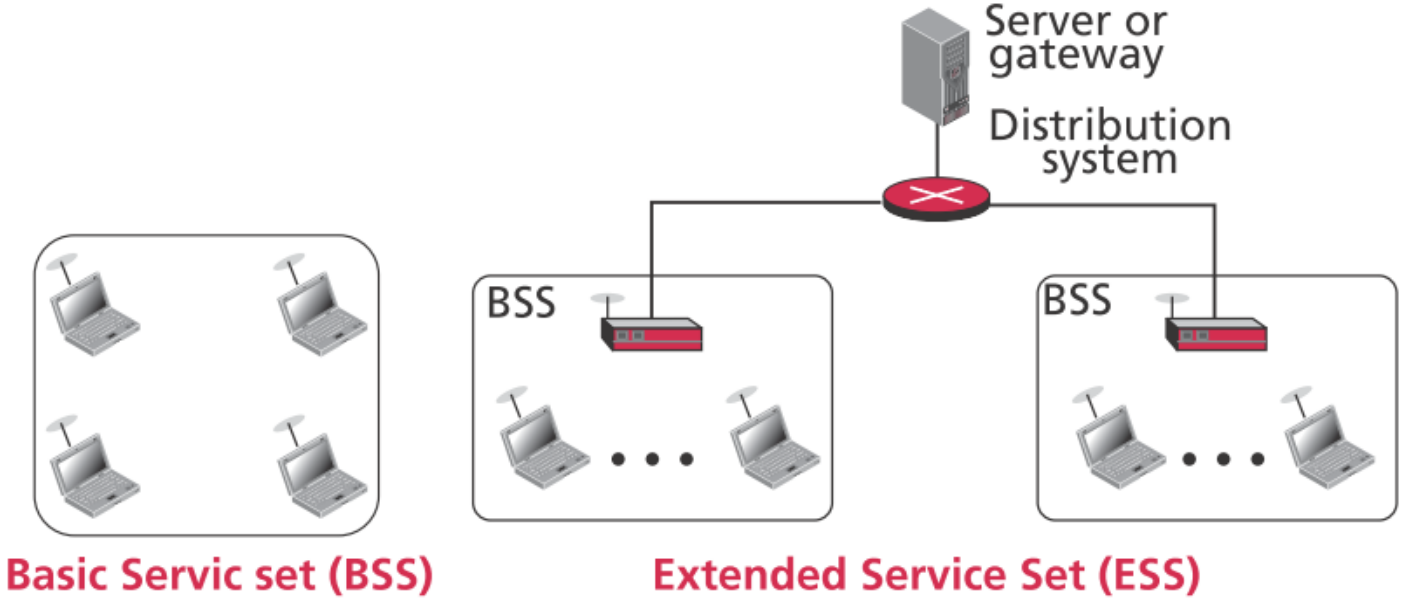


Local area networks (LANs) - Wired LANS

- Fast Ethernet (100 Mbps)
  - Most of the protocols such as addressing, frame format remained unchanged. However, features of the Standard Ethernet that depend on the *transmission rate* had to be revised
- Gigabit Ethernet (1000 Mbps)
  - The goals of the *Gigabit Ethernet* were to upgrade the data rate to 1 Gbps but keep the address length, the frame format, and the maximum and minimum frame length the same
- 10-Gigabit Ethernet
  - The idea is to extend the technology, the data rate, and the coverage distance so that the Ethernet can be used as LAN and MAN (*metropolitan area network*). This data rate is possible only with fiber-optic technology at this time

Local area networks (LANs) - Wireless LANs

- The first difference we can see between a wired and a wireless LAN is the medium
  - In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium
- Wireless Ethernet (WiFi)
  - The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS). The second service uses an extra device (access point or AP) that serves as a switch for connection to other LANs or WANs

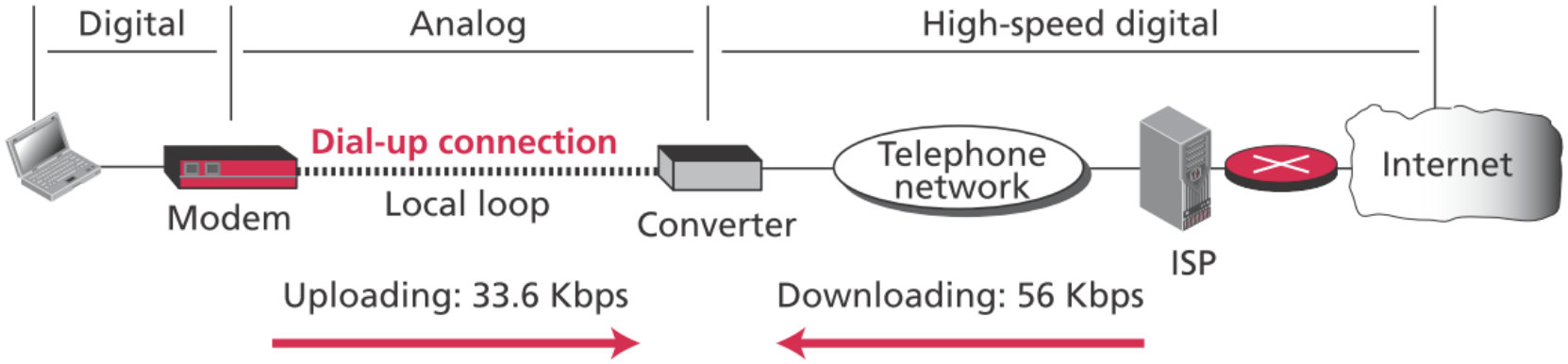


Local area networks (LANs) - Wireless LANs

- *Bluetooth* is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other
  - A Bluetooth LAN is an *ad hoc* network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet
  - Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology
  - Monitoring devices can communicate with sensor devices in a small healthcare center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference

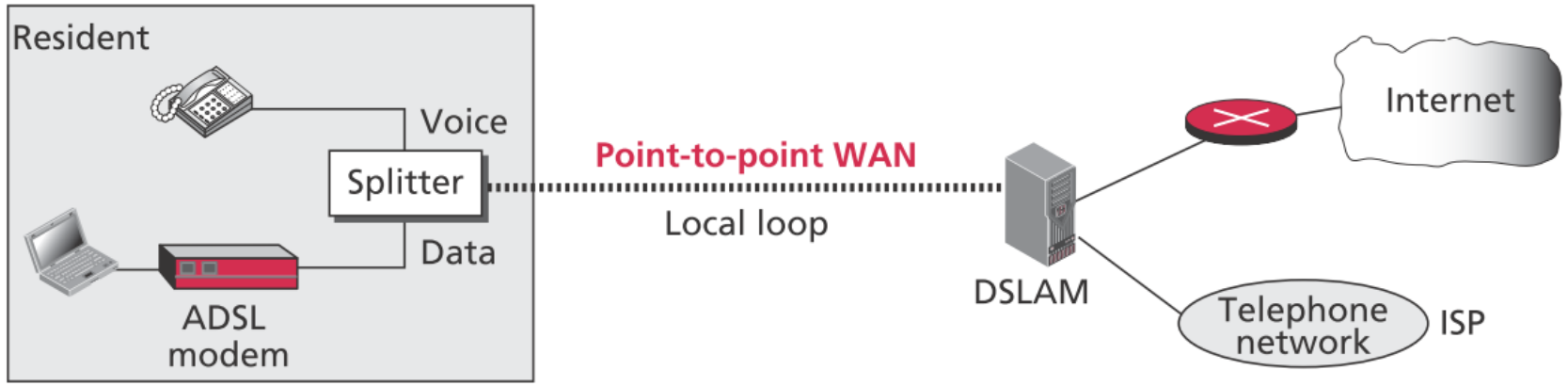
Wide area networks (WANs) - Wired WANs

- Point-to-point wireless WANs
  - Today we can use several point-to-point wireless networks to provide what is called last-mile service to connect residents and businesses to the Internet
- Dial-up service
  - A network or connection uses the services provided by telephone networks to transmit data
  - The term *modem* is a composite word that refers to the two functional entities that make up the device: a signal modulator and a signal demodulator. A *modulator* creates signal from data. A *demodulator* recovers the data from the modulated signal



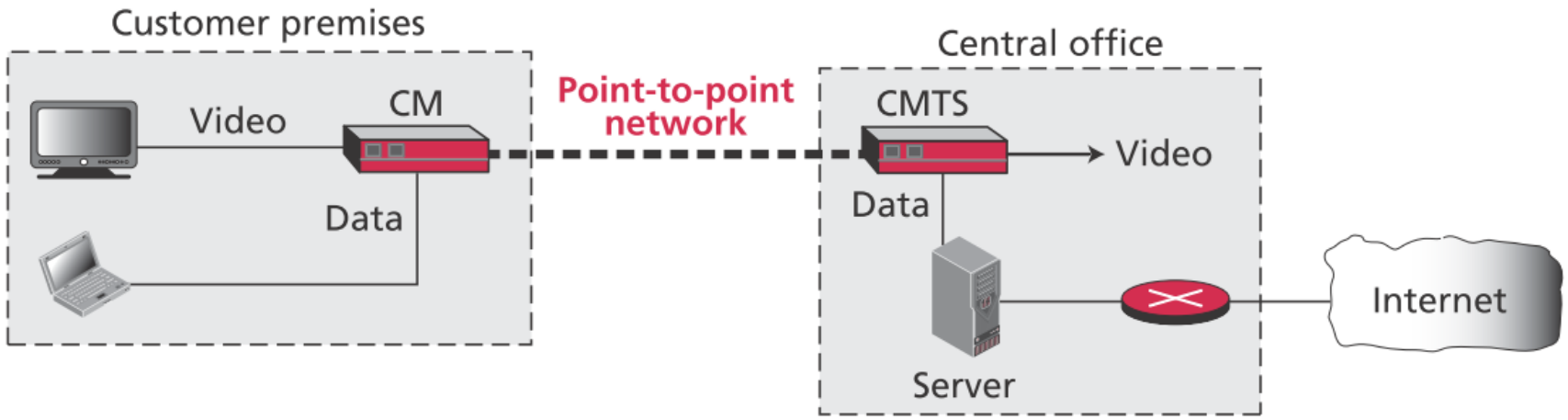
Wide area networks (WANs) - Wired WANs

- Digital subscriber line (DSL)
  - Telephone companies developed DSL to provide higher-speed access to the Internet
  - DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL)
  - *Asymmetric DSL (ADSL)* provides higher speed (bit rate) in the downstream direction (from the Internet to the resident) than in the upstream direction (from the resident to the Internet)
    - ADSL allows the subscriber to use the voice channel and the data channel at the same time



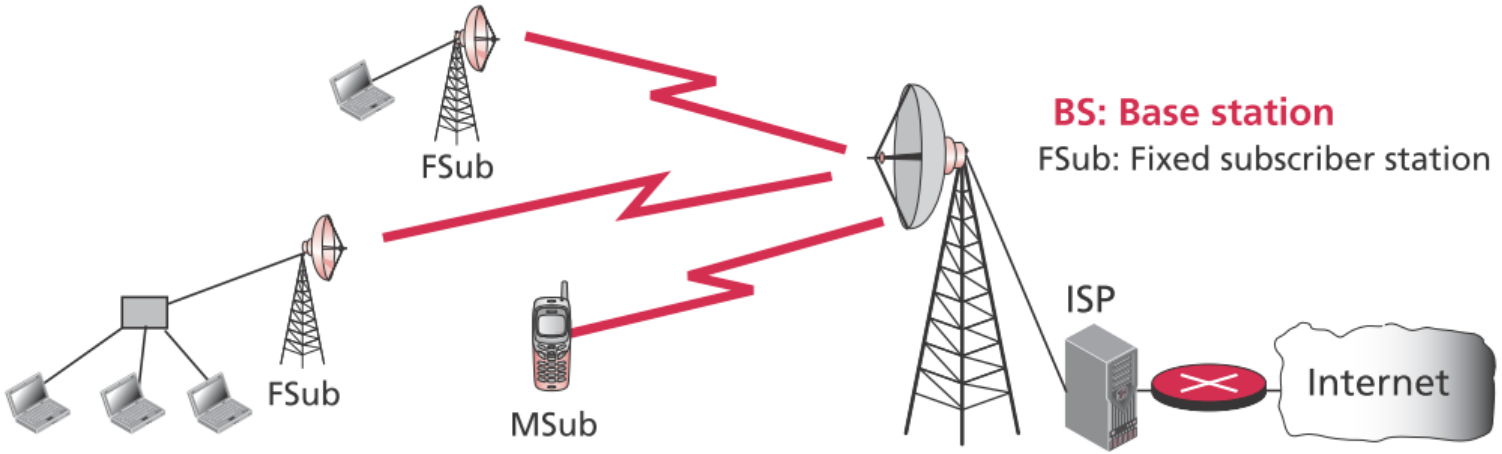
Wide area networks (WANs) - Wired WANs

- Cable network
  - Cable networks were originally created to provide access to TV programs
  - Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer



Wide area networks (WANs) - Wireless WANs

- Wireless WANs
  - The service area of the Internet is so large today that sometimes using only wired WANs cannot provide services to each corner of the world
- The *Worldwide Interoperability Access (WiMax)* is the wireless version of DSL/Cable connection to the Internet
  - It provides two types of services (fixed WiMax) to connect the main station to fixed station or to mobile stations such as cellular phones



Wide area networks (WANs) - Wireless WANs

- Cellular telephony network
  - Cellular network divides the earth into cells. The mobile stations communicate with the fixed antenna in the cell that they are inside at each moment. When the user moves to another cell, the communication is between the mobile device and the new antenna
- Satellite networks
  - A node in the network can be a satellite, an Earth station, an end-user terminal, or telephone
  - Satellite networks are like cellular networks in that they divide the planet into cells
  - It can make high-quality communication available to less well-developed parts of the world without requiring a huge investment in ground-based infrastructure

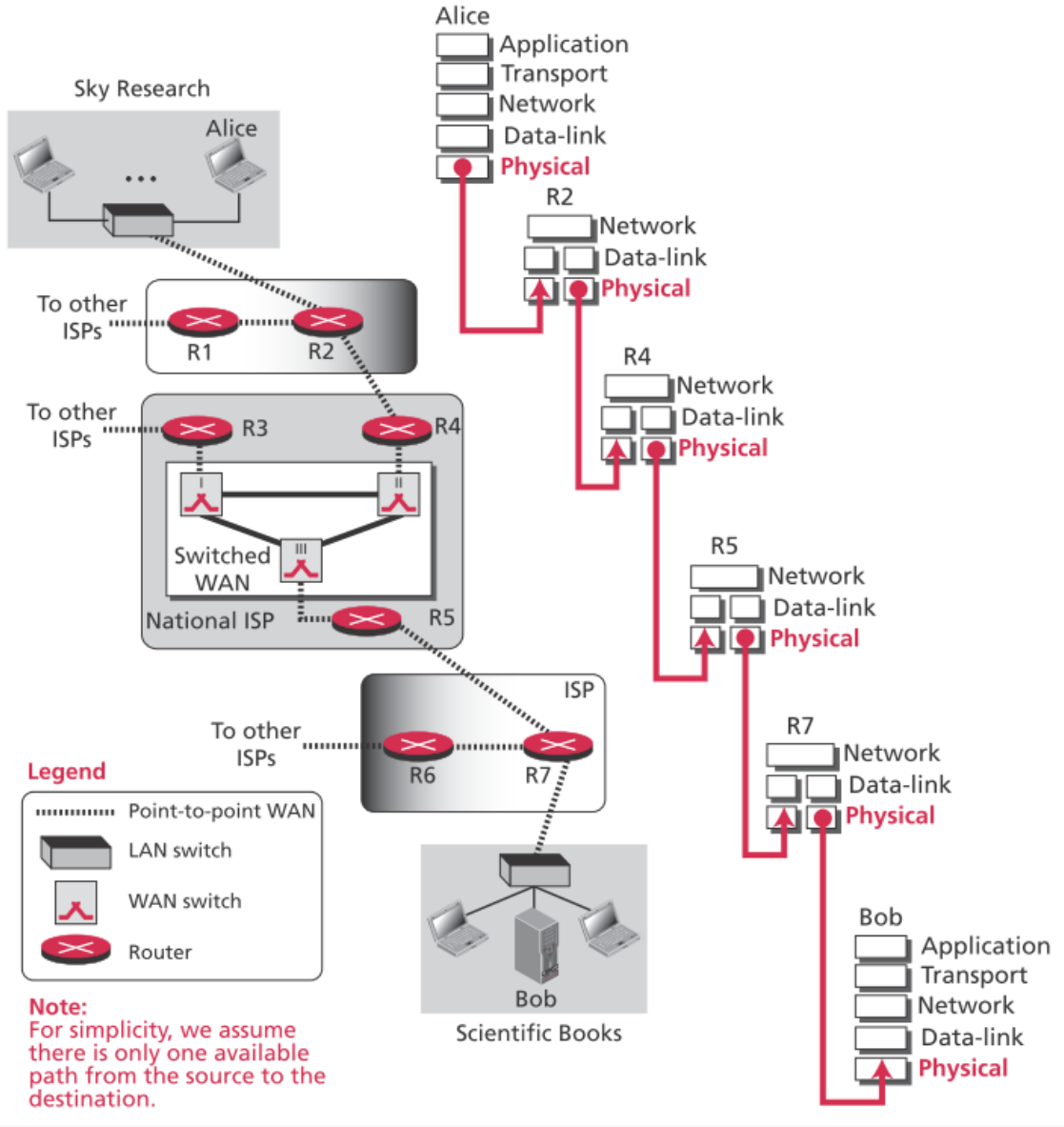
Appendix

Wide area networks (WANs)

- Switched wired WANs
  - We need switched wired WANs to connect the backbone of the Internet. Several protocols in the past have been designed for this purpose such as SONET or ATM

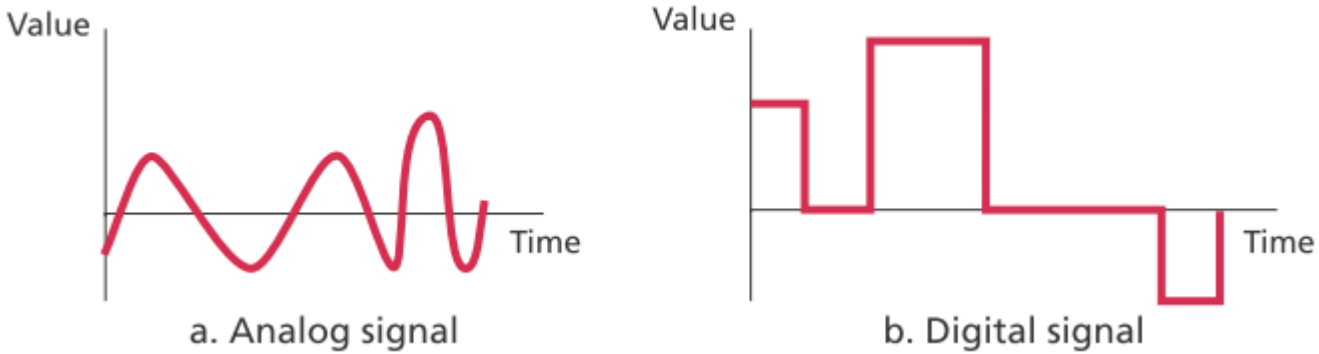
Physical layer

- The role of the *physical layer* is to transfer the bits received from the data-link layer and convert them to electromagnetic signals for transmission
  - At the physical layer, the communication is node-to-node, but the nodes exchange electromagnetic signals
  - The main duty is to efficiently convert these bits into electromagnetic signals



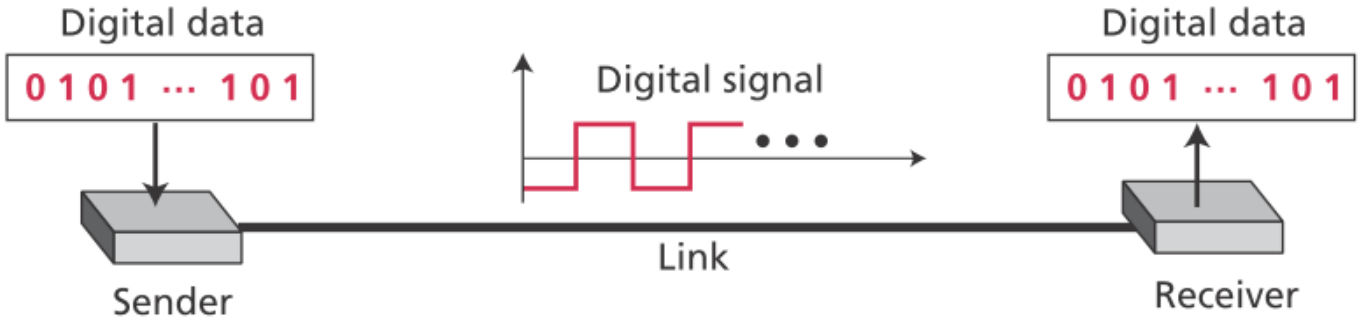
Analog and Digital

- Data can be analog or digital
  - Analog data take on continuous values while digital data take on discrete values
  - When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal
  - Digital data can be converted to a digital signal or modulated into an analog signal for transmission across a medium

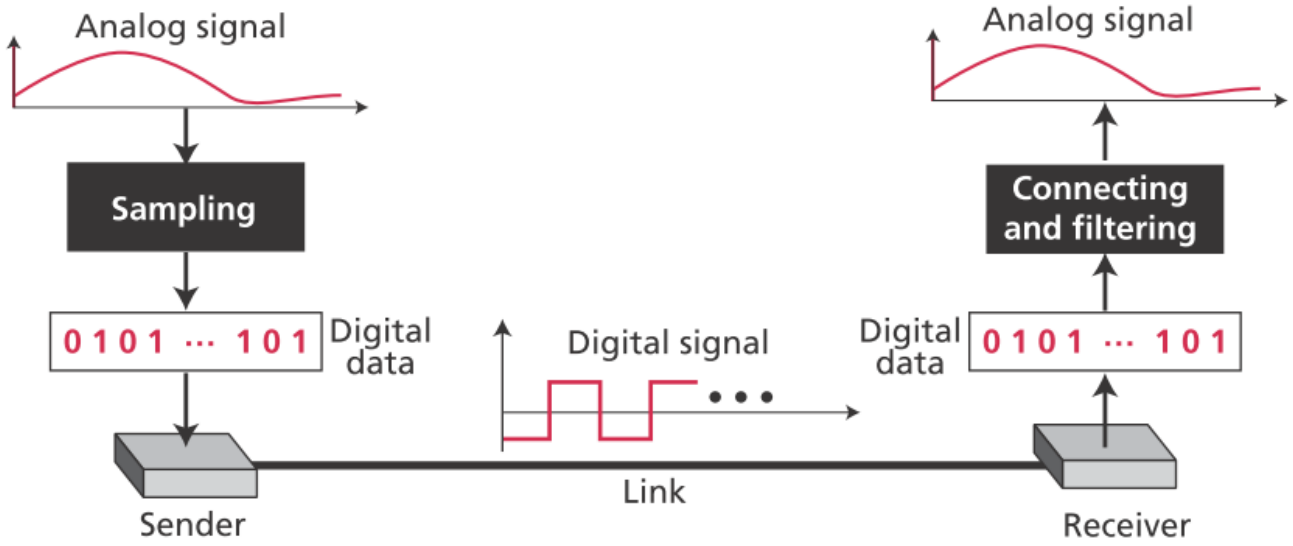


Digital transmission

- Digital-to-digital conversion
  - If our data is digital and we need to transmit digital signal, we can use digital-to-digital conversion to change the digital data to digital signal

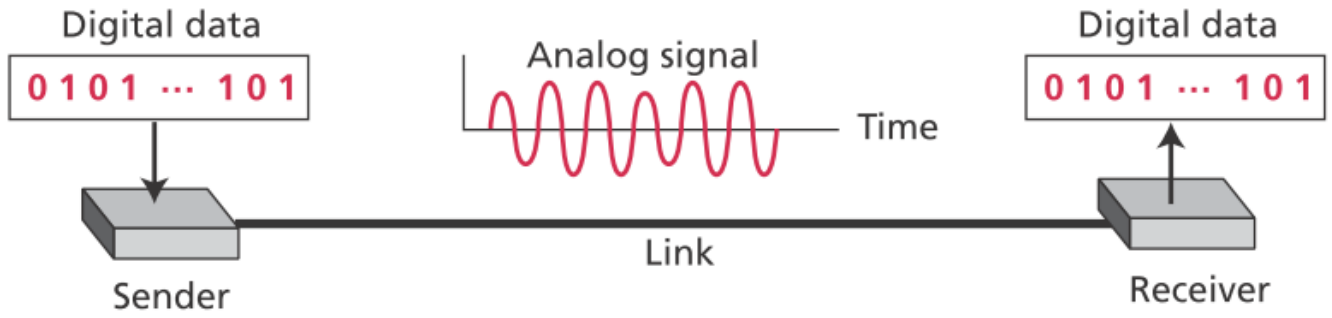


- Analog-to-digital conversion
  - We can sample the analog signal to create a digital data and convert the digital data to digital signal

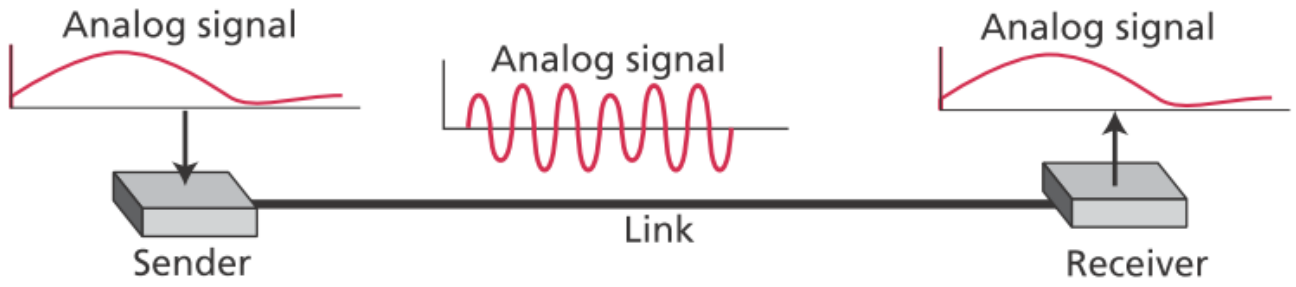


Analog transmission

- While digital transmission is desirable, it needs a dedicated channel; analog transmission is the only choice if we do not have a dedicated channel
- Digital-to-analog conversion

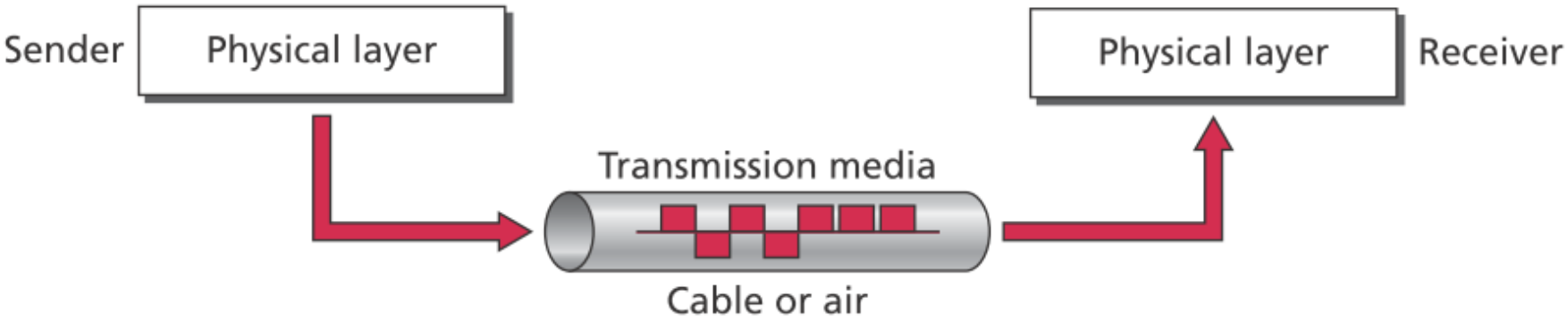


- Analog-to-analog conversion



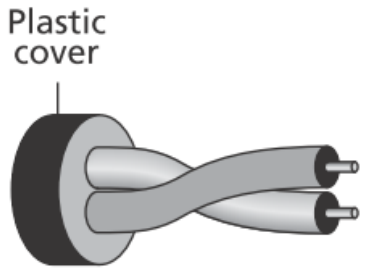
Transmission media

- Electrical signals created at the physical layer need *transmission media* to go from one point to another
  - Transmission media are actually located below the physical layer and are directly controlled by the physical layer
  - In telecommunications, transmission media can be divided into two broad categories: guided and unguided

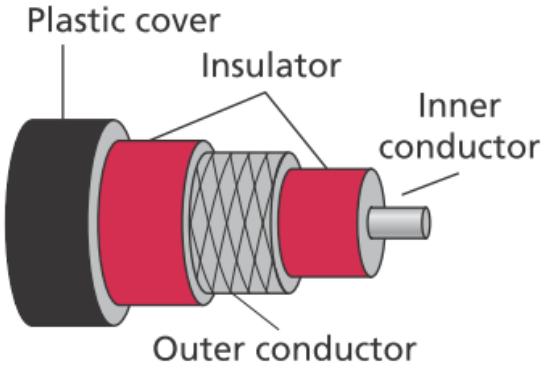


Guided media

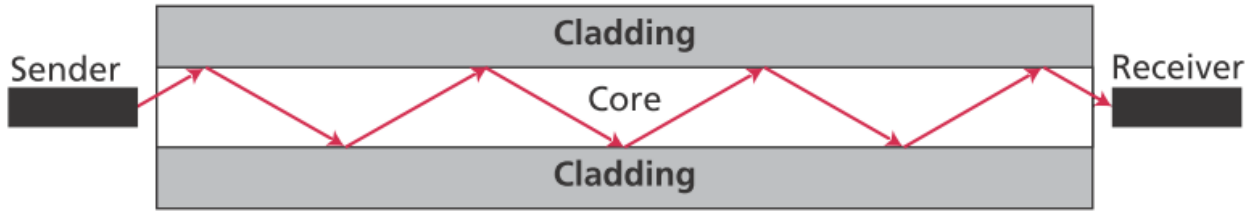
- Twisted-pair cable
  - The DSL lines that are used by the telephone companies to provide high-data-rate connections are twisted-pair cables
- Coaxial cable
  - Cable TV networks use coaxial cable
- Fiber-optic cable
  - Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective



a. Twistedpair



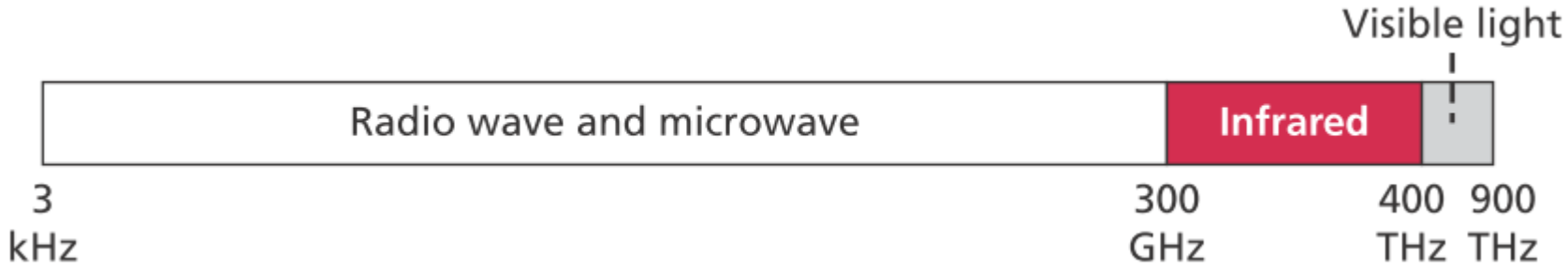
b. Coaxial



c. Fiber-optic

Unguided media: wireless

- This type of communication is often referred to as *wireless communication*
  - Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them



Unguided media: wireless

- Radio waves
  - Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. They are used mostly for radio communication
- Microwaves
  - Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned
- Infrared
  - Infrared waves, with frequencies from 300 GHz to 400 THz can be used for short-range communication
  - Having this high frequency it cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; However, this same characteristic makes infrared signals useless for long-range communication