COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

Network Defense
Fundamentals & Protocols

This title maps to

EC-Council | Network Security Administrator

This page was intentionally left blank

Fundamental and Protocols

EC-Council | Press

Volume 1 of 5 mapping to

E | NSA™

EC-Council | Network Security Administrator

Certification

COURSE TECHNOLOGY
CENGAGE Learning

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

COURSE TECHNOLOGY
CENGAGE Learning®

Fundamental and Protocols: EC-Council | Press

Course Technology/Cengage Learning Staff:

Vice President, Career and Professional Editorial: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

EC-Council:

President | EC-Council: Sanjay Bavisi

Sr. Director US | EC-Council: Steven Graham

Library of Congress Control Number: 2010923379

ISBN-13: 978-1-4354-8355-2

ISBN-10: 1-4354-8355-3

Cengage Learning
5 Maxwell Drive
Clifton Park, NY 12065-2919
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by
Nelson Education, Ltd.

For more learning solutions, please visit our corporate website at **www.cengage.com**

Printed in the United States of America
1 2 3 4 5 6 7 13 12 11 10

Brief Table of Contents

Table of Contents

Preface

Hacking and electronic crimes sophistication has grown at an exponential rate in recent years. In fact, recent reports have indicated that cyber crime already surpasses the illegal drug trade! Unethical hackers better known as *black hats* are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting it and profiting from the exercise. High profile crimes have proven that the traditional approach to computer security is simply not sufficient, even with the strongest perimeter, properly configured defense mechanisms like firewalls, intrusion detection, and prevention systems, strong end-to-end encryption standards, and anti-virus software. Hackers have proven their dedication and ability to systematically penetrate networks all over the world. In some cases *black hats* may be able to execute attacks so flawlessly that they can compromise a system, steal everything of value, and completely erase their tracks in less than 20 minutes!

The EC-Council Press is dedicated to stopping hackers in their tracks.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization comprised of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker,* C|EH program. The goal of this program is to teach the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the C|EH program has rapidly gained popularity around the globe and is now delivered in over 70 countries by over 450 authorized training centers. Over 80,000 information security practitioners have been trained.

C|EH is the benchmark for many government entities and major corporations around the world. Shortly after C|EH was launched, EC-Council developed the *Certified Security Analyst,* E|CSA. The goal of the E|CSA program is to teach groundbreaking analysis methods that must be applied while conducting advanced penetration testing. E|CSA leads to the *Licensed Penetration Tester,* L|PT status. The *Computer Hacking Forensic Investigator,* C|HFI was formed with the same design methodologies above and has become a global standard in certification for computer forensics. EC-Council through its impervious network of professionals, and huge industry following has developed various other programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed where standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

About the EC-Council | Press

The EC-Council | Press was formed in late 2008 as a result of a cutting edge partnership between global information security certification leader, EC-Council and leading global academic publisher, Cengage Learning. This partnership marks a revolution in academic textbooks and courses of study in Information Security, Computer Forensics, Disaster Recovery, and End-User Security. By identifying the essential topics and content of EC-Council professional certification programs, and repurposing this world class content to fit academic programs, the EC-Council | Press was formed. The academic community is now able to incorporate this powerful cutting edge content into new and existing Information Security programs. By closing the gap between academic study and professional certification, students and instructors are able to leverage the power of rigorous academic focus and high demand industry certification. The EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating the growing epidemic of cybercrime and the rising threat of cyber-war.

Network Defense Series

The EC-Council | Press *Network Defense* series, preparing learners for EINSA certification, is intended for those studying to become secure system administrators, network security administrators and anyone who is interested in network security technologies. This series is designed to educate learners, from a vendor neutral standpoint, how to defend the networks they manage. This series covers the fundamental skills in evaluating internal and external threats to network security, design, and how to enforce network level security policies, and ultimately protect an organization's information. Covering a broad range of topics from secure network fundamentals, protocols & analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS and firewalls, bastion host and honeypots, among many other topics, learners completing this series will have a full understanding of defensive measures taken to secure their organizations information. The series when used in its entirety helps prepare readers to take and succeed on the EINSA, Network Security Administrator certification exam from EC-Council.

Books in Series

- *Network Defense: Fundamentals and Protocols*/1435483553
- *Network Defense: Security Policy and Threats*/1435483561
- *Network Defense: Perimeter Defense Mechanisms*/143548357X
- *Network Defense: Securing and Troubleshooting Network Operating Systems*/1435483588
- *Network Defense: Security and Vulnerability Assessment*/1435483596

Fundamentals and Protocols *Fundamentals and Protocols* coverage includes network fundamentals, network protocols and analysis, IEEE standards as well as a discussion of security standards and various security organizations.

Chapter Contents

Chapter 1, *Fundamentals of Computer Networks*, discusses the operations of various key elements in a network, including IP address assignments, domain name spaces, working and functional categories of gateways, media types used to connect networks, media access methods, and more. Chapter 2, *Network Protocols* explains the concept of network protocol and discusses how to implement several different network protocols. Chapter 3, *Protocol Analysis*, focuses on TCP/IP protocol structures, the TCP and IP data packet structures, user-level commands implementation, TCP algorithms, and IPv6. C. Chapter 4, *IEEE Standards*, discusses the architecture and history of the IEEE 802 set of standards as well as ETSI and HiperLAN standards. Chapter 5, *Security Standards Organizations* discusses many of the major security standards organizations in the world today, including ICANN, ISO, NIST, W3C, and ANSI. Chapter 6, *Security Standards*, discusses Internet standards, explains Requests for Comments (RFC) and how to submit and obtain them. The chapter concludes with information about some of the common cabling standards for networks.

Chapter Features

Many features are included in each chapter and all are designed to enhance the learner's learning experience. Features include:

- *Objectives* begin each chapter and focus the learner on the most important concepts in the chapter.
- *Key Terms* are designed to familiarize the learner with terms that will be used within the chapter.
- *Chapter Summary*, at the end of each chapter, serves as a review of the key concepts covered in the chapter.
- *Review Questions* allow the learner to test their comprehension of the chapter content.
- *Hands-On Projects* encourage the learner to apply the knowledge they have gained after finishing the chapter. Files for the *Hands-On Projects* can be found on the Student Resource Center. Note: you will need your access code provided in your book to enter the site. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Student Resource Center

The Student Resource Center contains all the files you need to complete the Hands-On Projects found at the end of the chapters. Access the Student Resource Center with the access code provided in your book. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Additional Instructor Resources

Free to all instructors who adopt the *Fundamentals and Protocols* book for their courses is a complete package of instructor resources. These resources are available from the Course Technology web site, *www.cengage.com/coursetechnology*, by going to the product page for this book in the online catalog, and choosing "Instructor Downloads".

Resources include:

- *Instructor Manual*: This manual includes course objectives and additional information to help your instruction.
- *ExamView Testbank*: This Windows-based testing software helps instructors design and administer tests and pre-tests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.
- *PowerPoint Presentations*: This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.
- *Labs*: Additional Hands-on Activities to provide additional practice for your students.
- *Assessment Activities*. Additional assessment opportunities including discussion questions, writing assignments, internet research activities, and homework assignments along with a final cumulative project.
- *Final Exam*: Provides a comprehensive assessment of *Fundamentals and Protocols* content.

Cengage Learning Information Security Community Site

This site was created for learners and instructors to find out about the latest in information security news and technology.

Visit *community.cengage.com/infosec* to:

- Learn what's new in information security through live news feeds, videos and podcasts.
- Connect with your peers and security experts through blogs and forums.
- Browse our online catalog.

How to Become EINSA Certified

The EINSA certification ensures that the learner has the fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. EINSA certified individuals will know how to evaluate network and Internet security issues and design, and how to implement successful security policies and firewall strategies as well as how to expose system and network vulnerabilities and defend against them.

EINSA Certification exams are available through Prometric Prime. To finalize your certification after your training, you must:

1. Purchase an exam voucher from the EC-Council Community Site at Cengage: *www.cengage.com/community/eccouncil*.
2. **Speak with your Instructor or Professor about scheduling an exam session, or visit the EC-Council Community Site referenced above for more information.**
3. Take and pass the EINSA certification examination with a score of 70% or better.

About Our Other EC-Council | Press Products

Ethical Hacking and Countermeasures Series

The EC-Council | Press *Ethical Hacking and Countermeasures* series is intended for those studying to become security officers, auditors, security professionals, site administrators, and anyone who is concerned about or responsible for the integrity of the network infrastructure. The series includes a broad base of topics in offensive network security, ethical hacking, as well as network defense and countermeasures. The content of this series is designed to immerse the learner into an interactive environment where they will be shown how to scan, test, hack and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, ethical hackers are able to set up strong countermeasures and defensive systems to protect their organization's critical infrastructure and information. The series when used in its entirety helps prepare readers to take and succeed on the C|EH certification exam from EC-Council.

Books in Series:

- *Ethical Hacking and Countermeasures: Attack Phases*/143548360X
- *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*/1435483618
- *Ethical Hacking and Countermeasures: Web Applications and Data Servers*/1435483626
- *Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems*/1435483642
- *Ethical Hacking and Countermeasures: Secure Network Infrastructures*/1435483650

Computer Forensics Series

The EC-Council | Press *Computer Forensics* series, preparing learners for C|HFI certification, is intended for those studying to become police investigators and other law enforcement personnel, defense and military personnel, e-business security professionals, systems administrators, legal professionals, banking, insurance and other professionals, government agencies, and IT managers. The content of this program is designed to expose the learner to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Advanced techniques in computer investigation and analysis with interest in generating potential legal evidence are included. In full, this series prepares the learner to identify evidence in computer related crime and abuse cases as well as track the intrusive hacker's path through client system.

Books in Series:

- *Computer Forensics: Investigation Procedures and Response*/1435483499
- *Computer Forensics: Investigating Hard Disks, File and Operating Systems*/1435483502
- *Computer Forensics: Investigating Data and Image Files*/1435483510
- *Computer Forensics: Investigating Network Intrusions and Cybercrime*/1435483529
- *Computer Forensics: Investigating Wireless Networks and Devices*/1435483537

Penetration Testing Series

The EC-Council | Press *Penetration Testing* series, preparing learners for E|CSA/LPT certification, is intended for those studying to become Network Server Administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals. This series covers a broad base of topics in advanced penetration testing and security analysis. The content of this program is designed to expose the learner to groundbreaking methodologies in conducting thorough security analysis, as well as advanced penetration testing techniques. Armed with the knowledge from the Penetration Testing series, learners will be able to perform the intensive assessments required to effectively identify and mitigate risks to the security of the organization's infrastructure. The series when used in its entirety helps prepare readers to take and succeed on the E|CSA, Certified Security Analyst certification exam.

E|CSA certification is a relevant milestone towards achieving EC-Council's Licensed Penetration Tester (LPT) designation, which also ingrains the learner in the business aspect of penetration testing. To learn more about this designation please visit *http://www.eccouncil.org/lpt.htm*.

Books in Series:

- *Penetration Testing: Security Analysis*/1435483669
- *Penetration Testing: Procedures and Methodologies*/1435483677
- *Penetration Testing: Network and Perimeter Testing*/1435483685
- *Penetration Testing: Communication Media Testing*/1435483693
- *Penetration Testing: Network Threat Testing*/1435483707

Cyber Safety/1435483715

Cyber Safety is designed for anyone who is interested in learning computer networking and security basics. This product provides information cyber crime; security procedures; how to recognize security threats and attacks, incident response, and how to secure internet access. This book gives individuals the basic security literacy skills to begin high-end IT programs. The book also prepares readers to take and succeed on the Security|5 certification exam from EC-Council.

Wireless Safety/1435483766

Wireless Safety introduces the learner to the basics of wireless technologies and its practical adaptation. *Wireless|5* is tailored to cater to any individual's desire to learn more about wireless technology. It requires no pre-requisite knowledge and aims to educate the learner in simple applications of these technologies. Topics include wireless signal propagation, IEEE and ETSI Wireless Standards, WLANs and Operation, Wireless Protocols and Communication Languages, Wireless Devices, and Wireless Security Network. The book also prepares readers to take and succeed on the Wireless|5 certification exam from EC-Council.

Network Safety/1435483774

Network Safety provides the basic core knowledge on how infrastructure enables a working environment. Intended for those in an office environment and for the home user who wants to optimize resource utilization, share infrastructure and make the best of technology and the convenience it offers. Topics include foundations of networks, networking components, wireless networks, basic hardware components, the networking environment and connectivity as well as troubleshooting. The book also prepares readers to take and succeed on the Network|5 certification exam from EC-Council.

Disaster Recovery Series

The *Disaster Recovery Series* is designed to fortify virtualization technology knowledge of system administrators, systems engineers, enterprise system architects, and any IT professional who is concerned about the integrity of the their network infrastructure. Virtualization technology gives the advantage of additional flexibility as well as cost savings while deploying a disaster recovery solution. The series when used in its entirety helps prepare readers to take and succeed on the E|CDR and E|CVT, Disaster Recovery and Virtualization Technology certification exam from EC-Council. The EC-Council Certified Disaster Recovery and Virtualization Technology professional will have a better understanding of how to setup Disaster Recovery Plans using traditional and virtual technologies to ensure business continuity in the event of a disaster.

Books in Series

- *Disaster Recovery*/1435488709
- *Virtualization Security*/1435488695

Acknowledgements

Michael H. Goldner is the Chair of the School of Information Technology for ITT Technical Institute in Norfolk Virginia, and also teaches bachelor level courses in computer network and information security systems. Michael has served on and chaired ITT Educational Services Inc. National Curriculum Committee on Information Security. He received his Juris Doctorate from Stetson University College of Law, his undergraduate degree from Miami University and has been working over fifteen years in the area of Information Technology. He is an active member of the American Bar Association, and has served on that organization's Cyber Law committee. He is a member of IEEE, ACM and ISSA, and is the holder of a number of industrially recognized certifications including, CISSP, CEH, CHFI, CEI, MCT, MCSE/Security, Security +, Network + and A+. Michael recently completed the design and creation of a computer forensic program for ITT Technical Institute, and has worked closely with both EC-Council and Delmar/Cengage Learning in the creation of this EC-Council Press series.

Chapter 1

Fundamentals of Computer Networks

Objectives

After completing this chapter, you should be able to:

- List the operations of various key elements in a network
- Understand IP address assignments
- Create a domain name space
- List the functional categories and operations of gateways
- List the media types used to connect networks
- Use various media access methods
- Understand the OSI reference model
- Understand various data transmission methods
- Explain logical network arrangements
- Classify networks

Key Terms

Backbone a network component that combines many networks and subnets into a single channel

Bus topology a multipoint topology that consists of a long cable that acts like a support structure for the entire network

Domain name system (DNS) an Internet service that translates domain names into IP addresses

Gateway a node that routes traffic from one workstation to an outside network

IP address a unique 32-bit number assigned to all devices communicating in a network using the Internet Protocol (IP)

Network a group of computers connected together so that information can be exchanged among the computers

Operations security (OPSEC) a identifies, controls, and protects classified or sensitive information

Peer-to-peer network a network in which every computer operates as a client and a server

Subnet a logical grouping of the devices in a network, created by subdividing a larger network address

Introduction to the Fundamentals of Computer Networks

This chapter discusses the operations of various key elements in a network, including: IP address assignments, domain name spaces, working and functional categories of gateways, media types used to connect networks, media access methods, the OSI reference model, data transmission methods, logical network arrangements, network classes, physical arrangements of the network (including topologies), and network equipment functions.

Networks

A ***network*** is a group of computers connected together so that information can be exchanged among the computers. A network can be divided into several subnets depending on usage and the requirements. Network speed is measured in megabits per second (Mbps). Networking allows the user to perform the following tasks:

- Share a single Internet connection among many systems
- Share network resources like printers, scanners, etc.
- Share files and folders

Setting Up a Network

Table 1-1 shows how to connect computers together using an Ethernet adapter, Home Phoneline Networking Alliance (HPNA) adapter, or wireless network adapter.

Connection Type	Required Hardware	Computer Configuration
Ethernet	A network adapter is installed into each computer and then connected to a network hub.	Configure an Ethernet network using a network hub
HPNA	A network adapter is installed into each computer, and then they are plugged into phone jacks using telephone cables.	Configure a phone-line network
Wireless network	A wireless network adapter is installed into each computer.	Configure a wireless network

Table 1-1 This table shows the necessary elements of various connection types

Steps to Set Up a Network

The checklist below lists the steps, in order of completion, for setting up a home or small office network using the Wireless Network and Network Setup Wizards for a Windows XP/NT system. If a step does not apply, go on to the next step. Print this checklist for reference:

1. Sketch the network. Draw a diagram of the home or office, showing the location of each computer and printer.
2. Next to each computer, note the hardware, such as modems and network adapters, installed on each computer.
3. Choose the computer on which the residential gateway will be set up (or the computer that will be the Internet Connection Sharing [ICS] host computer). It is recommended that this computer be running Windows XP Home Edition, Windows XP Professional, Windows Vista, or Microsoft Windows XP Service Pack 2 (SP2).
4. Determine the type of network adapters needed for the network: Ethernet, HPNA, wireless.
5. Make a list of necessary hardware. This includes modems, network adapters, hubs, and cables.
6. Buy the hardware.
7. Install the correct network adapters and modems on each computer.
8. If the network will be wireless, run the Wireless Network Setup Wizard.

9. Physically connect the computers together. Plug the cables into hubs, phone jacks, and the computer.
10. Turn on all computers and printers.
11. Make sure the computer attached to the residential gateway (or the ICS host computer) has an active Internet connection. To establish an Internet connection, run the New Connection Wizard.
12. Run the Network Setup Wizard on the computer attached to the residential gateway (or the ICS host computer).
13. Run the Network Setup Wizard on the other computers on the network.

Backbone

A ***backbone*** combines many networks and subnets into a single channel. The capacity of the backbone is greater than that of the network. A backbone network uses a mesh topology, which provides many-to-many connections on the network. There was once just a single backbone network called ARPANET, but now each Internet service provider (ISP) has its own backbone network.

There are two types of backbones:

1. *Distributed backbones*: A distributed backbone runs through the premises/building and connects to each local area network (LAN) and subnet. A router is used to connect the network to the backbone.
2. *Collapsed backbones*: A collapsed backbone is configured with the star-wired topology. A hub or switch is placed in the center of the premises, and each network is connected to the central hub or switch.

80/20 and 20/80 Rule

Old network backbones were used to pass nearly 20% of the network traffic, and the remaining 80% was limited to LANs and subnets. This rule (known as 80/20) failed due to inadequate utilization of the network backbone.

The current backbones are designed in such a way that only 20% of the traffic remains limited to LANs and subnets, whereas 80% is passed to backbones. This rule (known as the 20/80 rule) increases the efficiency of backbones because approximately 80% of LAN traffic is passed to them through the central hub or switch.

Reasons to adopt the 20/80 rule include:

- Users communicate more to an external network than within the same network.
- Organizations typically use a centralized server.
- Network traffic is routed through the hub or switch due to the use of the Internet.

Segments

Large networks are divided into segments to improve the performance of the network. Segments also reduce IP address collisions. Routers, switches, bridges, and multihomed gateways are used to connect the different segments. Segments enable organizations to provide different levels of security to individual departments.

Any data packet sent from a host goes to the default gateway. The packet's destination IP address and subnet mask are matched with the host IP address and subnet mask. If the IP addresses and subnet masks match, the packet is forwarded to the host's local segment; otherwise, it is forwarded to the default gateway of the destination host. If the IP addresses and subnet masks match, traffic broadcasting and multicasting is done in the local segment without disturbing the traffic of other subnets.

Segments help in containing virus and malware attacks in a network, by limiting an attack on a segment of the network to that particular segment. Before segmenting a network, an administrator has to look for the following factors:

- Types of service available to users
- Broadcasting domains

Segmentation makes it easier to implement different technologies or applications, in different departments, according to their specific needs.

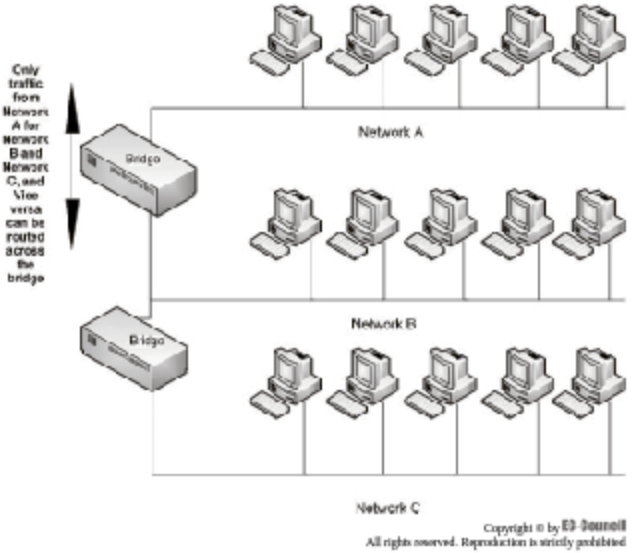


Figure 1-1 This figure represents segmentation with the use of a bridge.

Segmenting a Network with a Bridge

A bridge operates in the data-link layer and helps in collision detection. Bridges dynamically build a routing table containing MAC addresses and port addresses. Bridges are also used to connect different segments in a LAN. The forwarding of frames is done by the destination addresses in the frame. The primary issue with using a bridge is that it broadcasts to all network segments, as shown in Figure 1-1. This is called a *broadcast storm*.

Segmenting a Network with Switches

Many objectives are achieved in using a switch to segment a network. It offers the following advantages:

- Full-duplex communication
- Medium-rate adaptation
- Easy migration from one segment to another
- Switches can dynamically learn the network topology and filter the traffic

Segmenting a Network with Routers

Routers maintain a table of records for the devices connected to the network. Routers operate at the network layer of the OSI reference model and keep a record of the networks, irrespective of the hosts. Logical addresses perform packet filtering.

Subnet

A ***subnet*** is a logical grouping of the devices in a network, created by subdividing a larger network address. It is a logical partitioning of the network address into smaller, discrete sections. The addresses of the devices in the subnet have the same prefix. A subnet mask defines the boundary of the network. An IP address subnet can be identified by its subnet mask, as shown in Figure 1-2.

	Subnet mask	total addresses
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4

Figure 1-2 Subnet masks hide network architecture.

Subnets have the following advantages:

- Can hide the internal architecture or the network from the external router.
- Can be used to group hosts according to their actual logical structure in the organization's physical network; it gives each department an opportunity to implement specific security measures.

Tips to Find Subnets and Broadcast Addresses

Subnets and broadcast addresses can be identified by the subnet mask. The incremental number of the subnet mask can be calculated by subtracting the last octet of the subnet mask from 256.

For example, an IP address of 10.1.12.1 and subnet mask of 255.255.248.0 has an octet of 248. So 256 – 248, which equals 8, will be the incremental number for subnets 10.1.8.0, 10.1.16.0, and 10.1.24.0. In this example, each subnet network address will have an assignable range of 2,046 IP addresses from 10.1.8.1 to 10.1.15.254. This excludes the network address 10.1.8.0 and the broadcast address, which cannot be assigned to any device. Since 10.1.12.1 falls between 10.1.8.0 and 10.1.16.0, within the referred to range, the subnet address for IP 10.1.12.1 will be 10.1.8.0.

The broadcast address is one less than the next subnet address (10.1.16.0); thus, 10.1.15.255 will be the broadcast address of IP 10.1.12.1.

IP Address Assignments

IP Address

An ***IP address*** is a unique 32-bit number assigned to all devices communicating on a network using the Internet Protocol (IP). The IP address is also used to identify a network and its host. IPv4 addresses are represented in dotted-decimal notation, with four numbers, each ranging from 0 to 255, separated by dots. There are 2^{32} possible IP addresses.

IP address classifications include the following designations:

- *Class A*: Large networks with many devices
- *Class B*: Medium-sized networks
- *Class C*: Small businesses with fewer than 256 devices
- *Class D*: Multicast networks
- *Class E*: Not assigned; reserved for future purposes

The following IP address parameters apply to the various IP designations:

- *Default network*: The default IP address is 0.0.0.0.
- *Class A*: The first higher-order bit in the binary address starts with 0. The decimal number is between 0 and 127 and is mostly used by international companies. From the 32-bit address, the Class A address uses the leftmost 8 bits for identifying networks with a default subnet mask of 255.0.0.0. It should be noted that the 127 address range is used exclusively for testing, as in the loopback address 127.0.0.1.
- *Class B*: Medium-scale networks use the leftmost 16 bits of this class for the network part of the address, and the first two higher-order bits in the binary address are 10. The first octet has a decimal number from 128 to 191 and a default subnet mask of 255.255.0.0.
- *Class C*: The first three higher-order bits in the binary address of Class C are 110, so the decimal number can be anywhere between 192 and 223; it is mainly used for small businesses. It uses the first 24 bits, while the other 8 bits are used for the identification of the host on the network. Its default subnet mask is 255.255.255.0.
- *Class D*: The first four higher-order bits in the binary address are 1110, and the decimal address is between 224 and 239. This address range is used exclusively for multicasting.
- *Class E*: The first five higher-order bits in the binary addresses in this class are 11110 and are primarily reserved for future use.
- *Loopback address*: The address 127.0.0.1 is used as the loopback address, which is mainly used by the host computer to send messages to itself and for network testing.
- *Broadcast address*: Messages sent to all the computers on a network are broadcast using the address 255.255.255.255.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that manages the assignment of IP addresses, IP address spaces, and protocol identifier assignments. ICANN is a nonprofit organization. The aim of ICANN is to ensure that all users are assigned valid addresses. ICANN is not related to Internet content control, data protection, or unsolicited mail.

ICANN is responsible for the management of the following gTLDs (generic top-level domains):

- *.com*: For businesses
- *.net*: For network providers
- *.org*: Miscellaneous
- *.edu*: For educational institutes
- *.gov*: For government agencies
- *.mil*: For military agencies
- *.int*: For international organizations

"Country Code" Top-Level Domains

Top-level domains also exist for every country in the world (for example, .ca for Canada and .au for Australia).

In 2000, the ICANN Board selected seven new TLDs to be included in the first addition of a global TLD to the Internet since the 1980s.

They are the following:

- *.aero*: For the air transport industry
- *.biz*: For business organizations
- *.coop*: For cooperative organizations
- *.info*: For information services
- *.museum*: For museums

- *.name*: For individuals, by name
- *.pro*: For professionals

In the years 2005–2006, the following four additional gTLDs were sponsored:

- .cat
- .jobs
- .mobi
- .travel

IP Address Space

IPv4 addresses are made up of 32 bits, which provides a limited address space of 2^{32}. With the growing technology and the exponential increase in the number of Internet users, an IPv4 address shortage was inevitable. This has served as a motivation for development of a more-robust addressing system, IPv6, which has addresses made up of 128 bits and provides an address space of 2^{128}. In the meantime, organizations as well as the Internet community are adopting subnetting and the use of private IP addresses to manage the IP address shortage.

Purpose of Dots

It can be difficult to remember a particular decimal number address. To make it easier to remember, the decimal is used to divide it into four parts. With the logical classification of the address, it is easier to identify a particular host on the network. The scheme is based on decimal number and the address space used is binary. Certain schemes use binary numbers, whereas others use decimal numbers directly. Therefore, the 32-bit address space is further divided into four equal components, called octets, of 8 bits each. An example is 202.53.13.138.

Subnetting a Classful Address Space

The IP address space is divided into Classes A, B, C, D, and E. Subnetting these address class spaces into smaller sections is called classful addressing. Classful addressing is adopted to overcome the problem of duplication of addresses, as shown in Figure 1-3. However, public networks do not use classful addressing.

	Address Space Allocation Among Major Geographical Areas	
Address Space	Area of Allocation	Date Allocated
64.0.0.0 to 64.255.255.255	ARIN	Jul-99
128.0.0.0 to 191.255.255.255	Various registries	May-9
192.0.0.0 to 192.255.255.255	Multiregional	May-9
193.0.0.0 to 195.255.255.255	RIPE NCC-Europe	5/1/199
196.0.0.0 to 198.255.255.255	various registeries	5/1/199
199.0.0.0 to 199.255.255.255	ARIN-North America	May-9
200.0.0.0 to 200.255.255.255	ARIN-Central and South America	5/1/199
201.0.0.0 to 200.255.255.255	Reserved- Central and South America	May-9
202.0.0.0 to 203.255.255.255	APNIC-Pacific Rim	May-9
204.0.0.0 to 205.255.255.255	ARIN-North America	Mar-9
206.0.0.0 to 206.255.255.255	ARIN-North America	Apr-9
207.0.0.0 to 207.255.255.255	ARIN-North America	Nov-9
208.0.0.0 to 208.255.255.255	ARIN-North America	Apr-9
209.0.0.0 to 209.255.255.255	ARIN-North America	Jun-9
210.0.0.0 to 210.255.255.255	APNIC-Pacific Rim	Jun-9
211.0.0.0 to 211.255.255.255	APNIC-Pacific Rim	Jun-9
212.0.0.0 to 212.255.255.255	RIPE NCC-Europe	Oct-9
213.0.0.0 to 213.255.255.255	RIPE NCC-Europe	Mar-9
216.0.0.0 to 217.255.255.255	ARIN-North America	Apr-9

Figure 1-3 Address spaces are allocated to specific areas.

The following protocols are examples of those used to route information from one network or subnet to another:

- *RIP*: Routing Information Protocol
- *IGRP*: Internet Gateway Routing Protocol

IP Address Assignment

Every computer in a network can have a static IP address, as shown in Figure 1-4. In a network that has a shared connection, addresses can also be assigned dynamically. Generally, the ISP providing the connectivity assigns the IP addresses.

Addressing types include the following:

- Prefix-based addressing
- Per-interface based assignment
- Virtual addressing
- Static addressing
- Dynamic addressing

Prefixed-Based Addressing

The prefix can be used for general routing decisions. For example, the first 8 bits may identify the particular company, and then the next 8 bits may identify the particular department of the office. The next 8 bits may identify the particular network in that office. Finally, all 32 bits will identify the host on the network.

Per-Interface Assignment

A host can have an equal number of IP addresses and interfaces. An IP address can also represent an interface.

Virtual Addressing

Virtual addresses are used when a single server provides services through several addresses. There is no standard for virtual addressing.

Static Addressing

The following are the steps for assigning a static IP address in Windows:

1. From the Start menu, select **Control Panel**, and then open **Network Connections**.
2. Select **Network and Internet Connections**.
3. Double-click **Active LAN or Internet Connection**.
4. Select **Properties**.
5. As a result, the **Local Area Connection Properties** dialog box will be opened.
6. Double-click **Internet Protocol TCP/IP**.
7. Click the **Properties** button, as shown in Figure 1-5.
8. Select the **Use the following IP address** check box, as shown in Figure 1-4.
9. In the **IP address** field, type the IP address.
10. Insert the subnet mask used by your router.
11. The default gateway is the IP address of the router.
12. In the **Use the following DNS server address** field, enter the IP addresses of the DNS server the router is using.
13. Click **OK**.

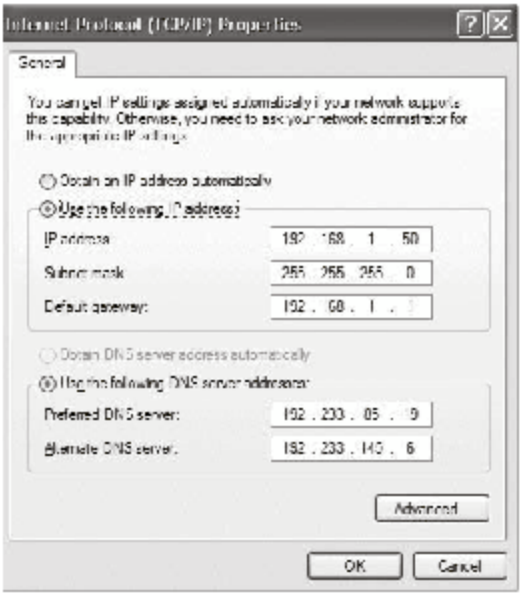


Figure 1-4 Static addressing can be performed through the Control Panel.

Dynamic Addressing

The following are the steps for assigning a dynamic address in Windows:

1. From the Start menu, select **Control Panel** and then double-click **Network Connections**.
2. Right-click **Desired Network Connection** to configure it, and then click **Properties**.
3. Select the **General** tab or **Networking** tab.
4. Click **Properties**.
5. Check the **Obtain the IP address automatically** check box, and then click **OK**, as shown in Figure 1-6.

To locate the current IP address, perform the following steps:

- Go to the Start menu
- Select **Run**
- Type **cmd**
- Run the **ipconfig /all** command

Check the **Dhcp Enabled** line to determine if the IP address is dynamically assigned or is static (Figure 1-7).

- *No* means the IP address is static.
- *Yes* means the IP address is dynamic.

The IP address shown is the current system IP address.

Figure 1-5 Click the **Properties** button.

Creating a Domain Name Space

Domain Name System

The ***domain name system (DNS)*** is an Internet service that translates domain names into IP addresses. It is a hierarchical and distributed database containing host and domain names. A fully qualified domain name (FQDN) can identify the particular host within the hierarchical tree architecture. DNS makes it possible to assign domain names independent of the physical routing hierarchy represented by the numerical IP address.

Domain Name System Organization

DNS is organized in the form of a hierarchy, as shown in Figure 1-8. The topmost level in the hierarchy is the root domain, which is represented as a dot (.) at the very end of the domain name, but is seldom shown in domain names. The next level in the hierarchy includes the top-level domains (TLDs).

The name of each node or domain could be up to 63 characters long. Traversal of DNS is done in reverse order from the leaf node to the root, meaning from the leftmost name to the rightmost. Whenever a particular message consists of multiple domains, the traversal will start from the first domain.

TLDs are divided into three categories:

1. *Country-code TLDs (ccTLDs)*: Domains associated with countries and territories. There are more than 240 ccTLDs. Examples include .uk, .in, and .jp.
2. *Sponsored generic TLDs (gTLDs)*: Specialized domains with a sponsor representing a community of interest. These TLDs include .edu, .gov, .int, .mil, .aero, .coop, and .museum.
3. *Unsponsored gTLDs*: Domains without a sponsoring organization. The list of unsponsored gTLDs includes .com, .net, .org, .biz, .info, .name, and .pro.

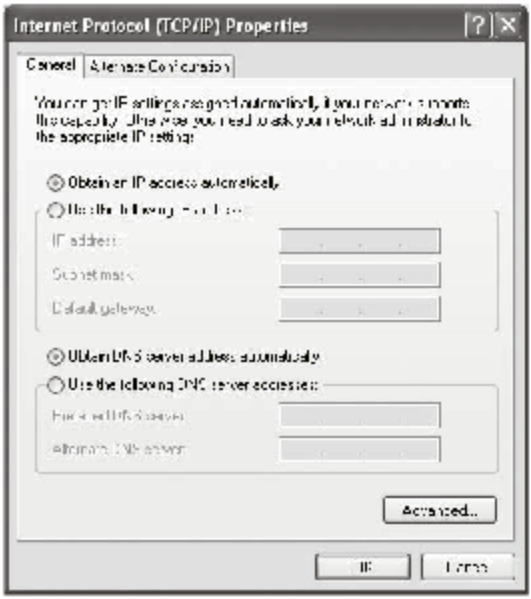


Figure 1-6 Users can also choose to assign an IP address automatically.

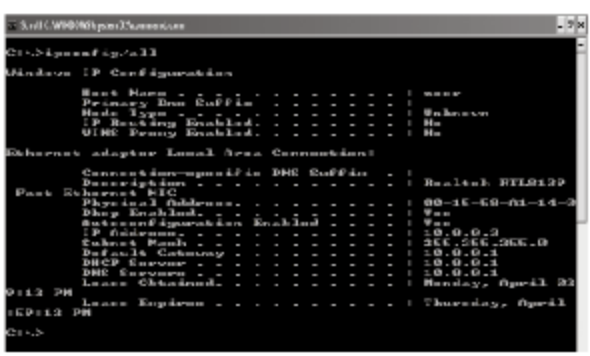


Figure 1-7 *Yes* or *no* on the Dhcp Enabled line indicates the state of the IP address.

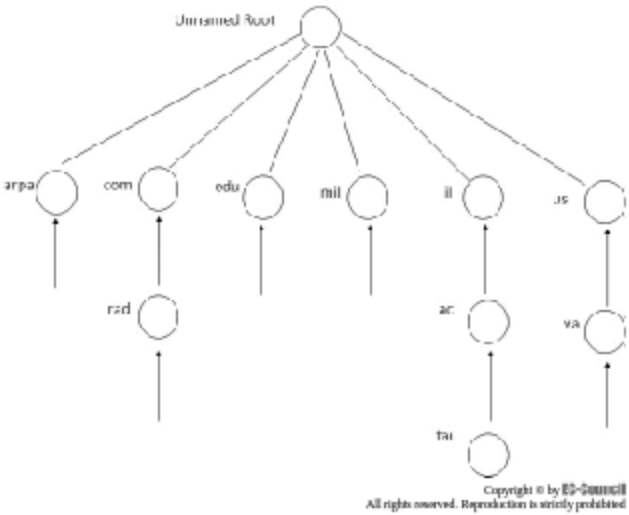


Figure 1-8 DNS is organized hierarchically.

Domain Names

Domain names give a unique identity to an organization or an entity on the Internet. Domain names should be catchy, short, and easy to remember. The domain name has to be registered before it can be used.

A domain name consists of a set of resource records (RR). An RR must have the host address and specifies the domain name. The RR consists of a resource type field, which specifies the type of resource the particular resource record has, and a class field, which specifies the format of the data.

Domains use the hierarchical format for the structured information. The different values used in the resource type field are the following:

- *A*: Host address that is associated with the domain
- *MF*: Identifies a mail forwarder for the domain
- *MX*: Mail Exchanger records
- *NS*: Identifies the name server that is authoritative for the domain
- *SOA*: Start of a zone for an authority
- *CNAME*: Lists the canonical name of an alias
- *PTR*: Pointer records that facilitate reverse lookup from an IP address to a domain name

Creating a New Domain Name The name should give an idea of what a particular organization does. Review the following naming conventions for domains:

- A dot
- Letters from A to Z in uppercase or lowercase
- Numbers from 0 to 9

- Combinations of alphabetic characters and numbers
- Maximum length should not exceed 64 bits
- Hyphens and underscores are also acceptable

Once the name is decided, the domain name should be registered. Domain names are registered by government agencies as well as nonprofit organizations. Every domain name has a set of registry policies that should be followed.

Components of a DNS

There are three main components of a DNS:

1. Domain name space and resource records
2. Name servers
3. Resolvers

Domain Name Space and Resource Records

These elements specify the structural hierarchy of the name space and the data associated with it. Each node has particular information associated with it. Queries are sent to get the specific information from the domains. The result is the domain name and the type of information required.

Name Servers

These contain information about the structure of the domain. Authoritative information is organized into units called zones, which can be automatically distributed to the name servers that provide redundant service for the data in a zone.

There are two types of name servers:

1. Authoritative
2. Caching

Resolvers Resolvers are programs that obtain information from name servers when they get the client request. Resolvers refer to at least one server, and answer a query directly or take the reference from the other servers. It is a system routine, which directly accesses the user programs.

Securing the Cache Against Pollution The DNS query response sometimes contains malicious data, but by default, DNS is secured against cache pollution. An attacker can successfully pollute the cache of a DNS server by sending resource records without the request of the server.

Disabling Recursion Recursion is not disabled in a DNS server. Because of this, a DNS server executes queries for the DNS clients repeatedly in response to a request. Attackers use recursion to reduce the performance of a DNS server.

Managing the DACL With a DACL (discretionary access control list), control of active directory users and groups is possible. The list for default groups, usernames, and permissions for the DNS server service is illustrated in Figure 1-9.

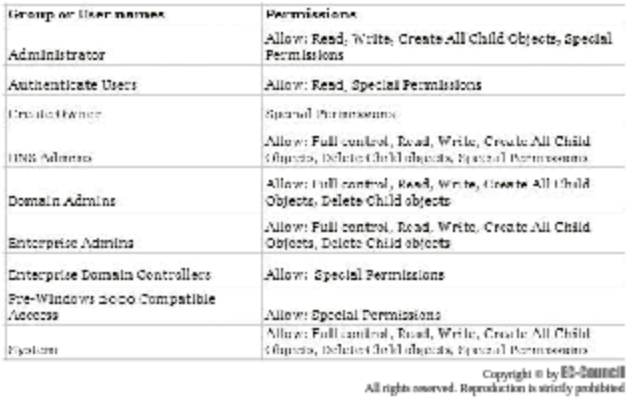
Threats to DNS

Rogue DNS Server Information on a rogue DNS server is not trustworthy. Host-name spoofing and DNS spoofing is done using rogue DNS servers. On the primary server, the PTR record in the ZONE data file is configured to point somewhere other than the correct record. Host-name spoofing can have a TTL of zero that results in caching of misleading information.

Denial of Service There is a chance of a negative response from a DNS server. Sending back a negative response for a DNS name that could not be resolved can result in a denial of service (DoS).

Another DoS attack involves cache poisoning, in which a CNAME record is inserted that refers to itself in its canonical form.

Client Flooding Client flooding results when the client sends a request and gets thousands of responses from a DNS server. This attack cannot be identified, as the client thinks that it is coming from an authorized DNS server. The flooding cannot be identified because the origin of the responses is unknown.



Group or user names:	Permissions
Administrator	Allow: Read, Write, Create All Child objects, Special Permissions
Authenticate Users	Allow: Read, Special Permissions
Creator Owner	Special Permissions
DNS Admins	Allow: Full control, Read, Write, Create All Child objects, Delete Child objects, Special Permissions
Domain Admins	Allow: Full control, Read, Write, Create All Child objects, Delete Child objects
Enterprise Admins	Allow: Full control, Read, Write, Create All Child objects, Delete Child objects
Enterprise Domain Controllers	Allow: Special Permissions
Pre-Windows 2000 Compatible Access	Allow: Special Permissions
System	Allow: Full control, Read, Write, Create All Child objects, Delete Child objects, Special Permissions

Figure 1-9 Specific permissions are assigned for the DNS server service.

Functional Categories and Operations of Gateways

Gateways

A *gateway* is a node that routes traffic from workstations to an outside network. For example, when an e-mail is sent, there is a gateway that permits the connection to take place. Gateways are also used as proxy servers and firewalls. Gateways consist of a router and switch. The router determines where the packets are to be sent, and the switch provides the actual path in and out of the gateway.

Functional Categories of Gateways

Gateways are commonly divided into three categories:

1. Data gateways
2. Multimedia gateways
3. Home-control gateways

Data Gateways These simple routers are basically used for data throughput. They support both wired and wireless networking, and they provide pass-through support for network protocols and services. Data gateways can be used to pool multiple Internet connections and secure private networks using firewalls. Some of these also provide storage, such as e-mail and voice-mail storage.

Multimedia Gateways Multimedia gateways provide features for audio and video content delivery. They are often used in combination with digital entertainment devices (including TVs and stereo systems) and provide centralized storage. They can behave like a home server for digital media such as photos, videos, MP3 files, and Web site hosting. In multimedia gateways, audio and video streaming are important features. Video on demand (VOD) and VoIP (Voice over IP) are gateways that include encoding capabilities that translate analog audio and video signals.

Home-Control Gateways Home-control gateways provide home-control and security management services on a network. For example, users can access automated lighting, heating, and security systems with a home-control gateway. They also permit network service providers to provide new service packages and generate new revenue streams.

Media Types Used to Connect Networks

Types of Network Media

There are three primary types of network cables:

1. Twisted-pair cables
2. Coaxial cables
3. Fiber-optic cables

Historical Versus Current Communication Methodology

The method of exchanging information from one system to another is a communication method. Historically, the means to communicate were direct connections or telecommunication used as media. However, this method was unstable as well as time consuming.

Currently, communication has evolved into various networking and highly secured features. Organizations can rely on data obtained through this communication. Communication has extended its growth to such an extent that information can be exchanged or sent globally within a short amount of time (for example, over the Internet).

Asynchronous Versus Synchronous

Communication between two parties is performed by the communication circuit as described in the physical layer and data-link layer of the Open System Interconnection (OSI) model. In general, there are two strategies for communication over the physical link: asynchronous and synchronous.

Asynchronous Communication

An asynchronous communication unit includes a transmitter, a receiver, and a wire. Each device uses a clock to measure the length of the message in terms of bits. The transmitter only transmits the message, and the receiving device looks at the incoming signal and coordinates to match it.

In order to match the data, the sender and receiver should use the same encoding and decoding techniques. This is very important, as it will decide where to look for the data in the transmitted signal as it is encoded. Asynchronous systems do not send separate information to indicate the data or clocking information; it is the responsibility of the receiver to decide the clocking of the signal. This means the receiver has to decide where the bits are starting and where they stop. Thus, communication in asynchronous transmission works without consulting the transmitting device.

In asynchronous communication, the data is not retransmitted; it is said to be more efficient when there is low loss and low error rates over the transmission medium. Additionally, no time is wasted in asynchronous communication because none is spent in setting up the connection at the beginning of transmission. Asynchronous communication is a faster means of sending data, but is less reliable.

Synchronous Communication

In synchronous communication, a connection between the transmitter and receiver is established before the communication begins. There is a process that decides which end should control the session. The transmitter, as well as the receiver, can exchange communication parameters and status information.

After the establishment of the connection between the transmitter and the receiver, the transmitter transmits the signal, and the receiver sends an acknowledgment of the data received along with the data. Synchronous communication takes a long time on low error-rate lines, but it is reliable.

Wired Media or Bounded Network Media

Bounded media are network media that travel in a dedicated conductor. It includes wires, cables, and fiber-optics. Copper cable is made of either stranded or solid core wire. Copper wire is affected by attenuation (signal degradation over long distances) and electrical noise. Fiber-optic cable is composed of a very thin glass core and needs to be protected. Fiber cables come in two categories: single mode and multimode.

As fiber cable uses light signals to transfer data, the rate of data transfer is very high. Single-mode fiber transfers data in a single direction, and only one signal at a time. Multimode fiber can be in the same direction or in opposite directions, carry more than one signal at a time.

Dedicated Line

A dedicated line is a communications cable dedicated to a specific application. It is active for and can transfer data for only one application. This is in contrast with shared resources.

Optical Remanence

After the removal of data from storage media, some residue of the information could remain on the media. Optical remanence deals with such residue information, which is the optical representation of information that remains on storage media after it is erased. It is possible to read information stored on CDs or DVDs even though it is erased. Thus, CDs and DVDs that are no longer being used should be destroyed.

Because optical media is not magnetic and cannot be erased by degaussing, destruction is the only choice for storage media such as CD-ROMs, CD-Rs, and DVD-Rs. It will help to fully erase the information stored on it. For media like CD-RWs and DVD-RWs, clearing the media by overwriting is a lengthy process, so these media should be destroyed.

Magnetic Remanence

Residual information can be found on magnetic storage media, such as hard drives and floppy disks, even after the removal of data. Magnetic remanence is the magnetic representation of residual information stored on hard drives, floppy disks, or magnetic tapes that may still be read even after the removal of data.

A degaussing device can remedy this issue. Degaussing is a process of thoroughly deleting data stored on magnetic media. It prevents data from being recovered.

Twisted-Pair Cable

Twisted-pair cable consists of two separately insulated copper wires twisted around each other to reduce interference from the other twisted-pairs in the cable. This is commonly used for telecommunications and modern Ethernet networks. The twisted-pairs in the cable provide protection against cross talk. When an electrical current flows through a wire, it creates a small circular magnetic field around the wire. When two wires in an electrical circuit are positioned close together, their magnetic fields are exactly opposite to each other. Thus, the two magnetic fields cancel each other out, eliminating the problem of cross talk. Cross talk can still be a problem at the ends of the cable when the wires are untwisted to insert into a terminal, such as an RJ-45 Ethernet interface.

There are two types of twisted-pair cable:

1. Unshielded twisted pair (UTP)
2. Shielded twisted pair (STP)

Unshielded Twisted Pair (UTP)

UTP is a cable that is composed of pairs of wires, as shown in Figure 1-10. It is used in different types of networks. It consists of eight individual copper wires, each of which is covered by insulating material, and wires in the pairs are twisted around each other. To reduce cross talk between pairs of UTP, the number of twists can vary between the pairs, with a tighter twist resulting in better transmission.

The quality of this cable may vary from telephone wire to high-speed network cable. These cables are easy to install and are less expensive than other network media.

UTP cable slowly relies on the cancellation effect generated by the twisted wire pairs to control signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). It is installed using a Registered Jack-45 (RJ-45) connector. RJ-45 is an eight-wire connector used to connect computers in a local area network (LAN), as shown in Figure 1-11.

The features of UTP cable are as follows:

- *Speed and throughput*: 10 to 1000 Mbps
- *Average cost per node*: Inexpensive
- *Media and connector size*: Small
- *Maximum cable length*: 100 m (short)

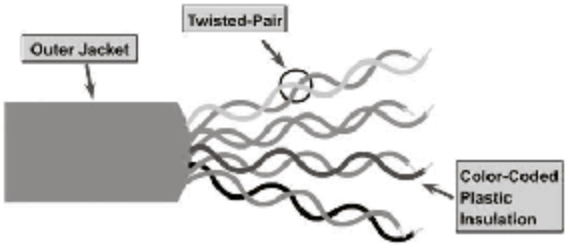


Figure 1-10 Unshielded twisted-pair cable has eight wires that are twisted in pairs.

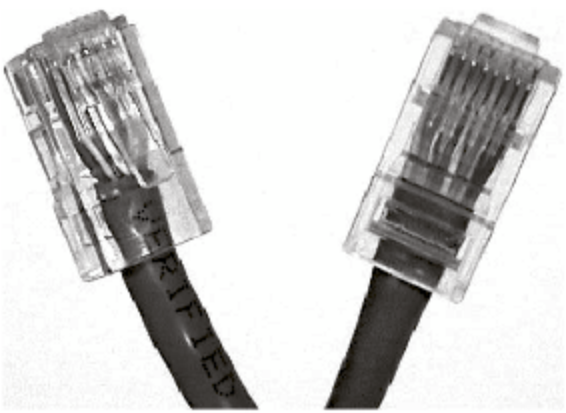


Figure 1-11 RJ-45 connectors are used to connect UTP cables.

The categories of commonly used UTP cabling are as follows:

- *Category 1*: This category is mainly used for telecommunications, not for transmitting data.
- *Category 2*: It is able to transmit data at speeds up to 4 Mbps.
- *Category 3*: It is used in 10BASE-T networks. It can transmit data at speeds up to 10 Mbps.
- *Category 4*: It is used in Token Ring networks. It can transmit data at speeds up to 16 Mbps.
- *Category 5*: It can transmit data at speeds up to 100 Mbps.
- *Category 5e*: It is used in networks running at speeds up to 1000 Mbps (1 Gbps).
- *Category 6*: This cable consists of four pairs of 24 American wire gauge (AWG) copper wires. It is currently the fastest standard for UTP.

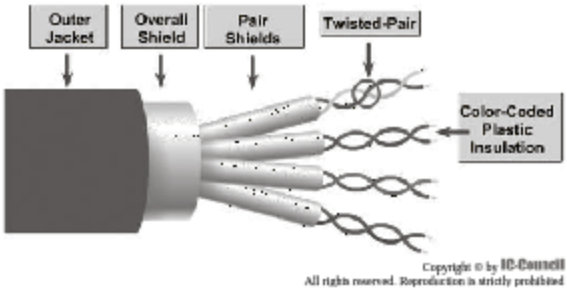


Figure 1-12 A shielded twisted-pair cable uses shielding to reduce electrical noise.

- *Category 7*: This cable standard was created to allow for 10-gigabit Ethernet over 100 m of copper cabling.
- *Category 7a (Augmented Category 7)*: This cable standard allows for operations at frequencies up to 1000 MHz, suitable for multiple applications in a single cable, including 40-gigabit Ethernet, 100-gigabit Ethernet, and CATV.

Shielded Twisted-Pair

STP is a cable that contains metal shielding over each pair of copper wires. It combines the techniques of shielding, cancellation, and wire twisting. Each pair of wires is covered in metallic foil. It reduces the electrical noise both within the cable (pair-to-pair coupling or cross talk) and from outside the cable (EMI and RMI), as shown in Figure 1-12. STP cable is installed with an STP data connector, which is specifically created for STP cables. It can also use the same RJ connector as UTP.

STP prevents interference better than UTP, but it is expensive and difficult to install. The metallic shielding must be grounded at both ends of an STP cable. If it is grounded improperly, the shield behaves like an antenna and picks up unnecessary signals. STP is rarely used in Ethernet networks because of its cost and difficulty with termination.

The following are some of the features of STP cable:

- *Speed and throughput*: 10 to 100 Mbps
- *Average cost per node*: Expensive
- *Media and connector size*: Medium to large
- *Maximum length of cable*: 100 m (short)

Coaxial Cable

Coaxial cable is a kind of copper wire that consists of a hollow cylindrical conductor that surrounds a single inner wire made up of two conducting elements:

1. A copper conductor located in the center of the cable. A flexible layer of insulation encases the copper conductor.
2. A woven copper braid or metallic foil over this insulating material acts both as a second wire in circuit and as a shield for the inner conductor, as shown in Figure 1-13. It can help reduce any outside interference.

Coaxial cable comes in different sizes. Because of its transmission length and noise-rejection characteristics, the diameter is specified to be 1 cm. This type of coaxial cable is referred to as *thicknet*. Thicknet cable is easy to install in some situations because of its thickness. This cable is used for special-purpose installations. A vampire tap is a device used to connect network devices to thicknet. The vampire tap is then connected to computers via a flexible cable, called the attachment unit interface (AUI).

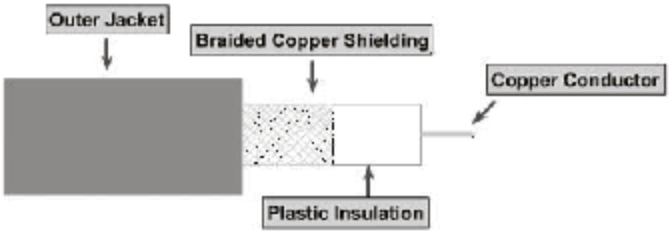


Figure 1-13 Coaxial cable uses plastic insulation over a single copper conductor.

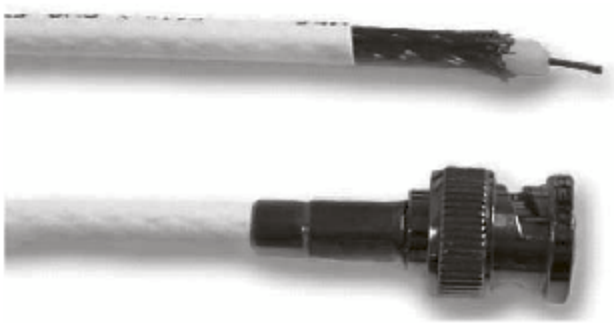


Figure 1-14 BNC T-connectors are used to connect coaxial cables.

Coaxial cables with an outer diameter of 0.35 cm were used in Ethernet networks. Such cables were used especially when they had to be twisted and turned. These are referred to as *thinnet cables*.

A common connector used with thinnet is BNC (Bayonet Neill-Concelman). It is a male connector mounted at each end of the cable. A BNC connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. The outside rotating ring locks the cable to any female connector. BNC T-connectors are female devices for connecting two cables to network interface cards (NICs), as shown in Figure 1-14.

The following are features of coaxial cable:

- *Speed and throughput*: 10 to 100 Mbps
- *Average cost per node*: Inexpensive
- *Media and connector size*: Medium
- *Maximum cable length*: 500 m (medium)

Fiber-Optic Cable

Fiber-optics is a technology that uses glass (or plastic) threads (fiber) to transmit data. It consists of bundles of glass threads, each of which is capable of transmitting messages modulated onto light waves. It is used for networking and consists of two fibers encased in separate sheaths. An outer jacket and many layers of protective buffer material, typically a plastic shield and reinforcing material made of a material such as Kevlar, cover each optical fiber. While the plastic meets fire codes, the outer jacket will protect the entire

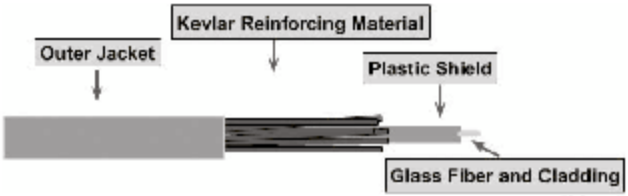


Figure 1-15 Fiber-optic cable uses a glass fiber to transfer data.

cable. The Kevlar furnishes additional cushioning and protection for the fragile, hair-thin glass fibers, as shown in Figure 1-15.

The light guiding of optical fiber parts is called the core and the cladding. The core is very pure glass with a high index of refraction. When a cladding layer of glass or plastic with a low index of refraction covers the core glass, light can be trapped in the core glass. This process is called total internal reflection. Fiber-optic media is more expensive than all other network media.

There are two types of fiber-optic cable:

1. Single-mode
2. Multimode

Single-Mode Single-mode cable allows only one mode (or wavelength) of light to propagate through the fiber. It is capable of higher bandwidth and greater distance than multimode. Single-mode is used for campus backbones. These types of fibers use lasers as a light-generating method. The maximum length of single-mode cable is 10 km (32,808.4 feet).

Multimode Multimode cable allows multiple modes of light to propagate through the fiber. It is also used for workgroup applications and intrabuilding applications, such as raisers. It uses light-emitting diodes (LEDs) as a light generating device. Multimode cable's maximum length is 2 km (6,561.7 feet).

The difference between single-mode and multimode connectors is the precision in the manufacturing process. A single-mode connector hole is smaller than a multimode connector hole. This ensures tighter tolerance in the connector assembly.

There are two types of fiber-optic connectors commonly used in the communications industry:

- *SC*: These types of connectors feature a push-pull connect and disconnect method. The connector is simply pushed into the receptacle to make a connection. Simply pull out the connector to disconnect.
- *ST*: This connector is a bayonet type of connector. The connector is fully inserted into the receptacle and is then twisted in a clockwise direction to lock it into place, as shown in Figure 1-16.

Plenum Cables

A plenum cable is a cable that runs into the plenum space of a building. As ordinary cables cannot withstand threats such as fire, these cables are built into the plenum area of the building. The outer material of a plenum cable is more resistant to flame, produces less smoke, and does not emit the toxic fumes other cables do when burning.

PVC Cables

Polyvinyl chloride (PVC) cables are the most commonly used electrical insulation material. They are primarily dominant in low-voltage applications. Telecommunication is also an important application for PVC. PVC cable includes the following features:

- It provides good electrical and insulation properties over a wide temperature range and provides safety from fire.
- It has excellent durability and long life expectancy.
- It is highly resistant to degradation from ultraviolet lights.

Figure 1-16 The ST fiber-optic connector is used to connect fiber-optic cable.

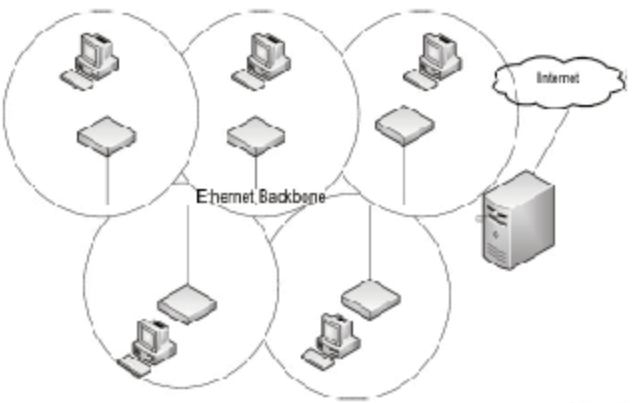


Figure 1-17 Wireless transmission utilizes an Ethernet backbone.

Wireless Transmission

Wireless transmission uses radio frequency (RF) and infrared (IR) waves to transmit data between the devices on a LAN. Components of a wireless network include antennas, amplifiers, and access points (APs), as shown in Figure 1-17.

The user must install a wireless adapter card (wireless NIC) on a PC/laptop in order to send and receive wireless signals. Wireless signals use portions of the RF spectrum to transmit voice, video, and data. Wireless frequencies range from 3 kHz to 300 GHz. The rate of data transmission ranges from 9 kbps to as high as 54 Mbps.

WLAN

A wireless LAN (WLAN) is made in accordance with Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. It uses radio waves (e.g., 902 MHz), microwaves (e.g., 2.4 GHz), and IR waves (e.g., 820 nm) for communication.

The following are some of the different types of wireless transmission:

- Infrared
- Microwave
- Satellite

Infrared Transmission The infrared transmission system is composed of three components: the transmitter, the infrared emitter (also called the radiator), and the receiver. The transmitter modulates the data signals onto a carrier frequency by using frequency modulation or digital techniques. The emitter converts this modulated signal into infrared light. The receiver decodes the infrared signal and converts it to a data signal.

The transmitter generates carrier waves for each channel in a multichannel system. All modulated carrier waves are mixed and sent via a coaxial cable from the transmitter to the infrared emitter.

Microwave Transmission Microwave transmission is a technique for transmitting information over a microwave link. It is used to transmit audio, video, and data using microwaves over distances ranging between a few feet to several miles. Microwave transmission is likely to be subject to attenuation caused by atmospheric conditions, especially at times of wet weather.

Satellite Transmission Satellite transmission offers consistently high transmission quality. It is extremely reliable, and it is used to receive virtually error-free digital transmission across the network. Satellite transmission is commonly used for television broadcasting, weather forecasting, radio communication, and Internet communications.

Line of Sight

Line of sight is one of the problems affecting wireless transmission. The path between the two antennas in wireless communication should be straight. Therefore, line of sight (LOS) is an unobstructed path between the sending and receiving antennas. LOS is easy to achieve for small distances, but difficult for large distances.

The Fresnel zone (an elliptical area immediately surrounding the visual path) is also taken into consideration. Fresnel zone clearance must be considered when determining the height of antennas.

To determine the line of site, the following two items must be identified:

1. Geographical change
2. Height of the antennas

Radio Frequency (Bandwidth)

A radio wave is an electromagnetic wave propagated by an antenna. These radio waves have different frequencies, which can be changed by tuning the radio receiver to a specific frequency (Figure 1-18).

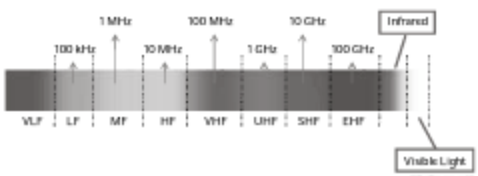


Figure 1-18 Radio waves are on the same spectrum as visible light.

Bandwidth Description	Frequency Range
Very low frequency (VLF)	3 KHz to 30 KHz
Low frequency (LF)	30 KHz to 300 KHz
Medium frequency (MF)	300 KHz to 3000 KHz
High frequency (HF)	3 MHz to 30 MHz
Very high frequency (VHF)	30 MHz to 300 MHz
Ultrafigh frequency (UHF)	300 MHz to 3000 MHz
Superhigh frequency (SHF)	3 GHz to 30 GHz

Table 1-2 This table illustrates the frequency ranges of various bandwidths

The Federal Communications Commission (FCC) determines the purpose of a particular frequency spectrum. In order to transmit on a particular frequency, a person has to obtain a license from the FCC; the fixed frequency will be reserved for the licensed person only. Table 1-2 lists the frequency ranges of certain bandwidths.

Public Switched Network

A public switched network (PSN) is a common carrier network that provides circuit switching for the general public. PSNs are usually telephone networks; they could also be data and packet-switched networks.

PSNs provide traffic routing from local users or from other switching centers, whereby a connection is established between the calling and called stations. The connection is released only when either the called or calling party hangs up. A PSN can be also defined as a network that can be accessed by the public for establishing and terminating telecommunications messages.

Emanations Security

Unwanted emanations result from computer technologies used for storing, calculating, and communicating data. These compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or unintentionally emitted by any number of sources within equipment and systems that process information from information-handling devices. If unauthorized individuals utilize this information it could give way to a serious security breach. Emanation security involves taking measures designed to restrict unauthorized persons from obtaining that information.

The term TEMPEST is broadly used for the entire field of emanations security. The term was coined in the 1970s as a codename for a National Security Agency operation to secure electronic communications equipment from potential eavesdropping by unauthorized individuals.

Media Access Methods

Media access methods determine whether or not a particular node can place data on the network. They can be put into two categories: connection based or competitive media access. Nodes themselves determine media access time.

Token Ring

Token Ring was developed by IBM and designed for a consistent network architecture based on the token-passing access control method. It is incorporated into IBM mainframe systems, such as the AS/400, and could possibly be used with PCs, minicomputers, and mainframes. It performs well with Systems Network Architecture (SNA) to connect with mainframe networks.

FDDI (Fiber Distributed Data Interface)

FDDI is a type of Token Ring network. Its implementation and topology is different from IBM's Token Ring LAN architecture, which is managed by IEEE 802.5. FDDI is also used for metropolitan area networks (MANs) or larger LANs that extend between several buildings in an office complex or campus.

LocalTalk

LocalTalk was developed by Apple Computer, Inc. and is suitable for small networks of Macs. It permits linear bus, star, or tree topologies to use twisted-pair cable. It allows up to 32 devices (computers, printers, and file servers). It transmits data at only 230 Kbps. LocalTalk uses the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) process for transmitting data.

Multiplexing

Time-Division Multiplexing (TDM)

TDM is a technique of placing multiple data streams in a single signal by dividing the signal into several segments, each with a short period. This data stream is reassembled at the receiving side, depending on the timing.

The circuit that merges signals at the transmitting end of a communication link is called a multiplexer. It takes the input from each user, divides each signal into several segments, and then allocates the segments to the combined signal in a rotating and repeating sequence. The composite signal then contains data from several senders. At the other end of the cable, individual signals are divided out by a circuit called a demultiplexer and routed to the proper users. Two-way communication circuits need a multiplexer/demultiplexer at every end of the long-distance, high-bandwidth cable.

Frequency-Division Multiplexing (FDM)

FDM is a method by which multiple signals are merged for transmission over a single communication line or channel. Each signal is allocated a separate frequency within the main channel.

An analog Internet connection on a twisted-pair cable needs 3 kHz of bandwidth for reliable data transfer. Twisted-pair cables are common in households and small businesses. But large telephone cables, which operate between large businesses such as government agencies and municipalities, are able to carry larger bandwidths.

If a long-distance cable has a bandwidth of 3 MHz, it means this is 3,000 kHz. Thus, it is possible to put 1,000 signals into a long-distance channel, each with a size of 3 kHz. The circuit that does this is known as a multiplexer. It takes the input from each end user and creates a signal on a different frequency for each of the inputs. This results in a high-bandwidth, complex signal that includes data from all of the end users. At the other end of the cable, the individual signals are divided by the demultiplexer and routed to the proper end users.

Polling

Polling is a method by which a central device contacts each node to see whether it has data to transmit. In the polling method, every node has guaranteed access to media, but network time can be wasted if polled nodes do not contain data.

Demand Priority

Demand priority is a polling method by which nodes will send their state to a hub as either ready to transmit or idle. The poll state of each node grants permission to transmit. A node can also tell the hub the priority of data that passes through it. The hub will favor high-priority transmission requests.

Token-Based Media Access Method

This is a media access method by which computers pass a special sequence of bits, called a token, between them. Only the node holding the token can transmit on the network. After transmitting data, or if it does not contain data, a node passes the token to the next computer on the network.

Advantages and Disadvantages

This method is said to be deterministic because every node has guaranteed access to the media. This is best for networks in which timing is critical. In addition, even when traffic is very high, every station has the same chance to transmit its data. However, token passing is ineffective when traffic is low because a station has to wait when other nodes hold the token and pass it on without transmitting data. Also, each node needs complex software to control the token-passing process and may need reconfiguring whenever a node is added to or removed from the network.

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

This is a contention-based media access method by which nodes can transmit whenever they have data to transmit. CSMA/CD must detect and manage expected collisions that take place when multiple nodes transmit at once.

In CSMA/CD:

1. A node has data to transmit.
2. The node determines whether the media is available or not.
3. If media is available, then the node transmits its data.
4. The node determines if a collision has occurred by detecting the fragmented data that results from the collision.
5. If there is a collision, the node waits for a random back-off time that is calculated in milliseconds, and then repeats the process until successful.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

CSMA/CA is a contention-based media access method by which nodes can transmit whenever they have data to transmit. However, they take the following steps before they transmit to ensure that the media is not in use:

1. A node has data to transmit.
2. The node determines whether the media are available or not.
3. If media are available, the node sends a jam signal to advertise its intent to transmit data.
4. The node waits until all nodes have time to receive the jammed signal.
5. The node then transmits its data.
6. When transmitting data, the node monitors the media for a jammed signal from another node. If a jammed signal is received, it stops transmitting the data and retries after a random delay.

Contention Domains

A contention, or collision, domain consists of nodes whose simultaneous transmission may interfere with that of another node. All devices in a contention domain compete for the right to transmit data. Any device in this domain transmits data if there is no other traffic on the media.

Automated Information Systems (AISs)

Automated Information Systems (AISs) are a combination of computer hardware, software, and firmware. AIS is specifically developed for critical information handling and protection. It is useful in processes such as communication, computation, dissemination, processing, and storage of information.

AIS is used in the following ways:

- *Management issues*: As more and more operations are dependent on computers, it has become important for a computer to fully manage all tasks. The need of management to handle critical issues creates the need for AIS.
- *Value of information and computing resources*: Processes such as communication and computation assure ready availability and high integrity, whereas confidentiality is a critical issue handled by AIS.

Historical Versus Current Technology

Hardware

Hardware is a general term used to refer to the physical components of a computer system. This includes keyboards, circuit boards, monitors, graphics cards, and mice.

Distributed Versus Standalone

Hardware that is offering its services to the whole system/organization is referred to as distributed hardware. It provides reliability, sharing of resources, and scalability. However, it lacks in its ability to provide security.

Hardware that restricts its services to a single computer is called standalone hardware. It offers security but provides limited benefits.

Microprocessors, Miniprocessors, and Mainframe Processors

Microprocessors

A microprocessor is a small and integrated version of a CPU (central processing unit). It combines the functions performed by the CPU into a small integrated circuit (IC). Previously, CPUs were so large that they were difficult to handle and consumed a large amount of space. The small size of the microprocessor makes it compact enough to fit in a small cabinet.

Microcomputers are differentiated on the basis of the following characteristics:

- *Instruction set*: The set of instructions that the microprocessor can execute.
- *Bandwidth*: The number of bits processed in a single instruction.
- *Clock speed*: The clock speed of the microprocessor determines how many instructions the processor can execute in one second. It is calculated in megahertz (MHz).

Miniprocessors

A miniprocessor is a low-cost logic circuit that uses integrated circuits (ICs). It has started a revolution in the computer field, as it is easy to handle and can be used to perform calculations in the engineering and science fields. It is very useful for scientific research and operations.

Mainframe Processors

Mainframe processors are large and expensive processors. The main advantage of this kind of processor is that it can handle complex calculations. It is useful for handling hundreds, or even thousands, of users simultaneously and can be placed just below supercomputers in power.

Components

Input and Output

Communication between the machine and user is possible when the machine sends output to a device based on the input the user provides. Basically, input is the signal or data received by the system, while output is the relevant signal or data sent from the system. Some devices are used to perform both operations. Modems and network cards fall under this category.

Central Processing Unit (CPU)

A central processing unit (CPU) is a device that carries out logical functioning and executes computer programs. Since their invention, CPUs have gone through logical and physical evolutionary changes. The CPU is now very compact and efficient. Today, the CPU is used in many applications for fast and appropriate functioning of appliances.

Memory

Memory is the capacity to store, retain, and subsequently retrieve information. It is the internal storage device in the computer where all data being used and currently running processes is stored.

There are several different types of memory:

- *RAM (random-access memory)*: It is possible to read stored data from, as well as write data to, RAM. However, this memory is volatile and requires a continuous power supply. Once the power supply is switched off, data stored in RAM is lost. Thus, it is also known as volatile memory.
- *ROM (read-only memory)*: This type of memory is present in almost all types of computers. ROM is typically used to hold the instructions to start the computer. Unlike RAM, ROM cannot be written to. It is only meant for reading instructions.
- *PROM (programmable read-only memory)*: PROM is a chip on which a program can be stored. It is permanent and cannot be wiped out. Once used, memory cannot be used for saving other data. Like ROM, PROM is nonvolatile.

- *EPROM (erasable programmable read-only memory)*: This is a special type of PROM that can be erased by exposing it to ultraviolet light.
- *EEPROM (electrically erasable programmable read-only memory)*: EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge.

Sequential In a computer, sequential-access memory (SAM) is a data storage device that reads data in a sequence. It is completely different than RAM, where the data is accessed in any order. Though sequential memory is read sequentially, a certain location can be accessed by seeking that location.

Random This memory type is different than sequential memory. Random memory allows a user to access stored data in any order. It refers to the fact that any piece of data can be returned in a constant time. Accessing the memory does not depend on the physical location and previous data.

Volatile Versus Nonvolatile Volatile memory, also known as a primary storage device, is a memory type that requires a constant power supply to maintain the stored information. Most random-access memory is volatile storage, including dynamic random-access memory and static random-access memory.

Nonvolatile memory, then, is the opposite of volatile memory. It is not affected by a disrupted power supply. It stores and retains information even when there is no power. Nonvolatile memory includes ROM, flash memory, hard disks, floppy disk drives, and magnetic tapes.

Nonvolatile memory is mainly used for the purposes of secondary storage or for the long-term storage of data. Nonvolatile memory is more costly and performs worse than volatile random-access memory.

Critical Information Characteristics

Information systems security is concerned with three characteristics of information: confidentiality, integrity, and availability.

Confidentiality

Confidentiality is critical for the security of an information system. A security policy is a set of rules that determines whether to permit or deny access to a particular object. Confidentiality is the assurance of access granted only to the authorized party, process, or object.

All organizations require protecting certain information. It is also important to differentiate between important and less important data, which will help in deciding what data requires protection from others.

Integrity

Integrity focuses on the fact that though confidentiality focuses on data security, there is a need for an individual who is authorized to modify the data. Integrity also includes accuracy, relevancy, and completeness. Integrity also focuses on the quality of information and the assurance that the data has not been corrupted or changed.

Availability

Availability is also included and is as important as confidentiality and integrity. Security mainly focuses on ensuring that information is provided to authorized users whenever required and asked. Information systems security has become a science of the study of compromises, as security and utility often conflict.

Information States

Transmission

Transmission is the act of sending information from one system to another. This transmitting of information is only possible when the computer is using a data transmission protocol.

Storage

Storage is the process of saving and retrieving information that can be reproduced when the stored information is needed.

Storage Devices

The devices that store data or information are known as storage devices. Few storage devices have the ability to process the information stored in them. Storage devices store data either in analog or digital form.

Processing

The act of analyzing data and transforming raw data into useful information is called processing. A computer usually automates processing.

Operations Security (OPSEC)

Operations security (OPSEC) identifies, controls, and protects classified or sensitive information. While classified information comprises only a small part of the information and activities processed by organizations every day, its security is critical. If classified information becomes known to a competitor or adversary, it could become a problem.

OPSEC is the process that allows a manager to look for possible security breaches in a system. Hence, it provides all possible ways by which adversary elements can intrude and misuse an organization's sensitive information. It basically focuses on finding and correcting ways for compromising the information. It is used by government agencies and contractors in the development and acquisition of new equipment and in intelligence collection.

OPSEC Process

The OPSEC process involves the following:

- *Identifying critical information*: OPSEC focuses on information that needs to be protected. This may be a stream of information or a complete process.
- *Analyzing the threat*: This will help determine the ways that a possible adversary could intrude and steal information.
- *Identifying vulnerabilities*: Focusing on vulnerabilities is a way to determine which information an adversary could use against an organization. It helps to observe what data the adversary would be interested in and how he or she would be able to obtain it.
- *Analyzing risk*: Risk analysis allows the manager of an organization to determine the hazards caused by loss of information. In risk evaluation, vulnerabilities are weighed against the cost of the loss of data.
- *Countermeasures*: Finally, managers have deployable solutions to reduce risks by eliminating vulnerabilities. Another way to do this is to disrupt the effective collection of information, in which all important information is not stored in the same place and is mixed with other information to mislead the intruder. The factors that determine the use of countermeasures are cost, timing, feasibility, and the imagination of the person involved.

INFOSEC and OPSEC Interdependency

Previously, INFOSEC (information security) and OPSEC were considered to be two separate compartments of the information security system of the organization. It is now clear, however, that both of these are interdependent and can be handled simultaneously. Today, information-dependent organizations need risk management to be dealt with through INFOSEC and OPSEC simultaneously. Recently, legislation and regulations such as Basel II (for banks), the Turnbull report (for the London Stock Exchange), and the Sarbanes-Oxley Act (for the New York Stock Exchange) say that if an organization does not have adequate mechanisms in place for controlling and auditing its flow of information, then the organization could lose a great deal of money.

Information security specialists are familiar with network threats and vulnerabilities. Figure 1-19 shows five levels of information security from operational security to strategic planning.

Unclassified Indicators

Unclassified indicators can be used to reveal critical information that requires OPSEC measures for additional protection. OPSEC mainly focuses on removing, minimizing, or covering the unclassified indicators that can compromise classified information, especially critical information. While programs like information security protect classified information, they cannot prevent all indicators of critical information, especially unclassified indicators, from being revealed.

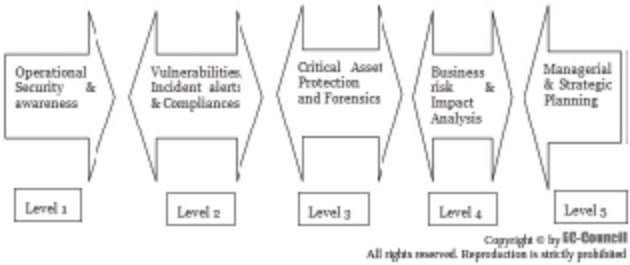


Figure 1-19 These are the five levels of information security.

OPSEC Surveys/OPSEC Planning

An OPSEC survey is a method for examining the sufficient protection of critical information during the planning, preparation, execution, and postexecution phases of any operation or activity. This survey will analyze all associated functions to identify sources of information, what they disclose, and what can be derived from the information.

An OPSEC survey is a time-intensive method, so it should only be conducted when necessary. Extremely sensitive programs, activities, or operations where the slightest compromise will result in mission failure and/or extreme damage to national security are rare examples where an OPSEC survey may be conducted.

Object Reuse

Object reuse focuses on the allocation or reallocation of storage objects. It is mandatory for security to avoid using a system resource that can be used to pass data from one process to another. This can be considered a violation of security policy. Objects normally use resources like buffers and caches. An operating system like UnixWare clears buffers and caches before assigning them to other processes. This ensures that no process inherits or reads the data of other processes, either intentionally or unintentionally. However, the controlled sharing of memory is a difficult task, as it allocates and reallocates the memory to different processes. UnixWare allows many processes to execute simultaneously in memory. This includes the allocation of memory to a process and again deallocating it, allowing the memory to be reallocated to another process. This reallocation may be a threat to security, as information may remain when a section of memory is reassigned to a new process.

Understanding the OSI Reference Model

In the early years of networking, communication between two different computers and different applications was difficult, as they adhered to different communication standards. Later, different standards bodies, users, and providers agreed upon a similar architecture for communication irrespective of the applications and operating systems that were being used.

The Open System Interconnection (OSI) model's protocol function is divided into separate layers, as shown in Figure 1-20. Each layer has specific functions. The design of the OSI model is based on the following principles:

- Each layer should have a fully defined function
- The boundaries of the layers are selected to reduce the flow of information in the interface
- When an additional level of abstraction is required, a layer is created
- Each layer contains the functions of the international standardized protocols

A type of system that implements the protocol behavior and consists of these layers is called a protocol stack. The OSI model contains the following layers:

- *Layer 1*: Physical layer
- *Layer 2*: Data-link layer

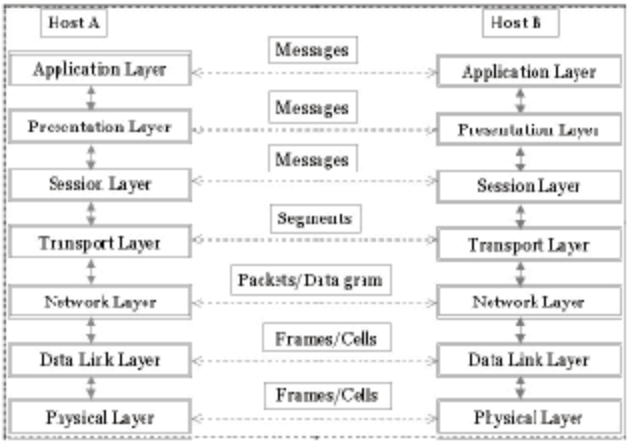


Figure 1-20 The OSI model is the standard networking model.

- *Layer 3*: Network layer
- *Layer 4*: Transport layer
- *Layer 5*: Session layer
- *Layer 6*: Presentation layer
- *Layer 7*: Application layer

Physical Layer

The physical layer manages the operations needed to send a stream of data over a physical medium, as shown in Figure 1-21. It deals with mechanical and electrical requirements. It also describes the methodologies and functionalities of the physical devices and interfaces to achieve the communication required.

The following are the responsibilities of the physical layer:

- *Features of the interfaces and media*: The physical layer defines the features of the interfaces between the devices and the communication media.
- *Depiction of data*: The data is depicted in the form of 0's and 1's without any encryption when passed through the physical layer. The data is encoded into signals that may be electrical signals or light signals.
- *Organization of data bits*: The sender and receiver must have their data organized at the bit-stream level.
- *Configuration of links*: The physical layer deals with the links of the devices to the medium. In a point-to-point connection, the devices are attached through a single link. In a multipoint design, a link is divided among many devices.
- *Topology of devices*: The topology deals with the position of devices through which they form a network. The devices can be connected in the network using mesh, star, ring, and bus topologies.
- *Mode of communication*: The physical layer also describes the mode of transmission between two devices. The available modes are simplex, full-duplex, and half-duplex types.

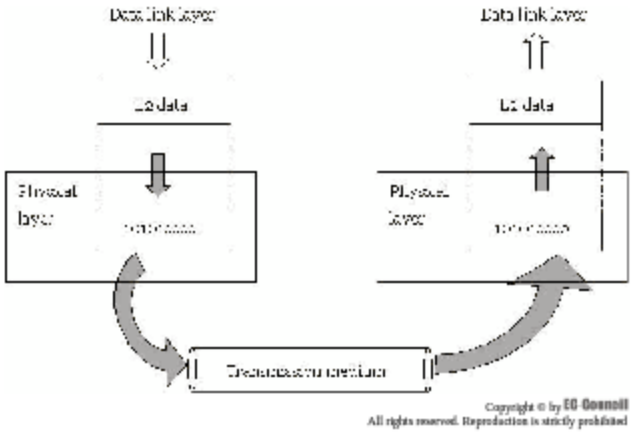


Figure 1-21 The data transmission path moves through the physical layer.

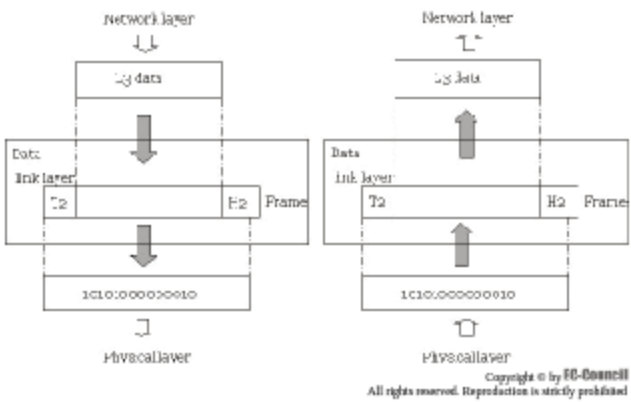


Figure 1-22 The data-link layer makes the physical layer secure.

Data-Link Layer

The data-link layer is responsible for device-to-device delivery. The objective of the data-link layer is to make the physical layer secure without any errors, as shown in Figure 1-22.

The following are the responsibilities of the data-link layer:

- *Grouping*: The data-link layer groups the bits of information received from the network layer into data packets, called frames.
- *Addressing*: The data-link layer adds a header to the packet to describe the original address of the sender or the receiver.

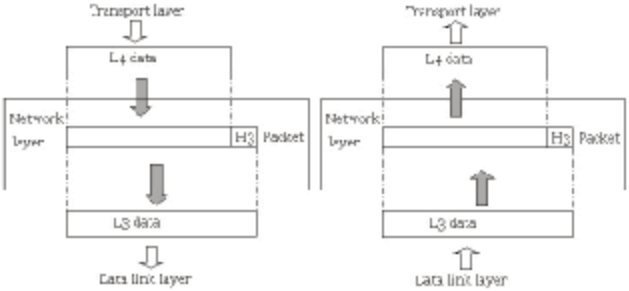


Figure 1-23 The network layer makes sure that packets are routed correctly.

- *Flow control*: Data taken by the receiver is received at a rate that is less than the rate generated by the sender. The data-link layer employs the flow-control mechanism to reduce data flooding at the receiver's end.
- *Access control*: When multiple devices share the same connection, the data-link layer employs certain protocols that are essential to determine the devices that have authority over other devices.

Network Layer

The network layer is useful for source-destination transmission of packets across multiple networks. The network layer makes sure that individual packets initiated from the source reach the destination, as shown in Figure 1-23.

The following are the responsibilities of the network layer:

- *Global addressing*: Global addressing is executed through the data-link layer, which deals with the addressing problem locally. If the packet passes the network border, another addressing system is essential to separate the source and destination systems. The network layer supplies a header to the packet that originates from the upper layers and includes the global address of the sender and receiver.
- *Routing of data packets*: The network layer is linked together to create an internetwork, which is a huge network, through which the linking devices route the packets to the final destination.
- *Fault handling*: The network layer is useful for fault control from source to destination. The sending network layer ensures that the whole message arrives at the receiving device without any errors.
- *Traffic control*: The network layer is useful for controlling the flow of traffic from source to destination so that the end user is not overwhelmed.

Transport Layer

The transport layer is useful for sending packets from the source to the destination. The transport layer makes sure that the entire message is transmitted without any deletions or modifications by helping in fault control and transmission control. For security enhancement, the transport layer can maintain a connection between the end points, as shown in Figure 1-24.

The following are the responsibilities of the transport layer:

- *Addressing*: The transport layer's packet has a header that is useful for holding the address of the service point address. The network layer transmits the exact packet to the transport layer and makes the whole message arrive at the exact process on that device; the transport layer gets the whole message to the exact process on the computer.

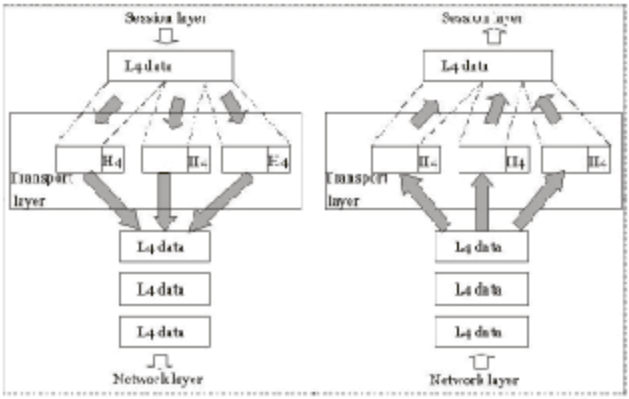


Figure 1-24 The transport layer ensures the correct transmission of data.

- *Isolation and reconstruction*: A message is broken into many segments for transmission, and each segment holds a sequence number. These numbers permit the transport layer to reconstruct the message appropriately at the destination and to recognize and replace packets that are lost during communication.
- *Link control*: The protocols are either connectionless or connection oriented. A connectionless transport layer considers each segment as an individual packet and sends it to the transport layer at the destination. A connection-oriented transport layer initially establishes a connection with the transport layer at the end machine before sending any packets.
- *Transmission control*: Fault control is performed from destination to destination through a single link. The sending transport layer ensures that the whole message arrives at the receiving device without any errors.
- *Error control*: The transport layer is useful for fault control from source to destination.

Session Layer

The session layer monitors the communication between two devices, as shown in Figure 1-25. The following are the responsibilities of the session layer:

- *Communication control*: The session layer permits two devices to establish a dialog between them. It permits communication between the devices to take place in full-duplex or half-duplex form.
- *Data organization*: The session layer permits the process to employ checkpoints. If a system is sending a file of 1,000 pages, checkpoints are inserted after every 100 pages to make sure that each 100-page unit is received. An acknowledgment for each unit is sent individually.

The advantage of the checkpoint system is that if a failure occurs, the entire file does not have to be retransmitted.

Presentation Layer

The presentation layer deals with the syntax and semantics of the data interchanged between two devices, as shown in Figure 1-26.

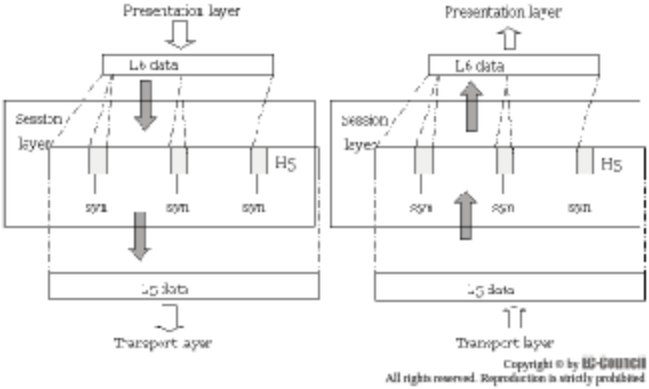


Figure 1-25 The session layer monitors the communication between two devices.

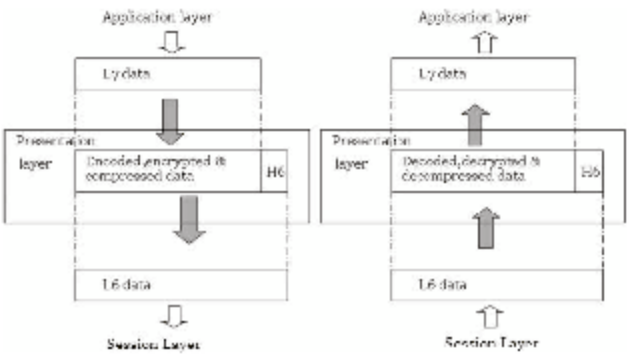


Figure 1-26 The presentation layer deals with the syntax and semantics of the data interchanged between two devices.

The following are the responsibilities of the presentation layer:

- *Translation*: Information must be converted into streams of data before it is sent. As different computers have different encoding systems, the presentation layer deals with the interchange between the various systems of encoding. The data are translated into a common format that the presentation layer at the receiving end will be able to understand. The format of the received data is dependent on the receiver's format.
- *Encryption*: To transmit confidential information, the system must be able to provide security. In encryption, the sender of the data changes the exact information into another format and broadcasts the resultant information.
- *Compression*: The compression of data reduces the number of bits sent. Data compression becomes significant in the transmission of information such as images, sound, and video.

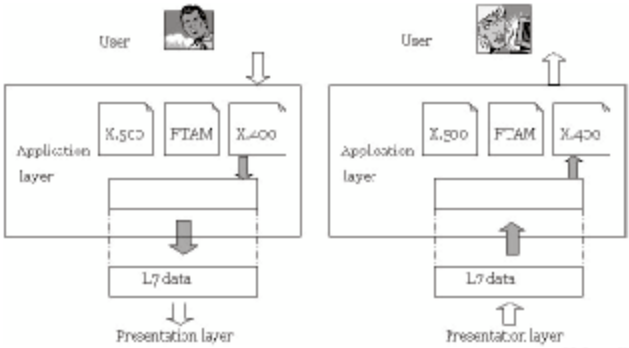


Figure 1-27 The application layer provides users with access to any network.

Application Layer

The application layer provides users with access to any network, as shown in Figure 1-27. It provides services such as interface and help services for e-mail distant file access. It also provides database management for shared systems and many other kinds of distributed systems.

The application layer provides many services, such as the following:

- *Network virtual terminal*: A network virtual terminal is a software system representing a terminal. It permits users to access remote systems. To achieve this, the application generates a software model of a terminal at the remote host. The user's terminal communicates with the software terminal, which again communicates with the original terminal that allows the users to log on to the system.
- *File transfer, file management, and file access*: The application layer permits a user to access files in distant places to get the files from remote computers and to administer the files in an isolated computer.
- *Directory services*: The application layer provides distributed database facilities and access for retrieving the information worldwide.
- *Mail services*: This application provides the foundation of e-mail sending and the storage of e-mail received.

Data Transmission Methods

Data Transmission Modes

A transmission mode is the term used to define the direction of a signal or the flow between two linked devices.

Data transmission modes include:

- Simplex transmission
- Half-duplex transmission
- Full-duplex transmission

Simplex Transmission

This is a type of data transmission in which information is transferred by only one device at a time. It is similar to a one-way road, as shown in Figure 1-28.

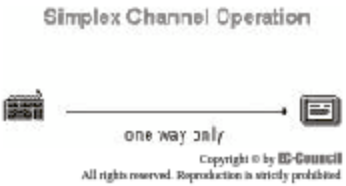


Figure 1-28 Simplex transmission is one-way data transmission.

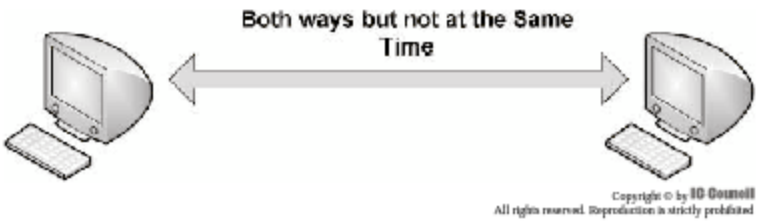


Figure 1-29 Half-duplex transmission can transmit information both ways, but not at the same time.

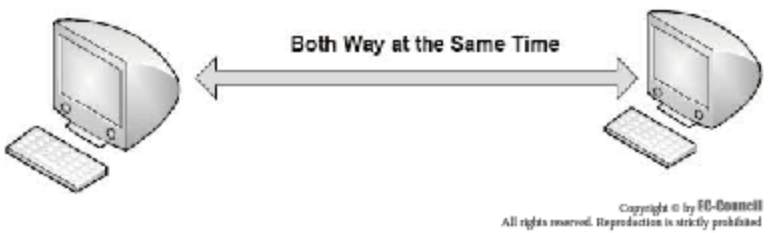


Figure 1-30 Full-duplex transmission can transmit information both ways simultaneously.

Half-Duplex Transmission

In half-duplex mode, data typically transmit in only one direction at a time. Both stations can transmit and receive data, but not at the same time. When one station is sending data, the other can only receive the data, and vice versa. For most LANs, half-duplex mode is efficient.

In half-duplex transmission, the channel transmitting at a particular time uses the entire capacity of a channel. A broadband network supports half-duplex communication. Walkie-talkies and band radios are examples of a half-duplex system, as shown in Figure 1-29.

Full-Duplex Transmission

In full-duplex mode, data can be transmitted in both directions at the same time. Both stations can transmit and receive data simultaneously, as shown in Figure 1-30.

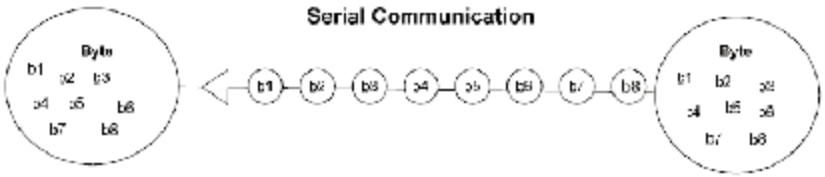


Figure 1-31 In serial data transmission, data bits are transferred over a single medium.

In full-duplex transmission, sharing can be done in two ways:

- The link must contain two physically separate transmission paths for sending and receiving.
- The capacity of the channel is divided between signals traveling in opposite directions.

Some manufacturers are making Ethernet equipment that makes it possible to convert half-duplex mode to full-duplex. Full-duplex Ethernet essentially doubles the throughput of the existing network. The most common example of this is a telephone network, where two people can talk and listen at the same time.

Types of Transmission

A transmission is a channel capable of carrying data from one terminal to another terminal. There are four different types of transmission:

- Serial data transmission
- Parallel data transmission
- Unicast transmission
- Multicast transmission

All these transmissions are used to transfer data, but in a different manner.

Serial Data Transmission

In serial data transmission, data bits are transmitted at a rate of one per clock cycle over a single transmission medium, as shown in Figure 1-31. The synchronization of bits, start/stop bits, and error correction bits are transmitted serially by limiting the overall throughput of data.

Data must pass through a serial interface to exit a computer as serial data. This communication is also called a "one-at-a-time transmission" because bits are transferred one after the other.

Figure 1-31 illustrates the flow of data from one terminal to another in a serial manner. Here, data is transferred in terms of bits.

Parallel Data Transmission

In parallel transmission, multiple bits are transmitted across multiple transmission lines, as shown in Figure 1-32. Many data bits or multiple bytes are also transferred per clock cycle. During this transmission, synchronization of bits, start/stop bits, and error correction bits are transmitted in a line of data bits, which in turn improves overall throughput of data by using additional parallel data lines.

Unicast Transmission

Unicast transmission is a type of transmission method in which information or data is transferred from a specific host address to a specific host destination address, as shown in Figure 1-33. In this transmission, there is only one sender and one receiver. The most familiar standard applications of this transmission are HTTP, FTP, SMTP, and telnet.

All LANs, like Ethernet and IP networks, support unicast transmission. This is an inefficient method as it carries the same information multiple times, which requires more bandwidth. Each unicast transmission over a

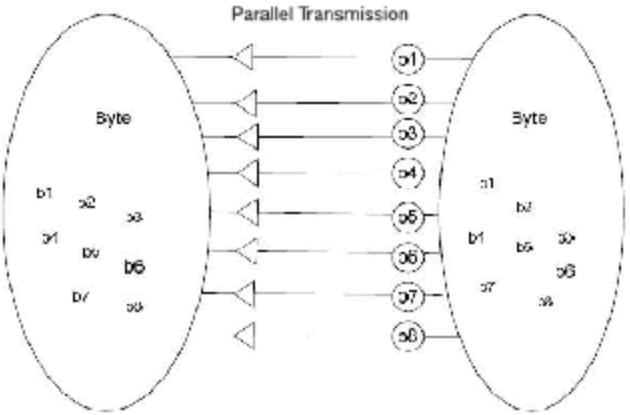


Figure 1-32 Parallel data transmission transfers data across multiple lines.

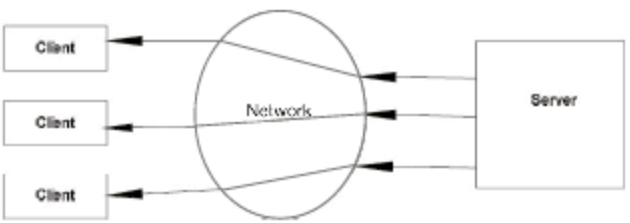


Figure 1-33 Unicast transmission transmits data from one address to another.

network must touch each point or node on the entire network to get to the intended receiver. This transmission is also called a point-to-point network.

Multicast Transmission

In the multicast transmission method, data is transmitted or sent from a server to a specific node that is defined as a member of a multicast group, as shown in Figure 1-34. In these transmissions, a piece of information is sent from one or more points to a set of other points.

Classifying the Network

This classification mainly deals with the logical connection of networks and concentrates on how a network is connected. A logical network combines together a set of entities (e.g., users) that are somehow connected.

There are three different network classifications:

1. Client-server networking
2. Peer-to-peer networking
3. Mixed-mode networking

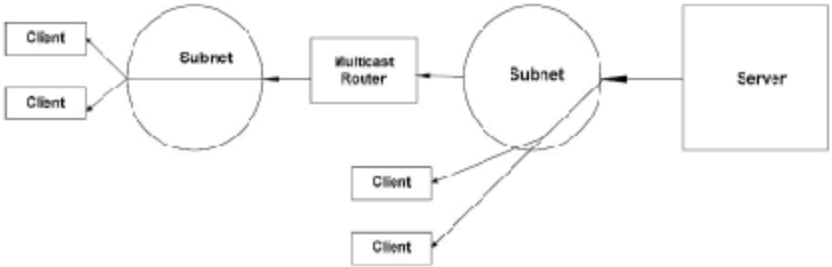


Figure 1-34 Multicast transmission sends data from a server to a specific node.

Client-Server Networking

In a client-server network, some computers act as clients and some act as servers. Clients are those computers who use services that a server provides. A server is a high-powered computer that provides services to computers on a network. It provides back-end support (i.e., all databases are present on the server side). It stores e-mail, Web pages, files, and/or applications.

The following are some of the different kinds of servers that control the sharing of data:

- File servers
- Print servers
- Application servers
- E-mail servers
- Web servers
- Database servers

A client-server network can be constructed by designating one or more of the networked computers as a server and the rest as clients, even when all of the computers can perform both functions. In most LANs and WANs, client-server technology is more useful. However, it is preferable to keep more than one computer as a server because if the server fails in a single server system, the entire system goes down.

A client-server network typically uses a directory service as a database to store information about the network and its users. Users (who use client computers) who want to use a service can log on to the directory service instead of logging on to individual computers, and administrators (who use the server computer) can control access to the entire network using the directory service as a central resource.

Server computers provide the necessary network security and control. The network manager functions as an administrator and manages the client-server network. The administrator determines which resources should be made available and sets permissions on the resources, as shown in Figure 1-35.

A server generally has large hard drives, additional random access memory, and additional hardware installed to manage all network functions. Client-server networks are much more common in businesses.

Peer-To-Peer Networking

In ***peer-to-peer networks***, every computer operates as a client and a server (i.e., any computer can share its resources with the network and access the shared resources on other computers). Peer-to-peer networks are easy to set up and require no special hardware or software or an expensive central computer.

The following are some disadvantages of peer-to-peer networks:

- This type of network can only be applied in some LANs because each system has to maintain its own user accounts and other security settings.
- There is no centralized management of the network.

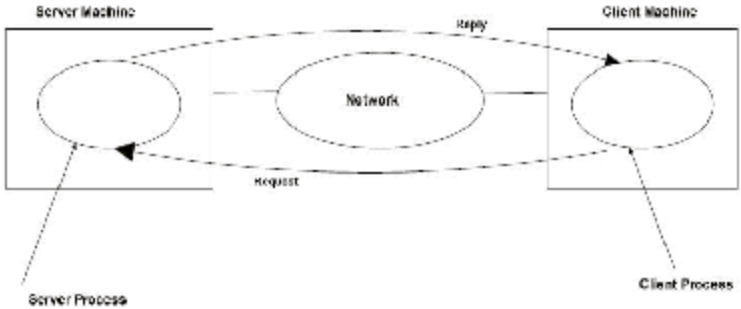


Figure 1-35 Client-server architecture uses a request-and-reply method of communication.

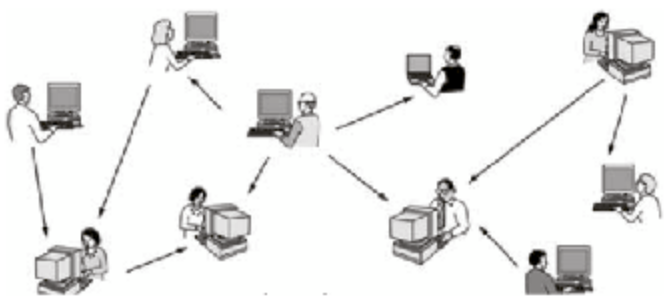


Figure 1-36 Peer-to-peer networking shares data equally among users.

- Each user has to make regular backups of data, because the data and software are located on several different computers.

Peer-to-peer networks are much more common in homes and small offices.

Figure 1-36 illustrates how peer-to-peer networks work. The data or information is shared among different users equally. This network gives equal importance to all the users.

Mixed-Mode Networking

A mixed-mode network is a combination of a client-server network and a peer-to-peer network. This network has elements of both of these two types of networks. One of the major uses of a mixed-mode network is a workgroup created to share local resources within a client-server network.

Network Topology

Network topology deals with the way in which connections are made within a network. Two or more devices connected to two or more links form a topology. Topology deals with a network's overall design and data flow. A physical topology is a topology that deals with the configuration of cables, computers, and other peripheral devices.

There are seven different types of topologies:

- Bus
- Star or hub
- Star-wired
- Mesh
- Ring
- Tree
- Hybrid

Data Sharing

A storage area network (SAN) improves the concept of data sharing. Though LANs allow the application and end user to access data at a central location, a SAN moves the data to a much faster infrastructure. This helps to transfer large files in parallel to multiple computers without affecting the corporate LAN.

Participating computers must be able to find and use the contents of a file while sharing the data. Thus, participating computers with different operating systems are required to use protocols for the transmission of data between protocol translation modules. This helps establish a common communication between the systems.

Data sharing is associated with primary storage devices but can be done with secondary storage as well. Storage devices, such as robotic tape libraries, contain multiple tape devices. More than one computer can access a large quantity of media using SANs. This increases the capability to share data on secondary storage devices.

Device Sharing

Consider an example: A ring-topology network includes adjacent stations that are attached in series independent of each other. Each station in the topology has the capacity to selectively receive data. This same data will not be received by any other station in the topology. Again, each station coordinates the received data with another station, which ensures that the device receives all the data.

File Servers

File servers have a large impact on backup performance. Backup performance can be calculated on the basis of a faster exchange of data. The faster the elimination and distribution of data across the wire, the larger the megabyte-per-minute backup rate will be.

A file server backup can be affected by the following:

- *Hard disk drives (HDDs)*: Most disks have an access time ranging from 10 to 40 ms. The access time affects the overall performance of the file server.
- *Network interface cards (NICs)*: Slow NICs also affect the performance of file servers. NICs may also take up large amounts of CPU utilization.
- *System memory*: The amount of RAM affects the file server backup when it is shared between the file server processes and the backup process. Most file server based backup systems require adding additional amounts of memory.

Bus Topology

Bus topology is a multipoint topology that consists of a long cable that acts as a support structure for the entire network, as shown in Figure 1-37. The long cable is called a bus, and it connects all devices in the network. In bus topology, all the devices in the network are connected to the bus cable using links, such as drop lines and taps. A tap is a connector that slices the bus cable to establish a contact with the metallic part. As the signals pass through the cable, some of the energy is converted into heat. As a result, it becomes fragile in the long run.

Bus topology has the following advantages:

- Installation is effortless.
- The bus cable can be set up through a best path, and in turn, the other connectors can be connected to the devices.

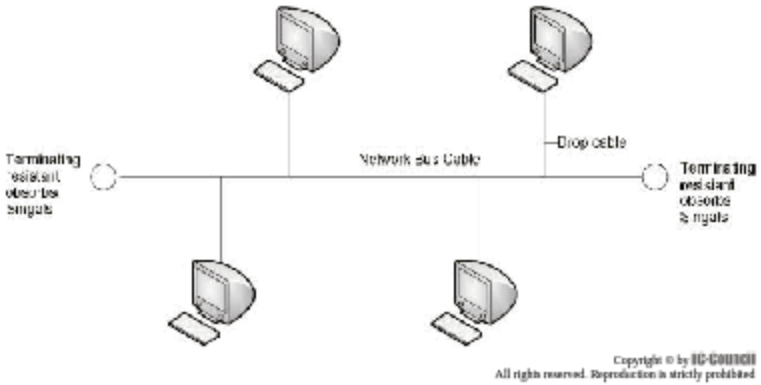


Figure 1-37 Bus topology uses a single cable as the support for the network.

- It requires less cabling compared to mesh, star, and tree topologies.
- Repetition is avoided in bus topology, as the same cable extends throughout the network irrespective of the other topologies.

Bus topology has the following disadvantages:

- It involves a rather difficult design.
- The defect separation is also difficult.
- Since the installation is difficult in the case of a bus, it is also very difficult to add new devices to the bus.
- Sometimes, mirroring of the signals occurs at the tap regions, which can cause signal quality to deteriorate.
- Defects in the bus cable can suspend all communication between devices on the same side.

Bus topology is further categorized into two types:

1. Linear bus
2. Distributed bus

Linear Bus

A linear bus is a type of bus topology that consists of a cable and a terminator at each end, as shown in Figure 1-38. This topology is mainly used in Ethernet and LocalTalk networks.

Linear bus topology has the following advantages:

- It requires fewer cables to connect various devices.
- This topology uses peer-to-peer LANs, coaxial cables, and 50- to 93-ohm terminators for connecting various systems at each end.
- A single cable supports the entire network.
- It is easy to connect new peripheral devices and systems to a linear bus.
- It requires less cable length when compared to a star topology.

Linear bus topology has the following disadvantages:

- Breakdowns in the main cable disable the entire network.
- The main cable uses terminators at both ends of the device.

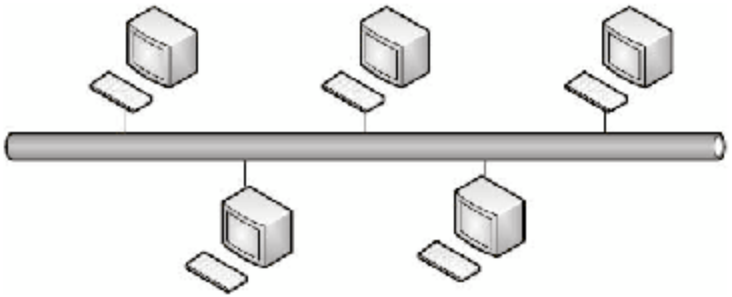


Figure 1-38 A linear bus uses a cable with a terminator at each end.

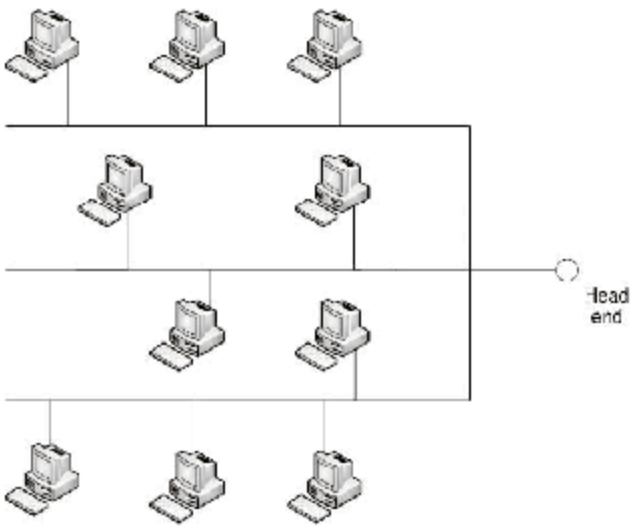


Figure 1-39 A distributed bus uses a single node with links.

- It is difficult to identify problems in this topology in case of network failure.
- This topology is not suited for large buildings that use more devices and systems.

Distributed Bus

Distributed bus is a complex topology. It uses a single node from the trunk cable, called a root or head end, which contains various links in the network.

Figure 1-39 illustrates a distributed bus that has different nodes connected at various branches. If the root fails, then the entire network goes down. All the nodes are connected to a common transmission medium,

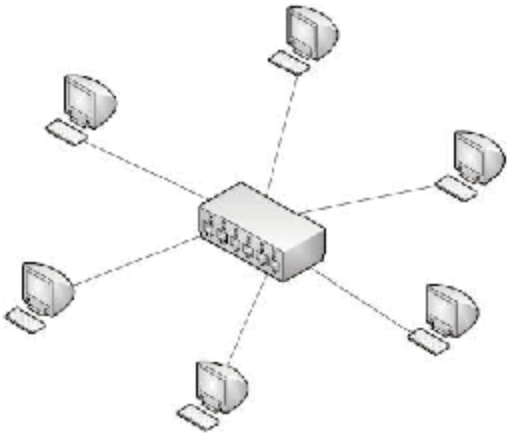


Figure 1-40 Star topology uses a single central computer as a router.

which has more than two endpoints created by adding branches to the main node. This topology is sometimes called a tree topology, as the structure looks like a tree, but it differs in that there is no central node connecting the other nodes.

Star Topology

Star topology is one of the more popular network topologies. Star topology consists of a central, or hub, computer that functions as a router to send messages, as shown in Figure 1-40. In star topology, each device has a devoted point-to-point communication to a central monitoring unit called a hub. The devices are not directly connected to each other. Star topology also does not permit direct traffic between the devices in the network. If one device wants to send data to another device, then the device has to send data to the central hub, which diverts the data to all the other devices in the network.

Star topology is comparatively cheaper than mesh topology, as each device needs only one cable and one I/O device to link to any of the other devices. This fact makes setting up and redesigning the topology more simple. This also leads to less wiring between the already existing devices and the newly installed devices. One of the biggest advantages of the star topology is its strength. If one link is lost, only that particular link is affected. All the other links continue working. This factor results in easy recognition and effortless detection of defects. The hub, as long as it is functioning properly, can examine connection problems and circumvent defective links.

Star topology has the following advantages:

- It is easy to execute and extend in large networks.
- It is adaptable for short-term networks.
- The destruction of a node other than the central node will not have significant effects on the operation of the network.

Star topology has the following disadvantages:

- It has a restricted cable length and supports a small number of stations.
- The cost of maintaining it may become higher in the future.
- Loss of the central node can disable the whole network.

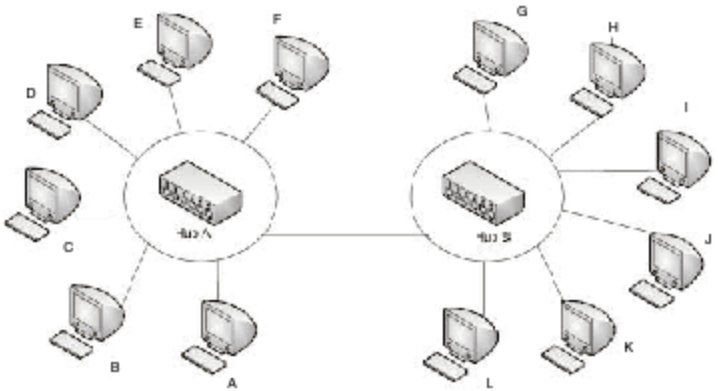


Figure 1-41 Star-wired ring topology combines elements of physical star and logical ring topologies.

Extended Star Topology

In the extended star topology, two or more networks that are arranged in physical star topology are connected using repeaters. The central node of one star network is connected to the terminal node of the other star network. The extended star topology connects multiple hubs of different stars.

Distributed Star Topology

In this kind of topology, two or more networks that are arranged in physical star topology are connected in a linear fashion, with no other nodes that explicitly connect them.

Star-Wired Ring Topology

A star-wired ring topology is the combination of physical star topology and logical ring topology. Devices arranged in this topology form a physical star, as shown in Figure 1-41. A single communication channel exists in the topology, forming a logical ring. Sent messages are forwarded from one device to another in the ring.

The following are advantages of star-wired ring topology:

- Troubleshooting is easy
- Expansion of the network is easy due to the modular design
- The connection of the hub is flexible

The following is a disadvantage of star-wired ring topology:

- Due to extreme flexibility of arrangement, configuration and cabling is difficult

Ring Topology

In ring topology, each device has a dedicated point-to-point communication with only one other device on each side of the device, as shown in Figure 1-42. A signal is sent along the ring in a unidirectional manner through each device until it reaches its destination. Each device in a ring has a router integrated in it. When a device receives a signal meant for another device, the repeater reproduces bits and sends them along the network. In ring topology, a signal keeps traveling through the network until it reaches its destination.

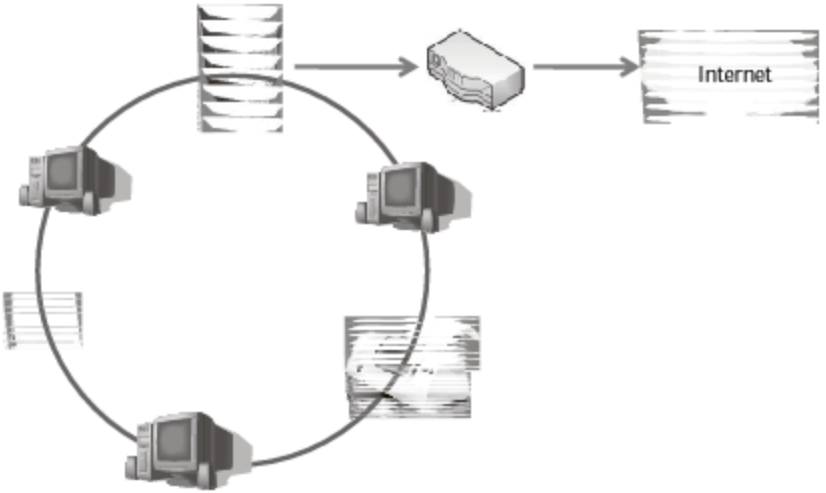


Figure 1-42 In ring topology, signals are sent point to point.

Ring topology has the following advantages:

- The ring is comparatively easy to set up and configure
- Addition or deletion of devices mandates shifting only two connections
- It is easy to find faults in ring topology

Ring topology has the following disadvantage:

- Unidirectional communication can be a defect, as a loss in the ring can cripple the entire network

Mesh Topology

In mesh topology, every device has a point-to-point link to all the other devices, as shown in Figure 1-43. A completely connected mesh network has $n(n-1)/2$ channels to connect n devices. To cater to all the connections, each device on the network needs to have $n-1$ input/output ports. The mesh has many advantages over other topologies. The usage of dedicated point-to-point links ensures that every connection can broadcast its data, reducing the traffic related issues that arise when connections are shared by more than one device. Physical boundaries prohibit unauthentic users from accessing the devices.

Point-to-point devices simplify fault detection and fault isolation. Routing of traffic can be done to reduce the links, which are vulnerable to certain security violations. This functionality enables the network administrator to find out the specific location of errors and helps in detecting the root of the problem and provides solutions.

Mesh topology has the following advantages:

- Mesh topology is strong, and if one of the links is lost, the others are not affected
- Mesh topology makes the network secure

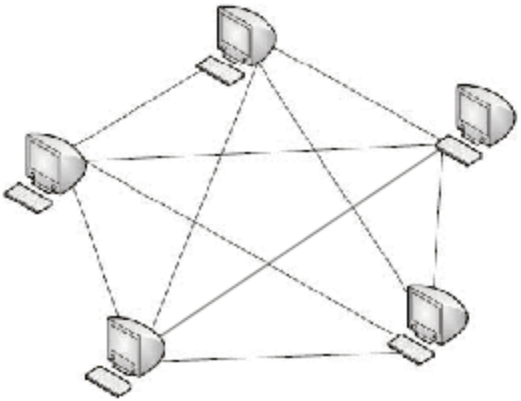


Figure 1-43 Mesh topology connects every unit in a network.

Mesh topology has the following disadvantages:

- A lot of cabling is involved, and more ports are needed
- Every device must be linked to every other device
- The setup and design are tedious
- More space is also required to accommodate all the wiring
- The hardware needed to connect all the links is also very costly
- The mesh topology is executed limitedly for linking the primary computers of networks that use several other topologies

Tree Topology

The tree topology is a version of star. The devices in a tree are connected to a central hub that monitors network traffic, as shown in Figure 1-44. The auxiliary hub is linked to several devices; the auxiliary hub in turn connects to the central hub. The central hub contains a repeater that reproduces the bit streams before sending them. Repeaters make the transmissions robust and enhance the distance signals travel. The auxiliary hub can be active or passive. A passive hub has simpler connections between the linked devices.

Cable-television technology can be considered a typical example of a tree topology. The primary cable is divided into many auxiliary cables, and each cable is further divided into subcables and so on.

Tree topology has the following advantage:

- It permits more devices to be linked to a central hub and thus increases the signal distance between two devices

Tree topology has the following disadvantages:

- If the root fails, the network fails
- It is complicated to configure
- There are slow access times when the network grows

There are two types of fundamental tree topologies:

1. *Minimum spanning tree*: It costs little to connect all the nodes in the topology.
2. *Steiner tree*: This is a least-cost tree that can connect a subset of all the nodes.

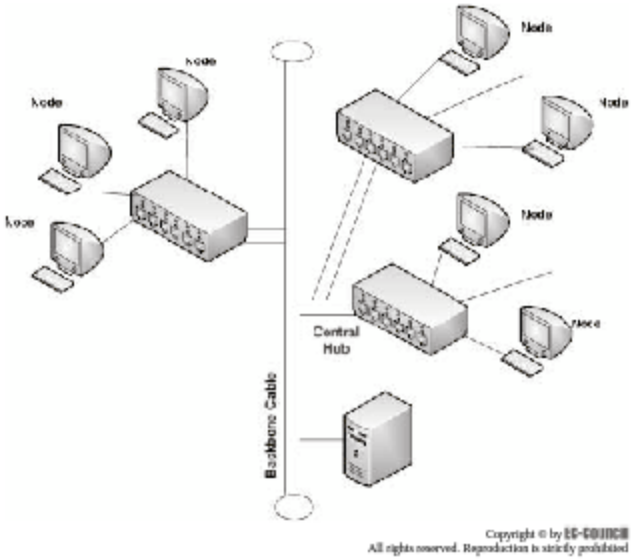


Figure 1-44 In tree topology, a central hub monitors traffic.

Hybrid Topology

The hybrid topology is the combination of any two or more different topologies. The most commonly used topologies are star-bus, as shown in Figure 1-45, or star-ring. A multistation access unit is used in a star-bus.

Physical Network Classification

Networks are classified according to their physical location or their geographical boundaries. The physical location of the network affects its throughput. The arrangement of devices is made according to the needs of the organization and the standards of the network. The following arrangements are among the many network classifications:

- Local area network (LAN)
- Wide area network (WAN)
- Metropolitan area network (MAN)
- Personal area network (PAN)
- Campus area network (CAN)
- Global area network (GAN)

Local Area Network

A local area network typically exists in private organizations and connects the nodes in a single organization or location, as shown in Figure 1-46. LANs usually vary based on the requirements and the type of technology used. A simple LAN consists of only PCs and some hardware devices, such as printers, for domestic purposes such as in homes.

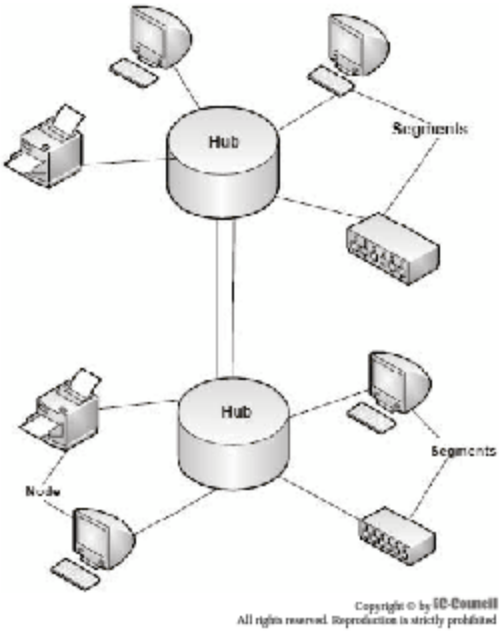


Figure 1-45 Hybrid topologies use one or more topologies together, such as star and bus.

LANs are designed to facilitate the sharing of resources between PCs or workstations. The assets to be shared include hardware devices, such as printers, and software. LANs in organizations are useful for linking the computers, which are allotted identical functionalities. In such a scenario, some of the computers are given higher storage capacities so they can act as servers and the others can act as clients. LANs are also differentiated from other types of networks based on their communication media and topology. Typically, a LAN uses only one type of communication medium. The most popular LAN topologies are bus, ring, and star.

Early LANs had data rates ranging from 4 to 16 Mbps. Now, speeds from 100 Mbps to 1 Gbps (1000 Mbps) are common. The protocols used by LANs also distinguish them from other kinds of networks. LANs can use client-server architecture or peer-to-peer architecture.

The following are some LAN technologies:

- Ethernet
- Token Ring
- FDDI (Fiber Distributed Data Interface)

Ethernet

The original Ethernet was developed by the Xerox Corporation and operated at a rate of 3 Mbps using the CSMA/CD protocol. In later years, three companies (Xerox Corporation, Intel Corporation, and Digital Equipment Corporation) jointly developed Ethernet version 1.0.

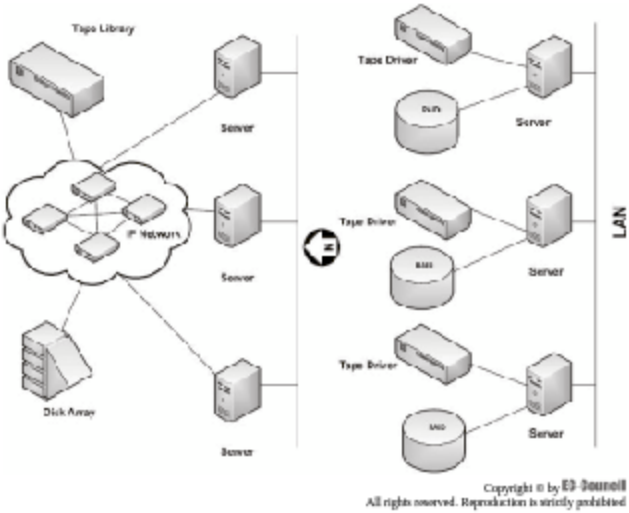


Figure 1-46 Local area networks connect the nodes in a single organization.

Ethernet Elements The Ethernet consists of network nodes and the interconnecting media. There are two major classes of network nodes:

1. *Data terminal equipment (DTE)*: DTEs are devices like PCs, workstations, and file servers.
2. *Data communication equipment (DCE)*: Repeaters, network switches, routers, interface cards, and modems are DCEs. These devices forward and receive data frames from the network.

Basic Ethernet Frame Format In the IEEE 802.3 standard, a data-frame format is provided for media access control implementation and other optional formats, which can extend the capability of the protocol, as shown in Figure 1-47.

Intranet

Intranet is the term for a group of private computer networks. With the help of an intranet, data and resources can be shared within an organization. Intranet uses technologies like Ethernet, Wi-Fi, TCP/IP, Web browsers, and Web servers. Users outside the intranet cannot access the intranet directly.

Wide Area Networks (WANs)

WANs are built to provide transmission solutions for companies or groups who need to interchange information such as data, voice, and images between two distant locations, as shown in Figure 1-48. As the distance involved is great, telecommunication organizations play a role in WAN communications. In fact, leased and public communication companies usually sustain WANs.

The major purpose of a WAN is to provide trustworthy, quick, and secure communication between two or more places with short delays and at low costs. WANs enable an organization to have one basic network between all its departments and offices, even though they are not present in the same building or city, facilitating communication between the organization and other locations worldwide. WANs are subject to a country's public communication department policies and rules.

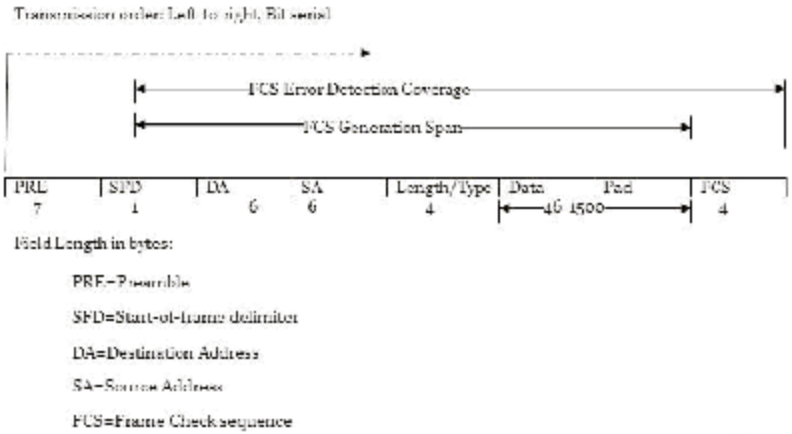


Figure 1-47 A data-frame format is provided for the media access control implementation.

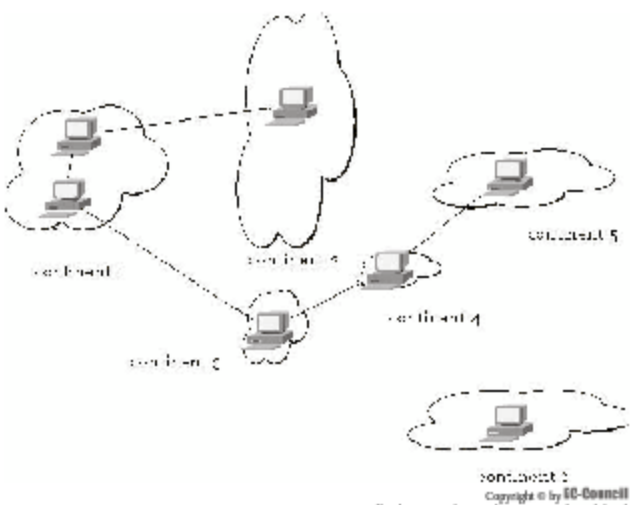


Figure 1-48 WANs facilitate data transmission between distant geographic locations.

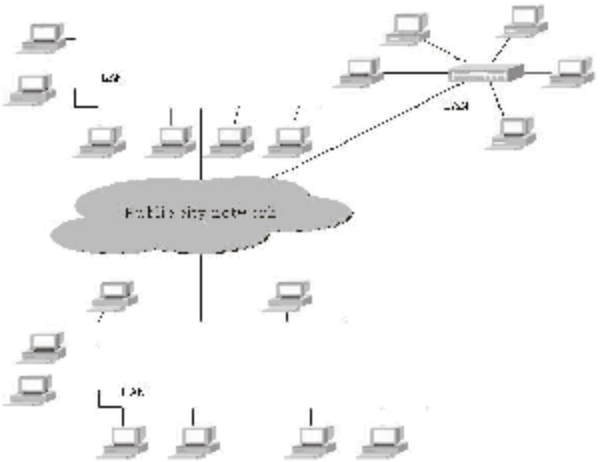


Figure 1-49 MANs are used for public networks.

WAN technologies include the following:

- Packet-switched WANs
- ATMs
- B-ISDNs

Metropolitan Area Networks (MANs)

Metropolitan area networks (MANs) are large computer networks ranging over an entire city. They use wireless communication or fiber-optic cables to connect their areas, as show in Figure 1-49.

For example, large educational institutions may have a MAN that links together many of its local area networks (LANs), which covers a distance that is less than a kilometer. The MAN can in turn link several WAN links to other educational institutions or the Internet. The MAN may be a single network or it can be a huge network, which may involve a number of LANs, facilitating the sharing of assets between the various devices on the network. An organization can communicate with its branch offices throughout a city using a MAN.

MAN technologies include the following:

- Ethernet-based MANs (Metro Ethernet)
- DQDB (Distributed Queue Dual Bus)
- SMDS (Switched Multimegabit Data Services)

Some LAN technologies used for this purpose are ATM, FDDI, and SMDS. These earlier technologies are on the verge of being replaced by Ethernet-based MANs (e.g., Metro Ethernet) in the majority of areas. MAN links into LANs that have been built without wires, using communication links such as optical fibers.

A MAN can be completely owned and monitored by a private organization, or it can be provided as a service by any public organization, such as a telecommunications company.

Personal Area Networks (PANs)

PAN refers to wireless communication that uses both radio and optical signals. PAN is quite similar to WLAN. PANs usually range in tens of feet. For specific PAN hardware, the range is typically up to 10 meters

(approximately 33 feet). PANs cover an individual's work area or workgroup; hence, PAN is known as a room-size network. Bluetooth is a PAN technology. PAN provides the following two different types of systems:

1. *Lower data-rate systems*: These types of systems are used to control and access larger systems like personal computers (PCs) or cell phones. The main use of PAN includes wireless audio, keyboards, mice, and inter-system (PC–cell phone) data links.
2. *Higher data-rate systems*: These types of systems are used for audio distribution and household video.

Campus Area Networks (CANs)

CANs cover a limited geographical area. This kind of network is appropriate for university campuses.

Global Area Networks (GANs)

A GAN is a combination of different interconnected computer networks. A GAN covers an unlimited geographical area. The Internet is an example of a GAN.

Network Equipment Functions

Network Interface Cards (NICs)

A network interface card, more commonly known as a NIC, is a device that allows computers to be linked together in a LAN, or local area network. Networked terminals communicate with each other using an existing protocol, or compliant language, for sending data packets between the different terminals, known as nodes. The network interface card acts as the connection for the machine to both transmit and receive data on the LAN. These cards normally use an Ethernet connection, and are available in 10Base-T, 100Base-T, and 1000Base-T configurations.

The most popular language, or protocol, for LANs is Ethernet, sometimes termed IEEE 802.3. When structuring a LAN, a NIC must be set up in each workstation on the network, and all NICs in the network must be of the same structural design.

An Ethernet NIC is fixed in an available opening inside the computer. The NIC allocates a distinctive 48-bit address, called a MAC (media access control) address, to the machine. The MACs on the network are used to send traffic between the computers. The back plate of the network interface card hosts a port that looks similar to a phone jack, but it is a little larger. This port lodges an Ethernet cable, which looks like a thicker version of a typical telephone line. An Ethernet cable must extend from each network interface card to a central hub or switch. The hub or switch passes information between computers using MAC addresses.

Wireless Ethernet cards are installed like their wired equivalents; but instead of a port for an Ethernet cable, the card hosts a small antenna. The card exchanges data with the central wireless switch or hub via radio waves. Wireless LANs may have some limitations depending on the materials used in the structures that house the equipment. For example, lead in walls can obstruct signals between the network interface card and the hub or switch.

NICs have the following advantages:

- A network interface card does not have to be fixed with physical cable.
- A NIC is used to send as well as receive data.

Access Points

An access point is a piece of wireless communications hardware that creates a central point of wireless connectivity. Similar to a hub, the access point is a common connection point for devices in a wireless network.

Switches

A networking switch is the fundamental device in a wired or wireless LAN. It receives signals from each terminal on the network through Ethernet cables in a wired network and through radio waves in a wireless LAN. In both cases, the networking switch sends traffic across the LAN, permitting the computers to communicate with each other and share resources. Whether wireless or wired, the networking switch acts as a relay, analyzing traffic packets as they arrive from the various machines and sending the packets to the indicated MAC address.

Switch Functions

A networking switch functioning in full-duplex mode implies a machine on the LAN that can receive and send data simultaneously. This is quicker than a networking hub, an alternating device that serves the same function as a switch but functions in half-duplex mode, allowing each machine either to send or receive at any given time. Another discrete difference between a networking switch and a hub is that the switch sends traffic separately, using MAC addresses to send traffic packets accurately to where they are supposed to reach. On the other hand, a networking hub sends all traffic on the network to all nodes, depending on filters within each machine to reject packets not sent to it. Doing so makes the network vulnerable to eavesdropping and loss of available bandwidth for regular network traffic. Network switches are low-priced devices that rise in price with the number of ports featured.

Switches have the following advantages:

- A networking switch is more advanced than a networking hub.
- Antisniffing software can be used on a switched network to sense packet sniffers.

Switches have the following disadvantages:

- A networking switch is not infallible. It can be misled into employing packet sniffers.
- Methods used to mislead the switch will leave traffic signatures, unlike the passive methods that can be used on a hub.

Concentrators/Hubs

Acting as a common connection point for devices in a network, hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Hubs are generally classified in the following ways:

- *Passive hubs*: Passive hubs do not intensify the signal strength of the data prior to transferring the data packets, but they act as a means to transfer data between the devices on the network. They are also known as concentrators.
- *Active hubs*: Active hubs strengthen the signal prior to transferring it to other devices on the network. Active hubs are referred to as multiport repeaters, as they have multiple ports.
- *Intelligent hubs*: Business-critical hubs need additional features. Those hubs to which additional features are added are called intelligent hubs.
- *Switching hubs*: Switching hubs view the destination address of each data packet before transferring it to the specified destination port.
- *Repeater hubs*: Repeater hubs relay inbound traffic. However, active (or switching) hubs transmit the data that is addressed for that specific host. Performance is also improved.

Certain hubs can be arranged for security at the MAC level (such that only specified MAC addresses are hooked up to specified ports). The latest hubs contain HTTP servers as a built-in feature; if feasible, they block access to a specified IP address/port.

Hubs have the following advantages:

- They are flexible and economical devices.
- Every port can make maximum use of the bandwidth without use of CSMA/CD.
- Adding hubs increases the number of ports.
- Hubs organized through SNMP provide tools and statistics for better management.
- Hubs are a low-cost solution.
- Hubs are used to route network traffic and prevent network crashes. They can also combine relatively slow Ethernet devices with those of higher speeds. This facilitates the addition of a variety of devices with a variety of speeds.
- Hubs are not used to control traffic.

Hubs have the following disadvantage:

- If hubs are not monitored, they can be compromised.

Modem

The term *modem* refers to a MOdulator-DEModulator. It is a device that converts digital signals into analog signals and vice versa. The signals from a computer are in digital form, and signals that are transferred over telephone lines are in analog form. The modem performs this conversion. Modulation is performed prior to sending the data, and demodulation is performed after receiving the data. A modulator is a device that converts a digital signal to an analog signal. A demodulator, then, is a device that reconverts an analog signal to a digital signal using the same carrier frequency. The functions of both devices are merged into a single device called a modem.

The following are some of the different types of modems:

- Internal devices that plug into expansion slots in a computer
- External devices that plug into serial or USB ports
- PCMCIA cards intended for use in laptops
- Specialized devices designed for use in handheld computers
- Integrated modems in laptops
- Rack-mounted modems for dial-up ISPs

Modems provide slow speeds for data access and communication. The fastest modem has a maximum speed of 56 kbps. The speed of a modem depends on certain factors, which include the quality of the phone line.

Modem speeds can be presented in either baud rate or bits per second (bps). The baud rate refers to the number of times a signal changes in each second. The bps rate is the number of bits of data that can be sent or received in one second. In some modems the figures are identical, whereas in others, the bps rate is higher than the baud rate.

Router

Routers are more complicated than devices like repeaters and bridges. Routers can access the Internet Protocol (IP) addresses of the network layer and can have incorporated software that helps them identify which of multiple paths are possible between the addresses and which channel is appropriate for the transmission of data.

Routers function in the physical, data-link, and network layers of the OSI model. Routers transmit packets among several interconnected networks. They send packets from a network to other important destinations. A packet sent from one destination to another traverses through the router initially and then moves to the destination network. The destination router, in turn, transmits the packet until the final destination is reached. Routers behave as stations on the network, as shown in Figure 1-50.

Routers receive packets from a linked network and transmit them to the next connected network. If a received packet contains the address of a node of a network to which the router does not belong, the router is capable of

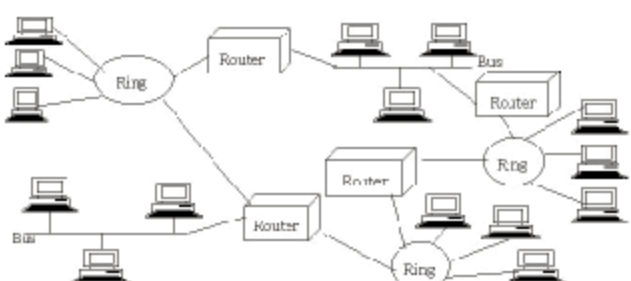


Figure 1-50 Routers act as stations on a network.

identifying which of the linked networks is the next best option for the packet. After identifying the appropriate route for the packet, the router transmits the packet to the other network.

A router maintains a routing table through which it can maintain the paths through which routing occurs as well as the cost of routing across the network. Static routing is a type of routing through which the network administrator monitors the entire routing process. Routing includes many concepts, such as least-cost routing, which shows which path is the shortest available (shortest, in terms of routing, also implies a path that is secure and fastest).

Routers can associate different networks, such as LAN and WAN, and can broadcast data. Routers prevent the collision of data during broadcast. Routers can also act like other devices, such as bridges, which can broadcast packets for a single protocol or group of protocols. When a router receives packets from a multiprotocol router, it receives the packets that correspond to one of the protocols for which they are configured and then sends the packets depending on the addresses of the network layer.

Routers have the following advantages:

- Routers operate at the protocol level.
- Routers provide remote management and design via SNMP.
- Routers support intricate networks.
- The more filtering done, the lower the performance.
- Routers provide security.
- Administrators are able to section networks reasonably.
- Broadcast collisions can be avoided.
- Routers regularly provide bridge functions.
- Routers use complicated routing protocols such as RIP, IGRP, and OSPF.

Routers have the following disadvantages:

- The security issues that routers face are that they do not have security controls that are very efficient, which leads to system compromises.
- Routers cause long delays in initializing sessions for protocols such as FTP. The following aspects must be checked before router transmissions:
  - Mapping between the ports
  - Internal addresses
  - External addresses
  - The port numbers of the internal and external addresses
- Routers are more expensive than other devices.
- Routers need protocols designed for routing.
- Routers are slower than other devices.
- Routers lead to overhead, as they are not capable of separating sent packets.

Brouter

A brouter operates as both a bridge and a router. It is a short name for bridge router because it combines features and operations of both. Normally, it routes routable protocols like TCP/IP and bridges nonroutable protocols.

Brouters operate like routers by relaying data transmission between nodes in a network. However, they also operate like bridges that forward data to the next segment using its physical address if it is found that the data is using an unfamiliar protocol.

Brouters perform the following functions:

- They have routing tables that enable TCP/IP packet traversals.
- Brouters operate without protocol restrictions.
- Brouters look at incoming frames and check the network-layer protocol of that frame. If the brouter recognizes the protocol, it acts like a router and establishes the shortest path. If it doesn't, it acts like a bridge and passes the frame to the next segment.

Brouters have the following advantages:

- They use physical addresses to perform routing.
- They route traffic that uses mixed protocols.
- Brouters efficiently replace routers and bridges.
- Brouters save the cost of installing routers and bridges separately.

Bridges

A bridge filters traffic at the network boundaries. Bridges can send data packets called frames between two segregated LANs at the data-link layer. Bridges are logical devices that can maintain each segment's traffic separately. Through this, bridges prevent congestion and segregation problems. Bridges that operate in the data-link layer permit access to the physical addresses of the terminals linked to it.

When a bridge receives a data packet, it checks the destination address against a lookup table, which contains the physical addresses of all the workstations linked to the bridge. When an address is found, the bridge determines which network segment the packet belongs to and sends the packet to the appropriate segment. Bridges use the MAC address to make decisions on relaying network packets. Bridges also act as filters, determining whether the packets have to be relayed to a segment or not.

Bridges can be classified into the following categories:

- Simple bridges
- Multiport bridges
- Transparent bridges

Transparent Bridging

A transparent bridge contains a forwarding table. Entries are added to the table whenever the bridge receives an incoming packet. If a packet's destination address is in the table, the bridge forwards the packet directly to the destination. If the address isn't in the table, the packet is forwarded to all the devices in the network except the source.

A system with a transparent bridge must satisfy three criteria:

1. Each station should forward frames from one station to another.
2. A forwarding table should be built up from incoming frames.
3. Loops are to be avoided.

Loop Problem Transparent bridges work efficiently if redundant bridges do not exist in the network. If there are two LANs and they are connected via two bridges, then a loop exists in the network, whereby frames can travel endlessly around the network.

ISDN Terminal Adapter

An ISDN terminal adapter is an interfacing device that allows a non-ISDN terminal or other computer device at the physical layer to communicate with an ISDN network. It is employed at the R reference point in ISDN network terminology.

It switches automatically between analog and digital depending on the type of call. An ISDN terminal adapter supports RJ-11 telephone connection plugs for voice access and RS-232C, V.35, and RS-449 interfaces for data.

Terminal adapters have the following advantages:

- Terminal adapters are used in ISDN when a user wants to access the Internet speedily, or for data and video transmission.
- Terminal adapters are available as: add-in expansion cards, which the user can install into computers; external devices like those that connect to the serial interfaces of PC systems; or modules in a router.

Terminal adapters have the following disadvantage:

- The major disadvantage of a terminal adapter is that information from the D-channel of the ISDN line does not pass fully through the terminal adapter. For this reason, non-ISDN equipment is unable to take full advantage of ISDN facilities.

Network Adapter

Each computer should have a network adapter through which it can be connected to the network.

How to Determine the Presence of a Network Adapter

Some computers have a built-in network adapter through which they can be connected to a wired network. To check for a network adapter, look for the network port on the back of the computer, as shown in Figure 1-51. The network ports have eight pins.

To see what kind of network may already be installed on a computer, use the following steps:

1. Click **Start**, then click **Control Panel** (Figure 1-52).
2. Click **Network and Internet Connections** (Figure 1-53).
3. Select a Control Panel icon and then click **Network Connections** (Figure 1-54).

The network adapter will be displayed. If a red cross appears over the icon, it means the network adapter is disconnected (Figure 1-55). If the network connection is blank, then there is no network adapter.

How to Install a USB Network Adapter

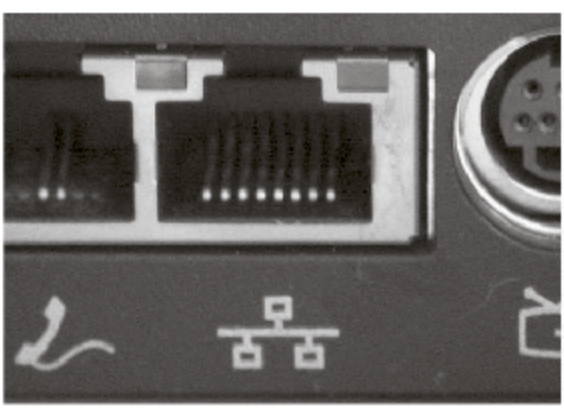
1. If the USB network adapter came with software, insert the CD or floppy disk and follow the manufacturer's instructions to install the software.
2. Find an available USB port on the computer. If there is no unused USB port, connect a USB hub to add additional ports. Then connect the USB network adapter to the unused USB port (Figure 1-56).
3. Connect the network cable to the network adapter (Figure 1-57).
4. Connect the other end of the network cable to the networking equipment (Figure 1-58).

Network Load Balancer

A network load balancer shares Web traffic between Web servers. The Zeus, Apache, and Microsoft Web server environments have basic clustering abilities built in, but software-based load balancing may not be as strong. Hardware load balancers are very expensive, though there are some affordable ones.

Repeaters

A repeater is used to connect two segments on a network cable, as shown in Figure 1-59. This is used to regenerate incoming signals and strengthen the signal without noise.



Source: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/G8571-ethernet-small.jpg. Accessed 2004.

Figure 1-51 Many computers have built-in network adapters.

In cable systems, repeaters look very simple and consist of an amplifier and a transformer. The purpose of an amplifier is to optimize the reflections of the signal during transmission. In wireless systems, the repeater contains a receiver, an amplifier, a transmitter, an isolator, and two antennas. In a fiber-optic network, a repeater consists of a photocell, an amplifier, and an LED or IRED for amplification. This fiber-optic repeater consumes

Figure 1-52 Click **Start** and then click **Control Panel**.

Figure 1-53 Click **Network and Internet Connections**.

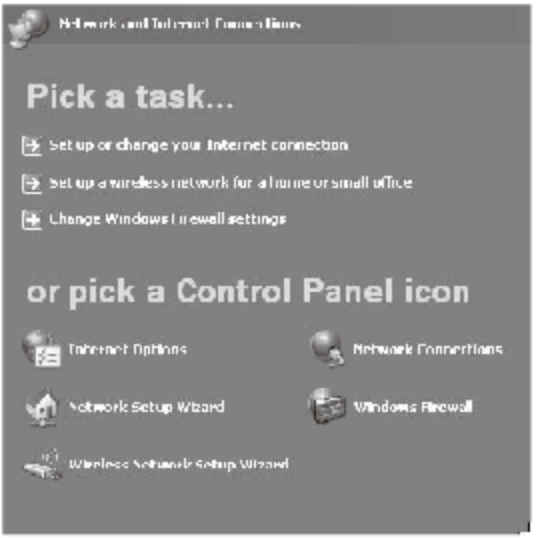


Figure 1-54 Click **Network Connections**.

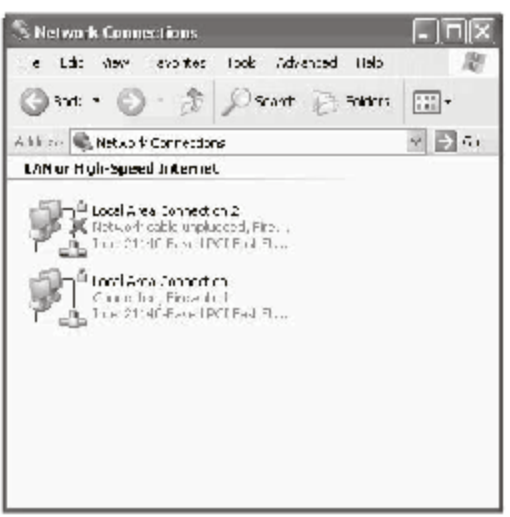
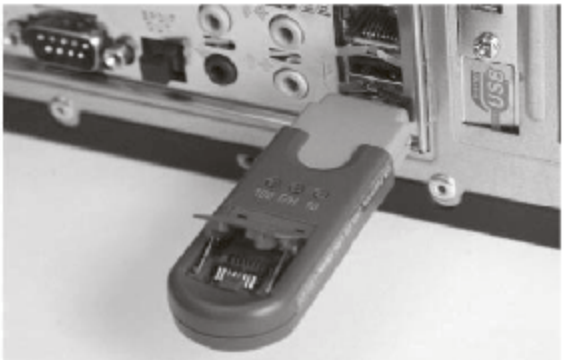
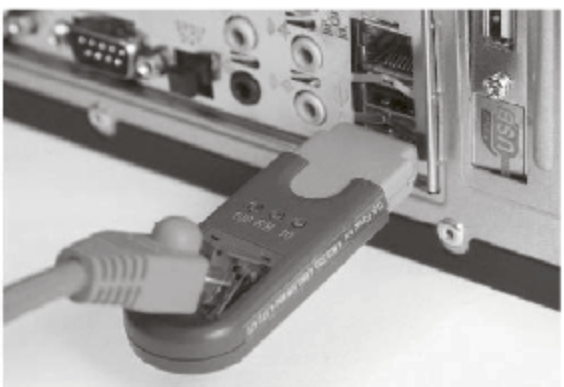


Figure 1-55 If a red cross appears over the icon, then the adapter is disconnected.



SOURCE: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/08571-wired-usb-no-cable-small.jpg. Accessed 2004.

Figure 1-56 USB network adapters can be used on most computers.

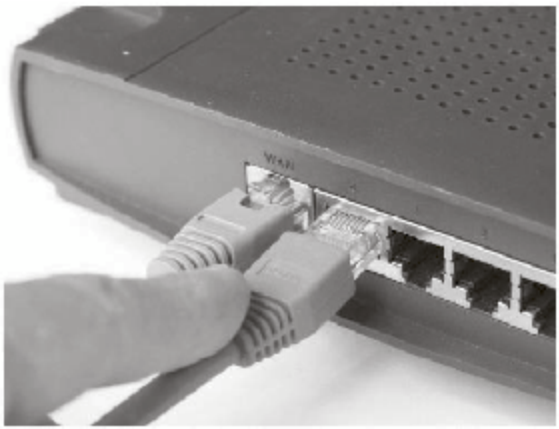


SOURCE: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/08571-wired-usb-with-cable-small.jpg. Accessed 2004.

Figure 1-57 Connect the network cable to the adapter.

less power than wireless repeaters. These repeaters are simple and inexpensive. A bus repeater is used to connect one computer bus to another system.

A repeater reproduces the actual bit sequence and places the renewed copy of the signal back on the connection medium. This allows a network to extend farther. A repeater does not alter the operation of the network. A repeater is sometimes compared to an amplifier, which is not accurate. An amplifier cannot differentiate between the original signal and noise. It amplifies all the signals that it produces. A repeater amplifies the original signal only.



Source: http://www.microsoft.com/library/media/1033/windowsxp/images/using/networking/setup/08573-connect-to-router-small.jpg. Accessed 2004.

Figure 1-58 Connect the other end of the cable.

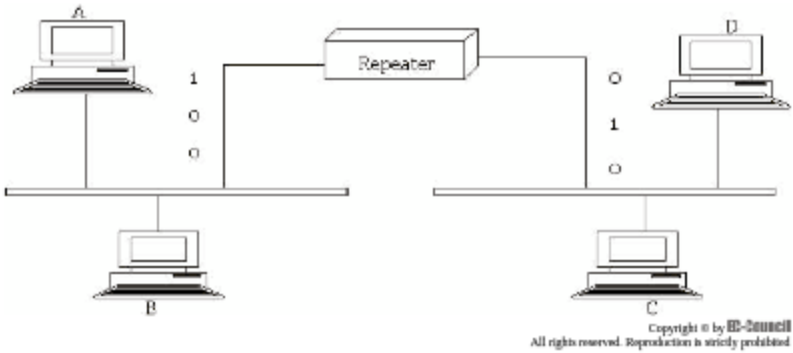


Figure 1-59 A repeater is used to connect two segments on a network line.

The positioning of a repeater is crucial. The repeater must be positioned in a place where signals reach it before any disturbance changes the original bit sequence. A minor disturbance can alter the accuracy of the voltage levels of the bits without corrupting its identity. If such compromised signals travel greater distances, the gathered disturbance can change the entire meaning of the bit sequence. If that happens, the original signal cannot be recovered, and the only way to correct the fault is to resend the signal.

Repeaters have the following advantages:

- Repeaters can increase the physical length of a network by increasing the signal power.
- Repeaters have the capability of transmitting signals through different appended segments.
- Some repeaters join multiple ports and can facilitate data transfer between the different segments of different media.

Repeaters have the following disadvantages:

- Repeaters augment the traffic on the network.
- There are restrictions on the number of repeaters that can be used in a single network.
- Repeaters broadcast errors on the network.
- Repeaters cannot be monitored or controlled through remote access.
- Repeaters cannot filter traffic.

Multiplexer

A multiplexer joins multiple inputs into a single output. In electronics, multiplexers integrate several signals into a single signal. Mutiplexers are useful for transmitting both digital and analog signals. In digital signal processing, a multiplexer uses several isolated data channels and combines them into a single channel. This data channel that is obtained is of higher intensity. The several data channels are transmitted from one place to another over one physical channel, which reduces costs.

At the destination end of the data channel, a counterpart called a demultiplexer, or demux, is generally required to break the high data-intensity stream into the actual lower-intensity streams. In some cases, the distant end system may have more responsibilities than a normal demultiplexer.

In general, it is common to combine a multiplexer and a demultiplexer together into one unit of equipment. Both pieces of equipment are required at both ends of a link, as most channel systems broadcast in both directions.

The following are the two types of multiplexing:

1. Frequency-division multiplexing
2. Time-division multiplexing

Gateway

A gateway is a device that is used to connect two different networks. A gateway allows users to protect, share, store, and access data over a network.

Gateway devices have two major functions:

1. *Connecting devices with each other*: In this function gateway devices help the users to connect different PCs and allow it to connect a printer and a scanner.
2. *Connecting devices to other networks*: Gateways connect devices and also connect devices to public and private networks.

Gateways are divided into three functional categories:

1. Data gateways
2. Multimedia gateways
3. Home-control gateways

Transceivers

A transceiver is a network device that is both a transmitter and a receiver. The transmitter transmits analog or digital signals, and the receiver receives analog or digital signals. Transceivers are available in three different configurations:

1. A chip-style device is the smallest type of transceiver that can be easily fixed and removed from a network system.
2. Board-style devices are directly fixed to a network board or card.
3. A module-style device is an external transceiver that is fixed outside the network and functions similarly to a standalone device.

Converters

Converters are used to connect several types of cables within an existing network. They get data from one type of cable and convert the signal for analog transmission on the other type of cable. Usually, network media converters are used to connect newer gigabit (1000 Mbps) Ethernet cabling to older 10Base-T or 100Base-T

networks. Some types of network media converters are separate devices that convert data between two different media. Others types are chassis-based models that are used to connect several media types in a single housing. These chassis-based devices are modular, stackable, and rack mounted. They contain an uplink or crossover switch to permit connections to either a workstation or a hub without the use of a cross-pinned cable.

Network media converters with an integrated circuit (IC) or printed circuit board (PCB) form factor are also available. The type of the network is important when choosing network media converters. Common types of networks contain asynchronous transfer mode, Ethernet, Token Ring, optical carrier, single-mode fiber, and multimode fiber. Choosing network media converters requires an analysis of port connectors. Attachment unit interface (AUI) connectors are used to connect Ethernet network stations and transceivers.

Terminals

Terminals are hardware devices used to enter data into a computer or to display data from the computer. Older terminals had a typewriter keyboard for input and a printing device for alphanumeric output. Newer variants contain a keyboard for input and a television-like screen for displaying the output.

Chapter Summary

- A network is a group of computers connected together so that information can be exchanged among the computers.
- A backbone combines many networks and subnets into a single channel.
- Large networks are divided into segments to improve the performance of the network.
- A subnet is a logical grouping of the devices in a network.
- The IP address space is divided into Classes A, B, C, D, and E.
- A gateway is a node that routes traffic from one workstation to an outside network on the Internet.
- There are three primary types of network cables: twisted-pair, coaxial, and fiber-optic.
- Operations security (OPSEC) identifies, controls, and protects generally classified or sensitive information.
- The OSI reference model is a standard networking model with seven layers.

Review Questions

1. What is a network backbone?

_____

_____

_____

_____

2. What is a subnet?

_____

_____

_____

_____

3. How are IP addresses assigned?

_____

_____

_____

_____

4. Name three domain naming conventions.

5. What are the types of threats to DNS?

6. What is a data gateway?

7. What are the types of twisted-pair cables?

8. What is a coaxial cable?

9. What are the types of wireless transmission?

10. What is Token Ring?

11. What is polling?

12. What are the layers in the OSI model?

13. Explain the flow of data in transmission modes.

14. Describe client-server networking.

15. Describe star topology.

Hands-On Projects

1. Perform the following steps:
   - Navigate to Chapter 1 of the Student Resource Center.
   - Open Asynchronous Transfer Mode Fundamentals.pdf and read the content.
2. Perform the following steps:
   - Navigate to Chapter 1 of the Student Resource Center.
   - Open What Is A LAN.pdf and read the content.
3. Perform the following steps:
   - Navigate to Chapter 1 of the Student Resource Center.
   - Open Lan Guide.pdf and read the content.

Chapter 2

Network Protocols

Objectives

After completing this chapter, you should be able to:

- Understand Internet Protocol (IP)
- Implement network protocols
- Implement application-layer protocols
- Implement presentation-layer protocols
- Implement session-layer protocols
- Implement transport-layer protocols
- Implement network-layer protocols
- Implement data-link-layer protocols

Key Terms

Binding the process of linking a home address with a care-of address using Mobile IP

Datagram a block of data transmitted unreliably

Packet a block of data

Zone a place where users can enter an organization through a security check

Introduction to Network Protocols

A protocol is a set of rules that enables communication between computers over a network. It defines what types of communications are available, how to communicate, and when to communicate.

The following are the three key elements of a protocol:

- *Syntax*: defines a structure or data format
- *Semantics*: the meaning of the data
- *Timing*: when the data is sent and at what speed

Protocols have the following functions:

- Segmentation/reassembly
- Encapsulation
- Connection control (data transfer can be either connectionless or connection oriented)
- Ordered delivery
- Flow control
- Error control
- Addressing
- Multiplexing

This chapter will discuss the implementation of several different network protocols.

Internet Protocol

Internet Protocol (IP) is an OSI network-layer protocol present in the TCP/IP communications protocol suite. Internet Protocol is used to transfer data over a packet-switched network.

Data is transmitted as blocks, called ***packets*** or ***datagrams***, at the network layer. The term *datagram* specifically refers to data submitted through unreliable means. IP does not guarantee the transfer of data packets. The packet can reach the destination with damage, may not reach the destination in order, and could even be replaced or dropped entirely.

In IP networking there is no need to establish a connection prior to sending data. IP offers universally defined addresses. The currently accepted network-layer protocol is IPv4, but that will be replaced by the improved IPv6 in the future. IPv6 allows 128-bit source and destination addresses, offering more addresses than IPv4 which only allows 32-bit addresses.

Internet Protocol: Attacks and Countermeasures

Some vulnerabilities in IP communications include the following:

- *Source routing*: The host can track the source route of a TCP open request, leaving the IP exposed to attacks. An attacker uses a machine that poses as the host machine and exploits any weak source routing for the source IP address. This enables the attacker to gain all privileges of the original host machine.
- *Routing information protocol attacks*: Routing information protocol (RIP) broadcasts routing information, which is not checked. This enables attackers to send false routing information to the targeted host and act as a specific trusted host.
- *Exterior gateway protocol attacks*: Exterior gateway protocols are used for data and request transfers between exterior gateways. In this attack, attackers act as a second exterior gateway for the same autonomous system, disabling the real gateway.

In order to avoid compromise from these vulnerabilities, an administrator should consider the following countermeasures:

- A paranoid gateway can be used to block any form of host spoofing.
- RIP packets should be authenticated in the absence of economical public-key signature schemes.

Implementing Network Protocols

Designing a Network Protocol

Someone designing a network protocol should consider the following issues:

- *Effectiveness*: It should be effective so that engineers, designers, and software developers can use it.
- *Reliability*: It should have some level of error detection and correction. If data are lost, the protocol should ensure that the data are retransmitted.
- *Resiliency*: It should guard against topological errors.

TCP/IP

The TCP/IP protocol suite is a combination of Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP is used to handle the flow of packets over the network, and IP is used to handle the routing of packets.

Configuring TCP/IP

To configure TCP/IP, the user must first assign an IP address to the machine. Follow these steps to configure TCP/IP through a LAN connection in Windows:

1. Right-click on the local area connection to be configured, and click **Properties**.
2. Click **Internet Protocol (TCP/IP)**, and then click the **Properties** button, as shown in Figure 2-1.
3. On the **General** tab, select the buttons, as shown in Figure 2-2, and then click the **Advanced** button.
4. Click the **IP Settings** tab, and check the **Automatic metric** check box, as shown in Figure 2-3.
5. Click the **DNS** tab, and select the settings shown in Figure 2-4.
6. Click the **WINS** tab and check the **Enable LMHOSTS lookup** check box, as shown in Figure 2-5. Leave the default NetBIOS setting.
7. On the **Options** tab, select **TCP/IP filtering** and click the **Properties** button, as shown in Figure 2-6.
8. In the **TCP/IP Filtering** window, check the **Enable TCP/IP Filtering (All adapters)** check box, as shown in Figure 2-7. This option will permit all traffic on TCP and UDP ports using Internet protocols. Click the **OK** button.

Figure 2-1 Click **Internet Protocol (TCP/IP)**, and then click the **Properties** button.

Source: http://technet.microsoft.com/en-us/library/bb726991.aspx#top. Accessed 2004.

Figure 2-2 Select these buttons on the **General** tab.

Figure 2-3 Click the **IP Settings** tab, and check the **Automatic metric** check box.

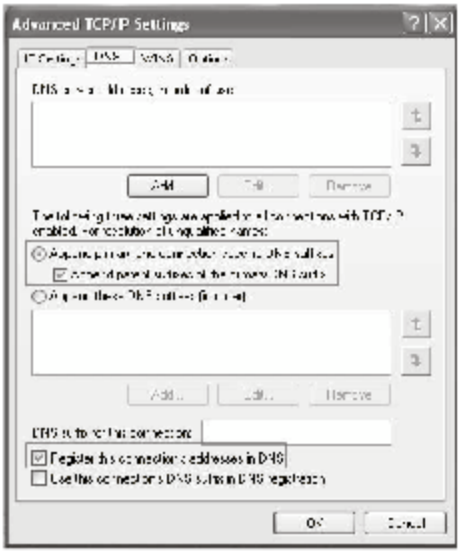


Figure 2-4 Select these settings on the **DNS** tab.

Network Classes

Network classes are used to identify the devices connected to the Internet or the network. A device's IP address is a 32-bit binary address that uniquely defines its connection to the network. These 32 bits are composed of four sets of numbers between 0 and 255, delimited by periods. Host number 0 is reserved for the network part of the address, and host number 255 is for use as a broadcast address.

There are five different IP address classes:

1. Class A
2. Class B
3. Class C
4. Class D
5. Class E

Figure 2-8 shows a breakdown of the bits in each class, while Figure 2-9 shows the range of addresses for each class.

Class A

Class A consists of IP addresses from 0.0.0.0 to 127.255.255.255. Of the 32 bits, the first 8 bits (called an octet) are allocated to the network ID (netid). The first higher-order bit of the netid octet is 0; this is the class identifier. The remaining 24 bits are allocated to the host ID (hostid). In general, if the first bit of an IP address is 0, then it falls under Class A. Class A addresses are designed for large organizations with large numbers of hosts or routers. Class A can support 16,777,214 hosts, using 127 network IDs.

Figure 2-5 Click the **WINS** tab and check the **Enable LMHOSTS lookup** check box.

Figure 2-6 On the **Options** tab, select **TCP/IP filtering** and click the **Properties** button.

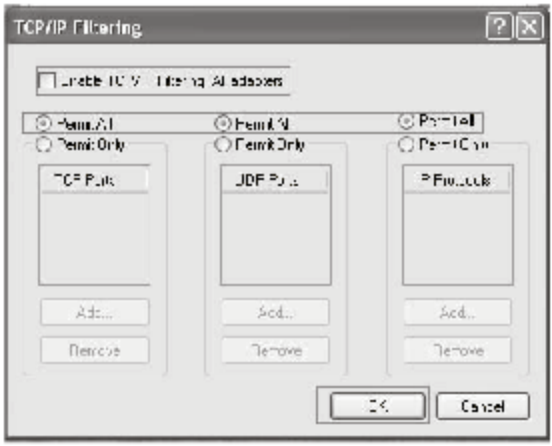


Figure 2-7 In the **TCP/IP Filtering** window, check the **Enable TCP/IP Filtering (All adapters)** check box.

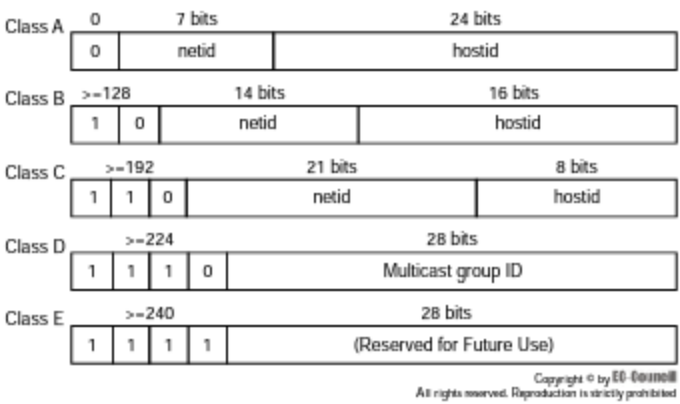


Figure 2-8 This shows how each bit in each IP address class is used.

Class B

An IP address in the range of 128.0.0.0 to 191.255.255.255 is a Class B address. The first two higher-order bits of a Class B IP address are 1 and 0. Here, the first 16 bits are allocated to the netid and the remaining 16 bits are allocated to the hostid. The first two bits are class identifiers. Therefore, a Class B address has thousands of network numbers and host numbers. Class B addresses are designed for organizations that cover tens of thousands of hosts or routers. Class B supports 65,534 addresses.

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 255.255.255.255

Figure 2-9 Each class has a specific range of IP addresses assigned to it.

Class C

An IP address between 192.0.0.0 and 223.255.255.255 is a Class C address. The first three bits of the Class C IP address are 1, 1, and 0. In Class C, the first 24 bits are allocated to the netid and the remaining eight bits are allocated to the hostid. Among the 24 netid bits, the first three bits are class identifiers. There are over 16 million network IDs and around 254 hosts. Class C is designed for small organizations with smaller numbers of hosts or routers.

Class D

If the IP address falls in the range of 224.0.0.0 to 239.255.255.255, it is a Class D address. The first four bits of this IP address will be 1, 1, 1, and 0. This class is designed for multicast group IDs.

Class E

If the first four bits of an IP address are 1, 1, 1, and 1, then it is a Class E address. This class is reserved for future use. Class E ranges from 240.0.0.0 to 255.255.255.255.

Telnet

Telnet is a network protocol used for Internet or local area network (LAN) connections, and is generally used to provide user-based command-line login sessions. It is a terminal emulation program for TCP/IP services and enables connecting a PC to a server on a network. The word *telnet* can also refer to a telnet program that enables users to enter network commands and execute them.

Telnet is a client-server protocol based on TCP. Clients usually connect to port 23 on the host. It can also be used to set up an interactive TCP connection to various other services on an Internet host due to its design and flexibility.

The telnet protocol consists of a central part and a set of extensions. The foundation protocol is described by IETF documents RFC 854 and RFC 855, which also includes STD 8 which outlines reasonably essential operating traits of the protocol and a way of outlining and creating extensions.

Telnet Vulnerabilities

Telnet vulnerabilities can be exploited by attackers to skip the normal system libraries and acquire direct root access to the server by setting the environment variable LD_LIBRARY_PATH. For instance, attackers can exploit UNIX accounts that have guessable passwords for server interruptions and application controls.

Installing the NWLink Protocol

1. Open Control Panel. Double-click on **Network Connections**.
2. Right-click on the connection where the NWLink protocol will be installed, and click **Properties**.
3. Click the **Install** button, as shown in Figure 2-10.

Figure 2-10 Click the **Install** button in the **Local Area Connection Properties** window.

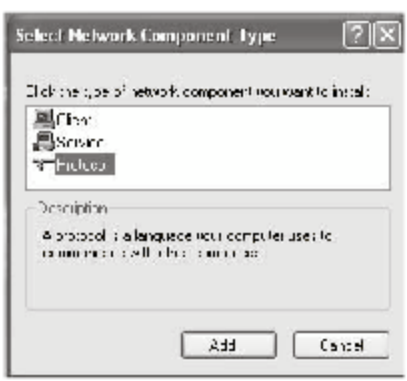


Figure 2-11 Select **Protocol** and click the **Add** button.

4. Select **Protocol** and click the **Add** button, as shown in Figure 2-11.
5. Select **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** and click the **OK** button, as shown in Figure 2-12.
6. NWLink will now appear in the connection properties, as shown in Figure 2-13.

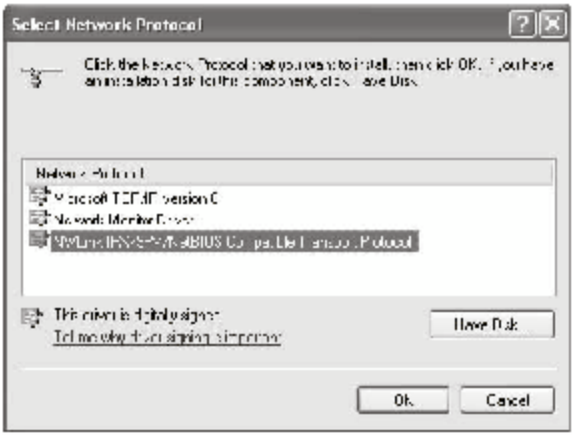
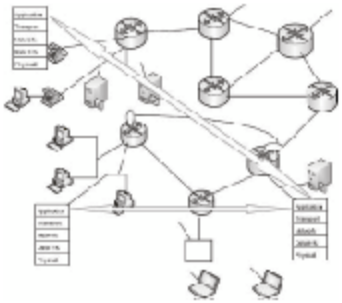


Figure 2-12 Select **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** and click the **OK** button.

Figure 2-13 NWLink is now configured.



Source: http://icawww1.epfl.ch/sc250_2004/lecture_notes/sc250_04_3.pdf. Accessed 2004.

Figure 2-14 The application layer enables communication between processes running on different hosts.

Implementing Application-Layer Protocols

The application layer provides user services to lower-layer protocols. It enables communication between processes running on different hosts. Figure 2-14 shows communication over an application layer through different processes.

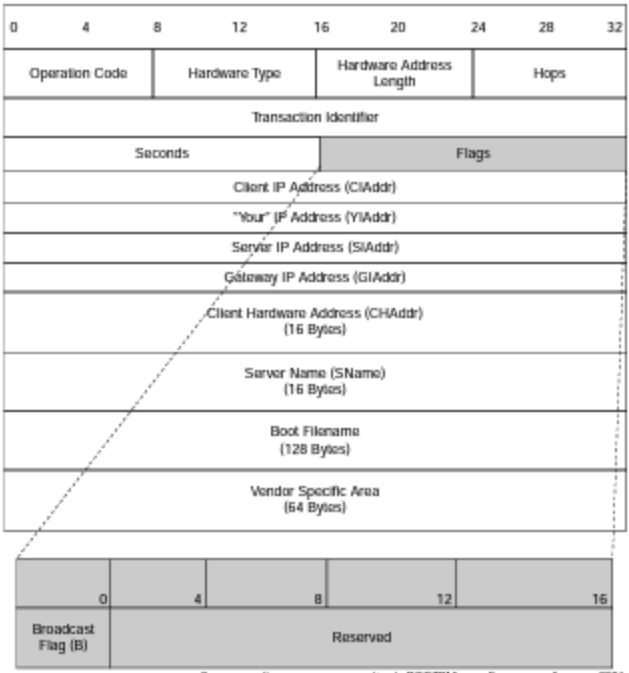
Bootstrap Protocol (BOOTP)

The BOOTP protocol allows a network user to configure a boot process automatically, without user involvement. BOOTP is a connectionless host configuration protocol developed prior to DHCP (Dynamic Host Configuration Protocol). Workstations use it to acquire IP addresses at boot time.

- A diskless workstation can acquire an IP address through BOOTP.
- BOOTP uses MAC addresses for identifying its workstations, which will be assigned an IP address.
- BOOTP uses UDP ports for network connections. It uses UDP port 67 for the BOOTP server and UDP port 68 for BOOTP clients. The BOOTP client broadcasts its physical network address through BOOTPREQUEST using address 255.255.255.255, which is a limited broadcast address.
- The server replies to the request using the BOOTPREPLY packet.
- The BOOTP protocol is defined by RFC 951.
- BOOTP provides a dynamic method to associate workstations with servers.

The BOOTP protocol format is shown in Figure 2-15. Each field is discussed in detail below.

- *Operation code*: This is an 8-bit field that specifies the type of message sent. Operation code 1 indicates a BOOTPREQUEST message, and operation 2 indicates a BOOTPREPLY message.
- *Hardware type*: This is an 8-bit field that indicates the type of hardware used in the network. Some of the hardware types and their HRD values are shown in Figure 2-16.
- *Hardware address length*: This is an 8-bit field that indicates the length of the message's hardware address.
- *Hops*: This is an 8-bit field and is set to 0 by the client before transmitting a request to a server. It also controls the flow of BOOTP messages.
- *Transaction identifier*: This is a 32-bit field used as an identifier by the client. This identifier matches the BOOTP server's requests with its replies.
- *Seconds*: This 16-bit field is the elapsed time since the client started trying to boot, in seconds. This information helps the BOOTP servers decide which requests to respond to first.



Source: http://www.tcpipguide.com/free/t_BOOTPMessageFormat.htm. Accessed 2004.

Figure 2-15 This is the BOOTP protocol format.

HRD Value	Hardware Type
1	Ethernet (10 Mb)
6	IEEE 802 Networks
7	ARCNET
15	Frame Relay
16	Asynchronous Transfer Mode (ATM)
17	High-Level Data-Link Control (HDLC)
18	Fiber Channel
19	Asynchronous Transfer Mode (ATM)
20	Serial Line

Source: http://www.tcpipguide.com/free/t_BOOTPMessageFormat.htm. Accessed 2004.

Figure 2-16 These are some of the BOOTP hardware-type options.

- *Flags*: This contains a 1-bit field indicating that the BOOTP server should send its reply by broadcast. The other 15 bits are reserved for future use.
- *Client IP address*: This 32-bit field keeps track of client IP addresses.
- *"Your" IP address*: This is a 32-bit field for the client's IP address and is assigned by the server if the client does not know its address.
- *Server IP address*: This is a 32-bit field that contains the IP address of the BOOTP server obtained from the BOOTP reply message.
- *Gateway IP address*: This is a 32-bit field, used to route BOOTP messages, that facilitates the communication between a client and a server on a different network or subnet. The client will set this field to 0, but when processing the BOOTREPLY, it should be ignored.
- *Client hardware address*: This 16-byte field contains the hardware address of the client.
- *Server name*: This is a 64-byte field that contains the name of the server when using a BOOTPREPLY.
- *Boot filename*: This is a 128-byte field that contains all the details of the path and filename of a boot file that the client downloads to complete the bootstrapping process. This field maintains a directory that contains the details of every boot filename.
- *Vendor-specific area*: This 64-byte field allows vendors to customize different hardware over a BOOTP.

Dynamic Host Configuration Protocol (DHCP)

This communication protocol is an extension of BOOTP. It allows network administrators to manage and automate the assigning of IP addresses in an organizational network. If there is no DHCP server, then an IP address must be entered manually at each computer and a new IP address must be entered when the computer enters a new network.

DHCP was designed to overcome the inflexibility of BOOTP by supporting three different methods to allocate IP addresses:

- Automatic allocation provides a permanent address to a client.
- Dynamic allocation provides a time-limited allocation.
- Static allocation works well for DHCP servers, because it allows both clients and DHCP relay agents to function directly with the server.

Figure 2-17 shows a DHCP transaction. The fields shown in the diagram are explained below.

- First, the client sends a DHCPDISCOVER message. The server sends the DHCPOFFER message in response to the client's DHCPDISCOVER message. It contains an IP address configuration. DHCPREQUEST is used by the client to ask for a specific IP configuration from the server.
- DHCPACK is an acknowledgment sent to the client by a server that its specific IP address is allocated.
- DHCPNack is a negative acknowledgement from the server that the client cannot use a specific IP address because that address has already been taken, or when the client moves to a different subnet and tries to restore the connection on the previous IP.
- Through DHCPDecline the client can tell the server that the assigned IP address is not valid.
- DHCPInform is sent from client to server to request additional configuration settings.
- DHCPDISCOVER is used to discover the presence of DHCP servers on the network.

Figure 2-18 shows the DHCP protocol format. Notice the similarities to BOOTP. Each field is the same as BOOTP, except for the Options field. This field holds any parameters required for DHCP operation. The size of this field is variable and is used by both client and server as needed. Figure 2-19 explains the differences between BOOTP and DHCP.

Data Link Switching Client Access Protocol (DCAP)

Data Link Switching Client Access Protocol (DCAP) is an application-layer protocol that acts as an interface between workstations and routers to handle NetBIOS/SNA traffic through the TCP session.

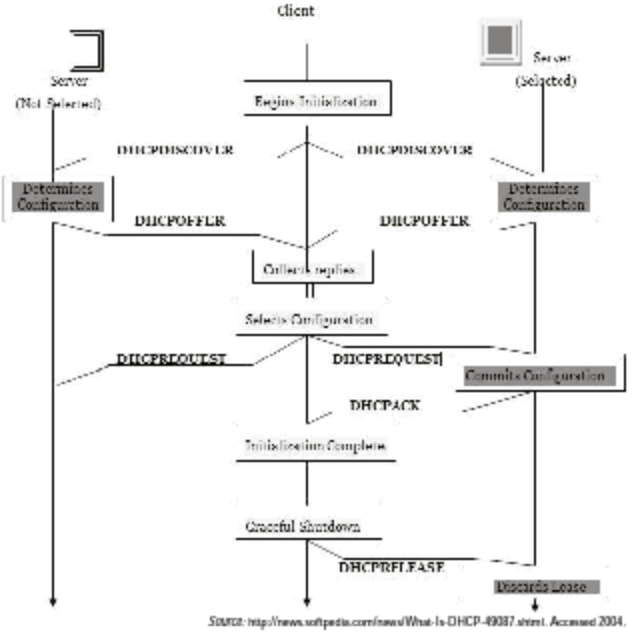


Figure 2-17 This diagram shows a DHCP transaction.

This protocol reduces scalability issues. It considers all clients as workstations to the router rather than peers, creating a client-server model. This can make it a very efficient protocol between workstations (clients) and routers (servers).

The DCAP packet-header format is shown in Figure 2-20.

DCAP contains the following three frames:

- *DCAP header*: This is a 4-byte field common to all frames that pass between client and server. It is used to identify the message type and length of the frame.
- *DCAP data*: This is an optional field that is used to process the data. The structure and size depends on the message carried in the DCAP frame.
- *User data*: These data will be sent by the local system to a remote system. During the transfer of data to the remote system, the data size is variable.

The DCAP header format contains the following:

- *Protocol ID*: This field uses the first four bits and is set to 1, 0, 0, 0.
- *Version number*: This field uses the next four bits of the DCAP header and has a value of 0, 0, 0, 1.
- *Message type*: This is an 8-bit field that shows the type of message.
- *Packet length*: This is a 16-bit field. The total packet length consists of DCAP header, DCAP data, and user data. The minimum size of the packet is four, which is the length of just the header.

The DCAP Messages field contains different messages related to frames. Figure 2-21 lists the messages available.

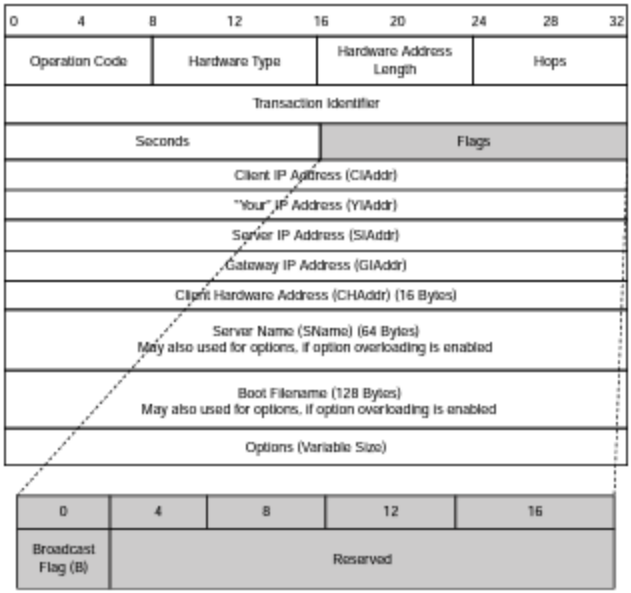
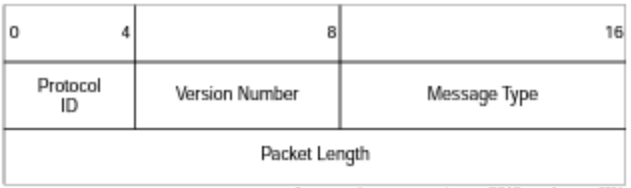


Figure 2-18 The DHCP protocol format is very similar to BOOTP.

BOOTP	DHCP
BOOTP is a BOOT Strap Protocol	DHCP is Dynamic Host Configuration Protocol
Mainly used to configure diskless workstations with limited BOOT Strap features	Mainly used to configure network computers that have local hard drives and contain full BOOTP features
BOOTP has a default expiration of 30 days for IP address leases	DHCP has a default expiration of 8 days for IP address leases
Supports a limited number of client configuration parameters	Supports large numbers of client configuration parameters
Describes a two-phase bootstrap configuration process, as: • Clients contact the BOOTP server to determine the address and to select the boot file name • Client uses Trivial FTP servers to perform file transfer of their boot image	Describes a single-phase boot configuration process, in this process, a DHCP client negotiates with a DHCP server to determine its IP address and obtain any other initial configuration details it needs for network operation
BOOTP clients do not renew or rebind configuration with the BOOTP server except when the system restarts	DHCP clients automatically enter a rebind state at set time intervals to renew their leased address allocation with the DHCP server

Source: http://technet.microsoft.com/en-us/library/cc781243%28WS.10%29.aspx. Accessed 2004.

Figure 2-19 These are the differences between BOOTP and DHCP.



Source: http://www.javvin.com/protocolDCAP.html. Accessed 2004.

Figure 2-20 This is the DCAP packet format.

Domain Name Service (DNS) Protocol

The Domain Name System (DNS) is a critical operational part of the Internet infrastructure, but it was created without strong security to provide data integrity or authentication. Extensions to DNS provide these security services through the use of cryptographic digital signatures stored in secured zones as resource records.

The DNS protocol acts as a directory for various Internet domains. It is a distributed database service used to translate between domain names and IP addresses. DNS provides three different services:

1. *Key distribution*: As DNS uses resource records, these records are defined to associate or document keys with various DNS names. Key distribution allows DNS to act as a public key, supporting DNS data authentication and security services.
2. *Data-origin authentication and integrity*: Associating resource records in DNS provides authentication. This authentication belongs to a zone that stores copies of data. Here, ***zone*** refers to a place where users can enter an organization through a security check.
3. *DNS transaction and request authentication*: The use of digital signatures protects resource records that are retrieved. The request is authenticated by including an SIG RR (digital-signature resource record) at the end of the request. The data-origin authentication service provided by the SIG RR protects retrieved resource records but provides no protection for DNS requests.
4. The syntax of an SIG resource record includes the type of the RR(s) being signed, the name of the signer, the time at which the signature was created, the time it expires (when it is no longer to be believed), its original time to live, the cryptographic algorithm in use, and the actual signature.

   As is normal in private-key infrastructure (PKI), private keys belong to the host composing the request or reply message, not to the zone involved. The corresponding public key is normally stored in and retrieved from the DNS.

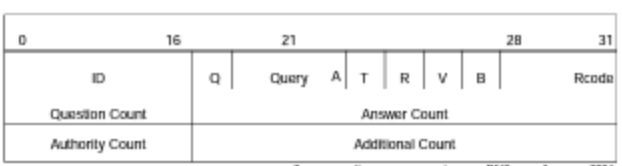
The DNS protocol structure is shown in Figure 2-22, and each field is detailed below.

- *ID*: This is a 16-bit field used to correlate queries and requests.
- *Q*: This is a 1-bit field that identifies the message as a query or response.
- *Query*: This is a 4-bit field that describes the message type:
  - 0: Standard query (name to address)
  - 1: Inverse query (address to name)
  - 2: Server status request
- *A*: This 1-bit field which, when set to 1, identifies the response as one made by an authoritative name server.
- *T*: This is also a 1-bit field. When set to 1, it says that the message has been truncated.
- *R*: This is a 1-bit field. When set to 1 by the resolver, it requests recursive service by the name server.
- *V*: This is a 1-bit field that signals the availability of the recursive service by the name server.
- *B*: This 1-bit field, reserved for future use, should be set to 0.
- *D*: This is a 1-bit field that indicates that all data in the answer and authority sections have been authenticated.
- *C*: This is a 1-bit field that indicates that checking is disabled.

DCAP Frame Name	Code	Function
CAN_U_REACH	0x01	Determine if the given station is reachable
I_CAN_REACH	0x02	Positive response to CAN_U_REACH
I_CANNOT_REACH	0x03	Negative response to CAN_U_REACH
START_DL	0x04	Setup session for given addresses
DL_STARTED	0x05	Session Started
START_DL_FAILED	0x06	Session Start failed
XID_FRAME	0x07	XID Frame
CONTACT_STN	0x08	Contact destination to establish SABME
STN_CONTACTED	0x09	Station contacted - SABME mode set
DATA_FRAME	0x0A	Connectionless Data Frame for a link
INFO_FRAME	0x0B	Connection oriented I Frame
HALT_DL	0x0C	Halt Data Link session
HALT_DL_NOACK	0x0D	Halt Data Link session without Ack
DL_HALTED	0x0E	Session Halted
FCM_FRAME	0x0F	Data Link Session Flow Control Message
DGRM_FRAME	0x11	Connectionless Datagram Frame for a Circuit
CAP_XCHANGE	0x12	Capabilities Exchange Message
CLOSE_PEER_REQUEST	0x13	Disconnect Peer Connection Request
CLOSE_PEER_RESPONSE	0x14	Disconnect Peer Connection Response
PEER_TEST_REQ	0x1D	Peer keepalive test request
PEER_TEST_RSP	0x1E	Peer keepalive response

Source: http://www.faqs.org/rfcs/rfc2114.html. Accessed 2004.

Figure 2-21 These are the different DCAP message frames.



Source: http://www.javvin.com/protocolDNS.html. Accessed 2004.

Figure 2-22 This is the DNS protocol structure.

- *Rcode*: This is a 4-bit field that is used as a response code. This field is set by the name server to identify the status of the query.
- *Question Count*: This is a 16-bit field used to define the number of entries in the question section.
- *Answer Count*: This 16-bit field is used to define the number of resource records in the answer section.
- *Authority Count*: This is a 16-bit field that defines the number of name-server resource records in the authority section.

- *Additional Count*: This is also a 16-bit field that defines the number of resource records in the additional records section.

File Transfer Protocol (FTP)

The most significant, universal file transfer protocol in TCP/IP is File Transfer Protocol (FTP). FTP runs over TCP to make sure that files are sent dependably with no data failure. The protocol utilizes a set of FTP commands delivered from an FTP client to an FTP server to carry out file transfer operations. The FTP server transmits FTP replies to the client that specify the success or failure of commands.

FTP is the set of rules and standards for exchanging files over the Internet. FTP functions much like HTTP does when sending Web pages from a server to a user's Web browser, or like SMTP when sending e-mail across the Internet. FTP can be used both to download a file from a server and to upload a file to a server.

While data is being sent across the data flow, flow control remains inactive. This can cause problems with huge data transfers through a firewall, which will lose sessions after long gaps without activity. Although the file is successfully sent, the control session can be removed by the firewall, leading to an error. FTP needs the user to sign in before data transfer can take place.

The following are some of the disadvantages of FTP:

- Passwords and data files are sent in plaintext.
- Numerous TCP/IP connections are used: one for the control connection and others for each download, upload, or directory enumeration. Firewall software requires special logic to report for these connections.
- It is difficult to filter active-mode FTP traffic on the client side by utilizing a firewall because the client creates a random port for receiving the connection. This hassle is usually solved by using passive-mode FTP.
- It is possible to misuse the protocol's incorporated proxy characters to tell a server to transmit data to a random port of a third computer.
- FTP is a slow protocol due to the number of commands needed to start a transfer.

In addition to these disadvantages, FTP has the following vulnerabilities:

- *Directory traversal*: Directory-traversal attacks permit remote attackers to find the FTP root and read arbitrary files by appending some strings to a CWD command.
- *Buffer overflow*: A buffer-overflow attack on an FTP server allows remote attackers to gain root privileges.
- *SITE EXEC command attack*: Remote attackers can execute arbitrary commands via the **SITE EXEC** command.
- *Vulnerable FTP server*: The FTP server might allow local and remote attackers to cause damage in the root directory if that directory has world-readable permissions.

Trivial File Transfer Protocol (TFTP)

FTP requires TCP for connections and data transmission. The dependence on TCP implies that any device desiring to use FTP requires not just the FTP program, but a complete TCP implementation as well. Trivial File Transfer Protocol (TFTP) is a very basic file transfer protocol with the operations of a very fundamental form of FTP.

TFTP uses UDP port 69 for transfer and lacks security features. Servers use TFTP to boot diskless workstations, terminals, and routers. It cannot enumerate directory contents and has no verification or encoding mechanisms.

Network Time Protocol (NTP)

NTP is used to synchronize system clocks over IP with Coordinated Universal Time (UTC) taken from time servers. Its main characteristics include the following:

- Fully automatic synchronization
- Can synchronize a single computer or a whole computer network
- Available in almost all computers that use time synchronization

- Highly fault tolerant
- Uses UTC time, independent of time zones and daylight saving time
- Accurate within 1 millisecond

Figure 2-23 explains how NTP synchronizes a system's clock.

In this diagram, BX, being a single computer, is synchronized with the A3 stratum server. The BY computer is configured with two synchronization servers: A2 and A3. Then, in LANZ, an organization is synchronized with a network of computers. Two LAN computers are set up as NTP local servers that are synchronized to three NTP servers (A1, A2, and A3); then the remaining computers (C1, C2, and C3) are connected to the local servers (B1 and B2) to synchronize. This connection reduces the network traffic between networks and keeps the configuration of the local network dependent only on the local servers (B1 and B2), that can be easily reconfigured against the external servers when necessary.

NTP is designed to produce clock offset, round-trip delay, and dispersion values.

- Clock offset represents the adjustments to the local clock necessary to synchronize it with the corresponding reference clock.
- Round-trip delay shows how long it takes for a packet to go back and forth between the server and the client.
- Dispersion represents the maximum errors of the local clock related to the reference clock.

Figure 2-24 shows the NTP protocol structure, and each field is discussed below.

- *LI*: This 2-bit field is a leap indicator, warning of an impending leap second to be inserted at the end of the last day of the current month.
- *VN*: This is a 3-bit field that is used to indicate the version number.
- *Mode*: This is a 3-bit field indicating the mode as follows:
  - 0: Reserved for future use
  - 1: Symmetric active mode
  - 3: Client mode
  - 4: Server mode
  - 5: Broadcast mode
  - 6: NTP control message mode
- *Stratum*: This 8-bit field identifies the stratum level of the local clock.
- *Poll*: This 8-bit field is a signed integer that indicates the maximum interval between successive messages, in seconds near to powers of two.
- *Precision*: This 8-bit field has a signed integer that indicates the precision of the local clock, in seconds near to powers of two.

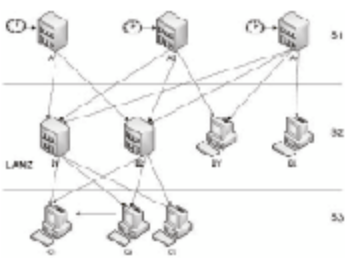
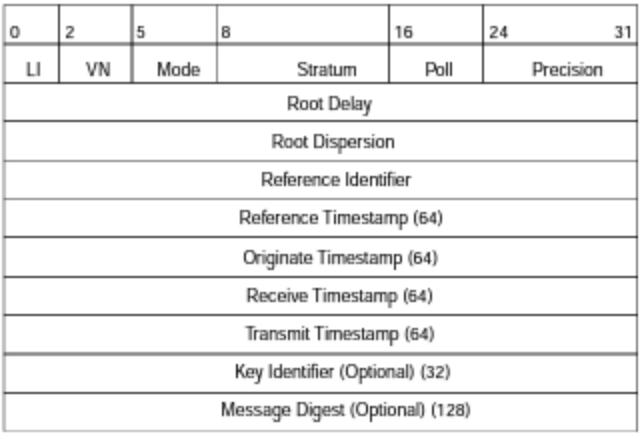


Figure 2-23 This shows how synchronization is carried out in NTP.



Source: http://www.javvin.com/protocolSNTP.html. Accessed 2004.

Figure 2-24 This is the structure of an NTP packet.

- *Root Delay*: This 32-bit field has a signed fixed-point number that indicates the total round-trip delay to the primary reference number, in seconds with a decimal point between bits 0 and 31.
- *Root Dispersion*: This 32-bit field has an unsigned fixed-point number that indicates the nominal error relative to the primary reference source, in seconds with a decimal point between bits 0 and 31.
- *Reference Identifier*: This 32-bit field is used to identify a particular reference number.
- *Reference Time Stamp*: This 64-bit field represents the time at which the client request is referred to the server, in a timestamp format.
- *Originate Time Stamp*: This is a 64-bit field representing the time at which the client sent the request.
- *Receive Time Stamp*: This is a 64-bit field representing the time at which the server received the request.
- *Transmit Time Stamp*: This 64-bit field contains the time at which the server sends the message to the client.
- *Key Identifier*: This is a 32-bit optional field used to identify the key.
- *Message Digest*: This is a 128-bit optional field.
- *Authenticator*: This is an optional field. When the NTP authentication scheme is implemented, both the key-identifier and message-digest fields contain Message Authentication Code (MAC) information.

Network News Transfer Protocol

The NNTP protocol uses TCP port 119 to provide communication between news clients and news servers. This protocol is also called the Usenet protocol, because it is mainly used for reading and posting Usenet articles. Figure 2-25 is a representation of how NNTP works.

Some of the key commands of NNTP include the following:

- *Article <message-ID>*: This command displays the header, a blank line, and the body (text) of the specified article. *Message-ID*, an optional field, is the message ID of an article as shown in that article's header. If it is left blank, the current article will be displayed.
- *Head*: This command is similar to the Article command except that it returns only the header lines of the article.

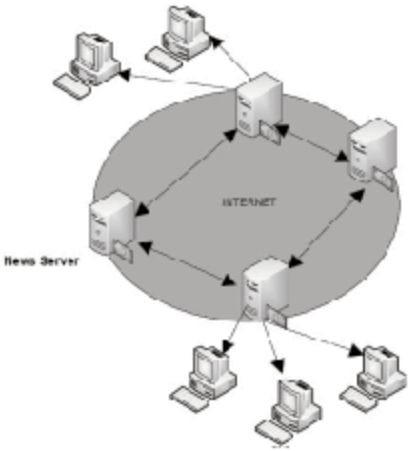


Figure 2-25 This diagram shows how NNTP works.

- *Status*: This command is similar to the Article command except that no text is returned.
- *Group <ggg>*: This command is used to select the newsgroup whose name is given by the parameter *ggg*. A successful selection response will return the article numbers of the first and last articles in the group, and an estimate of the number of articles in a group.
- *Body*: This command is similar to the Article command except that it returns only the text body of the article.
- *List*: This command returns a list of valid newsgroups and associated information.
- *NewGroups*: This command creates a list of newsgroups that have been created since a given date and time; the list is in the same format as that provided by the List command.
- *NewNews*: This command gives a list of message IDs posted to the specified newsgroups since a specified date.
- *Next*: This internally maintained current-article pointer is advanced to the next article in the current newsgroup.
- *Post*: This command is used when a response code 340 is returned, to indicate that the article is to be posted and sent.
- *Quit*: This command is used to close the client connection when the server sends an acknowledgment.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is used to communicate between network organization stations and managed devices over IP. It consists of a number of protocol operations that describe the discrete message exchanges that take place between devices, and a set of communication mappings that define the way messages are transferred across the network.

SNMP has three basic components:

- *Master agents*: A master agent is software on an SNMP-capable network element that responds to SNMP requests made by a management station. It acts as a server in a client-server environment or as a daemon in operating-system semantics. A master agent depends on subagents for data. Master agents can also be considered managed objects.

- *Subagents*: A subagent executes the data and administration operations defined by a definite MIB (management information base) of a particular subsystem (e.g., the Ethernet link layer). Some functions of the subagent are: assembling data from managed objects, designing fields of the managed objects, responding to managers' requests, and creating alarms.
- *Management stations*: The manager or management station is the last component in the SNMP architecture.

The following are some of the major SNMP security issues:

- MIB objects contain critical information about network devices. The construction of these objects is not robust.
- Community strings are embedded in messages in clear text that can be detected easily, providing weak authentication to the SNMP protocol. Community strings are like passwords for the members of the community.

SNMP Security Models

Party-Based Security Model A logical body, containing all mechanisms that SNMP performs, is called a party. It states concepts such as the following:

- Specification of authentication protocol
- Privacy or encryption protocol
- Transmission mechanism
- Keys

The information related to the party is generally used to verify that a specific request is authentic and to assure the agreement of encryption and decryption of data between sender and receiver.

User-Based Security Model (USM) To overcome the limitations in the party-based model, the user-based security model was introduced. The idea behind this model is to provide more emphasis to a user's access rights on a machine. To protect user access and message privacy, several authentication and encryption protocols can be used.

View-Based Access Control Model (VACM) This model provides a new method of control for accessing the objects of a device and, thus, provides security while accessing those objects. This allows the administrator to know about the users accessing the data. The set of MIB objects provided by a specific group in reference to a specific need is described by a view.

Internet Relay Chat Protocol (IRCP)

This protocol is mainly used to provide teleconferencing through the Internet. It is best suited for execution on distributed machines. It defines a network that involves a single server that acts as a central point, to which clients can connect, and that performs several functions, such as message delivery and multiplexing. IRCP provides communications between two clients, one-to-many clients, client to server, and server to server.

Some of the key commands of IRCP include the following:

- *User <username> <hostname> <servername> <realname>*: connects *username*, *hostname*, *servername*, and *realname* for a new user
- *Pass <password>*: used to set a connection password
- *Nick <nickname> <hopcount>*: used to give a user a nickname or change the previous one
- *Server <servername> <hopcount> <info>*: used to inform a server that the other end is also a new connected server
- *Oper <user> <password>*: requests operator privileges
- *Quit <quit message>*: ends a client session with a quit message
- *Squit <server> <comment>*: provides information related to zombie servers or quitting servers
- *Join <channel>*: used by the client to start listening to a specific channel
- *Topic <channel>*: used to change or view the topic of a channel

- *Names <channel>*: used to list all nicknames that are visible to a user on any channel
- *List <channel>*: used to list channels and their topics
- *Kick <channel> <user> <comment>*: used to forcibly remove a user from a channel

Service Location Protocol (SLP)

SLP is a discovery protocol that allows computers and other network devices to find services over a LAN connection without prior configuration. This protocol is designed to work with networks of various sizes and complexities, from small, unmanaged networks to large enterprise networks. SLP is designed to identify the network's resources, such as: printers, Web servers, fax machines, video cameras, file systems, backup devices, databases, directories, mail servers, calendars, and a variety of future services.

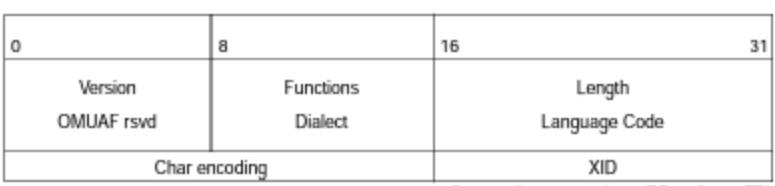
This protocol should be implemented with a client (a user agent) and a server (a service agent). The service agent broadcasts the existence, configuration, and location of a particular service. The user agent requests information from the service agent or from a directory agent. The directory agent acts as a centralized repository for service location information.

Some of the functions of SLP include the following:

- Provides services that are to be handled by the user agent
- Maintains directory of advertised services
- Discovers available service attributes
- Discovers available directory agents
- Discovers the available types of service agents

Figure 2-26 shows the SLP protocol format, with each field detailed below.

- *Version*: This is an 8-bit field that describes the version being used. The current version is 1.
- *Function*: This 8-bit field describes the operation of the service location datagram. This file contains message types, as shown in Figure 2-27.
- *Length*: This is a 16-bit field that gives the total length of the message in bytes, along with the service location header.
- *O*: This is a 1-bit overflow field.
- *M*: This is a 1-bit monolingual field.
- *U*: This 1-bit field contains URL authentication.
- *A*: This is a 1-bit field that contains attribute authentication.
- *F*: This is a 1-bit field. If the bit is set in a service acknowledgment, the directory agent has registered the service as a new entry.
- *Rsvd*: This field is reserved for future use. It must have a value of 0.
- *Dialect*: This is an 8-bit field that is to be used by future versions of SLP. This field should be set to 0.



Source: http://www.javvin.com/protocolSLP.html. Accessed 2004.

Figure 2-26 This is the SLP protocol format.

Function Value	Message Type	Message Abbreviation
1	Service Request	SrvReq
2	Service Reply	SrvRply
3	Service Registration	SrvReg
4	Service Deregister	SrvDereg
5	Service Acknowledge	SrvAck
6	Attribute Request	AtrReq
7	Attribute Reply	AttrRply
8	DA Advertisement	DAADvert
9	Service Type Request	SrvTypReq
10	Service Type Reply	SrvTypRply

SOURCE: http://www.javvin.com/protocolSLP.html. Accessed 2004.

Figure 2-27 These are the message types for all function values.

- *Language Code*: This 16-bit field provides a language through which the remainder of the message should be interpreted.
- *Char Encoding*: This is a 16-bit field. The characters making up strings within the remainder of this message may be encoded in any standardized encoding.
- *XID*: This is a 16-bit field called a transaction identifier that provides the ability to match replies to individual requests.

Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) functions in the application layer to transfer HTML pages from a Web server to a client's Web browser. HTTP is a stateless request/response protocol; each time the client wants to connect to the server, a new connection has to be established. Cookies are text files that are used to temporarily store session information.

HTTP's features include the following:

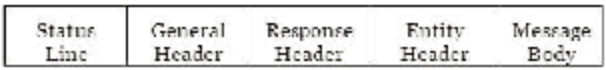
- Provides universally defined addresses
- Allows transmission that is independent of any lower-level protocol
- Connectionless and unreliable protocol
- Does not use acknowledgment after delivery

HTTP request methods include: GET, POST, PUT, DELETE, HEAD, TRACE, OPTIONS, and CONNECT. The following are some of HTTP's vulnerabilities:

- *Cross-site scripting*: The cross-site scripting vulnerability in CGIWrap permits remote attackers to execute arbitrary JavaScript on other Web clients by inserting the CGIWrap-generated JavaScript into an error message. CGIWrap is a program that allows users to execute CGI scripts on specific Web sites, without the danger of changing files outside their own Web space.
- *Directory traversal*: This vulnerability permits attackers to access hidden directories, allowing them to execute commands outside of the Web server's root directory.
- *MailMan Webmail*: MailMan Webmail permits remote attackers to execute random commands in the alternate_template parameter through shell metacharacters.
- *Buffer overflow*: A buffer overflow in the HTML parser permits remote attackers to execute random commands through a long password value present in a form field.
- *eWave*: eWave permits access to the UploadServlet Java/JSP servlet, which does not restrict remote attackers from checking files and executing arbitrary commands.

Source: http://www.javvin.com/protocolHTTPS.html. Accessed 2004.

Figure 2-28 This is the HTTP/HTTPS request message format.



Source: http://www.javvin.com/protocolHTTPS.html. Accessed 2004.

Figure 2-29 This is the HTTP/HTTPS response message format.

Hypertext Transfer Protocol Secure (HTTPS)

The HTTPS protocol is much like HTTP, except that it provides security for the information being transferred using Secure Sockets Layer (SSL) for encrypting and decrypting information. For example, take the following URL: *https://www.banking.com*.

When a user visits this URL, or any beginning with *https://*, HTTPS checks for security before opening the page and then allows users to browse that Web page only after security has been confirmed.

Operation of this protocol is similar to HTTP, as is the message format. The message format of HTTPS is similar to that of HTTP. An HTTP or HTTPS message consists of a request from client to server and a response from server to client. The request message format is shown in Figure 2-28.

The header format of HTTPS differs from HTTP in the request line: it uses a special "Secure" method, and uses the protocol designator "Secure-HTTP/1.4." Consequently, Secure-HTTP and HTTP processing can be intermixed on the same TCP port (often port 80). In order to prevent leakage of potentially sensitive information, the Request-URI should be "*".

HTTPS responses also use the same protocol designator: "Secure-HTTP/1.4." The response message format is shown in Figure 2-29.

In all other respects, HTTPS is the same as HTTP.

Implementing Presentation-Layer Protocols

Lightweight Presentation Protocol (LPP)

LPP is a presentation-layer protocol providing a streamlined approach that supports OSI application services on top of TCP/IP. LPP is designed to run the ISO Common Management Information Protocol (CMIP) in TCP/IP-based networks. It is designed for environments that contain only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). A Directory Services Element (DSE) is used by the application entity; LPP is not applicable to entities whose application context is extensive (for instance, those containing a Reliable Transfer Service Element).

The service provider is in one of the following states:

- IDLE
- WAIT1
- WAIT2
- DATA
- WAIT3
- WAIT4

The following are the possible events:

- PS-user P-CONNECT.REQUEST
- P-CONNECT.RESPONSE
- P-RELEASE.REQUEST
- P-RELEASE.RESPONSE
- P-DATA.REQUEST
- P-U-ABORT.REQUEST
- network TCP closed or errored(*)
- receive ConnectRequest PDU
- receive ConnectResponse PDU
- receive ReleaseRequest PDU
- receive ReleaseResponse PDU
- receive UserData(*) or CL-UserData(**) PDU
- receive user-initiated Abort PDU
- receive provider-initiated Abort PDU
- timer expires(**)

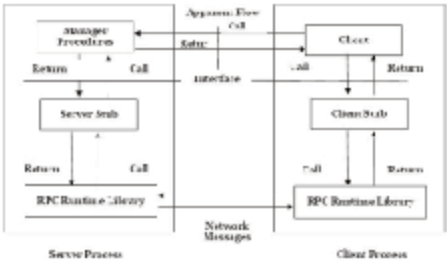
The following are the possible actions:

- PS-user P-CONNECT.INDICATION
- P-CONNECT.CONFIRMATION
- P-RELEASE.INDICATION
- P-RELEASE.CONFIRMATION
- P-DATA.INDICATION
- P-U-ABORT.INDICATION
- P-P-ABORT.INDICATION
- network open TCP(*)
- close TCP(*)
- send ConnectRequest PDU
- send ConnectResponse PDU
- send ReleaseRequest PDU
- send ReleaseResponse PDU
- send UserData(*) or CL-UserData(**) PDU
- send user-initiated Abort PDU
- send provider-initiated Abort PDU
- set timer(**)

Events and actions with a single star (*) apply only to TCP, while those with two stars (**) apply only to UDP.

Implementing Session-Layer Protocols

Session-layer protocols manage connections. These protocols provide a mechanism called SPM (Session Protocol Management) that is used to carry out the procedures in the session-layer protocols that communicate with service users through a Session Service Access Point (SSAP) by means of service primitives. These protocols use the transport layer to exchange protocol data units (PDUs) between these SPMs. The main functions of these session-layer protocols are dialogue management, data-flow synchronization, and resynchronization.



Source: http://www.javvin.com/protocolRPC.html. Accessed 2004.

Figure 2-30 This diagram shows the flow of a message using RPC.

Remote Procedure Call (RPC) Protocol

The RPC protocol enables a system to call and execute its operations on another system on the network. This protocol works similarly to the client-server model, where the requesting program is a client and the program providing the service is a server. This protocol uses TCP and UDP to transfer the message between the two programs.

Some of the key features of RPC include the following:

- *Request-reply*: RPC is a request-reply protocol that uses a single request and then block, awaiting a reply.
- *UDP or TCP transport*: RPC uses UDP and TCP to transport the message. RPC/UDP is a connectionless and stateless protocol. RPC/TCP is slower, but provides a reliable and stateful connection.
- *Standardized data representation*: This protocol uses the eXternal Data Representation (XDR) protocol to encode data.
- *Authentication*: RPC supports calling a program on the target machine from another machine using authentication. This authentication operates in different modes for checking privileges.

The flow of a message using RPC is shown in Figure 2-30.

The RPC protocol consists of two different messages. They are:

- *RPC call message*: This message contains unsigned integer fields to identify the remote procedures. These fields are:
  - Program number
  - Program version number
  - Procedure number
- *RPC reply message*: This looks for a reply regarding whether the call message is accepted or rejected by the server. The reply message indicates one of the following:
  - The call message is successfully executed by RPC.
  - The remote implementation of RPC is not version 2, and it returns the lowest and highest program version numbers.
  - The remote system does not contain the remote program.

Implementing Transport-Layer Protocols

The transport-layer protocols provide end-to-end data transfer over a network. Some of the functions of these protocols include the following:

- Segmentation and reassembly
- Multiplexing and demultiplexing

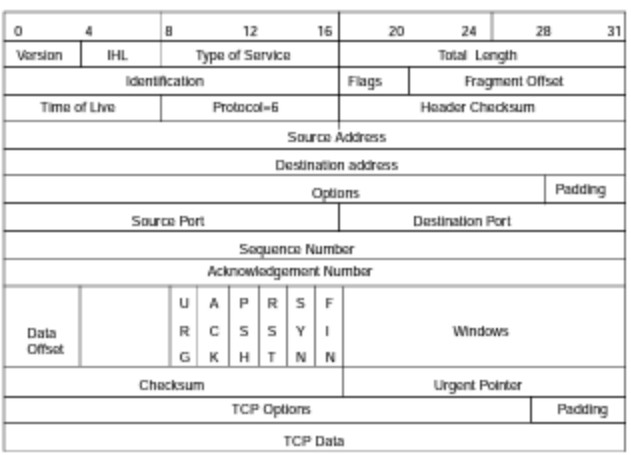
- Error control
- Flow control

Transmission Control Protocol (TCP)

TCP usually works in concert with IP to send data/messages between computers and the Internet. IP takes care of delivery of data, while TCP keeps track of individual data units or packets that divide messages for efficient routing over the Internet. For example, if an HTML file is sent to a user from a Web server, TCP at the transport layer divides that data into two or more packets. It assigns each of them unique numbers with the same destination IP address, and forwards them individually to IP, which is routed differently over a network. At the other end, TCP arranges the received data packets and forwards them in a single file.

Figure 2-31 shows the TCP protocol header format, with each field discussed below.

- *Version*: This 4-bit field indicates the version of IP that is presently in use.
- *IHL*: This 4-bit field indicates the header length of the Internet Protocol. The length of the header can be between 20 and 60 bytes.
- *Type of Service*: This is an 8-bit field that defines the class of datagram for quality of service (QoS) purposes. This is often an unused field, indicating the priority of packets with specific flags.
- *Total Length*: This is a 16-bit field that defines the total length (header and data) of the IP datagram or packet in terms of bytes. The length of data equals the total length minus the header length. Since the field is 16 bits, the total length of the IP packet is limited to 65,535 bytes, of which 20 to 60 bytes are for the header and the remaining are for data.
- *Identification*: This is a 16-bit Internet protocol field that is an identifying value assigned by the sender. It aids in assembling the fragments of a datagram.
- *Flags*: This is a 3-bit field in which the first bit is reserved. The second bit is called the Don't Fragment (DF) bit. If its value is 1, the datagram should not be fragmented. If its value is 0, the datagram should be fragmented. The third bit is the More Fragments (MF) bit and if its value is 1, then the datagram is not the last fragment, which means there are more fragments. If its value is 0, then it is the last or the only fragment.



Source: http://www.javvin.com/protocolTCP.html. Accessed 2004.

Figure 2-31 This is the TCP protocol header format.

- *Fragment Offset*: This 13-bit field shows the relative position of fragments with respect to the datagram. It is the offset of the data in the original datagram, measured in bytes.
- *Time to Live*: This 8-bit field is used to control the maximum number of hops visited by the datagram. Typically, it is 15 to 30 seconds. If a packet is lost during its transfer, then a signal is sent to the computer that the packet is lost and it retransmits the packet.
- *Protocol=6*: This 8-bit field defines the protocols that use the services of the IP layer. This field specifies the final destination protocol to which the IP datagram should be delivered.
- *Header Checksum*: This 16-bit field covers tvhe header of IP packets and not the data. The value of the checksum is set to zero.
- *Source Address*: This 32-bit field defines the IP address of the source. It should not be changed during the transfer of the IP datagram from the source to the destination host.
- *Destination Address*: This 32-bit field defines the IP address of the destination.
- *Options and Padding*: This 32-bit field is an optional field. These fields are used for network testing and debugging. If no options are used, then it is called padded and contains a 1. Padding is used to force a rounded byte value.
- *Source Port Address*: This 16-bit field defines the port number of the application program in the sending host.
- *Destination Port Address*: This 16-bit field defines the port number of the application program in the receiving host.
- *Sequence Number*: This 32-bit field identifies the number of first data octets in any given segment.
- *Acknowledgment Number*: This 32-bit field defines that when the ACK bit is set, this field contains the next sequence byte number that the sender of the segment is expected to receive from other users. If x is the number of bytes received, then $x + 1$ will be the acknowledgment number.
- *Data Offset*: This 4-bit field indicates where the data begins, implying the end of the header by offset.
- *Reserved*: This 6-bit field is reserved for future applications, so it should be set to 0.
- *Control Field*: This is a 6-bit field that has six different control bits or flags. One or more bits can be set or assigned at a time. All bits are capable of enabling flow control, connection establishment and termination, and data-transfer mode in TCP. The following are these fields:
  - *URG flag*: A 1-bit indicating whether the packet is urgent
  - *ACK flag*: A 1-bit acknowledgement field
  - *PSH flag*: A 1-bit field that is used to push the data or perform push functions
  - *RST flag*: A 1-bit field that is used to reset the connection
  - *SYN flag*: A 1-bit field that helps synchronize sequence numbers during connection
  - *FIN flag*: A 1-bit field that is used to terminate the connection
- *Window*: This 16-bit field defines the size of the windows, in bytes, that other users must maintain. The window field denotes the number of octets the recipient is willing to take. This starts with the packet in the ACK field.
- *Checksum*: This 16-bit field is used to calculate the checksum for TCP.
- *Urgent Pointer*: This 16-bit field is valid only if the urgent flag is set and is used when the segment contains that urgent data. This field shows the value of the URG pointer in the form of a positive offset of the sequence number from the octet that follows the URG data, or it points to the end of the urgent data.
- *TCP Options*: This variable-length field occupies a space that is a multiple of 8 bits in length. It contains optional information in the TCP header. There are two options:
  - *Type 1*: a single octet of option-kind
  - *Type 2*: an octet of option-kind, an octet of option-length, and the actual option-data octets

There are three different classes of options:

- *Class 0 option*: indicates an end of an option list that ends all options. This option should be used only if the option list does not merge with the end of the header.
- *Class 1 option*: mainly used for aligning and formatting
- *Class 2 option*: indicates the maximum segment size, which can only be included in the initial request. The main purpose of this option is to provide a size limit.

- *Padding*: This 8-bit field is used to pad the data.

TCP Attacks and Countermeasures

TCP communication takes place by way of the three-way handshake, in which the client system generates and sends an initial sequence number (ISN C) to the server in the form of a SYN request. The server then creates its own sequence number (ISN S) and SYN/ACK, and sends it to the client as a receipt of acknowledgment to the client's request. Normally, the client would then send an acknowledgment (ACK) back to the server and begin the exchange of data. In a SYN flood attack, however, this process is interrupted and the ACK packet is never sent, leaving the server waiting to complete the circuit, resulting in a denial of service. Attackers can also steal or guess these sequence numbers and hijack the session.

In a Transfer Control Protocol (TCP) sequence number prediction attack, an attacker can impersonate a trusted host and create a TCP packet sequence without the acknowledgment of the server response.

To prevent these attacks, the following measures should be taken:

- Randomize the initial sequence number
- Use efficient logging and a good attack alert mechanism

User Datagram Protocol

UDP is mainly used to send short messages over networked computers. It is an unreliable protocol, offering a limited amount of service during the transfer of messages between computers on a network that also uses IP.

The functions provided by this protocol are as follows:

- *Port numbers*: UDP provides port numbers to distinguish between different user requests. This is a 16-bit field that allows multiple processes to use UDP services on the same host. A UPD port address is a combination of a 32-bit IP address and a 16-bit port number.
- *Checksum*: A checksum is used to verify if the data that arrived is correct or not. This is also used to ensure data integrity over the network.

UDP is faster and more efficient for many lightweight or time-sensitive processes. UDP is mainly used for both broadcast and multicast purposes. It can help minimize lost messages, duplication, delivery out of order, and loss of connection.

Figure 2-32 shows the UDP header format, and its four fields are discussed below.

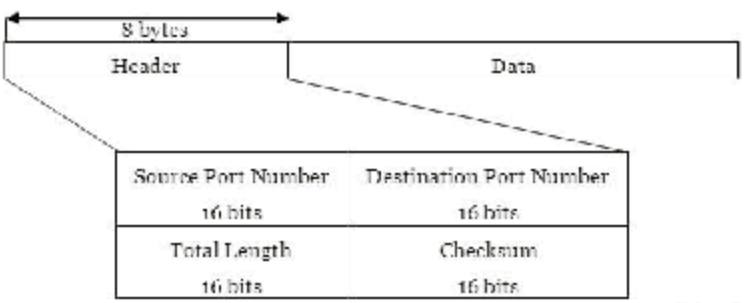


Figure 2-32 This is the UDP header format.

The UDP header consists of the four following 2-byte fields:

- *Source Port Number*: This field contains the port number of the sender or source. This is used by the process running on the source host. The port number ranges from 0 to 65,535. Some of them are static port numbers, others are dynamic port numbers.
- *Destination Port Number*: This port number is used by the processes that are running on the destination hosts. Recipients accept the packet through destination ports.
- *Total Length*: This field defines the total length of the user datagram that contains both header and data. Because the header length is a fixed size, this field essentially refers to the length of the variable-sized data portion (sometimes called the payload). The maximum size is 65, 535 bytes. UDP restricts the datagram to a smaller number, sometimes as low as 8,192 bytes.
- *Checksum*: The main purpose of this field is to detect errors both in the header and data.

UDP Attacks and Countermeasures

UDP contains no features for correcting errors, verifying transfers, or checking for duplication of data or disordering of data packets. This protocol also provides no flow control. This makes the UDP protocol vulnerable to many attacks.

Attackers can spoof UDP packets, which are easier to spoof than TCP packets because there is no sequencing or handshake between clients and servers.

Applications using UDP protocols add security measures to diminish attacks taking advantage of UDP vulnerabilities.

Reliable Data Protocol (RDP)

RDP is a connection-oriented protocol that supports large amounts of data for host monitoring, control applications, and remote debugging. This protocol is mainly designed to provide reliable data-transport services for packet-based applications, such as remote loading.

The key features of RDP include the following:

- RDP works under full duplex mode that uses two ports for transport connection.
- It tries to deliver messages to all users. If it cannot deliver, then it reports a failure message to that user. It uses the datagram service of IP to ensure reliable transfer.
- This protocol attempts to detect and discard duplicate packets. To achieve this, it uses a checksum and sequence number in each header.
- This protocol provides sequence delivery of packets that is specified optionally during connection establishment.
- RDP keeps note of any packets or segments that come out of sequence. This frees up resources for the sender.
- This protocol is considered to be simpler and less complex when compared to TCP.

Figure 2-33 shows the RDP protocol header format, with each field discussed below.

- *Control Bits*: The eight control bits are divided as follows:
  - SYN: A 1-bit field that indicates synchronization is present in the segment
  - ACK: A 1-bit field that indicates the acknowledgement number of the header
  - EAK: A 1-bit field that indicates that an extended acknowledgement is present
  - RST: A 1-bit field used to reset the segment or data
  - NUL: A 1-bit field that indicates that the packet is a null segment
  - 0: A 1-bit field whose value should be 0
- *Version Number*: This 2-bit field is used to indicate the version being used. The current version of RDP is 2.
- *Header Length*: This 8-bit field indicates the total length of the RDP header.
- *Source Port*: This 16-bit field is used to identify the source address of the process that originates the connection. The combination of source and destination address with port identifiers fully describes the connection. This allows RDP to differentiate multiple connections between two hosts.

0	1	2	3	4	5	6	8 15 bit
SYN	ACK	EAK	RST	NUL	0	Ver No	Header Length
Source Port							
Destination Port							
Data Length							
Sequence Number							
Acknowledgement Number							
Checksum							
Variable Header Area i							

Source: http://www.javvin.com/protocolRDP.html. Accessed 2004.

Figure 2-33 This is the RDP protocol header format.

- *Destination Port*: This 16-bit field is used to identify the process that uses the destination address for communication.
- *Data Length*: This 16-bit field gives the length of data in the segment in octets. This data length does not include the RDP header.
- *Sequence Number*: This 16-bit field gives the segment's sequence number.
- *Acknowledgment Number*: This is a 16-bit field. If the ACK bit is set in the header, this is the sequence number of the segment that the sender of this segment last received correctly and in sequence. Once a connection is established, an acknowledgment should always be sent.
- *Checksum*: This 16-bit field is used to ensure data integrity.
- *Variable Header Area*: This 16-bit field is used to transfer parameters for SYN and EAK segments.

Implementing Network-Layer Protocols

The network-layer protocols are mainly used to provide network applications.

Routing Protocols

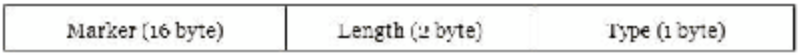
Border Gateway Protocol (BGP)

This routing protocol is used to transfer data or information over the Internet. This is the only protocol that provides multiple connections to unrelated routing domains.

The main function of BGP is to exchange network availability information with another BGP system. This protocol is scalable and robust in nature, and it supports complex routing policies. Figure 2-34 shows the BGP protocol format.

The following are the three different fields in this protocol:

- *Marker*: This is a 16-byte field that marks the beginning of a new message and is used in authentication.
- *Length*: This is a 2-byte field that gives the total length of the message, including the header.
- *Type*: This 1-byte field is used to provide different types of messages in BGP. There are four different types of BGP messages:
  - *Open message*: This message is used to create or initiate a connection with a neighboring router.
  - *Update message*: This is the main message of the BGP protocol. The router uses this to exchange information with neighboring systems. It contains withdraw routes, used by the router to withdraw



Source: http://www.javvin.com/protocolBGP.html. Accessed 2004.

Figure 2-34 This is the BGP protocol format.

0	8	16	24 31 bit
Version	Type	Code	Status
Checksum		Autonomous System Number	
Sequence Number		(The rest of the format is massage type specific)	

Source: http://www.javvin.com/protocolEGP.html. Accessed 2004.

Figure 2-35 This is the EGP structure.

destinations that have been previously announced, and the path, which contains information about the IP address and the address of the next router that is used to route the message to the destination system.

- *Keep-alive message*: This message is used by the peers' systems to exchange information regularly. If these messages are not received by the neighboring router, then it closes its connection and removes it from the routing information base.
- *Notification message*: This message is sent by the router whenever an error is detected, and is followed by an immediate closure of the connection with the neighboring router.

Exterior Gateway Protocol (EGP)

EGP is a gateway protocol that is used to exchange network availability information between two neighboring gateway hosts. This protocol monitors the neighbor routing information and controls error messages.

Some of the message types in EGP include the following:

- *Request*: used to request the acquisition of the neighbor and/or used to initialize the polling variables
- *Confirm*: confirms the acquisition to the neighbor and/or is used to initialize the polling variables
- *Refuse*: refuses the acquisition of the neighbor
- *Cease*: requests deacquisition from the neighbor
- *Cease-ack*: confirms the deacquisition of the neighbor
- *Hello*: requests availability information from the neighbor
- *I-H-U*: confirms the neighbor's availability
- *Poll*: requests to update network availability information
- *Update*: updates network availability
- *Error*: gives an error report

Figure 2-35 shows EGP's structure, while all of its fields are detailed below.

- *Version*: This is an 8-bit field that gives the version number of EGP. The present version is 2.
- *Type*: This 8-bit field identifies the type of message.
- *Code*: This 8-bit field identifies the message code.
- *Status*: This 8-bit field contains message-dependent status information.
- *Checksum*: This 16-bit field ensures the integrity of the message.
- *Autonomous System Number*: This 16-bit field assigns the number for particular autonomous systems.
- *Sequence Number*: This 16-bit field sends state variables or receives state variables.

Internet Control Message Protocol (ICMP)

ICMP (Internet Control Message Protocol) is a TCP/IP protocol that is used to transmit error and control messages. It is mainly used to send error messages through networked computers' operating systems that indicate, for example, that a requested service is unavailable or that a host or router could not be accessed.

ICMP differs in its functioning from TCP and UDP, as it cannot be directly accessed by network applications. The ping tool sends ICMP Echo Request messages (and receives Echo Response messages) to verify that a host is accessible and the time it takes for packets to be sent to and received from that host.

At the highest level, ICMP messages are divided into the following two classes:

- *Error messages*: These give feedback to a source device about the occurrence of an error. They are generally produced in response to some kind of action, usually the broadcasting of a datagram.
- *Informational (or query) messages*: These allow devices to swap information, execute definite IP-related features, and carry out testing. They do not specify errors and are normally not sent in reply to ordinary datagram broadcasts. They are produced if an application or device makes a request for information. Informational ICMP messages can be sent in reply to other informational ICMP messages. They frequently take place in functional pairs, such as request/reply and solicitation/advertisement.

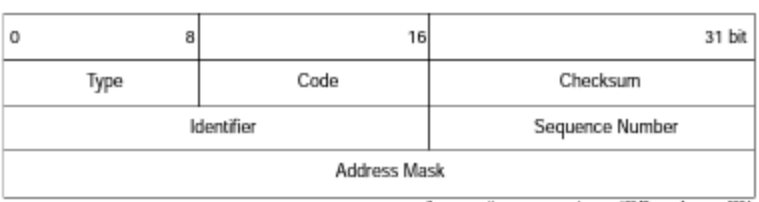
The protocol structure of ICMP is shown in Figure 2-36, with each of the fields detailed below.

- *Type*: Messages can be error or informational messages. Error messages can be Destination Unreachable, Source Quench, Redirect Message. Time Exceeded, or Parameter Problem. The possible informational messages are Echo Request, Echo Reply, Timestamp Request, Timestamp Reply, Infromation Request, Information Reply, Address Mask Request, and Address Mask Reply. These types are shown in Figure 2-37.
- *Code*: For each type of message, several different codes are defined. An example of this is the Destination Unreachable message, where possible messages are: no route to destination, communication with destination administratively prohibited, not a neighbor, address unreachable, or port unreachable.
- *Checksum*: This is the 16-bit complement of the complement sum of the ICMP message starting with the ICMP type. For computing the checksum, the checksum field should be zero.
- *Identifier*: This is an identifier to aid in matching requests and replies.
- *Sequence number*: This is a sequence number to aid in matching requests and replies.
- *Address mask*: This is a 32-bit mask.

To attack an ICMP protocol is not easy, though there are a few loopholes that can be compromised. The following are some ICMP attacks:

- *Redirect-message attack*: This attack is aimed against the ICMP Redirect message, which is employed by gateways to direct hosts to better routes. As such, it can frequently be harmed in the same way that RIP might be. Redirect messages can be bound to specific connections that are already established; there should be no unsolicited alterations to the host's routing tables. In addition, redirects are valid only in a restricted topology. They may be sent only from the initial gateway down the path to the initiating host. A next gateway might not direct that host or might not employ ICMP Redirect to direct other gateways.

  Assume, however, that an intruder has broken into a secondary gateway accessible to a target host, but not the main one. Suppose that the intruder wants to install a duplicate route to reliable host X from the



Source: http://www.javvin.com/protocolICMP.html. Accessed 2004.

Figure 2-36 This is the ICMP protocol structure.

TYPE	DESCRIPTION
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect Message
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (No Longer Used)
16	Information Reply (No Longer Used)
17	Address Mask Request
18	Address Mask Reply

Figure 2-37 These are the different ICMP types.

compromised secondary gateway. The intruder would transmit an error TCP open packet to the reliable host, declaring it to be from X. The main host responds through its open packet by routing it via the protected initial gateway. As this is in transfer, an error redirect can be sent, declaring it to be originating from the initial gateway, referring to the false connection. This packet appears as a valid control message; therefore, the routing variation it holds is accepted. If the main host does this modification to its global routing tables instead of only to the per-connection cached route, the attacker can continue to spoof host X.

- *Subnet-mask reply attacks*: By sending a fake subnet-mask reply message, the attacker can misuse the system. If any host will accept this message, even though it didn't send the query or request, the attacker can block all communications with that system.
- *Denial-of-service attacks*: An attacker can also use ICMP for denial-of-service attacks. To reset existing connections, messages such as Destination Unreachable and Time to Live Exceeded are used. The intruder, who knows the local and remote port numbers of the TCP connection, can forge the ICMP packet arriving at that connection.

The following are some countermeasures that can be deployed to fend off ICMP attacks:

- Restrict route changes to the specified location to prevent redirect attacks
- Check the reply packet only at a suitable time to block subnet-mask attacks
- Perform authentication of the ICMP message
- Randomize the source port number so that it becomes more difficult to guess
- To ignore the message, change the handling of ICMP hard-error messages for synchronized state connections

ICMP Router-Discovery Protocol (IRDP)

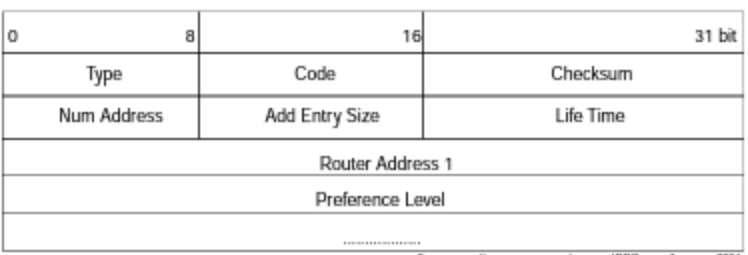
IRDP is used by host systems to determine the IP address of the router. This protocol removes manual configuration and is protocol independent. The host system must discover the router's IP address before it sends IP datagrams to outside subnets. This protocol uses ICMP to allow the host to discover addresses of routers on the subnets.

Figure 2-38 shows the structure of an IRDP advertising message header, while its fields are detailed below.

- *Type*: This 8-bit field describes the type of message; its value is 9.
- *Code*: This 8-bit field contains the ICMP message code; its value is 0.
- *Checksum*: This 16-bit field is used to ensure message integrity. The value of this field is set to 0 before computing the checksum.
- *Num Address*: This 8-bit field gives the number of the router address advertised in this message.
- *Address Entry Size*: This 8-bit field specifies the number of 32-bit words of information for each router address.
- *Lifetime*: This 16-bit field gives the maximum number of seconds that a router address is considered valid.
- *Router Address 1*: This is the sending router's IP address(es).
- *Preference Level 1*: This is the preference of each router address as a default router address, relative to other router addresses on the same subnet.

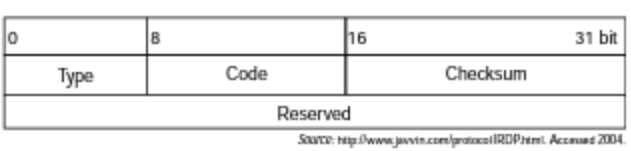
Figure 2-39 shows an IRDP solicitation message, with its fields detailed below.

- *Type*: This 8-bit field describes the type of message used, and its value is set to 10.
- *Code*: This 8-bit field contains the ICMP solicitation message code, and its value is set to 0.
- *Checksum*: The 16-bit checksum's default value is set to 0.
- *Reserved*: This field is reserved for the future, and it is set to 0. It is ignored on reception.



Source: http://www.javvin.com/protocolIRDP.html. Accessed 2004.

Figure 2-38 This is the structure of an IRDP advertising message header.



Source: http://www.javvin.com/protocolIRDP.html. Accessed 2004.

Figure 2-39 This is the structure of an IRDP solicitation message.

Mobile Support Protocol for IP (Mobile IP)

Mobile IP provides two different IP addresses. One IP address is meant for the home system, which is fixed, and another IP address (called the care-of IP address) is a dynamic address. During the movement of a mobile system, it must send its new IP address to the home system so that it can change its communication to that new address.

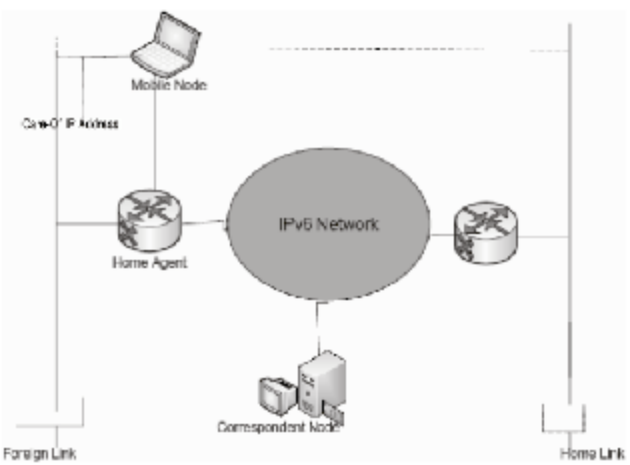
Some of the basic components of Mobile IP are explained in Figure 2-40.

Mobile IP has the following components:

- *Mobile Node*: This node can stay connected by maintaining an availability address at home.
- *Home Link*: This is the basic link for mobile mode.
- *Home Address*: This address is assigned to mobile mode through the attachment of a home link, which is reachable.
- *Home Agent*: This agent is maintained by the router that handles the registration of mobile nodes through their current addresses that are away from home system.
- *Foreign Link*: This is the only link that is not a home link for mobile nodes.
- *Care-of Address*: During the attachment of a foreign link, mobile node uses this address. Forming a link between a home address and a care-of address for a mobile node is called ***binding***.
- *Correspondent Node*: This node provides communication for the mobile node.

Figure 2-41 shows the format for Mobile IP, with its fields described below.

- *Next Header*: This 8-bit field identifies the protocol following this header.
- *Length*: This unsigned 8-bit field contains the total size of the header in bytes.
- *Type*: This is an 8-bit field that provides the type of message:
  - Type 0 is a 1-bit field that contains Binding Refresh Request.
  - Type 1 is a 1-bit field used to initialize Home Test (HoTI).
  - Type 2 is a 1-bit field used to initialize Care-of Test (CoTI).



Source: http://www.javvin.com/protocolMIP.html. Accessed 2004.

Figure 2-40 Mobile IP provides a link between a fixed home IP and a dynamic mobile connection.

Source: http://www.javvin.com/protocolMIP.html. Accessed 2004.

Figure 2-41 This is the format for Mobile IP packets.

Source: http://www.javvin.com/protocolNHRP.htm. Accessed 2004.

Figure 2-42 This is the NHRP format.

- Type 3 is a 1-bit field used for Home Test (HoT).
- Type 4 is a 1-bit field used for Care-of Test (CoT).
- Type 5 is a 1-bit field used to Update Binding (BU).
- Type 6 is a 1-bit field containing Binding Acknowledgment.
- Type 7 is a 1-bit field used to identify the Bit Error.

- *Reserved*: This 8-bit field should be zero, and the receiver should ignore it.
- *Checksum*: This 16-bit field is used to check for errors in the Mobile IP header.
- *Data*: This variable-length field is the actual data.

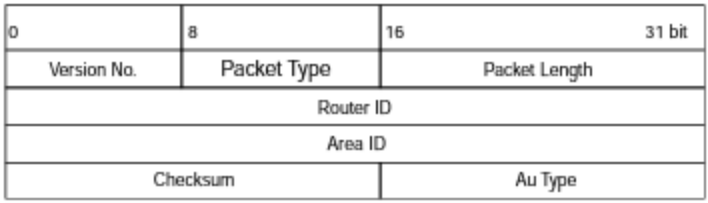
Next-Hop Resolution Protocol (NHRP)

This protocol provides a direct route to transfer data from one computer to another. If the packet received by the destination computer is in the same subnet as the local computer, then this protocol tells the subsequent data packets to send directly to the local computer using the global subsequent network address. This NBMA protocol allows a source system to communicate with a nonbroadcast multiaccess subnetwork to identify the layer address of NBMA for suitable next hops at the destination system or station. This protocol uses the multiprotocol environment for network layering over the NBMA network.

NHRP traverses one or more hops in a subnet before reaching the station that is expected to generate the response. Every station will choose a neighbor NHS to forward an NHRP request. These packets are not covered within the protocol header, but are covered in the NBMA layer, which is described in its own header.

Figure 2-42 shows the NHRP format, while its fields are described below.

- *ar$afn*: This 8-bit field defines the type of address carried by the link layer.
- *ar$pro.type*: This 16-bit unsigned integer field is reserved as follows:
  - 0x0000 to 0x00FF: Protocols defined by the equivalent NLPIDs
  - 0x0100 to 0x03FF: Reserved for future use by the IETF
  - 0x0400 to 0x04FF: Allocated for use by the ATM Forum
  - 0x0500 to 0x05FF: Experimental/local use
  - 0x0600 to 0xFFFF: Protocols defined by the equivalent Ethertypes
- *ar$pro.snap*: This 32-bit field deals with the protocol that has an assigned number in the ar$pro.type space (excluding 0x0080; if this value exists, then it must be zero on transmit and the receiver should



SOURCE: http://www.javvin.com/protocolOSPF.html. Accessed 2004.

Figure 2-43 This is the format of OSPF.

ignore it). The short form must be used when transmitting NHRP messages. Ethertype must be used during the transmission of both NLPIDs and Ethertype codes of NHRP messages.

- *ar$hopcnt*: This 8-bit field defines the hop count, which specifies the maximum number of hops to traverse before the packet is deleted.
- *ar$pktsz*: This 16-bit field is used to give the total length of NHRP packets in octets.
- *ar$chksum*: This 16-bit field is used to check the errors in the entire NHRP packet.
- *ar$extoff*: This 16-bit field is used for extensions that identify the existence and location of NHRP packets.
- *ar$op.version*: This 8-bit field determines the version used by this protocol.
- *ar$op.type*: This 8-bit field gives the type of NHRP packet. Possible values of NHRP types are as follows:
  - If the value is 1, then it is an NHRP Resolution Request.
  - If the value is 2, then it is an NHRP Resolution Reply.
  - If the value is 3, then it is an NHRP Registration Request.
  - If the value is 4, then it is an NHRP Registration Reply.
  - If the value is 5, then it is an NHRP Purge Request.
  - If the value is 6, then it is an NHRP Purge Reply.
  - If the value is 7, then it is an NHRP Error Indication.
- *ar$shtl*: This 8-bit field gives the type and length of the source NBMA address, which has been interpreted in the context of a family number of the address.
- *ar$sstl*: This 8-bit field gives the type and length of the source NBMA subaddress that is interpreted in the context of the address family number.

Open Shortest Path First (OSPF) Protocol

This protocol uses the link-state method to provide information about direct connections and links used by the other router. It maintains a database through which a table (called a routing table) is calculated by constructing a shortest-path tree. Information exchanged by the routers of OSPF is authenticated.

The protocol groups different networks together, and such groupings are called areas. An area is hidden from rest of the system and thereby enables a significant reduction in routing traffic.

Figure 2-43 shows the format of OSPF. Its fields are detailed below.

- *Version Number*: This is an 8-bit field that identifies the type of version being used by OSPF. The current version is 2.
- *Packet Type*: This 8-bit field gives the type of packet. There are five different types:
  - *Hello*: This type is used to establish and maintain relationships with neighbors.
  - *Database Description*: This field describes the contents of the database. These messages are exchanged during initialization.

- *Link-State Request*: This field requests the database to give information related to neighboring routers for exchanging information through database description.
- *Link-State Update*: This field responds to a link-state request. Several link-state algorithms are used to update the database packets.
- *Link-State Acknowledgment*: This field acknowledges the packets that are updated by the link state.

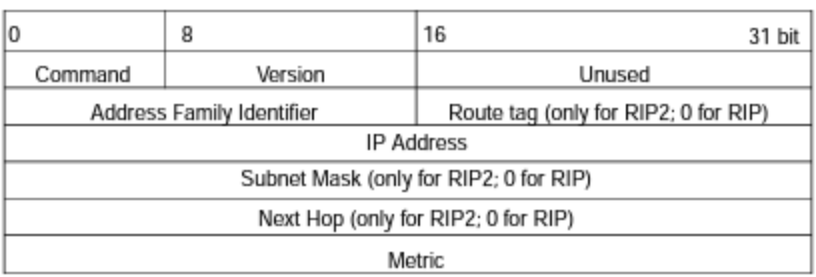
- *Packet Length*: This 16-bit field specifies the packet length, including the length of the OSPF header, in bytes.
- *Router ID*: This field identifies the source of the packet.
- *Area ID*: This field specifies the area to which a packet belongs. All packets are identified with a single area that travels in a single hop.
- *Checksum*: This field is used to check the entire contents of the packet header.
- *Authentication Type*: This field contains the authentication scheme used.
- *Authentication Scheme*: This 64-bit field contains specific information about authentication.
- *Data*: This field contains information related to the upper layer.

Routing Information Protocol (RIP)

This is a widely used distance vector protocol for exchanging information over a gateway and a host. It is used for routing traffic over the Internet through a single system. This is a simple protocol that is designed to work for a moderately sized network that uses homogeneous technology.

Figure 2-44 shows the RIP packet format, with its fields detailed below.

- *Command*: This is an 8-bit field that is used to specify the purpose of the datagram. There are five different commands:
  - *Request*: This command requests that the router send information from the routing table.
  - *Response*: This command is used to update the routing table or to respond to a request.
  - *Trace on*: This is an obsolete command.
  - *Trace off*: This is an obsolete command.
  - *Reserved*: This command is reserved for future use.
- *Version*: This 8-bit field gives the version number. The current version is 2.
- *Unused*: This is a 16-bit field that is not in use.
- *Address Family Identifier*: This 16-bit field specifies the address family used. As RIP is designed to carry routing information for several protocols, every entry will have an address family identifier to specify the type of address used.



Source: http://www.javvin.com/protocolBGMP.html. Accessed 2004.

Figure 2-44 This is the RIP packet format.

- *Route Tag*: This 16-bit field is used to separate internal and external RIP routes that are imported from IGP or EGP.
- *IP Address*: This specifies the IP addresses of source and destination systems.
- *Subnet Mask*: This 32-bit field carries the subnet mask for the entry. If the value is 0, then there is no subnet mask.
- *Next Hop*: This field indicates the IP address of the next hop to which packets for the entry should be forwarded.
- *Metric*: This 32-bit field indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route.

Multicasting Protocols

Border-Gateway Multicast Protocol

This is an interdomain multicasting protocol that supports source-specific multicast (SSM). This protocol uses TCP for carrying packets, and it uses the TCP port for establishing a connection.

Figure 2-45 shows the format of BGMP packets, with all of the fields discussed below.

- *Length*: This is a 8-bit field that gives the total length of the header in octets.
- *Type*: This 8-bit field represents the type of message used. Whenever the connection is established using a transport layer, then the first message received will be an OPEN message. If the OPEN message is accepted, then a KEEPALIVE message confirming the OPEN is sent back. Once the OPEN is confirmed, UPDATE, KEEPALIVE, and NOTIFICATION messages may be exchanged.
- *Reserved*: This 8-bit field is reserved for future use.

Distance-Vector Multicast Routing Protocol (DVRMP)

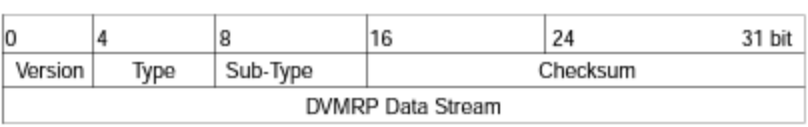
This protocol supports multicast data transmission over a network. This protocol can manage different networks that are not multicast-capable. The purpose of this protocol is to provide paths for multicast datagrams. This protocol uses IGMP (Internet Group Management Protocol) to exchange routing datagrams. It uses a reverse-path multicast algorithm to calculate the shortest path.

Figure 2-46 shows the DVRMP format, while its fields are discussed below.

- *Version*: This 4-bit field gives the version number. The current version is 1.
- *Type*: This is a 4-bit field that provides the type of message. Its value is three.
- *Subtype*: This 8-bit field contains four different subtypes:

SOURCE: http://www.javvin.com/protocolBGMP.html. Accessed 2004.

Figure 2-45 This is the BGMP format.



SOURCE: http://www.javvin.com/protocolDVMRP.html. Accessed 2004.

Figure 2-46 This is the DVRMP format.

- *Response*: This provides a response message to route to the destination system.
- *Request*: This requests the routes to a destination.
- *Nonmembership Report*: This provides a nonmembership message.
- *Nonmembership Cancellation*: This cancels a nonmembership message.

- *Checksum*: This field is used to check for errors in the packet header.
- *DVMRP Data Stream*: This field is used to tag the data. This streamed data is used to reduce redundant messages in data.

Other Network Protocols

The NetBEUI Protocol

This protocol is mainly used by small networks. NetBIOS Extended User Interface (NetBEUI) is a legacy protocol commonly used by older Windows networks. This is a simple and fast protocol that does not require any administrative configuration. It is implemented in the data-link layer of the OSI model. This protocol is not routable. It is not supported on Windows XP or Windows Server 2003.

Remote Authentication Dial-In User Service (RADIUS)

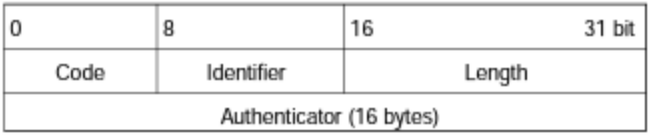
This is a client-server protocol. It acts as software that enables a remote-access server to communicate with a central server. This protocol allows a company to store user profiles in a database. It uses UDP as a transport protocol.

The key features of RADIUS include the following:

- *Client-server model*: With this protocol, the network-access server acts as a client to RADIUS. The client is capable of passing user information to RADIUS servers. They are responsible for receiving user connection requests, performing user authentication, and then returning all configuration information necessary for the client to deliver service to the user.
- *Network security*: This feature provides security to both client and server applications of the RADIUS protocol.
- *Flexible authentication*: This feature provides different methods to authenticate the user. It supports different protocols such as PAP, CHAP, PPP, UNIX login, and other mechanisms.
- *Extensible protocol*: This feature provides new attribute values that can be added to the existing protocol without disturbing its implementation.

Figure 2-47 shows the RADIUS protocol structure. Its fields are detailed below.

- *Code*: This is an 8-bit field that contains different types of codes as follows:
  - Code 1 is used for Access-Request.
  - Code 2 is used for Access-Reply.
  - Code 3 is used for Access-Reject.
  - Code 4 is used for Accounting-Request.
  - Code 5 is used for Accounting-Response.
  - Code 11 is used for Access-Change.



Source: http://www.javvin.com/protocolRADIUS.html. Accessed 2004.

Figure 2-47 This is the RADIUS protocol structure.

- Code 12 is used for Status-Server.
- Code 13 is used for Status-Client.
- Code 255 is reserved for future use.

- *Identifier*: This 8-bit field is used to identify request-and-reply matches.
- *Length*: This 16-bit field gives the total length of the header.
- *Authentication*: This 16-bit field is used to authenticate a user reply from the RADIUS server as well as the password-hiding algorithm.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) is used to transmit voice as packets over the Internet. The voice signal is converted into a digital signal and then compressed and converted into IP packets, which are then transmitted over an IP network.

Key benefits of this protocol include:

- It is a low-cost system
- Data can be easily integrated
- Both voice and video are available on the Internet

Some of the associated protocols and standards of VoIP include the following:

- *H.323*: This is an ITU standard developed for conferencing multimedia applications on a LAN. Some of the components are terminals, gateways, gatekeepers, and multipoint control units.
- *SIP*: The Session Initiation Protocol is an IETF standard used for establishing connections for VoIP. This application-layer protocol acts like a client-server protocol, capable of creating a connection, modifying the connection, and terminating the connection.
- *MEGACO*: This Media Gateway Control Protocol was developed by both ITU and IETF. This protocol is used to control the elements in a multimedia gateway that separate call control from media conversion. This protocol converts circuit-switched voice to packet-based traffic using a media gateway controller. It supports ATM networks.
- *MGCP*: This Media Gateway Control Protocol was developed by Cisco Systems. This protocol provides communication between call control elements and telephony gateways. This protocol is capable of monitoring events between IP phones and gateways and requests that they send media to a particular address.

Figure 2-48 shows how VoIP works.

Implementing Data-Link-Layer Protocols

Data-link-layer protocols mainly handle the protocols that are related to data applications.

Address Resolution Protocol

ARP (Address Resolution Protocol), a TCP/IP protocol, retrieves a node's physical address. A host sends an ARP request with the IP address of the target node that needs to communicate on the network, and the node with the specified address responds by returning its physical address and packets that are to be transmitted. All the stations in the entire network need to process the ARP request, which also requires the IP address of other machines.

Address Resolution Protocol will discover a host's MAC address when its IP address is known. The sender transmits an ARP packet that consists of the Internet address of the other machine and waits for it (or some other host) to send its MAC address in reply. Every machine maintains a cache of address translations to decrease waiting time and loading.

Some features of ARP include the following:

- ARP is used primarily for mapping IP addresses on a network.
- Earlier, ARP was used to resolve MAC addresses for various layer-3 protocols only. Later, it was also designed to resolve other layer-2 addresses, such as ATMARP and NSAP.
- ARP is a well defined dynamic resolution protocol that maps IP addresses to basic data-link-layer addresses.

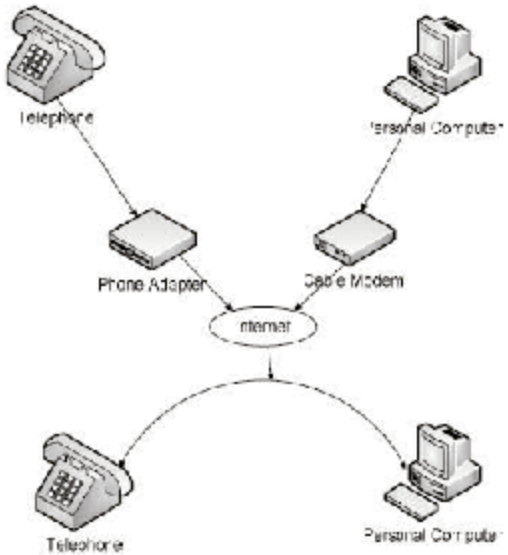
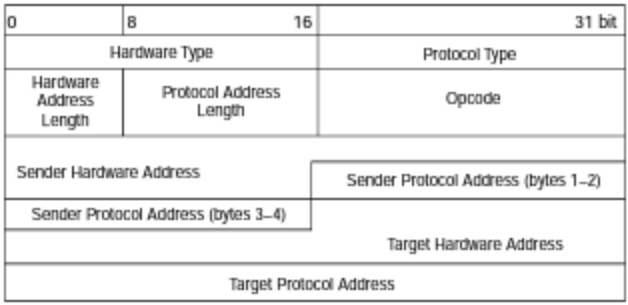


Figure 2-48 VoIP sends voice data over the Internet, even to and from telephones.

- ARP was designed to assist dynamic address resolution between IP and Ethernet that can also be used on other layer-2 technologies. It functions by permitting an IP device to transmit on the local network, requesting another device within that network to reply with its hardware address.
- Direct mapping and dynamic resolution are two fundamental techniques used to obtain the association of addresses.
- The essential process of ARP is to encode the IP address of the proposed addressee in a broadcast message.

Figure 2-49 shows the structure of an ARP packet. Its fields are discussed below.

- *Hardware Type*: This 16-bit field defines the type of hardware for transmitting ARP messages and also specifies the type of addressing used.
- *Protocol Type*: This 16 bit-field defines the type of addresses used in the message. The value for IPv4 addresses is 2,048, which is a 0x0800 hex.
- *Hardware Address Length*: This 8-bit field specifies the length of the hardware address for Internet messages. The value of this field is 6 for Ethernets and other networks that use IEEE 802 MAC addresses.
- *Protocol Address Length*: This 8-bit field specifies the length of the protocol address used in the message. Its value will be 4 for an IPv4 address.
- *Opcode*: This 16-bit field defines the nature of the ARP message to be sent.
- *Sender Hardware Address*: This field defines the hardware addresses of the devices that are used to send the messages.
- *Sender Protocol Address*: This field contains the IP addresses of the devices that are used to send the messages.



Source: http://www.tcpipguide.com/free/t_ARPMessageFormat.htm. Accessed 2004.

Figure 2-49 This is the structure of ARP.

- *Target Hardware Address*: This field contains the hardware addresses of the target machines that are going to receive the messages.
- *Target Protocol Address*: This field contains the IP address of the target machine that is going to receive the message.

ARP Vulnerabilities and Countermeasures

ARP has the following vulnerabilities:

- ARP does not provide an authentication mechanism for messages, such as requests or replies, so it is easy for a hacker to misuse the system by forging those messages. A forged request or reply can be used in ARP poisoning. ARP poisoning means updating the ARP cache of a remote system with a forged entry.
- ARP is a stateless protocol. Therefore, even if an ARP request is not sent to a user, that user can send the corresponding ARP reply.
- The man-in-the-middle attack is based upon persuading two hosts that the computer in the middle is the other host. If the system is using DNS for identifying the other host, then this attack will result in a domain name spoof or it may result in ARP spoofing on the LAN.

The following countermeasures can help prevent the exploitation of these vulnerabilities:

- Spoofed IP packets can update the contents of ARP tables. To avoid this, a rule-based firewall should be configured to block ARP.
- Run a batch file to create static ARP entries. This protects against ARP poisoning.

Reverse Address Resolution Protocol

RARP (Reverse ARP) is a TCP/IP protocol used with diskless computers to acquire their IP addresses. When a RARP request is sent in an Ethernet frame to the server, the server responds with a layer-3 (IP) address for the layer-2 (MAC) address that it just received.

It resolves an IP address starting from a known hardware address, such as the MAC address. Every MAC must be configured manually on a central server, and the server will only provide an IP address to computers with those MAC addresses. Subnetting, gateways, and other details must be set up manually.

RARP was superseded by BOOTP, which consists of an enhanced feature set.

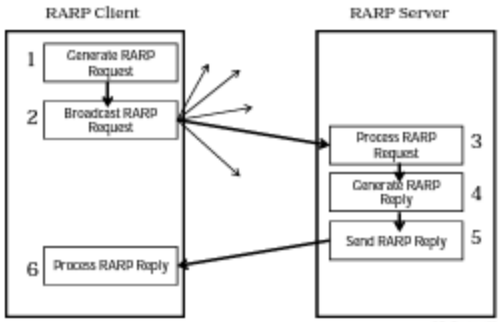


Figure 2-50 This shows how RARP works.

Figure 2-50 shows a RARP transaction diagram.
A RARP transaction works as follows:

1. The source device generates a RARP request frame.
2. The source device broadcasts the RARP request message.
3. The local device processes the RARP request message.
4. The RARP server generates a RARP reply message.
5. The RAP server sends the RARP reply message.
6. The source device processes the RARP reply message.

RARP's features include the following:

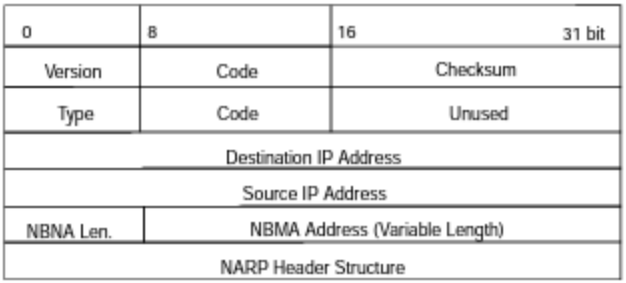
- RARP solves the bootstrapping problem.
- It performs the reverse of ARP's function.
- Each MAC must be manually configured on the central server.
- RARP is a non-IP protocol, which means it can't be managed by the TCP/IP stack that already exists on the client system. The client must have unique functionality to handle the unprocessed RARP packet.

NBMA Address Resolution Protocol (NARP)

The NBMA Address Resolution Protocol allows a host or a router to communicate with a nonbroadcast multiaccess link-layer network to identify the destination terminal of the NBMA address. Once the NBMA address of the destination is available, the source can send packets to the destination or it can establish a connection.

Figure 2-51 shows the NARP format, with its fields detailed below.

- *Version*: This 8-bit field is the version number. Currently, the value of this field is 1.
- *Hop Count*: This 8-bit field indicates the maximum number of NBMA ARP servers (NASs) to allow a request or reply packet to traverse before discarding.
- *Checksum*: This 16-bit field is used to check for errors for the entire packet.
- *Type*: This 8-bit field is used to describe the type of NARP packet. If the type code is 0, then it is a NARP request, and if the type code is 1, then it is a NARP reply.
- *Code*: This 8-bit field describes the type of code to be used.
- *Unused*: This field is not used by NARP.



Source: http://www.javvin.com/protocolNARP.html. Accessed 2004.

Figure 2-51 This is the NARP packet format.

- *Destination IP Address*: This field contains the IP address of the destination system.
- *Source IP Address*: This field contains the IP address of the source system.
- *NBMA Length and Address*: The NBMA length field is the length of the NBMA address of the source terminal in bits. The NBMA address itself is zero-filled to the nearest 32-bit boundary.

Chapter Summary

- *A protocol* is a set of rules that enables communication between computers over a network.
- Internet Protocol (IP) is a network-layer protocol present in the TCP/IP communications protocol suite.
- Network classes are used to identify the devices connected to the Internet or the network.
- The BOOTP protocol allows a network user to configure a boot process automatically without user involvement.
- The most significant, universal file transfer protocol in TCP/IP is File Transfer Protocol (FTP).
- NTP is used to synchronize system clocks over IP with Coordinated Universal Time (UTC) taken from time servers.
- TCP usually works in concert with IP to send data/messages between computers and the Internet.
- ICMP (Internet Control Message Protocol) is a TCP/IP protocol that is used to transmit error and control messages.

Review Questions

1. What is a protocol?

_____

_____

_____

_____

2. List the key elements of a protocol.

_____

_____

_____

_____

3. What are the functions of a protocol?

4. What is segmentation and reassembly?

5. List some kinds of IP attacks.

6. What are the three major issues of IP?

7. What is the function of DHCP?

8. List the applications in the presentation layer.

9. What is the difference between HTTP and HTTPS?

10. How do you configure LPP?

11. What are the applications of RPC?

12. List the features of the transport layer.

13. List the applications of RDP.

14. List the features of network-layer protocols.

15. Explain the difference between routing protocols and multicast protocols.

16. Identify the characteristics of network protocols.

17. What is ARP?

Hands-On Projects

1. Read an introduction to protocol analysis.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Read Introduction to Protocol Analysis.pdf.
2. Read a TCP/IP tutorial and technical overview.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Read TCPIP Tutorial and Technical Overview.pdf.
3. Read another introduction to TCP/IP.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Read Introduction to TCPIP.pdf.
4. Read about multicast routing.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Read Multicast Routing.pdf.
5. Read about RIP.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Read Network-Layer Protocol Lab RIP.pdf.

Chapter 3

Protocol Analysis

Objectives

After completing this chapter, you should be able to:

- Understand TCP/IP protocol structures
- Understand TCP data-packet structures
- Implement user-level commands
- Understand TCP algorithms
- Understand IP data-packet structures
- Understand IPv6

Key Terms

Asynchronous Transfer Mode (ATM) a lower-level network protocol that encodes data into small fixed cells and transmits them over a network medium

Checksum a value included in a header to ensure that the data has been transferred without error

Congestion window a value that indicates the maximum amount of data that can be sent out on a connection without an acknowledgment; when a connection is first established, the congestion window is set up as the size of one segment. The sender maintains the window and increments it for every ACK received.

DARPA (Defense Advanced Research Projects Agency) a project funded by the Department of Defense (DoD) that led to the creation of the Internet in the 1950s and 1960s; DARPA developed the TCP/IP protocols

Encapsulation the way data moves through the protocol stack as it is prepared for transmission; each layer adds its header information to the data as it moves down the protocol stack

Next-hop routing the way information is indirectly transmitted across the Internet through hops from router to router before reaching the destination network.

OSI (Open Systems Interconnection) reference model an abstract model for the implementation of network design, with the network divided into seven layers of abstraction

Transmission Control Protocol/Internet Protocol (TCP/IP) the protocol suite that handles communication over the Internet. TCP handles the packetizing of messages, and IP handles transferring those packets over the network.

Windowing a congestion-control measure that acts as a buffer to control data loss

Introduction to Protocol Analysis

This chapter primarily discusses TCP/IP protocol structures, the TCP and IP data-packet structures, user-level commands implementation, TCP algorithms, and IPv6. This chapter discusses the TCP/IP protocol suite, the layers of TCP/IP, sliding windowing, and acknowledgment. It then discusses the TCP header format and various options in the header. Next, this chapter covers the TCP/IP interfaces, user interface commands, and lower-level interface commands as well as TCP algorithms, checksums, performance estimation, and TCP-related problems. Then the chapter moves to IP, giving an overview of IP, the IP header format, the IP datagram concept, techniques associated with IP datagrams, and the parameter problem in IP. Finally, there is an introduction to the IPv6 header format, tunneling, and multicasting.

Understanding TCP/IP Protocol Structures

TCP/IP Protocol Suite

TCP/IP is the protocol suite that handles communication over the Internet. TCP handles the packetizing of messages, and IP handles transferring those packets over the network. The TCP/IP protocol suite maps to the conceptual model DARPA developed. ***DARPA*** is a project funded by the Department of Defense (DoD) that led to the creation of the Internet in the 1950s and 1960s. DARPA developed the TCP/IP protocols. The DARPA model is composed of four layers:

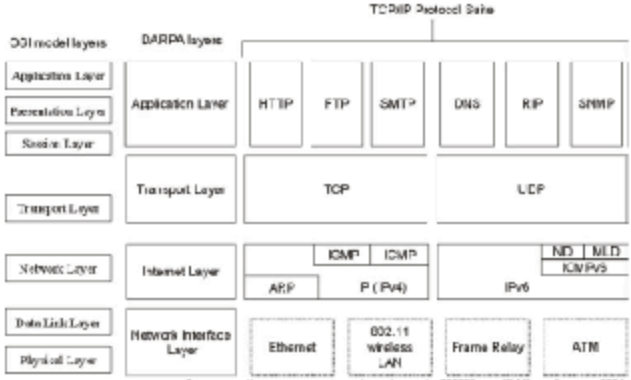
1. Application layer
2. Transport layer
3. Internet layer
4. Network-interface layer

Figure 3-1 shows the architecture of TCP/IP.

Network-Interface Layer

The network-interface layer is the lowest layer in the TCP/IP model. It is responsible for sending and receiving TCP/IP data packets to and from the network medium. The design of TCP/IP is not dependent on a particular network access method, frame format, or medium. TCP/IP can be used in different networks, including Ethernet, 802.11 wireless LAN, and Asynchronous Transfer Mode (ATM). ***ATM*** is a lower-level network protocol that encodes data into small fixed cells and transmits them over a network medium. The network-interface layer has all the functionality of the data-link and physical layers of the ***OSI reference model***—an abstract model for the implementation of network design, with the network divided into seven layers of abstraction. Ethernet is the most commonly used network-interface layer. The network-interface layer performs the following functions:

- Describes the physical connection necessary for communications
- Defines some services that are used by Internet layer, such as frame size, addressing capabilities (unicast, multicast, and broadcast), and quality-of-service (QoS) parameters
- Delivers data packets within a single network
- Encapsulates Internet-layer segments into frames
- Adds frame-check sequence (cyclic redundancy check) to the end of the data packet (error checking)
- Broadcasts or switches frames over the network using source and destination MAC addresses



Source: http://technet.microsoft.com/en-us/library/bb726993.aspx#EAEbsp. Accessed 2004.

Figure 3-1 This is the architecture of TCP/IP.

- Delivers data to devices on a directly attached network
- Defines rules to use the network for delivering IP datagrams
- Maps media access control (MAC) addresses to IP addresses using Address Resolution Protocol (ARP)

Implementation

Both hardware and software drivers are implemented in the network-interface layer. This is the only layer that usually keeps track of the physical characteristics of the underlying network that includes access rules, data-frame structure, and addressing.

Internet Layer

The Internet layer, also called the internetworking layer, is the second layer in the TCP/IP protocol stack. It is responsible for providing machine-to-machine communication. The Internet layer is also responsible for the addressing, packaging, and routing of data packets.

The TCP/IP protocol suite contains two sets of protocols at the Internet layer:

- IPv4, which is also known as IP, is used in almost all private intranets and the Internet.
- A newer protocol, IPv6 will replace IPv4. IPv6 is a routable protocol that addresses and routes packets.

The Internet layer acts as a communication interface between two networks, regardless of type, and handles the translation for different types of data addressing schemes. The Internet layer uses the IP, ARP, ICMP, and IGMP protocols.

- Address Resolution Protocol (ARP) resolves Internet-layer addresses to network-interface layer addresses.
- Internet Protocol (IP) is a routable protocol that addresses, routes, fragments, and reassembles packets.
- Internet Control Message Protocol (ICMP) reports errors and information that can be further analyzed when a failure in the delivery of a packet occurs.
- Internet Group Management Protocol (IGMP) helps in managing IP multicast groups.

The Internet layer also has some core protocols for IPv6, including the following:

- Neighbor Discovery Protocol (NDP) manages the interaction of IPv6 neighboring nodes.
- The Multicast Listener Discovery (MLD) protocol manages IPv6 multicast groups.

The Internet layer plays a major role in deciding the best route to send data packets. It deals with the entire network architecture. The router is the key device in this layer.

The following are some of the features of the Internet layer:

- Defines the datagram (packet) and addressing scheme
- Moves data between the network-interface layer and transport layer
- Routes datagrams to remote hosts
- Performs fragmentation and reassembly of datagrams

This layer provides the following three specific services:

- Connectionless delivery service
- Implements a mechanism to divide the data into individual packets or frames on the transmitting side and put them back together on the receiving side (fragmentation and reassembly)
- Provides a routing function for operating with other networks

Transport Layer

This layer provides communication among different connected systems. The transport layer, also known as the host-to-host transport layer, provides session and datagram communication services to the application layer. The transport layer in the TCP/IP model has the same functionality as the transport layer of the OSI model. TCP and UDP are the core protocols of the transport layer.

There are two methods of delivery in TCP/IP:

- Connection-oriented reliable delivery using TCP
- Connectionless best-effort delivery using UDP

TCP provides a one-to-one, connection-oriented reliable communication service. It sequences the packet, acknowledges the packet sent, and recovers lost packets.

UDP provides one-to-one and one-to-many connectionless services. It is an unreliable communication service. UDP transfers less data than TCP. TCP and UDP both operate on IPv4 and IPv6 networks.

The transport layer is capable of transporting data to and from various applications. It provides end-to-end communication.

The following are some of the features of the transport layer:

- This layer manages the transfer of data between TCP and UDP.
- It manages the connection between various network applications.
- It is the most visible layer to application designers.
- The transport layer provides a virtual end-to-end message pipe for applications and is the layer where direct host-to-host communication takes place.
- This layer makes it possible for the details of the underlying network to remain hidden. The basic functions of this layer are quality-control issues such as:
  - Reliability
  - Flow control
  - Error correction
  - Broadcasting

Application Layer

The application layer defines the protocols that the application is going to use for the transfer of data and allows access to the services of the other layers. There are many protocols in the application layer, and more are always being developed. The following are some of the protocols used in this layer:

- The Hypertext Transfer Protocol (HTTP) transfers files that make up Web pages on the Internet.
- The File Transfer Protocol (FTP) transfers individual files, typically in an interactive user session.
- The Simple Mail Transfer Protocol (SMTP) transfers e-mail messages and attachments.

Additionally, the following application-layer protocols help users use and manage TCP/IP networks.

- The Domain Name System (DNS) protocol resolves a host name, such as *www.apple.com*, to an IP address and copies name information between DNS servers.
- The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.
- The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices such as routers, bridges, and servers.

Windowing

Windowing (Figure 3-2) is a congestion-control measure that acts as a buffer to control data loss. Windowing requires the source device to receive an ACK from the destination after a certain amount of data is transmitted. The destination host reports a window size to the source host. This window size specifies the number of packets that the destination host is prepared to receive. The first packet is the ACK. When the window size is 3 bytes, the source device can send 3 bytes of data to the destination. The source device waits for an acknowledgment. When the acknowledgment is received, the source device can then transmit 3 more bytes to the destination. In an overflow condition where too much data is sent too quickly, the destination is unable to receive the 3 bytes, so no acknowledgment is sent to the source. This causes the source to retransmit the bytes, and the transmission rate slows down.

In Figure 3-2, the sender sends three packets before it expects an ACK. If the receiver can handle only two packets, the window drops packet three, specifies three as the next packet, and indicates a new window size of two. The sender sends the next two packets but still specifies a window size of three. This means that the sender will still expect a three-packet ACK from the receiver. The receiver replies with a request for packet five and again specifies a window size of two.

Sliding Window

Sliding window is a technique used by TCP to control the flow of packets in a network. It allows for a dynamic range of window sizes. The destination host must acknowledge all transmitted data. A single acknowledgment can assure the transmission of multiple data packets. The sender and receiver maintain a window for which no acknowledgment is received, and that window is the sequence of the message IDs. This starts with a low

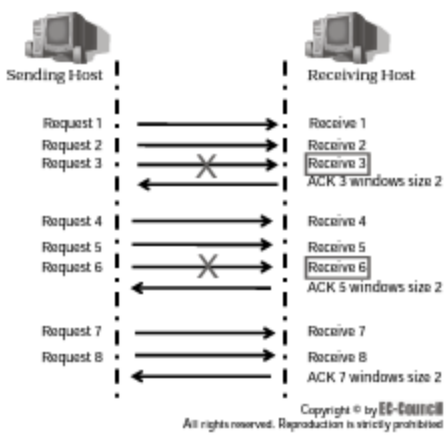


Figure 3-2 Windowing requires the source device to receive an acknowledgment from the destination after a certain amount of data is transmitted.

watermark and is bounded by high watermark. After the receipt of an acknowledgment, the low and high watermarks are incremented by 1. In turn, one more acknowledgment is received. The window is slid to the right. The ACK is discarded when the window is full. Sliding windows start with a given size, and sophisticated protocols adapt the window size dynamically.

The following are characteristics of the sliding-window technique:

- Error correction
- Flow control
- Message ordering (FIFO)

One-Bit Sliding-Window Protocol

In this protocol, the sender sends one frame and then waits for an acknowledgment before sending the next frame, so it is also called the stop-and-wait protocol. The disadvantage of the stop-and-wait protocol is that only one frame can be transmitted at a time.

Go-Back-n

During the transmission of packets, if a single frame—for example, K—is lost, then the whole sequence of frames $K + 1, K + 2, \ldots$ is discarded; no acknowledgment is then sent to the sender. When the sender doesn't receive an ACK, it retransmits the frames starting from K. It sets the receiver window size to 1. It is a waste of bandwidth. This technique is depicted in Figure 3-3.

Selective Repeat

Selective repeat (Figure 3-4) is a strategy where lost or damaged frames are re-sent. A buffer is maintained at the receiving end that buffers the entire frame after the lost one. When the sender identifies the problem, it retransmits the lost frames.

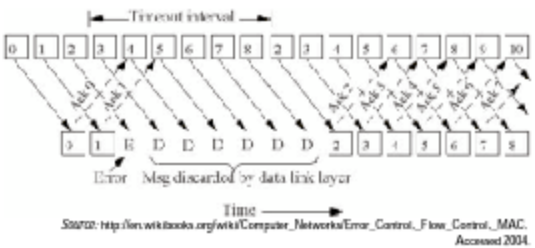


Figure 3-3 This shows the go-back-*n* technique.

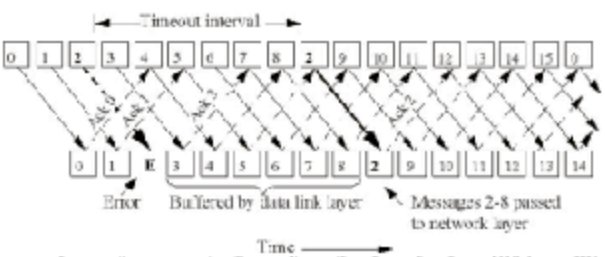


Figure 3-4 Selective repeat retransmits only those frames that have been lost.

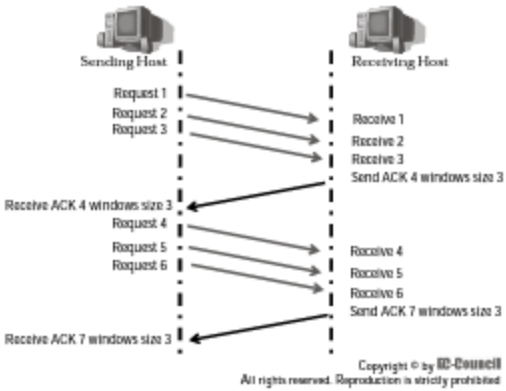


Figure 3-5 Positive acknowledgment involves sending an ACK when the data packets are received.

Acknowledgment

Reliable delivery means that when a stream of data is sent from one device to another, the data will reach the destination without any loss or duplication. Positive acknowledgment with retransmission guarantees the reliable delivery of data. In positive acknowledgment (Figure 3-5), the receiving end communicates with the sender and sends an ACK when the data are received. A record is maintained for each transmitted packet on the sender's end, and the sender expects an acknowledgment from the receiving end. A timer is maintained when a segment is transmitted, and the segment is retransmitted if the timer expires before the ACK arrives.

In Figure 3-5, the sender transmits data packets 1, 2, and 3. The receiver sends a receipt for the packets along with a request for packet 4. When the sender encounters the ACK, it sends packets 4, 5, and 6. If packet 5 doesn't arrive at the destination, the receiver sends a negative acknowledgment with a request to resend packet 5. The sender then retransmits packet 5, receives the ACK, and continues the transmission.

TCP provides sequencing of the segments in the forward reference acknowledgment. Every segment is numbered before the transmission. TCP reassembles the segments into a complete message at the destination end. Any unacknowledged segments in a given period of time will result in retransmission.

TCP Data-Packet Structures

Transmission Control Protocol (TCP)

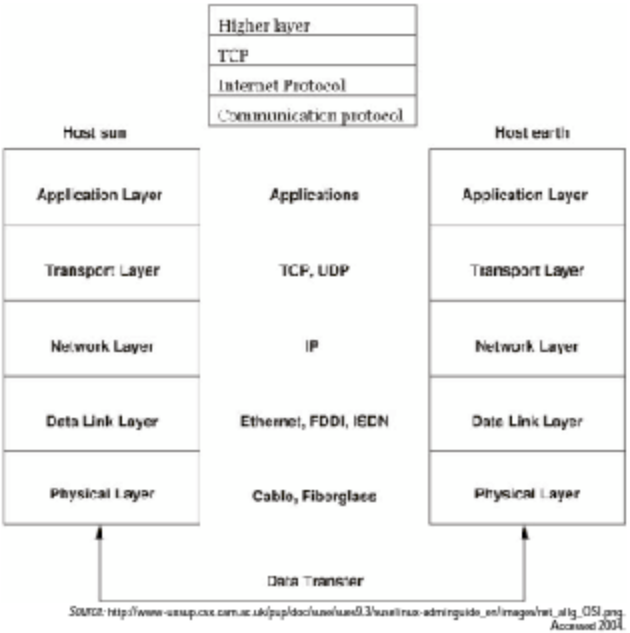
The Defense Advanced Research Projects Agency (DARPA) first developed the TCP/IP protocol suite. TCP is a connection-oriented protocol with point-to-point connectivity. The TCP/IP protocol had an important role in the development of the Internet. TCP/IP is often referred to as the Department of Defense protocol suite or the Internet Protocol suite. TCP/IP is called the backbone of the Internet because of its efficiency in transferring packets from one network to another. It works mostly in packet-switched networks. It is designed to fit into a layered hierarchy of protocols. It also provides reliable interprocess communication.

Protocol Layering

Figure 3-6 shows how protocols are layered in TCP/IP.

TCP Header Format

A TCP segment is transmitted in the same way as an Internet datagram. A datagram (the name of the data packet at the Internet layer) is a unit of information, containing both the data and addressing information, to



Source: http://www-uxsup.csx.cam.ac.uk/pub/doc/suse/sun9.3/suselinux-adminguide_en/images/net_stk_OSI.png. Accessed 2003.

Figure 3-6 Protocols are layered in the TCP/IP suite.

be transferred over a network. A TCP segment carries information such as the source and destination addresses. The TCP header structure (Figure 3-7) contains much information about the packet being transmitted, and the options in the TCP header are useful in the transfer of packets. The size of the TCP header is a multiple of 32 bits.

Source Address The source port is 16 bits.

Destination Address The destination port is 16 bits.

Sequence Number The sequence number is 32 bits. If SYN is present, the sequence number is the initial sequence number (ISN), and the first data octet is ISN + 1.

Acknowledgment Number When this field is set, it contains the value of the next sequence number of the acknowledgment that the sender is expecting to receive from the receiving end. After a connection, the acknowledgment is always forwarded to the sender.

Data Offset The data offset is 4 bits. This indicates the beginning of the data.

Reserved This field size is 6 bits and is reserved for future use.

Control Bits This field size is 6 bits and contains the following, from left to right:

- *U (URG)*: Urgent flag
- *A (ACK)*: Acknowledgment flag
- *P (PSH)*: Push function
- *R (RST)*: For resetting the connection

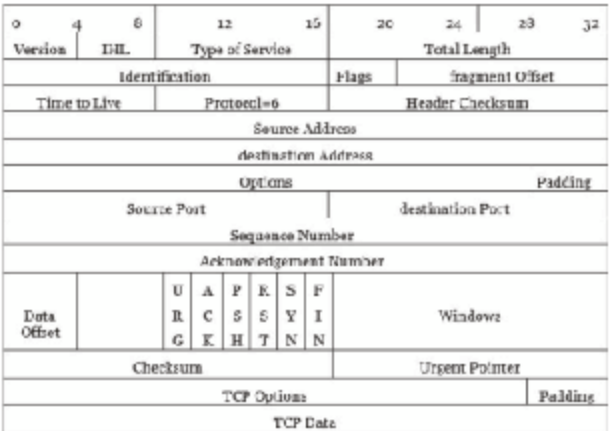


Figure 3-7 This is the TCP header structure.

- *S (SYN)*: Synchronize sequence number
- *F (FIN)*: No more data from the sender side

Window Size The window size is 16 bits. It is the number of data octets the sender is willing to accept. It begins with the octet indicated in the acknowledgment field.

Checksum A ***checksum*** is a value included in a header to ensure that the data has been transferred without error. The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header and text. If a segment contains an odd number of header and text octets to be checksummed, the last octet is padded on the right with zeros to form a 16-bit word for checksum purposes. The pad is not transmitted as part of the segment. While computing the checksum, the checksum field itself is replaced with zeros.

Options The size of the options may vary. It is necessary to pad the TCP header with zeros so that the segment will end at a 32-bit word boundary.

Data It carries the application data from the sender to the receiver.

Implementing User-Level Commands

TCP Interface

TCP interfaces with user or application processes (user/TCP interface) and on the other side to a lower-level protocol, such as Internet Protocol (TCP/lower-level interface).

The interface between an application process and TCP consists of a set of calls much like the calls an operating system provides to an application process for manipulating files. For example, there are calls to open and close connections and to send and receive data on established connections. It is also expected that TCP can asynchronously communicate with application programs. Although considerable freedom is permitted to TCP implementers to design interfaces that are appropriate to a particular operating system environment, a minimum functionality is required at the TCP/user interface for any valid implementation.

The interface between TCP and lower-level protocols is essentially unspecified except that it is assumed there is a mechanism whereby the two levels can asynchronously pass information to each other. Typically,

one expects the lower-level protocol to specify this interface. TCP is designed to work in a very general environment of interconnected networks. The lower-level protocol assumed throughout this document is the Internet Protocol.

User/TCP Interface

To ensure compatibility, all TCP implementations provide a minimum set of services. TCP provides a minimum set of services to guarantee that the same protocol hierarchy is supported by all TCP implementations.

TCP User Commands The TCP user-interface notations are the same as higher-level-language function calls. User commands can only define the supported functions for interprocess communications; the individual implementations define their own format and basic functions. In some implementations, a connection is automatically opened in the first send or receive a user issues for a given connection.

OPEN

```
Format: OPEN (local port, foreign socket, active/passive
[, timeout] [, precedence] [, security/compartment] [, options])

-> local connection name
```

The local TCP checks the authority of the process to use the connection specified. The local network and the TCP identifier for the source address are supplied by TCP or by the lower-level protocol; no process can masquerade as another without the collusion of TCP.

If the active/passive flag is set to passive, then the call is to listen for an incoming connection. A passive OPEN may have either a fully specified foreign socket to wait for a particular connection or an unspecified foreign socket to wait for any call. A fully specified passive call can be made active by the subsequent execution of a send. On an active OPEN command, TCP will begin the procedure to synchronize (i.e., establish) the connection at once.

The timeout specifies the timeout of the data; if the data are not delivered within the time limit, then TCP will abort the transfer. The default time limit is 5 minutes.

TCP will return a local connection name to the user. The local connection name can then be used as a shorthand term for the connection defined by the `<local socket, foreign socket>` pair.

SEND

```
Format: SEND (local connection name, buffer address, byte
count, PUSH flag, URGENT flag [,timeout])
```

This call sends the data in the user buffer to the intended connection. Before making a call to SEND, the connection should be opened or it will generate an error. In some cases, if the SEND call is detected, the connection is opened. If an unauthorized user wants to send, an error is returned to that user.

When the PSH flag is set, the data transmission is sent to the receiver. The PSH bit is the last bit to be set in the TCP segment created from the buffer. If it is not set, the data transmitted are combined with the subsequent send to increase the efficiency of the transmission.

If the URGENT flag is set, the transmitted segment will have an urgent pointer set in it. The purpose of the data is to inform the receiver to process the URGENT data and to indicate to the receiver when all the data has arrived.

The number of times the sending user's TCP signals urgent data will not necessarily be equal to the number of times the receiving user will be notified of the presence of urgent data. Users who make use of OPEN without specifying the foreign socket can make use of SEND without knowing the foreign-socket address. However, if a SEND is attempted before the foreign socket is set, an error will be returned. Users can use the STATUS call to determine the status of the connection. In some implementations, TCP may notify the user when an unspecified socket is bound.

RECEIVE

```
Format: RECEIVE (local connection name, buffer address,
byte count) -> byte count, urgent flag, push flag
```

This command allocates a receiving buffer associated with the specified connection. If no OPEN precedes this command or the calling process is not authorized to use this connection, an error is returned.

The RECEIVE call does not return control to the calling program and may be subject to deadlocks. Many RECEIVE commands can be run simultaneously. RECEIVE notifies the calling program that a buffer is filled or a PSH has been used.

If the buffer is filled and the PSH flag is used, the PSH flag will not be set in response to the RECEIVE. The buffer will be filled with as much as it can store. If the PSH is seen before the buffer is filled, the buffer is returned partially filled and the PSH is indicated.

When urgent data arrive, the TCP-to-user signal is given as soon as they arrive. The receiving user is in URGENT mode. When URGENT mode is off, the RECEIVE call returns all the urgent data and the user turns off urgent mode.

CLOSE

```
Format: CLOSE (local connection name)
```

This command closes the specified connection. If the calling process is not authorized for this call, an error is returned. It is a good practice to precede a CLOSE with a SEND. CLOSE means "I have no data to send," but it does not mean "I will not receive more." The user can close the connection anytime. CLOSE also implies a PSH.

STATUS

```
Format: STATUS (local connection name) -> status data
```

This is an implementation-dependent user command and could be excluded without adverse effect. Information returned would typically come from the TCB (transmission control block) associated with the connection.

This command returns a data block containing the following information:

- Local socket
- Foreign socket
- Local connection name
- Receive window
- Send window
- Connection state
- Number of buffers awaiting acknowledgment
- Number of buffers pending receipt
- Urgent state
- Precedence
- Security/compartment
- Transmission timeout

Depending on the state of the connection, or on the implementation itself, some of this information may not be available or meaningful. If the calling process is not authorized to use this connection, an error is returned. This prevents unauthorized processes from gaining information about a connection.

ABORT

```
Format: ABORT (local connection name)
```

This command causes all pending SENDs and RECEIVEs to be aborted, the TCB to be removed, and a special reset message to be sent to the TCP on the other side of the connection. Depending on the implementation, users may receive abort indications for each outstanding SEND or RECEIVE, or may simply receive an abort acknowledgment.

TCP-To-User Messages It is assumed that the operating system environment provides a means for TCP to asynchronously signal the user's program. When TCP does signal a user program, certain information is passed to the user. Often in the specification, the information will be an error message. In other cases, there will be information relating to the completion of processing a SEND, RECEIVE, or other user call.

The following information is provided:

- *Local connection name*: Always
- *Response string*: Always
- *Buffer address*: SEND and RECEIVE
- *Byte count (counts bytes received)*: RECEIVE PSH flag, RECEIVE URG flag, RECEIVE

TCP/Lower-Level Interface

TCP calls the lower-level protocol module to send and receive information over the network. If the lower-level module is Internet Protocol, it specifies the Type of Service and Time to Live fields. TCP uses the following settings for these parameters:

```
Type of Service = Precedence: routine, Delay: Normal, Throughput:
Normal, Reliability: normal; or 00000000.

Time to Live = one minute, or 00111100.
```

The maximum lifetime of a segment is two minutes.

If the lower-level Internet Protocol and source routing are used, the interface communicates the route interface information. It also preserves the return route to answer the connection request.

Event Processing The events that occur in this interface can be categorized into three categories:

- User calls
- Arriving segments
- Timeouts

- User calls
- OPEN
- SEND
- RECEIVE
- CLOSE
- ABORT
- STATUS

- Arriving Segments
- SEGMENT ARRIVES

- Timeouts
- USER TIMEOUT
- RETRANSMISSION TIMEOUT
- TIME-WAIT TIMEOUT

OPEN Call

`CLOSED STATE` (i.e., TCB does not exist)

OPEN creates a new transmission control block (TCB) to hold the state information of the connection. It fills in the local-socket identifier, foreign socket, precedence, security/compartment, and user-timeout information. If the caller does not have access to the local socket specified, this call returns "error: connection illegal for this process." If there is no room to create a new connection, it returns "error: insufficient resources."

```
OPEN Call

SYN-SENT STATE

SYN-RECEIVED STATE

ESTABLISHED STATE FIN-WAIT-1 STATE

FIN-WAIT-2 STATE
```

CLOSE-WAIT STATE

CLOSING STATE

LAST-ACK STATE

TIME-WAIT STATE

SEND Call

CLOSED STATE (i.e., TCB does not exist)

If the user does not have access to the connection, then this call returns "error: connection illegal for this process." Otherwise, it returns "error: connection does not exist."

LISTEN STATE

If active is specified and the foreign socket is specified, then the connection is changed from passive to active, selecting an ISS. The call sends a SYN segment, sets SND.UNA to ISS and SND.NXT to ISS + 1. It enters the SYN-SENT state. If no room is available to queue the request, the call responds with "error: insufficient resource"; if the foreign socket is not specified, then "error: foreign socket unspecified" is returned.

SYN-SENT STATE

SYN-RECEIVED STATE

The call queues the data for transmission after entering the ESTABLISHED state. If there is no space to queue, it responds with "error: insufficient resources."

ESTABLISHED STATE

CLOSE-WAIT STATE

The call segmentizes the buffer and sends it with a piggybacked acknowledgment (acknowledgment value = RCV.NXT). If there is insufficient space to remember this buffer, it simply returns "error: insufficient resources."

If the urgent flag is set, then SND.UP <- SND.NXT − 1 and the call sets the urgent pointer in the outgoing segments.

SEND Call

FIN-WAIT-1 STATE

FIN-WAIT-2 STATE

CLOSING STATE

LAST-ACK STATE

TIME-WAIT STATE

The call returns "error: connection closing" and does not service the request.

RECEIVE Call

CLOSED STATE (i.e., TCB does not exist)

If the user does not have access to the connection, the call returns "error: connection illegal for this process." Otherwise, it returns "error: connection does not exist."

LISTEN STATE

SYN-SENT STATE

SYN-RECEIVED STATE

The call queues the data for processing after entering the ESTABLISHED state. If there is no room to queue this request, the call responds with "error: insufficient resources."

ESTABLISHED STATE

FIN-WAIT-1 STATE

FIN-WAIT-2 STATE

If insufficient incoming segments are queued to satisfy the request, the call queues the request. If there is no queue space to remember the RECEIVE, the call responds with "error: insufficient resources."

The call reassembles queued incoming segments into the receive buffer and returns control to the user. It marks "push seen" (PSH) if this is the case.

If RCV.UP is set in advance of the data currently being passed to the user, the call notifies the user of the presence of urgent data.

When TCP takes responsibility for delivering data to the user, an acknowledgment must be sent. How the acknowledgment is constructed is described below in the discussion of processing an incoming segment.

```
RECEIVE Call

CLOSE-WAIT STATE
```

Since the remote side has already sent a FIN, RECEIVEs must be satisfied by data already on hand but not yet delivered to the user. If no data are awaiting delivery, the RECEIVE will get an "error: connection closing" response. Otherwise, any remaining data can be used to satisfy the RECEIVE.

```
CLOSING STATE

LAST-ACK STATE

TIME-WAIT STATE

Return "error: Connection closing."
```

CLOSE Call

```
CLOSED STATE (i.e., TCB does not exist)
```

If the user does not have access to the connection, the call returns "error: connection illegal for this process." Otherwise, it returns "error: connection does not exist."

```
LISTEN STATE
```

Any outstanding RECEIVEs are returned with "error: closing" responses. The call deletes the TCB, enters the CLOSED state, and returns.

```
SYN-SENT STATE
```

The call deletes the TCB and returns "error: closing" responses to any queued SENDs or RECEIVEs.

```
SYN-RECEIVED STATE
```

If no SENDs have been issued and there are no pending data to send, then the call forms a FIN segment and sends it, and enters the FIN-WAIT-1 state; otherwise, it queues the data for processing after entering the ESTABLISHED state.

```
ESTABLISHED STATE
```

The call queues this until all preceding SENDs have been segmentized; it then forms a FIN segment and sends it. It enters the FIN-WAIT-1 state.

```
FIN-WAIT-1 STATE

FIN-WAIT-2 STATE
```

Strictly speaking, this is an error and should receive an "error: connection closing" response. An "ok" response would be acceptable, too, as long as a second FIN is not transmitted (the first FIN may be retransmitted though).

```
CLOSE Call

CLOSE-WAIT STATE
```

The call queues this request until all preceding SENDs have been segmentized; then it sends a FIN segment and enters the CLOSING state.

```
CLOSING STATE

LAST-ACK STATE

TIME-WAIT STATE
```

The call responds with "error: connection closing."

ABORT Call

`CLOSED STATE` (i.e., TCB does not exist)

If the user should not have access to the connection, the call returns "error: connection illegal for this process." Otherwise, it returns "error: connection does not exist."

`LISTEN STATE`

Any outstanding RECEIVEs should be returned with "error: connection reset" responses. The call deletes the TCB, enters the CLOSED state, and returns.

`SYN-SENT STATE`

All queued SENDs and RECEIVEs should be given "error: connection reset" notifications. The call deletes the TCB, enters the CLOSED state, and returns.

`SYN-RECEIVED STATE`

`ESTABLISHED STATE`

`FIN-WAIT-1 STATE`

`FIN-WAIT-2 STATE`

`CLOSE-WAIT STATE`

`Send a RESET segment:`

`<SEQ=SND.NXT><CTL=RST>`

All queued SENDs and RECEIVEs should be given "error: connection reset" notifications; all segments queued for transmission (except for the RST formed above) or retransmission should be flushed. The call deletes the TCB, enters the CLOSED state, and returns.

`CLOSING STATE`

`LAST-ACK STATE`

`TIME-WAIT STATE`

The call responds with "ok" and deletes the TCB, enters the CLOSED state, and returns.

STATUS Call

`CLOSED STATE` (i.e., TCB does not exist)

If the user should not have access to the connection, the call returns "error: connection illegal for this process." Otherwise, it returns "error: connection does not exist."

`LISTEN STATE`

The call returns "state = LISTEN" and the TCB pointer.

`SYN-SENT STATE`

The call returns "state = SYN-SENT" and the TCB pointer.

`SYN-RECEIVED STATE`

The call returns "state = SYN-RECEIVED" and the TCB pointer.

`ESTABLISHED STATE`

The call returns "state = ESTABLISHED" and the TCB pointer.

`FIN-WAIT-1 STATE`

The call returns "state = FIN-WAIT-1" and the TCB pointer.

`FIN-WAIT-2 STATE`

The call returns "state = FIN-WAIT-2" and the TCB pointer.

`CLOSE-WAIT STATE`

The call returns "state = CLOSE-WAIT" and the TCB pointer.

```
CLOSING STATE
```

The call returns "state = CLOSING" and the TCB pointer.

```
LAST-ACK STATE
```

The call returns "state = LAST-ACK" and the TCB pointer.

```
STATUS Call
TIME-WAIT STATE
```

The call returns "state = TIME-WAIT" and the TCB pointer.

Understanding TCP Algorithms

Algorithms in TCP

Appropriate Byte Counting (ABC)

Appropriate Byte Counting (ABC) is an algorithm for increasing TCP's congestion window (CWND) to improve performance and security. The ***congestion window*** is typically a value that indicates the maximum amount of data that can be sent out on a connection without an acknowledgment. When a connection is first established, the congestion window is set up as the size of one segment. The sender maintains the window and increments it for every ACK received. Instead of increasing the TCP's congestion window based on the quantity of acknowledgments that arrive at the data sender, the congestion window is increased by the number of bytes that are acknowledged. This algorithm increases performance by minimizing the impact of delayed acknowledgment on the growth of CWND. The algorithm makes CWND growth proportionate to the capacity of the network path, providing a more measured response to acknowledgment that covers only a small amount of data compared to ACK counting. This improves the performance and prevents inappropriate growth in response to a misbehaving receiver. The other side of the coin in some cases is that the modified CWND growth algorithm can create a larger burst of network segments on the network.

Additive Increase Multiplicative Decrease (AIMD)

In the absence of congestion, the sender of a TCP segment increases its window by a maximum of one packet per round-trip time. When the congestion occurs after its indication, the TCP sender decreases its congestion window by half.

Selective Acknowledgment (SACK)

The SACK algorithm allows the receiver to acknowledge that all segments have arrived successfully, so the sender has to send only the packets that were not delivered or were lost. The algorithm has two options: the first is an enabling option where SACK is permitted, which can be sent in a SYN segment which indicates that the SACK option can be used only once when the connection is established. The second is the SACK option itself, which can be sent when the established connection gives permission.

TCP Friendly Rate Control (TFRC)

This mechanism is used for the unicast flow of information from source to the destination host operating in the Internet environment. It manages a reasonable flow of data when hosts are competing for bandwidth, but it has much lower variation of throughput with respect to time when compared with TCP/IP, making it a more suitable method for streaming videos, where the smooth flow and sending rate are important. It is designed for applications that use a fixed sending rate but vary their packet size in response to congestion.

TCP Checksum Calculation

The TCP checksum calculation involves a pseudoheader to be added to the TCP header. It includes the following:

- *IP source address*: 4 bytes
- *IP destination address*: 4 bytes

- *TCP protocol*: 2 bytes
- *TCP length*: 2 bytes

Then the checksum is calculated from all the octets of the pseudoheader, TCP header, and data. If an odd number of octets are in the data, the end of the data is padded with zeros. The pseudoheader and the padding are not transmitted with the packet.

In the example code, `u16 buff[]` is an array containing all the octets in the TCP header and `data`. `u16 len_TCP` is the length (number of octets) of the TCP header and data. `BOOL padding` is 1 if the data has an even number of octets and is 0 if the data has an odd number.

`u16 src_addr[4]` and `u16 dest_addr[4]` are the IP source and destination address octets.

```
/*
*****************************************************************************
* Function: TCP_sum_calc()
*****************************************************************************
* Description:
Calculate TCP checksum
*****************************************************************************
*/
typedef unsigned short u16;
typedef unsigned long u32;
u16 TCP_sum_calc(u16 len_TCP, u16 src_addr[],u16 dest_addr[], BOOL padding,
u16 buff[])
{
u16 prot_TCP=6;
u16 padd = 0; u16 word16; u32 sum;
// Find out if the length of data is even or odd number. If odd,
// add a padding byte = 0 at the end of packet if (padding&1 == 1){
padd = 1;
buff[len_TCP] = 0;
}
//initialize sum to zero sum = 0;
// make 16 bit words out of every two adjacent 8 bit words and
// calculate the sum of all 16 vit words
for (i = 0;i < len_TCP + padd;i = i + 2){
word16 = ((buff[i] << 8)&0xFF00) + (buff[i + 1]&0xFF);
sum = sum + (unsigned long)word16;
}
// add the TCP pseudo header which contains:
// the IP source and destinationn addresses,
for (i = 0;i < 4;i = i + 2){
word16 = ((src_addr[i] << 8)&0xFF00) + (src_addr[i + 1]&0xFF);
sum = sum + word16;
```

```
}
for (i = 0;i < 4;i = i + 2){
word16 = ((dest_addr[i] << 8)&0xFF00) + (dest_addr[i + 1]&0xFF);
sum = sum + word16;
}
// the protocol number and the length of the TCP packet
sum = sum + prot_TCP + len_TCP;
// keep only the last 16 bits of the 32 bit calculated sum and add the carries
while (sum >> 16)
sum = (sum & 0xFFFF)+(sum >> 16);
// Take the one's complement of sum sum = ~sum;
return ((unsigned short) sum);
}
//
```

Performance Estimation in TCP

Round-Trip Time Estimation

When a host transmits a TCP packet to the peers in the network, it waits for the period of time for the acknowledgment. If the reply does not come within the given period of time, the packet is assumed to have been lost and the packet is retransmitted to the destination. The question is "How long do we have to wait?" In an Ethernet, the acknowledgment comes within a part of a microsecond. In the Internet, the acknowledgment comes within a second or two. Monitoring the normal exchange of the data packets and estimating how long it will take is done by the TCP implementation. This is called the *round-trip time estimation*. Round-trip time is the most important parameter in the measurement of performance; especially if it is done on a large transfer of the data.

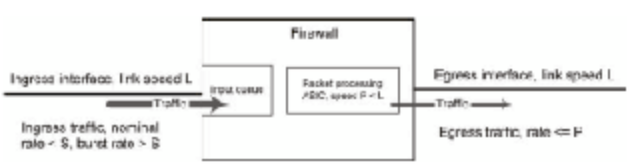
Problems Related to TCP

Packet Replication Packets are retransmitted over the network if there is congestion or if the packet is lost. When the packet is retransmitted, the packet is replicated.

Checksum Error The checksum is part of the TCP header field. The purpose of a checksum is to ensure data integrity. A failed checksum indicates a problem with the data in a packet. In this case, the packet has to be retransmitted.

Bottleneck Bandwidth Bottleneck bandwidth is the rate at which all bandwidth is used and even a single additional packet cannot be accommodated. The self-interference time can be calculated if the bottleneck bandwidth is known. It is good to measure at the buffer of the receiver.

Packet Loss Packet loss (Figure 3-8) is sometimes due to firewalls and network aggregation in devices that have small buffers. Other times, dirty links and hardware failure cause packet loss. Packet loss also can also



Source: http://www.es.net/pub/esnet-doc/TCP-Bulk-Data-Transfer.doc. Accessed 2004.

Figure 3-8 This depicts packet loss.

happen if the size of the firewall buffer is small, the network interface operates at a speed greater than the firewall can handle, and the incoming packet burst is too large.

Internet Protocol (IP)

The Internet Protocol (IP) is the method by which data is sent from one computer to another over a packet-switched network. The Internet Protocol uses datagrams for transmitting data blocks from the source to the destination. The source and the destination are identified by a fixed-length address. The Internet Protocol provides the facilities of fragmentation and defragmentation for large datagrams.

The Internet Protocol datagram has two basic features:

1. Fragmentation
2. Addressing

To transmit the datagram to the destination address, the Internet Protocol looks for the destination address in the header. The process of selecting the path from the sender to the receiver is called routing.

There are common rules for the interpretation of the address fields, fragmentation, and reassembling of an Internet Protocol datagram.

IP Header Format

Figure 3-9 shows the IP header format.

Version The version field is 4 bits. The version field indicates the version of IP used, such as IPv4 or IPv6.

IHL The IHL is the Internet header length. It is the length of the Internet header in 32-bit words.

Type of Service This field lists the quality of service desired. High-precedence traffic is passed first.

- *Precedence:* Precedence is the measure of the importance of the datagram.
- *Delay:* Datagrams that need to be delivered promptly have low delay settings.
- *Throughput:* This parameter is used to record the rate of the data transfer.
- *Reliability:* A higher level of effort is asked for to ensure delivery of datagrams with this indication.

The following describe the meanings of the bits for this field:

- *Bits 0–2:* Precedence
- *Bit 3:* 0 = Normal delay, 1 = Low delay
- *Bit 4:* 0 = Normal throughput, 1 = High throughput
- *Bit 5:* 0 = Normal reliability, 1 = High reliability
- *Bits 6–7:* Reserved for future use

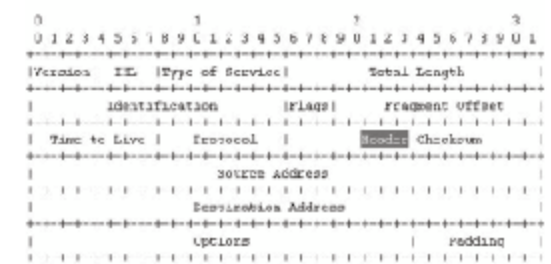


Figure 3-9 This shows the format of the IP header.

Total Length The length of the datagram is measured in octets, including the Internet header length and the data. The length of a datagram in this field is up to 65,535 octets. A minimum of 576 octets is to be accepted by the host. This number was selected so that the data can be sent in 512 bits and the remaining 64 bits are kept for the header.

Identification The identification field is 16 bits. It helps in reassembling the fragments of the datagram.

Flags This field is 3 bits. The following are the meanings of the bits:

- *Bit 0*: Reserved; must be zero
- *Bit 1*: (DF) 0 = May fragment, 1 = Do not fragment
- *Bit 2*: (MF) 0 = Last fragment, 1 = More fragments

Fragment Offset The fragment offset field is 13 bits. This field indicates the position of the fragment in the datagram. It is measured in octets of 8 units each (64 bits). The first fragment has an offset of 0.

Time-To-Live The time-to-live field is 8 bits. This field specifies the period of time a datagram is allowed to live on the network. If the value in this field is 0, then the datagram is destroyed at that time. Every module that processes a datagram decreases the value of the time-to-live field. The aim behind using the time-to-live field is to discard undeliverable packets.

Protocol This field is 8 bits. It indicates the next level of protocol used in the Internet datagram. The value for the protocol is given by the number assigned.

Header Checksum The header checksum is 16 bits, since there are some header fields that change every time a header is processed.

Source Address The source address is 32 bits and gives the address of the sender.

Destination Address The destination address is 32 bits and gives the address of the destination.

Options Options may or may not appear in the header, but all modules must implement ways to handle the options. There are some areas where the security option is required in all datagrams. This field is variable in length and may contain zero or more options. There are two cases for the format of this field:

- *Case 1*: A single option-type octet
- *Case 2*: An option-type octet, an option-length octet, and the actual option-data octets

The option-lengths octet includes the lengths of the option-type octet, the option-lengths octet, and the option-data octet.

The option-type octet has the following three fields:

- 1-bit copied flag
- 2-bit option class
- 5-bit option number

The copied flag indicates that this option is copied into all fragments on fragmentation:

- 0 = not copied
- 1 = copied

The following are the option classes:

- 0: Control
- 1: Reserved for future use
- 2: Debugging and measurement
- 3: Reserved for future use

IP Data-Packet Structures

IP Datagram

Maximum Transfer Unit

Network devices have to know about the technology on an IP network and its capacity to handle the traffic load. The limit an IP network is capable of supplying a datagram is called the maximum transmission unit (MTU). If a message is sent across the Internet through the IP layer, the size of the datagram is determined first. This size is checked against the MTU of the underlying network. If the size of the potential datagram is larger than the MTU, the IP layer will fragment the message.

Fragmentation

Some physical networks have smaller MTUs than others. Imagine a source device that wants to send an IP message that is 12,000 bytes long, but the MTU is 3,300 on the local network. The message has to be divided into four fragments for transmission. Figure 3-10 shows how the MTU can cause fragmentation.

Fragmentation introduces several issues:

- *Sequencing and placement*: IP message fragments are sent in sequential order, but they may arrive at the destination in a completely different order. The receiving device must be capable of rearranging the fragments into sequential order.
- *Separation of the fragmented message*: The source device may send one or more fragmented messages. Or it can send multiple datagrams, and the receiving device has to be able to put the multiple datagrams back together.
- *Completion*: The destination device must be available and prepared to receive data when it receives the fragments and when it starts the reassembly of the fragments.

Encapsulation ***Encapsulation*** is the way data moves through the protocol stack as it is prepared for transmission. Each layer adds its header information to the data as it moves down the protocol stack. The idea of encapsulation is analogous to sending a letter enclosed in an envelope. Only the destination name and address is on it. Data from the application layer are encapsulated and sent to the transport layer. The data segment is then passed from the transport-layer protocol TCP or UDP to IP. The data packets have the TCP or UDP header already, and this header is then encapsulated in the IP datagram. After the encapsulation of the data into the IP datagram, it is passed as a frame to the data-link layer for further transmission.

Delivery The job of the Internet Protocol is the transmission of messages from higher-layer protocols. Messages are packed and addressed and, if necessary, fragmented. Then they are delivered to the destination.

IP datagram delivery is divided into two types:

- *Direct delivery*: When the source and destination are on the same physical network, the datagrams are directly delivered.
- *Indirect delivery*: When the source and destination are not on the same network, then the datagram is delivered indirectly. The source device has to send the datagram through one or more intermediate devices.

Routing IP allows devices to connect over the Internet using indirect delivery. All this communication is through routers. It is totally dependent on the intermediate devices that connect thousands of networks. The datagram

Figure 3-10 Going from a network with a larger MTU to a network with a smaller MTU causes packet fragmentation.

follows the path from one router to another until it reaches the destination device. The packets from one message may not all follow the same path, and it is up to the destination system to reassemble the message using information in the packets. The term for this strategy is ***next-hop routing***.

Encapsulating Security Payload (ESP)

ESP is a mechanism that provides integrity and confidentiality to an IP datagram. Depending on the type of algorithm used, it can also provide authentication. The authentication header (AH) in IP can also provide nonrepudiation if it is used with some authentication algorithm. Users who require integrity and authentication without confidentiality use the IP authentication header instead of ESP. ESP provides confidentiality and integrity by encrypting data that is to be protected and places that encrypted data in the data portion of the IP ESP. Based on the requirements of the user, the ESP mechanism can be used to encrypt either a transport-layer segment or an entire IP datagram.

Modes in ESP

Tunnel Mode In tunnel-mode ESP, the original IP datagram is inserted into the encrypted portion of ESP. The entire ESP frame is then placed within a datagram that has an unencrypted IP header. The information stored in the unencrypted IP header is then used to route the secure datagram from the origin to the destination. The unencrypted IP routing header can also be placed in between the IP header and ESP.

Transport Mode In transport-mode ESP, the ESP header is inserted in the IP datagram before the transport-layer protocol header. Without the encrypted IP header or IP options, bandwidth is conserved.

Understanding IPv6

IPv6

IPv6 is Internet Protocol version 6 and is the successor to IPv4. IPv6 has increased the address size from 32 bits to 128 bits. The scalability of multicast routing is improved by adding a scope field to the multicast address.

The labeling of IPv6 packets also allows for specific sender requests requiring special handling, such as a specific quality of service or real-time service.

IPv6 Header Format

Figure 3-11 depicts the IPv6 header format.

Version This field contains the version of the Internet Protocol, which in this case is 6.

Priority This field enables a particular user to identify the priority of the delivery of a packet on the network. The priority values are then divided into ranges, where the source provides congestion-control features.

Flow Label The source uses the flow-label field to label those datagrams for which the source requires special handling by the IPv6 router. The flow has its own identity based on its source address and the nonzero flow label.

Payload Length The length of the payload packet is in octets.

Figure 3-11 This is the IPv6 header format.

Next Header This field indicates the type of header immediately following the IPv6 header.

Hop Limit This field is an 8-bit integer that is decremented by 1 when the node forwards a packet. When the hop limit hits zero, the packet is discarded.

Source Address The source address is a 128-bit address denoting the originator of the packet.

Destination Address The destination address is a 128-bit address that denotes the intended recipient of the packet.

Packet Tunneling

IPv6 tunneling is a technique by which a virtual link is established between two nodes transmitting data packets as payloads of IPv6 packets. These virtual links are called IPv6 tunnels, which seem like point-to-point links that act as link-layer protocols. These two IPv6 nodes have specific roles: one node encapsulates the original packets received from the other nodes or from itself, and then the tunnel packet is sent to the tunnel. The encapsulating node is called the tunnel entry-point node. The decapsulator node is called the tunnel exit point and is the destination of the packet.

IP Multicasting

IP multicasting is a technology used to conserve bandwidth by delivering a single stream of information to thousands of recipients. Multicasting is used in many applications like videoconferencing, dedicated communications, software distribution, and stock quotes. It is a technique for delivering information to many receivers without adding additional headers and using the least network bandwidth possible.

Multicast Group Concept In the multicast group concept, an arbitrary group of receivers receive a data stream, if they have an interest in receiving that particular data stream. Those hosts interested in receiving the data stream have to join that group using the IGMP protocol.

IP Multicast Address A multicast address specifies the group of hosts who have joined a group and want to receive the data stream.

Hop-By-Hop Option

The hop-by-hop option is used to carry optional information. This optional information is scanned and examined by every node that the packet passes through on its way to destination. Figure 3-12 shows the format of this field.

- *Next header*: This field is 8 bits and identifies the type of header that immediately follows the hop-by-hop option header.
- *Hdr Ext Len*: This field is an 8-bit unsigned integer and specifies the length of the hop-by-hop option header.
- *Options*: The options field is a large field that contains optional information. Its length is always a multiple of 8 bits.

Figure 3-12 This is the format of the hop-by-hop option field.

Chapter Summary

- The TCP/IP suite has four layers: the application layer, the transport layer, the Internet layer, and the network-interface layer.
- The network-interface layer sends and receives packets to and from the network medium.
- The Internet layer takes care of machine-to-machine communication.
- At the transport layer, communication is established with other connected systems.
- The application layer defines protocols for use by users for data transfer and other services.
- The TCP/IP protocol suite defines a number of methods to ensure the reliability and speed of data transfer.
- Windowing and acknowledgment between systems ensure that data packets are all transferred correctly.
- When packets of data are lost, they are retransmitted and the destination site must reassemble the whole message.
- IP version 6 increases the number of bits used for addresses, thus increasing the usable address space.

Review Questions

1. List the function of each layer in TCP/IP.

2. What is the one-bit sliding window protocol?

3. Why is a checksum used in the TCP header?

4. What is the function of the active and passive flags of the OPEN command in TCP user commands?

5. Explain the URGENT flag in SEND command of TCP user commands.

6. Explain checksum error and bottleneck bandwidth.

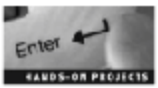
7. Explain the data fragmentation process.

8. Explain the modes in ESP.

9. What is a tunnel entry point?

10. Explain IP multicasting.

Hands-On Projects



1. Use Network Protocol Analyzer to analyze, debug, maintain, and monitor local networks and Internet connections.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the Network Protocol Analyzer program (Figure 3-13).

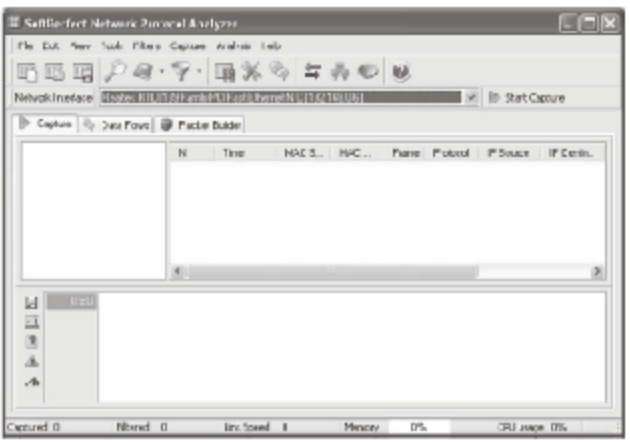


Figure 3-13 Launch Network Protocol Analyzer.

- To start the data capture, choose **Capture**, then **Start Capture** (Figure 3-14).

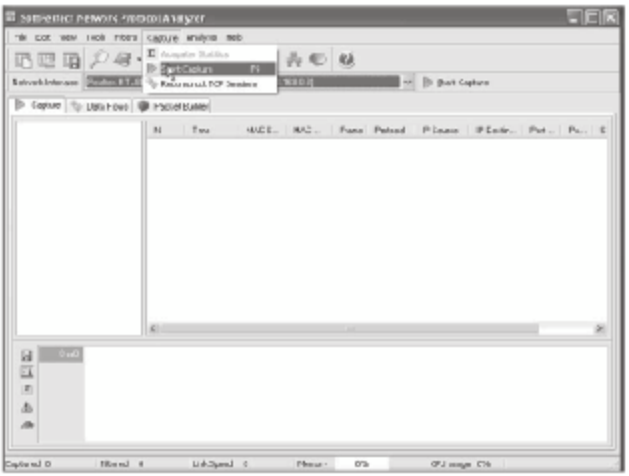


Figure 3-14 Choose **Capture**, then **Start Capture**.

- The captured packets are shown in Figure 3-15.

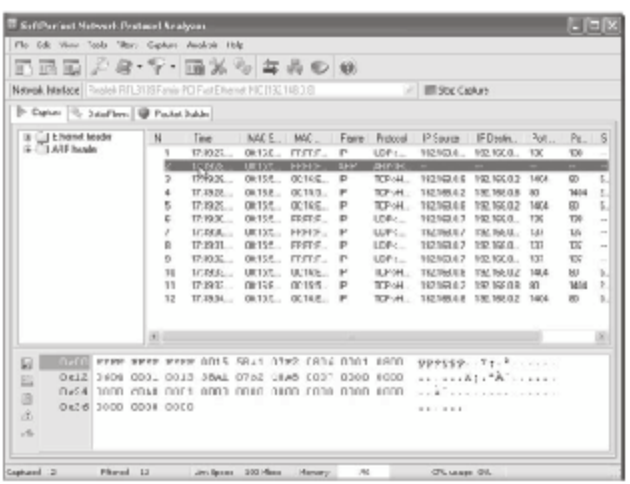


Figure 3-15 These are the packets Network Protocol Analyzer has captured.

- To save the packets to a file, click on the disk icon (Figure 3-16).

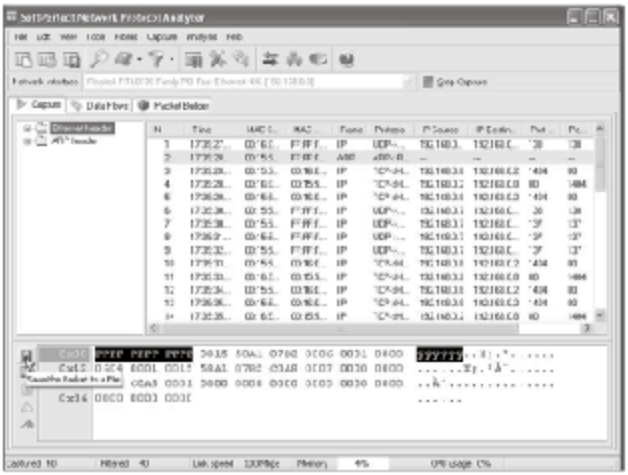


Figure 3-16 Click on the disk icon.

- Then browse the location for the file to save, type the filename, and click **Save**.
- To change the network packet size, click the ruler (Figure 3-17).

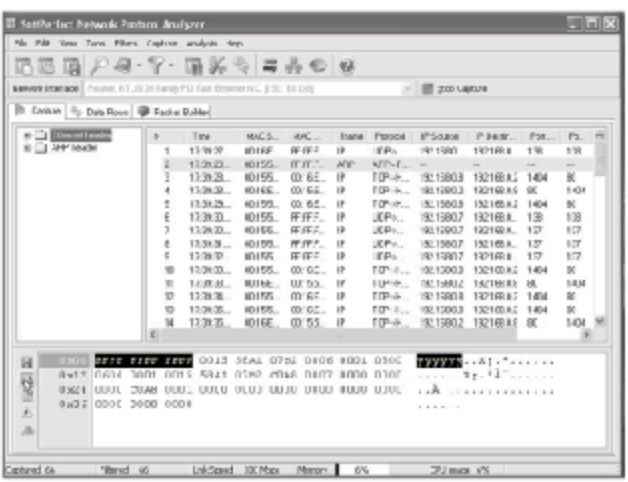


Figure 3-17 Change the network packet size.

- Enter the new packet size in the **Change Packet Size** window and click **OK** (Figure 3-18).

Figure 3-18 Enter the new packet size and click **OK**.

- To edit the packets, click the green arrow pointing upward (Figure 3-19).

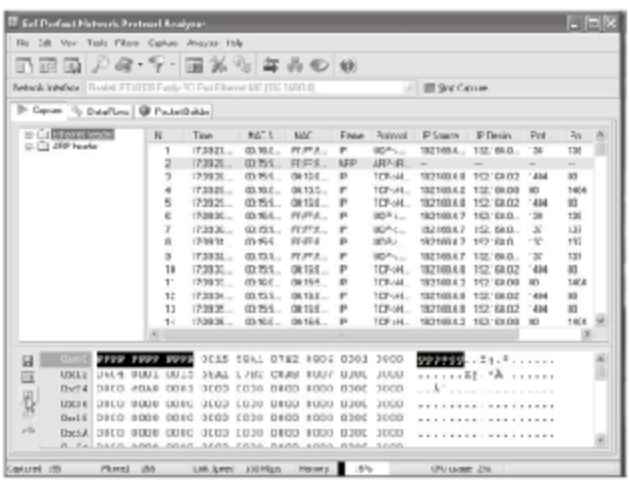


Figure 3-19 Edit the packets.

- For the protocol analyzer packet sender, click the caution icon (Figure 3-20).

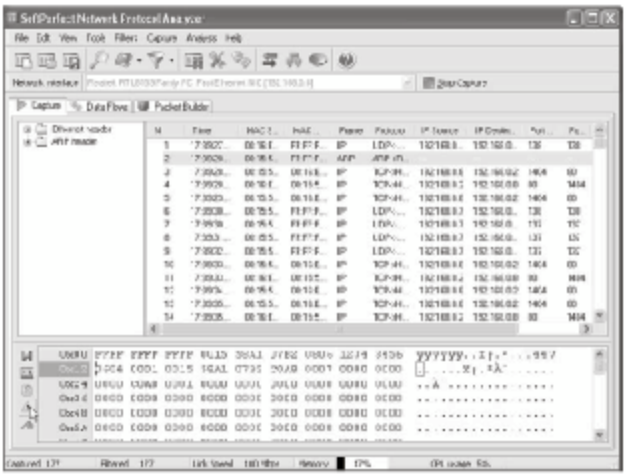


Figure 3-20 Open the packet sender.

- Set the interface **Delay between Packets** and **Number of Times** fields and click **Send Now** (Figure 3-21).

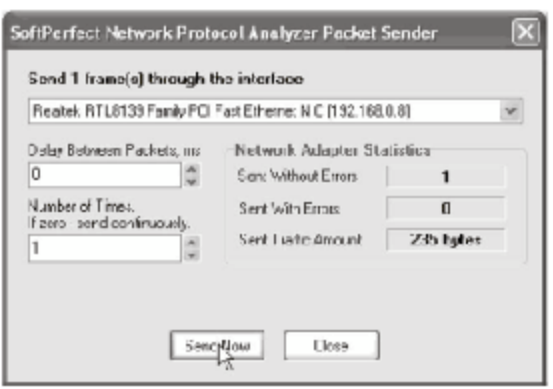


Figure 3-21 Fill in the Delay Between Packets and Number of Times fields.

- To stop capturing packets and start a new session, click the **New Capture** icon (Figure 3-22).

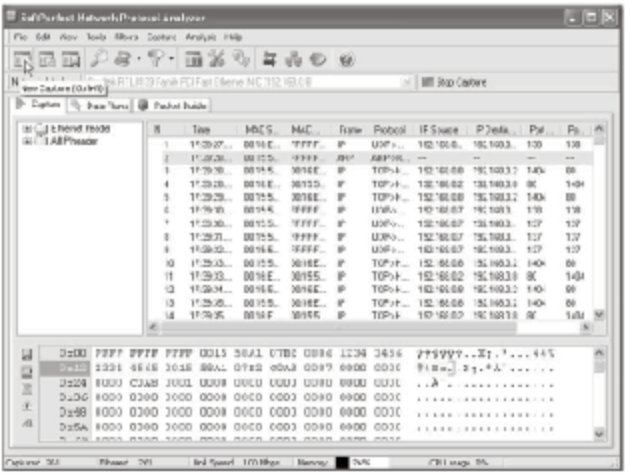


Figure 3-22 Start a new session.

- To set filter settings, choose **Filters**, then **Filter Settings** (Figure 3-23).

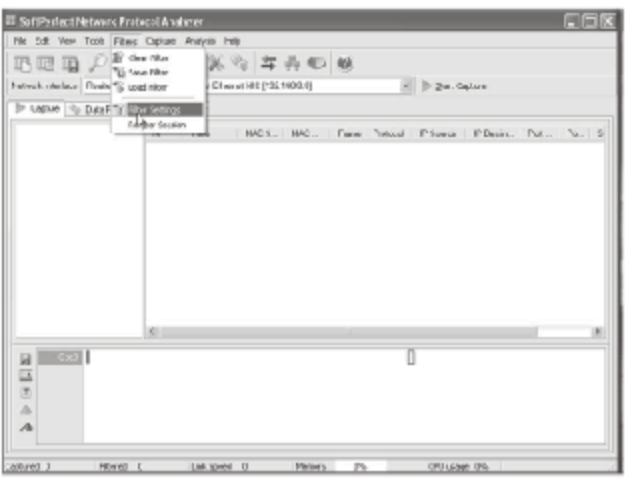


Figure 3-23 Set filter settings.

- To set the hardware filter settings, click **Hardware Filter** (Figure 3-24).

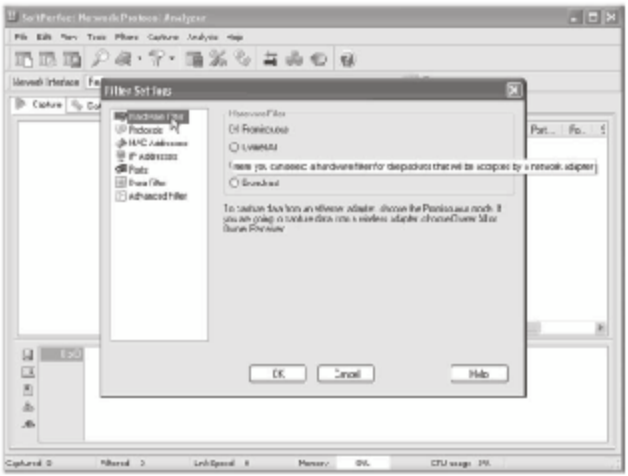


Figure 3-24 Set hardware filter settings.

- Click **Protocols** to set protocol filter settings (Figure 3-25).

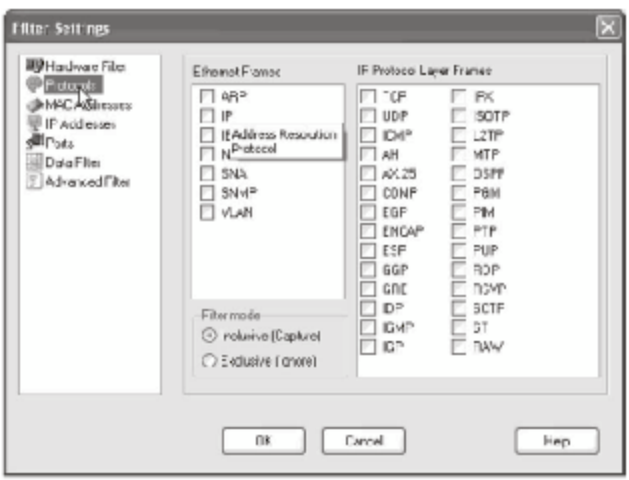


Figure 3-25 Set protocol filter settings.

- Click **MAC Addresses** to set MAC address filter settings (Figure 3-26).

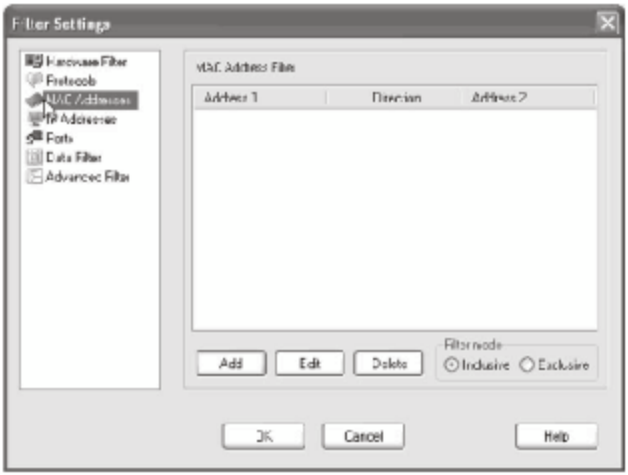


Figure 3-26 Set MAC address filter settings.

- Click the Add button and fill in the **Address 1** and **Address 2** fields in the **Add MAC Filter** window (Figure 3-27).

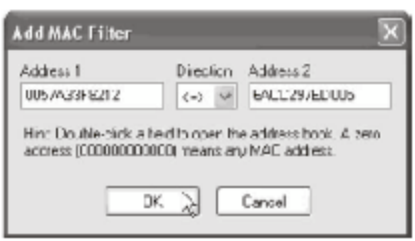


Figure 3-27 Fill in the **Address 1** and **Address 2** fields.

- Click **IP Addresses** to set IP address filter settings (Figure 3-28).

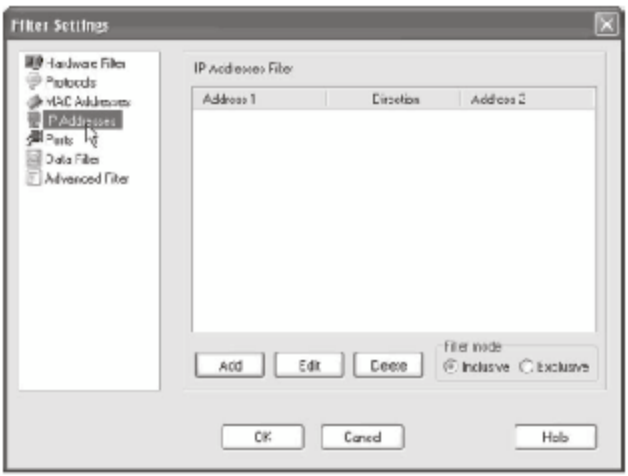


Figure 3-28 Set IP address filter settings.

- Click the Add button and fill in the **IP Address 1** and **IP Address 2** fields, and click **OK** (Figure 3-29).

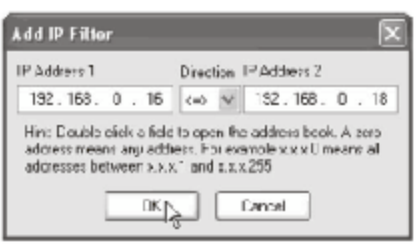


Figure 3-29 Fill in the **IP Address 1** and **IP Address 2** fields.

- To reconstruct the TCP sessions, choose **Capture**, then **Reconstruct TCP Sessions** (Figure 3-30).

Figure 3-30 Reconstruct the TCP sessions.

- Select the **Data Flows** tab to view the reconstructed TCP sessions (Figure 3-31).

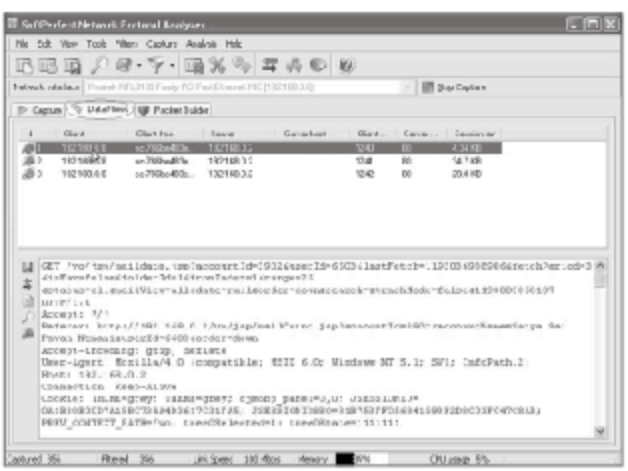


Figure 3-31 Select the **Data Flows** tab.

- To view the network traffic flow, click the network traffic flow button (Figure 3-32).

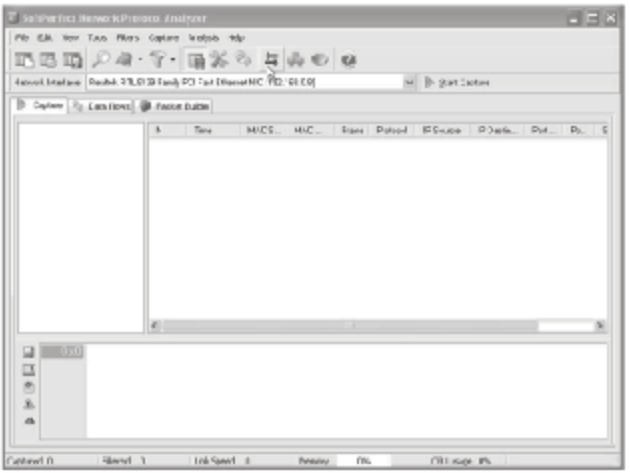


Figure 3-32 View the network traffic flow.

- The traffic flow analysis is shown in Figure 3-33.

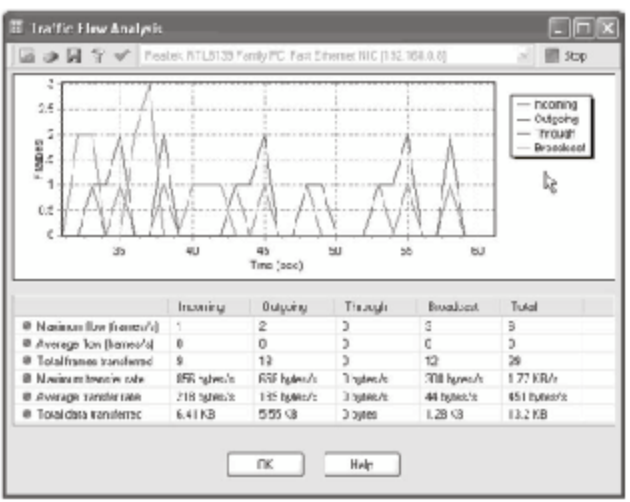


Figure 3-33 View the traffic flow analysis.

2. Use EffeTech HTTP Sniffer to capture IP packets containing the HTTP protocol, and rebuild and save the HTTP communications and files sent through the HTTP protocol. EffeTech HTTP Sniffer is a an HTTP network sniffer, packet analyzer, and file rebuilder.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the EffeTech HTTP Sniffer program (Figure 3-34).

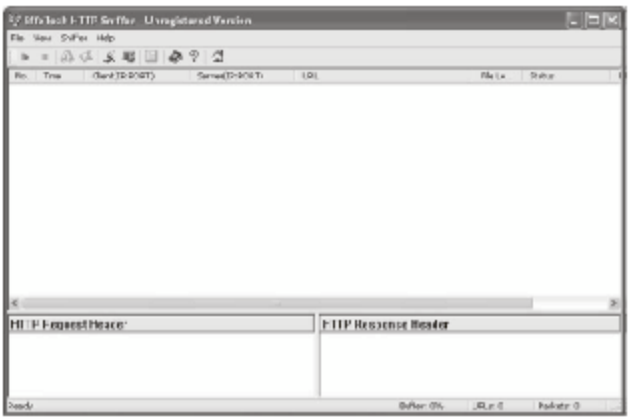


Figure 3-34 Launch EffeTech HTTP Sniffer.

   - Choose **Sniffer**, then **Adapter**, and select your adapter (Figure 3-35).

Figure 3-35 Select your network adapter.

- Click the **Start Sniffer** icon **Start** to start monitoring the network traffic (Figure 3-36).

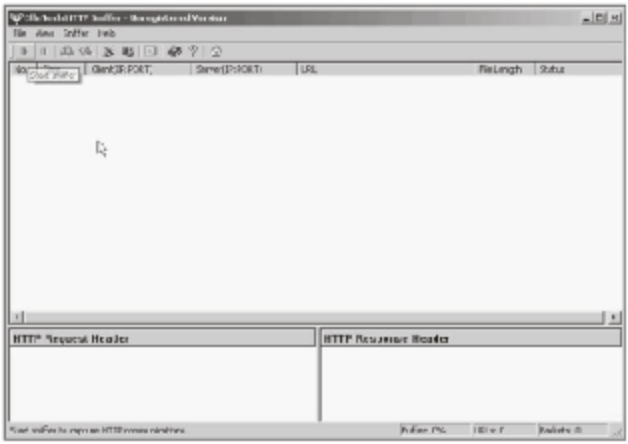


Figure 3-36 Start monitoring the network traffic.

- Wait for the Web traffic report to complete. Figure 3-37 shows what the screen will look like when the traffic report is generated.

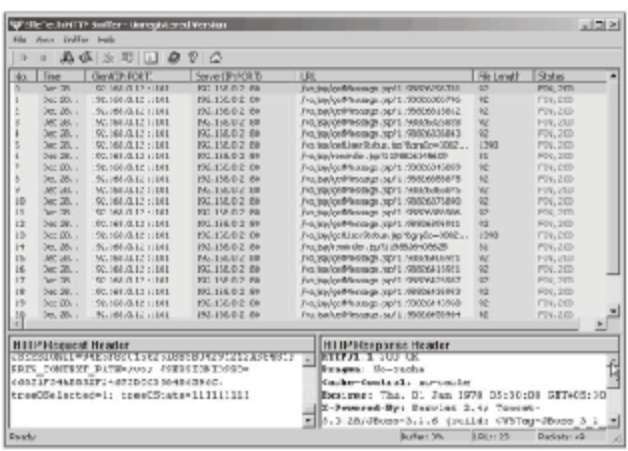


Figure 3-37 This is the Web traffic report.

- Choose **Filter**, then **Options**. The **Options** dialog box is displayed.
- Check the required fields and click **OK** in the **Options** dialog box (Figure 3-38).

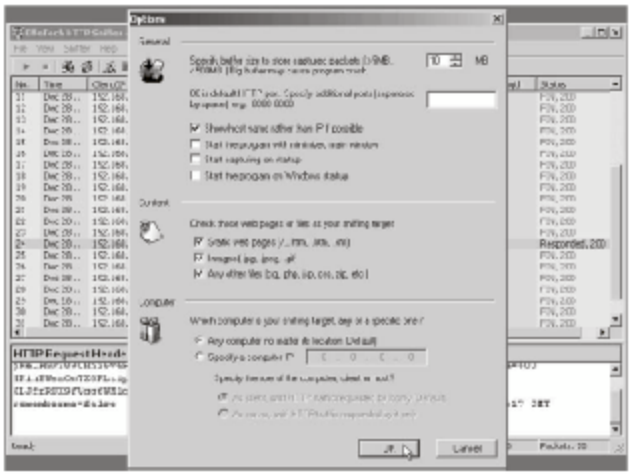


Figure 3-38 Check the required fields, as shown in the figure, and click **OK** in the **Options** dialog box.

- Click the **Adapter** button for the adapter that you want to monitor. The details of the current network adapter are displayed in the **Select the adapter through which to capture network traffic** dialog box (Figure 3-39).

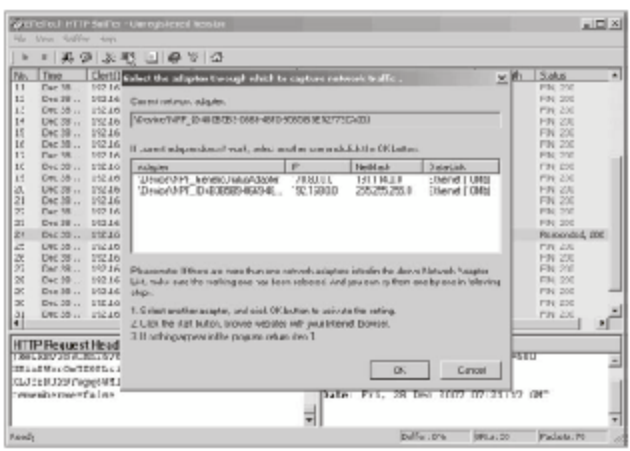


Figure 3-39 Select the network adapter.

- Click the **Export URL List** icon.
- Click **OK** (Figure 3-40).

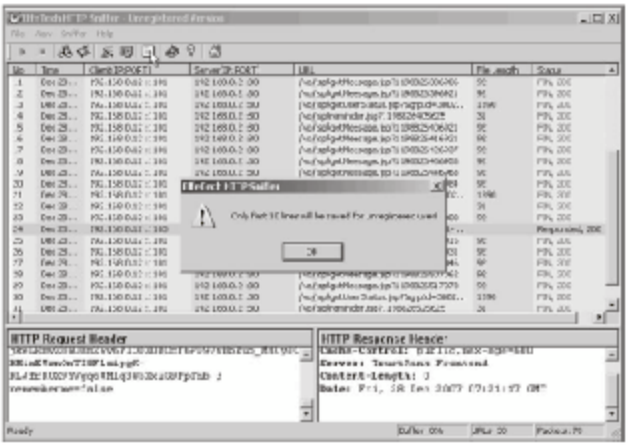


Figure 3-40 Click **OK**.

- In the **Select Export File Format** window, specify the required format for exporting the files.
- Click **OK** (Figure 3-41).

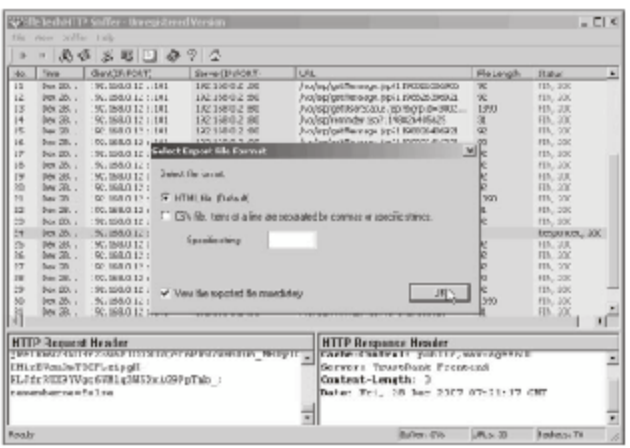


Figure 3-41 Click **OK**.

- To save the report, in the **Save As** dialog box, type the filename and select the file type, and click **Save** (Figure 3-42).

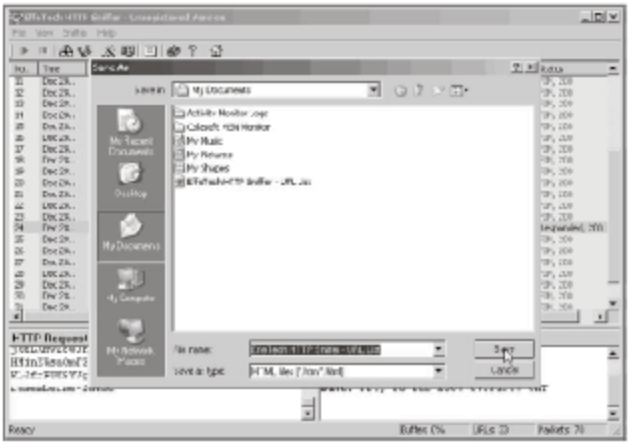


Figure 3-42 Click **Save**.

3. Use EtherDetect Packet Sniffer to capture and group all network traffic. It allows viewing real-time details for each packet, as well as the content.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the EtherDetect Packet Sniffer program (Figure 3-43).

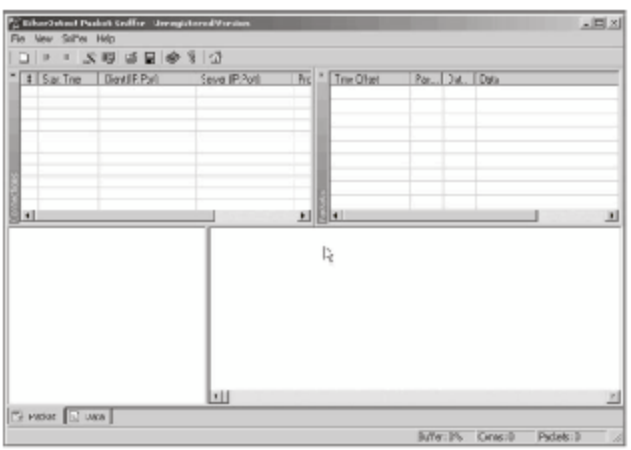


Figure 3-43 Launch EtherDetect Packet Sniffer.

- Click the play button to start capturing and grouping all network traffic (Figure 3-44).

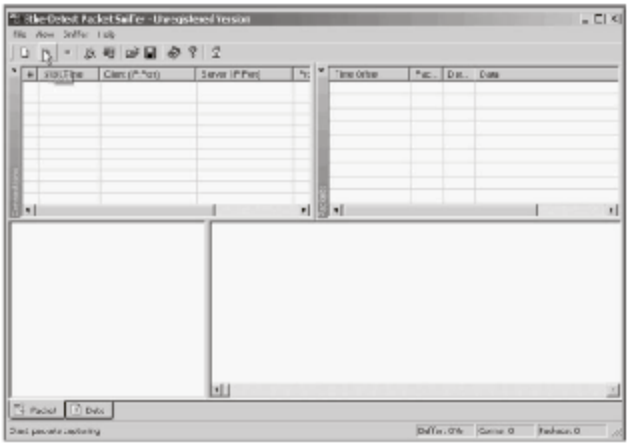


Figure 3-44 Start capturing and grouping network traffic.

- Click any one of the captured packets shown in Figure 3-45. Figure 3-46 shows data from the captured packet.

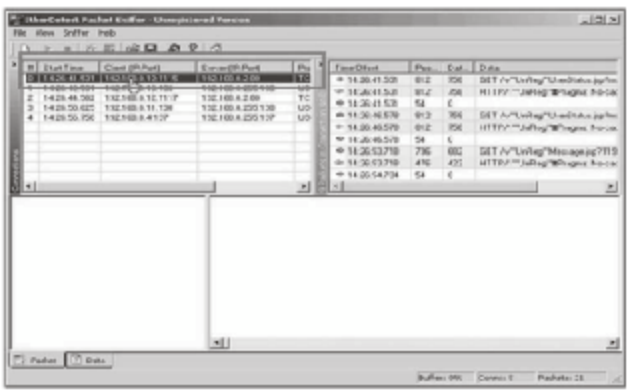


Figure 3-45 Select a captured packet.

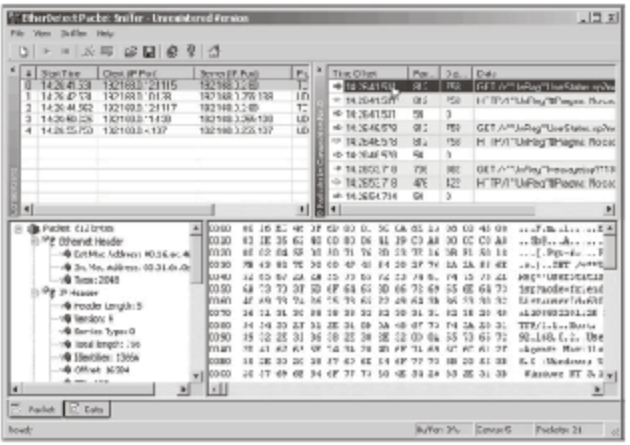


Figure 3-46 This is data from the captured packet.

- Click the **Configure** icon.
- Check for the required fields and click **OK** in the **Configuration For Packets Capturing** dialog box (Figure 3-47).

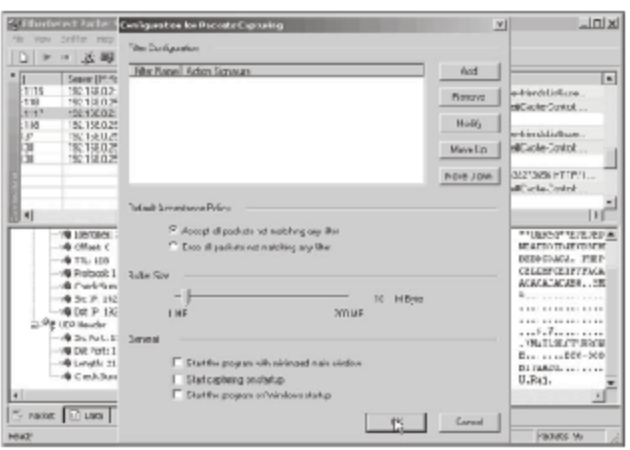


Figure 3-47 Click **OK**.

4. Perform the following steps:
   - Navigate to Chapter 3 of the Student Resource Center.
   - Open TCPIP overview.pdf and read the content.
5. Perform the following steps:
   - Navigate to Chapter 3 of the Student Resource Center.
   - Open TCPIP Tutorial and Technical Overview.pdf and read the content.
6. Perform the following steps:
   - Navigate to Chapter 3 of the Student Resource Center.
   - Open Security Problems in the TCPIP Protocol Suite.pdf and read the content.
7. Perform the following steps:
   - Navigate to Chapter 3 of the Student Resource Center.
   - Open IPv6 Tutorial.pdf and read the content.

Chapter 4

IEEE Standards

Objectives

After completing this chapter, you should be able to:

- Understand the history of IEEE 802
- Understand the architecture of IEEE 802
- Describe the different parts of the IEEE 802 standard
- Understand the IEEE 802 wireless networking standards
- Understand ETSI standards, including the HiperLAN family of standards

Key Terms

European Telecommunications Standards Institute (ETSI) an independent association whose aim is to provide standards related to telecommunications, broadcasting, and other information and communications technologies

IEEE 802 a family of IEEE standards that deals with local area networks (LANs) and metropolitan area networks (MANs), mainly for the lowest two levels of the Open Systems Interconnection (OSI) model

Institute of Electrical and Electronics Engineers (IEEE) a nonprofit organization that is one of the leading professional associations for the advancement of technology

Introduction to IEEE Standards

This chapter focuses on IEEE standards. It begins by discussing the architecture and history of the IEEE 802 set of standards. It then goes into further detail about IEEE 802. The chapter finishes with an overview of the ETSI and HiperLAN standards.

Specifications of IEEE Standards

The ***Institute of Electrical and Electronics Engineers (IEEE)*** is a nonprofit organization. It is one of the leading professional associations for the advancement of technology.

IEEE 802

Overview of IEEE 802

The IEEE 802 or LAN/MAN Standards Committee (LMSC) develops LAN and MAN standards. ***IEEE 802*** refers to a family of IEEE standards that deals with local area networks (LANs) and metropolitan area networks (MANs), mainly for the lowest two levels of the Open Systems Interconnection (OSI) model. Figure 4-1 shows how the IEEE 802 protocols fit into the OSI model.

History of IEEE 802

The first meeting of the IEEE Local Network Standard Committee for Project 802 was held in February 1980. (The project number 802 is the second number issued by the IEEE for standards projects.) It was supposed to be one LAN standard, with speeds from 1 to 20 MHz, divided into the media or physical layer (PHY), media access control (MAC), and higher-level interface (HILI). By the end of 1980, the token access method and three MACs were added: CSMA/CD, token bus, and token ring. After that, the other MAC and PHY groups were added for LAN security as well.

Architecture of IEEE 802

The architecture of IEEE 802 standard contains the following:

- Physical layer
- Media access control (MAC) layer
- Logical-link control (LLC) layer

Physical Layer

The physical layer of the IEEE 802 architecture performs the following functions:

- Encoding or decoding of the signal
- Preamble or removal (for synchronization)
- Bit transmission or reception
- Specification of transmission medium and topology

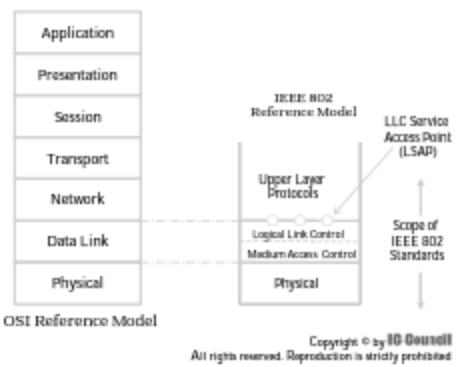


Figure 4-1 This shows how IEEE 802 fits into the OSI model.

Media Access Control (MAC) Layer

The MAC layer in the IEEE 802 architecture performs the following functions:

- It assembles data into a frame with address-recognition and error-detection fields on transmission.
- It disassembles a frame and performs address recognition and error detection on reception.
- It provides access to the LAN transmission medium.

The following is the MAC frame format:

- *MAC control*: This is the protocol control information needed for the MAC protocol's function.
- *Destination MAC address*: This is the destination physical address on the LAN.
- *Source MAC address*: This is the source physical address on the LAN.
- *Data*: This is the main body of the MAC frame.
- *Cyclic redundancy check (CRC)*: The CRC is the error-detecting code field.

The MAC layer is responsible for detecting errors and discarding frames that contain errors.

Logical-Link Control (LLC) Layer

LLC provides an interface to higher layers and performs flow control and error detection. It provides the logic required to manage access to a shared access medium. It is not found in the traditional layer 2, the data-link layer.

The LLC layer keeps track of the frames that have been successfully received and retransmits unsuccessful frames. LLC provides mechanisms for addressing across the medium for controlling the transmission of data between users.

The following are the services of LLC:

- *Unacknowledged connectionless service*: A datagram-style service that does not contain a flow-control or error-detection mechanism
- *Connection-mode service*: A service for a connection set up between two users, providing flow control and error detection
- *Acknowledged connectionless service*: A service wherein the datagram can be acknowledged but no logical connection is set up

Figure 4-2 shows a MAC frame and an LLC PDU (protocol data unit).

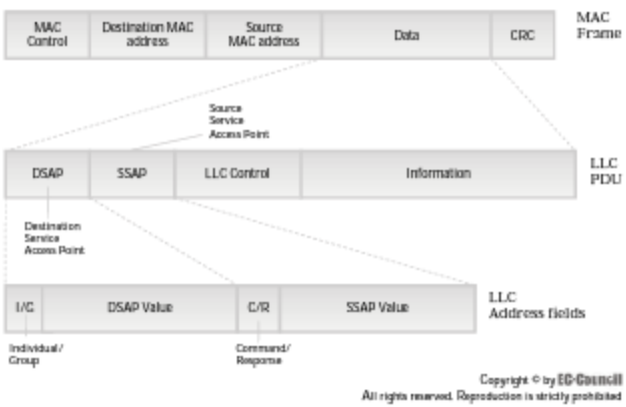


Figure 4-2 This shows the structure of a MAC frame and an LLC PDU.

Parts of IEEE 802

IEEE 802.1 Bridging and Management

The 802.1 is mainly concerned with bridging, which involves connecting two or more networks. The developed standards and recommended practices of this working group are as follows:

- 802 LAN/MAN architecture
- Internetworking among 802 LANs, MANs, and other wide area networks (WANs)
- 802 link security
- 802 overall network management and protocol layers above the MAC and LLC layers

IEEE 802.2 Logical-Link Control Layer

The logical-link control (LLC) layer is defined in the IEEE 802.2 protocol. It specifies implementation of LLC sublayers of the data-link layer. It is used in IEEE 802.3 (Ethernet) and 802.5 (token ring) LANs to perform the following functions:

- It manages data-link communication.
- It provides link addressing.
- It is used to define a service access point (SAP) and is also used for sequencing.

The LLC layer provides a way for upper layers to deal with MAC layers (for example, Ethernet 802.3 CSMA/CD or token ring, and 802.5 token passing).

LLC was inspired by the High-Level Data-Link Control (HDLC) protocol and uses a subclass of the HDLC specification.

LLC performs three types of operations for data communication:

1. *TYPE 1*: This connectionless operation basically sends data, but there is no guarantee of receipt.
2. *TYPE 2*: This connection-oriented operation provides four services for LLC:
   - Connection establishment
   - Confirmation and acknowledgment that data have been received
   - Error recovery by resending requests for bad data received
   - Sliding windows as a method of increasing the rate of data transfer
3. *TYPE 3*: This operation will give the acknowledgment with connectionless service.

The TYPE 1 LLC connectionless service specifies a static-frame format and permits network protocols to run on it.

The TYPE 2 LLC connection-oriented service provides reliable data transfer. It is used in a LAN environment that does not invoke network- and transport-layer protocols.

IEEE 802.3 CSMA/CD (Ethernet)

IEEE 802.3 CSMA/CD (Ethernet) is a LAN architecture that was developed by Xerox Corporation in cooperation with DEC and Intel in 1976. It uses a bus or star topology, and it supports a data transfer rate of 10 Mbps. The Ethernet specification has served as a basis for the IEEE 802.3 standard, which specifies the physical layer and lower software layers. The Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) to handle simultaneous demands. A newer version of Ethernet (100Base-T) supports a data transfer rate of 100 Mbps. Gigabit Ethernet supports a data transfer rate of 1 gigabit (1,000 megabits) per second.

10Base-5 This is a cabling standard used for Ethernet that uses coaxial cables. It supports a maximum data transfer speed of 10 Mbps. The 10Base-5 standard uses a baseband transmission and has a maximum cable length of 500 meters.

10Base-T This is an Ethernet (IEEE 802.3) standard for LANs. This standard uses a twisted-pair cable with a maximum length of 100 meters. The cable, which is thinner and more flexible than the coaxial cable, is used for 10Base-T or 10Base-5 standards. In a 10Base-T system, the cable is connected with an RJ-45 connector.

10Base-2 This is an Ethernet (IEEE 802.3) standard for LANs that uses 50-ohm coaxial cable (RG-58 A/U) with a maximum length of 185 meters. In a 10Base-2 system, the cable is connected with a Bayonet Neill-Concelman (BNC) connector.

100Base-T 100Base-T is a networking standard that supports a data rate of up to 100 Mbps. It is 10 times faster than Ethernet.

Gigabit Ethernet This version of Ethernet supports a data transfer rate of 1 gigabit (1,000 megabits) per second. The IEEE 802.3 committee introduced the first Gigabit Ethernet standard (802.3z) in 1998.

IEEE 802.4 Token-Passing Bus

The IEEE 802.4 standard defines a bus physical topology that uses a token message to grant the right to access the physical network medium. A token-passing system is a standard LAN technology. This system allows the use of maximum bandwidth even if the network is busy. It is designed for factory automation applications. The receiving station has control over the medium and may transmit data frames. Its bus topology is useful for industrial production lines.

IEEE 802.5 Token-Ring Passing

The IEEE 802.5 standard was originally developed by IBM in the 1970s and is still the primary LAN technology. IEEE 802.5-related specifications are almost identical to and compatible with this network. It is used to refer to both IBM's Token Ring and to IEEE 802.5 networks, which are basically compatible. Besides other differences like the types of media and information field routing, IBM's Token Ring specifies a star topology, with all stations connected to a device called a multistation access unit (MSAU).

IEEE 802.6 DQDB Access Method

This standard of IEEE 802.6 describes a MAN standard called Distributed Queue Dual Bus (DQDB). DQDB, whose architecture is shown in Figure 4-3, allows multiple systems to interconnect using two unidirectional logical buses. It is an open standard that is designed for compatibility with carrier transmission standards such as Switched Multimegabit Data Service (SMDS). SMDS is based on the DQDB standard. The paired bus usage provides a failure-tolerant configuration in the network. Networks using DQDB can be 30 miles long and function in a range of 34 Mbps to 155 Mbps. DQDB is able to carry data, voice, and video transmissions with bandwidth that is allocated using time slots on the bus. DQDB is composed of two bus lines, with both stations connected and a frame generator at the end of each bus. The buses run in a parallel fashion to allow the generated frames to travel across the stations in the opposite direction.

IEEE 802.7 Broadband LAN

The IEEE 802.7 broadband standard was first introduced in 1989. This standard identifies the recommended practices for broadband LANs. It describes the design, installation, and test parameters for a broadband cable. This standard was considered the grandfather of standards used for cable and xDSL modems.

IEEE 802.10 Security

The IEEE 802.10 security standard provides specifications for the interoperable data-link-layer security protocol and other associated security services. This Secure Data Exchange (SDE) standard is supported by an application-layer key management protocol (KMP) that establishes the security association for SDE and other security protocols. A security label option allows for rule-based access, which is implemented using the SDE protocol.

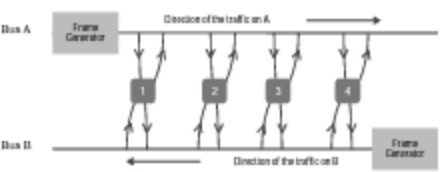


Figure 4-3 DQDB uses two unidirectional logical buses.

The following are features of the IEEE 802.10 standard:

- It provides security association management.
- It provides key management (manual and certificate based).
- It provides security labeling.
- It provides security services (data confidentiality, connectionless integrity, data origin authentication, and access control).

IEEE 802.11 Wireless LAN

This is the first wireless local area network (WLAN) standard adopted by IEEE, in 1997. It defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless access. This standard addresses local area networking where connected devices communicate through the air to other devices that are within close range of each other. To use different portions of the spectrum and to operate in different environments, many task groups are installed, from 802.11a (5 GHz) to 802.11i (security and authentication mechanisms).

IEEE 802.12 Demand Priority Access

The IEEE 802.12 standard defines demand priority access. HP also calls this 100VG-AnyLAN. Various methods are used to ensure clarity of access for all nodes and to guarantee access times for individual nodes. Round-robin selection procedures are used to give each node an equal opportunity to send data. Two levels of priority are provided so that time-critical traffic—such as an interactive video, audio, and multimedia—can be given priority services to guarantee low delay. The bandwidth allocator can be used to control the amount of bandwidth that each application uses.

IEEE 802.15 Wireless Personal Area Network

IEEE 802.15 provides specifications for wireless personal area networks (WPANs). Bluetooth is included in this standard. A Bluetooth radio is built into a small microchip and processes in the 2.4-GHz frequency band, which is available globally to ensure communication compatibility worldwide. A frequency-hopping spread spectrum technique is used to change the signal 1,600 times per second to prevent interception by unauthorized parties.

Bluetooth wireless technology has changed the personal connectivity market by providing freedom from wired connections. It provides links between mobile computers, mobile phones, portable handheld devices, and the Internet.

IEEE 802.16 Broadband Wireless MAN (WMAN)

This standard covers a frequency band in the 2-GHz to 11-GHz range, and it specifies a MAN protocol that provides a wireless alternative to cable. It also specifies DSL and T1 services for last-mile broadband access, and it provides backhaul for 802.11 hotspots (WLAN).

The IEEE 802.16a standard specifies a protocol that supports low-latency applications such as voice and video. It provides broadband connectivity without the need for direct line of sight (LOS) between a subscriber terminal and a base station (BST). This protocol, WiMAX, supports hundreds or even thousands of subscriber stations, each of which is mounted on a rooftop, from a single BST. By doing this, WiMAX will help accelerate the usage of broadband equipment in the market.

IEEE 802.17 Resilient Packet Ring

The IEEE 802.17 working group develops standards to help in the development and deployment of resilient packet-ring networks in LANs, MANs, and WANs for the resilient and efficient transmission of data packets at scalable rates. IEEE 802.17 builds upon physical-layer specifications.

Wireless Networking Standards

Wireless networking standards refer to the technology that allows two or more computers to communicate using standard networking protocols without network cable. This technology has produced a number of affordable wireless solutions that are growing in popularity with businesses and schools, and it has produced some applications that can be used where network wiring is not possible.

The IEEE defines the following standards for wireless networking:

- *802.1X*: 802.1X is an IEEE standard that attaches Extensible Authentication Protocol (EAP) over wired or wireless Ethernet and provides several authentication techniques like token cards, Kerberos, certificates, and public-key authentication.
- *802.11*: This standard is a working group for WLAN. It denotes an over-the-air interface between a wireless client and a base station or access point.
- *802.11a*: This standard has a data transfer rate of up to 26.4 Mbps and works at 40 MHz in the 5-GHz range.
- *802.11b*: This standard works at 20 MHz in the 2.4-GHz range. It has theoretical speeds of up to 11 Mbps.
- *802.11e*: 802.11e provides quality-of-service (QoS) support for LAN applications.
- *802.11g*: This standard works in the same frequency range as 802.11b. It has a theoretical throughput of 54 Mbps.
- *802.11h*: This standard is supplementary for the MAC layer to comply with European regulations for 5-GHz WLANs.
- *802.11i*: This is a standard for WLANs that provides better encryption for networks that use the popular 802.11a, 802.11b, and 802.11g standards.
- *802.11n*: This standard is based on multiple-input/multiple-output (MIMO) technology.
- *802.15*: This supplies standards for low-complexity and low-power-consumption wireless connectivity.
- *802.16 (WiMAX)*: The IEEE 802.16 is a broadband wireless access group, which provides standards for WMAN.
- *802.16a (WiMAX)*: This is a specification for fixed broadband WMAN access. It supports a data rate of 2 GHz to 11 GHz.

802.1X

802.1X is an IEEE standard that attaches EAP (Extensible Authentication Protocol) over wired or wireless Ethernet and provides several authentication techniques like token cards, Kerberos, certificates, and public-key authentication. 802.1X provides an authenticating and authorizing device to attach to LAN ports.

802.1X describes three different roles:

1. *Supplicant*: The user or client requesting authentication
2. *Authentication server*: The server that provides the authentication
3. *Authenticator*: The device that accesses the request from the supplicant and provides it to the authentication server; if the server provides authentication, then the authenticator sends the message to the supplicant

802.1X requires less power on the part of the authenticator, so it is better for wireless LAN applications. The 802.11i Robust Security Network (RSN) uses 802.1X for authenticating wireless devices to the network.

802.11

802.11 Standard

The IEEE developed an international WLAN standard identified as the IEEE 802.11 standard. This project was initiated in 1990, and several draft standards have been published for review. The main aim of this standard is to develop MAC- and PHY-layer specifications for wireless connectivity for fixed, portable, and moving stations within a local area.

The following are the two main purposes of this standard:

1. To provide wireless connectivity to automated machinery, equipment, or stations that require rapid deployment, which may be portable, handheld, or mounted on moving vehicles within a local area
2. To offer regulatory bodies standardized access to one or more frequency bands for the purpose of local area communication

The IEEE 802.11 draft standard describes mandatory support for a 1-Mbps WLAN, with optional support for a 2-Mbps data transmission rate. Mandatory support for asynchronous data transfer is specified, in addition to optional support for distributed time-bounded services (DTBS). Asynchronous data transfer refers to traffic that is relatively insensitive to time delay. Asynchronous data examples include available bit-rate traffic like e-mail and file transfers. Time-bounded traffic, on the other hand, is traffic that is bound by specified time delays to achieve an acceptable QoS (for example, packetized voice and video).

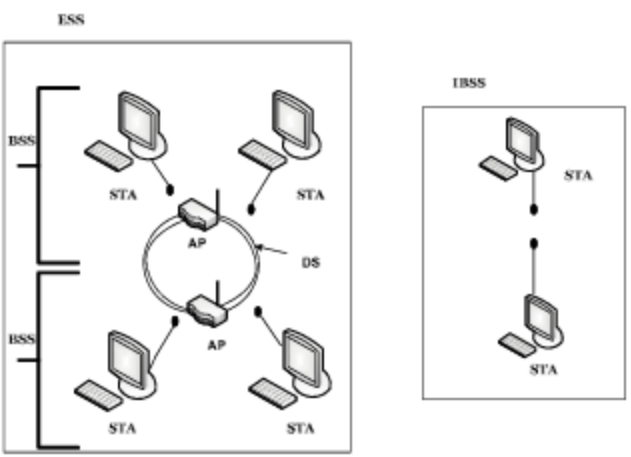
802.11 Architecture

The Basic Service Set (BSS) is the fundamental building block of the IEEE 802.11 architecture. It is defined as a group of stations that are under the direct control of a single coordination function (for example, a DCF [distributed coordination function] or PCF [point coordination function]). The geographical area covered by the BSS is known as the Basic Service Area (BSA), which is analogous to a cell in a cellular communications network. Conceptually, all stations in a BSS can communicate directly with all other stations in a BSS.

However, transmission medium degradations due to multipath fading, or interference from nearby BSSs reusing the same physical-layer characteristics (for example, frequency and spreading code, or hopping pattern), can cause some stations to appear hidden from other stations.

The 802.11 architecture (Figure 4-4) includes the following components:

- *Station (STA)*: The wireless STA includes an adapter card, a PC card, or an embedded device that gives wireless connectivity.
- *Wireless access point (WAP)*: The WAP works as a bridge between the wireless STAs and the existing network backbone for network access. Most of the time, access points (APs) are connected with wires. The AP gives connectivity to the wired LAN and supports the bridging functionality when one STA starts communicating with another STA or a node on the distribution system (DS).
- *Independent Basic Service Set (IBSS)*: IBSS is a wireless network consisting of a minimum of two STAs. It is also known as an ad hoc wireless network.
- *Basic Service Set (BSS)*: This is a wireless network that consists of a single AP. It supports one or many wireless clients. It is also known as an infrastructure wireless network. STAs in a BSS communicate through an AP.



Source: http://mia.eca.uic.edu/~papers/net/pdf00001.pdf. Accessed 2004.

Figure 4-4 This is the architecture of 802.11.

- *Distribution system (DS)*: The DS connects the APs of different BSSs. The DS offers distribution services to allow for the roaming of STAs between BSSs.
- *Extended Service Set (ESS)*: An ESS is a set in which two or more wireless APs are connected to the same wired network that defines a single logical network segment (known as a subnet) bounded by a router.

802.11a

802.11a is one of the IEEE standards for wireless LAN. The following are the basic features of the 802.11a standard:

- Works at 40 MHz in the 5-GHz range
- Supports bandwidth up to 54 Mbps
- Actual transfer rates of about 26.4 Mbps
- Limited in use because it is almost a line-of-sight transmittal, which necessitates multiple WAPs
- Uses a modulation technique called coded orthogonal frequency division multiplexing (COFDM)
- Cannot operate in the same range as 802.11b/g
- Absorbed more easily than other wireless implementations
- Overcomes the challenges of indoor radio frequency
- Uses single-carrier, delay-spread system

802.11b

In 1999, IEEE identified the 802.11b high-rate standard, also called Wi-Fi. The IEEE 802.11b specification family allows for a wireless data transmission rate of 11 Mbps as unlicensed use of the 2.4-GHz radio-frequency band. Wireless users can achieve performance, throughput, and availability with the IEEE 802.11b standard.

The following are the basic features of the 802.11b standard:

- Operates at 20 MHz in the 2.4-GHz range
- Most widely used and accepted form of wireless networking
- Theoretical speeds of up to 11 Mbps
- Actual speeds depend on implementation:
  - 5.9 Mbps when Transmission Control Protocol (TCP) is used (error checking)
  - 7.1 Mbps when User Datagram Protocol (UDP) is used (no error checking)
- Can transmit up to 8 km in a city
- Not as easily absorbed as an 802.11a signal
- Can cause interference to or receive interference from:
  - Microwave ovens (and microwaves in general)
  - Wireless telephones
  - Other wireless appliances operating in the same frequency

802.11e

QoS Support Mechanisms of 802.11e IEEE 802.11 Task Group E defines enhancements to the 802.11 MAC, called 802.11e, which introduces enhanced distributed coordination function (EDCF) and hybrid coordination function (HCF) to support QoS with priority schemes. Stations that operate under 802.11e are called enhanced stations. An enhanced station may optionally work as the centralized controller for all other stations within the same Quality-of-Service Basic Service Set (QBSS) and is called the hybrid coordinator (HC). A QBSS is a BSS that includes an 802.11e-compliant HC and stations. The HC will typically reside within an 802.11e AP.

Enhanced Distributed Coordination Function The EDCF in 802.11e is the basis for the HCF. QoS support is realized through the introduction of traffic categories (TCs). MAC service data units (MSDUs) are delivered through multiple backoff instances within one station; each backoff instance is parameterized with TC-specific parameters. In the CP (contention period), each TC within the station contends for a transmission opportunity (TXOP) and independently starts a backoff after detecting the channel being idle for an arbitration interframe space (AIFS); the AIFS is at least DIFS (DCF interframe space) and can be enlarged individually for each TC. After waiting for AIFS, each backoff sets a counter to a random number drawn from the interval [1, CW + 1]. The minimum size (CWmin[TC]) of the CW is another parameter dependent on the TC. Priority over legacy stations is provided by setting CWmin[TC] < 15 (in case of 802.11a PHY) and AIFS = DIFS. As in legacy DCF, when the medium is busy before the counter reaches zero, the backoff has to wait for the medium to be idle for AIFS again before continuing to count down the counter. A big difference from the legacy DCF is that when the medium is determined as being idle for the period of AIFS, the backoff counter is reduced by one at the beginning of the last slot interval of the AIFS period.

One crucial feature of the 802.11e MAC is the TXOP. A TXOP is defined as an interval of time when a station has the right to initiate transmissions, defined by a starting time and a maximum duration. TXOPs are allocated via contention (EDCF-TXOP) or granted through HCF (polled-TXOP). The duration of an EDCF-TXOP is limited by a QBSS-wide TXOP limit distributed in beacon frames, while the duration of a polled TXOP is specified by the duration field inside the poll frame. However, although the poll frame is a new frame as part of the upcoming 802.11e, the legacy stations set their NAVs upon receiving this frame.

802.11g

The 802.11g standard was ratified in June 2003. This flavor works in the 2.4-GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbps, or about 24.7 Mbps net throughput like 802.11a. 802.11g hardware will work with 802.11b hardware. Details of making b and g work well together occupied much of the lingering technical process. In older networks, however, the presence of an 802.11b participant significantly reduces the speed of an 802.11g network. The modulation scheme used in 802.11g is OFDM (orthogonal frequency division multiplexing) for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, and reverts to (like the 802.11b standard) CCK (complementary code keying) for 5.5 and 11 Mbps and DBPSK/DQPSK+DSSS (differential binary phase shift keying/differential quadrature phase shift keying + direct-sequence spread spectrum) for 1 and 2 Mbps. Although 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its similarities to 802.11a. The maximum range of 802.11g devices is slightly greater than that of 802.11b devices, but the range in which a client can achieve the full (54 Mbps) data rate is much shorter than that of 802.11b.

The 802.11g standard swept the consumer world of early adopters starting in January 2003, well before ratification. The corporate users held back and Cisco and other big equipment makers waited until ratification. By summer 2003, announcements were flourishing. Most of the dual-band 802.11a/b products became dual-band/trimode, supporting a, b, and g in a single mobile adaptor card or AP. Despite its major acceptance, 802.11g suffers from the same interference as 802.11b in the already crowded 2.4-GHz range. Devices operating in this range include microwave ovens, Bluetooth devices, and cordless telephones.

The following are the basic features of 802.11g:

- Operates in the same frequency range as 802.11b
- Theoretical throughput of 54 Mpbs
- Actual transmission rate is dependent on several factors but averages 24.7 Mbps
- Logical upgrade from 802.11b wireless networks and is backward compatible
- Suffers from same limitations as 802.11b network
- System may suffer significant decrease in network speeds if network is not completely upgraded from 802.11b

802.11h

This standard specifies dynamic channel selection and a transmit power control mechanism for 802.11-compliant equipment. In combination with 802.11e, it provides compliance with European regulations for 5-GHz WLANs. European radio regulations for the 5-GHz band require all products to have transmit power control and dynamic frequency selection.

IEEE 802.11h allows WLANs to meet regulations initially adopted by European countries and then made global requirements of the International Telecommunication Union (ITU) Radio Regulations at the World Radio Communication Conference in 2003.

The ITU Radio Regulations call for WLANs and other devices to detect the presence of radars and Earth Exploration Satellite Service (EESS) and Space Research Service (SRS) systems and then protect them from interference by selecting another operating channel or reducing transmit power. IEEE 802.11h creates a standard method to avoid interference so a manufacturer can create products that adhere to the ITU Radio Regulations and interoperate with similar products from other suppliers.

IEEE 802.11h amends the IEEE 802.11a PHY-layer standard and the underlying IEEE 802.11 MAC-layer standard to enhance network management and control extensions for spectrum and transmit power management in 5-GHz license-exempt bands. It improves channel energy measurement and reporting, channel coverage in many regulatory domains, dynamic channel selection, and transmit power control mechanisms.

802.11i

The 802.11i standard focuses on security and introduces two protocols: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). The standard deprecates WEP in favor of WPA and WPA2. TKIP provides encryption for legacy devices by wrapping additional security measures around WEP services. Wireless networks under 802.11i benefit from the added protection of a master encryption key, temporary session keys, and user authentication.

The following are the basic features of 802.11i:

- Provides improved encryption for networks that use the popular 802.11a, 802.11b, and 802.11g standards
- Officially ratified by the IEEE in June 2004
- Is a strong encryption standard that supports 128-bit, 192-bit, and 256-bit keys
- Security is made up of three parts:
  - 802.1X for authentication (EAP and authentication server)
  - Robust Security Network (RSN) to keep track of associations
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide confidentiality, integrity, and origin authentication

802.11n

802.11n is the next-generation Wi-Fi standard developed by Task Group N of the IEEE. This standard combines the use of multiple antennas, clever encoding, and optional spectrum doubling to achieve raw data rates of up to 600 Mbps.

The following are the basic features of 802.11n:

- The 802.11n standard, which is based on multiple-in/multiple out (MIMO) technology, is expected to boost throughput to potentially well over 100 Mbps.
- It specifies improvements to the PHY and MAC layers.
- 802.11n is supposed to have the following improvements over its predecessors:
  - Improved radio technology to increase physical data transfer
  - New mechanisms to implement effective management of enhanced PHY performance modes
  - Improved data transfer efficiency to reduce the performance impact of PHY headers and radio turnaround delays, which adversely affect the physical transfer rate

802.15

802.15 is a working group for WPAN. This IEEE 802.15 working group was formed in May 1999. It supplies standards for low-complexity and low-power-consumption wireless connectivity.

The following are four active task groups of 802.15:

1. *802.15.1*: This standard was published in June 2002 and is based on Bluetooth specifications.
2. *802.15.2*: This standard was published in 2003. It provides for the coexistence of wireless personal area networks and other wireless devices operating in unlicensed frequency bands.

3. *802.15.3*: This is a task group for high-rate (11 Mbps to 55 Mbps) WPANs.
4. *802.15.4*: This deals with an unlicensed international frequency band. It has data rates of 250 kbps, 40 kbps, and 20 kbps. It has two addressing modes: 16-bit short and 64-bit IEEE addressing. It supports critical-latency devices and provides automatic network establishment by the coordinator. It supports power management to ensure low power consumption.

802.16

IEEE 802.16 is a broadband wireless access group that provides standards for WMAN. It addresses the "first mile/last mile" connection in a WMAN. It supports the use of bandwidth between 10 GHz and 66 GHz and standardizes the MAC and PHY layers. It allows for interoperability between devices.

This standard supports the progress of fixed broadband wireless access systems to permit rapid worldwide operation of innovative, cost-effective, and interoperable multivendor broadband wireless access products.

IEEE 802.16 consists of a set of standards, including the following two major ones:

1. *802.16d for fixed WiMAX*: The IEEE 802.16d fixed WiMAX standard was approved in June 2006. It provides fixed point-to-multipoint broadband wireless access service, and the product profile utilizes the OFDM 256-FFT (fast Fourier transform) profile. The 802.16d fixed WiMAX standard supports both time-division duplex (TDD) and frequency-division duplex (FDD) services.
2. *802.16e for mobile WiMAX*: The IEEE 802.16e fixed mobile standard was approved in December 2005. It is based on an early 802.16a WiMAX standard and adds mobility features to WiMAX in the 2-GHz to 11-GHz licensed bands. It allows for fixed wireless and mobile non-line-of-sight (NLOS) applications by basically enhancing orthogonal frequency division multiple access (OFDMA).

WiMAX WiMAX, or Worldwide Interoperability for Microwave Access, was created in April 2001. It is a wireless technology that provides a high-throughput broadband connection over large areas. It is planned in such a way that it performs like a wireless MAN. This technology allows for the connection of all public wireless access points to each other and the Internet, and it is a wireless option for cable and DSL, providing last-mile wireless broadband access.

WiMAX is a point-to-multipoint technology that has a frequency range of 2 GHz to 11 GHz. It also can connect to the network endpoint without a direct line of sight. It provides a linear service area range of up to 31 miles (45 km). It provides a data rate of up to 75 Mbps.

The following are the advantages of WiMAX:

- It is used as a point-to-multipoint broadband technology.
- It can connect Wi-Fi (802.11) hotspots with each other and the Internet.
- It can be used as an alternative to cable and DSL (providing last-mile broadband access).
- It provides services like voice over IP (VoIP), video, and Internet access at the same time.
- It is low cost and easy to install.

IEEE P1451 Standards

IEEE P1451 is a family of smart-transducer interface standards. It describes a set of open network, independent communication interfaces to connect transducers to microprocessors, instrumentation systems, and the control/field network. The key of these standards is the definition of the Transducer Electronic Data Sheet (TEDS). It is a memory device that connects to a transducer and stores the transducer identification, calibration, correction data, measurement range, manufacturer-related information, and more. The IEEE 1451 standards family is sponsored by the IEEE Instrumentation and Measurement Society's Sensor Technology Technical Committee. The IEEE P1451 family includes the following standards:

- *IEEE P1451.0*: This standard defines a set of common commands, common operations, and TEDS for the family of IEEE 1451 smart-transducer standards. A user can access any sensors or actuators in 1451-based wired and wireless networks through this common set.
- *IEEE P1451.1*: This standard is defined as a common object model to describe the behavior of transducers. It defines a measurement model that streamlines the measurement process. It also defines the communication models that are used for the standards, which are included in client-server and public-subscribe models.

- *IEEE P1451.2*: This standard defines a transducer-to-NCAP interface and TEDS for point-to-point communication. The transducers are part of the Transducer Interface Model (TIM).
- *IEEE P1451.3*: This standard defines the transducer-to-NCAP interface and TEDS for a multidrop transducer using a distributed-communications architecture.
- *IEEE P1451.4*: This standard defines a mixed-mode interface for analog transducers with analog and digital operating modes. A TEDS was added to a traditional two-wire, constant-current excited sensor containing a field effect transistor (FET) amplifier.
- *IEEE P1451.5*: The P1451.5 is a working group of wireless standards that provide wireless communication methods and a data format for transducers (sensors and actuators). It improves the reception of wireless technology for transducer connectivity. This standard defines TEDS, which depends on the IEEE 1451 concept and protocols to access TEDS and transducer information. This standard also accepts important wireless interfaces and protocols to make easy use of technically different, existing wireless technology. It does not specify the transducers' design, signal conditioning, or the physical design of a wireless system.
- *IEEE P1451.6*: This standard defines a transducer-to-NCAP interface and TEDS using the high-speed Controller Area Network (CAN) open interface. Intrinsically safe and nonintrinsically safe applications are supported. P1451.6 defines mappings of the 1451 TEDS-to-CAN open dictionary entries as well as communication messages, process data, configuration parameters, and diagnosis information.

ETSI Standards

The ***European Telecommunications Standards Institute (ETSI)*** is an independent association whose aim is to provide standards related to telecommunications, broadcasting, and other information and communications technologies.

ETSI Standards for Wireless Communication

HIperLAN

This is a wireless LAN communications standard that ETSI developed. Table 4-1 summarizes the features of some of the versions of this family. This standard is defined by the Broadband Radio Access Network (BRAN) project in ETSI. The HiperLAN family consists of four versions, which are as follows:

- *HiperLAN/1*: This is the first version of HiperLAN. It has the capacity for communications of up to 20 Mbps in the 5-GHz band.
- *HiperLAN/2*: This is the second version of HiperLAN. It has the capacity for communications of up to 54 Mbps in the 5-GHz band.
- *HiperAccess*: This is used for point-to-multipoint communication.
- *HiperLink*: This is a very high-speed interconnection of HiperLAN and HiperAccess.
- *HiperMAN*: High Performance Radio Metropolitan Area Network (HiperMAN) was developed by the ETSI BRAN group. It is an interoperable broadband fixed wireless communication access system. It operates at radio frequencies between 2 GHz and 11 GHz.

	HiperLAN/1	HiperLAN/2	HiperAccess	HiperLink
Application	Wireless Ethernet (LAN)	Wireless ATM	Wireless local loop	Wireless point-to-point
Frequency range	5 GHz	5 GHz	5 GHz	17 GHz
Data rate	23.5 Mbps	Approximately 20 Mbps	Approximately 20 Mbps	Approximately 155 Mbps

Table 4-1 These are some of the major parts of the HiperLAN family of standards

HiperLAN/1 HiperLAN/1 is an ETSI standard. It operates at a bandwidth between 5.1 and 5.3 GHz, so it does not conflict with microwaves. It is completely ad hoc; it does not require a configuration and central controller.

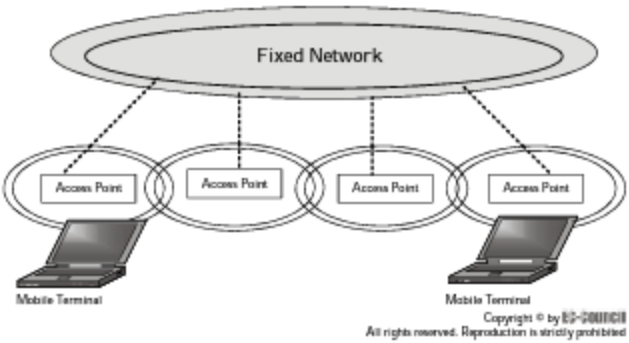


Figure 4-5 This is a HiperLAN/2 network.

As with 802.11, this standard contains the physical and MAC part of the data-link layer. It contains a new sublayer known as the Channel Access and Control (CAC) sublayer. CAC handles channel access requests, depending on the usage of the channel and the priority of the request. From the CAC-layer, hierarchical independence is obtained with the help of the Elimination-Yield Nonpreemptive Multiple Access (EY-NPMA) mechanism.

The following are the characteristics of HiperLAN/1:

- It has a short range of up to 50 m.
- It has low mobility (up to 1.4 m/s).
- It supports both synchronous and asynchronous traffic.
- It transmits sound with a speed of 32 Kbps and 10-ns latency.
- It transmits video with a speed of 2 Mbps and 100-ns latency.
- It transmits data with a speed of 10 Mbps and no latency.

HiperLAN/2 HiperLAN/2 (Figure 4-5) is an efficient, fast communication-network design. It uses the 5-GHz band (5.4 to 5.7), and it has a data rate of up to 54 Mbps. It includes physical, data-link control, and convergence layers. The convergence sublayer works on the physical layer to connect IP, ATM, and Universal Mobile Telecommunications System (UMTS) networks.

HiperLAN/2 provides high-speed access support to various networks:

- Supports 3G mobile core networks
- Supports ATM networks
- Supports IP-based networks
- Supports WLAN systems

The following are some of the features of HiperLAN/2:

- Supports high-speed data transmission
- Has connections that are unidirectional, bidirectional, or multidirectional
- Allocates a particular QoS in bandwidth, delay, bit error rate, and more
- Supports automatic frequency allocation
- Provides authentication and encryption
- Provides handover mobility support
- Is network and application independent
- Helps save power

HiperAccess HiperAccess supports a point-to-multipoint network. It is intended for high-speed (up to 120 Mbps) communications, and it also supports high- QoS fixed wireless access. The HiperAccess standard supports a frequency band above 11 GHz with a high spectral efficiency under line of sight.

The standardizations of HiperAccess focus on solutions that are optimized for frequency bands above 11 GHz (for example, 26, 28, 32, and 42 GHz) with high spectrum efficiency under line-of-sight conditions. The FDD and TDD channel arrangements, as well as HFDD terminals, support a bandwidth of 28 MHz.

The following are some of the features of HiperAccess:

- Supports backhauling for cellular networks such as GSMTM and UMTSTM
- Operates at 25 Mbps
- Provides long-range and fixed-radio connections to customer premises
- Allows for outdoor usage for residential and small- to medium-sized business applications, with coverage of up to 5 km
- Provides wireless access for private networks and public operators
- Provides efficient scheduling performance to support different services
- Provides full QoS
- Provides efficient support of ATM and IP-based core networks
- Is efficient for fast connection control management
- Provides strong security
- Supports robustness against losses of traffic and control information

HiperLink This is a very high-speed radio network for infrastructure-like applications. It is used to interconnect HiperAccess networks or HiperLAN access points into a fully wireless network. It supports the interconnection of HiperLANs and HiperAccess networks at speeds of up to 155 Mbps over a distance of up to 150 m. It operates at a radio frequency of 17 GHz.

HiperMAN HiperMAN was developed by the ETSI BRAN group. It is an interoperable broadband fixed wireless access system and operates at a radio frequency between 2 GHz and 11 GHz. This standard specifies the physical and data-link layers, which are the core-specific network convergence sublayers. It supports data transmission using various broadband frequency ranges, which keeps it from interfering with other wireless devices. HiperMAN is optimized for a packet-switched network.

The following are some of the features of HiperMAN:

- HiperMAN permits point-to-multipoint and flexible mesh patterns.
- It provides frame-based transmissions, where frames accept variable lengths.
- It provides full QoS.
- It supports fast connection control management.
- It provides strong security.
- It has the capabilities of fast adaptation to coding, modulation, and transmit power.

Chapter Summary

- IEEE 802 is a family of IEEE standards that deals with local area networks (LANs) and metropolitan area networks (MANs), mainly for the lowest two levels of the Open Systems Interconnection (OSI) model.
- IEEE 802 contains the physical layer, media access control (MAC) layer, and logical-link control (LLC) layer.
- IEEE 802.3 includes wired Ethernet standards.
- IEEE 802.11 includes wireless networking standards.
- IEEE 802.16 is a standard concerned with WiMAX.

- The European Telecommunications Standards Institute (ETSI) is an independent association whose aim is to provide telecommunications standards.
- ETSI developed the HiperLAN family of standards, which are concerned with wireless networking.

Review Questions

1. Explain the architecture of IEEE 802.

2. What is the function of the physical layer in the architecture of IEEE 802?

3. Describe the MAC frame format in IEEE 802.

4. What is the function of the IEEE 802.1 bridging and management standard?

5. Explain the operations the LLC layer performs for data communication.

6. Describe the 802.10 security standards.

7. Describe the functions of the 802.15 WPAN.

8. Describe the different roles of 802.1X.

9. Describe the architecture of 802.11.

10. Describe the QoS support mechanism of 802.11e.

11. Describe the IEEE P1451 standards.

12. Describe the ETSI standards.

13. Describe the specifications of HiperLAN.

Hands-On Projects

1. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open IEEE Standards Style Manual.pdf and read the content.
2. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open Ethernet IEEE 802.3.pdf and read the content.
3. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open IEEE 802.11.pdf and read the content.
4. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open WirelessNetworkingStandard.pdf and read the content.
5. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open WiMAXWhitepaper.pdf and read the content.
6. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open WI-MAX.pdf and read the content.
7. Perform the following steps:
   - Navigate to Chapter 4 of the Student Resource Center.
   - Open IEEE 802.11 Protocol.pdf and read the content.

Chapter 5

Security Standards Organizations

Objectives

After completing this chapter, you should be able to:

- Understand the Internet Corporation for Assigned Names and Numbers (ICANN) and its role and operations
- Understand the International Organization for Standardization (ISO) and how its standards benefit society
- Describe the structure of the International Telecommunication Union (ITU)
- Describe the structure of the American National Standards Institute (ANSI)
- Describe the structure of the Institute of Electrical and Electronics Engineers (IEEE)
- Describe the structure of the Electronic Industries Alliance (EIA)
- Describe the structure and services of the National Institute of Standards and Technology
- Describe the structure and activities of the World Wide Web Consortium (W3C)
- Describe the responsibilities of the board of directors and the structure of the Web Application Security Consortium (WASC)

Key Terms

Guideline suggested framework used to implement a procedure

Policy high-level statement, goal, or objective

Procedure set of detailed step-by-step instructions on how to achieve specific tasks and goals

Protocol convention or set of rules that controls or enables the connection, communication, and transfer of data between hosts across a network

Standard mandatory activity designed to provide policies with the support structure and specific direction required for policy implementation and enforcement

Introduction to Security Standards Organizations

This chapter focuses on security standards organizations. A ***standard*** is a mandatory activity designed to provide policies with the support structure and specific direction required for policy implementation and enforcement. This chapter discusses many of the major security standards organizations in the world today, including ICANN, ISO, NIST, W3C, and ANSI.

Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization responsible for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic top-level domain (gTLD) and country-code top-level domain (ccTLD) name system management, and root server system management functions.

Operated like a private-public partnership, it is dedicated to preserving the operational stability of the Internet, to promoting competition, to achieving a broad representation of global Internet communities, and to developing policy appropriate to its mission through bottom-up and consensus-based processes.

The late Jon Postel created ICANN in the fall of 1998 in response to a policy statement issued by the U.S. Department of Commerce. The diverse board of ICANN consists of 19 directors.

Role of ICANN

ICANN is responsible for consolidating the management of the technical elements of the DNS to ensure universal resolvability so that all users of the Internet can find valid addresses. ICANN does this by overseeing the distribution of unique technical identifiers used in Internet operations. It also delegates TLD names (such as .com and .info).

ICANN Operations

Under ICANN's structure, governments and international treaty organizations work in partnership with businesses, organizations, and skilled individuals involved in building and sustaining the global Internet. ICANN's participants work collectively to address those issues that are directly concerned with ICANN's mission of technical coordination.

An internationally diverse board of directors governs ICANN and oversees its policy development process. A ***policy*** is a high-level statement, goal, or objective. The president of ICANN directs an international staff working from three continents and ensures that ICANN meets its operational commitment to the Internet community. Figure 5-1 shows the structure of ICANN.

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is the world's largest developer and publisher of international standards. The ISO is a network of the national standards institutes of 157 countries, one member per country, with a central secretariat in Geneva, Switzerland, that coordinates the system. Member organizations work for the development and promotion of international standards. For example, the American National Standards Institute (ANSI) represents the United States. Among the standards, the ISO supports a universal reference model for communication protocols. A ***protocol*** is a convention or set of rules that controls or enables the connection, communication, and transfer of data between hosts across a network. Figure 5-2 shows the process for standard development at ISO.

How ISO Standards Benefit Society

ISO standards benefit the following sections of society in the following ways:

- *For businesses*: The adoption of international standards means that suppliers can base the development of their products and services on specifications that have wide acceptance. This means that businesses using international standards are increasingly free to seek success in many more markets around the world.

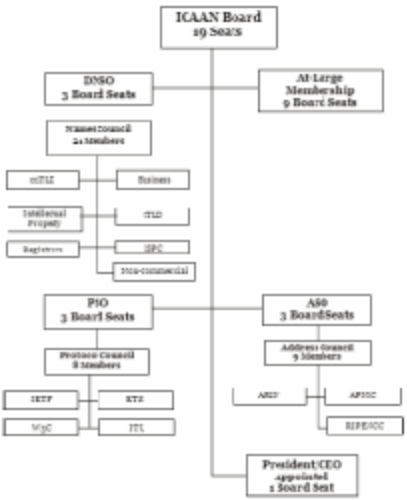


Figure 5-1 This chart shows ICANN's organizational structure.

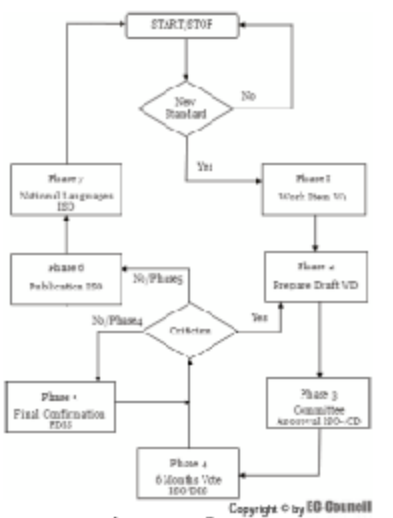
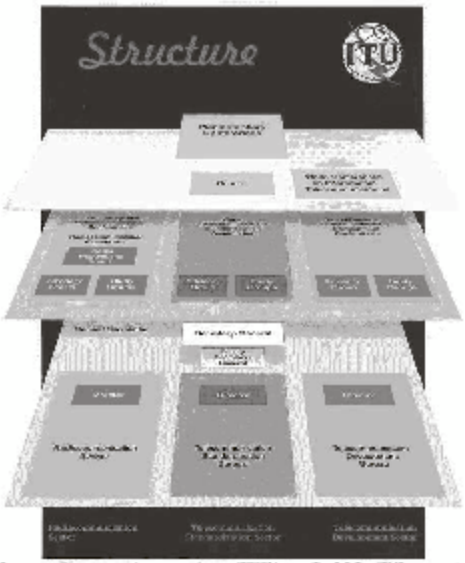


Figure 5-2 This flow chart depicts how standards are developed at ISO.



Source: http://cbdd.wsu.edu/kewlcontent/courses/TR501/images/Fig-3-3-The-ITUStructure.gif. Accessed 2004.

Figure 5-3 ITU is organized into a tiered structure.

- *For customers*: Products and services that are based on international standards open the doors for a wide choice of offerings. This also increases competition among suppliers, which is beneficial to consumers.
- *For governments*: For governments, the international standards provide technological and scientific base applications, and safety and environmental legislation.
- *For everyone*: International standards can enrich the quality of life in general by ensuring that the transport machinery and tools that are used are safe.

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is an intergovernmental organization through which public and private organizations develop telecommunications. It was created in 1865 and became a United Nations agency in 1947. ITU is responsible for adopting international treaties, regulations, and standards governing telecommunications. Historically, the standardization functions were performed by CCITT (International Telegraph and Telephone Consultative Committee) within ITU, but after a reorganization in 1992, the CCITT no longer exists as a separate entity.

ITU develops the standards that support the integration of national communication infrastructures into global networks allowing the seamless exchange of information, data, faxes, or simple voice telephone calls among all the countries in the world.

It works to introduce new technologies into the existing telecommunication network to allow for the development of new technologies such as the Internet, electronic mail, and multimedia.

The ITU manages the sharing of the radio-frequency spectrum and satellite orbital positions, finite resources that are used by a wide range of equipment including mobile phones, television and radio, satellite-based communication systems, aircraft and maritime navigation and safety systems, and wireless computer systems.

It strives to increase the accessibility of telecommunications in the developing world through policy advice, technical assistance, project management, training programs, and information resources, and by supporting partnerships between telecommunications companies, administrations, funding agencies, and private organizations.

ITU consists of 188 member states and more than 450 members from the private sector, all working together to develop cheaper telecommunication systems and bring them within the reach of as many of the world's people as possible.

Understanding the Policy Development Process

CCITT is a committee of ITU. ITU is composed of five subunits:

1. General Secretariat
2. Administrative Council
3. International Frequency Registration Board (IFRB)
4. CCITT
5. CCIR (International Radio Consultative Committee)

The purpose of CCITT is to recommend standards for communication systems. The purpose of these standards is to provide a specification for interconnecting existing telecommunication networks around the world and to provide a uniform access mechanism for these networks.

Approximately 160 nations participate in CCITT. These nations are represented by delegations formed by governmental agencies responsible for telecommunications. In some countries, these agencies also work for their postal, telegraph, and telephone (PTT) administrations. Historically, the United States has participated in CCITT through AT&T representatives, with State Department oversight.

The suppliers of telecommunication equipment and services are not directly involved in the approval of recommendations, but they can participate in the process of developing a recommendation through consultation with their national delegations.

CCITT membership classes are available for governmental participators or observers. The recognized private operating agencies (RPOA) are public or private companies that supply telecommunication services (e.g., AT&T and ITT).

The CCITT body is a plenary assembly made up of all interested administration members and any RPOA with the approval of an administration member. Figure 5-3 shows ITU's structure.

American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) combines the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders around the world.

ANSI oversees the creation, promulgation, and use of norms and ***guidelines*** (suggested frameworks used to implement procedures) that directly impact businesses in nearly every sector. It is also actively involved in accrediting programs that assess conformance to standards including globally recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.

What Is ANSI?

ANSI is a general standards organization in the United States that facilitates the voluntary standards establishment for many areas. The staff at ANSI does not create standards; instead, they combine organizations to provide a natural forum for the development of standards.

Throughout ANSI's history, it has maintained its primary goal of enhancing the global competitiveness of U.S. businesses and American quality of life by promoting and facilitating voluntary consensus standards, conformity, and assessment systems, and promoting their integrity.

It provides the facility to develop America's national standards by accrediting the procedures of standards development organizations (SDOs). A ***procedure*** is a set of detailed step-by-step instructions on how to achieve specific tasks and goals. SDOs work together to develop voluntary consensus standards.

ANSI promotes the use of U.S. standards internationally, supports U.S. policy and technical positions in international and regional standards organizations, and supports the adoption of international standards as national standards when they meet the requirements of the user community.

ANSI is the sole U.S. representative in two major nontreaty international standards organizations: the International Organization for Standardization (ISO) and, via the U.S. National Committee (USNC), the International Electrotechnical Commission (IEC). It plays a strong leadership role as a founding member of ISO in its governing body, while U.S. participation, via USNC, is equally strong in the IEC.

Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is a nonprofit organization and is the world's leading professional association for the advancement of technology. Figure 5-4 shows how IEEE is organized.

A Brief History of IEEE

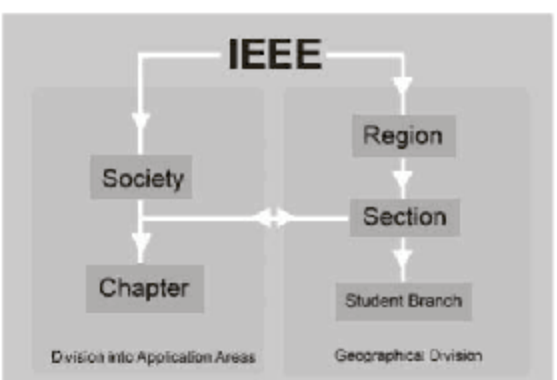
IEEE, an association dedicated to the fostering of technological innovation and excellence for the benefit of humanity, is the world's largest technical professional society. It is designed to serve professionals involved in all aspects of the electrical, electronic, and computing fields and related areas of science and technology that underlie modern civilization. IEEE's roots, however, go back to 1884, when electricity was just beginning to become a major force in society. There was one major established electrical industry, the telegraph, which—beginning in the 1840s—had come to connect the world with a communications system faster than the speed of transportation. A second major area had only barely gotten underway—electric power and light, originating in Thomas Edison's inventions and his pioneering Pearl Street Station in New York.

Electronic Industries Alliance (EIA)

The Electronic Industries Alliance (EIA) is a membership-based organization established to help further development of the electronic industry. It combines individual organizations that together have agreed on certain data transmission standards such as EIA/TIA-232 (formerly known as RS-232).

What Is EIA?

The EIA is a national trade organization that incudes a full spectrum of manufacturers. It is a partnership of electronic and high-tech associations and companies whose aim is to promote the develoment of market competitiveness of the U.S. high-tech industry by using domestic and international policy efforts.



Source: http://homes.esat.kuleuven.be/~isee_sb/images/structuur.png. Accessed 2004.

Figure 5-4 This shows the organization of IEEE.

EIA combines nearly 1,300 member companies whose products and services range from the smallest electronic components to the most complex components used by the defense and space industries, including the full range of consumer electronic products. The structure of EIA enables each sector association to have a unique autonomy. EIA represents the alliance issues that the entire industry agrees are imperative to the success of high technology in the United States.

EIA assists members in navigating the array of global environmetal policy issues affecting their ability to manufacture, market, and sell their products.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce's technology administration. Its primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurement, and standards. NIST was founded in the year 1901 and is a nonregulatory federal agency. Figure 5-5 shows the organizational chart for NIST.

Overview of Services

NIST carries out its mission in four cooperative programs:

1. *NIST Laboratories*: It conducts research in a wide variety of physical and engineering sciences. It is responsible for the industry needs for measurement methods, tools, data, and technology to continually improve the quality of products and services.

Figure 5-5 This shows the organization of NIST, which is mainly made up of laboratories and administrative divisions.

2. *Baldrige National Quality Program*: It promotes performance and excellence among U.S. manufacturers, service companies, educational institutions, and health care providers. It conducts outreach programs and manages the annual Malcolm Baldrige National Quality Award, which recognizes performance excellence and quality achievement.
3. *Hollings Manufacturing Extension Partnership*: It is a nationwide network of local centers offering technical and business assistance to small manufacturers.
4. *Advanced Technology Program*: It accelerates the development of innovative technologies for national benefit by cofunding R & D partnerships with the private sector.

World Wide Web Consortium (W3C)

The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. It is a forum for information, commerce, communication, and collective understanding. The W3C is an international consortium where member organizations, a full-time staff, and the public work together to develop Web standards.

Standards and Guidelines

W3C's primary purpose is to create Web standards and guidelines. Since 1994 W3C has published more than 90 such standards, called W3C recommendations. It also engages in education and outreach, develops software, and serves as an open forum for discussion about the Web. The most fundamental Web technologies must be compatible with one another and permit any hardware and software that accesses the Web to work together.

Overview of Services

W3C Activities

The activities of W3C are organized into groups:

- Working groups (for technical developments)
- Interest groups (for more general work)
- Coordination groups (for communication among related groups)

These groups are made up of participants from member organizations, the team, and invited experts, and produce the bulk of W3C's results. These groups also ensure coordination with other standards bodies and technical communities. Figure 5-6 shows the organization of W3C.

Web Application Security Consortium (WASC)

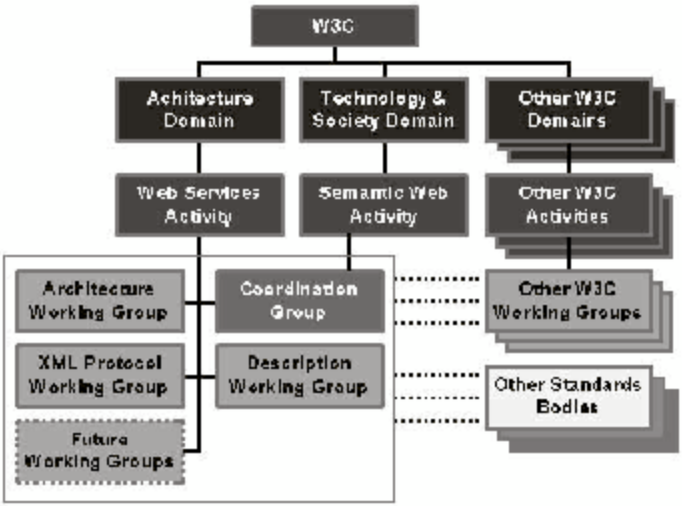
The Web Application Security Consortium (WASC) is an international group of experts, industry practitioners, and organizational representatives who provide open-source and widely agreed-upon best-practice security standards for the Web.

WASC provides the facility to exchange ideas and to organize different industry projects as an active community. It releases technical information, contributed articles, security guidelines, and other useful documentation. Businesses, governments, application developers, security professionals, and software vendors all over the world use WASC material to face the challenges presented by Web application security.

What WASC Will Do

The following are things WASC does:

- It creates an open forum for the creation, discussion, and dissemination of knowledge related to Web application security.
- It instructs the market about Web application security-related matters.
- It creates a vendor-neutral champion/voice of the Web application security industry.



Source: http://www.w3.org/2002/Talks/0826-sb-WSSecIntro/WSActivityOrgChart.png. Accessed 2004.

Figure 5-6 W3C is organized into groups and higher-level bodies.

What WASC Will Not Do

The following are things WASC does not do:

- It does not support vendor-specific technologies, services, or solutions.
- It does not talk on any one person or company's behalf, but rather on the industry's behalf as a champion of Web application security-related matters.

Board of Directors

The board of directors is a five-person group of officers. They are responsible for the management and oversight of the consortium's business dealings, in agreement with the charter. They are also responsible for managing corporate assets, allocating resources, and facilitating the organization's board objectives. The board provides oversight for projects to ensure timely completion and alignment with consortium goals.

Selection Process

The five people on the board of directors are selected by the officers during the first full week of May and December. During the two weeks previous to the next board of directors' vote, any nonemeritus officer of WASC who participated in the previous board of directors' vote may submit himself or herself as a candidate for a board of directors seat.

When the list of candidates is announced, every officer may vote for five of the listed candidates. Immediately following the close of the vote, the five candidates with the most votes are considered the new board of directors.

Overview of Services

Responsibilities The board is responsible for handling the following activities:

- Checking the status of projects that are in progress
- Examining new project offers

- Directing the vote for project plan approval
- Managing the vote for project deliverable approval
- Managing the vote for selected officers
- Managing the semiannual board of directors' selection process
- Reviewing officer and member requirement obligations

Chapter Summary

- The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization responsible for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic top-level domain (gTLD) and country-code top-level domain (ccTLD) name system management, and root server system management functions.
- The International Organization for Standardization (ISO) is the world's largest developer and publisher of international standards.
- The International Telecommunication Union (ITU) is an intergovernmental organization through which public and private organizations develop telecommunications.
- The American National Standards Institute (ANSI) combines the development and use of voluntary consensus standards in the United States, and represents the needs and views of U.S. stakeholders around the world.
- The Institute of Electrical and Electronics Engineers (IEEE) is a nonprofit organization and is the world's leading professional association for the advancement of technology.
- The Electronic Industries Alliance (EIA) is a membership-based organization established to help further development of the electronic industry.
- The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce's technology administration; NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurement, and standards.
- The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential.
- The Web Application Security Consortium (WASC) is an international group of experts, industry practitioners, and organizational representatives who provide open-source and widely agreed-upon best-practice security standards for the Web.

Review Questions

1. Explain the role of ICANN.

_____

_____

_____

_____

2. Explain the operational process of ICANN.

_____

_____

_____

_____

3. What is the structure of the ISO?

4. Explain the benefits of ISO standards.

5. Explain the structure of the ITU.

6. What are the functions of the ITU?

7. Describe the purpose and function of ANSI.

8. Describe the EIA.

9. Describe the structure of NIST.

10. Describe NIST's four programs.

11. Describe the structure of the W3C.

12. What are the responsibilities of the WASC board of directors?

Hands-On Projects

1. Navigate to Chapter 5 of the Student Resource Center. Open allen-to-icann-14apr06.pdf. Read the following topics:
   - Publication of Best Practices and Guidelines
   - Comment Letters
   - Summits, Forums and Conferences
2. Navigate to Chapter 5 of the Student Resource Center. Open Internet Corporation for Assigned Names and Numbers.pdf. Read the following topics:
   - Introduction
   - Role and Responsibilities in ICTs
   - Description and Analysis of ICT Activities
3. Navigate to Chapter 5 of the Student Resource Center. Open 20PembertonEs.pdf. Read the following topics:
   - World Wide Web Consortium Creates Order in Chaotic Internet World
   - Research
4. Navigate to Chapter 5 of the Student Resource Center. Open Introduction to the Internet Standard Management Framework.pdf. Read the following topics:
   - SNMP Protocol Operations
   - Transaction and Ports
   - SNMPv2 and SNMPv3 Operations

Chapter 6

Security Standards

Objectives

After completing this chapter, you should be able to:

- Understand Internet standards and the Standards Review Committee
- Understand the RFC submission process, and obtaining an RFC
- Understand cabling standards, including TIA/EIA-568 and UTP standards

Key Terms

Best Current Practice (BCP) an RFC category; a noncommittal suggested manner of proceeding that is in general the most logical choice

Shielded twisted pair (STP) cable a type of cabling that includes metal shielding over each individual pair of copper wires to protect against external EMI (electromagnetic interference)

Unshielded twisted pair (UTP) cable a type of cable that is not surrounded by any shielding; it is the primary wire type for telephone and computer networking.

Introduction to Security Standards

This chapter focuses on security standards. It begins by discussing Internet standards. It then goes into RFCs, how to submit them, and how to obtain them. The chapter ends with information about some of the common cabling standards for networks.

Introduction to Internet Standards

Internet Standards

The Internet is made possible by the creation and implementation of Internet standards at the technical and development level. Internet standards are developed by the Internet Engineering Task Force (IETF) and are then considered by the Internet Engineering Steering Group (IESG). The IETF is an international community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and the smooth operation of the Internet. The RFC editor is responsible for finalizing standards.

Internet standards provide security for data on the Internet. The security standards support the businesses that take advantage of working with computers and electronic commerce on the Internet. Although there are more data security products and security services available today, the rapid growth in Internet technology also creates new opportunities for hackers and businesses.

Standards Review Committee

The IEEE standards board selects and rejects standards based on its standards review committee's recommendations. This committee ensures that groups follow all procedures and guidelines when creating standards. As per the Project Authorization Requests (PARs), the complete draft of standards comes before the board four times a year or during an approval process. After approval, the IEEE-SA editor edits the standards, the final report is given to the working-group members, and then the standards are published. Once the standards come into use, there may be a need to clarify some portion of them. This is accomplished through an interpretations process based on questions officially submitted to the IEEE-SA. The sponsor makes the interpretation process. Completed interpretations are published on the IEEE-SA Web site, within a set of standards or in a separate interpretations volume. The standards are valid for up to five years after their publication time; during this period the working group develops the extensions of the standards. After five years, the standards are reconfirmed and revised, or withdrawn.

Revisions need PAR approval and follow the normal balloting process (75% return and 75% approval) and approval by the IEEE standards board. Standards that are out of date can be removed by going through a balloting process that requires a 50% return and a 75% approval rate.

RFCs

Requests for comment (RFCs) contain the technical and organizational documents of the Internet, including the technical specifications and policy documents that are submitted by the Internet Engineering Task Force (IETF).

RFCs are numbered consecutively, and these numbers provide a single unique label space for all RFCs. RFCs are published online through a number of repositories, and there is an online index of RFCs.

Categories of RFCs

The following are the categories of RFCs:

- *Standard, Draft Standard, and Proposed Standard*: These standards-track documents are the official specifications of the Internet protocol suite defined by the IETF and its streering group (IESG).
- ***Best Current Practice (BCP)***: This is a noncommittal suggested manner of proceeding that is in general the most logical choice. These are official guidelines and recommendations, but not standards, from the IETF.
- *Information and Experimental*: These non–standards documents may originate in the IETF or may be independent submissions.
- *Historic*: These are former standards that has been deprecated.

RFC Submission Process

RFCs from the IETF

RFCs in a standards-track best current practice (BCP) category and some information and experimental RFCs are created within the Internet Engineering Steering Group (IESG). IESG members include the IETF area directors (ADs) who are responsible for related working groups. The ADs, with IESG concurrence, may allow the documents that the working groups develop to be published.

Independent Submission

An RFC can be written by anyone and submitted independently to the RFC editor for publication. It will be published after a review for technical competence, revelance, and adequate writing. The RFC editor and the IETF also review the RFC for a possible conflict with an IETF process. After completing this process successfully, independent submissions enter the same publication process as an IETF submission.

Finally, the author who is making an individual submission via the IETF or an independent submission via the RFC editor should know that some documents either have to be from the IETF or would benefit from an IETF review. Sometimes, an appeal for an Internet Assigned Numbers Authority (IANA) allocation from a space that has a standard-action IANA rule can be made for a document. This type of action cannot come from independent submissions. This type of document should be processed as an AD-sponsored submission. The authors are responsible for the decision to follow the particular approach from the set of allowed options and for the effort of proposing a Birds-of-a-Feather (BoF) session, convincing the IESG or one of the ADs that the document needs to be sponsored.

Obtaining RFCs

RFCs can be obtained via FTP from *venera.isi.edu*, with the pathname in-notes/rfc*nnnn*.txt (where *nnnn* refers to the number of the RFC). Log in with the FTP username "anonymous" and password "guest."

RFCs can also be obtained via e-mail from *venera.isi.edu* by using the RFC-INFO service. Address the request to RFC-INFO@ISI.EDU with a message body of:

Retrieve: RFC
Doc-ID: RFC*nnnn*

Again, *nnnn* refers to the number of the RFC (four digits are always used, so, for instance, RFC 820's Doc-ID field would be RFC0820). The RFC-INFO@ISI.EDU server provides other ways of selecting RFCs based on keywords and more; for more information, a user can send a message to RFC-INFO@ISI.EDU with the message body "help: help."

Cabling Standards

Various institutions are expanding their networks and are planning to run 1,000-Mbps applications on their LANs to accommodate the demands of the latest operating systems and bandwidth-hungry applications. In this process, they sometimes neglect their cabling systems, and these systems may be old and outdated. Any network foundation with good cabling, proper installation, and proper maintainance should last for many years.

There have been new developments in cabling systems. In the past, unshielded twisted pair (UTP) category 5 cable was commonly installed in networks. ***Unshielded twisted pair cable*** is a type of cable that is not surrounded by any shielding. It is the primary wire type for telephone and computer networking. It is good for 10-Mbps equipment and also handles 100-Mbps LANs for higher network categories; CAT5e, also known as Enhanced Category 5, cable is better than CAT5.

A good cabling system will support voice, data, video, and multimedia systems.

TIA/EIA-568

In 1980, the Telecommunication Industry Association (TIA) started developing methods for cabling buildings, with the intention of developing uniform cabling systems that would support multiple products and environments. In 1991, TIA released the TIA/EIA-568 Commercial Building Telecommunication Cabling Standard. This cabling standard describes how to build and manage a structured cabling system. This means the system will be designed in blocks that have very specific characteristics. These blocks are arranged in a hierarchical manner to develop a unified communication system. This standard defines the use of fiber optic cables (single mode and multimode), shielded twisted pair (STP) cables, and UTP cables. *A **shielded twisted pair cable*** is a type of cabling that includes metal shielding over each individual pair of copper wires to protect against external EMI (electromagnetic interference).

The initial TIA/EIA-568 standard was followed by several updates. In 2000, the major updated standard, which incorporates previous changes, was released.

- *TIA/EIA-568-A-1995 (Commercial Building Telecommunication Cabling Standard)*: It provides the standard for building cable systems for commercial buildings that support data network, voice, and video. It also describes the technical and performance criteria for cabling.

Figure 6-1 UTP cable contains four pairs of wires, with the wires of each pair twisted around each other. The tighter the twisting of the cable pairs, the greater the integrity and transmission capacity.

- *TIA/EIA-568-A Updates (1998–1999)*: In this time period, the TIA/EIA-568 standard was updated several times. Update A1 outlines propagation-delay and delay-skew parameters. Update A2 defines miscellaneous changes. Update A3 specifies needs for bundled and hybrid cables. Update A4 specifies next and return loss requirements for path cables. Update A5 specifies performance needs for CAT5e.
- *TIA/EIA-568-B.1-2000 (Commercial Building Telecommunication Wiring Standard)*: This defines CAT5e cable, which is a preferred cable type that can support the minimum acceptable performance levels.
- *TIA/EIA-569-A-1995 (Commercial Building Standard for Telecommunication Pathway and Space)*: It describes how to build pathways and spaces for telecommunication media.
- *TIA 570-A-1998 (Residential and Light Commercial Telecommunications Wiring Standard)*: It specifies the standard for residential cabling.
- *TIA/EIA-606-1995 (Grounding and Bonding Requirements)*: This standard defines the grounding and bonding requirements for telecommunication cabling and equipment.

UTP

There are two types of twisted pair cables: shielded and unshielded. Unshielded twisted pair (UTP) cable (Figure 6-1) is the more popular. It has four pairs inside the cable, and the wires of each pair are twisted around each other to avoid interference with the other pairs in the cable. The Telecommunication Industry Association/Electronic Industry Association (TIA/EIA) has defined standards of UTP and has rated several categories of wires. These categories are described in Table 6-1.

Type	Use
Category 1 (currently unrecognized by TIA/EIA)	Previously used for POTS telephone communications, ISDN, and doorbell wiring
Category 2 (currently unrecognized by TIA/EIA)	Previously was frequently used on 4-Mbps Token Ring networks
Category 3 (currently defined in TIA/EIA-568-B)	Used for data networks using frequencies up to 16 MHz. Historically popular for 10-Mbps Ethernet networks.
Category 4 (currently unrecognized by TIA/EIA)	Provided performance of up to 20 MHz and was frequently used in 16-Mbps Token Ring networks
Category 5 (currently unrecognized by TIA/EIA)	Provided performance of up to 100 MHz and was frequently used in 100-Mbps Ethernet networks. May be unsuitable for 1000Base-T Gigabit Ethernet
Category 5e (currently defined in TIA/EIA-568-B)	Provides performance of up to 100 MHz and is frequently used in both 100-Mbps and 1000Base-T Gigabit Ethernet networks
Category 6 (currently defined in TIA/EIA-568-B)	Provides performance of up to 250 MHz, more than double categories 5 and 5e
Category 6a (currently defined in ANSI/TIA/EIA-568-B.2-10)	Provides performance of up to 500 MHz, double that of category 6. Suitable for 10GBase-T.

Table 6-1 These are the rated categories of UTP *(continues)*

Type	Use
Category 7 (an informal name applied to ISO/IEC 11801 Class F cabling)	This standard specifies four individually shielded pairs (STP) inside an overall shield. Provides performance of up to 600 MHz.
Category 7a (an informal name applied to Amendment 1 of ISO/IEC 11801 Class F cabling)	Provides performance of up to 1000 MHz. Suitable for 40-gigabit Ethernet.

Table 6-1 These are the rated categories of UTP *(continued)*

The categories of UTP each consist of different data ranges. If someone is designing a 10-Mbps Ethernet network and is considering saving costs by buying CAT3 wire instead of CAT5, CAT5 cable provides more "room to grow" as transmission technology improves. UTP in both CAT3 and CAT5 has a maximum segment length of 100 meters. CAT6 cable is relatively new and is used for gigabit connections. This is similar to CAT5 cable but contains a physical separator between the four pairs to reduce interference.

Chapter Summary

- The Internet Engineering Task Force (IETF) develops Internet standards.
- The IEEE standards board selects and rejects standards based on its standards review committee's recommendations.
- Requests for comment (RFCs) contain the technical and organizational documents of the Internet.
- The TIA/EIA-568 Commercial Building Telecommunication Cabling Standard describes how to build and manage a structured cabling system.
- Unshielded twisted pair (UTP) cable is the more popular type of twisted-pair cable. It has four pairs inside the cable, and the wires of each pair are twisted around each other to avoid interference with the other pairs in the cable.
- There are several categories of UTP cable.

Review Questions

1. What is an Internet standard?

2. Explain the standards review committee.

3. Define the submission process for RFCs.

4. Explain the process for obtaining an RFC.

5. Explain the cabling standards.

6. What are the categories of UTP cable?

Hands-On Projects

1. Navigate to Chapter 6 of the Student Resource Center. Open ICT networks.pdf. Read the following topics:
   - Guide to ICT Networks Cabling Standards
   - Horizontal Cabling Standard
   - Cable Routes
2. Navigate to Chapter 6 of the Student Resource Center. Open WhitePaper_Intro to Internet-based SCADA.pdf. Read the following topics:
   - Background
   - Benefits of Choosing the Internet
   - Interfacing Equipment to Internet-Based SCADA Systems
3. Navigate to Chapter 6 of the Student Resource Center. Open Internet Standards for the Web.pdf. Read the following topics:
   - Categories for Web Standards
   - Platform for Internet Content Selection

Index

O

P

R

S

T

U

V

W

Z