MOTOROLA

IP-101 NETWORKING BASICS

OVERVIEW

68P81013Y07-O
OCTOBER 6, 2005

Computer Software Copyrights

The Motorola products described in this document include a copyrighted Motorola computer program. Laws in the United States and other countries, as well as International Treaties, preserve for Motorola the exclusive rights for Motorola's copyrighted computer programs, including the exclusive right to copy, reproduce, distribute, or otherwise transfer said computer program(s). Accordingly, the copyrighted Motorola computer programs contained in this document may not be copied, decompiled, reverse engineered, or reproduced in any manner and on or within any media without the express written permission of Motorola. Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents, or patent applications of Motorola, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Document Copyrights

To order additional copies of this document contact your Motorola sales representative.

Disclaimer

The information in this document is carefully examined, and is believed to be entirely reliable. However, no responsibility is assumed for inaccuracies. Furthermore, Motorola reserves the right to make changes to any products herein to improve readability, function, or design. Motorola does not assume any liability arising out of the applications or use of any product or circuit described herein; neither does it cover any license under its patent rights nor the rights of others.

Trademark Information

The following are registered trademarks of Motorola, Inc.: Motorola, the Motorola logo, ASTRO, ASTRO-TAC, EMBASSY, FLASHport, FullVision, INTELLIREPEATER, MAXTRAC, MSF 5000, QUANTAR, QUANTRO, SECURENET, SMARTNET, SMARTZONE, SPECTRA, and STARTSITE.

The following are Motorola trademarks: CENTRACOM Series, CENTRACOM Gold Series, Micor, MOSCAD, Private Conversation, SABER, SMARTNET II, and Wireless Network Gateway.

HP, HP-UX, and Hewlett Packard are registered trademarks of Hewlett-Packard Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Any other brand or product names are trademarks or registered trademarks of their respective holders.

WARRANTY

Limited Software Warranty

For the first ninety (90) days following its initial shipment, Motorola warrants that when properly used, its software will be free from reproducible defects that cause a material variance from its published specification. However, Motorola does not warrant that program operation will be uninterrupted or error- free, that each defect will be corrected, or that any program will meet Licensee's particular requirements.

This warranty does not cover an item of Software (i) used in other than its normal and customary manner; (ii) subjected to misuse; or (iii) subjected to modifications by Licensee or by any party other than Motorola without the prior written consent of Motorola.

Limited Media Warranty

For the first ninety (90) days following its initial shipment, Motorola warrants that the media carrying the software will be free from defects that damage the performance of the software. Motorola will replace any damaged media free of charge during the warranty period. Warranted media is limited to that which is used to transport the software (such as floppy disks and authorization key). PROMs that may store the software in equipment are not covered under this warranty.

Limitation of Liability

Motorola's total liability and Licensee's sole remedy for any warranted software shall be limited to, at Motorola's option, software replacement or the payment of Licensee's actual damages, not to exceed the total licensed charge paid by Licensee to Motorola for the item of software that caused the damage.

The warranties set forth above extend only to the first licensee. Subsequent transferees accept these programs "as is" and without warranties of any kind. **This warranty is given in lieu of all other warranties, express or implied, including, without limitation, the warranties of merchantability and fitness for a particular purpose.**

In no event shall Motorola be liable for special, incidental, or consequential damages (including, without limitation, loss of use, time or data, inconvenience, commercial loss, and lost profits or savings) to the full extent that such may be disclaimed by law even if Motorola has been advised of the possibility of such damage against licensee by any other party.

Repair of Defects

The classification of defects in Motorola-supplied software shall be the responsibility of Motorola. Remedy of defects is at the sole discretion of Motorola. If Motorola agrees to remedy a software defect, the new software will be warranted until the end of the original limited warranty period.

Replacement of any software defect shall constitute Motorola supplying the Licensee with the appropriate software media and authorization key. Field installation and configuration are not included. Field software updates/upgrades and new enhancement option software will be warranted for ninety (90) days from the date of initial shipment.

All warranty service will be performed at service locations designated by Motorola. Travel and associated expenses of the Licensee or such expenses incurred by Motorola for visits to Licensee's location by Motorola personnel are not covered by this warranty.

CONTENTS

IP-101 NETWORKING BASICS

The Intent of This Guide vii
What the Reader Should Know vii

CHAPTER 1: ETHERNET TERMINOLOGY AND FUNDAMENTAL OPERATION

Ethernet Terminology 1-2
CSMA/CD Transmission Method 1-3
Characteristics 1-4
Topology 1-4
Ethernet and IEEE 802.3 Frame Formats 1-5

CHAPTER 2: NETWORKING BASICS AND PROTOCOLS

Networking Basics 2-2
Networking Protocols 2-3
TCP 2-3
Introduction to TCP/IP 2-4
UDP 2-6
Understanding Ports 2-7
Internetworking Basics 2-9
History of Internetworking 2-10
Internetworking Challenges 2-11

CHAPTER 3: THE OPEN SYSTEM INTERCONNECTION REFERENCE MODEL (OSI)

Introduction to OSI Model 3-2
Characteristics of the OSI Layers 3-4
Protocols 3-5
OSI Model and Communication Between Systems 3-6
Interaction Between OSI Model Layers 3-7
OSI Layer Services 3-9
OSI Model Layers and Information Exchange 3-10
Information Exchange Process 3-11
Layers of the OSI Model 3-12
Physical Layer 3-12
Data Link Layer 3-13

Network Layer . . . 3-14
Transport Layer . . . 3-14
Session Layer . . . 3-14
Presentation Layer . . . 3-15
Application Layer . . . 3-15
Information Formats . . . 3-16

CHAPTER 4: NETWORK HIERARCHY AND ADDRESSING

ISO Hierarchy of Networks . . . 4-2
Connection-Oriented and Connectionless Networks . . . 4-4
Internetwork Addresses . . . 4-5
Data Link Layer Addresses . . . 4-5
MAC Addresses . . . 4-6
Mapping Addresses . . . 4-7
Network Layer Addresses . . . 4-8
Hierarchical Versus Flat Address Space . . . 4-9
Address Assignments . . . 4-10
Addresses Versus Names . . . 4-10

CHAPTER 5: NETWORK FLOW CONTROL AND MULTIPLEXERS

Flow Control Basics . . . 5-2
Error-Checking Basics . . . 5-3
Multiplexing Basics . . . 5-4

CHAPTER 6: NETWORK DEVICES-TYPES AND BASIC OPERATION

Ethernet Devices . . . 6-2
Hubs and Repeaters . . . 6-3
Bridges . . . 6-4
Switches . . . 6-5
The 5-4-3 Rule . . . 6-6
Routers . . . 6-8

CHAPTER 7: STANDARDS ORGANIZATIONS

CHAPTER 8: NETWORK PHYSICAL MEDIA

Ethernet Transmission Physical Media . . . 8-2
Optical Communication Services . . . 8-6

CHAPTER 9: ETHERNET TERMS

LIST OF FIGURES

Figure 1-1: An Illustration of an Ethernet Bus 1-2
Figure 1-2: Ethernet and IEEE 802.3 Frame Formats 1-5
Figure 2-1: Network Layers. 2-2
Figure 2-2: Example of How TCP/IP Addressing Works 2-4
Figure 2-3: Communication of Server with Client 2-7
Figure 2-4: Communication with TCP/UDP 2-8
Figure 2-5: Different Network Technologies Can Be Connected to Create an Internetwork 2-9
Figure 3-1: The OSI Reference Model Contains Seven Independent Layers 3-2
Figure 3-2: Two Sets of Layers Make Up the OSI Layers 3-4
Figure 3-3: OSI Model Layers Communicate with Other Layers 3-8
Figure 3-4: Service Users, Providers, and SAPs Interact at the Network and Data Link Layers 3-9
Figure 3-5: Headers and Data Can Be Encapsulated During Information Exchange 3-10
Figure 3-6: Physical Layer Implementations Can Be LAN or WAN Specifications 3-12
Figure 3-7: The Data Link Layer Contains Two Sublayers 3-13
Figure 3-8: Data from Upper-Layer Entities Makes Up the Data Link Layer Frame 3-16
Figure 3-9: Three Basic Components Make Up a Network Layer Packet 3-16
Figure 3-10: Two Components Make Up a Typical Cell 3-17
Figure 4-1: A Hierarchical Network Contains Numerous Components 4-3
Figure 4-2: Each Interface on a Device Is Uniquely Identified by a Data-Link Address 4-5
Figure 4-3: MAC Addresses, Data-Link Addresses, and the IEEE Sublayers of the Data Link Layer 4-6
Figure 4-4: The MAC Address Contains a Unique Format of Hexadecimal Digits 4-6
Figure 4-5: Each Network Interface Must Be Assigned a Network Address for Each Protocol Supported 4-8
Figure 4-6: Hierarchical and Flat Address Spaces Differ in Comparison Operations 4-9
Figure 5-1: Multiple Applications Can Be Multiplexed into a Single Lower-Layer Data Packet 5-4
Figure 5-2: Multiple Devices Can Be Multiplexed into a Single Physical Channel 5-4
Figure 6-1: Hubs and Repeaters 6-3
Figure 6-2: Bridges 6-4
Figure 6-3: Switches 6-5
Figure 6-4: 5-4-3 Rule 6-6
Figure 6-5: Switch 6-7
Figure 6-6: Illustration of the 5-4-3 Rule 6-7
Figure 6-7: Routers 6-8
Figure 8-1: Twisted Pair 8-2
Figure 8-2: Crossover Ethernet Cable Pinouts 8-3

Figure 8-3: Standard Ethernet Cable Pinouts. 8-3
Figure 8-4: Coaxial Cable 8-4
Figure 8-5: Fiber Optic 8-4

LIST OF TABLES

Table 1-1: Transmission Speeds, Cable Lengths and Media. 1-4
Table 2-1: Different IP Address Classes 2-5
Table 3-1: OSI layer - Protocols Residing Here 3-7
Table 3-2: IEEE 802 Specifications 3-7
Table 6-1: Ethernet Devices - Their Primary OSI Operational Layer. 6-2
Table 9-1: IRQ (Interrupt Requests) 9-1
Table 9-2: Standard Topologies. 9-1
Table 9-3: Access Methods 9-2
Table 9-4: IBM Cabling System 9-2
Table 9-5: Wiring Transport Terms. 9-3
Table 9-6: UTP/STP Category Speeds 9-3
Table 9-7: Ethernet Specifications. 9-3
Table 9-8: Signal Transmissions 9-4
Table 9-9: OSI Model 9-4
Table 9-10: LAN Enhancement Components 9-5
Table 9-11: Protocols. 9-6
Table 9-12: Computer Name Resolution. 9-6
Table 9-13: Packet Switching Networks 9-7
Table 9-14: Security Levels. 9-7
Table 9-15: Network Diagnostic Tools 9-8

IP-101 NETWORKING BASICS

THE INTENT OF THIS GUIDE

The purpose of this document is to provide the dealer/customer with a basic understanding of theory of operation of Ethernet networks. This document is not meant to be a substitute for any training, technical or otherwise, which may be required for the dealer/customer to safely install and maintain their own or their customers networks.

WHAT THE READER SHOULD KNOW

- Have a basic understanding of Canopy products and has attended Canopy product training.
- Have a basic understanding of tower hardware and electrical requirements (i.e. the specifications noted in the R56 manual - http://R56.mot.com).
- Have a basic understanding of the actual bandwidth throughput available through the various Canopy AP, SM, and BH products, i.e.: that any/all single frequency radios operate in a half duplex mode - minus any overhead required between the pair of radios (subtract 30% from the aggregate Ethernet throughput for overhead - and then divide by the remaining bandwidth by 2 to derive the actual bi-directional full duplex Ethernet throughput).
- Ensure that all of the Canopy units/products noted in this document have been upgraded to the latest firmware revisions (as noted on the http://motorola.canopywireless.com/support_software.php Web site).

NOTE

Sources for the material used in this presentation include but are not limited to the following public Internet locations:

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm
- http://www.chaminade.org/MIS/Tutorials/NetworkingBasics.htm
- http://java.sun.com/docs/books/tutorial/networking/overview/networking.html
- http://www2.rad.com/networks/1997/nettut/ethernet.html

THIS PAGE INTENTIONALLY LEFT BLANK.

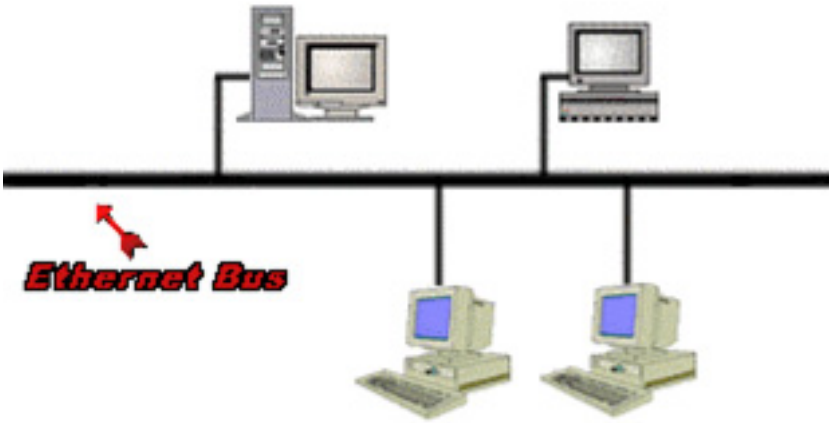
CHAPTER

1

ETHERNET TERMINOLOGY AND FUNDAMENTAL OPERATION

ETHERNET TERMINOLOGY

FIGURE 1-1 AN ILLUSTRATION OF AN ETHERNET BUS



Ethernet is, today, the de-facto hardware standard for local area networks. Ethernet (Version 2) and the very similar IEEE 802.3 standard define the physical and link layers of carrier sense multiple access/collision detection (CSMA/CD) LANs. In CSMA/CD LANs, all stations can access the network at any time. Before sending data, each station must "listen" to the network to see if it is already in use. Data is sent only if the station doesn't "hear" any data being sent.

Collision, is a situation where two stations detect silence on the network and send data at the same time. To overcome collision problems, Ethernet hardware is equipped with collision detection sensors. Whenever a collision is detected, the colliding data is ignored, at the stations that originally sent the data, will resend it.

CSMA/CD TRANSMISSION METHOD

Any single computer does not have any more authority than any other to control when and how messages are sent. Without scheduling authority, you would begin to wonder how one computer sends information to another without the interference that the other computers would produce if they transmitted at the same time.

The innovation of Ethernet is that computers schedule themselves by a random-access method.This method relies on the fact that all packets transmitted over the coaxial cable can be received by all transceivers, regardless of which computer might actually be the intended recipient. In communications terminology, Ethernet directly supports broadcast.

Each computer goes through the following steps to send a packet:

1. The computer senses the voltage across the cable to determine if another computer is transmitting.

2. If another computer is transmitting (i.e. the computer senses a voltage on the Ethernet network), the computer waits until the transmissions finish and then goes back to the first step. If the cable has no transmissions, the computer begins transmitting the packet.

3. If the receiver portion of the transceiver determines that no other computer is also sending a packet, the computer continues transmitting the packet until completion.

4. On the other hand, if the receiver senses interference from another computer's transmissions, all of the devices on the network immediately cease transmission, waiting a random amount of time to attempt the transmission again (go to step 1) until only one computer transmits and the others defer. The condition wherein two (or more) computers' transmissions interfere with others is known as a collision.

CHARACTERISTICS

Ethernet and IEEE 802.3 LANs come in a few “flavors,” each with its own length limits.

Table 1-1 describes the different Transmission Speeds, Cable Lengths and Media.

TABLE 1-1 TRANSMISSION SPEEDS, CABLE LENGTHS AND MEDIA

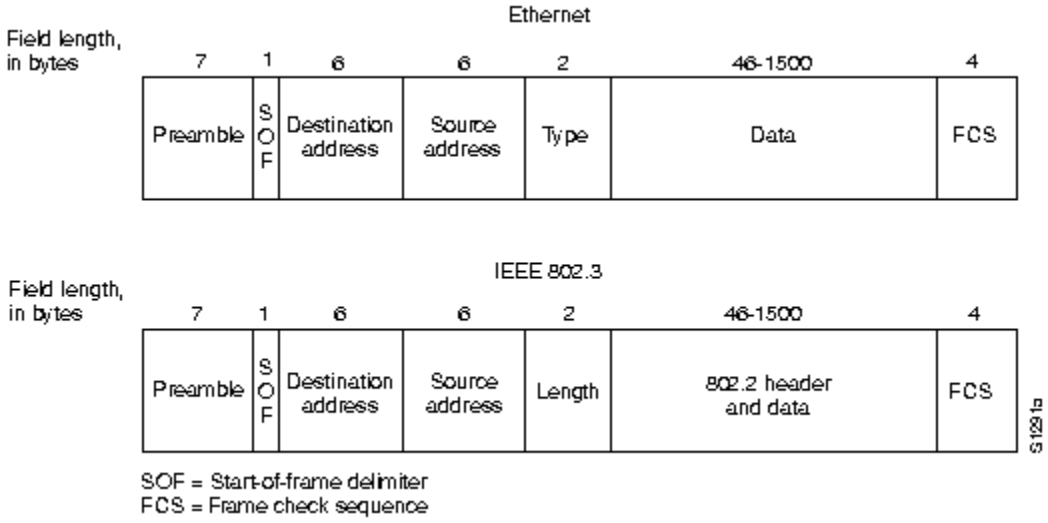
Terminology	Data Rate(Mbps)	Maximum Segment Length (m)	Media
Ethernet	10	500	50-ohm coax (thick)
10Base5 (IEEE 802.3)	10	500	50-ohm coax (thick)
10Base2 (IEEE 802.3)	10	185	50-ohm coax (thin)
1Base5 (IEEE 802.3)	1	250	Unshielded twisted-pairwire
10BaseT (IEEE 802.3)	10	100	Unshielded twisted-pairwire
10Broad36 (IEEE 802.3)	10	1800	75-ohm coax

TOPOLOGY

Ethernet LANs use a bus topology, i.e. all stations are connected to a single long cable. Any station can send a signal along the cable, which all other stations will receive. Unlike ring topologies, the cable doesn't close a loop.

ETHERNET AND IEEE 802.3 FRAME FORMATS

FIGURE 1-2 ETHERNET AND IEEE 802.3 FRAME FORMATS



Ethernet and IEEE 802.3 frames are similar. Both begin with an alternating pattern of ones and zeros (the Preamble), that tells the receiving stations that a frame is coming. Following the preamble, are the address of the destination station and the address of the source (sending) station.

In Ethernet frames, the 2-byte field following the source address is a type field, used to identify the data. In IEEE 802.3 frames, the 2-byte field following the source address is a length field, which indicates the number of bytes of data that follow this field and precede the frame check sequence (FCS) field.

Following the type/length field is the actual data contained in the frame, followed by a 4-byte FCS field containing a cyclic redundancy check (CRC) value. The CRC is created by the sending device and recalculated by the receiving device to check for damage that might have occurred to the frame in transit.

THIS PAGE INTENTIONALLY LEFT BLANK.

CHAPTER

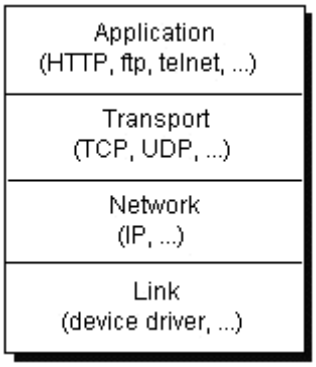
2

NETWORKING BASICS AND PROTOCOLS

NETWORKING BASICS

Computers running on the Internet communicate to each other using either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), as this diagram illustrates:

FIGURE 2-1 NETWORK LAYERS



When you write Java programs that communicate over the network, you are programming at the application layer. Typically, you don't need to concern yourself with the TCP and UDP layers. Instead, you can use the classes in the java.net package. These classes provide system-independent network communication. However, to decide which Java classes your programs should use, you do need to understand how TCP and UDP differ.

NETWORKING PROTOCOLS

TCP

When two applications want to communicate to each other reliably, they establish a connection and send data back and forth over that connection. This is analogous to making a telephone call. If you want to speak to Aunt Beatrice in Kentucky, a connection is established when you dial her phone number and she answers. You send data back and forth over the connection by speaking to one another over the phone lines. Like the phone company, TCP guarantees that data sent from one end of the connection actually gets to the other end and in the same order it was sent. Otherwise, an error is reported.

TCP provides a point-to-point channel for applications that require reliable communications. The Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Telnet are all examples of applications that require a reliable communication channel.

The order in which the data is sent and received over the network is critical to the success of these applications. When HTTP is used to read from a URL, the data must be received in the order in which it was sent. Otherwise, you end up with a jumbled HTML file, a corrupt zip file, or some other invalid information.

IMPORTANT

Definition: TCP (Transmission Control Protocol) is a connection-based protocol that provides a reliable flow of data between two computers.

INTRODUCTION TO TCP/IP

The TCP/IP protocol is the protocol that holds the Internet together. It is also found in most internal company networks.

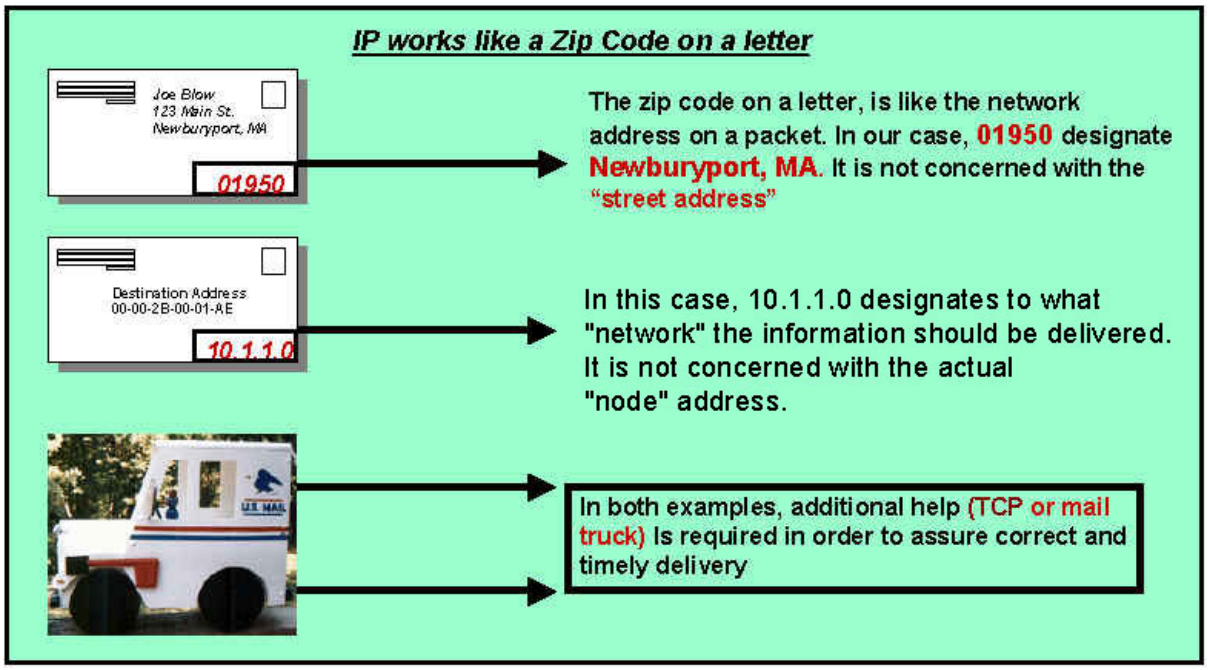
You might ask yourself, why should I learn about another protocol? The answer is simple:

As the internet becomes more popular and more applications are developed with a bias towards the Internet and TCP/IP, you will be forced to understand how this protocol works and maybe eventually install it on your own network.

WORKING OF TCP/IP

Each person is given (either automatically or manually) his or her own IP address. This IP address is unique to them and can not be used by anyone else inside your network. Think of an IP address as a telephone number, if several people had the same telephone number in your town, then there would be a conflict. A typical IP address might look something like this: 220.0.0.80. It's not a huge number that takes half an hour to type in, it's a simple four digit number that identifies your PC. You can't just make up these addresses, there is a numbering convention that you must use. Figure 2-2 is an example of how TCP/IP addressing works.

FIGURE 2-2 EXAMPLE OF HOW TCP/IP ADDRESSING WORKS



DIFFERENT IP ADDRESS CLASSES

There are different classes of IP address. The three most commonly talked about are Class A, Class B and Class C IP addresses. The IP address in the above example (220.0.0.x) is known as a Class C IP address.

TABLE 2-1 DIFFERENT IP ADDRESS CLASSES

Class	Network ID	Host ID	Example
A	1-126	x.x.x	1-126.x.x.x
B	128-191.f	x.x	128-191.f.x.x
C	192-223.f.f	X	192-223.f.f.x

(f) means fixed address that can not change.

(x) means a value between 0 and 255.

SUBNET MASKS

Your computer has no way of knowing what kind of IP address you have, this means that there has to be some way of letting your software extract the network ID from the IP address. To do this, you can use subnet masks.

Typically a subnet mask will look like this: 255.255.255.0. This tells us quickly that we are using a Class C IP address as the first three 255's tell us that these individual numbers can not change. The zero tells us that this is the only digit that we can use, so it has to be a Class C IP address.

If we had an IP address of 128.10.11.23 and a subnet mask of 255.255.0.0 then we can quickly see that we have a Class B IP address.

The purpose of a subnet mask is to tell the computer which is the Network ID and which is the host ID.

UDP

The UDP protocol provides for communication that is not guaranteed between two applications on the network. UDP is not connection-based like TCP. Rather, it sends independent packets of data, called datagrams, from one application to another. Sending datagrams is much like sending a letter through the postal service: The order of delivery is not important and is not guaranteed, and each message is independent of any other.

IMPORTANT

Definition: UDP (User Datagram Protocol) is a protocol that sends independent packets of data, called datagrams, from one computer to another with no guarantees about arrival. UDP is not connection-based like TCP.

For many applications, the guarantee of reliability is critical to the success of the transfer of information from one end of the connection to the other. However, other forms of communication don't require such strict standards. In fact, they may be slowed down by the extra overhead or the reliable connection may invalidate the service altogether.

Consider, for example, a clock server that sends the current time to its client when requested to do so. If the client misses a packet, it doesn't really make sense to resend it because the time will be incorrect when the client receives it on the second try. If the client makes two requests and receives packets from the server out of order, it doesn't really matter because the client can figure out that the packets are out of order and make another request. The reliability of TCP is unnecessary in this instance because it causes performance degradation and may hinder the usefulness of the service.

Another example of a service that doesn't need the guarantee of a reliable channel is the ping command. The purpose of the ping command is to test the communication between two programs over the network. In fact, ping needs to know about dropped or out-of-order packets to determine how good or bad the connection is. A reliable channel would invalidate this service altogether.

The UDP protocol provides for communication that is not guaranteed between two applications on the network. UDP is not connection-based like TCP. Rather, it sends independent packets of data from one application to another. Sending datagrams is much like sending a letter through the mail service: The order of delivery is not important and is not guaranteed, and each message is independent of any others.

NOTE

Many firewalls and routers have been configured not to allow UDP packets. If you're having trouble connecting to a service outside your firewall, or if clients are having trouble connecting to your service, ask your system administrator if UDP is permitted.

UNDERSTANDING PORTS

Generally speaking, a computer has a single physical connection to the network. All data destined for a particular computer arrives through that connection. However, the data may be intended for different applications running on the computer.

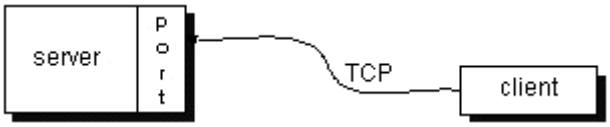
So how does the computer know to which application to forward the data?

Through the use of ports. Data transmitted over the Internet is accompanied by addressing information that identifies the computer and the port for which it is destined. The computer is identified by its 32-bit IP address, which IP uses to deliver data to the right computer on the network.

Ports are identified by a 16-bit number, which TCP and UDP use to deliver the data to the right application.

In connection-based communication such as TCP, a server application binds a socket to a specific port number. This has the effect of registering the server with the system to receive all data destined for that port. A client can then rendezvous with the server at the server's port, as illustrated Figure 2-3

FIGURE 2-3 COMMUNICATION OF SERVER WITH CLIENT

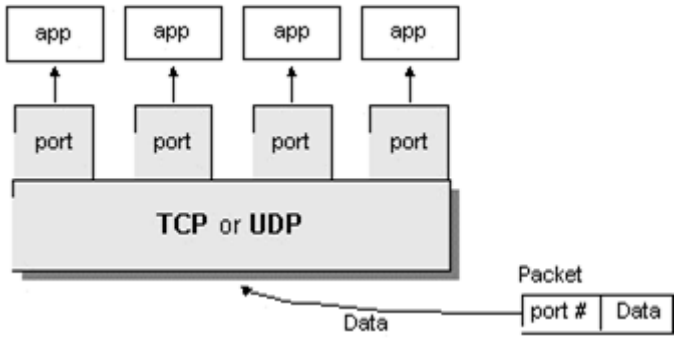


IMPORTANT

Definition: The TCP and UDP protocols use ports to map incoming data to a particular process running on a computer.

In datagram-based communication such as UDP, the datagram packet contains the port number of its destination and UDP routes the packet to the appropriate application, as illustrated in the Figure 2-4

FIGURE 2-4 COMMUNICATION WITH TCP/UDP



Port numbers range from 0 to 65,535 because ports are represented by 16-bit numbers. The port numbers ranging from 0 - 1023 are restricted; they are reserved for use by well-known services such as HTTP and FTP and other system services. These ports are called well-known ports. Your applications should not attempt to bind to them.

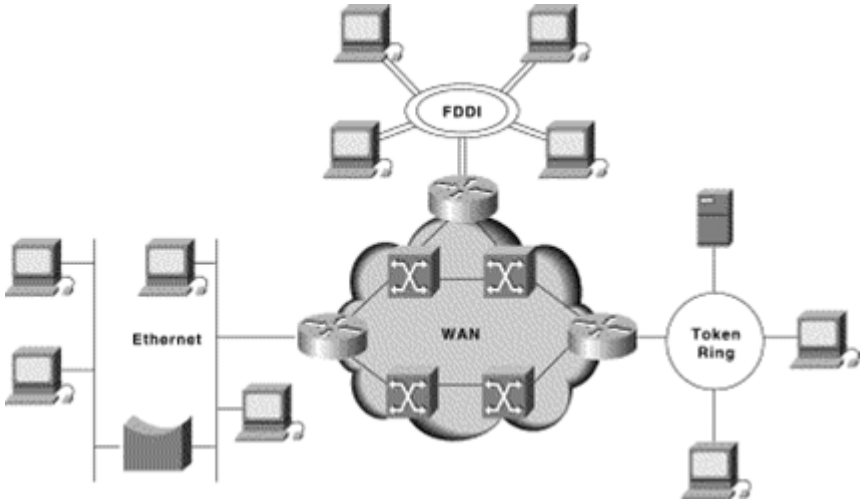
NETWORKING CLASSES IN THE JDK

Through the classes in java.net, Java programs can use TCP or UDP to communicate over the Internet. The URL, URLConnection, Socket, and Server Socket classes all use TCP to communicate over the network. The DatagramPacket, DatagramSocket, and MulticastSocket classes are for use with UDP.

INTERNETWORKING BASICS

An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network. Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks. Figure 2-5 illustrates some different kinds of network technologies that can be interconnected by routers and other networking devices to create an internetwork.

FIGURE 2-5 DIFFERENT NETWORK TECHNOLOGIES CAN BE CONNECTED TO CREATE AN INTERNETWORK



HISTORY OF INTERNETWORKING

The first networks were time-sharing networks that used mainframes and attached terminals. Such environments were implemented by both IBM's Systems Network Architecture (SNA) and Digital's network architecture.

LOCAL-AREA NETWORKS (LANS)

Evolved around the PC revolution. LANs enabled multiple users in a relatively small geographical area to exchange files and messages, as well as access shared resources such as file servers and printers.

WIDE-AREA NETWORKS (WANS)

Interconnect LANs with geographically dispersed users to create connectivity. Some of the technologies used for connecting LANs include T1, T3, ATM, ISDN, ADSL, Frame Relay, radio links, and others. New methods of connecting dispersed LANs are appearing everyday.

INTERNETWORKING

Today, high-speed LANs and switched internetworks are becoming widely used, largely because they operate at very high speeds and support such high-bandwidth applications as multimedia and videoconferencing.

Internetworking evolved as a solution to three key problems:

- Isolated LANs
- Duplication of resources
- Lack of network management

ISOLATED LANS

Isolated LANs made electronic communication between different offices or departments impossible.

DUPLICATION OF RESOURCES

Duplication of resources meant that the same hardware and software had to be supplied to each office or department, as did separate support staff.

LACK OF NETWORK MANAGEMENT

This lack of network management meant that no centralized method of managing and troubleshooting networks existed.

INTERNETWORKING CHALLENGES

Implementing a functional internetwork is no simple task. Many challenges must be faced, especially in the areas of connectivity, reliability, network management, and flexibility. Each area is key in establishing an efficient and effective internetwork. The challenge when connecting various systems is to support communication among disparate technologies. Different sites, for example, may use different types of media operating at varying speeds, or may even include different types of systems that need to communicate.

Companies rely heavily on data communication, internetworks must provide a certain level of reliability. This is an unpredictable world, so many large internetworks include redundancy to allow for communication even when problems occur.

Furthermore, network management must provide centralized support and troubleshooting capabilities in an internetwork.

Configuration, security, performance, and other issues must be adequately addressed for the internetwork to function smoothly.

Security within an internetwork is essential. Many people think of network security from the perspective of protecting the private network from outside attacks. However, it is just as important to protect the network from internal attacks, especially because most security breaches come from inside. Networks must also be secured so that the internal network cannot be used as a tool to attack other external sites.

THIS PAGE INTENTIONALLY LEFT BLANK.

CHAPTER

3

THE OPEN SYSTEM INTERCONNECTION REFERENCE MODEL (OSI)

The OSI Model:

- Layers
- Processes
- Architecture

INTRODUCTION TO OSI MODEL

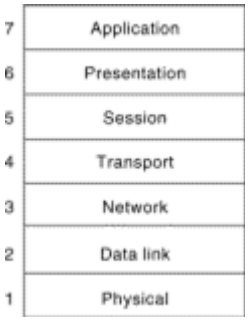
The Open System Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer.

The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The following list details the seven layers of the Open System Interconnection (OSI) reference model:

- Layer 7—Application
- Layer 6—Presentation
- Layer 5—Session
- Layer 4—Transport
- Layer 3—Network
- Layer 2—Data link
- Layer 1—Physical

FIGURE 3-1 THE OSI REFERENCE MODEL CONTAINS SEVEN INDEPENDENT LAYERS



NOTE

A handy way to remember the seven layers is the sentence "All people seem to need data processing." The beginning letter of each word corresponds to a layer.

All—Application layer

People—Presentation layer

Seem—Session layer

To—Transport layer

Need—Network layer

Data—Data link layer

Processing—Physical layer

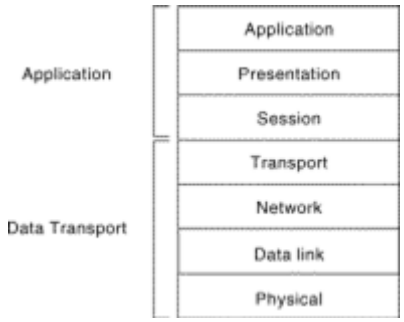
CHARACTERISTICS OF THE OSI LAYERS

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.

The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model.

The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium.

FIGURE 3-2 TWO SETS OF LAYERS MAKE UP THE OSI LAYERS



PROTOCOLS

The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols. In the context of data networking, a protocol is a formal set of rules and conventions that governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the OSI layers.A wide variety of communication protocols exist.

Some of these protocols include:

- LAN protocols
- WAN protocols
- Network protocols
- Routing protocols

LAN protocols operate at the physical and data link layers of the OSI model and define communication over the various LAN media.

WAN protocols operate at the lowest three layers of the OSI model and define communication over the various wide-area media.

Routing protocols are network layer protocols that are responsible for exchanging information between routers so that the routers can select the proper path for network traffic. Finally, network protocols are the various upper-layer protocols that exist in a given protocol suite.

Many protocols rely on others for operation. For example, many routing protocols use network protocols to exchange information between routers. This concept of building upon the layers already in existence is the foundation of the OSI model.

OSI MODEL AND COMMUNICATION BETWEEN SYSTEMS

Information being transferred from a software application in one computer system to a software application in another must pass through the OSI layers. For example, if a software application in System A has information to transmit to a software application in System B, the application program in System A will pass its information to the application layer (Layer 7) of System A. The application layer then passes the information to the presentation layer (Layer 6), which relays the data to the session layer (Layer 5), and so on down to the physical layer (Layer 1). At the physical layer, the information is placed on the physical network medium and is sent across the medium to System B. The physical layer of System B removes the information from the physical medium, and then its physical layer passes the information up to the data link layer (Layer 2), which passes it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of System B. Finally, the application layer of System B passes the information to the recipient application program to complete the communication process.

INTERACTION BETWEEN OSI MODEL LAYERS

A given layer in the OSI model generally communicates with three other OSI layers:

- The layer directly above it
- The layer directly below it
- Its peer layer in other networked computer systems

The data link layer in System A, for example, communicates with the network layer of System A, the physical layer of System A, and the data link layer in System B. Figure 3-3 illustrates this example.

TABLE 3-1 OSI LAYER - PROTOCOLS RESIDING HERE

Application	SMB, NCP
Presentation	NCP
Session	None
Transport	TCP, SPX, NWLink, NetBEUI
Network	IP, IPX, NetBEUI, DLC, DecNET
Data Link	Media Access Methods/Protocols
Physical	Media Access Methods/Protocols

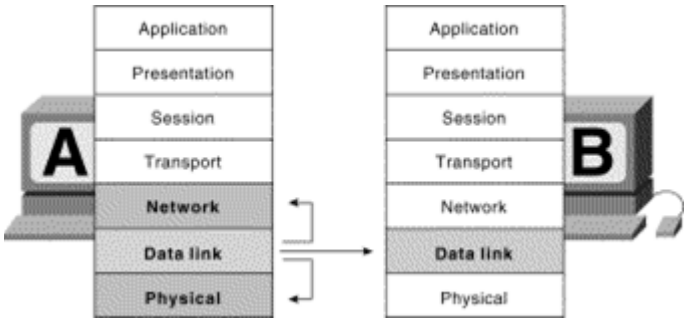
TABLE 3-2 IEEE 802 SPECIFICATIONS

802.1	Internetworking
802.2	LLC (Logical Link Control)
802.3	CSMA/CD - Ethernet
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	MAN (Metropolitan Area Network)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security

TABLE 3-2 IEEE 802 SPECIFICATIONS

802.11	Wireless Networks
802.12	Demand Priority Access LAN, 100 Base VG - AnyLAN

FIGURE 3-3 OSI MODEL LAYERS COMMUNICATE WITH OTHER LAYERS



OSI LAYER SERVICES

One OSI layer communicates with another layer to make use of the services provided by the second layer. The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other computer systems.

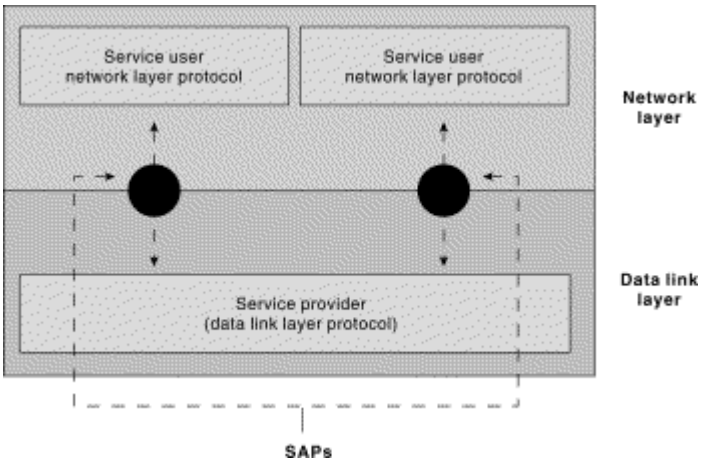
Three basic elements are involved in layer services:

- The service user
- The service provider
- The service access point (SAP).

In this context, the service user is the OSI layer that requests services from an adjacent OSI layer. The service provider is the OSI layer that provides services to service users. OSI layers can provide services to multiple service users. The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer.

Figure 3-4 illustrates how these three elements interact at the network and data link layers.

FIGURE 3-4 SERVICE USERS, PROVIDERS, AND SAPS INTERACT AT THE NETWORK AND DATA LINK LAYERS



OSI MODEL LAYERS AND INFORMATION EXCHANGE

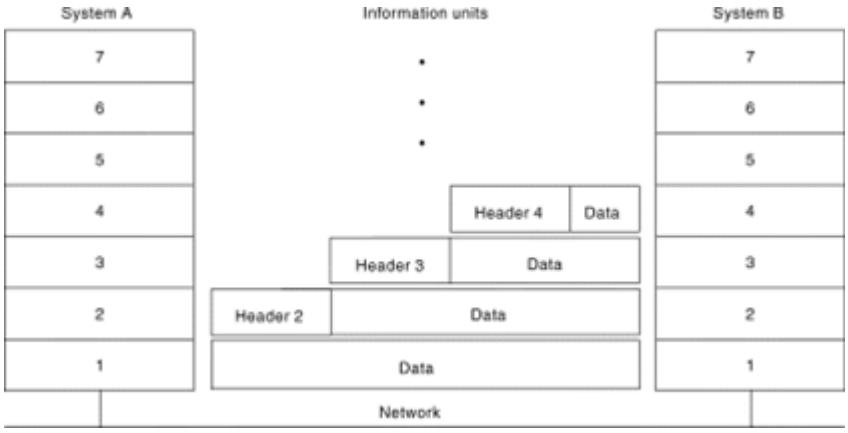
The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions that are exchanged between peer OSI layers.

Control information typically takes one of two forms: headers and trailers. Headers are prepended to data that has been passed down from upper layers. Trailers are appended to data that has been passed down from upper layers. An OSI layer is not required to attach a header or a trailer to data from upper layers.

Headers, trailers, and data are relative concepts, depending on the layer that analyzes the information unit. At the network layer, for example, an information unit consists of a Layer 3 header and data. At the data link layer, however, all the information passed down by the network layer (the Layer 3 header and the data) is treated as data.

In other words, the data portion of an information unit at a given OSI layer potentially can contain headers, trailers, and data from all the higher layers. This is known as encapsulation. Figure 1-6 shows how the header and data from one layer are encapsulated into the header of the next lowest layer.

FIGURE 3-5 HEADERS AND DATA CAN BE ENCAPSULATED DURING INFORMATION EXCHANGE



INFORMATION EXCHANGE PROCESS

The information exchange process occurs between peer OSI layers. Each layer in the source system adds control information to data, and each layer in the destination system analyzes and removes the control information from that data.

If System A has data from a software application to send to System B, the data is passed to the application layer. The application layer in System A then communicates any control information required by the application layer in System B by prepending a header to the data. The resulting information unit (a header and the data) is passed to the presentation layer, which prepends its own header containing control information intended for the presentation layer in System B. The information unit grows in size as each layer prepends its own header (and, in some cases, a trailer) that contains control information to be used by its peer layer in System B. At the physical layer, the entire information unit is placed onto the network medium.

The physical layer in System B receives the information unit and passes it to the data link layer. The data link layer in System B then reads the control information contained in the header prepended by the data link layer in System A. The header is then removed, and the remainder of the information unit is passed to the network layer. Each layer performs the same actions: The layer reads the header from its peer layer, strips it off, and passes the remaining information unit to the next highest layer. After the application layer performs these actions, the data is passed to the recipient software application in System B, in exactly the form in which it was transmitted by the application in System A.

LAYERS OF THE OSI MODEL

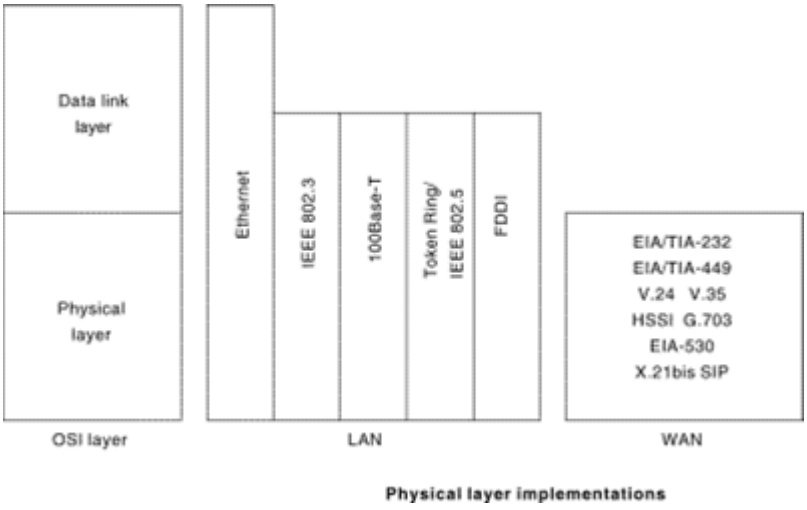
PHYSICAL LAYER

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems.

Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors. Physical layer implementations can be categorized as either LAN or WAN specifications.

Figure 3-6 illustrates some common LAN and WAN physical layer implementations.

FIGURE 3-6 PHYSICAL LAYER IMPLEMENTATIONS CAN BE LAN OR WAN SPECIFICATIONS



DATA LINK LAYER

The data link layer provides reliable transit of data across a physical network link. Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control.

Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer. Network topology consists of the data link layer specifications that often define how devices are to be physically connected, such as in a bus or a ring topology.

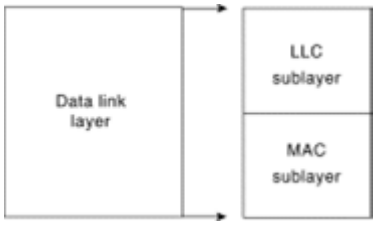
Error notification alerts upper-layer protocols that a transmission error has occurred, and the sequencing of data frames reorders frames that are transmitted out of sequence. Finally, flow control moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the data link layer into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

Figure 3-7 illustrates the IEEE sublayers of the data link layer.

FIGURE 3-7 THE DATA LINK LAYER CONTAINS TWO SUBLAYERS



THE LOGICAL LINK CONTROL (LLC)

The Logical Link Control (LLC) sublayer of the data link layer manages communications between devices over a single link of a network. LLC is defined in the IEEE 802.2 specification and supports both connectionless and connection-oriented services used by higher-layer protocols.IEEE 802.2 defines a number of fields in data link layer frames that enable multiple higher-layer protocols to share a single physical data link.

THE MEDIA ACCESS CONTROL (MAC)

The Media Access Control (MAC) sublayer of the data link layer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer.

NETWORK LAYER

The network layer defines the network address, which differs from the MAC address. Some network layer implementations, such as the Internet Protocol (IP), define network addresses in a way that route selection can be determined systematically by comparing the source network address with the destination network address and applying the subnet mask. Because this layer defines the logical network layout, routers can use this layer to determine how to forward packets. Because of this, much of the design and configuration work for internetworks happens at Layer 3, the network layer.

TRANSPORT LAYER

The transport layer accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer.

Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables data from several applications to be transmitted onto a single physical link. Virtual circuits are established, maintained, and terminated by the transport layer. Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves acting, such as requesting that data be retransmitted, to resolve any errors that occur.

The transport protocols used on the Internet are TCP and UDP.

SESSION LAYER

The session layer establishes, manages, and terminates communication sessions. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session layer. Some examples of session-layer implementations include Zone Information Protocol (ZIP), the AppleTalk protocol that coordinates the name binding process; and Session Control Protocol (SCP), the DECnet Phase IV session layer protocol.

PRESENTATION LAYER

The presentation layer provides a variety of coding and conversion functions that are applied to application layer data. These functions ensure that information sent from the application layer of one system would be readable by the application layer of another system. Some examples of presentation layer coding and conversion schemes include common data representation formats, conversion of character representation formats, common data compression schemes, and common data encryption schemes.

Common data representation formats, or the use of standard image, sound, and video formats, enable the interchange of application data between different types of computer systems. Conversion schemes are used to exchange information with systems by using different text and data representations, such as EBCDIC and ASCII. Standard data compression schemes enable data that is compressed at the source device to be properly decompressed at the destination. Standard data encryption schemes enable data encrypted at the source device to be properly deciphered at the destination.

Presentation layer implementations are not typically associated with a particular protocol stack. Some well-known standards for video include QuickTime and Motion Picture Experts Group (MPEG). QuickTime is an Apple Computer specification for video and audio, and MPEG is a standard for video compression and coding.

Among the well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF). GIF is a standard for compressing and coding graphic images. JPEG is another compression and coding standard for graphic images, and TIFF is a standard coding format for graphic images.

APPLICATION LAYER

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.

This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit.

When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

Some examples of application layer implementations include Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

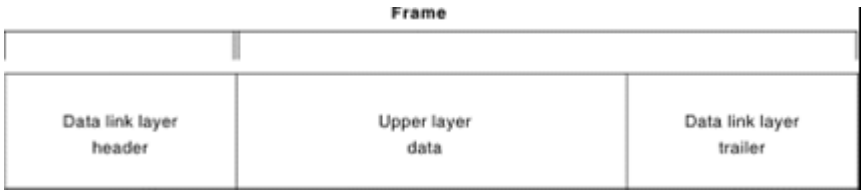
INFORMATION FORMATS

The data and control information that is transmitted through internetworks takes a variety of forms. The terms used to refer to these information formats are not used consistently in the internetworking industry but sometimes are used interchangeably. Common information formats include frames, packets, datagrams, segments, messages, cells, and data units.

A frame is an information unit whose source and destination are data link layer entities. A frame is composed of the data link layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the data link layer entity in the destination system. Data from upper-layer entities is encapsulated in the data link layer header and trailer.

Figure 3-8 illustrates the basic components of a data link layer frame.

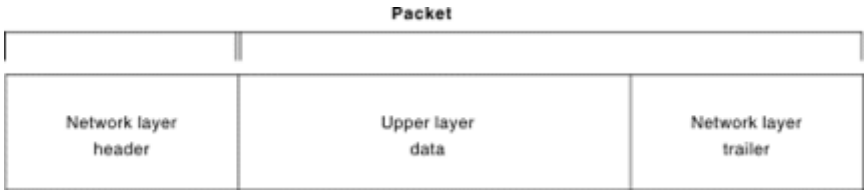
FIGURE 3-8 DATA FROM UPPER-LAYER ENTITIES MAKES UP THE DATA LINK LAYER FRAME



A packet is an information unit whose source and destination are network layer entities. A packet is composed of the network layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the network layer entity in the destination system. Data from upper-layer entities is encapsulated in the network layer header and trailer.

Figure 3-9 illustrates the basic components of a network layer packet.

FIGURE 3-9 THREE BASIC COMPONENTS MAKE UP A NETWORK LAYER PACKET



The term datagram usually refers to an information unit whose source and destination are network layer entities that use connectionless network service.

The term segment usually refers to an information unit whose source and destination are transport layer entities.

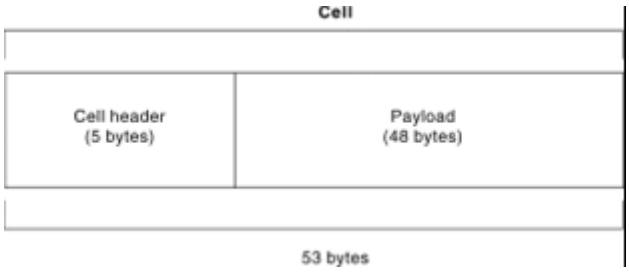
A message is an information unit whose source and destination entities exist above the network layer (often at the application layer).

A cell is an information unit of a fixed size whose source and destination are data link layer entities. Cells are used in switched environments, such as Asynchronous Transfer Mode (ATM) and Switched Multimegabit Data Service (SMDS) networks. A cell is composed of the header and payload. The header contains control information intended for the destination data link layer entity and is typically 5 bytes long. The payload contains upper-layer data that is encapsulated in the cell header and is typically 48 bytes long.

The length of the header and the payload fields always are the same for each cell.

Figure 3-10 depicts the components of a typical cell.

FIGURE 3-10 TWO COMPONENTS MAKE UP A TYPICAL CELL



Data unit is a generic term that refers to a variety of information units. Some common data units are service data units (SDUs), protocol data units, and bridge protocol data units (BPDUs). SDUs are information units from upper-layer protocols that define a service request to a lower-layer protocol. PDU is OSI terminology for a packet. BPDUs are used by the spanning-tree algorithm as hello messages.

THIS PAGE INTENTIONALLY LEFT BLANK.

CHAPTER

4

NETWORK HIERARCHY AND ADDRESSING

ISO HIERARCHY OF NETWORKS

Large networks typically are organized as hierarchies. A hierarchical organization provides such advantages as ease of management, flexibility, and a reduction in unnecessary traffic. Thus, the International Organization for Standardization (ISO) has adopted a number of terminology conventions for addressing network entities.

Key terms defined in this section include:

- End system (ES)
- Intermediate system (IS)
- Area
- Autonomous system (AS)

END SYSTEM (ES)

An ES is a network device that does not perform routing or other traffic forwarding functions. Typical ESs include such devices as terminals, personal computers, and printers.

INTERMEDIATE SYSTEM (IS)

An IS is a network device that performs routing or other traffic-forwarding functions. Typical ISs include such devices as routers, switches, and bridges. Two types of IS networks exist: intradomain IS and interdomain IS. An intradomain IS communicates within a single autonomous system, while an interdomain IS communicates within and between autonomous systems.

AREA

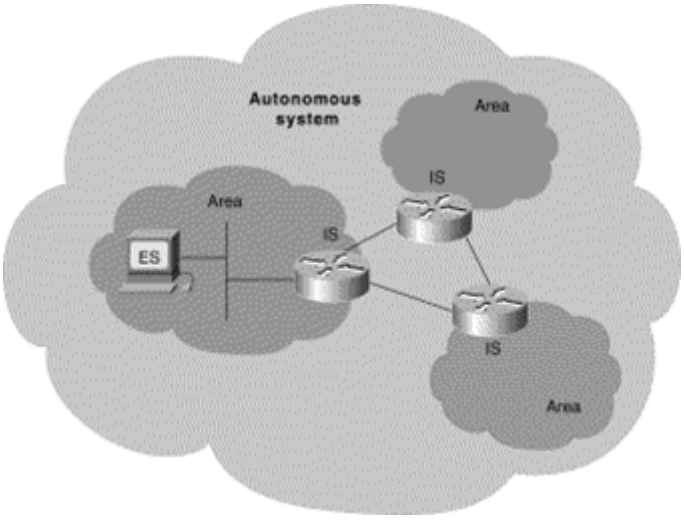
An area is a logical group of network segments and their attached devices. Areas are subdivisions of autonomous systems (AS's).

AUTONOMOUS SYSTEM (AS)

An AS is a collection of networks under a common administration that share a common routing strategy. Autonomous systems are subdivided into areas, and an AS is sometimes called a domain.

Figure 4-1 illustrates a hierarchical network and its components.

FIGURE 4-1 A HIERARCHICAL NETWORK CONTAINS NUMEROUS COMPONENTS



CONNECTION-ORIENTED AND CONNECTIONLESS NETWORKS

In general, transport protocols can be characterized as being either connection-oriented or connectionless. Connection-oriented services must first establish a connection with the desired service before passing any data. A connectionless service can send the data without any need to establish a connection first. In general, connection-oriented services provide some level of delivery guarantee, whereas connectionless services do not.

Connection-oriented service involves three phases:

- Connection establishment
- Data transfer
- Connection termination

CONNECTION ESTABLISHMENT

During connection establishment, the end nodes may reserve resources for the connection. The end nodes also may negotiate and establish certain criteria for the transfer, such as a window size used in TCP connections. This resource reservation is one of the things exploited in some denial of service (DOS) attacks. An attacking system will send many requests for establishing a connection but then will never complete the connection. The attacked computer is then left with resources allocated for many never-completed connections. Then, when an end node tries to complete an actual connection, there are not enough resources for the valid connection.

DATA TRANSFER

The data transfer phase occurs when the actual data is transmitted over the connection. During data transfer, most connection-oriented services will monitor for lost packets and handle resending them. The protocol is generally also responsible for putting the packets in the right sequence before passing the data up the protocol stack. When the transfer of data is complete, the end nodes terminate the connection and release resources reserved for the connection.

CONNECTION TERMINATION

Connection-oriented network services have more overhead than connectionless ones. Connection-oriented services must negotiate a connection, transfer data, and tear down the connection, whereas a connectionless transfer can simply send the data without the added overhead of creating and tearing down a connection. Each has its place in internetworks.

INTERNETWORK ADDRESSES

Identify devices separately or as members of a group. Addressing schemes vary depending on the protocol family and the OSI layer.

Three types of internetwork addresses are commonly used:

- Data link layer addresses
- Media Access Control (MAC) addresses
- Network layer addresses

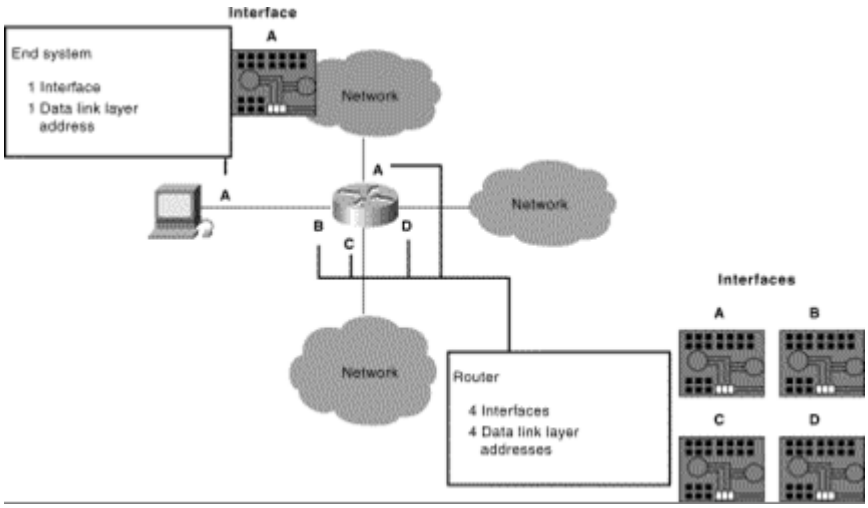
DATA LINK LAYER ADDRESSES

A data link layer address uniquely identifies each physical network connection of a network device. Data-link addresses sometimes are referred to as physical or hardware addresses. Data-link addresses usually exist within a flat address space and have a pre-established and typically fixed relationship to a specific device.

End systems generally have only one physical network connection and thus have only one data-link address. Routers and other internetworking devices typically have multiple physical network connections and therefore have multiple data-link addresses.

Figure 4-2 illustrates how each interface on a device is uniquely identified by a data-link address.

FIGURE 4-2 EACH INTERFACE ON A DEVICE IS UNIQUELY IDENTIFIED BY A DATA-LINK ADDRESS



MAC ADDRESSES

Media Access Control (MAC) addresses consist of a subset of data link layer addresses. MAC addresses identify network entities in LANs that implement the IEEE MAC addresses of the data link layer. As with most data-link addresses, MAC addresses are unique for each LAN interface.

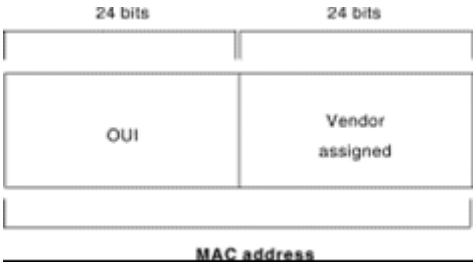
Figure 4-3 illustrates the relationship between MAC addresses, data-link addresses, and the IEEE sublayers of the data link layer.

FIGURE 4-3 MAC ADDRESSES, DATA-LINK ADDRESSES, AND THE IEEE SUBLAYERS OF THE DATA LINK LAYER

MAC addresses are 48 bits in length and are expressed as 12 hexadecimal digits. The first 6 hexadecimal digits, which are administered by the IEEE, identify the manufacturer or vendor and thus comprise the Organizationally Unique Identifier (OUI). The last 6 hexadecimal digits comprise the interface serial number, or another value administered by the specific vendor. MAC addresses sometimes are called burned-in addresses (BIAs) because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the interface card initializes.

Figure 4-4 illustrates the MAC address format.

FIGURE 4-4 THE MAC ADDRESS CONTAINS A UNIQUE FORMAT OF HEXADECIMAL DIGITS



MAPPING ADDRESSES

Because internetworks generally use network addresses to route traffic around the network, there is a need to map network addresses to MAC addresses. When the network layer has determined the destination station's network address, it must forward the information over a physical network using a MAC address. Different protocol suites use different methods to perform this mapping, but the most popular is Address Resolution Protocol (ARP).

Different protocol suites use different methods for determining the MAC address of a device.

The following three methods are used most often.

- Address Resolution Protocol (ARP) maps network addresses to MAC addresses.
- The Hello protocol enables network devices to learn the MAC addresses of other network devices.
- MAC addresses either are embedded in the network layer address or are generated by an algorithm.

Address Resolution Protocol (ARP) is the method used in the TCP/IP suite. When a network device needs to send data to another device on the same network, it knows the source and destination network addresses for the data transfer. It must somehow map the destination address to a MAC address before forwarding the data. First, the sending station will check its ARP table to see if it has already discovered this destination station's MAC address. If it has not, it will send a broadcast on the network with the destination station's IP address contained in the broadcast. Every station on the network receives the broadcast and compares the embedded IP address to its own. Only the station with the matching IP address replies to the sending station with a packet containing the MAC address for the station. The first station then adds this information to its ARP table for future reference and proceeds to transfer the data.

When the destination device lies on a remote network, one beyond a router, the process is the same except that the sending station sends the ARP request for the MAC address of its default gateway. It then forwards the information to that device. The default gateway will then forward the information over whatever networks necessary to deliver the packet to the network on which the destination device resides. The router on the destination device's network then uses ARP to obtain the MAC of the actual destination device and delivers the packet.

The Hello protocol is a network layer protocol that enables network devices to identify one another and indicate that they are still functional. When a new end system powers up, for example, it broadcasts hello messages onto the network. Devices on the network then return hello replies, and hello messages are also sent at specific intervals to indicate that they are still functional. Network devices can learn the MAC addresses of other devices by examining Hello protocol packets.

Three protocols use predictable MAC addresses. In these protocol suites, MAC addresses are predictable because the network layer either embeds the MAC address in the network layer address or uses an algorithm to determine the MAC address. The three protocols are Xerox Network Systems (XNS), Novell Internetwork Packet Exchange (IPX), and DECnet Phase IV.

NETWORK LAYER ADDRESSES

A network layer address identifies an entity at the network layer of the OSI layers. Network addresses usually exist within a hierarchical address space and sometimes are called virtual or logical addresses.

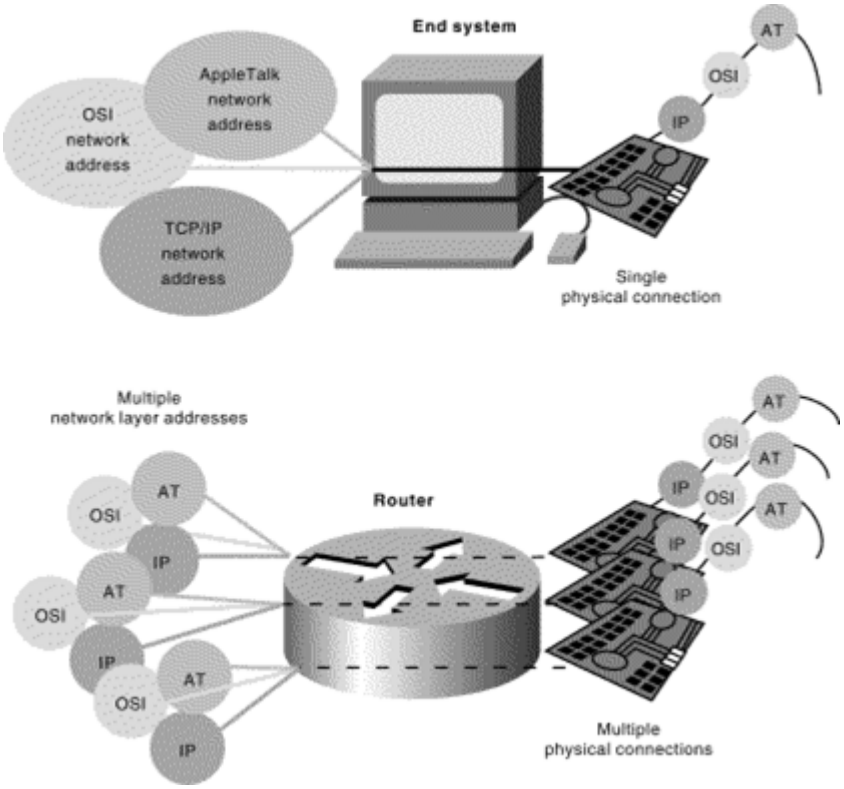
The relationship between a network address and a device is logical and unfixed; it typically is based either on physical network characteristics (the device is on a particular network segment) or on groupings that have no physical basis (the device is part of an AppleTalk zone).

End systems require one network layer address for each network layer protocol that they support. (This assumes that the device has only one physical network connection.) Routers and other internetworking devices require one network layer address per physical network connection for each network layer protocol supported.

For example, a router with three interfaces each running AppleTalk, TCP/IP, and OSI must have three network layer addresses for each interface. The router therefore has nine network layer addresses.

Figure 4-5 illustrates how each network interface must be assigned a network address for each protocol supported.

FIGURE 4-5 EACH NETWORK INTERFACE MUST BE ASSIGNED A NETWORK ADDRESS FOR EACH PROTOCOL SUPPORTED



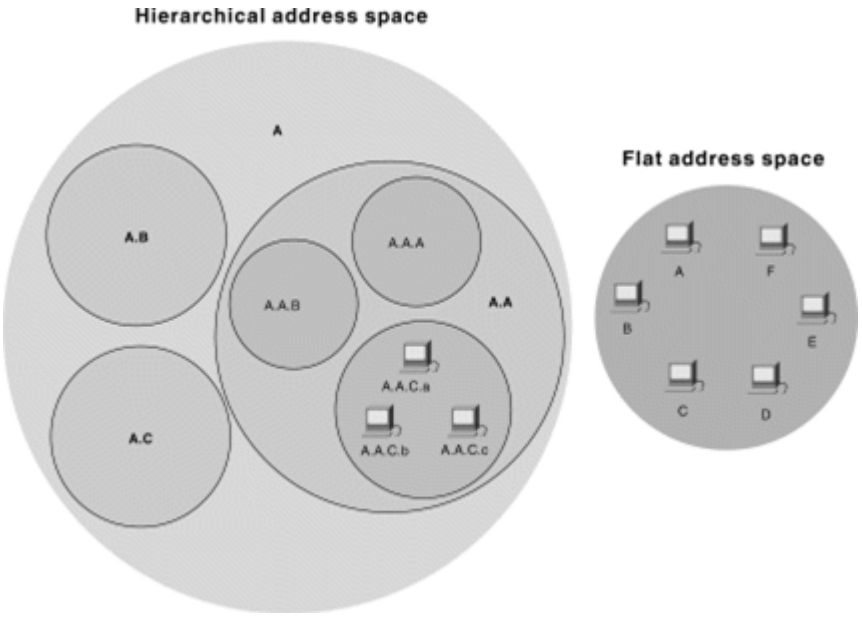
HIERARCHICAL VERSUS FLAT ADDRESS SPACE

Internetwork address space typically takes one of two forms: hierarchical address space or flat address space. A hierarchical address space is organized into numerous subgroups, each successively narrowing an address until it points to a single device (in a manner similar to street addresses). A flat address space is organized into a single group (in a manner similar to U.S. Social Security numbers).

Hierarchical addressing offers certain advantages over flat-addressing schemes. Address sorting and recall is simplified using comparison operations. For example, "Ireland" in a street address eliminates any other country as a possible location.

Figure 4-6 illustrates the difference between hierarchical and flat address spaces.

FIGURE 4-6 HIERARCHICAL AND FLAT ADDRESS SPACES DIFFER IN COMPARISON OPERATIONS



ADDRESS ASSIGNMENTS

Addresses are assigned to devices as one of two types:

- Static
- Dynamic

STATIC

Static addresses are assigned by a network administrator according to a preconceived internetwork addressing plan. A static address does not change until the network administrator manually changes it.

DYNAMIC

Dynamic addresses are obtained by devices when they attach to a network, by means of some protocol-specific process. A device using a dynamic address often has a different address each time that it connects to the network. Some networks use a server to assign addresses (a DHCP server). Server-assigned addresses are recycled for reuse as devices disconnect. A device is therefore likely to have a different address each time that it connects to the network.

ADDRESSES VERSUS NAMES

Internetwork devices usually have both a name and an address associated with them. Internetwork names typically are location-independent and remain associated with a device wherever that device moves (for example, from one building to another). Internetwork addresses usually are location-dependent and change when a device is moved (although MAC addresses are an exception to this rule). As with network addresses being mapped to MAC addresses, names are usually mapped to network addresses through some protocol.

The Internet uses Domain Name System (DNS) to map the name of a device to its IP address. For example, it's easier for you to remember www.cisco.com instead of some IP address. Therefore, you type www.cisco.com into your browser when you want to access Cisco's web site. Your computer performs a DNS lookup of the IP address for Cisco's web server and then communicates with it using the network address.

CHAPTER

5

NETWORK FLOW CONTROL AND MULTIPLEXERS

FLOW CONTROL BASICS

Flow control is a function that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. A high-speed computer, for example, may generate traffic faster than the network can transfer it, or faster than the destination device can receive and process it.

The three commonly used methods for handling network congestion are:

- Buffering
- Transmitting source-quench messages
- Windowing

BUFFERING

Buffering is used by network devices to temporarily store bursts of excess data in memory until they can be processed. Occasional data bursts are easily handled by buffering. Excess data bursts can exhaust memory, however, forcing the device to discard any additional datagrams that arrive.

SOURCE-QUENCH MESSAGES

Source-quench messages are used by receiving devices to help prevent their buffers from overflowing. The receiving device sends source-quench messages to request that the source reduce its current rate of data transmission. First, the receiving device begins discarding received data due to overflowing buffers. Second, the receiving device begins sending source-quench messages to the transmitting device at the rate of one message for each packet dropped. The source device receives the source-quench messages and lowers the data rate until it stops receiving the messages. Finally, the source device then gradually increases the data rate as long as no further source-quench requests are received.

WINDOWING

Windowing is a flow-control scheme in which the source device requires an acknowledgment from the destination after a certain number of packets have been transmitted. With a window size of 3, the source requires an acknowledgment after sending three packets, as follows. First, the source device sends three packets to the destination device. Then, after receiving the three packets, the destination device sends an acknowledgment to the source. The source receives the acknowledgment and sends three more packets. If the destination does not receive one or more of the packets for some reason, such as overflowing buffers, it does not receive enough packets to send an acknowledgment. The source then retransmits the packets at a reduced transmission rate.

ERROR-CHECKING BASICS

Error-checking schemes determine whether transmitted data has become corrupt or otherwise damaged while traveling from the source to the destination. Error checking is implemented at several of the OSI layers. One common error-checking scheme is the cyclic redundancy check (CRC), which detects and discards corrupted data.

Error-correction functions (such as data retransmission) are left to higher-layer protocols. A CRC value is generated by a calculation that is performed at the source device. The destination device compares this value to its own calculation to determine whether errors occurred during transmission. First, the source device performs a predetermined set of calculations over the contents of the packet to be sent. Then, the source places the calculated value in the packet and sends the packet to the destination. The destination performs the same predetermined set of calculations over the contents of the packet and then compares its computed value with that contained in the packet. If the values are equal, the packet is considered valid. If the values are unequal, the packet contains errors and is discarded.

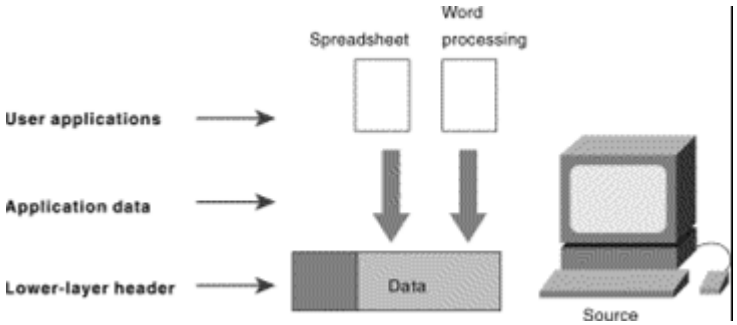
MULTIPLEXING BASICS

Multiplexing is a process in which multiple data channels are combined into a single data or physical channel at the source. Multiplexing can be implemented at any of the OSI layers.

Conversely, demultiplexing is the process of separating multiplexed data channels at the destination. One example of multiplexing is when data from multiple applications is multiplexed into a single lower-layer data packet.

Figure 5-1 illustrates this example.

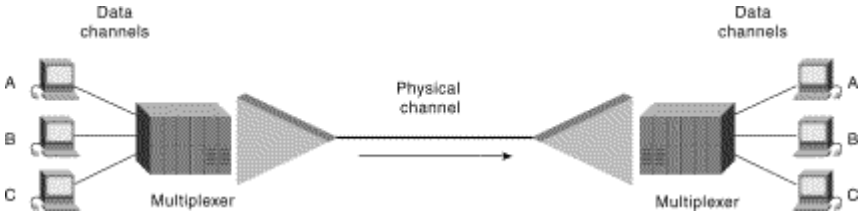
FIGURE 5-1 MULTIPLE APPLICATIONS CAN BE MULTIPLEXED INTO A SINGLE LOWER-LAYER DATA PACKET



Another example of multiplexing is when data from multiple devices is combined into a single physical channel (using a device called a multiplexer).

Figure 5-2 illustrates this example.

FIGURE 5-2 MULTIPLE DEVICES CAN BE MULTIPLEXED INTO A SINGLE PHYSICAL CHANNEL



A multiplexer is a physical layer device that combines multiple data streams into one or more output channels at the source. Multiplexers demultiplex the channels into multiple data streams at the remote end and thus maximize the use of the bandwidth of the physical medium by enabling it to be shared by multiple traffic sources. Some methods used for multiplexing data are:

- Time-division multiplexing (TDM)
- Asynchronous time-division multiplexing (ATDM)

- Frequency-division multiplexing (FDM)
- Statistical multiplexing

TIME-DIVISION MULTIPLEXING

In TDM, information from each data channel is allocated bandwidth based on preassigned time slots, regardless of whether there is data to transmit.

ASYNCHRONOUS TIME-DIVISION MULTIPLEXING

In ATDM, information from data channels is allocated bandwidth as needed by using dynamically assigned time slots.

FREQUENCY-DIVISION MULTIPLEXING

In FDM, information from each data channel is allocated bandwidth based on the signal frequency of the traffic.

STATISTICAL MULTIPLEXING

In statistical multiplexing, bandwidth is dynamically allocated to any data channels that have information to transmit.

THIS PAGE INTENTIONALLY LEFT BLANK.

CHAPTER

6

NETWORK DEVICES-TYPES AND BASIC OPERATION

ETHERNET DEVICES

Table 6-1 shows Ethernet Devices and their primary OSI operational layer.

TABLE 6-1 ETHERNET DEVICES - THEIR PRIMARY OSI OPERATIONAL LAYER

Repeater	Physical
Bridge	Data Link (MAC Sublayer)
Remote Bridge	Data Link (MAC Sublayer)
Router	Network
Brouter	Data Link and Network
Gateway	Transport, Session, Presentation and Application
Multiplexer	Physical
Switch	Data Link

SPANNING TREE ALGORITHM

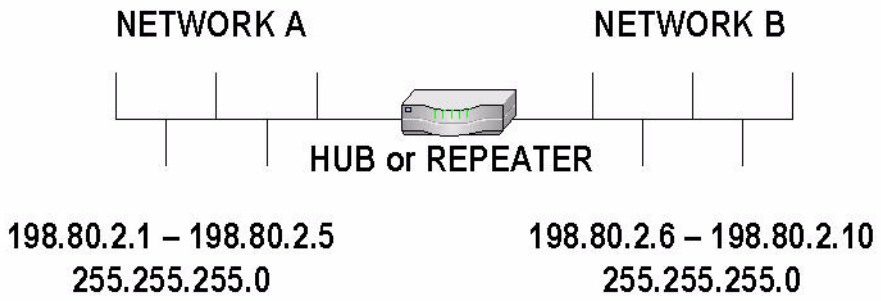
Spanning Tree Algorithm was developed for bridges to determine the most efficient network in path when there are multiple paths to choose from.

MULTIPLEXING

Several signals from different sources are collected into the component and are fed into one cable for transmission.

HUBS AND REPEATERS

FIGURE 6-1 HUBS AND REPEATERS



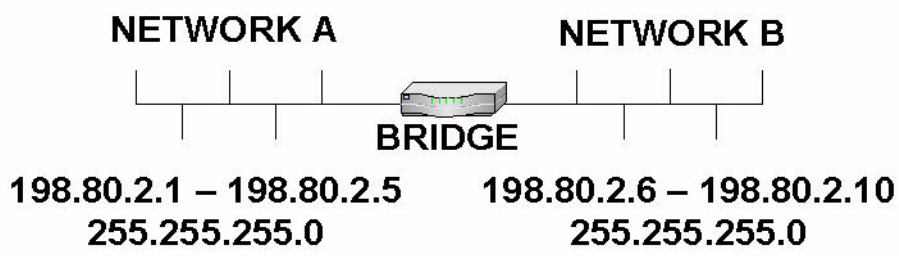
The Ethernet packets on the network illustrated in Figure 6-1 will be allowed unimpeded passage through the Hub or Repeater device. The Hub or Repeater simply re-amplifies and then forwards the packets between the 2 networks (both networks share the same network of subnetwork addressing scheme).

FEATURES OF HUBS

- Operate at the physical layer of the OSI model
- Perform Data packet signal retiming and amplification
- Perform Link Integrity Test on each port
- Provide port autopartitioning, which disconnects the port in the event of 30 consecutive collisions or jabber input
- Send packets through all its ports except the one that received it (even collisions!)
- Do NOT provide network segmentation
- Maximum of three concentrators (the three-repeater rule) in the data path between any two nodes applies

BRIDGES

FIGURE 6-2 BRIDGES



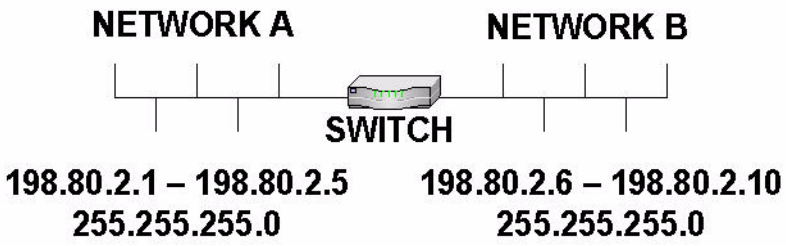
The Ethernet packets on the network illustrated in Figure 6-2 will be allowed unimpeded passage through the bridging device - only if the destination MAC address is on the opposite side of the Bridge. The Bridge verifies that the destination MAC address of the packets resides on the opposite side of the Bridge, at which time the Bridge re-amplifies and then forwards the packets between the 2 networks (again, both networks share the same network of subnetwork addressing scheme). If the Bridge determines that the destination MAC address resides on the same side of the network as the source of the packet, the bridge will not forward the packet to the second network. A Bridge would be considered a Layer 2 device.

FEATURES OF BRIDGES

- Connect two separate network segments to form a single logical network
- Can connect similar or different networks (e.g. Ethernet to Ethernet or Ethernet to Token Ring)
- Operate at the data link layer of the OSI model and rely on MAC addresses for their operation
- Provide network segmentation
- Have storage capacity to store frames and act as a store-and-forward device
- Each bridge port has a unique MAC address itself
- Do not propagate Ethernet collisions
- Help solve traffic bottleneck problems
- Cannot make decisions about packet routes
- Cannot prevent broadcast storms. They use every 60 seconds broadcasts to communicate with other bridges

SWITCHES

FIGURE 6-3 SWITCHES



The Ethernet packets on the network illustrated in Figure 6-3 will be allowed unimpeded passage through the switching device - only if the destination MAC address is on the opposite side of the Switch. The Switch verifies that the destination MAC address of the packets resides on the opposite side of the Switch, at which time the Switch re-amplifies and then forwards the packets between the 2 networks (again, both networks share the same network of subnetwork addressing scheme). If the Switch determines that the destination MAC address resides on the same side of the network as the source of the packet, the Switch will not forward the packet to the second network. A Switch would be considered a Layer2 device. A Switch can provide some basic Network Layer routing services, has a higher packet per second throughput than a Bridge, and will reset the “hop” count in a network.

FEATURES OF SWITCHES

- Operate at the data link layer of the OSI model and rely on MAC addresses for their operation
- Can be described as multiport bridges
- Allow dedicate maximum bandwidth availability on every switched port
- Provide network segmentation
- Use modern Application Specific Integrated Circuits (ASIC) technology and RISC processors
- Can contain network-layer routing services as well as MAC-layer switching services
- Require very little configuration
- Provide more aggregate bandwidth to the network
- Allow the creation of Virtual LANs (VLAN)

THE 5-4-3 RULE

The 5-4-3 rule is a design guideline for 10baseT Ethernet Networks that make use of only hubs/repeaters and do not contain bridges, switches or routers, these devices negate the rule. For an Ethernet LAN of any size to operate the 5-4-3 rule must apply with regards to hubs. There may be a maximum of 5 segments between two hosts in a network, and there may be at most 4 hubs between these hosts and finally there may only be users on 3 of the segments.

See the Figure 6-5 below.

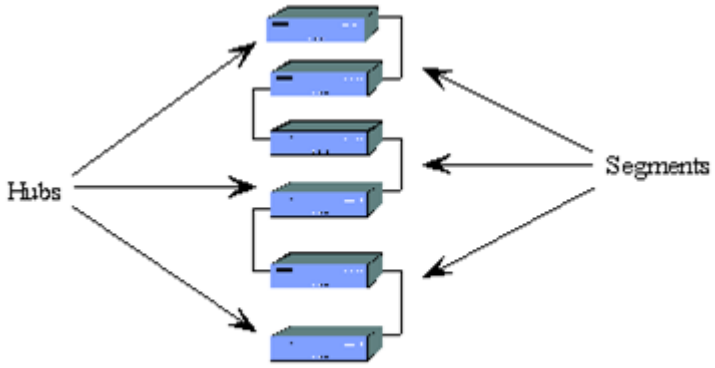
What are hosts?

Hosts may be servers, workstations or printers.

Where would I likely find a violation of the 5-4-3 Rule in my network?

Check for series of hubs "daisy chained" together with cross-over cables as shown in Figure 6-4 if a host was attached to the top hub and another host attached to the bottom hub the 5-4-3 Rule would be violated, since there would be 6 hubs and 7 segments between the 2 hosts.

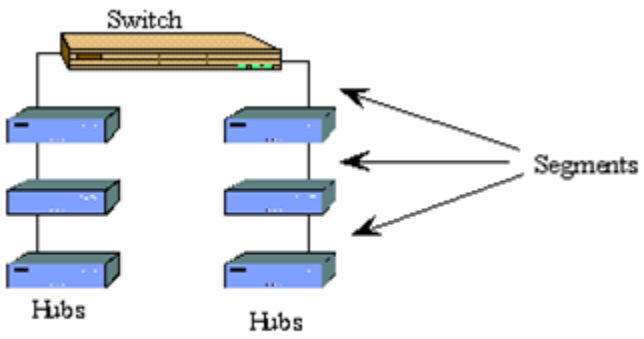
FIGURE 6-4 5-4-3 RULE



How might I fix this violation?

Add a switch or router to the stack and modify how each hub is attached to the stack of hubs as shown in Figure 6-5

FIGURE 6-5 SWITCH



By inserting a switch or router into the stack as shown above any host to host communication will not violate the 5-4-3 rule regardless of where they are attached. Remember that the switch or router negates the 5-4-3 rule since there are not any more than 4 hubs/repeaters or 5 segments between any host attached with out passing through the switch or router. This is only one possible solution, there are many more.

FIGURE 6-6 ILLUSTRATION OF THE 5-4-3 RULE

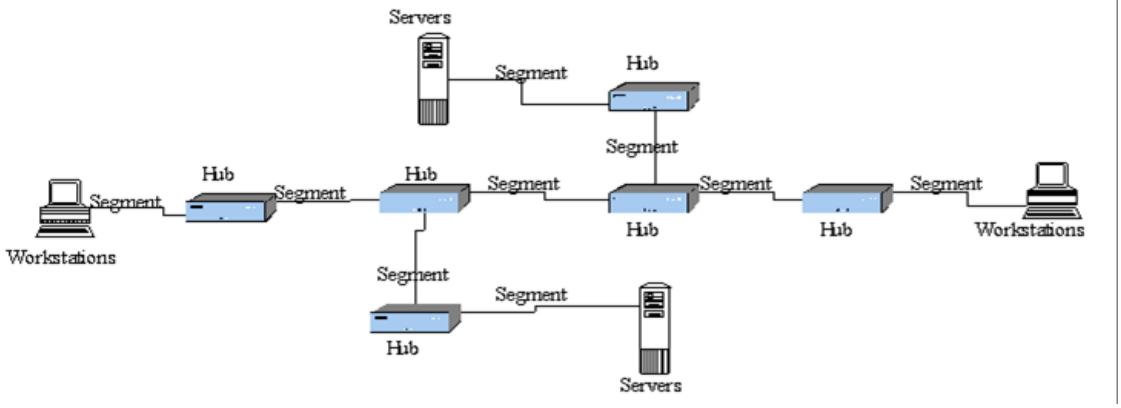
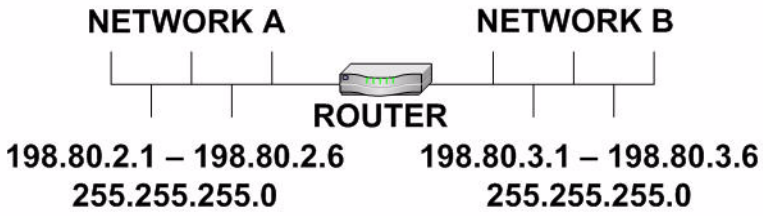


Figure 6-6 shows the limits of the 5-4-3 rule where there are 4 hubs and 5 segments between the workstations on the left and the workstations on the right.

ROUTERS

FIGURE 6-7 ROUTERS



The Ethernet packets on the network illustrated in Figure 6-7 would only be forwarded/routed through the router if the Router determined that the destination IP address of the packet was to reside on the opposite side of the Router (the Router maintains a routing table which contains all of the IP and MAC addresses for every device on each network). The router verifies that the destination IP address of the packets resides on the opposite side of the Router, at which time the Router re-amplifies and then forwards/routes the packets between the 2 networks (both networks must have different network or subnetwork addressing schemes). If the Router determines the destination IP address resides on the same network as the source of the packet, the Router will not forward/route the packet to the second network. A router would be considered a Layer3 device.

FEATURES OF ROUTERS

- Connect two separate physical networks to form a single logical network
- Can connect similar or different networks using similar or different network protocols (e.g. IPX and IP)
- Operate at the network layer of the OSI model and they rely on network and node addresses for their operation
- Provide network segmentation
- Are aware of many possible paths to get to a destination and are aware also of which path is optimal by using cost metrics
- Cost metrics are usually based on hops
- A hop is a path between two store-and-forward devices such as a router
- They store routing tables and are slower than bridges
- They can use dynamic or static routing tables
- Dynamic routing tables are set and updated automatically via the Routing Information Protocol (RIP), Open Shortest Path First (OSPF), XNS or other routing protocols. Static routing tables are entered manually into the router. Not all network protocols are routable. For example the NetBIOS protocol is not routable and it cannot cross a router, but it can cross a bridge
- Can filter out certain type of network traffic and prevent broadcast storms
- In an IP network a router decrements the Time To Live (TTL) by at least 1 or more. If the TTL reaches zero, the packet is discarded

THIS PAGE INTENTIONALLY LEFT BLANK.

CHAPTER 7

STANDARDS ORGANIZATIONS

A wide variety of organizations contribute to internetworking standards by providing forums for discussion, turning informal discussion into formal specifications, and proliferating specifications after they are standardized.

Most standards organizations create formal standards by using specific processes: organizing ideas, discussing the approach, developing draft standards, voting on all or certain aspects of the standards, and then formally releasing the completed standard to the public.

Some of the best-known standards organizations that contribute to internetworking standards include these:

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO is an international standards organization responsible for a wide range of standards, including many that are relevant to networking. Its best-known contribution is the development of the OSI reference model and the OSI protocol suite.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI, which is also a member of the ISO, is the coordinating body for voluntary standards groups within the United States. ANSI developed the Fiber Distributed Data Interface (FDDI) and other communications standards.

ELECTRONIC INDUSTRIES ASSOCIATION (EIA)

EIA specifies electrical transmission standards, including those used in networking. The EIA developed the widely used EIA/TIA-232 standard (formerly known as RS-232).

INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS (IEEE)

IEEE is a professional organization that defines networking and other standards. The IEEE developed the widely used LAN standards IEEE 802.3 and IEEE 802.5.

INTERNATIONAL TELECOMMUNICATION UNION TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T)

Formerly called the Committee for International Telegraph and Telephone (CCITT), ITU-T is now an international organization that develops communication standards. The ITU-T developed X.25 and other communications standards.

INTERNET ACTIVITIES BOARD (IAB)

IAB is a group of internetwork researchers who discuss issues pertinent to the Internet and set Internet policies through decisions and task forces. The IAB designates some Request For Comments (RFC) documents as Internet standards, including Transmission Control Protocol/ Internet Protocol (TCP/IP) and the Simple Network Management Protocol (SNMP).

CHAPTER

8

NETWORK PHYSICAL MEDIA

ETHERNET TRANSMISSION PHYSICAL MEDIA

There are three major forms of transmission media used for LANs:

- Twisted Pair Ethernet Medium:2-pair Category 5 Cable
- Data Rate: 10 Mbit/s (10BASE-T),100 Mbit/s (100BASE-TX)
- Segment Length: max. 100 m (point-to-point)Connection:RJ45 Connector

TWISTED PAIR

Two insulated copper wires twisted together in a regular spiral pattern; one pair establishes one communication link; it transmits electromagnetic signals. Twisted pairs are distinguished between shielded and unshielded twisted pairs according to their protection against electromagnetic fields.

FIGURE 8-1 TWISTED PAIR

CONNECTIONS USING TWISTED PAIR

FIGURE 8-2 CROSSOVER ETHERNET CABLE PINOUTS

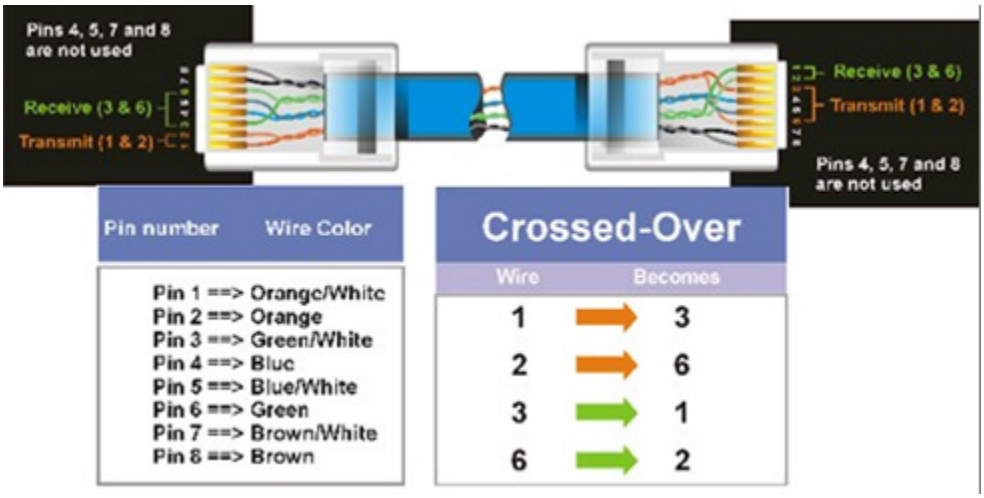
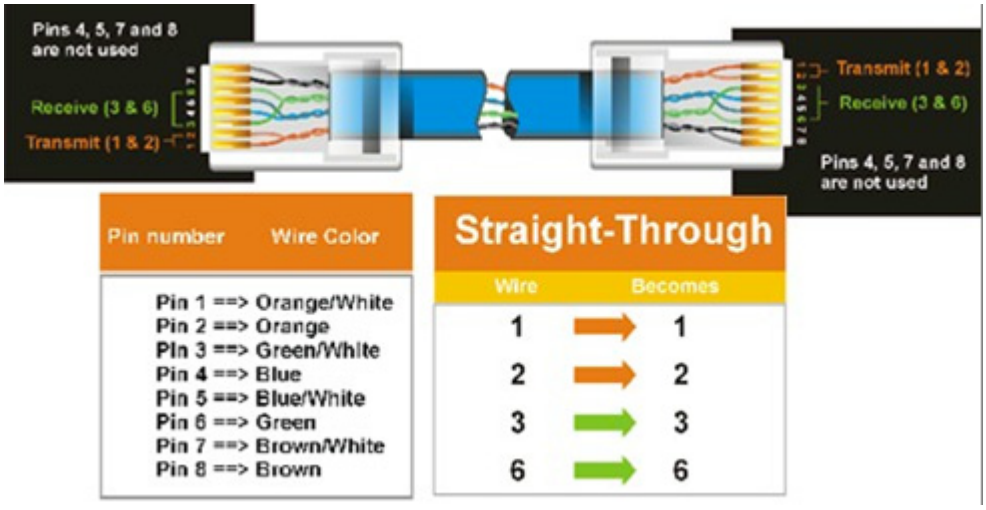


FIGURE 8-3 STANDARD ETHERNET CABLE PINOUTS



COAXIAL CABLE

A single insulated inner wire is surrounded by a cylindrical conductor which is covered with a shield; it transmits electromagnetic signals. Coaxial cable is classified into two categories: baseband (uses digital signals) and broadband (uses analog signals) coaxial cable.

Original Ethernet Other Names: Yellow Cable ThickwireMedium:Coaxial cable

Data Rate: 10 MbpsSegment Length:max. 500 mUsers:max. 100

Transceivers/segment Termination: 50 Ohm, 1 WattConnection:via Transceiver with Vampire tap

FIGURE 8-4 COAXIAL CABLE

FIBER OPTIC

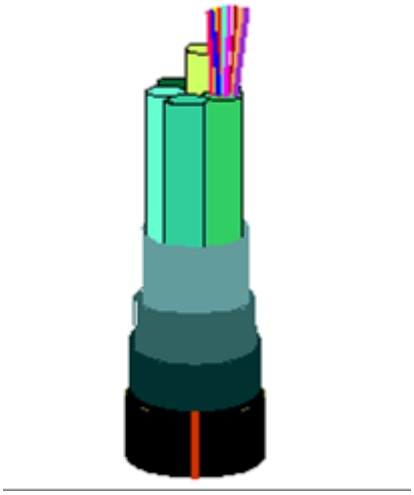
Consists of three concentric sections, the core (a fiber conducting optical rays), the cladding (reflecting optical rays) and the jacket (surrounding one or many fibers to protect them); transmits optical signals, which must be transformed to electromagnetic signals.

Fiber Optic EthernetMedium: 2 Fiber Pairs 50/125 or 62, 5/125)

Data Rate: 10 Mbit/s (10BASE-FL), 100 Mbit/s (100BASE-FX)

Segment Length: max. 2000 m (point-to-point)Connection:ST Connector (10-BASE-FL) Duplex SC Connector (100BASe-FX)

FIGURE 8-5 FIBER OPTIC



Each transmission media has its own advantages and disadvantages. They differ in costs, capacity, possible length, and electromagnetic isolation. Which media to be chosen depends on three other characterization features of LANs: firstly, which topology is to be implemented. Secondly, which capacity and reliability are needed.

OPTICAL COMMUNICATION SERVICES

SONET = Synchronous Optical Network

- Long term solution for a mid-span-meet between vendors
- SONET is synchronous
- Adding and/or dropping signals with single multiplexing process

Optical Communications Service Grades

- OC1: 51.84 Mbps
- OC3: 155.52 Mbps
- OC12: 622.08 Mbps
- OC48: 2.488 Gbps

Plans in motion for rates of ~10 Gbps

- Optical networking systems
- Fiber Distributed Data Interface (FDDI; 100 Mbps)
- High Performance Parallel Interface (HIPPI: 0.8 - 1.6 Gbps); can also be used over copper

CHAPTER 9

ETHERNET TERMS

TABLE 9-1 IRQ (INTERRUPT REQUESTS)

IRQ 1	Keyboard
IRQ 2(9)	Video Card
IRQ 3	Com2, Com4
IRQ 4	Com1, Com3
IRQ 5	Available (Normally LPT2 or sound card)
IRQ 6	Floppy Disk Controller
IRQ 7	Parallel Port (LPT1)
IRQ 8	Real-time clock
IRQ 9	Redirected IRQ2
IRQ 10	Available
IRQ 11	Available
IRQ 12	PS/2 Mouse
IRQ 13	Math Coprocessor
IRQ 14	Hard Disk Controller
IRQ 15	Available

TABLE 9-2 STANDARD TOPOLOGIES

Bus	A single cable (trunk) that connects all computers in a single line.
Star	Computers connect to a centralized hub via cable segments.

TABLE 9-2 STANDARD TOPOLOGIES

Ring	Connects all computers on a single cable. Ends are not terminated, but form a full loop connecting the last computer to the first computer.
Mesh	Commonly used in WAN configurations. Routers are connected to multiple links for redundancy and to give the ability to determine the quickest route to a destination.

TABLE 9-3 ACCESS METHODS

CSMA/CD Collision Detection	Listens to cable prior to sending data. (Ethernet)
CSMA/CA Collision Avoidance	Announces intention to send data. (AppleTalk)Token-Passing - Token revolves around ring, computer which has token is permitted to pass/ forward data (Token Ring). One device designated media administrator. Secondary device waits to be polled by primary device to check if it has data to be sent.

TABLE 9-4 IBM CABLING SYSTEM

Thinnet Coaxial	.25 inches thick, carries signal 185 meters. Known as RG-58 family, and has a 50 ohm impedance.
RG-58 /U	Solid Copper Core
RG-58 A/U	Stranded Wire Core
RG-58 C/U	Military Specification of RG-58 A/U
RG-59	Broadband transmission (Television Cable)
RG-62	ArcNet Network Cable When troubleshooting Thinnet coaxial cable, the cable terminator must read 50 ohms, and the cable and connector must measure infinite.
Thicknet Coaxial	.5 inches thick, carries signal 500 meters. A transceiver (Vampire Tap) is used to make a physical connection with the Thicknet core.
Unshielded Twisted Pair (UTP)	Twisted pair wiring, carries signal 100 meters. Is susceptible to crosstalk.
Shielded Twisted Pair (STP)	Twisted pair wiring, carries signal 100 meters. Has foil or braided jacket around wiring to help reduce crosstalk and to prevent electromagnetic interference.

TABLE 9-5 WIRING TRANSPORT TERMS

Attenuation	The degrading of a signal as it travels farther from its origination.
Crosstalk	Signal overflow from one wire to another adjacent wire.
Jitter	Instability in a signal wave. Caused by signal interference or an unbalanced FDDI ring or Token Ring.
Packet Switching	Packets are relayed across network along the best route available.
Beaconing	Computers are used to detect network faults, then transmit the fault signal to the server.

TABLE 9-6 UTP/STP CATEGORY SPEEDS

Cat 2	4 mbps
Cat 3	10 mbps
Cat 4	16 mbps
Cat 5	100 mbps
Fiber-Optic	Carries light pulse signals through glass core at speeds of between 10 Mbps – 10,000 Mbps.

TABLE 9-7 ETHERNET SPECIFICATIONS

Type	Cable Types	Connection Type	Max Length
10Base2	RG-58 Thinnet coaxial cable	BNC T Connector	185 meters (607 ft.)
10Base5	Thicknet coaxial cable	DIX/AUI	500 meters (1640 ft.)
10BaseT	Category 3, 4, or 5 UTP cable	RJ-45	100 meters (328 ft.)
100BaseT	Category 5 UTP cable	RJ-45	100 meters (328 ft.)

TABLE 9-8 SIGNAL TRANSMISSIONS

Baseband	Uses digital signaling over a single frequency. Transmits bi-directionally.
Broadband	Uses analog signaling over a range of frequencies. Transmits unidirectionally and uses amplifiers for signal regeneration.

QOS (QUALITY OF SERVICE)

Short for Quality of Service, a networking term that specifies a guaranteed throughput level. A broadly used term that refers to the performance attributes of an end-to-end connection. A QoS definition for data would address attributes such as error rates, lost packet rates, throughput, and delay. The IEEE 802.1p, 802.1Q and 802.1D standards define how Ethernet switches can classify frames in order to expedite delivery of time-critical traffic (I.e. the TOS bit within the IP frame).

TABLE 9-9 OSI MODEL

Application Layer (layer 7)	Allows applications to use the network. Handles network access, flow control and error recovery.
Presentation Layer (layer 6)	Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression.
Session Layer (layer 5)	Allows applications on connecting systems to establish a session. Provides synchronization between communicating computers.
Transport Layer (layer 4)	Responsible for packet handling. Ensures error-free delivery. Repackages messages into smaller packets, and handles error handling.
Network Layer (layer 3)	Translates system names into addresses. Responsible for addressing, determining routes for sending, managing network traffic problems, packet switching, routing, data congestion, and reassembling data.
Data Link Layer (layer 2)	Sends data from network layer to physical layer. Manages physical layer communications between connecting systems.
LLC (layer 2)	(802.2) Manages link control and defines SAP's (Service Access Points).

TABLE 9-9 OSI MODEL

MAC (layer 2)	(802.3, 802.4, 802.5, 802.12) Communicates with adapter card.
Physical Layer (layer 1)	Transmits data over a physical medium. Defines cables, cards, and physical aspects.

TABLE 9-10 LAN ENHANCEMENT COMPONENTS

Repeater	regenerates signals for retransmission. Moves packets from one physical media to another. Will pass broadcast storms. Cannot connect different network topologies or access methods.
Bridges	are used to segment networks. They forward packets based on address of destination node. Uses RAM to build a routing table based on hardware addresses. Will connect dissimilar network topologies. Will forward all protocols. Regenerates the signal at the packet level.
Remote Bridge	Same as bridge, but used for telephone communications. Uses STA (Spanning Tree Algorithm).
Router	routes packets across multiple networks. Uses RAM to build a routing table based on network addresses (i.e. TCP address). Shares status and routing information to other routers to provide better traffic management and bypass slow connections. Will not pass broadcast traffic. Are slower than bridges due to complex functions. Strips off Data Link Layer source and destination addresses and then recreates them for packets. Routers can accommodate multiple active paths between LAN segments. Will not pass unroutable protocols.
Brouter	Will act as a router for specified protocols and as a bridge for other specified protocols.
Gateway	Used for communications between different NOS's (i.e. Windows NT and IBM SNA). Takes the packet, strips off the old protocol and repackages it for the receiving network.
Multiplexer Device	that can divide transmissions into two or more channels. Switches - Hub with bridging capabilities. Switch filters traffic through MAC addresses. Creates sessions on ports within the hub. Used when upgrading to 100mb Fast Ethernet.

TABLE 9-11 PROTOCOLS

Routable	TCP/IP, IPX/SPX, OSI, AppleTalk, DecNET, XNS. Non-routable - NetBEUI, DLC, LAT.
NetBEUI	Microsoft protocol designed for small LANs; non-routable. Not compatible with UNIX networks.
IPX/SPX	Fast protocol for small and large Novell networks; is routable. Also known in NT as NWLink.
TCP/IP	Internet protocol; is routable. Used by UNIX networks.
DecNET	Defines communications over FDDI MANs; is routable. AppleTalk - Apple protocol designed for small LAN file and print sharing; is routable.
RIP (Routing Information Protocol)	Routers use this to communicate with each other to determine the least busy and shortest network routes.
OSPF (Open Shortest Path First)	Routers use this to communicate with each other to determine the shortest network routes.
NDIS (Microsoft) and ODI (Novell)	are used to bind multiple protocols to a network adapter.
SLIP (Serial Line IP)	Provides dial-up communications, but is unable to simultaneously transfer multiple protocols.
PPP (Point-to-Point Protocol)	Performs dynamic IP addressing, multi-protocol support, password login and error control. Common TCP/IP problems are caused by incorrect subnet masks and default gateways. Incorrect frame types will cause problems between two systems using IPX/SPX.

TABLE 9-12 COMPUTER NAME RESOLUTION

DNS (Domain Name Services)	Used to resolve DNS host name to an IP address.
WINS (Windows Internet Naming Service)	Used to resolve NetBIOS computer name to an IP address.
HOSTS	File which contains mappings between DNS host names and their IP addresses.
LMHOSTS	File which contains mappings between NetBIOS computer names and their IP addresses.

TABLE 9-13 PACKET SWITCHING NETWORKS

Type	Function
X.25	Designed to connect remote terminals to mainframe host systems. Is very slow due to constant error-checking. Frame Relay - Point-to-point system which uses digital leased lines. Will provide bandwidth as needed. Requires frame relay capable bridge or router for transmission.
ATM	Advanced implementation of packet switching. Transmits at speeds of 155Mbps to 622Mbps with capabilities of higher speeds. Transmits data in 53 byte (48 application, 5 header) cells. Uses switches as multiplexers to permit several computers to simultaneously transmit data on a network. Great for voice and video communications.
ISDN	Transmits at 128k/sec. Has three data channels - 2 B channels @ 64k/sec & 1 D channel @ 16k/sec. The B channels carry data while the D channel performs link management and signaling.
FDDI	100 Mbps token-passing ring network which uses fiber-optic media. Uses a dual-ring topology for redundancy and in case of ring failure. Each ring is capable of connecting 500 computers over 100 kilometers (62 miles). Can be used as a network backbone. Uses beaconing for ring troubleshooting.

TABLE 9-14 SECURITY LEVELS

Share-level security	Used in Windows 95 to share resources. A password is needed to access the resource.
User-level security	Used in Windows NT to share resources. When you attempt to access a shared resource, the server will make sure your user account has been authorized to access the resource.

TABLE 9-15 NETWORK DIAGNOSTIC TOOLS

Tool	Function
Digital Volt Meters (DVM)	Measures voltage passing through a resistance. Primarily used for network cable troubleshooting.
Time-Domain Reflectors (TDRs)	Sends sonar-like pulses to look for breaks, shorts or crimps in cables. Can locate a break within a few feet of actual fault.
Oscilloscope	Measures amount of signal voltage per unit of time. Displays crimps, shorts, opens, etc.
Network Monitor	Examines packet types, errors and traffic to and from each computer on a network.
Protocol Analyzer	Looks inside the packet to determine cause of problem. Contains built in Time-Domain Reflector. Gives insights to many problems including connection errors, bottlenecks, traffic problems, protocol problems, etc.