All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams

A Certification Guide with 2200 Sample Questions and Answers with Comprehensive Explanations
First Edition (Jan 2012)

Thaar AL_Taiey
MSNE, MSSE, BSEE, IWWHS, ITIL

ThaarTechnologies Publishing

All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams

A Certification Guide with 2200 Sample Questions and Answers with Comprehensive Explanations

First Edition (Jan 2012)

Thaar AL_Taiey
MSNE, MSSE, BSEE, IWWHS, ITIL

All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams

A Certification Guide with 2200 Sample Questions and Answers with Comprehensive Explanations

First Edition (Jan 2012)

Thaar AL_Taiey

ThaarTechnologies publishing

All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams A Certification Guide with 2200 Sample Questions and Answers with Comprehensive Explanations First Edition (Jan 2012)

Thaar AL_Taiey books may be ordered through booksellers or by contacting:

ThaarTechnologies
www.thaartechnologies.com
SAN: 8600503

ISBN: 978-0-9831212-6-8 (ebk)

Printed in the United States of America
Lightning Source Inc.
1246 Heil Quaker Blvd.
La Vergne, TN USA 37086

ThaarTechnologies rev. date: JAN/2012

Designer and Editor:
Thaar AL_Taiey
Technical reviewer:
Thaar AL_Taiey

Comments

The following reviews are received for the previous books of the author:

kirkusreviews
“http://www.kirkusreviews.com/book-reviews/non-fiction/thaar-al_taiey/complete-one-week-preparation-cisco-ccentccna-icnd/”
Editor Review (reviewed on November 23, 2010)
An ambitious collection of 2,000 practice questions and answers that attempts to familiarize the reader with the first CISCO networking exam, the CCENT.
Through the device of questions and answers, AL_Taiey encourages students to carefully read about the concepts essential to an understanding of how computer networks function and the process by which they are designed. By formatting the book into sections that map to critical concepts in the CISCO curriculum, AL_Taiey aids the student in concentrating on the areas in which they may feel they need to improve. The questions are direct even if the language is sometimes awkward. On several of AL_Taiey's "check all that apply" style of questions, all the listed answers are correct, which forces the reader to carefully read all of the foils. This is a valuable skill if one is preparing for any CCNA exam. While the book may prepare someone for the written parts of the exams, tackling the entire book in one week, as suggested by the title, would be a daunting task. AL_Taiey describes the step-by-step processes by which one configures routers and switches, and this provides a good base of technical knowledge, but the lab experiences, simulations and practical knowledge required to pass this particular exam will have to come from somewhere else. For a student who has worked in the field or someone who has had access to the CISCO Academy curriculum, this book would function well as additional study guide/test prep material. But without this foundation, the most likely outcome would be an improved score on the written portion of the test; what is commonly referred to as a "paper certification."
Addresses the written aspect of the CISCO Certification process but the reader will need to fill in the practical portion from other sources, or better yet from work experience, before attempting the CCENT Exam.

Great CCENT Preparation, October 6, 2010
By J_Williams (Boston, MA) Amazon.com
This book was very instrumental in preparing me for the CCENT exam. After going through every chapter and answering all the questions, I had a strong grasp of the objectives. It took me longer than a week, but persistence and perseverance paid off. I can't wait for his ICND 2 book to become available.

Read This Book, October 1, 2010
By Edward (USA) Amazon.com
Thanks to this book and the CCENT boson simulation, I completely understand the CISCO CCENT by one week. This is the first book I have read that uses this way of writing. It simply describes all CCENT topics by more than 2000 questions and answers. Each section of the book is written in the form of questions and answers, which makes the preparation of the CCENT certification very easy. Also, I found it a complete guide and it helped me as a beginner in the CISCO networking.

Name: Joel Philip, Dec 2009
Thank you for writing your CCNA ICND1 study guide book. I really appreciate the way you presented the content and this is how all books concerning technology should be written, I hope that I can experience one of your other books in the future. Thank you again.

About the Author

Thaar Al_Taiey holds a Master degree (MSc) in Nuclear Engineering (MSNE) specialist in Software Engineering (MSSE) and BSc degree in Electrical Engineering (BSEE). He also holds an ITIL V3 Certificate in the IT Service Management. He has more than 20 years' experience in Automated System fields. His experience in Distributed Control Systems (based VME), Internetworking based CISCO, 3COM, HP, UNIX Operating Systems (Ultrix-32, OSF-1, SCO, Solaris and Linux), Oracle ORDBMS and Windows OS. In these areas, he works as IT consultant and supervisor, Data Center Manager, Network manager, Network Designer and Sr. network Engineer, UNIX System administrator, Oracle DBA, Windows System administrator and technical support engineer. In the field of training, he has instructed and developed several technical courses including CISCO certified courses. Mr. AL_Taiey is the leading scientist for many thoughts and ideas in several fields of technology. For the past decade, AL_Taiey has been closely involved with the computer and networking system development. He is the author/co-author of several technical papers and books. He is the Chairman of ThaarTechnologies and is a member of the IWWHS.

Author Books

In addition to this book, Mr. Thaar AL_Taiey has several other books in the field of technology:

1. 4 in 1: The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three CISCO Simulated Exams A Certification Guide with over 2160 Sample Questions and Answers with Comprehensive Explanations Third Edition (Jan 2011), ISBN: 978-0-9831212-4-4 (pbk), ISBN: 978-0-9831212-5-1 (ebk)
2. The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822: A Certification Guide with over 2000 Sample Questions and Answers with Explanations Second Edition (March 2011), ISBN: 978-1-46200-934-3, ISBN: 978-1-46200-935-0 (ebk).
3. 4 in 1: The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three CISCO Simulated Exams A Certification Guide Based over 2160 Sample Questions and Answers with Comprehensive Explanations Third Edition (Dec 2010), ISBN: 978-0-9831212-2-0 (pbk), ISBN: 978-0-9831212-3-7 (ebk)
4. 3 in 1: The Complete Simulated Three CISCO Exams for the CISCO CCNA/CCENT ICND1 Certification Exam 640-822 with 160 Most Difficult Questions and Answers with Comprehensive Explanations (First Edition Nov 2010), ISBN: 978-0-9831212-0-6 (pbk), ISBN: 978-0-9831212-1-3 (ebk).
5. The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822: A Certification Guide Based over 2000 Sample Questions and Answers with Explanations Second Edition (July 2010), ISBN: 978-1450237055, ISBN: 978-1-4502-3706-2 (ebk).
6. CCNA ICND1 640-822 CCENT Study Guide and Examination Guide Q&A, First Edition Sept 2008, ISBN: 978-1419667589.

To all my family!
All my thanks!

Table of Content

Contents

List of Figures

CHAPTER 1 INTERNETWORKING ESSENTIALS

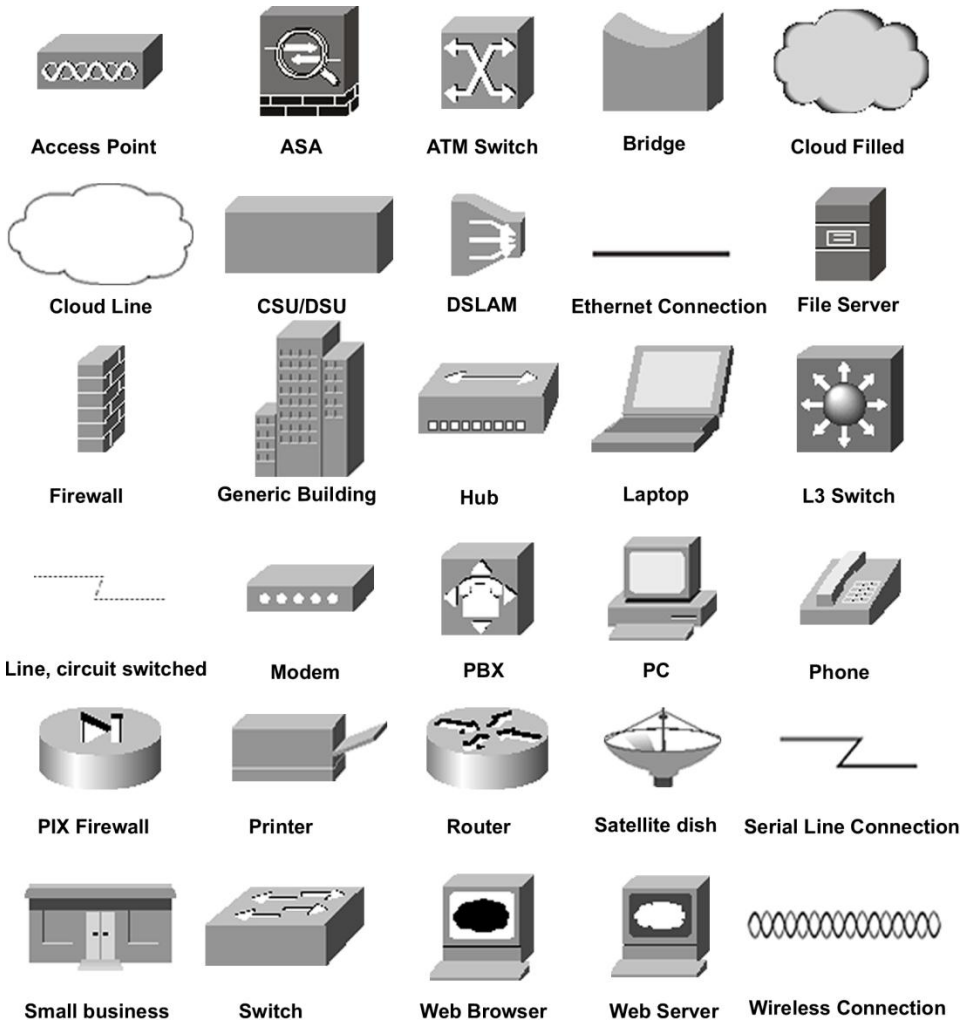
CHAPTER 2 INTERNETWORKING IP PROTOCOL AND IP ADDRESSING

List of Exhibits

List of Tables

List of Exams' Engines

CISCO Icons Used in This Book



Command Syntax Conventions

The CISCO IOS Command Reference conventions are used in this book to present command's syntax. These conventions are described as follows:

- **Bold** indicates commands and keywords that are entered literally by the user.
- Italic indicates arguments for which actual values are supplied.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction:

The book explains CISCO CCNA/CCENT internetworking routing and switching concepts and guarantees the certification to the readers, with a unique presentation in the field of internetworking. It is written like usual textbooks. The differences are; in the way of presenting the required information, which is so simple, the addition of more than 2200 learning questions, and the built-in of 13 exam engines and flash cards. The learning questions, at the end of a chapter, represent a review to the information presented in that chapter as well as provide an easy way for the preparation of the real exam. The questions are made to focus on the important information. You have two options to read the questions and their answers, either by using the built-in exam engine at the end of each chapter or by reading the questions and their answers in the EBook. With more than 840 pages, the book includes explanatory text and provides new types of test formats to simplify both the exam and the presenting of the information to the readers, including over 2200 challenging multiple-choices-single-answer, multiple-choices-multiple-answers, fill-in-the-blank, testlet, drag-and-drop, and simulation test formats. A variety of internetworking scenarios and exhibits are used in this book to illustrate the topics related to the CISCO internetworking fundamentals. In line with modern training and teaching methodology, the questions are included to encourage the reader to stop and think, as well as to test his knowledge in preparation for a successful CCNA CCENT examination.

The book also provides you three built-in CISCO CCNA/CCENT exams' engines. The exams mimic the format on real CISCO exams. The exams are highly organized, so that the reader can easily understand the concepts of the exams. To be more familiar with the real CISCO exam, each exam in this book contains only 50-60 questions. Moreover, the answers of the questions are comprehensively described so that you could understand the concepts behind each question very well and be more confident on the CISCO exam. The exams are made so that you could feel like on real CISCO exams. Therefore, the questions in this book require the same level of analysis as the question on the CCNA/CCENT ICND1 exams. Varieties of internetworking designing and troubleshooting scenarios are described in this book. While these scenarios prepare you for the exam, you will obtain strong experiences on CISCO switches, CISCO routers, CISCO internetworking and the associated protocols, and technologies. The three Simulated CISCOexams make you more confident in the real CISCO exam.

CCENT is the essential certification for the CISCO internetworking routing and switching track. Understanding the CCENT topics and passing this exam successfully, are crucial for those who want to be an Internetworking professional, and is an easy mission, just follow this book. The current track of the CCNA routing and switching contains two exams and two certifications, the CCENT/ICND1 exam 640-822 and the ICND2 exam 640-816. However, it is possible to obtain the CCNA exam 640-802 by one exam and one certification. Now, CCENT and CCNA are the most popular entry-level networking and internetworking certification programs. The CCENT certification proves that you have a firm foundation in the networking and internetworking field, and it proves that you have a solid understanding of IP protocol, IP routing, switching, and many of CISCO device's configurations.

The book provides in-depth coverage of all official CCNA CCENT exam objectives and uses 2800 router, 1841 router, catalyst 2960 switch, and many other CISCO devices to clarify the required concepts. It also provides an up-to-date information for the newest catalyst 2960-S switch and 802.11n wireless technology. It provides objective-by-objective coverage of all the material the student needs to know for the exam, signaling out critical information, outlining necessary procedures, and identifying the exam essentials.

The book is composed of ten chapters. Each chapter treats each internetworking entity with clear, simple, easy-to-follow sections, text boxes and numerous conceptual figures. The book contains more than 313 Figures, 33 Exhibits, 150 Tables, and hundreds of CISCO Switches' and Routers' Configurations. At the end of each chapter, a number of learning questions, exam engine with flash cards and a list of the commands, which are used in that chapter, are given. To make the reader/student more familiar with the CISCO exam, which is not requiring explaining the answer, some of the answers are not provided with explanations. However, explanations for these answers can be obtained easily from their questions. This will preserve the reader time by eliminating all the repeated information and it will not waste his/her time by extra statements. To encourage the reader to stop and

think as well as to test his knowledge, the answers are not given directly after the learning questions; instead, the answers are listed in Appendix A with complementary discussions.

This book uses mainly the passive voice way of writing to give the reader strong-straightforward information without confusing the reader by extra-not required statements. This way of writing is also used by CISCO for devices' configurations, and by several computer technical books and operating systems; hence, the reader will be more familiar with CISCO devices' configurations while he/she reads this book.

The 2200 questions are distributed across the book as shown below:

Chapter 1: Internetworking Essentials	312
Chapter 2: Internetworking IP Protocol and IP Addressing	308
Chapter 3: Subnetting IP Network and VLSMs	85
Chapter 4: Internetworking OS CISCO Devices	239
Chapter 5: Internetworking Routing Protocols	233
Chapter 6: Internetworking Switching	219
Chapter 7: Internetworking OS Management Facilities	216
Chapter 8: Internetworking WAN Technologies	188
Chapter 9: Internetworking Wireless Technology: an Introduction	143
Chapter 10: Internetworking Security: an Introduction	94
Exam E1	52
Exam E2	54
Exam E3	54

This book is a unique one that is designed to offer both the CCNA/CCENT study guide and examination guide, and includes 13 built-in exam engines with flash cards. The book covers essential topics on the Internetworking and security that can be understood, even if the students do not have a technical background. The book is necessary for any CISCO Internetworking and security related certifications. It is designed and organized for absolute beginners as well as for professional in CISCO internetworking. For beginners to be able to follow the train of thought and to ease the presenting of the technical information to them, the book gradually presents the information by highly organized only ten chapters, and then each chapter is decomposed into a number of sections and subsections. The TRUE/FALSE and Correct/Incorrect types of questions are used to review the important information easily to the beginners. For those who have a good technical background and ready for certification, the book can be used as an additional technological certification guide, and the learning questions and the three exams can be used as a refresher for their information before taking the exam. Moreover, Questions like "Try to decide which option gets in which blank" and "Match … etc." are used as a simulated "Drag-and-drop" type of questions in the exam. Therefore, the book knowledge is what the student needs to be a successful networking professional, and it is a valuable technological resource for those on the job with internetworking.

By understanding perfectly the information presented in this book, internetworking-engineering basics and answering the CCNA CCENT exam related questions would be guaranteed. The main questions herein are intended to reflect the type of questions presented on the CCNA and CCENT tests.

The book gives the student the right foundation to overtake the CCNA/CCENT exam in a straightforward-easy way with extreme confidence and high scores from the first time, by one week. More information and a free chapter can be found on thaartechnologies site "thaartechnologies.com/CCENT2010/CCENT2010.htm." Moreover, you can use CISCO key terms found on "www.chahada.com/docs/glossary.doc "as a glossary for this book.

The following CISCO CCNA/CCENT topics are described carefully in this book:

FIRST.	**Describing the operation of computer data networks**
SECOND.	**Describing the required CISCO Devices for CCENT**
THIRD.	**Operating CISCO Switches and Routers**
FOURTH.	**Implementing small switched CISCO networks**
FIFTH.	**Implementing an IP addressing scheme and IP services to meet the network requirements for small and large offices**
SIXTH.	**Implementing a small and a large routed network**
SEVENTH.	**Managing and verifying CISCO switches and routers**
EIGHTH.	**Explaining and selecting the appropriate administrative tasks required for a WLAN**
NINTH.	**Implementing and verifying several WAN links**
TENTH.	**Identifying security threats to a network and describing general methods to mitigate those threats**
ELEVENTH.	**Describing Wireless technology**
TWELFTH.	**Examining Yourself by Three CISCO Simulated CCENT/CCNA Exams**

The book covers all the CISCO CCNA/CCENT ICND1 exam objectives and provides the following features:

- **13 Built-in Exam Engines with 2200 Q&A**
- **Three Built-in CISCO Simulated Exams' Engines**
- **Built-in Flash Cards**
- **More than 2200 Q&A with explanations and examples**
- **Easy to read**
- **Easy to understand**
- **Easy to pass the exam by one week and from the first time**
- **No waste of time**
- **All expected Q&A**
- **Up to date testing techniques**
- **Enjoyment of CCNA/CCENT Learning**
- **Guaranteed the CCNA/CCENT Examination**
- **All types of the CISCO Exam Q&As**
- **Multiple-choice single answer**
- **Multiple-choice multiple answer**
- **Drag-and-drop**
- **Fill-in-the-blank**
- **Testlet**
- **Simulations**

Goals of the Book

The following are the main goals of this book:

1. Providing a self-study guide and a self-examination guide resource that covers all the CISCO CCNA/CCENT topics for 640-822 (ICND1) exam as well as the ICND1 material of the 640-802 (CCNA) exam.
2. Helping examiners to obtain the certification by one week and by one book
3. Providing all expected Q&As that can be faced in the 640-822 (ICND1) exam as well as the ICND1 part of the 640-802 (CCNA) exam.
4. Presenting the information in an easy way that makes the examiners prepare the exam directly while they are reading the book.

5. Helping network engineers to become familiar with CISCO switches, CISCO routers, CISCO internetworking and the associated protocols and technologies.
6. Providing Three Built-in CISCO Simulated Exams' Engines.
7. Providing 13 Built-in Exam Engines with 2200 Q&A and Flash Cards.

How to Use the Book

To read and understand the concepts behind this book easily, it is better to follow the guidelines below:

1. Read each chapter section by section.
2. Read and understand each section separately.
3. Read and answer the learning questions, at the end of each chapter, and their answers. You have two options to do this, either by using the built-in exam engine at the end of each chapter or by reading the questions and their answers in the e-book.
4. Read the book chapter by chapter from chapter one until chapter ten.
5. Exam yourself by the Three CISCO simulated exams in Appendix B. You have two options to do this, either by using the built-in exam engine at the end of each exam or by reading the questions and their answers in the e-book.

By doing so, you will obtain the following:

- Easily reading the whole book
- Easily understanding the subjects one by one
- Easily passing the exam
- No waste of time
- Enjoyment of CCENT Learning

This book covers all the CISCO CCENT/CCNA exams topics and presents three Simulated CISCOExams carefully compiled and written by thaar al_taiey. Try to understand the concepts very well and then, answer the learning questions, at the end of each chapter. The learning questions, at the end of a chapter, represent a review to the information presented in that chapter as well as they provide an easy way for the preparation of the real exam. The questions are made to focus on the important information.

To complete the book and take the exam successfully by one week, the following timetable can be followed: However, if you do not have a one year of experience, it is recommended to use a Network Simulator software while you are reading this book.

Day 1: Chapter 1, and Chapter 2. Mark the points that you need to repeat.
Day 2: Chapter 3, and Chapter 4. Mark the points that you need to repeat.
Day 3: Chapter 5, and Chapter 6. Mark the points that you need to repeat.
Day 4: Chapter 7, and Chapter 8. Mark the points that you need to repeat.
Day 5: Chapter 9, and Chapter 10. Mark the points that you need to repeat. Then, Test yourself using the three CISCO simulated exams, which are founded in Appendix B of this book.
Day 6: Review to the points that you marked to be repeated. Then, test yourself again using the three CISCO simulated exams, which are founded in Appendix B of this book.
Day 7: Take the real exam.

The Differences Between this Book and the other CCENT/CCNA Books by the Author Thaar AL_Taiey

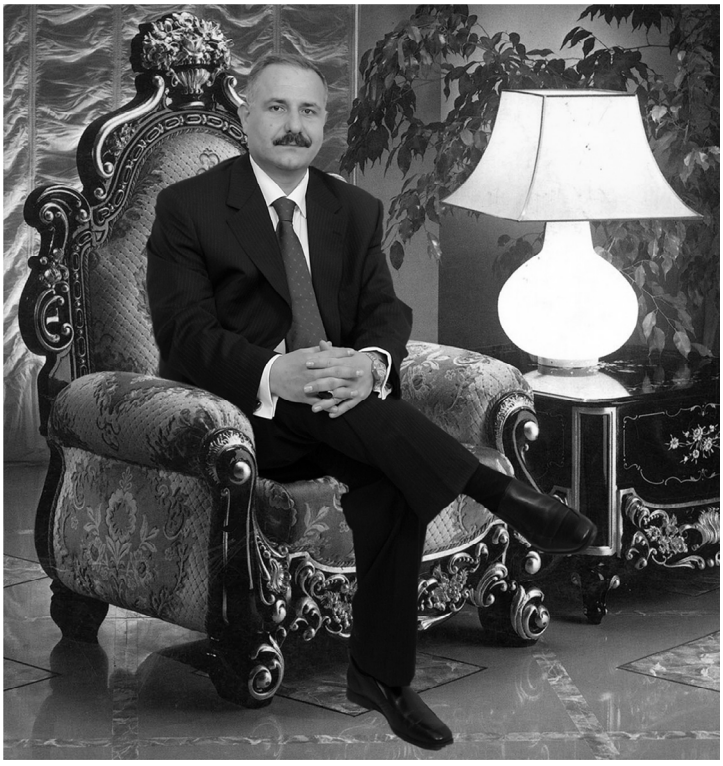
To cover the readers' needs, author Thaar AL_Taiey wrote the CCENT/CCNA certification guides using two different ways. The first way is based on the questions and answers, which means that the book is not a usual textbook, instead, each section of the book is written in the form of questions and answers. The second way is a usual textbook and the questions are put at the end of each chapter. Therefore, you need only to buy the book(s), which is/are suitable to you.

Based Questions and Answers Books

- 4 in 1: The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three CISCO Simulated Exams A Certification Guide Based over 2160 Sample Questions and Answers with Comprehensive Explanations Third Edition (Dec 2010), ISBN: 978-0-9831212-2-0 (pbk), ISBN: 978-0-9831212-3-7 (ebk)
- The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822: A Certification Guide Based over 2000 Sample Questions and Answers with Explanations Second Edition (July 2010), ISBN-13: 978-1450237055, ISBN: 978-1-4502-3706-2 (ebk).
- CCNA ICND1 640-822 CCENT Study Guide and Examination Guide Q&A, First Edition Sept 2008, ISBN-13: 978-1419667589.

Usual TextBooks

- 4 in 1: The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three CISCO Simulated Exams A Certification Guide with over 2160 Sample Questions and Answers with Comprehensive Explanations First Edition (Jan 2011), ISBN: 978-0-9831212-4-4 (pbk), ISBN: 978-0-9831212-5-1 (ebk)
- The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822: A Certification Guide with over 2000 Sample Questions and Answers with Explanations Second Edition (March 2011), ISBN: 978-1-46200-934-3, ISBN: 978-1-46200-935-0 (ebk).



CHAPTER 1 INTERNETWORKING ESSENTIALS

In this chapter, some fundamental concepts and terms that can be used in the internetworking are described.

This chapter summarizes some common themes presented throughout the remainder of this book. The chapter focuses mainly on mapping the Open System Interconnection (OSI) model to networking and internetworking functions; OSI model represents the building blocks for internetworks. The advantages of networking models are also stated in this chapter. Understanding the conceptual model helps understanding the complex pieces that make up an internetwork. This chapter also describes in details the concepts of Networking, Internetworking, Physical and Logical Network Topologies, and Ethernet LAN.

The following topics are emphasized in this chapter:

- Networking essentials
- Internetworking essentials
- Internetworking evolving
- Internetworking models
- OSI reference model
- OSI encapsulation and de-encapsulation terminologies
- Ethernet LANs
- Data transmission types
- CSMA/CD algorithm
- Ethernet addressing
- Ethernet connection and cabling

By understanding perfectly the information presented in this chapter and answering the 312 learning questions at the end of this chapter, understanding OSI reference model, understanding Ethernet LAN, and answering the CCNA/CCENT exam related questions will be guaranteed. The main questions herein are intended to reflect the type of questions presented on the CCENT Test.

Networking Essentials

In this section, networking essentials are presented and the types of networking topologies are described.

A network is a collection of connection devices (NICs-Network Interface Cards, routers, switches, firewalls) and end system machines (PCs, servers) interconnected together by some means. Networks carry data in many types of environments, including homes, and up to large enterprises. Networks also carry data in many types of media, including wired and wireless. To accomplish it tasks, network uses many types of connection devices such as NICs, hubs, bridges, switches and routers. These devices will be discussed deeply throughout this book.

Network Functions and Benefits

Today, the main function of computer networks, in addition to share and exchange information between computer machines, it provides communication. In business, networks play a major role. It simplifies and streamlines business processes through the use of data, application and hardware sharing.

Networks make rapidly data and information exchanging. Therefore, business's resources can be used more efficiently. However, several types of resources can be shared by computer networks. This includes but is not limited to: Data and applications, Physical resources, Network storage, Backup devices and of course networking devices and media. Furthermore, users of the network can use many types of networking applications, such as, E-mail, Web browsers, Internet talk, instant messaging, Download application, Broadcasting alerter, RSS feeds, Books reader, Collaboration and Database.

Generally, network applications can be one of the following types; system-to-system batch applications, user interactive applications, and user real-time applications.

Note: The terms above and several other terms in this chapter are given without further discussion because they are out of the scope of CCENT exam and this book does not want to confuse the reader by extra-information. However, more detail can be found from www.google.com.

Networks can be described and compared according to network performance and structured. This includes: Speed, Cost, Security, Availability, Scalability, Reliability, Manageability, and Topology. Today, cost of the network becomes the least affecting factor when selecting the network and factors such as speed, security and easily managed network become the main factors for selecting the network. However, this depends on the importance of the network to the business process.

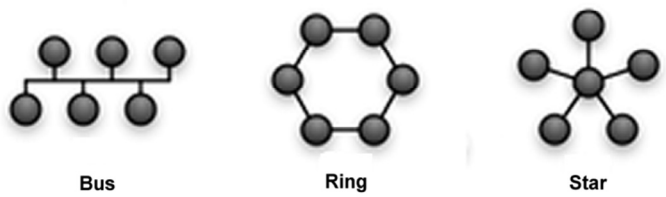
Physical and Logical Network Topologies

Topology defines the interconnection method used between devices, including the layout of the cabling and all paths used in data transmissions. Networks have two types of topologies; the physical and logical topologies. The physical topology is the arrangement of the network (nodes) devices, end systems (laptops, PCs and servers) and the network cables in wired networks. The logical topology, on the other hand, is the mapping of the data flows between the nodes in the network that forming the physical topology.

Physical Network Topology

As stated above, the physical topology is the arrangement of the network devices, end systems (laptops, PCs and servers) and the network cables in wired networks. Some of these topologies depend on the type of cabling that will be installed. Types of cables that are used in the network will be described in the following sections. However, the three basic categories of physical topologies are: Bus, Ring and Star. Figure 1-1 shows the basic physical topologies used in networking.

Figure 1-1 The Basic Physical Topologies



Bus Topology

In this topology, all network devices and automated machines are cabled together in a line. Each machine is connected to the single bus cable through some kind of connector. The main cable segment must end with a terminator that absorbs the electrical signal when it reaches the end of the cable. Since only one cable is utilized, it can be a single point of failure. If the network cable breaks, the entire network will be down, since there is only one cable. This is the main disadvantage of the bus network. Using only one cable, on the other hand, will make the transfer speed between the computers on the network faster. The bus topology includes both linear bus and distributed bus topologies. An example of this topology is a Thicknet Ethernet cable.

Ring Topology

In this topology, all network devices and automated machines are cabled together with the first device connected

to the last to form a ring. This means that each machine is connected to the network in a closed loop or ring. In the ring topology, data is transmitted within a "token". Token travels around the ring. If a machine wants to transmit data, it adds that data and the destination address to the token. The token move around the ring until it finds the destination device, which takes the data out of the token. The primary advantage of this topology is that no token collisions occur. On the other hand, the primary disadvantage of ring topology is the failure of one machine will cause the entire network to fail. Two types of ring topology exist: single-ring and dual-ring. As names imply, the first one uses one ring, whereas the second one uses two rings to transmit the token. The dual-ring uses two rings to allow token to be sent in both directions. This design provides redundancy as compared with the single-ring design, meaning that if one ring fails, token can be transmitted on the second ring.

Star Topology

In this topology, all network devices and automated machines are connected together by a central cabling device. In local area networks where the star topology is used, each machine is connected to a central hub/switch. This will provide each machine on the network a dedicated, point to point connection to the central hub/switch. An advantage of the star topology is the simplicity of adding other machines. Another advantage of using such a topology is that when a cable connected one machine to a central hub/switch is broken, only that one machine is affected and disconnected from the network, and the rest of the network remains operational. This advantage is important and it is the reason why almost every newly designed Ethernet LAN based on a physical star topology. The primary disadvantage of the star topology is the hub/switch represents a single point of failure. If the hub/switch were to fail the entire network would fail as a result of the hub/switch being connected to every machine on the network. The star topology includes both extended-star and distributed-star topologies. When a network is expanded to include an additional network device that is connected to the main network devices, the topology is referred to as an extended-star topology. A common deployment of this topology is in a hierarchical (Tree) design network such as a Campus LAN or an Enterprise or a WAN. Figure 1-2 shows the tree physical topology.

Today, most extended-star networks employ a redundant connection to a separate set of connection devices to prevent isolation in the event of a device failure, especially the central node (core switch, router, and firewall), since if one of these devices fails, a large portion of the network can become isolated. Distributed-star topology is composed of individual networks that are based upon the physical star topology connected together in a linear fashion, i.e., 'daisy-chained'. Therefore, the distributed-star topology has no central connection.

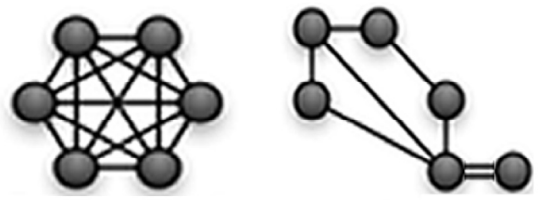
Figure 1-2 The Tree Physical Topology Network

Mesh Topology

In addition to the basic physical topologies discussed above there is a mesh topology. Mesh topology is similar to star topology. It provides redundancy between machines in a star topology. A network can be fully meshed or partial meshed depending on the level of redundancy required. Figure 1-3 shows these types of physical topology. The mesh topology increases the overall network cost, but it improves network availability and reliability. Full-meshed network connects each machine to all other machines with a point-to-point link for redundancy and fault tolerance– this makes it possible for data to be simultaneously transmitted from any single node to all the other nodes. This topology provides the highest fault tolerant capabilities because the failure of

any single link does not affect connectivity in the network. On the other hand, full-meshed network is expensive and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected. In a partial-meshed topology, at least one machine maintains to multiply connections to all other machines (meshed) using a point-to-point link. The most important machines should be meshed. This topology trades off the cost of meshing all machines by meshing only the most important machines. By taking some of the advantages of the physical fully mesh topology, such as, the redundancy, the expense and complexity required for a connection between every machine in the network, is not required. All the data that is transmitted between nodes in the partially meshed networks takes the shortest path between nodes, except in the case of a failure in one of the links. When one link is failed, the data must take an alternate path to the destination node.

Figure 1-3 The Fully Connected and Partial Connected Mesh Topologies



Logical Network Topology

The logical topology is the mapping of the data flows between the nodes in the network that forming the physical topology-that is, the way in which data accesses the network media and transmits bits across it. Logical topologies are often closely related to media access control (MAC) methods and protocols. The logical topologies are generally determined by the used network protocols, not by the physical layout of the network. Logical topologies can be dynamically reconfigured by special types of equipment such as routers, switches and firewalls.

The physical and logical topologies may or may not be identical in any particular network. For example; in a linear bus physical network topology, the data travels along the length of the bus. Therefore, the network has both a physical bus topology and a logical bus topology. On the other hand; in a star physical topology, the data may travels in a ring logical topology.

The most common implementation of LANs today is a star topology. In either a physical bus or a physical star, Ethernet uses a logical bus topology.

Internetworking Essentials

In this section, internetworking history is presented as well as the types of internetworking are described.

The CCNA exams, and particularly the CCENT (640-822) exam, focus on the concepts, protocols, and devices of two major networking types. These are: enterprise networking and the Small Office/Home Office or SOHO networking. An enterprise network is a network created by one corporation, or enterprise, for allowing its employees to communicate and to provide services to the outside customers. A SOHO networking allows a user to connect to the Internet using a PC or laptop or mobile and any Internet connection, such as the high-speed cable Internet connection or wireless connection. This type of networking uses the same concepts, protocols, and devices used to create enterprise networks, but both are differing by some features, which are required by

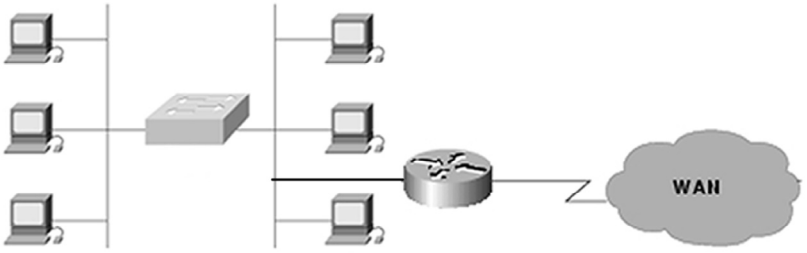
that type. Because most enterprise networks also connect to the Internet, the SOHO user can sit at home, or in a small office, and communicate with servers at the enterprise network, as well as with other hosts in the Internet.

In fact, the term "Internet" itself is formed by shortening the phrase “interconnected networks.” The Internet consists of most every enterprise network in the world, plus billions of devices connecting to the Internet directly through Internet service providers (ISPs). Basically, The ISP role is to provide internet services to others. Therefore, to create the Internet, ISPs offer Internet access, using a cable TV line, a phone line or a wireless connection. Each enterprise typically connects to at least one ISP, using permanent connections generally called wide-area network (WAN) links. Finally, the ISPs of the world also connect to each other. These interconnected networks—from the smallest PC based home network, to cellular phones and automated devices, to enterprise networks with thousands of devices—all connect to the global Internet.

Internetwork

An **internetwork** is a collection of individual networks, which function as a single large network, connected by intermediate networking devices (routers, switches, bridges). Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks. Figure 1-4 depicts some different kinds of network technologies that can be interconnected by routers and other networking devices to create an internetwork.

Figure 1-4 Internetworking Creation



The term internetwork is used in this book and in many other resources to refer generally to a network made up of routers, switches, bridges, cables, and other networking equipment, and the word **network** is used to refer to the more specific concept of an IP network.

History of the Internetworking

The first networks used mainframes and attached dummy terminals. These are time-sharing networks. Such environments were implemented by both IBM's Systems Network Architecture (SNA) and Digital's network architecture. Networks and networking have grown exponentially over the last 20 years.

Local-area networks (LANs) developed around the PC revolution in 1980’s. LANs connected multiple users in a relatively small geographical area to exchange files and messages, as well as access shared resources such as file servers and printers.

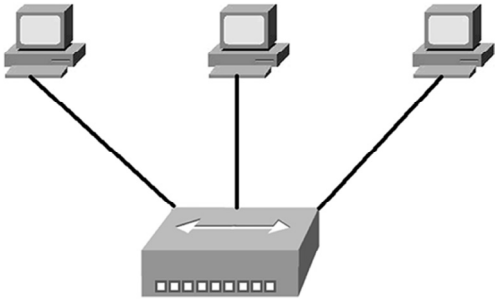
Wide-area networks (WANs) interconnect LANs with geographically dispersed users to create connectivity. Some of the technologies used for connecting LANs include T1, T3, ATM, ISDN, ADSL, Frame Relay, Radio links, Wireless and others.

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

Types of networking

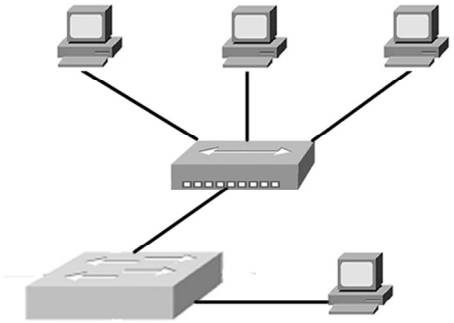
A basic LAN network is shown in Figure 1-5. This LAN connects three PCs together using a simple (now) networking device called a hub. This network is actually one collision domain and one broadcast domain, and these are the major weaknesses of this type of networking. As this network is growth, the problems such as network speed degradation will appear.

Figure 1-5 Hub Based Network



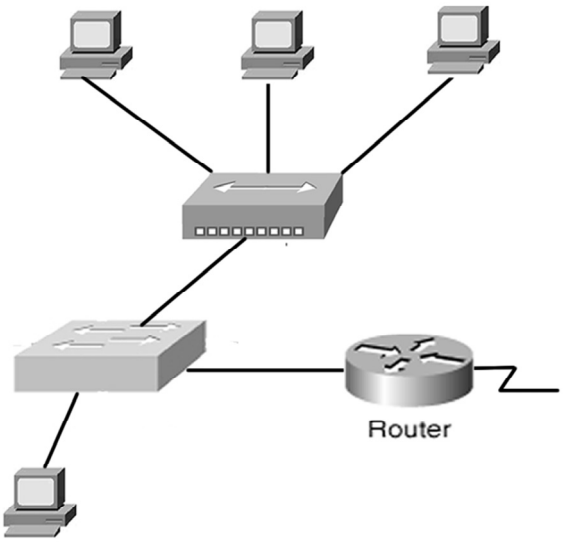
The above problem can be solved by using *network segmentation*, i.e. breaking up the large network into many smaller LANs. This is done by using devices like *bridges, switches*, and *routers*. Figure 1-6 displays a segmented network. By using a switch in this network, each segment/LAN connected to the switch is now a separate collision domain. However, this network is still one large broadcast domain.

Figure 1-6 Switched Based Network



To connect networks together and to route packets of data from one network to another, routers must be used. Routers, by default, break up the network *broadcast domain* into many smaller ones. The broadcast domain is a set of all automated machines on a network segment that listen to all the broadcasts sent on that network segment. Figure 1-7 shows the using of the router that creates an internetwork and breaks up broadcast domains as well as collision domains.

Figure 1-7 Router Based Network



Routers Vs Switches

Routers are used to break up **broadcast domains**. When an automated machine (IP network host) sends a broadcast message, every device on the network must listen, read and process that broadcast—unless there is a router in the network. When the router's interface receives this broadcast, it can discard the broadcast without forwarding it on to other networks, depending on the type of broadcast. Types of broadcast messages will be discussed in the following sections of this chapter. In addition to decompose broadcast domains, routers decompose collision domains as well. Routers can also filter the network based on layer 3 (Network layer) information (e.g., IP address). Router functions in the network can include Packet switching, Packet filtering, Internetwork communication and Path selection.

Routers are really layer 3 switches. Routers use logical network IP addressing and provide packet switching throughout the internetwork, whereas layer 2 switches are used to forward or filter frames (network Layer 2 concept) and switches are based on hardware addresses (MAC addresses). Routers can also provide packet filtering by using access lists (which will be discussed in ICND2 book). Routers use a routing table-a map of the Internetwork-to make network path selections and to forward packets to remote networks. When routers are used throughout the networks, the resulting network is called an internetwork.

Switches on another hand don't forward packets to other networks like routers do. Switches only switch frames from one port to another within the switched network. However, CISCO switches have other functionalities, such as, Port security and Power Over Ethernet (PoE). The main purpose of a switch is to optimize network performance and to provide more bandwidth for the LAN's users. This will be discussed in the following sections of this chapter.

By default, switches break up ***collision domains***. Each port on a switch represents its own collision domain. Collision domain is an Ethernet network terminology used to describe how hosts within an Ethernet network must be conducted. When one particular host sends a packet on Ethernet segment, all other devices on that same segment must receive this frame. If at the same time, a different host transmits a frame on the same Ethernet segment, a collision will occur. Hence, no one of the transmitted frames will be understood. Therefore, both sending hosts must retransmit, one at a time. Usually collisions do not occur in the switched network since each interface on a switch represents its own collision domain. Hubs represent a real medium for collisions since all

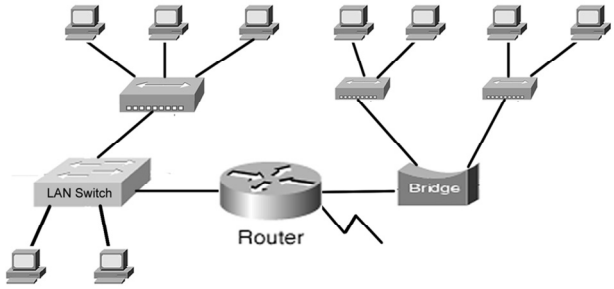
host segments connect to a hub represent only one collision domain and only one broadcast domain. Hence, Hubs create only one collision domain and only one broadcast domain and switches create multiple collision domains (one per interface) but a single broadcast domain, whereas, routers provide multiple collision domains (one per interface) and a separate broadcast domain for each interface (Ports in L3 switch).

Bridges and switches break up collision domains on a LAN. Switch is basically just a multiple-port bridge with more intelligent functions. Both bridges and switches cannot be used to isolate broadcast or multicast packets.

Obviously, there are several designs for each network but the best network design is one that's correctly configured to meet the business requirements of the organization it designs. Today, LAN switches with routers, is the best network design.

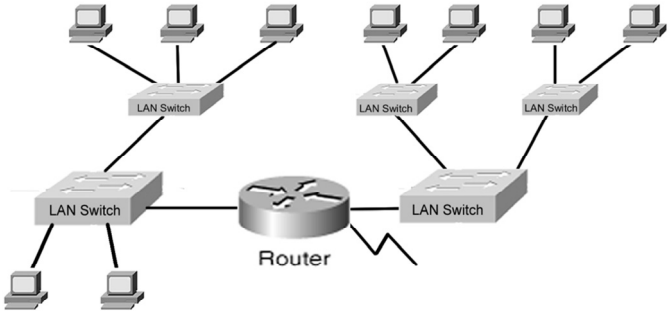
Let's take a look to Figure 1-8. How many collision domains and broadcast domains are in this network? It is found there are seven collision domains and two broadcast domains. Since, only the router breaks up broadcast domains by default. And since there are three connections for this router (one for WAN), that gives two broadcast domains. Now, how many collision domains in this network? The bridge network equals three collision domains. Adding the switch network of four collision domains—one for each switch port—and it is found the total number of collision domains in this network are seven.

Figure 1-8 Using Hub and Bridges



In Figure 1-9, each port on the switch is a separate collision domain and each VLAN (explanation of the VLAN can be found in chapter 6 of this book and ICND2 book in more details) is a separate broadcast domain. Router is still required for routing between VLANs. Now, how many collision domains are in this network? It is clear there are 14th collisions domains in this network—remember that connection between the switches is considered a collision domain The broadcast domain is still two as in the previous Figure 1-8 without using the VLAN.

Figure 1-9 Typical Internetworks



Internetworking Reference Models

To make computers from different venders communicate to each other, in the late 1970's, the International Standard Organization (ISO) introduces a reference model called Open Systems Interconnection (OSI). OSI is introduced to break the barrier of only one type of computers can communicate to each other. For example, companies ran DECnet propriety protocol (from Digital Equipment Corporation (DEC) company) can communicate with an IBM propriety protocol only if their devices depend on OSI model, otherwise, these devices will not be able to communicate to each other.

OSI is the Open System Interconnection reference model for communications. OSI Model is an abstract description for layered communications and computer network protocol design. The OSI model facilitates an understanding of how information travels throughout a network. The OSI model was introduced in 1984 to help vendors create interoperable network devices and software in the form of protocols and rules so that different vendor networks could work with each other. As compared with other reference models, the OSI model is considered as the primary architectural model for networking today. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer. Although some of the original protocols that comprised the OSI model are still used, the OSI as a whole never succeeded in the marketplace since several de facto protocols (such as TCP/IP) and their models are dominant in the marketplace. Now, the OSI model is mainly used as a point of reference for discussing other protocol specifications and especially the TCP/IP protocol. That is why it is required in CCNA/CCENT examinations. The OSI reference model breaks this approach into seven layers. A layer is a collection of conceptually similar functions that receives services from the layer below it and provides services to the layer above it. On each layer, an *instance* requests service from the layer below and provides services to the instances at the layer above. In the following subsections, a deep description to the layered approach will be given.

OSI Reference Model

A **reference model** is a conceptual scheme of how communications between computerized devices should be happened. It divides all the processes required for successful communication into logical groupings called **layers**. This type of system design is known as **layered architecture**.

To overtake the CCENT exam, the OSI reference model must be understood. OSI is the Open System Interconnection reference model for communications. The OSI model now is mainly used as a point of reference for discussing other protocol specifications.

To develop a network based software; developers use a reference model to find and understand the required communication processes and to see what types of functions need to be done on any one layer. To develop a network protocol for a certain layer, only the specific functions of that layer should be taken into account, not those of any other layer.

ISO-International Standard Organization: An international organization that is responsible for a wide range of standards, including those relevant to networking. The ISO developed the OSI reference model, a popular networking reference model.

OSI-Open Systems Interconnection reference model: A conceptual model defined by ISO to describe how any combination of devices can be connected for communication. The OSI model divides the task into seven functional layers, forming a hierarchy with the applications at the top and the physical medium at the bottom, and it defines the functions each layer must provide.

The Advantages of the layered approach

Too Many benefits can be obtained from adopting the layered approach (hierarchical). Layered approach is the process of breaking up the functions or tasks of networking into smaller pieces, called layers, and defining standard interfaces between these layers. The layers break a large, complex set of concepts and protocols into smaller pieces, making it easier to develop, easier to implement with hardware and software, and easier to troubleshoot. The most important benefit of the OSI model is to allow different vendors' networks to interoperate.

Example 1-1: A ftp software (like cuteftp) does not need to think about what the network topology looks like, the Ethernet card in the PC does not need to think about the contents of the files to be transferred by cuteftp, and a router that connected to the network does not need to think about the contents of the files as well. Each one of those is specified, implemented and operated in a separate layer.

The following list shows the benefits of layered specifications:

Interoperability: Computerized devices from multiple vendors can work the same network; this is by creating products to meet the same networking standards (standardization). It encourages industry standardization by defining what functions occur at each layer of the model.

Easy development and learning: Breaking the software into pieces allows easier program changes and faster product evolution. It divides the network communication process into smaller and simpler components, thus helping component development, design, and troubleshooting. It also prevents changes in one layer from affecting other layers. Clearly small pieces are easy to learn and understand.

Modularity: Several venders can participate in developing the same Software. One vendor can write software that implements higher layers programs (ex., web browser) and another vendor can write software that implements the lower layers (TCP/IP protocol).

OSI Layers

As stated previously, the OSI is used to describe how any combination of devices can be connected for communication. It also provides a framework for creating and implementing networking devices, standards and internetworking strategies.

The OSI can be divided into two groups. The upper layers of the OSI (application, presentation, and session) define functions focused on the application (how the applications within the hosts will communicate with each other and with end users). The bottom four layers (transport, network, data link, and physical) define how data is transmitted end-to-end (focused on end-to-end delivery of the data). Figure 1-10 shows the three upper layers and the four lower layers and their functions.

As shown in Figure 1-10, the OSI reference model consists of seven layers. These are:

- Application layer (layer 7)
- Presentation layer (layer 6)
- Session layer (layer 5)
- Transport layer (layer 4)
- Network layer (layer 3)
- Data Link layer (layer 2)
- Physical layer (layer 1)

Figure 1-10 clears that the computer user interfaces at the Application layer. It is also clear that the upper layers are dedicated for user applications communicating between hosts. Physical network characteristics, networking type, hardware addresses, routing or logical addresses are not related to these upper layers. These are the

responsibilities of the four bottom layers.

Figure 1-10 The OSI Upper and Lower Layers

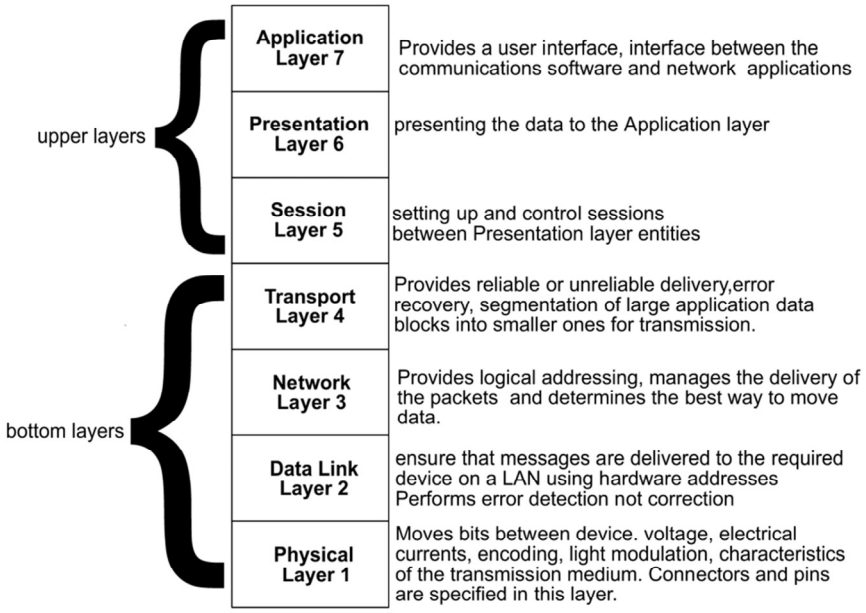
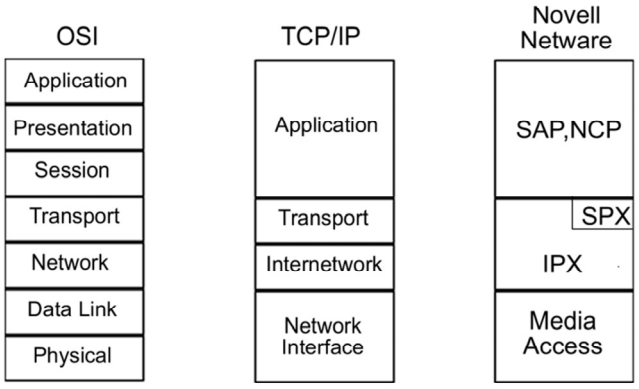


Figure 1-10 clears the four bottom layers that define how data is transferred through a physical medium. All data transmission functions between hosts are dedicated in these bottom layers.

Each layer defines a set of typical networking functions. The OSI model can be used as a standard of comparison to other networking models. Figure 1-11 shows OSI as compared with TCP/IP and Novell NetWare.

Figure 1-11 TCP/IP and Netware Protocol Stacks as Compared with OSI



As an example, TCP/IP's internetwork layer, as implemented by IP, equates most directly to the OSI network layer. So, it is widely known that IP is a network layer, or Layer 3 protocol, using OSI terminology and numbers

for the layer.

Both the CCENT and ICND2 exams focus on issues in the lower layers—in particular, with Layer 2 and Layer 3, where switching and routing technologies are implemented respectively.

Too many protocols are implemented on the OSI layers. Table 1-1 lists typical protocols considered to be comparable to the OSI layers.

Table 1-1 Typical Protocols, Devices and the OSI.

OSI Layer	Protocol Examples	Devices
7	Telnet, HTTP, FTP, internet browsers, SMTP gateways , SNMP, VoIP	Firewall, intrusion detection and preventation systems
6	JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, decryption, MPEG, MIDI.	Encryption systems, decryption systems
5	RPC, SQL, NFS, NetBIOS names, AppleTalk ASP, DECnet, SCP	RPC Servers, SQL Servers, NFS Servers, NetBIOS names Servers, WINS servers
4	TCP, UDP, SPX	Layer 4 switch
3	IP, IPX, AppleTalk DDP, ARP, RARP	Router
2	IEEE 802.3/802.2, 802.11, HDLC, Frame Relay, PPP, FDDI, ATM	LAN switch, Bridges, wireless access point, cable modem, DSL modem
1	EIA/TIA-232, V.35, EIA/TIA-449, RJ-45, Ethernet, 802.3, 802.5	LAN hub, repeater

Figure 1-12 shows a summary of the main functions defined at each layer of the OSI model.

Now, let us describe each layer in more details.

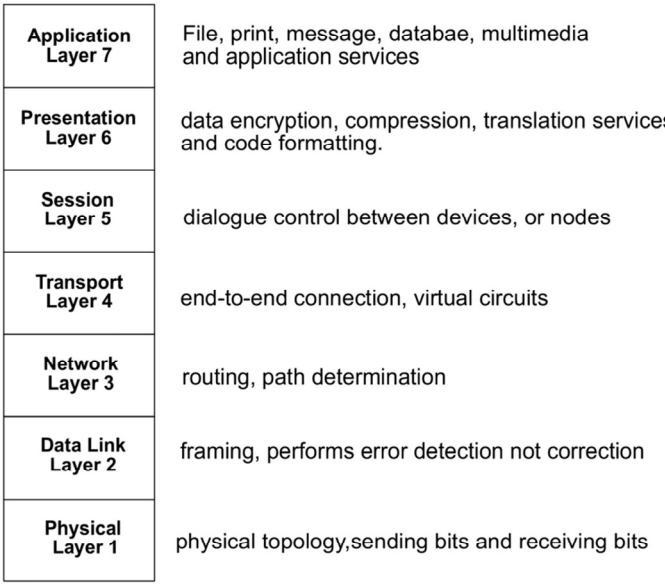
The application layer: This layer is the closest OSI layers to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer defines the interface between the communications software and any applications that need to communicate outside the computer on which the application resides. Some examples of application layer implementations include Telnet, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Secure FTP (SFTP) and Simple Mail Transfer Protocol (SMTP). For example, a Cuteftp is an application on a computer. The Cuteftp needs to obtain the file; OSI Layer 7 defines the protocols used on behalf of the application to obtain the file.

The presentation layer: This layer establishes a context between different application layer entities. This makes the higher-layer entities use different syntax and semantics, as long as the presentation service understands both and the mapping between them. The purpose of this layer is presenting the data to the Application layer. Furthermore, this layer is responsible for data translation and code formatting. This layer is a translator and provides coding and conversion functions. Functions like data compression, decompression, encryption, and decryption are dedicated in this layer. Some multimedia functions are also implemented in this layer.

The Session layer: This layer is responsible for setting up and control conversations (called sessions) between Presentation layer entities. This layer also provides dialogue (connection) control between devices, or nodes. It establishes, manages and terminates the connections between the local and remote application. It organizes the

system's communications by offering three different modes: simplex, half duplex, and full duplex. Moreover, it establishes a check pointing, adjournment, termination, and restart procedures. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

Figure 1-12 The Main Functions of the OSI



The transport layer: Layer 4 protocols focus on issues related to data delivery to the other computers—for instance, error recovery, segmentation of large application data blocks into smaller ones for transmission, and reassembly of those blocks of data on the receiving computer. The transport protocols provide end-to-end data transport services. Function like establishing a logical connection between end-to-end hosts on an internetwork is also implemented in this layer. This layer is dedicated for providing mechanisms for multiplexing upper layer applications, establishing sessions, and controlling virtual circuits. This layer also hides details of any specific network information from the higher layers by providing transparent data transfer. The term reliable networking is used at the Transport layer. It means that acknowledgments, sequencing, and flow control functions can be used. The Transport layer can be connectionless or connection-oriented. Some protocols are state and connection oriented. The connection-oriented means that the Transport Layer can keep track of the segments and retransmit those that fail. Although developed under the TCP/IP Model and not strictly conforming to the OSI definition of the Transport Layer, typical examples of Layer 4 protocols are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Tunneling protocols operate at the Transport Layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPSec. L2TP carries PPP frames inside transport packet.

The Network layer: This layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Layer 4. This layer (also called layer 3) manages the delivery of the packets (end-to-end communication) and determines the best way to move data. To accomplish this task this layer defines the Logical addressing so that any endpoint can be identified. The values of these addresses are chosen by the network engineer or defined automatically using DHCP server. This layer also defines how routing works and how routes are learnt so that the packets can be delivered. Routers (layer 3 devices) are specified at the Network layer and provide the routing services within an internetwork. This layer might also perform fragmentation and reassembly, and report delivery errors. The following duties are defined by the IP, which

operate at this layer:

- Examining the destination IP address of a packet.
- Comparing that address to the IP routing table.
- Fragmenting the packet if the outgoing interface requires smaller packets.
- Queuing the packet to be sent out to the interface.

Two types of packets are used at the Network layer. These are: data and route updates.

Internet Protocol (IP) in the TCP/IP is an example of layer 3 protocols. It manages the connectionless transfer of the data one hop at a time, from the end system to the ingress router, router to router, and from the egress router to the destination end system. It is only responsible for the detection of incorrect packets, so they may be discarded. Therefore, IP is not responsible for reliable delivery to a next hop. When the medium of the next hop cannot accept a packet in its current length, IP is responsible for **fragmenting** the packet into sufficiently small packets that the medium can accept.

Example 1-2: Router Main functions. When a packet is received on a router interface, the destination IP address is checked. If the packet isn't destined for that particular router, it will look up the destination network address in the routing table. Once the router chooses an exit interface, the packet will be sent to that interface to be framed and sent out on the local network. If the router can't find an entry for the packet's destination network in the routing table, the router drops the packet.

The data link layer: This layer (Layer 2) provides the physical transmission of the data and handles error notification, network topology, and flow control. This means that this layer will ensure that messages are delivered to the required device on a LAN using hardware addresses and translates messages from the Network layer into bits for the Physical layer to transmit. Data link layer also defines the format of a header and trailer that allows devices attached to the medium to send and receive data successfully. The data link trailer, which follows the encapsulated data, typically defines a Frame Check Sequence (FCS) field, which allows the receiving device to detect transmission errors. Examples of the specifications that work in this layer include the Ethernet IEEE 802.3 and 802.2 and –High Level Data Link Control (HDLC) for a point-to-point WAN link.

The physical layer: Typically, this layer refers to standards from other organizations. This layer deals with the physical characteristics of the transmission medium, which include the specification of connectors, pins, electrical currents, encoding, and light modulation. In particular, it defines the relationship between a device and a physical medium. This includes the layout of pins, voltages, cable specifications, Hubs, repeaters, network adapters, Host Bus Adapters (HBAs used in Storage Area Networks) and more. Multiple specifications sometimes are used to complete all details of the physical layer. The main duties of this layer are: sending bits and receiving bits

As a final comment in the OSI layer, some of the networking devices operate at all seven layers of the OSI model. The following is a list of some of these devices:

- Network hosts.
- Gateways.
- Web and application servers.
- Network management stations

OSI Encapsulation and De-encapsulation Terminologies

Data Encapsulation is a process of adding a header to wrap the data that flows down the OSI model. OSI like TCP/IP defines processes by which a higher layer asks for services from the next lower layer. This is done by encapsulating the higher layer's data behind a header by the lower layer.

OSI uses what is called a *protocol data unit*, or *PDU*. A PDU represents the message that includes the headers

and trailers for that layer, as well as the encapsulated data. A PDU for a specific layer has a specific format that implements the specifications and requirements of that layer. Layers 7 to 2 are communicated logically. The only hardware connection is at the physical layer or layer 1. Thus, in order for a layer to communicate across the network, it must pass down its PDU to the next lower layer for transmission. OSI refers to the PDU of each layer in the form of "Layer N PDU," with "N" referring to the number of the layer being discussed. As an example, a segment is a *Layer 4 PDU*. The term *L4PDU* is a shorter version of the phrase *Layer 4 PDU*.

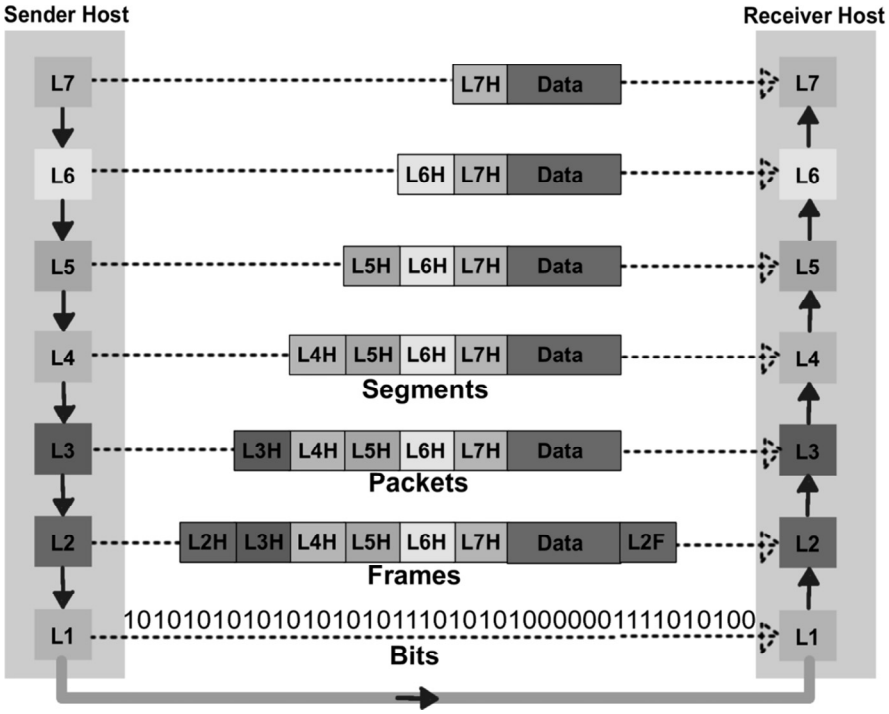
When layer N PDU wants to go down the model to Layer N-1, it becomes the data that the layer N-1 protocol is ***service***. Therefore, the layer N PDU is called the layer N-1 *service data unit (SDU)*. Now, layer N-1 adds its own PDU format, preceding the SDU with its own headers and appending trailers as necessary and the result will be N-1 PDU. This process is called *data encapsulation*, because the entire contents of the higher-layer message are encapsulated as the data payload of the message at the lower layer.

The process continues, all the way down the model to the physical layer. In the theoretical model, the whole encapsulation process ends up with a PDU at layer 1 that consists of application-layer data that is encapsulated with headers and trailers (as necessary) from each of layers 7 through 2 in turn, as shown in Figure 1-13.

Layers 7 through Layer 3 of the OSI define only a header, with the data from the next higher layer being encapsulated behind the header. The data link layer defines both a header and a trailer and places the L3PDU between the header and trailer. The L2 header contains the source and destination MAC address and the trailer contains the Frame check sequence (FCS) used for verifying the data integrity.

Figure 1-13 represents the typical encapsulation process, with the top of the figure showing the application data and application layer header, and the bottom of the figure showing the L2PDU that is transmitted onto the physical link.

Figure 1-13 The Typical Encapsulation Process



A reverse to encapsulation process is implemented in the recipient (remote) machine to interpret the data; this process is called *De-encapsulation*. When the recipient machine receives a sequence of bits, the layer 1 passes the bits to the layer 2 for manipulation. The layer 2 at the recipient machine checks the layer 2 trailer (the FCS) to see if the data is in error to be discarded, otherwise if the data is not in error, the layer 2 reads and interprets the control information in the layer 2 header. Then it strips the header and trailer and passes the remaining data up to layer 3 based on the control information in the data link header. The remaining layers perform similar de-encapsulation processes as necessary to deliver the actual data to the end user at the recipient machine.

The encapsulation and de-encapsulation processes at the source and destination machines produce a type of logical communication between peer layers in the OSI model. This form of communication is called *peer-to-peer communication*. During this communication, the protocols at each layer exchange PDU between peer layers, as shown in Figure 1-13.

Figure 1-13, depicts that segments, packets and frames are generated in layer 4, layer 3 and layer 2 respectively. These are TCP/IP terms and it will be discussed in details in the upcoming chapters of this book.

Ethernet LANs

Computers send bits to each other over a particular type of physical networking medium using physical and data link layers protocols. The OSI physical layer defines how to physically send bits over a particular physical networking medium. The OSI data link layer defines some rules about the data that is physically transmitted, including hardware (H/W) addresses of the sending device and recipient device, and rules that organize the sending time to prevent data collisions.

A LAN is a common type of network found in homes, small business offices, and large enterprise networks. It is considered as a basic part of large enterprise networks. An Enterprise network consists of several sites; each site can be made of several LANs. A LAN connects the end-user devices together, which allows the local computers to communicate with each other. LANs are connected by switches and other connecting devices, whereas sites are connected by routers. Routers are used to connect both the LAN and a wide-area network (WAN). This will provide connectivity between the various sites of the large enterprise network. With routers and a WAN, the computers at different sites can also communicate.

Understanding the LAN functions, network components, network topologies and standards, frames, Ethernet addresses, and network operational characteristics are important for an overall knowledge of the internetworking technologies.

This section explains some of the basics of the local-area networks (LAN). The term LAN refers to a set of Layer 1 and 2 standards designed to work together for implementing geographically small networks. Further Ethernet LAN explanations will be found in the upcoming chapters of this book.

Ethernet LAN Definition

A data communications system that operates at high speed over short distances (up to a few thousand meters), has a specific user group, and is not a public switched telecommunications network, but may be connected to one. A LAN is usually managed and owned by a single organization. A LAN permits users to exchange data, share a common printer or master a common computer (server), or execute a shared application. A LAN can vary widely in their sizes (from two computers up to hundreds of computers).

An interconnection of LANs within a limited geographical area, such as a government base, is commonly referred to as a *campus area network*. An interconnection of LANs over a city-wide geographical area is commonly called a *metropolitan area network* (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a *wide area network* (WAN). Furthermore, LANs are not subject to public

telecommunications regulations.

Ethernet Network Components

Ethernet LANs consist of several automated machines called network nodes and several types of interconnecting media. The network nodes can be one of two major classes:

- **Data terminal equipment (DTE)**—Devices that are either the source or the destination of data. DTEs are typically devices such as computers and network servers that often referred to as end stations.
- **Data communication equipment (DCE)**—Intermediate network devices that receive and forward data across the network. DCEs may be both standalone devices such as repeaters, network switches, network bridges and routers, or communications interface units such as network interface cards (NIC) and modems.

The current Ethernet media options include two general types of copper cable: unshielded twisted-pair (UTP) and shielded twisted-pair (STP), plus several types of optical fiber cable. However, the wireless network has no physical media.

In addition to the above components, Ethernet LANs require some software that working in the network nodes (including IOS in CISCO devices) and make LAN useful plus some protocols that manage its working, such as Ethernet protocols, TCP/IP suite and DHCP.

Ethernet History

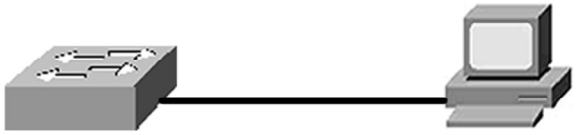
From decades the most common type of LAN is Ethernet. Like many inventions, Ethernet began inside a corporation that was looking for a solution to a specific problem "**The need is the mother of the invention**". Xerox needed an effective way to network the personal computer in its offices. From that, Ethernet was born. (See http://patft.uspto.gov/netacgi/nph-Parser?u=%2Fnetahtml%2Fsrchnum.htm&Sect1=PTO1&Sect2=HITOFF&p=1&r=1&l=50&f=G&d=PALL&s1=4063220.PN.&OS=PN/4063220&RS=PN/4063220 and http://inventors.about.com/library/weekly/aa111598.htm for more details on the history of Ethernet.) Xerox was developed the original Ethernet as an experimental coaxial cable network in the 1970s to operate with a data rate of 3 Mbps using a carrier sense multiple access with collision detection (CSMA/CD) protocol (which will be discussed in the next subsections of this chapter). Success with Xerox network led to the 1970s joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation (DEC), Intel Corporation, and Xerox Corporation. This Ethernet became known as *DIX Ethernet*, referring to DEC, Intel, and Xerox. It is called thicknet (because of the thickness of the coaxial cable used in this network). In 1980s this standard of Ethernet was updated to add more capabilities, and it was referred to as Ethernet Version 2.0 (Ethernet II). The first standard draft was published on September 30, 1980 within IEEE.

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organization that defines network standards. The IEEE formed two committees that worked directly on Ethernet based on the CSMA/CD—the IEEE 802.3 committee and the IEEE 802.2 committee. The 802.3 committee worked on physical layer standards as well on a sublayer of the data link layer called *Media Access Control (MAC)*. The IEEE assigned the other functions of the data link layer to the 802.2 committee. This upper part of the data link layer was called the *Logical Link Control (LLC)* sublayer. Notice that, the 802.2 standard applied to Ethernet as well as to other IEEE standards LANs such as Token Ring (See, http://tools.ietf.org/html/rfc1042 for modern LLC RFC.) This set of standards is most often referred to as simply "Ethernet". The original IEEE 802.3 standard was based on Ethernet II specifications, and it was very similar to the Ethernet Version 1.0 specifications. The draft standard was approved by the 802.3 working group in 1983 and was subsequently published as an official standard in 1985 (ANSI/IEEE Std. 802.3-1985). To take advantage of improvements and developments in the networking technologies, a number of supplements to the standard have been defined yet.

Ethernet Network Topologies and Structures

Regardless of LANs size or complexity, all will be a combination of only three basic interconnection structures or networking building blocks. The point-to-point interconnection is the simplest structure as shown in Figure 1-14. In this network only two network units are involved, and the connection may be DTE-to-DTE, DCE-to-DCE, or DTE-to-DCE. The cable in point-to-point interconnections is known as a network link. Depending on the type of cable and the transmission method that is used, the maximum allowable length of the link is set.

Figure 1-14 Point-to-Point Interconnections

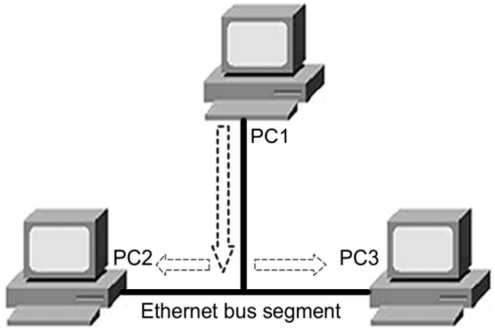


The original Ethernet networks were implemented with a coaxial bus topology, as shown in Figure 1-15. The physical Ethernet consists of the coaxial cabling, which is a bus topology, and collective Ethernet NICs in the computers (nodes). The bus is shared among all nodes on the Ethernet. When a node wants to send some bits to another node on the bus, it sends an electrical signal, and the electricity propagates to all nodes on the Ethernet.

10BASE5 and 10BASE2 are types of old Ethernets. The 10 represents the maximum transmission speed, which is 10Mbps. The *BASE* stands for baseband signaling. The 5 in 10BASE5 represents the maximum length of cable, which is 500 m. Whereas, the 2 in 10BASE2 represents the maximum length of cable which is 200 m. 10BASE5 also known as thicknet, whereas, 10BASE2 known as thinnet. This is a simple description to these Ethernets. More detail will be found in this chapter.

Figure 1-15 shows a sample of 10BASE2 Ethernet, which uses a single bus, created with coaxial cable and Ethernet NICs.

Figure 1-15 Coaxial Bus Topologies



The solid lines in Figure 1-15 represent the physical network cabling. The dashed lines with arrows represent the path that it will be taken by PC1's transmitted frames. PC1 sends an electrical signal across its Ethernet NIC onto the cable, and PC2 and PC3 receive the signal since this is a bus topology which means that the transmitted signal is received by all stations on the LAN.

Ethernets that use a single bus need another logic/protocol to manage the network. Imagine what happened if two or more electrical signals were sent at the same time on a single bus. Of course, they would overlap and collide, making both signals unintelligible. So to ensure that only one device sends traffic on the Ethernet at one

time, Ethernet defined an algorithm, known as the *carrier sense multiple access with collision detection* (*CSMA/CD*) algorithm. Otherwise, the Ethernet would have been unusable. This algorithm, manages how the bus is accessed. This is similar to what happened in a room with many people. It's hard to understand what more than one person are saying at the same time, so usually, one-person talks, and the rest listen.

The CSMA/CD algorithm, which is applied for both 10BASE5 and 10BASE2 Ethernets, can be summarized as follows:

- A device that wants to send a frame checks the LAN before sending a frame to ensure that the LAN is silent—in other words, no frames are currently being sent.
- If there is a frame on the bus, the device that wants to send a frame waits for a random amount of time until the LAN is silent and then sends the frame.
- If a collision occurs, the devices that caused the collision wait for a random amount of time and then try again.

A collision occurs in these Ethernets because the transmitted electrical signal travels along the entire length of the bus and when two stations send a frame at the same time, their frames overlap, causing a collision. So, all devices on a 10BASE5 or 10BASE2 Ethernet need to use CSMA/CD to make a LAN useful by avoiding collisions and recovering a LAN when collisions occur.

Common Ethernet Standards

10BASE5 and 10BASE2 Ethernet networks used coaxial cable for physical layer connectivity. From 1990, the use of twisted pair cables was begun. **Ethernet over twisted pair** refers to the use of cables that contain insulated copper wires twisted together in pairs for the physical layer of an Ethernet network. IEEE defined several Ethernet standards for twisted pair cables. The most widely used are **10BASE-T** (1990), **100BASE-TX** (1995), and **1000BASE-T** (1999), running at 10Mbps, 100Mbps, and 1000Mbps (1Gbps) respectively. Table 1-2 lists the most commonly used IEEE Ethernet standards. The **number** (10, 100, or 1000) in the beginning of the standard name refers to the theoretical maximum transmission speed in megabits per second (Mbps). The **BASE** is short for baseband signaling, meaning that there is no frequency-division multiplexing (FDM) or other frequency shifting modulation in use; each signal has full control of wire, on a single frequency. The **T** designates twisted pair cable, where the pair of wires for each signal is twisted together to reduce radio frequency interference and crosstalk between pairs (FEXT and NEXT). Where there are several standards for the same transmission speed, they are distinguished by a letter or digit following the T, such as *TX*. To support these new standards, networking devices called hubs and switches were also created.

Table 1-2 Most Common Ethernet Standards

Network Name	Speed Mbps	Technical Name	IEEE Standard Name	Cable Type, Maximum Length
Ethernet	10	10BASE-T	IEEE 802.3	Copper, 100 m
Fast Ethernet	100	100BASE-TX	IEEE 802.3u	Copper, 100 m
Gigabit Ethernet	1000	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Fiber, 5 km (LX), 550 m (SX)
Gigabit Ethernet	1000	1000BASE-T	IEEE 802.3ab	Copper, 100 m

Repeaters

Because of many reasons such as the ***Attenuation***, 10BASE5 and 10BASE2 had limitations on the total length of a cable. With 10BASE5, the limit was 500 m; with 10BASE2, it was 185 m (approximately 200 m). The number of DTEs did not exceed 1024 in 10BASE5. To overcome these limitations a *repeater* is used.

Attenuation means that electrical signals pass over a cable, suffer from weaknesses in the strength of the signal as it travels farther along the cable.

As shown in Figure 1-5, repeater (hub) connects multiple cable segments, receives the electrical signal from one cable, interprets the electrical signals (bits), and generates clean (without noise), strong (amplification) signals out the other cable. Repeater only examines and generates electrical signals and does not interpret what the bits mean. Therefore, a repeater is considered to operate at Layer 1 of the OSI model.

Hubs

Hubs are basically multiport repeaters. That means, the hub simply regenerates the electrical signal that comes in one port and sends the clean, strong generated signal out every other port. That also means, the hub generates several electrical buses (but internally, Hub creates One Shared Electrical Bus), as shown in Figure 1-5, just like 10BASE2 and 10BASE5. One bus for each LAN connected to a specific hub port. Therefore, the use of CSMA/CD algorithm will still be required since collisions can still occur in 10BASE-T.

The use of hubs in network design solved some big problems with 10BASE5 and 10BASE2 networks. One of the biggest problems is the availability. In 10BASE5 and 10BASE2 LANs any single cable problem could, and probably did, take down the whole network. Whereas in the 10BASE-T network, a cable connects each device to the hub, so a single cable problem affects only one device/one LAN. This means that 10BASE-T networks are much higher availability than 10BASE5 and 10BASE2 networks. Furthermore, the use of twisted pair cables, in a star topology, lowered the cost of purchasing and installing the cabling.

Today, switches are more likely to be used instead of hubs.

Switches

Switches are intelligent devices and therefore, switches can perform much more functions than hubs and can play much better than hubs (See the datasheet for CAT2.96K switch on www.cisco.com.) LAN switches increase the available bandwidth of the Ethernet network and significantly reduce, or even eliminate, the number of collisions on a LAN. Unlike hubs, switches do not create a single shared electrical bus, forward received electrical signals out all other ports. Instead, switches do the following:

- Switches interpret the bits in the received frame so that they can typically send the frame out to the required port, rather than all other ports of the switch.
- Switches can forward one frame at a time, buffering other frames in memory when they need to forward multiple frames out the same port, thereby avoiding collisions.

LAN switches increase the available bandwidth of the Ethernet network as compared with hubs. In particular:

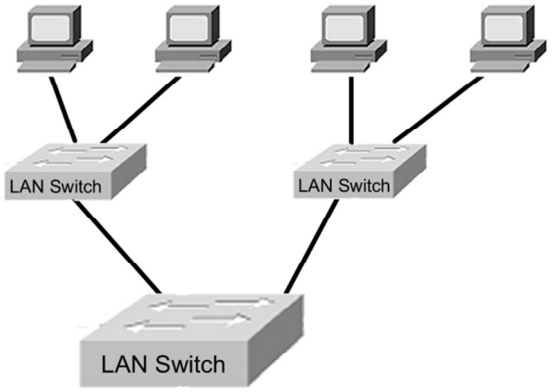
- No collisions can occur when only one device is connected to each port of a switch.
- Each port of the switch has its own separate bandwidth, which is not shared with devices connected to another switch port. This means that a switch with 1000-Mbps ports has 1000 Mbps of bandwidth *per port* (2000 Mbps full-duplex). This is the real difference between *shared Ethernet* and *switched Ethernet*. Hub is a shared Ethernet network where all ports share the same hub bandwidth, whereas the switch is a switched Ethernet where each port has a separate bandwidth.

Since, the switch's logic requires that the switch look at the Ethernet frame header, which is considered a Layer 2 feature. Therefore, switches are considered to operate as a Layer 2 device, whereas hubs are Layer 1 devices.

As a final comment in this section, since the early 1990s, the cabled network design of choice has been the star-connected topology, shown in Figure 1-16. The central network device is either a hub or a network switch. All connections in a star network are point-to-point links implemented with either twisted-pair or optical fiber cable.

These networks are still suffering from collision and broadcast problems. However, collision cannot be occurred, and broadcast can be stopped, in switches based networks. More details about the use of switches in the network will be found in this book.

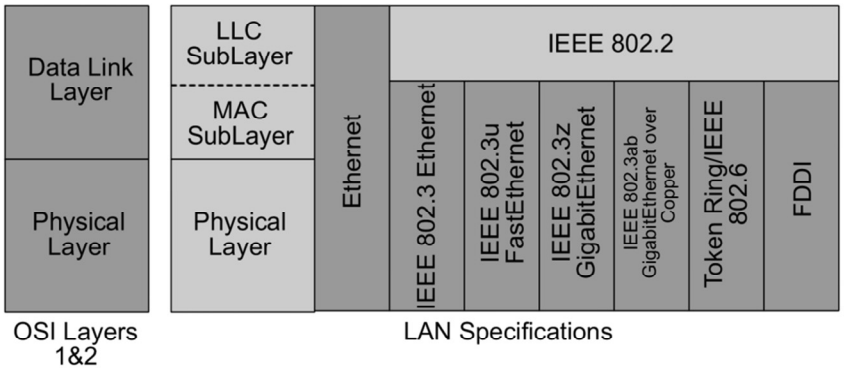
Figure 1-16 Switched Star-Connected Topology



Ethernet LAN standards

Ethernet LAN standards specify cabling and signaling at both the physical and data link layers of the OSI model. This section describes the Ethernet data-link protocols. It covers Ethernet standards, CSMA/CD algorithm, Ethernet addressing, framing, and error detection. Figure 1-17 shows how LAN protocols are mapped to the OSI mode.

Figure 1-17 Mapping Ethernet LAN Protocols to the OSI Model



As with all IEEE 802 protocols, the OSI data link layer is divided into two IEEE 802 sublayers, the *Media Access Control* (MAC) sublayer and the *Logical Link Control* (*LLC*) sublayer. The IEEE 802.3 physical layer corresponds to the OSI physical layer.

All Ethernet standards use the same small set of data-link standards. From 10BASE5 and up to 10-Gbps Ethernet networks, the Ethernet addressing works the same on all the types of Ethernet. Furthermore, the CSMA/CD algorithm is applying to most types of Ethernet, unless it has been disabled. These are the most significant strengths of the Ethernet family of standards.

LLC Sublayer

The *Logical Link Control* (*LLC*) sublayer of the data link layer manages communications between devices over a single link of a network. IEEE 802.2 specifications defined LLC to support both connectionless and connection-oriented services used by higher-layer protocols. LLC is created to allow part of the data link layer to function independently from existing technologies. IEEE 802.2 defines a number of fields in data link layer frames that enable multiple higher-layer protocols to share a single physical data link. It also participates in the encapsulation process.

MAC Sublayer

The *Media Access Control* (*MAC*) sublayer of the data link layer manages protocol access to the physical network medium. The IEEE 802.3 MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer. A device to be networked must have a unique MAC address. This identification is made by using MAC table of physical addresses of devices. The MAC table is maintained by LLC sublayer.

The MAC sublayer has two primary functions:

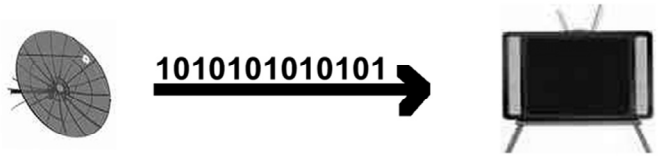
- Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception
- Media access control, including initiation of frame transmission and recovery from transmission failure

Data Transmission Types: Simplex, Half-Duplex, and Full-Duplex

Before studying the CSMA/CD algorithm, it is better to review who is vulnerable to collisions in the networking. This depends on the type of data transmission used. Some types of data transmission are virtually invulnerable to collisions- while others are vulnerable to collisions.

Simplex data transmission is a connection in which data will always flow in one direction. Therefore, it will not suffer collisions. Since data flows in one direction, there is no mutual communication between the sending and receiving stations- therefore, simplex transmission will not be seen in everyday networks. Simplex transmissions, however, are using in broadcasting companies when they want to send a video in a one-way data transmission to a home television, as shown in Figure 1-18.

Figure 1-18 Simplex Transmission



Half-duplex data transmission allows mutual communication between the sending and receiving stations, as shown in Figure 1-19. A device either sends or receives data at any point in time, but never both at the same time. Half-Duplex is where almost all collisions will happen: since each device may not know the other is transmitting. If a collision occurs, the data collides over the bus, and the data is corrupted.

For a practical example, the phones can be taken here as a reference. When two persons talk at the same time in the same phone call, their taking will collide and will not be understood to both persons, and they must repeat their talking, one person in one direction at a time.

Full-duplex data transmission allows devices to send and receive data at any point in time, as shown in Figure

1-20. Virtually, no collisions take place on a full-duplex transmission, so there is no need for CSMA/CD. Full-duplex increases the overall throughput- since sending and receiving are taken place on two different channels. Theoretically, Full-duplex doubles the data transfer rate.

Figure 1-19 Half-Duplex Transmission

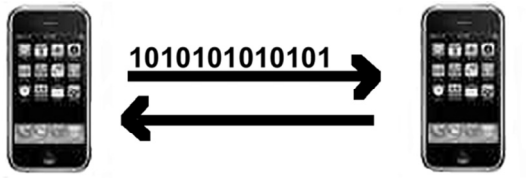
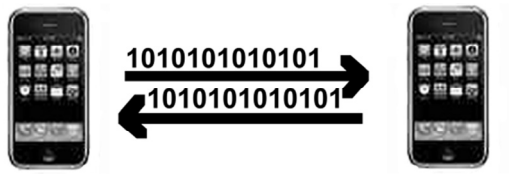


Figure 1-20 Full-Duplex Transmission



The collisions will be eliminated when the Full-duplex and switches are used. However, collisions may still occur when a Full-duplex transmission is configured for a network that operates under a hub. This is because switches forward data only to nodes that need it using *micro segmentation* technology, while hubs forward incoming data to all computers connected to it. Thus, the fault lies within the collision-prone characteristics of the hub. CSMA/CD must be deployed whenever collisions could occur, in hub networks of course.

Moreover, switches can buffer frames in memory. Switches can completely eliminate collisions on switch ports that connect to a single host. In such network collisions cannot occur, since this network connects the switch to one host per port, which allows the use of full-duplex operation.

To implement full duplex in a switched network, CSMA/CD logic on the devices on both ends of the cable must be disabled. As a result, the performance of such a switched Ethernet on that cable has been doubled by allowed simultaneous transmission in both directions.

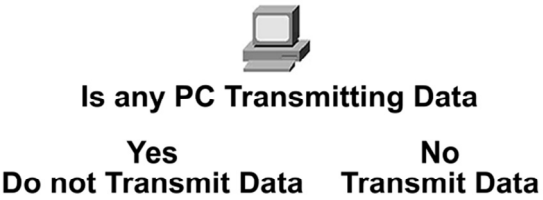
CSMA/CD Algorithm

Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**), is a layer 2 protocol in the OSI model. It is used in the networking as a control protocol in which a carrier sensing and collision detection algorithms are used. The CSMA/CD protocol was originally developed as a means by which two or more stations could share a common medium in a switch-less environment. Each Ethernet MAC determines for itself when it will be allowed to send a frame.

The CSMA/CD access rules are summarized by the protocol's acronym:

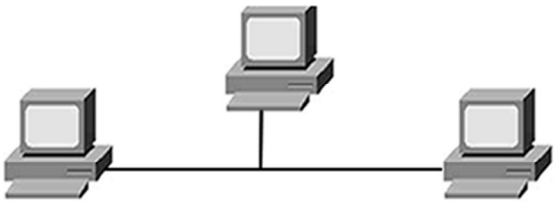
- **Carrier Sense (CS)**—each station continuously listens for signal (carrier) on the medium to determine when the medium is idle. Carrier sense, as shown in Figure 1-21, is the ability of a NIC to check the network for any communication. The NIC will attempt to transmit the data, if there is no traffic on the network, otherwise, the NIC should not attempt to transmit data. However, by carrier sense only, it is impossible to be sure that data isn't in the process of being sent by other computers and therefore, collision may occur.

Figure 1-21 Carrier Sense



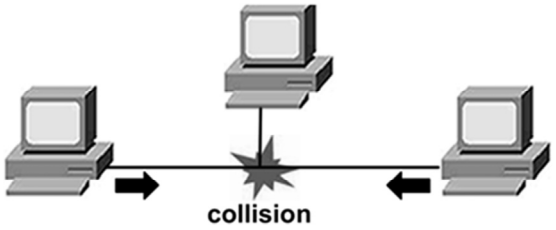
- **Multiple Access (MA)**—Stations may begin transmitting any time they detect that the network is idle (there is no traffic). The MA, as shown in Figure 1-22, provides the ability to multiple devices to access the network with the same priority, which is the perfect environment. This, of course, means that collisions are more possible to occur.

Figure 1-22 Multiple Access



- **Collision Detect (CD)**—if two or more devices in the same CSMA/CD network (collision domain), listen for network traffic, hear nothing, and begin transmitting at the same time, the data streams from the transmitting stations will collide with each other as shown in Figure 1-23, and both transmissions will be destroyed. Therefore, each transmitting device must be capable of detecting that a collision has occurred before sending its frame. Each transmitting device must stop transmitting as soon as it has detected the collision, transmits a jam signal, and then must wait for a random time interval (determined by a back-off algorithm) before attempting to retransmit the frame, as shown in Figure 1-24. Collisions are normally resolved in microseconds.

Figure 1-23 Collision Detection

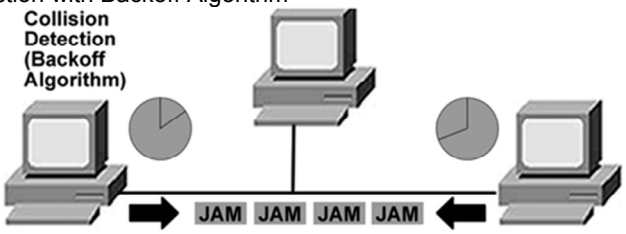


CSMA/CD is a modification of pure CSMA. CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, and reducing the probability of a second collision on retry.

There are several methods for CD. CD methods are media dependent. On an electrical bus such as Ethernet, collisions can be detected by comparing transmitted data with received data. If they are not identical, another transmitter is overlaying the first transmitter's signal, collision is occurred, and transmission terminates immediately. A jam signal is sent, which will cause all transmitters to back off by backoff delay, reducing the probability of a collision when the first retry is attempted. Ethernet is the classic CSMA/CD protocol. However, in Full Duplex Ethernet, collisions are impossible since data is transmitted and received on different wires, and each segment is connected directly to a specific switch port. Therefore, CSMA/CD is not used on Full Duplex Ethernet networks. In addition, CSMA/CD is no longer used in the 10 Gigabit Ethernet specifications, due to the

requirement of switching based network. Similarly, few implementations support CSMA/CD (half duplex) in the Gigabit Ethernet and in practice it is nonexistent.

Figure 1-24 Collision Detection with Backoff Algorithm



The CSMA/CD algorithm is implemented in the following steps:

Step 1 A device that wants to send a frame listens until the Ethernet is idle.

Step 2 The transmitter station(s) start(s) sending the frame, if the Ethernet is idle.

Step 3 After sending the frame, the transmitter station (s) listen(s) again to make sure that no collision has occurred in the network.

Step 4 If a collision occurs; devices involved in the collision keep transmitting (jamming signal) for a short period of time, to make sure all devices on the network see the collision.

Step 5 Each device sees the jamming signal, and invokes the back-off algorithm. Each device will have a random timer that determines when it can transmit again.

Step 6 When each random timer expires, the process starts again with Step 1.

CSMA/CD does not completely prevent collisions, but it does ensure that the Ethernet work sufficiently if collisions may occur. However, the CSMA/CD algorithm has several impacts on network performance. The CD algorithm adds a delay to the network which degrades the overall performance. Furthermore, CS causes devices to wait until the Ethernet is idle before sending data. This process means that only one device can send data at any one instant in time. Therefore, the overall network bandwidth is shared by all devices connected to the same hub. Notice that, waiting to send until the LAN is idle means that a device either sends or receives data at any point in time, which is called half duplex.

Ethernet Frames

The IEEE 802.3 standard defines a basic data Ethernet frame format that is required for all MAC implementations, plus several additional optional formats that are used to extend the protocol's basic capability. The framing used for Ethernet has changed a couple of times over the years. The recent changes to Ethernet framing are made by IEEE in 1997. It includes some of the features of the original Xerox Ethernet framing (1970s), along with the framing defined by the IEEE (1980s).

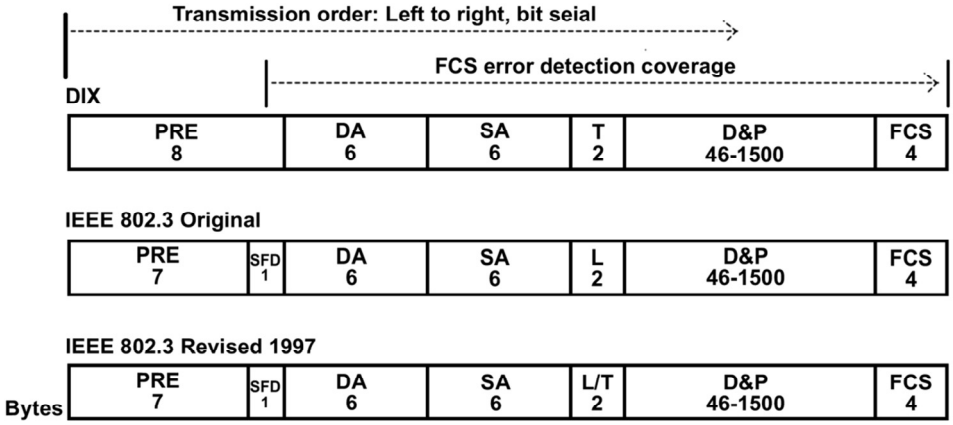
One of the most significant strengths of the all Ethernet family of protocols is that these protocols use the same small set of data-link standards. First, the CSMA/CD algorithm is applying to most types of Ethernet, unless it has been disabled. Clearly, CSMA/CD is technically a part of the data link layer. Second, Ethernet addressing works the same on all the types of Ethernet, from 10BASE5 and up to 10Gbps Ethernet. However, framing has changed several times over the years as stated above.

Framing defines how a string of bits is interpreted in the Data-link protocols. In other words, framing defines the

meaning of the bits transmitted and received over a network through the physical layers of the sending and receiving devices. Frame can also be defined as a “container” into which data is placed for transmission in Ethernet LAN network. The frame contains the actual data that is being transmitted in addition to header and trailer information.

The basic MAC sublayer data frame format contains the seven fields shown in Figure 1-25.

Figure 1-25 LAN MAC Frame Format



Ethernet Frame consists of the following fields:

- **Preamble (PRE)**: This field consists of 7 bytes. The PRE is an alternating pattern of 1s and 0s that tells receiving stations that a frame is coming, and that provides a means to **synchronize** the frame-reception portions of receiving physical layers with the incoming bit stream.
- **Start-of-frame delimiter (SFD)**: This field consists of 1 byte. The SFD is an alternating pattern of 1s and 0s. It tells the receiving computer that the transmission of the actual frame is about to start. SFD ends with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination MAC address.
- **Destination address (DA)**: This field consists of 6 bytes, which contains the MAC address of NIC on the local network to which the frame is being sent. The DA field identifies which station(s) should receive the frame. The left-most bit in the DA field indicates whether the address is an individual address (indicated by a 0) or a group address (indicated by a 1). The second bit from the left indicates whether the DA is globally unique (indicated by a 0) or locally administered (indicated by a 1). The remaining 46 bits are a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network.
- **Source addresses (SA)**: This field consists of 6 bytes. The SA field identifies the frame sending station. The SA is always an individual address and the left-most bit in the SA field is always 0.
- **Length/Type (L/T)**: This field consists of 2 bytes. This field indicates either the number of data bytes that are contained in the data field of the frame, or the frame type ID (the type of protocol listed inside the frame) if the frame is assembled using an optional format. Either length or type is presented in the frame, but not both. If the Length/Type field value is less than or equal to 1500, the number of LLC bytes in the Data field is equal to the Length/Type field value. If the Length/Type field value is greater than 1536, the frame is an optional type frame, and the Length/Type field value identifies the particular type of frame being sent or received.
- **Data and Pad (D&P)**: This field consists of the packet (L3 PDU) that is received by receiving station from layer 3 on the transmitting station. This field is basically, a sequence of n bytes of any value, where n is less than or equal to 1500. If the length of the Data field is less than 46 (too short), the

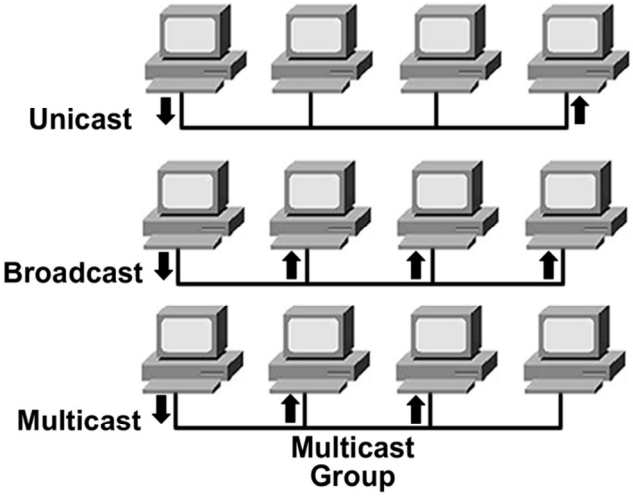
Data field must be extended by adding a filler (a pad) sufficient to bring the Data field length to 46 bytes. Notice that, the IEEE 802.3 specification limits the data portion of the 802.3 frame to a maximum of 1500 bytes. The Data field was designed to hold Layer 3 packets, which must be confirmed with the maximum transmission unit (MTU) that defines the maximum Layer 3 packet that can be sent over a medium. The largest IP MTU allowed over an Ethernet is 1500 bytes.

- **Frame check sequence (FCS)**: This field consists of 4 bytes. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to ensure that the frame has transmitted without corruption. The FCS is generated over the DA, SA, Length/Type, and Data fields.

Ethernet Frames addressing

Ethernet frames are addressed according to communication types that occurred in the LAN. In general, there are three types of communication in the network, these are: unicast, multicast and broadcast. Each Ethernet address is 6 bytes long. It is usually written in a hexadecimal format that is organized in pairs or quads, such as the following: 00:00:1d:34:bc:00 or 0000:1d34:bc00. In CISCO devices, the MAC address is written with periods separating each set of four hex digits. For example, 0000.0C12.1A3E is a valid Ethernet address. Figure 1-26 indicates the forms of Ethernet LAN communications.

Figure 1-26 Ethernet Network Communication



The IEEE defines the following types of communication for the Ethernet:

- **Unicast:** It is used to identify a single NIC on the Ethernet. This type of network communication sends a frame from one sender node and addressed to one destination node. Nodes use unicast addresses to identify the sender and receiver nodes of an Ethernet frame. This type of communication is the predominant form of communication on LANs and within the internet.

  For Group addresses, which identify more than one NIC in the LAN, the IEEE defines two more categories. These are:

- **Multicast:** It is used to identify a group of NICs on the Ethernet. This type of network communication sends a frame from one sender node and addressed to a group of destination nodes. This type allows a group of nodes on a LAN to communicate. Nodes must be members of a multicast group to receive the

information. To use IP multicasts over an Ethernet, the multicast MAC addresses used by IP must follow this format: 0100.5e*xx.xxxx*. Any value can be used instead of the *x's*.

- **Broadcast:** It is used to identify all NICs on the Ethernet. This type of network communication sends a frame from one sender node and addressed to all destination nodes. This type allows all nodes on a LAN to communicate and to process the same frame. Broadcast address is the most often used of the IEEE group MAC addresses. It has a value of FFFF.FFFF.FFFF (hexadecimal notation).

When a host needs to provide information to all the hosts on the network or when the location of special services/devices for which the address is not known, broadcast transmission is used.

Here are examples for the using of broadcast transmission:

- Requesting unknown host address
- Mapping upper layer addresses to lower layer addresses
- Exchanging routing information by routing protocols (routing updates)

Broadcast packets are usually restricted to the local network by routers, whereas unicast packets can be routed throughout the internetwork. This restriction is dependent on the configuration of the router that borders the network and the type of broadcast. There are two types of broadcasts. These are:

Directed Broadcast

A directed broadcast is sent to all hosts on a specific network (non-local network). For example, for a host outside of the 172.16.2.0 /24 network to communicate with the hosts within this network, the destination address of the packet would be 172.16.2.255. Although the routers do not forward directed broadcasts by default, they may be configured to do so.

Limited Broadcast

This type of broadcast is used for communication that is limited to the hosts on the local network (not to host on the non-local network). These packets use a destination address 255.255.255.255. Routers do not forward this broadcast. Packets addressed to the limited broadcast address will only appear on the local network. For this reason, an IPv4 network is also referred to as a *broadcast domain* where the router forms the boundary for this broadcast domain. As an example, a host within the 172.16.2.0 /24 network would broadcast to all the hosts in its network using a packet with a destination address of 255.255.255.255.

Ethernet Addressing

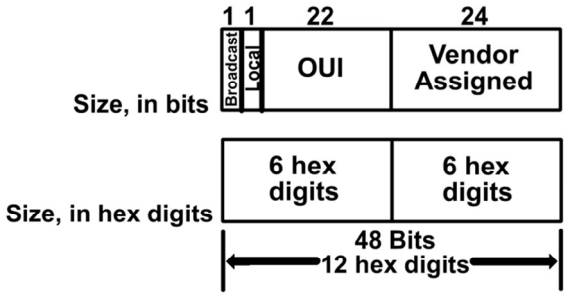
Ethernet address, MAC address, NIC address, hardware address, physical address, LAN address, universally administered address (UAA) and burned-in address, all are names of the same thing that is Ethernet address. It is the means by which data is addressed and directed to the proper receiving node in the network. Because, the MAC sublayer protocols in the Data Link layer such as IEEE 802.3 define the addressing details, the IEEE calls these addresses the "MAC addresses". The IEEE defines the format and assignment of Ethernet addresses. Each NIC on the network must have a unique unicast MAC address according to the IEEE specification so that it is possible to identify that NIC globally. This address is often referred to as the burned-in address (BIA) that is burned into the ROM chip on the card by Ethernet card manufacturers and cannot be changed, and to meet some private needs, some vendors allow the modification of this address. Because the IEEE universally regulates the address assignment of Ethernet addresses, BIAs sometimes are called *universally administered addresses (UAA).*

A MAC address can be decomposed into two parts:

- The first half– IEEE Assigned (24-bit) of the address uniquely identifies the manufacturer of the card which is assigned by the IEEE to each manufacturer, is called the *organizationally unique identifier (OUI)*. Within the OUI, the first two bits have the following meaning only when used in the destination MAC address:
  - **Broadcast or multicast bit:** The left-most bit indicates whether the address is an individual address (indicated by a 0) or a group address (indicated by a 1).
  - **Locally administered address bit:** The second bit from the left indicates whether the MAC address is globally unique (indicated by a 0) or locally administered (indicated by a 1).
- The second half–Vendor Assigned (24-bit) of the address uniquely identifies the NICs for one manufacturer so that one MAC address must not be used on another card of the same manufacturer.

Each manufacturer assigns a MAC address with its own OUI as the first half of the address, with the second half of the address. Figure 1-27 shows the structure of Ethernet address.

Figure 1-27 Structure of Ethernet Addresses



The use of Length/Type Field in the Ethernet Frames

To identify the different network layer (Layer 3) protocols from different vendors on the Ethernet, the protocol Type field is added in the frame, so that the receiving node knows what type of L3 PDU is in the Ethernet frame. For example, to make the receiving node knows that an IP packet is inside an Ethernet frame, the Type field (as shown in Figure 1-25) would have a value of 0800 hexadecimal (2048 decimal).

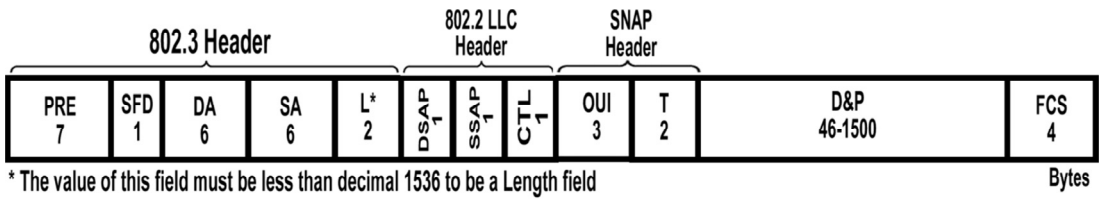
Because of the changes to Ethernet framing over the years, the protocol Type field can be identified by another option in the frame, particularly when sending IP packet and in this case the original Type field is used as a Length field for that frame, identifying the length of the entire Ethernet frame. If the 802.3 Type/Length field (in Figure 1-25) has a value less than 0600 hexadecimal (1536 decimal), the Type/Length field is used as a Length field for that frame. Therefore, another field (Type field) is needed to identify the type of L3 protocol inside the frame.

To create a Type field for frames that use the Type/Length field as a Length field, either one or two additional headers are added after the Ethernet 802.3 header but before the L3 PDU. For example, when sending IP packets, the Ethernet frame has two additional headers:

- An IEEE 802.2 Logical Link Control (LLC) header
- An IEEE Subnetwork Access Protocol (SNAP) header

Both the SNAP header Type field and Ethernet Type/Length field have the same purpose, with the same reserved values. Figure 1-28 shows an Ethernet frame with these additional headers.

Figure 1-28 The 802.2 SNAP Headers



Error Detection in Ethernet Frames

As stated previously, Ethernet defines a trailer at the end of each frame, with the trailer containing a FCS field used for the purpose of error detection. Error detection is the process of discovering if a frame's bits incorrect as a result of transmission over the network. Generally such errors may occur as a result of some kind of signal interference during frames transmission.

To detect an error, the sending machine calculates a complex mathematical function, with the frame contents as input, putting the result into the frame's FCS field. The receiving device does the same mathematical function on the receiving frame; if its calculation doesn't match the FCS field, an error occurred, the frame is discarded and retransmission is required (retransmission occurs by Layer 4 TCP protocol as part of error recovery procedures), otherwise, nothing will be happened.

Ethernet Frames Reception

Clearly, Frame reception is the reverse of frame transmission. For both half-duplex and full-duplex transmissions, Ethernet frame reception is essentially the same, except that full-duplex MACs must have separate frame buffers and data paths to allow for simultaneous frame transmission and reception.

When the frame is received, the destination address of the received frame is checked and matched against the machine's address list (its MAC address, its group addresses, and the broadcast address) to determine whether the frame is destined for that machine. If an address match is found, the frame length is checked, and the received FCS is compared to the FCS that was generated during frame reception. If the frame length is the same and there is an FCS match, the frame type is determined by the contents of the Length/Type field. The frame is then parsed and forwarded to the appropriate upper layer in the destination machine.

Ethernet Connection and Cabling

Some of Ethernet cable standards use coaxial cable or optical fiber; others are using **Ethernet over twisted pair.** There are several different standards for this copper-based physical medium. The most widely used are **10BASE-T** (Ethernet), **100BASE-TX** (Fast Ethernet; FE), and **1000BASE-T** (Gigabit Ethernet; GE). Ethernet over twisted pair refers to the use of cables that contain insulated copper wires twisted together in pairs for the physical layer of an Ethernet network—that is, a network in which the Ethernet standard protocol provides the data link layer. All these three standards use the same RJ45 connectors. Generally, different generations of Ethernet equipments can be freely mixed, since higher speed implementations always support the lower speeds. These standards always use eight positions modular connectors, usually called RJ45. The cables are four-pairs of twisted cable. Each of the three standards support both full-duplex and half-duplex communication. All these standards operate over distances of up to 100 meters. Some key differences however exist, particularly with the number of wire pairs needed in each case, and in the type (category) of cabling. Moreover, Power over Ethernet (PoE) technique can be implemented over UTP cables.

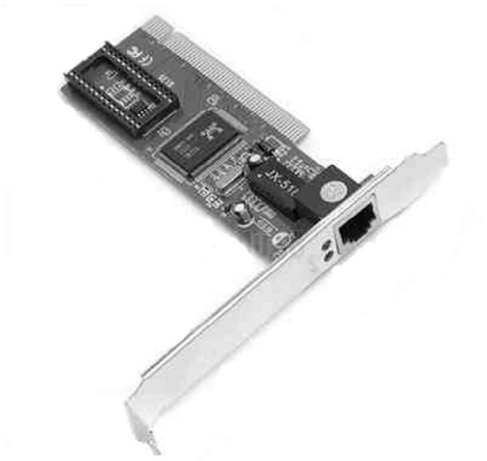
Understanding the Ethernet connection components is important in the CCENT studying. This section describes

the use of UTP cabling in Ethernet network with a sufficient detail.

Ethernet Network Interface Cards (NICs)

Personal Computers (PCs) are connected to Ethernet LAN using NICs. The NIC is a printed circuit board as shown in Figure 1-29. It provides network communication features to and from PCs on a network.

Figure 1-29 Ethernet LAN NIC



The NIC implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet or token ring. The protocols used in the NIC provides a base for a full network protocol suite, allowing communication on the same LAN for small groups of computers as well as communication on a large-scale network (WAN, Internet) through routable protocols, such as IP.

The NIC can be plugged into a motherboard PCI expansion slots, in this case it's called LAN adapter, and it can be built within a motherboard as a build-in Ethernet port. It provides the PC an interface to the LAN and it has a MAC address which is burned and stored in ROM by manufacture. To make the NIC work efficiently with the PC, it has some requirements. These are: IRQ line, I/O address, a memory space, and drivers. Sometimes the word *controller* is used to refer to the NIC.

Ethernet Connection Media

EIA/TIA standards body defined the Ethernet cables and connectors specifications. This means that RJ-45 connector and Ethernet cabling categories are derived from the EIA/TIA specifications. Several types of connection media can be used in a LAN deployment. Figure 1-30 presents the typical connection media types.

The RJ-45 connector represents the most common type of connection media, where the letters "RJ" stands for registered jack and the number "45" refers to a specific physical connector that has eight conductors. Another type of connection media is presented in Figure 1-31.

In addition to the popular RJ-45 connectors and ports, CISCO LAN switches have a few interfaces that use either Gigabit Interface Converters (GBIC) or Small-Form Pluggables (SFP). Figure 1-32 shows a 1000BASE-T GBIC. A GBIC is a hot-swappable I/O device that plugs into a Gigabit Ethernet switch port; this means that physical ports can be changed without having to purchase a whole new switch. A GBIC is interchangeable, which gives

the flexibility to deploy other 1000BASE-X technology without having to change the physical interface or the model of the router or switch. Using a different kind of GBIC or SFP, CISCO switch can use a variety of cable connectors and types of cabling and support different cable lengths. GBICs are typically used for Uplinks of the LAN backbone.

Figure 1-30 Types of Connection Media

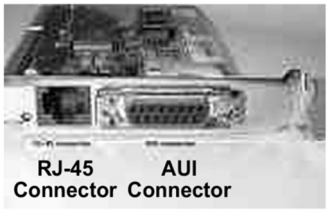


Figure 1-31 Fiber Optical Connector

Figure 1-32 1000BASE-T GBIC

GBICs support copper UTP and fiber-optic media for Gigabit Ethernet transmission. There are several types of the fiber-optic GBICs, as shown in Figure 1-33. These types are:

- Short wavelength (1000BASE-SX)
- Long wavelength (1000BASE-LX/LH)
- Extended distance (1000BASE-ZX)

Figure 1-33 Fiber GBIC

Fiber-Optic GBIC

GBIC Fiber Optic
Shields

The fiber-optic GBIC is a transceiver that converts serial electric currents to optical signals and vice versa.

Twisted-Pair Cables and RJ-45 Connectors

Twisted-Pair (TP) cable is a copper wire-based that can be either unshielded (UTP) or shielded (STP). The most popular Ethernet standards are using UTP cabling, which include either two or four pairs of wires. The wires inside the cable have an outer jacket of flexible plastic to protect the wires since these wires are thin and subtile. To prevent the wire from breaking, a thin plastic coating (insulation material) covers each individual copper wire and to make it easy to look at the ends of the cable and identify the ends of an individual wire, the plastic coating on each wire has a different color.

The wires in each pair are twisted around each other as shown in Figure 1-34. This will give one of the advantages of TP cables, which is the ability to cancel interferences from Electro-Magnetic Interference (EMI) and Radio Interference (RFI). An electro-magnetic field is created outside the wire when the current passes over any wire. The magnetic field can in turn cause electrical noise on other wires in the cable. By twisting together the wires in the same pair, with the current running in opposite directions on each wire, the magnetic field created by one wire mostly cancels out the magnetic field created by the other wire. Moreover, to reduce crosstalk between the pairs, the number of twists varies. The permitted number of twists per meter must follow accurate specifications defined in ANSI/TIA/EIA-568-A (for CAT 5). Because of its small size and lightweight, TP cables can be installed easily.

Figure 1-34 TP Cable

There are several categories of UTP cable. Table 1-3 lists these categories. The most commonly used categories in the network today are Cat. 1, 5, 5e, and 6.

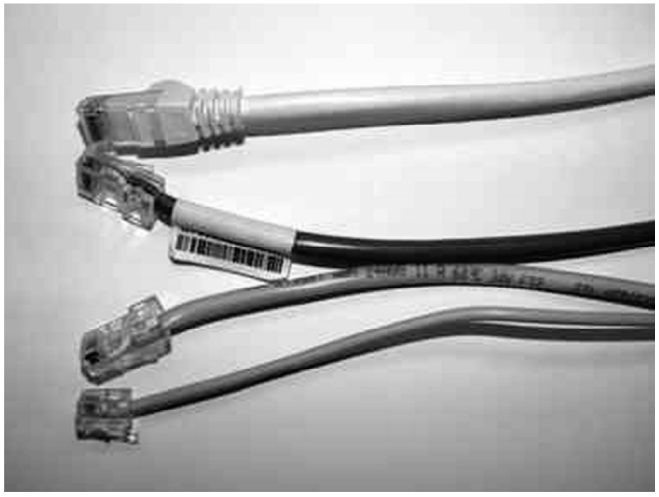
Table 1-3 UTP Categories

Type	Speed	Description
Cat. 1	Up to 20KHz	Used for telephone communication.
Cat. 2	Up to 4Mbps	Used for data transfer at speed up to 4 Mbps.
Cat. 3	Up to 10Mbps	Used in 10BASE-T Ethernet networks.
Cat. 4	Up to 16Mbps	Used in Token Ring networks.
Cat. 5	10/100/1000Mbps	Used in FastEthernet networks. It can be used for 10Mbps Ethernet. It can also be used for 1000Mbps for 10 meters.
Cat. 5e	10/100/1000Mbps	Used in Ethernet up to Gigabit networks. Cat. 5e generally provides the best price for performance.
Cat. 6	10/100/1000Mbps 10Gbps	Used in Ethernet up to Gigabit networks and 10Gbps over shorter distances.
Cat. 6a	10/100/1000Mbps	Used in network up to 10 Gigabit data transfer

	10GbE	for 100 meters.
Cat. 7	10/100/1000Mbps 10Gbps/100Gbps	Used in network up to 10 Gigabit data transfer and it may support the upcoming 100Gbps standard
Cat. 7a	Unknown	Upcoming standard that supports Ethernet bandwidths have not been defined.

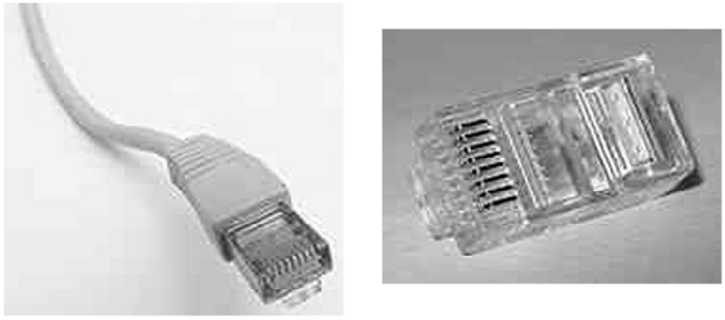
Figure 1-35 shows Cat. 6, Cat. 5e, Cat. 5, and a standard telephone cable for comparison.

Figure 1-35 Types of UTP Categories.



The RJ-45 connector is used at the end of UTP cable with the ends of the wires inserted into the connector. The RJ-45 connector has eight specific physical locations, called *pins,* into which the eight wires of the cable can be inserted into the correct positions. The RJ-45 connector needs to be inserted into an *RJ-45 port* in the switch or any other networking device. Figure 1-36 shows the UTP cables, and RJ-45 connectors. Figure 1-30 shows an RJ-45 port.

Figure 1-36 RJ-45 Connectors and Cables



UTP Cabling Pinouts Implementation

To implement UTP cable in a LAN, the connection type i.e., straight-through or crossover cable and the EIA/TIA

type of cable must be determined at first. The wires in the UTP cable must be connected to the correct pin positions in the RJ-45 connectors in order for communication between two end points to work correctly. The RJ-45 connector has eight *pins*, into which the eight copper wires of the UTP cable are inserted. The wiring *pinouts* must conform to the EIA/TIA Ethernet cabling standards described in this section.

The Telecommunications Industry Association (TIA) and the Electronics Industry Alliance (EIA) groups (not IEEE), define standards for UTP cabling, color coding for wires, and standard pinouts on the cables. (For more details, see http://www.tiaonline.org and http://www.eia.org). Figure 1-37 shows two pinout standards from the EIA/TIA, with the color coding and pair numbers listed.

Figure 1-37 EIA/TIA Standard Ethernet Cabling Pinouts

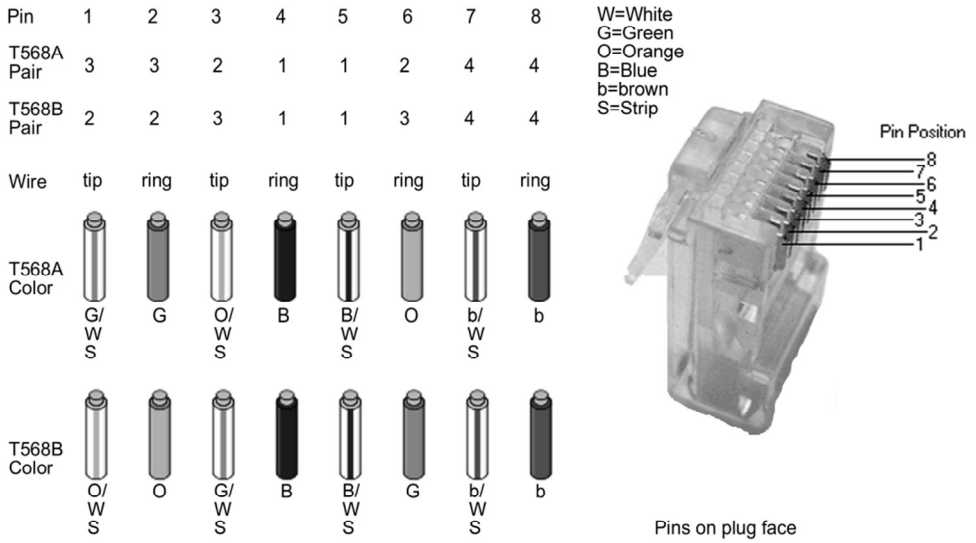


Figure 1-37 shows that the eight wires in a UTP cable have either a solid color (green, orange, blue, or brown) or a striped color scheme using white and one of the other four colors. Furthermore, a single-wire pair uses the same base color. For example, the green wire and the green/white striped wire are paired and twisted. For example, in Figure 1-37, the notation's G/W refers to the green-and white striped wire and so on.

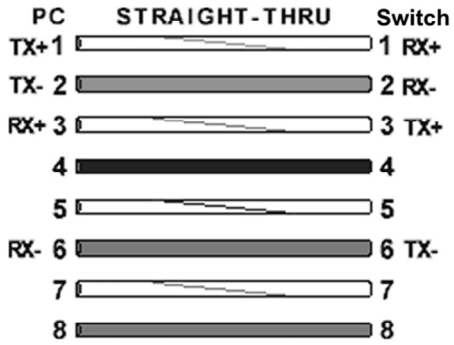
Four of the wires (two pairs) carry the positive voltage, and the other four wires carry the negative voltage. The positive are called “tip” (T1 through T4) while the negative are called “ring” (R1 through R4). At the end of the UTP cable, the RJ-45 plug is connected, which is the male component. The male component is inserted into a female component (the jack, i.e., a socket). The jack is found in a network device, wall, patch panel or cubicle portion outlet. Figure 1-36 shows the male component whereas Figure 1-29 shows the female component. The front view of the male component, shown in Figure 1-37, identifies the pin locations which are numbered from 8 on the left to 1 on the right.

Correct wiring pinout on each end of the cable is required to build a working Ethernet LAN. For 10BASE-T and 100BASE-TX networks, two pairs of wires of the UTP cable are required, whereas four pairs of wires are required for 1000BASE-T.

In 10BASE-T and 100BASE-TX Ethernets, one pair should be used to send data in one direction, and the other pair should be used to receive data. Two wires are used for full-duplex networks. Ethernet NICs should send data using pair 3 according to the T568A pinout standard (the pair connected to pins 1 and 2). While, Ethernet NICs should receive data using pair 2 according to the T568A standard (the pair at pins 3 and 6). On the other

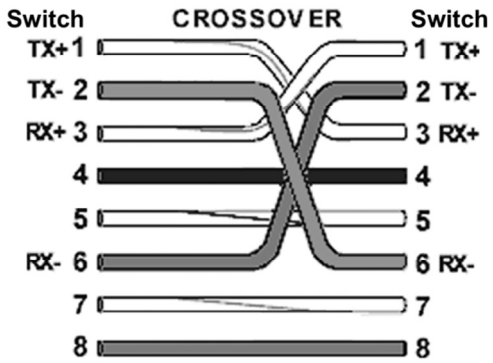
hand, hubs and switches do the opposite—they receive on the pair 3 according to the T568A pinout standard (the pair at pins 1, 2), and they send on the pair 2 according to the T568A pinout standard (the pair at pins 3, 6). Therefore, to create a straight-through LAN cable, both ends of the cable must use the same EIA/TIA pinout standard on each end of the cable. This means that the pin number of the wire must be the same at both end of the wire when an Ethernet straight-through cable is used. To be more clarify, wire at pin 1 on one end of the cable must be connected to pin 1 at the other end of the cable; the wire at pin 2 must be connected to pin 2 on the other end of the cable; and so on. Figure 1-38 shows how to use the straight-through cable.

Figure 1-38 The Use of Straight-Through Cable



From the above description, clearly that, devices on the ends of the cable use opposite pins when they transmit/receive data. For such cases (connecting PC_NIC to a hub, switch …etc.) a straight-through cable is used. On the other hand, there are some cases that require connecting PC_NIC to PC_NIC or router to a router or switch to switch or switch to a router …etc. These cases require connecting two devices that both ends of the cable use the same pins to transmit and the same pins to receive. Therefore, the pinouts of the cable must be set up to swap/cross the wire pair. This type of cable is called a *crossover cable*. For example, when connecting two switches directly, both switches send on the pair at pins 3,6, and receive on the pair at pins 1,2, the cable must cross the pairs. Figure 1-39 shows the connection of a switch to a switch using a crossover cable.

Figure 1-39 A Switch to Switch Connection Using a Crossover Ethernet Cable



As a summary, devices on opposite ends of a cable that use the same pair of pins to transmit need a crossover cable (T568A at one end; T568B at the other). Devices that use an opposite pair of pins to transmit need a straight-through cable (either T568A or T568B at each end). Table 1-4 lists the network devices and the pin pairs

they use for 10BASE-T and 100BASE-TX Ethernets.

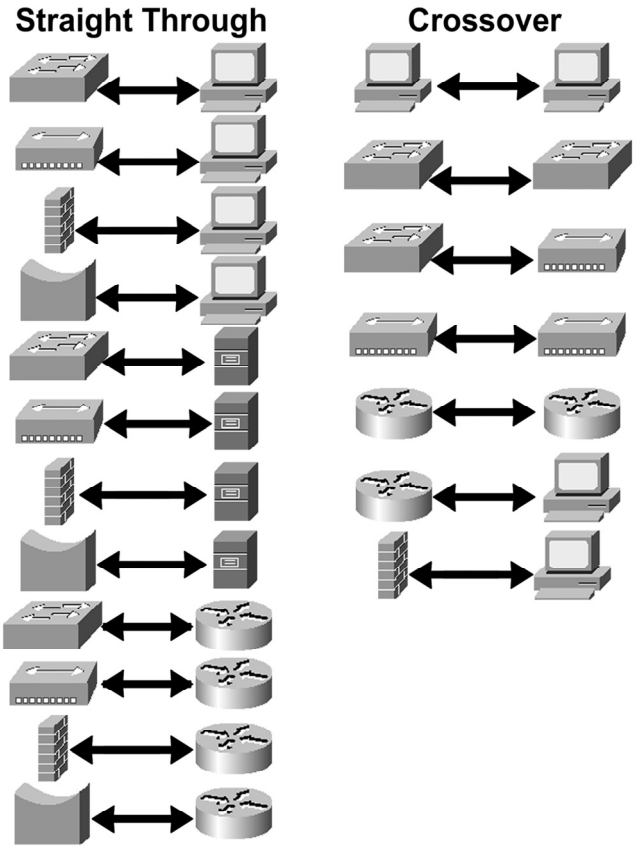
Table 1-4 The Used Pin Pairs for the devices in 10BASE-T and 100BASE-TX

Devices That Use 1,2 for Transmitting and 3,6 for Receiving	Devices That Use 3,6 for Transmitting and 1,2 for Receiving
PC NICs	Hubs
Wireless Access Point	Bridges
Networked printers	Switches
Routers	Firewalls

The logic above differs in 1000BASE-T for the cabling and pinouts. First, Gigabit Ethernet requires four wire pairs. Secondly, Gigabit Ethernet transmits and receives on each of the four wire pairs simultaneously. However, Gigabit Ethernet does have a concept of straight-through and crossover cables, with a minor difference in the crossover cables. The pinouts for a straight-through cable are the same—pin 1 to pin 1, pin 2 to pin 2, and so on. The crossover cable crosses the same two-wire pair as the crossover cable for the other types of Ethernet—the pair at pins 1,2 and 3,6—as well as crossing the two other pairs (the pair at pins 4,5 with the pair at pins 7,8).

To choose which type of cable to use when interconnecting CISCO devices, it is better to follow Figure 1-40 for different type of interconnections.

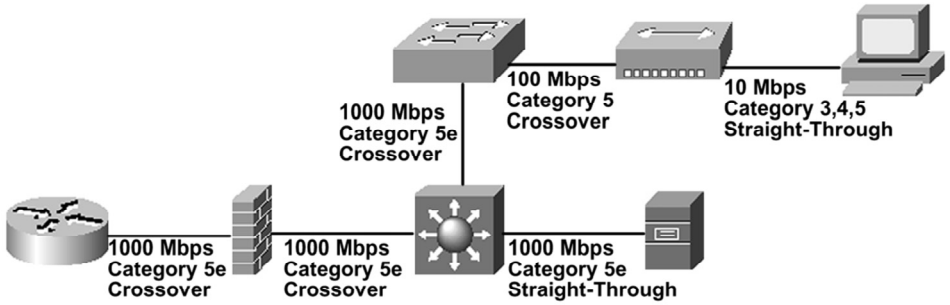
Figure 1-40 Straight-through Cable versus a Crossover Cable



Now, there is no need to take care about which type (crossover or straight-through) to be used in the LAN, all are working. The current CISCO switches have a feature called auto-mdix that notices when the wrong cabling pinouts are used. This feature makes the cable work in spite of its type by readjusting the switch's logic.

To know how an enterprise network can be interconnected with different types of UTP cable, see Figure 1-41.

Figure 1-41 Different Types of UTP Cables in the Enterprise Network.

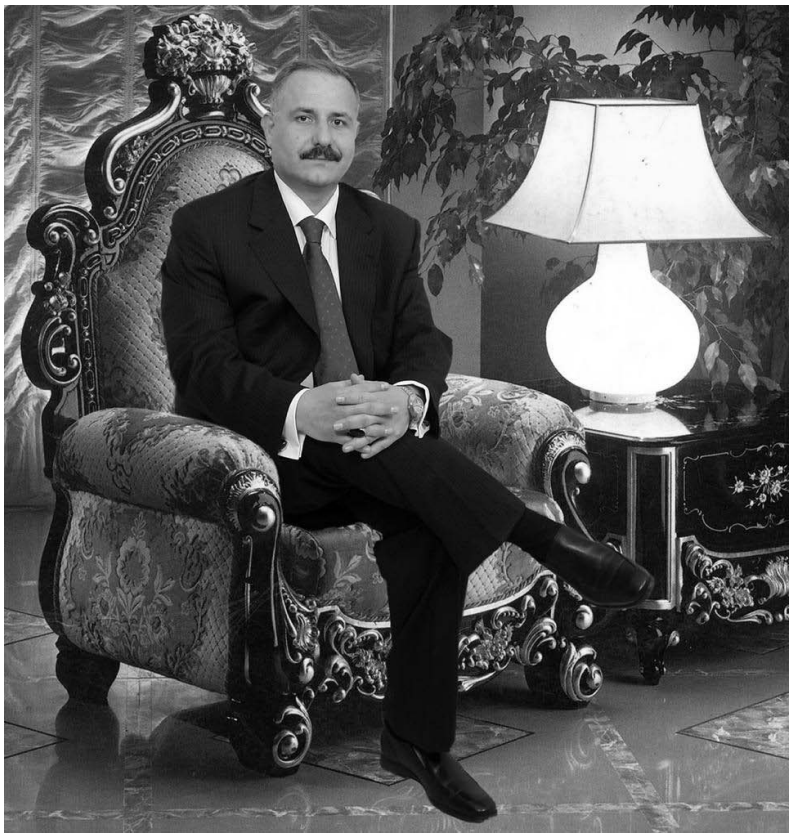


Summary

In this chapter, a strong foundation for networking and internetworking are presented. The background presented here is essential for understanding the rest of the book and undertaking the examination. A solid foundation to build a comprehensive knowledge of the networking technology is provided in this chapter. The following subjects are covered:

- Networking essentials
- Internetworking essentials
- Internetworking evolving
- Internetworking models
- OSI reference model
- OSI encapsulation and de-encapsulation terminologies
- Ethernet LANs
- Data transmission types
- CSMA/CD algorithm
- Ethernet addressing
- Ethernet connection and cabling

At the end of the chapter, several learning questions are given to evaluate the learning level from this chapter. The correct answers and solutions with complementary discussions are found in appendix A, "Answers to Chapters Learning Questions."

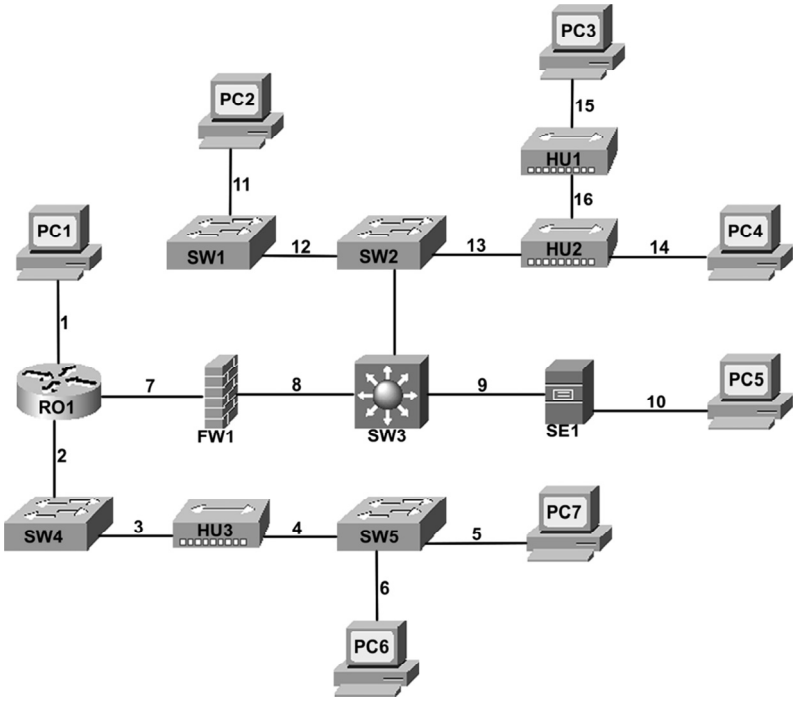


Appendix B
Three Simulated CISCO Exams

Exam E1
E1 Exam Engine

E1-1. Which of the following statements is true regarding the internetwork shown in Figure E1-1? (Select all that apply)

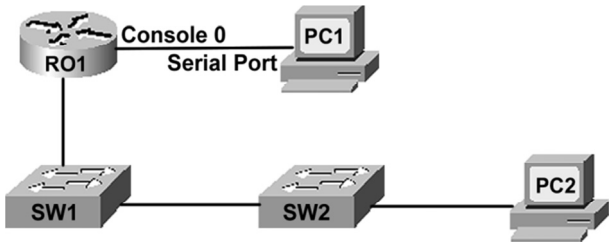
Figure E1-1 A Sample Internetwork



A. The link number 15 uses a straight-through cable.
B. The link number 11 uses a straight-through cable.
C. The frames that SW4 sends over the link number 3 could collide with the frames that SW5 sends over the link number 4.
D. The frames that PC6 sends should never collide with other frames, assuming that the link number 6 uses full duplex.
E. The link number 2 uses a rollover cable.
F. The link number 6 uses a crossover cable.
G. The link number 12 uses a straight-through cable.

E1-2. In Figure E1-2, PC1 management station can successfully ping to SW1, but the Telnet connection fails, with a message indicating that the passwords are missed. Using a password of **cisco**, which of the following commands, when entered in the correct order, recover Telnet issue of this internetwork? (Assuming that, the IP configuration of the whole internetwork is accurate.)

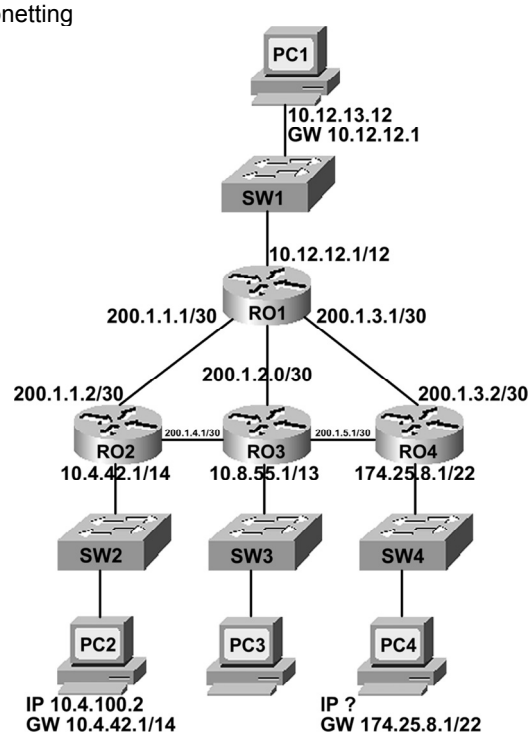
Figure E1-2 Telnet Failed Internetwork



A. **login**
B. **password cisco**
C. **line telnet 0 4**
D. **enable telnet**
E. **line vty 0 4**
F. **cisco password**
G. **enable telnet cisco password**

E1-3. Which of the following statements is true about the internetwork shown in Figure E1-3? (Assume that RIP-2 and the **ip subnet zero** command are configured correctly on all the routers, and autosummarization is disabled.)

Figure E1-3 An Enterprise Subnetting

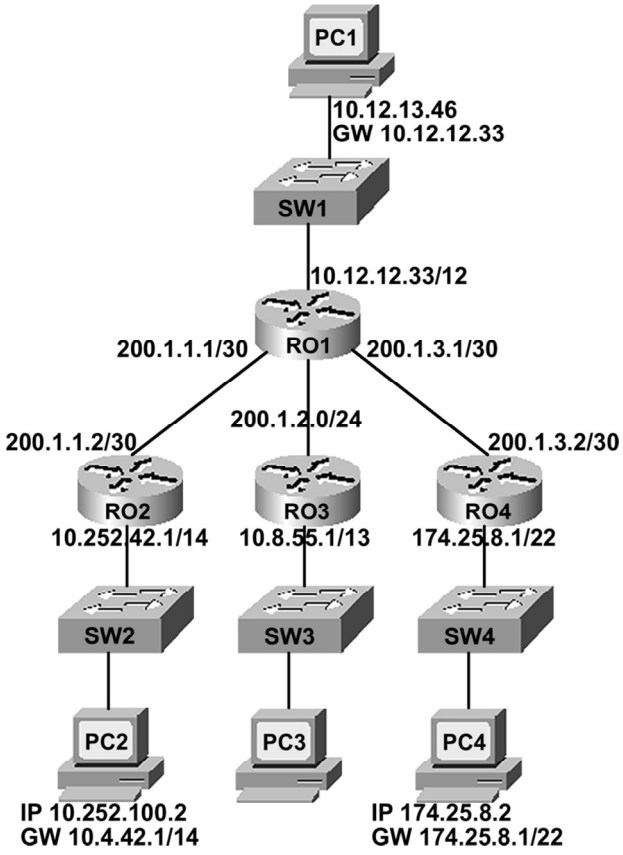


A. To allow PC4 pings PC1, an IP address of 174.25.8.45/17, could be assigned to PC4.
B. To allow PC4 pings PC1, an IP address of 174.25.8.45/24, could be assigned to PC4.

C. To allow PC2 pings other PCs, the prefix of /13 could be used by PC2 and RO2 on its LAN interface.
D. To allow PC2 pings other PCs, the prefix of /16 could be used by PC2 and RO2 on its LAN interface.

E1-4. Which of the following statements is true about the internetwork shown in Figure E1-4? (Assume that RIP-2 and the **ip subnet zero** command are configured correctly on all the routers, and autosummarization is disabled.)

Figure E1-4 An Enterprise with Different Types of Subnetting



A. Pinging from PC1 to RO3 tends that the ICMP Echo request passes over a non-subnetting serial link.
B. Pinging from PC4 to PC2 tends that the ICMP Echo request passes over three zero subnets.
C. Pinging from PC1 to PC4 tends that the ICMP Echo request is discarded because a zero subnet is used in the route.
D. Pinging from PC4 to PC2 tends that the ICMP Echo request flows over a broadcast subnet.

E1-5. Match each of the following packet's destinations IP addresses to the route that the router would use when forwarding the packet. (Assume that the classful routing is used.)

1. 172.18.10.1
2. 10.5.25.10
3. 10.5.1.1
4. 10.5.10.1

5. 10.5.24.35

   A. 10.5.1.1/30 [120/1] via… Serial0/0/1
   B. 0.0.0.0/0 [120/1] via… Serial1/0/0
   C. 10.5.0.0/19 [120/1] via… Serial0/1/0
   D. 10.5.0.0/22 [120/1] via… Serial0/1/1
   E. 10.5.0.0/18 [120/1] via… Serial1/1/0

E1-6. What is the first reaction for a switch, if it receives a frame whose source MAC address has not been seen by the switch since the switch was most recently powered ON?

A. It drops the frame.
B. It checks the frame for loops using STP.
C. It adds the source MAC address to the switch MAC table.
D. It adds the source and destination MAC address to the MAC table associated with the interface, which receives the frame.
E. It forwards the frame out all ports, except the one on which the frame received.

E1-7. Which of the following statements are true about the access to router Thaar? (Assume that this Router is configured correctly according to the configuration shown in Exhibit E1-1, and the user can ping the Router from his PC.)

Exhibit E1-1 The **show run** Command Output

```
hostname Thaar
!
enable secret cisco123
enable password cisco
!
interface Fa0/0
ip address 172.18.18.1 255.255.255.0
!
line con 0
password con123
login
!
line vty 0 4
transport input telnet ssh
password terminal123
login
```

A. To access privileged mode from user mode, the user must supply the password **cisco**.
B. To access privileged mode from user mode, the user must supply the password **cisco123**.
C. Telnet connection to Thaar is allowed and the Router will ask the user to supply a user mode password.
D. SSH connection to Thaar is rejected and is not even allowed to try to supply a user mode password.

E1-8. Match each of the following problems to its suitable OSI layer, which can isolate the problem.

1. A 2960's SYST LED is solid (non-blinking) amber.
2. The **show interfaces** command lists "up and down" status.
3. When you tried to execute the **traceroute** command, the output lists three routers, but it never completes.
4. You can ping the web server, but when you try to access a web page, the result will be "page not found."

A. Application
B. Presentation
C. Session
D. Transport
E. Network
F. Data Link
G. Physical

E1-9. Which of the following configurations would cause a router to load its ROM Monitor code and enter ROMMON mode after the router is reloaded?

A. The router's configuration register is set to 0x2100.
B. The router's configuration register is set to 0x2101.
C. The router's configuration register is set to 0x2102.
D. The router's configuration register is set to 0x2102, but only if the router fails to obtain an IOS from flash, TFTP, and ROM.
E. The router's configuration register is set to 0x2104, but only if the router fails to obtain an IOS from flash, TFTP, and ROM.
F. Only if the router fails to obtain an IOS from flash, TFTP, and ROM.

E1-10. Which of the following commands describe in at least three lines of output a neighboring CISCO device?

A. **show cdp traffic**
B. **show cdp neighbor**
C. **show cdp interface** [*type number*]
D. **show cdp neighbor detail**
E. **show cdp entry** *name*

E1-11. Which of the following statements accurately describe Exhibit E1-2, which shows the output from a command prompt on a PC, with the PC connected to a CISCO switch?

Exhibit E1-2 The **ipconfig /all** Command Output

```
C:\>ipconfig /all
Windows IP Configuration
Host Name . . . . . . . . . . . . : thaar
Primary Dns Suffix . . . . . . . :
Node Type . . . . . . . . . . . . : Unknown
IP Routing Enabled. . . . . . . . : No
WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
Media State . . . . . . . . . . . : Media disconnected
Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connection
Physical Address. . . . . . . . . : 00-15-F2-F3-C1-D4
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 192.168.0.2
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.2.1
DNS Servers . . . . . . . . . . . : 4.2.2.2
4.1.1.1
```

Answers to Exam E1 Questions

E1-1. A-D. Since, SW5 usually creates a separate collision domain for each port; PC6 should never have collisions, and hence PC6 disables its CSMA/CD logic. However, because SW4 and SW5 are separated by a hub, collisions can occur, and both switches must use half duplex when communicating through the hub. In the Ethernet, pairs of PCs, pairs of routers, and pairs of switches use crossover cables between each other, and all other links use straight-through cables. Moreover, the connection between a PC's serial port and the console of a CISCO device, such as, the link number 1, use the rollover cables. Rollover cable is a type of null-modem cable that is used to connect a computer terminal to a router's console port. It is also known as CISCO console cable or the Yost cable or more appropriately the "Yost Serial Device Wiring Standard." It gets the name rollover because the pinouts on one end are reversed from the other, as if the wire had been rolled over. Rollover cables could be an RJ-45 Rolled or RJ-45 to DB-9 Female or RJ-45 to RS 232. Table E1-1 shows how the pins are rolled when using RJ-45 Rolled. You can visit "http://www.cisco.com/en/US/products/hw/routers/ps332/products_tech_note09186a0080094ce6.shtml" for more information about CISCO cables.

Table E1-1 RJ-45 Rolled Pins

RJ-45 Pin	RJ-45 Pin
1	8
2	7
3	6
4	5
5	4
6	3
7	2
8	1

E1-2. A, B, E. The SW2 will be ready to accept incoming Telnet sessions, when the commands **line vty 0 4**, **login**, and **password cisco** are entered in this order, from the configuration mode.

E1-3. D. The first two answers are incorrect since the suggested IP address of 174.25.8.45 for PC4 is not located in the same subnet as RO4's IP 174.25.8.1 address.

For PC2 to function in this network, it must be in the same subnet as RO2's LAN IP address. By focusing on the third octet in the IP addresses of RO2 and PC2, you will find that only last answer is correct.

E1-4. A, B, D. Clearly the question is related to the use of a zero subnet, broadcast subnet and other types of subnetting. A zero subnet is the one subnet of a classful network for which all the subnet bits are 0. It is possible to discover the use of subnet zero by calculating the subnet number and finding if it is the same as the classful network number.

The zero subnets in the Figure E1-4 are the serial links between RO1 and RO2, and between RO1 and RO4, and the RO4 LAN.

The RO1-RO3 serial link is not using subnetting. It uses the Class C default subnet mask.

The RO2 LAN uses a broadcast subnet. A broadcast subnet is one for which the subnet broadcast address is the same as the network-wide broadcast address, and it is the last numeric subnet in a network.

Note that with the **ip subnet zero** command configured and a classless protocol in use, the zero subnets are allowed and will work, and the broadcast subnet is allowed without additional special commands. However, keep in your mind that even though the broadcast and zero subnets are supported, it is still best to avoid them.

E1-5.

1 B
3 A
4 C
5 C

Looking at the routing table, it contains five routes, one is the default route, and four are for subnets of network 10.0.0.0.

Only the packet to 172.18.10.1 could match the default route, since, with classful routing, the default route would not be used for packets sent to destinations in network 10.0.0.0 that do not match the other four routes. For destinations in the network 10.0.0.0 that matched multiple routes, the router will choose the more-specific (longer prefix length) routes. Please, note that if the question includes a network simulator, you can easily find the matched route by using the **show ip route** *address* command. This command will list the route matched for the IP address given in the command.

E1-6. C. For any new address, the switch/bridge first creates an entry in its MAC table; then it forwards the frame based on the switch's rules.

E1-7. B, C, D. The router (or switch) will require the **enable secret** password only if both the **enable password** and **enable secret** commands are configured. Since, the VTY lines use simple password security, which is configured correctly, Telnet access will be successful. However, SSH requires VTY login security that uses both a username and password, which are not configured on Router Thaar, so the router will reject SSH connection requests without even asking for a username and password.

E1-8.

1 G
2 F
3 E
4 A

When the SYST light on a 2960 switch is solid amber, this means that the switch physically failed to boot, so it cannot communicate with any attached devices.

When the two interface state settings on a router/switch being "up and down," the problem is most likely to be a data link layer problem.

When the output of the **traceroute** command lists three routers, but it never completes, the problem may not be a network layer problem, but the next step is to look at Layer 3 issues at the last router listed in the command output.

When the server can be pinged, this means that the network layer (and below) work well because. A "page not found" means that the web server replied with an HTTP message, and the problem is in the application layer.

E1-9. A. The last hex digit in the boot field of the configuration register indicates whether the router loads Rom Monitor software when it is set to hex 0 or not, ignoring all other options.

E1-10. D, E. The answers A and C list commands, which provide information about the operation of CDP, not the information learned by CDP. The **show cdp neighbor** command provides only a single line of summary information. The correct answers' commands provide the same full detailed information about a neighbor in roughly 15 lines of information.

E1-11. B, C, D. It is clear from Exhibit E1-2, which the PC has DHCP enabled, and there is a leased period of 16 days. Therefore, its IP address 192.168.0.2 is obtained dynamically using the DHCP server and at the time the command is executed on the host. The remaining leased period is less than 16 days. From Exhibit E1-2, it's also clear that the DHCP server's IP address is 192.168.2.1- which is not in the same host classful network, and the DNS server is on a different network, and it may be obtained using the DHCP server.

E1-12. D.

ICMP (Internet Control Message Protocol) is composed of a series of protocols used for network connectivity test.

DHCP (Dynamic Host Configuration Protocol) is used to dynamically provide IP information to hosts.

DNS (Domain Name Service) associates FQDN names with IP addresses.

ARP (Address Resolution Protocol) uses broadcasts' messages to find the corresponding MAC address for a known IP address.

RARP (Reverse Address Resolution Protocol) uses broadcasts to find the corresponding IP address for a known MAC address.

All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams is an intensive, one-week study guide that provides students with all the knowledge they need to excel on the CCNA/CCENT exam. This certification guide is designed to make even the most difficult internetworking concepts easy to understand.

Author Thaar AL_Taiey highlights critical information, outlines necessary procedures, and identifies exam essentials. Students can understand the concepts and, then, test their knowledge, by 13 built-in exam engines, on about two thousand, and two hundred challenging questions that mimic the formats found on the exam, including multiple-choice-single-answer, multiple-choice-multiple-answers, fill-in-the-blank, testlet, drag-and-drop, and simulations. Students have two options to read the questions and their answers, either by using the built-in exam engine at the end of each chapter or by reading the questions and their answers in the EBook. Each chapter follows a strict organization (Description of chapter topics, Main exposition of topics, Chapter summary, A commands reference, A list of the suggested learning questions, and Exam Engine with Flash Cards.)

All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams provides in-depth coverage of all official CCNA/CCENT exam objectives and uses 2800 router, 1841 router, catalyst 2960 switch, and many other CISCO devices to clarify the required concepts. The book uses many highly-professional figures, exhibits, tables, configurations, and real internetworking scenarios to clarify the required concepts. It also provides up-to-date information on the newest catalyst 2960-S switch and 802.11n wireless technology.

Designed and organized for absolute beginners as well as for CISCO internetworking professionals. All-in-One for Beginners (EBook, 13 Exam Engines, and Flash cards): The Complete One-Week Preparation for the CISCO CCENT/CCNA ICND1 Exam 640-822 with Three Simulated CISCO Exams gives students the necessary foundation to overtake the CCNA/ CCENT exam with extreme confidence and post high scores.

The following CISCO CCNA/CCENT topics are covered carefully in this book:
Describing the operation of computer data networks • Describing the required CISCO Devices for CCENT • Operating CISCO Switches and Routers • Implementing small switched CISCO networks • Implementing an IP addressing scheme and IP services to meet the network requirements for small and large offices • Implementing a small and a large routed network • Managing and verifying CISCO switches and routers • Explaining and selecting the appropriate administrative tasks required for a WLAN • Implementing and verifying several WAN links • Identifying security threats to a network and describing general methods to mitigate those threats •Describing Wireless technology.

Thaar Al_Taiey holds a Master degree (MSc) in Nuclear Engineering (MSNE) specialist in Software Engineering (MSSE) and BSc degree in Electrical Engineering (BSEE). He also holds an ITIL V3 Certificate in the IT Service Management. He has more than 20 years' experience in Automated System fields. His experience in Distributed Control Systems (based VME), Internetworking based CISCO, 3COM, HP, UNIX Operating Systems (Ultrix-32, OSF-1, SCO, Solaris and Linux), Oracle ORDBMS and Windows OS. In these areas, he works as IT consultant and supervisor, Data Center Manager, Network manager, Network Designer and Sr. network Engineer, UNIX System administrator, Oracle DBA, Windows System administrator and technical support engineer. In the field of training, he has instructed and developed several technical courses including CISCO certified courses. Mr AL_Taiey is the leading scientist for many thoughts and ideas in several fields of technology. For the past decade, AL_Taiey has been closely involved with the computer and networking system development. He is the author/co-author of several technical papers and books. He is the Chairman of ThaarTechnologies and is a member of the IWWHS.

Computers/Certification Guides/Cisco
Computers/Internet

ThaarTechnologies Publishing
www.thaartechnologies.com

USD149.95

ISBN 978-0-9831212-6-8
5 14095
9 780983 121268