Designing for Cisco Network Service Architectures (ARCH)

Foundation Learning Guide

(CCDP ARCH 300-320)

Fourth Edition

Marwan Al-shawi, CCDE No. 20130066
André Laurent, CCIE No. 21840 I CCDE No. 20120024

ciscopress.com

Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide, Fourth Edition

CCDP ARCH 300-320

Marwan Al-shawi, CCDE No. 20130066

André Laurent, CCDE No. 20120024, CCIE No. 21840

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide, Fourth Edition

Marwan Al-shawi and André Laurent

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

Printed in the United States of America

First Printing December 2016

Library of Congress Control Number: 2016958010

ISBN-13: 978-1-58714-462-2

ISBN-10: 1-58714-462-x

Warning and Disclaimer

This book is designed to provide information about designing Cisco Network Service Architectures. 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

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.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Ron Fligge

Product Line Manager: Brett Bartow

Acquisitions Editor: Michelle Newcomb

Managing Editor: Sandra Schroeder

Development Editor: Ginny Munroe

Senior Project Editor: Tonya Simpson

Copy Editor: Chuck Hutchinson

Technical Editors: Denise Fishburne, Orhan Ergun

Editorial Assistant: Vanessa Evans

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Lisa Stumpf

Proofreader: Deepa Ramesh

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.

About the Authors

Marwan Al-shawi, CCDE No. 20130066, is a Cisco Press author whose titles include the top Cisco certification design books *CCDE Study Guide* and *Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide*, Fourth Edition. He also is an experienced technical architect. Marwan has been in the networking industry for more than 12 years and has been involved in architecting, designing, and implementing various large-scale networks, some of which are global service provider–grade networks. Marwan holds a Master of Science degree in internetworking from the University of Technology, Sydney. He enjoys helping and assessing network designs and architectures; therefore, he was selected as a Cisco Designated VIP by the Cisco Support Community (CSC) (official Cisco Systems forums) in 2012 and by the Solutions and Architectures subcommunity in 2014. In addition, Marwan was selected as a member of the Cisco Champions program in 2015 and 2016. In his spare time, Marwan provides CCDP- and CCDE-related training and blogs at netdesignarena.com.

André Laurent, 3xCCIE No. 21840, CCDE No. 20120024, is the worldwide director of engineering for enterprise networking sales at Cisco Systems and a Cisco Press author. Outside his own personal development, André has an equal passion for helping others develop their systems and assisting them with the certification process. André is recognized in the industry as a subject matter expert in the areas of routing, switching, security, and design. Although he wears a Cisco badge, André takes a neutral approach in helping clients establish a long-term business and technology vision covering necessary strategy, execution, and metrics for measuring impact.

About the Technical Reviewers

Denise "Fish" Fishburne, CCDE No. 20090014, CCIE No. 2639 (R&S, SNA), is an engineer and team lead with the Customer Proof of Concept Lab (CPOC) in North Carolina. Fish is a geek who absolutely adores learning and passing it on. She works on many technologies in the CPOC, but her primary technical strength is troubleshooting. Fish has been with Cisco since 1996 and CPOC since 2001, and has been a regular speaker at Networkers/Cisco Live since 2006. Cisco Live is a huge passion for Fish! As such, in 2009, she got even more deeply involved with it by becoming a Cisco Live session group manager. Look for Fish swimming in the bits and bytes all around you, or just go to www.NetworkingWithFish.com.

Orhan Ergun, CCDE No. 2014:0017, CCIE No. 2014:0017 (CCNP, CCDP, JNCIS, and JNCIP), is a network architect who focuses on service providers, data centers, virtualization, cloud, and network security. He has more than 13 years of IT experience and has worked on many medium- and large-scale network design and deployment projects. He teaches Cisco network design concepts and writes exam questions for Cisco Systems.

Dedications

I would like to dedicate this book to my wonderful mother for her continued support, love, encouragement, guidance, and wisdom, as well as to the people in my life who always support and encourage me.

And most importantly, I would like to thank God for all blessings in my life.

—Marwan

I would like to dedicate this book to the women in my life. My mother, for her unconditional dedication and love. My sister, for rescuing me from the drifter life and setting me up with my first job in the industry. My beautiful wife, who continues to stand by my side while encouraging me through all the new challenges, opportunities, and experiences life brings.

—André

Acknowledgments

A special thank you goes to the Pearson Cisco Press team for their support in making this book possible.

A big thank you goes to André for being part of this publication and adding his expert perspective. It's always a pleasure to work with an experienced and extremely helpful person like André.

We would like to give special recognition to the wonderful technical reviewers Denise Fishburne and Orhan Ergun for their valuable contributions in editing the book. Both Denise and Orhan are very experienced network designers and CCDE certified; therefore, their suggestions and feedback helped shape and optimize the quality of the contents on multiple areas.

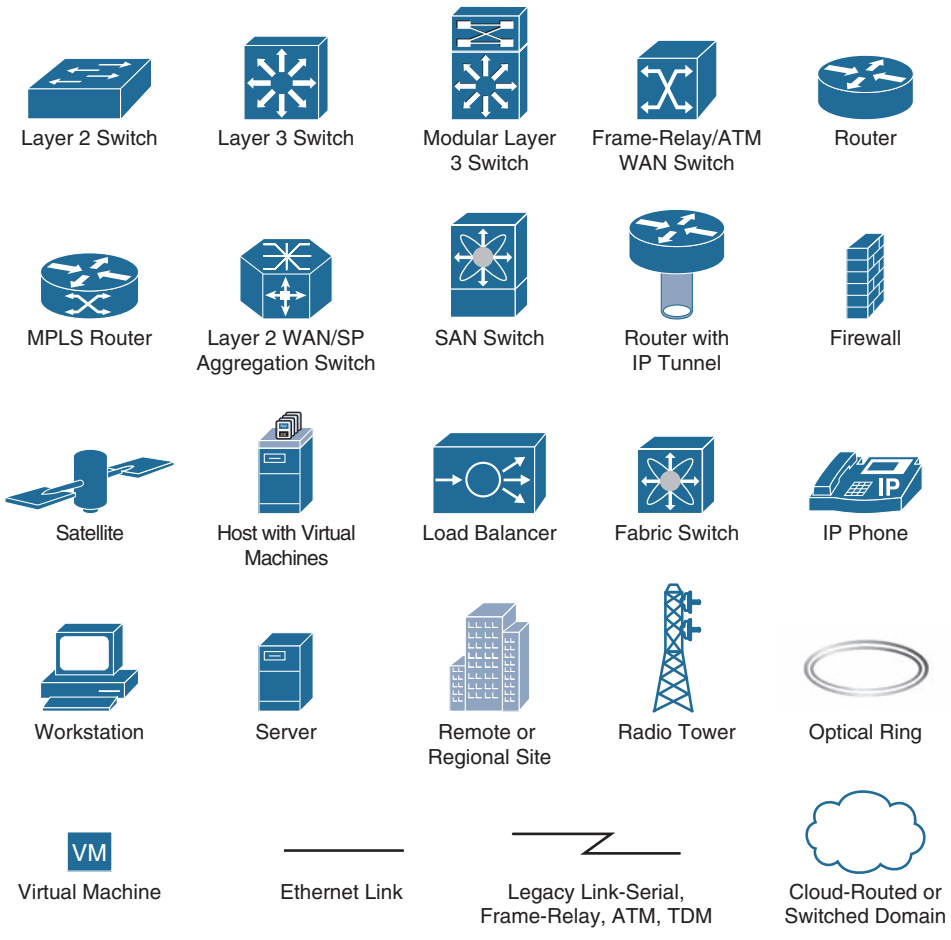
In addition, a special thank you to Maurizio Portolani (Cisco Press author and distinguished system engineer at Cisco Systems) and John Weston (systems engineer at Cisco) for their help and support with the technical review and optimization of the ACI chapter.

Also, we want to thank Adrian Arumugam (network engineer for a major content provider) for his technical review and valuable comments of certain chapters.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Reader Services

Register your copy at www.ciscopress.com/title/9781587144622 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587144622 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Enterprise environments require networks designed for performance, availability, and scalability to achieve outcomes. Seasoned IT professionals with progressive end-to-end network design expertise are crucial in ensuring networks deliver to meet today's requirements while future-proofing investments. For senior network design engineers, principal system engineers, network/solution architects, and CCDA professionals looking to build on your fundamental Cisco network design expertise, the Cisco CCDP certification program focuses on advanced addressing and routing protocols, WANs, service virtualization, and integration strategies for multilayered enterprise architectures.

This exam tests a candidate's knowledge and skills needed to design or help in designing an enterprise network. Successful candidates will be able to design and understand the inner workings of all elements within the common enterprise network, including internal routing, BGP routing, modern WAN connectivity, modern data center and data center interconnect, basic network security considerations, advanced quality-of-service design, transition to IPv6, and multicast routing design.

Goals of This Book

Designing Cisco Network Service Architectures (ARCH) enables network designers, engineers, architects, and CCDP candidates to perform the conceptual, intermediate, and detailed design of a network infrastructure that supports desired network solutions over intelligent network services to achieve effective performance, scalability, and availability. By applying solid Cisco network solution models and recommended design practices, ARCH enables learners to provide viable, stable enterprise internetworking solutions. This book presents concepts and examples necessary to design converged enterprise networks. Also, this new edition has content addressing software-defined networks (SDNs). You will learn additional aspects of modular campus design, advanced routing designs, WAN service designs, enterprise data center design, and security design.

Who Should Read This Book

Besides those who are planning or studying for the CCDP certification, this book is for

- Network designers, architects, consultants, or engineers seeking a thorough understanding of enterprise network design
- Network engineers or architects who are studying for the CCDE certification and need to improve their foundational knowledge of modern enterprise network design
- Anyone wanting to understand basic and advanced network design with an intermediate to advanced level of experience

How This Book Is Organized

This book is organized into eight distinct sections.

Part I of the book explains briefly the various design approaches, requirements, and principles required to design an optimum enterprise campus network. Also, it focuses on enterprise routing design, covering the different design options, considerations, and design implications with regard to business and other design requirements.

- **Chapter 1, "Optimal Enterprise Campus Design":** This chapter discusses how to design a scalable and reliable enterprise campus taking into account applications and business requirements.
- **Chapter 2, "EIGRP Design":** This chapter highlights, analyzes, and discusses different design options and considerations of EIGRP that any network designer must be aware of.
- **Chapter 3, "OSPF Design":** This chapter looks at the different design options and considerations of OSPF that any network designer must be aware of, such as OSPF area design.
- **Chapter 4, "IS-IS Design":** This chapter discusses IS-IS level design. It also compares the key functionalities of IS-IS and OSPF as link-state routing protocols.
- **Chapter 5, "Border Gateway Protocol Design":** This chapter highlights, analyzes, and discusses different design options and considerations of BGP that any network designer must be aware of. It also provides some advanced BGP design approaches to address enterprise design needs.

Part II of the book focuses on IPv6 and how to plan and migrate your network to be IPv6 enabled along with the different design considerations and implications.

- **Chapter 6, "IPv6 Design Considerations in the Enterprise":** This chapter highlights and explains the different design considerations and approaches of migrating IPv4 networks to IPV6.
- **Chapter 7, "Challenges of the Transition to IPv6":** This chapter discusses the different challenges associated with migration to IPv6 that you need to take into account.

Part III of the book focuses on the different models of modern enterprise wide-area network design.

- **Chapter 8, "Service Provider–Managed VPNs":** This chapter highlights and discusses the MPLS Layer 3 and Layer 2 VPN-based WAN modes along with the different design considerations and aspects that you need to be aware of.
- **Chapter 9, "Enterprise-Managed WAN":** This chapter discusses the different enterprise-controlled VPN-based WAN models that can be used in today's enterprise networks.

- **Chapter 10, "Enterprise WAN Resiliency Design":** This chapter explains how to optimize the enterprise-managed WAN model to design a resilient overlay WAN model.

Part IV of the book focuses on the design options and technologies required to design an enterprise data center network.

- **Chapter 11, "Multitier Enterprise Data Center Designs":** This chapter analyzes, explains, and compares the different data center design options and where each should be used.
- **Chapter 12, "New Trends and Techniques to Design Modern Data Centers":** This chapter analyzes, explains, and compares the different modern data center design options and technologies and the drivers of each. It also introduces you to the data center overlay and SDN concepts.
- **Chapter 13, "Cisco Application-Centric Infrastructure":** This chapter analyzes and explains the foundations of the Cisco ACI and the design concepts and terms that are ACI-specific, along with the different migration options from a traditional data center network to an ACI-based data center network.
- **Chapter 14, "Data Center Connections":** This chapter analyzes, explains, and compares the different data center interconnect design options and considerations.

Part V of the book focuses on designing quality of service (QoS) for an optimized user experience and dives deeper, discussing QoS design for the different places in the network.

- **Chapter 15, "QoS Overview":** This chapter explains the different QoS design concepts, techniques, and tools that any design engineer needs to be fully aware of its foundations.
- **Chapter 16, "QoS Design Principles and Best Practices":** This chapter explains the different QoS design principles and strategies required to design a reliable QoS-enabled network.
- **Chapter 17, "Campus, WAN, and Data Center QoS Design":** This chapter explains the best-practice design principles for enabling QoS in campus, WAN, and data center networks.
- **Chapter 18, "MPLS VPN QoS Design":** This chapter covers the basics of designing QoS for MPLS VPN networks.
- **Chapter 19, "IPsec VPN QoS Design":** This chapter reviews QoS-related considerations for IPsec VPNs.

Part VI of the book is an entry point to IP multicast services. It presents the functional model of IP multicast and gives an overview of technologies that are present in IP multicasting. The part is composed of an introduction to IP multicast concepts as well as a discussion of distribution trees and protocols.

- **Chapter 20, "Enterprise IP Multicast Design":** This chapter reviews the foundations of IP multicast and how a multicast-enabled network delivers traffic from a source to a receiver. Also, it explains the most current scalable IP multicast routing protocol.
- **Chapter 21, "Rendezvous Point Distribution Solutions":** This chapter offers an overview of RP distribution solutions. It explains the drawbacks of manual RP configuration and describes the Auto-RP and the BSR mechanisms. The chapter also introduces the concept of Anycast RP, which works in combination with the MSDP.

Part VII of the book focuses on how to design security services and what solutions are available today to implement network-level security.

- **Chapter 22, "Designing Security Services and Infrastructure Protection":** This chapter explains how to secure the network infrastructure as it is a critical business asset.
- **Chapter 23, "Designing Firewall and IPS Solutions":** This chapter explains the common firewall and IPS architectures, high-availability modes, and firewall virtualization along with design recommendations.
- **Chapter 24, "IP Multicast Security":** This chapter describes the challenges with IP multicast security along with recommendations of how to secure a multicast network edge, Auto-RP, BSR, and MSDP.
- **Chapter 25, "Designing Network Access Control Solutions":** This chapter discusses the different access control design approaches, including IEEE 802.1X–based access control and Cisco TrustSec technology.

Part VIII of the book offers some design scenarios that help you, as design engineer, practice designing technology solutions based on business and technical requirements.

- **Chapter 26, "Design Case Studies":** This chapter provides different design scenarios that cover the design of IGP, BGP, WAN, data center networks, security, IPv6, and QoS.

Chapter 16

QoS Design Principles and Best Practices

Upon completing this chapter, you will be able to

- Describe basic classification and marking design principles
- Describe basic policing and remarking design principles
- Explain queuing design principles
- Explain basic dropping design principles
- Explain what are per-hop behavior queue design principles
- Explain the role of RFC 4594 recommendation
- List and describe QoS strategy models
- Describe the 4-class QoS strategy model
- Describe the 8-class QoS strategy model
- Describe the 12-class QoS strategy model

Now that we have covered the various tools for enabling quality of service (QoS) in the network, it is possible to create a QoS strategy that best meets an organization's requirements. This chapter presents some best practice QoS design principles and QoS strategy models that are used to implement the numerous QoS tools we have at our disposal. Remember that usually more than one solution fits the given QoS requirements, so simplifying the models leveraged can significantly accelerate and ensure proper QoS deployment.

QoS Overview

Quality of service is critical to ensuring application performance consistency and optimized end-user experiences. As discussed in Chapter 15, "QoS Overview," the fundamental purpose of QoS is to manage contention for network resources while

addressing applications that require differentiated levels of service. Prior to developing a QoS strategy, you must perform the proper discovery to identify current and future applications and application characteristics within the environment. This information, coupled with an understanding of the end-to-end network design and traffic patterns, will drive the QoS design strategy model that is most appropriate for the business. Following are some common questions that you need to answer:

- What traffic needs to be classified and marked?
- Is it possible to leverage a 4-class, 8-class, or 12-class QoS strategy model from end to end?
- Will traffic-marking characteristics stay in place as data traverses the infrastructure?
- What traffic needs to be prioritized?
- What traffic requires bandwidth reservations?
- What traffic needs to be policed?
- Is shaping required at the WAN edge or at other places within the infrastructure such as the Data Center Interconnect (DCI)?
- How can congestion management and congestion avoidance techniques be leveraged to optimize TCP traffic?

Classification and Marking Design Principles

The first fundamental design principle is that QoS policies should always be enabled in hardware whenever possible. Some Cisco routers perform QoS in software, and such behavior can increase the load on the CPU. Cisco Catalyst switches have dedicated hardware called application-specific integrated circuits (ASIC), which are used to perform QoS operations. Switches can perform complex QoS policies under maximum traffic load without any marginal CPU spike. Some platforms, such as the Cisco ASR, can perform QoS operations (such as queuing) in dedicated hardware ASICs, but other functions (such as deep packet inspection) are still processed in software via the CPU.

Based on design recommendations, classification and marking should be done closest to the source of traffic as administratively and technically possible. This design principle promotes DiffServ and per-hop behaviors (PHB) as the recommended end-to-end design.

Note "As administratively close as possible" refers to an administrative domain, in scenarios in which you are not controlling the end-to-end traffic flow path of a packet; you need to classify/mark as close to the source as possible within your administrative domain.

As a rule, it is not recommended to trust markings set by end users leveraging PCs or other endpoint devices. End users can intentionally or unintentionally abuse QoS policies that trust markings of end devices. If users and unclassified applications take advantage of the configured QoS policy as a result of trusting end devices, this can result in easily starving priority queues with nonpriority traffic, ruining quality of service for real-time applications. However, if QoS markings for end devices and associated applications are administered centrally across the enterprise, this can be an acceptable design option. An additional area of exception might also include wireless devices that can leverage Wireless Multimedia (WMM) QoS provisioning in the upstream direction.

The next important recommendation is to use Differentiated Services Code Point (DSCP) marking whenever technically possible. DSCP markings are the recommended method for marking IP traffic for the following reasons:

- It has support for end-to-end Layer 3 marking.
- It is a more granular method of marking that supports 64 levels as compared to class of service (CoS) and MPLS Experimental EXP, which have 8 levels.
- It is more extensible than Layer 2 markings as these markings are lost when media changes.

To provide interoperability on the border between enterprise and service provider networks, you should use standard-based DSCP PHB markings because the use of such markings can streamline interoperability and compliance with service provider classes of service. Classification and marking design principles covered in this section are illustrated in Figure 16-1.

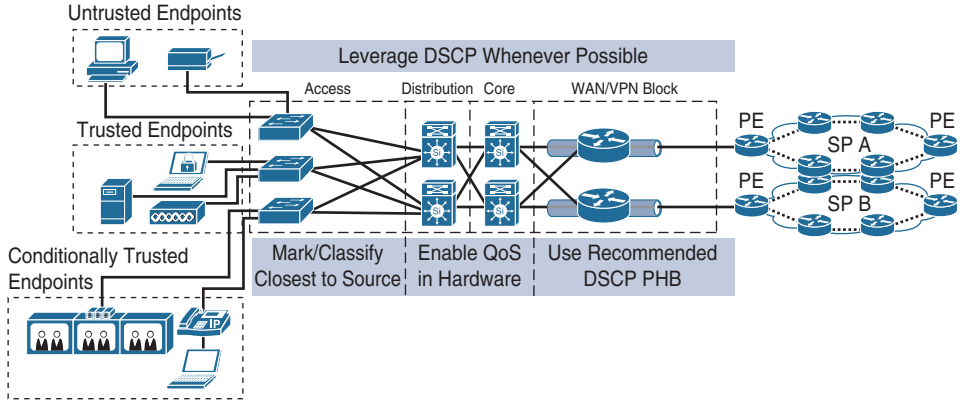
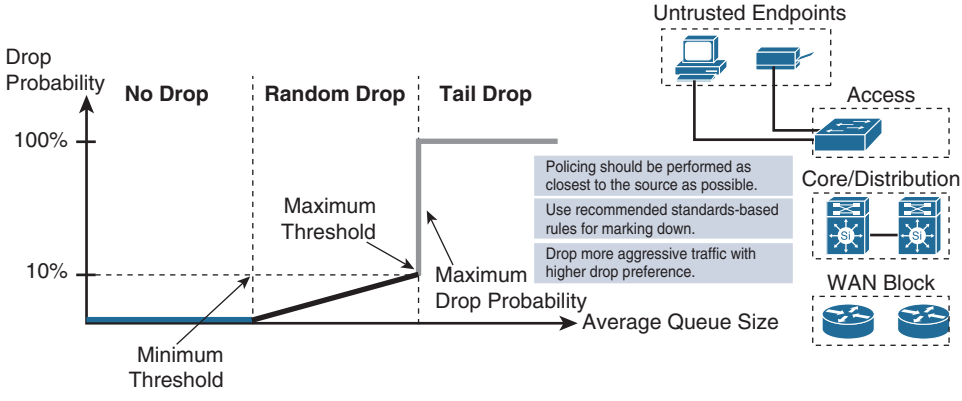


Figure 16-1 *QoS Classification and Marking Architecture*

Policing and Remarking Design Principles

Traffic that is unwanted should be discarded as soon as possible to preserve network resources from unnecessary consumption. Undesirable traffic can be the result of denial of service (DoS) or worm attacks. Furthermore, excessive unwanted traffic could cause a network outage as a result of high impact on the CPU and memory resources of network devices. Malicious traffic can mask under legitimate TCP/UDP ports that are used by well-known applications, and this traffic can create large amounts of unwanted traffic. Traffic behavior must be monitored and marked down as close as possible to the source under such circumstances.

Traffic should be marked down using RFC recommendations. Those recommendations ensure interoperability and end-to-end QoS network design. Examples of these recommendations are RFC 2597 and RFC 2698, where excess traffic with marking of AFx1 should be marked down to AFx2 or AFx3. Note that 2 or 3 in AFx2 and AFx3 represent drop probability. This markdown principle should be combined properly with other QoS tools. For example, with DSCP-based WRED, AFx2 should be dropped more aggressively than AFx1 but less aggressively than AFx3. Figure 16-2 illustrates the policing and remarking design principles covered in this section.



Class	Value		
AF1	001	**dd**	0
AF2	010	dd	0
AF3	011	dd	0
AF4	100	dd	0

Drop Probability (dd)	Value	AF Value
Low	01	AF11
Medium	10	AF12
High	11	AF13

Figure 16-2 *Policing and Remarking Concepts*

Queuing Design Principles

The only way to provide QoS service guarantees to business-critical applications is to enable queuing to every node that has the potential for congestion. Queuing should be enabled regardless of whether congestion is occurring rarely or frequently. Although frequently deployed at the WAN edge, this principle must be applied not only to congested WAN links but also within the campus network. Speed mismatch, link aggregation, and link subscription ratios can create congestion in the network devices by filling up queuing buffers.

Because each distinctive application class requires unique QoS service requirements, it is recommended you provide a distinctive queue for each traffic class. One of the main justifications for leveraging distinctive queues is that each QoS service class can accept certain QoS-enabled behaviors such as bandwidth allocation and dropping ratios.

It is recommended you use a minimum of four standards-based queuing behaviors on all platforms and service provider links when deploying end-to-end QoS across the network infrastructure:

- RFC 3246 Expedited Forwarding PHB (used for real-time traffic)
- RFC 2597 Assured Forwarding PHB (used for guaranteed bandwidth queue)
- RFC 2474 Default Forwarding PHB (default nonprioritized queue, best effort)
- RFC 3662 Lower Effort Per-Domain Behavior (less than best-effort queue, bandwidth constrained)

Dropping Design Principles

As covered in Chapter 15, congestion avoidance mechanisms are used to selectively drop packets when a predefined limit is reached. As a review, by dropping packets early, congestion avoidance helps prevent bottlenecks downstream the network. Congestion avoidance mechanisms include RED and WRED. If WRED is designed per recommendations where every traffic class has its own queue, WRED should be used for only some types of queues (not necessarily all of them).

It is recommended that WRED not be used for the strict-priority queue, scavenger traffic queue, and control traffic queue. Traffic for the strict-priority queue and control traffic queue are highly sensitive to dropping. Scavenger traffic is often provisioned with a small amount of bandwidth, typically below 1 percent, and for this type of queue, WRED is not needed. Considering that the WRED feature is performed in software, enabling WRED for scavenger traffic class will consume additional CPU resources with no significant gain.

For AF-marked queues with DSCP-based WRED, typically traffic marked with AFx3 is more aggressively dropped than AFx2, which is in turn more aggressively dropped than AFx1.

All traffic types that are not explicitly defined in other queues fall into default (DF) traffic class. For this traffic class, it is recommended to enable WRED. WRED should be enabled in the default queue because, as explained in Chapter 15, it increases throughput by reducing the TCP synchronization effect. In the case of the default queue where all different traffic types are equally marked with a DSCP value of zero, there is no mechanism to fairly weight less aggressive applications when WRED is not enabled.

Per-Hop Behavior Queue Design Principles

The goal of convergence in the network is to enable voice, video, and data applications to seamlessly coexist in the network by providing each with appropriate QoS service expectations and guarantees.

When real-time applications are the only ones that consume link bandwidth, non-real–time applications' performance can be significantly degraded. Extensive testing results show that there is significant performance impact on non-real–time applications when more than one-third of the links is used by real-time applications as part of a strict-priority queue. Thus, it is recommended that no more than a third of link bandwidth be used for strict-priority queuing. This principle prevents non-real–time applications from being dropped out of their required QoS recommendations. In other words, it is recommended that no more than 33 percent of the bandwidth be used for the expedite forwarding (EF) queue. It is also important to note that this 33 percent design principle is simply a best practices design recommendation and not necessarily a mandatory rule.

It is recommended that a minimum of one queue be provisioned for assured forwarding per-hop behavior (AF PHB), but up to four subclasses can be defined within the AF class: AF1x, AF2x, AF3x, and AF4x. Each queue belonging to the specified AF subclass must have a bandwidth guarantee that corresponds to the application requirements of that traffic subclass.

The default forwarding (DF) class consists of all traffic that is not explicitly defined in other queues. If an enterprise is using many applications, it is important to have adequate space for those traffic types. It is recommended that typically 25 percent of link bandwidth be used for this service class. Figure 16-3 illustrates an example of bandwidth allocation leveraging these recommended best practices.

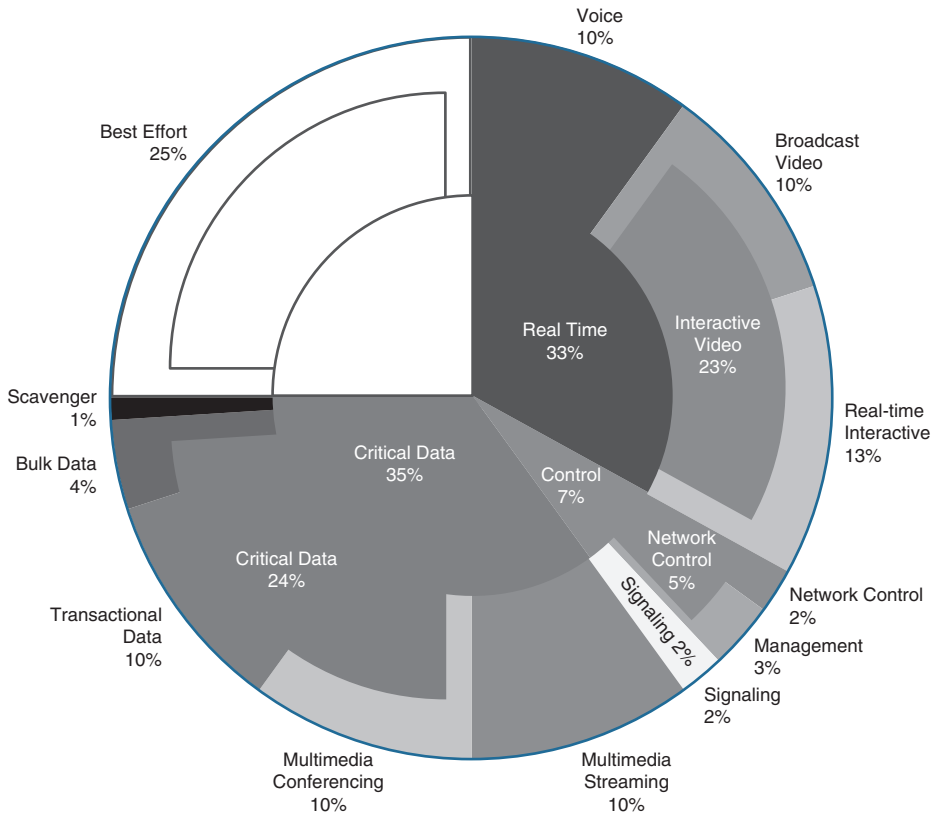


Figure 16-3 *Bandwidth Allocation Example*

RFC 4594 QoS Recommendation

RFC 4594 QoS provides guidelines for marking, queuing, and dropping principles for different types of traffic. Cisco has made a minor modification to its adoption of RFC 4594, namely the switching of Call-Signaling and Broadcast Video markings (to CS3 and CS5, respectively). A summary of Cisco's implementation of RFC 4594 is presented in Figure 16-4.

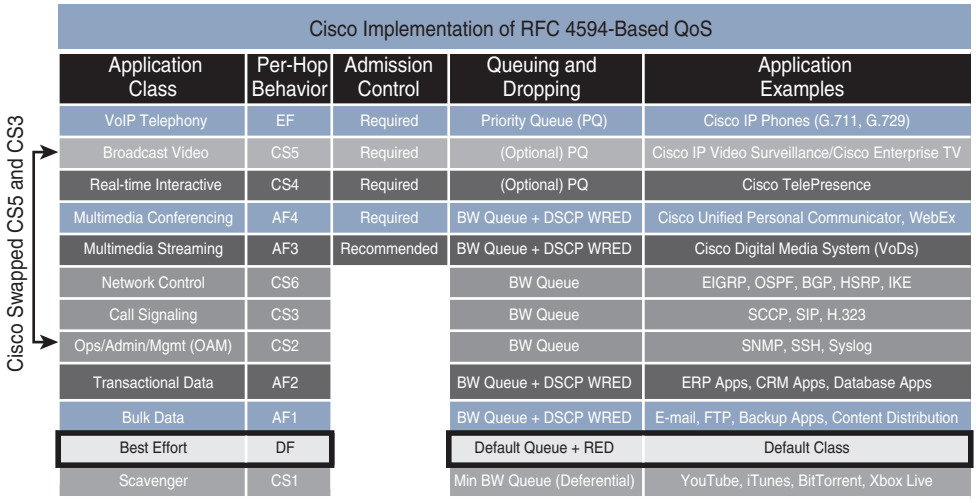


Figure 16-4 *QoS Marking—RFC 4594*

RFC 4594 is the recommendation but not the standard; it resides in the category of draft proposal RFCs. It recommends guidelines on how to configure 14 traffic classes that are associated with 28 different code-point marking values. Note that some of the PHBs shown in Figure 16-4 include multiple DSCP-associated values. For example, the AF class for multimedia streaming can have AF31, AF32, and AF33 DSCP values. RFC 4594 includes information on which PHBs should be used for certain traffic types and also what queuing and dropping mechanism should be used for that same traffic class.

Some sample recommendations highlighted in Figure 16-4 include

- Voice traffic should be marked to EF/DSCP 46.
- Voice should be queued using strict-priority queuing.
- Broadcast video traffic should be marked to CS5/DSCP 40.
- Multimedia conferencing should be treated with an AF PHB, provisioned with a guaranteed-bandwidth queue.

RFC 4594 is not a final RFC standard and will more than likely continue to be developed considering that needs and trends for QoS application requirements change over the time.

QoS Strategy Models

Before applying any QoS tools, organizations need to define the strategy and goals for different applications running in their network. This will result in defining a certain number of traffic classes to meet the end-to-end QoS objectives of an organization.

Three basic QoS strategy models can be deployed, depending on the granularity of applications running within an organization's network:

- 4-Class QoS Strategy Model
- 8-Class QoS Strategy Model
- 12-Class QoS Strategy Model

Although the more classes you define, the more specific and granular traffic treatment will be per application, the selection of a certain strategy model must be based on application requirements coupled with the WAN provider QoS model (if there is any WANs with QoS). The following sections provide a detailed view into each of these QoS strategy models.

4-Class QoS Strategy

The 4-class QoS strategy model is the simplest of the three models (in terms of QoS polices) and typically accounts for telephony, signaling, transactional/mission-critical, and best-effort data. When businesses deploy telephony applications in their network, three classes of traffic are typically required (telephony, signaling, and default/best effort).

Typically, the fourth class is the Assured Forwarding (AF) class. The AF class is used for transactional and mission-critical data applications such as SQL databases. The AF class can also be used for multimedia conferencing, multimedia streaming, and bulk data applications.

The 4-class QoS strategy model, as shown in Figure 16-5, is an example of where an organization has deployed IP telephony. In addition to separating telephony, signaling, and default/best-effort traffic, the organization has defined one mission-critical transactional data class.

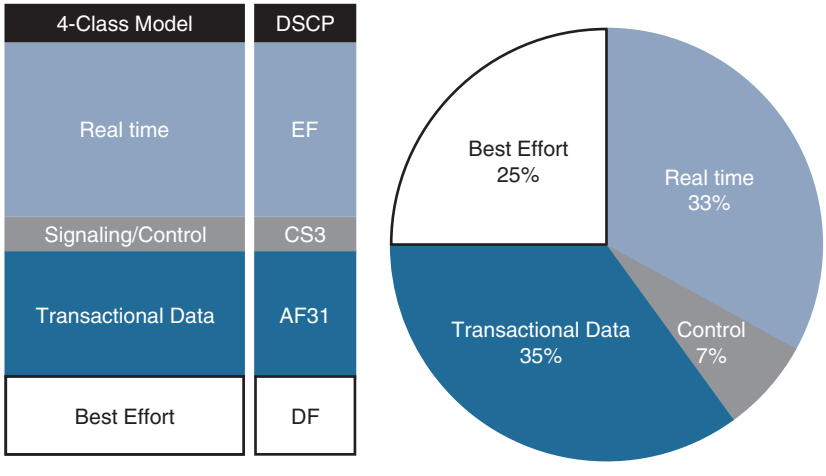


Figure 16-5 *The 4-Class QoS Strategy Model*

The four traffic classes of QoS markings and guarantees are as follows:

- **Voice (Real time):** Marked with EF and provisioned to leverage up to one-third of link bandwidth
- **Signaling:** Marked with CS3 and provisioned to leverage a minimum of 7 percent of link bandwidth
- **Mission-critical data (Transactional Data):** Marked with AF31 and provisioned to leverage 35 percent of link bandwidth
- **Default (best-effort data):** Marked with DF and provisioned to take advantage of 25 percent of link bandwidth

Voice and signaling guarantees must be selected based on the volume of voice calls and the VoIP codec that is used through the given link. Mission-critical data is selected based on the decision of the director of each company department who has given info about critical business application needs to the networking team.

8-Class QoS Strategy

The 8-class QoS strategy model builds upon the 4-class model and includes the following additional classes:

- Multimedia conferencing
- Multimedia streaming
- Network control
- Scavenger

The two additional multimedia traffic types in this model are multimedia conferencing and multimedia streaming. The explicitly defined network control traffic class is used for applications such as network routing protocol updates or network infrastructure control traffic such as OAM. The 8-class QoS strategy model is illustrated in Figure 16-6.

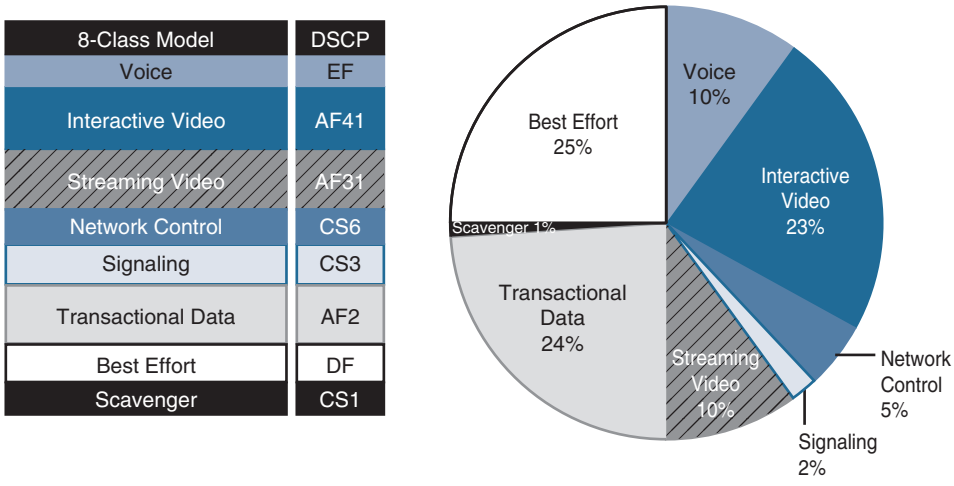


Figure 16-6 *The 8-Class QoS Strategy Model*

As can be seen from Figure 16-6, the recommendations for each traffic class in this model are as follows:

- **Voice:** Marked with EF and limited to 10 percent of link bandwidth in a strict-priority queue
- **Multimedia conferencing (Interactive video):** Marked with AF41 or sometimes as EF and limited to 23 percent of link bandwidth in a strict-priority queue
- **Multimedia streaming:** Marked with AF31 and guaranteed 10 percent of link bandwidth with WRED enabled
- **Network control:** Marked with CS6 and guaranteed 5 percent of link bandwidth
- **Signaling:** Marked with CS3 and provisioned with minimum of 2 percent of link bandwidth
- **Transactional data:** Marked with AF21 and provisioned with 24 percent of link bandwidth with WRED enabled
- **Default (best-effort data):** Marked with DF and provisioned with 25 percent of link bandwidth
- **Scavenger:** Marked with CS1 and provisioned with a maximum of 1 percent of link bandwidth

Note It is important to note the difference as some traffic types, such as voice traffic, are limited by bandwidth defined in a strict-priority queue, and other traffic types, such as multimedia streaming, have guaranteed provisioned bandwidth.

12-Class QoS Strategy

The 12-class QoS strategy model builds upon the 8-class model and includes the following additional classes:

- Real-time Interactive
- Broadcast Video
- Management/OAM
- Bulk Data

The 12-class QoS strategy model represents Cisco's interpretation of the RFC 4594 recommendation and, as previously noted, incorporates a slight modification by swapping the markings used for signaling and broadcast video. The 12-class QoS strategy model is illustrated in Figure 16-7.

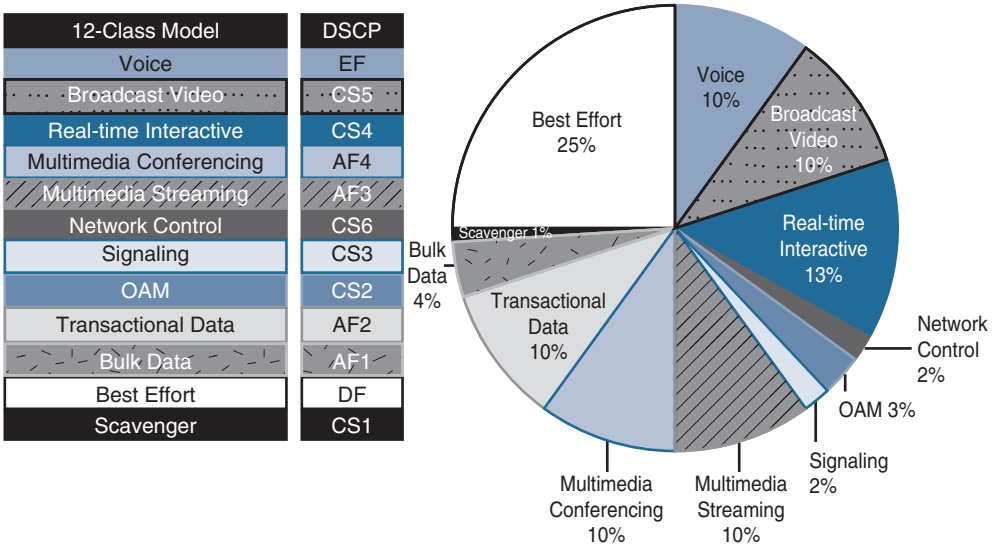


Figure 16-7 *The 12-Class QoS Strategy Model*

As can be seen from Figure 16-7, the recommendations for each traffic class in this model are as follows:

- **Voice:** Marked with EF and limited to 10 percent of link bandwidth in a strict-priority queue
- **Broadcast video:** Marked with CS5 or sometimes as EF and limited to 10 percent of link bandwidth in a strict-priority queue
- **Real-time interactive:** Marked with CS4 or sometimes as EF and limited to 13 percent of link bandwidth in a strict-priority queue

- **Multimedia conferencing:** Marked with AF41 or sometimes as EF and limited to 10 percent of link bandwidth in a strict-priority queue
- **Multimedia streaming:** Marked with AF31 and guaranteed 10 percent of link bandwidth with WRED enabled
- **Network control:** Marked with CS6 and provisioned as guaranteed bandwidth 2 percent of link bandwidth
- **Signaling:** Marked with CS3 and provisioned with a minimum of 2 percent of link bandwidth
- **Management/OAM:** Marked with CS2 and provisioned with a minimum of 3 percent of link bandwidth
- **Transactional data:** Marked with AF21 and provisioned with 10 percent of link bandwidth with WRED enabled
- **Bulk data:** Marked with AF11 and provisioned with 4 percent of link bandwidth with WRED enabled
- **Default (best-effort data):** Marked with DF and provisioned with 25 percent of link bandwidth
- **Scavenger:** Marked with CS1 and provisioned with a maximum of 1 percent of link bandwidth

Summary

- Use QoS policies in hardware rather than in software whenever possible.
- Classify, mark, and police applications as close to the source as possible.
- Use DSCP marking whenever possible.
- Define a queue for the traffic class and enable queuing on each node that has potential congestion.
- Limit the strict-priority queue to one-third of the link bandwidth.
- Do not use WRED for priority or scavenger traffic classes.
- Use one of the three QoS strategy models to govern end-to-end QoS design.

Review Questions

After answering the following questions, please refer to Appendix A, "Answers to Review Questions," for the answers.

1. Which of the following is recommended for a QoS queuing design?
   a. You should implement queuing policy very selectively.
   b. Classes should share queues in order to save resources.

c. You should use at minimum 4 classes of queuing behavior.
d. You should use at minimum 11 classes of queuing behavior.

2. Match the application classes with their PHBs as per RFC 4594.

VoIP Telephony	EF
Transactional Data	CS1
Network Control	CS6
Call Signaling	CS4
Real-time Interactive	AF21

3. Select the four classes of the 4-class QoS model.
a. Voice, signaling, mission-critical data, and best effort
b. Video, signaling, mission-critical data, and best effort
c. Voice, signaling, mission-critical data, and scavenger
d. Real-time interactive, signaling, mission-critical data, and best effort

4. Why is it recommended to leverage DSCP markings wherever possible?
a. Support for end-to-end Layer 3 marking.
b. It is a more granular method of marking that supports 64 levels as compared to CoS and MPLS EXP, which have 8 levels.
c. It is more extensible than Layer 2 markings because these markings are lost when media change.
d. All the above.
e. None of the above.

5. Traffic should be marked down using which RFC recommendations? (Select two.)
a. RFC 2957
b. RFC 2597
c. RFC 2698
d. RFC 2968

Index

Numbers

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z