شبكات كمبيوتر
م/ اخوان المضاحكة

ENC-254

Computer Networks (1)

Eng. Nawaf Almudhahka

١/٧٥٠

COURSE TECHNOLOGY
CENGAGE Learning

Network+ Guide to Networks 5th Edition

Chapter 1
An Introduction to Networking

Goals of This Chapter

- List the advantages of networked computing relative to standalone computing
- Distinguish between client/server and peer-to-peer networks
- List elements common to all client/server networks
- Describe several specific uses for a network
- Identify some of the certifications available to networking professionals
- Identify the kinds of skills and specializations that will help you excel as a networking professional

Why Use Networks?

- Network
  - Group of computers and devices
    - Connected by transmission media
- Stand-alone computer
  - Not connected to other computers
  - Uses local software and data
- Advantages of networks over standalone computers
  - Device sharing by multiple users
    - Saves money and time
  - Central network management

Types of Networks

- Models vary according to:
  - Computer positioning
  - Control levels over shared resources
  - Communication and resource sharing schemes
- Network models
  - Peer-to-Peer
  - Client/server

Peer-to-Peer Network

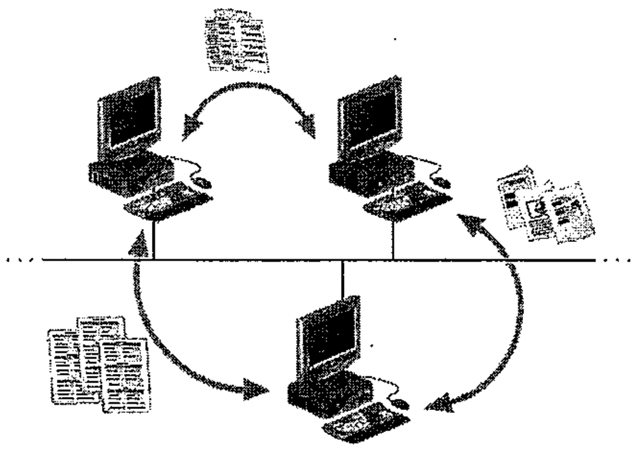


Figure 1-1 Resource sharing on a simple peer-to-peer network

Peer-to-Peer Networks

- Typical in a home with several computers
- Direct computer communication
  - Equal authority
- Individual resource sharing
  - May share resources
  - May prevent access to resources
- Each computer can send data to every other computer on the network

Peer-to-Peer Networks

- Advantages
  - Simple configuration
  - Inexpensive to set up
- Disadvantages
  - Not flexible
  - Not necessarily secure
  - Not practical for large installations

Peer-to-Peer Networks

- Resource sharing method
  - Modify file sharing controls
    - A user responsibility
  - Not centrally controlled
    - Potential variations and security issues
- Environments
  - Small home or office
  - Large networks using the Internet
    - Gnutella, Freenet, original Napster
    - BitTorrent software

Obama's Helicopter Secrets Revealed

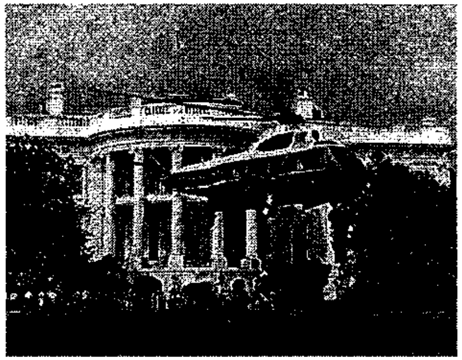
- Because of misconfigured peer-to-peer file sharing
- Link Ch 1a on the course Web page
- samsclass.info
- Click on **CNIT 106**

Marine One details leaked from P2P net

Posted by: Richard Koman @ March 1, 2009 @ 2:07 PM

Categories: Government technology

Tags: P2P, Iran, Peer To Peer (P2P), Productivity, Aerospace & Defense, Internet, Manufacturing, Richard Koman



A company that monitors P2P networks says it found details about the president's helicopter, Marine One, on a computer in Tehran. Pittsburgh station WPXI reports.

Client/Server Networks

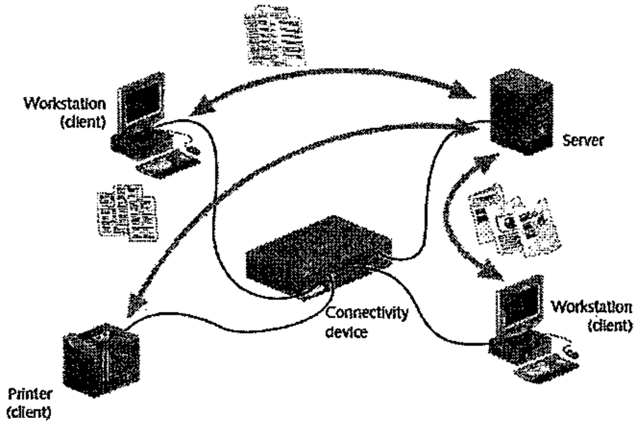


Figure 1-2 Resource sharing on a client/server network

Client/Server Networks

- Central computer (server)
  - Facilitates communication and resource sharing
- Clients (other computers)
  - Personal computers
    - Known as workstations
- Central resource sharing controlled by server
  - Data sharing, data storage space, devices
  - No direct sharing of client resources

Client/Server Networks

- Computer roles
  - Server
  - Clients
    - Run local applications
    - Store data locally
    - Use server shared applications, data, devices
    - Use server as intermediary
- Communication
  - Switches or routers

Client/Server Networks

- Server requirement
  - Network operating system
    - Manages client data, resources
    - Ensures authorized user access
    - Controls user file access
    - Restricts user network access
    - Dictates computer communication rules
    - Supplies application to clients
- Server examples
  - UNIX, Linux, Microsoft Server 2003 and 2008, MAC OS X Server

Client/Server Networks

- Server features relative to clients
  - More memory, processing, storage capacity
  - Equipped with special hardware
    - Provides network management functions
- Disadvantages relative to peer-to-peer networks
  - Complex in design and maintenance

Client/Server Networks

- Advantages relative to peer-to-peer networks
  - User credential assigned from one place
  - Multiple shared resource access centrally controlled
  - Central problem monitoring, diagnostics, correction capabilities → Central maintainence
  - User response time optimization capabilities
  - Efficient processing on large networks
  - Scalability
- Popular in medium- and large-scale organizations

LANs, MANs, and WANs

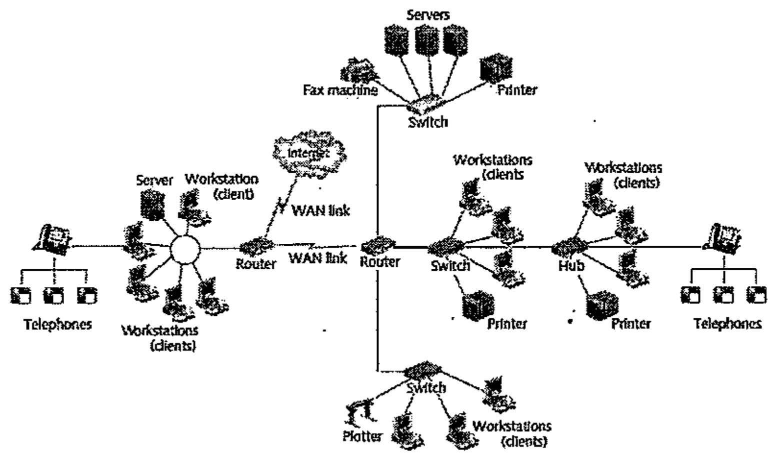


Figure 1-3 A more complex client/server network

LANs, MANs, and WANs

- LAN (local area network)
  - Network confined to a relatively small space
  - 1980s
    - LANs became popular as peer-to-peer based
  - Today
    - Larger and more complex client/server network
- MAN (metropolitan area network)
  - Network extends beyond building boundaries
  - Larger than LAN
  - Connects clients and servers from multiple buildings

LANs, MANs, and WANs

- WAN (wide area network)
  - Connects two or more geographically distinct LANs or MANs
  - Comparison to LANs
    - Use slightly different transmission methods and media
    - Use greater variety of technologies
  - Network connection
    - Separate offices in same organization
    - Separate offices in different organizations

LANs, MANs, and WANs (cont'd.)

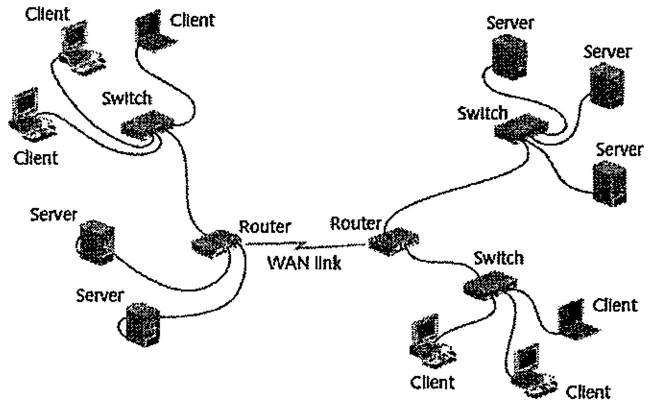


Figure 1-4 A simple WAN

Warriors of the Net Video

- Links Ch 1b, 1c

Elements Common to Client/Server Networks

- Client
  - Network computer requesting resources or services from another network computer
  - Client workstation human user
  - Client software installed on workstation
- Server
  - Network computer managing shared resources
  - Runs network operating system
- Workstation
  - Personal computer
    - May or may not be connected to network

Elements Common to Client/Server Networks

- NIC (network interface card)
  - Device inside computer
    - Connects computer to network media
    - Allows communication with other computers
- NOS (network operating system)
  - Server software
  - Enables server to manage data, users, groups, security, applications, and other networking functions

Ethernet NIC

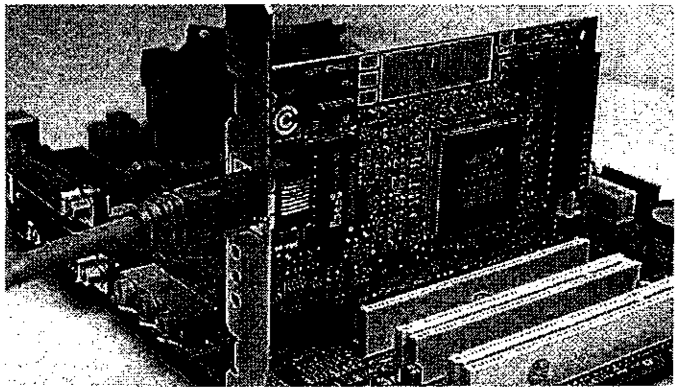


Figure 1-5 A NIC (network interface card)

Elements Common to Client/Server Networks

- Host
  - A computer that enables other computers to share resources
- Node
  - Client, server, or other device
    - Communicates over a network
    - Identified by unique number (network address)
- Connectivity device
  - Allows multiple networks or multiple parts of one network to connect and exchange data
  - Such as a switch or router

Elements Common to Client/Server Networks

- Segment
  - Group of nodes
    - Use same communications channel for traffic
- Backbone
  - Connects segments and significant shared devices
  - "A network of networks"
- Topology
  - Computer network physical layout
  - Ring, bus, star or hybrid formation

A LAN Backbone

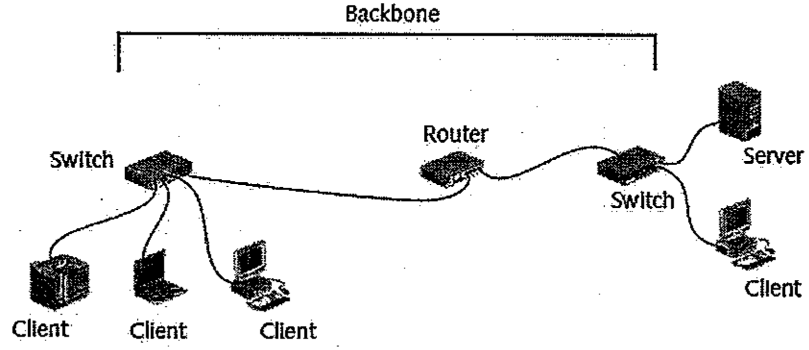


Figure 1-6 A LAN backbone

Common Network Topologies

which is which

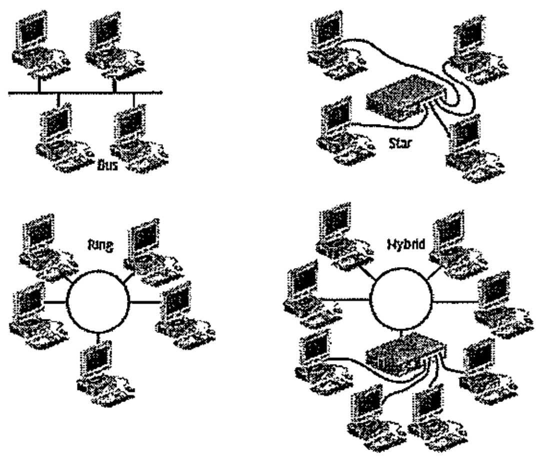


Figure 1-7 Common network topologies

Elements Common to Client/Server Networks

- Protocol
  - Standard method or format for communication between networked devices
- Data packets
  - Distinct data units exchanged between nodes
- Addressing
  - Scheme for assigning unique identifying number to every node

IP

- Transmission media
  - Means through which data is transmitted and received

Transmission Media

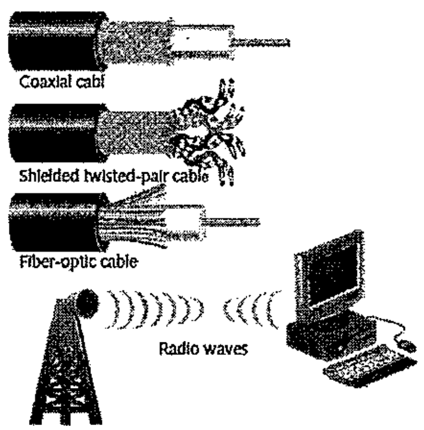


Figure 1-8 Examples of network transmission media

How Networks Are Used

- Network services
  - Functions provided by a network
  - Most visible
    - E-mail
  - Other vital services
    - Printer sharing, file sharing, Internet access and Web site delivery, remote access capabilities, the provision of voice (telephone) and video services, network management

File and Print Services

- File services
  - Capability of server to share data files, applications and disk storage space
- File server
  - Provides file services
- File services provide foundation of networking
- Print services
  - Share printers across network
  - Saves time and money

Access Services

- Allow remote user network connection
- Allow network users to connect to machines outside the network
- Remote user
  - Computer user on different network or in different geographical location from LAN's server
- Network operating systems include built-in access services

Access Services

- Provide LAN connectivity when WAN connection is not cost-effective
  - External staff used to diagnose problems
- Allow external users to use network resources and devices
  - Same as if logged on to office workstation

Communications Services

- Convergence
  - Multiple types of communications services on the same network
    - Phone calls, fax, text messages, video…
- Unified communications
  - Centralized management of network-based communications
- E-mail
  - Oldest and most frequently used
- Mail server
  - Computer responsible for mail services
    - Coordinates storage and transfer of e-mail

Communications Services

- Additional tasks of mail servers
  - Intercept spam
  - Handle objectionable content
  - Route messages according to rules
  - Provide Web-based client
  - Notify administrators or users if certain events occur
  - Schedule e-mail transmission, retrieval, storage, maintenance functions
  - Communicate with mail servers on other networks
- Mail server runs specialized mail server software

Internet Services

- Supplying Web pages
  - Servers work together to bring Web pages to user's desktop
  - Web server
    - Computer installed with appropriate software to supply Web pages to many different clients upon demand
- Other Internet services
  - File transfer capabilities, Internet addressing schemes, security filters, means for directly logging on to other Internet computers

Management Services

- Small network management
  - Single network administrator
  - Network operating system's internal functions
- Today's larger network management
  - Centrally administered network management tasks

Management Services

- Other important services
  - Traffic monitoring and control
  - Load balancing
  - Hardware diagnosis and failure alert
  - Asset management
  - License tracking
  - Security auditing
  - Address management
  - Backup and restoration of data

Becoming a Networking Professional

- Job market
  - Many job postings for computer professionals
  - Expertise levels required vary
- To prepare for entering job market
  - Master general networking technologies
  - Select areas of interest
  - Study those specialties
  - Hone communication and teamwork skills
  - Stay abreast of emerging technologies

Mastering the Technical Challenges

- Networking positions utilizing logical and analytical thinking
  - Obtain skill sets desired
- Positions in high demand
  - Consider a general knowledge of all
  - Specialize in a few
- Determine appropriate personal learning methods
- Obtain hands-on experience

Developing Your “Soft Skills”

- Soft skills
  - Not easily measurable
  - Important to networking projects
    - Customer relations
    - Oral and written communications
    - Dependability
    - Teamwork
    - Leadership abilities

Pursuing Certification

- Certification process
  - Master material
    - Pertaining to particular hardware system, operating system, programming language, software application
  - Proving mastery
    - Pass exams
- Professional organizations
  - CompTIA
- Vendors
  - Microsoft , Cisco

Pursuing Certification

- Benefits
  - Better salary
  - Greater opportunities
  - Professional respect
  - Access to better support
- Drawback
  - Number of people obtaining and pursuing them
  - Cheating and fraud (strangely not mentioned in the book)

Finding a Job in Networking

- Job research methods
  - Search the Web
  - Read the newspaper
  - Visit a career center
  - Network
  - Attend career fairs
  - Enlist a recruiter

Joining Professional Associations

- Provide varying benefits
  - Connect with people having similar interests
  - New learning opportunities
  - Specialized information access
  - Tangible assets (free goods)
  - Publications
  - Technical workshops and conferences
  - Free software, prerelease software
  - Expensive hardware lab access

Joining Professional Associations

Professional organization	Web site
Association for Computing Machinery (ACM)	*www.acm.org*
Association for Information Technology Professionals	*www.aitp.org*
IEEE Computer Society	*www.computer.org*
Network Professional Association	*www.npanet.org*
Women in Technology International (WITI)	*www.witi.org*

Table 1-1 Networking organizations

CENGAGE Learning

Network+ Guide to Networks 5th Edition

Chapter 2

Networking Standards and the OSI Model

Objectives

- Identify organizations that set standards for networking
- Describe the purpose of the OSI model and each of its layers
- Explain specific functions belonging to each OSI model layer

Objectives (cont'd.)

- Understand how two network nodes communicate through the OSI model
- Discuss the structure and purpose of data packets and frames
- Describe the two types of addressing covered by the OSI model

Networking Standards Organizations

- Standard
  - Documented agreement
  - Technical specifications/precise criteria
  - Stipulates design or performance of particular product or service
- Standards are essential in the networking world
  - Wide variety of hardware and software
    - Ensures network design compatibility
- Standards define minimum acceptable performance
  - Not ideal performance

Networking Standards Organizations (cont'd.)

- Many different organizations oversee computer industry standards
  - Organizations may overlap responsibilities
    - Example: ANSI and IEEE set wireless standards
- Network professional's responsibility
  - Be familiar with groups setting networking standards
  - Understand critical aspects of standards required by own networks

ANSI

- ANSI (American National Standards Institute)
  - 1000+ representatives from industry and government
  - Determines standards for electronics industry and other fields
- Requests voluntarily compliance with standards
- Obtaining ANSI approval requires rigorous testing
- ANSI standards documents available online

EIA and TIA

- EIA (Electronic Industries Alliance)
  - Trade organization
    - Representatives from United States electronics manufacturing firms
  - Sets standards for its members
  - Helps write ANSI standards
  - Lobbies for favorable computer and electronics industries legislation

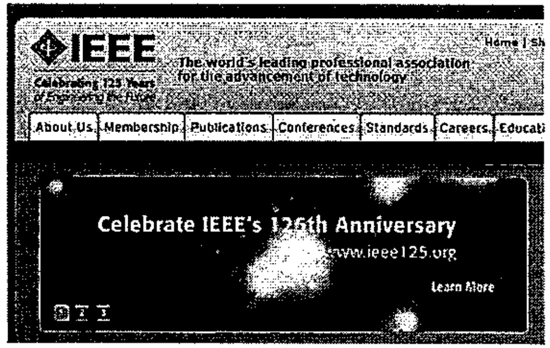
EIA and TIA (cont'd.)

- TIA (Telecommunications Industry Association)
  - Formed in 1988
    - EIA subgroup merged with former United States Telecommunications Suppliers Association (USTSA)
  - Focus of TIA
    - Standards for information technology, wireless, satellite, fiber optics, and telephone equipment
- TIA/EIA 568-B Series
  - Guidelines for installing network cable in commercial buildings

IEEE

- IEEE (Institute of Electrical and Electronics Engineers)
  - International engineering professionals society
- Goal of IEEE
  - Promote development and education in electrical engineering and computer science fields
- Hosts symposia, conferences, and chapter meetings
- Maintains a standards board
- IEEE technical papers and standards
  - Highly respected

IEEE Student Chapter at CCSF



- Last semester, the chapter arranged a tour of a data center
- I'll let you know what's coming up this semester

ISO

- ISO (International Organization for Standardization)
  - Headquartered in Geneva, Switzerland
  - Collection of standards organizations
    - Representing 57 countries
- Goal of ISO
  - Establish international technological standards to facilitate global exchange of information and barrier free trade
- Widespread authority

ITU

- ITU (International Telecommunication Union)
  - Specialized United Nations agency
  - Regulates international telecommunications
  - Provides developing countries with technical expertise and equipment
  - Founded in 1865
    - Joined United Nations in 1947
  - Members from 191 countries
- Focus of ITU
  - Global telecommunications issues
  - Worldwide Internet services implementation

ISOC

- ISOC (Internet Society)
  - Founded in 1992
  - Professional membership society
  - Establishes technical Internet standards
- Current ISOC concerns
  - Rapid Internet growth
  - Keeping Internet accessible
  - Information security
  - Stable Internet addressing services
  - Open standards

ISOC (cont'd.)

- ISOC oversees groups with specific missions
  - IAB (Internet Architecture Board)
    - Technical advisory group
    - Overseeing Internet's design and management
  - IETF (Internet Engineering Task Force)
    - Sets Internet system communication standards
    - Particularly protocol operation and interaction
    - Anyone may submit standard proposal
    - Elaborate review, testing, and approval processes

IANA and ICANN

- IP (Internet Protocol) address
  - Address identifying computers in TCP/IP based (Internet) networks
  - Reliance on centralized management authorities
- IP address management history
  - Initially: IANA (Internet Assigned Numbers Authority)
  - 1997: Three RIRs (Regional Internet Registries)
    - ARIN (American Registry for Internet Numbers)
    - APNIC (Asia Pacific Network Information Centre)
    - RIPE (Réseaux IP Européens)

IANA and ICANN (cont'd.)

- IP address management history (cont'd.)
  - Late 1990s: ICANN (Internet Corporation for Assigned Names and Numbers)
    - Private nonprofit corporation
    - Remains responsible for IP addressing and domain name management
    - IANA performs system administration
- Users and business obtain IP addresses from ISP (Internet service provider)

ICANN's Stormy History

- 2002: ICANN was sued by one of their own board members to force them to disclose financial documents
- 2003: ICANN sued Verisign to make them shut down their "Site Finder" service, which captured all mistyped URLs and showed them Verisign ads
- 2004 Verisign sued ICANN saying they had overstepped their authority
- 2008 Ten worst spam offenders notified by ICANN
  - Links Ch 2a, 2b, 2c

The OSI Model

- Model for understanding and developing network computer-to-computer communications
- Developed by ISO (1980s)
- Divides network communications into seven layers
  - Physical, Data Link, Network, Transport, Session, Presentation, Application

The OSI Model (cont'd.)

- Protocol interaction
  - Layer directly above and below
- Application layer protocols
  - Interact with software
- Physical layer protocols
  - Act on cables and connectors

The OSI Model (cont'd.)

- Theoretical representation describing network communication between two nodes
- Hardware and software independent
- Every network communication process represented
- PDUs (protocol data units) what is
  - Discrete amount of data
  - Application layer function
  - Flow through layers 6, 5, 4, 3, 2, and 1
- Generalized model and sometime imperfect

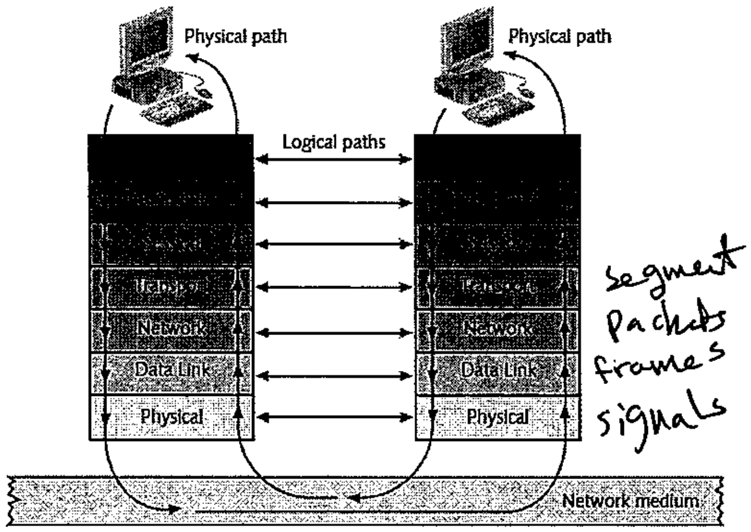


Figure 2.1 Flow of data through the OSI model

Mnemonics for the OSI Model

- Bottom Up
  - Please
  - Do
  - Not
  - Throw
  - Sausage
  - Pizza
  - Away
- Top Down
  - All
  - People
  - Seem
  - To
  - Need
  - Data
  - Processing

Application Layer

- Top (seventh) OSI model layer
- No software applications
- Protocol functions
  - Facilitates communication
    - Between software applications and lower-layer network services
  - Network interprets application request
  - Application interprets data sent from network

Presentation Layer

- Protocol functions
  - Accept Application layer data
  - Formats data to make it understandable to different applications and hosts
- Examples
  - Text encoding methods ASCII and ANSI
  - Compression methods like JPEG and MP3
  - Data encryption and decryption

Session Layer

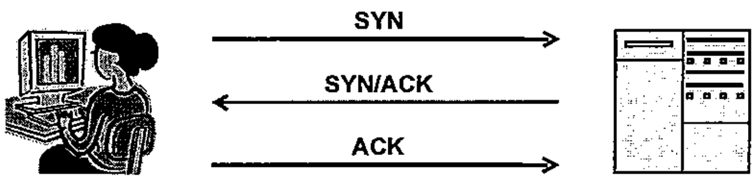
- Protocol functions
  - Coordinate and maintain communications between two nodes
- Session
  - Connection for ongoing data exchange between two parties
    - Example: between Web browser client and Web server
- Functions
  - Establishing and keeping alive communications link
    - For session duration
  - Determining if communications ended
    - Determining where to restart transmission
  - Terminating communications

Transport Layer

- Protocol functions
  - Accept data from Session layer
  - Provides **flow control**, **segmentation**, and **error control**
- Primary Transport Layer Protocols: **TCP and UDP**

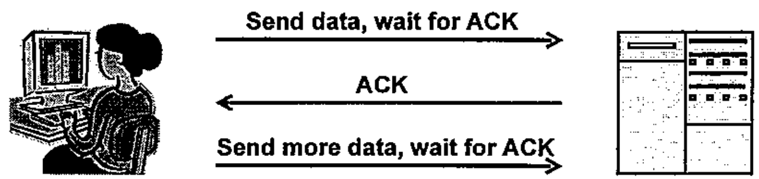
Transport Layer

- **TCP**
- Connection-oriented
  - Establishes a connection before transmitting data
  - Three-way handshake



Transport Layer

- **TCP**
  - Require acknowledgements from receiver to ensure data was received correctly
  - Checksum
    - Unique character string allowing receiving node to determine if arriving data unit exactly matches data unit sent by source
    - Ensures data integrity



Transport Layer

- **UDP**: A connectionless protocol
  - Do not establish connection with another node before transmitting data—no handshake
  - Make no effort to ensure data is delivered free of errors
  - Faster than connection-oriented protocol
  - Useful when data must be transferred quickly, such as streaming music or video

Transport Layer

- **Segmentation**
  - Breaking large data units received from Session layer into multiple smaller units called segments
  - Increases data transmission efficiency
- **MTU** (maximum transmission unit)
  - Largest data unit network will carry
  - Ethernet default: 1500 bytes
  - Discovery routine used to determine MTU

Transport Layer (cont'd.)

- Reassembly
  - Process of reconstructing segmented data units
- Sequencing
  - Method of identifying segments belonging to the same group of subdivided data

Transport Layer (cont'd.)

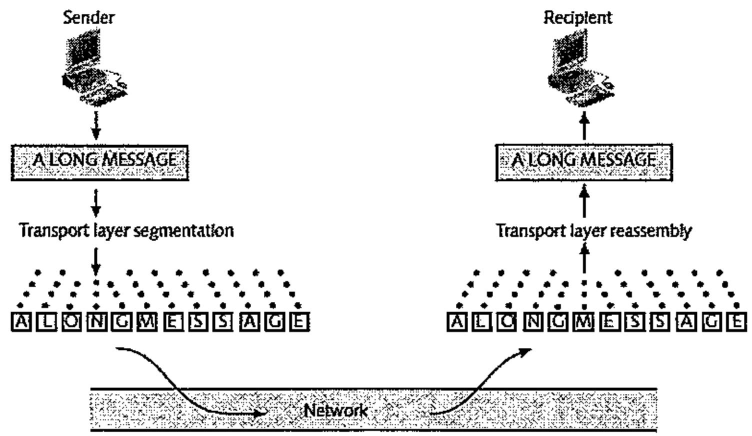


Figure 2-2 Segmentation and reassembly

Error in Textbook

- On page 50, the textbook says that the Network layer translates IP addresses like 147.144.51.121 into MAC addresses like 00-30-48-82-11-BD
- **That is false.** MAC addresses are used at layers 2 and 1 only. Layer 3 works with IP packets which have had the MAC addresses removed from them.

Network Layer

- Packet formation
  - Transport layer segment is encapsulated by a Network layer packet
    - Network layer adds logical addressing information—IP address
- Routing
  - Determine path from point A on one network to point B on another network
- Routing considerations
  - Delivery priorities, network congestion, quality of service, cost of alternative routes

Network Layer

- Common Network layer protocol
  - IP (Internet Protocol)
- Fragmentation
  - Network layer protocol (IP) subdivides Transport layer segments received into smaller packets
  - This is usually avoided by adjusting the Maximum Segment Size in the Transport layer, because it makes data transfer inefficient
    - Link Ch 2e

Data Link Layer

raw data	SMAC	DMAC	EC

- Function of protocols
  - Divide data received into distinct frames for transmission in Physical layer
  - Add Physical address to the frame: MAC addresses like 00-30-48-82-11-BD
- Frame
  - Structured package for moving data
    - Includes raw data (payload), sender's and receiver's physical addresses, error checking and control information

Data Link Layer (cont'd.)

- Frames may be damaged as they pass through the Physical layer, so the Data Link layer has error-checking
  - Error checking
    - Frame check sequence
    - CRC (cyclic redundancy check)
- Possible glut of communication requests
  - Data Link layer controls flow of information
    - Allows NIC to process data without error

Data Link Layer (cont'd.)

- Two Data Link layer sublayers
  - LLC (Logical Link Control) sublayer
  - MAC (Media Access Control) sublayer
- MAC address components
  - Block ID
    - Six-character sequence unique to each vendor
  - Device ID
    - Six-character number added at vendor's factory
- MAC addresses frequently depicted in hexadecimal format

Example of MAC Address

12 x

48

- Whole MAC address: 00-30-48-82-11-BD
  - Block ID
    - 00-30-48
    - Identifies the vendor
  - Device ID
    - 82-11-BD
    - Different for each NIC from the same vendor
- If two NICs have the same MAC address, they have problems networking
  - This can happen with cheaply made refurbished NICs, or with copied virtual machines

Data Link Layer (cont'd.)

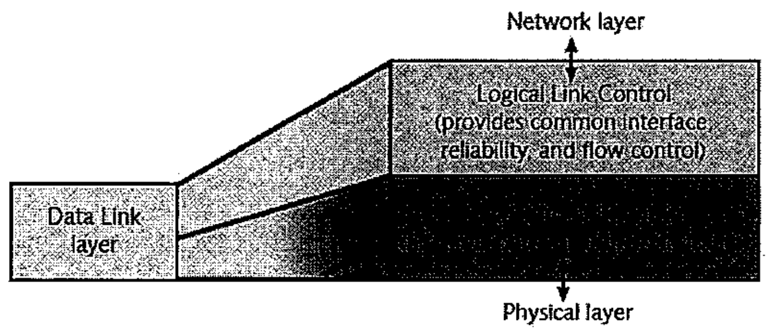


Figure 2-5 The Data Link layer and its sublayers

Data Link Layer (cont'd.)

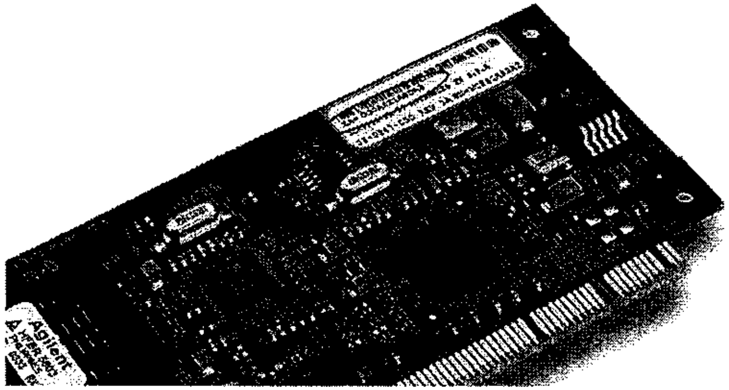
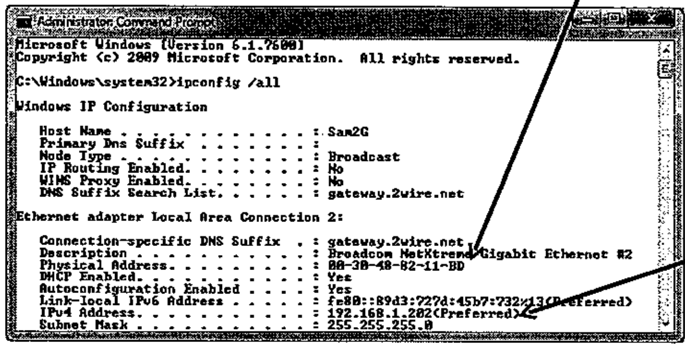


Figure 2-6 A NIC's Mac address

Finding Your MAC Address

- Start, CMD, Enter
- IPCONFIG /ALL
- Scroll up to see the first entry



Physical Layer

- Functions of protocols
  - Accept frames from Data Link layer
  - Generate signals as changes in voltage at the NIC
- Copper transmission medium
  - Signals issued as voltage
- Fiber-optic cable transmission medium
  - Signals issued as light pulses
- Wireless transmission medium
  - Signals issued as electromagnetic waves

Physical Layer (cont'd.)

- Physical layer protocols responsibility when receiving data
  - Detect and accept signals
  - Pass on to Data Link layer
  - Set data transmission rate
  - Monitor data error rates
  - No error checking
- Devices operating at Physical layer
  - Hubs and repeaters
- NICs operate at both Physical layer and Data Link layers

Applying the OSI Model

OSI model layer	Function
Application (layer 7)	Provides interface between software applications and network for interpreting applications' requests and requirements
Presentation (layer 6)	Allows hosts and applications to use a common language; performs data formatting, encryption, and compression
Session (layer 5)	Establishes, maintains, and terminates user connections
Transport (layer 4)	Ensures accurate delivery of data through flow control, segmentation and reassembly, error correction, and acknowledgment
Network (layer 3)	Establishes network connections; translates network addresses into their physical counterparts and determines routing
Data Link (layer 2)	Packages data in frames appropriate to network transmission method
Physical (layer 1)	Manages signaling to and from physical network connections

Table 2-1 Functions of the OSI layers

Communication Between Two Systems

- Data transformation
  - Original software application data differs from the bits sent onto the cable by the NIC
    - Header data added at each layer
- Each layer has a different data structure, called a **Protocol Data Unit (PDU)**
- **Segments**
  - Generated in Transport layer
  - Unit of data resulting from subdividing larger PDU from the Session layer
  - Addressed with TCP Ports (when using TCP)

Communication Between Two Systems (cont'd.)

- **Packets**
  - Generated in Network layer
  - Data with logical addressing information added to segments
  - Addressed with IP addresses
- **Frames**
  - Generated in Data Link layer
  - Composed of several smaller components or fields
  - Addressed with MAC addresses

Communication Between Two Systems (cont'd.)

- Encapsulation
  - Occurs in each layer
  - Process of wrapping one layer's PDU with protocol information
    - Allows interpretation by lower layer

Communication Between Two Systems (cont'd.)

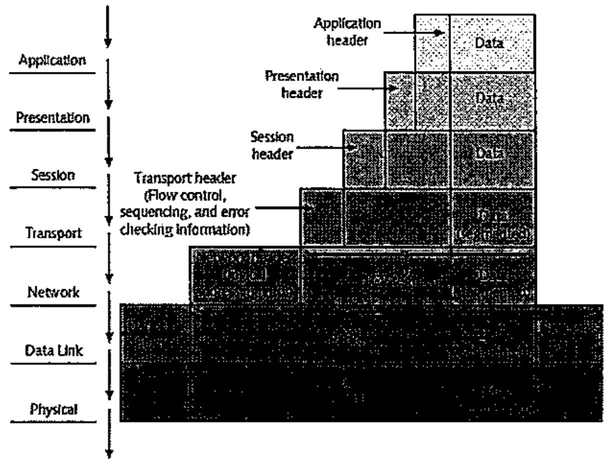


Figure 2-7 Data transformation through the OSI model

Frame Specifications

- Frames
  - Composed of several smaller components or fields
- Frame characteristic dependencies
  - Network type where frames run
  - Standards frames must follow
- Ethernet
  - Developed by Xerox
  - Four different types of Ethernet frames
  - Most popular: IEEE 802.3 standard

Frame Specifications (cont'd.)

- Token ring
  - Developed by IBM
  - Relies upon direct links between nodes and ring topology
  - Nearly obsolete
  - Defined by IEEE 802.5 standard
- Ethernet frames and token ring frames differ
  - Will not interact with each other
  - Devices cannot support more than one frame type per physical interface or NIC

IEEE Networking Specifications

- IEEE's Project 802
  - Effort to standardize physical and logical network elements
    - Frame types and addressing
    - Connectivity
    - Networking media
    - Error-checking algorithms
    - Encryption
    - Emerging technologies
- 802.3: Ethernet
- 802.11: Wireless

IEEE Networking Specifications (cont'd.)

Standard	Name	Topic
802.1	Internetworking	Routing, bridging, and network-to-network communications
802.2	Logical Link Control	Error and flow control over data frames
802.3	Ethernet LAN	All forms of Ethernet media and interfaces
802.5	Token ring LAN	All forms of token ring media and interfaces
802.11	Wireless Networks	Standards for wireless networking for many different broadcast frequencies and usage techniques
802.15	Wireless personal area networks	The coexistence of wireless personal area networks with other wireless devices in unlicensed frequency bands
802.16	Broadband wireless metropolitan area networks	The atmospheric interface and related functions associated with broadband wireless connectivity; also known as WiMAX
802.17	Resilient packet rings	Access method, physical layer specifications, and management of shared packet-based transmission on resilient rings (such as SONET)
802.20	Mobile broadband wireless network	Packet handling and other specifications for multivendor, mobile high-speed wireless transmission; nicknamed "mobile WiMAX"
802.22	Wireless regional area networks (WRAN)	Wireless, broadcast-style network to operate in the UHF/VHF frequency bands formerly used for TV channels

Table 2-2 IEEE 802 standards

COURSE TECHNOLOGY
CENGAGE Learning

Network+ Guide to Networks 5th Edition

Chapter 3
Transmission Basics and Networking Media

Objectives

- Explain basic data transmission concepts, including full duplexing, attenuation, latency, and noise
- Describe the physical characteristics of coaxial cable, STP, UTP, and fiber-optic media
- Compare the benefits and limitations of different networking media
- Explain the principles behind and uses for serial connector cables
- Identify wiring standards and the best practices for cabling buildings and work areas

Transmission Basics

- Transmit
  - Issue signals along network medium
- Transmission
  - Process of transmitting
  - Signal progress after transmitted
- Transceiver
  - Transmit and receive signals

Analog and Digital Signaling

- Important data transmission characteristic
  - Signaling type: analog or digital
- Volt
  - Electrical current pressure
- Electrical signal strength
  - Directly proportional to voltage
  - Signal voltage
- Signals
  - Current, light pulses, electromagnetic waves

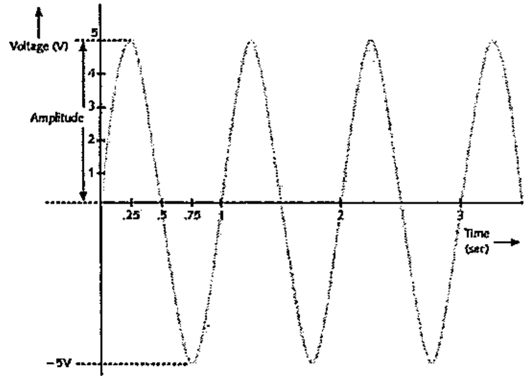


Figure 3-1: An example of an analog signal

- Analog data signals
  - Voltage varies continuously
  - Properties
    - Amplitude, frequency, wavelength, phase

Analog and Digital Signaling (cont'd.)

- Amplitude
  - Analog wave's strength
- Frequency
  - Number of times amplitude cycles over fixed time period
  - Measure in hertz (Hz)
- Wavelength
  - Distance between corresponding wave cycle points
  - Inversely proportional to frequency
  - Expressed in meters or feet

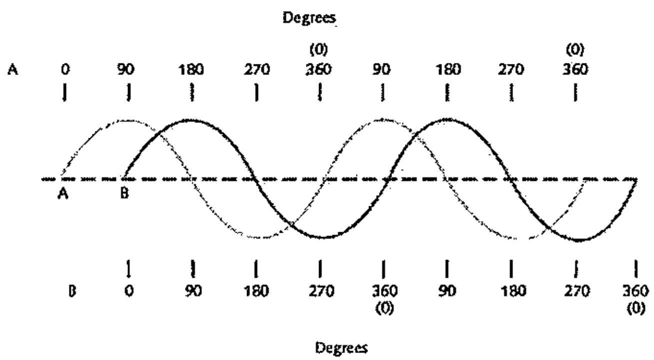


Figure 3-2: Waves with a 90-degree phase difference

- Phase
  - Wave's progress over time in relationship to fixed point

Analog and Digital Signaling (cont'd.)

- Analog signal benefit over digital
  - More variable
    - Convey greater subtleties with less energy
- Drawback of analog signals
  - Varied and imprecise voltage
    - Susceptible to transmission flaws
- Digital signals
  - Pulses of voltages
    - Positive voltage represents a 1
    - Zero voltage represents a 0

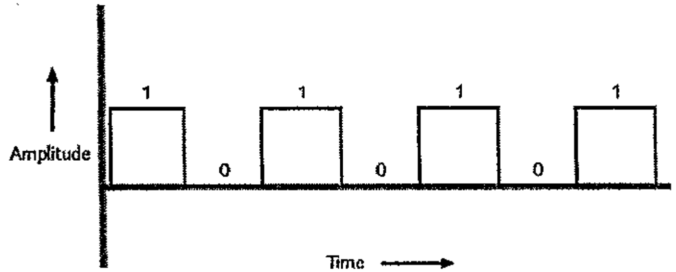


Figure 3-3 An example of a digital signal

- Binary system
  - 1s and 0s represent information
- Bit (binary digit)
  - Possible values: 1 or 0
  - Digital signal pulse

Bit position:	7	6	5	4	3	2	1	0
Binary exponential:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value if bit = 1:	128	64	32	16	8	4	2	1

Figure 3-4 Components of a byte

- Byte
  - Eight bits together
- Computers read and write information
  - Using bits and bytes
- Find decimal value of a bit
  - Multiply the 1 or 0 by 2^x (x equals bit's position)

Analog and Digital Signaling (cont'd.)

- Convert byte to decimal number
  - Determine value represented by each bit
  - Add values
- Convert decimal number to a byte
  - Reverse the process
- Convert between binary and decimal
  - By hand or calculator

Binary to Decimal conversion

- Binary numbers are sometimes written prefixed with 0b

- 0b0001 = 0*8 + 0*4 + 0*2 + 1*1 = 1
- 0b1010 = 1*8 + 0*4 + 1*2 + 0*1 = 10
- 0b1011 = 1*8 + 0*4 + 1*2 + 1*1 = 11

Decimal to Binary

- 14 = 8+4+2 = 1*8 + 1*4 + 1*2 + 0*1 = 0b1110
- 3 = 2+1 = 0*8 + 0*4 + 1*2 + 1*1 = 0b0011
- 6 = 4+2 = 0*8 + 1*4 + 1*2 + 0*1 = 0b0110

Larger Values

128= 1*128 + 0*64 + 0*32 +0*16 +0*8 +0*4 + 0*2 +0*1
128 = 0b10000000

162= 128 + 32 + 2
162= 1*128 + 0*64 + 1*32 +0*16 +0*8 +0*4 + 1*2 +0*1
162 = 0b10100010

0b1111000 =
1*128 + 1*64 + 1*32 +1*16 +0*8 +0*4 + 0*2 +0*1 0 =
128 + 64 + 32 +16 = 240

Binary on Quizzes

- I'll add a binary question to the next quiz, and maybe the one after that, as extra credit
- I recommend that you learn binary conversion, but I don't require it

Analog and Digital Signaling (cont'd.)

- Digital signal benefit over analog signal
  - More reliable
  - Less severe noise interference
- Digital signal drawback
  - Many pulses required to transmit same information
- Overhead
  - Nondata information
    - Required for proper signal routing and interpretation
    - Such as addressing information

Data Modulation

- Data relies on digital transmission
- Network connection may handle only analog signals
- Modem
  - Accomplishes translation
  - Modulator/demodulator
- Data modulation
  - Technology modifying analog signals
  - Make data suitable for carrying over communication path

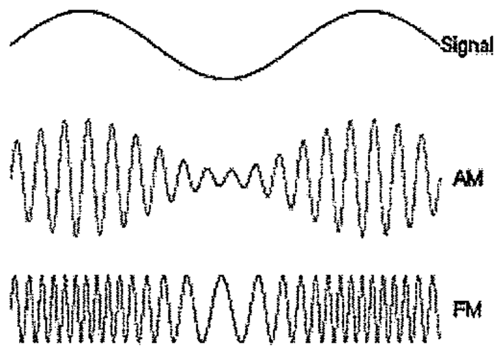
Data Modulation (cont'd.)

- Carrier wave
  - Combined with another analog signal
  - Produces unique signal
    - Transmitted from one node to another
  - Preset properties
  - Purpose
    - Convey information
- Information wave (data wave)
  - Added to carrier wave
  - Modifies one carrier wave property

Data Modulation (cont'd.)

- Frequency modulation (FM)
  - Carrier frequency modified
    - By application of data signal
- Amplitude modulation (AM)
  - Carrier signal amplitude modified
    - By application of data signal

AM and FM



- From link Ch 3a

Simplex, Half-Duplex, and Duplex

- Simplex
  - Signal transmission: one direction
  - Like broadcast TV
- Half-duplex transmission
  - Signal transmission: both directions
    - One at a time
  - One communication channel
    - Shared for multiple nodes to exchange information
- Full-duplex
  - Signals transmission: both directions simultaneously
  - Used on data networks

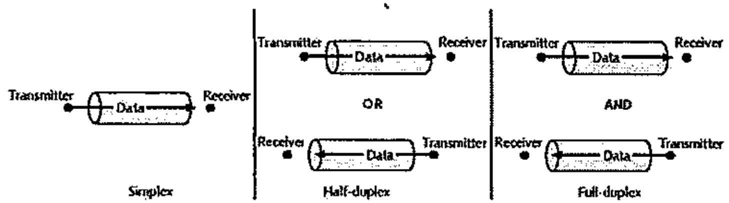


Figure 3-6 Simplex, half-duplex, and full duplex transmission

- Channel
  - Distinct communication path between nodes
  - Separated physically or logically
- Full duplex advantage
  - Increases speed

Multiplexing

- Multiplexing
  - Multiple signals
  - Travel simultaneously over one medium
- Subchannels
  - Logical multiple smaller channels
- Multiplexer (mux)
  - Combines many channel signals
- Demultiplexer (demux)
  - Separates combined signals
  - Regenerates them

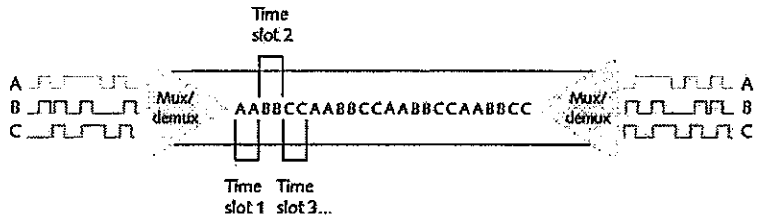


Figure 3-7 Time division multiplexing

- TDM (time division multiplexing)
  - Divides channel into multiple time intervals

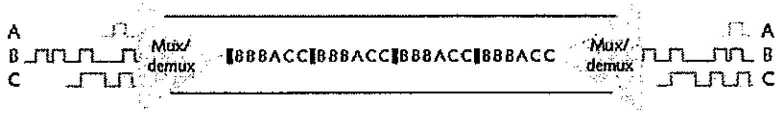


Figure 3-8 Statistical multiplexing

- Statistical multiplexing
  - Transmitter assigns slots to nodes
    - According to priority, need
  - More efficient than TDM

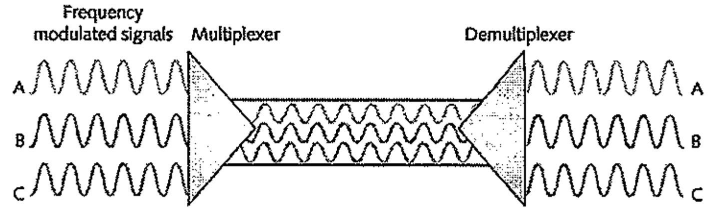


Figure 3-9 Frequency division multiplexing

- FDM (frequency division multiplexing)
  - Unique frequency band for each communications subchannel
  - Two types
    - Cellular telephone transmission
    - DSL Internet access

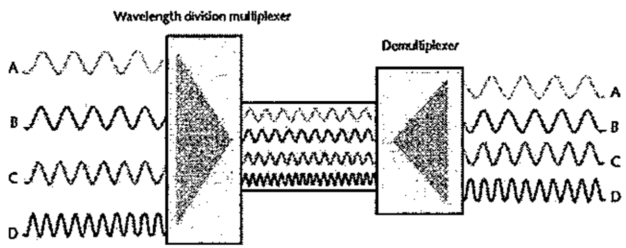


Figure 3-10 Wavelength division multiplexing

- WDM (wavelength division multiplexing)
  - One fiber-optic connection
  - Carries multiple light signals simultaneously
- DWDM (dense wavelength division multiplexing)
  - Used on most modern fiber-optic networks
  - Extraordinary capacity

Relationships Between Nodes

- Point-to-point transmission
  - One transmitter and one receiver
- Point-to-multipoint transmission
  - One transmitter and multiple receivers
  - **Broadcast transmission**
    - One transmitter and multiple, undefined receivers
    - Used on wired and wireless networks
      - Simple and quick
  - **Nonbroadcast**
    - One transmitter and multiple, defined receivers

Transmission Flaws

- Noise
  - Any undesirable influence degrading or distorting signal
- Types of noise
  - EMI (electromagnetic interference)
    - EMI/RFI (radiofrequency interference)
  - Cross talk
    - NEXT (near end cross talk)
    - Potential cause: improper termination
  - Environmental influences
    - Heat

Transmission Flaws (cont'd.)

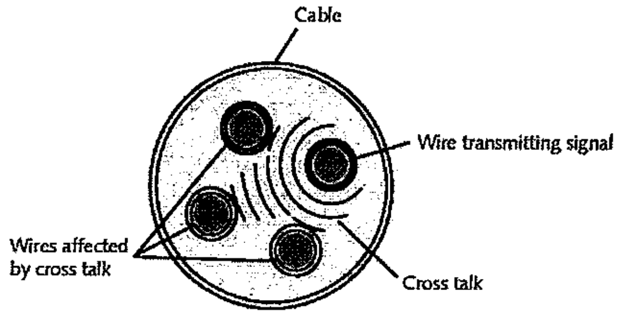


Figure 3-12 Cross talk between wires in a cable

Transmission Flaws (cont'd.)

- Attenuation
  - Loss of signal's strength as it travels away from source
- Signal boosting technology
  - Analog signals pass through amplifier
    - Noise also amplified
  - Regeneration
    - Digital signals retransmitted in original form
    - Repeater: device regenerating digital signals
  - Amplifiers and repeaters
    - OSI model Physical layer

Transmission Flaws (cont'd.)

- Latency
  - Delay between signal transmission and receipt
- Causes
  - Cable length
  - Intervening connectivity device
- RTT (round trip time)
  - Time for packet to go from sender to receiver, then back from receiver to sender
  - Measured in milliseconds
- May cause network transmission errors

Common Media Characteristics

- Selecting transmission media
  - Match networking needs with media characteristics
- Physical media characteristics
  - Throughput
  - Cost
  - Size and scalability
  - Connectors
  - Noise immunity

Throughput

- Most significant transmission method factor
- Causes of limitations
  - Laws of physics
  - Signaling and multiplexing techniques
  - Noise
  - Devices connected to transmission medium
- Fiber-optic cables allows faster throughput
  - Compared to copper or wireless connections

Cost

- Precise costs difficult to pinpoint
- Media cost dependencies
  - Existing hardware, network size, labor costs
- Variables influencing final cost
  - Installation cost
  - New infrastructure cost versus reuse
  - Maintenance and support costs
  - Cost of lower transmission rate affecting productivity
  - Cost of obsolescence

Noise Immunity

- Noise distorts data signals
  - Distortion rate dependent upon transmission media
    - Fiber-optic: least susceptible to noise
- Limit impact on network
  - Cable installation
    - Far away from powerful electromagnetic forces
  - Select media protecting signal from noise
  - Antinoise algorithms

Size and Scalability

- Three specifications
  - Maximum nodes per segment
  - Maximum segment length
  - Maximum network length
- Maximum nodes per segment dependency
  - Attenuation and latency
- Maximum segment length dependency
  - Attenuation and latency plus segment type

Size and Scalability (cont'd.)

- Segment types
  - Populated: contains end nodes
  - Unpopulated: No end nodes
    - Link segment
- Segment length limitation
  - After certain distance, signal loses strength
    - Cannot be accurately interpreted

Connectors and Media Converters

- Connectors
  - Hardware connecting wire to network device
  - Specific to particular media type
  - Affect costs
    - Installing and maintaining network
    - Ease of adding new segments or nodes
    - Technical expertise required to maintain network
- Media converter
  - Hardware enabling networks or segments running on different media to interconnect and exchange signals

Connectors and Media Converters (cont'd.)

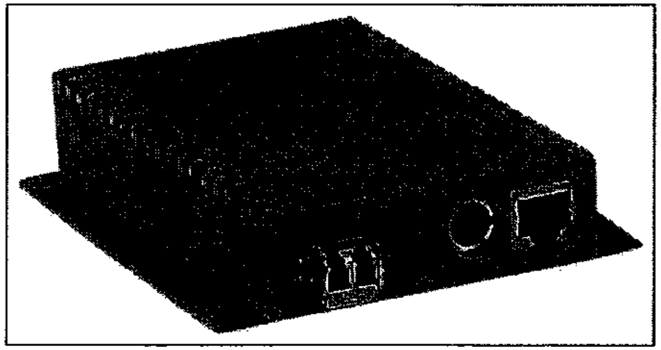


Figure 3-15 Copper wire-to-fiber media converter

Coaxial Cable

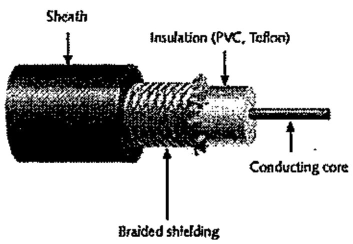


Figure 3-16 Coaxial cable

- Central metal core (often copper)
  - Surrounded by insulator
- Braided metal shielding (braiding or shield)
- Outer cover (sheath or jacket)

Coaxial Cable (cont'd.)

- High noise resistance
- Advantage over twisted pair cabling
  - Carry signals farther before amplifier required
- Disadvantage over twisted pair cabling
  - More expensive
- Hundreds of specifications
  - RG specification number
  - Differences: shielding and conducting cores
    - Transmission characteristics

Coaxial Cable (cont'd.)

- Conducting core
  - American Wire Gauge (AWG) size
- Data networks usage
  - RG-6: Used in modern cable TV connections, most common
  - RG-8: Thicknet--obsolete
  - RG-58: Thinnet—also obsolete for data networks
  - RG-59: Used for short spans in modern cable TV connections

Coaxial Cable (cont'd.)

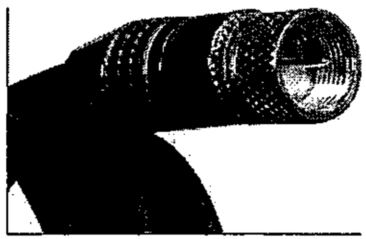


Figure 3-17 F-type connector

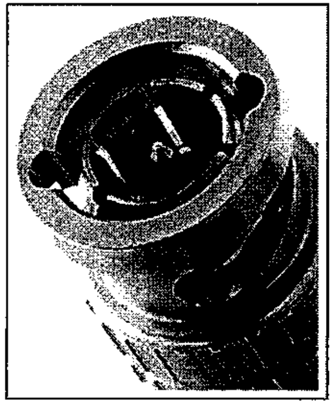


Figure 3-18 BNC Connector

Twisted Pair Cable

- Color-coded insulated copper wire pairs
  - 0.4 to 0.8 mm diameter
  - Encased in a plastic sheath

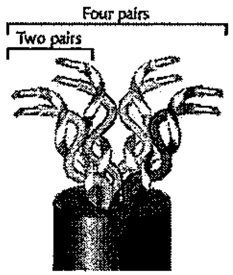


Figure 3-19 Twisted pair cable

Twisted Pair Cable (cont'd.)

- More wire pair twists per foot
  - More resistance to cross talk
  - Higher-quality
  - More expensive
- Twist ratio
  - Twists per meter or foot
- High twist ratio
  - Greater attenuation

Twisted Pair Cable (cont'd.)

- Hundreds of different designs
  - Dependencies
    - Twist ratio, number of wire pairs, copper grade, shielding type, shielding materials
  - 1 to 4200 wire pairs possible
- Wiring standard specification
  - TIA/EIA 568
- Twisted pair wiring types
  - Cat (category) 3, 4, 5, 5e, 6, and 6e, Cat 7
  - CAT 5 most often used in modern LANs

Twisted Pair Cable (cont'd.)

- Advantages
  - Relatively inexpensive
  - Flexible
  - Easy installation
  - Spans significant distance before requiring repeater
  - Accommodates several different topologies
  - Handles current faster networking transmission rates
- Two categories
  - STP (shielded twisted pair)
  - UTP (unshielded twisted pair)

STP (Shielded Twisted Pair)

- Individually insulated
- Surrounded by metallic substance shielding (foil)
  - Barrier to external electromagnetic forces
  - Contains electrical energy of signals inside
  - May be grounded

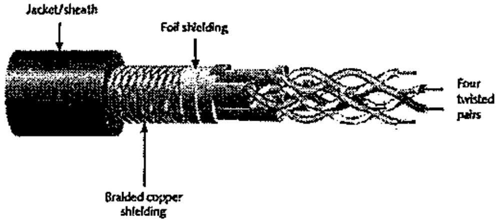


Figure 3-20 STP cable

UTP (Unshielded Twisted Pair)

- One or more insulated wire pairs
  - Encased in plastic sheath
  - No additional shielding
    - Less expensive, less noise resistance

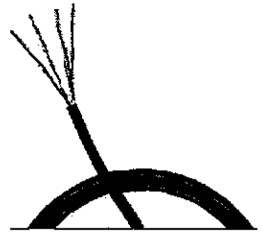


Figure 3-21 UTP cable

UTP (Unshielded Twisted Pair) (cont'd.)

- EIA/TIA standards
  - Cat 3 (Category 3)
  - Cat 4 (Category 4)
  - Cat 5 (Category 5)
  - Cat 5e (Enhanced Category 5)
  - Cat 6 (Category 6)
  - Cat 6e (Enhanced Category 6)
  - Cat 7 (Category 7)

UTP (Unshielded Twisted Pair) (cont'd.)

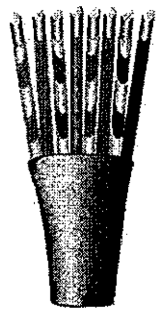


Figure 3-22 A Cat 5 UTP cable with pairs untwisted

Comparing STP and UTP

- Throughput
  - STP and UTP transmit the same rates
- Cost
  - STP and UTP vary
- Noise immunity
  - STP more noise resistant
  - UTP subject to techniques to offset noise
- Size and scalability
  - STP and UTP maximum segment length
    - 100 meters

Comparing STP and UTP (cont'd.)

- Connector
  - STP and UTP use RJ-45 (Registered Jack 45)
  - Telephone connections use RJ-11 (Registered Jack 11)

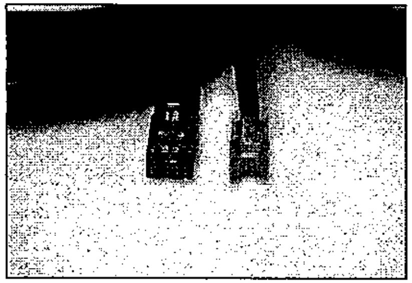
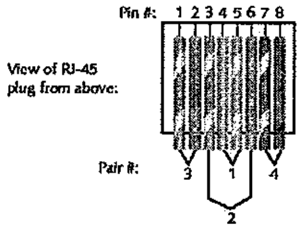


Figure 3-23 RJ-45 and RJ-11 connectors

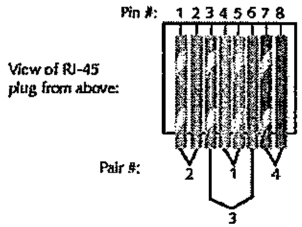
Terminating Twisted Pair Cable

- Patch cable
  - Relatively short cable
  - Connectors at both ends
- Proper cable termination techniques
  - Basic requirement for two nodes to communicate
- Poor terminations
  - Lead to loss or noise
- TIA/EIA standards
  - TIA/EIA 568A
  - TIA/EIA 568B



Pin #	Color	Pair #	Function
1	White with green stripe	3	Transmit +
2	Green	3	Transmit -
3	White with orange stripe	2	Receive +
4	Blue	1	Unused
5	White with blue stripe	1	Unused
6	Orange	2	Receive -
7	White with brown stripe	4	Unused
8	Brown	4	Unused

Figure 3-24 TIA/EIA 568A standard terminations



Pin #	Color	Pair #	Function
1	White with orange stripe	2	Transmit +
2	Orange	2	Transmit -
3	White with green stripe	3	Receive +
4	Blue	1	Unused
5	White with blue stripe	1	Unused
6	Green	3	Receive -
7	White with brown stripe	4	Unused
8	Brown	4	Unused

Figure 3-25 TIA/EIA 568B standard terminations

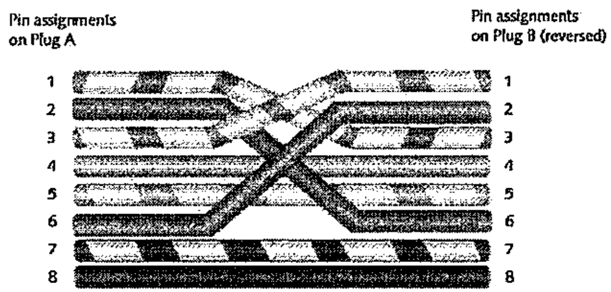


Figure 3-26 RJ-45 terminations on a crossover cable

- Straight-through cable
  - Terminate RJ-45 plugs at both ends identically
- Crossover cable
  - Transmit and receive wires on one end reversed

Terminating Twisted Pair Cable (cont'd.)

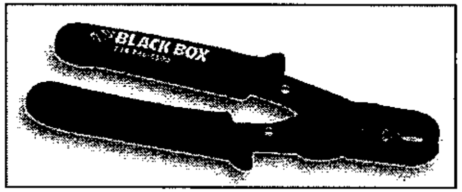


Figure 3-27 Wire cutter

- Termination tools
  - Wire cutter
  - Wire stripper
  - Crimping tool

Terminating Twisted Pair Cable (cont'd.)

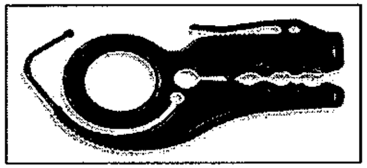


Figure 3-28 Wire stripper

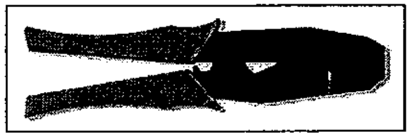


Figure 3-29 Crimping tool

- After making cables
  - Verify data transmit and receive

Fiber-Optic Cable

- Fiber-optic cable (fiber)
  - One (or several) glass or plastic fibers at its center (core)
- Data transmission
  - Pulsing light sent from laser
  - LED (light-emitting diode) through central fibers
- Cladding
  - Layer of glass or plastic surrounding fibers
  - Different density from glass or plastic in strands
  - Reflects light back to core
    - Allows fiber to bend

Fiber-Optic Cable (cont'd.)

- Plastic buffer
  - Outside cladding
  - Protects cladding and core
  - Opaque
    - Absorbs any escaping light
- Kevlar strands (polymeric fiber) surround plastic buffer
- Plastic sheath covers Kevlar strands

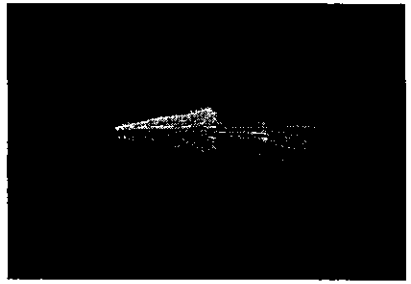


Figure 3-30 A fiber-optic cable

- Different varieties
  - Based on intended use and manufacturer
- Two categories
  - Single-mode
  - Multimode

SMF (Single-Mode Fiber)

- Uses narrow core (< 10 microns in diameter)
  - Laser generated light travels over one path
    - Little reflection
  - Light does not disperse
- Accommodates
  - Highest bandwidths, longest distances
  - Connects carrier's two facilities
- Costs prohibit typical LANs, WANs use

SMF (Single-Mode Fiber) (cont'd.)

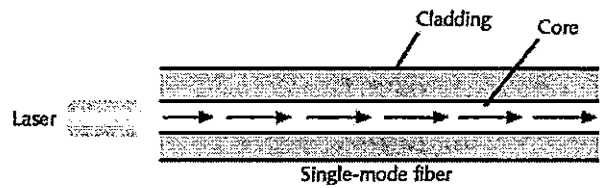


Figure 3-31 Transmission over single-mode fiber-optic cable

MMF (Multimode Fiber)

- Uses core with larger diameter than single-mode fiber
  - Common size: 62.5 microns
- Laser or LED generated light pulses travel at different angles
- Common uses
  - Cables connecting router to a switch
  - Cables connecting server on network backbone

MMF (Multimode Fiber) (cont'd.)

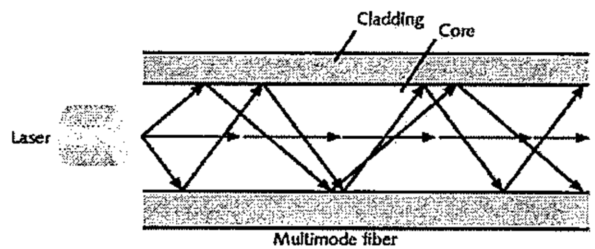


Figure 3-32 Transmission over multimode fiber-optic cable

MMF (Multimode Fiber) (cont'd.)

- Benefits
  - Extremely high throughput
  - Very high resistance to noise
  - Excellent security
  - Ability to carry signals for much longer distances before requiring repeaters than copper cable
  - Industry standard for high-speed networking
- Drawback
  - More expensive than twisted pair cable
  - Requires special equipment to splice

MMF (Multimode Fiber) (cont'd.)

- Throughput
  - Reliable transmission rates
    - Can reach 100 gigabits (or 100,000 megabits) per second per channel (but only for singlemode, not multimode)
- Cost
  - Most expensive transmission medium
- Connectors
  - ST (straight tip)
  - SC (subscriber connector or standard connector)
  - LC (local connector)
  - MT-RJ (mechanical transfer registered jack)

MMF (Multimode Fiber) (cont'd.)

- Noise immunity
  - Unaffected by EMI
- Size and scalability
  - Segment lengths vary
    - 150 to 40,000 meters
    - Due primarily to optical loss

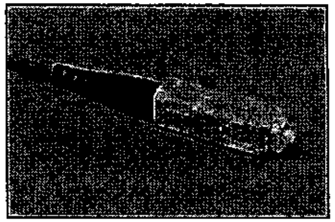


Figure 3-33 ST (straight tip) connector

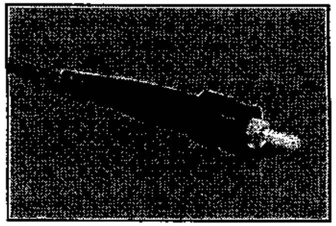


Figure 3-34 SC (subscriber connector or standard connector)

Figure 3-35 LC (local connector)

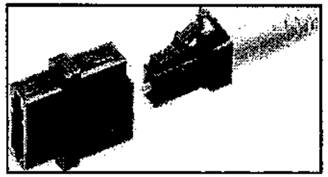


Figure 3-36 MT-RJ (mechanical transfer-register jack) connector

DTE (Data Terminal Equipment) and DCE (Data Circuit-Terminating Equipment) Connector Cables

- DTE (data terminal equipment)
  - Any end-user device
- DCE (data circuit-terminating equipment)
  - Device that processes signals
  - Supplies synchronization clock signal

DTE and DCE Connector Cables (cont'd.)

- DTE and DCE connections
  - Serial
    - Pulses flow along single transmission line
    - Sequentially
  - Serial cable
    - Carries serial transmissions

DTE and DCE Connector Cables (cont'd.)

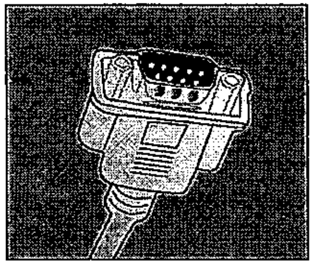


Figure 3-37 DB-9 connector

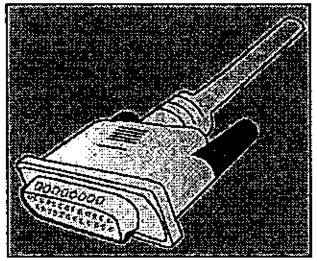


Figure 3-38 DB-25 connector

DTE and DCE Connector Cables (cont'd.)

- RS-232 (Recommended Standard 232)
  - EIA/TIA standard
  - Physical layer specification
    - Signal voltage, timing, compatible interface characteristics
  - Connector types
    - RJ-45 connectors, DB-9 connectors, DB-25 connectors
- RS-232 used between PC and router today
- RS-232 connections
  - Straight-through, crossover, rollover

Structured Cabling

- Cable plant
  - Hardware making up enterprise-wide cabling system
- Standard
  - TIA/EIA joint 568 Commercial Building Wiring Standard

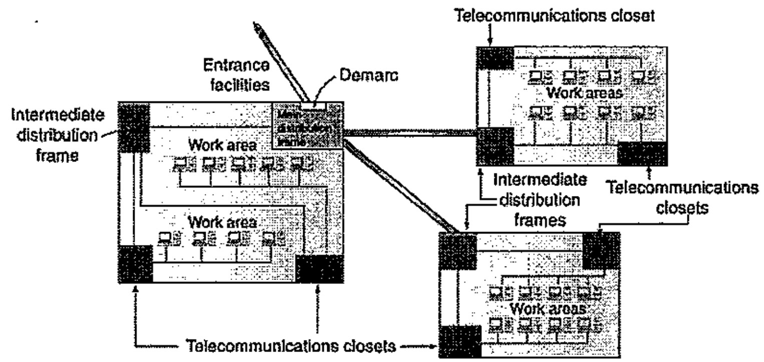


Figure 3-39 TIA/EIA structured cabling in an enterprise

Structured Cabling (cont'd.)

- Components
  - Entrance facilities
  - MDF (main distribution frame)
  - Cross-connect facilities
  - IDF (intermediate distribution frame)
  - Backbone wiring
  - Telecommunications closet
  - Horizontal wiring
  - Work area

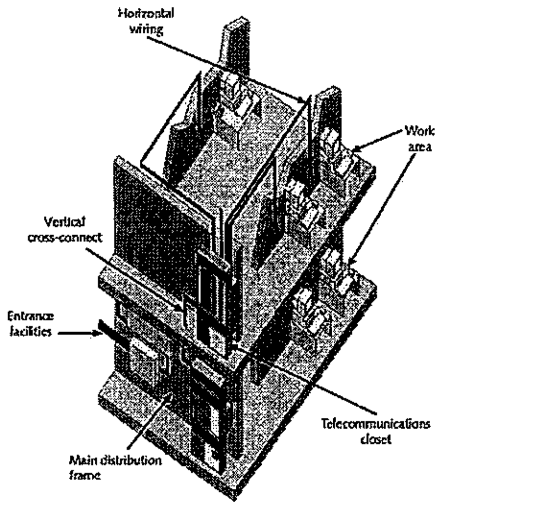


Figure 3-40 TIA/EIA structured cabling in a building

Structured Cabling (cont'd.)

Cable type	Cross-connects to telecommunications closet	MDF or IDF to telecommunications closet	Cross-connects to IDF or MDF
UTP	800 m (voice specification)	500 m	300 m
Single-mode fiber	3000 m	500 m	1500 m
Multimode fiber	2000 m	500 m	1500 m

Table 3-2 TIA/EIA specifications for backbone cabling

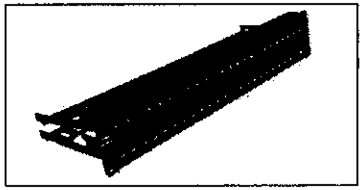


Figure 3-41 Patch panel

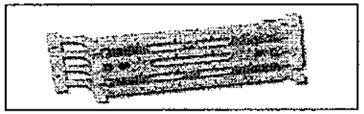


Figure 3-42 Patch panel

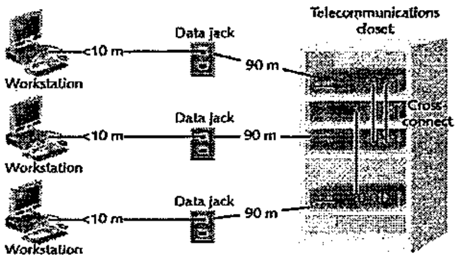


Figure 3-43 Horizontal wiring

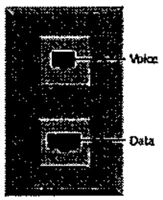


Figure 3-44 A standard TIA/EIA outlet

Best Practices for Cable Installation and Management

- Choosing correct cabling
  - Follow manufacturers' installation guidelines
  - Follow TIA/EIA standards
- Network problems
  - Often traced to poor cable installation techniques
- Installation tips to prevent Physical layer failures

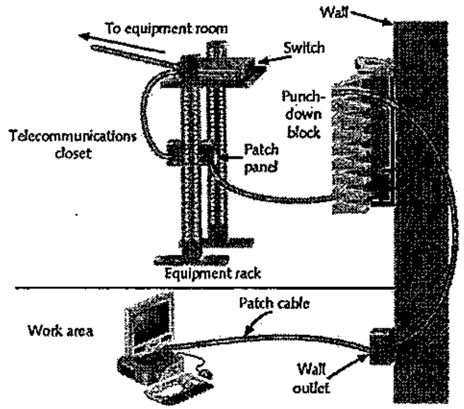


Figure 3-45 A typical UTP cabling installation

COURSE TECHNOLOGY
CENGAGE Learning

Network+ Guide to Networks 5th Edition

Chapter 4
Introduction to TCP/IP Protocols

Objectives

- Identify and explain the functions of the core TCP/IP protocols
- Explain how the TCP/IP protocols correlate to layers of the OSI model
- Discuss addressing schemes for TCP/IP in IPv4 and IPv6 protocols

Objectives (cont'd.)

- Describe the purpose and implementation of DNS (Domain Name System) and DHCP (Dynamic Host Configuration Protocol)
- Identify the well-known ports for key TCP/IP services
- Describe common Application layer TCP/IP protocols

Characteristics of TCP/IP (Transmission Control Protocol/ Internet Protocol)

- Protocol Suite
  - "TCP/IP"
  - Subprotocols
    - TCP, IP, UDP, ARP
- Developed by Department of Defense
  - ARPANET (1960s)
    - Internet precursor

Characteristics of TCP/IP (cont'd.)

- Popularity
  - Low cost
  - Communicates between dissimilar platforms
  - Open nature
  - Routable
    - Spans more than one LAN (LAN segment)
  - Flexible
    - Runs on combinations of network operating systems or network media
    - Disadvantage: requires more configuration

The TCP/IP Core Protocols

The TCP/IP Core Protocols

- TCP/IP suite subprotocols
- Operates in Transport or Network layers of OSI model
- Provide basic services to protocols in other layers
- Most significant protocols in TCP/IP
  - TCP
  - IP

TCP (Transmission Control Protocol)

- Transport layer protocol
- Provides reliable data delivery services
  - Connection-oriented subprotocol
    - Establish connection before transmitting, with the TCP Handshake
  - Sequencing and checksums
  - Flow control
    - Transmitter waits for ACK before sending more
- TCP segment format
  - Encapsulated by IP datagram in Network layer
    - Becomes IP datagram's "data"

TCP Segment

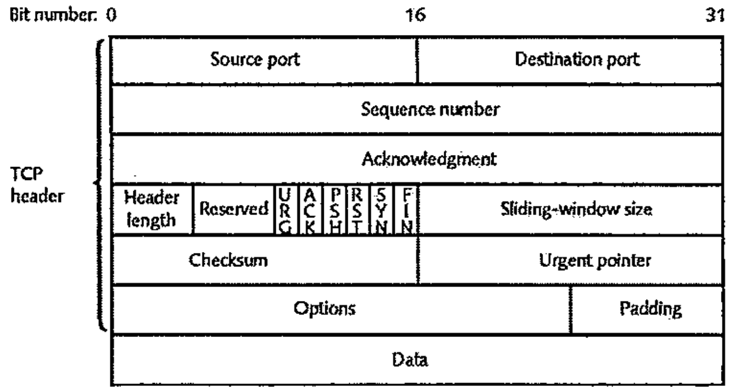


Figure 4-1 A TCP segment

Important TCP Header Fields

- Flags, especially SYN and ACK
  - Indicates purpose of segment
- Source Port and Destination Port
  - Guides data to the correct process on the destination computer
- SEQ number and ACK number
  - Used to arrange segments in the correct order

TCP Handshake

- Computer A sends SYN to Computer B
  - SYN flag set
    - SEQ field: Random initial sequence number (ISN)
    - ACK field: Empty (zeroes)
- Computer B replies with SYN/ACK
  - SYN and ACK flags set
    - SEQ field: Computer B's random initial sequence number (ISN)
    - ACK field: Computer A's ISN plus 1
- Computer A responds with ACK
  - ACK flag set
    - SEQ field: Computer A's ISN plus 1
    - ACK field: Computer B's ISN plus 1

Ending a TCP Session

- FIN flag indicates transmission end

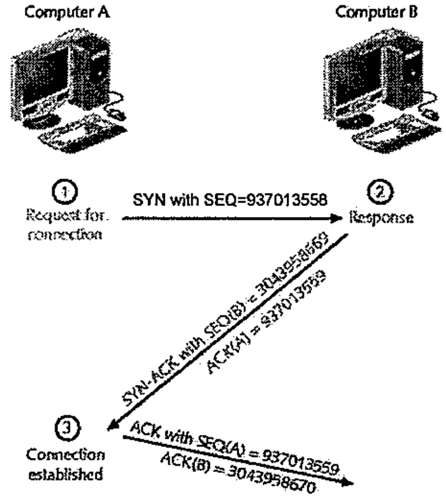
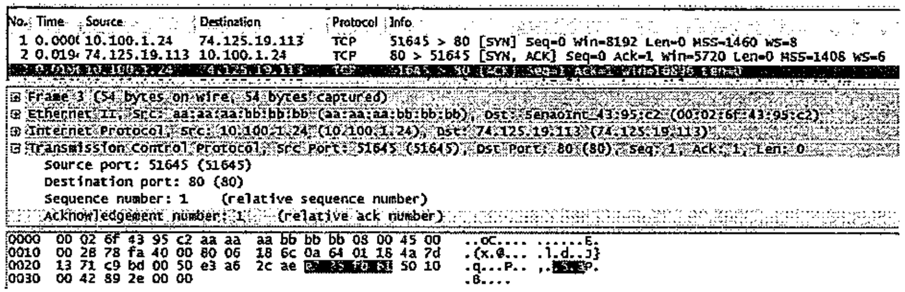


Figure 4-3 Establishing a TCP connection

Wireshark Demonstration

- Relative SEQ and ACK numbers at top
- Absolute SEQ and ACK values at bottom, in hexadecimal



UDP (User Datagram Protocol)

- Transport layer protocol
- Provides unreliable data delivery services
  - Connectionless transport service
    - No assurance packets received in correct sequence
    - No guarantee packets received at all
    - No error checking, sequencing
  - Lacks sophistication
    - More efficient than TCP
- Useful situations
  - Great volume of data transferred quickly

UDP (cont'd.)

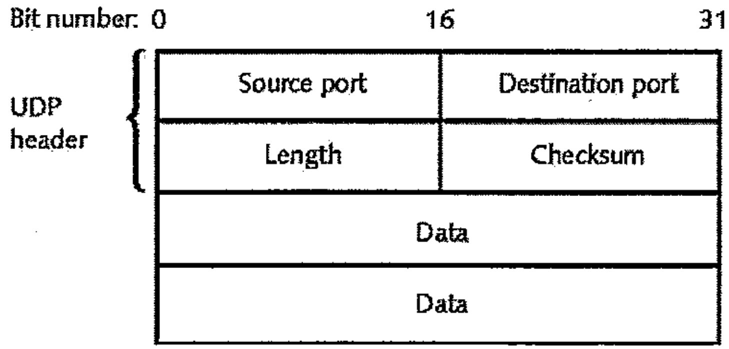


Figure 4-4 A UDP segment

IP (Internet Protocol)

- Network layer protocol
  - Routes packets using IP addresses
- Enables TCP/IP to internetwork
  - **Routers** move IP packets move from one network to another
- Unreliable, connectionless protocol
  - No guaranteed data delivery, no handshake
- Some higher level protocols provide reliability, like TCP

IP (cont'd.)

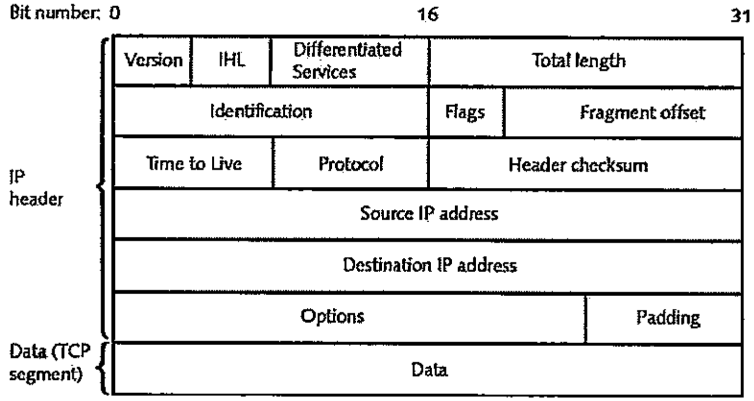


Figure 4-5 An IP datagram

Important IP Header Fields

- TTL (Time to Live)
  - Decreases by one for each router the packet passes through (a "hop")
  - When TTL reaches zero, the packet is discarded
- Source Destination IP Addresses
  - Used to deliver packet and response

ICMP (Internet Control Message Protocol)

- Network layer protocol
  - Reports on data delivery success/failure
- Announces transmission failures to sender
  - Network congestion
  - Data fails to reach destination
  - Data discarded: TTL expired
- ICMP cannot correct errors
  - Provides critical network problem troubleshooting information

IGMP (Internet Group Management Protocol)

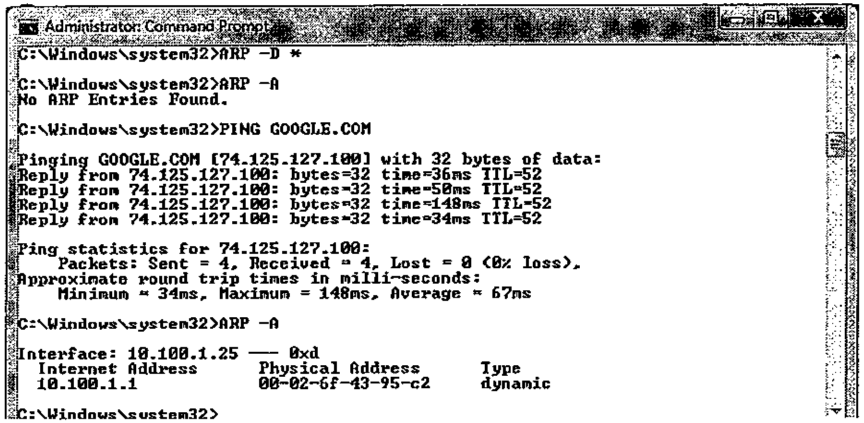
- Network layer protocol
- Manages multicasting
  - Allows one node to send data to defined group of nodes
- Uses
  - Internet teleconferencing
  - Routers sending traffic reports to each other

ARP (Address Resolution Protocol)

- Network layer protocol
- Obtains a MAC address from an IP address
- ARP table (ARP cache)
  - Computers store recently-used MAC-to-IP address mappings
  - Increases efficiency
- Controlled by ARP command

ARP Demonstration

- ARP -D *
  - Clears the ARP cache
- ARP -A
  - Shows the ARP cache



```
Administrator: Command Prompt
C:\Windows\system32>ARP -D *

C:\Windows\system32>ARP -A
No ARP Entries Found.

C:\Windows\system32>PING GOOGLE.COM

Pinging GOOGLE.COM [74.125.127.100] with 32 bytes of data:
Reply from 74.125.127.100: bytes=32 time=36ms TTL=52
Reply from 74.125.127.100: bytes=32 time=50ms TTL=52
Reply from 74.125.127.100: bytes=32 time=148ms TTL=52
Reply from 74.125.127.100: bytes=32 time=34ms TTL=52

Ping statistics for 74.125.127.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 148ms, Average = 67ms

C:\Windows\system32>ARP -A

Interface: 10.100.1.25 --- 0xd
  Internet Address      Physical Address      Type
  10.100.1.1            00-02-6f-43-95-c2     dynamic

C:\Windows\system32>
```

RARP (Reverse Address Resolution Protocol)

- Converts MAC address to IP Address
  - Obsolete—replaced by DHCP

IPv4 Addressing

IPv4 Addressing

- Networks recognize two addresses
  - Logical (Network layer)
  - Physical (MAC, hardware) addresses
- IP protocol handles logical addressing
- Specific parameters
  - Unique 32-bit number
    - Divided into four octets (sets of eight bits)
    - Separated by periods
- Example: 144.92.43.178

IPv4 Addressing (cont'd.)

Network class	Beginning octet	Number of networks	Maximum addressable hosts per network
A	1–126	126	16,777,214
B	128–191	>16,000	65,534
C	192–223	>2,000,000	254

Table 4-1 Commonly used TCP/IP classes

- IP address information
  - Network Class determined by first octet
    - Class A, Class B, Class C

IPv4 Addressing (cont'd.)

- Class D, Class E rarely used (never assign)
  - Class D: value between 224 and 230
    - Multicasting
  - Class E: value between 240 and 254
    - Experimental use
- Eight bits have 256 combinations
  - Networks use 1 through 254
  - 0: reserved as placeholder
    - 10.0.0.0
  - 255: reserved for broadcast transmission
    - 255.255.255.255

IPv4 Addressing (cont'd.)

- Class A devices
  - Share same first octet (bits 0-7)
    - Network ID
  - Host: second through fourth octets (bits 8-31)
- Class B devices
  - Share same first two octet (bits 0-15)
  - Host: second through fourth octets (bits 16-31)
- Class C devices
  - Share same first three octet (bits 0-23)
  - Host: second through fourth octets (bits 24-31)

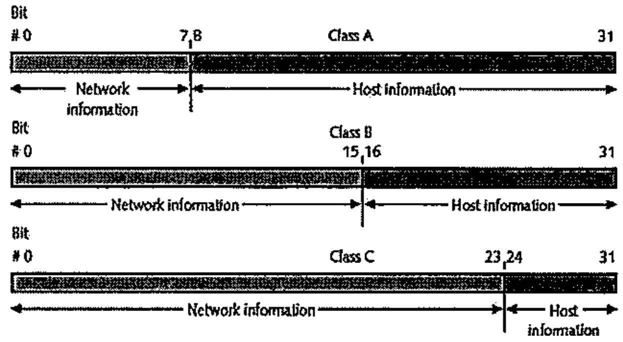


Figure 4-8 IP addresses and their classes

- Running out of addresses
  - IPv6 incorporates new addressing scheme

IPv4 Addressing (cont'd.)

- Loop back address
  - First octet equals 127 (127.0.0.1)
- Loopback test
  - Attempting to connect to own machine
  - Powerful troubleshooting tool
- Windows XP, Vista
  - **`ipconfig`** command
- Unix, Linux
  - **`ifconfig`** command

IPv4 Addressing (cont'd.)

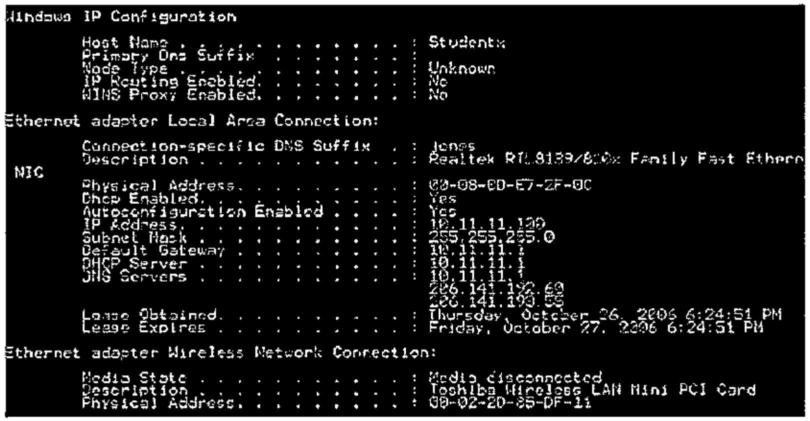


Figure 4-9 Results of the `ipconfig /all` command on a Windows XP or Windows Vista workstation

IPv4 Addressing (cont'd.)

Figure 4-10 Results of the `ifconfig -a` command on a UNIX workstation

Binary and Dotted Decimal Notation

- Decimal number between 0 and 255 represents each binary octet
- Period (dot) separates each decimal
- Dotted decimal address has binary equivalent
  - Converting each octet
  - Remove decimal points

Subnet Mask

- Identifies every device on TCP/IP-based network
- 32-bit number (net mask)
  - Identifies device's subnet
    - Combines with device IP address
    - Informs network about segment, network where device attached
- Four octets (32 bits)
  - Expressed in binary or dotted decimal notation
- Assigned same way as IP addresses
  - Manually, or automatically (via DHCP)

Network class	Beginning octet	Default subnet mask
A	1–126	255.0.0.0
B	128–191	255.255.0.0
C	192–223	255.255.255.0

Table 4-2 Default subnet masks

- Subnetting
  - Subdividing network single class into multiple, smaller logical networks (segments)
    - Control network traffic
    - Make best use of limited number of IP addresses
  - Subnet mask varies depending on subnetting
- Nonsubnetted networks use defaults

Assigning IP Addresses

Assigning IP Addresses

- Government-sponsored organizations
  - Dole out IP address blocks to companies
  - IANA, ICANN, RIRs
- Companies, individuals
  - Obtain IP addresses from ISPs
- Every network node must have unique IP address
  - Otherwise it cannot send or receive Internet packets

Static and Automatic IP Address Assignment

- Static IP address
  - Manually typed into each device
  - Modify client workstation TCP/IP properties
    - Only way to change
  - Human error cause duplicates
- Automatic IP addressing
  - BOOTP and DHCP
  - Reduce duplication error

BOOTP (Bootstrap Protocol)

- Mid-1980s
- Application layer protocol
- Central list
  - IP addresses, associated devices' MAC addresses
  - Assign client IP addresses dynamically
- Dynamic IP address
  - Assigned to device upon request
  - Changeable

BOOTP (cont'd.)

- BOOTP process
  - Client connects to network
  - Sends broadcast message asking for IP address
    - Includes client's NIC MAC address
  - BOOTP server looks up client's MAC address in BOOTP table
  - Responds to client
    - Client's IP address
    - Server IP address
    - Server host name
    - Default router IP address

BOOTP (cont'd.)

- Process resembles RARP
  - Difference
    - RARP requests, responses not routable
    - RARP only capable of issuing IP address to client
    - BOOTP may issue additional information (client's subnet mask)
- BOOTP surpassed by DHCP (Dynamic Host Configuration Protocol)
  - More sophisticated IP addressing utility
  - DHCP requires little intervention
    - BOOTP difficult to maintain on large networks

DHCP (Dynamic Host Configuration Protocol)

- Assigns network device unique IP address
  - Automatically
- Application layer protocol
- Developed by IETF (BOOTP replacement)
- Operation
  - Similar to BOOTP
  - Lower administrative burden
    - Administrator does not maintain table
  - Requires DHCP service on DHCP server

Reasons to Use DHCP

- Saves time spent assigning IP addresses
- Prevents accidental duplicate IP addresses
- Allows users to move devices (like laptops) without having to change their TCP/IP configuration

DHCP Leasing Process

- Device borrows (leases) IP address
  - Devices use IP address temporarily
    - Specified time limit
- Lease time
  - Determine when client obtains IP address at log on
  - User may force lease termination
- DHCP service configuration
  - Specify leased address range
  - Configure lease duration
- Several steps to negotiate client's first lease

DHCP Leasing Process (cont'd.)

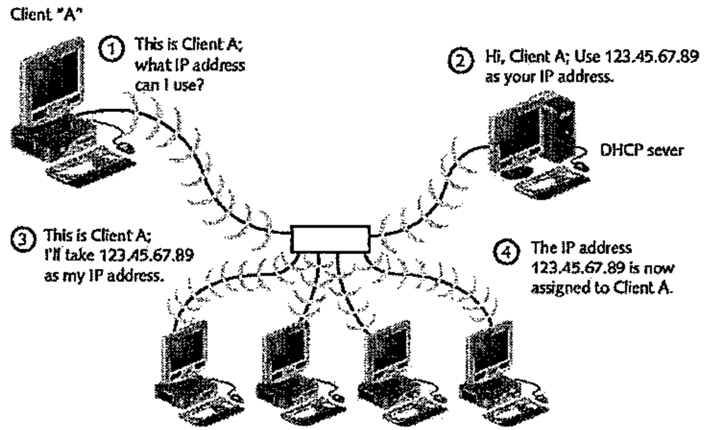


Figure 4-11 The DHCP leasing process

Terminating a DHCP Lease

- Lease expiration
  - Automatic
    - Established in server configuration
  - Manually terminated at any time
    - Client's TCP/IP configuration
    - Server's DHCP configuration
- Circumstances requiring lease termination
  - DHCP server fails and replaced
    - Windows: release of TCP/IP settings
- DHCP services run on several server types
  - Installation and configurations vary

APIPA (Automatic Private IP Addressing)

- Client cannot communicate without valid IP address
- What if DHCP server not running?
  - Microsoft Windows offers Automatic Private IP Addressing
    - Provides IP address automatically
- IANA (Internet Assigned Numbers Authority) reserved predefined pool of addresses
  - 169.254.0.0 through 169.254.255.255

APIPA (cont'd.)

- APIPA
  - Assigns a random IP address from the 169.254.y.x range
  - Assigns default Class B subnet mask
    - 255.255.0.0
- Disadvantage
  - Computer only communicates with other nodes using addresses in APIPA range
  - Cannot normally connect to the Internet with a 169.254.y.z address

APIPA (cont'd.)

- APIPA suitable use
  - Small networks: no DHCP servers
- APIPA unsuitable use
  - Networks communicating with other subnets, WAN
- APIPA enabled by default: OK
  - First checks for DHCP server
    - Allows DHCP server to assign addresses
  - Does not reassign new address if static
  - Works with DHCP clients
  - Disabled in registry

IPv6 Addressing

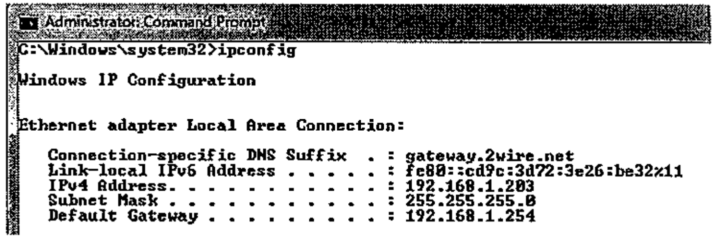
IPv6 Addressing

- IP next generation (IPng)
  - Replacing IPv4 (gradually)
- IPv6 support
  - Most new applications, servers, network devices
- Delay in implementation
  - Cost of upgrading infrastructure
- IPv6 advantages
  - More efficient header, better security, better prioritization provisions, automatic IP address configuration
  - Billions of additional IP addresses

IPv6 Addressing (cont'd.)

- Difference between IPv4 and IPv6 addresses
  - Size
    - IPv4: 32 bits
    - IPv6: eight 16-bit fields (128 bits)
    - IPv6: 2^{96} (4 billion times 4 billion times 4 billion) available IP addresses
  - Representation
    - IPv4: binary numbers separated by period
    - IPv6: hexadecimal numbers separated by colon
    - IPv6 shorthand: "::" any number of multiple, zero-value fields

Demo: IPv6 Addresses in Windows 7



- US Government requires IPv6 compatibility on its devices now
  - Links Ch 4f, 4g

IPv6 Addressing (cont'd.)

- Difference between IPv4 and IPv6 addresses (cont'd.)
  - Representation (cont'd.)
    - IPv6 loopback address is 0:0:0:0:0:0:0:1
    - Abbreviated loopback address ::1
  - Scope
    - IPv6 addresses can reflect scope of transmission's recipients
    - Unicast address represents single device interface
    - Multicast address represents multiple interfaces (often on multiple devices)

IPv6 Addressing (cont'd.)

- Difference between IPv4 and IPv6 addresses (cont'd.)
  - Scope (cont'd.)
    - Anycast address represents any one interface from a group of interfaces
    - Any one can accept transmission
  - Format Prefix (IPv6)
    - Beginning of address
    - Variable-length field
    - Indicates address type: unicast, multicast, anycast

Sockets and Ports

Sockets and Ports

- Processes assigned unique port numbers
- Process's socket
  - Port number plus host machine's IP address
- Port numbers
  - Simplify TCP/IP communications
  - Ensures data transmitted correctly
- Example
  - Telnet port number: 23
  - IPv4 host address: 10.43.3.87
  - Socket address: 10.43.3.87:23

Sockets and Ports (cont'd.)

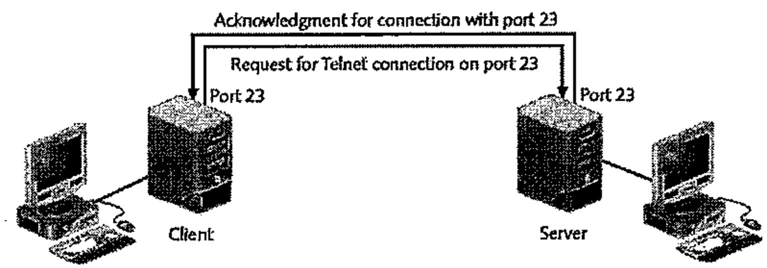


Figure 4-12 A virtual connection for the Telnet service

Sockets and Ports (cont'd.)

- Port number range: 0 to 65535
- Three types
  - Well Known Ports
    - Range: 0 to 1023
    - Operating system or administrator use
  - Registered Ports
    - Range: 1024 to 49151
    - Network users, processes with no special privileges
  - Dynamic and/or Private Ports
    - Range: 49152 through 65535
    - No restrictions

Sockets and Ports (cont'd.)

Port number	Process name	Protocol used	Description
20	FTP-DATA	TCP	File transfer—data
21	FTP	TCP	File transfer—control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP and UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP and UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

Table 4-3 Commonly used TCP/IP port numbers

Using Non-Standard Ports

- A server could be configured to use an unusual port, such as a Web server on port 8080
    - Not good idea: standards violation
  - Sometimes done for security or testing

Host Names and DNS (Domain Name System)

Host Names and DNS (Domain Name System)

- TCP/IP addressing
  - Long, complicated numbers
  - Good for computers
- People remember words better
  - Internet authorities established Internet node naming system
- Host
  - Internet device
- Host name
  - Name describing device

Domain Names

- Domain
  - Group of computers belonging to same organization
  - Share common part of IP address
- Domain name
  - Identifies domain (loc.gov)
  - Associated with company, university, government organization
- Fully qualified host name (jasmine.loc.gov)
  - Local host name plus domain name

Domain suffix	Type of organization
ARPA	Reverse lookup domain (special Internet function)
COM	Commercial
EDU	Educational
GOV	Government
ORG	Noncommercial organization (such as a nonprofit agency)
NET	Network (such as an ISP)
INT	International Treaty Organization
MIL	United States military organization
BIZ	Businesses
INFO	Unrestricted use
AERO	Air-transport industry
COOP	Cooperatives
MUSEUM	Museums
NAME	Individuals
PRO	Professionals such as doctors, lawyers, and engineers

Table 4-4 Top-level domains

Domain Names (cont'd.)

- Label (character string)
  - Separated by dots
  - Represents level in domain naming hierarchy
- Example: www.google.com
  - Top-level domain (TLD): com
  - Second-level domain: google
  - Third-level domain: www
- Second-level domain
  - May contain multiple third-level domains
- ICANN established domain naming conventions

Domain Names (cont'd.)

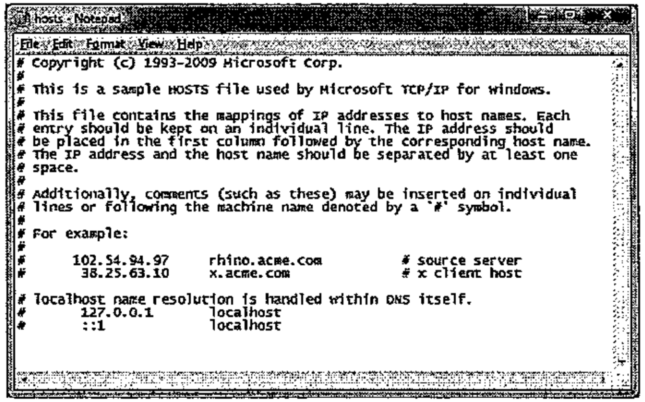
- ICANN approved over 240 country codes
- Host and domain names restrictions
  - Any alphanumeric combination up to 63 characters
  - Include hyphens, underscores, periods in name
  - No other special characters

Hosts Files

- ARPAnet used HOSTS.TXT file
  - Associated host names with IP addresses
  - Host matched by one line
    - Identifies host's name, IP address
    - Alias provides nickname
- UNIX-/Linux-based computer
  - Host file called hosts, located in the /etc directory
- Windows 9x, NT, 2000, XP, Vista computer
  - Host file called hosts
  - Located in %systemroot%\system32\drivers\etc folder

Windows Hosts File

- Rarely used, but still present



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

DNS (Domain Name System)

- Hierarchical Distributed Database
  - Associates domain names with IP addresses
- DNS refers to:
  - Application layer service accomplishing association
  - Organized system of computers; databases making association possible
- DNS redundancy
  - Many computers across globe related in hierarchical manner
  - Root servers
    - 13 computers (ultimate authorities)

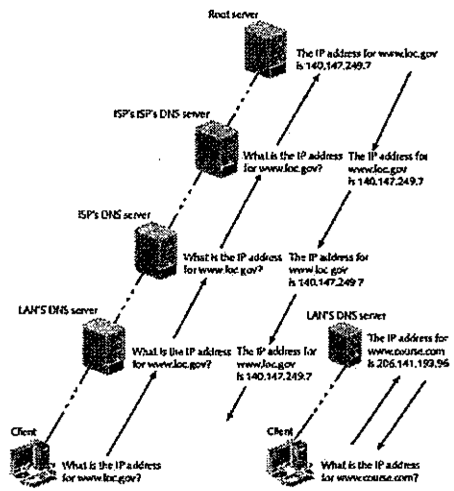


Figure 4-14 Domain name resolution

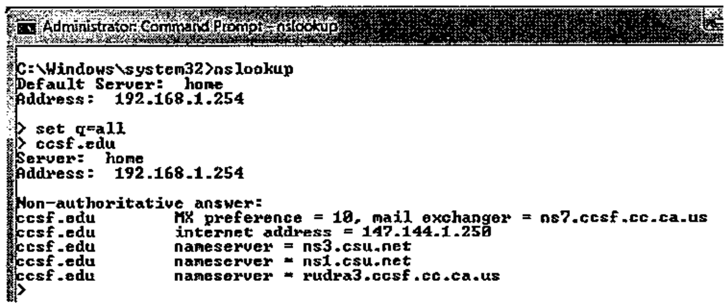
Name servers (DNS servers)

- Servers that contain databases of associated names, IP addresses
- Provide information on request
  - To convert names like **www.ccsf.edu** into IP addresses like **147.144.1.212**
- This process is called **name resolution**

DNS (cont'd.)

- Resource record
  - Describes one piece of DNS database information
  - Many different types
    - Dependent on function
  - Contents
    - Name field
    - Type field
    - Class field
    - Time to Live field
    - Data length field
    - Actual data

Demo: CCSF's Name Servers



Configuring DNS

- Large organizations
  - Often maintain two name servers
    - Primary and secondary
  - Ensures Internet connectivity
- Each device must know how to find server
  - Automatically by DHCP
  - Manually configure workstation TCP/IP properties

Configuring DNS (cont'd.)

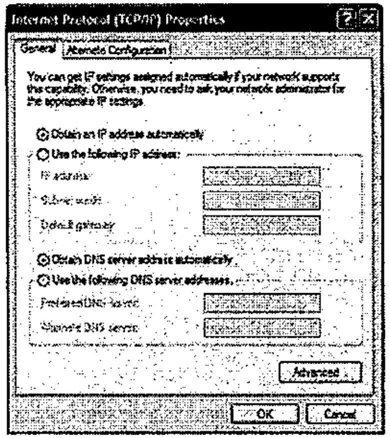


Figure 4-15 Windows XP Internet Protocol (TCP/IP) Properties dialog box

DDNS (Dynamic DNS)

- Allows a user to host a Web site on a computer with a dynamic IP address
- Process
  - Service provider runs program on user's computer
    - Notifies service provider when IP address changes
  - Service provider's server launches routine to automatically update DNS record
    - Effective throughout Internet in minutes
- Not as good as a real static IP address
- Larger organizations pay for statically assigned IP address

Application Layer Protocols

Application Layer Protocols

- Work over TCP or UDP plus IP
  - Translate user requests
    - Into format readable by network
- HTTP
  - Application layer protocol central to using Web
- BOOTP and DHCP
  - Automatic address assignment

Telnet

- Terminal emulation protocol
  - Log on to remote hosts
    - Using TCP/IP protocol suite
  - TCP connection established
    - Keystrokes on user's machine act like keystrokes on remotely connected machine
- Often connects two dissimilar systems
- Can control remote host
- Drawback
  - Notoriously insecure

FTP (File Transfer Protocol)

- Send and receive files via TCP/IP
- Host running FTP server portion
  - Accepts commands from host running FTP client
- FTP commands
  - Operating system's command prompt
    - No special client software required
- FTP hosts allow anonymous logons
- After connected to host
  - Additional commands available
  - Type `help`

FTP (cont'd.)

- Graphical FTP clients
  - MacFTP, WS_FTP, CuteFTP, SmartFTP
    - Rendered command-line method less common
- FTP file transfers directly from modern Web browser
  - Point browser to FTP host
  - Move through directories, exchange files
- SFTP
  - More secure

TFTP (Trivial File Transfer Protocol)

- Enables file transfers between computers
  - Simpler (more trivial) than FTP
- TFTP relies on Transport layer UDP
  - Connectionless
  - Does not guarantee reliable data delivery
- No ID and password required
  - Security risk
- No directory browsing allowed
- Useful to load data, programs on diskless workstation
- Used to put software on IP phones and routers

NTP (Network Time Protocol)

- Synchronizes network computer clocks
- Depends on UDP Transport layer services
  - Benefits from UDP's quick, connectionless nature
    - Time sensitive
    - Cannot wait for error checking
- Time synchronization importance
  - Routing
  - Time-stamped security methods
  - Maintaining accuracy, consistency between multiple storage systems

NNTP (Network News Transfer Protocol)

- Facilitates newsgroup messages exchange
  - Between multiple servers, users
- Similar to e-mail
  - Provides means of conveying messages
- Differs from e-mail
  - Distributes messages to wide group of users at once
- User subscribes to newsgroup server host
- News servers
  - Central collection, distribution point for newsgroup messages

PING (Packet Internet Groper)

- Provides verification
  - TCP/IP installed, bound to NIC, configured correctly, communicating with network
  - Host responding
- Uses ICMP services
  - Send echo request and echo reply messages
    - Determine IP address validity
- Ping IP address or host name
- Ping loopback address: 127.0.0.1
  - Determine if workstation's TCP/IP services running

PING (cont'd.)

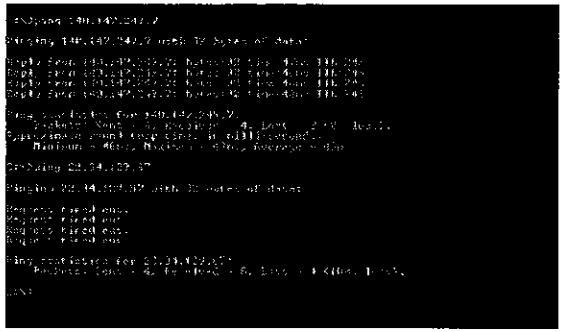


Figure 4-17 Output from successful and unsuccessful PING tests

- Operating system determines Ping command options, switches, syntax

CENGAGE Learning

Network+ Guide to Networks 5th Edition

Chapter 5

Topologies and Ethernet Standards

Objectives

- Describe the basic and hybrid LAN physical topologies, and their uses, advantages, and disadvantages
- Describe the backbone structures that form the foundation for most LANs
- Understand the transmission methods underlying Ethernet networks
- Compare the different types of switching used in data transmission

Topologies

Simple Physical Topologies

- Physical topology
  - Physical network nodes layout
  - Depicts broad scope
  - Does not specify:
    - Device types
    - Connectivity methods
    - Addressing schemes
  - Fundamental shapes
    - Bus, ring, star
    - Hybrid

Bus

- Bus topology
  - Bus
    - Single cable
    - Connecting all network nodes
    - No intervening connectivity devices
  - One shared communication channel
  - Physical medium
    - Coaxial cable
  - Passive topology
    - Node listens for, accepts data
    - Use broadcast to send

Bus (cont'd.)

- Bus topology (cont'd.)
  - Broadcast domain
    - Node communicates using broadcast transmission
  - Terminators
    - 50-ohm resistors
    - Stops signal at end of wire
  - Signal bounce
    - Signals echo between two network ends
  - One end grounded
    - Removes static electricity

Bus (cont'd.)

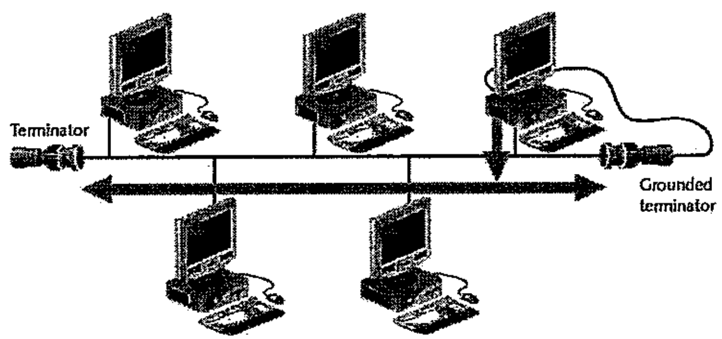


Figure 5-1 A terminated bus topology network

Bus (cont'd.)

- Advantages
  - Relatively inexpensive
- Disadvantage
  - Does not scale well
    - All nodes share a fixed amount of total bandwidth
  - Difficult to troubleshoot
  - Not very fault tolerant

Ring

- Ring topology
  - Node connects to nearest two nodes
  - Circular network
  - Clockwise data transmission
    - One direction (unidirectional) around ring
  - Active topology
    - Workstation participates in data delivery
    - Data stops at destination
  - Physical medium
    - Twisted pair or fiber-optic cabling

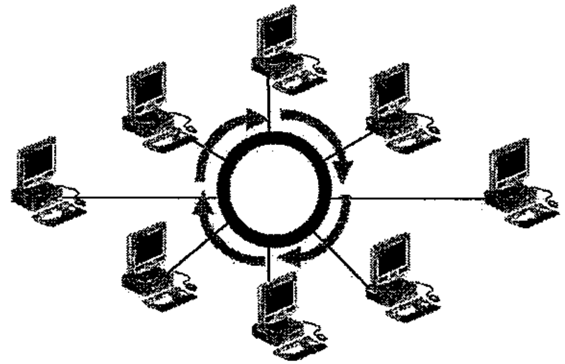


Figure 5-2 A typical ring topology network

- Drawback
  - Malfunctioning workstation can disable network
  - Not flexible or scalable

Star

- Star topology
  - Node connects through central device
    - Hub, router, or switch
  - Physical medium
    - Twisted pair or fiber-optic cabling
  - Single cable connects two devices
  - Require more cabling, configuration
- Advantage
  - Fault tolerance
    - Centralized connection point can be a single point of failure, however
  - Scalable

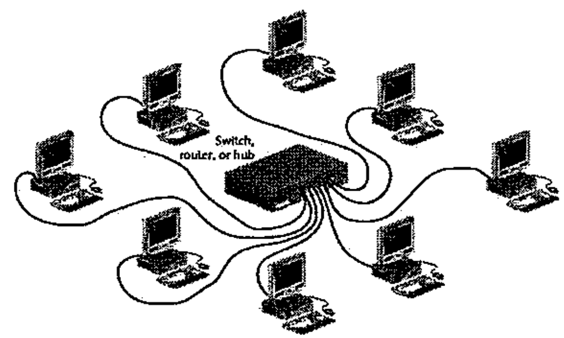


Figure 5-3 A typical star topology network

- Most popular fundamental layout
  - Ethernet networks based on star topology
- 1024 addressable logical network nodes maximum

Logical Topologies

- Describes data transmission between nodes
- Most common: bus, ring
- Bus logical topology
  - Signals travel from one device to all other devices
  - May or may not travel through intervening connectivity device
  - Bus logical topology used by networks with:
    - Physical bus topology
    - Star, star-wired bus topology
  - Ethernet

Logical Topologies (cont'd.)

- Ring logical topology
  - Signals follow circular path
  - Ring logical topology used by networks with:
    - Pure ring topology
    - Star-wired ring hybrid physical topology
  - Token ring

Hybrid Physical Topologies

- Pure bus, ring, star topologies
  - Rarely exist
    - Too restrictive
- Hybrid topology
  - More likely
  - Complex combination of pure topologies
  - Several options

Star-Wired Ring

- Star-wired ring topology
  - Star physical topology
  - Ring logical topology
- Benefit
  - Star fault tolerance
- Network use
  - Token Ring networks
    - IEEE 802.5

Star-Wired Ring (cont'd.)

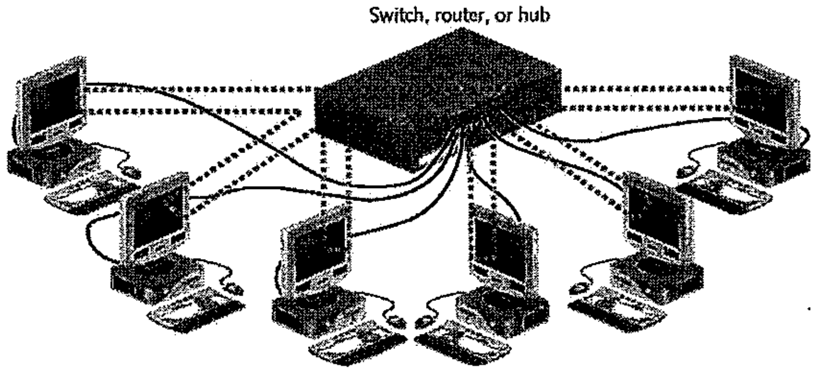


Figure 5-4 A star-wired ring topology network

Star-Wired Bus

- Star-wired bus topology
  - Workstation groups
    - Star-connected devices
    - Networked via single bus
- Advantage
  - Cover longer distances
  - Easily interconnect, isolate different segments
- Drawback
  - Cabling, connectivity device expense
- Basis for modern Ethernet networks

Star-Wired Bus (cont'd.)

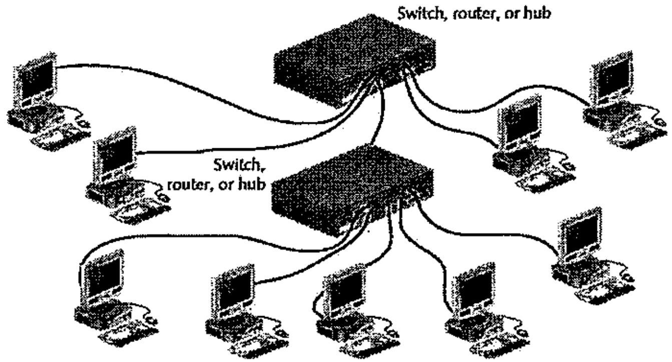


Figure 5-5 A star-wired bus topology network

Backbone Networks

- Cabling connecting hubs, switches, routers
- More throughput
- Large organizations
  - Fiber-optic backbone
  - Cat 5 or better for hubs, switches
- Enterprise-wide network backbones
  - Complex, difficult to plan
- Enterprise
  - Entire organization
  - Significant building block: backbone

Serial Backbone

- Simplest backbone
  - Two or more internetworking devices
  - Connect using single daisy-chain cable
- Daisy-chain
  - Linked series of devices
- Benefit
  - Logical growth solution
    - Modular additions
  - Low-cost LAN infrastructure expansion
    - Easily attach hubs

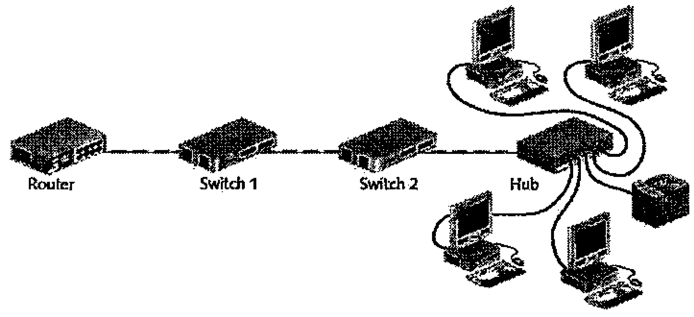


Figure 5-6 A serial backbone

- Backbone components
  - Hubs, gateways, routers, switches, bridges

Serial Backbone (cont'd.)

- Serial connection of repeating devices
  - Essential for distance communication
- Standards
  - Define number of hubs allowed
  - Exceed standards
    - Intermittent, unpredictable data transmission errors

Distributed Backbone

- Connectivity devices
  - Connected to a hierarchy of central connectivity devices
- Benefit
  - Simple expansion, limited capital outlay
- More complicated distributed backbone
  - Connects multiple LANs, LAN segments
    - Using routers

Distributed Backbone (cont'd.)

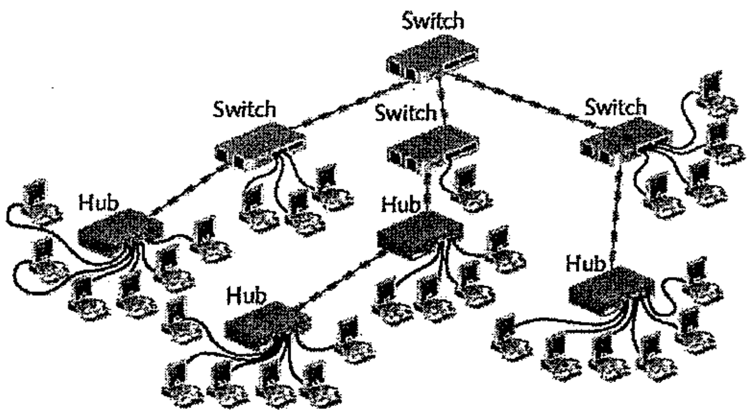


Figure 5-7 A simple distributed backbone

Distributed Backbone (cont'd.)

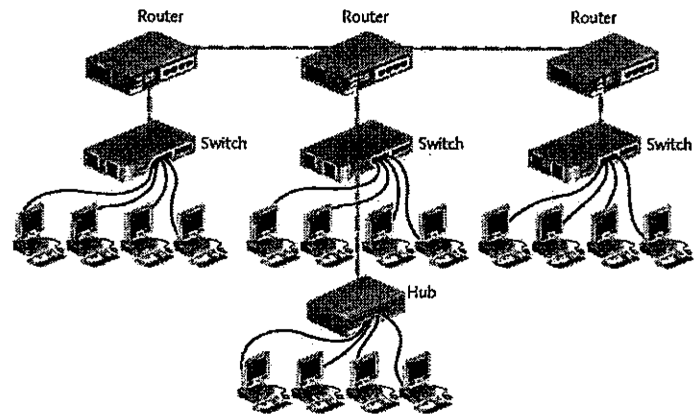


Figure 5-8 A distributed backbone connecting multiple LANs

Distributed Backbone (cont'd.)

- More benefits
  - Workgroup segregation
  - May include daisy-chain linked hubs
    - Consider length
- Drawback
  - Potential for single failure points

Collapsed Backbone

- Uses router or switch
  - Single central connection point for multiple subnetworks
- Highest layer
  - Router with multiprocessors
- Central router failure risk
- Routers may slow data transmission
- Advantages
  - Interconnect different subnetwork types
  - Central management

Collapsed Backbone (cont'd.)

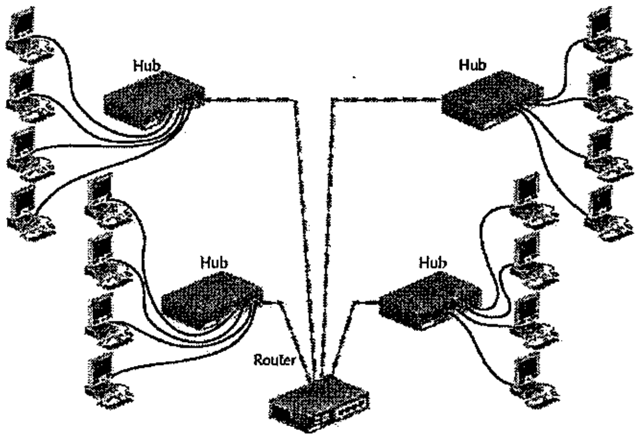


Figure 5-9 A collapsed backbone

Parallel Backbone

- Most robust network backbone
- More than one central router, switch
  - Connects to each network segment
- Requires duplicate connections between connectivity devices
- Advantage
  - Redundant links
  - Increased performance
  - Better fault tolerance

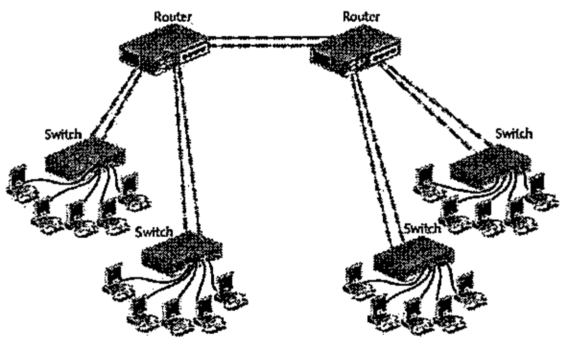


Figure 5-10 A parallel backbone

- Disadvantage
  - More cabling
- Used to connect most critical devices

Switching

Switching

- Logical network topology component
- Determines connection creation between nodes
- Three methods
  - Circuit switching
  - Message switching
  - Packet switching

Circuit Switching

- Connection established between two network nodes
  - Before transmitting data
- Dedicated bandwidth
- Data follows same initial path selected by switch
- Monopolizes bandwidth while connected
  - Resources are wasted
- Uses
  - Old analog phone calls
  - Live audio, videoconferencing
  - Home modem connecting to ISP

Message Switching

- Connection established between two devices
  - Data transferred then connection broken
  - Information stored and forwarded in second device
- Repeat store and forward routine
  - Until destination reached
- All information follows same physical path
- Connection not continuously maintained
- Device requirements
  - Sufficient memory, processing power
- Not commonly used in modern networks, but will be used in space
  - See link Ch 5a, Delay-Tolerant Networking (DTN)

Packet Switching

- Most popular, used by Ethernet and the Internet
- Breaks data into packets before transporting
- Packets
  - Travel any network path to destination
  - Find fastest circuit available at any instant
  - Need not follow the same path
  - Need not arrive in sequence
  - Reassembled at destination
- Requires speedy connections for live audio, video transmission

Packet Switching

- Advantages
  - No wasted bandwidth
  - Devices do not process information

MPLS (Multiprotocol Label Switching)

- IETF
  - Introduced in 1999
- Multiple layer 3 protocols
  - Travel over any one of several connection-oriented layer 2 protocols
- Supports IP
- Common use
  - Layer 2 WAN protocols

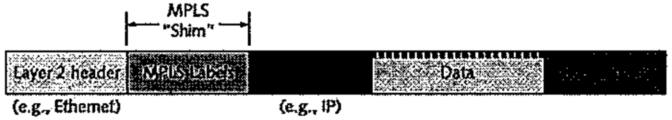


Figure 5-11 MPLS shim within a frame

- Advantages
  - Use packet-switched technologies over traditionally circuit switched networks
  - Create end-to-end paths
    - Act like circuit-switched connections
  - Addresses traditional packet switching limitations
  - Better QoS (quality of service)

Flow Routing (not in textbook)

- New technique connects streams of related packets so they all travel along the same path
- No need to make routing decisions after the first packet
- Saves time and power (link Ch 5c)

A Radical New Router

One of the founders of the Internet says network routers are too slow, costly, and power hungry-and he knows how to fix them

EMAIL PRINT SHARE PAGE 1 2 3 // VIEW ALL

PHOTO: Jonathan Sprague/Redux

Router Master

Internet pioneer Lawrence G. Roberts has reengineered the network router to handle streaming media.

Ethernet

Ethernet

- Developed by Xerox: 1970s
  - Improved by:
    - Digital Equipment Corporation (DEC), Intel, Xerox (DIX)
- Benefits
  - Flexible
  - Excellent throughput
    - Reasonable cost
- Popular network technology
- All variations
  - Share common access method
    - CSMA/CD

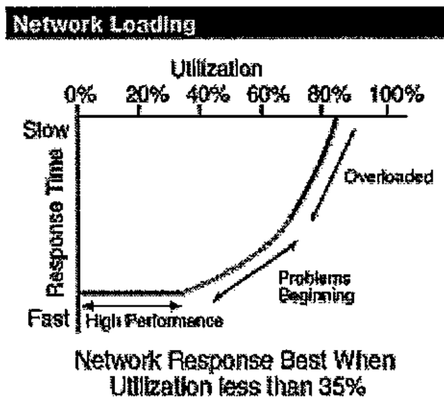
CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- Network access method
  - Controls how nodes access communications channel
  - Necessary to share finite bandwidth
- Carrier sense
  - Ethernet NICs listen, wait until free channel detected
- Multiple access
  - Ethernet nodes simultaneously monitor traffic, access media

CSMA/CD (cont'd.)

- Collision
  - Two nodes simultaneously:
    - Check channel, determine it is free, begin transmission
- Collision detection
  - Nodes detect unusually high voltages
    - Perform collision detection routine
  - Jamming
    - NIC issues 32-bit sequence
    - Indicates previous message faulty
  - Retransmit data

Collisions Limit Network Traffic



- See link Ch5e

CSMA/CD (cont'd.)

- Heavily trafficked network segments
  - Collisions common
- Segment growth
  - Performance suffers
  - "Critical mass" number dependencies
    - Data type and volume regularly transmitted
- Collisions corrupt data, truncate data frames
  - Network must compensate for them

CSMA/CD (cont'd.)

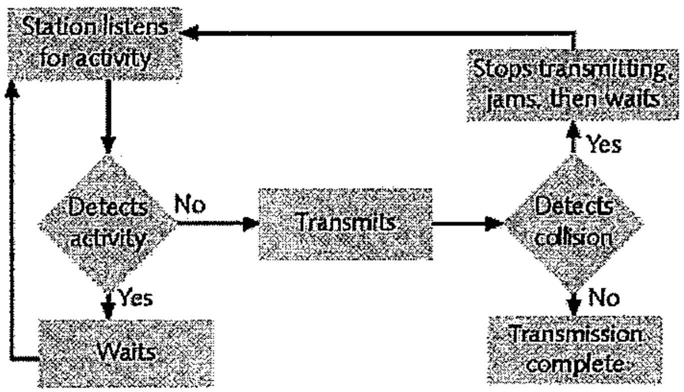
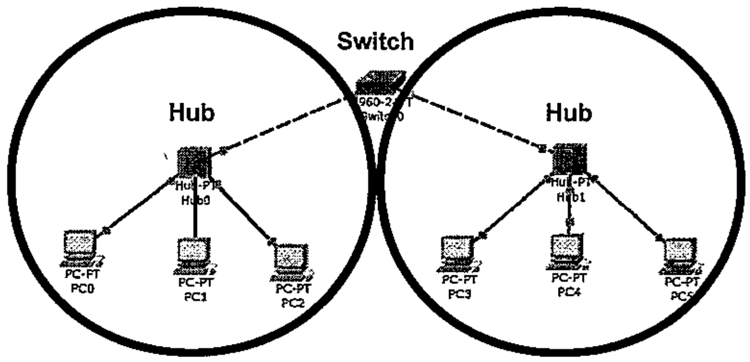


Figure 5-12 CSMA/CD process

CSMA/CD (cont'd.)

- Collision domain
  - Portion of network where collisions occur
- Ethernet network design
  - Repeaters repeat collisions
    - Result in larger collision domain
  - Switches and routers
    - Separate collision domains
- Collision domains differ from broadcast domains

Two Collision Domains But One Broadcast Domain



CSMA/CD (cont'd.)

- Ethernet cabling distance limitations
  - Affected by collision domains
- Data propagation delay
  - Time for data to travel
    - From one segment point to another point
  - Too long
    - Cannot identify collisions accurately
  - 100 Mbps networks
    - Three segment maximum connected with two hubs
  - 10 Mbps buses
    - Five segment maximum connected with four hubs

Ethernet Standards for Copper Cable

- IEEE Physical layer standards
  - Specify how signals transmit to media
  - Differ significantly in signal encoding
    - Affect maximum throughput, segment length, wiring requirements

Ethernet Standards for Copper Cable (cont'd.)

- **10Base-T**
  - 10 represents maximum throughput: 10 Mbps
  - Base indicates baseband transmission
  - T stands for twisted pair
  - Two pairs of wires: transmit and receive
    - Full-duplex transmission
  - Follows 5-4-3 rule of networking
    - Five network segments
    - Four repeating devices
    - Three populated segments maximum

Ethernet Standards for Copper Cable (cont'd.)

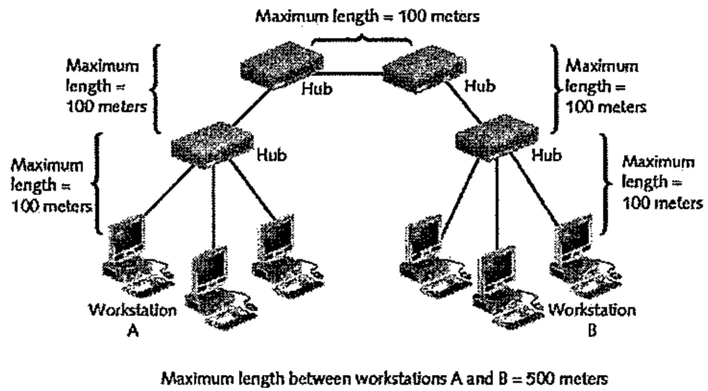


Figure 5-13 A 10Base-T network

Ethernet Standards for Copper Cable (cont'd.)

- **100Base-T (Fast Ethernet)**
  - IEEE 802.3u standard
  - Similarities with 10Base-T
    - Baseband transmission, star topology, RJ-45 connectors
  - Supports three network segments maximum
    - Connected with two repeating devices
    - 100 meter segment length limit between nodes
  - 100Base-TX
    - 100-Mbps throughput over twisted pair
    - Full-duplex transmission: doubles effective bandwidth

Ethernet Standards for Copper Cable (cont'd.)

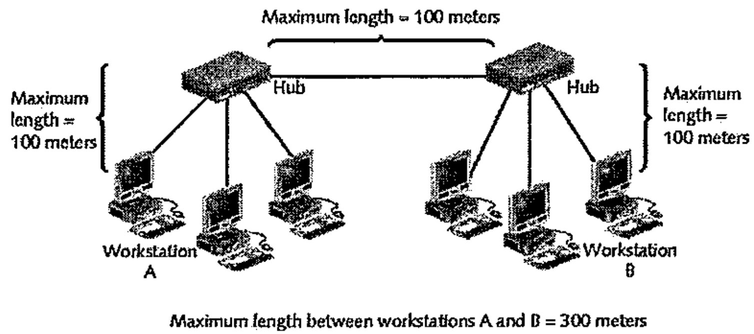


Figure 5-14 A 100Base-T network

Ethernet Standards for Copper Cable (cont'd.)

- **1000Base-T** (Gigabit Ethernet)
  - IEEE 802.3ab standard
  - 1000 represents 1000 Mbps
  - Base indicates baseband transmission
  - T indicates twisted pair wiring
  - Four pairs of wires in Cat 5 or higher cable
    - Transmit and receive signals
  - Data encoding scheme: different from 100Base-T
  - Standards can be combined
  - Maximum segment length: 100 meters, one repeater

Ethernet Standards for Copper Cable (cont'd.)

- **10GBase-T**
  - IEEE 802.3an
  - Pushing limits of twisted pair
    - Requires Cat 6 or Cat 7 cabling
    - Maximum segment length: 100 meters
  - Benefit
    - Very fast data transmission, lower cost than fiber-optic
  - Use
    - Connect network devices
    - Connect servers, workstations to LAN

Ethernet Standards for Fiber-Optic Cable

- **100Base-FX** (Fast Ethernet)
  - 100-Mbps throughput, broadband, fiber-optic cabling
    - Multimode fiber containing: at least two strands
  - Half-duplex mode
    - One strand receives, one strand transmits
    - 412 meters segment length
  - Full duplex-mode
    - Both strands send and receive
    - 2000 meters segment length
  - One repeater maximum
  - IEEE 802.3u standard

Ethernet Standards for Fiber-Optic Cable (cont'd.)

- **1000Base-LX** (1-Gigabit Ethernet)
  - IEEE 802.3z standard
  - 1000: 1000-Mbps throughput
  - Base: baseband transmission
  - LX: reliance on 1300 nanometers wavelengths
  - Longer reach than any other 1-gigabit technology
  - Single-mode fiber: 5000 meters maximum segment
  - Multimode fiber: 550 meters maximum segment
  - One repeater between segments
  - Excellent choice for long backbones

Ethernet Standards for Fiber-Optic Cable (cont'd.)

- **1000Base-SX** (1-Gigabit Ethernet)
  - IEEE 802.3z standard
  - Differences over 1000Base-LX
    - Multimode fiber-optic cable (installation less expensive)
    - Uses short wavelengths (850 nanometers)
  - Maximum segment length dependencies
    - Fiber diameter, modal bandwidth used to transmit signals

Ethernet Standards for Fiber-Optic Cable (cont'd.)

- **1000Base-SX** (1-Gigabit Ethernet) (cont'd.)
  - Modal bandwidth measurement
    - Highest frequency of multimode fiber signal (over specific distance)
    - MHz-km
    - Higher modal bandwidth, multimode fiber caries signal reliably longer
  - 50 micron fibers: 550 meter maximum length
  - 62.5 micron fibers: 275 meter maximum length
  - One repeater between segments
  - Best suited for shorter network runs

10-Gigabit Fiber-Optic Standards

- Extraordinary potential for fiber-optic cable
  - Pushing limits
- 802.3ae standard
  - Fiber-optic Ethernet networks
  - Transmitting data at 10 Gbps
  - Several variations
  - Common characteristics
    - Star topology, allow one repeater, full-duplex mode
  - Differences
    - Signal's light wavelength, maximum allowable segment length

10-Gigabit Fiber-Optic Standards

- **10GBase-SR and 10GBase-SW**
  - 10G: 10 Gbps
  - Base: baseband transmission
  - S: short reach
  - Physical layer encoding
    - R works with LAN fiber connections
    - W works with SONET fiber connections
  - Multimode fiber: 850 nanometer signal transmission
  - Maximum segment length
    - Depends on fiber diameter

10-Gigabit Fiber-Optic Standards

- **10GBase-LR and 10GBase-LW**
  - 10G: 10 Gbps
  - Base: baseband transmission
  - L: long reach
  - Single-mode fiber: 1319 nanometer signal transmission
  - Maximum segment length
    - 10,000 meters
  - 10GBase-LR: WAN or MAN
  - 10GBase-LW: SONET WAN links

10-Gigabit Fiber-Optic Standards

- **10GBase-ER and 10GBase-EW**
  - E: extended reach
  - Single-mode fiber
    - Transmit signals with 1550 nanometer wavelengths
  - Longest fiber-optic segment reach
    - 40,000 meters (25 miles)
  - 10GBase-EW
    - Encoding for SONET
  - Best suited for WAN use

Summary of Common Ethernet Standards

Standard	Maximum Transmission Speed (Mbps)	Maximum Distance per Segment (m)	Physical Media
10Base-T	10	100	Cat 3 or higher UTP
100Base-TX	100	100	Cat 5 or higher UTP
1000Base-T	1000	100	Cat 5 or higher UTP (Cat 5e is preferred)
10GBase-T	10,000	100	Cat 6 or Cat 7 (preferred)
100Base-FX	100	2000	MMF
1000Base-LX	1000	Up to 550, depending on wavelength and fiber core diameter 5000	MMF SMF
1000Base-SX	1000	Up to 500, depending on modal bandwidth and fiber core diameter	MMF
10GBase-SR and 10GBase-SW	10,000	Up to 300, depending on modal bandwidth and fiber core diameter	MMF
10GBase-LR and 10GBase-LW	10,000	10,000	SMF
10GBase-ER and 10GBase-EW	10,000	40,000	SMF

Table 5-1 Common Ethernet standards

Ethernet Frames

- Four types
  - Ethernet_802.2 (Raw)
  - Ethernet_802.3 (Novell proprietary)
  - Ethernet_II (DIX)
  - Ethernet_SNAP
- Frame types differ slightly
  - Coding and decoding packets
- No relation to topology, cabling characteristics
- Framing
  - Independent of higher-level layers

Ethernet Frames (cont'd.)

- **Using and Configuring Frames**
  - Ensure all devices use same, correct frame type
    - Node communication
  - Ethernet_II used today in almost all networks
  - Frame type configuration
    - Through NIC configuration software
    - NIC autodetect, autosense
  - Importance
    - Know frame type for troubleshooting

Ethernet Frames (cont'd.)

- **Frame Fields**
  - Common fields
    - 7-byte preamble, 1-byte start-of-frame delimiter
    - SFD (start-of-frame delimiter) identifies where data field begins
    - 14-byte header
    - 4-byte FCS (Frame Check Sequence)
    - Frame size range: 64 to 1518 total bytes
  - Larger frame sizes result in faster throughput
  - Improve network performance
    - Properly manage frames

Ethernet Frames (cont'd.)

- **Ethernet_II (DIX)**
  - Developed by DEC, Intel, Xerox (abbreviated DIX)
    - Before IEEE
  - Contains 2-byte type field
    - Identifies the Network layer protocol
  - Ethernet_SNAP frame type
    - Provides type field
    - Calls for additional control fields
    - Less room for data
  - Most commonly used on contemporary Ethernet networks

Ethernet Frames (cont'd.)

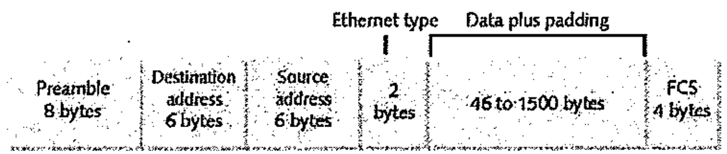


Figure 5-15 Ethernet_II (DIX) frame

PoE (Power over Ethernet)

- IEEE 802.3af standard
  - Supplying electrical power over Ethernet connections
- Two device types
  - PSE (power sourcing equipment)
  - PDs (powered devices)
- Requires Cat 5 or better copper cable
- Connectivity devices must support PoE
- Compatible with current 802.3 installations

PoE (cont'd.)

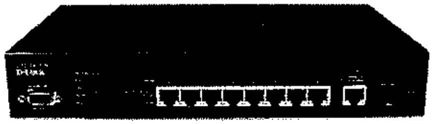


Figure 5-16 PoE-capable switch

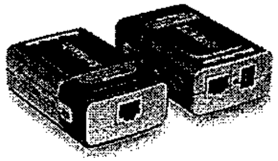


Figure 5-17 PoE adapters

Relationships Between Nodes (cont'd.)

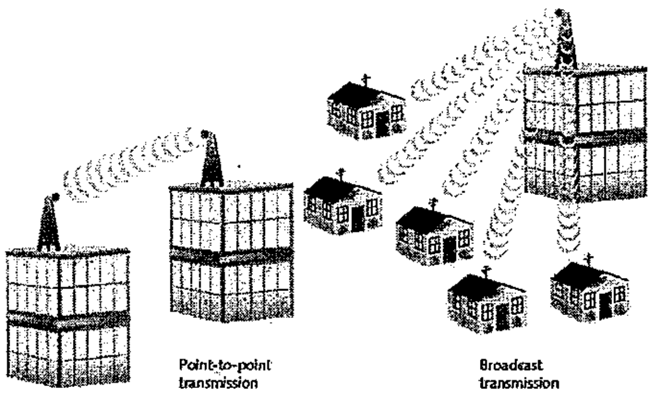


Figure 3-11 Point-to-point versus broadcast transmission

Throughput and Bandwidth

- Throughput
  - Measures amount of data transmitted during given time period
  - Capacity or bandwidth
  - Quantity of bits transmitted per second
- Bandwidth (strict definition)
  - Measures difference between highest and lowest frequencies medium can transmit
  - Range of frequencies
  - Measured in hertz (Hz)

Throughput

Quantity	Prefix	Complete example	Abbreviation
1 bit per second	n/a	1 bit per second	bps
1000 bits per second	kilo	1 kilobit per second	Kbps
1,000,000 bits per second	mega	1 megabit per second	Mbps
1,000,000,000 bits per second	giga	1 gigabit per second	Gbps
1,000,000,000,000 bits per second	tera	1 terabit per second	Tbps

Table 3-1 Throughput measures

Baseband and Broadband

- Baseband transmission
  - Digital signals sent through direct current (DC) pulses applied to wire
  - Requires exclusive use of wire's capacity
    - Transmit one signal (channel) at a time
  - Example: Ethernet
- Broadband transmission
  - Signals modulated
    - Radiofrequency (RF) analog waves
    - Uses different frequency ranges
  - Does not encode information as digital pulses

Public Authority for Applied Education and Training
College of Technological Studies
ENC-254 Computer Networks (1)
Problems Set No. 1

Q1. Fill the blanks using the following words:

1. The network model that is typical in a home with several computers **peer-to-peer**
2. In **client-server** the central resource sharing controlled by server.
3. **LAN** is smaller than MAN and WAN.
4. **WAN** connects two or more geographically distinct LANs or MANs.
5. **client** is a network computer requesting resources or services from another network computer.
6. **server** is a network computer managing shared resources
7. **NIC** is a device inside computer.
8. **connectivity device** allows multiple networks or multiple parts of one network to connect and exchange data.
9. The group of nodes is called a **segment** .
10. **Protocol** is a standard method or format for communication between networked devices.
11. **Packets** are distinct data units exchanged between nodes.

Q2. Multiple choices. CHOOSE ONE ANSWER ONLY:

- Which of the following is an advantage of peer-to-peer network model?
  A) **Inexpensive** B) Not flexible C) Not secure D) Not practical for large installations

- The peer-to-peer network model is good for:
  A) Home network B) Small office C) Large companies D) **Both (A) and (B)**

- UNIX, Linux, Microsoft Server 2003 and 2008, and MAC OS X Server are all examples of:
  A) Games B) Antivirus
  C) Client operating systems D) **Server operating systems.**

- The disadvantage of client-server relative to peer-to-peer networks is:
  A) Client-server is more complex in design and maintenance.
  B) Peer-to-peer is more complex in design and maintenance.
  C) Client-server is cheaper than peer-to-peer.
  D) Peer-to-peer is more secure than client-server.

- Central problem monitoring, diagnostics, correction capabilities is:
  A) **Advantage of client-server networks.**
  B) Disadvantage of client-server networks.
  C) Advantage of peer-to-peer networks.
  D) Disadvantage of peer-to-peer networks.

- A computer that enables other computers to share resources is called:
  A) **<u>Host</u>** B) NIC
  C) Switch D) Router

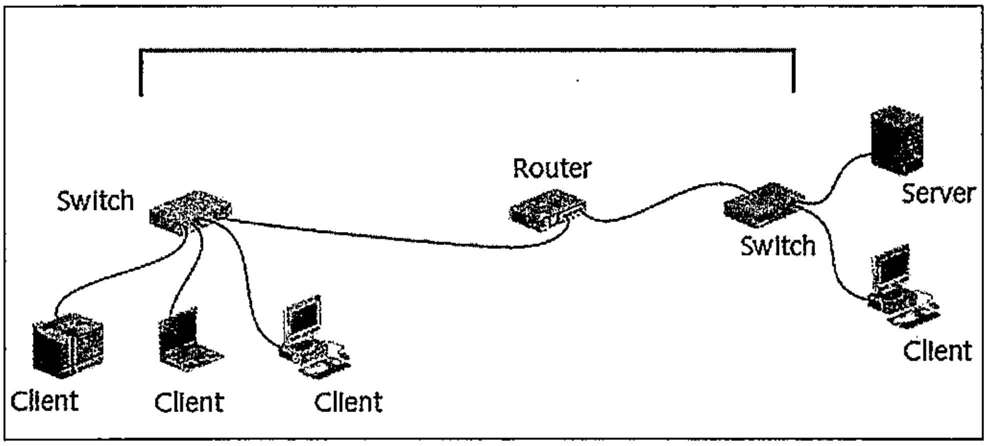
- Which of the following is a connectivity device:
  A) Switch B) Server
  C) Router **<u>D) Both (A) and (C)</u>**

- Capability of server to share data files, applications and disk storage space:
  <u>A) File services</u> B) Web services
  C) Print services D) Mail services

- Computer user on different network or in different geographical location from LAN's server
  A) Local user B) Super user
  C) Normal user **<u>D) Remote user</u>**

<u>Q3. Elements Common to LAN Network:</u>

Answer the below questions for the network in the following diagram.



a. How many nodes are connected to this network? ___ 5 ___.

b. How many workstations are connected to this network? ___ 3 ___.

c. How many connectivity devices are in this network? ___ 3 ___.

d. How many segments are in this network? ___ 2 ___.

e. How many backbones are in this network? ___ 1 ___.

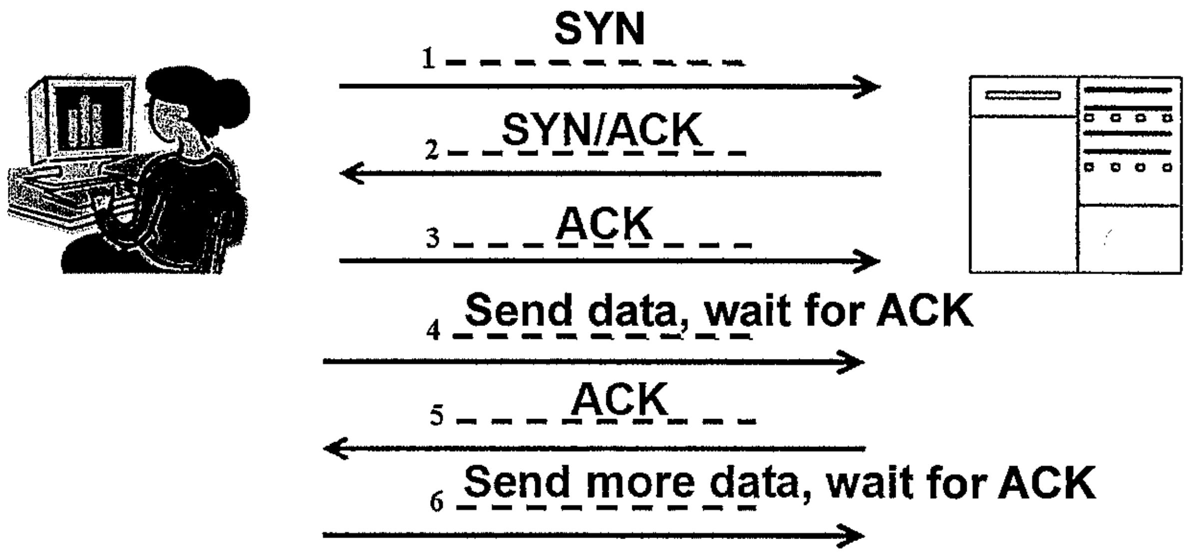
Public Authority for Applied Education and Training
College of Technological Studies
ENC-254 Computer Networks (1)
Problems Set No. 2

Q1. Fill the blanks using the following words:

1. ___ **OSI** ___ is a model for understanding and developing network computer-to-computer communications
2. _ **application layer** __ is the top (seventh) OSI model layer.
3. The layer that formats data to make it understandable to different applications and hosts **presentation layer.**
4. ___ **session** __ is a connection for ongoing data exchange between two parties
5. The layer that Accept data from Session layer and Provides flow control, segmentation, and error control is the **transport layer.**
6. _ **TCP** ___ is a connection-oriented that establishes a connection before transmitting data and makes a three-way handshake.
7. __ **UDP** ____ is a connectionless protocol that do not establish connection with another node before transmitting data—no handshake.
8. Breaking large data units received from Session layer into multiple smaller units called segments is called __ **segmentation** ____ .
9. ____ **reassembly** ___ is process of reconstructing segmented data units .
10. The layer that makes packet formation, routing, and adds the logical address is _ **network layer**
11. Determining path from point A on one network to point B on another network ___ **routing** _ _.
12. __ **IP** ____ is the most common network layer protocol.
13. The layer that divides data received into distinct frames for transmission in Physical layer and adds physical address to the frame is __ **data link layer** __.
14. Block ID and Device ID are the components of _ **MAC address** ___.
15. The layer that accepts frames from Data Link layer and generates signals as changes in voltage at the NIC is _ **physical layer** ____.

Q2:

a. Complete the figure below and show the signals of the Three-way hand shake in TCP protocol.



b. Fill the following table.

Layer No.	Layer Name	Protocol Data Unit	Protocol Example
1	Physical	Signals	
2	Data Link	Frame	
3	Network	Packet	IP
4	Transport	Segment	TCP, UDP
5	Session	X	X
6	Presentation	X	X
7	Application	X	X

c. The below figure that shows a layer-2 frame. What information should go to the empty fields 1, 2, and 3 ?

Sender's Physical Address	Receiver's Physical Address	Raw Data	Error Checking & Control

Public Authority for Applied Education and Training
College of Technological Studies
ENC-254 Computer Networks (1)
Eng. Nawaf Almudhahka
Problems Set No. 3 (Due 6-11-2013)

Q1. Fill the blanks using the following words:

1. Can be current, light pulses, or electromagnetic waves (**signals**)
2. Transmit and receive signals (**transceiver**)
3. Data signals in which voltage varies continuously (**analog signals**)
4. Uses core with larger diameter than single-mode fiber and laser or LED generated light pulses travel at different angles (**MMF**)
5. Data signals in which positive voltage represents a binary 1 and zero voltage represents a binary 0 (**digital signals**)
6. A device that separates combined signals (**demultiplexer**)
7. Make data suitable for carrying over communication path (**modulation**)
8. Signal transmission in one direction like broadcast TV (**simplex**)
9. Signals transmission: both directions simultaneously (**full-duplex**)
10. Signal transmission: both directions but one at a time (**half-duplex**)
11. A device that combines many channel signals (**multiplexer**)
12. One transmitter and one receiver (**point-to-point transmission**)
13. Hardware enabling networks or segments running on different media to interconnect and exchange signals (**media converter**)
14. Laser generated light travels over one path in (**SMF**)

Q2. Multiple choices:

- Digital signal benefit over analog signal is that:
  A) Digital is more reliable and less sever to noise B) Digital is more reliable and more sever to noise
  C) Digital is less reliable and less sever to noise D) Digital is less reliable and more sever to noise

- Converting digital signals to analog signals is called:
  A) **Modulation** B) Demodulation C) Filtration D) Bypassing

- Carrier frequency is modified in:
  A) Amplitude modulation B) Phase modulation
  C) **Frequency modulation** D) Data modulation

- Carrier signal amplitude is modified in:
  A) **Amplitude modulation** B) Phase modulation
  C) Frequency modulation D) Data modulation

- Full duplex advantage is:
  A) Increase overhead B) Decrease overhead
  C) **Increase speed** D) Decrease speed

- Divides channel into multiple time intervals:
  A) **TDM** B) FDM
  C) STDM D) WDM

- Unique frequency band for each communications sub channel:
  A) TDM B) **FDM**
  C) STDM D) WDM

- Point-to-point transmission:
  A) **One transmitter and one receiver**
  B) One transmitter and multiple, undefined receivers
  C) One transmitter and multiple, undefined receivers
  D) One transmitter and multiple, defined receivers

- Types of noise are:
  A) EMI, Cross over, and Environmental B) **EMI, Cross talk, and Environmental**
  C) EMI, modulation, and Environmental D) Multiplexing, Cross talk, and Environmental

- The F-type connecter and the BNC connector are used with:
  A) STP cable B) UTP cable
  C) Fiber Optic cable D) **Coaxial cable**

- Which of the following transmission media has the best noise resistance?
  A) STP cable B) UTP cable
  C) **Fiber Optic cable** D) Coaxial cable

- Which of the following transmission media has lowest cost?
  A) STP cable B) **UTP cable**
  C) Fiber Optic cable D) Coaxial cable

- All the following connectors are used with fiber optic cables EXCEPT:
  A) ST B) SC
  C) LC D) **RJ-45**

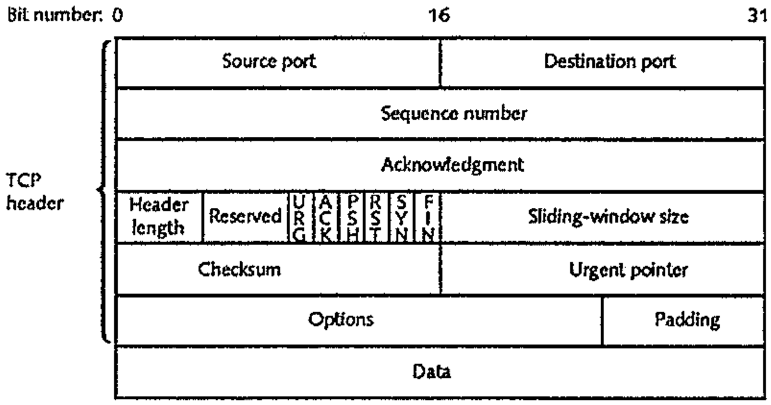
- DTE and DCE connections are:
  A) **Serial** B) Parallel
  C) USB D) UTP

- The device that processes signals and supplies synchronization clock signal:
  A) DTE B) **DCE**
  C) UTE D) RJ-11

- Time for packet to go from sender to receiver, then back from receiver to sender:
  A) **Round Trip Time (RTT)** B) One-way Time (OWT)
  C) Extra Trip Time (ETT) D) Half-Trip Time (HTT)

Public Authority for Applied Education and Training
College of Technological Studies
ENC-254 Computer Networks (1)
Eng. Nawaf Almudhahka
Problems Set No. 4 (Due 1-12-2013)

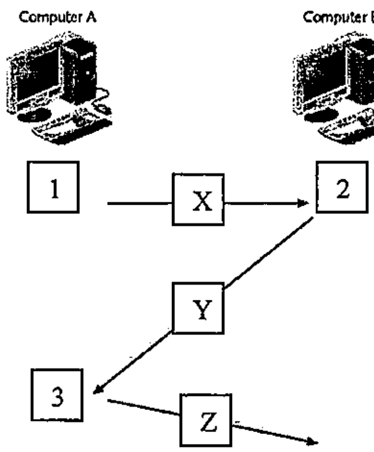
Q1.



The above figure shows the process of establishing a TCP connection; choose an answer for each of following questions:

- The field that guides data to the correct process on the destination computer:
  A) Destination port B) Checksum C) Sequence number D) Header length
- The field that is used to arrange segments in the correct order:
  A) Destination port B) Checksum **C) Sequence number** D) Header length
- The flags, especially SYN and ACK:
  A) Indicates purpose of segment B) Used to arrange segments in the correct order
  C) Indicates type of the protocol D) Guides data to the correct process on the destination
- Why the transmitter waits for ACK before sending more data?
  A) To maintain flow control B) To make sure that the receiver was not hacked
  C) To save the power D) To reset the data field
- Which of the following is TRUE about the UDP segment?
  A) It has exactly the same header fields as the TCP segment
  B) It has less header fields as the TCP segment
  C) It has more header fields as the TCP segment
  D) All of the above

Q2.



The above figure shows the process of establishing a TCP connection. Assuming that SEQ starts at 468506779 for computer-A and starts at 384238929 for computer-B, choose an answer for each of the following questions

- State $\boxed{1}$ represents:
  A) Request for connection B) Response
  C) Connection established D) Connection terminated

- State $\boxed{2}$ represents:
  1) Request for connection **2) Response**
  3) Connection established 4) Connection terminated

- State $\boxed{3}$ represents:
  1) Request for connection 2) Response
  3) Connection established 4) Connection terminated

- Transaction $\boxed{X}$ must be:
  1) SYN with SEQ= 468506779 2) SYN with SEQ= 937013558
  3) ACK(B) = 4685067780 4) ACK(B) = 384238929

- Transaction $\boxed{Y}$ must be:
  1) SYN with SEQ= 468506779 2) SYN-ACK with SEQ(B) = 384238929
  3) ACK(A) = 468506780 **4) Both (2) and (3)**

- Transaction $\boxed{Z}$ must be:
  1) SYN-ACK with SEQ(B) = 384238929 2) SYN-ACK with SEQ(A) = 468506780
  3) ACK(B) = 384238930 **4) Both (2) and (3)**

- What is the indication of FIN flag?
  1) Transmission end 2) Transmission start
  3) Transmission repeat 4) Transmission failed

Q3:

138.141.38.91

Given the above IP address, choose an answer for each of the below questions:

- The address above is:
  1) IPv4 and consists of 32 bits 2) IPv6 and consists of 32 bits
  3) IPv4 and consists of 128 bits 4) IPv6 and consists of 128 bits

- The above IP address consists of four portions and each one of them is called :
  1) Bit 2) Byte
  3) Octet **4) Both (2) and (3)**

- The above IP address is of class:
  1) A **2) B**
  3) C 4) D

- The beginning octet range for this IP class is:
  1) 1-126 **2) 128-191**
  3) 192-223 4) 224-230

- The number of networks for this IP class is:
  1) 2^8 **2) 2^{16}**
  3) 2^{24} 4) 2^{32}

- The maximum addressable hosts per network for this IP class is:
  1) 2^8 **2) 2^{16}**
  3) 2^{24} 4) 2^{32}

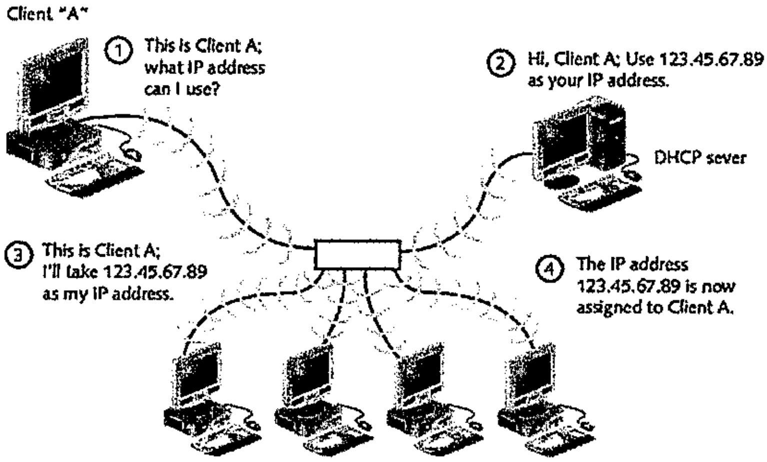
- The IP address 138.141.255.255 is reserved as :
  1) Network address 2) Loop back
  3) Broadcast address 4) APIPA

- The address 138.141.0.0 is reserved as :
  1) Network address 2) Local host
  3) Broadcast address 4) APIPA

- The address 138.141.38.91:23 is:
  1) A physical address 2) An IP Address
  3) A socket address 4) A host name

- Which command you will use to make sure that the machine with the above IP address is communicating with network?
  1) `ping 138.141.38.91` 2) `ping 138.141.38.255`
  3) `ipconfig 138.141.38.91` 2) `bing 138.141.38.91`

Q.4:



Given the DHCP leasing process on the figure above, choose an answer for each of the below questions:

1. The message of transaction-1 is:
   A) Broadcast B) Multicast C) Unicast D)Loopback

2. The message of transaction-2 is:
   A) Broadcast B) Multicast **C) Unicast** D)Loopback

3. The message of transaction-3 is:
   A) Broadcast B) Multicast **C) Unicast** D)Loopback

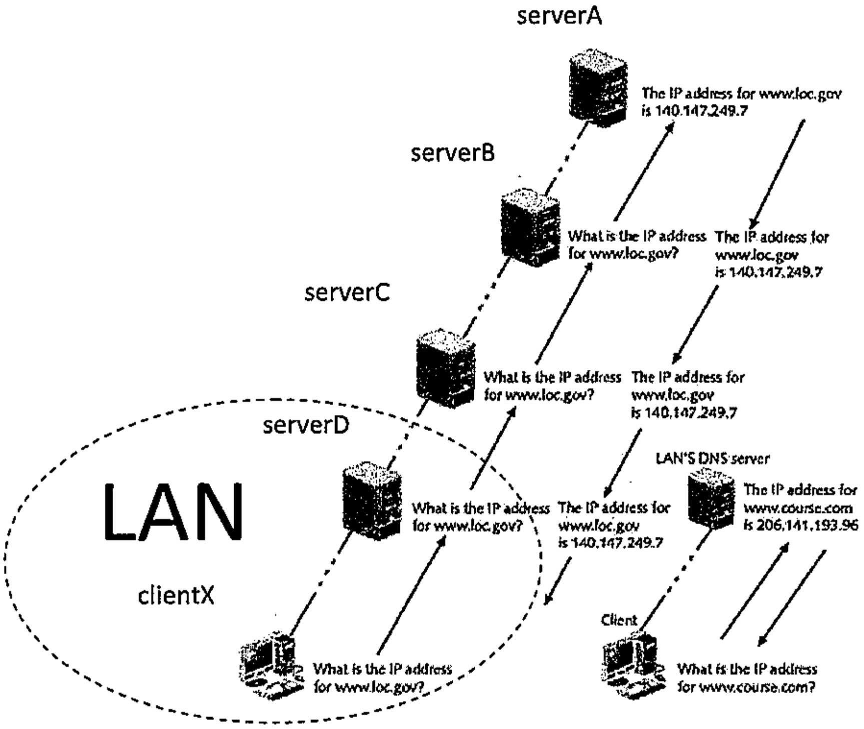
4. The message of transaction-4 is:
   A) Broadcast B) Multicast C) Unicast D)Loopback

5. What is the use of transaction-4 is:
   A) Acknowledging the lease to Client-A
   B) Informing all the other DHCP clients about Client-A MAC and IP
   C) Testing the connection between the DHCP server and Client-A
   D) Renewing the lease for all the DHCP clients

6. Can you manually configure the TCP/IP for Client-A?
   A) Yes and I can choose any IP address.
   B) No, I must use the DHCP service.
   C) Yes, but I have to look for an unassigned IP address
   D) Yes, even if I used an already assigned IP address

7. How you can terminate your DHCP lease?
   A) By manually changing the TCP/IP configurations on the client
   B) By manually changing the DHCP server configurations
   C) You cannot terminate your DHCP lease until its time expires
   D) Both (A) & (B)

Q.5:



The above figure shows the domain name resolution process, choose an answer for each of the below questions:

1. The root server is represented on the figure as:
   ■ serverB ■ serverC ■ serverD <u>■ serverA</u>

2. The LAN DNS server is represented on the figure as:
   ■ serverB ■ serverC <u>■ serverD</u> ■ serverA

3. The process of getting the IP address of **www.loc.gov** is called:
   ■ Name mapping ■ Name translation <u>**■ Name resolution**</u> ■ Name conversion

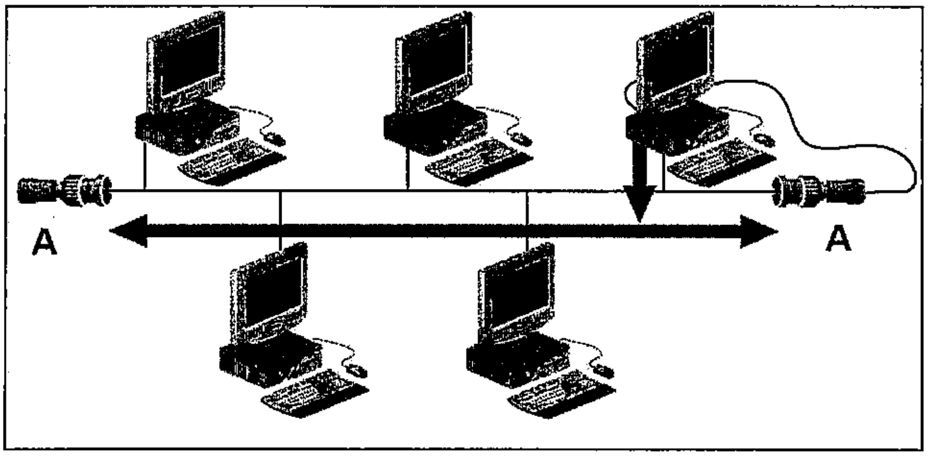
4. Which server has the largest database of domain names and IP addresses?
   ■ serverB ■ serverC ■ serverD <u>**■ serverA**</u>

5. Assume that the following was set on TCP/IP configurations of clientX:
   Primary DNS server = serverC
   Secondary DNS server = serverD
   What will happen if the clientX wants the IP address of **www.loc.gov** and serverC is down?
   ■ Error! **www.loc.gov** cannot be found
   <u>**■ clientX will forward the request to serverD**</u>
   ■ clientX will forward the request directly to serverA
   ■ clientX will forward the request directly to serverB

6. The DNS is:
   ■ Layer-4 service ■ Layer-5 service ■ Layer-6 service <u>**■ Layer-7 service**</u>

Public Authority for Applied Education and Training
College of Technological Studies
ENC-254 Computer Networks (1)
Eng. Nawaf Almudhahka
Problems Set No. 5 (Due 12-12-2013)

Q1.



Given the network topology on the above figure, circle the answer for each of the following questions:

1. The above topology is called:
   A) Star B) Ring C) Hybrid **D) Bus**

2. The components that should be installed in the position "A" shown on the figure are called:
   A) Hubs B) Routers C) Switches **D) Terminators**

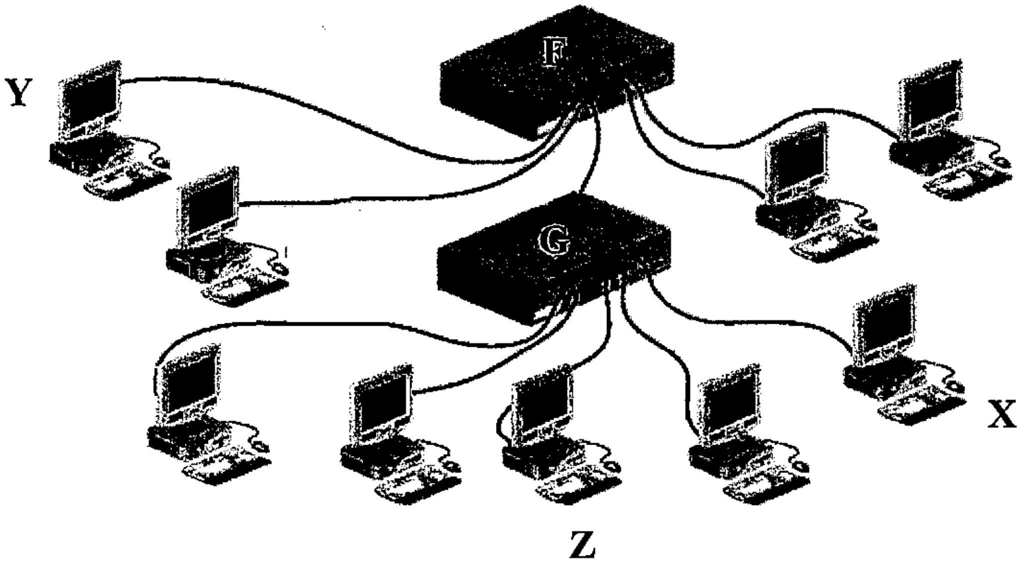
3. The main advantage of the above topology is that it is:
   A) Fault-tolerant B) Expensive C) Scalable **D) Inexpensive**

4. The physical media that is used to implement the above topology is:
   A) Twisted pair B) Fiber optic **C) Coaxial** D) Wireless

5. This topology is:
   A) Fault-tolerant B) Expensive C) Scalable **D) Difficult to troubleshoot**

6. If any node in the above topology wants to send data, then it uses:
   A) **Broadcast** B) Unicast C) Multicast

Q2.



Given the network topology on the above figure, circle the answer for each of the following questions:

1. The devices **F** and **G** are:
   A) **Switches** B) NICs C) Repeaters D) Both B & C

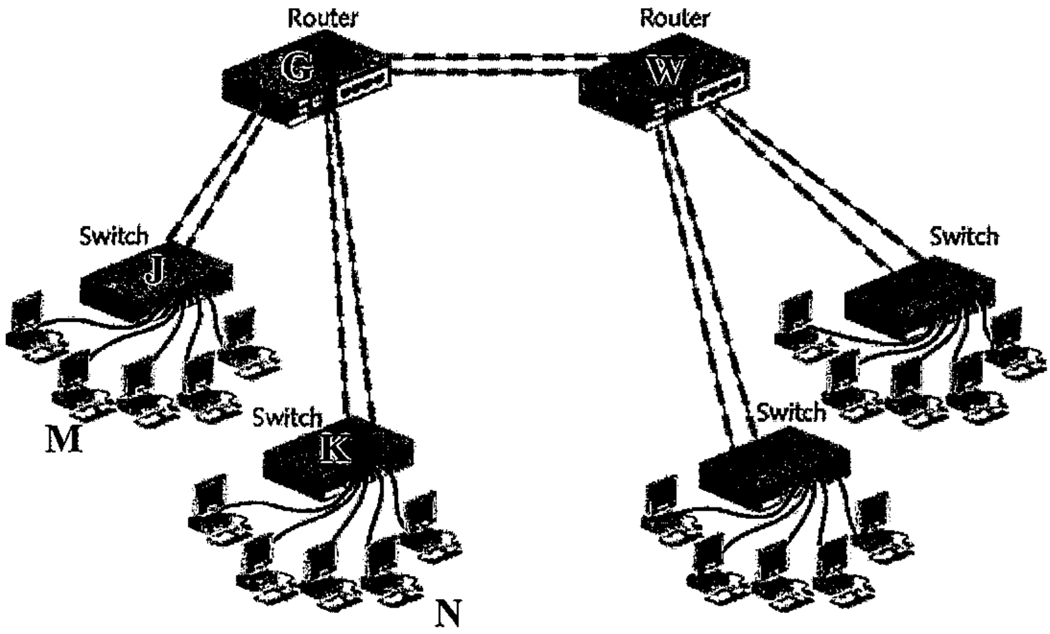
2. The topology on the above figure is called:
   A) Star-Wired Ring **B) Star-Wired Bus** C) Ring D) Bus

3. Device **G** on the above network can know the MAC address of:
   A) All the nodes directly connected to it.
   B) Device **F** only.
   C) All the nodes that are directly connected to it in addition to device **F**.
   D) Cannot know or understand MAC addresses.

4. Node **X** wants to send a message to node **Z**, then it will use:
   A) Broadcast at the first time, then unicasts. B) Broadcasts all the time.
   C) Unicasts all the time. D) Multicasts all the time.

5. Device **G** wants to send a message to node **Y**, then it will use:
   A) **Broadcast at the first time, then unicasts.** B) Broadcasts all the time.
   C) Unicasts all the time. D) Multicasts all the time.

Q3.



Given the network topology on the above figure, circle the answer for each of the following questions:

1. The topology on the above figure is called:
   A) Star-Wired Ring B) Star-Wired Bus
   C) Parallel Backbone D) Collapsed Backbone

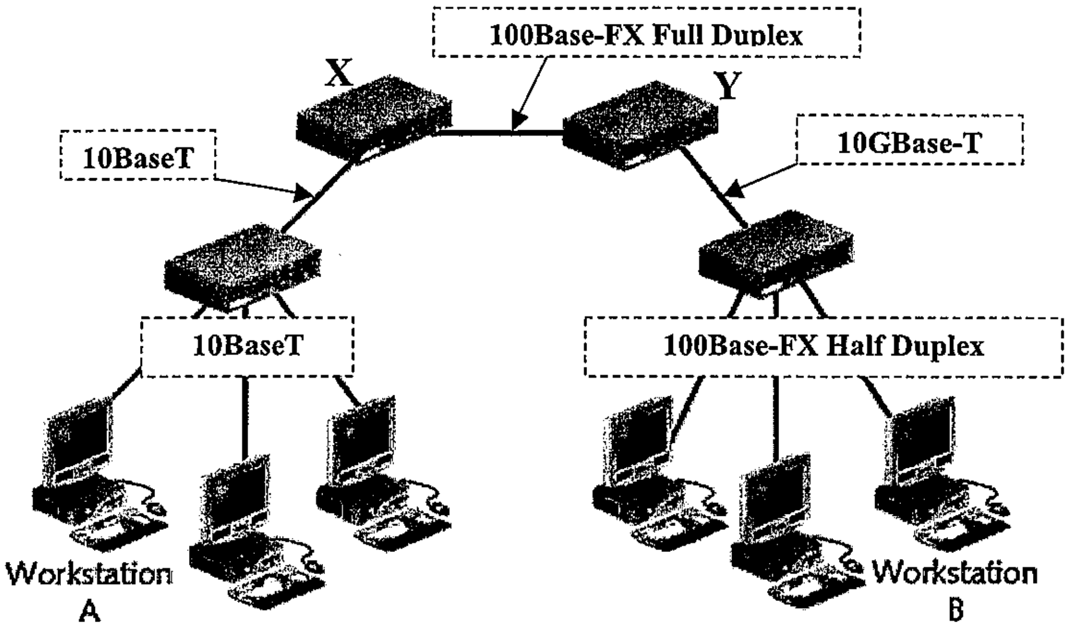
2. The topology in the above figure has:
   A) **Overall fault tolerance.** B) Fault tolerance for the switches ONLY.
   C) No fault tolerance. D) Fault tolerance for the two routers ONLY.

3. The topology in the above figure has:
   A) High cost because of the redundant links.
   B) Low cost because of the redundant links.
   C) Low cost because it is very difficult to implement.
   D) High cost because it is very easy to implement.

4. The switch **K** can know the MAC address of :
   A) Node **M.** B) Router **G.** C) Node **N.** **D) Router G & Node N.**

5. If we completely separated the router **G** with the switches (**J** , **K**) and all the nodes connected to them in a new network, then the topology of that new network will become :
   A) Star-Wired Ring B) Star-Wired Bus
   C) Parallel Backbone **D) Collapsed Backbone**

Q4.



Given the network diagram above, circle the answer for each of the following questions:

1. The maximum length between **Workstation A** and **Workstation B** is:
   A) 2300 m **B) 2712 m** C) 1124 m D) 4900 m

2. The Ethernet standard that has the maximum throughput in the above network is:
   A) 10BaseT **B) 10GBaseT** C) 100Base-FX Half Duplex D) 100Base-FX Full Duplex

3. Any of the following transmission medias can be used in the above network EXCEPT:
   A) UTP B) STP C) MMF **D) SMF**

4. The most expensive Ethernet standard among the ones used in the above network is:
   A) 10BaseT B) 10GBaseT C) 100Base-FX Half Duplex **D) 100Base-FX Full Duplex**

5. The topology of the above network is:
   A) Star-Wired Ring **B) Star-Wired Bus**
   C) Parallel Backbone D) Collapsed Backbone

6. Suppose that you want to extend the distance between the switches **X** and **Y** using a repeater. What will be the new maximum distance between switches **X** and **Y** after installing the repeater in between?
   A) 200 m B) 824 m C) 1412 m **D) 4000 m**