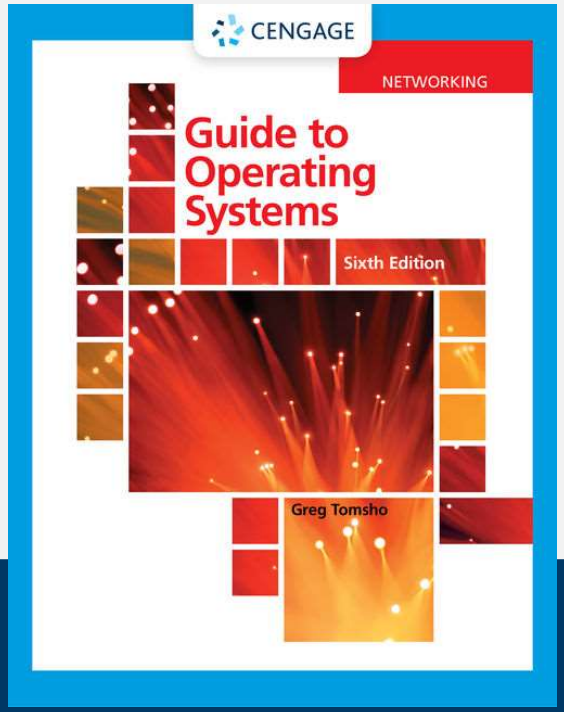

Guide to Operating Systems, 6th Edition

Module 9: Network Fundamentals and Configuration

function of a network: connected, communication
what we need: computers, transmission medium, network card (nic) (wired or wireless), router (routes info, segregates data domain)

Learning Objectives

By the end of this module, you should be able to:

- Explain the fundamentals of network communication
- Define common networking terms
- Compare and describe network device types
- Configure and describe network protocols
- Describe the OSI model of networking
- Configure networking in an operating system
- Wireshark?

CENGAGE

The Fundamentals of Network Communication

- A computer network consists of two or more computers connected by some kind of transmission medium
  - A transmission medium can be a cable or airwaves
- In order to access the Internet, a computer has to be able to connect to a network
- The next few slides will cover what is required to turn a standalone computer into a networked computer

Network Components (1 of 2)

- Hardware components needed to create a networked computer:
  - A *network interface card (NIC)* is an add-on card plugged into an expansion slot that provides a connection between the computer and the network
  - A *network medium* cable plugs into the NIC and makes the connection between a computer and the rest of the network
    - Network media can also be the airwaves, as in wireless networks
  - An *interconnecting device* allows two or more computers to communicate on the network without having to be connected directly to one another

wired or wireless

Network Components (2 of 2)

- Network software categories:
  - *Network clients and servers*
    - **Network client software** requests information stored on another network computer or device
    - **Network server software** allows a computer to share its resources
  - *Protocols* – define the rules and formats a computer must use when sending information across the network differs on what they need to accomplish
  - *NIC device driver* – receives data from protocols and forwards this data to the physical NIC

Steps of Network Communication

- 1. An application tries to access a network resource by sending a message
- 2. Network client software formats the message and passes it on to the network protocol
- 3. The protocol packages the message in a format suitable for the network and sends it to the NIC driver
- 4. The NIC driver sends data in the request to the NIC card to be converted into necessary signals to be transmitted on the network
- The steps taken on the server side are essentially the reverse of the steps above, which are taken on the client side

Layers of the Network Communication Process

- Each step required for a client to access network resources is referred to as a “layer”
- Each layer has a task and all layers work together

reversing the process to go up the stack

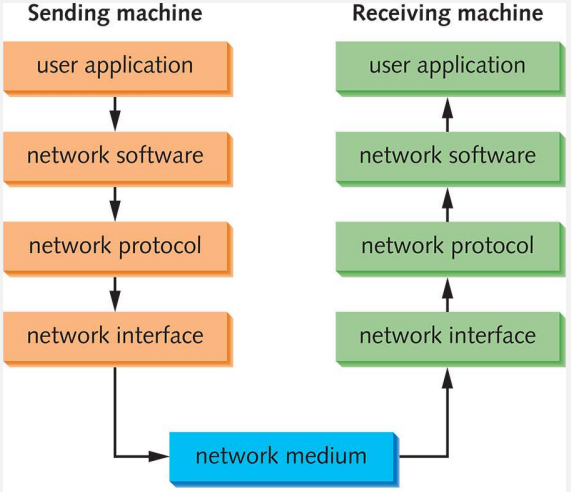

Figure 9-2 Layers of the network communication process

How Two Computers Communicate on a LAN (1 of 3)

- TCP/IP is the most common protocol (language) used on networks
- TCP/IP uses two addresses to identify devices:
  - Logical address (IP address) obtain this from DHCP server
  - Physical address (**Media Access Control** or **MAC address**) on NIC
- Just as a mail person needs an address to deliver mail, TCP/IP needs an address in order to deliver data to the correct device on a network
- Think of the logical address as a zip code and the physical address as a street address

How Two Computers Communicate on a LAN (2 of 3)

1. A user at Computer A types *ping 10.1.1.2* at a command prompt
2. Network software creates a ping message
3. The network protocol packages the message by adding the IP addresses of the sending and destination computers and acquires the destination computer's MAC address source and destination into the packet

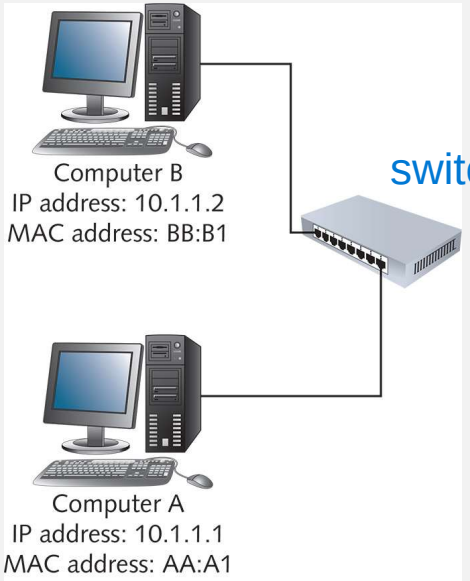

Figure 9-3 Communication between two computers

How Two Computers Communicate on a LAN (3 of 3)

4. The network interface software adds the MAC addresses of the sending and destination computers
5. Computer B receives the message, verifies that the addresses are correct, and then sends a reply to Computer A using steps 2 through 4

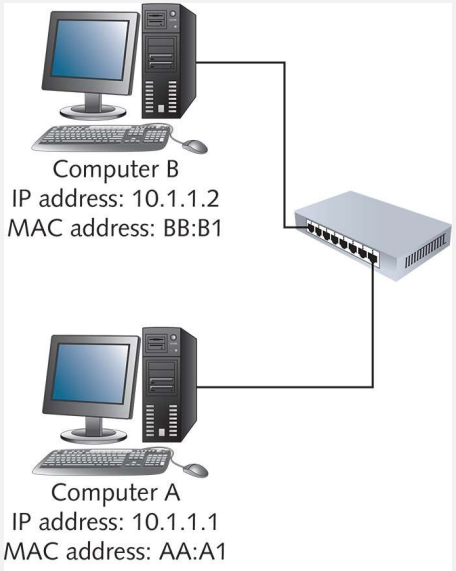

Figure 9-3 Communication between two computers

Network Terminology

- Every profession has its own language and acronyms
- It is essential to know the language of networks to be able to study them

LANs, Internetworks, WANs, and MANs (1 of 3)

- A local area network (LAN) is a small network limited to a single collection of machines and connected by one or more interconnecting devices in a small geographic area

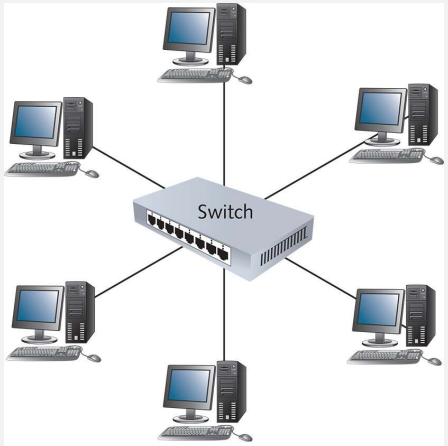

Figure 9-4 A LAN with computers interconnected by a switch

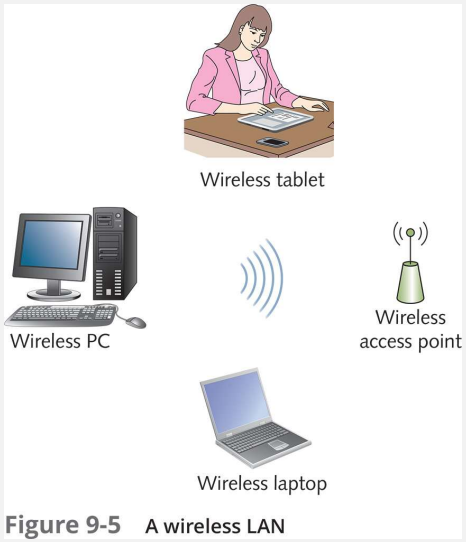

Figure 9-5 A wireless LAN

LANs, Internetworks, WANs, and MANs (2 of 3)

- An **internetwork** is a collection of LANs connected by devices such as routers
- Some reasons for creating an internetwork:
  - Two or more groups of users and their computers need to be logically separated but still need to communicate
  - The number of computers in a single LAN has grown and is no longer efficient

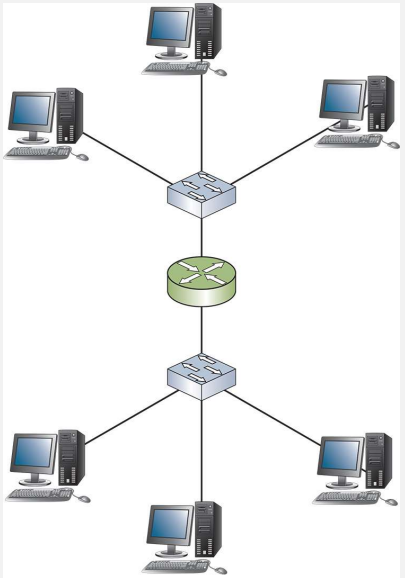

Figure 9-6 An internetwork with two LANs connected by a router

LANs, Internetworks, WANs, and MANs (3 of 3)

- **Wide area networks (WANs)** use the services of third-party communication providers to carry network traffic from one location to another
- **Metropolitan area networks (MANs)** use WAN technologies to interconnect LANs in a specific geographic region, such as a county or city

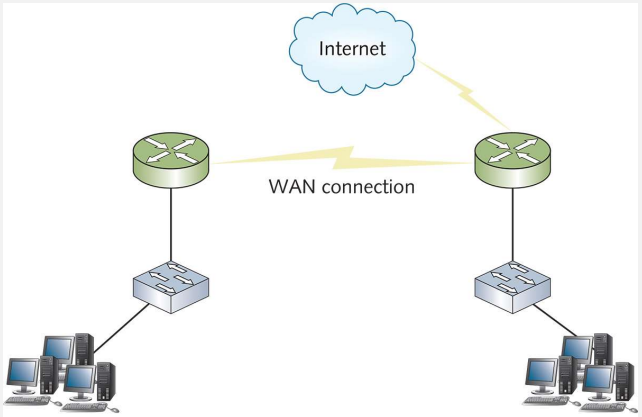

Figure 9-7 A WAN with a connection to the Internet

Packets and Frames (1 of 3)

- Computers transfer information across networks in short bursts of about 1500 bytes of data so that:
  - If an error occurs during transmission of a large file, only the chunks of data involved in the error have to be sent again
  - Pauses between bursts allow other computers to transfer data
  - The pause also allows the receiving computer to process received data
  - It allows the receiving computer to receive data from other computers at the same time
  - The pause gives the sending computer an opportunity to receive data from other computers and perform other processing tasks

Packets and Frames (2 of 3)

- The chunks of data sent across the network are usually called packets or frames; *packets* is the better-known term
- A **packet** is a chunk of data with a source and destination IP address added to it
- Using the US mail analogy, you can look at a packet as an envelope that has had the zip code added but not the street address

Packets and Frames (3 of 3)

- A **frame** is a packet with the source and destination MAC addresses added to it
  - The packet is "framed" by the MAC addresses on one end and an error-checking code on the other
- The process of adding IP addresses and MAC addresses to chunks of data is called **encapsulation**
- Information added to the front of the data is called a **header** and information added to the end is called a **trailer**

VPN is higher encapsulation

Clients and Servers (1 of 2)

- A **client** can be a workstation running a client OS
  - Or, *client* can refer to the network software on a computer that requests network resources from a server
- The word *client* is typically used in these three contexts:
  - *Client operating system* – the OS installed on a computer
  - *Client computer* – the computer's primary role is to run user applications and access network resources
  - *Client software* – software that requests network resources from server software on another computer

Clients and Servers (2 of 2)

- A computer becomes a **server** when software is installed on it that provides a network service to client computers
- The term *server* is also used in three contexts:
  - *Server operating system* – an OS installed on a computer designed to share network resources and provide other network services
  - *Server computer* – the computer's primary role in the network is to give client computers access to network resources and services
  - *Server software* – software that responds to requests for network resources from client software

Peer-to-Peer and Client/Server Networks (1 of 3)

- A network model defines how and where resources are shared and how access to these resources is regulated
- Network models fall into two major types:
  - **Peer-to-peer network** – most computers function as clients or servers (no centralized control over who has access to network resources)
  - **Server-based network** – certain computers take on specialized roles and function mainly as servers, and ordinary users' machines tend to function mainly as clients

Peer-to-Peer and Client/Server Networks (2 of 3)

- A **domain** is a collection of users and computers whose accounts are managed by Windows servers called **domain controllers**
- Users and computers in a domain are subject to network access and security policies defined by a network administrator
  - The software that manages this security is referred to as a **directory service**
  - On Windows servers, the directory service software is **Active Directory**
- Linux administrators use a service compatible with Active Directory called **Lightweight Directory Access Protocol (LDAP)**

Peer-to-Peer and Client/Server Networks (3 of 3)

- Other network services found on network servers:
  - *Naming services* – translate computer names to their addresses
  - *E-mail services* – manage incoming and outgoing email
  - *Application services* – grant client computers access to complex applications that run on the server
  - *Communication services* – give remote users access to a network
  - *Web services* – provide comprehensive Web-based application services

Knowledge Check 1

- Which of the following is considered the final state of data before it's placed on the network medium as bits?
  - A) segment
  - B) frame
  - C) packet
  - D) header

Knowledge Check 1: Answer

- Which of the following is considered the final state of data before it’s placed on the network medium as bits?

it has all the parts (mac address), need the whole thing to place on the network since we're talking mac address to mac address

- B) frame

Network Device Fundamentals

- LANs, WANs, MANs, and internetworks are built with a variety of network hardware
- This section covers a wide variety of network devices

Network Switches

- A network switch is used to interconnect multiple computers so that they can communicate with one another
- A switch's operation can be summarized in these steps:
  1. The switch receives a frame
  2. The switch reads the source and destination MAC addresses
  3. The switch looks up the destination MAC address in its switching table
  4. The switch forwards the frame to the port where the computer that owns the MAC address is found
  5. The switching table is updated with the source MAC address and port information

Wireless Access Points

- The heart of a wireless network is the wireless **access point (AP)**
- Each computer on a wireless network sends a frame to the AP, which then retransmits the frame to the destination computer
- The destination device then sends an acknowledgment back to the sending device to indicate that the frame was received
- When the sending device receives the acknowledgment, it knows that no error has occurred

Network Interface Cards

- Attaching a computer to a network requires a **network interface card (NIC)** to create and mediate the connection between a computer and the networking medium
  - The networking medium might be copper wire, fiber-optic cable, or airwaves
  - Data is represented as bit signals that the NIC transmits or receives

data is serial, works like block storage

Routers (1 of 3)

- **Routers** are the most complex devices discussed in this module
- Routers connect LANs together to create an internetwork
  - Typically, routers have two or more network ports to which switches or hubs are connected
- Routers are devices that enable multiple LANs to communicate with one another by forwarding packets from one LAN to another

Routers (2 of 3)

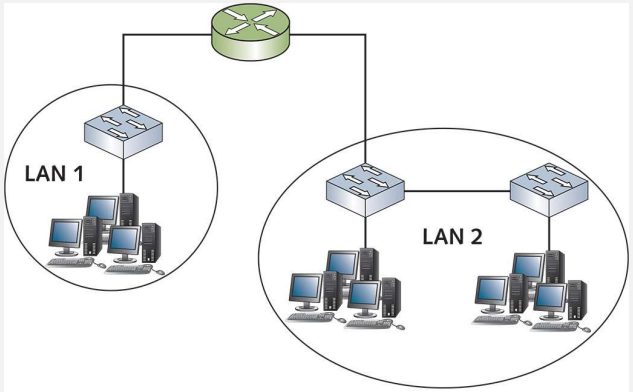

Figure 9-14 Two LANs connected by a router to make an internetwork

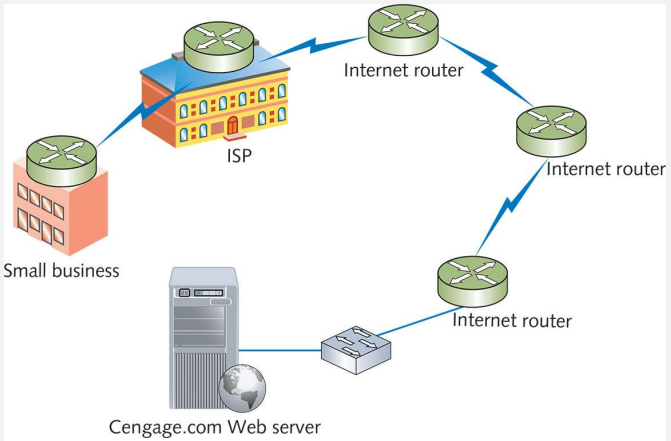

Figure 9-15 Routers interconnect LANs to form the Internet

Routers (3 of 3)

- Note the following differences between routers and switches:
  - Routers connect LANs, switches connect computers
  - Routers work with logical (IP) addresses, switches work with physical (MAC) addresses needs source and destination
  - Routers work with packets, switches work with frames
  - Routers don’t forward broadcasts, switches do
  - Routers use routing tables, switches use switching tables

Network Protocol Fundamentals (1 of 5)

- **Protocols** are rules and procedures for communication and behavior
  - Computers must “speak” the same language and agree on the rules of communication
- When a set of protocols works cooperatively, it is called a **protocol suite** (or *protocol stack*)
- The most common protocol stack is **Transmission Control Protocol/Internet Protocol (TCP/IP)**
- TCP/IP is composed of more than a dozen protocols operating at different levels of the communication process

Network Protocol Fundamentals (2 of 5)

- Example of how the layers work together:
  - You start your Web browser
  - The Web browser formats a request for your home page by using the Application layer protocol HTTP
  - The unit of information the Application layer works with is simply called “data”

Figure 9-17 The Application layer creates data

Network Protocol Fundamentals (3 of 5)

work down the stack

- Example continued:
  - The Application layer protocol HTTP passes the request down to the Transport layer protocol (TCP)
  - TCP adds a header to the request
  - The unit of information the Transport layer works with is called a **segment**
  - TCP passes the segment to the Internetwork layer protocol (IP)

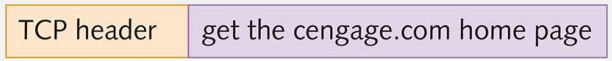

Figure 9-18 The Transport layer adds its header to make a segment

Network Protocol Fundamentals (4 of 5)

- Example continued:
  - IP places its header on the segment
  - The unit of information is now called a packet
  - The packet is passed down to the Network access layer, where the NIC operates

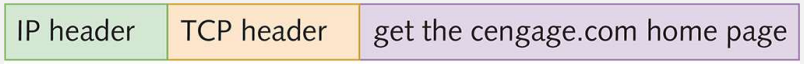

Figure 9-19 The Internetwork layer creates a packet

Network Protocol Fundamentals (5 of 5)

- Example continued:
  - A frame header and trailer are added
  - The frame is delivered to the network medium as bits on its way to the *www.cengage.com* server
  - The Web server processes it and returns a Web page

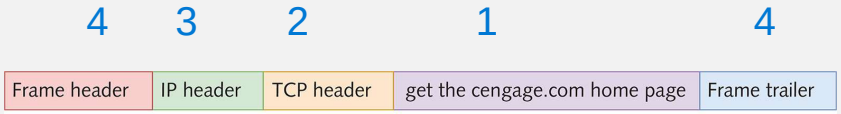

Figure 9-20 The frame is created and ready for delivery on the medium

Application Layer Protocols (1 of 12)

- The Application layer provides network services to user applications that access network resources
- The Application layer provides these functions:
  - Access by applications to network services user layer
  - Client/server data access
  - Name resolution
  - Dynamic address assignment
  - Authentication/user logon
  - Data formatting and translation

Application Layer Protocols (2 of 12)

- **HTTP** is the protocol that browsers use to access data on the World Wide Web
  - Originally, HTTP's main purpose was to transfer static Web pages written in HTML
  - Now, it is used for general file transfer and for downloading and displaying multimedia files
    - It is also used to deliver scripts for animated and interactive Web pages
  - HTTP uses TCP as its Transport layer protocol
    - The default TCP port number is 80

Application Layer Protocols (3 of 12)

- Common email protocols are POP3, IMAP, and SMTP
  - **Post Office Protocol version 3** (**POP3**) is used to download incoming messages from email servers to local desktops
  - **Internet Message Access Protocol version 4** (**IMAP4**) is used to manage email messages locally, but it stores the messages on a server
  - **Simple Mail Transfer Protocol** (**SMTP**) is the standard protocol for sending email over the Internet

Application Layer Protocols (4 of 12)

- **Server Message Block** (**SMB**) is the protocol that Windows file and printer services use to share resources between Windows computers
  - SMB is used almost exclusively in a private network instead of across the Internet
  - It uses TCP port 445
- Linux and Mac OS X also support SMB with their own variations

Application Layer Protocols (5 of 12)

- A drawback of using TCP/IP in a large network is keeping track of assigned addresses and the machines to which they are assigned
- **Dynamic Host Configuration Protocol** (**DHCP**) is used to automatically assign IP addresses as needed
  - A computer requests an IP address from a server that is configured as a DHCP server
    - The request is sent in the form of a broadcast message
  - The server assigns an address for a specific amount of time

Application Layer Protocols (6 of 12)

- **DHCP Server**
  - A DHCP server is composed of the following:
    - *IP address scope* – a range of IP addresses the server leases to clients
    - *DHCP Server service* – runs in the background and listens on UDP port 69 for IP address requests
  - Benefit of using DHCP
    - Computers can easily be moved and request new IP configuration from a DHCP server on the new segment

no need to fix an address

  - DHCP uses UDP

Application Layer Protocols (7 of 12)

- **DHCP Client**
  - DHCP client software runs as a service that starts when the computer starts
    - You can stop, start, restart, and view the status of the service in Windows by double-clicking DHCP Client in the Services control panel
    - This service runs even if your IP address is assigned statically
    - To prevent it from running, disable it in the DHCP Client Properties dialog box or from the command line with the *net* command

Application Layer Protocols (8 of 12)

- **Domain Name System** (**DNS**) is a name-to-address resolution protocol that keeps a list of computer names and their IP addresses
- With DNS, a user can use a computer's name instead of its IP address
- DNS is organized as a treelike hierarchy
  - When you put all the names of a branch together, separated by periods, you have the **fully qualified domain name (FQDN)** of the network resource
- Top-level domains are organized into categories such as commercial (.com), nonprofit organizations (.org), government (.gov), or country of origin (indicated by a two-letter code)

Application Layer Protocols (9 of 12)

- In DNS, second-level domains are usually the name of a company or institution
- The subdomain level is optional and can consist of names separated by a period
- The host level represents individual computers hosting network services
- For example, in *www.books.tomsho.com*:
  - com is the top-level domain name, tomsho is the second-level domain, books is the subdomain, and www is the host name

Application Layer Protocols (10 of 12)

- **DNS Client**
  - The DNS client is responsible for communicating with a DNS server to resolve computer and domain names to IP addresses
  - The DNS client is referred to as a “resolver”
  - An OS must be configured to use DNS and needs at least one address of a DNS server that it can query
  - In Windows, the first DNS server configured is called the preferred DNS server and the second one is the alternate DNS server
  - DNS servers require a domain name in addition to a computer name

Application Layer Protocols (11 of 12)

- **DNS Client** (continued)
  - In Windows, the default domain appended to DNS lookups is called the "primary DNS suffix"
  - Windows supports **Dynamic DNS** (**DDNS**), which allows computers and other devices to contact their primary DNS server whenever their name or address changes

Application Layer Protocols (12 of 12)

- **DNS Server**
  - DNS servers are composed of the following:
    - *DNS zones* – a database of primarily host name and IP address pairs
    - *Resource records* – the data contained in a zone
    - *Cache* – results of queries are cached
    - *Root hints* – a file containing a list of all IP addresses of Internet root servers
    - *DNS Server service* – runs in the background and listens for DNS queries on UDP port 53

rowan.edu

www

everytime query DNS record, whoever creates that makes a timetolive (you can cache something for that time)

Transport Layer Protocols (1 of 2)

- Transport layer protocols are used with most Application layer protocols because they:
  - Supply a header field to identify the Application layer
  - Provide reliability and flow control for applications
- The Transport layer has two protocols:
  - **Transmission Control Protocol** (**TCP**) is connection oriented and designed for reliable transfer of information in complex internetworks
  - **User Datagram Protocol** (**UDP**) is connectionless and designed for efficient communication of generally small amounts of data

Transport Layer Protocols (2 of 2)

- The TCP and UDP protocols perform the following tasks:
  - Work with segments (TCP) or datagrams (UDP)
  - Provide a means to identify the source and destination applications involved in a communication
  - Protect data with a checksum
- TCP and UDP use **port numbers** to specify the source and destination Application layer protocols

Internetwork Layer Protocols (1 of 5)

- The Internetwork layer is where administrators usually do the most network configuration
- An IP address is assigned to every computer and network device using TCP/IP for communications
- IP addresses are used for two main purposes:
  - To identify a network device at the Internetwork layer
  - To identify the network on which a device resides

Internetwork Layer Protocols (2 of 5)

- When a device receives an IP packet, it compares the destination IP address with its own:
  - If it matches or is a broadcast, the packet is processed
  - If it does not match, it is discarded
- Every IP address contains two parts:
  - A network ID
  - A host ID

Internetwork Layer Protocols (3 of 5)

10.1.1.10

- An **IPv4 address** is a 32-bit number divided into four 8-bit values called octets; each octet can have a value from 0 to 255
  - Four decimal numbers are separated by periods in a format called **dotted decimal notation**
- Subnet masks are also 32-bit numbers that serve to determine how many bits are allocated to a network ID and how many are allocated to a host ID
- When written in binary, 1s in the subnet mask that correspond to bits in the IP address mean the matching bit locations are part of the network ID

Internetwork Layer Protocols (4 of 5)

- IPv6 Addresses
  - IPv6 uses 128 bits, instead of IPv4's 32 bits, for an address
  - IPv6 addresses don't use subnet masks to determine the network ID and host ID
  - IPv6 addresses are written as eight 16-bit hexadecimal numbers separated by colons—for example, fe80:0:0:0:18ff:0024:8e5a:60

Internetwork Layer Protocols (5 of 5)

- IPv6 includes the following improvements over IPv4:
  - Larger address space
  - Hierarchical address space
  - Autoconfiguration helps give ip addresses to everyone since there's not enough usually
  - Built-in Quality of Server (QoS) support
  - Built-in support for security
  - Support for mobility

Network Access Layer Protocols (1 of 2)

- Some tasks performed by the Network access layer:
  - Provides a physical (MAC) address for the network interface
  - Verifies that incoming frames have the correct destination MAC address
  - Defines and follows media access rules
  - Receives packets from the Internetwork layer and encapsulates them to create frames
  - De-encapsulates received frames and sends the resulting packets to the Internetwork layer

Network Access Layer Protocols (2 of 2)

- Some tasks performed by the Network access layer (continued):
  - Often provides frame error detection in the form of a CRC code
  - Transmits and receives bit signals
  - Defines the signaling needed to transmit bits, whether electrical, light pulses, or radio waves
  - Defines the media and connectors needed to make a physical network connection

Knowledge Check 2

- What Application layer protocol is used to automatically assign IP addresses as needed?
  - A) SMB
  - B) DNS
  - C) FTP
  - D) DHCP

Knowledge Check 2: Answer

- What Application layer protocol is used to automatically assign IP addresses as needed?

- D) DHCP

Introducing the OSI Model of Networking

- The **Open Systems Interconnection (OSI) reference model** provides a common framework for developers and students of networking to work with and learn from
- The OSI model is not specific to any protocol suite and can be applied to most networking protocols
- The OSI model is a seven-layer organization of how data travels from place to place on any given network

Structure of the OSI Model

- Each layer in the OSI model has its own set of well-defined functions
  - The functions of each layer communicate and interact with the layers immediately above and below it
  - For example, the Transport layer works with the Network layer below it and the Session layer above it

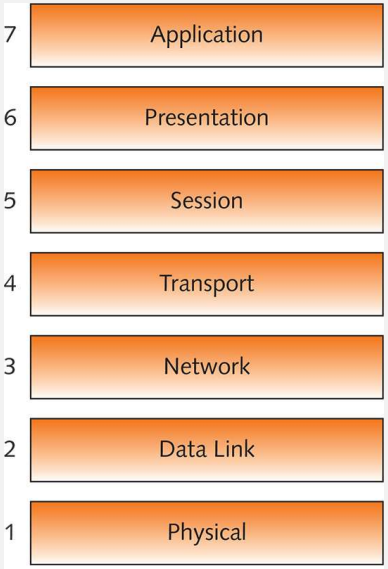

Figure 9-31 The seven layers of the OSI reference model

bottom 4 asked questions on rather than top 3

Configuring Networking in an Operating System

- Network configuration in an OS follows a similar pattern as the steps in the network communication process
- All functions of the network model must be accounted for

Configuring the Network Interface

- In most cases, you don’t have to configure the NIC
  - If a NIC is installed, the OS will usually install the proper driver
  - You may need to install a new or different driver if an update is available
- Linux and macOS offer configuration settings for the network interface
  - Use the command-line tool *ethtool* to display and change network interface settings
  - In macOS, use the advanced settings in the Network dialog box

Configuring IPv4 Addresses (1 of 3)

- Configuration of an IP address consists of the following parts:
  - IP address
  - Subnet mask
  - Default gateway
  - Preferred DNS server
  - Alternate DNS server

172.31.21.21
172.32.23.23

not on the same network (first two sets of numbers)

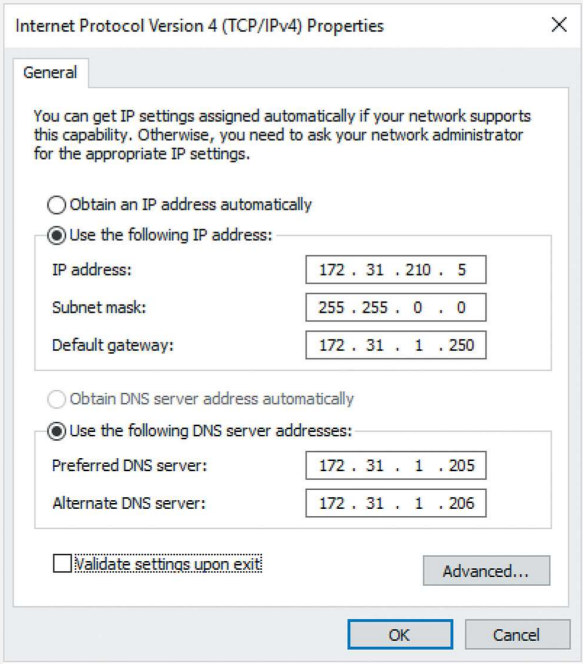

Figure 9-35 The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box

Configuring IPv4 Addresses (2 of 3)

- Windows is configured to obtain an IP address automatically by default using DHCP
- If you need a **static IP address**, it must be manually configured
- Configure a static IPv4 address in Windows using a GUI or the *netsh* command from the command line
- To configure an interface named Ethernet0:
  - *netsh interface ipv4 set address "Ethernet0" static 10.1.1.1 255.255.0.0*
  - You can include the default gateway by adding the address to the end of the command

Configuring IPv4 Addresses (3 of 3)

- To configure an IP address to an interface named eth0, use the following command from the shell prompt:
  - *ifconfig eth0 10.1.1.1 netmask 255.255.0.0*
- To configure a default gateway in Linux, use the *route* command:
  - *route add default gw 10.1.1.250*
- Most Linux installations have a GUI tool for configuring IP address settings

Configuring IPv6 Addresses

- A computer with IPv6 enabled is always automatically assigned a **link-local IPv6 address**
  - It always begins with fe80 and is self-configuring
- IPv6 autoconfiguration occurs by two methods:
  - *Stateless autoconfiguration* – the node listens for router advertisement messages from a local router
  - *Stateful autoconfiguration* – the node uses an autoconfiguration protocol, such as DHCPv6, to obtain its IPv6 address and other configuration information

Summary (1 of 2)

- Components needed to make a standalone computer a networked computer include a NIC, a network medium, and usually an interconnecting device
- The layers of the network communication process can be summarized as the user application, network software, network protocol, and network interface
- The terms used to describe networks of different scope are LAN, internetwork, WAN, and MAN
- Packets and frames are the units of data handled by different network components

multiple sites long distances

two sites through a network??

Summary (2 of 2)

- LANs, WANs, MANs, and internetworks are built with a variety of network hardware
- TCP/IP is the main protocol suite used in networks
- The Open Systems Interconnection (OSI) reference model explains how networks behave within an orderly, seven-layered model for communication
- Network configuration in an OS follows a similar pattern as the steps in the network communication process, the TCP/IP model, and the OSI model