

ExamLabs

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

Study Guide

Exam 300-410

Contents at a Glance

Chapter 1 IPv4/IPv6 Addressing and Routing Review

Chapter 2 EIGRP

Chapter 3 Advanced EIGRP

Chapter 4 Troubleshooting EIGRP for IPv4

Chapter 5 EIGRPv6

Chapter 6 OSPF

Chapter 7 Advanced OSPF

Chapter 8 Troubleshooting OSPFv2

Chapter 9 OSPFv3

Chapter 10 Troubleshooting OSPFv3

Chapter 11 BGP

Chapter 12 Advanced BGP

Chapter 13 BGP Path Selection

Chapter 14 Troubleshooting BGP

Chapter 15 Route Maps and Conditional Forwarding

Chapter 16 Route Redistribution

Chapter 17 Troubleshooting Redistribution

Chapter 18 VRF, MPLS, and MPLS Layer 3 VPNs

Chapter 19 DMVPN Tunnels

Chapter 20 Securing DMVPN Tunnels

Chapter 21 Troubleshooting ACLs and Prefix Lists

Chapter 22 Infrastructure Security

Chapter 23 Device Management and Management Tools Troubleshooting

Glossary

Contents

Chapter 1 IPv4/IPv6 Addressing and Routing Review

- “Do I Know This Already?” Quiz

- Foundation Topics

- IPv4 Addressing

 - IPv4 Addressing Issues

 - Determining IP Addresses Within a Subnet

- DHCP for IPv4

 - Reviewing DHCP Operations

 - Potential DHCP Troubleshooting Issues

 - DHCP Troubleshooting Commands

- IPv6 Addressing

 - IPv6 Addressing Review

 - EUI-64*

- IPv6 SLAAC, Stateful DHCPv6, and Stateless DHCPv6

 - SLAAC

 - Stateful DHCPv6

 - Stateless DHCPv6

 - DHCPv6 Operation

 - DHCPv6 Relay Agents

- Packet-Forwarding Process

 - Reviewing the Layer 3 Packet-Forwarding Process

 - Troubleshooting the Packet-Forwarding Process

Routing Information Sources

Data Structures and the Routing Table

Sources of Routing Information

Static Routes

IPv4 Static Routes

IPv6 Static Routes

Trouble Tickets

IPv4 Addressing and Addressing Technologies Trouble Tickets

Trouble Ticket 1-1

Trouble Ticket 1-2

IPv6 Addressing Trouble Tickets

Trouble Ticket 1-3

Trouble Ticket 1-4

Static Routing Trouble Tickets

Trouble Ticket 1-5

Trouble Ticket 1-6

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Command Reference to Check Your Memory

Chapter 2 EIGRP

“Do I Know This Already?” Quiz

Foundation Topics

EIGRP Fundamentals

Autonomous Systems

EIGRP Terminology

Topology Table

EIGRP Neighbors

Inter-Router Communication

Forming EIGRP Neighbors

EIGRP Configuration Modes

Classic Configuration Mode

EIGRP Named Mode

EIGRP Network Statement

Sample Topology and Configuration

Confirming Interfaces

Verifying EIGRP Neighbor Adjacencies

Displaying Installed EIGRP Routes

Router ID

Passive Interfaces

Authentication

Keychain Configuration

Enabling Authentication on the Interface

Path Metric Calculation

Wide Metrics

Metric Backward Compatibility

Interface Delay Settings

Custom K Values

Load Balancing

References in This Chapter

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 3 Advanced EIGRP

“Do I Know This Already?” Quiz

Foundation Topics

Failure Detection and Timers

Convergence

Stuck in Active

Route Summarization

Interface-Specific Summarization

Summary Discard Routes

Summarization Metrics

Automatic Summarization

WAN Considerations

EIGRP Stub Router

Stub Site Functions

IP Bandwidth Percentage

Split Horizon

Route Manipulation

Route Filtering

Traffic Steering with EIGRP Offset Lists

References in This Chapter

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 4 Troubleshooting EIGRP for IPv4

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting EIGRP for IPv4 Neighbor Adjacencies

- Interface Is Down

- Mismatched Autonomous System Numbers

- Incorrect Network Statement

- Mismatched K Values

- Passive Interface

- Different Subnets

- Authentication

- ACLs

- Timers

Troubleshooting EIGRP for IPv4 Routes

- Bad or Missing network Command

- Better Source of Information

- Route Filtering

- Stub Configuration

- Interface Is Shut Down

- Split Horizon

Troubleshooting Miscellaneous EIGRP for IPv4 Issues

- Feasible Successors

- Discontiguous Networks and Autosummarization

Route Summarization

Load Balancing

EIGRP for IPv4 Trouble Tickets

Trouble Ticket 4-1

Trouble Ticket 4-2

Trouble Ticket 4-3

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 5 EIGRPv6

“Do I Know This Already?” Quiz

Foundation Topics

EIGRPv6 Fundamentals

EIGRPv6 Inter-Router Communication

EIGRPv6 Configuration

EIGRPv6 Classic Mode Configuration

EIGRPv6 Named Mode Configuration

EIGRPv6 Verification

IPv6 Route Summarization

Default Route Advertising

Route Filtering

Troubleshooting EIGRPv6 Neighbor Issues

Interface Is Down

Mismatched Autonomous System Numbers

Mismatched K Values

Passive Interfaces

Mismatched Authentication

Timers

Interface Not Participating in Routing Process

ACLs

Troubleshooting EIGRPv6 Routes

Interface Not Participating in the Routing Process

Better Source of Information

Route Filtering

Stub Configuration

Split Horizon

Troubleshooting Named EIGRP

EIGRPv6 and Named EIGRP Trouble Tickets

Trouble Ticket 5-1

Trouble Ticket 5-2

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 6 OSPF

“Do I Know This Already?” Quiz

Foundation Topics

OSPF Fundamentals

Areas

Inter-Router Communication

Router ID

OSPF Hello Packets

Neighbors

Requirements for Neighbor Adjacency

OSPF Configuration

OSPF Network Statement

Interface-Specific Configuration

Passive Interfaces

Sample Topology and Configuration

Confirmation of Interfaces

Verification of OSPF Neighbor Adjacencies

Viewing OSPF Installed Routes

External OSPF Routes

Default Route Advertisement

The Designated Router and Backup Designated Router

Designated Router Elections

DR and BDR Placement

OSPF Network Types

Broadcast

Nonbroadcast

Point-to-Point Networks

Point-to-Multipoint Networks

Loopback Networks

Failure Detection

Hello Timer

Dead Interval Timer

Verifying OSPF Timers

Authentication

References in This Chapter

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 7 Advanced OSPF

“Do I Know This Already?” Quiz

Foundation Topics

Link-State Advertisements

LSA Sequences

LSA Age and Flooding

LSA Types

LSA Type 1: Router Link

LSA Type 2: Network Link

LSA Type 3: Summary Link

LSA Type 5: External Routes

LSA Type 4: ASBR Summary

LSA Type 7: NSSA External Summary

LSA Type Summary

OSPF Stubby Areas

Stub Areas

Totally Stubby Areas

Not-So-Stubby Areas

Totally NSSAs

OSPF Path Selection

Link Costs

Intra-Area Routes

Interarea Routes

External Route Selection

E1 and N1 External Routes

E2 and N2 External Routes

Equal-Cost Multipathing

Summarization of Routes

Summarization Fundamentals

Interarea Summarization

Configuration of Interarea Summarization

External Summarization

Discontiguous Network

Virtual Links

References in This Chapter

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 8 Troubleshooting OSPFv2

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting OSPFv2 Neighbor Adjacencies

Interface Is Down

Interface Not Running the OSPF Process

Mismatched Timers

Mismatched Area Numbers

Mismatched Area Type

Different Subnets

Passive Interface

Mismatched Authentication Information

ACLs

MTU Mismatch

Duplicate Router IDs

Mismatched Network Types

Troubleshooting OSPFv2 Routes

Interface Not Running the OSPF Process

Better Source of Information

Route Filtering

Stub Area Configuration

Interface Is Shut Down

Wrong Designated Router Elected

Duplicate Router IDs

Troubleshooting Miscellaneous OSPFv2 Issues

Tracking OSPF Advertisements Through a Network

Route Summarization

Discontiguous Areas

Load Balancing

Default Route

OSPFv2 Trouble Tickets

Trouble Ticket 8-1

Trouble Ticket 8-2

Trouble Ticket 8-3

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 9 OSPFv3

“Do I Know This Already?” Quiz

Foundation Topics

OSPFv3 Fundamentals

OSPFv3 Link-State Advertisement

OSPFv3 Communication

OSPFv3 Configuration

OSPFv3 Verification

The Passive Interface

IPv6 Route Summarization

Network Type

OSPFv3 Authentication

OSPFv3 Link-Local Forwarding

OSPFv3 LSA Flooding Scope

References in This Chapter

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 10 Troubleshooting OSPFv3

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting OSPFv3 for IPv6

 OSPFv3 Troubleshooting Commands

OSPFv3 Trouble Tickets

 Trouble Ticket 10-1

 Trouble Ticket 10-2

Troubleshooting OSPFv3 Address Families

OSPFv3 AF Trouble Ticket

 Trouble Ticket 10-3

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 11 BGP

“Do I Know This Already?” Quiz

Foundation Topics

BGP Fundamentals

 Autonomous System Numbers (ASNs)

 BGP Sessions

 Path Attributes

 Loop Prevention

 Address Families

 Inter-Router Communication

BGP Messages

BGP Neighbor States

Basic BGP Configuration

- Verification of BGP Sessions

- Prefix Advertisement

- Receiving and Viewing Routes

Understanding BGP Session Types and Behaviors

- iBGP

 - iBGP Full Mesh Requirement*

 - Peering Using Loopback Addresses*

- eBGP

- eBGP and iBGP Topologies

- Next-Hop Manipulation

- iBGP Scalability Enhancements

 - Route Reflectors*

 - Confederations*

Multiprotocol BGP for IPv6

- IPv6 Configuration

- IPv6 Summarization

- IPv6 over IPv4

References in This Chapter

- Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Use the Command Reference to Check Your Memory

Chapter 12 Advanced BGP

- “Do I Know This Already?” Quiz

- Foundation Topics

Route Summarization

- Aggregate Addresses

- The Atomic Aggregate Attribute

- Route Aggregation with AS_SET

BGP Route Filtering and Manipulation

- Distribution List Filtering

- Prefix List Filtering

- AS_Path Filtering

 - Regular Expressions (Regex)*

 - AS_Path ACLs*

- Route Maps

- Clearing BGP Connections

BGP Communities

- Enabling BGP Community Support

- Well-Known Communities

 - The No_Advertise BGP Community*

 - The No_Export BGP Community*

 - The Local-AS (No_Export_SubConfed) BGP Community*

- Conditionally Matching BGP Communities

- Setting Private BGP Communities

Maximum Prefix

- Configuration Scalability

- IOS Peer Groups

- IOS Peer Templates

References in This Chapter

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 13 BGP Path Selection

“Do I Know This Already?” Quiz

Foundation Topics

Understanding BGP Path Selection

BGP Best Path

Weight

Local Preference

Phase I: Initial BGP Edge Route Processing

Phase II: BGP Edge Evaluation of Multiple Paths

Phase III: Final BGP Processing State

Locally Originated in the Network or Aggregate Advertisement

Accumulated Interior Gateway Protocol (AIGP)

Shortest AS_Path

Origin Type

Multi-Exit Discriminator

Missing MED Behavior

Always Compare MED

BGP Deterministic MED

eBGP over iBGP

Lowest IGP Metric

Prefer the Oldest EBGP Path

Router ID

Minimum Cluster List Length

Lowest Neighbor Address

BGP Equal-Cost Multipath

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 14 Troubleshooting BGP

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting BGP Neighbor Adjacencies

Interface Is Down

Layer 3 Connectivity Is Broken

Path to the Neighbor Is Through the Default Route

Neighbor Does Not Have a Route to the Local Router

Incorrect neighbor Statement

BGP Packets Sourced from the Wrong IP Address

ACLs

The TTL of the BGP Packet Expires

Mismatched Authentication

Misconfigured Peer Groups

Timers

Troubleshooting BGP Routes

Missing or Bad network mask Command

Next-Hop Router Not Reachable

BGP Split-Horizon Rule

Better Source of Information

Route Filtering

Troubleshooting BGP Path Selection

Understanding the Best-Path Decision-Making Process

Private Autonomous System Numbers

Using debug Commands

Troubleshooting BGP for IPv6

BGP Trouble Tickets

Trouble Ticket 14-1

Trouble Ticket 14-2

Trouble Ticket 14-3

MP-BGP Trouble Ticket

Trouble Ticket 14-4

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 15 Route Maps and Conditional Forwarding

“Do I Know This Already?” Quiz

Foundation Topics

Conditional Matching

Access Control Lists (ACLs)

Standard ACLs

Extended ACLs

Prefix Matching

Prefix Lists

IPv6 Prefix Lists

Route Maps

Conditional Matching

Multiple Conditional Match Conditions

Complex Matching

Optional Actions

Continue

Conditional Forwarding of Packets

PBR Configuration

Local PBR

Trouble Tickets

Trouble Ticket 15-1

Trouble Ticket 15-2

Trouble Ticket 15-3

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 16 Route Redistribution

“Do I Know This Already?” Quiz

Foundation Topics

Redistribution Overview

Redistribution Is Not Transitive

Sequential Protocol Redistribution

Routes Must Exist in the RIB

Seed Metrics

Protocol-Specific Configuration

Source-Specific Behaviors

Connected Networks

BGP

Destination-Specific Behaviors

EIGRP

EIGRP-to-EIGRP Redistribution

OSPF

OSPF-to-OSPF Redistribution

OSPF Forwarding Address

BGP

Reference in This Chapter

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 17 Troubleshooting Redistribution

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting Advanced Redistribution Issues

Troubleshooting Suboptimal Routing Caused by
Redistribution

Troubleshooting Routing Loops Caused by Redistribution

Troubleshooting IPv4 and IPv6 Redistribution

Route Redistribution Review

Troubleshooting Redistribution into EIGRP

Troubleshooting Redistribution into OSPF

Troubleshooting Redistribution into BGP

Troubleshooting Redistribution with Route Maps

Redistribution Trouble Tickets

Trouble Ticket 17-1

Trouble Ticket 17-2

Trouble Ticket 17-3

Trouble Ticket 17-4

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 18 VRF, MPLS, and MPLS Layer 3 VPNs

“Do I Know This Already?” Quiz

Foundation Topics

Implementing and Verifying VRF-Lite

VRF-Lite Overview

Creating and Verifying VRF Instances

An Introduction to MPLS Operations

MPLS LIB and LFIB

Label Switching Routers

Label-Switched Path

Labels

Label Distribution Protocol

Label Switching

Penultimate Hop Popping

An Introduction to MPLS Layer 3 VPNs

MPLS Layer 3 VPNs

MPLS Layer 3 VPNv4 Address

MPLS Layer 3 VPN Label Stack

Reference in This Chapter

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 19 DMVPN Tunnels

“Do I Know This Already?” Quiz

Foundation Topics

Generic Routing Encapsulation (GRE) Tunnels

GRE Tunnel Configuration

GRE Sample Configuration

Next Hop Resolution Protocol (NHRP)

Dynamic Multipoint VPN (DMVPN)

Phase 1: Spoke-to-Hub

Phase 2: Spoke-to-Spoke

Phase 3: Hierarchical Tree Spoke-to-Spoke

DMVPN Phase Comparison

DMVPN Configuration

DMVPN Hub Configuration

DMVPN Spoke Configuration for DMVPN Phase 1 (Point-to-Point)

Viewing DMVPN Tunnel Status
Viewing the NHRP Cache
DMVPN Configuration for Phase 3 DMVPN (Multipoint)
IP NHRP Authentication
Unique IP NHRP Registration
Spoke-to-Spoke Communication
Forming Spoke-to-Spoke Tunnels
NHRP Routing Table Manipulation
NHRP Routing Table Manipulation with Summarization
Problems with Overlay Networks
Recursive Routing Problems
Outbound Interface Selection
Front Door Virtual Routing and Forwarding (FVRF)
Configuring Front Door VRF (FVRF)
FVRF Static Routes
DMVPN Failure Detection and High Availability
DMVPN Hub Redundancy
IPv6 DMVPN Configuration
IPv6-over-IPv6 Sample Configuration
IPv6 DMVPN Verification
References in This Chapter
Exam Preparation Tasks
Review All Key Topics
Define Key Terms
Use the Command Reference to Check Your Memory

Chapter 20 Securing DMVPN Tunnels

“Do I Know This Already?” Quiz

Foundation Topics

Elements of Secure Transport

IPsec Fundamentals

Security Protocols

Authentication Header

Encapsulating Security Payload (ESP)

Key Management

Security Associations

ESP Modes

DMVPN Without IPsec

DMVPN with IPsec in Transport Mode

DMVPN with IPsec in Tunnel Mode

IPsec Tunnel Protection

Pre-Shared Key Authentication

IKEv2 Keyring

IKEv2 Profile

IPsec Transform Set

IPsec Profile

Encrypting the Tunnel Interface

IPsec Packet Replay Protection

Dead Peer Detection

NAT Keepalives

Complete IPsec DMVPN Configuration with Pre-Shared Authentication

Verification of Encryption on DMVPN Tunnels

[IKEv2 Protection](#)

[References in This Chapter](#)

[Exam Preparation Tasks](#)

[Review All Key Topics](#)

[Define Key Terms](#)

[Use the Command Reference to Check Your Memory](#)

Chapter 21 Troubleshooting ACLs and Prefix Lists

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Troubleshooting IPv4 ACLs](#)

[Reading an IPv4 ACL](#)

[Using an IPv4 ACL for Filtering](#)

[Using a Time-Based IPv4 ACL](#)

[Troubleshooting IPv6 ACLs](#)

[Reading an IPv6 ACL](#)

[Using an IPv6 ACL for Filtering](#)

[Troubleshooting Prefix Lists](#)

[Reading a Prefix List](#)

[Prefix List Processing](#)

[Trouble Tickets](#)

[Trouble Ticket 21-1: IPv4 ACL Trouble Ticket](#)

[Trouble Ticket 21-2: IPv6 ACL Trouble Ticket](#)

[Trouble Ticket 21-3: Prefix List Trouble Ticket](#)

[Exam Preparation Tasks](#)

[Review All Key Topics](#)

[Define Key Terms](#)

Use the Command Reference to Check Your Memory

Chapter 22 Infrastructure Security

“Do I Know This Already?” Quiz

Foundation Topics

Cisco IOS AAA Troubleshooting

Troubleshooting Unicast Reverse Path Forwarding (uRPF)

Troubleshooting Control Plane Policing (CoPP)

Creating ACLs to Identify the Traffic

Creating Class Maps to Define a Traffic Class

Creating Policy Maps to Define a Service Policy

Applying the Service Policy to the Control Plane

CoPP Summary

IPv6 First-Hop Security

Router Advertisement (RA) Guard

DHCPv6 Guard

Binding Table

IPv6 Neighbor Discovery Inspection/IPv6 Snooping

Source Guard

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 23 Device Management and Management Tools Troubleshooting

“Do I Know This Already?” Quiz

Foundation Topics

Device Management Troubleshooting

Console Access Troubleshooting

vtty Access Troubleshooting

Telnet

SSH

Password Encryption Levels

Remote Transfer Troubleshooting

TFTP

HTTP(S)

SCP

Management Tools Troubleshooting

Syslog Troubleshooting

SNMP Troubleshooting

Cisco IOS IP SLA Troubleshooting

Object Tracking Troubleshooting

NetFlow and Flexible NetFlow Troubleshooting

Bidirectional Forwarding Detection (BFD)

Cisco DNA Center Assurance

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory

Chapter 24 Final Preparation

Advice About the Exam Event

Think About Your Time Budget Versus Numbers of Questions

[A Suggested Time-Check Method](#)

[Miscellaneous Pre-Exam Suggestions](#)

[Exam-Day Advice](#)

[Reserve the Hour After the Exam in Case You Fail](#)

[Take Practice Exams](#)

[Advice on How to Answer Exam Questions](#)

[Assessing Whether You Are Ready to Pass \(and the Fallacy of Exam Scores\)](#)

[Study Suggestions After Failing to Pass](#)

[Other Study Tasks](#)

Chapter 1. IPv4/IPv6 Addressing and Routing Review

This chapter covers the following topics:

- **IPv4 Addressing:** This section provides a review of IPv4 addressing and covers issues you might face and how to troubleshoot them.
- **DHCP for IPv4:** This section reviews DHCP for IPv4 operations, explores potential DHCP issues, and examines the output of various DHCP **show** commands.
- **IPv6 Addressing:** This section provides a brief review of IPv6 addressing.
- **IPv6 SLAAC, Stateful DHCPv6, and Stateless DHCPv6:** This section explores how clients obtain IPv6 addressing information using SLAAC, stateful DHCPv6, and stateless DHCPv6.
- **Packet-Forwarding Process:** This section discusses the packet-forwarding process and the commands to verify the entries in the data structures that are used for this process. It also provides you with a collection of Cisco IOS Software commands that could prove useful when troubleshooting related issues.
- **Routing Information Sources:** This section explains which sources of routing information are the most believable and how the routing table interacts with various data structures to populate itself with the best information.
- **Static Routes:** This section reviews how to configure and verify IPv4 and IPv6 static routes.
- **Trouble Tickets:** This section provides a number of trouble tickets that demonstrate how a structured troubleshooting process is used to solve a reported problem.

IPv6 is currently being deployed, but that deployment is occurring at a slow pace. Most networks still rely on IPv4, and many new networks and network additions are being deployed with IPv4. Therefore, you still need the skills to successfully configure, verify, and troubleshoot IPv4 addressing. Therefore, this chapter provides a review of IPv4 addressing.

Typically, when deploying IPv4 addresses, Dynamic Host Configuration Protocol (DHCP) is used so that addresses can be dynamically assigned. However, with this dynamic process, issues may arise that prevent a device from successfully obtaining an IPv4 address from a DHCP server. Therefore, this chapter reviews how DHCP operates and how to identify the issues that may prevent a client from obtaining an IP address from a DHCP server.

Sooner or later, organizations will have to switch to IPv6. There is a whole lot more to IPv6 than just having a larger address space than IPv4. This chapter reminds you how IPv6-enabled devices determine whether a destination is local or remote and explores the various options for address assignment and what to look out for when troubleshooting.

Before you dive into the advanced routing topics such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP), you need to review the packet-delivery process (also known as the routing process). This is the process that a router goes through when a packet arrives at an ingress interface and needs to be packet switched to an egress interface. It does not matter whether the packet is an IPv4 or IPv6 packet. Either way, the router goes through the same steps to successfully take a packet from an ingress interface and packet switch it to the egress interface. You also need to review how a router populates the routing table with “the best” routes. What classifies those routes as the best? Is an EIGRP-learned route better than a static route? What about an OSPF-learned route or a BGP-learned route? How do they compare to the other sources of routing information? When multiple sources provide the same routing information, you need to be able to identify why the router made the decision it made.

Static routes are part of every network. However, because they are manually configured, they are prone to human error, which can produce suboptimal routing or routing loops; therefore, this chapter reviews IPv4 and IPv6 static routing configuration and verification.

Notice that this chapter is mostly a review of IPv4/IPv6 addressing, DHCP for IPv4/IPv6, the packet-forwarding process, administrative distance, and static routing that you learned in CCNA or ENCORE. I encourage you not to skip this chapter as it is a great place to warm up for what is to come in the rest of this book, which prepares you for the Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) exam.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. [Table 1-1](#) lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in [Appendix A](#), “Answers to the ‘Do I Know This Already?’ Quiz Questions.”

Table 1-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
IPv4 Addressing	1–3
DHCP for IPv4	4–6
IPv6 Addressing	7–8
IPv6 SLAAC, Stateful DHCPv6, and Stateless DHCPv6	9–12
Packet-Forwarding Process	13–15
Routing Information Sources	16–17
Static Routes	18–19

Caution

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What occurs when a PC with the IP address 10.1.1.27/28 needs to communicate with a PC that has IP address 10.1.1.18? (Choose two.)
 - a. It sends the frame to its default gateway.
 - b. It sends the frame directly to the destination PC.
 - c. It uses ARP to get the MAC address of the default gateway.
 - d. It uses ARP to get the MAC address of the destination PC.
2. What occurs when a PC with the IP address 10.1.1.27/29 needs to communicate with a PC that has IP address 10.1.1.18? (Choose two.)
 - a. It sends the frame to its default gateway.
 - b. It sends the frame directly to the destination PC.
 - c. It uses ARP to get the MAC address of the default gateway.
 - d. It uses ARP to get the MAC address of the destination PC.
3. Which command enables you to verify the IP address configured on a router's interface?
 - a. **ipconfig**
 - b. **show ip interface**
 - c. **arp -a**
 - d. **show ip arp**
4. What is the correct order of operations for the DHCP for IPv4 process?
 - a. Offer, Request, Ack, Discover
 - b. Discover, Request, Ack, Offer
 - c. Request, Offer, Discover, Ack
 - d. Discover, Offer, Request, Ack
5. Which command is needed on a router interface to forward DHCP Discover messages to a DHCP server on a different subnet?
 - a. **ip address dhcp**

- b. **ip helper-address**
 - c. **ip dhcp-forwarder**
 - d. **ip dhcp server**
6. Which command enables a router interface to obtain an IP address from a DHCP server?
- a. **ip dhcp client**
 - b. **ip dhcp server**
 - c. **ip address dhcp**
 - d. **ip helper-address**
7. What protocol is used with IPv6 to determine the MAC address of a device in the same local area network?
- a. Address Resolution Protocol
 - b. Inverse Address Resolution Protocol
 - c. Neighbor Discovery Protocol
 - d. Neighbor Solicitation
8. Which of the following are true when using EUI-64? (Choose two.)
- a. The interface MAC address is used unmodified.
 - b. The interface MAC address is used with FFFE added to the middle.
 - c. The seventh bit from the left in the MAC address is flipped.
 - d. The seventh bit from the right in the MAC address is flipped.
9. What command is used on a Cisco IOS router to enable SLAAC on an interface?
- a. **ipv6 address autoconfig**
 - b. **ipv6 address dhcp**
 - c. **ipv6 address *prefix* eui-64**
 - d. **ipv6 nd ra suppress**
10. Which of the following are requirements for stateless address autoconfiguration to function? (Choose three.)
- a. The prefix must be /64.
 - b. The router must be sending and not suppressing RA messages.
 - c. The router must be enabled for IPv6 unicast routing.
 - d. The router must be sending RS messages.

11. Which command is used to enable a router to inform clients that they need to get additional configuration information from a DHCPv6 server?
 - a. **ipv6 nd ra suppress**
 - b. **ipv6 dhcp relay destination**
 - c. **ipv6 address autoconfig**
 - d. **ipv6 nd other-config-flag**
12. What command enables you to configure a router interface as a DHCPv6 relay agent?
 - a. **ipv6 forwarder**
 - b. **ipv6 helper-address**
 - c. **ipv6 dhcp relay destination**
 - d. **ipv6 dhcp client**
13. Which two data structures reside at the router's data plane?
 - a. IP routing table
 - b. ARP cache
 - c. Forwarding Information Base
 - d. Adjacency table
14. Which command enables you to verify routes in the FIB?
 - a. **show ip route**
 - b. **show ip arp**
 - c. **show ip cef**
 - d. **show adjacency detail**
15. Which of the following populate a routing protocol's data structure, such as the EIGRP topology table? (Choose three.)
 - a. Updates from a neighbor
 - b. Redistributed routes
 - c. Interfaces enabled for the routing process
 - d. Static routes
16. Which of the following has the lowest default administrative distance?
 - a. OSPF
 - b. EIGRP (internal)
 - c. RIP

- d. eBGP
- 17.** What is the default administrative distance of an OSPF intra-area route?
- a. 90
 - b. 110
 - c. 115
 - d. 120
- 18.** How can you create a floating static route?
- a. Provide the static route with a metric higher than the preferred source of the route.
 - b. Provide the static route with a metric lower than the preferred source of the route.
 - c. Provide the static route with an AD higher than the preferred source of the route.
 - d. Provide the static route with an AD lower than the preferred source of the route.
- 19.** What occurs when you create an IPv4 static route with an Ethernet interface designated instead of a next-hop IP address?
- a. The router uses ARP to get the MAC address of the directly connected router's IP address.
 - b. The router forwards the packet with the destination MAC address FFFF:FFFF:FFFF.
 - c. The router uses ARP to get the MAC address of the IP address in the source of the packet.
 - d. The router uses ARP to get the MAC address of the IP address in the destination of the packet.

Foundation Topics

IPv4 Addressing

Just as your personal street address uniquely defines where you live, an IPv4 address uniquely defines where a device resides in a network. Your street

address is made of two parts—the street name and the number of your residence—and the combination of these is unique within your city/town. As a result, a pizza delivery person can bring your pizza to your house in 30 minutes, or it is free. If your house is addressed incorrectly, you may not get your pizza, and you do not want that to happen.

Similarly, with IPv4 addressing, if devices are addressed incorrectly, they may not receive the packets that are intended for them. Therefore, it is imperative that you have a solid understanding of IPv4 addressing and how to verify that devices are addressed correctly on a network. This section provides a review of IPv4 addressing and discusses issues you might face and how to troubleshoot them.

IPv4 Addressing Issues

An IPv4 address is made up of two parts: a network/subnet portion and a host portion. It is imperative that all devices in the same network/subnet share exactly the same network/subnet portion. If they are not the same, the PC could end up addressing the Layer 2 frame incorrectly and sending the packet in the wrong direction. [Figure 1-1](#) shows a sample subnet (10.1.1.0/26) with two PCs and their default gateway, R1.

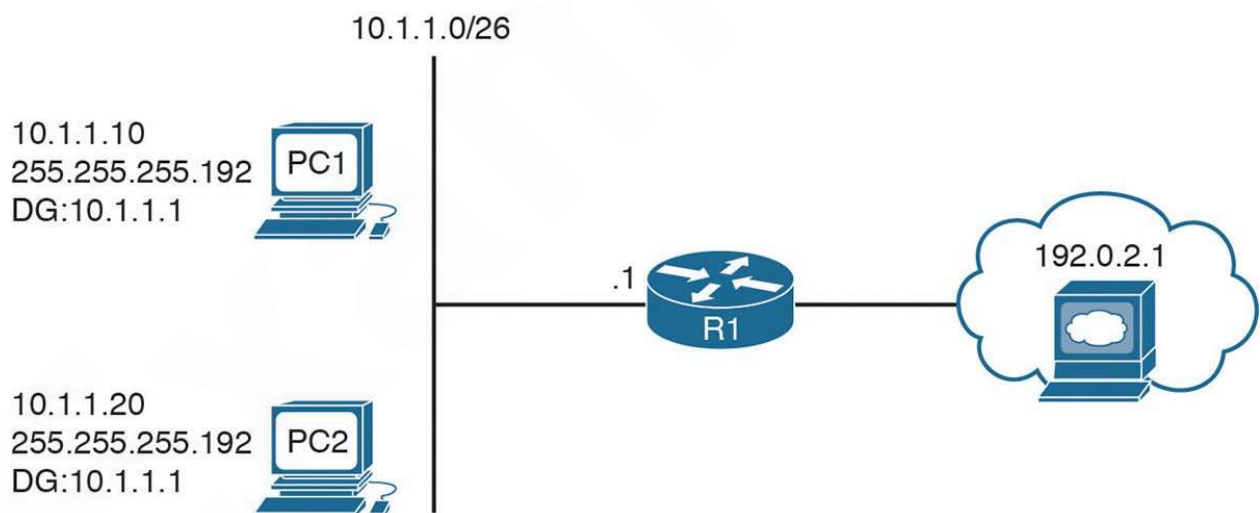


Figure 1-1 *Correct IPv4 Addressing Example*



When PC1 needs to communicate with PC2, it does a DNS lookup for the IP address of PC2. The IP address 10.1.1.20 is returned. Now PC1 needs to determine whether PC2 is located in the same subnet because this determines whether the frame has the MAC address of PC2 or the MAC address of the default gateway (DG). PC1 determines its network/subnet portion by comparing its IP address to its subnet mask in binary, as follows:

[Click here to view code image](#)

```
00001010.00000001.00000001.00001010 - PC1 IP address in binary
11111111.11111111.11111111.11000000 - PC1 subnet mask in binary
-----
00001010.00000001.00000001.00 - PC1 network/subnet ID
```

(The 1s in the subnet mask identify the network portion.)

Now PC1 compares exactly the same binary bits to those binary bits in PC2's address, as follows:

[Click here to view code image](#)

```
00001010.00000001.00000001.00 - PC1 network/subnet ID
00001010.00000001.00000001.00010100 - PC2 IP address in binary
```

Because the binary bits are the same, PC1 concludes that PC2 is in the same network/subnet; therefore, it communicates directly with it and does not need to send the data to its default gateway. PC1 creates a frame with its own source MAC address and the MAC address of PC2 as the destination.

Consider what occurs when PC1 needs to communicate with the web server at 192.0.2.1. It does a DNS lookup for the IP address of the web server. The IP address 192.0.2.1 is returned. Now PC1 needs to determine whether the web server is located in the same network/subnet. This determines whether the frame has the MAC address of the web server or the MAC address of the DG. PC1 determines its network/subnet portion by comparing its IP address to its subnet mask in binary, as follows:

[Click here to view code image](#)

```
00001010.00000001.00000001.00001010 - PC1 IP address in binary
11111111.11111111.11111111.11000000 - PC1 subnet mask in binary
```

00001010.00000001.00000001.00 - PC1 network/subnet ID

(The 1s in the subnet mask identify the network portion.)

Now PC1 compares exactly the same binary bits to those binary bits in the web server address, as follows:

[Click here to view code image](#)

```
00001010.00000001.00000001.00 - PC1 network/subnet ID
11000000.00000000.00000010.00000001 - web server IP address in
binary
```

PC1 concludes that the web server is in a different network/subnet because the bits are not the same; therefore, to communicate with the web server, it needs to send the data to its default gateway. PC1 creates a frame with its own source MAC address and the MAC address of R1 as the destination.

As you can see, accurate IP addressing is paramount for successful communication. Let's look at what happens if PC1 is configured with the wrong subnet mask (255.255.255.240), as shown in [Figure 1-2](#).

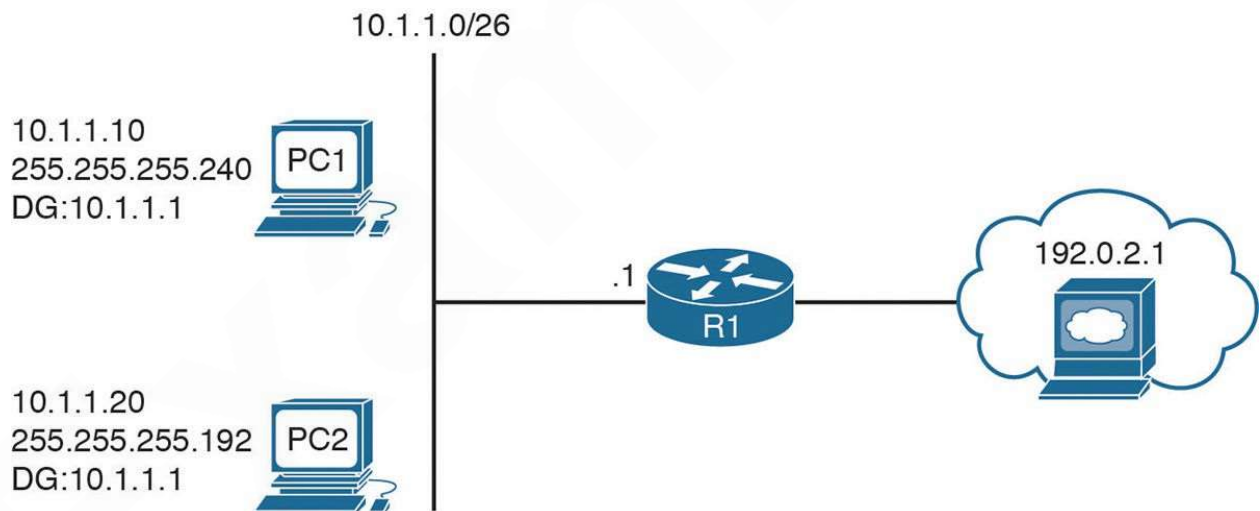


Figure 1-2 *Incorrect IPv4 Addressing Example*



PC1 determines its network/subnet portion by comparing its IP address to its

subnet mask in binary, as follows:

[Click here to view code image](#)

```
00001010.00000001.00000001.00001010 - PC1 IP address in binary
11111111.11111111.11111111.11110000 - PC1 subnet mask in binary
-----
00001010.00000001.00000001.0000 - PC1 network/subnet ID
```

Now PC1 compares exactly the same binary bits to those binary bits in PC2's address, as follows:

[Click here to view code image](#)

```
00001010.00000001.00000001.0000 - PC1 network/subnet ID
00001010.00000001.00000001.00010100 - PC2 IP address in binary
```

PC1 concludes that PC2 is not in the same network/subnet because the binary bits are not the same. Therefore, it cannot communicate directly with it and needs to send the frame to the router so that the router can route the packet to the subnet PC2 is in. However, the PCs are actually connected to the same subnet, and as a result, there is an IPv4 addressing and connectivity issue.

Not only does an *improper subnet mask* cause issues, but an *inappropriate IP address combined with the correct subnet mask* also causes issues. In addition, if the *default gateway is not configured correctly* on the PCs, packets are not forwarded to the correct device when packets need to be sent to a different subnet.

As a troubleshooter, you must recognize these issues and eliminate them as possible issues quickly. You verify the IP addressing information on a Windows PC by using the **ipconfig** command, as shown in [Example 1-1](#). On an IOS router or IOS switch, you verify IP addressing information by using the **show ip interface interface_type interface_number** command, as also shown in [Example 1-1](#).



Example 1-1 Verifying IP Addressing on a PC and on a Router

[Click here to view code image](#)

```
C:\>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter PC1:
```

```
Connection-specific DNS Suffix . :
```

```
IP Address. . . . .: 10.1.1.10
```

```
Subnet Mask . . . . .: 255.255.255.192
```

```
IP Address. . . . .: 2001:10::10
```

```
IP Address. . . . .: fe80::4107:2cfb:df25:5124%7
```

```
Default Gateway . . . . .: 10.1.1.1
```

```
R1# show ip interface gigabitEthernet 1/0
```

```
GigabitEthernet1/0 is up, line protocol is up
```

```
Internet address is 10.1.1.1/26
```

```
...output omitted...
```



Determining IP Addresses Within a Subnet

This section describes a quick way to determine all the IP addresses that will be in a particular subnet. Refer to [Figure 1-3](#) as you are exploring this method.

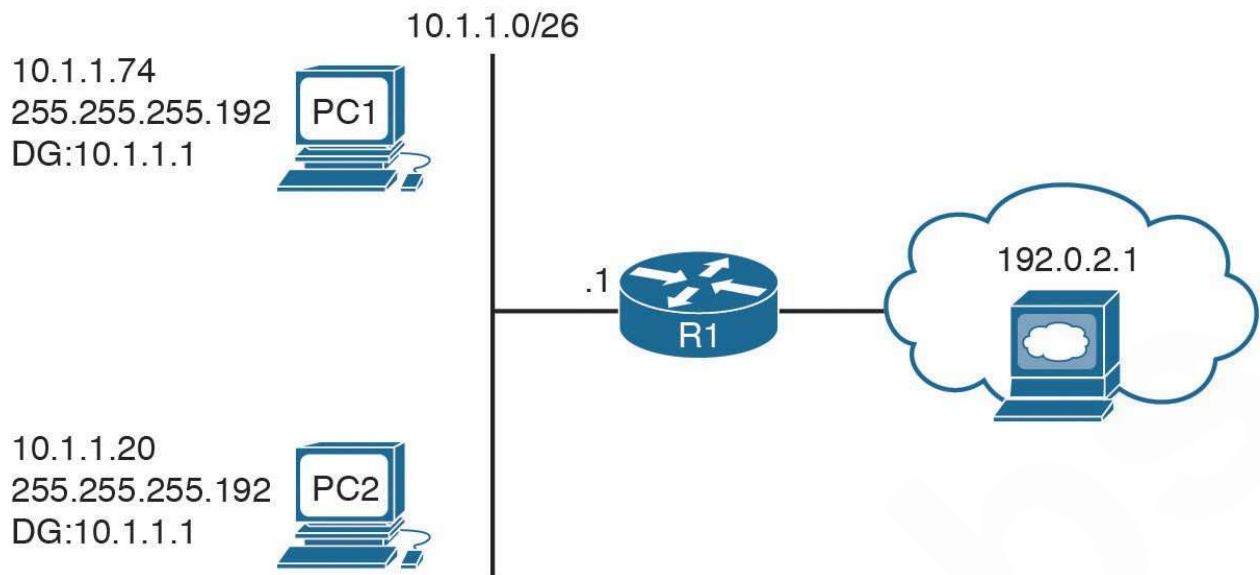


Figure 1-3 *Determining IP Addresses Within a Subnet*

In the subnet mask, find the most interesting octet. In binary, it's the octet with the last binary 1. In decimal, it's the last octet that is greater than 0. In this case, for 255.255.255.192, the fourth octet is the last octet with a value greater than 0. The value of this octet is 192. If your subnet mask were 255.255.192.0, then it would be the third octet. Consider the subnet mask 255.255.255.0. Because the fourth octet is a 0, it would be the third octet, as it's the last octet with a value greater than 0.

Now, subtract 192 from 256. The result is 64. The number 64 represents the block size or the number you are counting by in that octet. The subnet in this case is 10.1.1.0/26, and because the block size is 64, this subnet begins at 10.1.1.0/26 and ends at 10.1.1.63/26. The next subnet is 10.1.1.64/26 to 10.1.1.127/26. The third subnet is 10.1.1.128/26 to 10.1.1.191/26, and so on.

Now compare the addresses of devices with the subnet ranges you just identified. In this case, PC1, PC2, and an interface on R1 are supposed to be in the same subnet. As a result, they better all be addressed correctly, or communication will not occur correctly. For example, if you are reviewing the output of **ipconfig** on PC1, as shown in [Example 1-2](#), now that you have the ranges, you can easily see that PC1 is not in the same subnet as R1 and PC2. Although they have the same subnet mask, in this case PC1 falls in the range 10.1.1.64/26 to 10.1.1.127/26, whereas PC2 and the default gateway fall in the range 10.1.1.0/26 to 10.1.1.63/26. PC1 is in a different

network/subnet, but it should be in the same subnet, according to [Figure 1-3](#). You must fix the address on PC1 so that it is within the correct network/subnet.

Example 1-2 *Verifying IP Addressing on a PC with the **ipconfig** Command*

[Click here to view code image](#)

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 10.1.1.74
    Subnet Mask . . . . . : 255.255.255.192
    IP Address. . . . . : 2001:10::10
    IP Address. . . . . : fe80::4107:2cfb:df25:5124%7
    Default Gateway . . . . . : 10.1.1.1
```

DHCP for IPv4

Dynamic Host Configuration Protocol (DHCP) is commonly used for assigning IPv4 address information to a network host. Specifically, DHCP allows a DHCP client to obtain an IP address, subnet mask, default gateway IP address, DNS server IP address, and other types of IP addressing information from a DHCP server. The DHCP server can be local within the subnet, in a remote subnet, or the same device that is also the default gateway.

Because using DHCP is the most common way to deploy IPv4 addresses, you need to be well versed in the DHCP process and able to recognize issues related to DHCP. This section explains how DHCP operates and focuses on how to identify DHCP-related issues.

Reviewing DHCP Operations

If you have a cable modem, Digital Subscriber Line (DSL), or fiber connection in your home, your router more than likely obtains its IP address from your service provider through DHCP. The router is also acting as a DHCP server for the devices in your home. In corporate networks, when a PC boots, that PC receives its IP address configuration information from a corporate DHCP server. [Figure 1-4](#) illustrates the exchange of messages (Discover, Offer, Request, Acknowledgment [DORA] process) that occurs as a DHCP client obtains IP addressing information from a DHCP server.

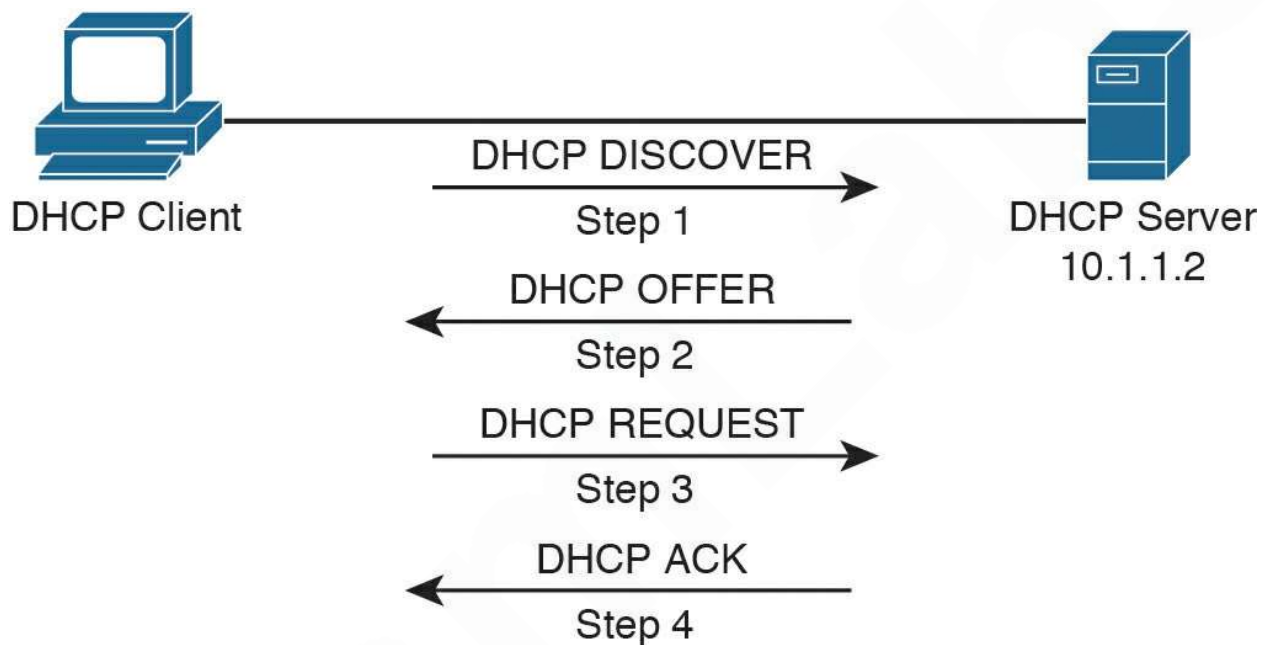


Figure 1-4 *DHCP DORA Process*



The DORA process works as follows:

- Step 1.** When a DHCP client initially boots, it has no IP address, default gateway, or other such configuration information. Therefore, the way a DHCP client initially communicates is by sending a broadcast message (that is, a DHCPDISCOVER message) to destination IP address 255.255.255.255 and destination MAC address FFFF:FFFF:FFFF in an attempt to discover a DHCP server.

The source IP address is 0.0.0.0, and the source MAC address is the MAC address of the sending device.

- Step 2.** When a DHCP server receives a DHCPDISCOVER message, it can respond with a DHCPOFFER message with an unleased IP address, subnet mask, and default gateway information. Because the DHCPDISCOVER message is sent as a broadcast, more than one DHCP server might respond to this Discover message with a DHCPOFFER. However, the client typically selects the server that sent the first DHCPOFFER response it received.
- Step 3.** The DHCP client communicates with the selected server by sending a broadcasted DHCPREQUEST message indicating that it will be using the address provided in the DHCPOFFER and, as a result, wants the associated address leased to itself.
- Step 4.** Finally, the DHCP server responds to the client with a DHCPACK message indicating that the IP address is leased to the client and includes any additional DHCP options that might be needed at this point, such as the lease duration.

Notice that in step 1, the DHCPDISCOVER message is sent as a broadcast. The broadcast cannot cross a router boundary. Therefore, if a client resides on a different network from the DHCP server, you need to configure the default gateway of the client as a DHCP relay agent to forward the broadcast packets as unicast packets to the server. You use the **ip helper-address** *ip_address* interface configuration mode command to configure a router to relay DHCP messages to a DHCP server in the organization.

To illustrate, consider [Figure 1-5](#) and [Example 1-3](#). In the figure, the DHCP client belongs to the 172.16.1.0/24 network, whereas the DHCP server belongs to the 10.1.1.0/24 network. Router R1 is configured as a DHCP relay agent, using the syntax shown in [Example 1-3](#).

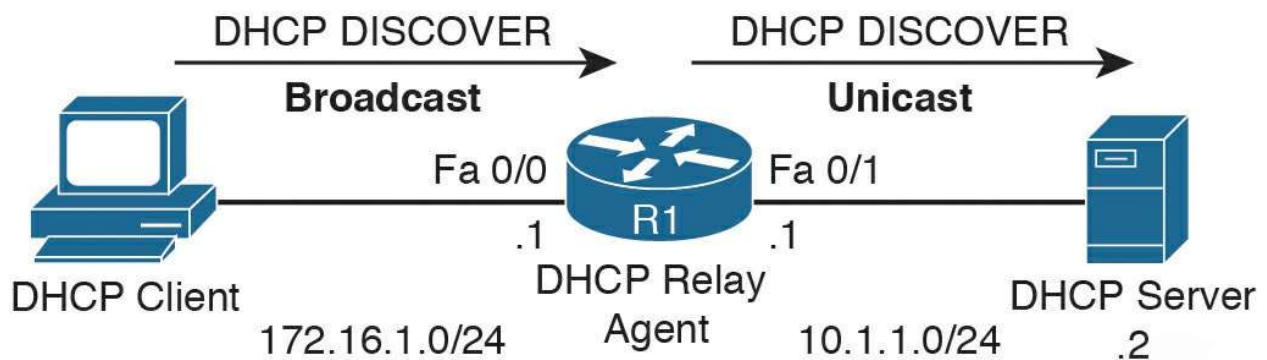


Figure 1-5 *DHCP Relay Agent*



Example 1-3 *DHCP Relay Agent Configuration*

[Click here to view code image](#)

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# service dhcp
R1(config)# interface fa 0/0
R1(config-if)# ip helper-address 10.1.1.2
```

In the configuration, notice the **service dhcp** command. This command enables the DHCP service on the router, which must be enabled for the DHCP services to function. This command is usually not required because the DHCP service is enabled by default; however, when troubleshooting a DHCP relay agent issue, you might want to confirm that the service is enabled. Also, the **ip helper-address 10.1.1.2** command specifies the IP address of the DHCP server. If the wrong IP address is specified, the DHCP messages are relayed to the wrong device. In addition, the **ip helper-address** command must be configured on the interface that is receiving the DHCPDISCOVER messages from the clients. If it isn't, the router cannot relay the DHCP messages.

When you configure a router to act as a DHCP relay agent, realize that it

relays a few other broadcast types in addition to a DHCP message. Other protocols that are forwarded by a DHCP relay agent include the following:

- TFTP
- Domain Name System (DNS)
- Internet Time Service (ITS)
- NetBIOS name server
- NetBIOS datagram server
- BootP
- TACACS

As a reference, [Table 1-2](#) provides a comprehensive list of DHCP message types you might encounter while troubleshooting a DHCP issue.

Table 1-2 DHCP Message Types

DHCP Message	Description
DHCPDISCOVER	A client sends this message in an attempt to locate a DHCP server. This message is sent to broadcast IP address 255.255.255.255, using UDP port 67.
DHCPOFFER	A DHCP server sends this message in response to a DHCPDISCOVER message, using UDP port 68.
DHCPREQUEST	This broadcast message is a request from the client to the DHCP server for the IP addressing information and options that were received in the DHCPOFFER message.
DHCPDECLINE	This message is sent from a client to a DHCP server to inform the server that an IP address is already in use on the network.

DHCPACK	A DHCP server sends this message to a client and includes IP configuration parameters.
DHCPNAK	A DHCP server sends this message to a client and informs the client that the DHCP server declines to provide the client with the requested IP configuration information.
DHCPRELEASE	A client sends this message to a DHCP server and informs the DHCP server that the client has released its DHCP lease, thus allowing the DHCP server to reassign the client IP address to another client.
DHCPINFORM	This message is sent from a client to a DHCP server and requests IP configuration parameters. Such a message might be sent from an access server requesting IP configuration information for a remote client attaching to the access server.

In addition to acting as a DHCP relay agent, a router might act as a DHCP client. Specifically, the interface of a router might obtain its IP address from a DHCP server. [Figure 1-6](#) shows a router acting as a DHCP client, where the router's Fast Ethernet 0/1 interface obtains its IP address from a DHCP server. [Example 1-4](#) provides the configuration for the router in the topology (that is, router R1). Notice that the **dhcp** option is used in the **ip address** command, instead of the usual IP address and subnet mask information.