Cisco IP Solution Center Quality of Service User Guide, 4.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-7647-01

Cisco IP Solution Center Quality of Service User Guide, 4.1

CONTENTS

FIGURES

About This Guide

This guide describes how to get started using the Quality-of-Service (QoS) management feature for Cisco IP Solution Center (ISC), 4.1.

This preface defines the following:

Audience

This guide is designed for service provider network managers and operators who are responsible for provisioning QoS policies within a service provider network. The network manager and operators should be familiar with the following topics:

- Basic concepts and terminology used in internetworking
- Quality of Service (QoS) terms and technology, both IP QoS and Ethernet QoS
- Network topologies and protocols, including knowledge of device capabilities

Organization

This guide contains the following chapters and appendixes:

- Chapter 1, “Introduction”
- Chapter 2, “Getting Started”
- Chapter 3, “Provisioning Process for IP QoS”
- Chapter 4, “Provisioning Process for Ethernet QoS”
- Chapter 5, “Managing and Auditing Service Requests”

- Appendix A, “Network Architecture and Service Model”
- Appendix B, “IP QoS Policy Parameters”
- Appendix C, “Ethernet QoS Policy Parameters”
- Appendix D, “Sample Configurations”
- Appendix E, “Metro Ethernet Use Cases”
- Index

Related Documentation

The entire documentation set for Cisco IP Solution Center, 4.1 can be accessed at:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1
The following documents comprise the ISC 4.1 documentation set.
General documentation (in suggested reading order):

- *Cisco IP Solution Center Getting Started and Documentation Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/docguide/index.htm
- *Release Notes for Cisco IP Solution Center, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/relnotes/index.htm
- *Cisco IP Solution Center Installation Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/install/index.htm
- *Cisco IP Solution Center Infrastructure Reference, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/infrastr/index.htm
- *Cisco IP Solution Center System Error Messages, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mess/index.htm

Application and technology documentation (listed alphabetically):

- *Cisco IP Solution Center L2VPN User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/l2vpn/index.htm
- *Cisco IP Solution Center MPLS VPN User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mpls/index.htm
- *Cisco IP Solution Center Quality of Service User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/qos/index.htm
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/tem/index.htm
- *Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/trble/index.htm

API Documentation:

- *Cisco IP Solution Center API Programmer Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_gd/index.htm
- Index: *Cisco IP Solution Center API Programmer Reference, 4.1*

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_ref/index.htm

Note All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

Technology-Related Documentation

- Packet Magazine White Paper - Deploying QoS in the Enterprise:

  http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac205/about_cisco_packet_feature09186a0080101513.html
- Reference Guide to Implementing Crypto and QoS:

  http://www.cisco.com/warp/public/105/crypto_qos.html
- QoS at a Glance:

  http://www.cisco.com/warp/public/784/packet/oct02/pdfs/qos.pdf
- MQC Based Frame Relay Traffic Shaping:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bc6.html
- QoS Classification and Marking:

  http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Introduction

This guide describes the Cisco IP Solution Center Quality of Service (ISC QoS) product, including features, graphical user interface, and the step-by-step procedures needed to perform various QoS-related tasks.

This chapter contains the following sections:

Overview

When network congestion occurs, all traffic has an equal chance of being dropped. Quality of service (QoS) provisioning categorizes network traffic, prioritizes it according to its relative importance, and provides priority treatment through various techniques. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

QoS classifies traffic by assigning class of service (CoS) values to frames at supported ingress interfaces. QoS implements scheduling on egress interfaces with transmit queue drop thresholds and multiple transmit queues that use CoS values to give preference to higher-priority traffic.

QoS manages bandwidth to assure the desired performance for network applications. For example, e-mail generally does not require high performance from a network, but real-time applications such as IP telephony or video streaming do. If the network is not consistently providing data flow control for these applications, the performance suffers.

Service provider network architecture contains access routers, distribution routers, core routers and ATM switches. The access routers terminate customer connections. The Cisco IP Solution Center (ISC) configures QoS at the access circuit, which involves the access router (called provider edge devices, or PEs) in the service provider network and the customer equipment (CE) in the customer network. A QoS policy is applied to the selected set of access circuits using a QoS service request.

In this document, Ethernet QoS refers to Metro Ethernet QoS, which now offers a wide array of features comparable with that of IP QoS.

There are three ways to provision QoS using ISC:

- IP QoS—Select the device interfaces, create a QoS policy and apply it to the specified device interfaces. IP QoS can be implemented independent of VPN services and is the most common method for QoS provisioning using ISC.

  IP QoS provisioning is described in Chapter 3, “Provisioning Process for IP QoS.”.

- IP QoS for MPLS VPN—Apply an MPLS VPN-aware QoS policy to an MPLS service request.

  IP QoS MPLS VPN is described in IP QoS for MPLS VPNs, page 3-28.

- Ethernet QoS—Select an L2VPN or VPLS service request that has already been deployed and apply QoS provisioning to that service request.

  QoS provisioning for MPLS VPN is described in IP QoS for MPLS VPNs, page 3-28.

A configuration trial in a lab setting is recommended.

This chapter describes the basic concepts for QoS as it is used in the ISC application.

How to Implement ISC QoS Effectively

QoS provisioning is a method for optimizing the flow of traffic in a network. If you have an enterprise network with services facilitated across a service provider MPLS infrastructure, QoS provisioning can guarantee that all applications receive the service levels required to meet expected performance in the network.

For complete QoS implementation you should identify:

- Low-latency applications (video and voice-over-IP, or VoIP) and mark them for high-priority treatment throughout the network
- Applications that require bandwidth guarantees should be marked and protected
- Applications that use more than their fair share of bandwidth can be identified and controlled

QoS is a collection of technologies that allows applications to request and receive predictable service levels in terms of bandwidth, latency variations, and delay.

Table 1-1 describes the typical QoS requirements for a multimedia network.

Table 1-1 Typical Multimedia QoS Requirements

Traffic Type	Max. Packet Loss	Max. One-way Latency	Max. Jitter	Guaranteed Priority Bandwidth Per Session
VoIP	1 percent	200 ms	30 ms	12 to 106 kbps*
Videoconferencing	1 percent	200 ms	30 ms	Size of the session plus 20 percent
Streaming Video	2 percent	5 seconds	N/A	Depends on encoding format and video stream rate.
Data	Variable	Variable	Variable	Variable

*Depending on sampling rate, codec, and Layer 2 overhead.

Voice and video applications are less tolerant of loss, delay, and delay variation (jitter) than data, but their QoS requirements are more obvious. Data applications vary widely in their QoS requirements, and should be profiled before you determine the appropriate classification and scheduling treatment.

QoS Components

There are three primary configuration components to IP QoS:

- Classification—Identifying and marking packets so that varying service levels can be enforced throughout the network.
- Scheduling—Assigning packets to one of multiple queues and associated service types based on classification for specific service level treatment by the network.
- Resource management—Accurately calculating the required bandwidth for all applications plus overhead.

In ISC, the QoS components used to achieve classification, scheduling, and resource management are:

- Predefined Ethernet QoS Policies, page 1-3
- Traffic Classification, page 1-5
- Marking, page 1-6
- Rate Limiting, page 1-7
- Traffic Shaping, page 1-8
- Congestion Management, page 1-8
- Congestion Avoidance (IP QoS only), page 1-9

Each of these components is described in the following sections.

Predefined Ethernet QoS Policies

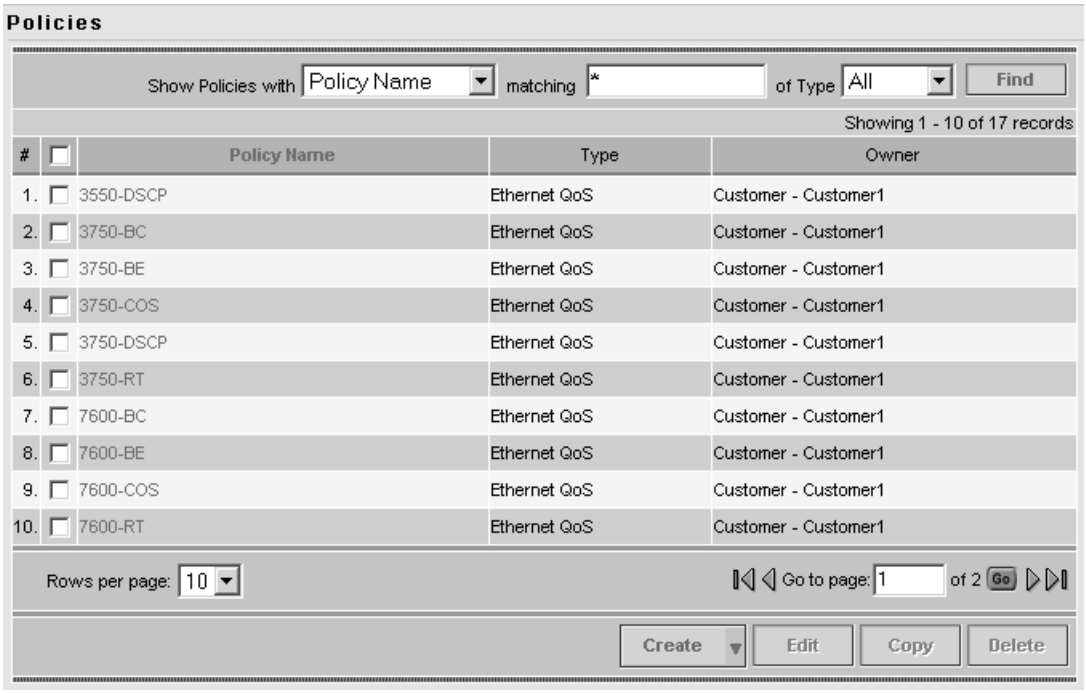
Predefined policies are only available for Ethernet QoS, not IP QoS.

The recommended way to provision Ethernet QoS using Cisco IP Solution Center is to use the predefined policies provided with Cisco IP Solution Center as a basis for new policies (if such are required).

The predefined policies correspond to typical Metro Ethernet cases on 3550, 3750-ME, and 7600 series routers. The use cases are described in Appendix E, “Metro Ethernet Use Cases.”

Figure 1-1 shows the predefined Ethernet QoS policies provided in the Policy Manager.

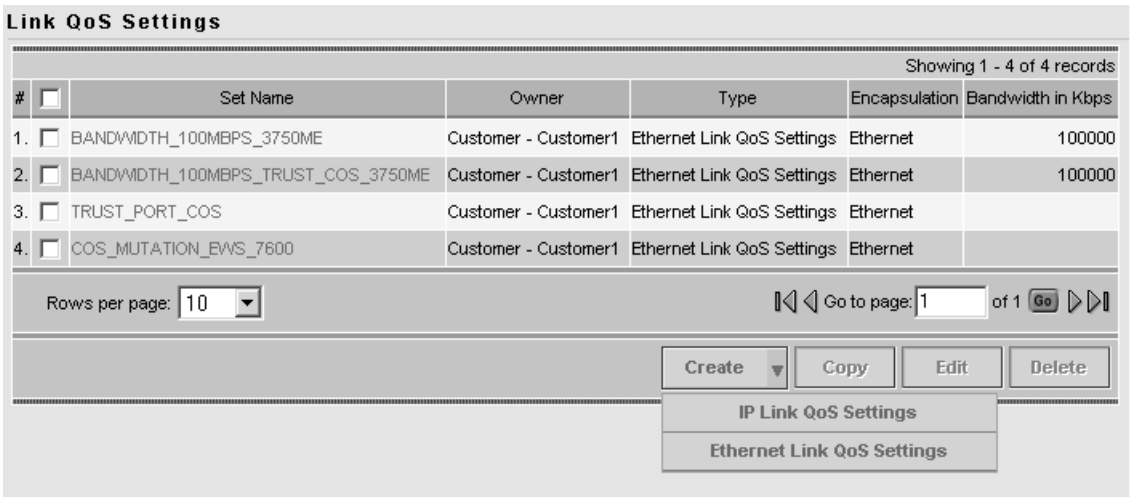
Figure 1-1 Predefined Policies in Cisco IP Solution Center



For a description of how the predefined policies are used to provision Ethernet QoS, see Chapter 4, "Provisioning Process for Ethernet QoS."

ISC QoS also offers four predefined Ethernet Link QoS policies. These are depicted in the Link QoS Settings window shown in Figure 1-2.

Figure 1-2 Link QoS Settings



For a description of how the predefined policies are used to provision Ethernet QoS, see Chapter 4, "Provisioning Process for Ethernet QoS."

Traffic Classification

Traffic classification (also called packet classification) partitions traffic into multiple priority levels, or classes of service.

For example, using the three precedence bits in the type of service (ToS) field of the IP packet header, you can categorize packets into a limited set of up to eight traffic classes (0 through 7). After you classify packets, you can use other QoS components to assign the appropriate traffic handling policies for each traffic class.

Packets can also be classified by external sources such as by a customer, or by a downstream network provider. You can either allow the network to accept the external classification, or override it and reclassify the packet according to the Ethernet QoS policy you specify in ISC.

The differences between IP QoS and Ethernet QoS when it comes to traffic classification are described below.

IP QoS

For IP QoS, ISC allows you to classify traffic based on source address, source port, destination port, port ranges, protocol ID, DSCP, IP Precedence values, routing protocols (RIP, OSPF, BGP or EIGRP), and transport protocols (FTP, http, telnet, SMTP, TFTP, or other user defined TCP or UDP protocol number or range).

ISC uses traffic classification to associate packets with a specific Classes of Service (Voice, Data, Management, etc.).

IP QoS has a default Class of Service. If you add a new Class of Service, it is always **Data**. Once you delete the Management, Routing, or VoIP class of service, it cannot be readded.

ISC provides five template service classes to use for traffic classification.

- VoIP
- RP (Routing Protocol)
- Mgmt (Management)
- Busin (Business-Data-1)
- BE (Best Effort)

A typical network uses three service classes in a QoS policy: a VoIP service class, a management service class (which is often combined with a routing protocol service class), and a data service class.

Ethernet QoS

For Ethernet QoS, you can classify traffic based on Class of Service (CoS), DSCP, and IP Precedence values.

ISC uses traffic classification to associate frames with a specific class of service (Routing, Business Critical, Best Effort, etc). There are no default Ethernet QoS Classes of Service.

- Real Time (RT)
- Business Critical
- Best Effort

For more information on traffic classification in service classes, see Service Level Ethernet QoS Policy, page A-15.

Marking

Marking is a way to identify packet flows to differentiate them. Packet marking allows you to partition your network into multiple priority levels or classes of service.

For IP QoS

ISC supports marking based on the following bits in the IP QoS type of service (ToS) byte for the packet:

- IP Precedence value
- IP differentiated services code point (DSCP) value
- MPLS Experimental (MPLS Exp) value

These markings can be used to identify traffic within the network, and other interfaces can match traffic based on the IP Precedence or DSCP markings. You can set up to 8 different IP Precedence markings (0 through 7) and 64 different IP DSCP markings (0 through 63).

IP Precedence and DSCP markings are used in the following QoS concepts:

- Congestion Management—Used to determine how packets should be scheduled.
- Congestion Avoidance—Used to determine how packets should be treated in Weighted Random Early Detection (WRED), a packet dropping mechanism used in congestion avoidance.
- Rate Limiting—Used to set the IP Precedence and DSCP values as well as the MPLS Exp. bit (imposition, top most) for packets entering the network. Networking devices within the network can then use the adjusted IP Precedence values to determine how the traffic should be treated based on the transmission rate.

MPLS Experimental Values (IP QoS)

Marking with the MPLS Exp. value in addition to standard IP QoS ensures the following:

- Standard IP QoS policies are followed before the packets enter the MPLS network.
- At the ingress router to the MPLS network (PE device), the packet's DSCP or IP Precedence value is mapped to the MPLS Exp. field. These mappings are part of the QoS policy.
- The DSCP or IP Precedence value in the IP header continues to be the basis for IP QoS when the packet leaves the MPLS network.

The MPLS Exp. bit setting directs packet behavior for QoS provisioning components, congestion management and congestion avoidance. It is updated automatically (copied from upper three bits of the ToS byte).

Note Marking packets with the MPLS Exp. value does not modify the DSCP/IP Precedence markings in the IP header.

For more information on marking with the MPLS Exp. value, see MPLS Experimental Values (IP QoS), page 1-6.

Ethernet QoS

In Ethernet QoS, marking can be enabled to work in one of the following two mutually exclusive ways:

- Set:
  - COS: Mark packets with 802.1p Class of Service Marking.
  - DSCP: Mark packets with a DSCP value.
    Note: You can mark packets with either DSCP or IP Precedence, but not both.
  - IP Precedence: Mark packets with an IP Precedence value.
- Trust—This is a way of defining which markings should be trusted in the QoS Policy. Thus, you can select Trust for either COS, DSCP, or IP Precedence.

IP Precedence and DSCP markings are used in the following concepts in Ethernet QoS:

- Congestion Management—Used to determine how packets should be scheduled.
- Rate Limiting—Used to set the IP Precedence or DSCP values for packets entering the network. Networking devices within the network can then use the adjusted IP Precedence values to determine how the traffic should be treated based on the transmission rate.

Rate Limiting

Rate limiting allows you to control the maximum rate of traffic sent or received on an interface. Rate limiting is configured on the CE and PE device interfaces at the edge of the network and limits traffic into or out of the network. Traffic that falls within the rate parameters is sent, while traffic that exceeds the parameters is dropped or sent with a different priority.

Note The traffic classification feature within the IP QoS policy actually creates a policer command. The interface aggregate rate-limiter in the Link QoS policy (also knows as the non-MQC feature, CAR, Committed Access Rate) creates a rate-limiting command.

ISC supports class-based rate limiting and interface-based aggregated rate limiting.

- Class-based rate limiting applies rate limiting parameters to an ISC service class.
- Interface-based aggregated rate limiting matches all packets, or a subset of packets, on an interface or subinterface and allows you to control the maximum rate of traffic sent or received. You can also specify traffic handling policies for traffic that either conforms to or exceeds the specified rate limits.
- Per-Port-Per-VLAN rate limiting for Metro Ethernet QoS

Rate limiting parameters in ISC include:

- Mean or peak rate
- Burst sizes
- Conform, exceed, and violate actions

For more information on configuring rate limiting IP QoS parameters in ISC, see Interface-Based Aggregated Rate Limiters, page B-31.

Traffic Shaping

Traffic shaping allows you to control the traffic exiting an interface to match its flow to the speed of the remote target interface and to ensure that traffic conforms to the policies assigned to it.

ISC supports class-based traffic shaping and aggregated traffic shaping.

- Class-based traffic shaping applies traffic shaping to an ISC service class.
- Aggregated traffic shaping applies these parameters to an interface instead of to a class of traffic.
- VLAN shaping for hierarchical QoS for the 3750-ME (Ethernet QoS only)

Specifying traffic shaping allows you to make better use of available bandwidth.

IP QoS traffic shaping parameters in ISC include:

- Average rate or peak rate for class-based traffic shaping
- Cell rates for ATM traffic shaping
- Rate factors for ATM traffic shaping
- Aggregated traffic shapers:
  - Frame Relay (FR) Traffic Shaper
  - FR Traffic Shaper (Non-MQC)
  - Parent-level Class-based Shaper
  - ATM Traffic Shaper (VBR-rt)
  - ATM Traffic Shaper (VBR-nrt)
  - ATM Traffic Shaper (CBR)
  - ATM Traffic Shaper (ABR)

Tip The difference between a rate limiter parameter and a traffic shaping parameter is that the rate limiter drops traffic in the presence of congestion, while a traffic shaper delays excess traffic using a buffer, or queueing mechanism.

For more information on configuring traffic shaping parameters in ISC, see Aggregated Traffic Shapers, page B-21.

Congestion Management

Congestion management controls congestion by determining the order in which packets are sent out on an interface based on priorities assigned to those packets.

Congestion management involves:

- Creating queues
- Assigning packets to those queues based on packet classification
- Scheduling packets in a queue for transmission

With congestion management, packets are scheduled for transmission according to their assigned priority and the queueing mechanism configured for the interface. The router determines the order of packet transmission by controlling which packets are placed in which queue and how queues are serviced with respect to each other.

The congestion management component of QoS offers different types of queueing techniques, each of which allows you to specify creation of a different number of queues, with greater or lesser degrees of differentiation of traffic, and to specify the order in which that traffic is sent.

Congestion management parameters in ISC include:

- Bandwidth
- Queue limits
- Priority queue

Congestion management parameters are configured at the service class level in ISC. For more information, see Service Level IP QoS Parameters, page B-1.

Congestion Avoidance (IP QoS only)

Congestion avoidance monitors network traffic loads in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks. Congestion management parameters provide preferential treatment for priority class traffic under congestion situations, while concurrently maximizing network throughput and capacity utilization and minimizing packet loss and delay.

ISC implements congestion avoidance parameters through packet dropping methods, such as WRED. WRED is used in combination with DSCP and IP Precedence and provides buffer management. WRED is frequently used to slow down TCP flows.

Congestion avoidance parameters are configured at the service class level in ISC. For more information, see Service Level IP QoS Parameters, page B-1.

CHAPTER 2

Getting Started

Starting QoS provisioning through the ISC GUI requires for certain steps to be completed.

First, examine the general system recommendations and requirements in the *Cisco IP Solution Center Installation Guide, 4.1* to determine if your environment is properly set up for running ISC.

Secondly, study the QoS specific prerequisites described in Prerequisites and Assumptions, page 2-1 in this chapter.

Finally, install the necessary licenses as described in this chapter.

This chapter contains the following sections:

Prerequisites and Assumptions

To implement QoS parameters for a network using the Cisco IP Solution Center (ISC) 4.1, you must have specific configuration information about the devices participating in QoS provisioning.

This section describes how to check your devices for QoS configuration prerequisites, lists configuration and implementation assumptions, describes how to preconfigure certain QoS parameters using the ISC properties file.

Review all prerequisites and assumptions before you implement QoS provisioning.

This section contains the following:

General Prerequisites

To install ISC, you are required to have the necessary license keys. License installation is described in Chapter 2, “Getting Started.”

To use the ISC user interface, you must be using Netscape Version 7.0 or later or Microsoft Internet Explorer, Version 6.0 or later.

See *Cisco IP Solution Center Installation Guide, 4.1* for general system recommendations.

Configuration Information and Assumptions

ISC requires that you have certain pieces of configuration information about the devices participating in QoS provisioning. This configuration information can be obtained by ISC through configuration collection.

This operation is described in *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Configuration Assumptions (IP QoS)

This section describes device configuration assumptions for QoS provisioning. Other system requirements are described in *Release Notes for Cisco IP Solution Center, 4.1*.

QoS provisioning requires that you enable Cisco express forwarding (CEF) or Distributed CEF (dCEF) on all CE and PE devices.

- CEF is an advanced, layer 3 switching technology inside a router. It defines the fastest method by which a Cisco router uses to forward packets from ingress to egress interfaces.
- CEF enables distributed forwarding on versatile interface processors (VIPs) in the Cisco 7500 series and high-performance line cards in the Cisco 12000 series.

Note For Cisco 7500 series routers, MQC supports VIP-based QoS only. Therefore, ISC supports 7500 series (Distributed) routers and not RSP-based 7500 series routers.

Implementation Assumptions

The QoS implementation model deployed in ISC is based upon the Differentiated Services (DiffServ) architecture. DiffServ describes a set of end-to-end QoS parameters that can be used in conjunction with Cisco IOS software, and allows the use of the differentiated service code point (DSCP) marking of the IP header. The DSCP header adds the capability of up to 64 service classes in a QoS policy.

ISC supports the following layer 2 encapsulations for QoS provisioning:

- Ethernet 802.1q (& QinQ)
- ISL
- HDLC
- PPP
- MLPPP
- Frame Relay
- ATM

ISC supports the following Cisco IOS command structures for QoS provisioning:

- Modular QoS CLI framework (MQC)—The Modular QoS CLI is a CLI structure that allows users to create traffic policies and attach these polices to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.
- Non-MQC commands —for the following QoS components in Cisco IOS software:
  - FRTS
  - FRF.12
  - CAR
  - LFI over MLPPP.

See the appropriate Cisco IOS documentation on Cisco.com for more information on Cisco IOS commands.

ISC QoS Setup and Installation

Before setting up ISC QoS, the ISC software must be installed. To do so, see *Cisco IP Solution Center Installation Guide, 4.1*.

To set up a new ISC QoS user, one or more users with a QoS role must be created. For step by step instructions and for an explanation of license keys in ISC, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

To install a QoS license, use the following steps:

Step 1 Make sure you have administrative priviliges to install licenses.

Step 2 Navigate **Administration** > **Control Center** > **Licensing**.

Step 3 Enter the QoS license key:

- Click **Install**.
- Enter the license key.
- Click **Save**.

Step 4 Log out as administrator.

Step 5 Log in as the user created above.

You are now ready to start using ISC QoS.

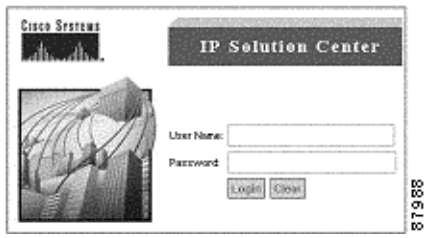
Launching the ISC GUI

To launch the ISC GUI:

Step 1 Open a web browser and enter the following URL to access the login screen (Figure 2-1):

http://<*hostname or IP address of ISC Interface server*>:8030/isc/login

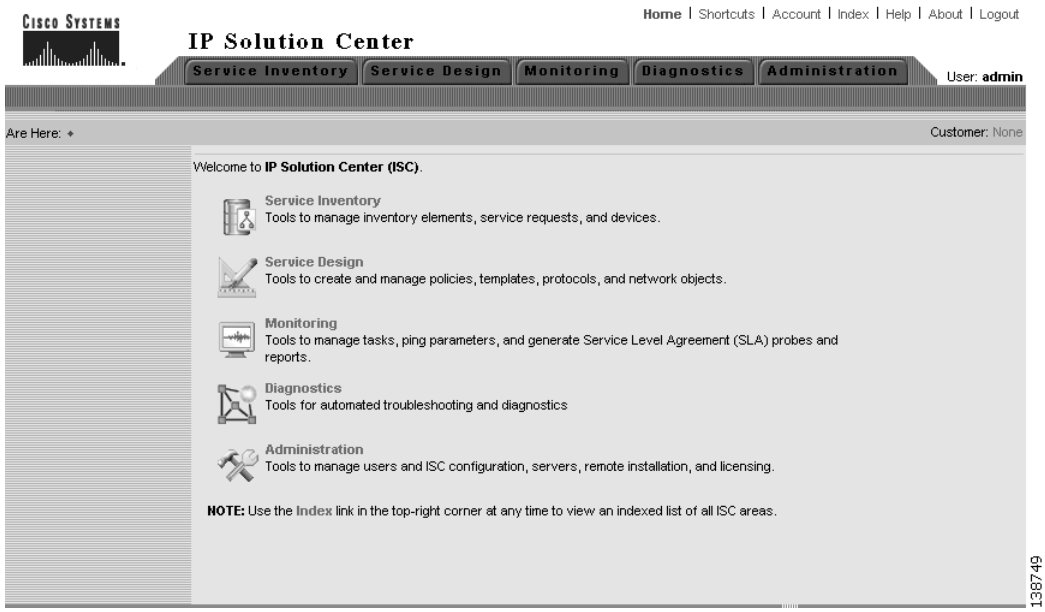
Figure 2-1 ISC Login Screen



Step 2 Enter your User Name and Password and click **Login**. Contact the network administrator if you cannot log into the ISC GUI.

Step 3 If the login is successful, the ISC home window appears (Figure 2-2).

Figure 2-2 ISC Home



The home window provides access to the five main areas of operation in ISC; Service Inventory, Service Design, Monitoring, Diagnostics and Administration.

For QoS provisioning, the two main areas of operation are:

- Service Inventory—In this area you can construct QoS service requests and deploy them to the network. Here, some distinction needs to be made between IP QoS and Ethernet QoS:
  - QoS provisioning in this area involves either defining QoS link endpoints and then manually selecting these defined endpoints during QoS service creation or using an existing MPLS service request for link definition (no need to define link endpoints). These operations are described in Creating QoS Link Candidate Objects, page 3-2 and IP QoS for MPLS VPNs, page 3-28 respectively.
  - For Ethernet QOS, the Service Inventory is used in a similar way but without editing of link endpoints. Existing Layer 2 services must be used for link definition (L2VPN or VPLS services).
- Service Design—QoS provisioning in this area includes creating a QoS policy and defining link level QoS settings. These operations are described in Creating IP QoS Policies, page 3-9 and Configuring Link-Level IP QoS Settings, page 3-15 for IP QoS and Creating Ethernet QoS Policies, page 4-3 and Configuring Link-Level Ethernet QoS Settings, page 4-9 for Ethernet QoS.

Note The ISC home window that appears depends on the licensed service packages you purchased.

QoS User Roles

ISC is designed so that different types of users can manage different aspects of the QoS provisioning process.

The roles available for your installation are listed under Administration > Security > User Roles.

There are two predefined QoS user roles that represent distinct levels of access permission:

- QoSRole—supports the ability to create both QoS Policies and QoS Services
- QoSServiceOpRole—only supports the ability to create QoS Services

You can also create new user roles. How to manage user roles is described in *Cisco IP Solution Center Infrastructure Reference, 4.1.1*

Provisioning Process for IP QoS

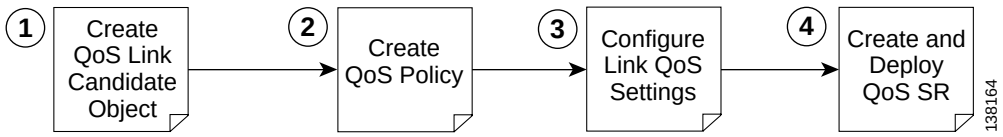
This chapter describes the steps required to provision IP QoS for a network using the Cisco IP Solution Center (ISC) graphical user interfaces.

This chapter describes how to set up IP QoS provisioning independent of VPN services. To set up QoS provisioning for MPLS VPN services, see IP QoS for MPLS VPNs, page 3-28.

The chapter contains the following sections:

IP QoS Process Model

Figure 3-1 Process Flow for IP QoS Provisioning



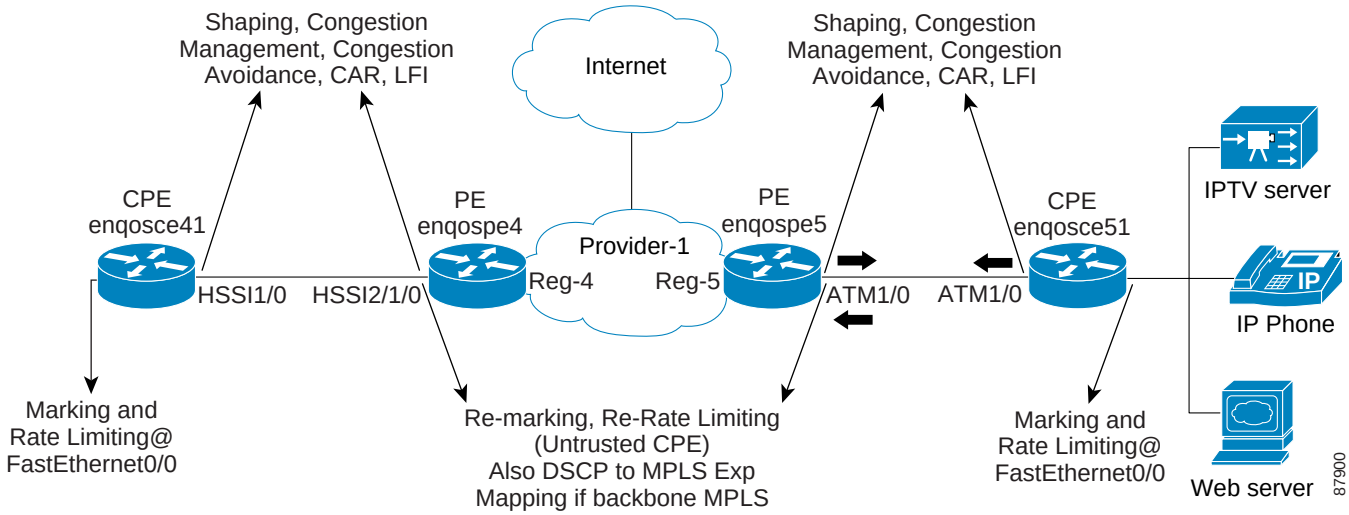
The QoS process model in ISC is designed so that different types of users (for example, network administrators and service operators), can define different aspects of the QoS provisioning process.

The IP QoS provisioning process in ISC is illustrated in Figure 3-1 and includes four operations:

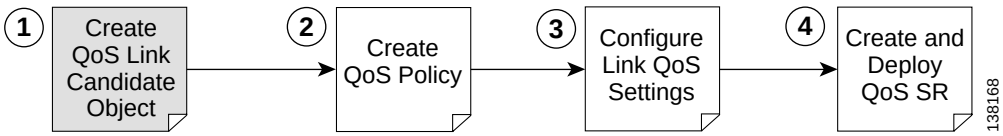
1. Creating QoS Link Candidate Objects—Identifying device interfaces for QoS provisioning
2. Creating IP QoS Policies—QoS policy based on service classes
3. Configuring Link-Level IP QoS Settings—QoS parameters that are sensitive to link bandwidth and Layer 2 encapsulation.
4. Creating and Deploying IP QoS Service Requests—Create a container for the QoS policy and QoS link settings and apply these parameters to the devices in the service provider network.

The rest of this chapter guides you through the QoS provisioning process using the ISC user interface. For each operation, a screen shot and example values for each entry field are provided. For reference, all examples in this chapter see the following network configuration (Figure 3-2).

Figure 3-2 Example of QoS Policy Deployment



Creating QoS Link Candidate Objects



Before you can provision QoS commands on a network device, you must select the device interfaces as QoS candidates. For more information on determining which device interfaces might be congestion points and might benefit from QoS provisioning, see IP QoS Provisioning Strategies, page A-9.

In the ISC GUI, the process of selecting device interfaces is called defining QoS link candidates.

You can use the Service Inventory tab to identify the device interfaces to be used for QoS provisioning. The device interfaces are either link end-points or mark/rate interfaces, and when selected, these device interfaces become QoS link candidates to be used later in the QoS service request (Step 4).

For QoS provisioning, you must select both interfaces in the CE-PE link. A typical device interface selection is as follows:

- For the CE device:
  - The provider-facing device interface is selected as the link endpoint
  - The customer-facing LAN interface is selected for marking and rate limiting

Note Marking and rate limiting on the customer-facing LAN interface is optional.

- For the PE device:
  - The customer-facing interface is selected as a link endpoint

The interfaces selected as link endpoints can be provisioned with QoS parameters such as policing, traffic shaping, congestion management, congestion avoidance, link efficiency, and CAR. You apply these parameters later in the provisioning process.

This section describes how to use the ISC GUI to select device interfaces as QoS candidates and includes:

- Selecting CE Device Interfaces for QoS, page 3-3
- Selecting PE Device Interfaces for QoS, page 3-6

Selecting CE Device Interfaces for QoS

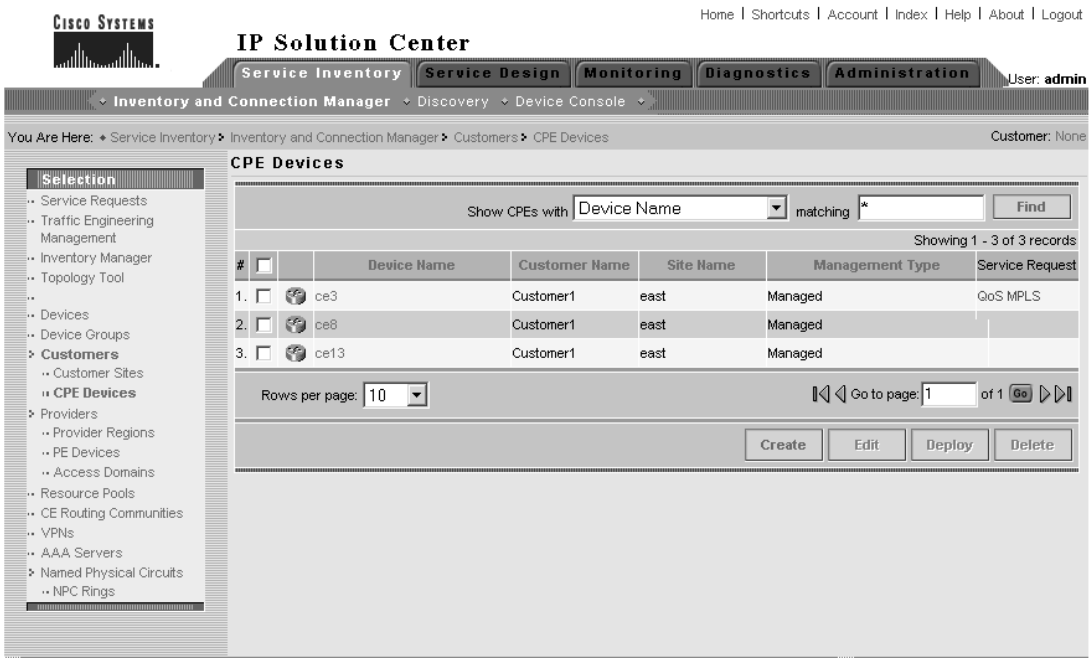
Typically, the service provider supplies the list of devices and interfaces to be selected for QoS provisioning. This section describes how to select device interfaces for QoS.

To select interfaces in a CE device for QoS:

Step 1 On the Service Inventory tab, click **Inventory and Connection Manager**. The left pane of the CE devices window shows the TOC for this operation area and an icon in the right pane shows a graphical representation and short description. You can access an area of operation from either the TOC link or the icon link.

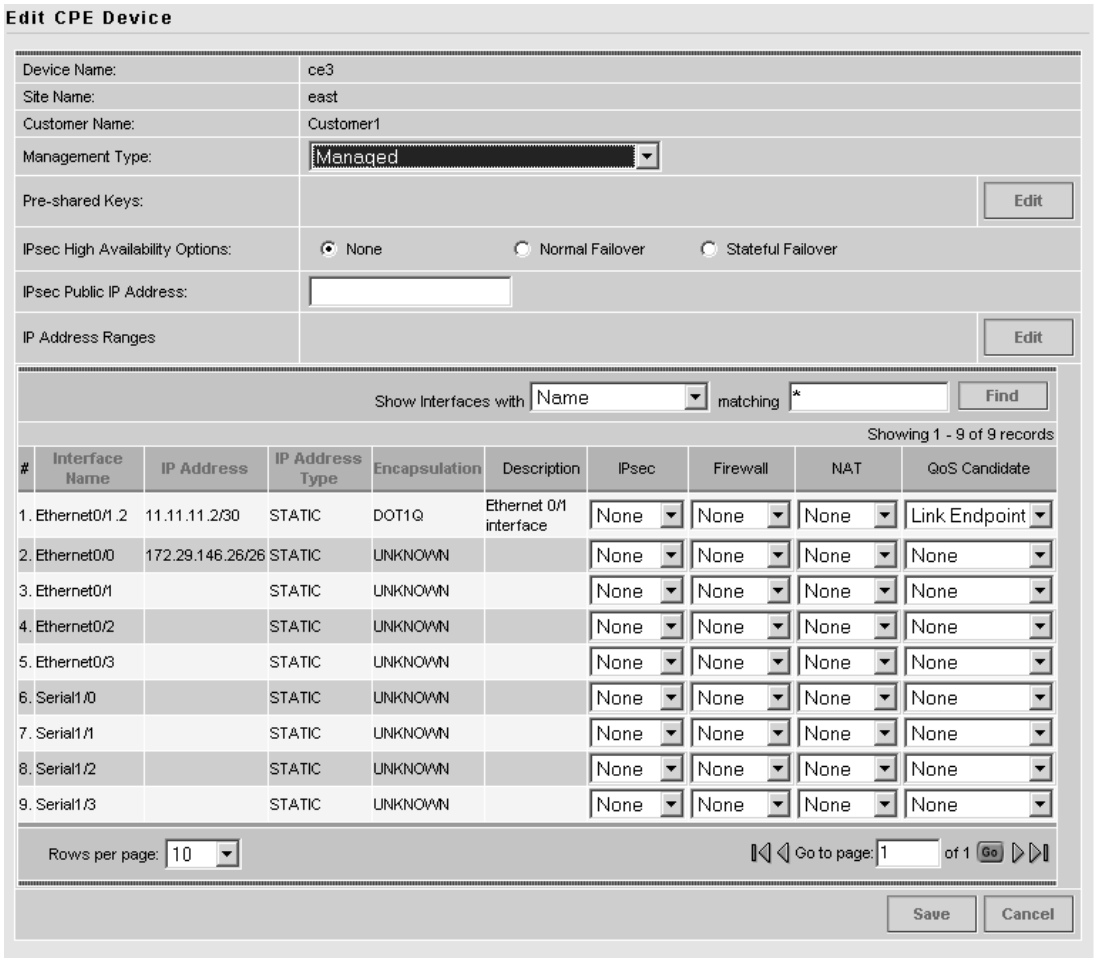
Step 2 From the TOC, click **CE Devices**, which is located under Customers in the hierarchy pane. This displays the CE Devices window and lists all CE devices that can be edited (Figure 3-3).

Figure 3-3 CE Devices List



Step 3 Select the check box next to the CE device (for example, ce3) and click **Edit**. The Edit CPE Device window appears (Figure 3-4). This window lists device details and all interfaces that might be candidates for QoS provisioning.

Figure 3-4 Identify CE Device Interface as QoS Candidate



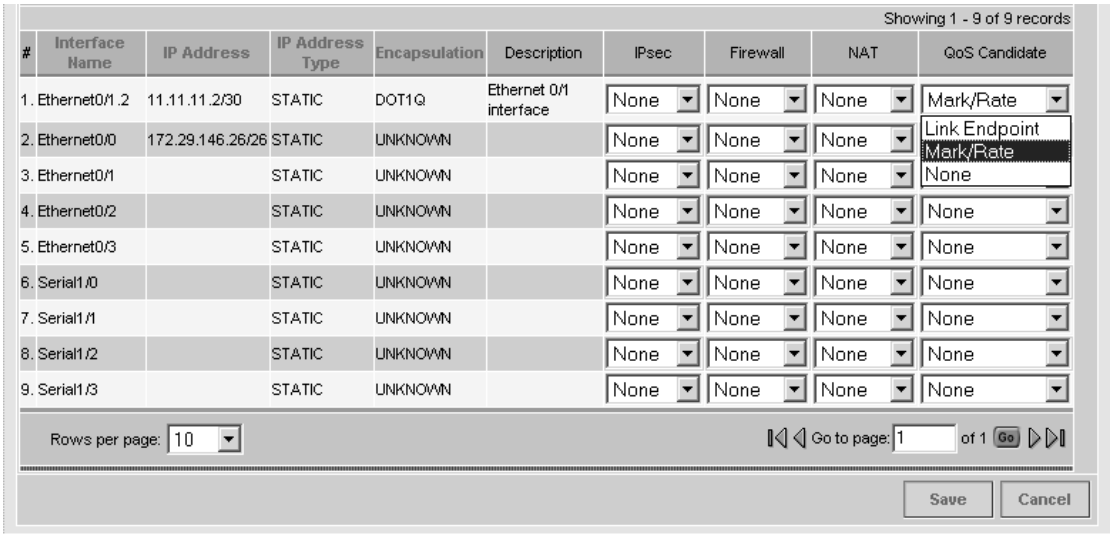
Step 4 Select the device interface for QoS provisioning. Select **Link Endpoint** from the QoS Candidate drop-down menu. This selects the interface on this CE device as a link endpoint for QoS provisioning.

For information on the other entry fields in the Edit CPE Device window, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Step 5 For the same CE device, select the customer-facing LAN interface. Select **Mark/Rate** from the QoS Candidate menu (Figure 3-5). This selects the interface on this CE device for marking and rate limiting.

Note Step 5 is optional, but recommended. If you bypass Step 5, the interface selected in Step 4 is used for marking and rate limiting.

Figure 3-5 Identify Customer-Facing LAN Interface as QoS Candidate



Step 6 Click **Save**. This saves the QoS interface information for the CE device.

Step 7 Repeat Steps 1 through 4 for each CE device that requires QoS provisioning. For each CE device, specify the provider-facing interface as the QoS Candidate Link Endpoint, and specify the Mark/Rate parameter for the corresponding customer-facing LAN interface.

For the network example, mark CE device enqosce51 with interface ATM1/0.52 defined as the QoS Candidate Link Endpoint, and FastEthernet 0/0 as the customer-facing LAN interface to be edited for Mark/Rate Limit.

Selecting PE Device Interfaces for QoS

You must also mark the PE device in the CE-PE link for QoS provisioning. Typically, the PE device is marked for QoS parameters at the customer-facing interface.

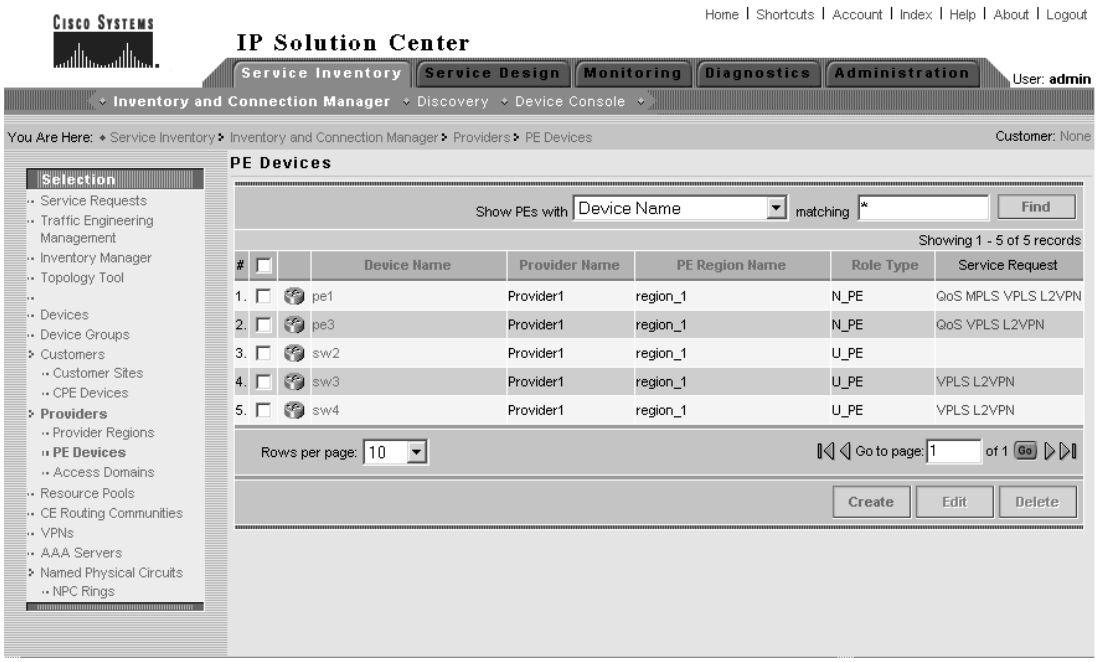
Note If you have an untrusted CE, one that is not managed or only partially managed by ISC, you can also re-mark and re-rate limit at the PE interface. Re-marking and re-rate limiting for PE devices is provisioned within the service class policy. See Creating the Service Level IP QoS Policy, page 3-9.

To mark a PE device:

Step 1 On the Service Inventory tab, click **Inventory and Connection Manager**.

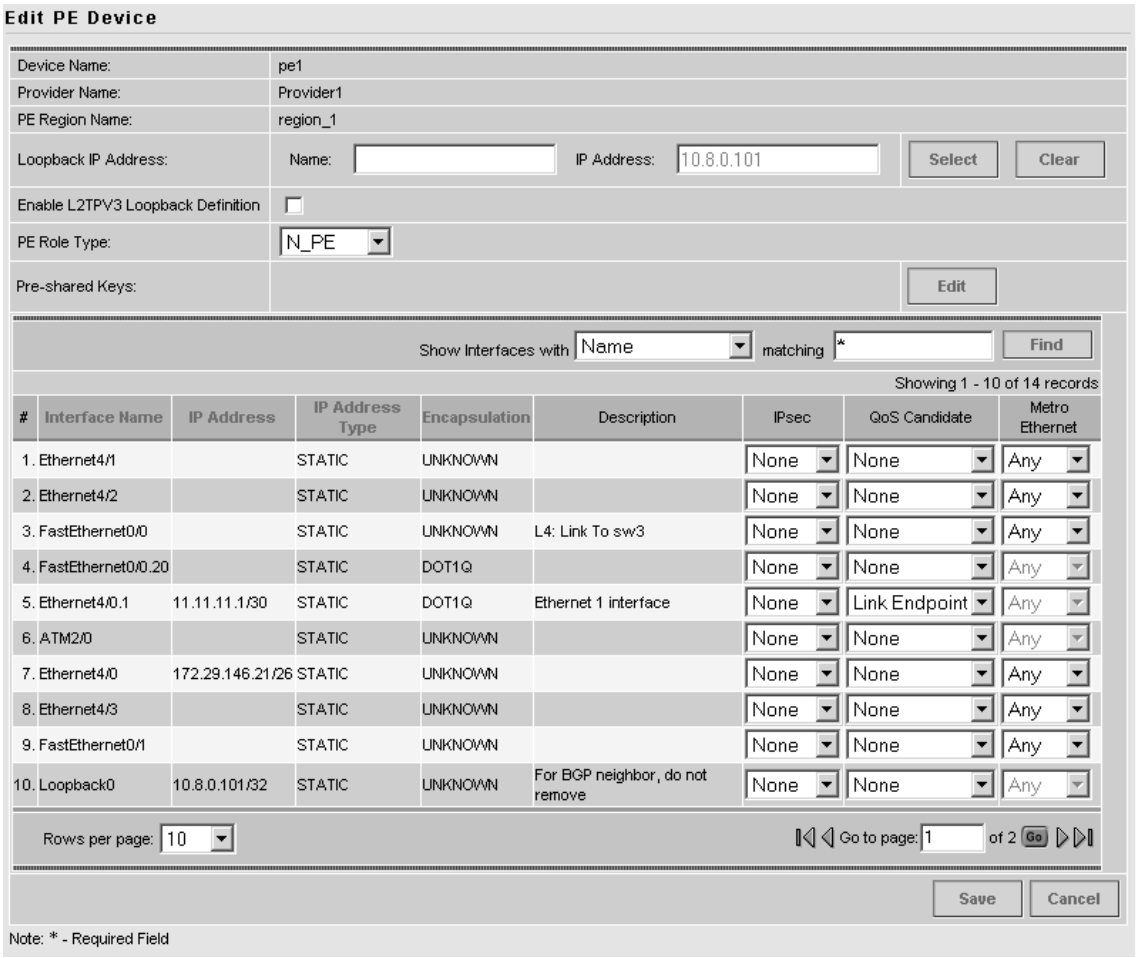
Step 2 From the TOC, select **PE Devices**, which is located under Providers in the hierarchy pane. This displays the PE Devices window and lists all PE devices that can be edited (Figure 3-6).

Figure 3-6 PE Devices List



Step 3 Select the check box next to the PE device (for example, pe1) and click **Edit.** The Edit PE Device window appears (Figure 3-7). This window lists device details and all interfaces that might be candidates for QoS provisioning.

Figure 3-7 Identify PE Device Interface as QoS Candidate



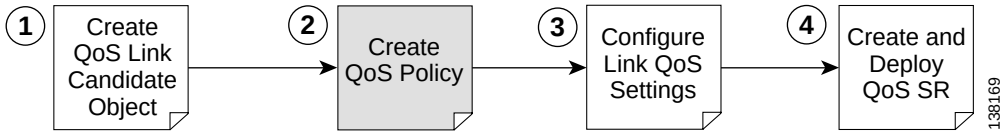
Step 4 Select the interface (for example Ethernet4/0.1) for QoS provisioning. Select **Link Endpoint** from the QoS Candidate menu. This marks the interface on this PE device as a link endpoint for QoS provisioning.

Step 5 Click **Save**. This saves the QoS interface information for the PE device.

Step 6 Repeat Steps 1 through 3 for each PE device that requires QoS provisioning. For each device, specify an interface as the QoS Candidate Link Endpoint.

For the network example, mark PE device enqosce5 with interface ATM1/0.52 defined as the QoS Candidate Link Endpoint.

Creating IP QoS Policies



A QoS service policy is divided into two policy categories; service level policies and link level policies. Most networks have a combination of both policy types.

These two parts of the ISC QoS policy are managed in different parts of the user interface.

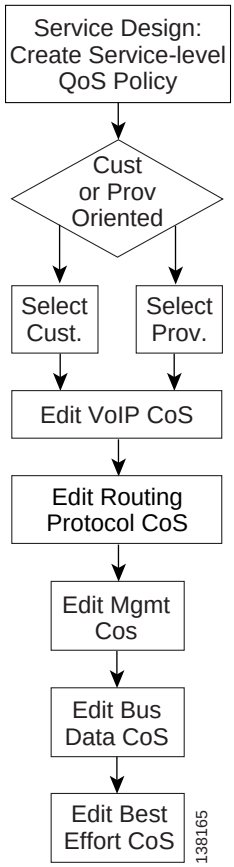
- The service-level QoS policy is managed using **Service Design > Policies**.
- The link-level IP QoS policy is managed using **Service Design > Link QoS**.

This section describes how to create a IP QoS service-level policy using the ISC GUI. The process of creating a link-level QoS Policy is described in Configuring Link-Level IP QoS Settings, page 3-15.

Creating the Service Level IP QoS Policy

This section describes how to create a service level IP QoS policy.

Figure 3-8 IP QoS: Create a Service Level QoS Policy



The IP QoS policy is the set of rules or conditions that apply to packets as they come across each interface that has been assigned as a link endpoint. This set of rules is defined in a QoS service class.

A typical IP QoS policy consists of at least three service classes. ISC provides, by default, five different services class templates to use or modify.

- VoIP—VoIP
- RP—Routing Protocol
- Mgmt—Management
- Busin—Business Data
- BE—Best Effort

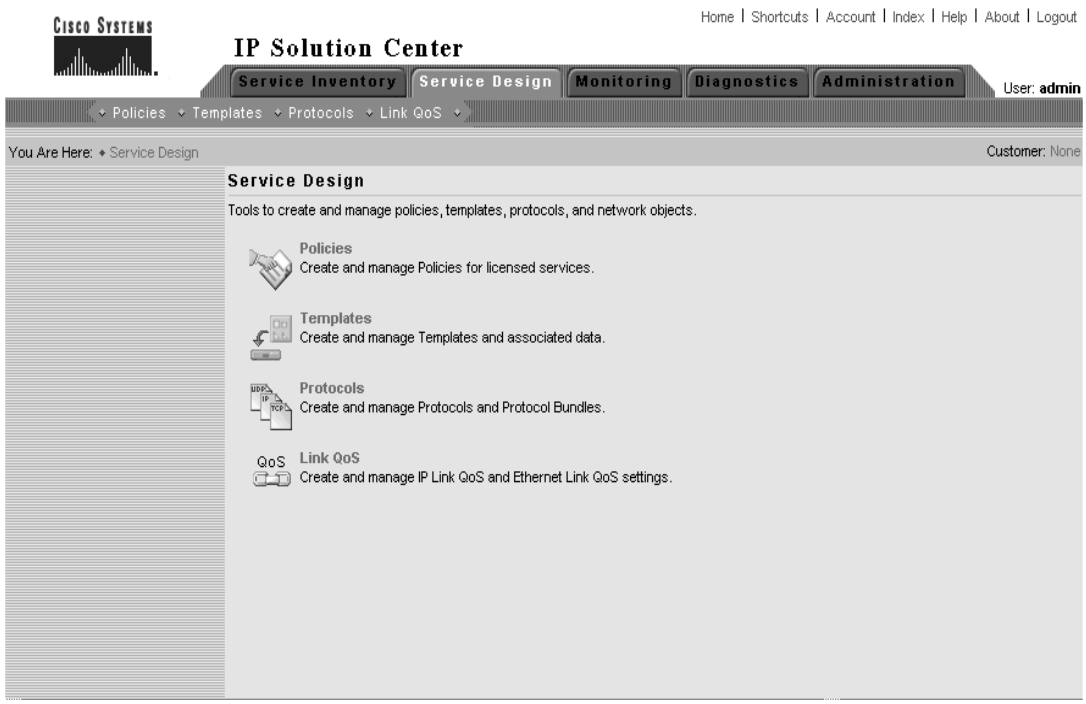
Select the service classes to use in the QoS policy and edit each one with the required parameters. All service classes except the Voice Class of Service require that you enter at least the bandwidth. You can also delete an unused service class, change the order of the service classes, or add another data service class, if needed.

The following sections describe how to create the service class portion of an IP QoS Policy using the ISC user interface. For detailed information on the entry fields for each service class parameter, see Appendix B, “IP QoS Policy Parameters.”.

To create an IP QoS policy:

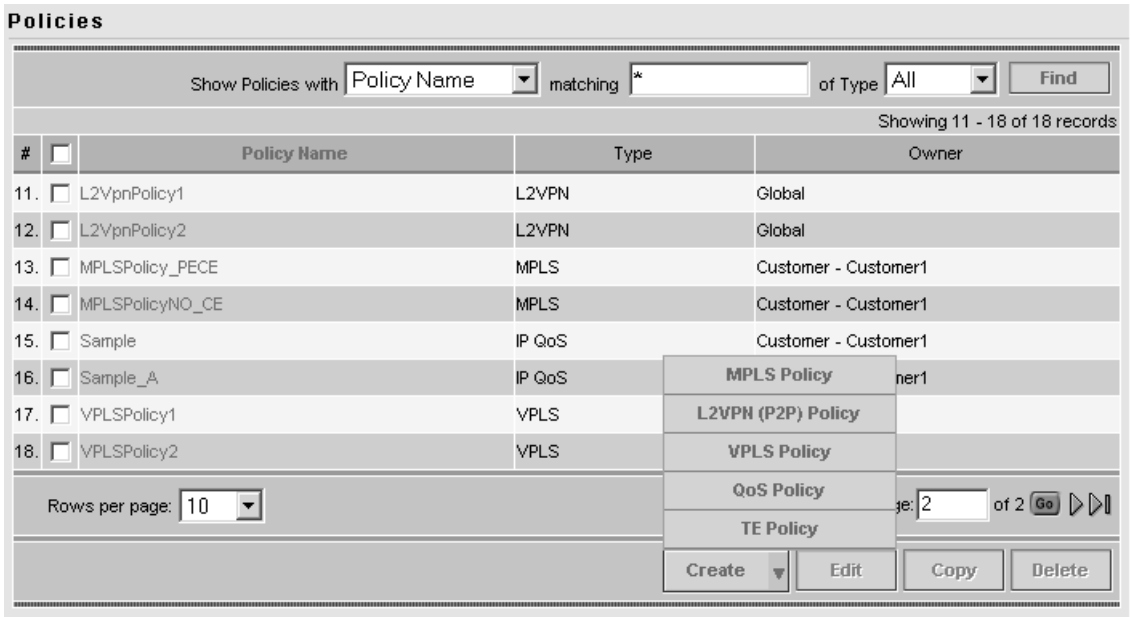
Step 1 On the ISC home page, select the Service Design tab. The Service Design window in Figure 3-9 appears.

Figure 3-9 Service Design



Step 2 Select Policies to open up the Policies window (Figure 3-10).

Figure 3-10 Policies



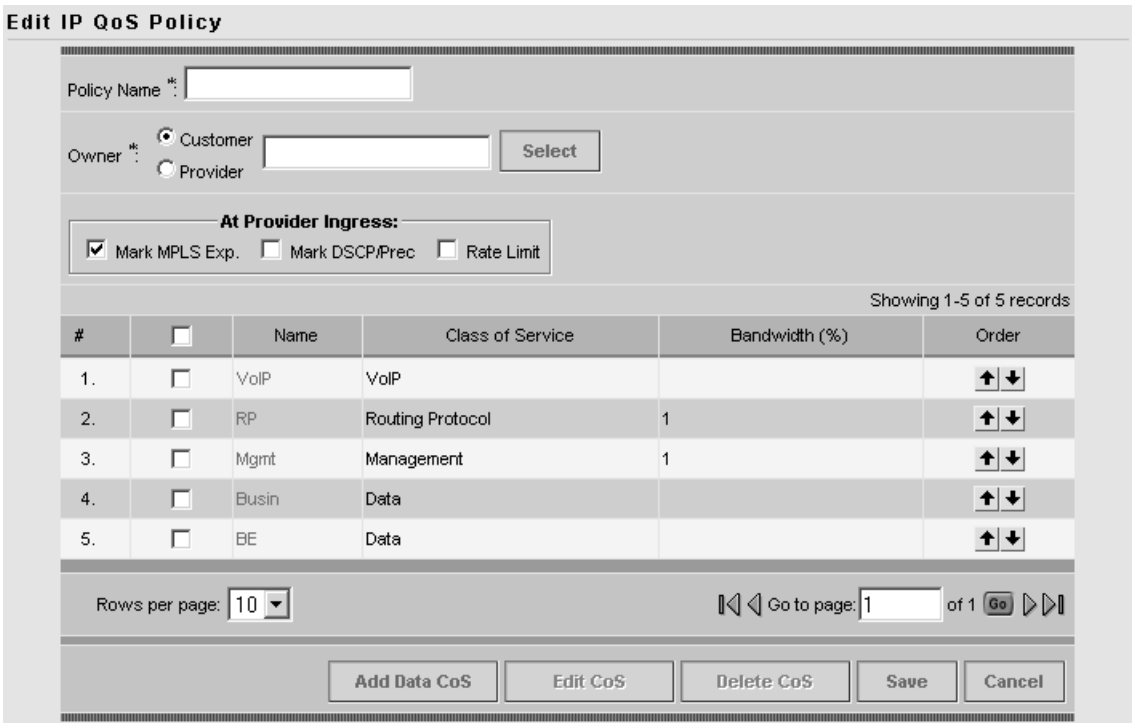
The Policies window lists all policies that currently exist for the different ISC services. Use this window to make changes to an existing policy, or to delete an unwanted service policy.

Step 3 Click **Create** and select **QoS Policy** from the menu. The Qos Policy Creation window appears (Figure 3-11).

Figure 3-11 Create QoS Policy

Step 4 Select **IP QoS** from the TOC at left. The Edit IP QoS Policy window appears (Figure 3-12).

Figure 3-12 Edit IP QoS Policy



The Edit IP QoS Policy window lists the policy name, the customer or provider for this policy, and displays the five recommended default service classes. Use this window to select and edit the service classes to use in the QoS policy.

In addition to the service classes, you can re-mark or add re-rate limiting parameters to a PE device using the following check boxes.

- **Mark MPLS Exp.**—Select this check box to enable an MPLS Exp check box to appear in the traffic classification section of the Voice and Data Class of Services. Use this parameter when provisioning QoS for a PE device that is in an MPLS network.
- **Mark DSCP/Prec**—Select this check box to cause ISC to generate class-map/policy-map commands that reclassify the traffic and remark the traffic on the PE in the same manner as on the ingress of the CE. Use this parameter to mark traffic based on the IP DSCP or precedence value.
- **Rate Limit**—Select this check box to cause ISC to apply both an ingress and egress rate-limiting command on the PE link endpoint. Enable this parameter if the CE is an untrusted device. An untrusted CE is a device that is either not managed by ISC or only partially-managed by ISC.

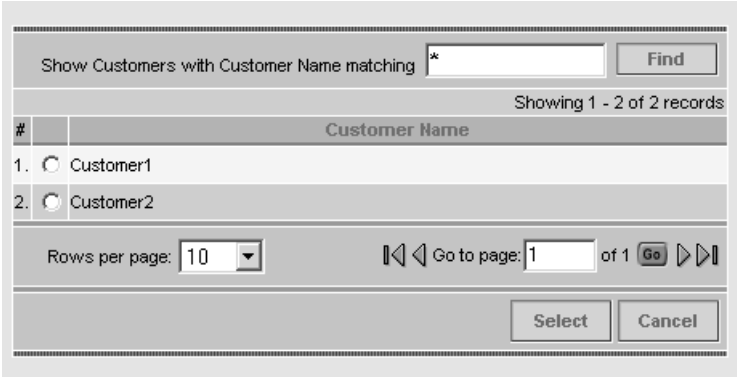
Step 5 In the Edit IP QoS Policy window, enter the **Policy Name**. Select a policy name that is easily identified for your network. For example, if your customer is CustomerA, the policy name might be A-QoS.

Note We recommend that you use short customer names, policy names, and class-of-service names inside a QoS Policy. ISC combines the customer name and the QoS policy name to provision the policy-map command. Further, ISC combines the customer name, policy name, and class-of-service name to provision the class-map command. IOS has a limit of 40 characters for both policy-map and class-map command names. When the combination exceeds 40 characters, ISC attempts to truncate the combination and this might lead to service request deployment problems.

Step 6 Choose an Owner (Customer or Provider) for this QoS policy. Click the appropriate radio button and then **Select**.

Step 7 In the Customer (or Provider) for QoS Policy popup, select the customer (provider) and click **Select** (Figure 3-13).

Figure 3-13 Select Customer for QoS Policy

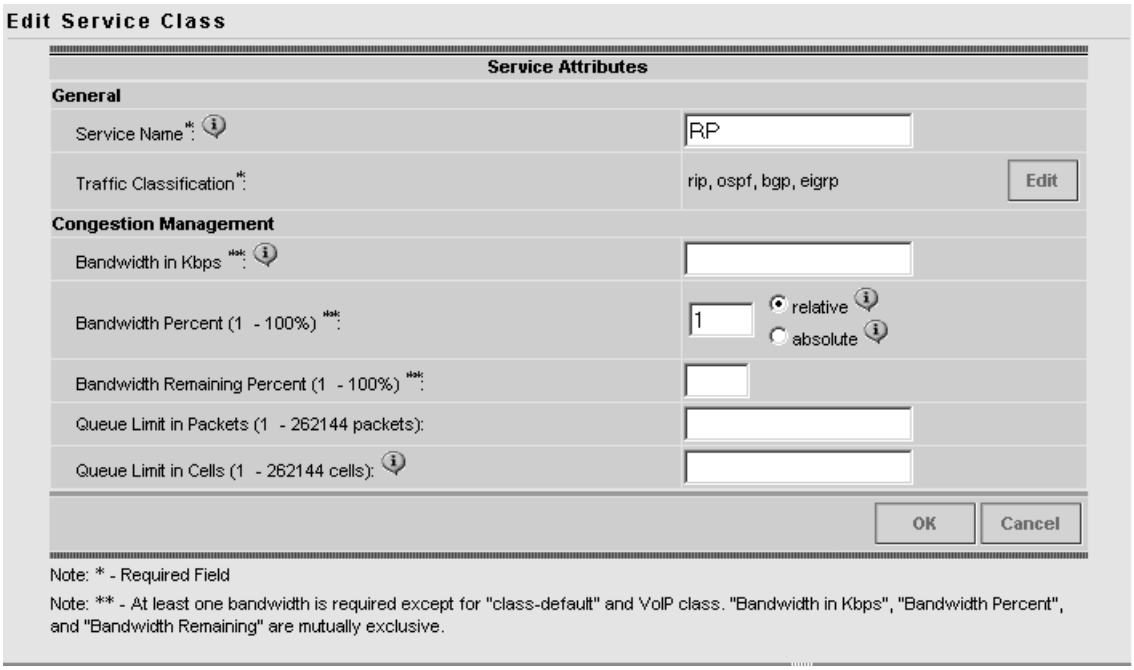


This identifies the customer for the QoS policy. You return to the Edit IP QoS Policy window.

The next step in defining the service level QoS policy is to edit the service classes. You can apply one or more service classes to the QoS policy. Edit the default service classes provided by ISC, delete the unwanted service classes, and add a data service class if necessary. A typical QoS policy consists of 3 service classes; VoIP, Management, and a data service class, such as Best Effort.

Step 8 To apply a service class to an IP QoS policy, select the class of service and click **Edit CoS**. The Edit Service Class window appears (Figure 3-14).

Figure 3-14 Edit Service Class—Routing Protocol



Step 9 From the Edit Service Class window, enter the QoS parameters, or service attributes, to apply to this service class and click **OK**.

Depending on the service class you are editing, you receive the appropriate window. For a detailed explanation of the entry fields for this service class and the windows for the other service classes, see Service Level IP QoS Parameters, page B-1.

Step 10 Repeat Steps 7 and 8 for all services classes that you want applied to your QoS policy.

To change the processing order of the service classes, use the up and down arrow keys on the Edit IP QoS Policy window. The service class policies are applied to the network devices in the order they are presented on the Edit IP QoS Policy window.

Step 11 Add another service class, if required. See Adding a Data Service Class, page B-20.

Step 12 Delete any service classes that you do not require for this QoS Policy. See Deleting a Service Class, page B-20.

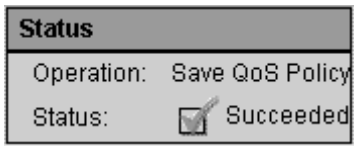
Step 13 After you edit and apply the required service classes, click **Save** to save the Qos Policy.

Note All service classes except Voice Class of Service require that you specify a bandwidth before you save the QoS Policy.

When you save an IP QoS policy, a status information box is displayed on the bottom left of the ISC window. The following examples show the different status messages and user action required, to correct any problems.

a. Save succeeded. No further action is required. (Figure 3-15).

Figure 3-15 Save is Successful

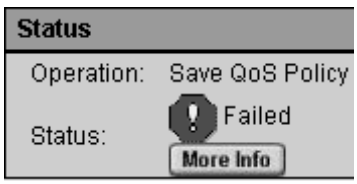


b. Policy is in use and cannot be edited (Figure 3-16). To read the warning message, click **More Info** and take the necessary action to resolve the issue.

Figure 3-16 Edit QoS Policy with Warning

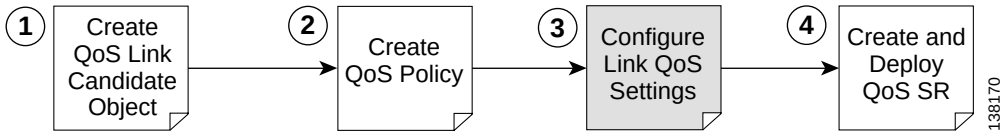
c. Save QoS policy failed (Figure 3-17). Click **More Info** to determine the source of the problem. You must fix all errors and resave before you can continue.

Figure 3-17 Save Unsuccessful



Note Not all devices and Cisco IOS platforms support all QoS parameter options.

Configuring Link-Level IP QoS Settings



The second part of an ISC IP QoS policy is the link level policy, also called the link QoS setting. The link QoS setting describes the specific CE-PE link QoS parameters to use.

The link QoS setting is a group of QoS parameters that are sensitive to link bandwidth and the CE-PE link's layer 2 encapsulation type. Typically, a service provider requires several different link QoS settings, one for each link bandwidth.

Link QoS settings are associated with each link in the QoS Service Request. For each CE-PE link in the QoS service request, you can have one corresponding link QoS setting.

Link QoS Policy

Use the Link QoS policy to configure the link-specific QoS information.

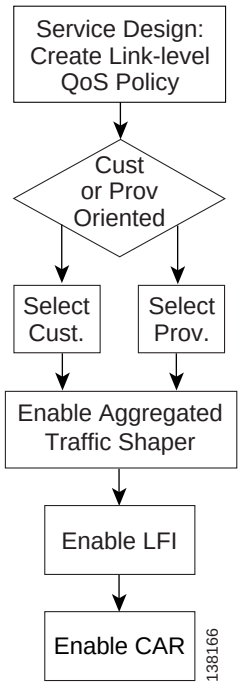
Create the link QoS setting using the Link QoS operation area of the ISC GUI. The Link QoS policy allows you to create and manage the following link QoS settings:

- IP Link QoS Settings—Specify the QoS settings to apply to the link, such as aggregated traffic shaping and aggregated rate limiting. You also use the IP Link QoS Settings to specify Link Efficiency Settings, or LFI and interface-based aggregated rate limiting (also known as CAR, Committed Access Rate).

Creating a Link QoS Setting

This section describes how to create a link QoS setting for a network.

Figure 3-18 Creating a Link IP QoS Setting



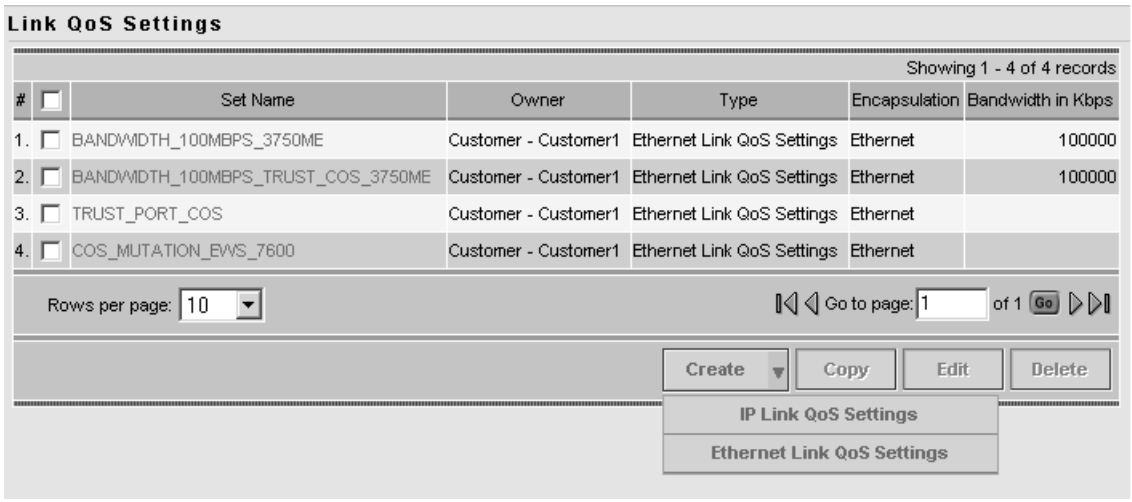
To create the link QoS setting:

Step 1 On the Service Design tab (Figure 3-19), click **Link QoS**.

Figure 3-19 Service Design

Step 2 The Link QoS Settings window appears (Figure 3-20).

Figure 3-20 Link QoS Settings



Step 3 The Link QoS Settings window displays the current link QoS settings available for QoS service requests, including the following information about each link QoS setting:

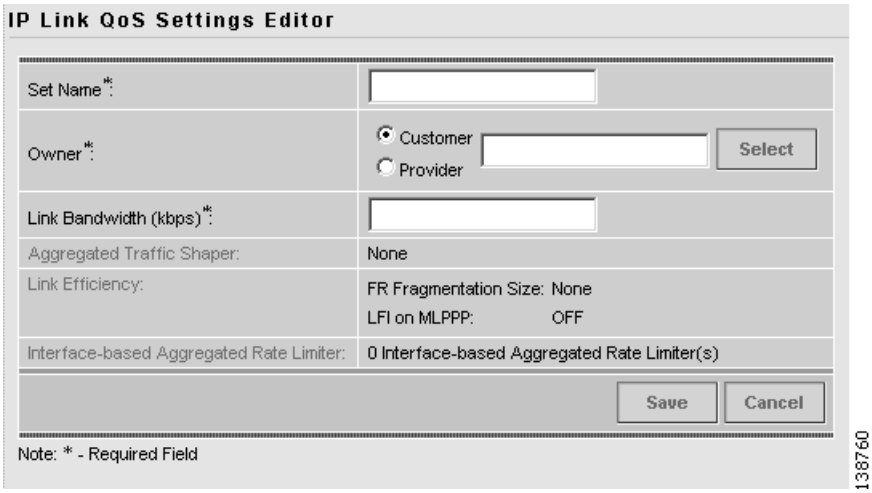
- **Set Name**—The name of your link QoS setting

- **Owner**—Customer or provider
- **Type**—IP Link Setting
- **Encapsulation**—Layer 2 encapsulation type.
- **Bandwidth in Kbps**—Enter this value manually. For IP Link QoS Settings only.

You can select an existing link QoS setting or create a new one. For the network example, create a new IP Link QoS setting.

Step 4 Click **Create** and select **IP Link QoS Settings** in the drop-down list. The IP Link QoS Settings Editor window appears (Figure 3-21).

Figure 3-21 IP Link QoS Settings Editor



Step 5 Enter the values in the IP Link QoS Settings Editor window. The entry fields are described in Table 3-1.

Table 3-1 IP Link QoS Settings Editor Entry Field

Entry Field	Description
Set Name	The name of the link QoS settings. Specify a name that describes the service offered by the settings. For example: Frame_64K_Gold; ATM_2Mb_Silver. The name Frame_64K_Gold indicates that this set should be used on a CE-PE link of bandwidth 64kbps, whose layer-2 encapsulation is Frame Relay and to meet an SLA of Gold.
Owner (Customer or Provider)	Click **Select** to choose from a list of customers or providers.
Link Bandwidth	This is a required field. The link bandwidth specifies the maximum amount of bandwidth allocated for packets belonging to this link.
Aggregated Traffic Shaper	Applies traffic shaping QoS parameters to the device interface. Click **Aggregated Traffic Shaper** to set these parameters. Use this method instead of applying traffic shaping parameters with a service class. For more information on the parameters for aggregated traffic shaping, see Aggregated Traffic Shapers, page A-7.

Table 3-1 IP Link QoS Settings Editor Entry Field

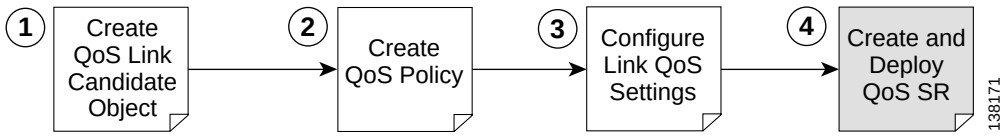
Entry Field	Description
Link Efficiency	Click **Link Efficiency** to set these parameters. For more information on the link efficiency parameters, see Link Efficiency Settings, page B-30.
Interface-based Aggregated Rate Limiter	This provides rate limiting for the traffic on a particular interface for the CE-PE link. Click **Interface-Based Aggregated Rate Limiter** to set these parameters. For more information on the interface-based aggregated rate limiter parameters, see Interface-Based Aggregated Rate Limiters, page B-31.

Step 6 Click **OK**.

Step 7 Repeat Steps 1 through 7 to add more IP Link QoS settings. Link QoS settings are associated with each CE-PE link in the QoS Service Request. For each link in the QoS service request, you can optionally have one corresponding link QoS setting.

Step 8 Click **Save** to save the IP Link QoS settings.

Creating and Deploying IP QoS Service Requests



After both the service level and the link level QoS polices are created, the final steps in the QoS provisioning process are to create and deploy a QoS service request.

A QoS service request contains one or more QoS links. A QoS link can contain two interfaces (CE-PE link) or just one interface (CE only or PE only). Each link can optionally be associated with a QoS link setting. A QoS policy can be associated with a QoS service request.

A QoS service request should:

- Contain a QoS policy
- Contain QoS links

All QoS links in the service request can optionally be associated with a link QoS setting

To apply QoS policies to network devices, you must deploy the QoS service request.

When a QoS SR is deployed (commissioned), the provisioning engine (besides uploading the latest configs) will determine the device/linecard and IOS version associated with the target device (both CE and PEs). This information will determine the QoS feature set that is supported by the device/linecard. Armed with this feature set, a delta config is created (comparing the existing repository with the latest upload) to satisy the service request.

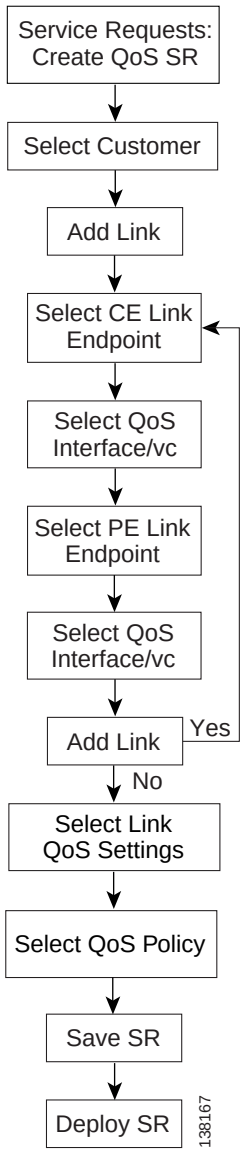
This section describes how to use the ISC GUI to create and deploy an IP QoS service request and includes:

- Creating an IP QoS Service Request, page 3-20
- Deploying an IP QoS Service Request, page 3-26

Creating an IP QoS Service Request

This section describes how to create a QoS service request, independent of VPN services.

Figure 3-22 Create an IP QoS Service Request



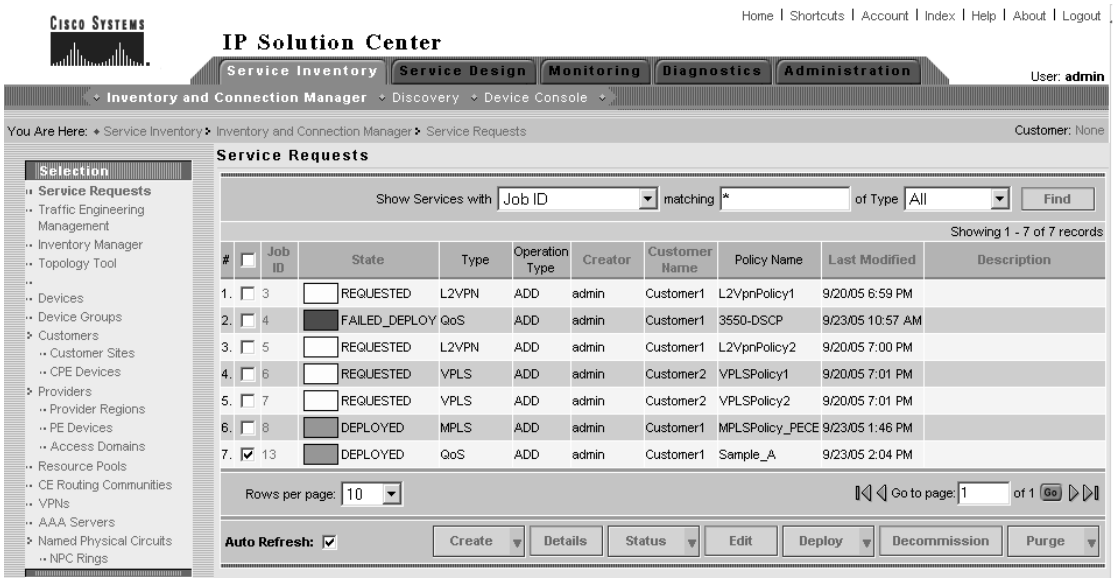
To create a QoS service request for MPLS services, see IP QoS for MPLS VPNs, page 3-28.

To create an IP QoS service request:

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears. (Figure 3-23).

Figure 3-23 Service Requests List



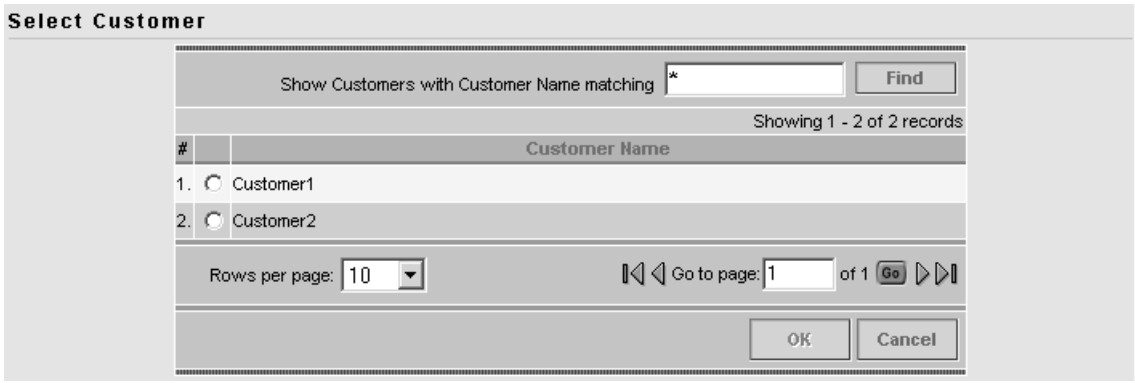
The Service Requests window lists the current service requests.

Note For more information on service requests, see QoS Service Requests, page 5-3.

Step 2 From the Service Requests window, click **Create** and choose **QoS**.

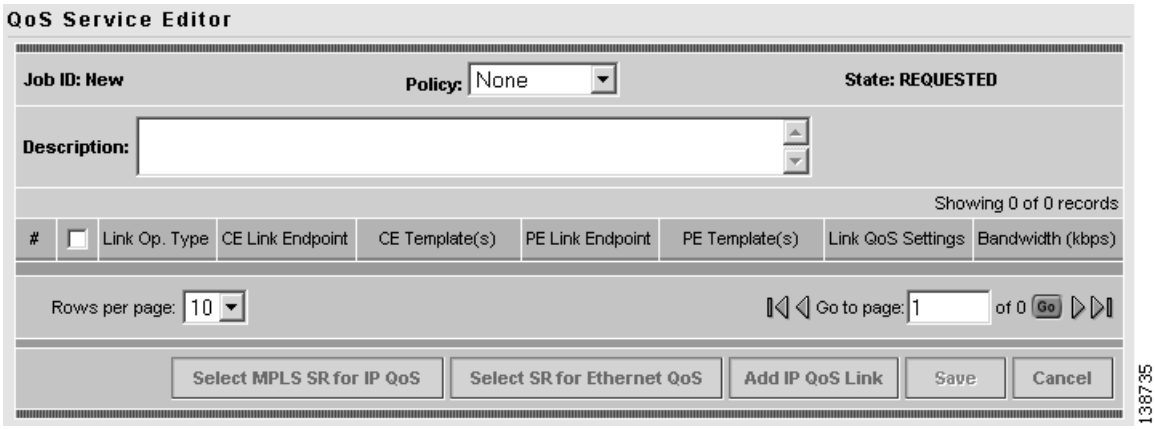
Step 3 Select the customer for this service request and click **OK** (Figure 3-24).

Figure 3-24 Select Customer



The QoS Service Editor window appears (Figure 3-25).

Figure 3-25 QoS Service Editor



The QoS Service Editor window displays the following information about each QoS links:

- Link Op. Type—The link operation type for this CE-PE link. For example, ADD means that you are adding this link to the service request. DELETE means that you are deleting this link from the service request.
- CE Link Endpoint—The CE device interface that was selected as a link endpoint QoS candidate.
- CE Templates—Add a set of commands (that ISC does not include) to the CE device by associating a template with the CE device. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for information on creating templates.
- PE Link Endpoint—The PE device interface identified as a link endpoint QoS candidate.
- PE Templates—Add a set of commands (that ISC does not include) to the PE device by associating a template with the PE device. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for information on creating templates.
- Link QoS Settings—Previously configured link QoS setting to use for this CE-PE link.
- Bandwidth—This value automatically populates when you choose a link qos setting, or you can enter it manually.

Use the QoS Service Editor window to manage CE-PE links, or to select MPLS service requests for IP QoS provisioning. You can also select link QoS settings for the CE-PE links from this window.

Note If you are provisioning QoS for an MPLS service request, see IP QoS for MPLS VPNs, page 3-28.

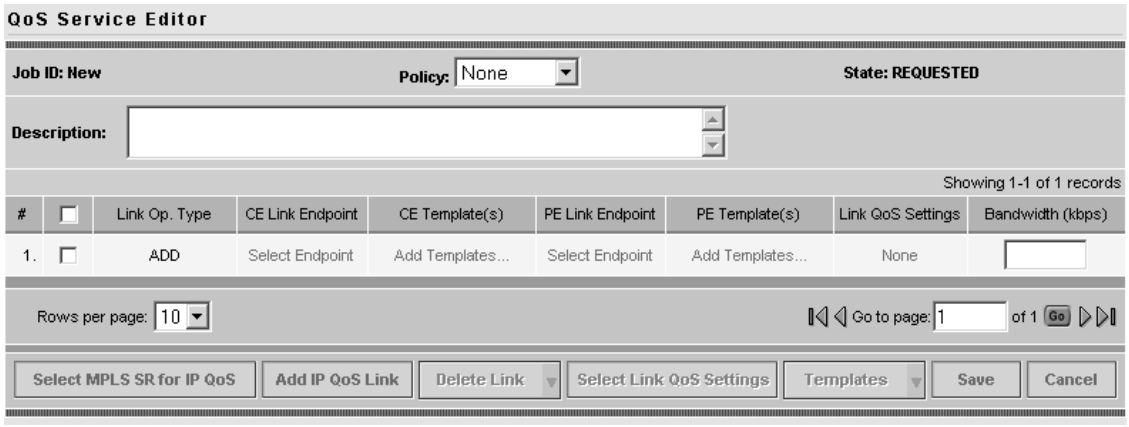
If you add CE and PE link endpoints, you get a CE-PE QoS link. If you select link QoS settings for the CE-PE link, you get link level QoS policy. Typically, a QoS service request has both a service level policy and link level QoS settings.

Step 4 Use the **Policy** drop-down menu to select a QoS policy to apply to this service request. For the network example, use CustomerA-QoS-Policy.

Step 5 To add a QoS link, click **Add IP QoS Link**.

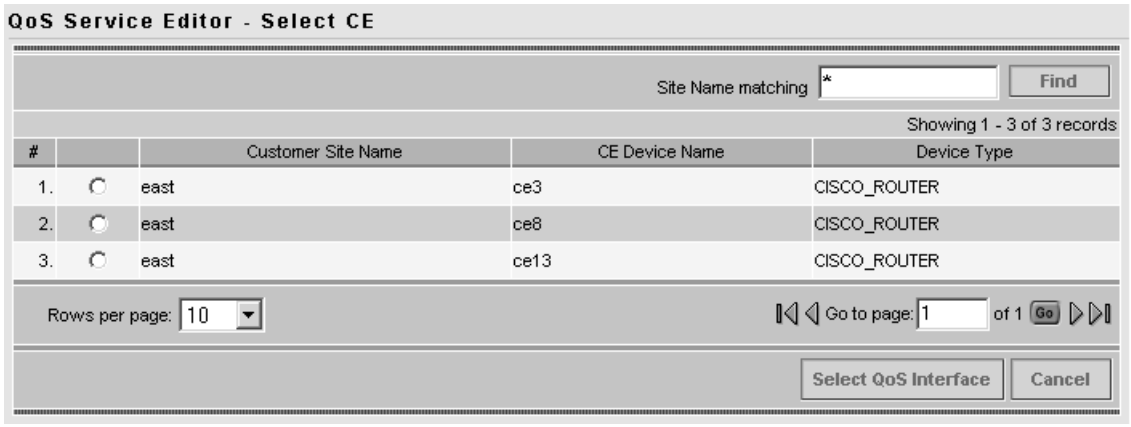
The QoS Service Editor window displays two endpoints: **CE Link Endpoint**, and **PE Link Endpoint**. (Figure 3-26).

Figure 3-26 Select Link Endpoints



Step 6 Click **Select Endpoint** in the CE Link Endpoint field. The QoS Service Editor - Select CE window appears (Figure 3-27).

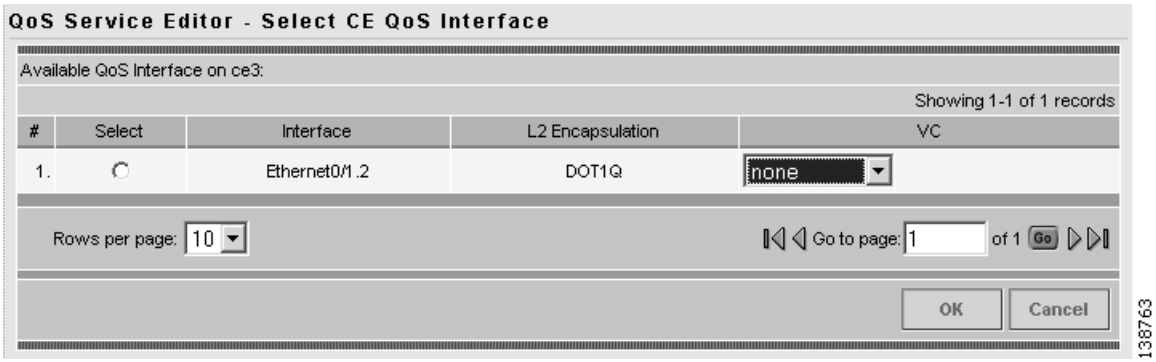
Figure 3-27 Select CE



This window lists all CE devices, including the Customer Site Name, CE device Name, and Device Type.

Step 7 Select a CE device and click **Select QoS Interface**. For example, select ce3. The QoS Service Editor - Select CE QoS Interface window appears (Figure 3-28).

Figure 3-28 Select CE QoS Interface



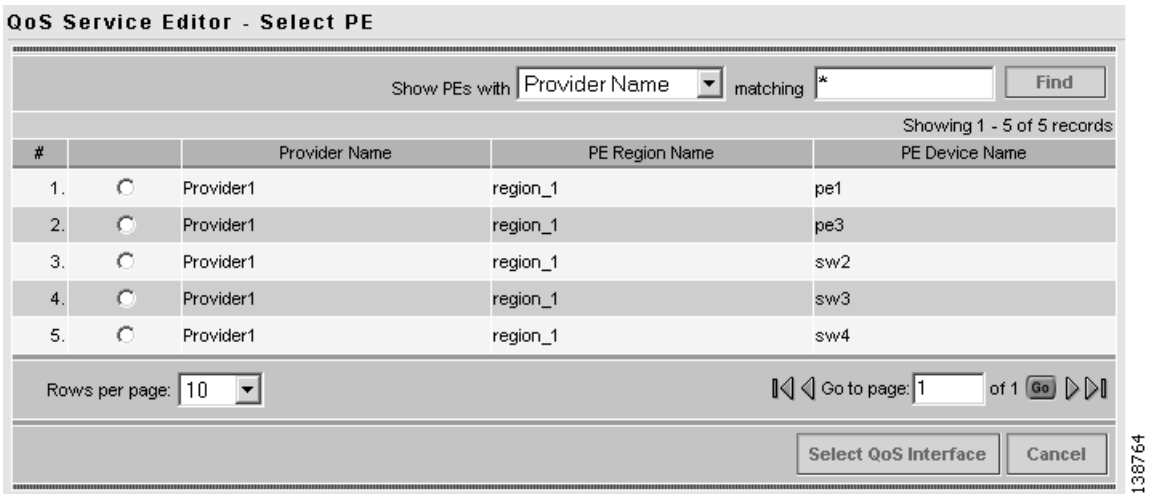
This window lists the CE device interfaces identified during the Selecting CE Device Interfaces for QoS operation, and includes the following information about the CE device interfaces:

- Interface name—The name of the CE device interface marked as a QoS candidate.
- Layer 2 (L2) Encapsulation—Layer 2 encapsulation type. For a list of supported encapsulation types, see Implementation Assumptions, page 2-2
- VC—ATM or Frame Relay virtual circuits. Choose from a list of circuit identifiers.

Step 8 Select the CE QoS interface and click **OK**. For example, select QoS Interface Ethernet0/1.2 with Vlan id = 100. You return to the QoS Service Editor window. The interface information for the CE link endpoint is listed.

Step 9 Next, select the corresponding PE link endpoint. From the QoS Service Editor window, Click **Select Endpoint** in the PE Link Endpoint field. The QoS Service Editor - Select PE Window appears (Figure 3-29).

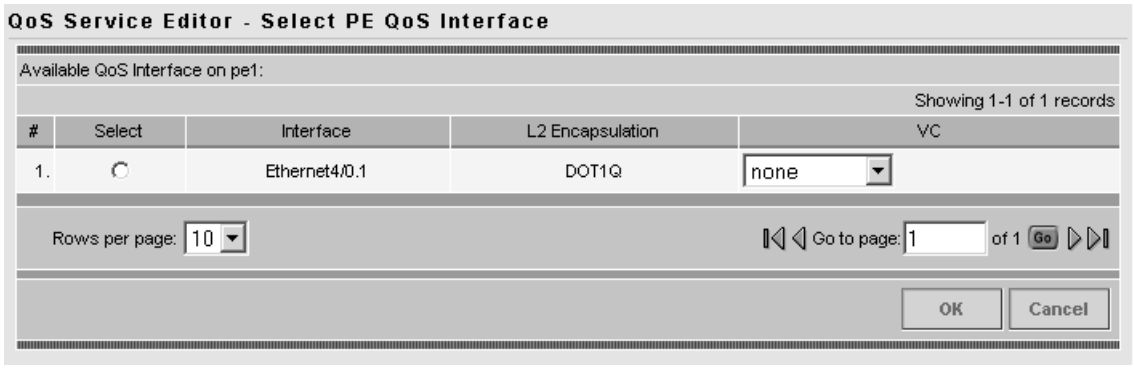
Figure 3-29 Select PE



This window lists all PE devices, including the Provider Name, Provider Region Name, and PE device Name.

Step 10 Select a PE device and click **Select QoS Interface**. For example, select pe1. The QoS Service Editor - Select PE QoS Interface window appears (Figure 3-30).

Figure 3-30 Select PE QoS Interface

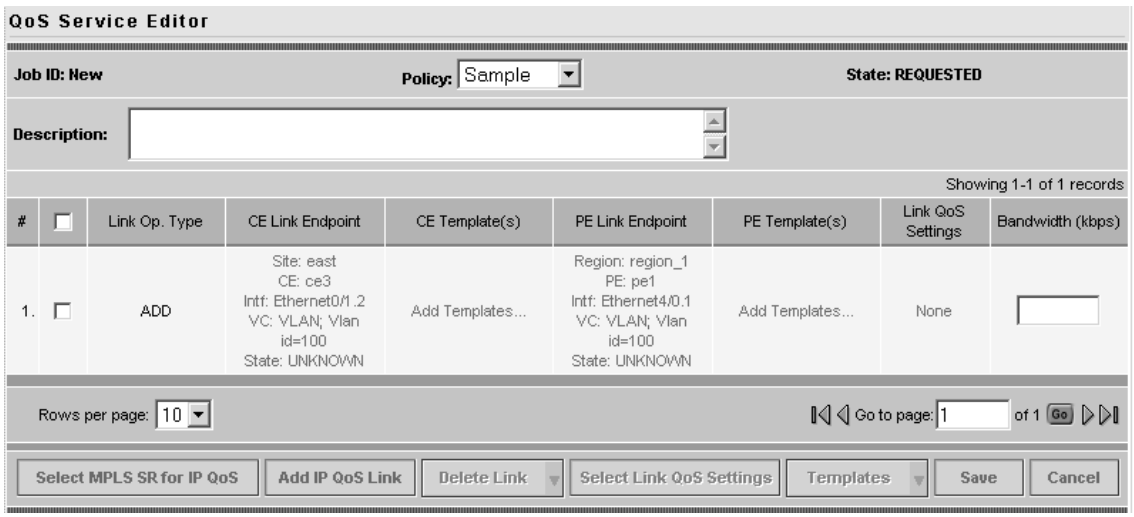


This window lists the PE device interfaces identified during the Selecting PE Device Interfaces for QoS operation, and includes the following information about the PE device interfaces:

- Interface name—The name of the PE device interface marked as a QoS candidate.
- Layer 2 (L2) Encapsulation—Layer 2 encapsulation type. For a list of supported encapsulation types, see Implementation Assumptions, page 2-2.
- VC—ATM or Frame Relay virtual circuits. Choose from a list of circuit identifiers.

Step 11 Select the PE QoS interface and click **OK**. For example, select QoS interface Ethernet4/0.1 with VC Vlan id = 100. You return to the QoS Service Editor window (Figure 3-31).

Figure 3-31 QoS Service Editor with CE and PE Endpoints

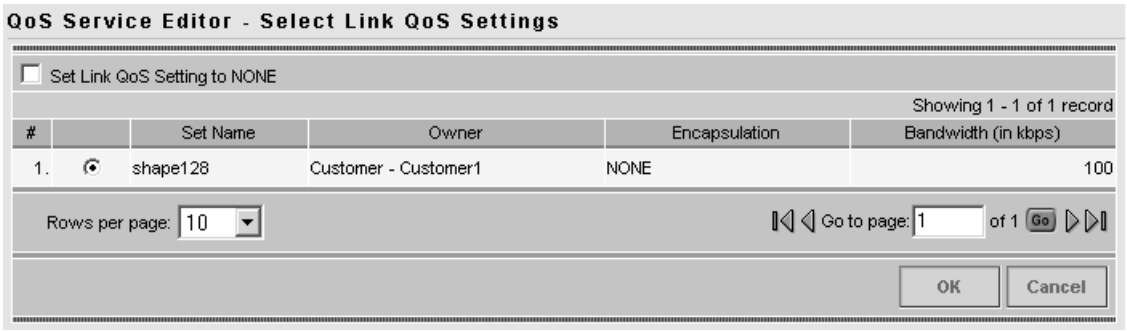


The interface information for the PE link endpoint is listed.

Step 12 Repeat Steps 1 to 11 to add more CE and PE link endpoints.

Step 13 To add a link level QoS policy to this link, click **None** in the Link QoS Settings field or select the link with the check box in the second column and click **Select Link QoS Settings**. The Select Link QoS Settings window appears (Figure 3-32).

Figure 3-32 Select Link QoS Settings



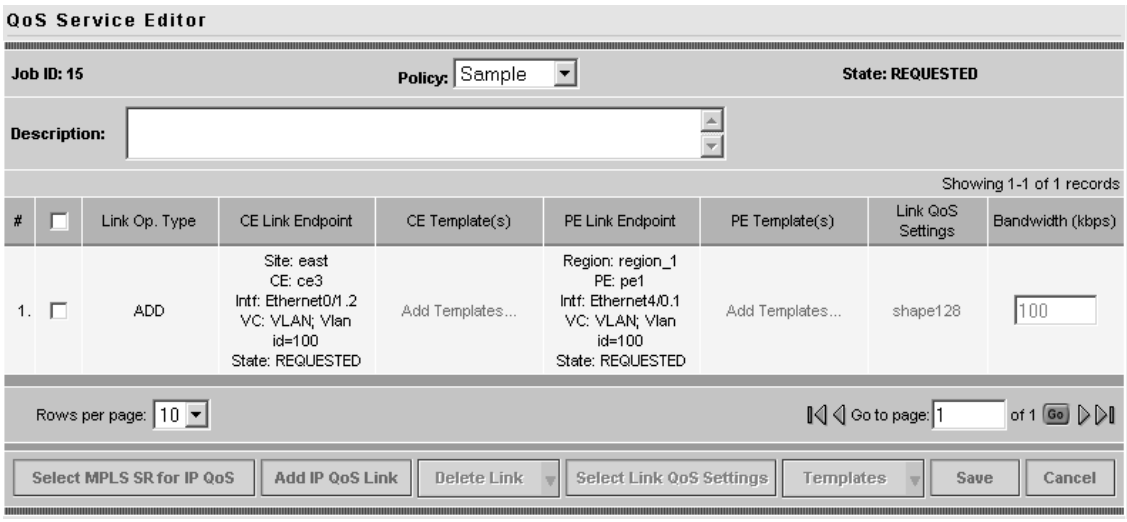
This window lists all set names (link QoS settings) created during the Configuring Link-Level IP QoS Settings operation.

Step 14 Select the link QoS setting (set name) to apply to this CE-PE link and click **OK**.

When you have finished adding all CE and PE Link Endpoints, the service request creation process is complete.

Step 15 Save the QoS service request by clicking **Save** (Figure 3-33).

Figure 3-33 QoS Service Editor with Link QoS Setting



This saves the QoS service request parameters to the ISC Repository. The ISC-generated configlet is downloaded to the network device when the service request is deployed. See the following section.

For more information on the ISC Repository, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Deploying an IP QoS Service Request

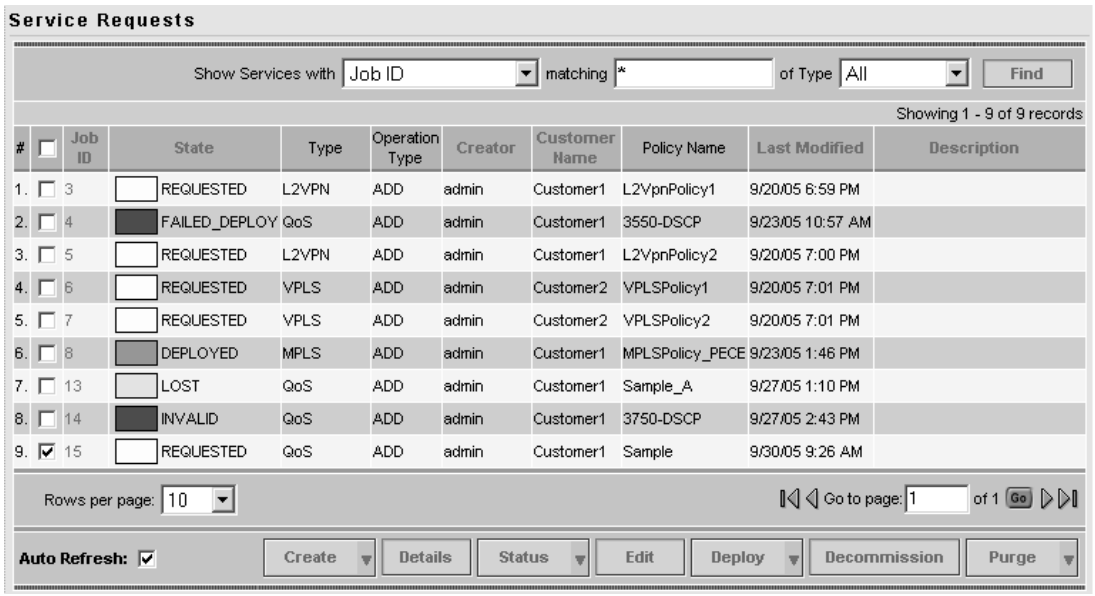
To apply QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC generates a configlet to download to each device.

When the configlets are generated, the QoS service request enters the *Pending* state once the configlets have been generated and downloaded to the device(s) and the AUDIT task is in-process. When the configlets are downloaded to all the devices in the service request and the result of the AUDIT task is successful, the QoS service request enters the *Deployed* state.

To deploy a QoS service request:

Step 1 Select **Service Inventory > Inventory and Collection Manager > Service Requests**. The Service Requests window appears (Figure 3-34).

Figure 3-34 Deploy QoS Service Request



This window shows all active service requests for this user name and the following service request information: JobID, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified Date, and the Description.

From the Service Requests window, you can Create, view the Details, Edit, Deploy, Decommission, and Purge an active service request.

Step 2 Create and schedule a deployment task by clicking the **Deploy** button. Select **Deploy** from the menu.

Tip **Force Deploy** generates configlets for a service request that is already in the *Deployed* state and downloads it to the network devices. Use Force Deploy when a device configuration is lost or when you replace or change equipment.

ISC generates the QoS configlet and downloads it to the network device.

To see if a QoS service request is successfully deployed, check the State field on the Service Requests window.

Note For more information on QoS service requests, see QoS Service Requests, page 5-3.

IP QoS for MPLS VPNs

ISC supports the following QoS parameters for MPLS VPNs:

- IP QoS based on DSCP or IP Precedence value before the packet enters the MPLS network
- Map DSCP or IP Precedence value to MPLS Exp. value at the ingress router to the MPLS Network (PE ingress interface)
- IP QoS based on DSCP or IP Precedence values continues after the packet leaves the MPLS network

The following sections describes how to apply IP QoS parameters to an MPLS service request.

Checking Prerequisites

For an MPLS network, ISC marks packets with MPLS Experimental values (MPLS Exp.) at the PE ingress interface. Before you can apply QoS parameters to an MPLS network, you must already have:

- An existing IP QoS policy.
- An existing MPLS service request. This service request can either be in the *Requested*, *Deployed*, *Failed Deployed*, or *Pending* state. However, we recommend that you use an MPLS service request that is in the *Deployed* state because the QoS service request might rely on interface configuration from the MPLS service request.

  See *Cisco IP Solution Center MPLS VPN User Guide, 4.1* for more information on creating MPLS service requests.
- Select the Mark MPLS Exp. check box for the QoS policy. This is configured for the QoS service level policy on the Edit QoS Policy window. See Creating the Service Level IP QoS Policy, page 3-9 for more information.

Creating a QoS Service Request from an MPLS Service Request

Use the following procedure to create a QoS service request from an MPLS service request:

Step 1 Select **Service Inventory >Inventory and Connection Manager > Service Requests**. The Service Requests window appears. (Figure 3-35).

Figure 3-35 Service Requests

The Service Requests window lists the current list of service requests.

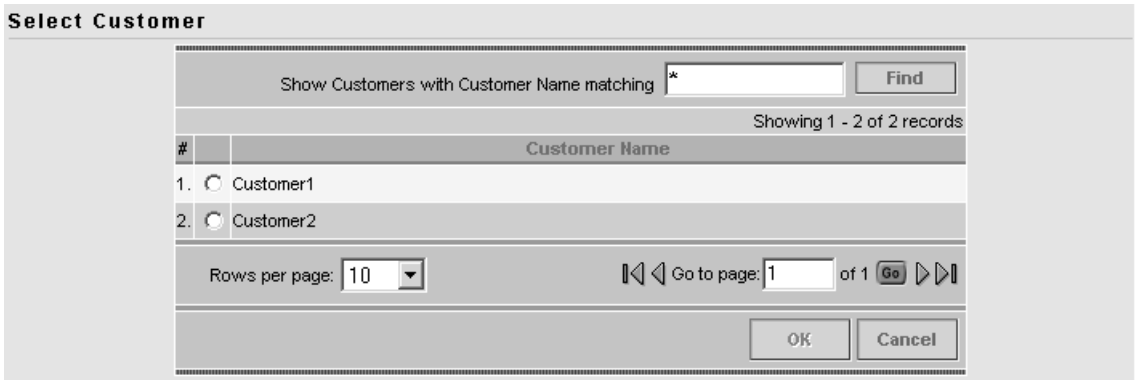
Note For more information on service requests, see QoS Service Requests, page 5-3.

Step 2 From the Service Requests window, click **Create** and choose **QoS**.

The Select Customer window appears (Figure 3-24).

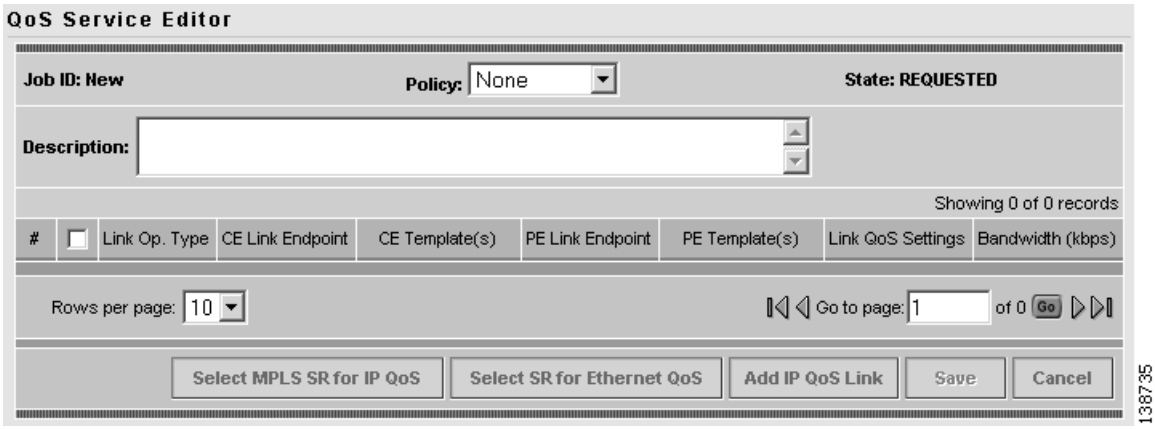
Step 3 Select the customer for this service request and click **OK**.

Figure 3-36 Select Customer



The QoS Service Editor window appears (Figure 3-25).

Figure 3-37 QoS Service Editor

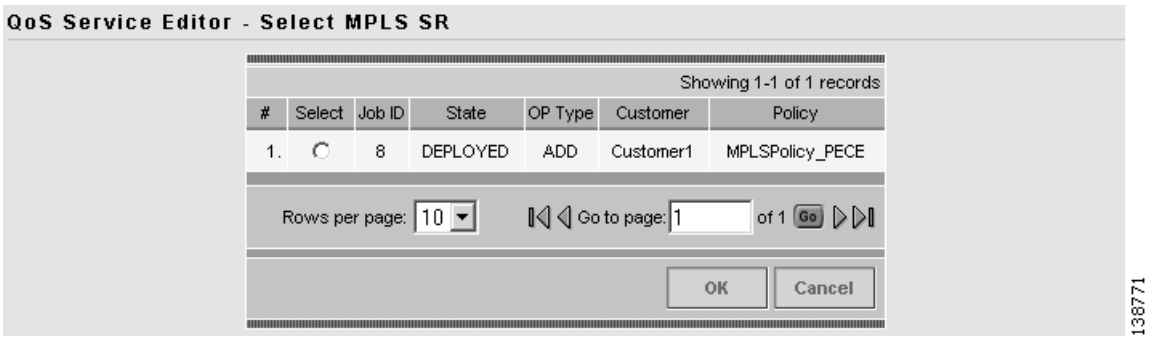


The QoS Service Editor window displays the following information about a link:

- Link Op. Type—The link operation type for this CE-PE link. For example, ADD means that you are adding this link to the service request.
- CE Link Endpoint—The CE device interface identified as a link endpoint QoS candidate.
- CE Templates—Add a set of commands (that ISC does not include) to the CE device by associating a template with the CE device. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for information on creating templates.
- PE Link Endpoint—The PE device interface identified as a link endpoint QoS candidate.
- PE Templates—Add a set of commands (that ISC does not include) to the PE device by associating a template with the PE device. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for information on creating templates
- Link QoS Settings—Previously configured link QoS setting to use for this CE-PE link.
- Bandwidth—You can enter the value for this manually, or it can be pre-populated when you choose a link qos setting.

Step 4 Click **Select MPLS SR for IP QoS**. The QoS Service Editor–Select MPLS SR window appears (Figure 3-38).

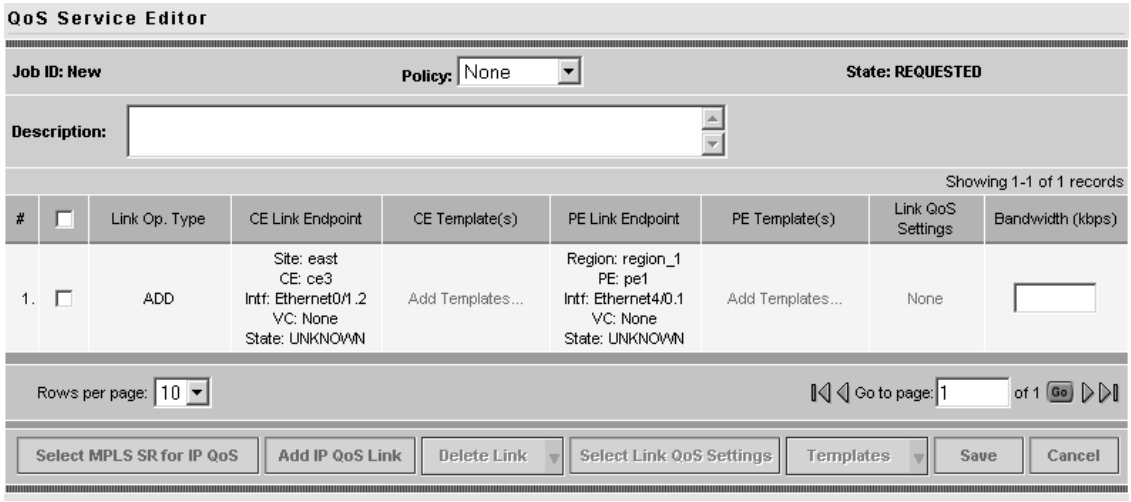
Figure 3-38 Select MPLS Service Request for QoS



This window lists existing MPLS service requests, including the deployment state, the customer, and policy name.

Step 5 Select an existing MPLS service request for creating your QoS service request and click **OK**. The next QoS Service Editor window appears (Figure 3-39).

Figure 3-39 QoS Service Editor

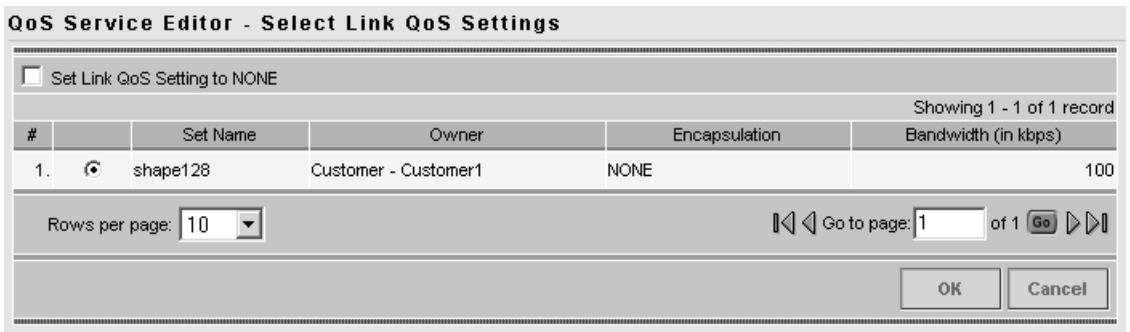


This window lists the CE and PE links that were created during MPLS provisioning. For more information on MPLS provisioning, see *Cisco IP Solution Center MPLS VPN User Guide, 4.1*.

From this window you can delete or add more links and apply link QoS settings to a link endpoint pair.

Step 6 To apply link QoS settings, select a link endpoint pair and click **Select Link QoS Settings**. Alternately, you can click **None** in the Link QoS Settings column. The QoS Service Editor–Select Link QoS settings appears (Figure 3-40).

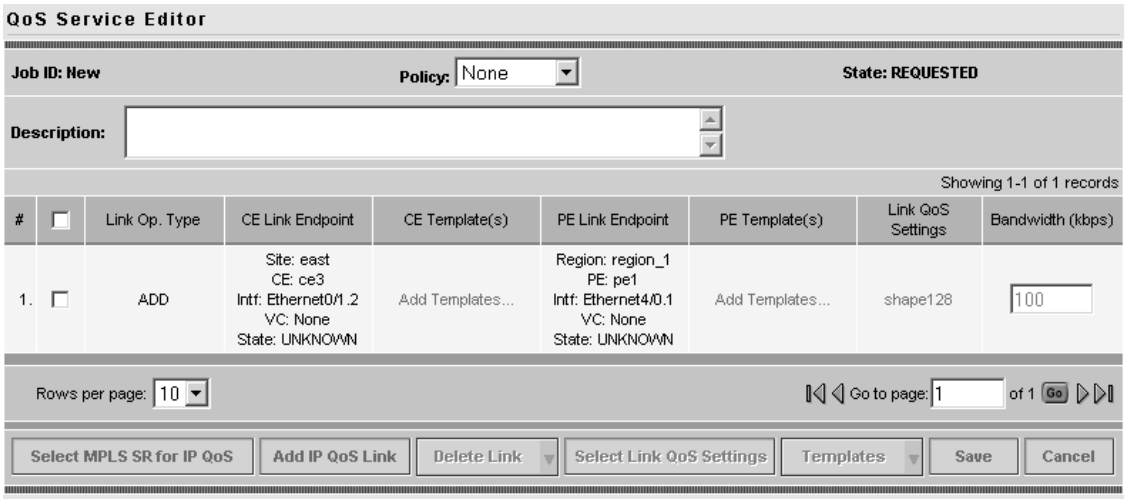
Figure 3-40 QoS Service Editor - Select Link QoS Settings



This window lists all set names (link QoS settings) previously defined in the link level QoS policy. See Configuring Link-Level IP QoS Settings, page 3-15 for more information.

Step 7 Select the link QoS setting (set name) to apply to this CE-PE link and click **OK**. You return to the QoS Service Editor window (Figure 3-41).

Figure 3-41 Completed QoS Service Request from MPLS Service Request



The CE-PE links and link QoS settings for the QoS service request are listed. These are the QoS parameters that will be applied to the MPLS service request.

Step 8 Click **Save** to save the QoS service request.

Step 9 To apply QoS policies to the VPN service request, you must deploy the QoS service request. When you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

When the configlets are generated and downloaded to the devices, the QoS service request enters the *Pending* state. When the devices are audited, the QoS service request enters the *Deployed* state.

Note For more information on deploying and auditing QoS service requests, see QoS Service Requests, page 5-3.

Provisioning Process for Ethernet QoS

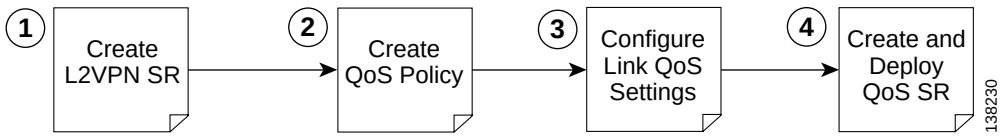
This chapter describes the steps required to provision Ethernet QoS for a network using the Cisco IP Solution Center (ISC) graphical user interfaces.

Before starting the provisioning process, be sure to read Chapter 2, "Getting Started."

This chapter describes how to set up Ethernet QoS provisioning for L2VPN and VPLS.

The chapter contains the following sections:

Ethernet QoS Process Model

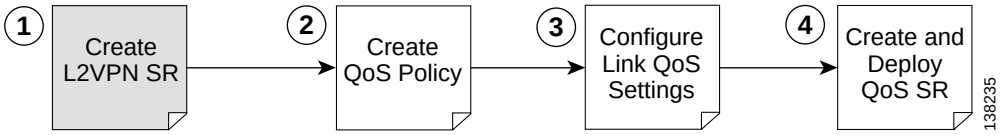


The Ethernet QoS process model in ISC is designed so that different types of users (for example, network administrators and service operators), can define different aspects of the QoS provisioning process.

The Ethernet QoS provisioning process shown above includes four operations:

1. Creating an L2VPN Service Request—At least one L2VPN service request (SR) is needed in order to create an Ethernet QoS service request.
2. Creating Ethernet QoS Policies—QoS policy based on service classes
3. Configuring Link-Level Ethernet QoS Settings—QoS parameters that are sensitive to link bandwidth and Layer 2 encapsulation.
4. Creating and Deploying Ethernet QoS Service Requests—Create a container for the QoS policy and QoS link settings and apply these parameters to the selected L2VPN service request(s).

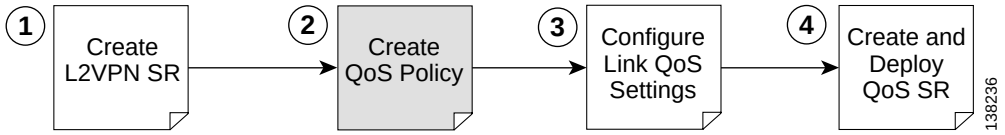
Creating an L2VPN Service Request



The first step in provisioning Ethernet QoS is to create an L2VPN service request. This is needed because an Ethernet QoS service request is created by importing an L2VPN service request into a QoS service request.

To create an L2VPN service request, see *Cisco IP Solution Center L2VPN User Guide, 4.1*.

Creating Ethernet QoS Policies



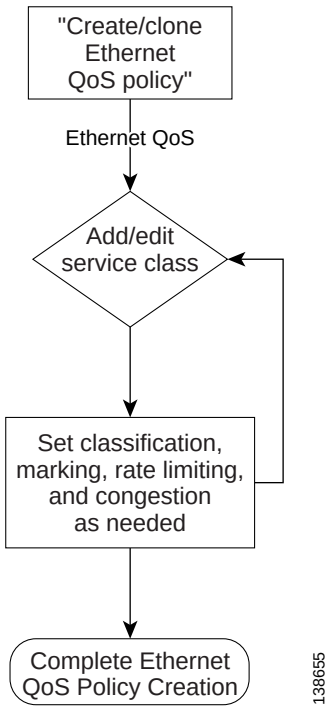
A QoS service policy is divided into two policy categories; service level policies and link level policies. Most networks have a combination of both policy types.

These two parts of the ISC QoS policy are managed in different parts of the user interface.

- The service-level QoS policy is managed using **Service Design > Policies** (Step 2).
- The link-level Ethernet QoS policy is managed using **Service Design > Link QoS** (Step 3).

This section describes how to create an Ethernet QoS service-level policy using the ISC GUI. The process of creating a link-level QoS Policy is described in Configuring Link-Level Ethernet QoS Settings, page 4-9.

Figure 4-1 Create a Service-Level Ethernet QoS Policy



Creating an Ethernet QoS Policy

ISC provides a selection of predefined Ethernet QoS policies that in most cases can be used as a basis for new policies. It is recommended that this option be used whenever possible.

However, if none of the predefined policies available prove suitable, a new policy can be created from scratch (see Step 2 in the following procedure).

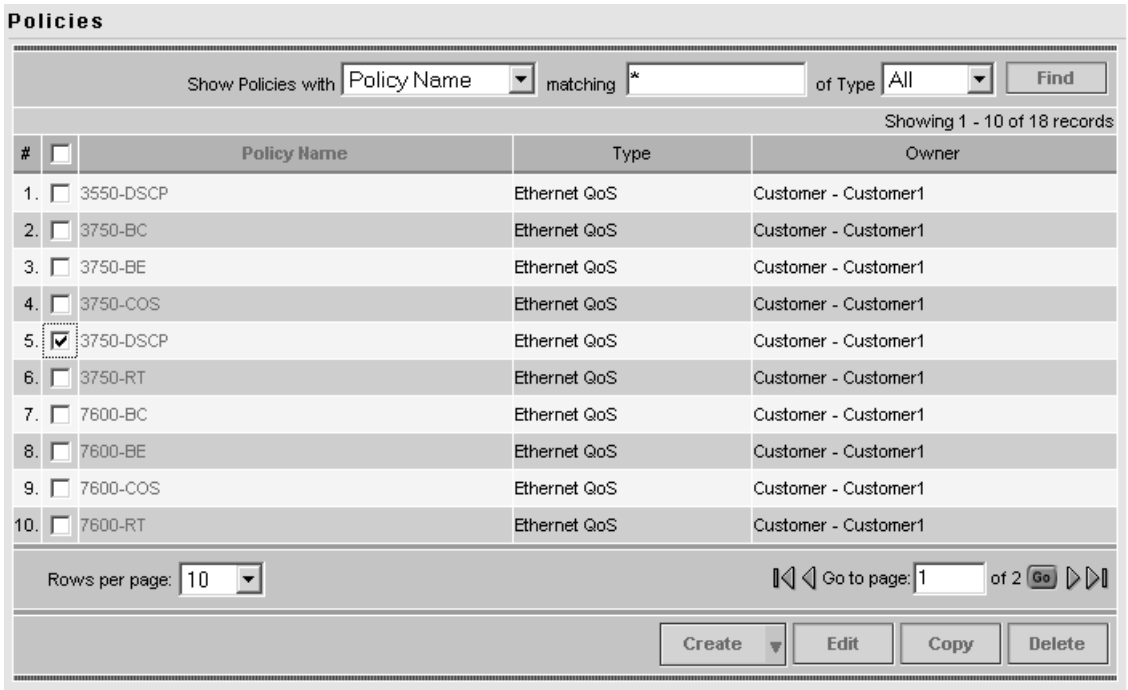
To create an Ethernet QoS policy using predefined policies:

Step 1 On the Service Design tab, click **Policies** (Figure 4-2).

Figure 4-2 Policies

The Policies window appears (Figure 4-3).

Figure 4-3 Predefined Policies



The Policies window lists all policies that currently exist for the different ISC services. The ones listed in Figure 4-3 are the ten predefined Ethernet QoS policies supplied with ISC. See Appendix E, "Metro Ethernet Use Cases" for at description of the corresponding use cases and hardware platforms.

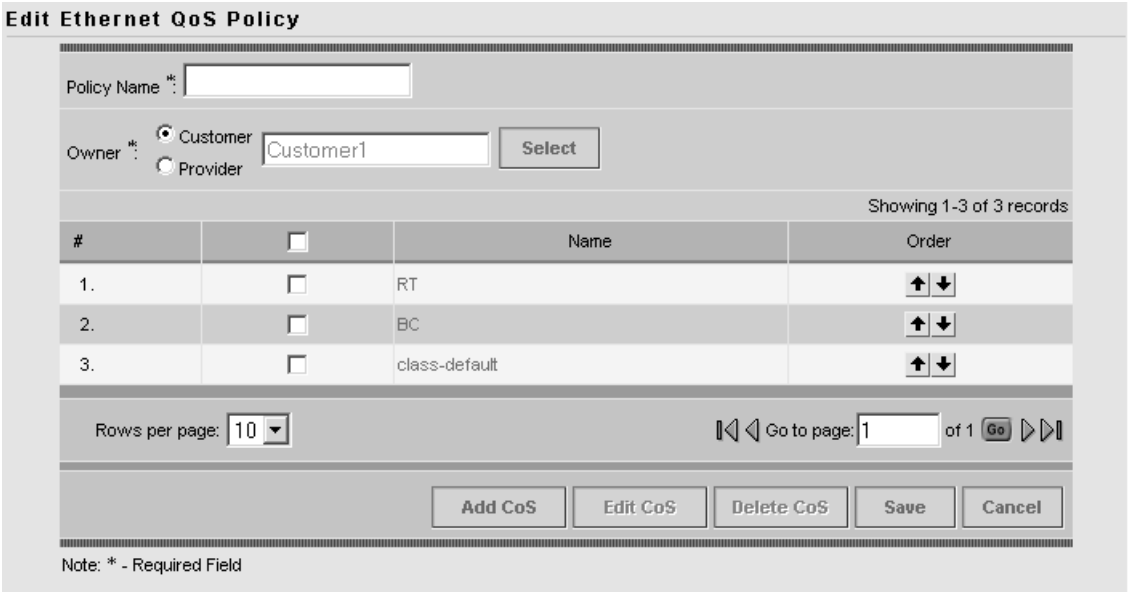
Note Policies that are currently associated with a QoS service request cannot be edited or deleted.

Step 2 The quickest and easiest way to create an Ethernet QoS policy is to clone a predefined policy. As an alternative, you can create a policy from scratch using the **Create > QoS Policy > Ethernet QoS**.

Select the predefined policy that most closely match your needs and click **Copy**.

The Edit Ethernet QoS Policy window appears (Figure 4-4).

Figure 4-4 Edit Ethernet QoS Policy



The Edit Ethernet QoS Policy window lists the policy name, the owner (customer or provider) for this policy, and any existing service classes tied to it. Use this window to add, delete, or edit service classes for the Ethernet QoS policy.

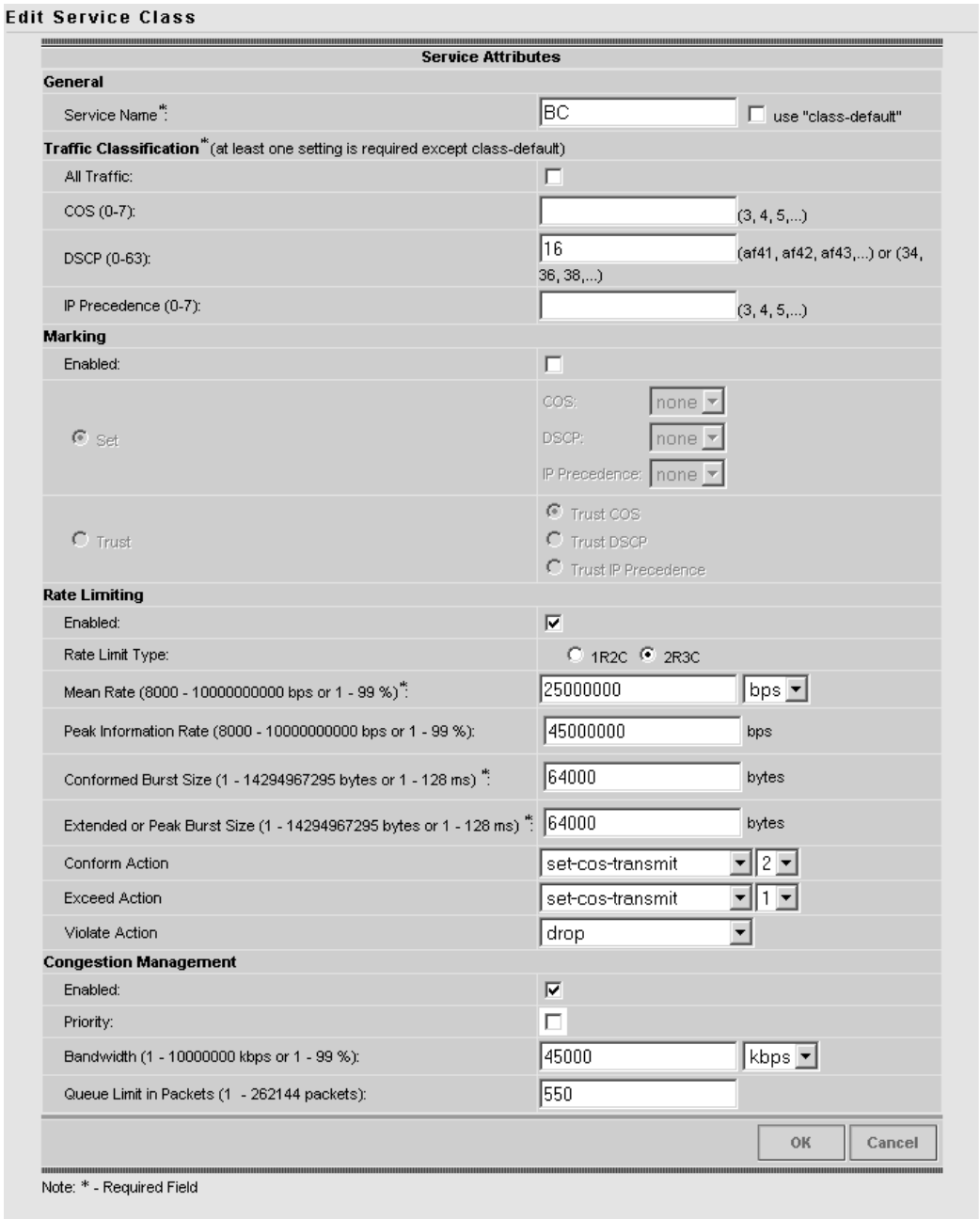
Step 3 Enter a policy name in the **Policy Name** field, edit the **Owner** field as needed, and decide whether to add, delete, or edit a service class.

Note The policy name length is limited to 10 characters.

Step 4 Add, delete, or edit a service class as needed. As an example, we elect to edit the **BC** service class. Select the **BC CoS** and click the **Edit CoS** button.

The Edit Service Class window appears (Figure 4-5).

Figure 4-5 Edit Service Class



For a detailed explanation of Edit Service Class parameters, see Appendix C, "Ethernet QoS Policy Parameters." .

Step 5 In the Edit Service Class window, edit the Ethernet QoS parameters to modify the policy as needed and click **OK** to return to the Edit Ethernet QoS Policy window.

Step 6 Repeat Steps 4 and 5 for all service classes that you want applied to your QoS policy.

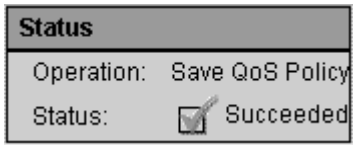
To change the processing order of the service classes, use the up and down arrow keys on the Edit Ethernet QoS Policy window. The processing order dictates the order in which the class-maps are applied to the policy map and subsequently the order in which they are processed.

Step 7 After you have made the necessary service class modifications, click **Save** to save the Ethernet QoS policy.

When you save an Ethernet QoS policy, a status information box is displayed on the bottom left of the ISC window. The following examples show the different status messages and user action required, to correct any problems.

a. Save succeeded. No further action is required. (Figure 4-6).

Figure 4-6 Save is Successful

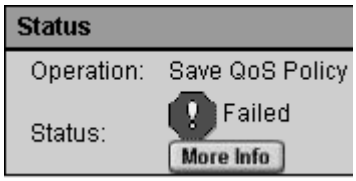


b. Policy is in use and cannot be edited or deleted (Figure 4-7). To read the warning message, click **More Info** and take the necessary action to resolve the issue.

Figure 4-7 Edit QoS Policy with Warning

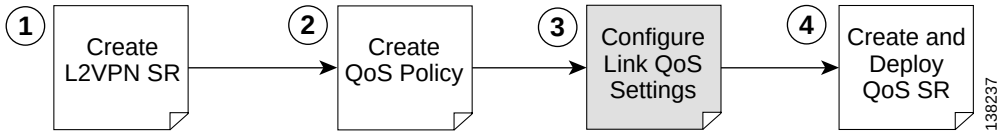
c. Save QoS policy failed (Figure 4-8). Click **More Info** to determine the source of the problem. You must fix all errors and resave before you can continue.

Figure 4-8 Save Unsuccessful



Note Not all devices and Cisco IOS platforms support all QoS parameter options. If you have specified an option for a device that is not supported, you don't receive the warning or error until after you deploy the service request.

Configuring Link-Level Ethernet QoS Settings



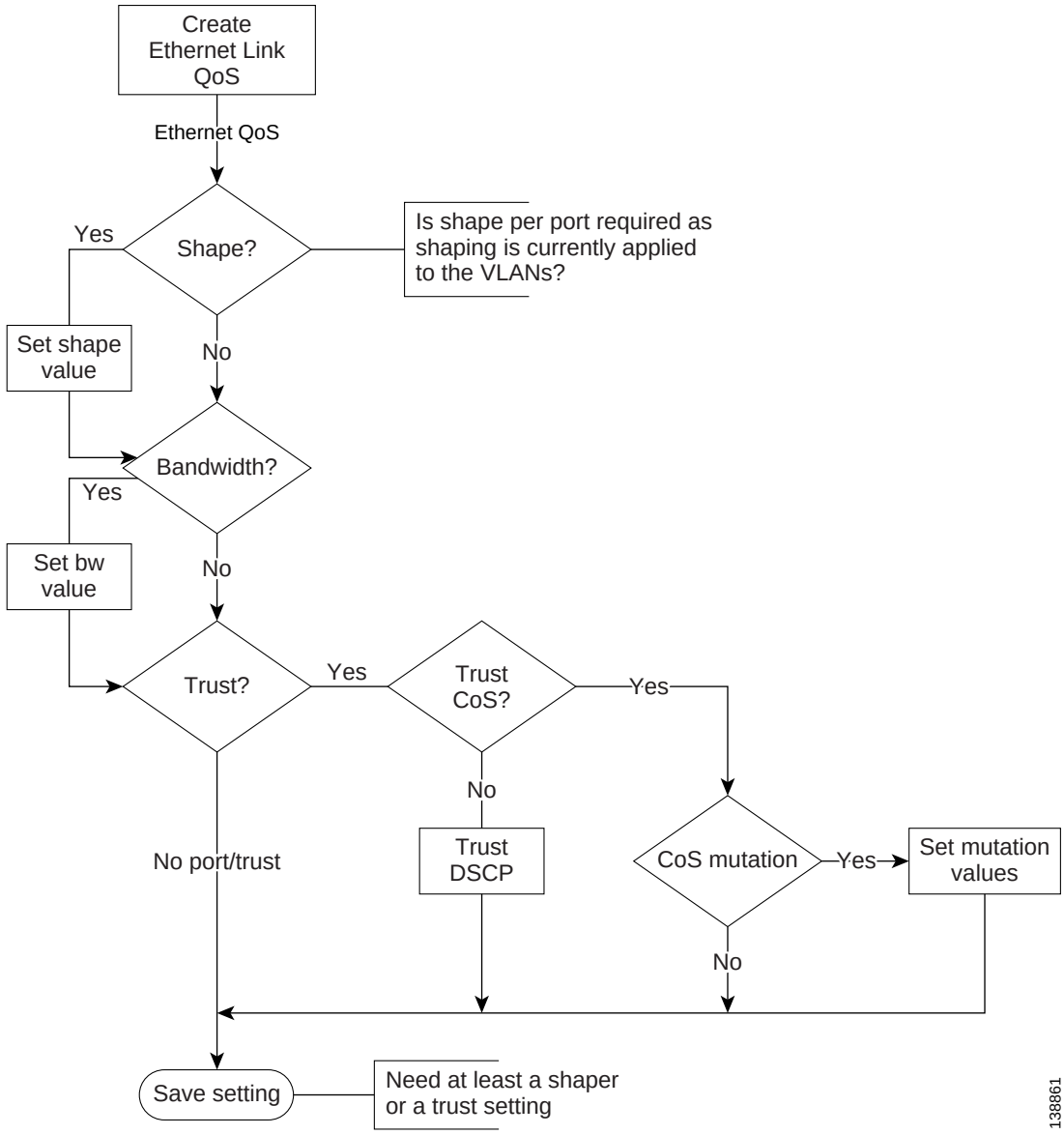
The second part of an ISC Ethernet QoS policy is the link level policy, also called the link QoS setting. The link QoS setting describes the specific UNI and VLAN level QoS parameters to use.

Link QoS settings are associated with each link in the QoS Service Request.

Creating a Link QoS Setting

This section describes how to create a link QoS setting for a network.

Figure 4-9 Create a Link Ethernet QoS Setting



To create the link QoS setting:

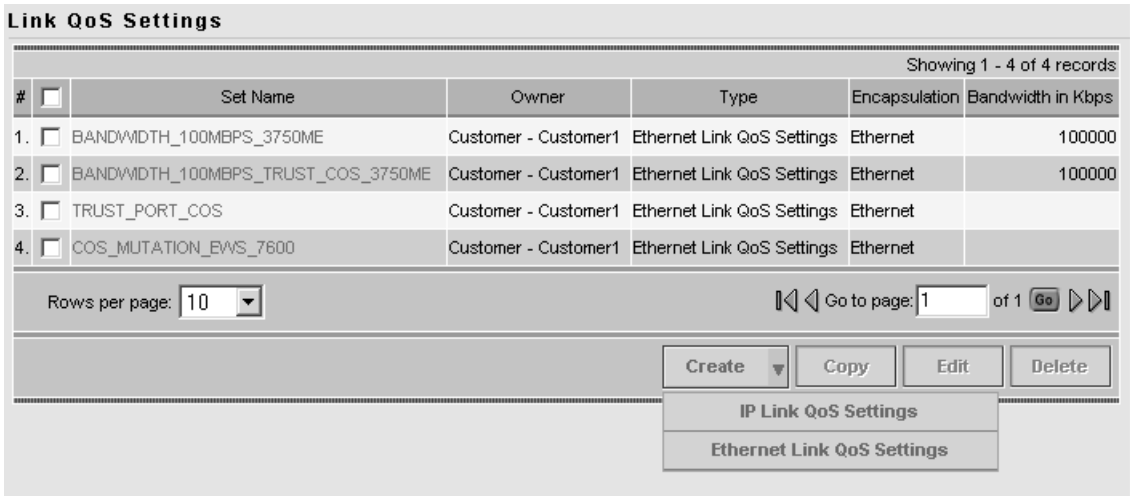
Step 1 On the Service Design tab, click **Link QoS** (Figure 4-10).

Figure 4-10 Service Design

The Link QoS Settings window appears (Figure 4-11).

The four Link QoS names listed in Figure 4-3 are the four predefined Ethernet Link QoS policies supplied with ISC.

Figure 4-11 Link QoS Settings



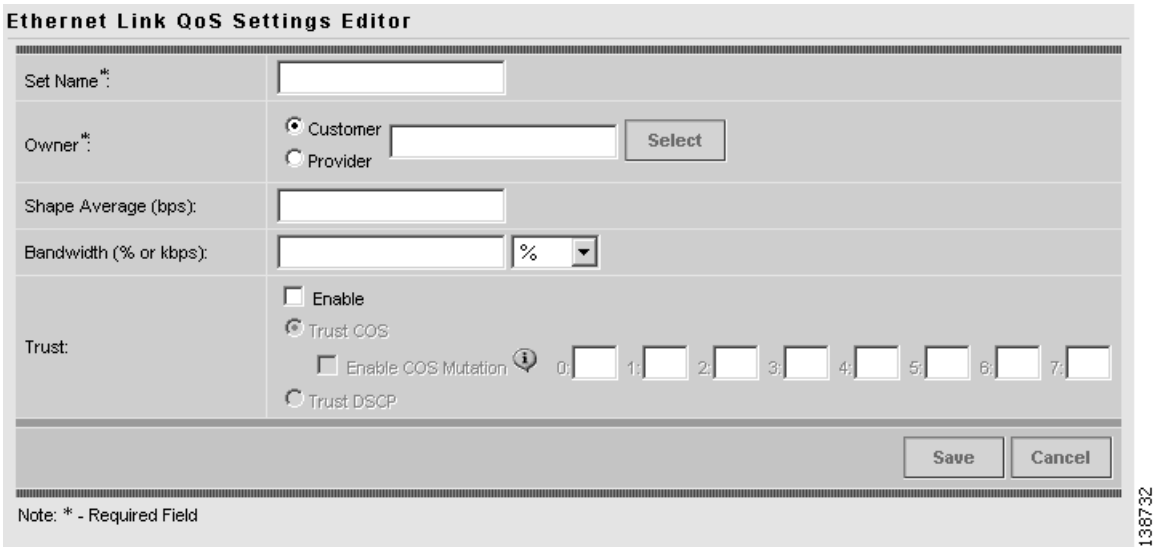
Step 2 To create an Ethernet Link QoS policy, you can clone a predefined link QoS policy and modify as needed. Select the predefined policy that most closely match your needs, click **Copy**, make the desired changes and save it.

You can also create a policy from scratch and this is described in the following.

Click **Create** to open a drop-down menu with two options, **IP Link QoS Settings** and **Ethernet Link QoS Settings**. Select the **Ethernet Link QoS Settings** to create an Ethernet Link QoS.

The Ethernet Link QoS Settings window appears (Figure 4-12).

Figure 4-12 Ethernet Link QoS Settings Editor

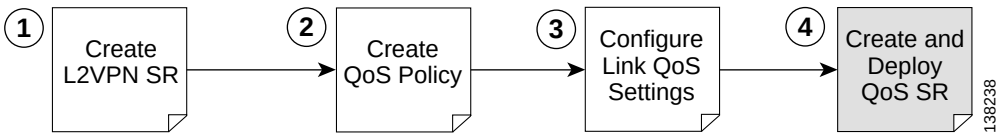


Step 3 The Ethernet Link QoS Settings window displays the current link QoS settings available for QoS service requests.

Add the desired settings. An explanation of the link QoS setting parameters is provided in Appendix C, "Ethernet QoS Policy Parameters."

Step 4 Click **Save** to keep the modified settings.

Creating and Deploying Ethernet QoS Service Requests



After both the service level and the link level QoS polices are created, the final steps in the QoS provisioning process are to create and deploy a QoS service request.

A QoS service request contains one or more QoS links. A QoS link can contain two interfaces or just one interface. Each link can optionally be associated with a QoS link setting. A QoS policy can be associated with a QoS service request.

A QoS service request should:

- Contain a QoS policy
- Contain QoS links

All QoS links in the service request can optionally be associated with a link QoS setting.

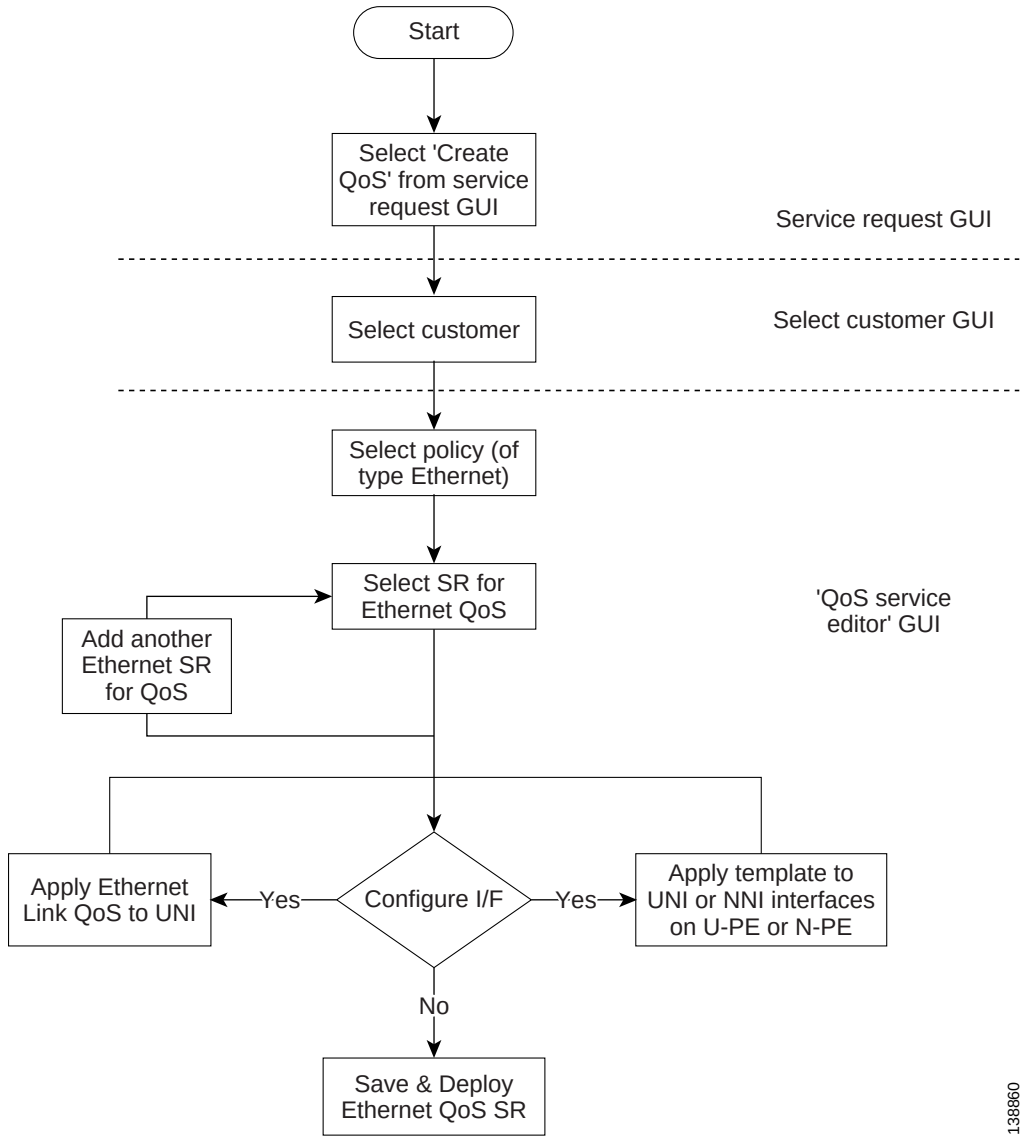
To apply QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

This section describes how to use the ISC GUI to create and deploy an Ethernet QoS service request and includes the following sections:

Creating an Ethernet QoS Service Request

This section describes how to create an Ethernet QoS service request, independent of VPN services.

Figure 4-13 Create an Ethernet QoS Service Request

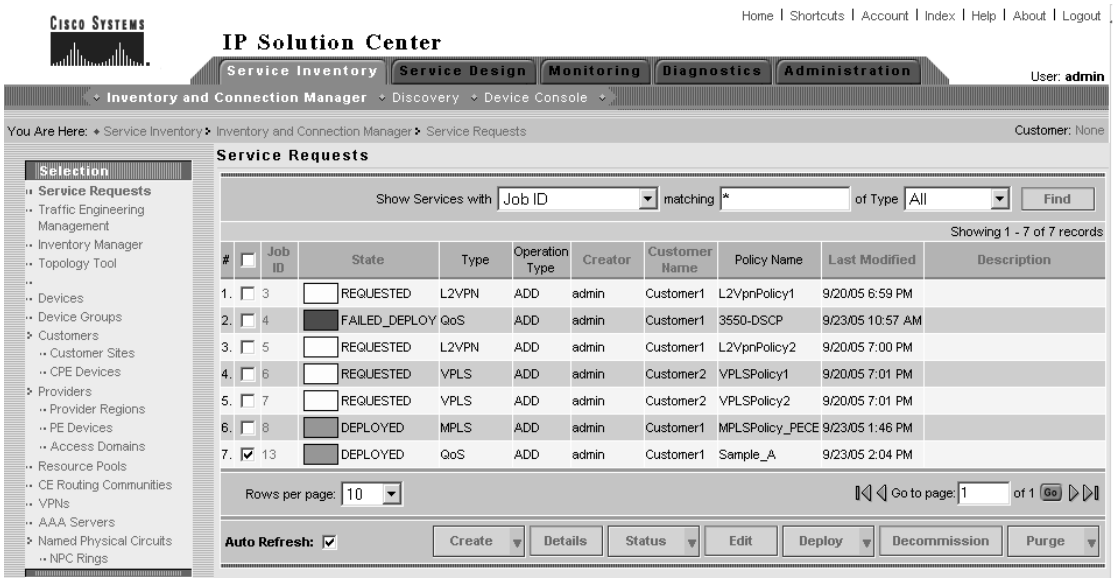


To create an Ethernet QoS service request:

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Request**.

The Service Requests window appears. (Figure 4-14).

Figure 4-14 Service Requests



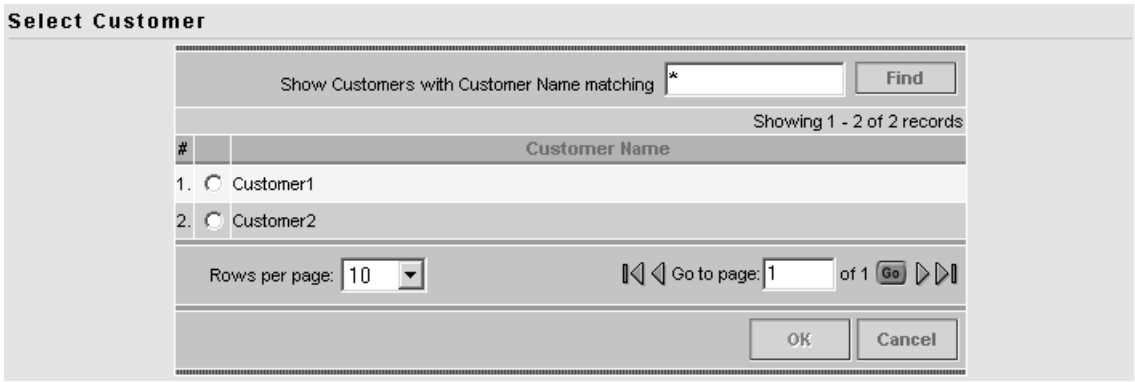
The Service Requests window lists the current service requests.

Note For more information on service requests, see QoS Service Requests, page 5-3.

Step 2 From the Service Requests window, click **Create** and choose **QoS**.

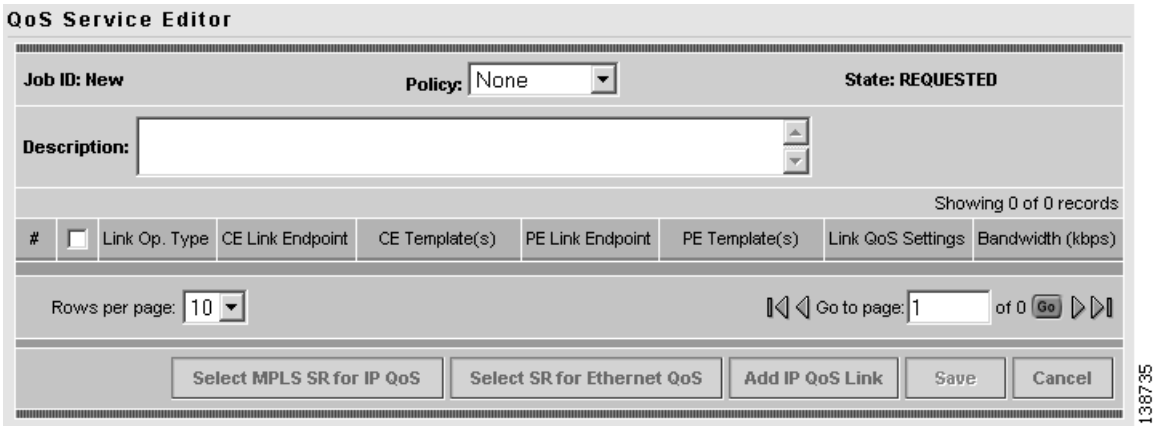
Step 3 Select the customer for this service request and click **OK** (Figure 4-15).

Figure 4-15 Select Customer



The QoS Service Editor window appears (Figure 4-16).

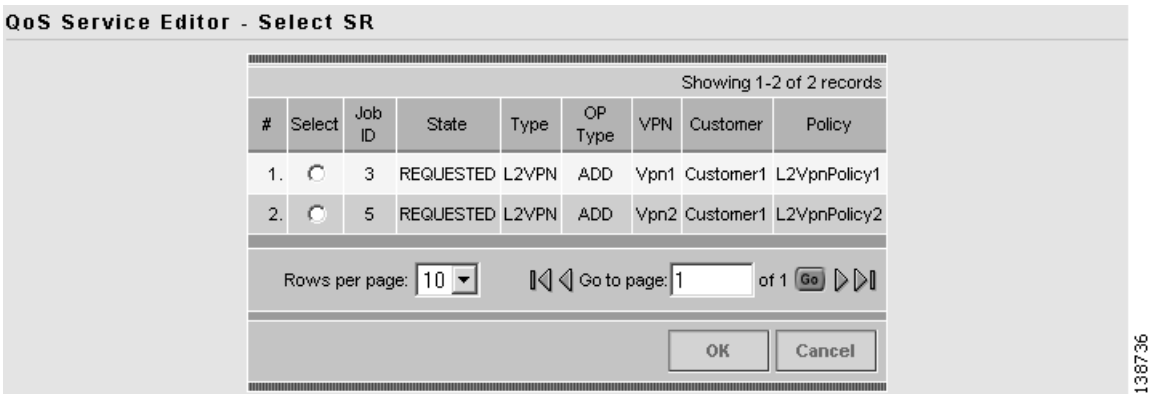
Figure 4-16 Default QoS Service Editor



Step 4 To add an Ethernet QoS link, click **Select SR for Ethernet QoS**.

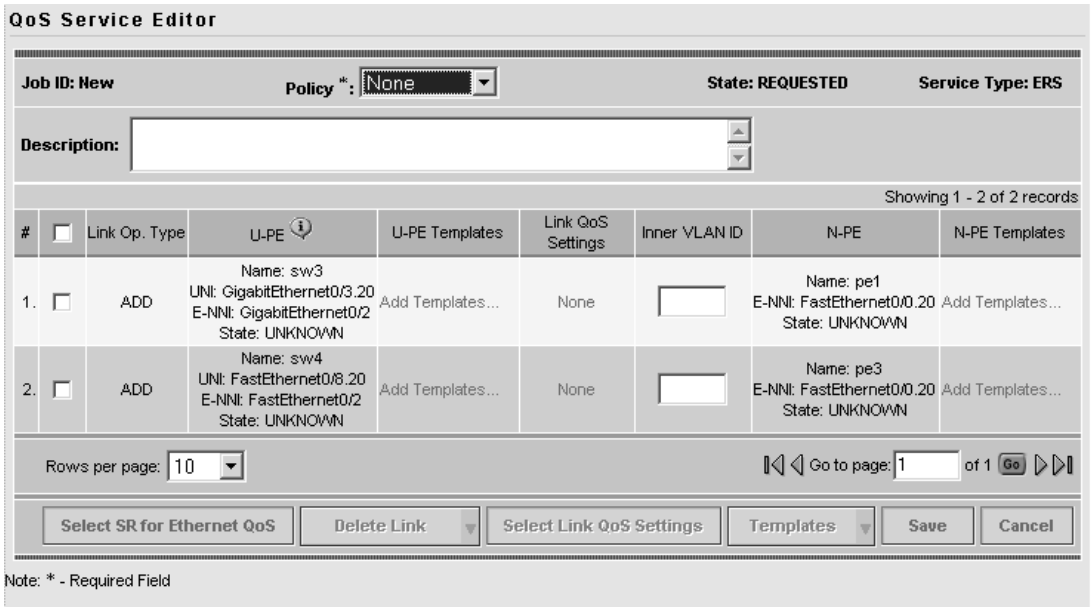
The QoS Service Editor window displays the available service requests (Figure 4-17).

Figure 4-17 Select Service Request



Step 5 Select a service request and click **OK**. The QoS Service Editor switches to Ethernet QoS service request editor mode (Figure 4-18).

Figure 4-18 QoS Service Editor - Ethernet QoS Service Request Mode



This window lists the link information for the selected service requests.

The QoS Service Editor window displays the following information about each QoS link:

- **Link Op. Type**—The link operation type for this U-PE to N-PE link. For example, ADD means that you are adding this link to the service request. DELETE means that you are deleting this link from the service request.
- **U-PE**—U-PE device, UNI, E-NNI, and state information of the link.
- **U-PE Templates**—Add a set of commands (that ISC does not include) to the U-PE device by associating a template with the U-PE device. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for information on creating templates.
- **Inner VLAN ID**—CE-VLAN ID of a L2VPN EWS or VPLS. (See General Metro Ethernet Service Types, page E-1 for a definition of Metro Ethernet terminology).
- **N-PE**—N-PE device, E-NNI, and state information.
- **N-PE Templates**—Add a set of commands (that ISC does not include) to the N-PE device by associating a template with the PE device. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for information on creating templates.
- **Link QoS Settings**—Previously configured link QoS setting to use for this Ethernet QoS link.

Use the QoS Service Editor window to select a service request for Ethernet QoS provisioning.

Step 6 To add more service requests, repeat steps 4 and 5.

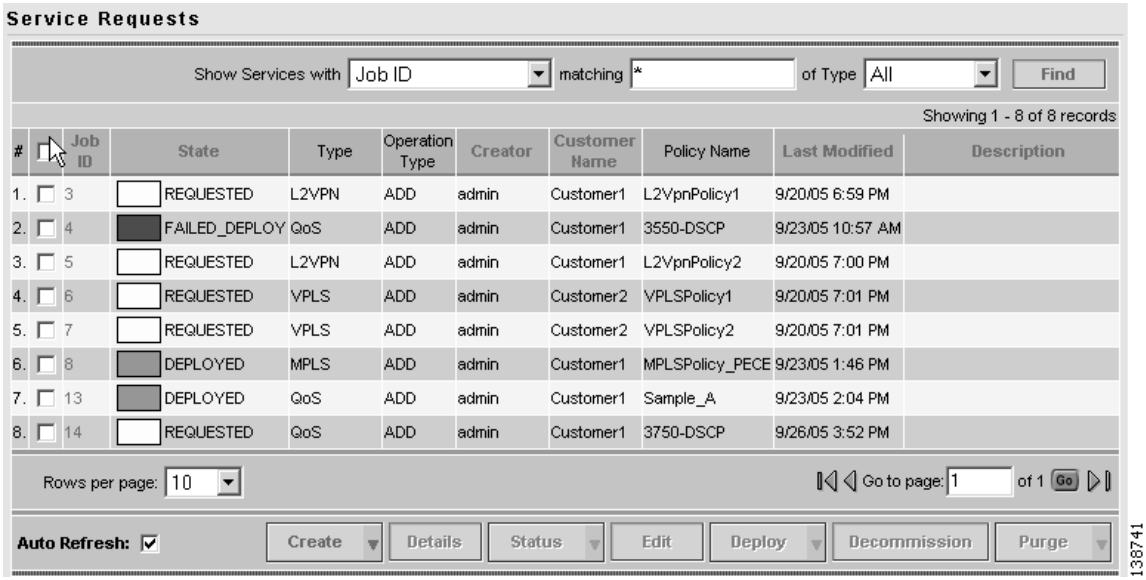
Step 7 Use the **Policy** drop-down menu to select a QoS policy to apply to this service request.

Step 8 You can now associate U-PE Templates, Link QoS Settings, and N-PE Templates by clicking the corresponding links to bring up the selection window.

Step 9 To save the QoS service request, click **Save**.

The newly created QoS service request now appears in the Service Requests window (Figure 4-19).

Figure 4-19 Service Requests with Newly Added QoS Service Request



This saves the QoS service request parameters to the ISC Repository. The ISC-generated configlet is uploaded to the network device when the service request is deployed. This step is described in the following section.

For more information on the ISC Repository, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Deploying an Ethernet QoS Service Request

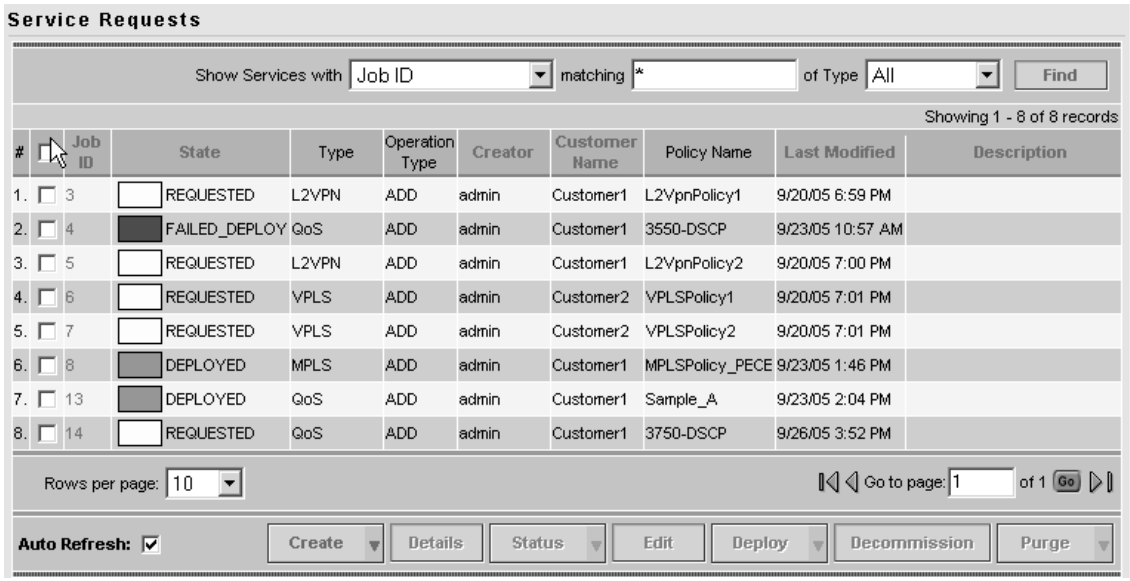
To apply QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC generates a configlet to download to each device.

When the configlets are generated, the QoS service request enters the *Pending* state. When the configlets are uploaded to all the devices in the service request, the QoS service request enters the *Deployed* state.

To deploy a QoS service request:

Step 1 Select **Service Inventory > Inventory and Collection Manager > Service Requests**. The Service Requests window appears (Figure 4-20).

Figure 4-20 Deploy QoS Service Request



This window shows all active service requests for this user name and specific service request information.

From the Service Requests window, you can Create, view the Details, view the Status of SR Links or Logs, Edit, Deploy, Decommission, and Purge an active service request.

Step 2 Create and schedule a deployment task by clicking the **Deploy** button. Select **Deploy** from the menu.

Tip **Force Deploy** generates configlets for a service request that is already in the *Deployed* state and downloads it to the network devices. Use Force Deploy when a device configuration is lost or when you replace or change equipment.

ISC generates the QoS configlet and downloads it to the network device.

To see if a QoS service request has been successfully deployed, check the **State** field on the Service Requests window.

Note For more information on QoS service requests, see QoS Service Requests, page 5-3.

Inner VLAN for 3750-ME

This section describes L2VPN EWS/VPLS classification on outer and inner VLAN. (See General Metro Ethernet Service Types, page E-1 for a definition of Metro Ethernet terminology.)

This QoS model based on inner C-VLAN ID classification is only found in Catalyst 3750-ME. Therefore it is not part of the mainstream ME3.1 solution, although this fact does not restrict its use.

With this approach, one could create a H-QoS policy that matches on two VLAN ID values (outer and inner) and then also look at the inner CoS or even DSCP information within that outer/inner VLAN combination.

Note Inner VLAN ID classification only applies to L2VPN EWS and VPLS. (See General Metro Ethernet Service Types, page E-1 for a definition of Metro Ethernet terminology.)

Note An Inner VLAN value of a requested/deployed Metro Ethernet QoS service request cannot be modified.

The following CLI shows how inner and outer VLAN is specified in a class-map.

```
class-map match-all rtvlan_102
match vlan 108
match vlan inner 102
!
class-map match-all bcvlan_104
match vlan 108
match vlan inner 104
!
class-map match-all bevlan_108
match vlan 108
!
policy-map RT_VLAN_102
class match_any
police cir 30000000 bc 64000 pir 30000000 be 64000 conform-action set-cos-transmit 5
exceed-action drop violate-action-drop
priority
!
policy-map BC_VLAN_104
class class-default
police cir 20000000 bc 64000 pir 40000000 be 64000 conform-action set-cos-transmit
2 exceed-action set-cos-transmit 1 violate-action drop
bandwidth 40000
queue-limit 550
!
policy-map BE_VLAN_108
class class-default
set cos 0
bandwidth 30000
queue-limit 3
!
policy-map VLAN_Outbound
class rtvlan_102
bandwidth 30000
service-policy RT_VLAN_102
class bcvlan_104
bandwidth 40000
service-policy BC_VLAN_104
class bevlan_108
bandwidth 30000
service-policy BE_VLAN_108
!
policy-map ES_Port_Outbound
class class-default
```

CHAPTER 5

Managing and Auditing Service Requests

Each time a QoS service request is deployed in the Cisco IP Solution Center (ISC), a configuration audit occurs. You can view the results of these in QoS configuration audit reports. Use configuration audits and reports to verify that the ISC generated configlet represents the correct QoS configuration to download to the network device.

This chapter describes how to generate and view a configuration audit, how to manage QoS service requests, and how to access task logs.

The chapter includes the following sections:

QoS Configuration Auditing

A configuration audit occurs automatically each time you deploy a QoS service request. During this configuration audit, ISC verifies that all Cisco IOS commands are present and that they have the correct syntax. An audit also verifies that there were no errors during deployment.

The configuration audit verifies the service request deployment by examining the commands configured by the QoS service request on the target devices. If the device configuration does not match what is defined in the service request, the audit flags a warning and sets the service request to a *Failed Audit* or *Lost* state.

You can create audit reports for new or existing QoS service requests.

- Audit new services—This type of audit is for service requests that have just been deployed. This type of audit identifies problems with the configuration files downloaded to the devices.
- Audit existing services—This type of audit checks and evaluates the configuration of deployed service requests to see if the service request is still in effect.

We recommend that you schedule a service request audit on a regular basis to verify the state of the network provisioning requests.

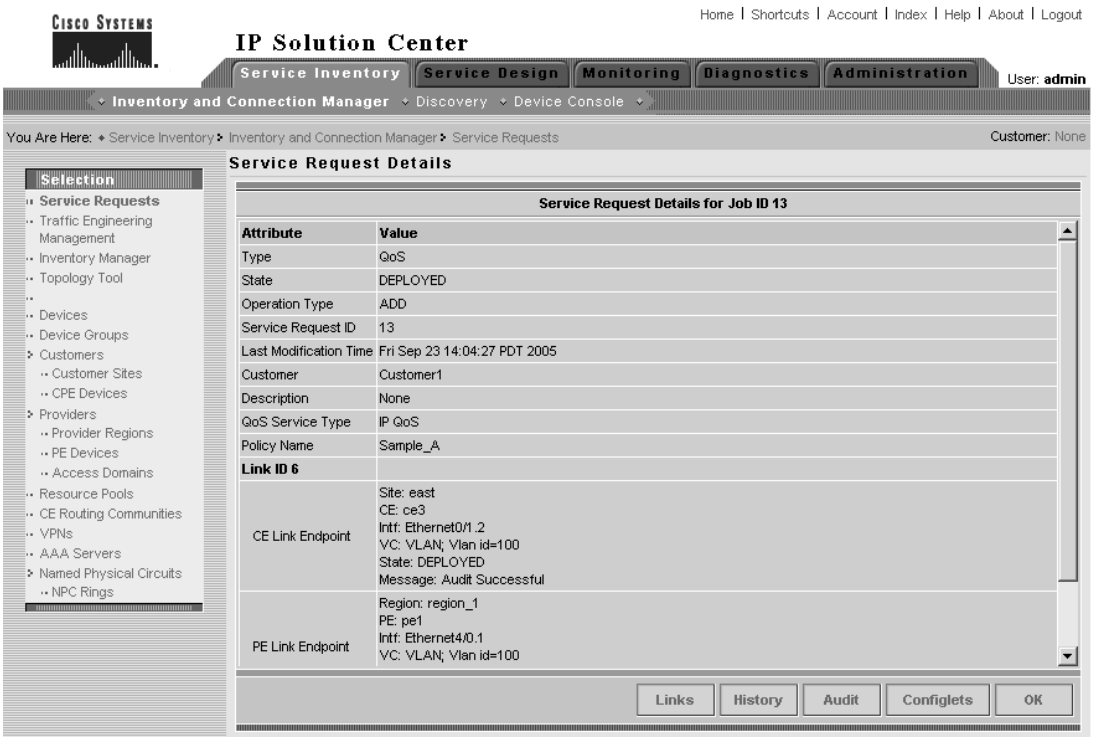
This section describes how to manually generate a configuration audit and view the audit report.

To manually generate a configuration audit:

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

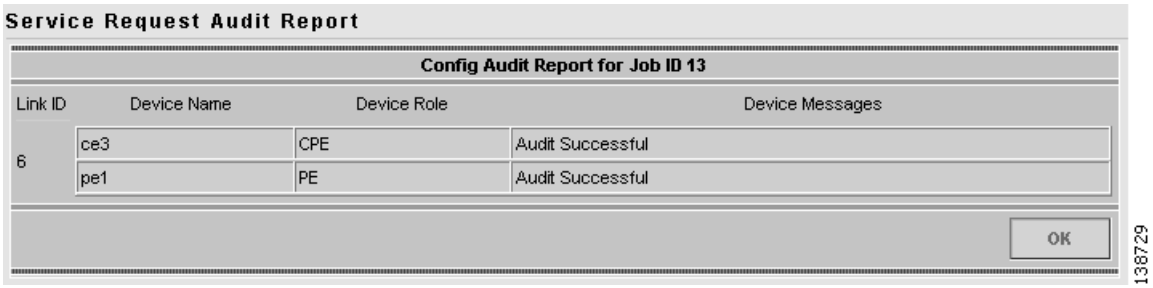
Step 2 Select a QoS service request in Deployed state for the configuration audit and click **Details**. The Service Request Details window appears (Figure 5-1).

Figure 5-1 Service Request Details



Step 3 Click **Audit**. The Service Request Audit Report window appears. Figure 5-2 shows an example of a successful configuration audit.

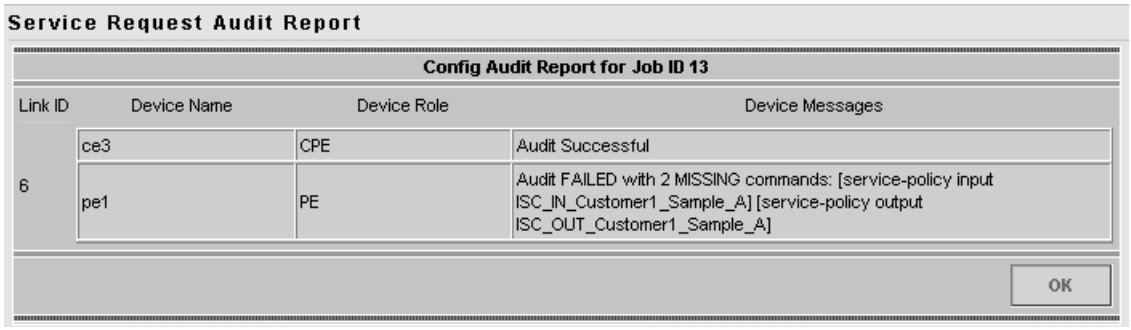
Figure 5-2 Service Request Audit Report—Successful



This window shows the device name and role, and a message regarding the status of your configuration audit.

If the audit is unsuccessful, the message field shows details on the failed audit. Figure 5-3 shows an example of a failed audit message for a QoS service request.

Figure 5-3 Service Request Audit Report—Failed



The audit failure message indicates that some commands are missing. Carefully review the information in the message field. If the audit fails, you must correct all errors and redeploy the service request.

Step 4 Click **OK** to return to the Service Request Details window.

QoS Service Requests

A QoS service request contains one or more QoS links. Each link can optionally be associated with a QoS link setting. A QoS policy can be associated with a QoS service request.

A QoS service request should:

- Contain a QoS policy
- Contain one or more QoS links
- All links in the service request can be associated with a QoS link setting (it can be the same or a different link policy for each link)

To apply QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

Use a QoS service request to apply a QoS policy to a network or to an existing L2VPN, MPLS, or VPLS service request.

The following sections describe:

Managing QoS Service Requests, page 5-4

Verifying QoS Service Requests, page 5-5

Service Request States, page 5-5

Service Request States, page 5-5

Changing Service Request Parameters, page 5-7

Note See Chapter 3, “Provisioning Process for IP QoS” and Chapter 4, “Provisioning Process for Ethernet QoS” for more information on the create and deploy operations.

Managing QoS Service Requests

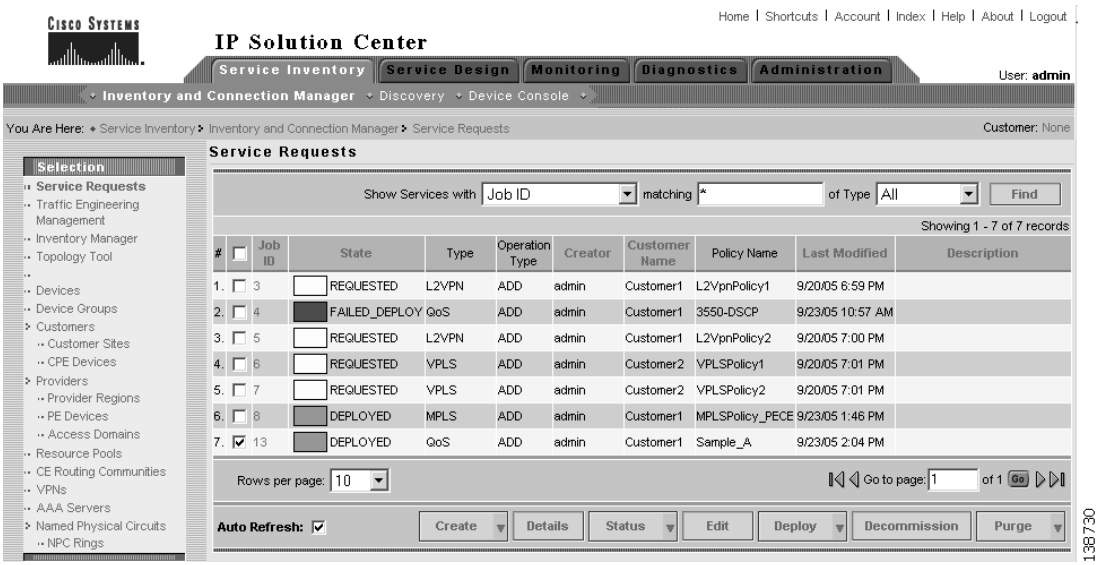
To manage QoS service request, select **Service Inventory > Inventory and Connection Manager > Service Requests**.

From the Service Requests window you can perform the following operations for QoS service requests:

- Create
- View Details
- Edit
- Deploy
- Decommission
- Purge

Figure 5-4 shows an example of the Service Requests window.

Figure 5-4 Service Requests List



The Service Requests window shows the current list of service requests for this username. The list includes the following information about each service request:

- JobID—The job number assigned to the service request by ISC. Table 5-1 describes ISC service request states.
- State—The transition state for the service request. See Service Request States, page 5-5 for more information.
- Type—The type of service request. For example, MPLS VPN, L2VPN, VPLS, QoS, or TE.
- Operation Type—The operation type for the service request. For example, ADD means that you are adding this service request, MODIFY that a service request has been changed from an earlier state, and DELETE that you are decommissioning this service request.
- Creator—Username identity of person who created or last modified the service request.
- Customer Name—Customer name for the service request.

- Policy Name—Name of policy assigned to this service request.
- Last Modified—Date and time the service request was created or last modified.
- Description—Optional text description of the service request.

Verifying QoS Service Requests

After you deploy a QoS service request, you should verify that there were no errors.

You can verify a QoS service request through the following:

- Transition state—The transition state of a QoS service request is listed on the Service Requests window in the State column. See Service Request States, page 5-5 for more information.
- View service request details—From the Service Requests Details window, you can view the QoS link endpoints and the QoS configlets for this service request. See Changing Service Request Parameters, page 5-7 for more information.
- Task Logs—Access the task logs either from the **Monitoring** > **Task Manager** or from **Service Inventory** > **Inventory and Connection Manager** > **Service Requests** (**Status** button) to help you troubleshoot a failed service request or to view more details about a service request. See QoS Task Logs, page 5-14 for more information.

Service Request States

A service request transition state describes the different stages a service request enters during the QoS provisioning process.

For example, when you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a QoS configlet for each device. When the configlets are generated and downloaded to the devices, the QoS service request enters the *Pending* state. When the devices are audited, the QoS service request enters the *Deployed* state.

Table 5-1 describes the transition states for an ISC service request.

Table 5-1 Cisco IP Solution Center Service Request States

Service Request Type	Description
Broken (valid only for L2TPv3 and MPLS services)	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to **Broken** if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent.
Closed	A service request moves to **Closed** if the service request should no longer be used during the provisioning or auditing process. A service request moves to the **Closed** state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.

Table 5-1 Cisco IP Solution Center Service Request States (continued)

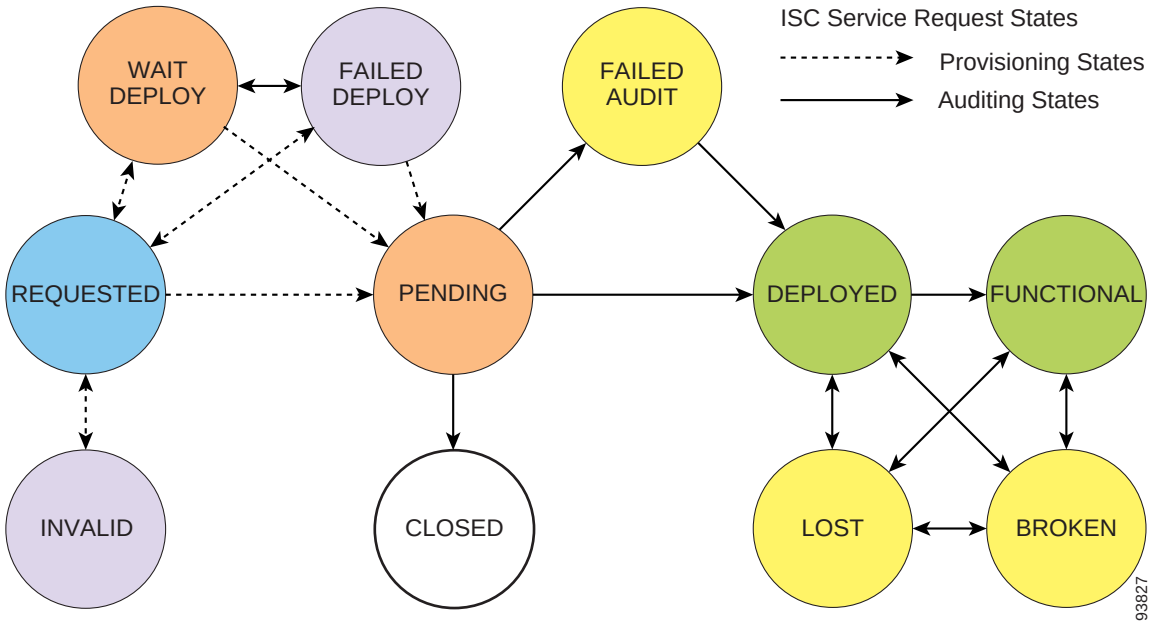
Service Request Type	Description
Deployed	A service request moves to **Deployed** if the intention of the service request is found in the router configuration file. **Deployed** indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the **Deployed** state. The **Failed Audit** state is initiated from the **Pending** state. After a service request is deployed successfully, it cannot re-enter the **Failed Audit** state (except if the service request is redeployed).
Failed Deploy	The cause for a **Failed Deploy** status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional (valid only for L2TPv3 and MPLS services)	An MPLS service request moves to **Functional** when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful.
Invalid	**Invalid** indicates that the service request information is incorrect in some way. A service request moves to **Invalid** if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to **Lost** when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the **Deployed** state, but now some or all router configuration information is missing. A service request can move to the **Lost** state *only* when the service request had been **Deployed**.
Pending	A service request moves to **Pending** when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. **Pending** indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.

Table 5-1 Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains **Requested**, the service is in an error state.
Wait Deploy	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. **Wait Deploy** indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the **Wait Deploy** state are then downloaded to the Cisco CNS-CE server.

Figure 5-5 illustrates which service request states relate to the QoS configuration auditing process, and which states relate to the provisioning process.

Figure 5-5 Service Requests States



Changing Service Request Parameters

You can change the QoS parameters associated with a deployed service request without decommissioning the service. For example, you might want to change a configuration to increase the bandwidth on the UNI interface.

To change the parameters, use the following procedure:

Step 1 Create a new QoS policy that represents the new level of service.

Step 2 Select the existing QoS service and edit that service request.

Step 3 Select the new policy (created in Step 1) and save the service request.

The QoS service request goes from DEPLOYED state to REQUESTED state and the Operation Type from ADD to MODIFY with the new QoS policy displayed.

Step 4 Deploy the QoS service request.

The provisioning engine first removes the replaced policy parameters and immediately replaces them with the new policy parameters (see the following configlet).

```
interface Vlan201
  no service-policy input isc_in_Customer_A_Default_GE2/1.201
  no shutdown
!
no policy-map isc_in_Customer_A_Default_GE2/1.201
!
no class-map match-all Customer_ADefault_EFFORTGE2/1.201vlan201
!
no class-map match-all Customer_ADefaultRITICALGE2/1.201vlan201
!
no class-map match-all Customer_ADefaultAVVIDGE2/1.201vlan201
!
no class-map match-all Customer_ADefaultCONTROLGE2/1.201vlan201
!
class-map match-all Customer_Adefault2AVVIDGE2/1.201vlan201
  match ip precedence 5
!
class-map match-all Customer_Adefault2ONTROLGE2/1.201vlan201
  match ip precedence 3
!
class-map match-all Customer_Adefault2ITICALGE2/1.201vlan201
  match ip precedence 2
!
class-map match-all Customer_Adefault2EFFORTGE2/1.201vlan201
  match ip precedence 0 1 2 3 4 5 6 7
!
policy-map isc_in_Customer_A_default2_GE2/1.201
  class Customer_Adefault2AVVIDGE2/1.201vlan201
    set ip precedence 5
    police 40000 bps 40000 byte conform-action transmit exceed-action drop
  class Customer_Adefault2ONTROLGE2/1.201vlan201
    set ip precedence 3
    police 40001 bps 40001 byte conform-action transmit exceed-action drop
  class Customer_Adefault2ITICALGE2/1.201vlan201
    set ip precedence 2
    police 40002 bps 40002 byte conform-action transmit exceed-action drop
  class Customer_Adefault2EFFORTGE2/1.201vlan201
    set ip precedence 0
    police 40003 bps 40003 byte conform-action transmit exceed-action drop
!
interface Vlan201
  service-policy input isc_in_Customer_A_default2_GE2/1.201
!
```

Note The policy parameters that were not changed (congestion management parameters in this case (tx-queue statements) are not removed, as shown in the following configlet.

```
interface GigabitEthernet2/1
  tx-queue 3
```

```
    bandwidth 16000 bps
    priority high
  tx-queue 4
    bandwidth 16001 bps
  tx-queue 2
    bandwidth 16002 bps
  tx-queue 1
    bandwidth 16003 bps
!
interface Vlan201
  no shutdown
!
```

Viewing QoS Service Request Details

The QoS service request details include the link endpoints for the QoS service request, the history, and the QoS configlet generated during the service request deployment operation. Use the service request details to help you troubleshoot a problem or error with the service request or to check the QoS commands in the configlet.

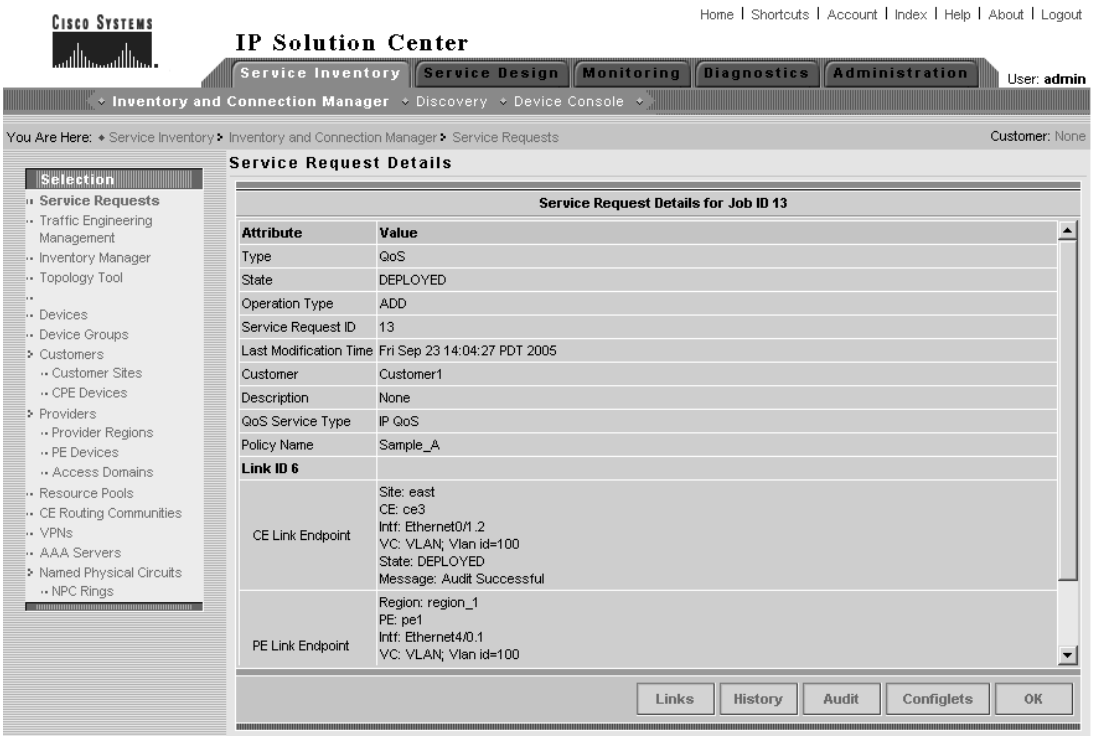
This section describes how to view the details of a QoS service request, including the history, link details, and QoS configlets.

To view QoS service request details:

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

Step 2 Select the QoS service request and click **Details**. The Service Request Details window appears as shown in Figure 5-6.

Figure 5-6 QoS Service Request Details—Attributes



The service request attribute details include the type, transition state, operation type, ID, modification history, customer, Description, QoS Service Type, and policy name.

The service request link ID details include the link endpoints, link bandwidth, and link operation type.

From the Service Request Details page, you can view more information about:

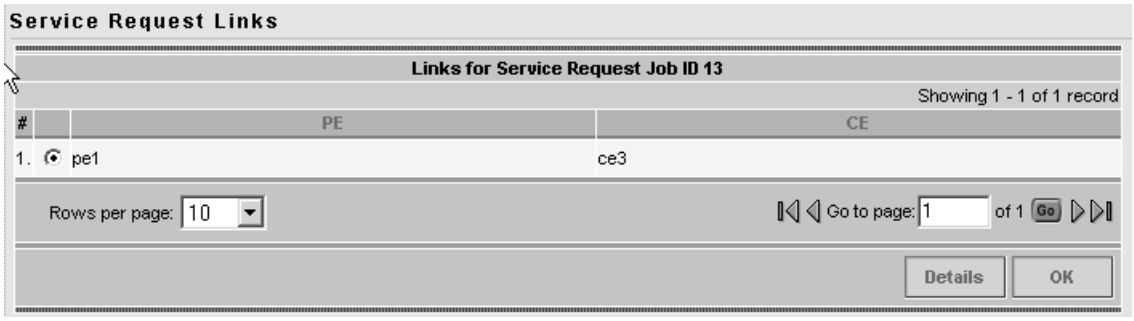
- Links—The link endpoint details.
- History—Service request history report
- Audit—Audit reports for the link IDs
- Configlets—View the ISC generated configlet for the QoS service request

The following sections describe the links, history, and configlet details for a QoS service request. The audit details are described in QoS Configuration Auditing, page 5-1.

Links

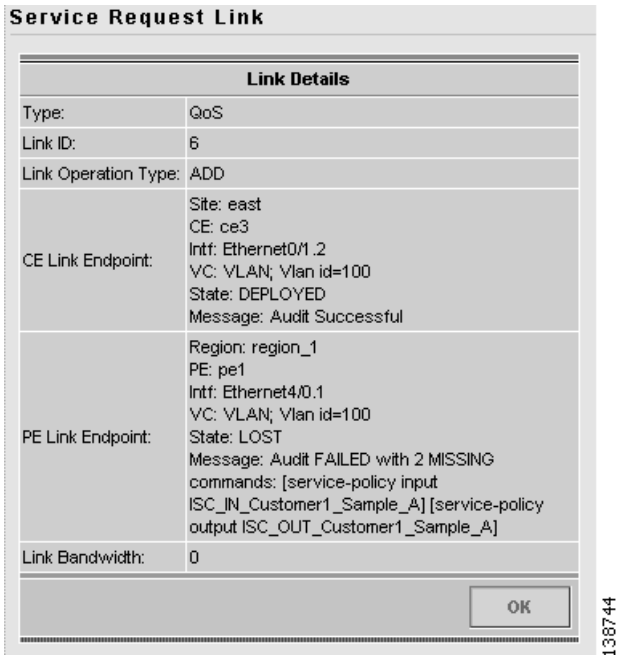
Service Request links are displayed in the Service Request Links window (Figure 5-7).

Figure 5-7 QoS Service Request Links



Click **Details** to display the devices marked with link QoS settings for this service request (Figure 5-8).

Figure 5-8 Service Request Link Details

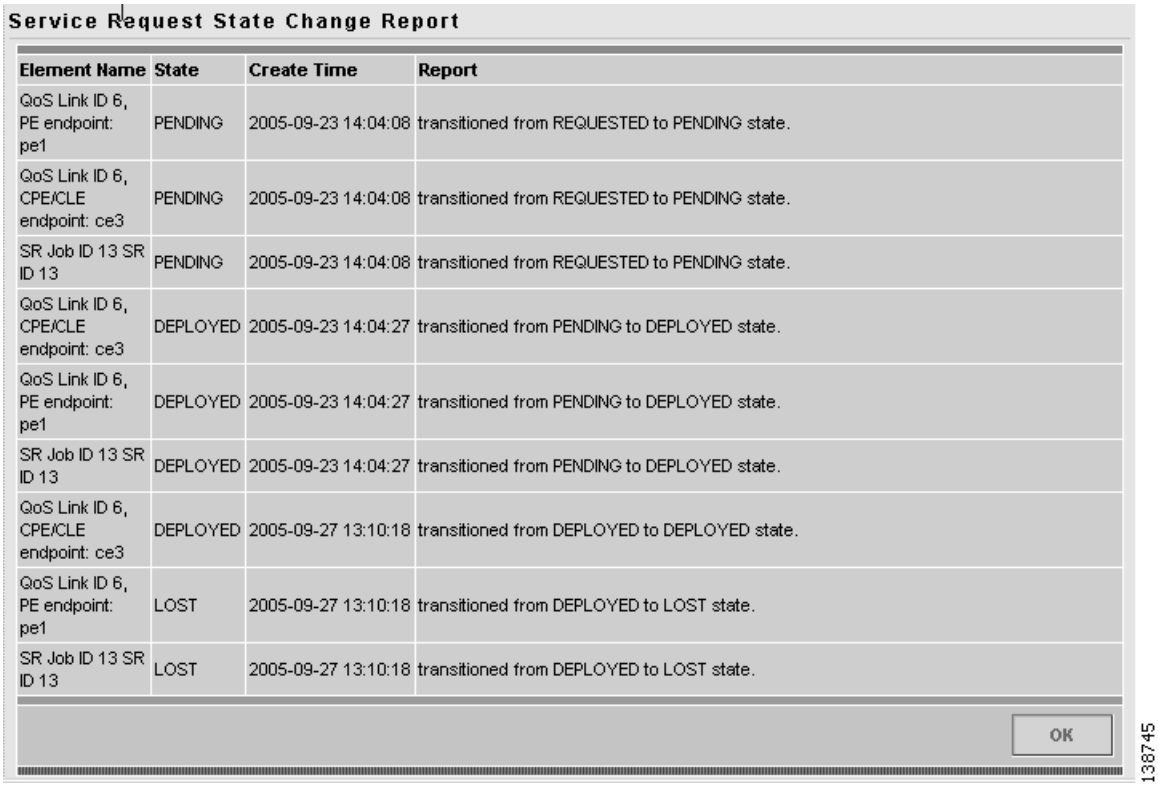


Click **OK** (twice) to return to the Service Request Details page.

History

Figure 5-9 shows the Service Request History Report window.

Figure 5-9 Service Request History Report



Service Request State Change Report

Element Name	State	Create Time	Report
QoS Link ID 6, PE endpoint: pe1	PENDING	2005-09-23 14:04:08	transitioned from REQUESTED to PENDING state.
QoS Link ID 6, CPE/CLE endpoint: ce3	PENDING	2005-09-23 14:04:08	transitioned from REQUESTED to PENDING state.
SR Job ID 13 SR ID 13	PENDING	2005-09-23 14:04:08	transitioned from REQUESTED to PENDING state.
QoS Link ID 6, CPE/CLE endpoint: ce3	DEPLOYED	2005-09-23 14:04:27	transitioned from PENDING to DEPLOYED state.
QoS Link ID 6, PE endpoint: pe1	DEPLOYED	2005-09-23 14:04:27	transitioned from PENDING to DEPLOYED state.
SR Job ID 13 SR ID 13	DEPLOYED	2005-09-23 14:04:27	transitioned from PENDING to DEPLOYED state.
QoS Link ID 6, CPE/CLE endpoint: ce3	DEPLOYED	2005-09-27 13:10:18	transitioned from DEPLOYED to DEPLOYED state.
QoS Link ID 6, PE endpoint: pe1	LOST	2005-09-27 13:10:18	transitioned from DEPLOYED to LOST state.
SR Job ID 13 SR ID 13	LOST	2005-09-27 13:10:18	transitioned from DEPLOYED to LOST state.

OK

138745

The history report shows the following information about the service request:

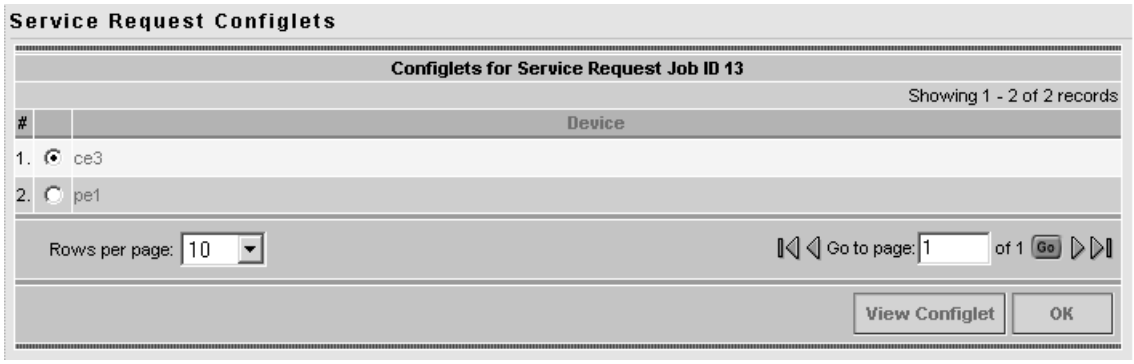
- Element name—The device, interface, and subinterfaces participating in this service request.
- State—The transition states the element has gone through.
- Create Time—The time the element was created for this service request.
- Report—The action taken by ISC for the element in this service request.

Configlets

To view QoS configlets:

Step 1 Click **Configlets** on the Service Request Details window. The Service Request Configlets window appears (Figure 5-10).

Figure 5-10 Service Request Configlets

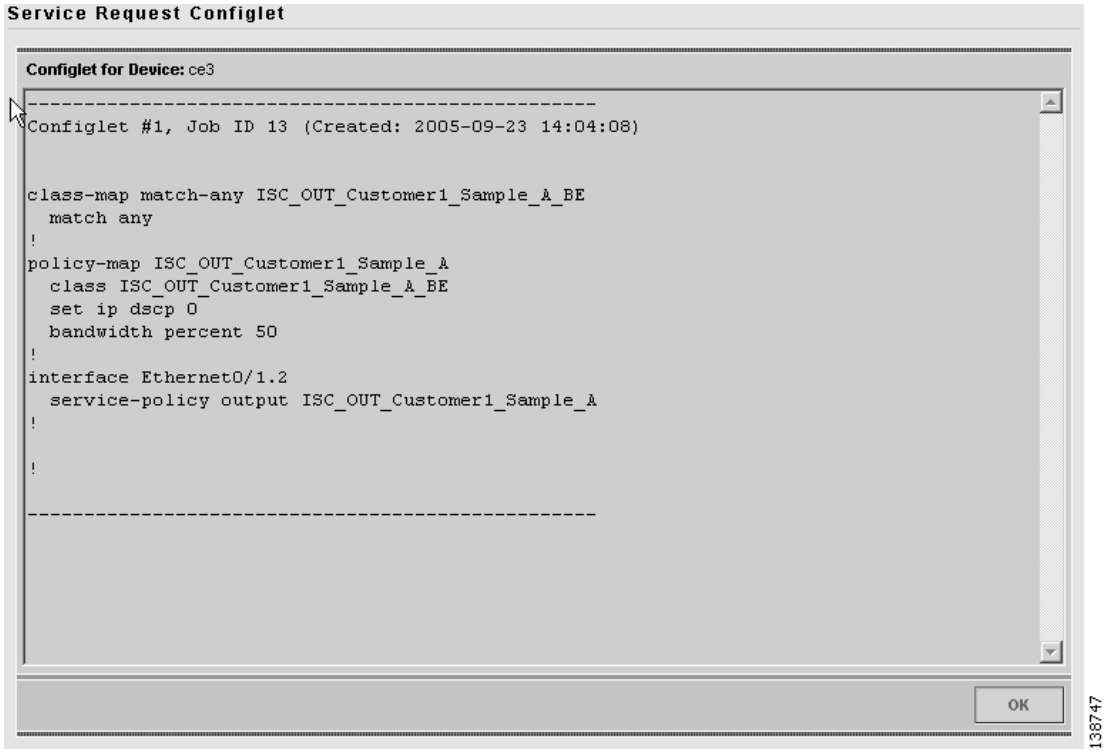


This window shows all devices whose configuration is affected by the service request.

Step 2 Select the device to view the configlet.

Step 3 Click **View Configle**t. The Configlet for Device window appears (Figure 5-11).

Figure 5-11 QoS Configlet Example



The device configlet shows all commands downloaded to the device configuration during the service request deployment operation.

Note For Ethernet QoS, access lists corresponding to the Traffic Classifications **All IP Traffic** and **All Mac Traffic** are generated only once for a device and not each time a service request is deployed to that device. As a result, these access lists will not be removed from the device when you decommission a service request.

Step 4 Click **OK** to exit.

QoS Task Logs

Use the task logs to help you troubleshoot why a service request has failed or to find more details about a service request. This section describes how to view the task logs generated for configuration messages.

There are two ways to access the task logs:

- From Service Inventory > Inventory and Connection Manager > Service Requests
  This is easier if you are already working in the Service Requests window.
- From Monitoring > Task Manager

To access the task logs:

Step 1 Use one of the following:

- From the Service Requests window, click the **Status** button and select **Logs**
- From the Task Manager window, select **Logs** in the TOC at far left

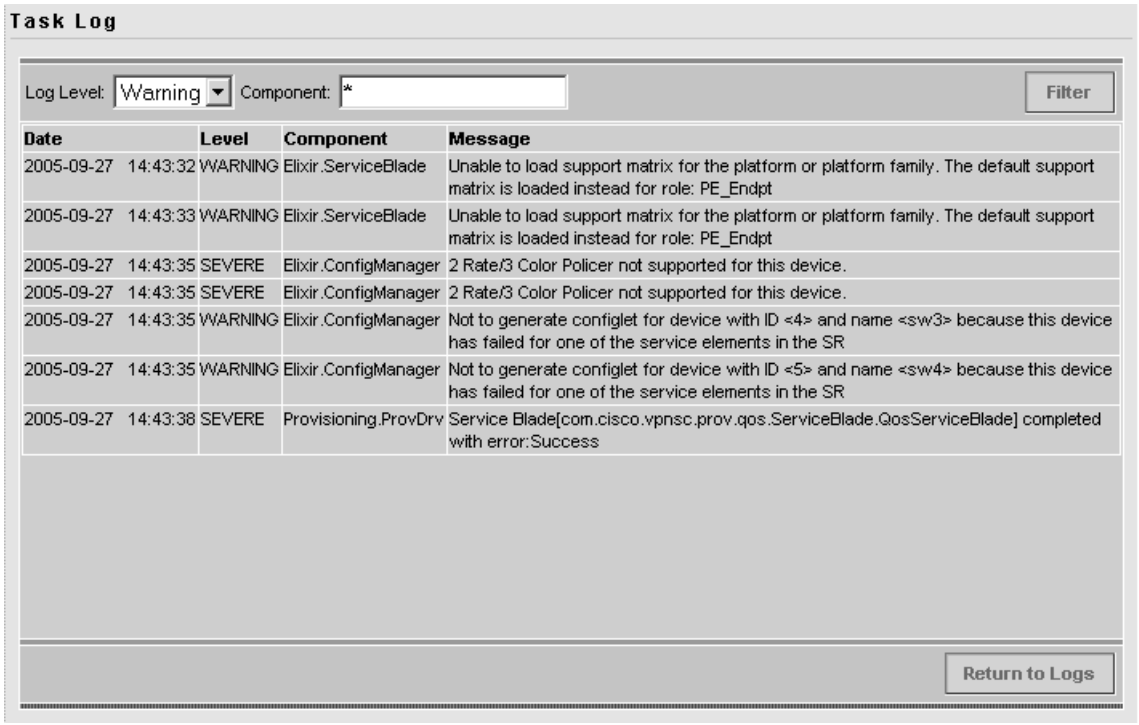
Step 2 Select the task to view the logs for and click **Instances**.

Step 3 Select the log to view and click **Log**. The Task Log window appears.

Step 4 Select the log level from the drop-down menu and click **Filter**. The log levels are All, Severe, Warning, Info, Config, Fine, Finer, Finest.

Figure 5-12 shows an example of the information contained in an ISC task log.

Figure 5-12 Task Log Example



Step 5 For example, this window shows the task log for a service request that failed audit.

Step 6 To exit from task logs, click **Task Manager** above the TOC to the left of the main window.

Network Architecture and Service Model

A service provider network architecture contains access routers, distributed routers and core routers or ATM switches. Access routers terminate customer connections at the edge of the network.

IP QoS provisioning with the Cisco IP Solution Center (ISC) is configured on the access circuit that involves the access router (provider edge devices, or PEs) in the service provider network and the customer equipment (CEs) in the customer network.

Ethernet QoS provisioning with ISC supports a subset of the features required for the Metro Ethernet 3.1 Solution. With Ethernet QoS, ISC can deploy QoS Policies on Cisco Catalyst switches in a provider's network.

This appendix includes the following sections:

IP QoS

This section describes network architecture and service model for IP QoS in ISC.

It includes the following sections:

The section contains the following subsections:

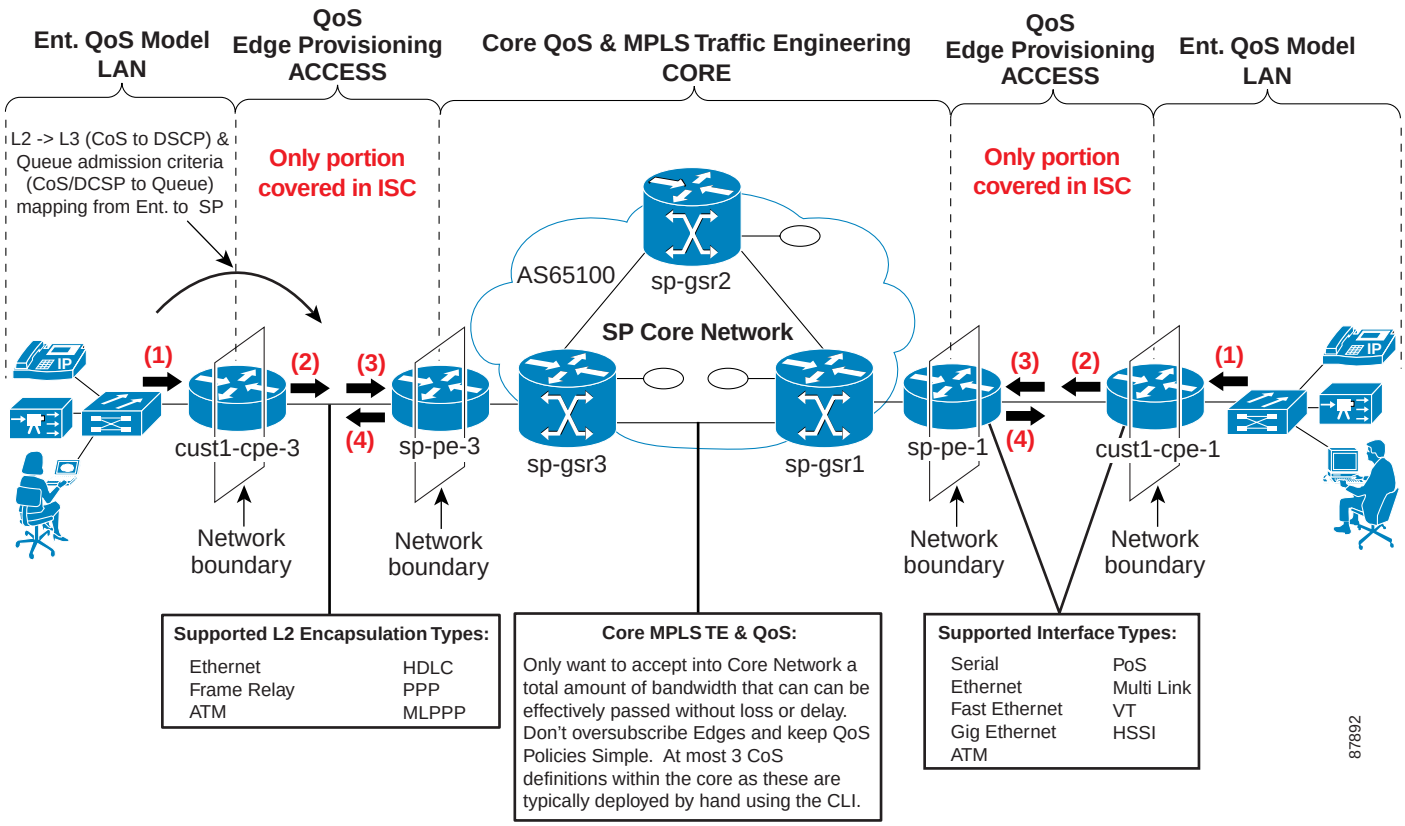
IP QoS Service Provider Network Architecture

The service provider network architecture, supported within the scope of the IP QoS provisioning model in ISC is:

- Access circuit (CEs)
- Distribution routers (PEs)
- Core (routers and ATM switches)

These QoS components and concepts are represented in Figure A-1.

Figure A-1 QoS Components and Concepts



IP QoS Service Model Overview

The IP QoS service model in ISC is designed so that QoS provisioning is implemented for traffic that enters the access circuit at the network edge (CE), and through the distribution portion (the CE-PE link).

This section provides an overview of the IP QoS service model in ISC.

The ISC implementation of IP QoS provisioning involves traffic through several different types of devices, link speeds, and encapsulation types. For this reason, an ISC QoS policy is divided into two categories:

- Service level IP QoS policy–The service level policy corresponds to IP QoS service classes. QoS service classes provide a method for classifying traffic.

  Typically, a service provider creates three or four service classes for each QoS policy. For example, a service provider might have a platinum, gold, silver, and bronze QoS policies, and each of these policies might contain 3 service classes; a VoIP, a management, and a data service class (Best-Effort or Business-Data-1).

- Link level QoS policy—The link level QoS policy is a grouping of QoS parameters that are sensitive to the CE-PE link's bandwidth and layer 2 encapsulation. Link level parameters include Frame Relay traffic shaper, ATM shaper, FRF.12, LFI over MLPPP, cRTP, and interface-based rate limiting.

  Typically, a service provider creates several link level QoS settings. For example, a service provider might create a link QoS setting for different bandwidths and encapsulation types, such as; FR_64K_gold, FR_64K_silver, FR_128K_bronze, ATM_1MBPS_gold, and Ethernet_2mbps_Silver.

ISC provides two levels of QoS policies because a QoS service request might contain one or more links with different circuit bandwidths and encapsulation types. The service level policy is designed for a type of service, like voice, but can apply to more than one link type. The link level policy is designed for different link speeds, like 1 Mbps, and can apply QoS provisioning per link.

To provision QoS parameters for devices in a service request, a network operator must:

- Select the appropriate service level QoS policy
- Associate a corresponding link level policy with each link in the service request.

  For example, if the QoS service request is comprised of two links; a Frame Relay link with a bandwidth of 64kbps, and an ATM link, with a bandwidth of 1 mbps, and the service level agreement (SLA) purchased by the enterprise customer is the Gold policy, the following settings might be associated with the QoS service request:

  - Gold service level QoS policy
  - FR_64K_gold link level QoS settings tied to the Frame Relay link
  - ATM_1MBPS_gold link level QoS settings tied to the ATM link

QoS policies can either be customer-oriented or provider-oriented. Typically, service provider networks have a combination of both service level and link level QoS policies.

Service Model Components

A QoS policy is a set of parameters that control and condition the traffic flowing through a service provider network.

The Cisco IP Solution Center (ISC) configures QoS at the access circuit, which involves the PEs in the service provider network and the CEs in the customer network. A QoS policy is applied to the selected set of access circuits using a QoS service request. The ISC provisioning engine generates the QoS configuration from the service request and downloads the configuration to the specified CE and PE devices.

A QoS service request can be integrated with VPN provisioning accomplished through ISC or deployed on its own if VPN services are not provisioned through ISC.

In ISC, the IP QoS service model is comprised of:

- IP QoS Link—contains device (CE and PE) interface information.
- IP QoS Policy—ISC offers two different levels of polices. Most networks have a combination of both policy types.
  - Service level QoS policy—The part of the QoS policy where you define service classes for the different service level agreements (SLA) purchased by customers.
  - Link level QoS policy—The part of the QoS policy that specifies QoS parameters that are specific to the CE-PE link.
- IP QoS Service Request—a container for the link objects and QoS policies to be applied to the device.

Note To set up QoS provisioning for MPLS VPN services, see IP QoS for MPLS VPNs, page 3-28.

QoS Link Definition

A QoS Link can contain two interfaces (for both the CE and PE) or one interface (CE only or PE only). For QoS provisioning, you can select both interfaces in the CE-PE link. A typical device interface selection is as follows:

- For the CE device:
  - The provider-facing device interface is selected as the link endpoint.
  - The customer-facing LAN interface is selected for marking and rate limiting.

  Note Marking and rate limiting on the customer-facing LAN interface is optional and is done using a CE device editor as part of defining QoS link candidates.
- For the PE device:
  - The customer-facing interface is marked as a link endpoint.

The interfaces selected as link endpoints can be provisioned with QoS parameters such as policing, traffic shaping, congestion management, congestion avoidance, link efficiency, and CAR. You apply these parameters later in the provisioning process.

See Creating QoS Link Candidate Objects, page 3-2 for information on defining QoS link candidate interfaces in the ISC user interface.

Service Level IP QoS Policy

The service level portion of the QoS policy corresponds to service classes. A QoS service class provides a method for classifying traffic flows into classes so that you can apply the appropriate QoS parameters to a class of traffic instead of applying them to all traffic. For example, all TCP traffic might be grouped into a single class so that bandwidth is allocated for the class and not for individual traffic flows.

A QoS service class can include:

- Methods for classifying traffic (protocol, DSCP value, IP precedence value, source address)
- Methods for marking traffic (DSCP or IP precedence values)

- Traffic shaping parameters (average/peak, rate)
- Rate limiting parameters (mean/peak rate, burst size, conform/exceed/violate actions)
- Congestion management parameters (bandwidth and queue limit)
- Congestion avoidance parameters (drop, exponential weighing constant)

A typical service provider network might create different QoS policies, and each QoS policy might contain three to five service classes. For example, a service provider might have a gold, silver, and bronze QoS policies, each specifying different service level agreements (SLA), and each of those QoS policies might contain one or more service classes. Most networks require at least a voice, a management, and a data service class.

ISC provides five default or template service classes for you to modify and use for a service level QoS policy:

- VoIP—voice service class
- Routing Protocol—routing protocol service class
- Management—management service class
- Business-Data-1—data service class
- Best Effort—data service class

See Creating the Service Level IP QoS Policy, page 3-9 for information on defining the service level QoS policy in the ISC user interface.

The following section describes the five service classes provided with ISC.

QoS Service Classes

A QoS service class defines how each QoS parameter is applied.

Network traffic can be categorized into voice traffic, data traffic, and control traffic. Voice and data traffic are common in enterprise networks. Control traffic refers to routing protocol traffic and management traffic, which are commonly used in the service provider portion of the network.

The five default service classes provided with ISC cover most networks, which require at least one for interactive voice traffic, one for management traffic, and at least one service class for data traffic.

You can either remove or add more service classes if required. ISC supports the number of service classes defined by the Cisco differentiated services (DiffServ) architecture; up to 64 classes for DSCP traffic, and up to 8 service classes for IP Precedence traffic.

See Adding a Data Service Class, page B-20 for more information.

VoIP Service Class

Interactive voice traffic in ISC refers to any voice traffic (telephone calls, faxes) that is IP-encapsulated and sent over the network, such as Voice-over-IP (VoIP).

Mandatory QoS components for this service class:

- Traffic classification
- Marking
- Congestion management
- Rate-limiting (optional)

Routing Protocol Service Class

Routing protocol traffic refers to traffic control messages, such as route update messages, hellos, database descriptors, keepalives, and database refresh messages. We recommended the minimum bandwidth, one percent, for your routing protocol service class.

Mandatory QoS components for this service class:

- Traffic classification
- Congestion management

Management Service Class

Management traffic refers to the traffic between the management station at the provider core and the access routers. We recommended the minimum bandwidth, one percent, for your management service class.

Mandatory QoS components for this service class:

- Traffic classification
- Marking
- Congestion management

QoS parameters for the VoIP, Routing Protocol, and Management service classes are described in VoIP, Routing Protocol, and Management Service Classes, page B-2.

Business-Data-1 and Best Effort Service Classes

The two data service classes, Business-Data-1 and Best Effort, are nearly identical. The only difference between them is the Traffic Classification parameter. For Business-Data-1, traffic is classified by protocol. Best-Effort classifies all traffic.

The QoS requirements for data applications can vary. Each data application should be profiled before you determine the appropriate classification and scheduling treatment.

Mandatory QoS components for this service class:

- Traffic classification
- Marking
- Congestion management

Optional components:

- Traffic shaping or rate limiting
- Congestion avoidance

Note A typical network requires traffic shaping or rate limiting, but not both.

QoS parameters for the Business-Data-1 and Best-Effort service classes are described in Business Data and Best Effort Service Classes, page B-10.

Link Level IP QoS Policy

The link level portion of the QoS policy corresponds to QoS parameters that are sensitive to link bandwidth and the CE-PE link's encapsulation type. A link level QoS policy, called link QoS settings in the ISC user interface, provides a method for defining policies specific to the CE-PE link. For example, you might require different policies for Frame Relay and ATM links because of the different encapsulation involved.

Link level QoS parameters in ISC include:

- Link bandwidth (bandwidth specified in kbps)
- Aggregated traffic shaper types (Frame Relay traffic shapers, ATM traffic shapers, and parent level traffic shapers for nested policies)

Note Aggregated traffic shapers are different from class-based traffic shapers. Aggregated traffic shapers apply to traffic through a particular CE-PE link. Class-based traffic shapers apply to all traffic specified in the service class.

- Link efficiency settings (FRF.12, LFI on MLPPP, and cRTP)
- Interface-based aggregated rate limiters (traffic classification, direction, mean rate, burst size, and conform/exceed action)

Note Interface-based aggregated rate limiters are different from class-based rate limiters. Interface-based aggregated rate limiters apply to traffic through a particular CE-PE link. Class-based rate limiters apply to all traffic specified in the service class.

Aggregated Traffic Shapers

Aggregated traffic shaping allows you to control the traffic leaving an interface. You can select an aggregated traffic shaper for each CE-PE link.

Aggregated traffic shapers are optional. ISC supports the following aggregated traffic shapers:

- Frame Relay traffic shaper, or FRTS
- FRTS (non-MQC Based)
- Parent level Class-based Shaper
- ATM traffic shaper (VBR-rt)
- ATM traffic shaper (VBR-nrt)
- ATM traffic shaper (CBR)
- ATM traffic shaper (ABR)

See Aggregated Traffic Shapers, page B-21 for more information on defining the aggregated traffic shapers parameters in the ISC user interface.

Link Efficiency

Link efficiency settings are based on the bandwidth of the CE-PE link itself and are used to minimize serialization delay on the link. ISC uses methods of fragmentation and compression to minimize this delay.

ISC supports the following link efficiency settings:

- LFI on Frame Relay (FRF.12)–Supports the transport of real-time voice and data traffic on Frame Relay virtual circuits (VCs) without causing excessive delay to the real-time traffic.
- LFI on MLPPP—Multilink PPP (MLPPP) provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLPPP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.
- cRTP header compression–cRTP compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 5 bytes. Use cRTP on any WAN interface where bandwidth is at a premium and much of the traffic is RTP traffic.

See Link Efficiency Settings, page B-30 for information on defining the link efficiency parameters in the ISC user interface.

Interface-Based Aggregated Rate Limiters

Interface-based aggregated rate limiters allow you to control the maximum rate of traffic sent or received on an interface for the CE-PE link. You can also specify traffic handling policies for when the traffic conforms or exceeds the specified rate limit.

Aggregate rate limits match all packets or a subset of packets on an interface or subinterface. To specify class-based rate limiting parameters, see Creating the Service Level IP QoS Policy, page 3-9.

ISC supports the following interface-based rate limiter parameters:

- Traffic classification
- Direction
- Mean rate
- Burst sizes (conformed and extended)
- Conform and exceed actions

See Interface-Based Aggregated Rate Limiters, page B-31 for information on defining the interface-based rate limiters in the ISC user interface.

IP QoS Service Requests

An IP QoS service request contains one or more QoS links. Each link can optionally be associated with a link QoS setting. A QoS policy can be associated with a QoS service request.

An IP QoS service request should:

- Contain an IP QoS policy
- All links in the service request can be associated with a link QoS setting

To apply IP QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

See Creating an IP QoS Service Request, page 3-20 for information on creating the QoS service request using the ISC user interface.

See *Cisco IP Solution Center Infrastructure Reference, 4.0* for more information on the ISC Repository.

IP QoS Provisioning Strategies

ISC configures IP QoS at the access circuit, which involves the PE devices in the service provider network and the CE devices in the customer network. A QoS policy is applied to the selected set of access circuits using a QoS service request.

Typically, the points of congestion in the access circuit are:

- The provider-facing interface on the CE, with traffic flowing from the CE to the PE (egress traffic).
- The customer-facing interfaces on the PE, with traffic flowing from the PE to the CE (egress traffic).

This section describes a QoS provisioning strategy: where the congestion points in the network might be, where to apply QoS parameters, and which QoS provisioning components to use.

Managed CE Scenario

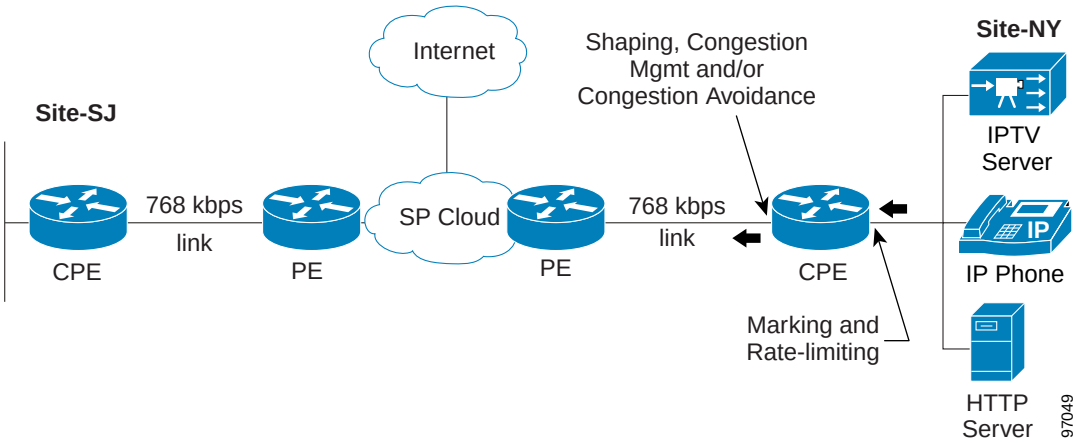
A managed CE scenario occurs when the CE is owned and managed by the service provider. In this network scenario, you can either apply QoS provisioning for the CE only or for both the CE and PE.

This section describes QoS provisioning strategies for both CE only and CE-PE scenarios.

Managed CE Only

Figure A-2 illustrates a network where QoS provisioning is configured only for the managed CE device.

Figure A-2 Managed CE Scenario



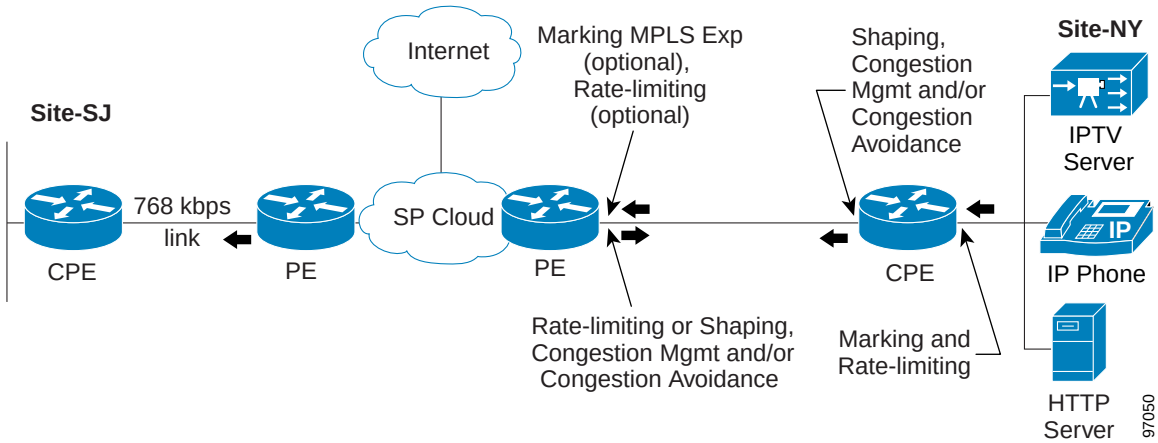
In this QoS provisioning scenario:

- Optionally configure marking and rate limiting at the customer-facing CE interface so that packets can be marked before they are encapsulated by the IPSec, GRE, and L2F and L2TP tunnels. **- IPsec and GRE are not supported in this release. -**
- Configure traffic shaping, congestion management, and congestion avoidance at the provider-facing CE interface and subinterfaces.

Managed CE and PE

Figure A-3 illustrates a network where QoS provisioning is configured for both the managed CE and the PE device.

Figure A-3 Managed CE and PE Scenario



In this QoS provisioning scenario:

- For traffic flowing from the CE to the PE, marking and rate-limiting are configured at the customer-facing CE interfaces, while traffic shaping, congestion management, and congestion avoidance are configured at the provider-facing CE interfaces and subinterfaces.
- For traffic flowing from the PE to the CE, QoS configuration is applied at customer-facing interfaces and subinterface for the PE. The configuration at the PE interfaces might be symmetrical to what is configured at provider-facing interfaces of a CE, but it is not required.
- If you are provisioning QoS for an MPLS VPN and you enable MPLS marking in the service level QoS policy, marking with MPLS experimental values is configured at the customer-facing PE interfaces and subinterfaces for traffic flowing from CE to PE.

Unmanaged CE Scenario

An unmanaged CE scenario occurs when the CE is not owned by the service provider, but ISC is aware of the device configuration and interface information. This information must be provided by the owner of the CE device.

In this QoS provisioning scenario:

- You must first create the CE device in ISC so that the device configuration and interface information can be stored in the ISC repository. A configlet is generated for the unmanaged CE, however, the configlet is not downloaded to the unmanaged CE device. A configuration audit is not performed for the unmanaged CE device.

  See *Cisco IP Solution Center Infrastructure Reference, 4.0* for more information on manually creating CE devices.

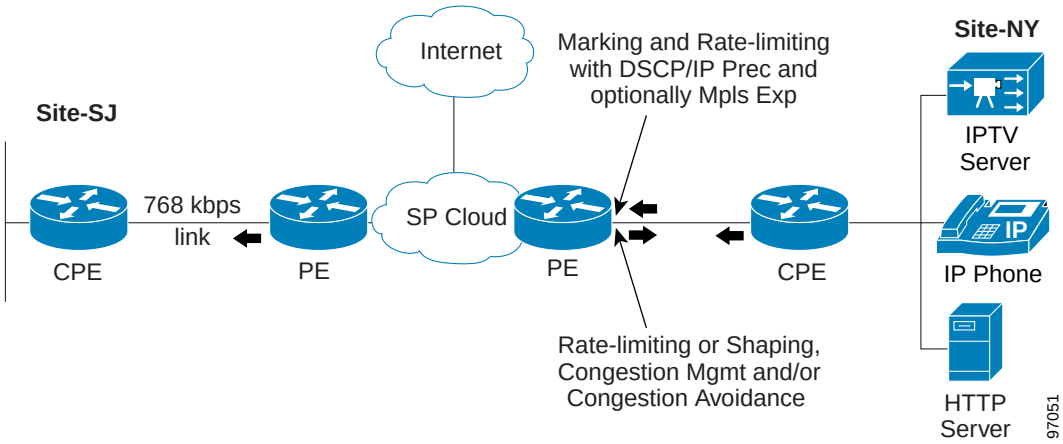
- An untrusted CE is either not managed by the service provider or is only partially-managed by the service provider. We recommend that you re-mark and re-rate limit at the provider ingress interface for the untrusted CE device. Configure the re-marking and re-rate limiting parameters in the service level policy.

  See Creating the Service Level IP QoS Policy, page 3-9 for more information.

PE Only Scenario

For a PE only scenario, the service provider's enterprise customer is responsible for applying the QoS configuration at the CE interfaces.

Figure A-4 PE Only Scenario



In this QoS provisioning scenario:

- For traffic flowing from the CE device to the PE device, configure marking and rate-limiting at customer-facing interfaces of the PE device.
- For traffic flowing from the PE device to the CE device, configure traffic shaping, rate-limiting, congestion management, and congestion avoidance at the same customer-facing interfaces and subinterfaces of the PE device.

See Chapter 3, "Provisioning Process for IP QoS," for more information on the QoS provisioning process.

Ethernet QoS

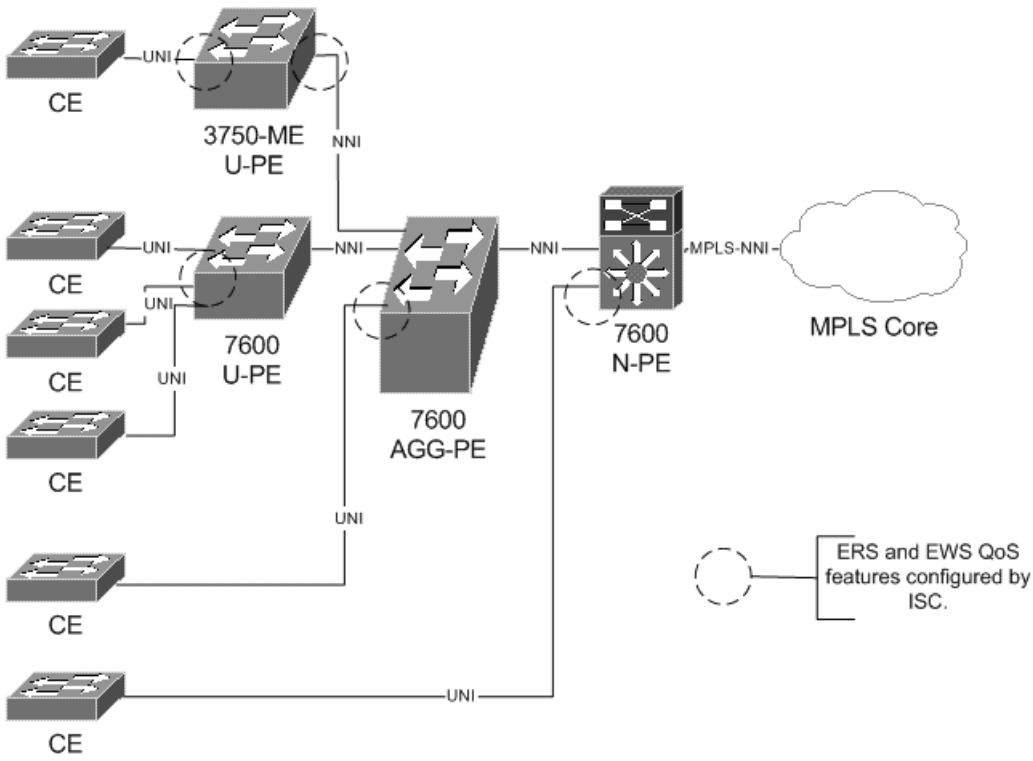
This section describes network architecture and service model for Ethernet QoS in ISC.

It includes the following sections:

Service Provider Network Architecture

In the Ethernet QoS implementation of ISC, the 3750-ME and 7600 devices can fulfill different roles as shown in Figure A-5.

Figure A-5 ISC Ethernet Network Diagram



The traffic flow is from the CE switches towards the MPLS/IP core. In general, QoS will be applied to the UNI interfaces for the ingress direction.

An exception hereto is UNI-NNI traffic on the 3750 ME switch. In this case, the policies would be situated on the enhanced ES ports on the egress direction.

Ethernet QoS Service Model Overview

Provisioning with Ethernet QoS involves traffic through several different types of devices, link speeds, and encapsulation types. For this reason, an ISC QoS policy is divided into two categories:

- Service level Ethernet QoS policy
- Link level Ethernet QoS policy

The Ethernet QoS service model in ISC is implemented for traffic that enters the User Network Interface(UNI) and either goes out to the Network-to-Network Interface(NNI) or is switched locally within the U-PE.

Ethernet QoS policies correspond to Ethernet QoS service classes. Each QoS service class provides a method to classify, mark, condition, queue, and schedule traffic based on specified criteria, such as Class of Service, VLAN ID, etc.

A typical service provider network might create different QoS policies, and each QoS policy might contain three to four service classes. For example, a service provider might have gold, silver, and bronze QoS policies, each specifying different service level agreements (SLA), and each of those QoS policies might contain one or more service classes. Most networks require at least a voice and a data service class.

To provision Ethernet QoS parameters for devices in a service request, a network operator must:

- Create an Ethernet QoS Policy as described in Creating an Ethernet QoS Policy, page 4-3.
- Create a link QoS policy, if needed.
- Create a QoS service request.
- Select a customer.
- Select a service request for L2VPN, VPLS, or MPLS (the service request must already exist).
- Select a QoS Policy created for Ethernet QoS.
- Select a link QoS policy, if needed.
- Save the service request.
- Deploy the service request.

Ethernet QoS policies can either be customer-owned or provider-owned.

For more information on the Ethernet QoS service model, see Chapter 4, “Provisioning Process for Ethernet QoS.”

QoS Link Definition

An Ethernet QoS Link can contain two interfaces (for both the U-PE and N-PE) or one interface (U-PE only or N-PE only). For Ethernet QoS provisioning, you can select both interfaces. A typical device interface selection is as follows:

For the U-PE device:

- The provider-facing device interface is selected as the link endpoint.
- The customer-facing LAN interface is selected for marking and rate limiting.

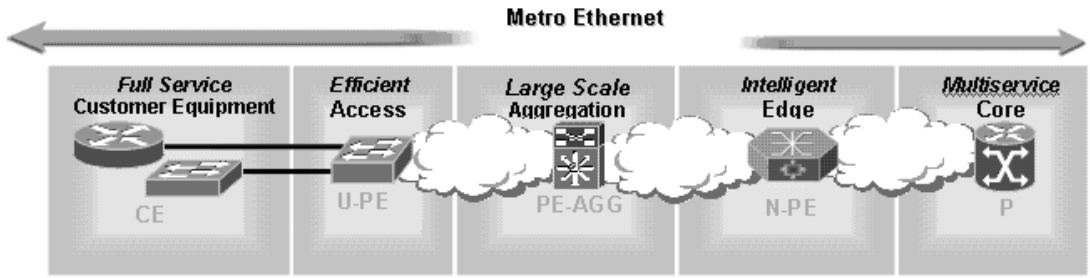
Service Model Components

In ISC, the Ethernet QoS service model is comprised of:

- Ethernet QoS Link—Contains device interface information.
- Ethernet QoS Policy—ISC offers two different levels of polices. Most networks have a combination of both policy types.
  - Service level QoS policy—The part of the QoS policy where you define service classes for the different service level agreements (SLA) purchased by customers.
  - Link level QoS policy—The part of the QoS policy that defines link-specific QoS parameters.
- Ethernet QoS Service Request—A container for the link objects and QoS policies to be applied to the device.

Figure A-6 shows a high-level view of an Ethernet network, sometimes referred to as a Metro Ethernet network, where ISC is used to apply Ethernet QoS.

Figure A-6 ISC Ethernet Network Diagram



Terminology

To understand the Ethernet QoS service model used in ISC, one needs to be familiar with the following terminology.

Devices

The following device types are used in Ethernet QoS for ISC:

- U-PE—User Facing Provider Edge within the Access layer.
- PE-AGG—Provider Edge Aggregation within the Aggregation layer.
- N-PE—Network Facing Provider Edge within the Edge layer.
- P—Provider Core within the Core layer.

Interfaces

The following interface types are used in Ethernet QoS for ISC:

- User Network Interface (UNI)—The physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.
- Network to Network Interface (NNI)—The physical network port which connect between the Service Provider devices.
- Ethernet Network to Network Interface (E-NNI)—An Ethernet NNI.
- MPLS Network to Network Interface (MPLS-NNI)—A MPLS NNI.

Service Definitions

Following the MEF (Metro Ethernet Forum) approach, the services that comprise the Metro Ethernet 3.1 solution can be classified into two general categories:

- Point-to-Point (PTP)—Services of this connection type consist of a single point-to-point Ethernet circuit provisioned between two User Network Interfaces (UNIs).
- Multipoint-to-Multipoint (MPtMP)—Services of this connection type consist of single multipoint-to-multipoint Ethernet circuit provisioned between two or more UNIs. When there are only two UNIs in the circuit, more UNIs can be added to the same EVC if required, which distinguishes this from the point-to-point type.

In the MEF terminology this maps to the following Ethernet service types:

- Ethernet Line Service Type (E-Line)—A point-to-point Ethernet service
- Ethernet LAN Service Type (E-LAN)—A multipoint-to-multipoint Ethernet service

Within these two service types, Metro Ethernet services can be created by assigning values to a set of attributes grouped according to:

- User Network Interface (UNI)—The physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.
- Ethernet Virtual Connection (EVC)—An association of two or more UNIs that limits the exchange of Service Frames to UNIs within the EVC.

Service Level Ethernet QoS Policy

The service level portion of the QoS policy corresponds to service classes. A QoS service class provides a method for classifying traffic flows into classes so that you can apply the appropriate QoS parameters to a class of traffic instead of applying them to all traffic. For example, all TCP traffic might be grouped into a single class so that bandwidth is allocated for the class and not for individual traffic flows.

A QoS service class can include:

- Methods for classifying traffic (protocol, DSCP value, IP precedence value, source address)
- Methods for marking traffic (DSCP or IP precedence values)
- Rate limiting parameters (mean/peak rate, burst size, conform/exceed/violate actions)
- Congestion management parameters (bandwidth and queue limit)

A typical service provider network might create different QoS policies, and each QoS policy might contain three to five service classes. For example, a service provider might have a gold, silver, and bronze QoS policies, each specifying different service level agreements (SLA), and each of those QoS policies might contain one or more service classes.

You can create real time, business critical, and best effort classes, etc., within a policy.

See Creating Ethernet QoS Policies, page 4-3, for information on defining the service level Ethernet QoS policy in the ISC user interface.

Link Level Ethernet QoS Policy

The link level portion of the QoS policy corresponds to QoS parameters that are sensitive to link bandwidth and the UNI's encapsulation type. A link level QoS policy, called link QoS settings in the ISC user interface, provides a method for defining link-specific policies. For example, you might require different policies for Frame Relay and ATM links because of the different encapsulation involved.

Link level QoS parameters in ISC include:

- VLAN bandwidth (in kbps or %) (3750-ME only)
- VLAN shaper (3750-ME only)
- Port trust
- CoS mutation (7600 only)

Ethernet QoS Service Requests

An Ethernet QoS service request contains one or more QoS links. Each link can optionally be associated with a link QoS setting. A QoS policy can be associated with a QoS service request.

An Ethernet QoS service request should:

- Contain an Ethernet QoS policy
- All links in the service request can be associated with a link QoS setting

To apply Ethernet QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

See Creating an Ethernet QoS Service Request, page 4-13 for information on creating the QoS service request using the ISC user interface.

See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information on the ISC Repository.

IP QoS Policy Parameters

This appendix describes the parameters, both required and optional, for IP QoS provisioning using the Cisco IP Solution Center (ISC) user interface.

This appendix contains the following sections and subsections:

Note For information on service level Ethernet QoS parameters, see Service Level Ethernet QoS Parameters, page C-1.

Service Level IP QoS Parameters

Service level IP QoS parameters see the entry fields on the service class windows and dialog boxes. These parameters include all entry fields in the VoIP, Management, Routing Protocol, Business-Data-1 and Best Effort service classes, and the traffic classification options for data service classes.

You must enter the bandwidth parameter for all service classes. Typically, a value of one percent is sufficient for Routing Protocol traffic. However, it is common for customers or providers to combine the Management and Routing Protocol into one service class policy. In this case, a larger percentage of bandwidth might be required.

Any class of service can be a *class-default* class of service. You can simply name the class of service as *class-default* and ISC will generate the same. Bandwidth is not mandatory for this class of service. Traffic classification is assumed to be *rest of traffic.*

Note *Class-default* is a reserved class of service name in IOS and is created by IOS if ISC does not create one.

VoIP, Routing Protocol, and Management Service Classes

Each service class has a different set of entry fields. The VoIP, Routing Protocol, and Management service classes require similar parameters, and are combined in this section. Figure B-1 displays these service classes.

For Business-Data-1 and Best Effort service class entry fields, see Business Data and Best Effort Service Classes, page B-10. The window you see depends on the service class being edited.

Figure B-1 Edit VoIP Service Class

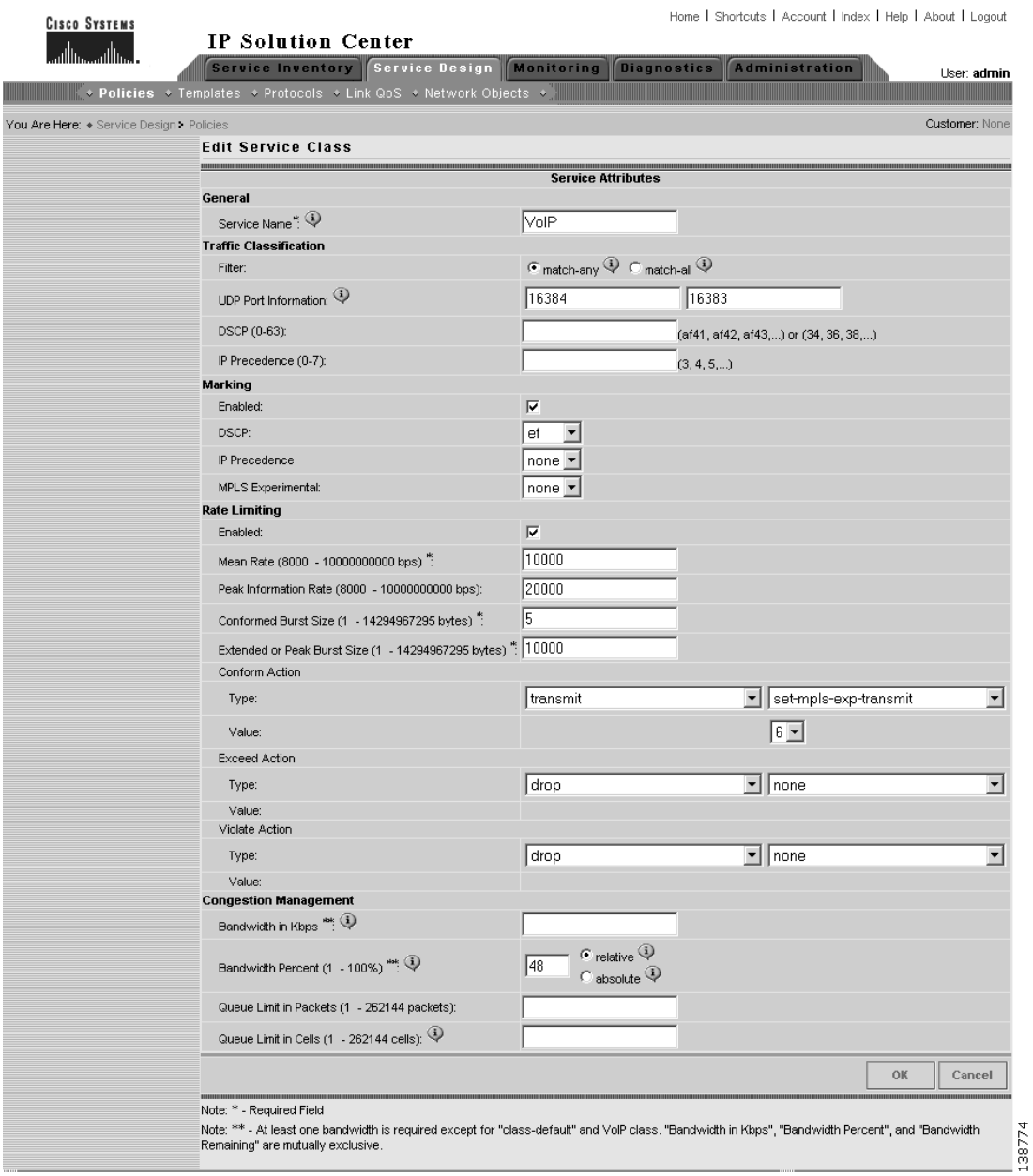


Table B-1 describes the entry fields for the VoIP, Routing Protocol, and Management service classes.

Table B-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management)

Entry Field	Description
General	
Service Name	The name of the service class (VoIP, Routing Protocol, Management, or the name of your choice).
Traffic Classification (Routing Protocol service class only)	Traffic classification based on routing protocol. Choose from the list of routing protocols. Click **Edit** to activate one or more of the following routing protocols: RIP, BGP, OSPF, EIGRP. These options are further described in Editing the Routing Protocol Service Class, page B-7.
Traffic Classification	
Filters:	**match-any:** Traffic classification passes when any one of the following classifications is met. **match-all:** Traffic classification passes when all of the below classifications are met. This is restrictive; for example, combination of UDP Port and DSCP makes sense but not UDP Port and DSCP and IP_Precedence because an IP packet cannot have DSCP and IP_Precedence values at the same time.
UDP Port Information (VoIP service class only)	On routers supporting MQC these two fields see “lower bound UDP port” and “upper bound UDP port”. On non-MQC routers, the two fields see port range.
DSCP (VoIP and Management service classes only)	Traffic classification based on the packet’s DSCP marking.
IP Precedence (VoIP and Management service classes only)	Traffic classification based on the packet’s IP Precedence marking.
Management LAN Address (Management service class only)	Traffic classification based on management LAN address.
Marking (VoIP and Management service classes only)	
Enabled	Enable packet marking.
DSCP	Mark packets with a DSCP value. **Note** You can mark packets with either DSCP or IP Precedence, but not both.
IP Precedence	Mark packets with an IP Precedence value.
MPLS Experimental	Mark packets with an MPLS Experimental value. This field only appears if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Rate Limiting (VoIP service class only)	
Enabled	Enable rate-limiting
Mean Rate	The long-term average transmission rate.

Table B-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)

Entry Field	Description
Peak Information Rate	Allows support for sustained excess rate.
Conformed Burst Size	How large traffic bursts can be before some traffic exceeds the rate limit. **Note** IOS silently re-adjusts the conformed burst size to the MTU size of the interface if the MTU is greater than the conformed burst size entered in the ISC IP Link QoS Settings for Interface-based Aggregated Rate Limiter. The ISC QoS service request will then go to Failed-Audit. Ensure that the conformed burst size is greater than the interface MTU size.
Extended or Peak Burst Size	How large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the conformed burst size and the extended burst size exceeds the rate limit with a probability that increases as the burst size increases. Configure extended burst by setting the extended burst value greater than the conformed burst value.
Conform Action–Type	The action to take on packets that conform to the specified rate limit. **Single Action** • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. **Note** If you select **Set-dscp-transmit** or **Set-prec-transmit**, you must specify the DSCP or IP Precedence in the Conform-Action Value field. **Dual Action** • set-mpls-exp-transmit—Sets MPLS exp value and sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. **Note** The set-mpls fields only appear if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Conform Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Conform Action-Type.

Table B-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)

Entry Field	Description
Exceed Action–Type	The action to take on packets that conform to the specified rate limit. **Single Action** • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. **Note** If you select **Set-dscp-transmit** or **Set-prec-transmit**, you must specify the DSCP or IP Precedence in the Conform-Action Value field. **Dual Action** • set-mpls-exp-transmit—Sets MPLS exp value and sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. **Note** The set-mpls fields only appear if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Exceed Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Exceed Action-Type.

Table B-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)

Entry Field	Description
Violate Action–Type	The action to take on packets that conform to the specified rate limit. **Single Action** • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. **Note** If you select **Set-dscp-transmit** or **Set-prec-transmit**, you must specify the DSCP or IP Precedence in the Conform-Action Value field. **Dual Action** • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. **Note** The set-mpls fields only appear if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Violate Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Violate Action-Type.
Congestion Management	Routing Protocol and Management CoS can be configured with Bandwidth Remaining.
Bandwidth in kbps	The bandwidth in kbps (absolute bandwidth) for this service class. This field translates to Priority *x* and Bandwidth *x* commands where *x* is in kbps.

Table B-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)

Entry Field	Description
Bandwidth Percent	Percentage of bandwidth to dedicate to congestion management parameters. The range is 1-100 percent. Bandwidth is relative or absolute. • Relative: This field specifies the bandwidth in percentage that you need to allocate to this CoS. This corresponds to relative bandwidth commands Priority Percent *x* and Bandwidth Percent *x* where *x* is the percentage specified. • Absolute: The percentage specified is used in conjunction with the circuit (or link) bandwidth to compute the absolute bandwidth (in kbps) that needs to be allocated to this CoS. Although this field translates to the same command as that for Bandwidth in kbps, it differs as follows: the absolute bandwidth varies with the circuit (or link) bandwidth. For example, if the percentage specified is 10 and if the policy is applied to a 64 kbps link, then absolute bandwidth allocated for this CoS is 6.4 kbps. If the same policy is applied to a 128 kbps link, then the absolute bandwidth allocated for this CoS is 12.8 kbps. Thus, the policy can be used on disparate bandwidth links.
Queue Limit in Packets	Limit the queue depth of the congesting traffic. The range is 1 to 262144 packets.
Queue Limit in Cells	Limit the queue depth of the congesting traffic. The range is 1 to 262144 cells.

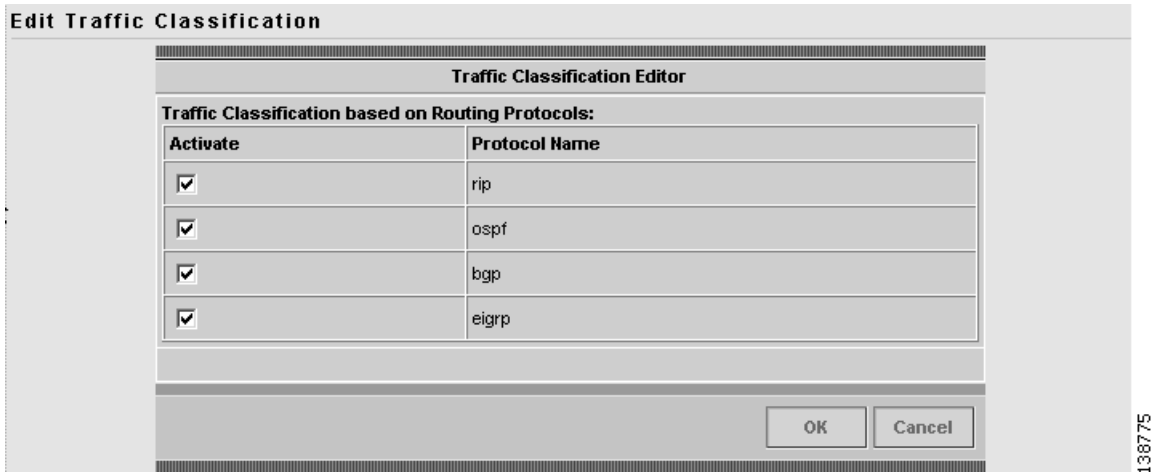
Note The process for marking packets with DSCP and IP Precedence bits is described in detail in the following document on Cisco.com:
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Editing the Routing Protocol Service Class

The Routing Protocol service class provides you with a method of classifying traffic based on the routing protocols. This is the default method for traffic classification in ISC.

Use the Edit Traffic Classification window (Policies > Edit RP > Edit Traffic Classification) to change the list of protocols to use for the Routing Protocol service class (Figure B-2).

Figure B-2 Edit Traffic Classification—Routing Protocol Service Class



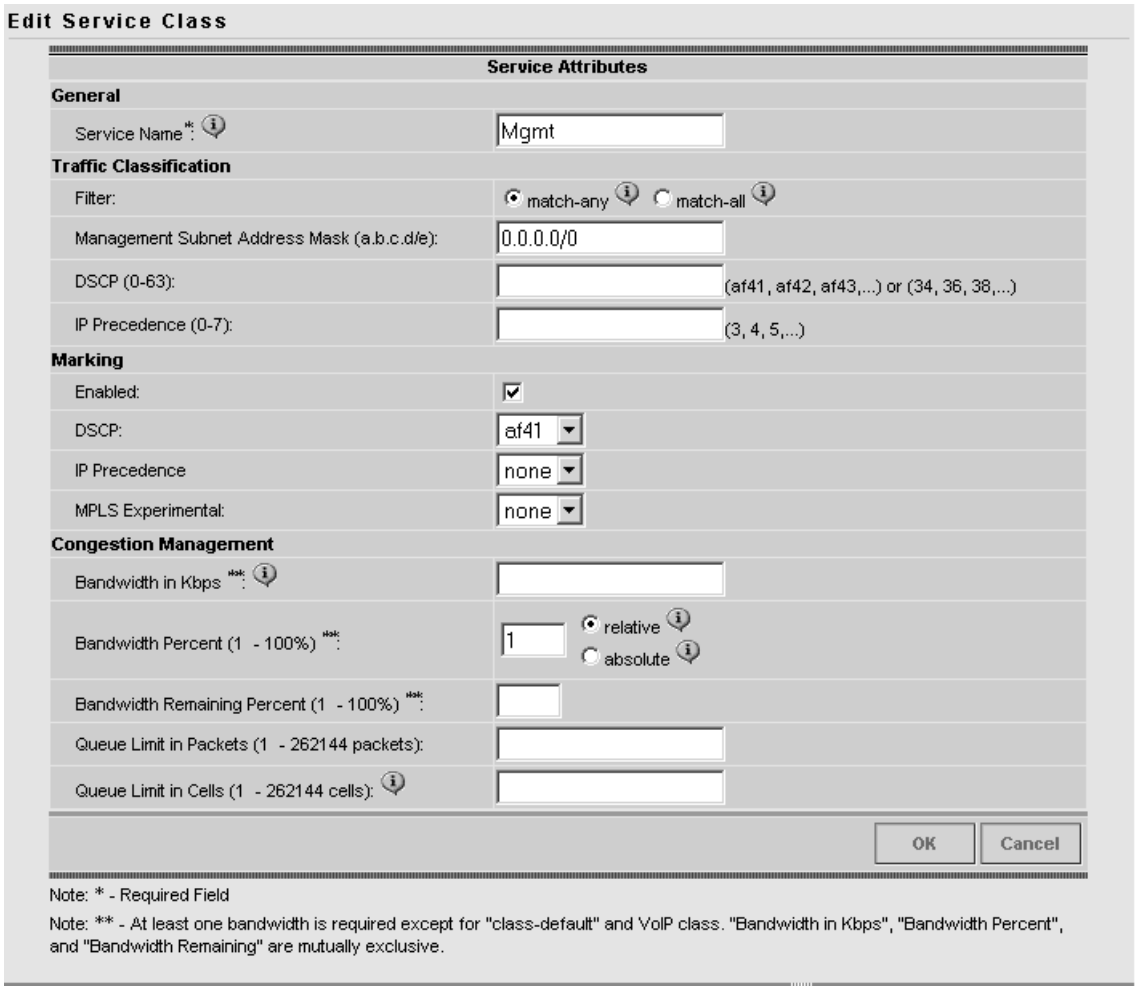
Select the routing protocols to use and click **OK**.

Editing the Management Service Class

This section describes how to edit the Management service class.

Figure B-3 shows the Edit Service Class window for the Management service class.

Figure B-3 Edit Management Service Class



Use this window to specify QoS parameters for the Management service class. The following are required fields:

- Name—This field is prepopulated with the name Management. However, you can enter a new name.
- Management LAN Address—Specifies the management LAN address for traffic classification.
- DSCP—Specifies the traffic classification based on the packet's DSCP marking.
- IP Precedence—Specifies the traffic classification based on the packet's IP Precedence marking.
- Bandwidth—Specifies the bandwidth to dedicate to congestion management parameters. See Table B-1 for an explanation of the bandwidth fields.

Note The bandwidth in kbps is an absolute bandwidth for this service class. Bandwidth specified as a percentage of link bandwidth can be an absolute value or a relative value. The percentage is converted to an absolute value (if the percent command is not supported) when the QoS configlet is generated during service request deployment.

To add another Management service class, use the **Add Data CoS** button on the Edit QoS Policy window. See Adding a Data Service Class, page B-20 for more information.

Business Data and Best Effort Service Classes

For the two data service classes, Business Data (Busin) and Best Effort (BE), the parameters are nearly identical. The entry field descriptions are combined in this section. The only difference between the two data service classes is the Traffic Classification parameter:

- Business Data classifies traffic using selected protocols, packet markings, or network addresses.
- Best Effort uses the traffic classification “All Traffic.”

For VoIP, Routing Protocol, and Management service class entry fields, see VoIP, Routing Protocol, and Management Service Classes, page B-2.

Figure B-4 shows the general information, marking, and shaping fields for the Business Data service class (Busin).

Figure B-4 Edit Business Data Service Class

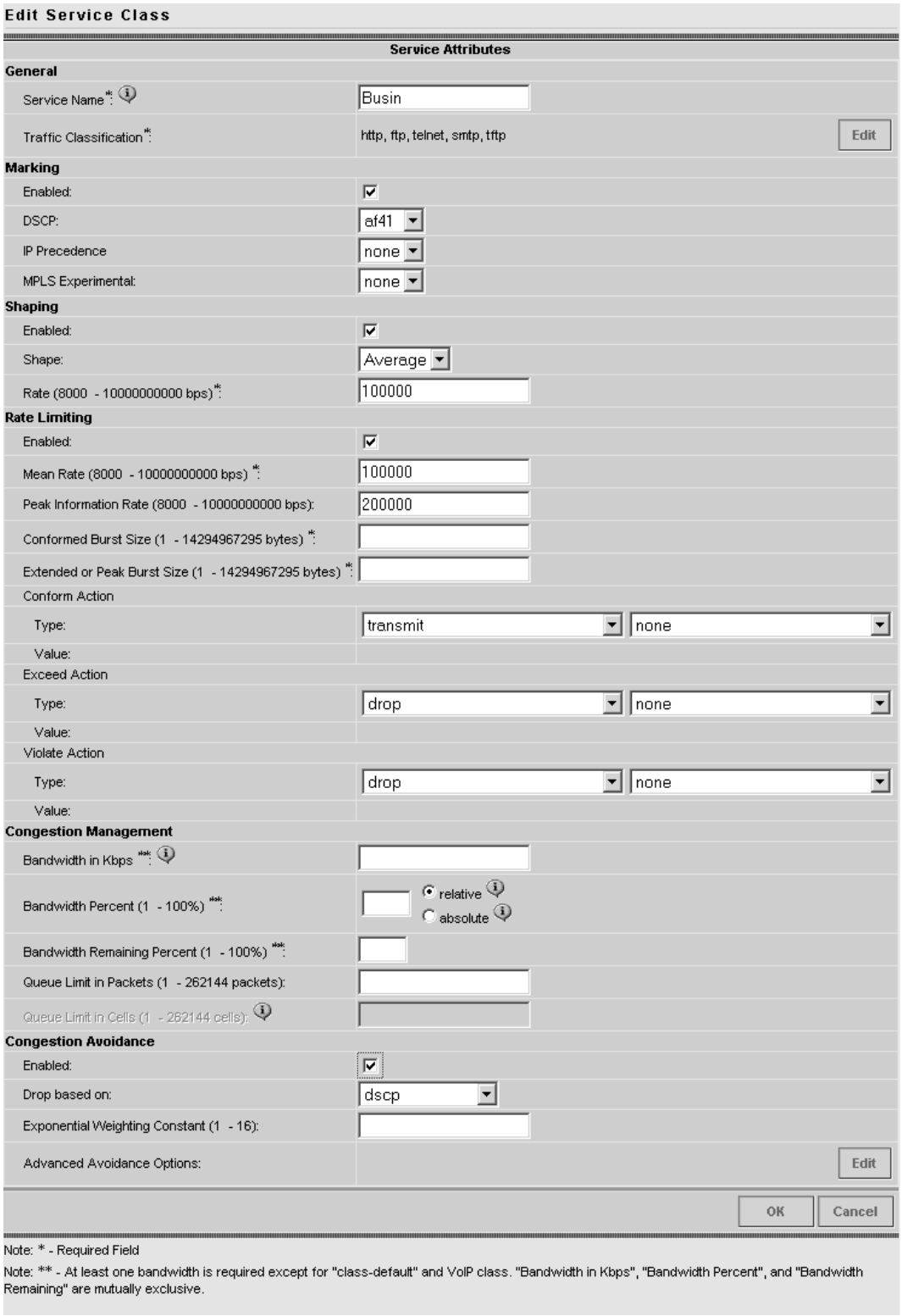


Table B-2 describes the entry fields for the data service classes. The entry fields you see depend on which service class is being edited.

Table B-2 Edit Service Class Entry Fields (Business Data and Best Effort)

Entry Field	Description
General	
Service Class	The name of the service class (Busin, BE, or the name of your choice).
Traffic Classification	Traffic classification based on protocols. Choose from the list of protocols, or add another protocol. Click **Edit** to activate one or more of the following protocols: HTTP, FTP, Telnet, SMTP, TFTP. These options are further described in Traffic Classification, page B-16.
Marking	
Enabled	Enable packet marking.
DSCP	Mark packets with a DSCP value. **Note** You can mark packets with either DSCP or IP Precedence, but not both.
IP Precedence	Mark packets with an IP Precedence value.
MPLS Experimental	Mark packets with an MPLS Experimental value. This field only appears if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Shaping	
Enabled	Enable class-based traffic shaping parameters. To specify interface-based traffic shaping parameters, see Aggregated Traffic Shapers, page B-21.
Shape	Specify average or peak rate shaping. • Average rate shaping limits the transmission rate to the committed information rate (CIR). • Peak rate shaping configures the router to send more traffic than the CIR. **Note** ISC does NOT provision ATM shapers and class-based shapers at the same time. If you configure an ATM shaper, ISC automatically turns off the class-based shaper. This shape is for class-based shaper support when the ATM shaper is not configured.
Rate	Committed information rate.
Rate Limiting	
Enabled	Enable rate-limiting
Mean Rate	The long-term average transmission rate.
Peak Information Rate	Allows support for sustained excess rate.

Table B-2 Edit Service Class Entry Fields (Business Data and Best Effort) (continued)

Entry Field	Description
Conformed Burst Size	How large traffic bursts can be before some traffic exceeds the rate limit. **Note** IOS silently re-adjusts the conformed burst size to the MTU size of the interface if the MTU is greater than the conformed burst size entered in the ISC IP Link QoS Settings for Interface-based Aggregated Rate Limiter. The ISC QoS service request will then go to Failed-Audit. Ensure that the conformed burst size is greater than the interface MTU size.
Extended or Peak Burst Size	How large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the conformed burst size and the extended burst size exceeds the rate limit with a probability that increases as the burst size increases. Configure extended burst by setting the extended burst value greater than the conformed burst value.
Conform Action–Type	The action to take on packets that conform to the specified rate limit. **Single Action** • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. **Note** If you select **Set-dscp-transmit** or **Set-prec-transmit**, you must specify the DSCP or IP Precedence in the Conform-Action Value field. **Dual Action** • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. **Note** The set-mpls fields only appear if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Conform Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Conform Action-Type.

Table B-2 Edit Service Class Entry Fields (Business Data and Best Effort) (continued)

Entry Field	Description
Exceed Action–Type	The action to take on packets that conform to the specified rate limit. **Single Action** • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. **Note** If you select **Set-dscp-transmit** or **Set-prec-transmit**, you must specify the DSCP or IP Precedence in the Conform-Action Value field. **Dual Action** • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. **Note** The set-mpls fields only appear if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Exceed Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Exceed Action-Type.

Table B-2 Edit Service Class Entry Fields (Business Data and Best Effort) (continued)

Entry Field	Description
Violate Action–Type	The action to take on packets that conform to the specified rate limit. **Single Action** • Transmit—Sends the packet. • Drop—Drops the packet. • Set-dscp-transmit—Sets the DSCP value and transmits the packet. • Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet. **Note** If you select **Set-dscp-transmit** or **Set-prec-transmit**, you must specify the DSCP or IP Precedence in the Conform-Action Value field. **Dual Action** • set-mpls-exp-transmit—Sends the packet. • set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet. • set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet. **Note** The set-mpls fields only appear if you select the **Mark MPLS Exp.** check box under At Provider Ingress: on the first window of the policy creation.
Violate Action–Value	The DSCP or IP Precedence or MPLS Exp value for the Violate Action-Type.
Congestion Management	Routing Protocol and Management CoS can be configured with Bandwidth Remaining.
Bandwidth in kbps	The bandwidth in kbps (absolute bandwidth) for this service class. This field translates to Bandwidth x commands where x is in kbps.

Table B-2 Edit Service Class Entry Fields (Business Data and Best Effort) (continued)

Entry Field	Description
Bandwidth Percent	Percentage of bandwidth to dedicate to congestion management parameters. The range is 1-100 percent. Bandwidth is relative or absolute. • Relative: This field specifies the bandwidth in percentage that you need to allocate to this CoS. This corresponds to relative bandwidth command Bandwidth Percent *x* where *x* is the percentage specified. • Absolute: The percentage specified is used in conjunction with the circuit (or link) bandwidth to compute the absolute bandwidth (in kbps) that needs to be allocated to this CoS. Although this field translates to the same command as that for Bandwidth in kbps, it differs as follows: the absolute bandwidth varies with the circuit (or link) bandwidth. For example, if the percentage specified is 10 and if the policy is applied to a 64 kbps link, then absolute bandwidth allocated for this CoS is 6.4 kbps. If the same policy is applied to a 128 kbps link, then the absolute bandwidth allocated for this CoS is 12.8 kbps. Thus, the policy can be used on disparate bandwidth links.
Bandwidth Remaining Percent	The range is 1-100 percent.
Queue Limit in Packets	Limit the queue depth of the congesting traffic. The range is 1-262144 packets.
Queue Limit in Cells	Limit the queue depth of the congesting traffic. The range is 1-262144 cells.
Congestion Avoidance	
Enabled	Enable congestion avoidance.
Drop based on	Drops packets based on the IP Precedence or DSCP value.
Exponential Weighing Constant	The value used in the average queue size (weighted random early detection, or WRED) calculation. This value is used to determine the queue reserved for this service class.
Advanced Avoidance Options	Click **Edit** to add Advanced Avoidance Options. See Advanced Avoidance Options, page B-19.

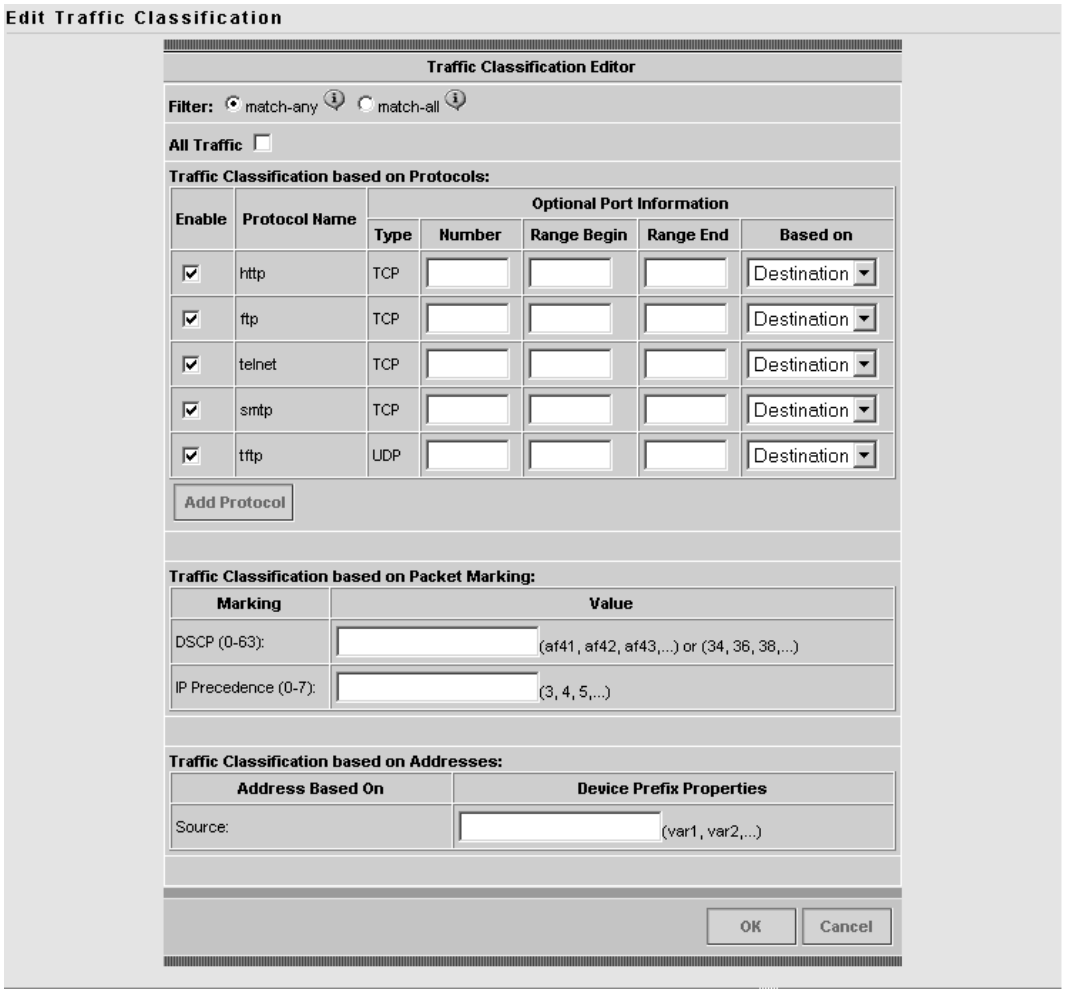
Editing the Data Service Classes

This section describes how to change the traffic classification parameters for the data service classes and how to add advanced options for congestion avoidance.

Traffic Classification

Use the Traffic Classification window to set or change the traffic classification parameters. Figure B-5 show the traffic classification settings for this service class. It includes some protocols that are enabled by default.

Figure B-5 Traffic Classification Editor—Business Data Service Class



The entry fields are described in Table B-3.

Table B-3 Traffic Classification Editor Entry Fields

Entry Field	Description
Filter:	**match-any: Traffic** classification passes when any one of the following classifications is met. **match-all:** Traffic Classification passes when all of the conditions below are met. This is restrictive; for example, a combination of any one protocol and DSCP makes sense but not more than one protocol and DSCP and IP_PRECEDENCE since an IP packet cannot belong to more than one Protocol and cannot have DSCP and IP_PRECEDENCE values at the same time.
All Traffic	Selects traffic classification based on all protocols.
Traffic Classification Based on Protocols	
Enable	Enables traffic classification for this protocol.

Table B-3 Traffic Classification Editor Entry Fields (continued)

Entry Field	Description
Port Type	TCP or UDP port (optional).
Port Number	The TCP or UDP port number to use for this protocol. (optional)
Port Range Begin	Specifies the beginning port number in a range of ports. (optional)
Port Range End	Specifies the end port number in a range of ports. (optional)
Based On	Traffic classification is based on the source or destination port for this protocol. (optional)
Add Protocol	Add another protocol to use for traffic classification.
NBAR	NBAR (Network Based Application Recognition) On platforms running IOS that support NBAR based traffic classification, you can provide NBAR support such as: • match protocol *protocol name* where *protocol name* is citrix, cuseeme, for example. • match protocol http url *url name* To make use of this feature, enter the *protocol* or *url name* in the protocol name field. Do not edit the remaining fields for the protocol.
Extended ACL	Extended ACL (Access Control List) To create named ACLs such as: • permit *port_type* any any eq *port_number*, • permit *port_type* any range *port_range_begin port_range_end any* where *port_type is* UDP or TCP. Port information can be source-based or destination-based. To make use of this feature, leave the protocol name field blank.
Traffic Classification Based on Packet Marking	
DSCP (0-63):	Selects traffic classification based on DSCP value.
IP Precedence (0-7):	Selects traffic classification based on IP Precedence value.
Traffic Classification Based on Addresses	
Source	Selects traffic classification based on source IP addresses. This is accomplished using variables defined using the Network Objects Manager. For more information, see the Traffic Classification, page 1-5.

Advanced Avoidance Options

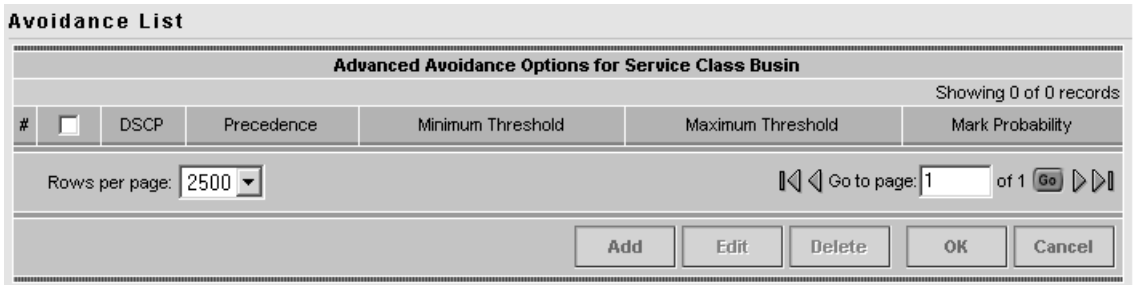
This section describes the advanced congestion avoidance parameters for the data service classes.

To add advanced congestion avoidance options:

Step 1 From the Edit Service Class window for a data service class, enable congestion avoidance.

Step 2 Click **Edit** next to the Advanced Avoidance Options field on the Edit Service Class window. The Avoidance List window appears (Figure B-6).

Figure B-6 Avoidance List

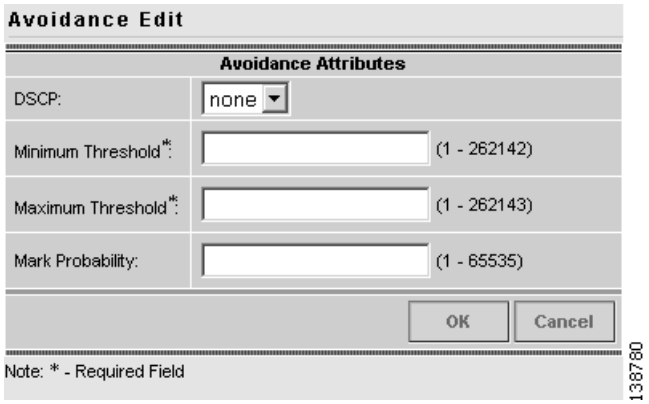


This window lists any available congestion avoidance options that have been configured, including the DSCP or IP Precedence value, the minimum and maximum threshold, and the mark probability.

From this window you can also Add, Edit, or Delete any congestion avoidance option.

Step 3 Click **Edit** to add a new option. The Avoidance Edit window appears as shown in Figure B-7.

Figure B-7 Avoidance Edit



Step 4 Enter the congestion avoidance attributes.

- DSCP or IP Precedence value—This value corresponds to the "Drop based on" value for this service class.
- Minimum and Maximum Threshold—When a packet arrives at a router, the following happens:
  - The average queue size is calculated.
  - If the average is less than the minimum queue threshold, the arriving packet is queued.
  - If the average is between the minimum queue threshold for a particular type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for the traffic.
  - If the average queue size is greater than the maximum threshold, the packet is dropped.
- Mark Probability—The fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if this value is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold.

Step 5 Click **OK** (twice) to return to the Edit Service Class window.

Adding a Data Service Class

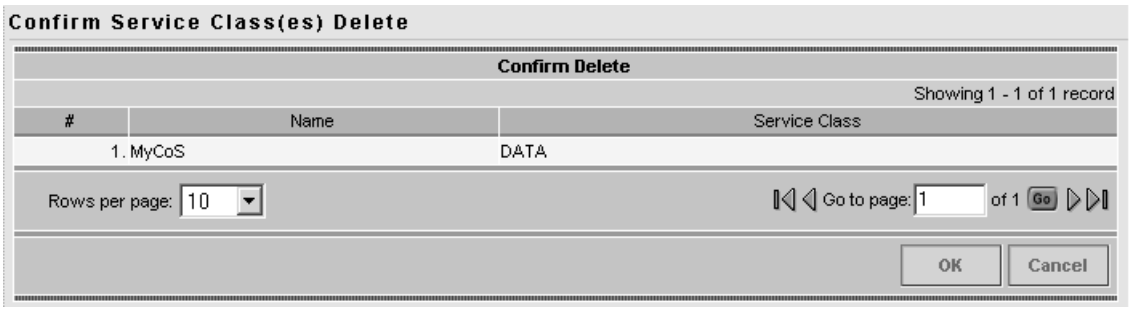
If your QoS policy requires additional service classes, use the data service class template provided with ISC to add another management or data service class.

To add another service class, click **Add Data CoS** from the Edit QoS Policy window. Enter a name and the service class attributes. See Table B-2 for a description of each field.

Deleting a Service Class

To delete an unwanted service class from your QoS policy, select the service class on the Edit QoS Policy window. Click **Delete**, confirm (Figure B-8), and click **OK**.

Figure B-8 Delete Service Class



Link Level QoS Parameters

Link level QoS parameters see QoS settings that are based on the CE-PE link (called IP link QoS settings). These interface-based parameters include aggregated traffic shaping, link efficiency settings, and interface-based rate limiting.

This section describes the link level QoS parameters for IP link QoS settings. Link level QoS parameters include all entry fields for the link QoS settings.

Aggregated Traffic Shapers

Aggregated traffic shaping allows you to control the traffic leaving an interface. In ISC, you can select an aggregated traffic shaper for each IP link.

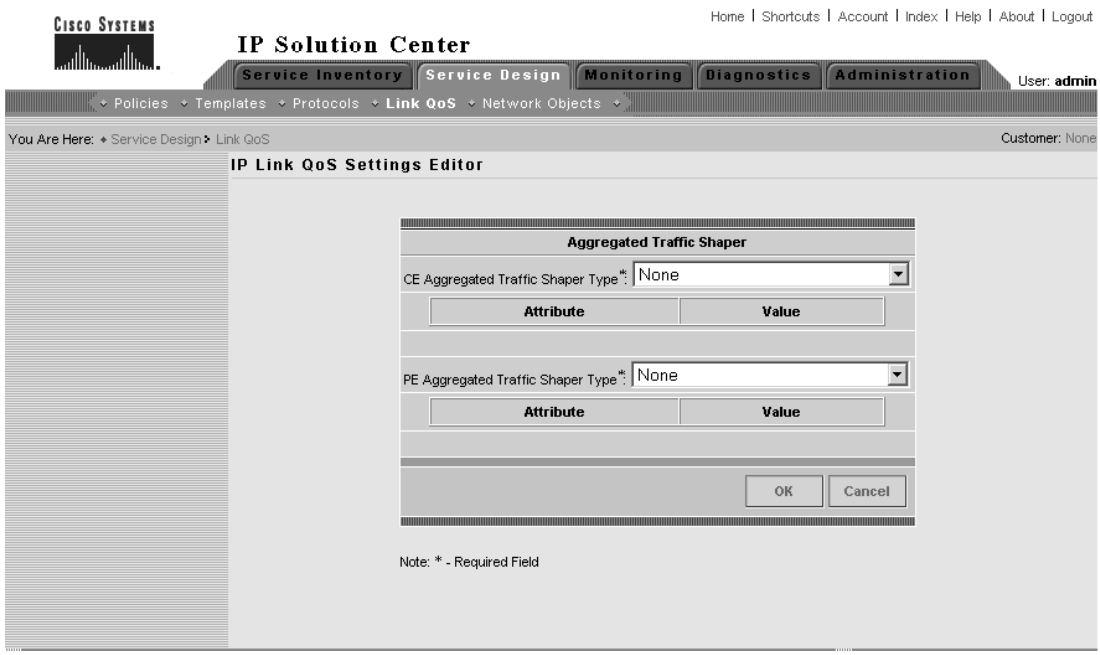
To apply class-based traffic shaping parameters, see the Editing the Data Service Classes, page B-16.

Aggregated traffic shapers are optional. ISC supports the following aggregated traffic shapers:

- Frame Relay (FR) Traffic Shaper
- FR Traffic Shaper (Non-MQC)
- Parent-level Class-based Shaper
- ATM Traffic Shaper (VBR-rt)
- ATM Traffic Shaper (VBR-nrt)
- ATM Traffic Shaper (CBR)
- ATM Traffic Shaper (ABR)

You set aggregated traffic shaping parameters from the IP Link QoS Settings Editor window by clicking the Aggregated Traffic Shaper link. This opens the Aggregated Traffic Shaper window (Figure B-9).

Figure B-9 Select Aggregated Traffic Shaper Type



Select one aggregated traffic shaper for the CE and one for the PE. Table B-4 describes the aggregated traffic shaper types.

Table B-4 Aggregated Traffic Shaper Types

Shaper Type	Description
FR Traffic Shaper	Frame Relay Traffic Shaper—A version of a class-based parent level shaper that operates only in distributed mode on versatile interface processor-based routers, such as the Cisco 7500 series platforms.
FR Traffic Shaper (Non-MQC)	Frame Relay Traffic Shaper—This shaper operates on the Cisco 7200 series and low-end routers.
Parent-level Class-based Shaper	Used for nested policies where a bottom-level policy identifies one or more classes of traffic, and a top-level policy shapes the output of the traffic classes into a single shape rate. You can apply nested policies to interfaces or subinterfaces.
ATM Traffic Shaper (VBR-rt)	Variable bit rate-real time—Intended for real-time applications, such as compressed voice over IP and video-conferencing, that require tightly constrained delays (cell transfer delay or cell delay variation).
ATM Traffic Shaper (VBR-nrt)	Variable bit rate-non real time—Follows a leaky bucket or token bucket algorithm.

Table B-4 Aggregated Traffic Shaper Types (continued)

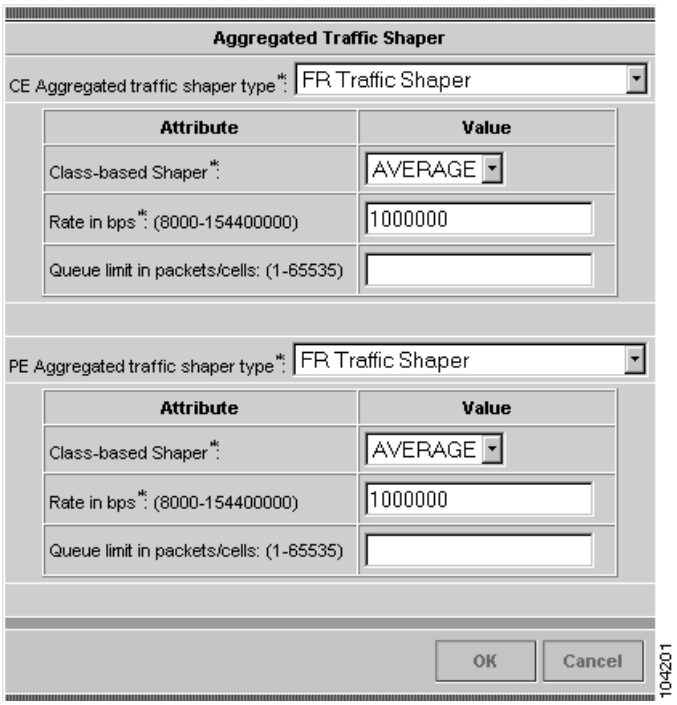
Shaper Type	Description
ATM Traffic Shaper (CBR)	Constant bit rate—Designed for ATM virtual circuits (VCs) that need a static amount of bandwidth that is continuously available for the duration of the active connection.
ATM Traffic Shaper (ABR)	Available bit rate—Configures a router to transmit at a rate that varies with the amount of bandwidth available in the network or along the end-to-end transmission path.

The following sections describe the windows and entry fields for the aggregated shaper types. You see a different dialog box depending on which of the following you choose.

FR Traffic Shaper

The FR Traffic Shaper (Figure B-10) is a version of a class-based parent level shaper that operates only in distributed mode on versatile interface processor-based routers, such as the Cisco 7500 series platforms.

Figure B-10 FR Traffic Shaper



The entry fields are described in Table B-5.

Table B-5 Frame Relay Traffic Shaper Entry Fields

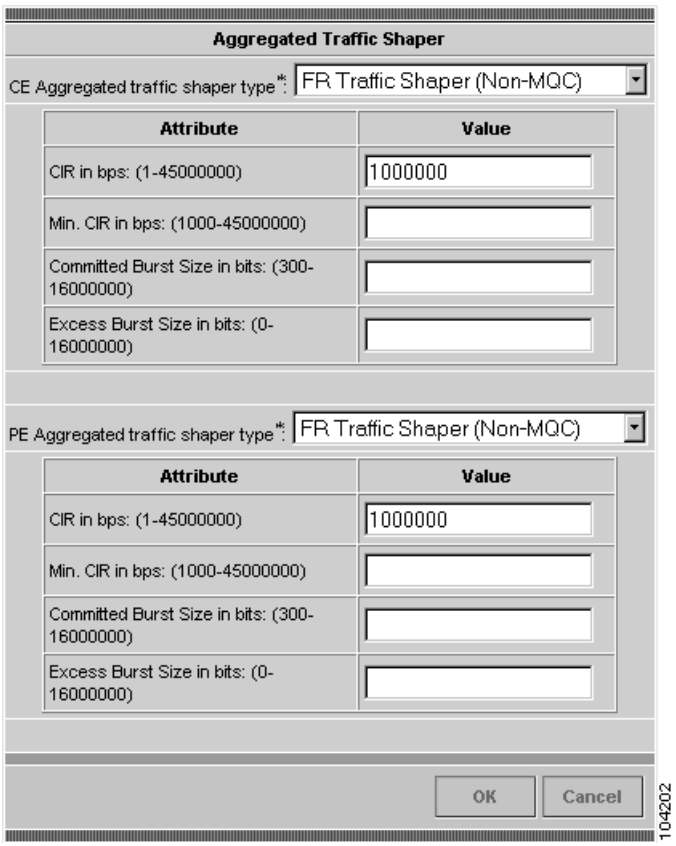
Attribute	Description
Class-based Shaper	Choose average or peak. Peak rate shaping allows you to make better use of available bandwidth because it allows you to send more data than the CIR, if the bandwidth is available.
Rate in bps	This field might be prepopulated with the bandwidth value from the IP Link QoS Settings Editor window. The range is 8000 to 1554400000.
Queue limit in packets/cells	The maximum number of packets or cells allowed in the priority queue. The range is 1 to 65535.

FR Traffic Shaper (Non-MQC)

The Non-MQC Frame Relay traffic shaper (FRTS) uses queues on a Frame Relay network to limit surges that can cause congestion. Data is buffered and then sent into the network in regulated amounts to ensure that the traffic will fit within the promised traffic envelope for the particular connection.

Use FRTS Non-MQC (Figure B-11) on all ISC-supported low-end router platforms (Cisco 7200 series and below).

Figure B-11 FRTS Non-MQC



The entry fields are described in Table B-6.

Table B-6 Frame Relay Traffic Shaper (Non-MQC) Entry Fields

Attribute	Description
CIR in bps	This field might be prepopulated with the bandwidth value from the IP Link QoS Settings Editor window. The range is 1 to 45000000.
Min. CIR in bps	The range is 1000 to 45000000.
Committed Burst Size in bits	The range is 300 to 16000000.
Excess Burst Size in bits	The range is 0 to 16000000.

Note The CIR value is a required field even though it is not listed on the GUI as required.

Parent-level Class-Based Traffic Shaper

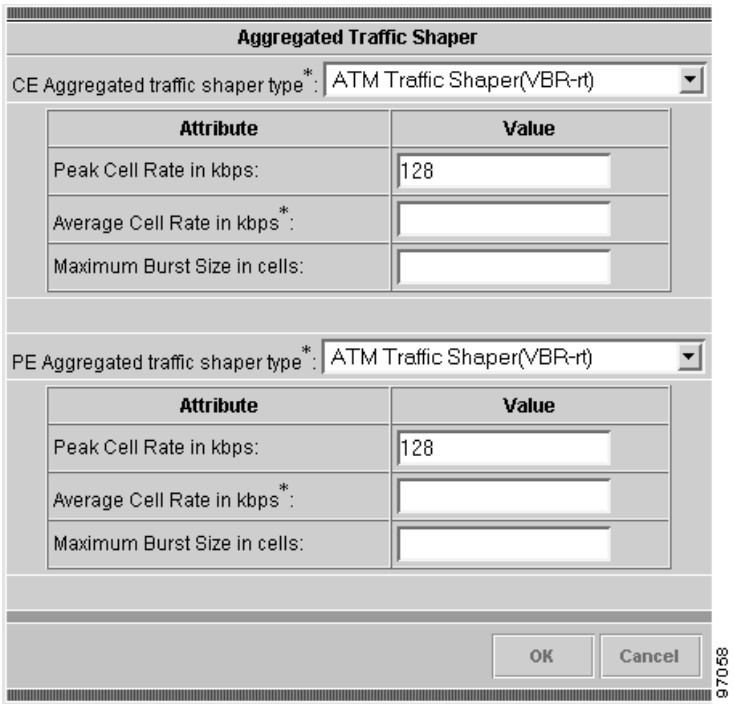
Parent-level class-based traffic shapers are used for nested policies where a bottom-level policy identifies one or more classes of traffic, and a top-level policy shapes the output of the traffic classes into a single shape rate. You can apply nested policies to interfaces or subinterfaces.

The parent-level class-based shaper dialog box and entry fields are the same as the FR Traffic Shaper. See FR Traffic Shaper, page B-23.

ATM Traffic Shaper (VBR-rt)

VBR-rt is intended for real-time applications, (for example, those requiring tightly constrained delay and delay variation, like voice and video applications). VBR-rt connections are characterized in terms of a peak cell Rate (PCR), sustainable cell rate (SCR), and maximum burst size (MBS). See Figure B-12.

Figure B-12 ATM Traffic Shaper VBR-rt



The entry fields are described in Table B-7.

Table B-7 Frame Relay Traffic Shaper VBR-rt Entry Fields

Attribute	Description
Peak Cell Rate in kbps	The maximum rate at which you expect to transmit data, voice and video.
Average Cell Rate in kbps	The sustained rate at which you expect to transmit data, voice and video. SCR is the true bandwidth of a VC and not the long-term average traffic rate
Maximum Burst Size in cells	The amount of time or the duration at which the router sends at PCR.

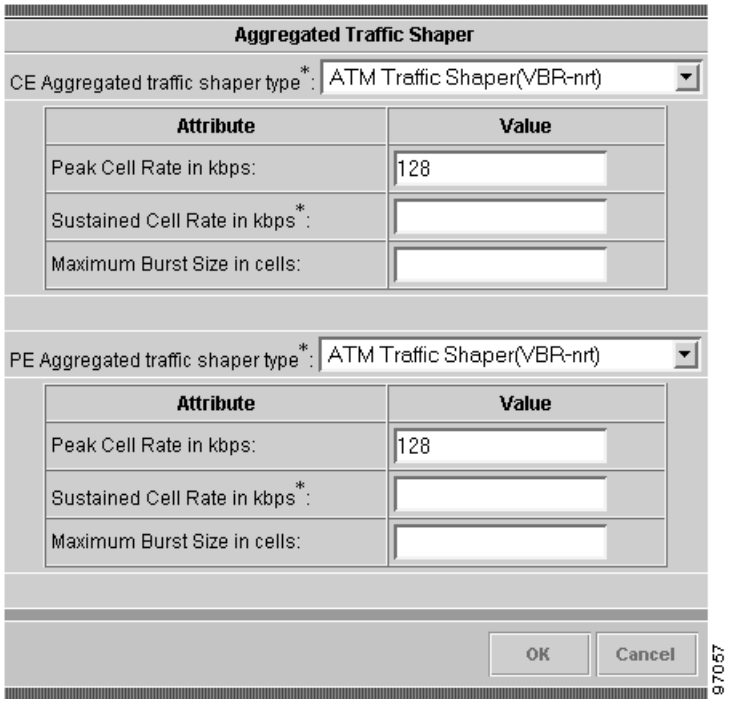
Tip Configure PCR and MBS parameters for reducing latency, not increasing bandwidth.

ATM Traffic Shaper (VBR-nrt)

This section describes ATM traffic shaping using variable bit rate non real-time.

VBR-nrt implementations follow a leaky bucket or token bucket algorithm. An ATM VC requires a token in the bucket to transmit a cell. The algorithm replenishes tokens in the bucket at the rate of the sustained cell rate (SCR). If a source is idle and does not transmit for a period of time, tokens accumulate in the bucket. An ATM VC can use the accumulated tokens to burst at the rate of peak cell rate (PCR) until the bucket is empty, at which point tokens are replenished at the rate of SCR. See Figure B-13.

Figure B-13 ATM Traffic Shaper VBR-nrt



The entry fields are described in Table B-8.

Table B-8 ATM Traffic Shaper VBR-nrt Entry Fields

Attribute	Description
Peak Cell Rate in kbps	The maximum rate at which you expect to transmit data, voice and video.
Sustained Cell Rate in kbps	The sustained rate at which you expect to transmit data, voice and video. SCR is the true bandwidth of a VC and not the long-term average traffic rate.
Maximum Burst Size in cells	The amount of time or the duration at which the router sends at PCR.

Tip Configure PCR and MBS parameters for reducing latency, not increasing bandwidth.

The values for this dialog box can be calculated using the following formulas:

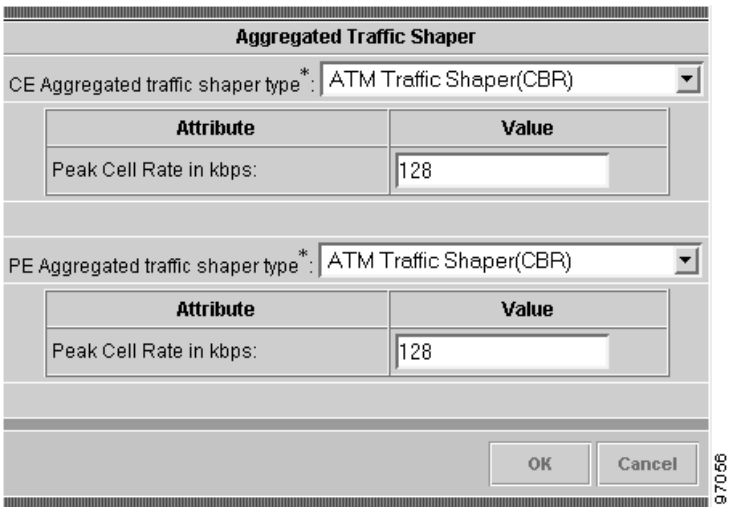
- (2 x maximum number of calls) x 16 Kbps= peak cell rate (PCR)
- (1 x maximum number of calls) x 16 Kbps = sustained cell rate (SCR)
- (4 x maximum number of calls) = burst size in cells (MBS)

Tip Both real-time and non-real-time VBR services are characterized by PCR, SCR and MBS or burst tolerance (BT). VBR-rt makes better use of bandwidth if the traffic tends to burst, since the ATM interface reserves bandwidth equal to the SCR only.

ATM Traffic Shaper (CBR)

The CBR traffic shaper is used by connections that require static amount of bandwidth that is continuously available during the connection lifetime. This amount of bandwidth is characterized by a Peak Cell Rate (PCR) value. Use CBR traffic shapers for real-time traffic. See Figure B-14.

Figure B-14 ATM Traffic Shaper CBR

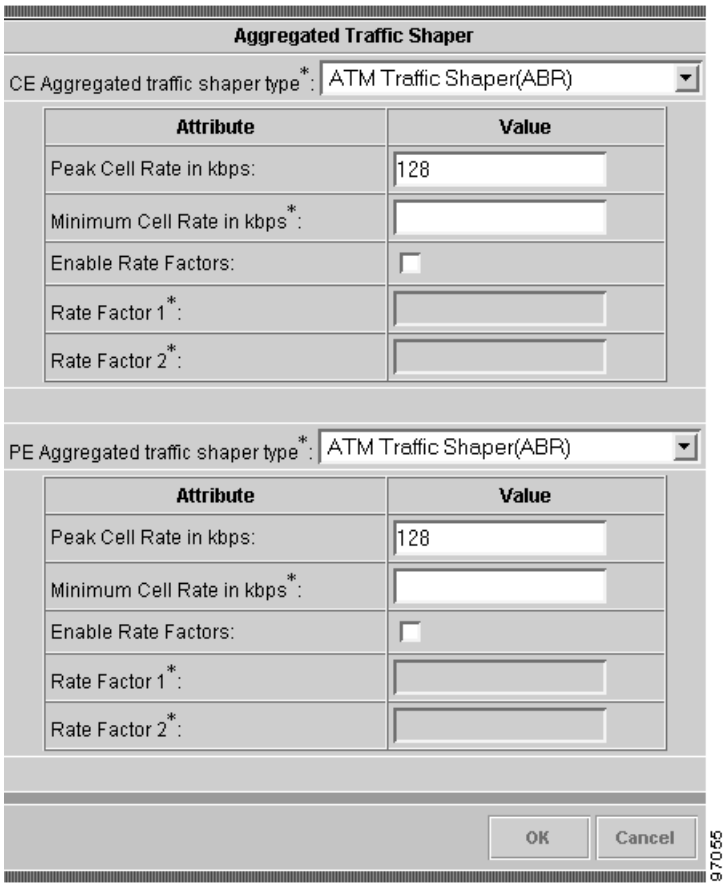


The Peak Cell Rate is the maximum rate at which you expect to transmit data, voice and video.

ATM Traffic Shaper (ABR)

ABR traffic shaping configures a router to transmit at a rate that varies with the amount of bandwidth available in the network or along the end-to-end transmission path. When the network is congested and other source devices are transmitting, there is little available or leftover bandwidth. However, when the network is not congested, bandwidth is available for use by other active devices. ABR allows end-system devices like routers to take advantage of this extra bandwidth and increase their transmission rates. See Figure B-15.

Figure B-15 ATM Traffic Shaper ABR



The entry fields are described in Table B-9.

Table B-9 ATM Traffic Shaper ABR Entry Fields

Attribute	Description
Peak Cell Rate in kbps	Maximum cell rate at which the source can transmit.
Minimum Cell Rate in kbps	Rate at which a source router can always send.
Enable Rate Factors	Enable rate factors.
Rate Factor 1	Rate Factor 1 is the inverse of RIF. The rate increase factor (RIF). The amount by which the transmission rate increases after the source interface receives a resource management (RM) cell with no increase (NI) and congestion indication (CI) set to zero. The value is specified as a (negative) power of two (2x). The range is between 1/32768 and 1.
Rate Factor 2	Rate Factor 2 is the inverse of RDF. The rate decrease factor (RDF). The amount by which the transmission rate decreases after the source interface receives an RM cell with the CI bit set to one. The value is specified as a power of two (2x). The range is between 1 and 1/32768.

Link Efficiency Settings

Link efficiency settings are based on the CE-PE link itself and are used to minimize serialization delay on the link. ISC uses methods of fragmentation and compression to minimize this delay.

ISC supports the following link efficiency settings:

- LFI on Frame Relay (FRF.12)–Supports the transport of real-time voice and data traffic on Frame Relay virtual circuits (VCs) without causing excessive delay to the real-time traffic.
- LFI on MLPPP—Multilink PPP (MLPPP) provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLPPP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.

Figure B-16 shows the IP Link QoS Settings Editor window.

Figure B-16 Link Efficiency Settings

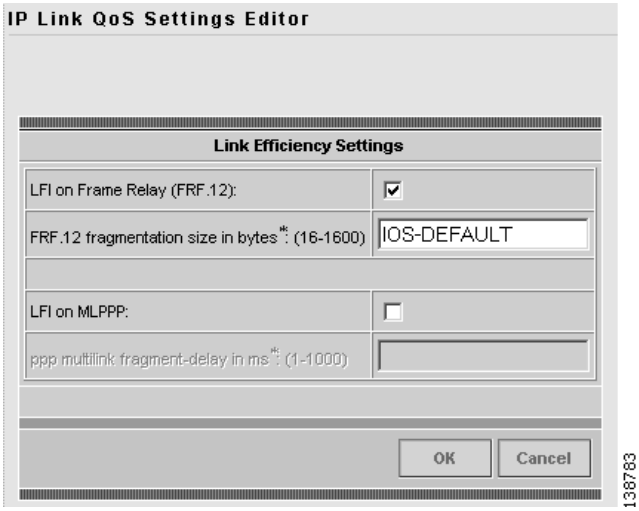


Table B-10 describes the entry fields for the Link Efficiency Settings window.

Table B-10 Link Efficiency Settings Entry Fields

Entry fields	Description
LFI on Frame Relay (FRF.12)	Enables LFI settings on Frame Relay interfaces.
FRF.12 fragmentation size in bytes.	The range is 16 to 1600 bytes. If you enable this LFI setting, the Cisco IOS default setting can be used, or you can enter a value manually.
LFI on MLPPP	Enables LFI settings for Multi link Point-to-Point interfaces. You must enter the PPP multilink fragment delay.
PPP multilink fragment delay in ms	The amount of delay between packet fragments. The range is 1 to 1000 ms.

Interface-Based Aggregated Rate Limiters

Interface-based aggregated rate limiters allow you to control the maximum rate of traffic sent or received on an interface for the CE-PE link. You can also specify traffic handling policies for when the traffic conforms or exceeds the specified rate limit.

Aggregate rate limits match all packets or a specified subset of packets on an interface or subinterface. To specify class-based rate limiting parameters, see the Creating the Service Level IP QoS Policy, page 3-9.

ISC supports the following interface-based rate limiter parameters:

- Traffic classification
- Direction
- Mean rate
- Burst sizes (conformed and extended)
- Conform and exceed actions

Figure B-17 shows the Interface-based Aggregated Rate Limiter window.

Figure B-17 Interface Based Aggregated Limiter

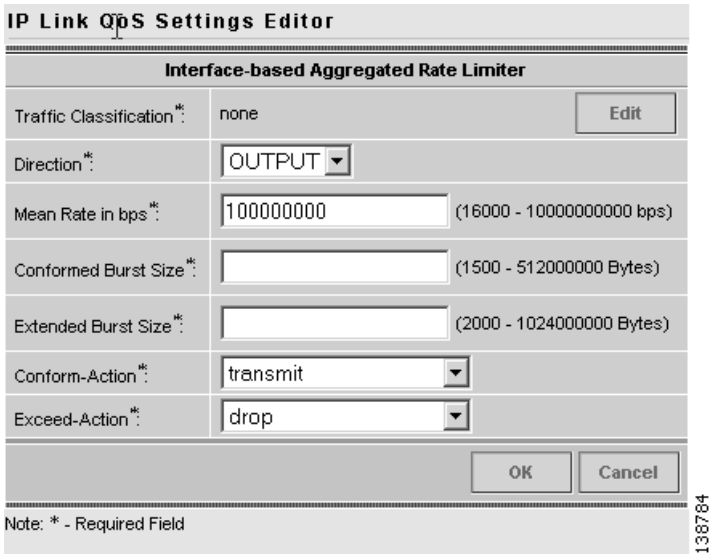


Table B-11 describes the entry fields for the Interface-based Aggregated Rate Limiter window. All fields in this window are required.

Table B-11 Interface-based Aggregated Rate Limiter Entry Fields

Entry field	Description
Traffic Classification	Specifies the method for classifying traffic. Click **Edit** to access the Traffic Classification Editor. For more information, see Traffic Classification, page B-16.
Direction	The direction of traffic to apply rate limiting parameters to. Choose from Input or Output.

Table B-11 Interface-based Aggregated Rate Limiter Entry Fields (continued)

Entry field	Description
Mean rate in bps	The range is 8000 to 2000000000 bps.
Conformed burst size in bytes	The range is 1000 to 512000000 bytes. **Note** IOS silently re-adjusts the conformed burst size to the MTU size of the interface if the MTU is greater than the conformed burst size entered in the ISC IP Link QoS Settings for Interface-based Aggregated Rate Limiter. The ISC QoS service request will then go to Failed-Audit. Ensure that the conformed burst size is greater than the interface MTU size.
Extended burst size in bytes	The range is 2000 to 1024000000 bytes.
Conform-Action	Specifies how to handle packets that conform to the configured rate limit. • Transmit—Sends the packet. • Drop—Drops the packet. **Note** If you select any of the following, you must specify the DSCP, IP, or MPLS Precedence value in the adjacent drop-down menus. • Set-dscp-transmit—Sets the DSCP value (0-63) and transmits the packet. • Set-prec-transmit—Sets the IP precedence value (0 to 7) and sends the packet. • Set-mpls-exp-transmit—Sets the MPLS value (0 to 7) and transmits the packet. • Set-dscp-continue—Sets the DSCP value (0 to 63) and transmits the packet. • Set-prec-continue—Sets the IP precedence (0 to 7) value and sends the packet. • Set-mpls-exp-continue—Sets the MPLS value (0-7) and sends the packet.
Exceed-Action	Specifies how to handle packets that exceed the configured rate limit. The options are the same as Conform-Action.

Ethernet QoS Policy Parameters

This appendix describes the parameters, both required and optional, for Ethernet QoS provisioning using the Cisco IP Solution Center (ISC) user interface.

This appendix contains the following sections:

Service Level Ethernet QoS Parameters

Service level Ethernet QoS parameters include the entry fields in the service class windows and dialog boxes. However, the Ethernet QoS policy is not pre-populated with any Class of Service. These must be added using the **Add CoS** button on the Edit Ethernet QoS Policy page.

You must enter the bandwidth parameter for all service classes. Typically, a value of one percent is sufficient for Routing Protocol traffic. However, it is common for customers or providers to combine the Management and Routing Protocol into one service class policy. In this case, a larger percentage of bandwidth might be required.

Any class of service can be a *class-default* class of service. You can simply name the class of service as *class-default* and ISC will generate the same. Bandwidth is not mandatory for this class of service. Traffic classification is assumed to be *rest of traffic*.

Note *Class-default* is a reserved class of service name in IOS and is created by IOS if ISC does not create one.

Service Class Parameters

Each service class is characterized by a set of parameters that are defined in the Edit Service Class window (Figure C-1).

Figure C-1 Edit Service Class

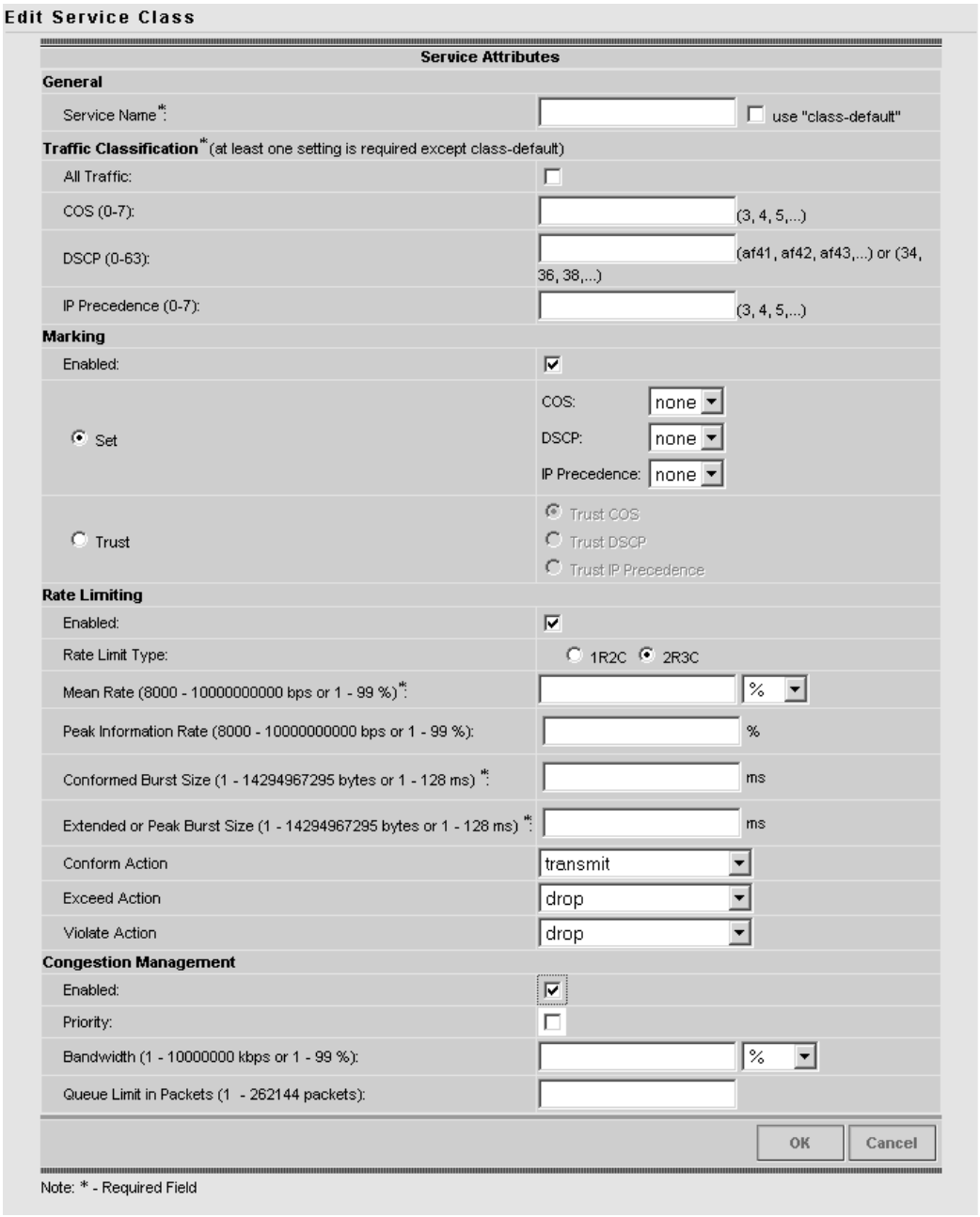


Table C-1 provides a definition for each of the service class parameters.

Table C-1 Edit Service Class Entry Fields

Entry Field	Description
General	
Service Name	The name of the service class. Max. 8 characters in length. **use "class-default":** Check the "use Class Default" check box if you want the service class to be a class-default class.
Traffic Classification	
All Traffic	Check this box if the policy is to be applied to all traffic.
COS (0-7)	A class of service.
DSCP	Traffic classification based on the packet's DSCP marking.
IP Precedence	Traffic classification based on the packet's IP Precedence marking.
Marking	
Enabled	Enable packet marking.
Set	Three options: • COS: Mark packets with 802.1p Class of Service Marking. • DSCP: Mark packets with a DSCP value. Note: You can mark packets with either DSCP or IP Precedence, but not both. • IP Precedence: Mark packets with an IP Precedence value.
Trust	Defines which markings should be trusted in the QoS Policy.
Rate Limiting (VoIP service class only)	
Enabled	Enable rate-limiting.
Rate Limit Type	This sets which type of policer is created and, therefore, which values are required. Two options: • One rate two color • Two rate three color
Mean Rate	The long-term average transmission rate.
Peak Information Rate	Allows support for sustained excess rate.
Conformed Burst Size	How large traffic bursts can be before some traffic exceeds the rate limit.
Extended or Peak Burst Size	How large traffic bursts can be before all traffic exceeds the rate limit. Configure extended burst by setting the extended burst value greater than the conformed burst value.

Table C-1 Edit Service Class Entry Fields (continued)

Entry Field	Description
Conform Action–	The action to take on packets that conform to the specified rate limit: • **transmit**—Sends the packet. • **drop**—Drops the packet. • **policed-dscp-transmit**—Marks down the DSCP value and then transmits. • **set-cos-transmit**—Sets the L2 CoS value and transmits the packet. • **set-dscp-transmit**—Sets the DSCP value and transmits the packet. • **set-prec-transmit**—Sets the IP precedence (0 to 7) value and sends the packet.
Exceed Action–	The action to take on packets that conform to the specified rate limit. • **transmit**—Sends the packet. • **drop**—Drops the packet. • **policed-dscp-transmit**—Marks down the DSCP value and then transmits. • **set-cos-transmit**—Sets the L2 CoS value and transmits the packet. • **set-dscp-transmit**—Sets the DSCP value and transmits the packet. • **set-prec-transmit**—Sets the IP precedence (0 to 7) value and sends the packet.
Violate Action–	The action to take on packets that conform to the specified rate limit. • **transmit**—Sends the packet. • **drop**—Drops the packet. • **policed-dscp-transmit**—Marks down the DSCP value and then transmits. • **set-cos-transmit**—Sets the L2 CoS value and transmits the packet. • **set-dscp-transmit**—Sets the DSCP value and transmits the packet. • **set-prec-transmit**—Sets the IP precedence (0 to 7) value and sends the packet.
Congestion Management	(Applicable to 3750-ME only)
Enabled	Enable congestion management.
Priority	Assign a traffic class to the strict priority queue

Table C-1 Edit Service Class Entry Fields (continued)

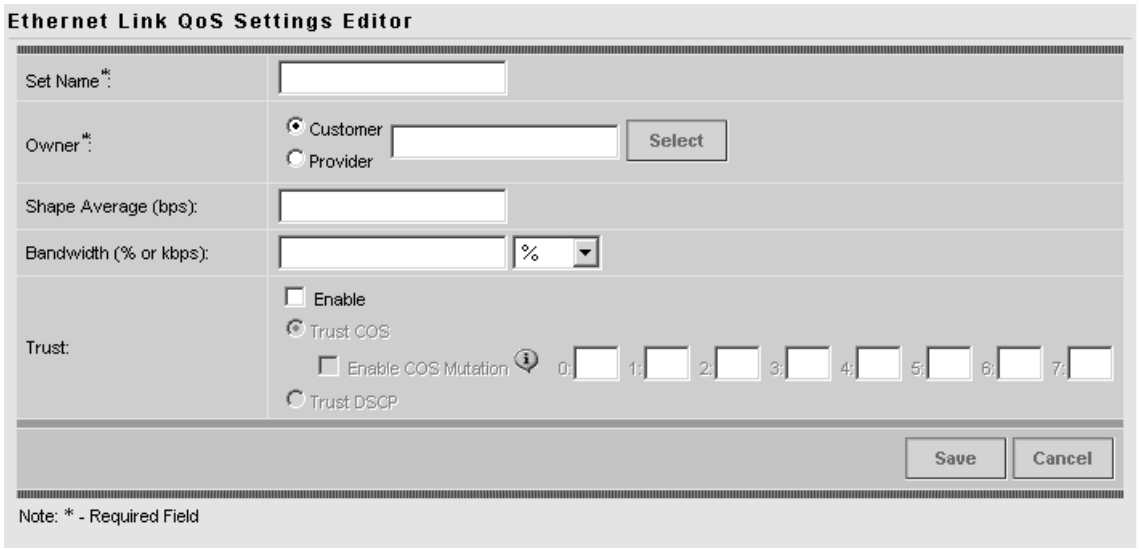
Entry Field	Description
Bandwidth	The bandwidth in kbps (absolute bandwidth) or percent for this service class to dedicate to congestion management parameters.
Queue Limit in Packets	Limit the queue depth of the congesting traffic. The range is 1 to 32768 packets.

Note The process for marking packets with DSCP and IP Precedence bits is described in detail in the following document on Cisco.com:
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Link Level Ethernet QoS Parameters

This section describes the link level QoS parameters for Ethernet link QoS settings. These settings are intended for either the VLAN level or the interface level.

Figure C-2 Link QoS Settings



The Ethernet Link QoS Settings window displays the current link QoS settings available for QoS service requests, including the following information about each link QoS setting:

- Set Name—The name of your link QoS setting.
- Owner—Customer or provider.
- Shape Average—Enable VLAN level average-rate traffic shaping. It limits the affected traffic to a certain data transmission rate in bps.
- Bandwidth—Desired VLAN level bandwidth. Enter this value manually in kbps or percent to allocate a minimum bandwidth for the VLAN.

- Trust—Port level trust
  - Enable—Check this box to enable trust.
  - Trust COS—Trust CE L2 CoS.

    - Enable COS Mutation—Enable CE L2 CoS classification for 7600 L2VPN EWS and VPLS. (See General Metro Ethernet Service Types, page E-1 for a definition of Metro Ethernet terminology.)
  - Trust DSCP—Trust CE DSCP.

Sample Configurations

This appendix lists sample configurations and contains the following sections:

ISC-Generated Configlets

The following are examples of configlets generated by Cisco IP Solution Center (ISC) for the network example shown in Figure A-1 in Provisioning Process for IP QoS, page 3-1.

Device enqospe4:

Configlet #1 (Created: 2003-04-24 16:44:57)

Job #124 Service Request #124

```
ip access-list extended
ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
permit ip any 10.10.10.0 0.0.0.255
!
ip access-list extended
ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Business-Data-1
permit TCP any any eq www
permit TCP any any eq telnet
permit UDP any any eq tftp
permit TCP any any eq ftp
permit TCP any any eq smtp
!
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
permit UDP any any eq rip
permit TCP any any eq bgp
permit ospf any any
permit eigrp any any
!
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
permit ip 10.10.10.0 0.0.0.255 any
!
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
```

```
match ip rtp 16384 16383
!
class-map match-any ISC_IN_Customer-A_Management
match access-group name
ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
class-map match-any ISC_IN_Customer-A_Business-Data-1
match access-group name
ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Business-Data-1
!
class-map match-any ISC_IN_Customer-A_Best-Effort
match any
!
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
match ip dscp 46
!
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
!
class-map match-any ISC_OUT_Customer-A_Management
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
class-map match-any ISC_OUT_Customer-A_Business-Data-1
match ip dscp 34
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
match ip dscp 0
!
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
set ip dscp 46
class ISC_IN_Customer-A_Management
set ip dscp 34
class ISC_IN_Customer-A_Business-Data-1
set ip dscp 34
class ISC_IN_Customer-A_Best-Effort
set ip dscp 0
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
priority percent 10
class ISC_OUT_Customer-A_Routing_Protocol
bandwidth percent 1
class ISC_OUT_Customer-A_Management
bandwidth percent 1
class ISC_OUT_Customer-A_Business-Data-1
bandwidth percent 20
class ISC_OUT_Customer-A_Best-Effort
bandwidth percent 25
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy_TOP
class class-default
shape average 128000
service-policy ISC_OUT_Customer-A_CustA-QoSPolicy
!
map-class frame-relay ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy_TOP
frame-relay fragment
!
interface Hssi2/1/0.41 point-to-point
frame-relay ip rtp header-compression
```

```
frame-relay interface-dlci 41
class ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
!
```

Device enqosce41:

Configlet #1 (Created: 2003-04-24 16:44:58)

Job #124 Service Request #124

```
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
permit UDP any any eq rip
permit TCP any any eq bgp
permit ospf any any
permit eigrp any any
!
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
permit ip any 10.10.10.0 0.0.0.255
!
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
match ip rtp 16384 16383
!
class-map match-any ISC_IN_Customer-A_Business-Data-1
match protocol http
match protocol telnet
match protocol tftp
match protocol ftp
match protocol smtp
!
class-map match-any ISC_IN_Customer-A_Best-Effort
match any
!
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
match ip dscp 46
!
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
!
class-map match-any ISC_OUT_Customer-A_Management
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
class-map match-any ISC_OUT_Customer-A_Business-Data-1
match ip dscp 34
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
match ip dscp 0
!
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
set ip dscp 46
class ISC_IN_Customer-A_Business-Data-1
set ip dscp 34
class ISC_IN_Customer-A_Best-Effort
set ip dscp 0
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
```

```
priority percent 10
class ISC_OUT_Customer-A_Routing_Protocol
bandwidth percent 1
class ISC_OUT_Customer-A_Management
set ip dscp 34
bandwidth percent 1
class ISC_OUT_Customer-A_Business-Data-1
bandwidth percent 20
class ISC_OUT_Customer-A_Best-Effort
bandwidth percent 25
!
map-class frame-relay ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy
frame-relay cir 128000
frame-relay mincir 64000
!
interface FastEthernet0/0
service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
!
interface Hssi1/0
frame-relay traffic-shaping
!
interface Hssi1/0.41 point-to-point
frame-relay ip rtp header-compression
frame-relay interface-dlci 41
class ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
!
```

Device enqospe5:

Configlet #1 (Created: 2003-04-24 16:44:58)

Job #124 Service Request #124

```
ip access-list extended
ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
permit ip any 10.10.10.0 0.0.0.255
!
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
permit UDP any any eq rip
permit TCP any any eq bgp
permit ospf any any
permit eigrp any any
!
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
permit ip 10.10.10.0 0.0.0.255 any
!
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
match ip rtp 16384 16383
!
class-map match-any ISC_IN_Customer-A_Management
match access-group name
ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
class-map match-any ISC_IN_Customer-A_Business-Data-1
match protocol http
match protocol telnet
match protocol tftp
match protocol ftp
```

```
match protocol smtp
!
class-map match-any ISC_IN_Customer-A_Best-Effort
match any
!
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
match ip dscp 46
!
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
!
class-map match-any ISC_OUT_Customer-A_Management
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
class-map match-any ISC_OUT_Customer-A_Business-Data-1
match ip dscp 34
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
match ip dscp 0
!
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
set ip dscp 46
class ISC_IN_Customer-A_Management
set ip dscp 34
class ISC_IN_Customer-A_Business-Data-1
set ip dscp 34
class ISC_IN_Customer-A_Best-Effort
set ip dscp 0
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
priority percent 10
class ISC_OUT_Customer-A_Routing_Protocol
bandwidth percent 1
class ISC_OUT_Customer-A_Management
bandwidth percent 1
class ISC_OUT_Customer-A_Business-Data-1
bandwidth percent 20
class ISC_OUT_Customer-A_Best-Effort
bandwidth percent 25
!
interface ATM1/0.52 point-to-point
pvc 0/51
vbr-nrt 128 64 2000
service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy
!
```

Device enqosce52:

Configlet #1 (Created: 2003-04-24 16:44:57)

Job #124 Service Request #124

```
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
permit UDP any any eq rip
permit TCP any any eq bgp
```

```
permit ospf any any
permit eigrp any any
!
ip access-list extended
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
permit ip any 10.10.10.0 0.0.0.255
!
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
match ip rtp 16384 16383
!
class-map match-any ISC_IN_Customer-A_Business-Data-1
match protocol http
match protocol telnet
match protocol tftp
match protocol ftp
match protocol smtp
!
class-map match-any ISC_IN_Customer-A_Best-Effort
match any
!
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
match ip dscp 46
!
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
!
class-map match-any ISC_OUT_Customer-A_Management
match access-group name
ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
class-map match-any ISC_OUT_Customer-A_Business-Data-1
match ip dscp 34
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
match ip dscp 0
!
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
set ip dscp 46
class ISC_IN_Customer-A_Business-Data-1
set ip dscp 34
class ISC_IN_Customer-A_Best-Effort
set ip dscp 0
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
priority percent 10
class ISC_OUT_Customer-A_Routing_Protocol
bandwidth percent 1
class ISC_OUT_Customer-A_Management
set ip dscp 34
bandwidth percent 1
class ISC_OUT_Customer-A_Business-Data-1
bandwidth percent 20
class ISC_OUT_Customer-A_Best-Effort
bandwidth percent 25
!
interface FastEthernet0/0
service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
!
interface ATM1/0.52 point-to-point
pvc 0/52
service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy
```

```
!
```

Device Configurations

The following examples are full device configuations after a QoS Service Request deployment. The portions in bold are commands that represent the QoS configlets for the network example in Chapter 3, "Provisioning Process for IP QoS."

Device enqospe4:

```
version 12.0
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
no service single-slot-reload-enable
!
hostname enqospe4
!
boot system flash:rsp-pv-mz.120-24.S.bin
boot system flash rsp-pv-mz.122-4.T3.bin
redundancy
 no keepalive-enable
enable password 7 cisco
!
ip subnet-zero
ip cef distributed
ip tftp source-interface Loopback0
no ip domain-lookup
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
  match ip dscp 0
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
  match ip rtp 16384 16383
class-map match-any ISC_OUT_Customer-A_Business-Data-1
  match ip dscp 34
class-map match-any ISC_OUT_Customer-A_Management
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
class-map match-any ISC_IN_Customer-A_Best-Effort
  match any
class-map match-any ISC_IN_Customer-A_Business-Data-1
  match access-group name ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Business-Data-1
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
  match ip dscp 46
class-map match-any ISC_IN_Customer-A_Management
  match access-group name ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
  class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
    priority percent 10
  class ISC_OUT_Customer-A_Routing_Protocol
    bandwidth percent 1
  class ISC_OUT_Customer-A_Management
    bandwidth percent 1
  class ISC_OUT_Customer-A_Business-Data-1
```

```
    bandwidth percent 20
  class ISC_OUT_Customer-A_Best-Effort
    bandwidth percent 25
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy_TOP
  class class-default
    shape average 128000 512 512
   service-policy ISC_OUT_Customer-A_CustA-QoSPolicy
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
  class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
   set ip dscp 46
  class ISC_IN_Customer-A_Management
   set ip dscp 34
  class ISC_IN_Customer-A_Business-Data-1
   set ip dscp 34
  class ISC_IN_Customer-A_Best-Effort
   set ip dscp 0
!
mpls ldp logging neighbor-changes
no mpls traffic-eng auto-bw timers frequency 0
!
!
controller T1 1/1/0
 clock source internal
 channel-group 1 timeslots 1-24
!
controller T1 1/1/1
 clock source internal
 channel-group 1 timeslots 1-24
!
!
interface Loopback0
 description DNS entry for enqospe4 ! DON'T MODIFY or REMOVE !
 ip address 192.168.114.4 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/0/0.4 point-to-point
 description Link to enqospe1 ! DON'T MODIFY OR REMOVE !
 ip address 12.12.12.14 255.255.255.252
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 0/6
  encapsulation aal5snap
 !
!
interface FastEthernet0/1/0
 description Access Link to enqossw1 ! DON'T MODIFY or REMOVE !
 ip address 11.11.11.7 255.255.255.0
 no ip directed-broadcast
 speed auto
!
interface Serial1/1/0:1
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no keepalive
!
interface Serial1/1/1:1
 no ip address
```

```
 no ip directed-broadcast
 encapsulation frame-relay
 no keepalive
!
interface Hssi2/1/0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 no keepalive
 hssi internal-clock
!
interface Hssi2/1/0.41 point-to-point
 description QoS Link to enqosce41 ! DON'T MODIFY or REMOVE !
 ip address 141.141.141.1 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 no cdp enable
 frame-relay interface-dlci 41
  class ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
 frame-relay ip rtp header-compression
!
router ospf 1
 log-adjacency-changes
 network 11.11.11.7 0.0.0.0 area 0
 network 192.168.114.4 0.0.0.0 area 0
!
no ip classless
!
ip pim bidir-enable
!
!
ip access-list extended ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Business-Data-1
 permit tcp any any eq www
 permit tcp any any eq telnet
 permit udp any any eq tftp
 permit tcp any any eq ftp
 permit tcp any any eq smtp
ip access-list extended ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
 permit ip any 10.10.10.0 0.0.0.255
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
 permit udp any any eq rip
 permit tcp any any eq bgp
 permit ospf any any
 permit eigrp any any
!
!
map-class frame-relay ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
 no frame-relay adaptive-shaping
 service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
 service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy_TOP
 frame-relay fragment 53
snmp-server community public RO
snmp-server community private RW
!
!
line con 0
 exec-timeout 30 0
 password 7 cisco
 login
line aux 0
 exec-timeout 30 0
```

```
 password 7 cisco
 login
line vty 0 4
 exec-timeout 60 0
 password 7 cisco
 login
!
end
```

Device enqosce41:

```
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname enqosce41
!
enable password 7 cisco
!
!
!
ip subnet-zero
!
!
ip tftp source-interface Loopback0
no ip domain-lookup
!
ip cef
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
  match ip dscp 0
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
  match ip rtp 16384 16383
class-map match-any ISC_OUT_Customer-A_Business-Data-1
  match ip dscp 34
class-map match-any ISC_OUT_Customer-A_Management
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
class-map match-any ISC_IN_Customer-A_Best-Effort
  match any
class-map match-any ISC_IN_Customer-A_Business-Data-1
  match protocol http
  match protocol telnet
  match protocol tftp
  match protocol ftp
  match protocol smtp
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
  match ip dscp 46
!
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
  class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
    priority percent 10
  class ISC_OUT_Customer-A_Routing_Protocol
   bandwidth percent 1
  class ISC_OUT_Customer-A_Management
   set ip dscp 34
   bandwidth percent 1
  class ISC_OUT_Customer-A_Business-Data-1
   bandwidth percent 20
```

```
  class ISC_OUT_Customer-A_Best-Effort
   bandwidth percent 25
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
  class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
   set ip dscp 46
  class ISC_IN_Customer-A_Business-Data-1
   set ip dscp 34
  class ISC_IN_Customer-A_Best-Effort
   set ip dscp 0
!
!
!
interface Loopback0
 description DNS entry for enqosce41 ! DON'T MODIFY or REMOVE !
 ip address 192.168.114.9 255.255.255.255
!
interface FastEthernet0/0
 description Access Link to enqossw1 ! DON'T MODIFY or REMOVE !
 ip address 11.11.11.9 255.255.255.0
 duplex auto
 speed auto
 service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Hssi1/0
 description QoS Link to enqospe4 ! DON'T MODIFY or REMOVE !
 no ip address
 encapsulation frame-relay
 no keepalive
 hssi internal-clock
 clockrate 64158
 frame-relay traffic-shaping
!
interface Hssi1/0.41 point-to-point
 description QoS Link to enqospe4 ! DON'T MODIFY or REMOVE !
 ip address 141.141.141.2 255.255.255.252
 frame-relay interface-dlci 41
  class ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
 frame-relay ip rtp header-compression
!
router ospf 1
 log-adjacency-changes
 network 11.11.11.9 0.0.0.0 area 0
 network 192.168.114.9 0.0.0.0 area 0
!
!
no ip classless
ip http server
ip pim bidir-enable
!
!
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
 permit ip any 10.10.10.0 0.0.0.255
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
 permit udp any any eq rip
 permit tcp any any eq bgp
 permit ospf any any
 permit eigrp any any
!
```

```
map-class frame-relay ISC_OUT_FR_MAP_CLASS_Customer-A_CustA-QoSPolicy
 frame-relay cir 128000
 frame-relay mincir 64000
 no frame-relay adaptive-shaping
 service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy
!
!
snmp-server community public RO
snmp-server community private RW
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 30 0
 password 7 cisco
 login
line aux 0
 exec-timeout 30 0
 password 7 cisco
 login
line vty 0 4
 exec-timeout 30 0
 password 7 cisco
 login
!
!
end
```

Device enqospe5:

```
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname enqospe5
!
enable password 7 cisco
!
ip subnet-zero
ip cef
!
!
ip tftp source-interface Loopback0
no ip domain-lookup
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
  match ip dscp 0
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
  match ip rtp 16384 16383
class-map match-any ISC_OUT_Customer-A_Business-Data-1
  match ip dscp 34
class-map match-any ISC_OUT_Customer-A_Management
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
```

```
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
class-map match-any ISC_IN_Customer-A_Best-Effort
  match any
class-map match-any ISC_IN_Customer-A_Business-Data-1
  match protocol http
  match protocol telnet
  match protocol tftp
  match protocol ftp
  match protocol smtp
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
  match ip dscp 46
class-map match-any ISC_IN_Customer-A_Management
  match access-group name ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
!
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
  class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
    priority percent 10
  class ISC_OUT_Customer-A_Routing_Protocol
   bandwidth percent 1
  class ISC_OUT_Customer-A_Management
   bandwidth percent 1
  class ISC_OUT_Customer-A_Business-Data-1
   bandwidth percent 20
  class ISC_OUT_Customer-A_Best-Effort
   bandwidth percent 25
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
  class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
   set ip dscp 46
  class ISC_IN_Customer-A_Management
   set ip dscp 34
  class ISC_IN_Customer-A_Business-Data-1
   set ip dscp 34
  class ISC_IN_Customer-A_Best-Effort
   set ip dscp 0
!
!
!
!
interface Loopback0
 description DNS entry for enqospe5 ! DON'T MODIFY or REMOVE !
 ip address 192.168.114.5 255.255.255.255
!
interface Multilink100
 ip address 192.168.0.14 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 CE-5
 ip pim sparse-dense-mode
 no ip mroute-cache
 load-interval 30
 no cdp enable
 ppp multilink
 multilink-group 100
!
interface FastEthernet0/0
 description Access Link to enqossw1 ! DON'T MODIFY or REMOVE !
 ip address 11.11.11.8 255.255.255.0
 duplex half
 speed 100
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex half
 speed 100
!
interface ATM1/0
 no ip address
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
!
!
interface ATM1/0.52 point-to-point
 description QoS Link to enqosce52 ! DON'T MODIFY or REMOVE !
 ip address 152.152.152.1 255.255.255.252
 pvc 0/51
  vbr-nrt 128 64 2000
  encapsulation aal5snap
  service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
  service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy
!
interface ATM2/0
 no ip address
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
!
interface ATM2/0.5 point-to-point
 description Link to enqospe1 ! DON'T MODIFY OR REMOVE !
 ip address 12.12.12.10 255.255.255.252
 pvc 0/5
  encapsulation aal5snap
  protocol ppp Virtual-Template173
 !
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 log-adjacency-changes
 network 11.11.11.8 0.0.0.0 area 0
 network 192.168.114.5 0.0.0.0 area 0
!
!
no ip classless
no ip http server
ip pim bidir-enable
!
!
ip access-list extended ISC_IN_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
 permit ip any 10.10.10.0 0.0.0.255
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
 permit udp any any eq rip
 permit tcp any any eq bgp
 permit ospf any any
 permit eigrp any any
!
snmp-server community public RO
snmp-server community private RW
!
!
call rsvp-sync
!
```

```
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 30 0
 password 7 cisco
 login
line aux 0
 exec-timeout 30 0
 password 7 cisco
 login
line vty 0 4
 exec-timeout 60 0
 password 7 cisco
 login
!
!
end
```

Device enqosce52:

```
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname enqosce52
!
enable password 7 cisco
!
ip subnet-zero
ip cef
!
!
ip tftp source-interface Loopback0
no ip domain-lookup
!
!
class-map match-any ISC_OUT_Customer-A_Best-Effort
  match ip dscp 0
class-map match-any ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
  match ip rtp 16384 16383
class-map match-any ISC_OUT_Customer-A_Business-Data-1
  match ip dscp 34
class-map match-any ISC_OUT_Customer-A_Management
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
class-map match-any ISC_OUT_Customer-A_Routing_Protocol
  match access-group name ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
class-map match-any ISC_IN_Customer-A_Best-Effort
  match any
class-map match-any ISC_IN_Customer-A_Business-Data-1
  match protocol http
  match protocol telnet
  match protocol tftp
  match protocol ftp
  match protocol smtp
class-map match-any ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
```

```
  match ip dscp 46
!
!
policy-map ISC_OUT_Customer-A_CustA-QoSPolicy
  class ISC_OUT_Customer-A_CustA-QoSPolicy_VoIP
    priority percent 10
  class ISC_OUT_Customer-A_Routing_Protocol
   bandwidth percent 1
  class ISC_OUT_Customer-A_Management
   set ip dscp 34
   bandwidth percent 1
  class ISC_OUT_Customer-A_Business-Data-1
   bandwidth percent 20
  class ISC_OUT_Customer-A_Best-Effort
   bandwidth percent 25
policy-map ISC_IN_Customer-A_CustA-QoSPolicy
  class ISC_IN_Customer-A_CustA-QoSPolicy_VoIP
   set ip dscp 46
  class ISC_IN_Customer-A_Business-Data-1
   set ip dscp 34
  class ISC_IN_Customer-A_Best-Effort
   set ip dscp 0
!
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller T1 0/0
 framing sf
 linecode ami
 channel-group 0 timeslots 1-24
!
!
!
!
interface Loopback0
 description DNS entry for enqosce52 ! DON'T MODIFY or REMOVE !
 ip address 192.168.114.12 255.255.255.255
!
interface FastEthernet0/0
 description Access Link to enqossw1 ! DON'T MODIFY or REMOVE !
 ip address 11.11.11.13 255.255.255.0
 duplex auto
 speed auto
 service-policy input ISC_IN_Customer-A_CustA-QoSPolicy
!
interface Serial0/0:0
 no ip address
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface ATM1/0
 description QoS Link to enqospe5 ! DON'T MODIFY or REMOVE !
 no ip address
 no atm ilmi-keepalive
!
interface ATM1/0.52 point-to-point
 description QoS Link to enqospe5 ! DON'T MODIFY or REMOVE !
 ip address 152.152.152.2 255.255.255.252
```

```
 pvc 0/52
  encapsulation aal5snap
  service-policy output ISC_OUT_Customer-A_CustA-QoSPolicy
 !
!
router ospf 1
 log-adjacency-changes
 network 11.11.11.13 0.0.0.0 area 0
 network 192.168.114.12 0.0.0.0 area 0
!
no ip classless
ip http server
ip pim bidir-enable
!
!
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Management
 permit ip any 10.10.10.0 0.0.0.255
ip access-list extended ISC_OUT_QOS_ACL_Customer-A_CustA-QoSPolicy_Routing_Protocol
 permit udp any any eq rip
 permit tcp any any eq bgp
 permit ospf any any
 permit eigrp any any
!
!
snmp-server community public RO
snmp-server community private RW
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 30 0
 password 7 cisco
 login
line aux 0
 exec-timeout 30 0
 password 7 cisco
 login
line vty 0 4
 exec-timeout 60 0
 password 7 cisco
 login
line vty 5 15
 login
!
!
end
```

ISC Ethernet QoS Configurations

In this section, four Ethernet QoS sample configurations are depicted:

- 3550-DSCP
- 3750-DSCP with Inner VLAN
- 7600-CoS

3550-DSCP

```
mls qos cos policy-map
!
ip access-list extended isc_in_ip_acl
  permit ip any any
!
mac access-list extended isc_in_mac_acl
  permit any any
!
class-map match-all isc_in_ip_cmap
  match access-group name isc_in_ip_acl
!
class-map match-all isc_in_mac_cmap
  match access-group name isc_in_mac_acl
!
mls qos aggregate-policer isc_in_Cust_3550-DSCP_RT_FastEthernet0/5.106_vlan106 10000000
312500 exceed-action drop
!
mls qos aggregate-policer isc_in_Cust_3550-DSCP_BC_FastEthernet0/5.106_vlan106 10000000
312500 exceed-action drop
!
class-map match-all 3550-DSCPRTFA0/5.106vlan106
  match ip DSCP 46
!
class-map match-all 3550-DSCPRTFA0/5.106vlan106V
  match vlan 106
  match class-map 3550-DSCPRTFA0/5.106vlan106
!
class-map match-all 3550-DSCPBCFA0/5.106vlan106
  match ip DSCP 16
!
class-map match-all 3550-DSCPBCFA0/5.106vlan106V
  match vlan 106
  match class-map 3550-DSCPBCFA0/5.106vlan106
!
class-map match-all 3550-DSCPBEFA0/5.106vlan106V
  match vlan 106
  match class-map isc_in_ip_cmap
!
class-map match-all 3550-DSCPBEFA0/5.106vlan106VL2
  match vlan 106
  match class-map isc_in_mac_cmap
!
policy-map isc_in_FA0/5
  class 3550-DSCPRTFA0/5.106vlan106V
  police aggregate isc_in_Cust_3550-DSCP_RT_FastEthernet0/5.106_vlan106
  trust dscp
  class 3550-DSCPBCFA0/5.106vlan106V
  police aggregate isc_in_Cust_3550-DSCP_BC_FastEthernet0/5.106_vlan106
  set cos 2
  trust dscp
```

```
  class 3550-DSCPBEFA0/5.106vlan106V
  set cos 0
trust dscp
```

3750-DSCP with Inner VLAN

```
mls qos
!
no mls qos rewrite ip dscp
!
class-map match-all ISC_OUT_VLAN103_INNERVLAN3
match vlan 103
match vlan inner 3
!
class-map match-any ISC_OUT_RT_3750-DSCP
match ip dscp 46
!
class-map match-any ISC_OUT_BC_3750-DSCP
match ip dscp 16
!
policy-map ISC_OUT_3750-DSCP
class ISC_OUT_RT_3750-DSCP
police cir 25000000 bc 64000 pir 25000000 be 64000 conform-action set-cos-transmit 5
exceed-action drop violate-action drop
priority
class ISC_OUT_BC_3750-DSCP
police cir 25000000 bc 64000 pir 45000000 be 64000 conform-action set-cos-transmit 2
exceed-action set-cos-transmit 1 violate-action drop
bandwidth 45000
queue-limit 550
class class-default
bandwidth 30000
set cos 0
!
policy-map ISC_OUT_GigabitEthernet1/1/1_VLAN
class ISC_OUT_VLAN103_INNERVLAN3
bandwidth 100000
service-policy ISC_OUT_3750-DSCP
!
policy-map ISC_OUT_GigabitEthernet1/1/1
class class-default
service-policy ISC_OUT_GigabitEthernet1/1/1_VLAN
!
interface GigabitEthernet1/1/1
service-policy output ISC_OUT_GigabitEthernet1/1/1
```

7600-CoS

```
interface Vlan150
no shutdown
!
mac access-list extended isc_in_RT_7600-COS_VLAN150
permit any any cos 5 vlan 150
!
mac access-list extended isc_in_BC_7600-COS_VLAN150
permit any any cos 2 vlan 150
!
mac access-list extended isc_in_BE_7600-COS_VLAN150
permit any any cos 0 vlan 150
!
mac access-list extended isc_in_Default_7600-COS_VLAN150
```

```
permit any any vlan 150
!
class-map match-any isc_in_RT_7600-COS_VLAN150
match access-group name isc_in_RT_7600-COS_VLAN150
!
class-map match-any isc_in_BC_7600-COS_VLAN150
match access-group name isc_in_BC_7600-COS_VLAN150
!
class-map match-any isc_in_BE_7600-COS_VLAN150
match access-group name isc_in_BE_7600-COS_VLAN150
!
class-map match-any isc_in_Default_7600-COS_VLAN150
match access-group name isc_in_Default_7600-COS_VLAN150
!
policy-map isc_in_GigabitEthernet3/11
class isc_in_RT_7600-COS_VLAN150
police 20000000 3125000 3125000 conform-action transmit exceed-action drop
trust cos
class isc_in_BC_7600-COS_VLAN150
police cir 100000000 bc 3125000 pir 200000000 be 3125000 conform-action transmit
exceed-action policed-dscp-transmit violate-action drop
trust cos
class isc_in_BE_7600-COS_VLAN150
trust cos
class isc_in_Default_7600-COS_VLAN150
police 100000000 312500 312500 conform-action drop exceed-action drop
!
interface Vlan150
mac packet-classify
!
```

Metro Ethernet Use Cases

Key to provisioning Ethernet QoS, or Metro Ethernet QoS, in ISC QoS is a set of predefined policies that correspond to a variety of typical use cases.

This appendix provides a list of matching predefined policies and use and contains the following sections:

Metro Ethernet Service Type Definitions

In this section, general and QoS specific Metro Ethernet service types are defined.

General Metro Ethernet Service Types

In the Metro Ethernet 3.1 solution, the following service types apply:

- Ethernet Relay Service (ERS)—A point-to-point VLAN-based E-Line service, that is used primarily for establishing a point-point connection between customer routers.
- Ethernet Wire Service (EWS)—A point-to-point port-based E-Line service that is used primarily to connect geographically remote LANs over an SP network.
- Ethernet Multipoint Service (EMS)—A multipoint-to-multipoint port-based E-LAN service that is used for transparent LAN applications.
- Ethernet Relay Multipoint Service (ERMS)—A multipoint-to-multipoint VLAN-based E-LAN service that is used primarily for establishing a multipoint-to-multipoint connection between customer routers.
- Ethernet Private Line (EPL)—A port-based point-to-point E-Line service that maps Layer 2 traffic directly on to a TDM circuit.

Metro Ethernet QoS Service types

For Metro Ethernet QoS, the following service types are used:

- EVC—Best Effort, Business, and/or Real Time QoS on a per EVC Class of Service Identifier.
- <EVC + DSCP>—Best Effort, Business, and/or Real Time QoS on a per <EVC, DSCP> Class of Service Identifier.
- <EVC + CoS>—Best Effort, Business, and/or Real Time QoS on a per <EVC,CoS> Class of Service Identifier.

Use Cases

In the following tables, ERS and EWS represent ISC L2VPN service and ERMS, whereas EMS represents ISC VPLS service.

Use Case 1 — 3750-ME UNI to E-NNI Service Flow

This section describes the use case 3750-ME UNI to E-NNI Service Flow (Table E-1).

Table E-1 Use Case 1: 3750-ME UNI to E-NNI Service Flow

Service Type	Device	Class Type	Predefined Policy	Ethernet Link Policy
EMS, ERS, ERMS, EWS	3750-ME	EVC	3750-BE	Bandwidth: 100Mbps
EMS, ERS, ERMS, EWS	3750-ME	EVC	3750-BC	Bandwidth: 100Mbps
EMS, ERS, ERMS, EWS	3750-ME	EVC	3750-RT	Bandwidth: 100Mbps
EMS, ERS, ERMS, EWS	3750-ME	EVC + DSCP	3750-RT+BC + BE	Bandwidth: 100Mbps
ERS, ERMS	3750-ME	EVC + CoS	3750-RT+BC-BE	Bandwidth: 100Mbps
EWS, EMS	3750-ME	EVC + Inner VLAN	RT, BC, BE	Bandwidth: 100Mbps

Use Case 2 — 7600 with UNI Port

This section describes the use case 7600 with UNI port (Table E-2).

Table E-2 Use Case 2: 7600 with UNI Port

Service Type	Device	Class Type	Template	Link Template
EMS, ERS, ERMS, EWS	7600	EVC	7600-BE	Bandwidth: 100Mbps
EMS, ERS, ERMS, EWS	7600	EVC	7600-BC	Bandwidth: 100Mbps
EMS, ERS, ERMS, EWS	7600	EVC	7600-RT	Bandwidth: 100Mbps
EMS, ERS, ERMS, EWS	7600	EVC + CoS	7600-RT+BC + BE	Bandwidth: 100Mbps

Use Case 3 — 3550 UNI to E-NNI Service Flow

This section describes the use case 3550 UNI to E-NNI Service Flow (Table E-3).

Table E-3 Use Case 3: 3550 UNI to E-NNI Service Flow

Service Type	Device	Class Type	Template	Link Template
EMS, ERS, ERMS, EWS	3550	EVC + DSCP	3550-DSCP	N/A

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W