Course Booklet

CCNA Exploration

Routing Protocols and Concepts

Version 4.0

ciscopress.com

Cisco | Networking Academy
Mind Wide Open

CCNA Exploration Course Booklet Routing Protocols and Concepts, Version 4.0

Cisco Networking Academy

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing September 2009

Library of Congress Cataloging-in-Publication Data is available upon request

ISBN-13: 978-1-58713-251-3

ISBN-10: 1-58713-251-6

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Cisco Representative
Erik Ullanderson

Cisco Press Program Manager
Anand Sundaram

Executive Editor
Mary Beth Ray

Managing Editor
Patrick Kanouse

Project Editor
Bethany Wall

Editorial Assistant
Vanessa Evans

Cover Designer
Louisa Adair

Composition
Mark Shirar

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.cisco.com/edu.

Warning and Disclaimer

This book is designed to provide information about the protocols and concepts of routing. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Course Introduction

Welcome

Welcome to the CCNA Exploration Routing Protocols and Concepts course. The goal is to develop an understanding of how a router learns about remote networks and determines the best path to those networks. This course includes both static routing and dynamic routing protocols. The specific skills covered in each chapter are described at the start of each chapter.

More than just information

This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and gradebook
- Packet Tracer 4.1 simulation tool
- Additional software for classroom activities.

A global community

When you participate in the Networking Academy, you are joining a global community linked by common goals and technologies. Schools, colleges, universities and other entities in over 160 countries participate in the program. You can see an interactive network map of the global Networking Academy community at http://www.academynetspace.com.

The material in this course encompasses a broad range of technologies that facilitate how people work, live, play, and learn by communicating with voice, video, and other data. Networking and the Internet affect people differently in different parts of the world. Although we have worked with instructors from around the world to create these materials, it is important that you work with your instructor and fellow students to make the material in this course applicable to your local situation.

Keep in Touch

These online instructional materials, as well as the rest of the course tools, are part of the larger Networking Academy. The portal for the program is located at http://cisco.netacad.net. There you will obtain access to the other tools in the program such as the assessment server and student grade book), as well as informational updates and other relevant links.

Mind Wide Open®

An important goal in education is to enrich you, the student, by expanding what you know and can do. It is important to realize, however, that the instructional materials and the instructor can only

facilitate the process. You must make the commitment yourself to learn new skills. Below are a few suggestions to help you learn and grow.

1. Take notes. Professionals in the networking field often keep Engineering Journals in which they write down the things they observe and learn. Taking notes is an important way to help your understanding grow over time.
2. Think about it. The course provides information both to change what you know and what you can do. As you go through the course, ask yourself what makes sense and what doesn't. Stop and ask questions when you are confused. Try to find out more about topics that interest you. If you are not sure why something is being taught, consider asking your instructor or a friend. Think about how the different parts of the course fit together.
3. Practice. Learning new skills requires practice. We believe this is so important to e-learning that we have a special name for it. We call it e-doing. It is very important that you complete the activities in the online instructional materials and that you also complete the hands-on labs and Packet Tracer® activities.
4. Practice again. Have you ever thought that you knew how to do something and then, when it was time to show it on a test or at work, you discovered that you really hadn't mastered it? Just like learning any new skill like a sport, game, or language, learning a professional skill requires patience and repeated practice before you can say you have truly learned it. The online instructional materials in this course provide opportunities for repeated practice for many skills. Take full advantage of them. You can also work with your instructor to extend Packet Tracer, and other tools, for additional practice as needed.
5. Teach it. Teaching a friend or colleague is often a good way to reinforce your own learning. To teach well, you will have to work through details that you may have overlooked on your first reading. Conversations about the course material with fellow students, colleagues, and the instructor can help solidify your understanding of networking concepts.
6. Make changes as you go. The course is designed to provide feedback through interactive activities and quizzes, the online assessment system, and through interactions with your instructor. You can use this feedback to better understand where your strengths and weaknesses are. If there is an area that you are having trouble with, focus on studying or practicing more in that area. Seek additional feedback from your instructor and other students.

Explore the world of networking

This version of the course includes a special tool called Packet Tracer 4.1®. Packet Tracer is a networking learning tool that supports a wide range of physical and logical simulations. It also provides visualization tools to help you to understand the internal workings of a network.

The Packet Tracer activities included in the course consist of network simulations, games, activities, and challenges that provide a broad range of learning experiences.

Create your own worlds

You can also use Packet Tracer to create your own experiments and networking scenarios. We hope that, over time, you consider using Packet Tracer – not only for experiencing the activities included in the course, but also to become an author, explorer, and experimenter.

The online course materials have embedded Packet Tracer activities that will launch on computers running Windows® operating systems, if Packet Tracer is installed. This integration may also work on other operating systems using Windows emulation.

Course Overview

The primary focus of this course is on routing and routing protocols. The goal is to develop an understanding of how a router learns about remote networks and determines the best path to those networks. This course includes both static routing and dynamic routing protocols. By examining multiple routing protocols, you will gain a better understanding of each of the individual routing protocols and a better perspective of routing in general. Learning the configuration of routing protocols is fairly simple. Developing an understanding of the routing concepts themselves is more difficult, yet is critical for implementing, verifying, and troubleshooting routing operations.

Each static routing and dynamic routing protocol chapter uses a single topology throughout that chapter. You will be using that topology to configure, verify, and troubleshoot the routing operations discussed in the chapter.

The labs and Packet Tracer activities used in this course are designed to help you develop an understanding of how to configure routing operations while reinforcing the concepts learned in each chapter.

Chapter 1 Introduction to Routing and Packet Forwarding - In Chapter 1, you will be introduced to the router, its role in the networks, its main hardware and software components, and the packet forwarding process. You will also be given an overview of directly connected networks, static routing, and dynamic routing protocols, along with a brief introduction to the routing table. Each of these topics is discussed in more detail in later chapters. Chapter1 also includes a review of basic Cisco IOS commands.

Chapter 2 Static Routing - Chapter 2 focuses on the role and configuration of static routes. The routing table process is introduced, and you will be shown how to verify route entries as they are added and deleted from the routing table. This chapter also discusses Cisco Discovery Protocol, which is a tool that you can use to help verify network operations.

Chapter 3 Introduction to Dynamic Routing Protocols – Chapter 3 provides an overview of routing protocol concepts and the various dynamic routing protocols available for routing in IP networks. In this chapter, you will examine the role of routing protocols. There is an overview of the classification of dynamic routing protocols. This overview is useful for comparing and contrasting the different protocols. Most of the information in this chapter is examined in more detail in later chapters.

Chapter 4 Distance Vector Routing Protocols – Chapter 4 presents two different types of routing protocols: distance vector and link-state. You will examine distance vector concepts and operations, including network discovery, routing table maintenance, and the issue of routing loops. In this chapter, you will also be introduced to the concepts used in RIPv1, RIPv2, and EIGRP routing protocols. These routing protocols are discussed in more detail in later chapters.

Chapter 5 RIP version 1 – Chapter 5 is the first chapter that focuses on a specific dynamic routing protocol. In this chapter, you will learn about RIP (Routing Information Protocol) version 1. RIPv1, a classful, distance vector routing protocol, was one of the first IP routing protocols. You will examine the characteristics, operations, and limitations of RIPv1. You will also learn about RIPv1 configuration, verification, and troubleshooting techniques.

Chapter 6 VLSM and CIDR - Chapter 6 reviews VLSM (Variable Length Subnet Masking) and CIDR (Classless Inter-Domain Routing) concepts that were presented in the Network Fundamentals course. You will explore the benefits of VLSM along with the role and benefits of CIDR in today's networks. Next, you will be introduced to the role of classless routing protocols. Classless routing protocols RIPv2, EIGRP, and OSPF are examined in later chapters.

Chapter 7 RIPv2 - Chapter 7 examines the next routing protocol presented in this course, RIPv2. RIPv2 is a classless, distance vector routing protocol. You will see how RIPv2 demonstrates the advantages and operations of a classless routing protocol. The chapter begins with a discussion of the limitations of the classful routing protocol, RIPv1. Then RIPv2 is introduced, to show how a classless routing protocol can be used to overcome these limitations. In this chapter, you will also learn the commands necessary to configure and verify RIPv2.

Chapter 8 The Routing Table: A Closer Look – Chapter 8 examines Cisco's IPv4 routing table in detail. The chapter begins with a discussion of the structure of the routing table. While examining the routing table, you will learn about the lookup process, how the routing table process determines the best match with a packet's destination IP address, and how to enter a route in the routing table. The chapter concludes with a discussion about the differences between classful and classless routing behaviors.

Chapter 9 EIGRP – Chapter 9 focuses on Cisco EIGRP (Enhanced Interior Gateway Routing Protocol). EIGRP is a classless, enhanced distance vector routing protocol. You will examine the advantages and operations of EIGRP's DUAL (Diffusing Update Algorithm). Then you will learn about the configuration of EIGRP, including verification and troubleshooting commands.

Chapter 10 Link-State Routing Protocols – Chapter 10 examines link-state routing protocol concepts. You will be introduced to link-state terminology and the link-state routing process. The chapter discusses the benefits and advantages of a link-state routing protocol compared to a distance vector routing protocol. You will then examine the Shortest Path First (SPF) algorithm and how it is used to build a topology map of the network. The link-state routing protocol OSPF is discussed in the following chapter.

Chapter 11 OSPF – The final chapter in this course is an examination of the classless, link-state routing protocol OSPF (Open Shortest Path First). In this chapter, you will examine OSPF operations and configuration, including verification and troubleshooting commands. By the end of this course, you should feel confident in your knowledge of routing and routing protocols. With continued study and practice, you will be able to put your new skills to work.

CHAPTER 3

Introduction to Dynamic Routing Protocols

Chapter Introduction

Refer to **Figure** in online course

The data networks that we use in our everyday lives to learn, play, and work range from small, local networks to large, global internetworks. At home, you may have a router and two or more computers. At work, your organization may have multiple routers and switches servicing the data communication needs of hundreds or even thousands of PCs.

In the previous chapters you discovered how routers are used in packet forwarding and that routers learn about remote networks using both static routes and dynamic routing protocols. You also know how routes to remote networks can be configured manually using static routes.

This chapter introduces dynamic routing protocols, including how different routing protocols are classified, what metrics they use to determine best path, and the benefits of using a dynamic routing protocol.

Dynamic routing protocols are usually used in larger networks to ease the administrative and operational overhead of using only static routes. Typically, a network uses a combination of both a dynamic routing protocol and static routes. In most networks, a single dynamic routing protocol is used, however there are cases where different parts of the network may use different routing protocols.

Since the early 1980's, several different dynamic routing protocols have emerged. In this chapter we will begin to discuss some of the characteristics and differences in these routing protocols, however this will become more evident in later chapters when we discuss several of these routing protocols in detail.

Although many networks will only use a single routing protocol or use only static routes, it is important for a network professional to understand the concepts and operations of all the different routing protocols. A network professional must be able to make an informed decision regarding when to use a dynamic routing protocol and which routing protocol is the best choice for a particular environment.

3.1 Introduction and Advantages

3.1.1 Perspective and Background

Refer to **Figure** in online course

The Evolution of Dynamic Routing Protocols

Dynamic routing protocols have been used in networks since the early 1980s. The first version of RIP was released in 1982, but some of the basic algorithms within the protocol were used on the ARPANET as early as 1969.

As networks have evolved and become more complex, new routing protocols have emerged. The figure shows the classification of routing protocols.

One of the earliest routing protocols was ***Routing Information Protocol (RIP)***. RIP has evolved into a newer version RIPv2. However, the newer version of RIP still does not ***scale*** to larger net-

work implementations. To address the needs of larger networks, two advanced routing protocols were developed: ***Open Shortest Path First (OSPF)*** and Intermediate System-to-Intermediate System (IS-IS). Cisco developed Interior Gateway Routing Protocol (IGRP) and ***Enhanced IGRP (EIGRP)***, which also scales well in larger network implementations.

Additionally, there was the need to interconnect different internetworks and provide routing among them. ***Border Gateway Routing (BGP)*** protocol is now used between ISPs as well as between ISPs and their larger private clients to exchange routing information.

With the advent of numerous consumer devices using IP, the IPv4 addressing space is nearly exhausted. Thus IPv6 has emerged. To support the communication based on IPv6, newer versions of the IP routing protocols have been developed (see the IPv6 row in the table).

Note: This chapter presents an overview of the different dynamic routing protocols. More details about RIP, EIGRP, and OSPF routing protocols will be discussed in later chapters. The IS-IS and BGP routing protocols are explained in the CCNP curriculum. IGRP is the predecessor to EIGRP and is now obsolete.

Refer to **Figure** in online course

The Role of Dynamic Routing Protocol

What exactly are dynamic routing protocols? Routing protocols are used to facilitate the exchange of routing information between routers. Routing protocols allow routers to dynamically share information about remote networks and automatically add this information to their own routing tables. This is shown in the animation.

Routing protocols determine the best path to each network which is then added to the routing table. One of the primary benefits to using a dynamic routing protocol is that routers exchange routing information whenever there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths when there is a link failure to a current network.

Compared to static routing, dynamic routing protocols require less administrative overhead. However, the expense of using dynamic routing protocols is dedicating part of a router's resources for protocol operation including CPU time and network link bandwidth. Despite the benefits of dynamic routing, static routing still has its place. There are times when static routing is more appropriate and other times when dynamic routing is the better choice. More often than not, you will find a combination of both types of routing in any network that has a moderate level of complexity. We will discuss the advantages and disadvantages of static and dynamic routing later in this chapter.

3.1.2 Network discovery and routing table maintenance

Refer to **Figure** in online course

The Purpose of Dynamic Routing Protocols

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of a routing protocol includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

What are the components of a routing protocol?

- ***Data structures -*** Some routing protocols use tables and/or databases for its operations. This information is kept in RAM.
- ***Algorithm*** - An algorithm is a finite list of steps used in accomplishing a task. Routing protocols use algorithms for facilitating routing information and for best path determination.
- ***Routing protocol messages -*** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.

Dynamic Routing Protocol Operation

All routing protocols have the same purpose - to learn about remote networks and to quickly adapt whenever there is a change in the topology. The method that a routing protocol uses to accomplish this depends upon the algorithm it uses and the operational characteristics of that protocol. The operations of a dynamic routing protocol vary depending upon the type of routing protocol and the routing protocol itself. In general, the operations of a dynamic routing protocol can be described as follows:

- The router sends and receives routing messages on its interfaces.
- The router shares routing messages and routing information with other routers that are using the same routing protocol.
- Routers exchange routing information to learn about remote networks.
- When a router detects a topology change the routing protocol can advertise this change to other routers.

Play the animation to see dynamic routing protocols in operation.

Note: Understanding dynamic routing protocol operation and concepts and using them in real networks requires a solid knowledge of IP addressing and subnetting. Three subnetting scenarios are available at the end of this chapter for your practice.

3.1.3 Advantages

Refer to **Figure** in online course

Static Routing Usage

Before identifying the benefits of dynamic routing protocols, we need to consider the reasons why we would use static routing. Dynamic routing certainly has several advantages over static routing. However, static routing is still used in networks today. In fact, networks typically use a combination of both static and dynamic routing.

Static routing has several primary uses, including:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from stub networks (see Chapter 2).
- Use of a single default route, used to represent a path to any network that does not have a more specific match with another route in the routing table.

Static Routing Advantages and Disadvantages

In the table dynamic and static routing features are directly compared. From this comparison, we can list the advantages of each routing method. The advantages of one method are the disadvantages of the other.

Static routing advantages:

- Minimal CPU processing.
- Easier for administrator to understand.
- Easy to configure.

Static routing disadvantages:

- Configuration and maintenance is time-consuming.
- Configuration is error-prone, especially in large networks.
- Administrator intervention is required to maintain changing route information.
- Does not scale well with growing networks; maintenance becomes cumbersome.
- Requires complete knowledge of the whole network for proper implementation.

Dynamic Routing Advantages and Disadvantages

Dynamic routing advantages:

- Administrator has less work maintaining the configuration when adding or deleting networks.
- Protocols automatically react to the topology changes.
- Configuration is less error-prone.
- More scalable, growing the network usually does not present a problem.

Dynamic routing disadvantages:

- Router resources are used (CPU cycles, memory and link bandwidth).
- More administrator knowledge is required for configuration, verification, and troubleshooting.

3.2 Classifying Dynamic Routing Protocols

3.2.1 Overview

Refer to **Figure** in online course

Dynamic Routing Protocols Classification

Routing protocols can be classified into different groups according to their characteristics. The most commonly used routing protocols are:

- ***RIP -*** A distance ***vector*** interior routing protocol
- ***IGRP -*** The ***distance vector*** interior routing developed by Cisco (deprecated from 12.2 IOS and later)
- ***OSPF -*** A link-state interior routing protocol
- ***IS-IS -*** A link-state interior routing protocol
- ***EIGRP -*** The advanced distance vector interior routing protocol developed by Cisco
- ***BGP -*** A path vector exterior routing protocol

Note: IS-IS and BGP are beyond the scope of this course and are covered in the CCNP curriculum.

The classification criteria are explained later in this chapter.

Drag and drop each protocol onto the correct category in the figure.

3.2.2 IGP and EGP

Refer to **Figure** in online course

An autonomous system (AS) - otherwise known as a routing ***domain*** - is a collection of routers under a common administration. Typical examples are a company's internal network and an Internet service provider's network. Because the Internet is based on the autonomous system concept, two types of routing protocols are required: interior and exterior routing protocols. These protocols are:

- ***Interior Gateway Protocols*** (IGP) **are used for intra-autonomous system routing - routing inside an autonomous system.**
- **Exterior Gateway Protocols (EGP)** are used for inter-autonomous system routing - routing between autonomous systems.

The figure is a simplified view of the difference between IGPs and EGPs. The autonomous system concept will be explained in more detail later in the chapter.

Characteristics of IGP and EGP Routing Protocols

IGPs are used for routing within a routing domain, those networks within the control of a single organization. An autonomous system is commonly comprised of many individual networks belonging to companies, schools, and other institutions. An IGP is used to route within the autonomous system, and also used to route within the individual networks themselves. For example, CENIC operates an autonomous system comprised of California schools, colleges and universities. CENIC uses an IGP to route within its autonomous system in order to interconnect all of these institutions. Each of the educational institutions also uses an IGP of their own choosing to route within its own individual network. The IGP used by each entity provides best path determination within its own routing domains, just as the IGP used by CENIC provides best path routes within the autonomous system itself. IGPs for IP include RIP, IGRP, EIGRP, OSPF, and IS-IS.

Routing protocols, and more specifically the algorithm used by that routing protocol, use a metric to determine the best path to a network. The metric used by the routing protocol RIP is hop count, which is the number of routers that a packet must traverse in reaching another network. OSPF uses bandwidth to determine the shortest path.

EGPs on the other hand, are designed for use between different autonomous systems that are under the control of different administrations. BGP is the only currently-viable EGP and is the routing protocol used by the Internet. BGP is a ***path vector protocol*** that can use many different attributes to measure routes. At the ISP level, there are often more important issues than just choosing the fastest path. BGP is typically used between ISPs and sometimes between a company and an ISP. BGP is not part of this course or CCNA; it is covered in CCNP.

Refer to **Packet Tracer Activity** for this chapter

In this activity, the network has already been configured within the autonomous systems. You will configure a default route from AS2 and AS3 (two different companies) to the ISP (AS1) to simulate the Exterior Gateway Routing that would take place from both companies to their ISP. Then you will configure a static route from the ISP (AS1) to AS2 and AS3 to simulate the Exterior Gateway Routing that would take place from the ISP to its 2 customers AS2 and AS3. View the routing table before and after both static routes and default routes are added to observe how the routing table has changed.

3.2.3 Distance Vector and Link State

Refer to **Figure** in online course

Interior Gateway Protocols (IGPs) can be classified as two types:

- Distance vector routing protocols
- ***Link-state*** routing protocols

Distance Vector Routing Protocol Operation

Distance vector means that routes are advertised as vectors of distance and direction. Distance is defined in terms of a metric such as hop count and direction is simply the next-hop router or exit interface. Distance vector protocols typically use the Bellman-Ford algorithm for the best path route determination.

Some distance vector protocols periodically send complete routing tables to all connected neighbors. In large networks, these routing updates can become enormous, causing significant traffic on the links.

Play the animation to see the operation of distance vector routing protocols.

Although the Bellman-Ford algorithm eventually accumulates enough knowledge to maintain a database of reachable networks, the algorithm does not allow a router to know the exact topology of an internetwork. The router only knows the routing information received from its neighbors.

Distance vector protocols use routers as sign posts along the path to the final destination. The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there. Distance vector routing protocols do not have an actual map of the network topology.

Distance vector protocols work best in situations where:

- The network is simple and flat and does not require a special hierarchical design.
- The administrators do not have enough knowledge to configure and troubleshoot link-state protocols.
- Specific types of networks, such as hub-and-spoke networks, are being implemented.
- Worst-case ***convergence*** times in a network are not a concern.

Distance vector routing protocol functions and operations will be explained in the next chapter. You will also learn about the operations and configuration of the distance vector routing protocols RIP and EIGRP.

Refer to **Figure** in online course

Link-state Protocol Operation

In contrast to distance vector routing protocol operation, a router configured with a ***link-state routing protocol*** can create a "complete view" or topology of the network by gathering information from all of the other routers. To continue our analogy of sign posts, using a link-state routing protocol is like having a complete map of the network topology. The sign posts along the way from source to destination are not necessary, because all link-state routers are using an identical "map" of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.

Play the animation.

With some distance vector routing protocols, routers send periodic updates of their routing information to their neighbors. Link-state routing protocols do not use periodic updates. After the network has ***converged***, a link-state update only sent when there is a change in the topology. For example, the link-state update in the animation is not sent until the 172.16.3.0 network goes down.

Link-state protocols work best in situations where:

- The network design is hierarchical, usually occurring in large networks.
- The administrators have a good knowledge of the implemented link-state routing protocol.
- Fast convergence of the network is crucial.

Link-state routing protocol functions and operations will be explained in later chapters. You will also learn about the operations and configuration of the link-state routing protocol OSPF.

3.2.4 Classful and Classless

Refer to **Figure** in online course

Classful Routing Protocols

Classful routing protocols do not send subnet mask information in routing updates. The first routing protocols such as RIP, were classful. This was at a time when network addresses were allocated based on classes, class A, B, or C. A routing protocol did not need to include the subnet mask in the routing update because the network mask could be determined based on the first octet of the network address.

Classful routing protocols can still be used in some of today's networks, but because they do not include the subnet mask they cannot be used in all situations. Classful routing protocols cannot be used when a network is subnetted using more than one subnet mask, in other words ***classful routing protocols*** do not support variable length subnet masks (VLSM).

There are other limitations to classful routing protocols including their inability to support ***discontiguous*** networks. Classful routing protocols, discontiguous networks and VLSM will all be discussed in later chapters.

Classful routing protocols include RIPv1 and IGRP.

Classless Routing Protocols

Classless routing protocols include the subnet mask with the network address in routing updates. Today's networks are no longer allocated based on classes and the subnet mask cannot be determined by the value of the first octet. Classless routing protocols are required in most networks today because of their support for VLSM, discontiguous networks and other features which will be discussed in later chapters.

In the figure, notice that the classless version of the network is using both /30 and /27 subnet masks in the same topology. Also notice that this topology is using a discontiguous design.

Classless routing protocols are RIPv2, EIGRP, OSPF, IS-IS, BGP.

3.2.5 Convergence

Refer to **Figure** in online course

What is Convergence?

Convergence is when all routers' routing tables are at a state of consistency. The network has converged when all routers have complete and accurate information about the network. Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables. A network is not completely operable until the network has converged; therefore, most networks require short convergence times.

Convergence is both collaborative and independent. The routers share information with each other but must independently calculate the impacts of the topology change on their own routes. Because they develop an agreement with the new topology independently, they are said to converge on this consensus.

Refer to **Packet Tracer Activity** for this chapter

Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. Routing protocols can be rated based on the speed to convergence; the faster the convergence, the better the routing protocol. Generally, RIP and IGRP are slow to converge, whereas EIGRP and OSPF are faster to converge.

In this activity, the network has already been configured with 2 routers, 2 switches and 2 hosts. A new LAN will be added and you will watch the network converge.

3.3 Metrics

3.3.1 Purpose of a Metric

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate between the available paths. For this purpose a **metric** is used. A metric is a value used by routing protocols to assign costs to reach remote networks. The metric is used to determine which path is most preferable when there are multiple paths to the same remote network.

Refer to **Figure** in online course

Each routing protocol uses its own metric. For example, RIP uses hop count, EIGRP uses a combination of bandwidth and delay, and Cisco's implementation of OSPF uses bandwidth. Hop count is the easiest metric to envision. The hop count refers to the number of routers a packet must cross to reach the destination network. For R3 in the figure, network 172.16.3.0 is two hops, or two routers away.

Note: The metrics for a particular routing protocol and how they are calculated will be discussed in the chapter for that routing protocol.

3.3.2 Metrics and Routing Protocols

The Metric Parameters

Different routing protocols use different metrics. The metric used by one routing protocol is not comparable to the metric used by another routing protocol. Two different routing protocols might choose different paths to the same destination due to using different metrics.

Play the animation.

Refer to **Figure** in online course

RIP would choose the path with the least amount of hops, whereas OSPF would choose the path with the highest bandwidth.

Metrics used in IP routing protocols include:

- ***Hop count -*** A simple metric that counts the number of routers a packet must traverse
- ***Bandwidth -*** Influences path selection by preferring the path with the highest bandwidth
- ***Load -*** Considers the traffic utilization of a certain link
- ***Delay -*** Considers the time a packet takes to traverse a path
- ***Reliability -*** Assesses the probability of a link failure, calculated from the interface error count or previous link failures
- ***Cost -*** A value determined either by the IOS or by the network administrator to indicate preference for a route. Cost can represent a metric, a combination of metrics or a policy.

Note: At this point, it is not important to completely understand these metrics; they will be explained in later chapters.

Refer to **Figure** in online course

The Metric Field in the Routing Table

The metric for each routing protocol is:

- ***RIP:*** Hop count - Best path is chosen by the route with the lowest hop count.
- ***IGRP and EIGRP:*** Bandwidth, Delay, Reliability, and Load - Best path is chosen by the route with the smallest composite metric value calculated from these multiple parameters. By default, only bandwidth and delay are used.
- ***IS-IS and OSPF:*** Cost - Best path is chosen by the route with the lowest cost. . Cisco's implementation of OSPF uses bandwidth. IS-IS is discussed in CCNP.

Routing protocols determine best path based on the route with the lowest metric.

Refer to the example in the figure The routers are using the RIP routing protocol. The metric associated with a certain route can be best viewed using the **show ip route** command. The metric value is the second value in the brackets for a routing table entry. In the figure, R2 has a route to the 192.168.8.0/24 network that is 2 hops away.

```
R 192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/0/1
```

Note: More detailed information about specific routing protocol metrics and how to calculate them will be available in the later chapters describing the individual routing protocols.

3.3.3 Load Balancing

Refer to **Figure** in online course

We have discussed that individual routing protocols use metrics to determine the best route to reach remote networks. But what happens when two or more routes to the same destination have identical metric values? How will the router decide which path to use for packet forwarding? In this case, the router does not choose only one route. **Instead, the router "load balances" between these equal cost paths**. The packets are forwarded using all equal-cost paths.

To see whether load balancing is in effect, check the routing table. **Load balancing is in effect if two or more routes are associated with the same destination.**

Note: Load balancing can be done either per packet or per destination. How a router actually load balances packets between the equal-cost paths is governed by the switching process. The switching process will be discussed in greater detail in a later chapter.

Play the animation.

R2 load balances traffic to PC5 over two equal cost paths.

The **show ip route** command reveals that the destination network 192.168.6.0 is available through 192.168.2.1 (Serial 0/0/0) and 192.168.4.1 (Serial 0/0/1).

```
R 192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
 [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
```

All the routing protocols discussed in this course are capable of automatically load balancing traffic for up to four equal-cost routes by default. EIGRP is also capable of load balancing across unequal-cost paths. This feature of EIGRP is discussed in the CCNP.

3.4 Administrative Distances

3.4.1 Purpose of Administrative Distance

Refer to **Figure** in online course

Multiple Routing Sources

We know that routers learn about adjacent networks that are directly connected and about remote networks by using static routes and dynamic routing protocols. In fact, a router might learn of a

route to the same network from more than one source. For example, a static route might have been configured for the same network/subnet mask that was learned dynamically by a dynamic routing protocol, such as RIP. The router must choose which route to install.

Note: You might be wondering about equal cost paths. Multiple routes to the same network can only be installed when they come from the same routing source. For example, for equal cost routes to be installed they both must be static routes or they both must be RIP routes.

Although less common, more than one dynamic routing protocol can be deployed in the same network. In some situations it may be necessary to route the same network address using multiple routing protocols such as RIP and OSPF. Because different routing protocols use different metrics, RIP uses hop count and OSPF uses bandwidth, it is not possible to compare metrics to determine the best path.

So, how does a router determine which route to install in the routing table when it has learned about the same network from more than one routing source?

The Purpose of Administrative Distance

Administrative distance (***AD***) defines the preference of a routing source. Each routing source - including specific routing protocols, static routes, and even directly connected networks - is prioritized in order of most- to least-preferable using an administrative distance value. Cisco routers use the AD feature to select the best path when it learns about the same destination network from two or more different routing sources.

Administrative distance is an integer value from 0 to 255. The lower the value the more preferred the route source. An administrative distance of 0 is the most preferred. Only a directly connected network has an administrative distance of 0, which cannot be changed.

It is possible to modify the administrative distance for static routes and dynamic routing protocols. This is discussed in CCNP.

An administrative distance of 255 means the router will not believe the source of that route and it will not be installed in the routing table.

Note: The term trustworthiness is commonly used when defining administrative distance. The lower the administrative distance value the more trustworthy the route.

Refer to **Figure** in online course

Click `show ip route` in the figure.

The AD value is the first value in the brackets for a routing table entry. Notice that R2 has a route to the 192.168.6.0/24 network with an AD value of 90.

```
D 192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
```

R2 is running both RIP and EIGRP routing protocols. (Remember: it is not common for routers to run multiple dynamic routing protocols, but is used here to demonstrate how administrative distance works.) R2 has learned of the 192.168.6.0/24 route from R1 through EIGRP updates and from R3 through RIP updates. RIP has an administrative distance of 120, but EIGRP has a lower administrative distance of 90. So, R2 adds the route learned using EIGRP to the routing table and forwards all packets for the 192.168.6.0/24 network to router R1.

Click `show ip rip database` in the figure.

What happens if the link to R1 becomes unavailable? Then R2 would not have a route to 192.168.6.0. Actually, R2 still has the RIP route information for 192.168.6.0 stored in the RIP database. This can be verified with the **`show ip rip database`** command. This command shows all RIP routes learned by R2, whether or not the RIP route is installed in the routing table.

3.4.2 Dynamic Routing Protocols

Refer to **Figure** in online course

Click `show ip route` in the figure.

You already know that you can verify these AD values with the **`show ip route`** command.

Click `show ip protocols` in the figure.

The AD value can also be verified with the **`show ip protocols`** command. This command displays all pertinent information about routing protocols operating on the router. We will look at the **`show ip protocols`** command in detail many times during the rest of the course. However, for now notice the highlighted output: R2 has two routing protocols listed and the AD value is called **Distance**.

Click AD Table in the figure.

Notice the different administrative distance values for various routing protocols.

3.4.3 Static Routes

Refer to **Figure** in online course

As you know from Chapter 2, static routes are entered by an administrator who wants to manually configure the best path to the destination. For that reason, static routes have a default AD value of 1. This means that after directly connected networks, which have a default AD value of 0, static routes are the most preferred route source.

There are situations when an administrator will configure a static route to the same destination that is learned using a dynamic routing protocol, but using a different path. The static route will be configured with an AD greater than that of the routing protocol. If there is a link failure in the path used by the dynamic routing protocol, the route entered by the routing protocol is removed from the routing table. The static route will then become the only source and will automatically be added to the routing table. This is known as a floating static route and is discussed in CCNP.

A static route using either a next-hop IP address or an exit interface has a default AD value of 1. However, the AD value is not listed in **`show ip route`** when you configure a static route with the exit interface specified. When a static route is configured with an exit interface, the output shows the network as directly connected via that interface.

Click `show ip route` in the figure.

The static route to 172.16.3.0 is listed as **directly connected**. However, there is no information on what the AD value is. It is a common misconception to assume that the AD value of this route must be 0 because it states "directly connected." However, that is a false assumption. The default AD of any static route, including those configured with an exit interface is 1. Remember, only a directly connected network can have an AD of 0. This can be verified by extending the **`show ip route`** command with the **`[route]`** option. Specifying the **`[route]`** reveals detailed information about the route, including its distance, or AD value.

Click `show ip route 172.16.3.0` in the figure.

The command **`show ip route 172.16.3.0`** reveals that, in fact, the administrative distance is 1.

3.4.4 Directly Connected Networks

Refer to **Figure** in online course

Directly connected networks appear in the routing table as soon as the IP address on the interface is configured and the interface is enabled and operational. The AD value of directly connected networks is 0, meaning that this is the most preferred routing source. There is no better route for a

router than having one of its interfaces directly connected to that network. For that reason, the administrative distance of a directly connected network cannot be changed and no other route source can have an administrative distance of 0.

Click `show ip route` in the figure.

The output of the **`show ip route`** command displays the directly connected networks with no information about the AD value. The output is similar to the output for static routes that point to an exit interface. The only difference is the letter **C** at the beginning of the entry, which indicates that this is a directly connected network.

To see the AD value of a directly connected network, use the **`[route]`** option.

Click `show ip route 172.16.1.0` in the figure.

The **`show ip route 172.16.1.0`** command reveals that the distance is 0 for that directly connected route.

Refer to **Packet Tracer Activity** for this chapter

In this activity, you will use version of the **`show ip route`** command to see details of routing table entries.

3.5 Routing Protocols and Subnetting Activities

3.5.1 Identifying Elements of the Routing Table

Refer to **Figure** in online course

The purpose of this exercise is to practice how to correctly identify the route source, administrative distance, and metric for a given route based on output from the **`show ip route`** command.

The output is not common for most routing tables. Running more than one routing protocol on the same router is rare. Running three, as shown here, is more of an academic exercise and has value in that it will help you learn to interpret the routing table output.

Drag and drop the appropriate responses to the corresponding space in the table.

- Use the information from the Show IP Route as reference.
- Not all answers are used.
- Some answers are used more than once.

3.5.2 Subnetting Scenario 1

Refer to **Lab Activity** for this chapter

In this activity, you have been given the network address 192.168.9.0/24 to subnet and provide the IP addressing for the network shown in the Topology Diagram.

Refer to **Packet Tracer Activity** for this chapter

Use this Packet Tracer Activity to implement your addressing scheme.

A summary of the instructions are provided within the activity. Use the Lab PDF for more details.

3.5.3 Subnetting Scenario 2

Refer to **Lab Activity** for this chapter

In this activity, you have been given the network address 172.16.0.0/16 to subnet and provide the IP addressing for the network shown in the Topology Diagram.

Refer to **Packet Tracer Activity** for this chapter

Use this Packet Tracer Activity to implement your addressing scheme.

A summary of the instructions are provided within the activity. Use the Lab PDF for more details.

3.5.4 Subnetting Scenario 3

Refer to **Lab Activity** for this chapter

Refer to **Packet Tracer Activity** for this chapter

In this activity, you have been given the network address 192.168.1.0/24 to subnet and provide the IP addressing for the network shown in the Topology Diagram.

Use this Packet Tracer Activity to implement your addressing scheme.

A summary of the instructions are provided within the activity. Use the Lab PDF for more details.

Summary and Review

Refer to **Figure** in online course

Summary

Dynamic routing protocols are used by routers to automatically learn about remote networks from other routers. In this chapter you were introduced to several different dynamic routing protocols.

You learned that routing protocols can be classified as either classful or classless, either distance vector, link-state, or path vector, and whether a routing protocol is an interior gateway protocol or an exterior gateway protocol. The differences in these classifications will become better understood as you learn more about these routing concepts and protocols in later chapters.

Routing protocols not only discover remote networks, but also have a procedure for maintaining accurate network information. When there is a change in the topology it is the function of the routing protocol to inform other routers about this change.

When there is a change in the network topology, some routing protocols can propagate that information throughout the routing domain faster than other routing protocols. The process of bringing all routing tables to a state of consistency is called convergence. Convergence is when all of the routers in the same routing domain or area have complete and accurate information about the network.

Metrics are used by routing protocols to determine the best path or shortest path to reach a destination network. Different routing protocols may use different metrics. Typically, a lower metric means a better path. Five hops to reach a network is better than 10 hops.

Routers sometimes learn about multiple routes to the same network from both static routes and dynamic routing protocols. When a router learns about a destination network from more than one routing source, Cisco routers use the administrative distance value to determine which source to use. Each dynamic routing protocol has a unique administrative value, along with static routes and directly connected networks. The lower the administrative value, the more preferred the route source. A directly connected network is always the preferred source, followed by static routes and then various dynamic routing protocols.

All of the classifications and concepts in this chapter will be discussed more thoroughly in the rest of the chapters of this course. At the end of this course you may wish to review this chapter to get a review and overview of this information.

Refer to **Figure** in online course

Refer to **Packet Tracer Activity** for this chapter

The Packet Tracer Skills Integration Challenge Activity for this chapter is very similar to the activity you completed at the end of Chapter 2. The scenario is slightly different, allowing you to better practice your skills. In this activity, you build a network from the ground up. Starting with an addressing space and network requirements, you must implement a network design that satisfies the specifications. Then you must implement an effective static routing configuration.

Packet Tracer Skills Integration Instructions (PDF)

Refer to **Figure** in online course

To Learn More

Border Gateway Protocol (BGP) is an inter-autonomous routing protocol - the routing protocol of the Internet. Although BGP is only briefly discussed in this course (it is discussed more fully in CCNP), you might find it interesting to view routing tables of some of the Internet core routers.

Route servers are used to view BGP routes on the Internet. Various web sites provide access to these route server, for example www.traceroute.org. When choosing a route server in a specific autonomous system, you will start a telnet session on that route server. This server is mirroring an Internet core router which is most often a Cisco router.

You can then use the **show ip route** command to view the actual routing table of an Internet router. Use the **show ip route** command followed by the public or global network address of your school, for example **show ip route 207.62.187.0**.

You will not be able to understand much of the information in this output, but these commands should give you a sense of the size of a routing table on a core Internet router.

Go to the online course to take the quiz.

Chapter Quiz

Take the chapter quiz to test your knowledge.

Your Chapter Notes