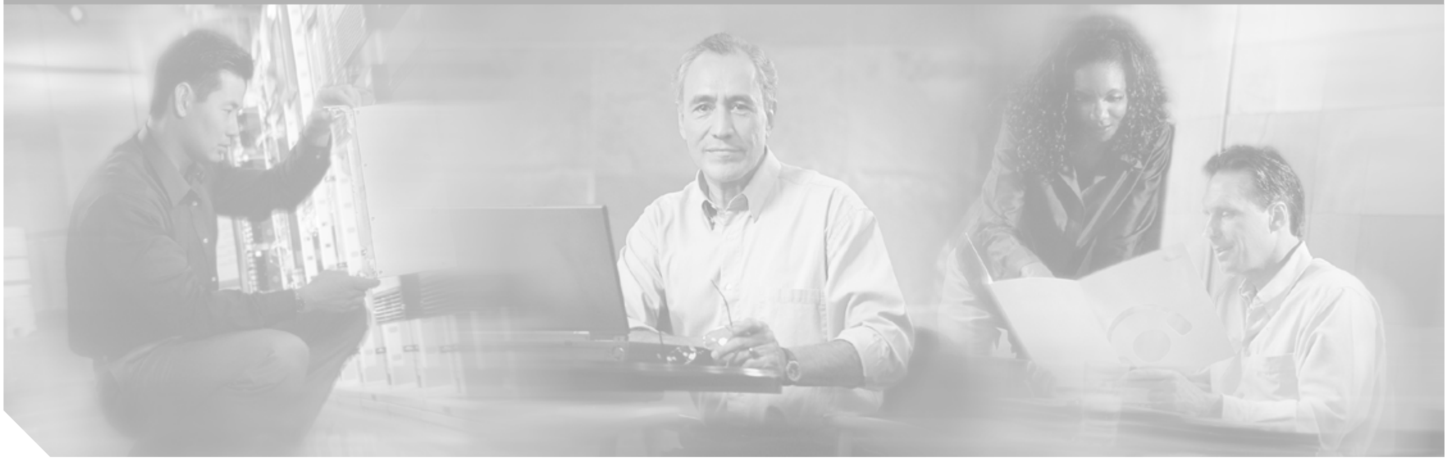


# Cisco IP Solution Center Quality of Service User Guide, 4.0

**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-6374-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO *CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.*

*Cisco IP Solution Center Quality of Service User Guide, 4.0*

# CONTENTS

# FIGURES

# TABLES

# About This Guide

This guide describes how to get started using the Quality-of-Service (QoS) management feature for the Cisco IP Solution Center (ISC), 4.0.

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
- Network topologies and protocols

## Organization

This getting started guide contains the following chapters and appendixes:

- Chapter 1, "ISC Quality of Service Concepts"
- Chapter 2, "Network Architecture"
- Chapter 3, "QoS Service Model Overview"
- Chapter 4, "Prerequisites and Assumptions"
- Chapter 5, "Provisioning Process for IP QoS"
- Chapter 6, "IP QoS Policy Parameters"

- Chapter 7, “Applying QoS Policies to VPN Services”
- Chapter 8, “Managing and Auditing Service Requests”
- Appendix A, “Sample Configurations”
- Index

# Related Documentation

TThe entire documentation set for Cisco IP Solution Center, 4.0 can be accessed at:

**http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_0**

The following documents comprise the ISC 4.0 documentation set.

General documentation (in suggested reading order):

- *Cisco IP Solution Center Documentation Guide, 4.0*
- *Cisco IP Solution Center Release Notes, 4.0*
- *Cisco IP Solution Center Installation Guide, 4.0*
- *Cisco IP Solution Center Infrastructure Reference, 4.0*
- *Cisco IP Solution Center System Error Messages, 4.0*

Application and technology documentation (listed alphabetically):

- *Cisco IP Solution Center L2VPN User Guide, 4.0*
- *Cisco IP Solution Center MPLS VPN User Guide, 4.0*
- *Cisco IP Solution Center Quality of Service User Guide, 4.0*
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0*

API documentation:

- *Cisco IP Solution Center API Programmer Guide, 4.0*
- Index: *Cisco IP Solution Center API Programmer Reference, 4.0*

**Note** All documentation *might* be upgraded.

# 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 & 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/univercd/home/home.htm

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

# Documentation Feedback

You can send comments about technical 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.

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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

- *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

- 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

# ISC Quality of Service Concepts

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 congestion avoidance 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, email 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 premise equipment (CPE) in the customer network. A QoS policy is applied to the selected set of access circuits using a QoS service request.

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 5, “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 Chapter 7, “Applying QoS Policies to VPN Services.”
- Ethernet QoS—Select an L2VPN, MPLS VPN, or VPLS service request that has already been deployed and apply QoS provisioning to that service request.

  QoS provisioning for MPLS VPN, L2VPN, and VPLS is described in Chapter 7, “Applying QoS Policies to VPN Services.”

This chapter describes the basic concepts for Quality of Service (QoS) as it is used in the ISC application.

This chapter contains the following sections:

# Introduction to ISC QoS

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* |
| Video-conferencing | 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.

# ISC QoS Components

There are three primary configuration components to 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:

- Traffic Classification, page 1-3
- Marking, page 1-4

- Rate Limiting, page 1-5
- Traffic Shaping, page 1-5
- Congestion Management, page 1-6
- Congestion Avoidance, page 1-6

Each of these components is described in the following sections.

# Traffic Classification

Traffic classification (also called packet classification) partitions traffic into multiple priority levels, or classes of service. Traffic classification is the primary component of class-based QoS provisioning.

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 six traffic classes. 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 re-classify the packet according to the QoS policy you specify in ISC.

ISC allows you to classify traffic based on source address, source port, destination port, port ranges, protocol ID, DSCP, and IP Precedence values.

## IP QoS Traffic Classification

For IP QoS, ISC uses traffic classification to associate packets with a specific service level IP QoS policy. ISC provides five template service classes to use for traffic classification.

- VoIP
- Routing Protocol
- Management
- Business-Data-1
- 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.

For more information on traffic classification in service classes, see Creating the Service Level IP QoS Policy, page 5-10.

## Ethernet QoS Traffic Classification

For Ethernet QoS, ISC uses traffic classification to associate packets with a specific service level Ethernet QoS policy. ISC provides four template service classes for Ethernet QoS to use for traffic classification.

- Architecture for Voice, Video and Integrated Data (AVVID)
- Call Control
- Business Critical
- Best Effort

A typical network uses three service classes in a QoS policy; an AVVID service class, a call control service class, and a data service class.

For more information on traffic classification in service classes, see Service Level Ethernet QoS Policy, page 7-1.

# 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.

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

**Note** See Service Level Ethernet QoS Policy Entry Fields, page 7-8 for information on Ethernet QoS packet marking.

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 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.

## MPLS Experimental Values

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.

Packet behavior for the QoS provisioning components, congestion management and congestion avoidance, are derived from the MPLS Exp. bit.

**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 Traffic Classification Based on Variables, page 4-6 for IP QoS and Service Level Ethernet QoS Policy, page 7-1 for Ethernet QoS.

## 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 CPE 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.

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.

Rate limiting parameters in ISC include:

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

For more information on configuring rate limiting QoS parameters in ISC, see Interface-Based Aggregated Rate Limiters, page 6-31 for IP QoS and Service Level Ethernet QoS Policy Entry Fields, page 7-8 for Ethernet QoS.

## 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.

Specifying traffic shaping allows you to make better use of available bandwidth. 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 a 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 6-22.

# Congestion Management

Congestion management controls congestion by determining the order in which packets are sent out 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

Congestion management parameters are configured at the service class level in ISC. For more information, see Service Level IP QoS Parameters, page 6-1 or Service Level Ethernet QoS Policy Entry Fields, page 7-8.

# Congestion Avoidance

Congestion avoidance monitors network traffic loads in an effort to anticipate and avoid congestion at common network 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 techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks before it becomes a problem.

Congestion avoidance parameters are configured at the service class level in ISC. For more information, see Service Level IP QoS Parameters, page 6-1.

# Network Architecture

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 premise equipment (CPEs) in the customer network.

Ethernet QoS provisioning with ISC supports a subset of the features required for the Metro Ethernet 2.1 Solution (Upper Kensington). With Ethernet QoS, ISC can deploy QoS Policies on Cisco Catalyst switches in a provider's network.

This chapter includes the following sections:

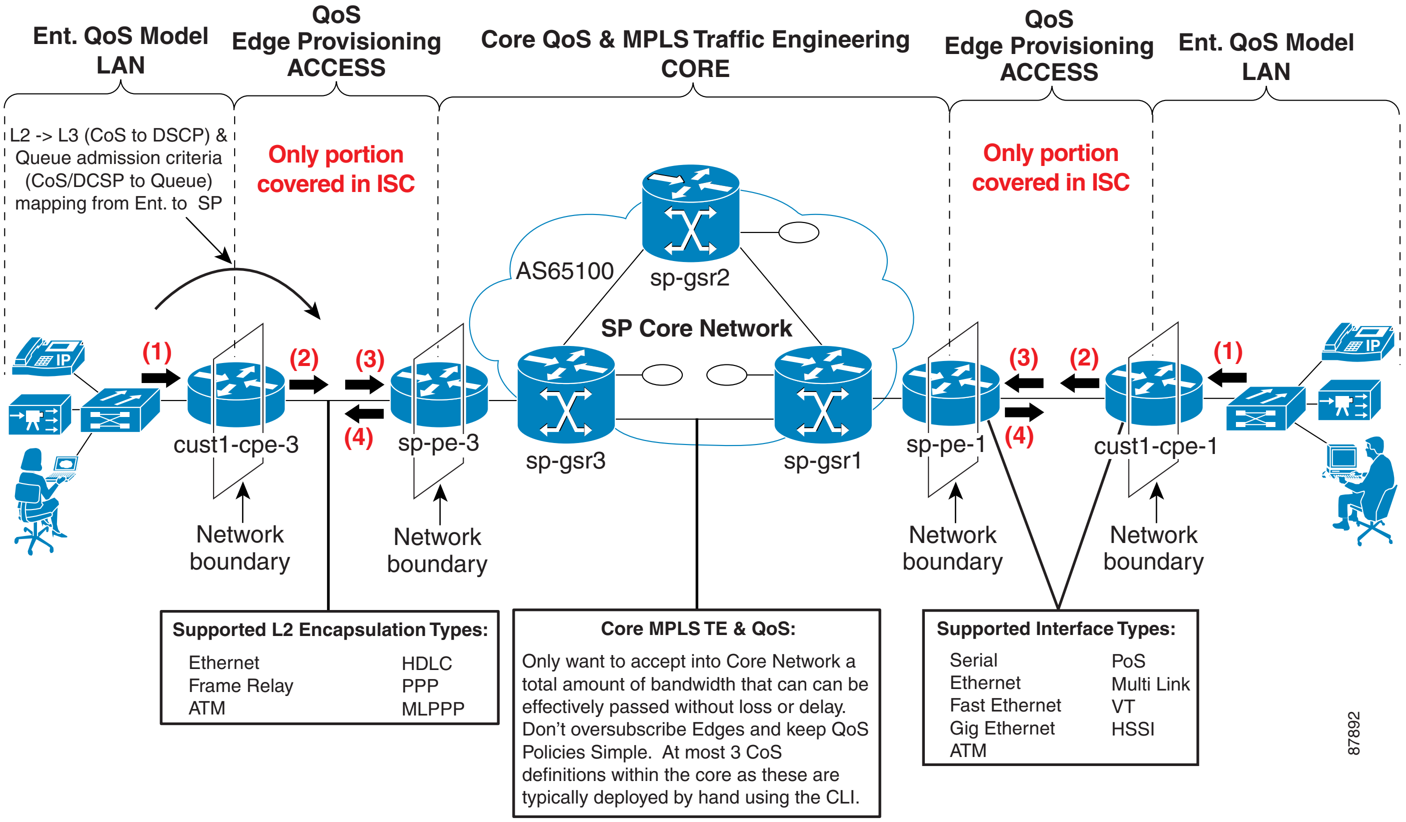
## Service Provider Network Architecture

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

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

These QoS components and concepts are represented in Figure 2-1.

*Figure 2-1 QoS Components and Concepts*



L2 -> L3 (CoS to DSCP) & Queue admission criteria (CoS/DCSP to Queue) mapping from Ent. to SP

**Supported L2 Encapsulation Types:**

Ethernet
Frame Relay
ATM
HDLC
PPP
MLPPP

**Core MPLS TE & QoS:**

Only want to accept into Core Network a total amount of bandwidth that can can be effectively passed without loss or delay. Don't oversubscribe Edges and keep QoS Policies Simple. At most 3 CoS definitions within the core as these are typically deployed by hand using the CLI.

**Supported Interface Types:**

Serial
Ethernet
Fast Ethernet
Gig Ethernet
ATM
PoS
Multi Link
VT
HSSI

# IP QoS Service Model

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 (CPE), and through the distribution portion (the CPE-PE link).

This type 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 3 or 4 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 CPE-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.

For more information on the QoS service model, see Chapter 3, “QoS Service Model Overview.”

# IP QoS Provisioning Strategies

ISC configures IP QoS at the access circuit, which involves the PE devices in the service provider network and the CPE 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 CPE, with traffic flowing from the CPE to the PE (egress traffic).
- The customer-facing interfaces on the PE, with traffic flowing from the PE to the CPE (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 CPE Scenario

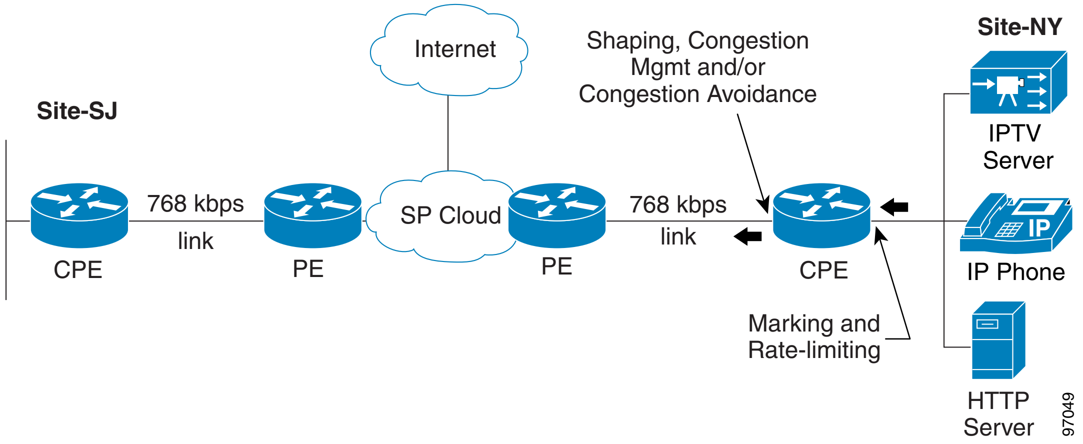
A managed CPE scenario occurs when the CPE is owned and managed by the service provider. In this network scenario, you can either apply QoS provisioning for the CPE only or for both the CPE and PE.

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

## Managed CPE Only

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

***Figure 2-2 Managed CPE Scenario***



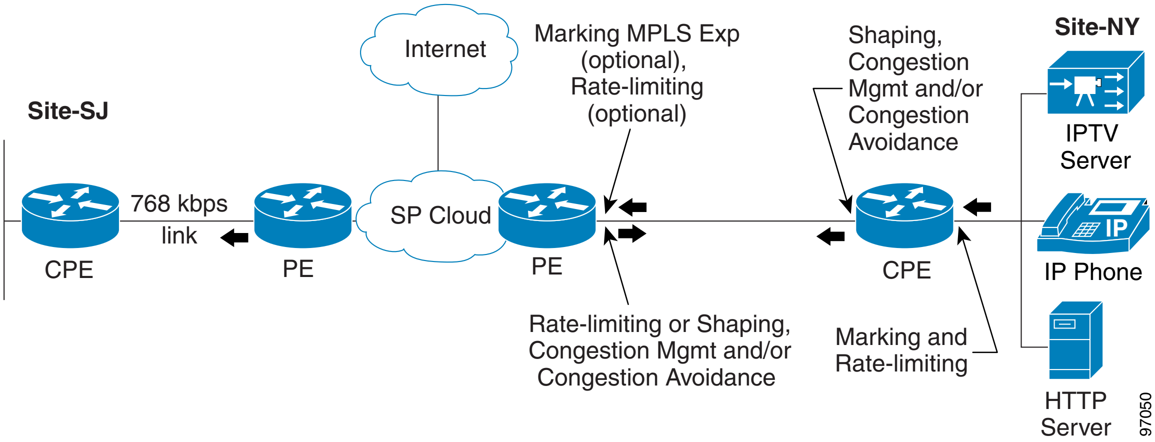
In this QoS provisioning scenario:

- Optionally configure marking and rate limiting at the customer-facing CPE 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 CPE interface and subinterfaces.

## Managed CPE and PE

Figure 2-3 illustrates a network where QoS provisioning is configured for both the managed CPE and the PE device.

*Figure 2-3 Managed CPE and PE Scenario*


Internet
Marking MPLS Exp (optional), Rate-limiting (optional)
Shaping, Congestion Mgmt and/or Congestion Avoidance
Site-NY
Site-SJ
IPTV Server
768 kbps link
SP Cloud
CPE
PE
PE
CPE
IP
IP Phone
Rate-limiting or Shaping, Congestion Mgmt and/or Congestion Avoidance
Marking and Rate-limiting
HTTP Server
97050

In this QoS provisioning scenario:

- For traffic flowing from the CPE to the PE, marking and rate-limiting are configured at the customer-facing CPE interfaces, while traffic shaping, congestion management, and congestion avoidance are configured at the provider-facing CPE interfaces and subinterfaces.
- For traffic flowing from the PE to the CPE, 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 CPE, 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 CPE to PE.

## Unmanaged CPE Scenario

An unmanaged CPE scenario occurs when the CPE 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 CPE device.

In this QoS provisioning scenario:

- You must first create the CPE 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 CPE, however, the configlet is not downloaded to the unmanaged CPE device. A configuration audit is not performed for the unmanaged CPE device.

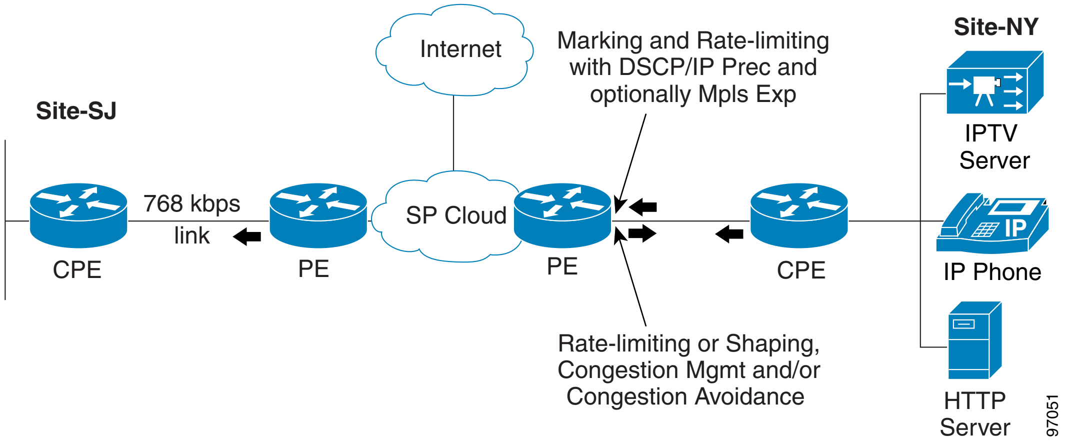
  See *Cisco IP Solution Center Infrastructure Reference, 4.0* for more information on manually creating CPE devices.
- An untrusted CPE is either not managed by the service provider or is only partially-managed by the service provider. We recommend that you re-mark and re-rate limit at the provider ingress interface for the untrusted CPE device. Configure the re-marking and re-rate limiting parameters in the service level policy.

  See Creating the Service Level IP QoS Policy, page 5-10 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 CPE interfaces.

*Figure 2-4 PE Only Scenario*



In this QoS provisioning scenario:

- For traffic flowing from the CPE 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 CPE 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 5, "Provisioning Process for IP QoS," for more information on the QoS provisioning process.

# Ethernet QoS Service Model

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

Ethernet QoS policies correspond to Ethernet QoS service classes. QoS service classes provide a method for classifying traffic.

A typical service provider network might create different QoS policies, and each QoS policy might contain 3 to 4 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 Service Level Ethernet QoS Policy, page 7-1.
- 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.
- 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 7, “Applying QoS Policies to VPN Services”.

# Ethernet QoS Provisioning Strategies

Each Ethernet link in a service request (L2VPN, MPLS, or VPLS) might contain one or two attachment circuits (end-to-end link). Each attachment circuit corresponds to one point-to-cloud QoS Link. A link contains one or two end-points: PE-CLE and PE-POP

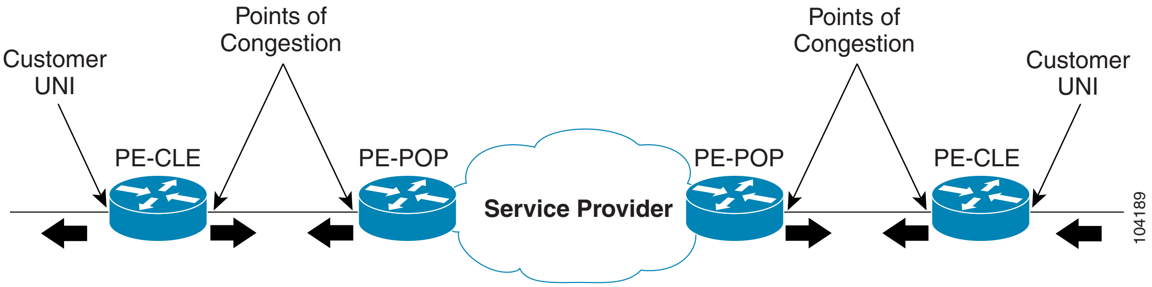
An Ethernet QoS service request binds one or more QoS links to a QoS policy. A QoS template can be attached to each end-point in a QoS link.

In a service-provider managed Ethernet QoS environment, the following three points in the access circuit are regarded as potential points of congestion:

- PE-CLE provider facing interface(s) with traffic flowing from PE-CLE to PE-POP (egress traffic)
- PE-POP customer facing interface(s) with traffic flowing from PE-POP to PE-CLE (egress traffic)
- PE-CLE customer UNI interfaces) with traffic flowing from PE-CLE to customer LAN

Figure 2-5 shows the Ethernet QoS points of congestion.

*Figure 2-5 Ethernet QoS Points of Congestion*



CHAPTER 3

# QoS Service Model Overview

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 CPEs 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 CPE 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 (CPE 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 CPE-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 VPN services, see Chapter 7, "Applying QoS Policies to VPN Services".

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

The chapter contains the following sections:

# QoS Link

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

- For the CPE 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 CPE 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 Defining QoS Link Candidates, page 5-5 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 5-10 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 6-21 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 6-2.

## 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-1 and Best Effort Service Classes, page 6-11.

# Link Level QoS Policy

The link level portion of the QoS policy corresponds to QoS parameters that are sensitive to link bandwidth and the CPE-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 CPE-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 CPE-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 CPE-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 CPE-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 6-22 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 CPE-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 6-30 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 CPE-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 5-10.

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 6-31 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 the QoS Service Request, page 5-18 for information on creating the QoS service request using the ISC user interface.

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

# Prerequisites and Assumptions

To implement QoS parameters for a network using the Cisco IP Solution Center (ISC) 4.0, you must have specific configuration information about the devices participating in QoS provisioning.

This chapter 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 chapter contains the following sections:

## Prerequisites for QoS Provisioning

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 one of the following three operations:

- Configuration import
- Autodiscovery
- Configuration collection

These operations are described in *Cisco IP Solution Center Infrastructure Reference, 4.0*.

### Viewing Device Configuration

This section describes how to view the configuration for a device and determine if you have sufficient configuration information for QoS provisioning.

To view configuration information for a device:

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

**Step 2** Under the Inventory and Connection Manager TOC, click **Devices**.

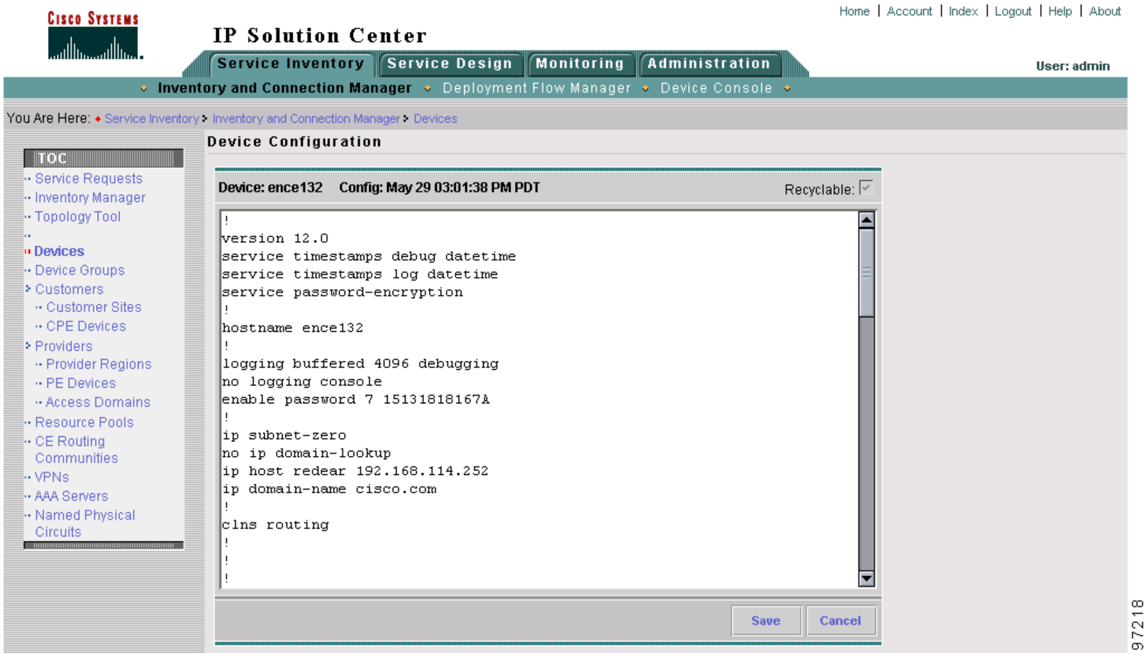
**Step 3** From the Devices window, select a device to view the configuration and click **Config**.

**Step 4** Select a date for the configuration you want to view and click **Edit**.

> **Note** Step 4 is not required if only one date is available.

The Device Configuration window appears (Figure 4-1).

*Figure 4-1 Device Configuration Example*



Device: ence132 Config: May 29 03:01:38 PM PDT Recyclable: ✓

```
!
version 12.0
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname ence132
!
logging buffered 4096 debugging
no logging console
enable password 7 15131818167A
!
ip subnet-zero
no ip domain-lookup
ip host redear 192.168.114.252
ip domain-name cisco.com
!
clns routing
!
!
!
```

This window shows the configuration information for the selected device.

# Required Device Information

For QoS provisioning, you must also have the following device information. See System Requirements in *Cisco IP Solution Center Installation Guide, 4.0* for specific configuration information.

- Cisco IOS Version
- Platform information
- Line card/port adapter information
- Device interface information
- Layer 2 encapsulation information—This is required for link level QoS configuration.

# Configuration Assumptions

This section describes device configuration assumption for QoS provisioning. These assumptions and other system requirements are further described in *Cisco IP Solution Center Release Notes, 4.0*.

All CPE and PE devices participating in a QoS provisioning service request must have the following as part of the initial configuration:

- IPv4—IPv4 connectivity must be in place before the QoS provisioning process can be completed.
- Cisco express forwarding (CEF) or Distributed CEF (dCEF)—QoS provisioning requires that you enable CEF or dCEF on all CPE 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.
  - dCEF 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.

ISC treats the global **mls qos** command as a prerequisite for Metro Ethernet QoS deployment. You must use this command to enable QoS on the Catalyst 3550. ISC does not automatically provision the **mls qos** command but requires it to be part of the initial configuration.

The **mls qos** command has a global effect on the switch and is not ever disabled by ISC. If you do not enable the QoS switch on the Catalyst 3550 with the **mls qos** command, all the QoS commands provisioned by ISC do download to the switch and the QoS service request does go to the DEPLOYED state. However QoS is not in effect until it is enabled with the **mls qos** command.

## 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 QoS provisioning in the context of the following:

- GRE **- GRE is not supported in this release. -**
- IPsec **- IPsec is not supported in this release. -**
- L2F/L2TP

ISC supports the following layer 2 encapsulations for QoS provisioning:

- Ethernet
- 802.1q
- 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.

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

# Editing the Properties File

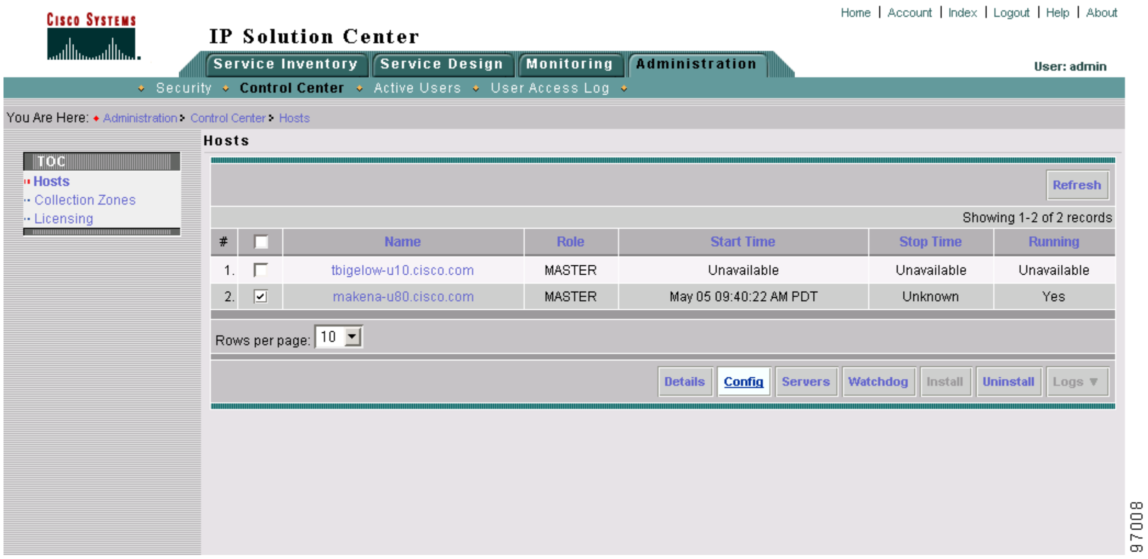
The ISC Dynamic Component Properties Library (DCPL) file, which is the system properties file for ISC 4.0, contains several QoS-specific properties that can be preconfigured or edited prior to QoS provisioning.

The QoS configuration property in the DCPL file is the Management LAN Address

To edit QoS properties in the DCPL file:

**Step 1** From the Administration tab, click **Control Center**. The Hosts window appears (Figure 4-2).

***Figure 4-2 ISC Hosts***

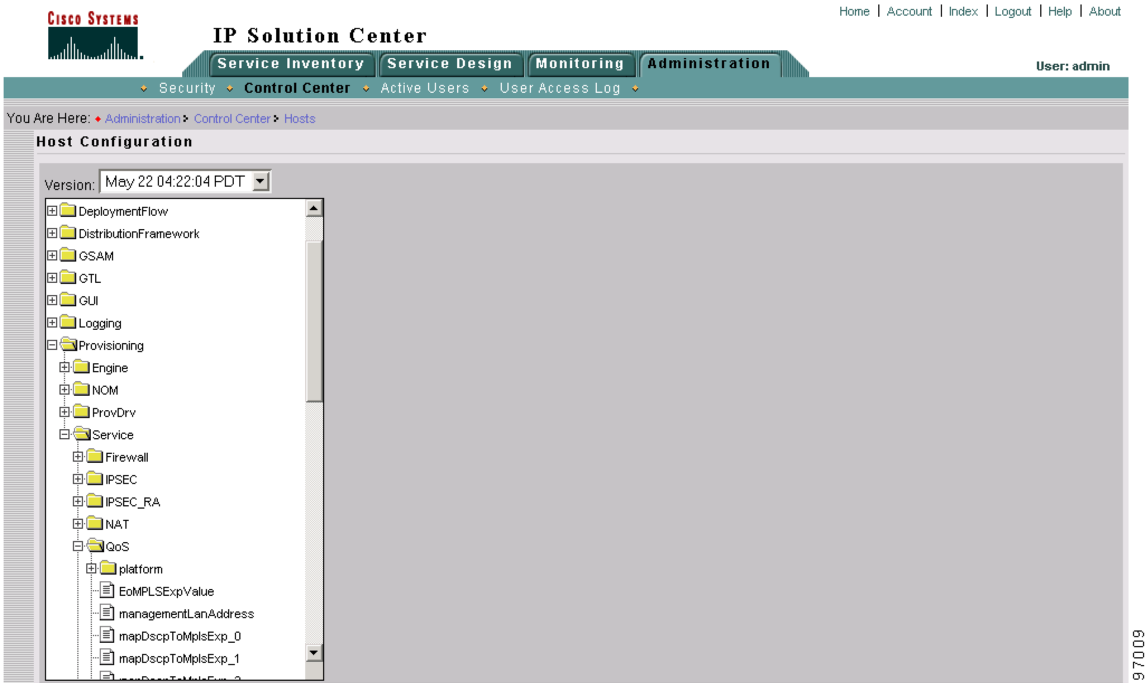


| # | ☐ | Name | Role | Start Time | Stop Time | Running |
|---|---|---|---|---|---|---|
| 1. | ☐ | tbigelow-u10.cisco.com | MASTER | Unavailable | Unavailable | Unavailable |
| 2. | ☑ | makena-u80.cisco.com | MASTER | May 05 09:40:22 AM PDT | Unknown | Yes |

The Host window lists ISC servers available for configuration edits.

**Step 2** Select a host and click **Config**. The Host Configuration window appears (Figure 4-3).

*Figure 4-3 Host Configuration Files*



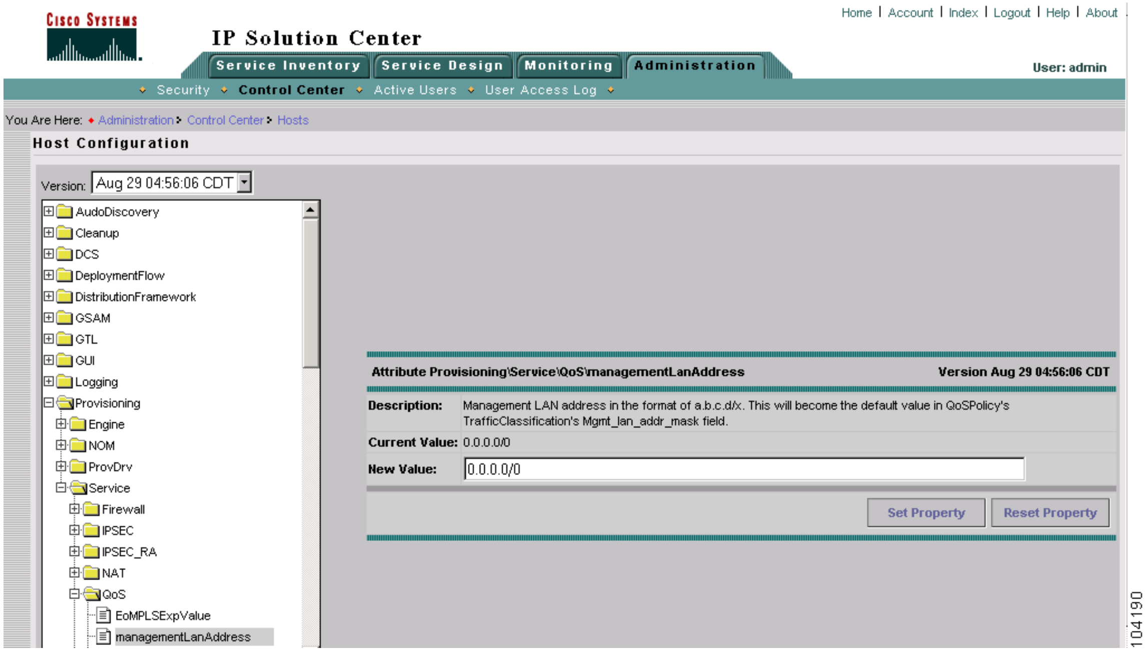
This window displays the folder structure in the DCPL file. Each folder has a list of properties whose configurations can be edited.

This section describes the QoS configuration properties. For more information on other properties in the DCPL file, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

**Step 3** Navigate to the QoS folder (**Provisioning > Service > QoS**).

**Step 4** Select **managementLanAddress**. The Management LAN Address Attribute Provisioning window opens as shown in Figure 4-4.

*Figure 4-4 Host Configuration—Management LAN Address*



Version: Aug 29 04:56:06 CDT

Attribute Provisioning\Service\QoS\managementLanAddress Version Aug 29 04:56:06 CDT

Description: Management LAN address in the format of a.b.c.d/x. This will become the default value in QoSPolicy's TrafficClassification's Mgmt_lan_addr_mask field.

Current Value: 0.0.0.0/0

New Value: 0.0.0.0/0

**Step 5** Edit this value to preconfigure the management LAN address to use for traffic classification in the Management service class. For more information, see Editing the Management Service Class, page 6-9.

Enter the new management LAN address and subnet mask. This becomes the new default for the traffic classification field for the Management service class.

**Step 6** Click **Set Property**.

# Traffic Classification Based on Variables

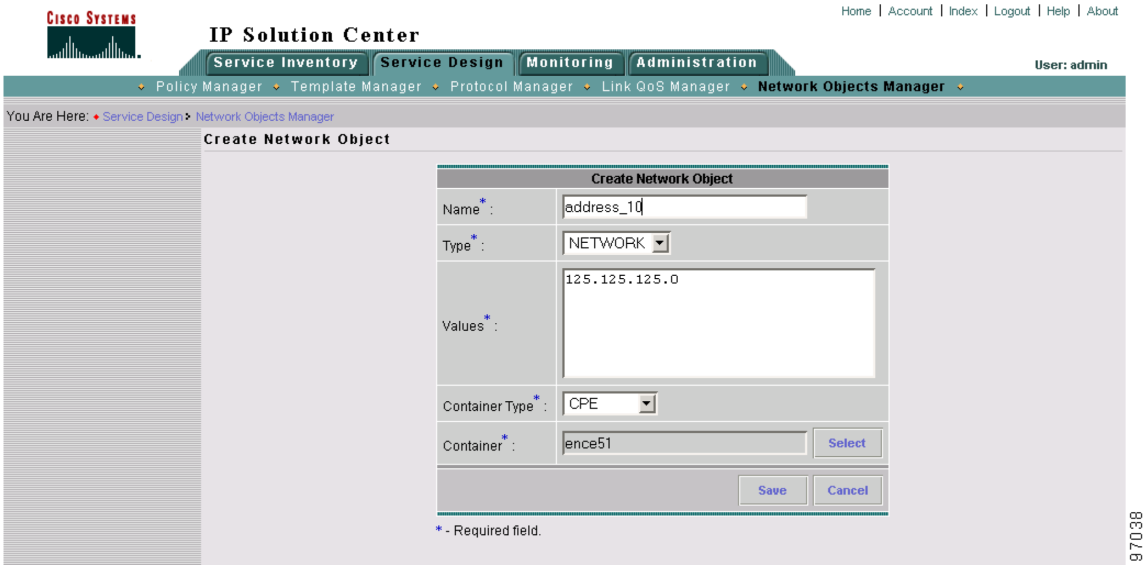
This section describes how to enter a variable containing a network address in the Network Objects Manager to be used later in the QoS provisioning process. This example describes how to classify traffic based on network addresses contained in variables, instead of based on protocols. You can then use this variable when configuring the traffic classification section within a service class.

To create network object variable:

**Step 1** From the Service Design window, click **Network Objects Manager**.

**Step 2** Click **Create**. The Create Network Object window appears (Figure 4-5).

*Figure 4-5 Create Network Object*



Create Network Object

| Create Network Object | |
|---|---|
| Name* : | address_10 |
| Type* : | NETWORK |
| Values* : | 125.125.125.0 |
| Container Type* : | CPE |
| Container* : | ence51 |

* - Required field.

**Step 3** Enter the object attributes. All fields are required.

For example, to configure a network address range, enter the following:

- Name—Address_10
- Type—Network
- Values—125.125.125.0/24
- Container Type—CPE
- Container—Select the CPE device participating in QoS provisioning.

**Step 4** Click **Save**.

This variable name (Address_10) is the value you enter in the Source field when configuring traffic classification based on addresses in a QoS service level policy. For more information on traffic classification based on addresses, see Traffic Classification, page 6-17.

The ISC configlet for this network address variable example becomes:

```
permit ip 125.125.125.0 0.0.0.255 any
```

Instead of:

```
match any
```

The create network object variable feature can also be used by other ISC services.

# 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 VPN services, such as MPLS, L2VPN, and VPLS, see Chapter 7, "Applying QoS Policies to VPN Services."

The chapter contains the following sections:

## IP QoS Process Model

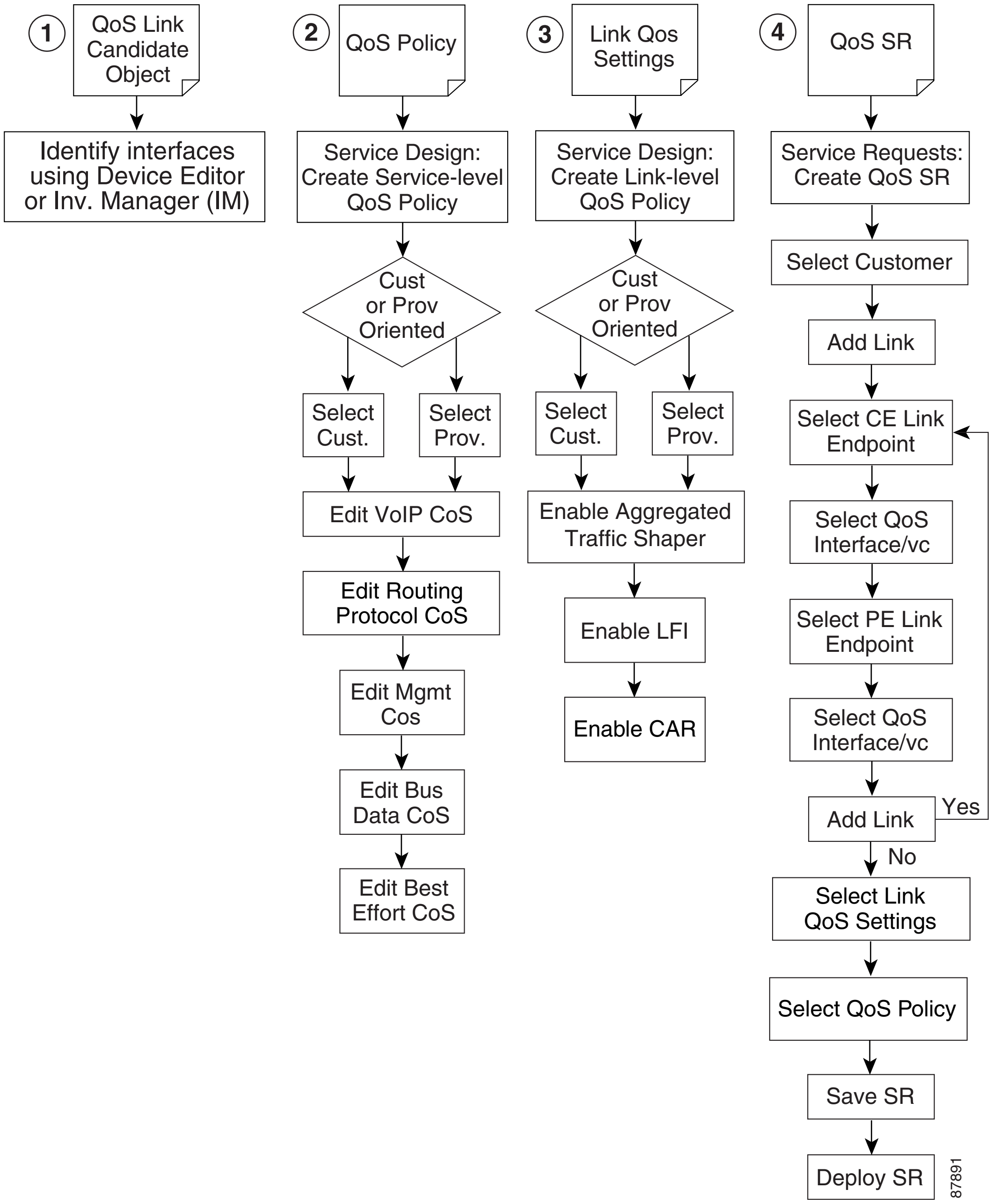
The QoS process model in ISC is designed so that different types of users (for example, network administrators and service operators), can define different aspects of the QoS provisioning process.

The QoS provisioning process in ISC includes four operations:

- Defining the QoS Link Candidates—Identifying device interfaces for QoS provisioning
- Defining the QoS Policy—QoS policy based on service classes
- Defining the Link QoS Settings—QoS parameters that are sensitive to link bandwidth and Layer 2 encapsulation.
- Create and deploy the QoS service request—Create a container for the QoS policy and QoS link settings and apply these parameters to the devices in the service provider network.

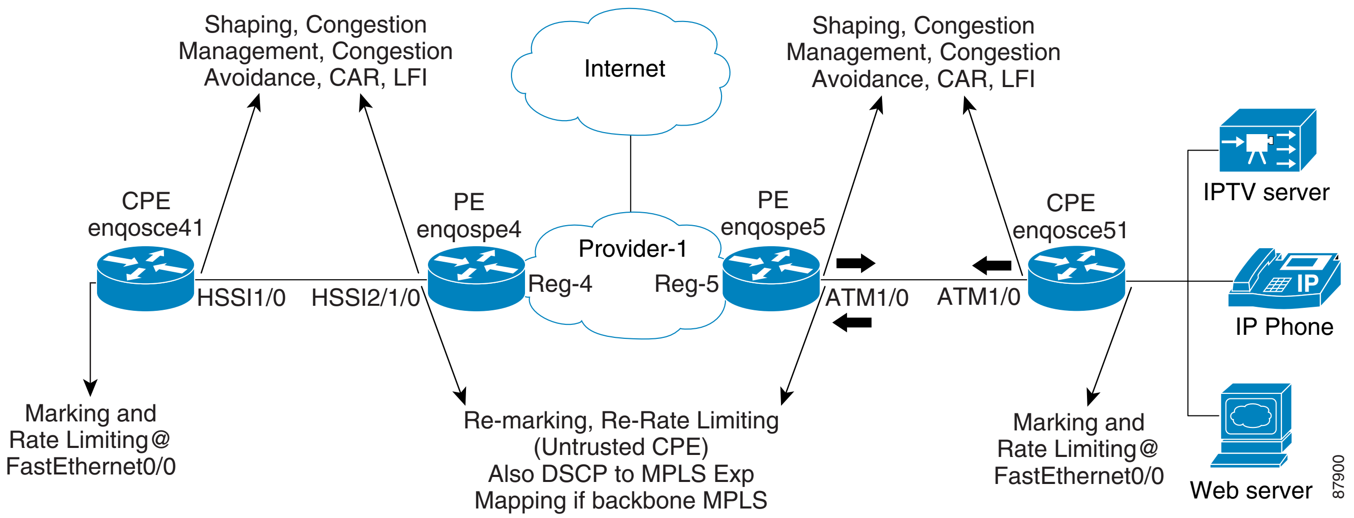
Figure 5-1 depicts the ISC process flow for QoS provisioning.

*Figure 5-1 Process Flow for IP QoS Provisioning*



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 5-2).

*Figure 5-2 Example of QoS Policy Deployment*


Shaping, Congestion Management, Congestion Avoidance, CAR, LFI
Internet
Shaping, Congestion Management, Congestion Avoidance, CAR, LFI
IPTV server
CPE enqosce41
PE enqospe4
Provider-1
PE enqospe5
CPE enqosce51
HSSI1/0
HSSI2/1/0
Reg-4
Reg-5
ATM1/0
ATM1/0
IP
IP Phone
Marking and Rate Limiting@ FastEthernet0/0
Re-marking, Re-Rate Limiting (Untrusted CPE) Also DSCP to MPLS Exp Mapping if backbone MPLS
Marking and Rate Limiting@ FastEthernet0/0
Web server
87900

# Launching the GUI

The ISC user interface is designed so that different types of users can manage different aspects of the QoS provisioning process. For example:

- A network operator can use the Service Inventory tab to identify the device interfaces to be used for QoS provisioning. The device interfaces are called link end-points in the ISC GUI, and when selected, the device interface becomes a QoS Link Candidate to be used later in the QoS service request.
- A second network operator can use the Service Design tab to create service level and link level QoS polices. Use the Policy Manager hyperlink to create the service level QoS polices, and use the Link QoS Manager hyperlink to create the link level QoS polices.
- A service operator can use the Service Inventory tab to construct a QoS service request and deploy it in to the network.

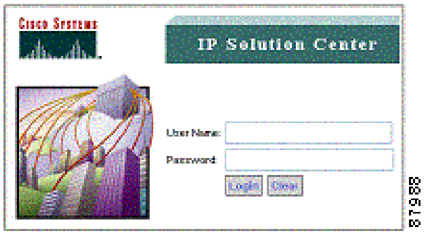
**Note** To use the ISC user interface, you must be using Netscape Version 7.0 or later or Microsoft Internet Explorer, Version 6.0 or later.

To launch the ISC GUI:

**Step 1** Open a web browser and enter the following URL to access the login screen (Figure 5-3):

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

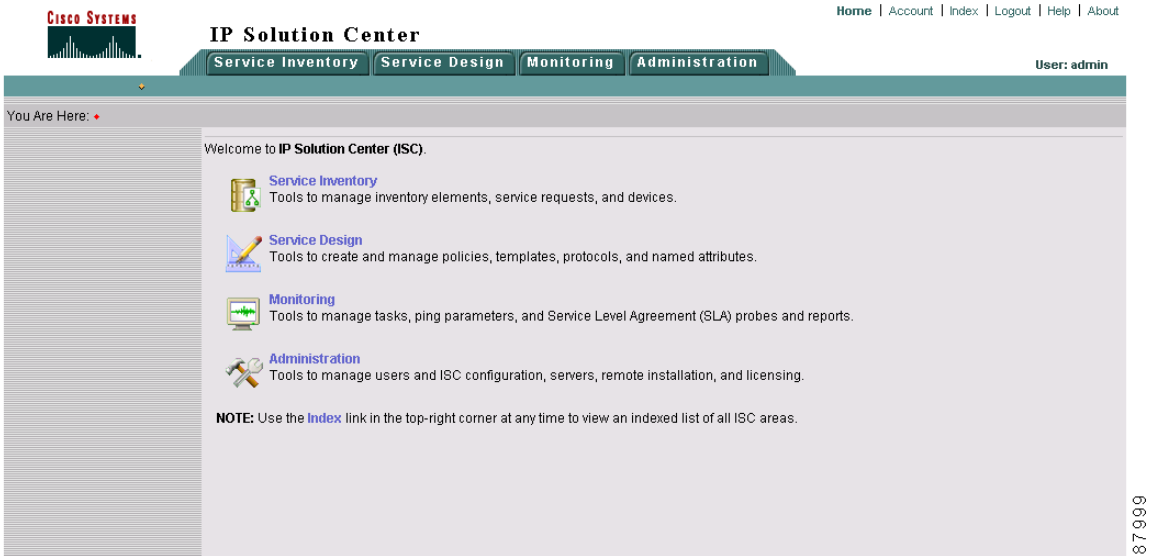
*Figure 5-3 ISC Login Screen*



**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 5-4).

*Figure 5-4 ISC Home Window*



Welcome to **IP Solution Center (ISC)**.

Service Inventory
Tools to manage inventory elements, service requests, and devices.

Service Design
Tools to create and manage policies, templates, protocols, and named attributes.

Monitoring
Tools to manage tasks, ping parameters, and Service Level Agreement (SLA) probes and reports.

Administration
Tools to manage users and ISC configuration, servers, remote installation, and licensing.

**NOTE:** Use the Index link in the top-right corner at any time to view an indexed list of all ISC areas.

The home window provides access to the four main areas of operation in ISC; Service Inventory, Service Design, Monitoring, and Administration. For QoS provisioning, the two main operation areas are:

- Service Inventory—QoS provisioning in this area includes marking device interfaces for QoS provisioning. This operation is described in Defining QoS Link Candidates, page 5-5.
- Service Design—QoS provisioning in this area includes creating a QoS policy and defining link level QoS settings. These operations are described in Defining QoS Policies, page 5-9 and Defining the Link Level QoS Policy, page 5-15.

**Note** The ISC home window you see depends on the licensed service packages you purchased.

# Defining QoS Link Candidates

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 2-3.

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

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

- For the CPE 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 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.

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

- Selecting CPE Device Interfaces for QoS, page 5-5
- Selecting PE Device Interfaces for QoS, page 5-7

## Selecting CPE Device Interfaces for QoS

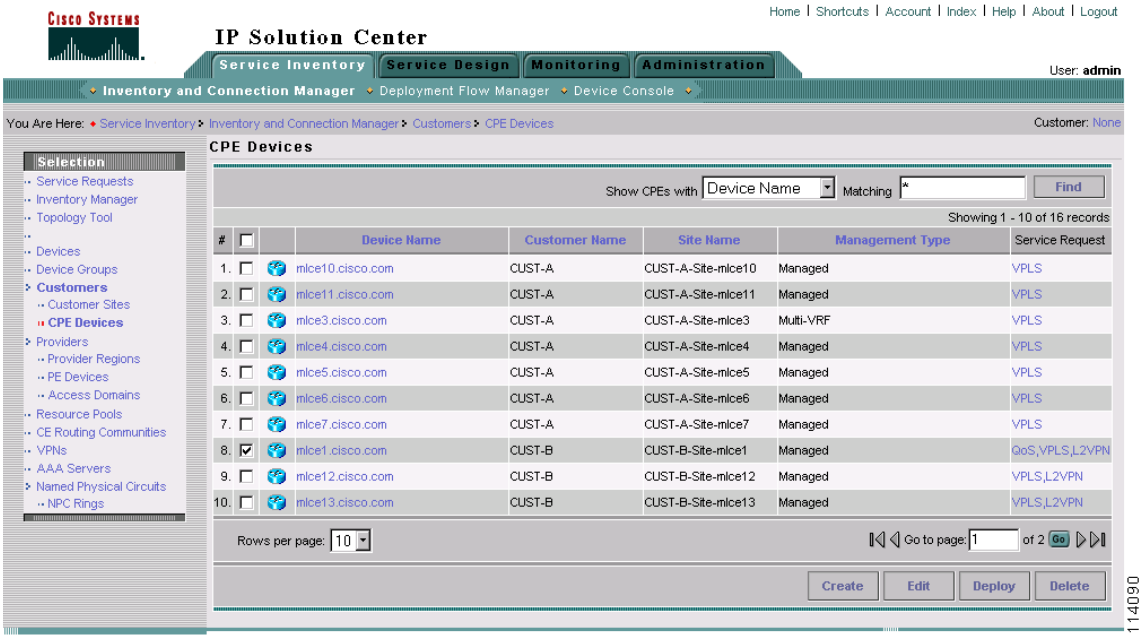
Typically, the service provider supplies the list of devices and interfaces to be selected for QoS provisioning. This section describes how to select device interfaces for QoS.

To select interfaces in a CPE device for QoS:

**Step 1** On the Service Inventory tab, click **Inventory and Connection Manager**. The left pane of the CPE 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 **CPE Devices**, which is located under Customers in the hierarchy pane. This displays the CPE Devices window and lists all CPE devices that can be edited (Figure 5-5).

*Figure 5-5 CPE Devices List*



CPE Devices

Show CPEs with: Device Name  Matching: *

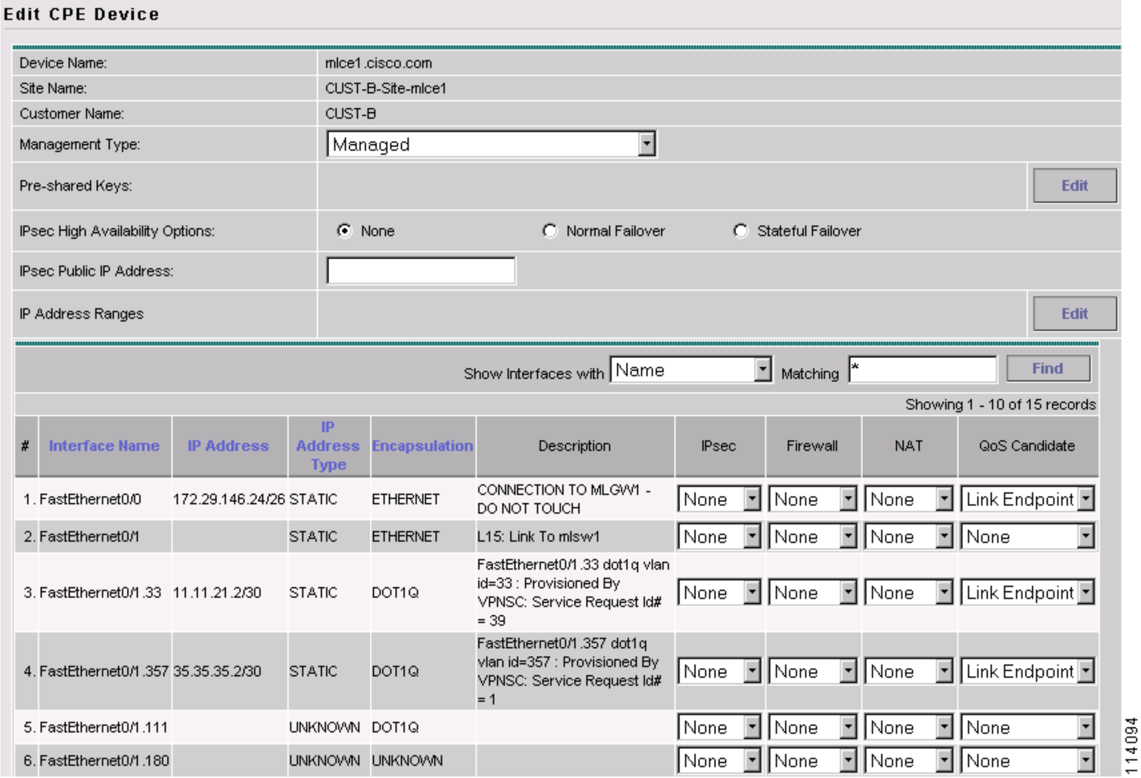
Showing 1 - 10 of 16 records

| # | ☐ | | Device Name | Customer Name | Site Name | Management Type | Service Request |
|---|---|---|---|---|---|---|---|
| 1. | ☐ | | mlce10.cisco.com | CUST-A | CUST-A-Site-mlce10 | Managed | VPLS |
| 2. | ☐ | | mlce11.cisco.com | CUST-A | CUST-A-Site-mlce11 | Managed | VPLS |
| 3. | ☐ | | mlce3.cisco.com | CUST-A | CUST-A-Site-mlce3 | Multi-VRF | VPLS |
| 4. | ☐ | | mlce4.cisco.com | CUST-A | CUST-A-Site-mlce4 | Managed | VPLS |
| 5. | ☐ | | mlce5.cisco.com | CUST-A | CUST-A-Site-mlce5 | Managed | VPLS |
| 6. | ☐ | | mlce6.cisco.com | CUST-A | CUST-A-Site-mlce6 | Managed | VPLS |
| 7. | ☐ | | mlce7.cisco.com | CUST-A | CUST-A-Site-mlce7 | Managed | VPLS |
| 8. | ☑ | | mlce1.cisco.com | CUST-B | CUST-B-Site-mlce1 | Managed | QoS,VPLS,L2VPN |
| 9. | ☐ | | mlce12.cisco.com | CUST-B | CUST-B-Site-mlce12 | Managed | VPLS,L2VPN |
| 10. | ☐ | | mlce13.cisco.com | CUST-B | CUST-B-Site-mlce13 | Managed | VPLS,L2VPN |

Rows per page: 10  Go to page: 1 of 2

**Step 3** Select the check box next to the CPE device (for example, mlce1) and click **Edit**. The Edit CPE Device window appears (Figure 5-6). This window lists device details and all interfaces that might be candidates for QoS provisioning.

*Figure 5-6 Identify CPE Device Interface as QoS Candidate*



Edit CPE Device

| | |
|---|---|
| Device Name: | mlce1.cisco.com |
| Site Name: | CUST-B-Site-mlce1 |
| Customer Name: | CUST-B |
| Management Type: | Managed |
| Pre-shared Keys: | |
| IPsec High Availability Options: | ● None ○ Normal Failover ○ Stateful Failover |
| IPsec Public IP Address: | |
| IP Address Ranges | |

Show Interfaces with: Name  Matching: *

Showing 1 - 10 of 15 records

| # | Interface Name | IP Address | IP Address Type | Encapsulation | Description | IPsec | Firewall | NAT | QoS Candidate |
|---|---|---|---|---|---|---|---|---|---|
| 1. | FastEthernet0/0 | 172.29.146.24/26 | STATIC | ETHERNET | CONNECTION TO MLGW1 - DO NOT TOUCH | None | None | None | Link Endpoint |
| 2. | FastEthernet0/1 | | STATIC | ETHERNET | L15: Link To mlsw1 | None | None | None | None |
| 3. | FastEthernet0/1.33 | 11.11.21.2/30 | STATIC | DOT1Q | FastEthernet0/1.33 dot1q vlan id=33 : Provisioned By VPNSC: Service Request Id# = 39 | None | None | None | Link Endpoint |
| 4. | FastEthernet0/1.357 | 35.35.35.2/30 | STATIC | DOT1Q | FastEthernet0/1.357 dot1q vlan id=357 : Provisioned By VPNSC: Service Request Id# = 1 | None | None | None | Link Endpoint |
| 5. | FastEthernet0/1.111 | | UNKNOWN | DOT1Q | | None | None | None | None |
| 6. | FastEthernet0/1.180 | | UNKNOWN | UNKNOWN | | None | None | None | None |

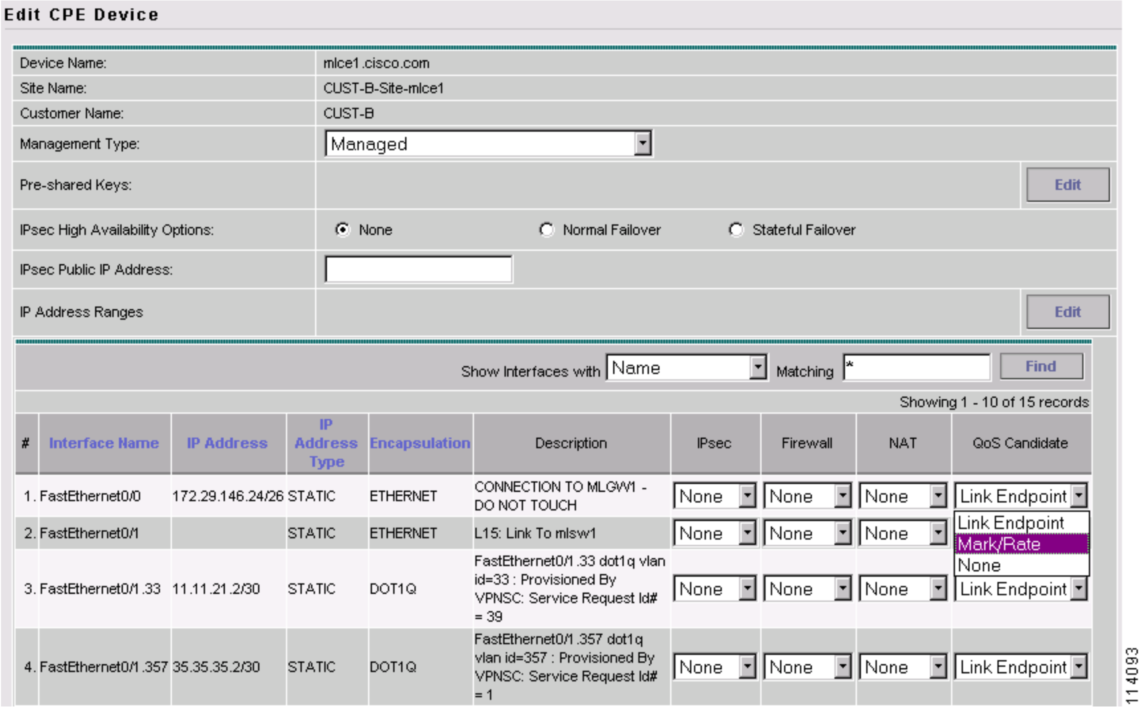
**Step 4** Select the device interface for QoS provisioning. Select **Link Endpoint** from the QoS Candidate drop-down menu. This selects the interface on this CPE device as a link endpoint for QoS provisioning.

For information on the other entry fields in the Edit CPE Device window, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

**Step 5** For the same CPE device, select the customer-facing LAN interface. Select **Mark/Rate** from the QoS Candidate menu (Figure 5-7). This selects the interface on this CPE 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 5-7 Identify Customer-Facing LAN Interface as QoS Candidate***



Edit CPE Device

| | |
|---|---|
| Device Name: | mlce1.cisco.com |
| Site Name: | CUST-B-Site-mlce1 |
| Customer Name: | CUST-B |
| Management Type: | Managed |
| Pre-shared Keys: | Edit |
| IPsec High Availability Options: | ● None ○ Normal Failover ○ Stateful Failover |
| IPsec Public IP Address: | |
| IP Address Ranges | Edit |

Show Interfaces with Name Matching * Find

Showing 1 - 10 of 15 records

| # | Interface Name | IP Address | IP Address Type | Encapsulation | Description | IPsec | Firewall | NAT | QoS Candidate |
|---|---|---|---|---|---|---|---|---|---|
| 1. | FastEthernet0/0 | 172.29.146.24/26 | STATIC | ETHERNET | CONNECTION TO MLGW1 - DO NOT TOUCH | None | None | None | Link Endpoint |
| 2. | FastEthernet0/1 | | STATIC | ETHERNET | L15: Link To mlsw1 | None | None | None | Link Endpoint<br>Mark/Rate<br>None |
| 3. | FastEthernet0/1.33 | 11.11.21.2/30 | STATIC | DOT1Q | FastEthernet0/1.33 dot1q vlan id=33 : Provisioned By VPNSC: Service Request Id# = 39 | None | None | None | Link Endpoint |
| 4. | FastEthernet0/1.357 | 35.35.35.2/30 | STATIC | DOT1Q | FastEthernet0/1.357 dot1q vlan id=357 : Provisioned By VPNSC: Service Request Id# = 1 | None | None | None | Link Endpoint |

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

**Step 7** Repeat Steps 1 through 4 for each CPE device that requires QoS provisioning. For each CPE 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 CPE 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 CPE-PE link for QoS provisioning. Typically, the PE device is marked for QoS parameters at the customer-facing interface.

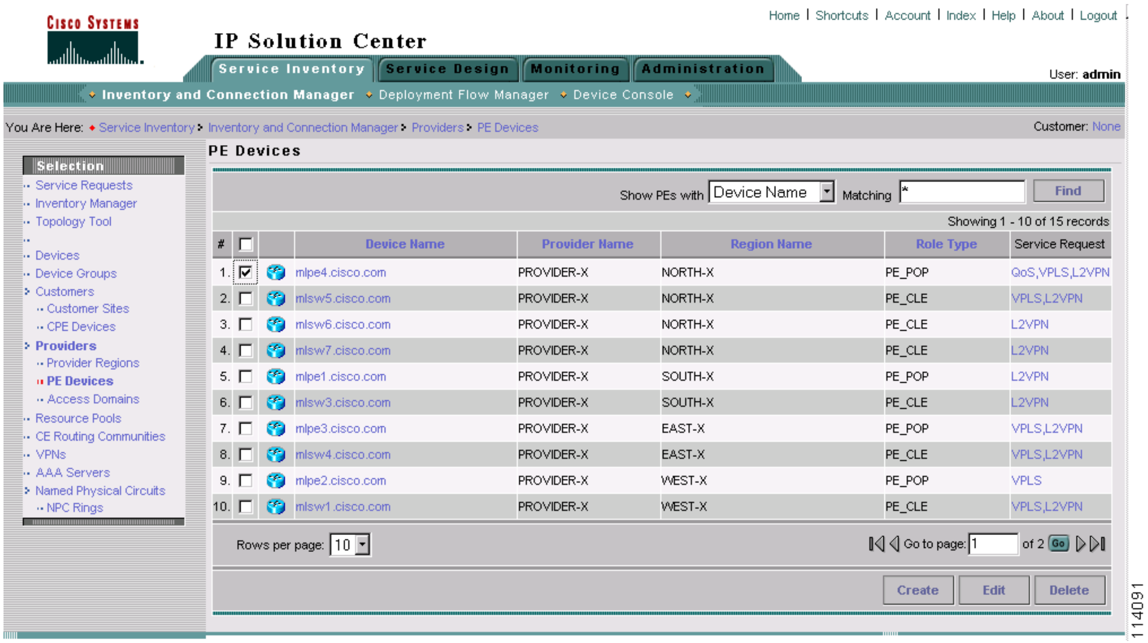
**Note** If you have an untrusted CPE, one that is not managed or only partially managed by ISC, you can also re-mark and re-rate limit at the PE interface. Re-marking and re-rate limiting for PE devices is provisioned within the service class policy. See Creating the Service Level IP QoS Policy, page 5-10.

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 5-8).

***Figure 5-8 PE Devices List***



You Are Here: Service Inventory > Inventory and Connection Manager > Providers > PE Devices

Customer: None

PE Devices

Show PEs with Device Name Matching *

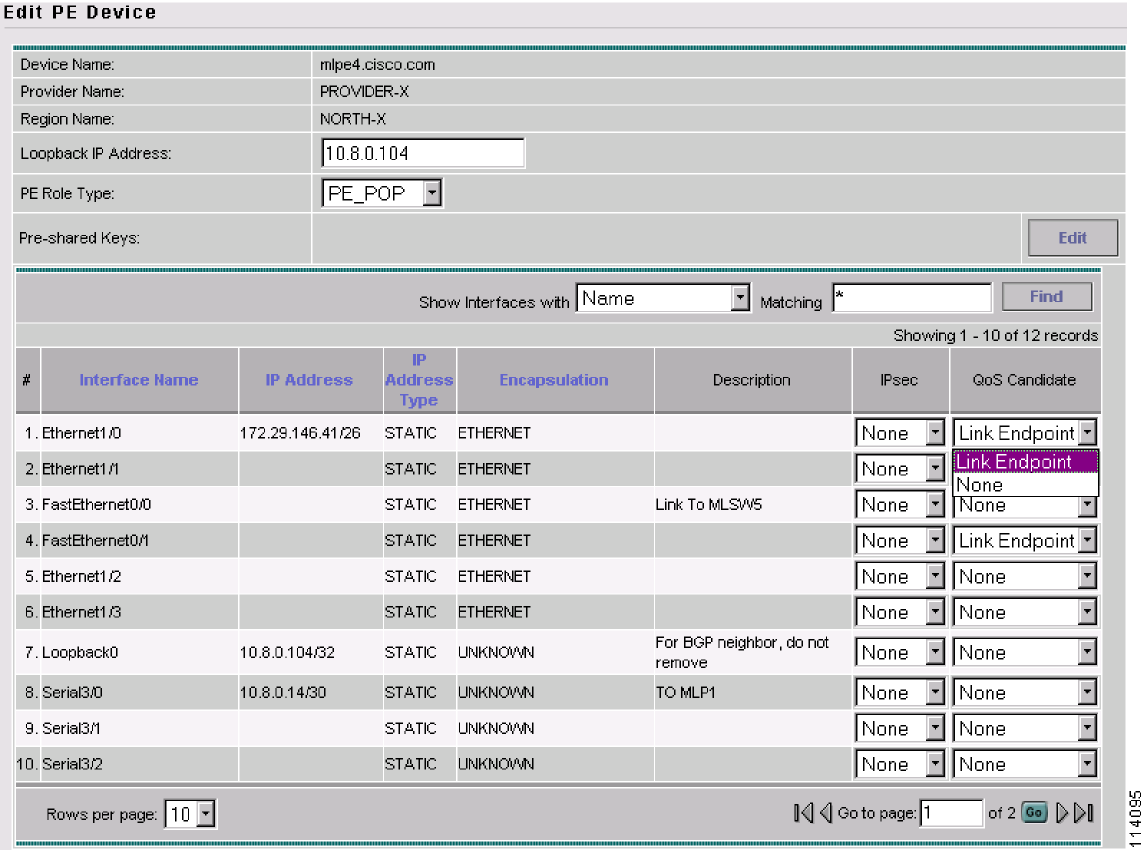
Showing 1 - 10 of 15 records

| # | □ | Device Name | Provider Name | Region Name | Role Type | Service Request |
|---|---|---|---|---|---|---|
| 1. | ☑ | mlpe4.cisco.com | PROVIDER-X | NORTH-X | PE_POP | QoS,VPLS,L2VPN |
| 2. | □ | mlsw5.cisco.com | PROVIDER-X | NORTH-X | PE_CLE | VPLS,L2VPN |
| 3. | □ | mlsw6.cisco.com | PROVIDER-X | NORTH-X | PE_CLE | L2VPN |
| 4. | □ | mlsw7.cisco.com | PROVIDER-X | NORTH-X | PE_CLE | L2VPN |
| 5. | □ | mlpe1.cisco.com | PROVIDER-X | SOUTH-X | PE_POP | L2VPN |
| 6. | □ | mlsw3.cisco.com | PROVIDER-X | SOUTH-X | PE_CLE | L2VPN |
| 7. | □ | mlpe3.cisco.com | PROVIDER-X | EAST-X | PE_POP | VPLS,L2VPN |
| 8. | □ | mlsw4.cisco.com | PROVIDER-X | EAST-X | PE_CLE | VPLS,L2VPN |
| 9. | □ | mlpe2.cisco.com | PROVIDER-X | WEST-X | PE_POP | VPLS |
| 10. | □ | mlsw1.cisco.com | PROVIDER-X | WEST-X | PE_CLE | VPLS,L2VPN |

Rows per page: 10 Go to page: 1 of 2 Go

**Step 3** Select the check box next to the PE device (for example, mlpe4) and click **Edit.** The Edit PE Device window appears (Figure 5-9). This window lists device details and all interfaces that might be candidates for QoS provisioning.

*Figure 5-9 Identify PE Device Interface as QoS Candidate*



Edit PE Device

| | |
|---|---|
| Device Name: | mlpe4.cisco.com |
| Provider Name: | PROVIDER-X |
| Region Name: | NORTH-X |
| Loopback IP Address: | 10.8.0.104 |
| PE Role Type: | PE_POP |
| Pre-shared Keys: | Edit |

Show Interfaces with Name Matching * Find

Showing 1 - 10 of 12 records

| # | Interface Name | IP Address | IP Address Type | Encapsulation | Description | IPsec | QoS Candidate |
|---|---|---|---|---|---|---|---|
| 1. | Ethernet1/0 | 172.29.146.41/26 | STATIC | ETHERNET | | None | Link Endpoint |
| 2. | Ethernet1/1 | | STATIC | ETHERNET | | None | Link Endpoint<br>None |
| 3. | FastEthernet0/0 | | STATIC | ETHERNET | Link To MLSW5 | None | None |
| 4. | FastEthernet0/1 | | STATIC | ETHERNET | | None | Link Endpoint |
| 5. | Ethernet1/2 | | STATIC | ETHERNET | | None | None |
| 6. | Ethernet1/3 | | STATIC | ETHERNET | | None | None |
| 7. | Loopback0 | 10.8.0.104/32 | STATIC | UNKNOWN | For BGP neighbor, do not remove | None | None |
| 8. | Serial3/0 | 10.8.0.14/30 | STATIC | UNKNOWN | TO MLP1 | None | None |
| 9. | Serial3/1 | | STATIC | UNKNOWN | | None | None |
| 10. | Serial3/2 | | STATIC | UNKNOWN | | None | None |

Rows per page: 10 Go to page: 1 of 2 Go

**Step 4** Select the interface (for example Ethernet1/0) 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.

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 5-10.

**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.

# Defining 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 Manager**.

This section describes how to define a QoS policy using the ISC GUI and includes the following:

- Creating the Service Level IP QoS Policy, page 5-10
- Defining the Link Level QoS Policy, page 5-15

## Creating the Service Level IP 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
- Routing Protocol
- Management
- Business-Data-1
- Best Effort

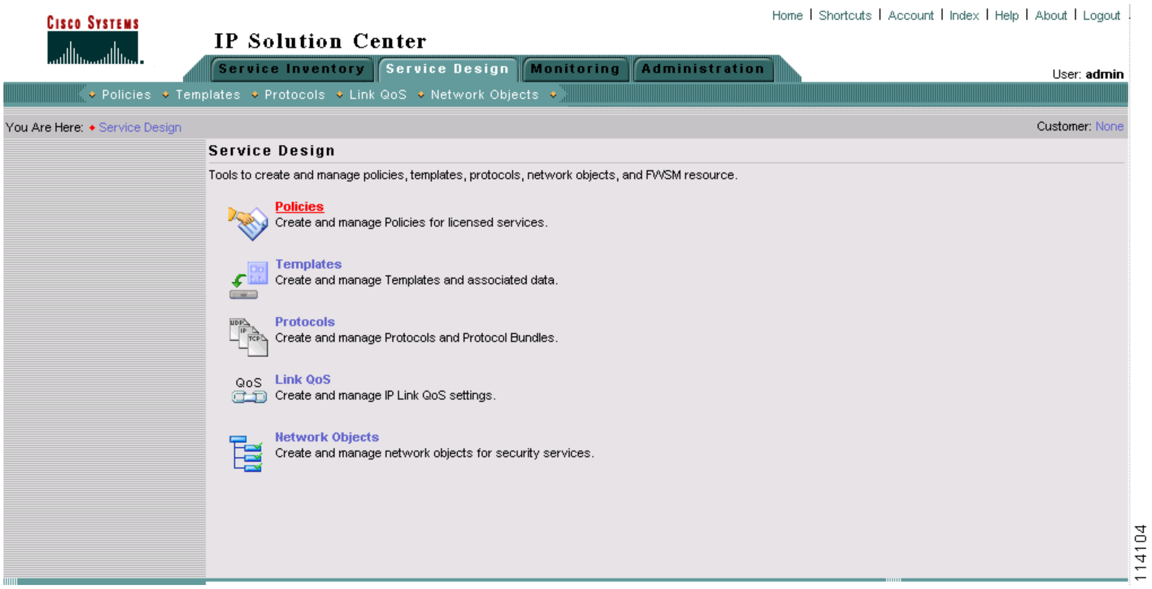
Select the service classes to use in the QoS policy and edit each one with the required parameters. All service classes require that you enter at least the bandwidth. You can also delete an unused service class, change the order of the service classes, or add another data service class, if needed.

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 the Chapter 6, "IP QoS Policy Parameters".

To create an IP QoS policy:

**Step 1** On the Service Design tab, click **Policy Manager** (see Figure 5-10).

***Figure 5-10 Policy Manager***



Service Design

Tools to create and manage policies, templates, protocols, network objects, and FWSM resource.

Policies
Create and manage Policies for licensed services.

Templates
Create and manage Templates and associated data.

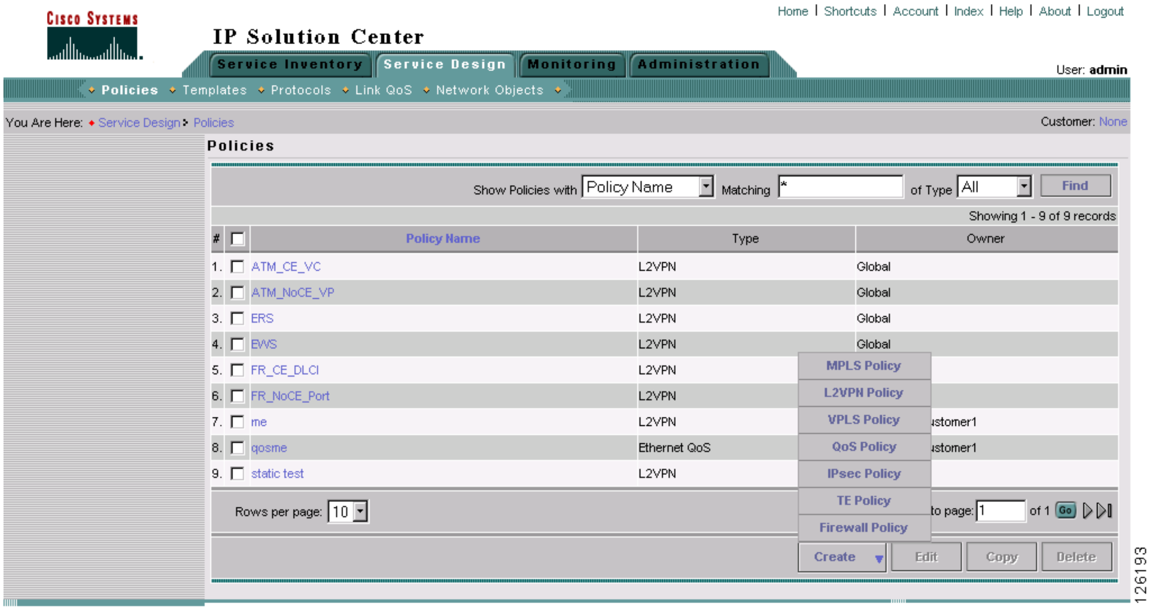
Protocols
Create and manage Protocols and Protocol Bundles.

Link QoS
Create and manage IP Link QoS settings.

Network Objects
Create and manage network objects for security services.

The Policies window appears (Figure 5-11).

*Figure 5-11* *Create QoS Policy*



You Are Here: ◆ Service Design ▸ Policies

Customer: None

Policies

Show Policies with Policy Name Matching * of Type All

Showing 1 - 9 of 9 records

| # | □ | Policy Name | Type | Owner |
|---|---|---|---|---|
| 1. | □ | ATM_CE_VC | L2VPN | Global |
| 2. | □ | ATM_NoCE_VP | L2VPN | Global |
| 3. | □ | ERS | L2VPN | Global |
| 4. | □ | EWS | L2VPN | Global |
| 5. | □ | FR_CE_DLCI | L2VPN | |
| 6. | □ | FR_NoCE_Port | L2VPN | |
| 7. | □ | me | L2VPN | ustomer1 |
| 8. | □ | qosme | Ethernet QoS | ustomer1 |
| 9. | □ | static test | L2VPN | |

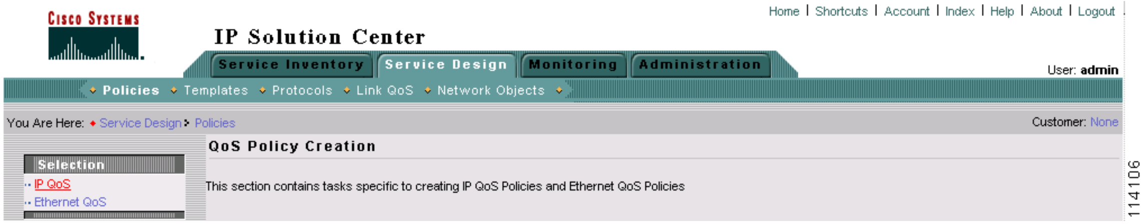
Rows per page: 10

to page: 1 of 1

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 2** Click **Create** and select **QoS Policy** from the menu. The Qos Policy Creation window appears (see Figure 5-12).

*Figure 5-12* *Create QoS Policy*



You Are Here: ◆ Service Design ▸ Policies

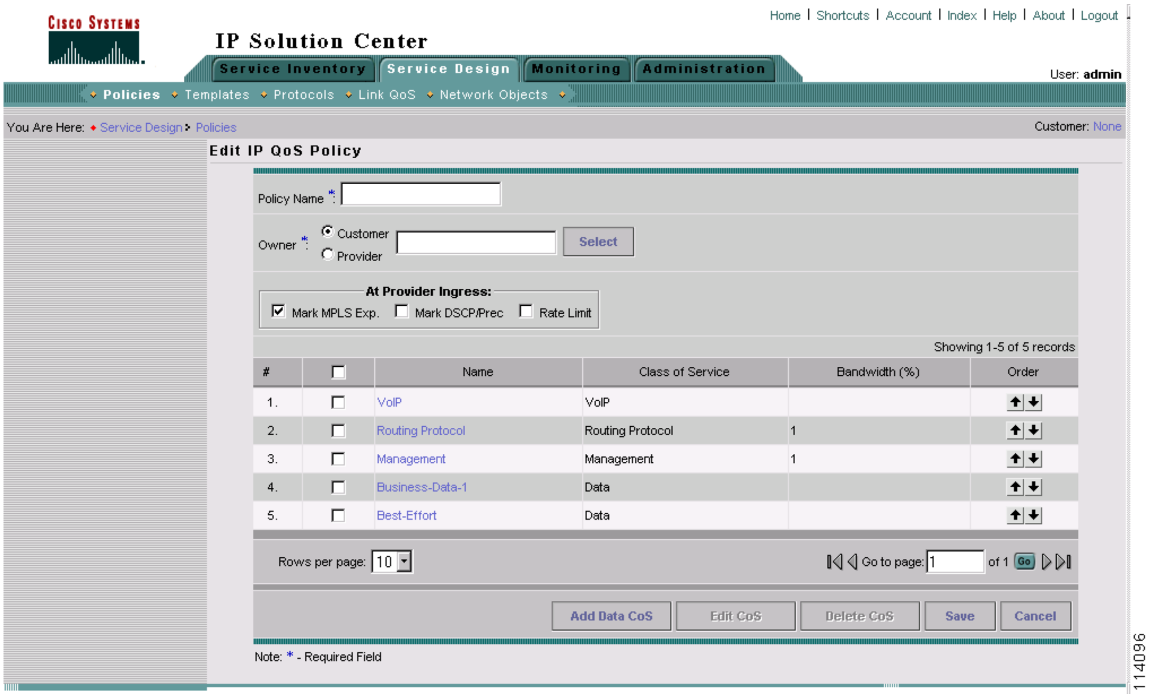
Customer: None

QoS Policy Creation

This section contains tasks specific to creating IP QoS Policies and Ethernet QoS Policies

**Step 3** Select **IP QoS** from the TOC at left. The Edit IP QoS Policy window (Figure 5-13) appears.

*Figure 5-13 Edit IP QoS Policy*



Edit IP QoS Policy

Policy Name *:

Owner *: ● Customer ○ Provider

At Provider Ingress:

☑ Mark MPLS Exp. □ Mark DSCP/Prec □ Rate Limit

Showing 1-5 of 5 records

| # | □ | Name | Class of Service | Bandwidth (%) | Order |
|---|---|---|---|---|---|
| 1. | □ | VoIP | VoIP | | ↑↓ |
| 2. | □ | Routing Protocol | Routing Protocol | 1 | ↑↓ |
| 3. | □ | Management | Management | 1 | ↑↓ |
| 4. | □ | Business-Data-1 | Data | | ↑↓ |
| 5. | □ | Best-Effort | Data | | ↑↓ |

Rows per page: 10

Go to page: 1 of 1 Go

Note: * - Required Field

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.**—Use this parameter when provisioning QoS for a PE device that is in an MPLS network.
- **Mark DSCP/Prec**—Use this parameter to mark traffic based on the IP DSCP or precedence value.
- **Rate Limit**—Enable this parameter if the CPE is an untrusted device. An untrusted CPE is a device that is either not managed by ISC or only partially-managed by ISC.

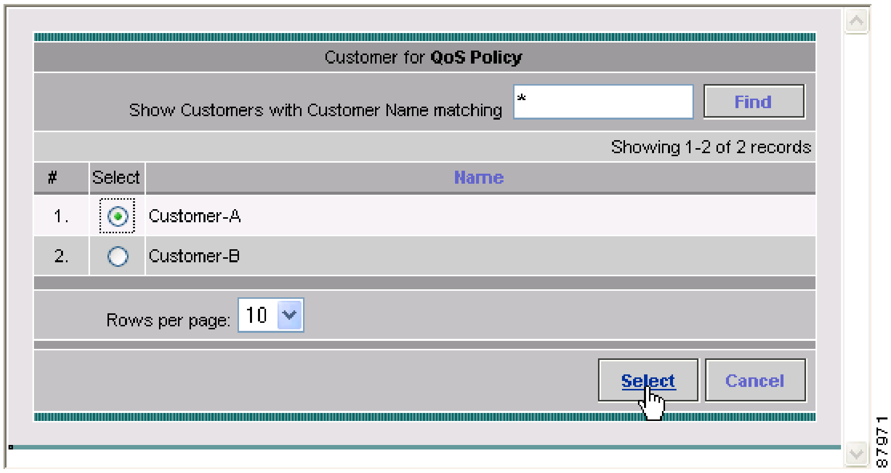
**Step 4** In the Edit IP QoS Policy window, enter the **Policy Name**. Select a policy name that is easily identified for your network. For example, if your customer is CustomerA, the policy name might be A-QoS.

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

**Step 6** In the Customer (or Provider) for QoS Policy popup, select the customer (provider) and click **Select** (Figure 5-14).

*Figure 5-14 Select Customer for QoS Policy*



Customer for **QoS Policy**

Show Customers with Customer Name matching [*] Find

Showing 1-2 of 2 records

| # | Select | Name |
|---|---|---|
| 1. | ● | Customer-A |
| 2. | ○ | Customer-B |

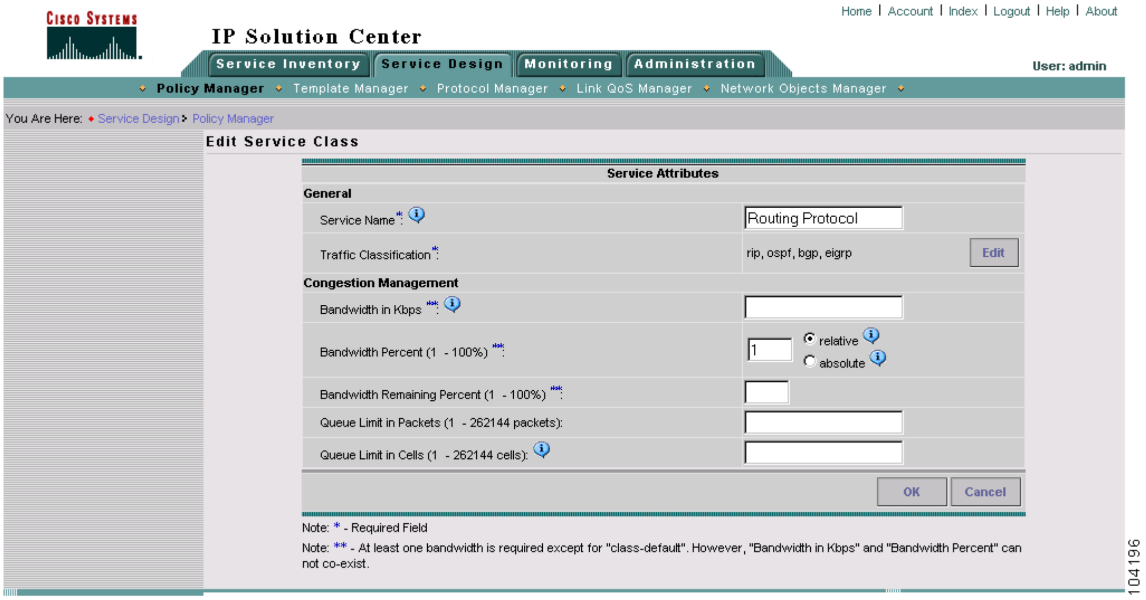
Rows per page: 10

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 7** 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 5-15).

*Figure 5-15 Edit Service Class—Routing Protocol*



Edit Service Class

Service Attributes

**General**

| | |
|---|---|
| Service Name*: | Routing Protocol |
| Traffic Classification*: | rip, ospf, bgp, eigrp |

**Congestion Management**

| | |
|---|---|
| Bandwidth in Kbps **: | |
| Bandwidth Percent (1 - 100%) **: | 1 ● relative ○ absolute |
| Bandwidth Remaining Percent (1 - 100%) **: | |
| Queue Limit in Packets (1 - 262144 packets): | |
| Queue Limit in Cells (1 - 262144 cells): | |

Note: * - Required Field
Note: ** - At least one bandwidth is required except for "class-default". However, "Bandwidth in Kbps" and "Bandwidth Percent" can not co-exist.

**Step 8** 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 6-1.

**Step 9** 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 10** Add another service class, if required. See Adding a Data Service Class, page 6-21.

**Step 11** Delete any service classes that you do not require for this QoS Policy. See Deleting a Service Class, page 6-21.

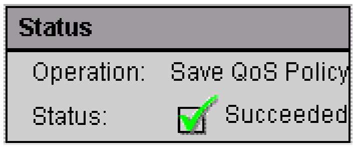
**Step 12** After you edit and apply the required service classes, click **Save** to save the Qos Policy.

**Note** You must specify a bandwidth for each service class before you can 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 5-16).

***Figure 5-16 Save is Successful***



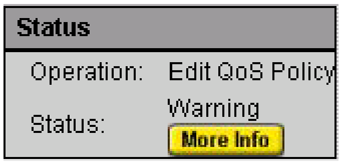
Status

Operation: Save QoS Policy

Status: ✓ Succeeded

b. Policy is in use and cannot be edited (Figure 5-17). To read the warning message, click **More Info** and take the necessary action to resolve the issue.

***Figure 5-17 Edit QoS Policy with Warning***



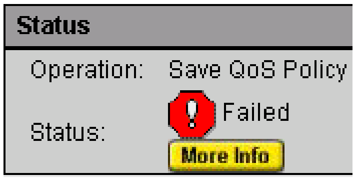
Status

Operation: Edit QoS Policy

Status: Warning

c. Save QoS policy failed (Figure 5-18). Click **More Info** to determine the source of the problem. You must fix all errors and resave before you can continue.

*Figure 5-18 Save Unsuccessful*



Status

Operation: Save QoS Policy

Status: Failed

**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.

# Defining the Link Level QoS Policy

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 CPE-PE link QoS parameters to use.

The link QoS setting is a group of QoS parameters that are sensitive to link bandwidth and the CPE-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 CPE-PE link in the QoS service request, you can have one corresponding link QoS setting.

## Link QoS Manager

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

Create the link QoS setting using the Link QoS Manager operation area of the ISC GUI. The Link QoS Manager 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).

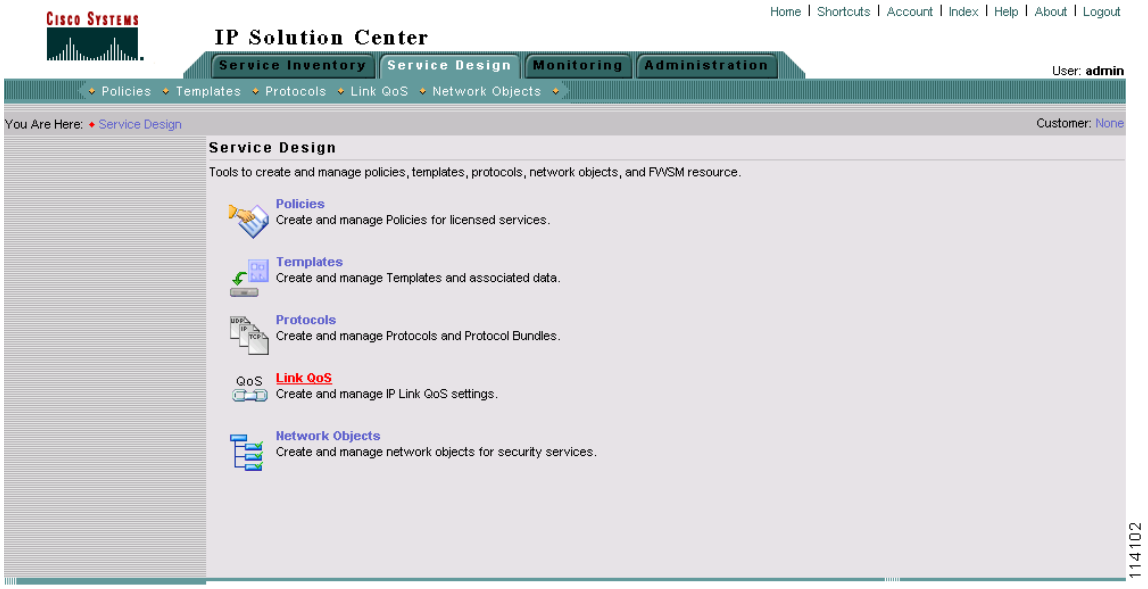
## Creating the Link QoS Setting

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

To create the link QoS setting:

**Step 1** On the Service Design tab, click **Link QoS Manager** (Figure 5-19).

*Figure 5-19* *Link QoS Manager*



Service Design

Tools to create and manage policies, templates, protocols, network objects, and FWSM resource.

Policies
Create and manage Policies for licensed services.

Templates
Create and manage Templates and associated data.

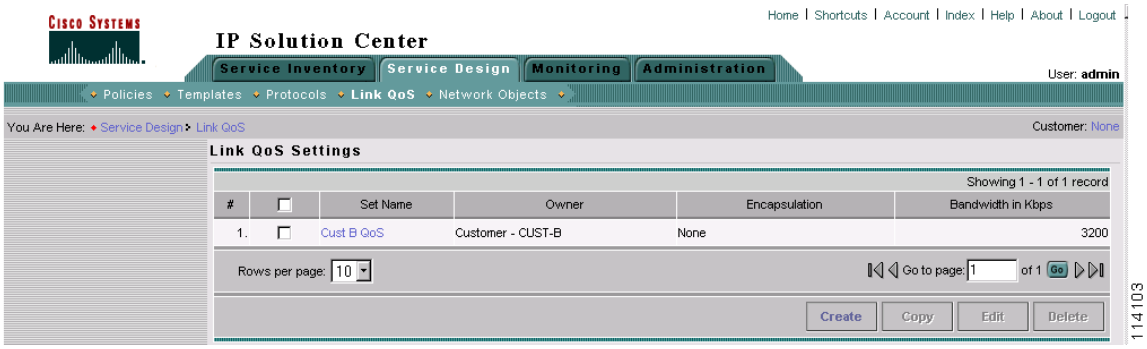
Protocols
Create and manage Protocols and Protocol Bundles.

Link QoS
Create and manage IP Link QoS settings.

Network Objects
Create and manage network objects for security services.

**Step 2** The Link QoS Settings window appears (Figure 5-20).

*Figure 5-20* *Link QoS Settings*



Link QoS Settings

Showing 1 - 1 of 1 record

| # | □ | Set Name | Owner | Encapsulation | Bandwidth in Kbps |
|---|---|---|---|---|---|
| 1. | □ | Cust B QoS | Customer - CUST-B | None | 3200 |

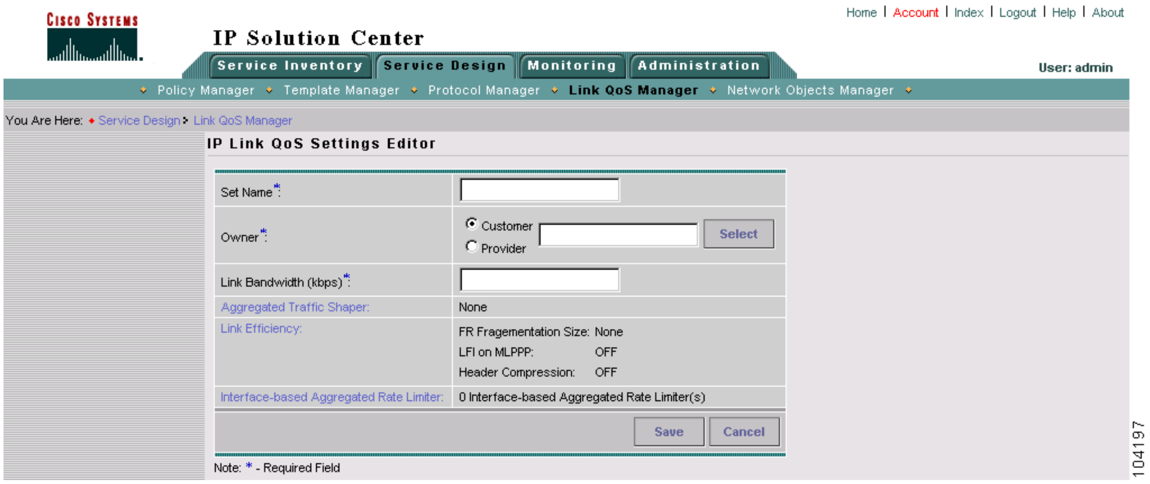
**Step 3** The Link QoS Settings window displays the current link QoS settings available for QoS service requests, including the following information about each link QoS setting:

- Set Name—The name of your link QoS setting
- Owner—Customer or provider
- Type—IP Link Setting
- Encapsulation—Layer 2 encapsulation type.
- Bandwidth—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**. The IP Link QoS Settings Editor window appears (Figure 5-21).

*Figure 5-21 IP Link QoS Settings Editor*



IP Link QoS Settings Editor

| | |
|---|---|
| Set Name*: | |
| Owner*: | ● Customer<br>○ Provider |
| Link Bandwidth (kbps)*: | |
| Aggregated Traffic Shaper: | None |
| Link Efficiency: | FR Fragementation Size: None<br>LFI on MLPPP: OFF<br>Header Compression: OFF |
| Interface-based Aggregated Rate Limiter: | 0 Interface-based Aggregated Rate Limiter(s) |

Note: * - Required Field

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

*Table 5-1 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 CPE-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 6-22. |
| Link Efficiency | Click **Link Efficiency** to set these parameters. For more information on the link efficiency parameters, see Link Efficiency Settings, page 6-30. |
| Interface-based Aggregated Rate Limiter | This provides rate limiting for the traffic on a particular interface for the CPE-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 6-31. |

**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 CPE-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 the QoS Service Request

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 (CPE-PE link) or just one interface (CPE 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

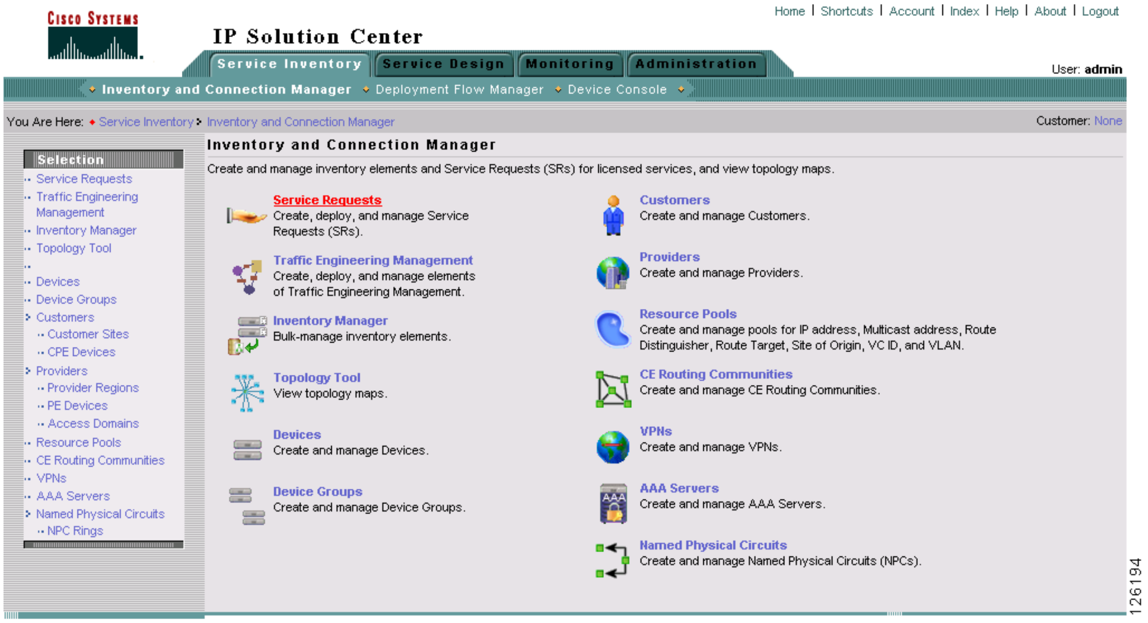
To apply QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

This section describes how to create a QoS service request, independent of VPN services. To create a QoS service request for MPLS, L2VPN, or VPLS services, see Chapter 7, “Applying QoS Policies to VPN Services”.

To create an IP QoS service request:

**Step 1** Select **Service Inventory > Inventory and Connection Manager > Service Request** (Figure 5-22).

***Figure 5-22 Service Requests***



Inventory and Connection Manager

Create and manage inventory elements and Service Requests (SRs) for licensed services, and view topology maps.

**Service Requests**
Create, deploy, and manage Service Requests (SRs).

**Traffic Engineering Management**
Create, deploy, and manage elements of Traffic Engineering Management.

**Inventory Manager**
Bulk-manage inventory elements.

**Topology Tool**
View topology maps.

**Devices**
Create and manage Devices.

**Device Groups**
Create and manage Device Groups.

**Customers**
Create and manage Customers.

**Providers**
Create and manage Providers.

**Resource Pools**
Create and manage pools for IP address, Multicast address, Route Distinguisher, Route Target, Site of Origin, VC ID, and VLAN.

**CE Routing Communities**
Create and manage CE Routing Communities.

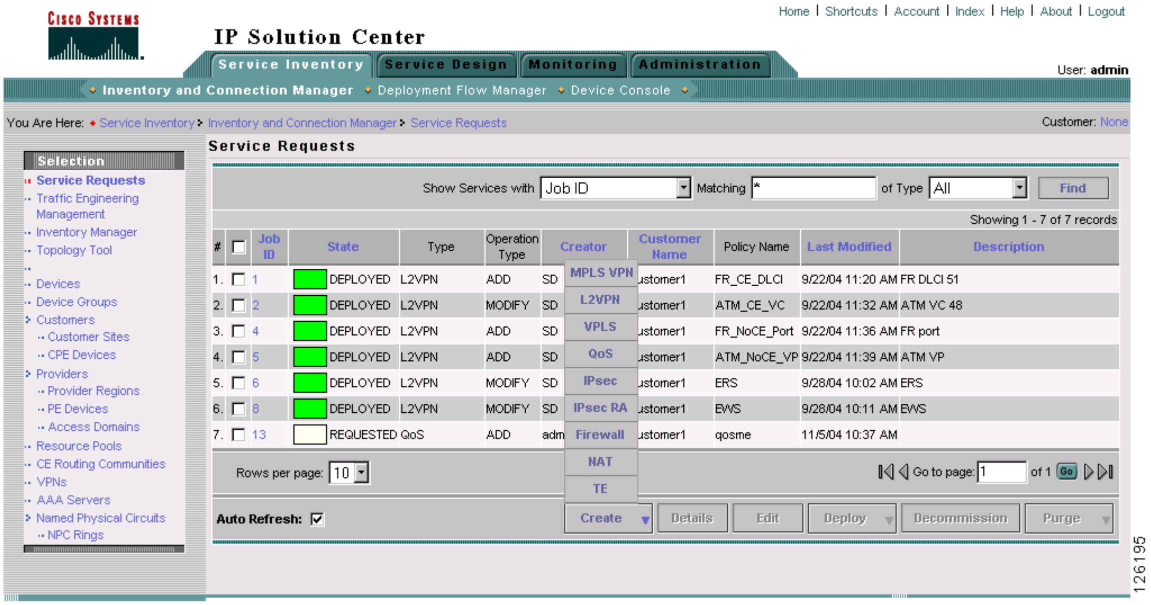
**VPNs**
Create and manage VPNs.

**AAA Servers**
Create and manage AAA Servers.

**Named Physical Circuits**
Create and manage Named Physical Circuits (NPCs).

The Service Request window appears. (Figure 5-23).

*Figure 5-23 Service Requests List*



Service Requests

Show Services with: Job ID Matching: * of Type: All

Showing 1 - 7 of 7 records

| # | ☐ | Job ID | State | Type | Operation Type | Creator | Customer Name | Policy Name | Last Modified | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | ☐ | 1 | 🟩 DEPLOYED | L2VPN | ADD | SD | ustomer1 | FR_CE_DLCI | 9/22/04 11:20 AM | FR DLCI 51 |
| 2. | ☐ | 2 | 🟩 DEPLOYED | L2VPN | MODIFY | SD | ustomer1 | ATM_CE_VC | 9/22/04 11:32 AM | ATM VC 48 |
| 3. | ☐ | 4 | 🟩 DEPLOYED | L2VPN | ADD | SD | ustomer1 | FR_NoCE_Port | 9/22/04 11:36 AM | FR port |
| 4. | ☐ | 5 | 🟩 DEPLOYED | L2VPN | ADD | SD | ustomer1 | ATM_NoCE_VP | 9/22/04 11:39 AM | ATM VP |
| 5. | ☐ | 6 | 🟩 DEPLOYED | L2VPN | MODIFY | SD | ustomer1 | ERS | 9/28/04 10:02 AM | ERS |
| 6. | ☐ | 8 | 🟩 DEPLOYED | L2VPN | MODIFY | SD | ustomer1 | EWS | 9/28/04 10:11 AM | EWS |
| 7. | ☐ | 13 | ☐ REQUESTED | QoS | ADD | adm | ustomer1 | qosme | 11/5/04 10:37 AM | |

Rows per page: 10 Go to page: 1 of 1

Auto Refresh: ☑

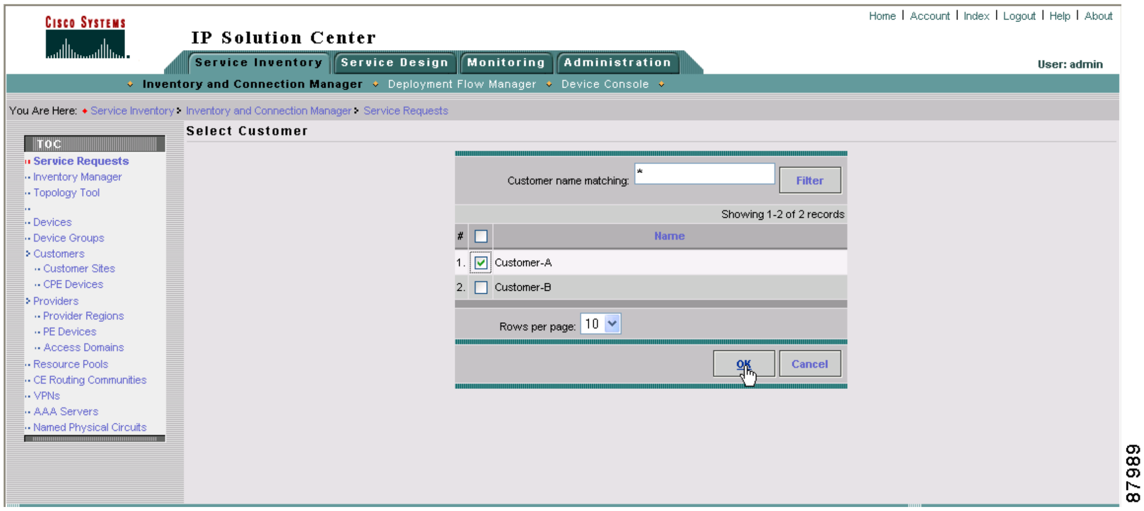
The Service Requests window lists the current service requests.

**Note** For more information on service requests, see QoS Service Requests, page 8-3.

**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 5-24).

*Figure 5-24 Select Customer*



Select Customer

Customer name matching: *

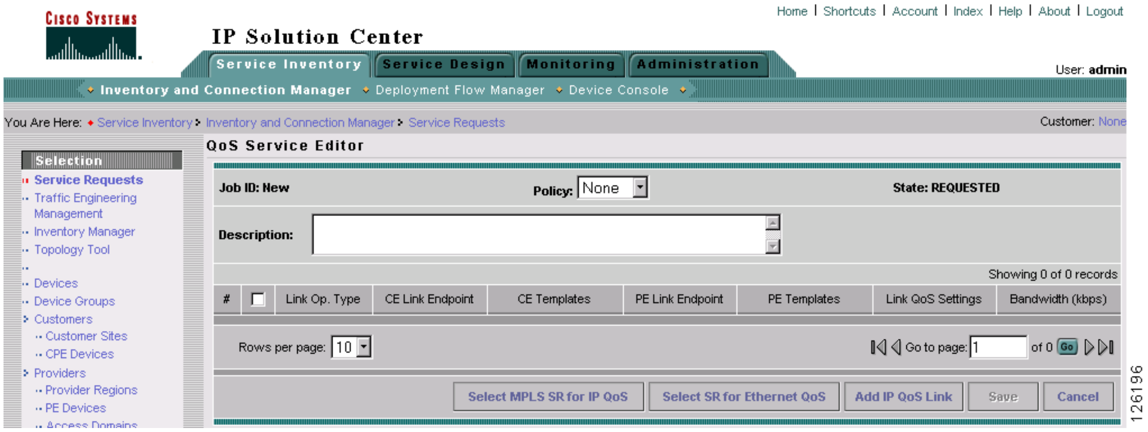
Showing 1-2 of 2 records

| # | ☐ | Name |
|---|---|---|
| 1. | ☑ | Customer-A |
| 2. | ☐ | Customer-B |

Rows per page: 10

The QoS Service Editor window appears (Figure 5-25).

*Figure 5-25 QoS Service Editor*



QoS Service Editor

Job ID: New Policy: None State: REQUESTED

Description:

Showing 0 of 0 records

| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|

Rows per page: 10 Go to page: 1 of 0

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

- Link Op. Type—The link operation type for this CPE-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, 4.0* 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, 4.0* for information on creating templates.
- Link QoS Settings—Previously configured link QoS setting to use for this CPE-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 CPE-PE links, or to select MPLS service requests for IP QoS provisioning. You can also select link QoS settings for the CPE-PE links from this window.

**Note** If you are provisioning QoS for an MPLS, L2VPN, or VPLS service request, see Chapter 7, "Applying QoS Policies to VPN Services.".

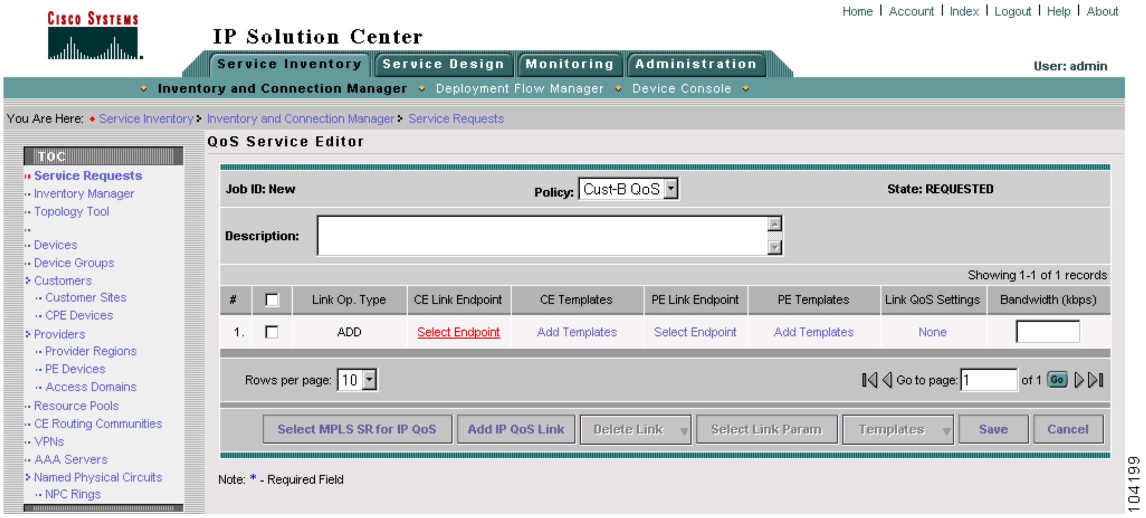
If you add CE and PE link endpoints, you get a CPE-PE QoS link. If you select link QoS settings for the CPE-PE link, you get link level QoS policy. Typically, a QoS service request has both a service level policy and link level QoS settings.

**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 5-26).

*Figure 5-26 Select Link Endpoints*



QoS Service Editor

Job ID: New　Policy: Cust-B QoS　State: REQUESTED

Description:

Showing 1-1 of 1 records

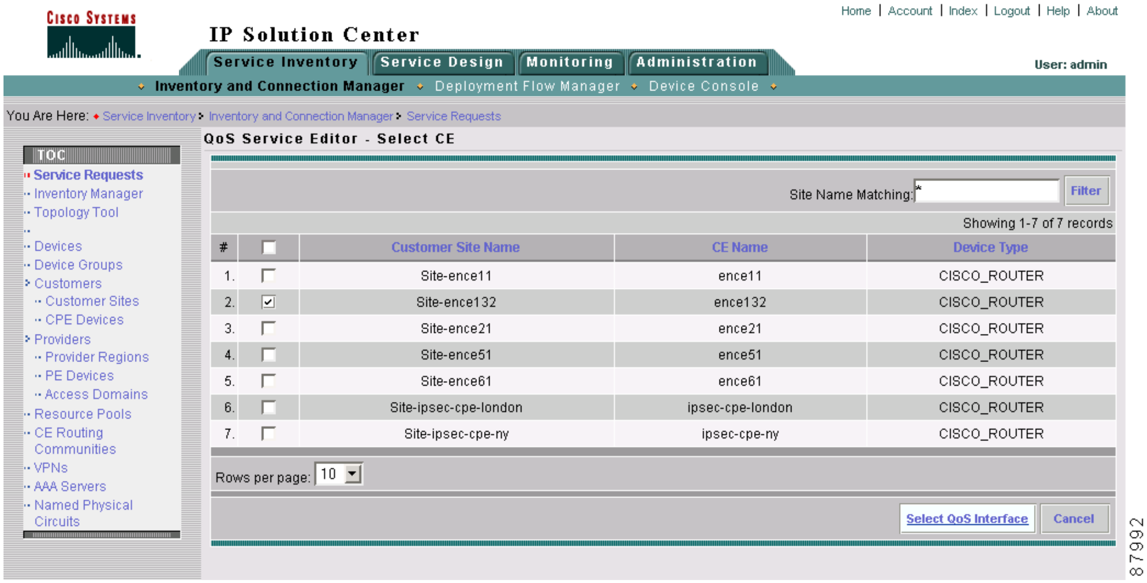
| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|
| 1. | □ | ADD | Select Endpoint | Add Templates | Select Endpoint | Add Templates | None | |

Rows per page: 10　Go to page: 1 of 1 Go

Note: * - Required Field

**Step 6** Click **Select Endpoint** in the CE Link Endpoint field. The QoS Service Editor - Select CE window appears (Figure 5-27).

*Figure 5-27 Select CE*



QoS Service Editor - Select CE

Site Name Matching: *

Showing 1-7 of 7 records

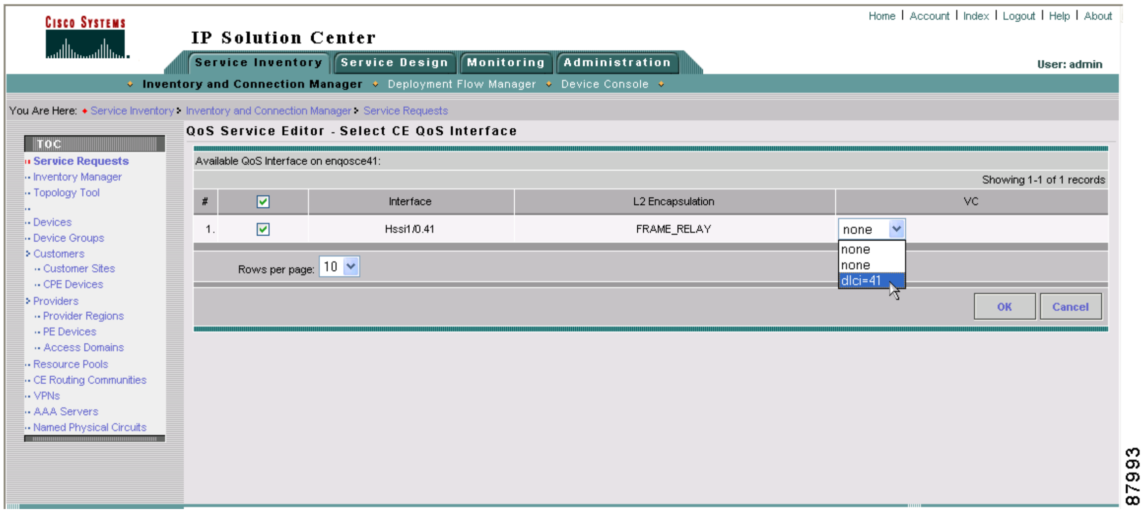
| # | □ | Customer Site Name | CE Name | Device Type |
|---|---|---|---|---|
| 1. | □ | Site-ence11 | ence11 | CISCO_ROUTER |
| 2. | ☑ | Site-ence132 | ence132 | CISCO_ROUTER |
| 3. | □ | Site-ence21 | ence21 | CISCO_ROUTER |
| 4. | □ | Site-ence51 | ence51 | CISCO_ROUTER |
| 5. | □ | Site-ence61 | ence61 | CISCO_ROUTER |
| 6. | □ | Site-ipsec-cpe-london | ipsec-cpe-london | CISCO_ROUTER |
| 7. | □ | Site-ipsec-cpe-ny | ipsec-cpe-ny | CISCO_ROUTER |

Rows per page: 10

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 enqosce41.The QoS Service Editor - Select CE QoS Interface window appears (Figure 5-28).

*Figure 5-28 Select CE QoS Interface*



QoS Service Editor - Select CE QoS Interface

Available QoS Interface on enqosce41:

Showing 1-1 of 1 records

| # | ☑ | Interface | L2 Encapsulation | VC |
|---|---|---|---|---|
| 1. | ☑ | Hssi1/0.41 | FRAME_RELAY | none |

Rows per page: 10

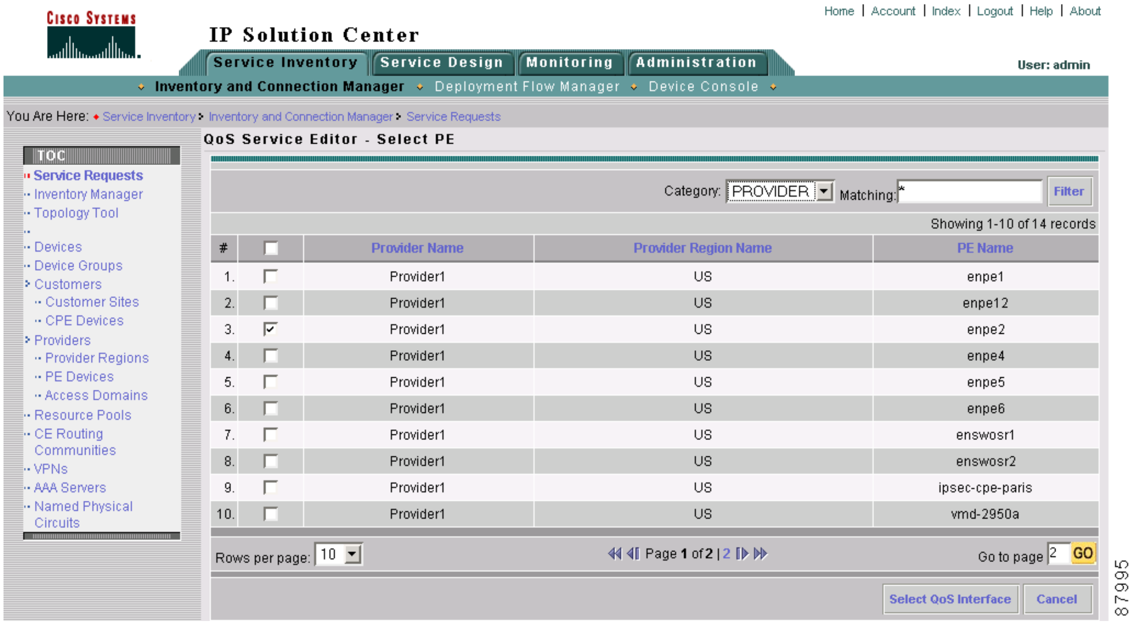
This window lists the CPE device interfaces identified during the Selecting CPE Device Interfaces for QoS operation, and includes the following information about the CPE device interfaces:

- Interface name—The name of the CPE 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 4-3
- 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 HSSI 1/0.41 with VC dlci41. 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 5-29).

*Figure 5-29 Select PE*



QoS Service Editor - Select PE

Category: PROVIDER Matching: *

Showing 1-10 of 14 records

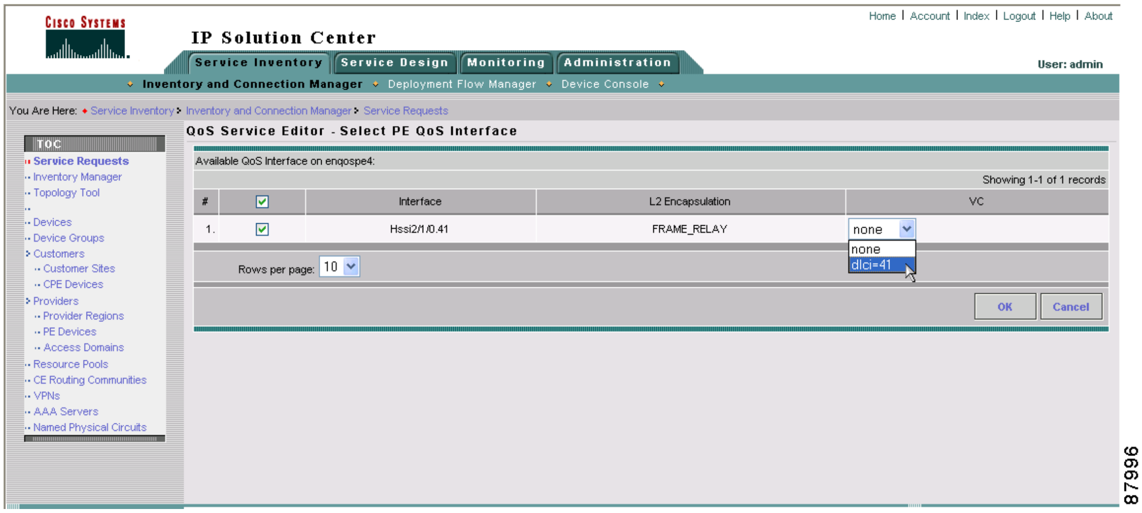
| # | □ | Provider Name | Provider Region Name | PE Name |
|---|---|---|---|---|
| 1. | □ | Provider1 | US | enpe1 |
| 2. | □ | Provider1 | US | enpe12 |
| 3. | ☑ | Provider1 | US | enpe2 |
| 4. | □ | Provider1 | US | enpe4 |
| 5. | □ | Provider1 | US | enpe5 |
| 6. | □ | Provider1 | US | enpe6 |
| 7. | □ | Provider1 | US | enswosr1 |
| 8. | □ | Provider1 | US | enswosr2 |
| 9. | □ | Provider1 | US | ipsec-cpe-paris |
| 10. | □ | Provider1 | US | vmd-2950a |

Rows per page: 10 Page 1 of 2 | 2 Go to page 2

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 enqospe4. The QoS Service Editor - Select PE QoS Interface window appears (Figure 5-30).

*Figure 5-30 Select PE QoS Interface*



QoS Service Editor - Select PE QoS Interface

Available QoS Interface on enqospe4:

Showing 1-1 of 1 records

| # | ☑ | Interface | L2 Encapsulation | VC |
|---|---|---|---|---|
| 1. | ☑ | Hssi2/1/0.41 | FRAME_RELAY | none |

Rows per page: 10

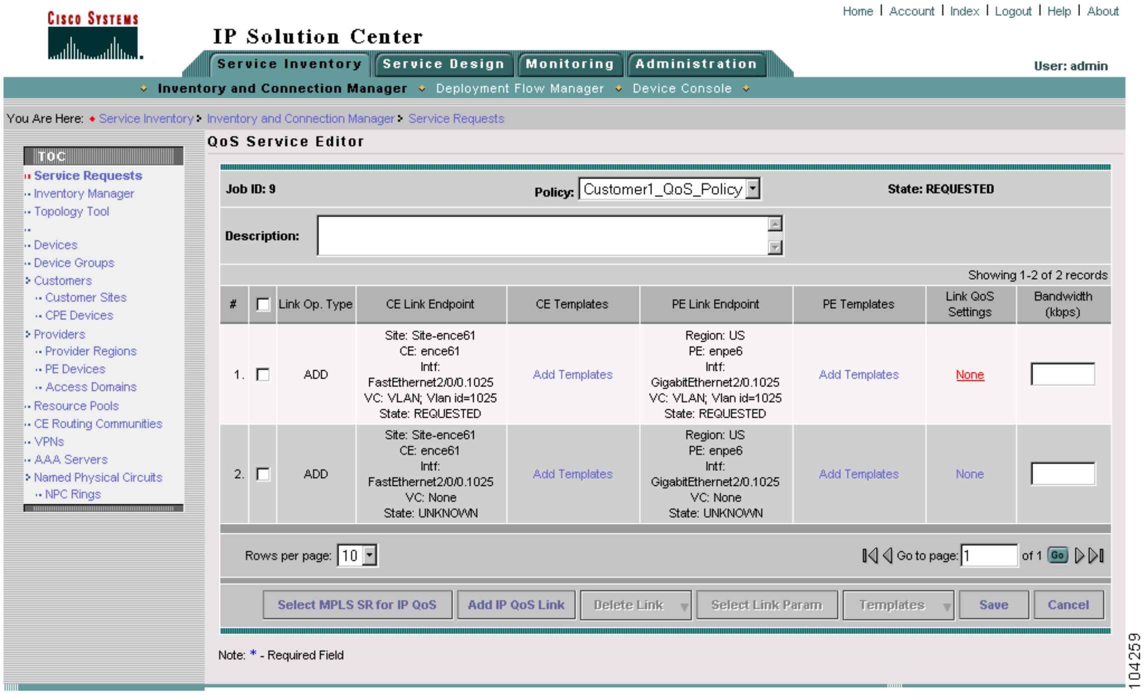
This window lists the PE device interfaces identified during the Selecting PE Device Interfaces for QoS operation, and includes the following information about the PE device interfaces:

- 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 4-3.
- 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 HSSI 2/1/0.41 with VC dlci41. You return to the QoS Service Editor window (Figure 5-31).

*Figure 5-31 QoS Service Editor*



QoS Service Editor

Job ID: 9 Policy: Customer1_QoS_Policy State: REQUESTED

Description:

Showing 1-2 of 2 records

| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|
| 1. | □ | ADD | Site: Site-ence61<br>CE: ence61<br>Intf: FastEthernet2/0/0.1025<br>VC: VLAN; Vlan id=1025<br>State: REQUESTED | Add Templates | Region: US<br>PE: enpe6<br>Intf: GigabitEthernet2/0.1025<br>VC: VLAN; Vlan id=1025<br>State: REQUESTED | Add Templates | None | |
| 2. | □ | ADD | Site: Site-ence61<br>CE: ence61<br>Intf: FastEthernet2/0/0.1025<br>VC: None<br>State: UNKNOWN | Add Templates | Region: US<br>PE: enpe6<br>Intf: GigabitEthernet2/0.1025<br>VC: None<br>State: UNKNOWN | Add Templates | None | |

Rows per page: 10 Go to page: 1 of 1 Go

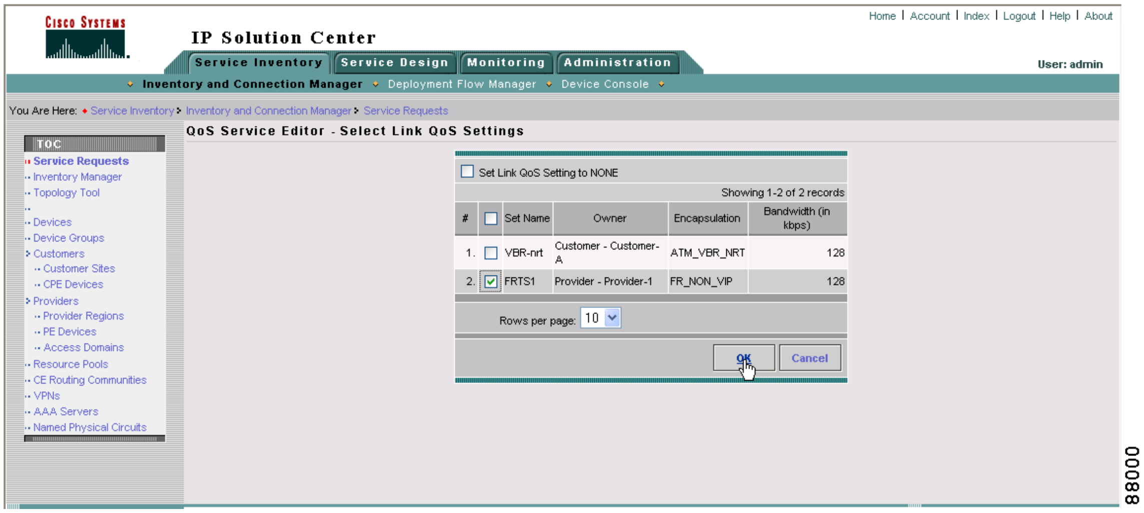
Note: * - Required Field

The interface information for the PE link endpoint is listed.

**Step 12** Repeat Steps 1-11 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 Param**. The Select Link QoS Settings window appears (Figure 5-32).

*Figure 5-32 Select Link QoS Settings*



You Are Here: • Service Inventory > Inventory and Connection Manager > Service Requests

QoS Service Editor - Select Link QoS Settings

□ Set Link QoS Setting to NONE

Showing 1-2 of 2 records

| # | □ | Set Name | Owner | Encapsulation | Bandwidth (in kbps) |
|---|---|---|---|---|---|
| 1. | □ | VBR-nrt | Customer - Customer-A | ATM_VBR_NRT | 128 |
| 2. | ☑ | FRTS1 | Provider - Provider-1 | FR_NON_VIP | 128 |

Rows per page: 10

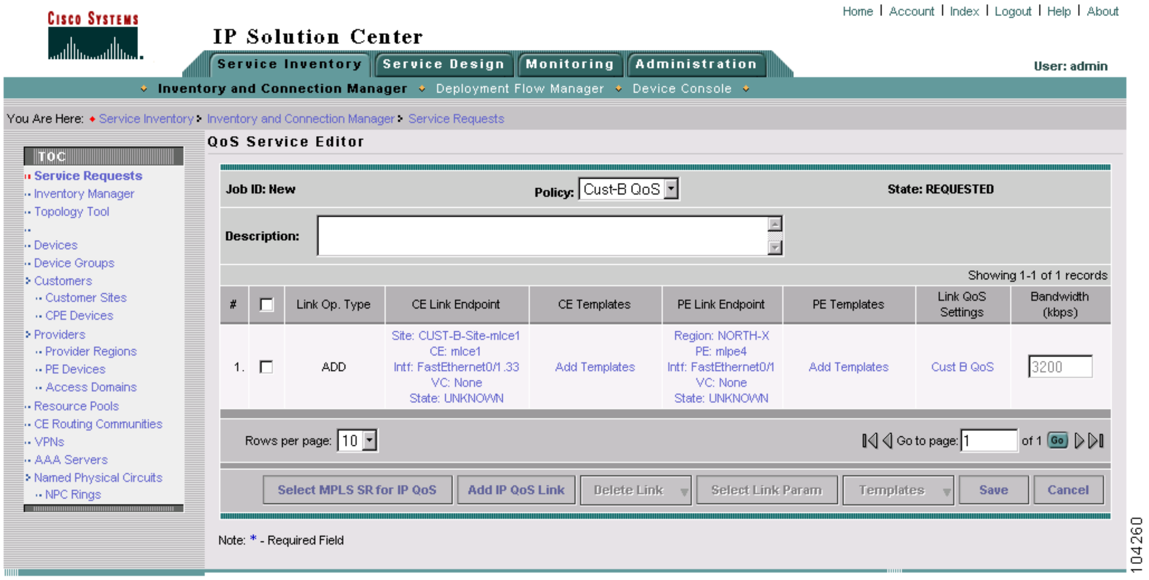
This window lists all set names (link QoS settings) created during the Defining the Link Level QoS Policy operation.

**Step 14** Select the link QoS setting (set name) to apply to this CPE-PE link. For example, select FRTS1, and click **OK**.

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

**Step 15** Save the QoS service request by clicking **Save** (Figure 5-33).

*Figure 5-33 Save QoS Service Request*



You Are Here: • Service Inventory > Inventory and Connection Manager > Service Requests

QoS Service Editor

Job ID: New Policy: Cust-B QoS State: REQUESTED

Description:

Showing 1-1 of 1 records

| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|
| 1. | □ | ADD | Site: CUST-B-Site-mlce1<br>CE: mlce1<br>Intf: FastEthernet0/1.33<br>VC: None<br>State: UNKNOWN | Add Templates | Region: NORTH-X<br>PE: mlpe4<br>Intf: FastEthernet0/1<br>VC: None<br>State: UNKNOWN | Add Templates | Cust B QoS | 3200 |

Rows per page: 10 Go to page: 1 of 1

Note: * - Required Field

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, 4.0*.

# Deploying the QoS Service Request

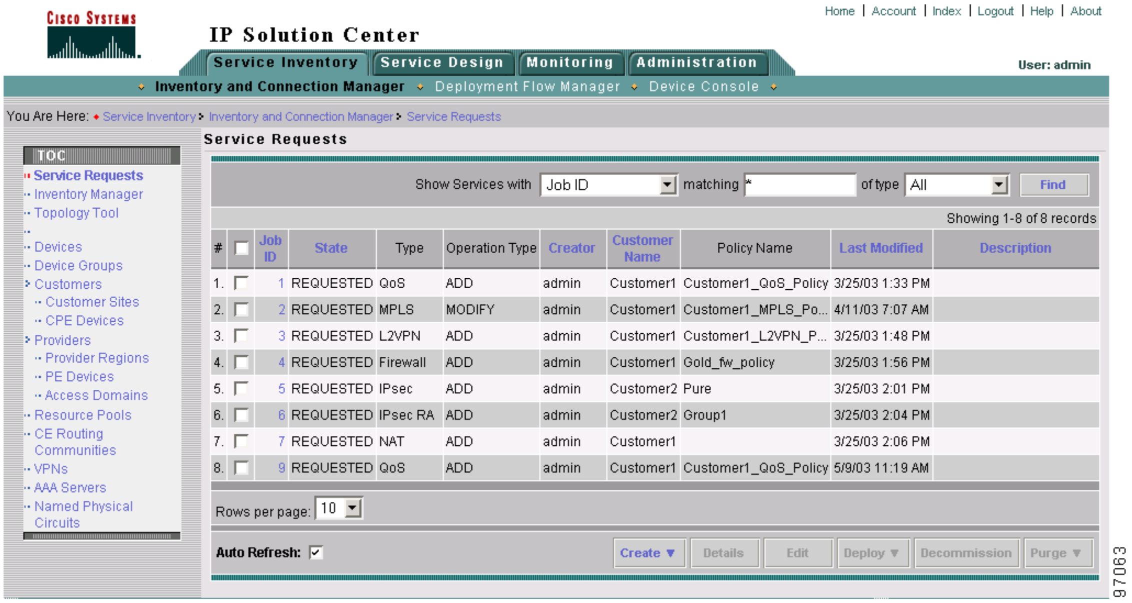
To apply QoS policies to network devices, you must deploy the QoS service request. When you deploy a QoS service request, ISC generates a configlet to download to each device.

When the configlets are generated, the QoS service request enters the *Pending* state. When the configlets are downloaded 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 5-34).

***Figure 5-34 Deploy QoS Service Request***



Service Requests

Show Services with Job ID matching * of type All Find

Showing 1-8 of 8 records

| # | □ | Job ID | State | Type | Operation Type | Creator | Customer Name | Policy Name | Last Modified | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | □ | 1 | REQUESTED | QoS | ADD | admin | Customer1 | Customer1_QoS_Policy | 3/25/03 1:33 PM | |
| 2. | □ | 2 | REQUESTED | MPLS | MODIFY | admin | Customer1 | Customer1_MPLS_Po... | 4/11/03 7:07 AM | |
| 3. | □ | 3 | REQUESTED | L2VPN | ADD | admin | Customer1 | Customer1_L2VPN_P... | 3/25/03 1:48 PM | |
| 4. | □ | 4 | REQUESTED | Firewall | ADD | admin | Customer1 | Gold_fw_policy | 3/25/03 1:56 PM | |
| 5. | □ | 5 | REQUESTED | IPsec | ADD | admin | Customer2 | Pure | 3/25/03 2:01 PM | |
| 6. | □ | 6 | REQUESTED | IPsec RA | ADD | admin | Customer2 | Group1 | 3/25/03 2:04 PM | |
| 7. | □ | 7 | REQUESTED | NAT | ADD | admin | Customer1 | | 3/25/03 2:06 PM | |
| 8. | □ | 9 | REQUESTED | QoS | ADD | admin | Customer1 | Customer1_QoS_Policy | 5/9/03 11:19 AM | |

Rows per page: 10

Auto Refresh: ☑

Create ▼ Details Edit Deploy ▼ Decommission Purge ▼

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 Request 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 Request window.

**Note** For more information on QoS service requests, see QoS Service Requests, page 8-3.

# IP QoS Policy Parameters

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

This chapter contains the following sections and subsections:

**Note** For information on service level Ethernet QoS parameters, see Service Level Ethernet QoS Policy Entry Fields, page 7-8.

## 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*.

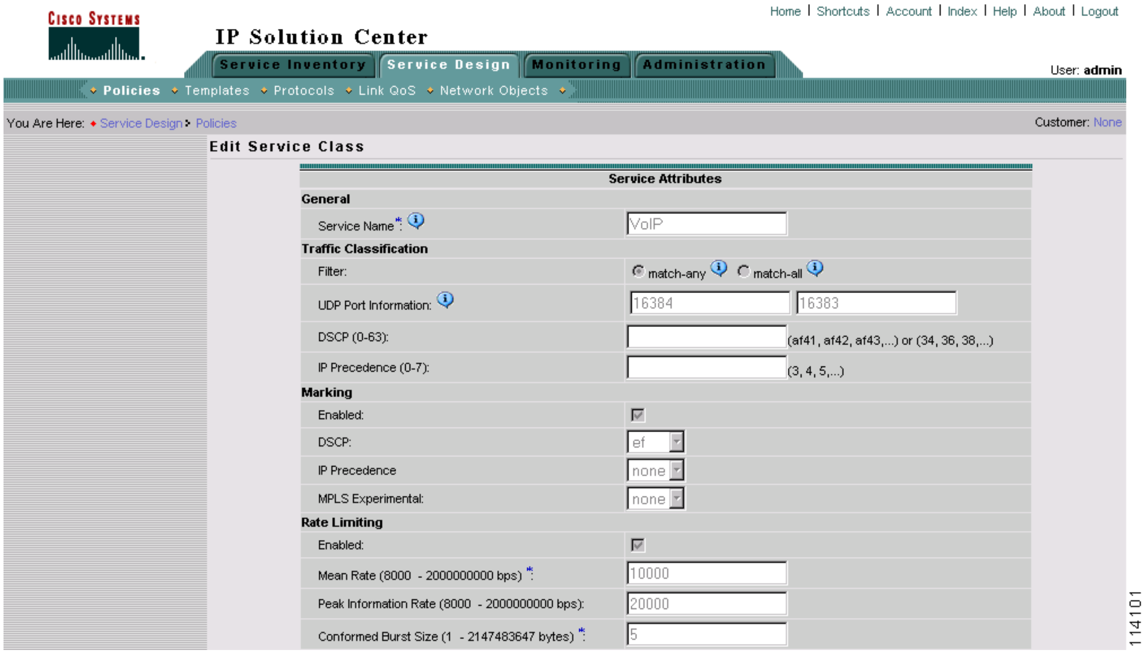
**Note** *Class-default* is a reserved class of service name in IOS and is created by IOS if ISC does not create one.

# 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 6-1 and Figure 6-2 display these service classes.

For Business-Data-1 and Best Effort service class entry fields, see Business-Data-1 and Best Effort Service Classes, page 6-11. The window you see depends on the service class being edited.

***Figure 6-1 Edit VoIP Service Class***

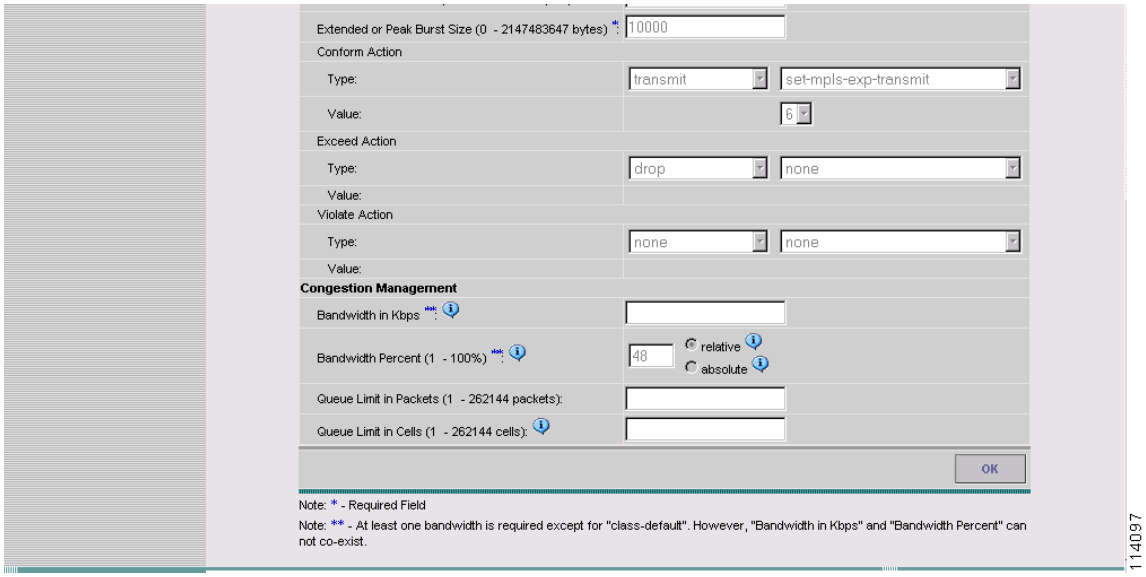


Edit Service Class

Service Attributes

| | |
|---|---|
| **General** | |
| Service Name*: | VoIP |
| **Traffic Classification** | |
| Filter: | ● match-any ○ match-all |
| UDP Port Information: | 16384 16383 |
| DSCP (0-63): | (af41, af42, af43,...) or (34, 36, 38,...) |
| IP Precedence (0-7): | (3, 4, 5,...) |
| **Marking** | |
| Enabled: | ☑ |
| DSCP: | ef |
| IP Precedence | none |
| MPLS Experimental: | none |
| **Rate Limiting** | |
| Enabled: | ☑ |
| Mean Rate (8000 - 2000000000 bps)*: | 10000 |
| Peak Information Rate (8000 - 2000000000 bps): | 20000 |
| Conformed Burst Size (1 - 2147483647 bytes)*: | 5 |

*Figure 6-2 Edit VoIP Service Class (Continued)*



Extended or Peak Burst Size (0 - 2147483647 bytes) *: 10000

Conform Action

Type: transmit | set-mpls-exp-transmit

Value: 6

Exceed Action

Type: drop | none

Value:

Violate Action

Type: none | none

Value:

**Congestion Management**

Bandwidth in Kbps **:

Bandwidth Percent (1 - 100%) **: 48 ● relative ○ absolute

Queue Limit in Packets (1 - 262144 packets):

Queue Limit in Cells (1 - 262144 cells):

Note: * - Required Field

Note: ** - At least one bandwidth is required except for "class-default". However, "Bandwidth in Kbps" and "Bandwidth Percent" can not co-exist.

Table 6-1 describes the entry fields for the VoIP, Routing Protocol, and Management service classes.

*Table 6-1 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.<br>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 6-8. |
| **Traffic Classification** | |
| Filters: | **match-any:** Traffic classification passes when any one of the following classifications is met.<br>**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. |

*Table 6-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)*

| Entry Field | Description |
|---|---|
| Management LAN Address (Management service class only) | Traffic classification based on management LAN address.<br>To change the default setting for this entry field, see Editing the Properties File, page 4-4. |
| **Marking** (VoIP and Management service classes only) | |
| Enabled | Enable packet marking. |
| DSCP | Mark packets with a DSCP value.<br>**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. |
| 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.<br>**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. |

*Table 6-1 Edit Service Class Entry Fields (VoIP, Routing Protocol, and Management) (continued)*

| Entry Field | Description |
|---|---|
| Conform Action–Type | The action to take on packets that conform to the specified rate limit.<br>**Single Action**<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>• Set-dscp-transmit—Sets the DSCP value and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet.<br>**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.<br>**Dual Action**<br>• set-mpls-exp-transmit—Sets MPLS exp value and sends the packet.<br>• set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet.<br>• set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet.<br>**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 6-1 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.<br>**Single Action**<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>• Set-dscp-transmit—Sets the DSCP value and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet.<br>**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.<br>**Dual Action**<br>• set-mpls-exp-transmit—Sets MPLS exp value and sends the packet.<br>• set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet.<br>• set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet.<br>**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 6-1 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.<br>**Single Action**<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>• Set-dscp-transmit—Sets the DSCP value and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet.<br>**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.<br>**Dual Action**<br>• set-mpls-exp-transmit—Sends the packet.<br>• set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet.<br>• set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet.<br>**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 6-1 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.<br>• 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.<br>• 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. |

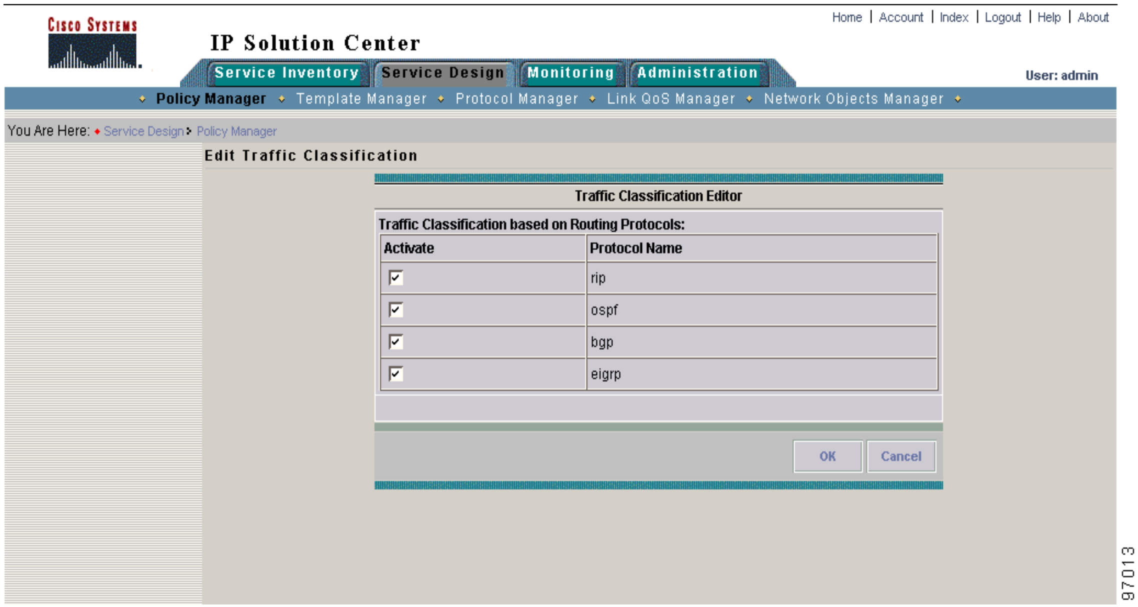
**Note** The process for marking packets with DSCP and IP Precedence bits is described in detail in the following document on Cisco.com:
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

## 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 to change the list of protocols to use for the Routing Protocol service class (Figure 6-3).

*Figure 6-3 Edit Traffic Classification*



Edit Traffic Classification

Traffic Classification Editor

Traffic Classification based on Routing Protocols:

| Activate | Protocol Name |
|---|---|
| ☑ | rip |
| ☑ | ospf |
| ☑ | bgp |
| ☑ | eigrp |

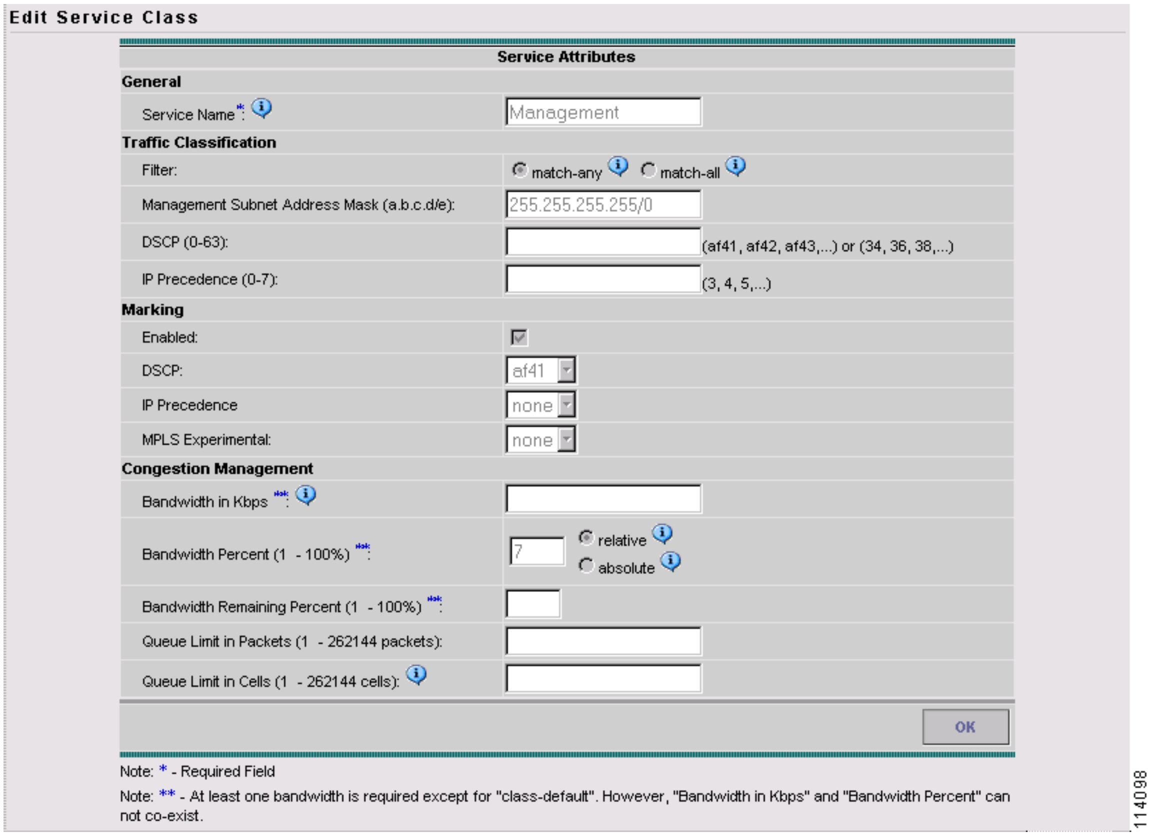
Select the routing protocols to use and click **OK**.

## Editing the Management Service Class

This section describes how to edit the Management service class.

Figure 6-4 shows the Edit Service Class window for the Management service class.

*Figure 6-4 Edit Management Service Class*



Edit Service Class

Service Attributes

| | |
|---|---|
| **General** | |
| Service Name*: | Management |
| **Traffic Classification** | |
| Filter: | ● match-any ○ match-all |
| Management Subnet Address Mask (a.b.c.d/e): | 255.255.255.255/0 |
| DSCP (0-63): | (af41, af42, af43,...) or (34, 36, 38,...) |
| IP Precedence (0-7): | (3, 4, 5,...) |
| **Marking** | |
| Enabled: | ☑ |
| DSCP: | af41 |
| IP Precedence | none |
| MPLS Experimental: | none |
| **Congestion Management** | |
| Bandwidth in Kbps **: | |
| Bandwidth Percent (1 - 100%) **: | 7 ● relative ○ absolute |
| Bandwidth Remaining Percent (1 - 100%) **: | |
| Queue Limit in Packets (1 - 262144 packets): | |
| Queue Limit in Cells (1 - 262144 cells): | |

Note: * - Required Field

Note: ** - At least one bandwidth is required except for "class-default". However, "Bandwidth in Kbps" and "Bandwidth Percent" can not co-exist.

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. To change the default setting for this field, see Editing the Properties File, page 4-4.
- 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 6-1 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 6-21 for more information.

# Business-Data-1 and Best Effort Service Classes

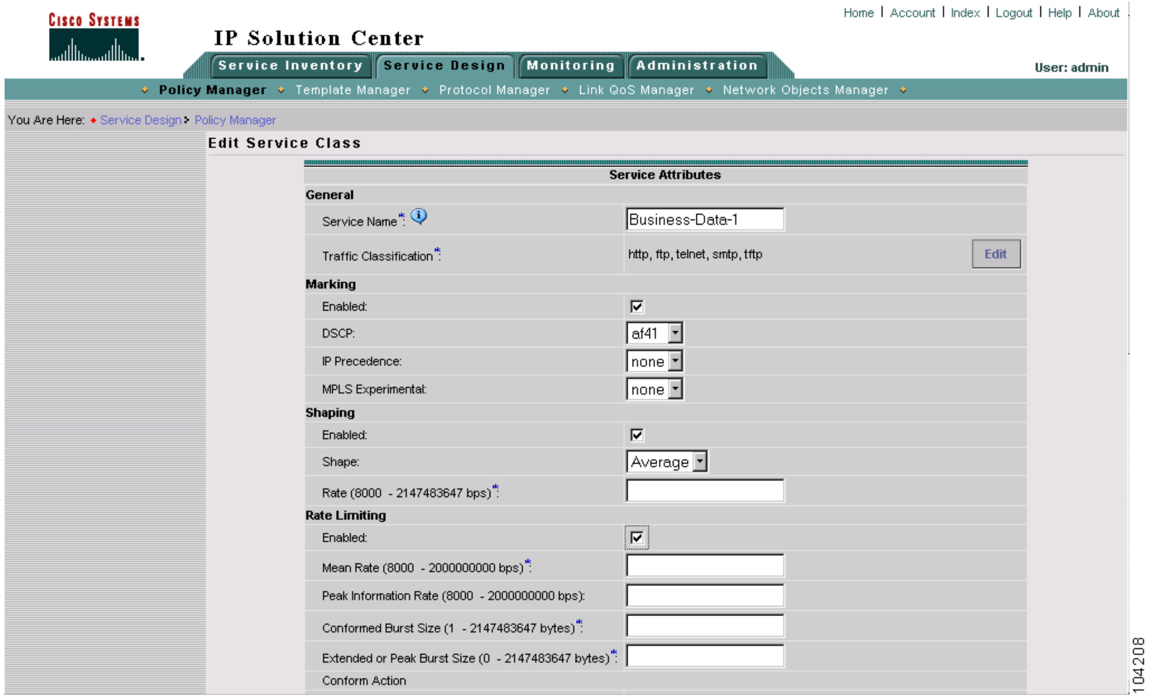
For the two data service classes, Business-Data-1 and Best Effort, the parameters are nearly identical. The entry field descriptions are combined in this section. The only difference between the two data service classes is the Traffic Classification parameter:

- Business-Data-1 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 6-2.

Figure 6-5 and Figure 6-6 show the general information, marking, and shaping fields for the Business-Data-1 service class.

*Figure 6-5* *Business-Data-1*



Edit Service Class

Service Attributes

General

Service Name*: Business-Data-1

Traffic Classification*: http, ftp, telnet, smtp, tftp

Marking

Enabled: ☑

DSCP: af41

IP Precedence: none

MPLS Experimental: none

Shaping

Enabled: ☑

Shape: Average

Rate (8000 - 2147483647 bps)*:

Rate Limiting

Enabled: ☑

Mean Rate (8000 - 2000000000 bps)*:

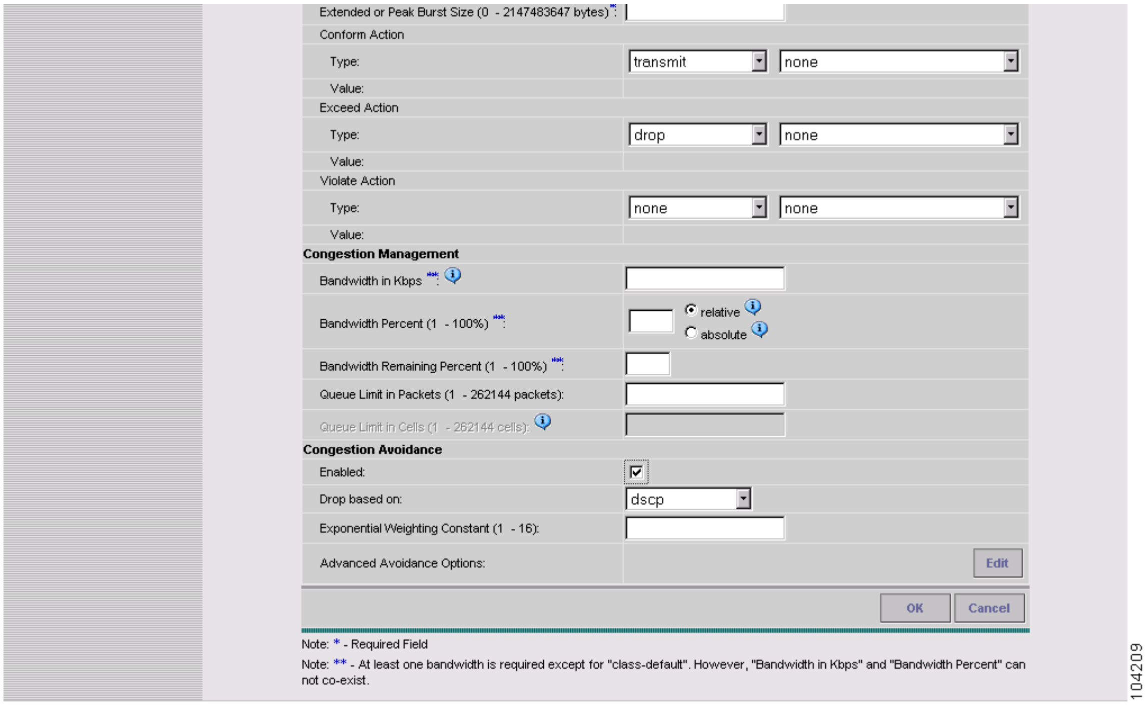
Peak Information Rate (8000 - 2000000000 bps):

Conformed Burst Size (1 - 2147483647 bytes)*:

Extended or Peak Burst Size (0 - 2147483647 bytes)*:

Conform Action

*Figure 6-6 Business-Data-1 (continued)*



Extended or Peak Burst Size (0 - 2147483647 bytes)**:

Conform Action
Type: transmit / none
Value:

Exceed Action
Type: drop / none
Value:

Violate Action
Type: none / none
Value:

**Congestion Management**

Bandwidth in Kbps **:

Bandwidth Percent (1 - 100%) **: ● relative ○ absolute

Bandwidth Remaining Percent (1 - 100%) **:

Queue Limit in Packets (1 - 262144 packets):

Queue Limit in Cells (1 - 262144 cells):

**Congestion Avoidance**

Enabled: ☑

Drop based on: dscp

Exponential Weighting Constant (1 - 16):

Advanced Avoidance Options: Edit

OK Cancel

Note: * - Required Field

Note: ** - At least one bandwidth is required except for "class-default". However, "Bandwidth in Kbps" and "Bandwidth Percent" can not co-exist.

Table 6-2 describes the entry fields for the data service classes. The entry fields you see depend on which service class is being edited.

*Table 6-2 Edit Service Class Entry Fields (Business Data-1 and Best Effort)*

| Entry Field | Description |
|---|---|
| **General** | |
| Service Class | The name of the service class (Business-Data-1, Best Effort, or the name of your choice). |
| Traffic Classification | Traffic classification based on protocols.<br>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.<br>These options are further described in Traffic Classification, page 6-17. |
| **Marking** | |
| Enabled | Enable packet marking. |
| DSCP | Mark packets with a DSCP value.<br>**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. |

*Table 6-2 Edit Service Class Entry Fields (Business Data-1 and Best Effort) (continued)*

| Entry Field | Description |
|---|---|
| **Shaping** | |
| Enabled | Enable class-based traffic shaping parameters.<br>To specify interface-based traffic shaping parameters, see Aggregated Traffic Shapers, page 6-22. |
| Shape | Specify average or peak rate shaping.<br>• Average rate shaping limits the transmission rate to the committed information rate (CIR).<br>• Peak rate shaping configures the router to send more traffic than the CIR.<br>**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. |
| Conformed Burst Size | How large traffic bursts can be before some traffic exceeds the rate limit.<br>**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. |

*Table 6-2 Edit Service Class Entry Fields (Business Data-1 and Best Effort) (continued)*

| Entry Field | Description |
|---|---|
| Conform Action–Type | The action to take on packets that conform to the specified rate limit.<br>**Single Action**<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>• Set-dscp-transmit—Sets the DSCP value and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet.<br>**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.<br>**Dual Action**<br>• set-mpls-exp-transmit—Sends the packet.<br>• set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet.<br>• set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet.<br>**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 6-2 Edit Service Class Entry Fields (Business Data-1 and Best Effort) (continued)*

| Entry Field | Description |
|---|---|
| Exceed Action–Type | The action to take on packets that conform to the specified rate limit.<br>**Single Action**<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>• Set-dscp-transmit—Sets the DSCP value and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet.<br>**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.<br>**Dual Action**<br>• set-mpls-exp-transmit—Sends the packet.<br>• set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet.<br>• set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet.<br>**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 6-2 Edit Service Class Entry Fields (Business Data-1 and Best Effort) (continued)*

| Entry Field | Description |
|---|---|
| Violate Action–Type | The action to take on packets that conform to the specified rate limit.<br>**Single Action**<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>• Set-dscp-transmit—Sets the DSCP value and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence (0 to 7) value and sends the packet.<br>**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.<br>**Dual Action**<br>• set-mpls-exp-transmit—Sends the packet.<br>• set-mpls-imposition-transmit—Sets the MPLS imposition value and transmits the packet.<br>• set-mpls-topmost-transmit—Sets the MPLS topmost value and transmits the packet.<br>**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 6-2 Edit Service Class Entry Fields (Business Data-1 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.<br>• 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.<br>• 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 6-19. |

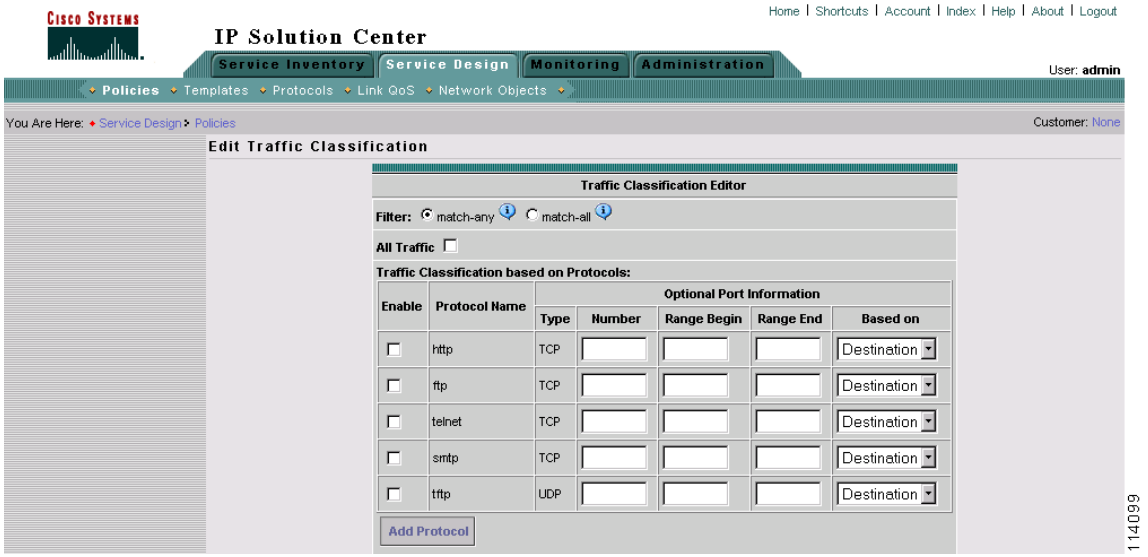
## Editing the Data Service Classes

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 6-7 and Figure 6-8 show the traffic classification settings for this service class. It includes some protocols that are enabled by default.

*Figure 6-7 Traffic Classification Editor—Data Service Class*



Edit Traffic Classification

Traffic Classification Editor

Filter: ● match-any ○ match-all

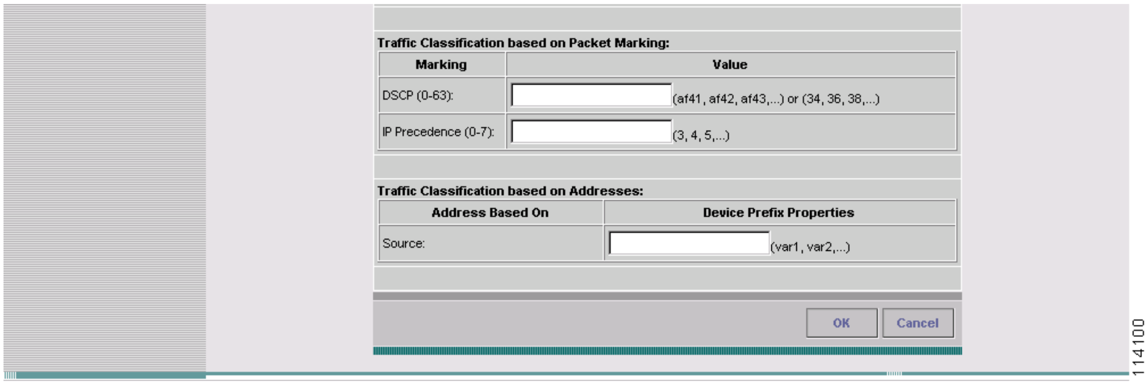
All Traffic □

Traffic Classification based on Protocols:

| Enable | Protocol Name | Optional Port Information | | | | |
|---|---|---|---|---|---|---|
| | | Type | Number | Range Begin | Range End | Based on |
| □ | http | TCP | | | | Destination |
| □ | ftp | TCP | | | | Destination |
| □ | telnet | TCP | | | | Destination |
| □ | smtp | TCP | | | | Destination |
| □ | tftp | UDP | | | | Destination |

Add Protocol

*Figure 6-8 Traffic Classification Editor—Data Service Class (continued)*



Traffic Classification based on Packet Marking:

| Marking | Value |
|---|---|
| DSCP (0-63): | (af41, af42, af43,...) or (34, 36, 38,...) |
| IP Precedence (0-7): | (3, 4, 5,...) |

Traffic Classification based on Addresses:

| Address Based On | Device Prefix Properties |
|---|---|
| Source: | (var1, var2,...) |

OK Cancel

The entry fields are described in Table 6-3.

*Table 6-3 Traffic Classification Editor Entry Fields*

| Entry Field | Description |
|---|---|
| **Filter:** | **match-any: Traffic** classification passes when any one of the following classifications is met.<br>**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 6-3 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)<br>On platforms running IOS that support NBAR based traffic classification, you can provide NBAR support such as:<br>• match protocol *protocol name*<br>where *protocol name* is citrix, cuseeme, for example.<br>• match protocol http url *url name*<br>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)<br>To create named ACLs such as:<br>• permit *port_type* any any eq *port_number*,<br>• permit *port_type* any range *port_range_begin port_range_end any*<br>where *port_type is* UDP or TCP. Port information can be source-based or destination-based.<br>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 Based on Variables, page 4-6. |

## Advanced Avoidance Options

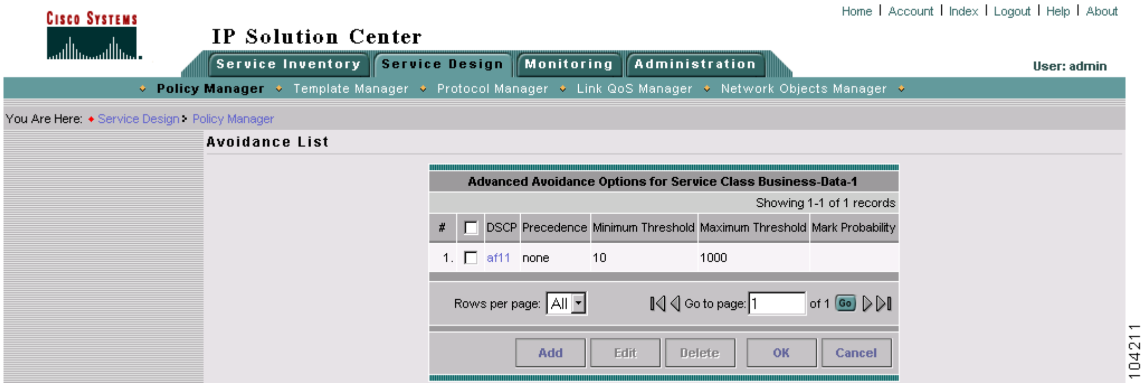
This section describes the advanced congestion avoidance parameters for the data service classes.

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 6-9).

***Figure 6-9 Avoidance List***



Avoidance List

Advanced Avoidance Options for Service Class Business-Data-1

Showing 1-1 of 1 records

| # | □ | DSCP | Precedence | Minimum Threshold | Maximum Threshold | Mark Probability |
|---|---|---|---|---|---|---|
| 1. | □ | af11 | none | 10 | 1000 | |

Rows per page: All | Go to page: 1 of 1 Go

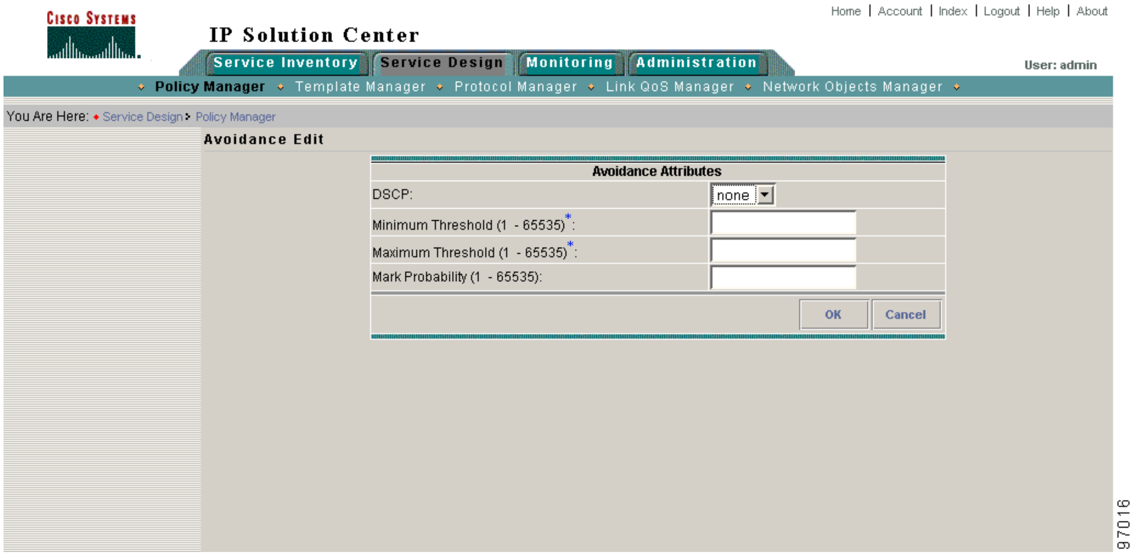
Add | Edit | Delete | OK | Cancel

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 6-10.

***Figure 6-10 Avoidance Edit***



Avoidance Edit

Avoidance Attributes

| | |
|---|---|
| DSCP: | none |
| Minimum Threshold (1 - 65535)*: | |
| Maximum Threshold (1 - 65535)*: | |
| Mark Probability (1 - 65535): | |

OK | Cancel

**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

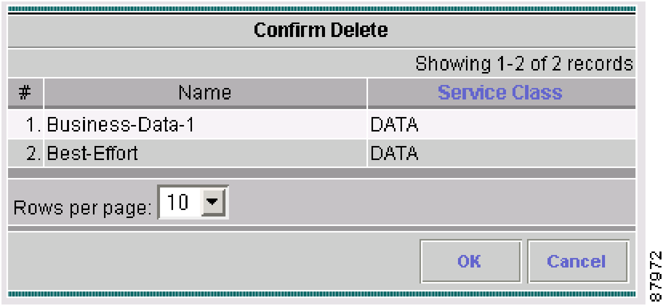
If your QoS policy requires additional service classes, use the data service class template provided with ISC to add another management or data service class.

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 6-2 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 6-11), and click **OK**.

*Figure 6-11 Delete Service Class*



Confirm Delete

Showing 1-2 of 2 records

| # | Name | Service Class |
|---|---|---|
| 1. | Business-Data-1 | DATA |
| 2. | Best-Effort | DATA |

Rows per page: 10

# Link Level QoS Parameters

Link level QoS parameters see QoS settings that are based on the CPE-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.

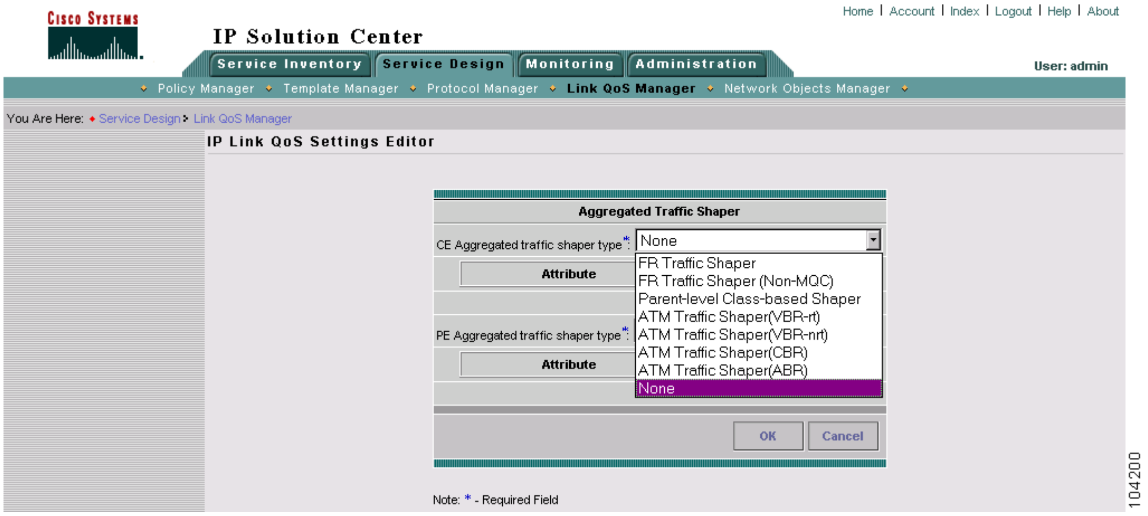
To apply class-based traffic shaping parameters, see the Editing the Data Service Classes, page 6-17.

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 (Figure 6-12).

*Figure 6-12 Select Aggregated Traffic Shaper Type*



CE Aggregated traffic shaper type*: None

PE Aggregated traffic shaper type*:

Note: * - Required Field

Select one aggregated traffic shaper for the CE and one for the PE. Table 6-4 describes the aggregated traffic shaper types.

*Table 6-4 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. |

*Table 6-4 Aggregated Traffic Shaper Types (continued)*

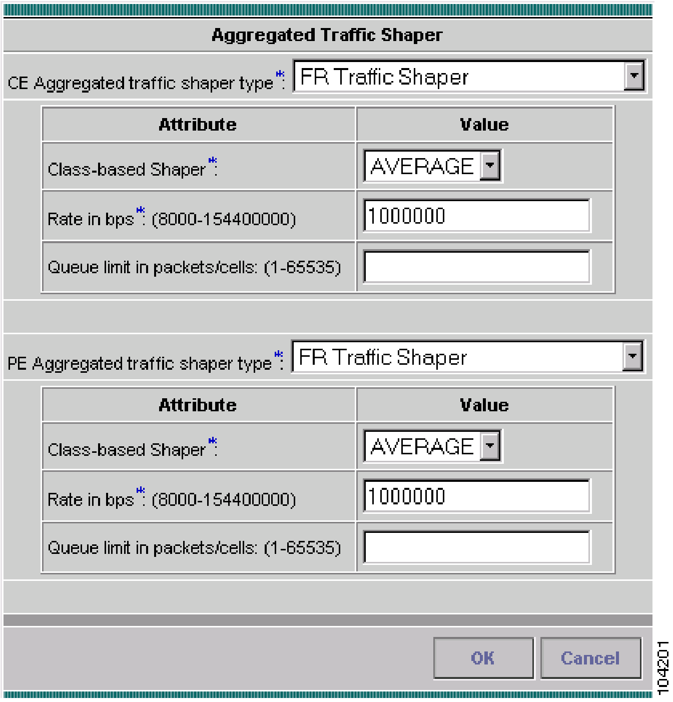
| Shaper Type | Description |
|---|---|
| Parent-level Class-based Shaper | Used for nested policies where a bottom-level policy identifies one or more classes of traffic, and a top-level policy shapes the output of the traffic classes into a single shape rate. You can apply nested policies to interfaces 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. |
| 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 6-13) 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 6-13 FR Traffic Shaper*



Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: FR Traffic Shaper

| Attribute | Value |
|---|---|
| Class-based Shaper*: | AVERAGE |
| Rate in bps*: (8000-154400000) | 1000000 |
| Queue limit in packets/cells: (1-65535) | |

PE Aggregated traffic shaper type*: FR Traffic Shaper

| Attribute | Value |
|---|---|
| Class-based Shaper*: | AVERAGE |
| Rate in bps*: (8000-154400000) | 1000000 |
| Queue limit in packets/cells: (1-65535) | |

The entry fields are described in Table 6-5.

*Table 6-5 Frame Relay Traffic Shaper Entry Fields*

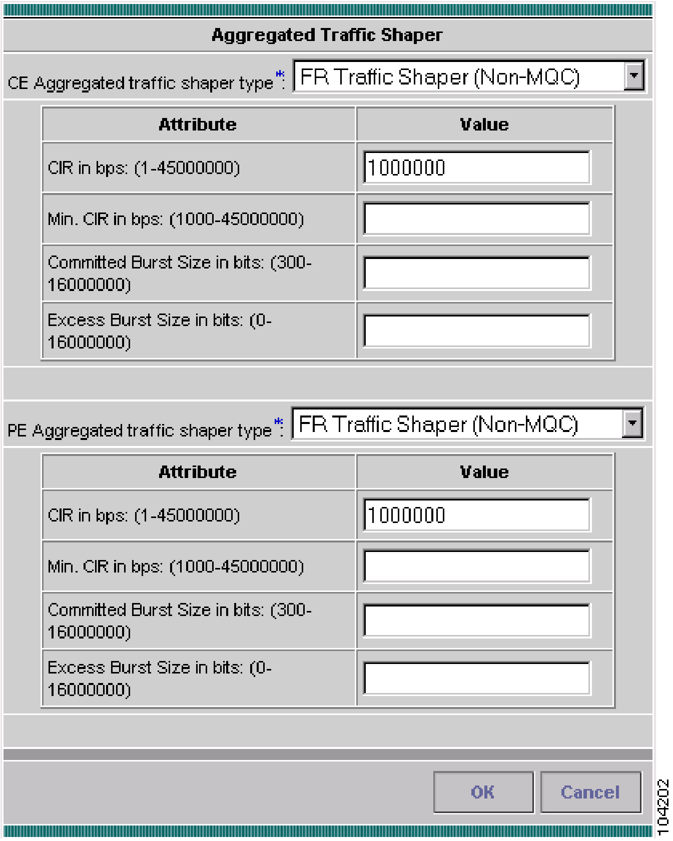
| Attribute | Description |
|---|---|
| Class-based Shaper | Choose average or peak. Peak rate shaping allows you to make better use of available bandwidth because it allows you to send more data than the CIR, if the bandwidth is available. |
| Rate in bps | This field might be prepopulated with the 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 6-14) on all ISC-supported low-end router platforms (Cisco 7200 series and below).

*Figure 6-14 FRTS Non-MQC*



Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: FR Traffic Shaper (Non-MQC)

| Attribute | Value |
|---|---|
| CIR in bps: (1-45000000) | 1000000 |
| Min. CIR in bps: (1000-45000000) | |
| Committed Burst Size in bits: (300-16000000) | |
| Excess Burst Size in bits: (0-16000000) | |

PE Aggregated traffic shaper type*: FR Traffic Shaper (Non-MQC)

| Attribute | Value |
|---|---|
| CIR in bps: (1-45000000) | 1000000 |
| Min. CIR in bps: (1000-45000000) | |
| Committed Burst Size in bits: (300-16000000) | |
| Excess Burst Size in bits: (0-16000000) | |

The entry fields are described in Table 6-6.

*Table 6-6 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

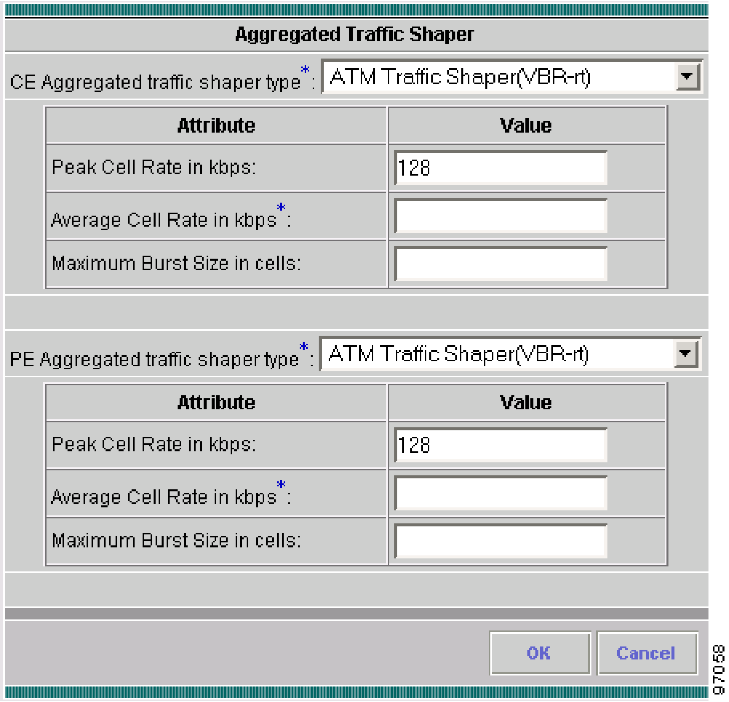
Parent-level class-based traffic shapers are used for nested policies where a bottom-level policy identifies one or more classes of traffic, and a top-level policy shapes the output of the traffic classes into a single shape rate. You can apply nested policies to interfaces or subinterfaces.

The parent-level class-based shaper dialog box and entry fields are the same as the FR Traffic Shaper. See FR Traffic Shaper, page 6-23.

## 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 6-15.

*Figure 6-15 ATM Traffic Shaper VBR-rt*



Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-rt)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |
| Average Cell Rate in kbps*: | |
| Maximum Burst Size in cells: | |

PE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-rt)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |
| Average Cell Rate in kbps*: | |
| Maximum Burst Size in cells: | |

The entry fields are described in Table 6-7.

*Table 6-7 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. |

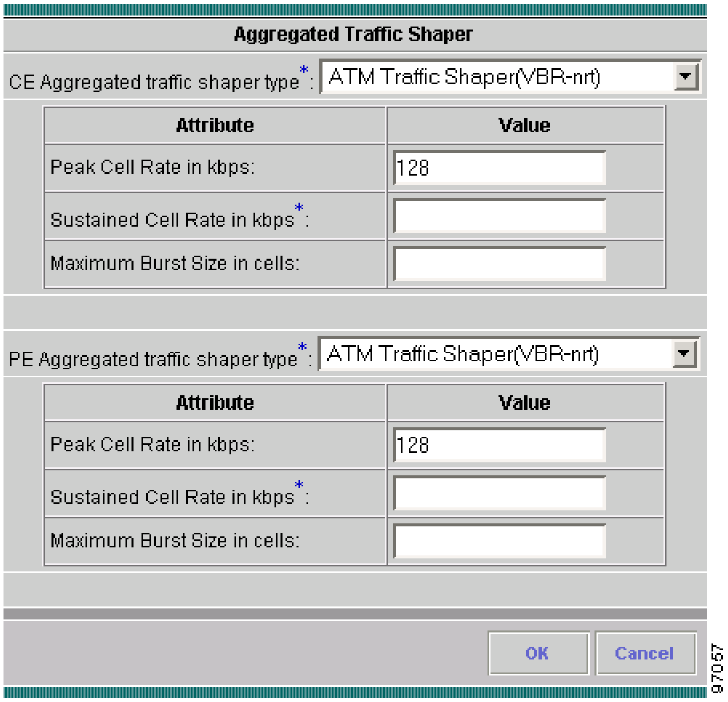
**Tip** Configure PCR and MBS parameters for reducing latency, not increasing bandwidth.

## 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 6-16.

*Figure 6-16 ATM Traffic Shaper VBR-nrt*



Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-nrt)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |
| Sustained Cell Rate in kbps*: | |
| Maximum Burst Size in cells: | |

PE Aggregated traffic shaper type*: ATM Traffic Shaper(VBR-nrt)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |
| Sustained Cell Rate in kbps*: | |
| Maximum Burst Size in cells: | |

The entry fields are described in Table 6-8.

*Table 6-8 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)

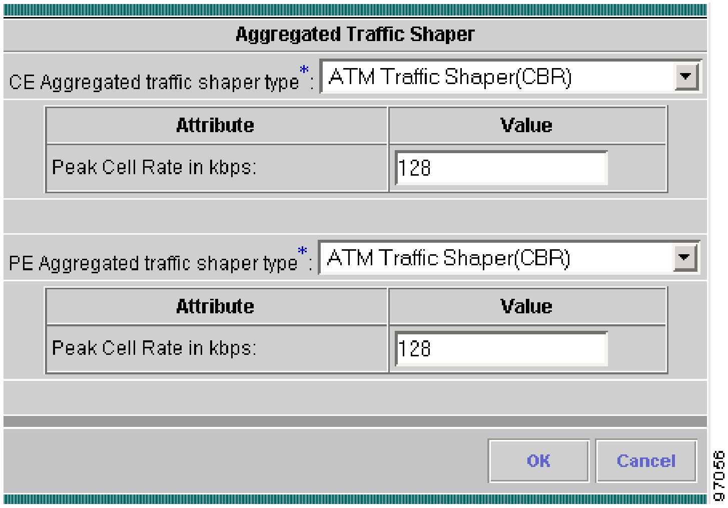
- (1 x maximum number of calls) x 16 Kbps = sustained cell rate (SCR)
- (4 x maximum number of calls) = burst size in cells (MBS)

**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 6-17.

*Figure 6-17 ATM Traffic Shaper CBR*



Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: ATM Traffic Shaper(CBR)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |

PE Aggregated traffic shaper type*: ATM Traffic Shaper(CBR)

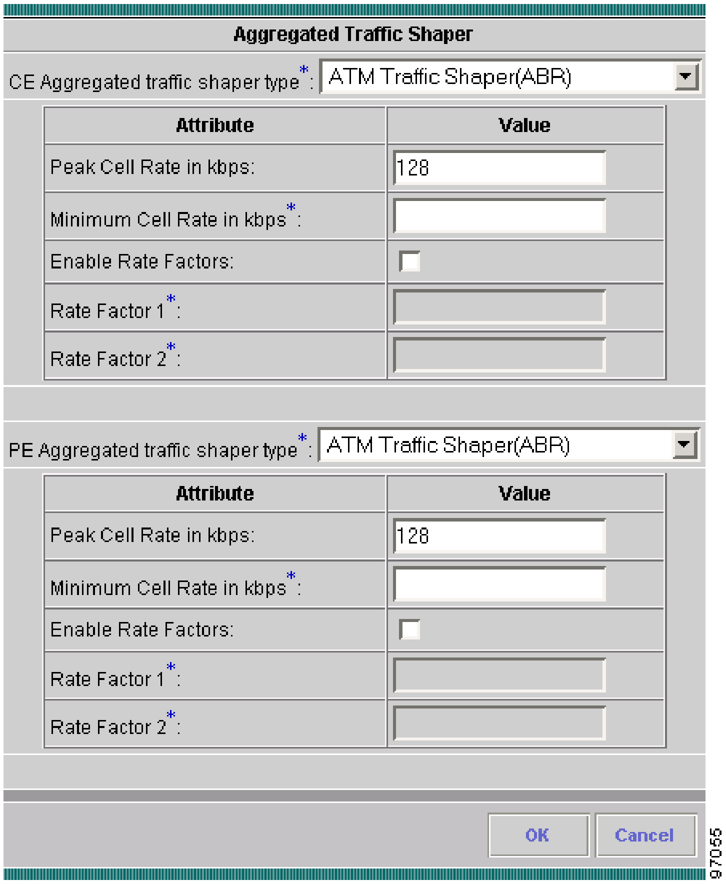
| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |

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 6-18.

*Figure 6-18 ATM Traffic Shaper ABR*



Aggregated Traffic Shaper

CE Aggregated traffic shaper type*: ATM Traffic Shaper(ABR)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |
| Minimum Cell Rate in kbps*: | |
| Enable Rate Factors: | □ |
| Rate Factor 1*: | |
| Rate Factor 2*: | |

PE Aggregated traffic shaper type*: ATM Traffic Shaper(ABR)

| Attribute | Value |
|---|---|
| Peak Cell Rate in kbps: | 128 |
| Minimum Cell Rate in kbps*: | |
| Enable Rate Factors: | □ |
| Rate Factor 1*: | |
| Rate Factor 2*: | |

The entry fields are described in Table 6-9.

*Table 6-9 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

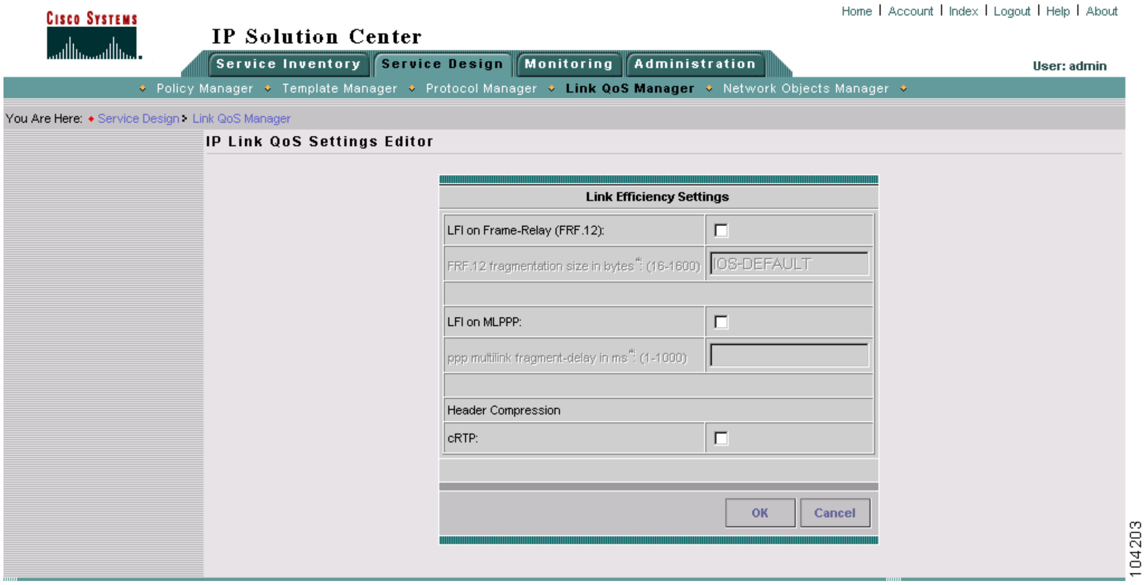
Link efficiency settings are based on the CPE-PE link itself and are used to minimize serialization delay on the link. ISC uses methods of fragmentation and compression to minimize this delay.

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 an issue and much of the traffic is RTP traffic.

Figure 6-19 shows the IP Link QoS Settings Editor window.

*Figure 6-19 Link Efficiency Settings*



IP Link QoS Settings Editor

Link Efficiency Settings

LFI on Frame-Relay (FRF.12): ☐

FRF.12 fragmentation size in bytes*: (16-1600) IOS-DEFAULT

LFI on MLPPP: ☐

ppp multilink fragment-delay in ms*: (1-1000)

Header Compression

cRTP: ☐

Table 6-10 describes the entry fields for the Link Efficiency Settings window.

*Table 6-10 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. |

*Table 6-10 Link Efficiency Settings Entry Fields (continued)*

| Entry fields | Description |
|---|---|
| PPP multilink fragment delay in ms | The amount of delay between packet fragments. The range is 1 to 1000 ms. |
| cRTP | Enables cRTP header compression. |

**Tip** We recommend that you do not select cRTP for high-speed interfaces (anything over T1) because it might affect the rate of traffic.

## 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 CPE-PE link. You can also specify traffic handling policies for when the traffic conforms or exceeds the specified rate limit.

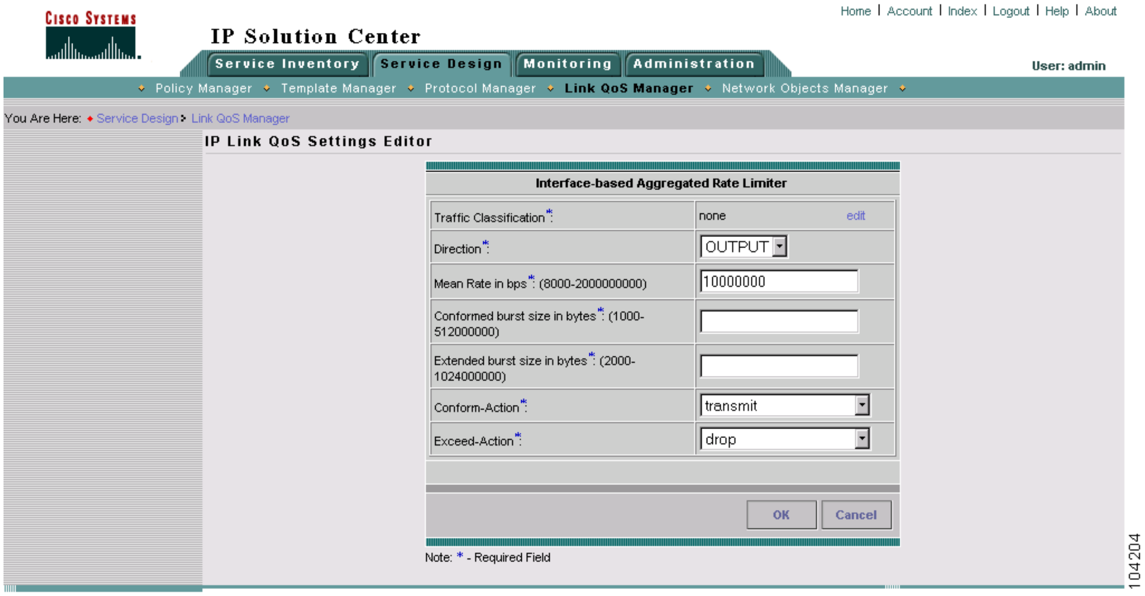
Aggregate rate limits match all packets or a specified subset of packets on an interface or subinterface. To specify class-based rate limiting parameters, see the Creating the Service Level IP QoS Policy, page 5-10.

ISC supports the following interface-based rate limiter parameters:

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

Figure 6-20 shows the Interface-based Aggregated Rate Limiter window.

*Figure 6-20 Interface Based Aggregated Limiter*



IP Link QoS Settings Editor

Interface-based Aggregated Rate Limiter

| | |
|---|---|
| Traffic Classification*: | none edit |
| Direction*: | OUTPUT |
| Mean Rate in bps*: (8000-2000000000) | 10000000 |
| Conformed burst size in bytes*: (1000-512000000) | |
| Extended burst size in bytes*: (2000-1024000000) | |
| Conform-Action*: | transmit |
| Exceed-Action*: | drop |

Note: * - Required Field

Table 6-11 describes the entry fields for the Interface-based Aggregated Rate Limiter window. All fields in this window are required.

*Table 6-11 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 6-17. |
| Direction | The direction of traffic to apply rate limiting parameters to. Choose from Input or Output. |
| Mean rate in bps | The range is 8000 to 2000000000 bps. |
| Conformed burst size in bytes | The range is 1000 to 512000000 bytes.<br>**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. |

***Table 6-11 Interface-based Aggregated Rate Limiter Entry Fields (continued)***

| Entry field | Description |
|---|---|
| Conform-Action | Specifies how to handle packets that conform to the configured rate limit.<br>• Transmit—Sends the packet.<br>• Drop—Drops the packet.<br>**Note** If you select any of the following, you must specify the DSCP, IP, or MPLS Precedence value in the adjacent drop-down menus.<br>• Set-dscp-transmit—Sets the DSCP value (0-63) and transmits the packet.<br>• Set-prec-transmit—Sets the IP precedence value (0 to 7) and sends the packet.<br>• Set-mpls-exp-transmit—Sets the MPLS value (0 to 7) and transmits the packet.<br>• Set-dscp-continue—Sets the DSCP value (0 to 63) and transmits the packet.<br>• Set-prec-continue—Sets the IP precedence (0 to 7) value and sends the packet.<br>• 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. |

CHAPTER 7

# Applying QoS Policies to VPN Services

The Cisco IP Solution Center (ISC) supports Ethernet QoS provisioning at the access circuit (the CPE-PE link). ISC can provision QoS policies for a network independent of VPN services (IP QoS) or in addition to VPN services that have been provisioned by ISC (Ethernet QoS and IP QoS for MPLS VPN).

- IP QoS provisioning is described in Chapter 5, "Provisioning Process for IP QoS."
- QoS policies for VPN services (Ethernet QoS) are deployed on top of an existing VPN service request; such as MPLS, L2VPN, and VPLS. ISC derives interface configuration information from the VPN service and applies the QoS policy to the interfaces.

Additionally, ISC supports the following QoS parameters for VPN services:

- For an MPLS network, marking packets with MPLS Experimental values (MPLS Exp.) at the PE ingress interface.

This chapter describes how to apply QoS policies to VPN services provisioned by ISC.

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

- Ethernet Qos Policy
- Ethernet Qos policies applied to an Ethernet (L2VPN, MPLS VPN, VPLS) service request

The chapter contains the following sections:

## Service Level Ethernet QoS Policy

The Ethernet QoS policy is the set of rules or conditions that apply to frames as they come across each port. This set of rules is defined in an Ethernet QoS service class.

An Ethernet QoS service class provides a method for classifying traffic flows into classes of service (CoS) so that you can apply the appropriate QoS parameters to a class of traffic instead of applying them to all traffic. For example, all IP traffic might be grouped into a single class so that bandwidth is allocated for the class and not for individual traffic flows.

An Ethernet QoS service class can include:

- Methods for classifying traffic (all IP traffic, all Mac traffic, DSCP value, IP precedence value)
- Methods for marking traffic (class of service)

- Rate limiting parameters (mean, burst size, conform/exceed)
- Congestion management parameters (bandwidth and queue limit)

A typical service provider network might create different QoS policies, and each QoS policy might contain 3 to 4 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.

ISC provides four default CoS templates to modify.

- Architecture for Voice, Video and Integrated Data (AVVID)
- Call Control
- Business Critical
- Best Effort

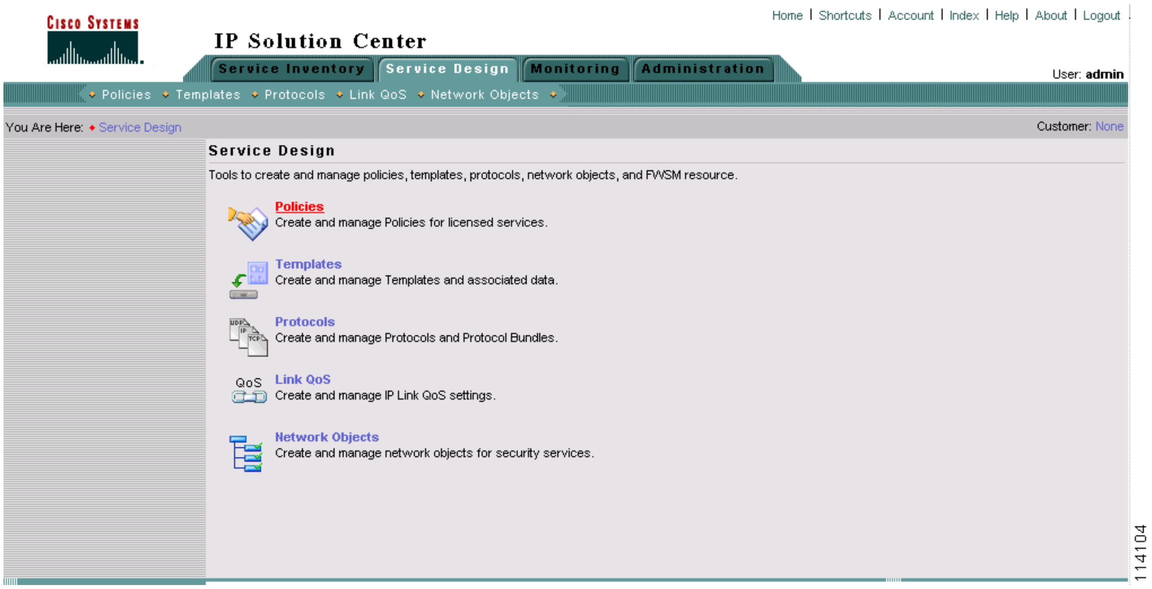
Select the service classes to use in the Ethernet QoS policy and edit each one with the required parameters. All service classes should contain, at least, rate limiting information. You can also add a service class, delete an unused service class, or change the order of the service classes. ISC supports 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.

The following sections describe how to create the CoS portion of an Ethernet QoS Policy using the ISC user interface. For detailed information on the entry fields for each service class parameter, see Service Level Ethernet QoS Policy Entry Fields, page 7-8.

To create an Ethernet QoS policy:

**Step 1** On the Service Design tab, click **Policy Manager** (see Figure 7-1).

***Figure 7-1 Policy Manager***



Service Design

Tools to create and manage policies, templates, protocols, network objects, and FWSM resource.

Policies
Create and manage Policies for licensed services.

Templates
Create and manage Templates and associated data.

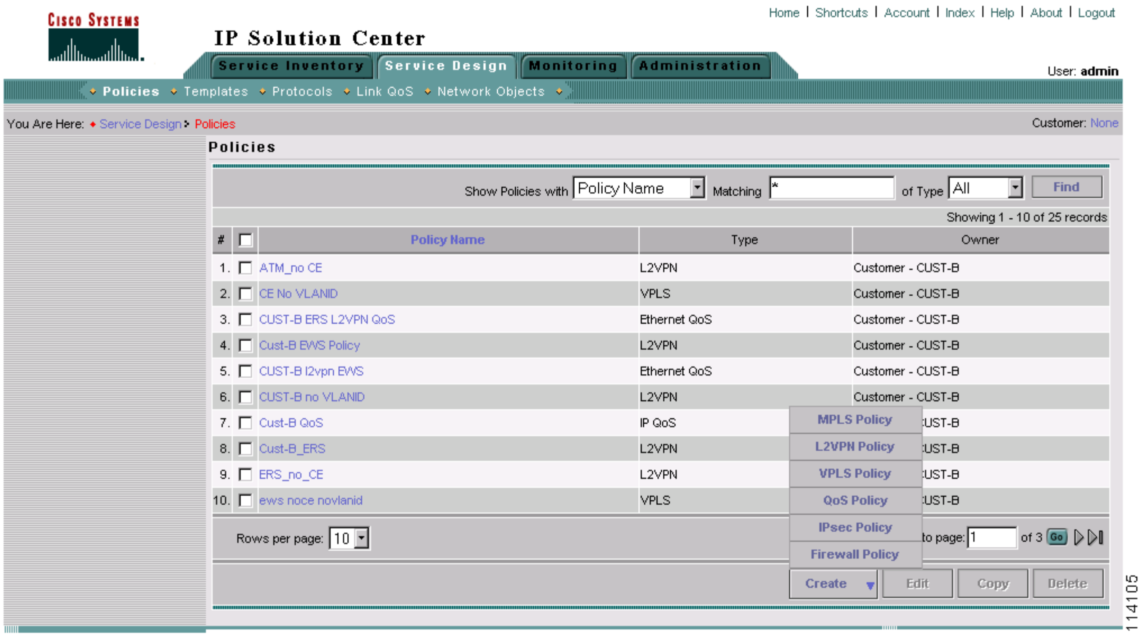
Protocols
Create and manage Protocols and Protocol Bundles.

Link QoS
Create and manage IP Link QoS settings.

Network Objects
Create and manage network objects for security services.

The Policies window appears (Figure 7-2).

*Figure 7-2* ***Create QoS Policy***



Policies

Show Policies with Policy Name Matching * of Type All

Showing 1 - 10 of 25 records

| # | □ | Policy Name | Type | Owner |
|---|---|---|---|---|
| 1. | □ | ATM_no CE | L2VPN | Customer - CUST-B |
| 2. | □ | CE No VLANID | VPLS | Customer - CUST-B |
| 3. | □ | CUST-B ERS L2VPN QoS | Ethernet QoS | Customer - CUST-B |
| 4. | □ | Cust-B EWS Policy | L2VPN | Customer - CUST-B |
| 5. | □ | CUST-B l2vpn EWS | Ethernet QoS | Customer - CUST-B |
| 6. | □ | CUST-B no VLANID | L2VPN | Customer - CUST-B |
| 7. | □ | Cust-B QoS | IP QoS | UST-B |
| 8. | □ | Cust-B_ERS | L2VPN | UST-B |
| 9. | □ | ERS_no_CE | L2VPN | UST-B |
| 10. | □ | ews noce novlanid | VPLS | UST-B |

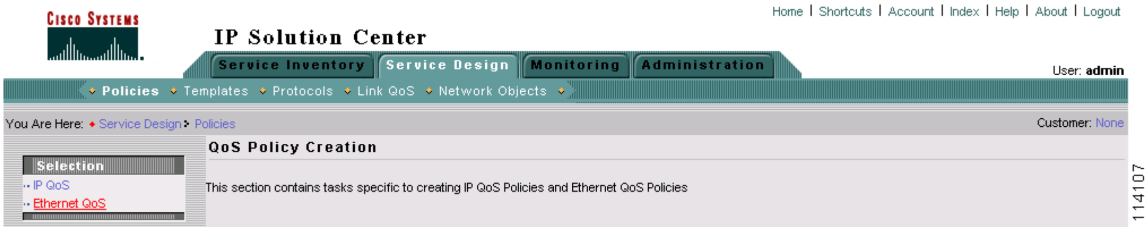
Rows per page: 10 to page: 1 of 3

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

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

**Step 2** Click **Create** and choose **QoS Policy** from the menu. The Qos Policy Creation window appears (see Figure 7-3).

*Figure 7-3* ***Create QoS Policy***

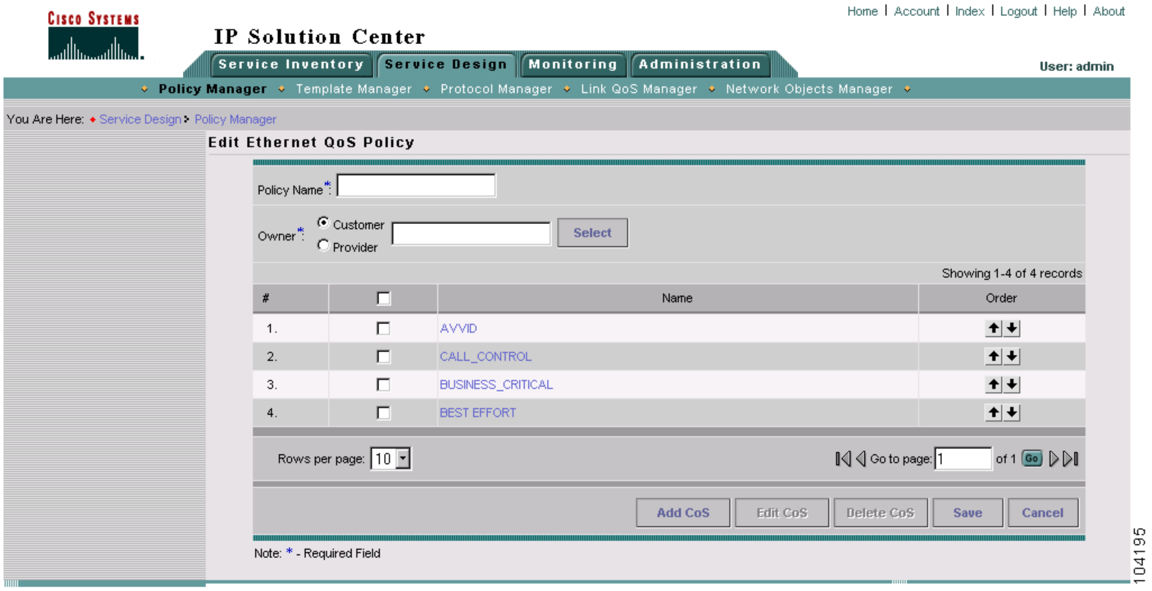


QoS Policy Creation

This section contains tasks specific to creating IP QoS Policies and Ethernet QoS Policies

**Step 3** Select **Ethernet QoS** from the TOC at left. The Edit Ethernet QoS Policy window (Figure 7-4) appears.

*Figure 7-4 Edit Ethernet QoS Policy*



Policy Name*:

Owner*: ● Customer ○ Provider

Showing 1-4 of 4 records

| # | ☐ | Name | Order |
|---|---|---|---|
| 1. | ☐ | AVVID | ↑↓ |
| 2. | ☐ | CALL_CONTROL | ↑↓ |
| 3. | ☐ | BUSINESS_CRITICAL | ↑↓ |
| 4. | ☐ | BEST EFFORT | ↑↓ |

Rows per page: 10 Go to page: 1 of 1

Note: * - Required Field

The Edit Ethernet QoS Policy window lists the policy name, the owner (customer or provider) for this policy, and the four default service classes for ISC. Use this window to select and edit the service classes to use in the QoS policy.

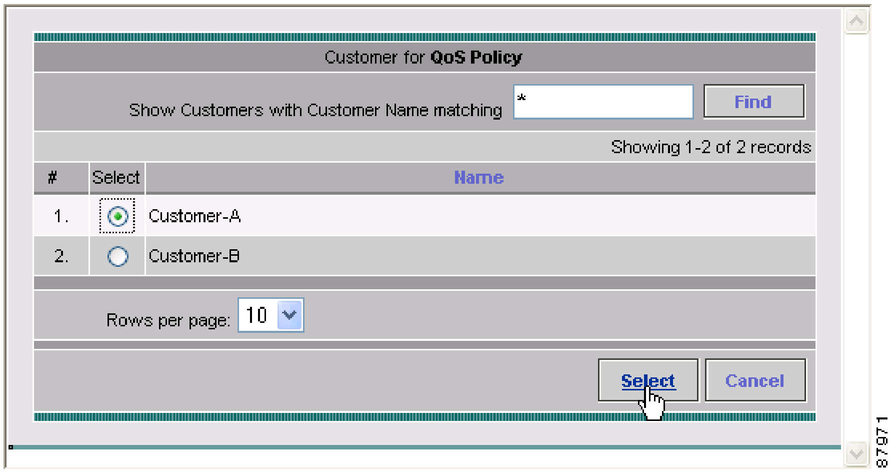
**Step 4** In the Edit Ethernet QoS Policy window, enter the **Policy Name**. Choose a policy name that is easily identified for your network. For example, if your customer is CustomerA, the policy name might be CustomerA-QoS-Policy.

**Note** We recommend that you choose an abbreviated policy name because it becomes part of the policy map name in the device configuration, and the policy map name cannot exceed 40 characters.

**Step 5** Select an Owner (Customer or Provider) for this QoS policy. Click the appropriate radio button and then click **Select**.

**Step 6** In the Customer (or Provider) for QoS Policy popup, choose the customer (provider) and click **Select** (Figure 7-5).

*Figure 7-5* ***Select Customer for QoS Policy***



Customer for **QoS Policy**

Show Customers with Customer Name matching: *

Showing 1-2 of 2 records

| # | Select | Name |
|---|---|---|
| 1. | ● | Customer-A |
| 2. | ○ | Customer-B |

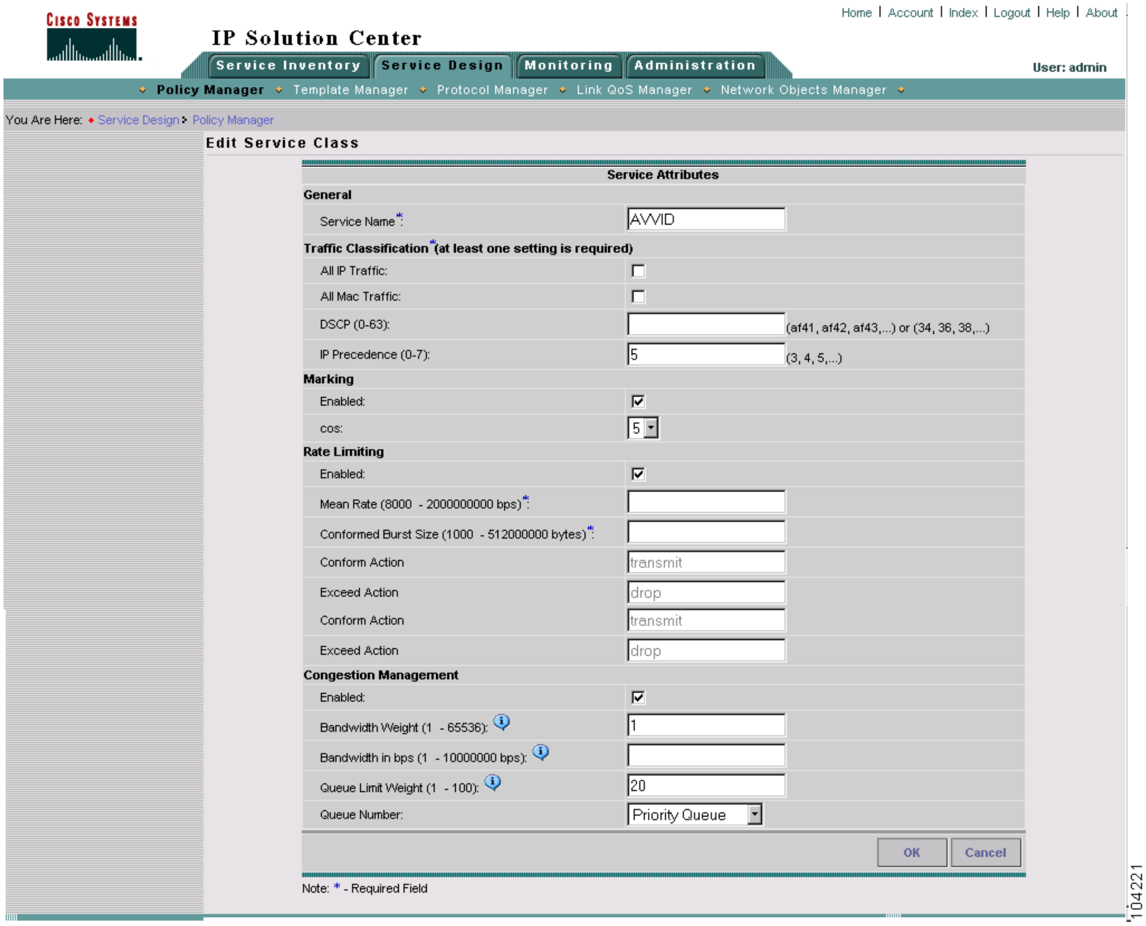
Rows per page: 10

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

**Step 7** The next step in defining the service level Ethernet QoS policy is to edit the service classes. You can include one or more service classes with the QoS policy. Edit the default service classes provided by ISC, delete the unwanted service classes, or create additional data service classes (**Add CoS**) if necessary.

**Step 8** To modify a service class to an Ethernet QoS policy, select the class of service and click **Edit CoS**. The Edit Service Class window appears (Figure 7-6 and Figure 7-7).

*Figure 7-6 Edit Service Class—AVVID*



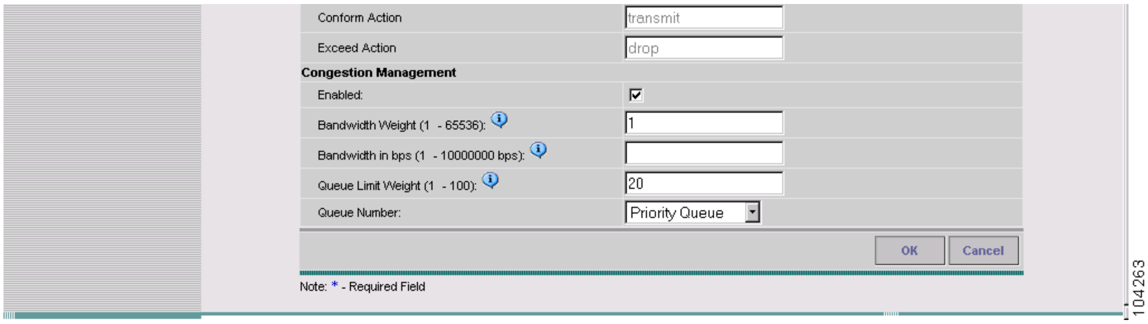
Edit Service Class

Service Attributes

| | |
|---|---|
| **General** | |
| Service Name*: | AVVID |
| **Traffic Classification*(at least one setting is required)** | |
| All IP Traffic: | □ |
| All Mac Traffic: | □ |
| DSCP (0-63): | (af41, af42, af43,...) or (34, 36, 38,...) |
| IP Precedence (0-7): | 5 (3, 4, 5,...) |
| **Marking** | |
| Enabled: | ☑ |
| cos: | 5 |
| **Rate Limiting** | |
| Enabled: | ☑ |
| Mean Rate (8000 - 2000000000 bps)*: | |
| Conformed Burst Size (1000 - 512000000 bytes)*: | |
| Conform Action | transmit |
| Exceed Action | drop |
| Conform Action | transmit |
| Exceed Action | drop |
| **Congestion Management** | |
| Enabled: | ☑ |
| Bandwidth Weight (1 - 65536): | 1 |
| Bandwidth in bps (1 - 10000000 bps): | |
| Queue Limit Weight (1 - 100): | 20 |
| Queue Number: | Priority Queue |

Note: * - Required Field

*Figure 7-7 Edit Service Class AVVID (continued)*



| | |
|---|---|
| Conform Action | transmit |
| Exceed Action | drop |
| **Congestion Management** | |
| Enabled: | ☑ |
| Bandwidth Weight (1 - 65536): | 1 |
| Bandwidth in bps (1 - 10000000 bps): | |
| Queue Limit Weight (1 - 100): | 20 |
| Queue Number: | Priority Queue |

Note: * - Required Field

**Step 9** From the Edit Service Class window, enter the QoS parameters 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 Ethernet QoS Policy Entry Fields, page 7-8.

**Step 10** Repeat Steps 7 and 8 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 11** Add another service class, if required. See Adding a Data Service Class, page 6-21.

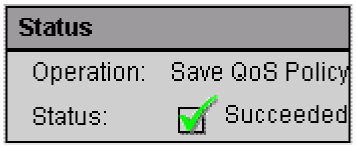
**Step 12** Delete any service class that you do not require for this QoS policy. See Deleting a Service Class, page 6-21.

**Step 13** After you edit and create the required service classes, 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 7-8).

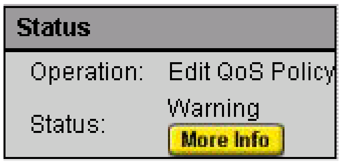
***Figure 7-8 Save is Successful***



Status
Operation: Save QoS Policy
Status: ✓ Succeeded

**b.** Policy is in use and cannot be edited or deleted (Figure 7-9). To read the warning message, click **More Info** and take the necessary action to resolve the issue.

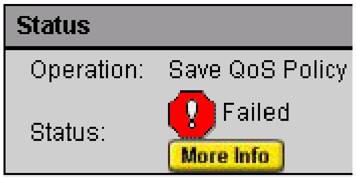
***Figure 7-9 Edit QoS Policy with Warning***



Status
Operation: Edit QoS Policy
Status: Warning

**c.** Save QoS policy failed (Figure 7-10). Click **More Info** to determine the source of the problem. You must fix all errors and resave before you can continue.

***Figure 7-10 Save Unsuccessful***



Status
Operation: Save QoS Policy
Status: ! Failed

**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.

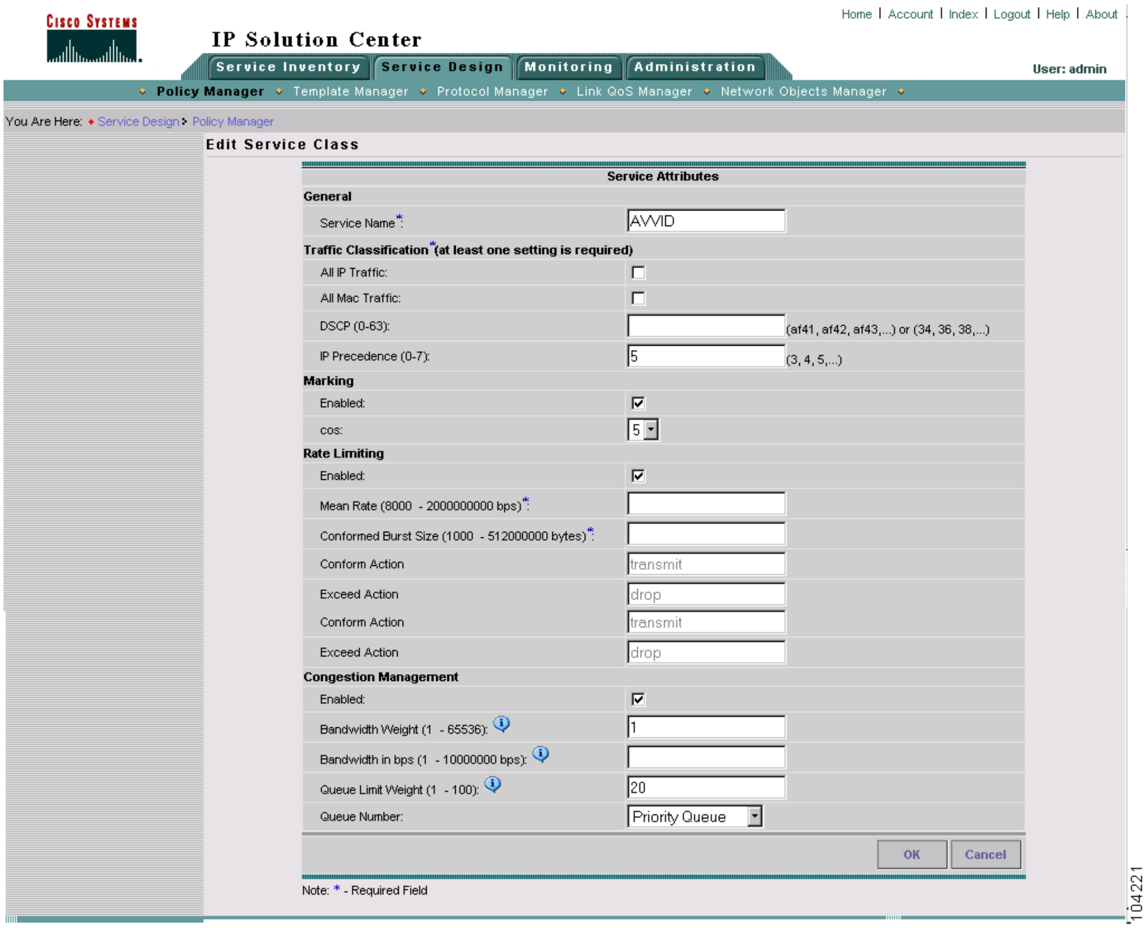
# Service Level Ethernet QoS Policy Entry Fields

The service level Ethernet QoS policy contains entry fields on the service class windows and dialog boxes. These include all entry fields in the Architecture for Voice, Video and Integrated Data (AVVID), Call Control, Business Critical, and Best Effort service classes.

All the Ethernet QoS service classes have the same set of entry fields, including newly created service classes.

The window you see depends on the service class being edited. Figure 7-11 and Figure 7-12 show the Edit Service Class window for the AVVID service class.

***Figure 7-11 Edit Ethernet QoS Service Class***



Edit Service Class

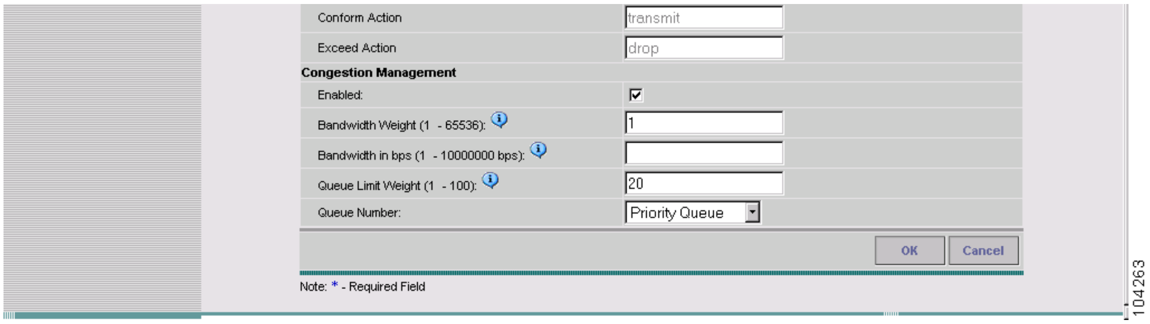
Service Attributes

| | | |
|---|---|---|
| **General** | | |
| Service Name*: | AVVID | |
| **Traffic Classification*(at least one setting is required)** | | |
| All IP Traffic: | □ | |
| All Mac Traffic: | □ | |
| DSCP (0-63): | | (af41, af42, af43,...) or (34, 36, 38,...) |
| IP Precedence (0-7): | 5 | (3, 4, 5,...) |
| **Marking** | | |
| Enabled: | ☑ | |
| cos: | 5 | |
| **Rate Limiting** | | |
| Enabled: | ☑ | |
| Mean Rate (8000 - 2000000000 bps)*: | | |
| Conformed Burst Size (1000 - 512000000 bytes)*: | | |
| Conform Action | transmit | |
| Exceed Action | drop | |
| Conform Action | transmit | |
| Exceed Action | drop | |
| **Congestion Management** | | |
| Enabled: | ☑ | |
| Bandwidth Weight (1 - 65536): | 1 | |
| Bandwidth in bps (1 - 10000000 bps): | | |
| Queue Limit Weight (1 - 100): | 20 | |
| Queue Number: | Priority Queue | |

OK Cancel

Note: * - Required Field

*Figure 7-12 Edit Ethernet QoS Service Class (continued)*



| | |
|---|---|
| Conform Action | transmit |
| Exceed Action | drop |
| **Congestion Management** | |
| Enabled: | ☑ |
| Bandwidth Weight (1 - 65536): | 1 |
| Bandwidth in bps (1 - 10000000 bps): | |
| Queue Limit Weight (1 - 100): | 20 |
| Queue Number: | Priority Queue |

Note: * - Required Field

Table 7-1 describes the entry fields for the service classes.

*Table 7-1 Edit Ethernet Service Class Entry Fields*

| Entry Field | Description |
|---|---|
| **General** | |
| Service Name | The name of the service class (AVVID, CALL_CONTROL, BUSINESS_CRITICAL, BEST EFFORT, or the name of your choice). |
| **Traffic Classification** | |
| All IP Traffic | Select all IP traffic. |
| All Mac Traffic | Select all Mac traffic |
| DSCP (0-63) | Selects traffic classification based on the packet's DSCP value. |
| IP Precedence | Selects traffic classification based on the packet's IP Precedence value. |
| **Marking** | |
| Enabled | Enable packet marking. |
| cos | Select a class of service. The range is 0 to 7. |
| **Rate Limiting** | |
| Enabled | Enable rate limiting. |
| Mean Rate | The long-term average transmission rate. The range is 8000 to 2000000000 bps. |
| Conformed Burst Size | The maximum size that traffic bursts can be before some traffic exceeds the rate limit. The range is 1000-512000000 bps. |
| Conform Action | The action to take on packets that conform to the specified rate limit. The default for Ethernet QoS is **transmit**—Sends the packet. |
| Exceed Action | The action to take on packets that exceed the specified rate limit. The default for Ethernet QoS is **drop**—drop the packet. |
| **Congestion Management** | |
| Enabled | Enable congestion management parameters. |
| Bandwidth Weight | The bandwidth guarantee for this service class. The range is 1 to 65536. This parameter is for the Catalyst 3550 switch only. |

*Table 7-1 Edit Ethernet Service Class Entry Fields (continued)*

| Entry Field | Description |
|---|---|
| Bandwidth in bps | The bandwidth in bps for this service class. The range is 1 to 10000000 bps. This parameter is for the Catalyst 4x00 switch only. |
| Queue Limit Weight | Limit the queue depth of the congesting traffic. The range is 1 to 100. This parameter is for the Catalyst 3550 switch only. |
| Queue Number | Choose a queue number from the drop-down menu. The choices are: 1, 2, Voice Ctrl Queue, or Priority queue. |

# Ethernet QoS for L2VPN, VPLS, and Layer 2 Access into MPLS VPN

This section describes how to apply QoS parameters to an existing Ethernet (L2VPN, MPLS, or VPLS) service request.

**Note** Layer 2 access into the MPLS VPN service is a specialized service within MPLS VPN. See *Cisco IP Solution Center MPLS VPN User Guide, 4.0* for more information.

## Checking Prerequisites

Before you can apply QoS parameters to an Ethernet network, you must already have:

- An existing Ethernet QoS policy.
- An existing L2VPN, MPLS, or VPLS service request. This service request can either be in the *Requested*, *Deployed*, or *Failed Deployed* state. However, we recommend that you use an L2VPN, MPLS, or VPLS service request that is in the *Deployed* state because the QoS service request might rely on port/interface configuration from the L2VPN, MPLS, or VPLS service request.

  See *Cisco IP Solution Center L2VPN User Guide, 4.0* for more information on creating L2VPN and VPLS service requests.

## Creating a QoS Service Request from an L2VPN, MPLS, or VPLS Service Request

The steps for creating an Ethernet QoS service request are as follows:

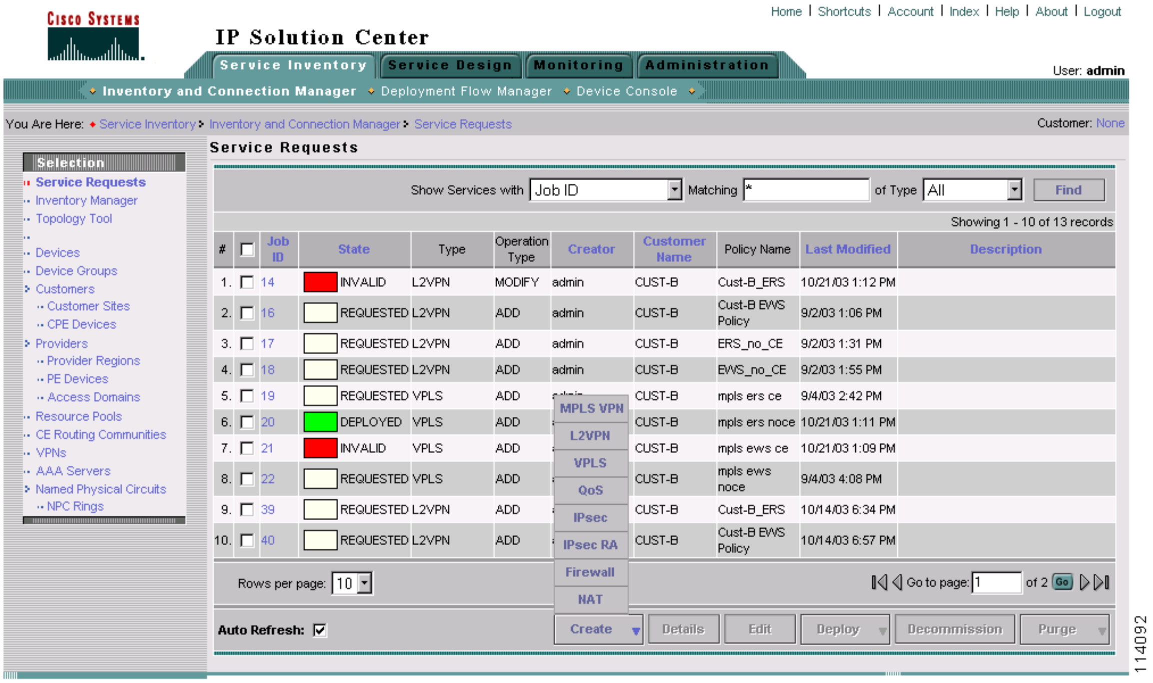
- Create a Ethernet QoS Policy as described in Service Level Ethernet QoS Policy, page 7-1.
- Create a QoS service request.
- Select a customer.
- Select a service request for L2VPN, MPLS, or VPLS (the service request must already exist)
- Select a QoS Policy (created in Step 1 above).
- Save the service request.

- Deploy the service request.

Use the following procedure to create a QoS service request from an L2VPN, MPLS, or VPLS Service Request:

**Step 1** Select **Service Inventory > Inventory and Connection Manager > Service Request**. The Service Requests window appears (Figure 7-13).

***Figure 7-13 Service Requests List***



User: admin

You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests

Customer: None

Service Requests

Show Services with Job ID Matching * of Type All

Showing 1 - 10 of 13 records

| # | ☐ | Job ID | State | Type | Operation Type | Creator | Customer Name | Policy Name | Last Modified | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | ☐ | 14 | 🟥 INVALID | L2VPN | MODIFY | admin | CUST-B | Cust-B_ERS | 10/21/03 1:12 PM | |
| 2. | ☐ | 16 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B EWS Policy | 9/2/03 1:06 PM | |
| 3. | ☐ | 17 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | ERS_no_CE | 9/2/03 1:31 PM | |
| 4. | ☐ | 18 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | EWS_no_CE | 9/2/03 1:55 PM | |
| 5. | ☐ | 19 | □ REQUESTED | VPLS | ADD | admin | CUST-B | mpls ers ce | 9/4/03 2:42 PM | |
| 6. | ☐ | 20 | 🟩 DEPLOYED | VPLS | ADD | [illegible] | CUST-B | mpls ers noce | 10/21/03 1:11 PM | |
| 7. | ☐ | 21 | 🟥 INVALID | VPLS | ADD | [illegible] | CUST-B | mpls ews ce | 10/21/03 1:09 PM | |
| 8. | ☐ | 22 | □ REQUESTED | VPLS | ADD | [illegible] | CUST-B | mpls ews noce | 9/4/03 4:08 PM | |
| 9. | ☐ | 39 | □ REQUESTED | L2VPN | ADD | [illegible] | CUST-B | Cust-B_ERS | 10/14/03 6:34 PM | |
| 10. | ☐ | 40 | □ REQUESTED | L2VPN | ADD | [illegible] | CUST-B | Cust-B EWS Policy | 10/14/03 6:57 PM | |

Rows per page: 10

Go to page: 1 of 2

Auto Refresh: ☑

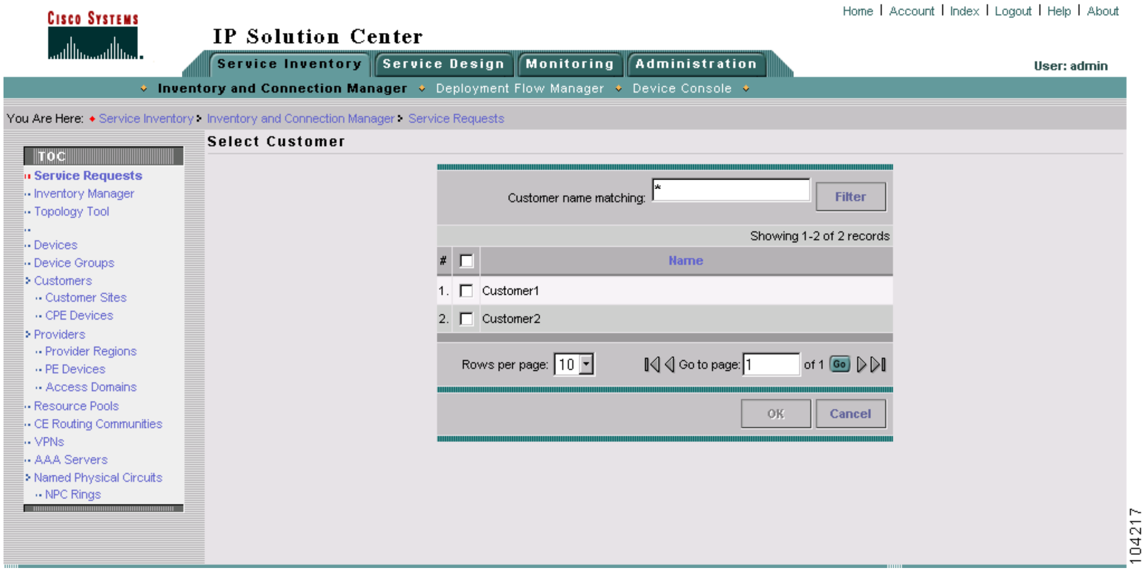
The Service Requests window lists the current list of service requests for this user name.

**Note** For more information on service requests, see QoS Service Requests, page 8-3.

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

**Step 3** Select the customer for this QoS service request and click **OK** (Figure 7-14).

*Figure 7-14 Select Customer*



Select Customer

Customer name matching: *

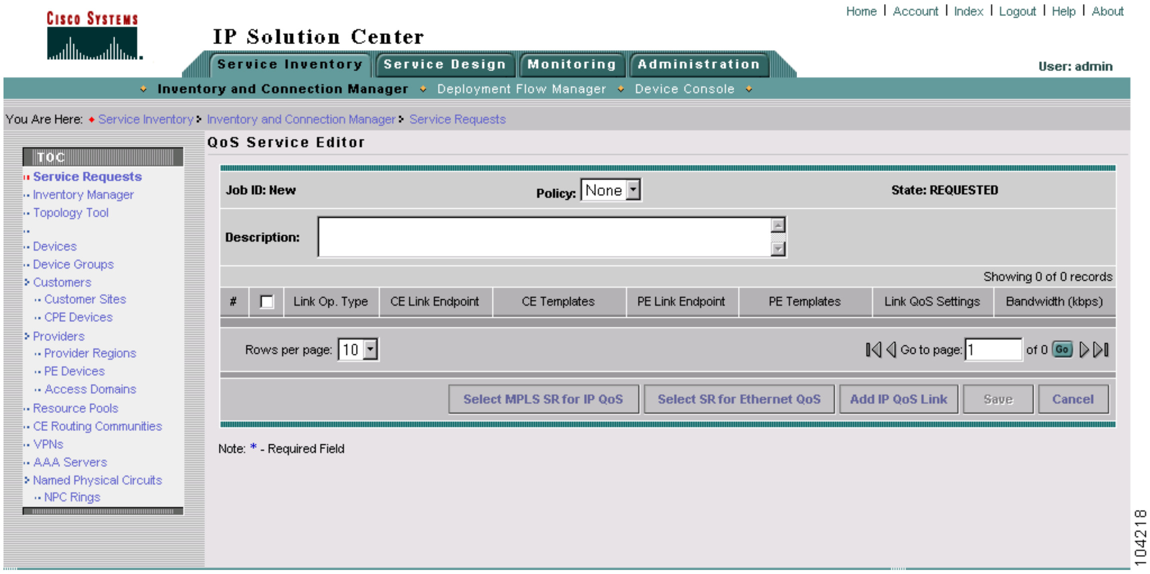
Showing 1-2 of 2 records

| # | □ | Name |
|---|---|---|
| 1. | □ | Customer1 |
| 2. | □ | Customer2 |

Rows per page: 10 Go to page: 1 of 1

The QoS Service Editor window appears (Figure 7-15).

*Figure 7-15 QoS Service Editor*



QoS Service Editor

Job ID: New Policy: None State: REQUESTED

Description:

Showing 0 of 0 records

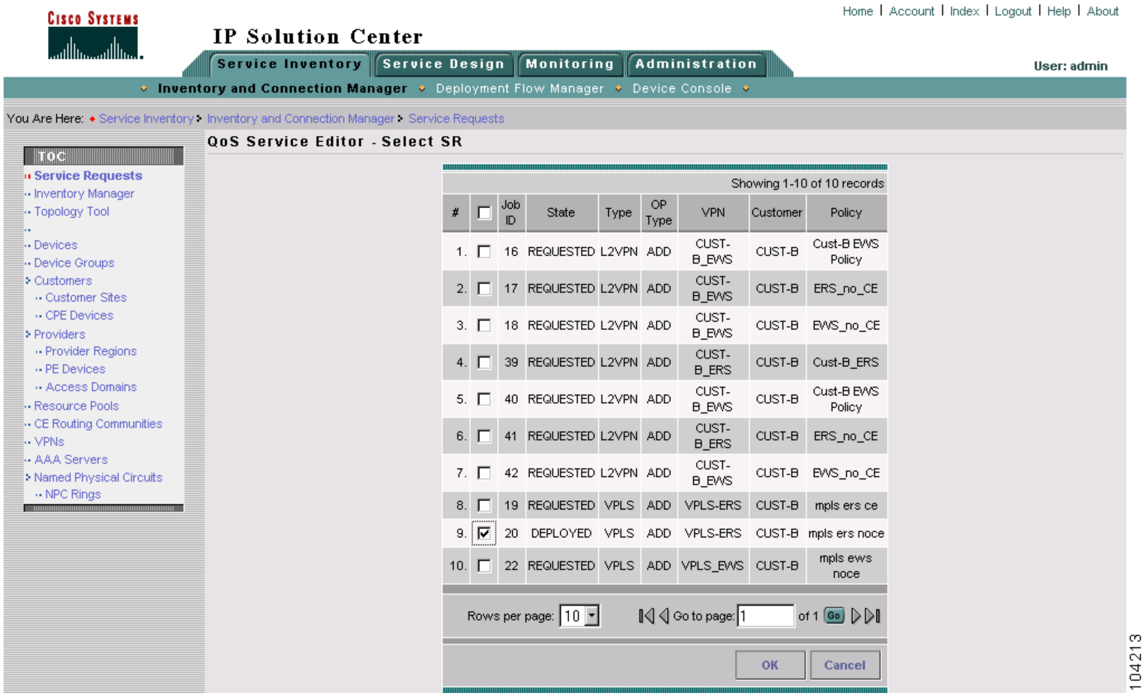
| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|

Rows per page: 10 Go to page: 1 of 0

Note: * - Required Field

**Step 4** Click **Select SR for Ethernet QoS**. The QoS Service Editor–Select SR window appears (Figure 7-16).

*Figure 7-16 Select L2VPN Service Request for QoS*



QoS Service Editor - Select SR

Showing 1-10 of 10 records

| # | □ | Job ID | State | Type | OP Type | VPN | Customer | Policy |
|---|---|---|---|---|---|---|---|---|
| 1. | □ | 16 | REQUESTED | L2VPN | ADD | CUST-B_EWS | CUST-B | Cust-B EWS Policy |
| 2. | □ | 17 | REQUESTED | L2VPN | ADD | CUST-B_EWS | CUST-B | ERS_no_CE |
| 3. | □ | 18 | REQUESTED | L2VPN | ADD | CUST-B_EWS | CUST-B | EWS_no_CE |
| 4. | □ | 39 | REQUESTED | L2VPN | ADD | CUST-B_ERS | CUST-B | Cust-B_ERS |
| 5. | □ | 40 | REQUESTED | L2VPN | ADD | CUST-B_EWS | CUST-B | Cust-B EWS Policy |
| 6. | □ | 41 | REQUESTED | L2VPN | ADD | CUST-B_ERS | CUST-B | ERS_no_CE |
| 7. | □ | 42 | REQUESTED | L2VPN | ADD | CUST-B_EWS | CUST-B | EWS_no_CE |
| 8. | □ | 19 | REQUESTED | VPLS | ADD | VPLS-ERS | CUST-B | mpls ers ce |
| 9. | ☑ | 20 | DEPLOYED | VPLS | ADD | VPLS-ERS | CUST-B | mpls ers noce |
| 10. | □ | 22 | REQUESTED | VPLS | ADD | VPLS_EWS | CUST-B | mpls ews noce |

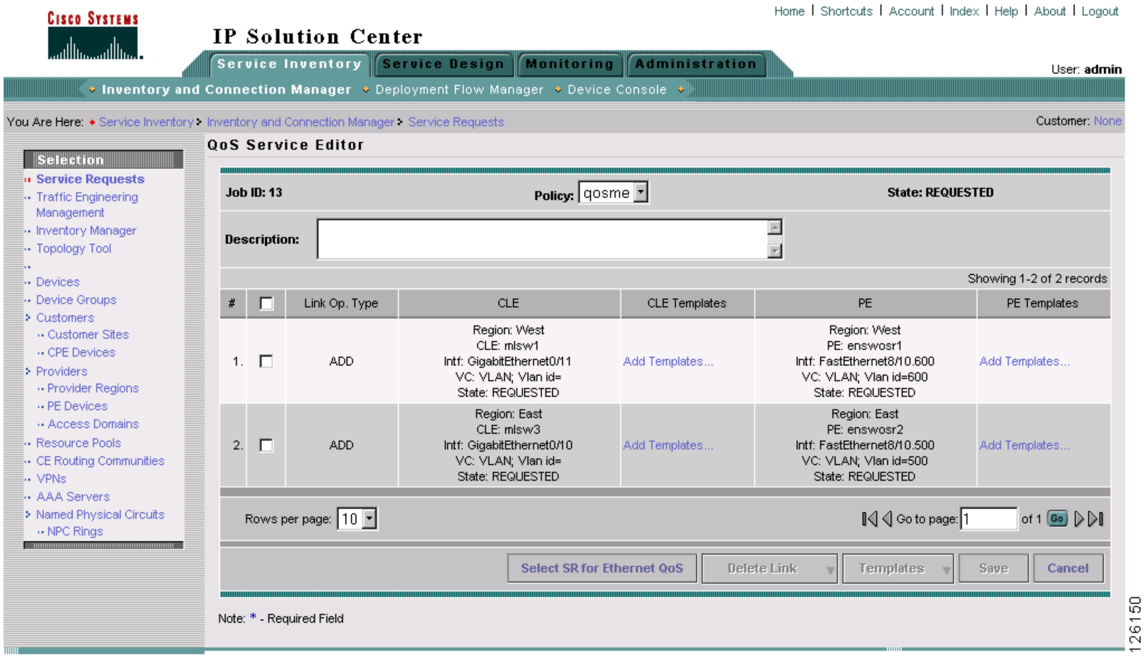
Rows per page: 10 Go to page: 1 of 1 Go

OK Cancel

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

**Step 5** Select an existing service request and click **OK**. The QoS Service Editor window appears (Figure 7-17).

*Figure 7-17 QoS Service Editor*



QoS Service Editor

Job ID: 13 Policy: qosme State: REQUESTED

Description:

Showing 1-2 of 2 records

| # | □ | Link Op. Type | CLE | CLE Templates | PE | PE Templates |
|---|---|---|---|---|---|---|
| 1. | □ | ADD | Region: West<br>CLE: mlsw1<br>Intf: GigabitEthernet0/11<br>VC: VLAN; Vlan id=<br>State: REQUESTED | Add Templates... | Region: West<br>PE: enswosr1<br>Intf: FastEthernet8/10.600<br>VC: VLAN; Vlan id=600<br>State: REQUESTED | Add Templates... |
| 2. | □ | ADD | Region: East<br>CLE: mlsw3<br>Intf: GigabitEthernet0/10<br>VC: VLAN; Vlan id=<br>State: REQUESTED | Add Templates... | Region: East<br>PE: enswosr2<br>Intf: FastEthernet8/10.500<br>VC: VLAN; Vlan id=500<br>State: REQUESTED | Add Templates... |

Rows per page: 10 Go to page: 1 of 1 Go

Select SR for Ethernet QoS | Delete Link | Templates | Save | Cancel

Note: * - Required Field

This window lists the QoS links and includes the following information about the CLE-PE link:

- Link Op. Type—The link operation type for this CLE-PE link. For example, ADD means that you are adding this link to the service request.
- CLE—The CLE (customer location equipment) device interface. CLE refers to a switch for the L2VPN link.
- CLE Templates —Associate a template with the CLE device. See *Cisco IP Solution Center Infrastructure Reference, 4.0* for information on creating templates
- PE—The PE device interface.
- PE Templates —Associate a template with the PE device. See *Cisco IP Solution Center Infrastructure Reference, 4.0* for information on creating templates

**Note** Templates enable additional commands that are not specifically associated with the service request to be included in the provisioning (download).

For more information on L2VPN and VPLS provisioning, see *Cisco IP Solution Center L2VPN User Guide, 4.0*. For more information on MPLS VPN provisioning, see *Cisco IP Solution Center MPLS VPN User Guide, 4.0*.

From this window you can delete links.

**Step 6** Select a Policy from the **Policy** drop-down menu.

**Step 7** Click **Save SR** to save the QoS service request.

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 successfully audited, the QoS service request enters the *Deployed* state.

# 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.

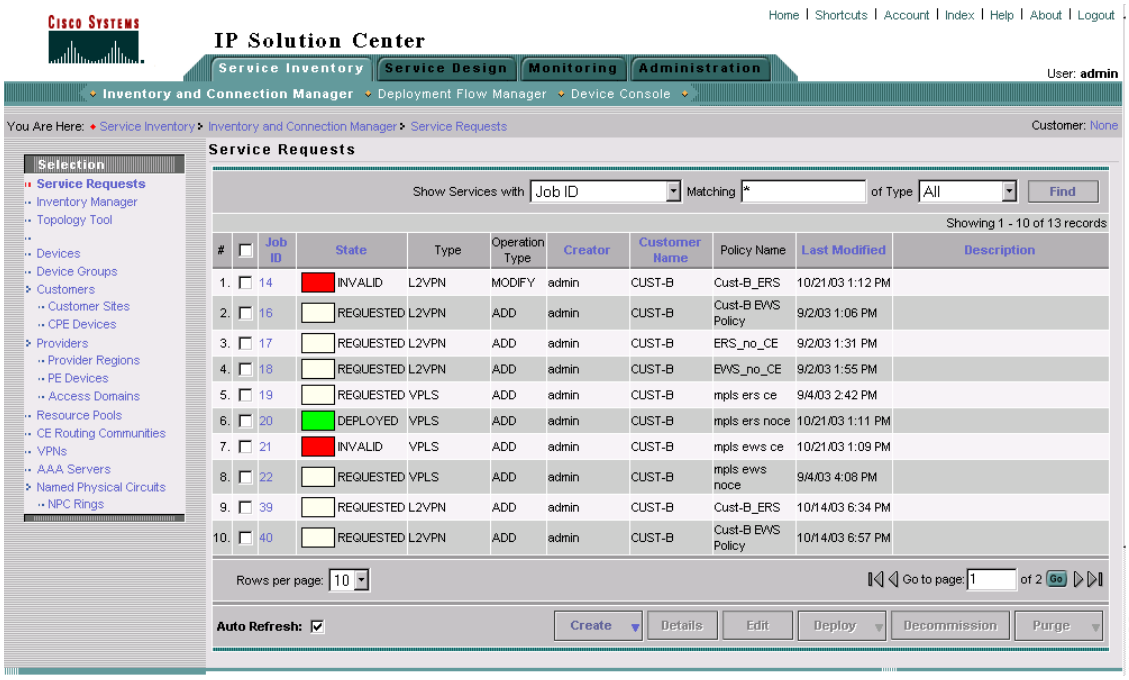
  See *Cisco IP Solution Center MPLS VPN User Guide, 4.0* for more information on creating MPLS service requests.
- Select the Mark MPLS Exp. check box for the QoS policy. This is configured for the QoS service level policy on the Edit QoS Policy window. See Creating the Service Level IP QoS Policy, page 5-10 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 Request**. The Service Request window appears. (Figure 7-18).

***Figure 7-18 Service Requests List***



User: admin

You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests

Customer: None

Service Requests

Show Services with Job ID Matching * of Type All

Showing 1 - 10 of 13 records

| # | □ | Job ID | State | Type | Operation Type | Creator | Customer Name | Policy Name | Last Modified | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | □ | 14 | 🟥 INVALID | L2VPN | MODIFY | admin | CUST-B | Cust-B_ERS | 10/21/03 1:12 PM | |
| 2. | □ | 16 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B EWS Policy | 9/2/03 1:06 PM | |
| 3. | □ | 17 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | ERS_no_CE | 9/2/03 1:31 PM | |
| 4. | □ | 18 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | EWS_no_CE | 9/2/03 1:55 PM | |
| 5. | □ | 19 | □ REQUESTED | VPLS | ADD | admin | CUST-B | mpls ers ce | 9/4/03 2:42 PM | |
| 6. | □ | 20 | 🟩 DEPLOYED | VPLS | ADD | admin | CUST-B | mpls ers noce | 10/21/03 1:11 PM | |
| 7. | □ | 21 | 🟥 INVALID | VPLS | ADD | admin | CUST-B | mpls ews ce | 10/21/03 1:09 PM | |
| 8. | □ | 22 | □ REQUESTED | VPLS | ADD | admin | CUST-B | mpls ews noce | 9/4/03 4:08 PM | |
| 9. | □ | 39 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B_ERS | 10/14/03 6:34 PM | |
| 10. | □ | 40 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B EWS Policy | 10/14/03 6:57 PM | |

Rows per page: 10

Go to page: 1 of 2 Go

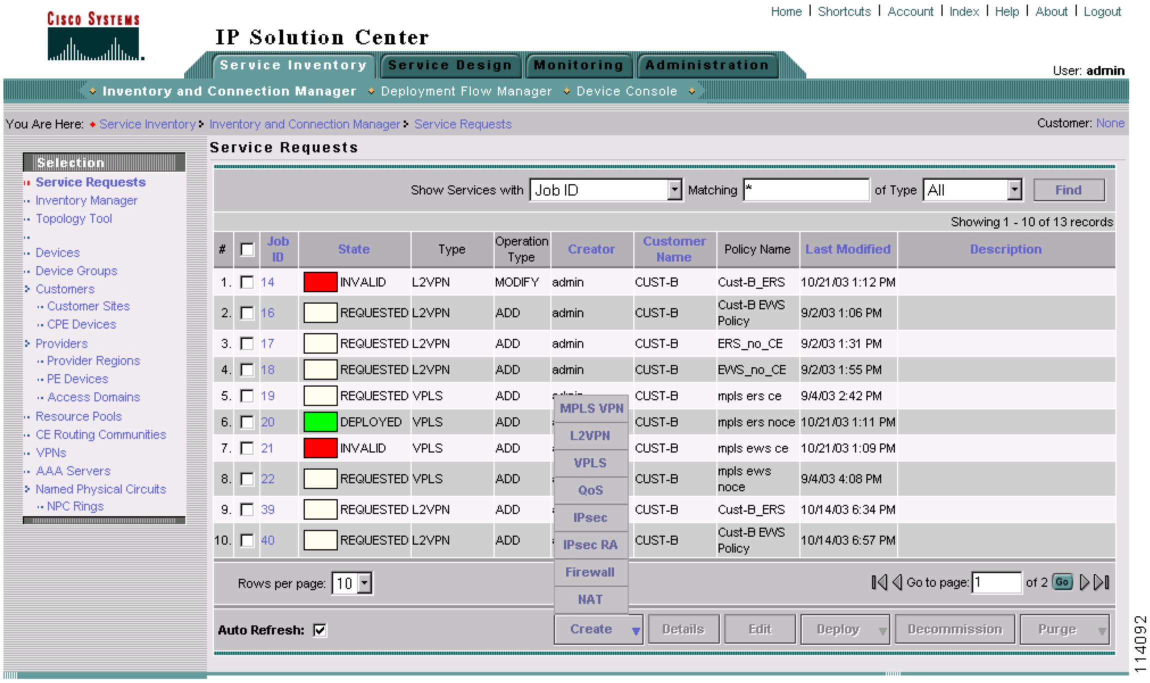
Auto Refresh: ☑

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

**Note** For more information on service requests, see QoS Service Requests, page 8-3.

**Step 2** From the Service Requests window, click **Create** and choose **QoS** (Figure 7-19).

*Figure 7-19 Create QoS Service Request*



You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests

Customer: None

**Service Requests**

Show Services with: Job ID  Matching: *  of Type: All

Showing 1 - 10 of 13 records

| # | □ | Job ID | State | Type | Operation Type | Creator | Customer Name | Policy Name | Last Modified | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | □ | 14 | 🟥 INVALID | L2VPN | MODIFY | admin | CUST-B | Cust-B_ERS | 10/21/03 1:12 PM | |
| 2. | □ | 16 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B EWS Policy | 9/2/03 1:06 PM | |
| 3. | □ | 17 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | ERS_no_CE | 9/2/03 1:31 PM | |
| 4. | □ | 18 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | EWS_no_CE | 9/2/03 1:55 PM | |
| 5. | □ | 19 | □ REQUESTED | VPLS | ADD | admin | CUST-B | mpls ers ce | 9/4/03 2:42 PM | |
| 6. | □ | 20 | 🟩 DEPLOYED | VPLS | ADD | a | CUST-B | mpls ers noce | 10/21/03 1:11 PM | |
| 7. | □ | 21 | 🟥 INVALID | VPLS | ADD | a | CUST-B | mpls ews ce | 10/21/03 1:09 PM | |
| 8. | □ | 22 | □ REQUESTED | VPLS | ADD | a | CUST-B | mpls ews noce | 9/4/03 4:08 PM | |
| 9. | □ | 39 | □ REQUESTED | L2VPN | ADD | a | CUST-B | Cust-B_ERS | 10/14/03 6:34 PM | |
| 10. | □ | 40 | □ REQUESTED | L2VPN | ADD | a | CUST-B | Cust-B EWS Policy | 10/14/03 6:57 PM | |

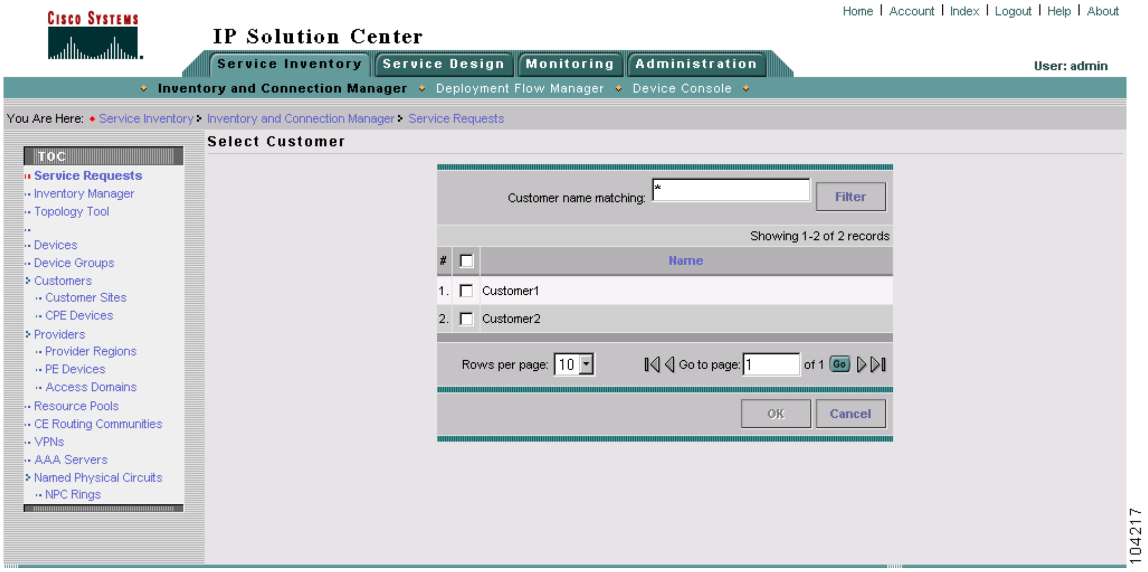
Rows per page: 10  Go to page: 1 of 2

Auto Refresh: ☑

The Select Customer window appears as shown in Figure 7-20.

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

*Figure 7-20 Select Customer*



You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests

**Select Customer**

Customer name matching: *

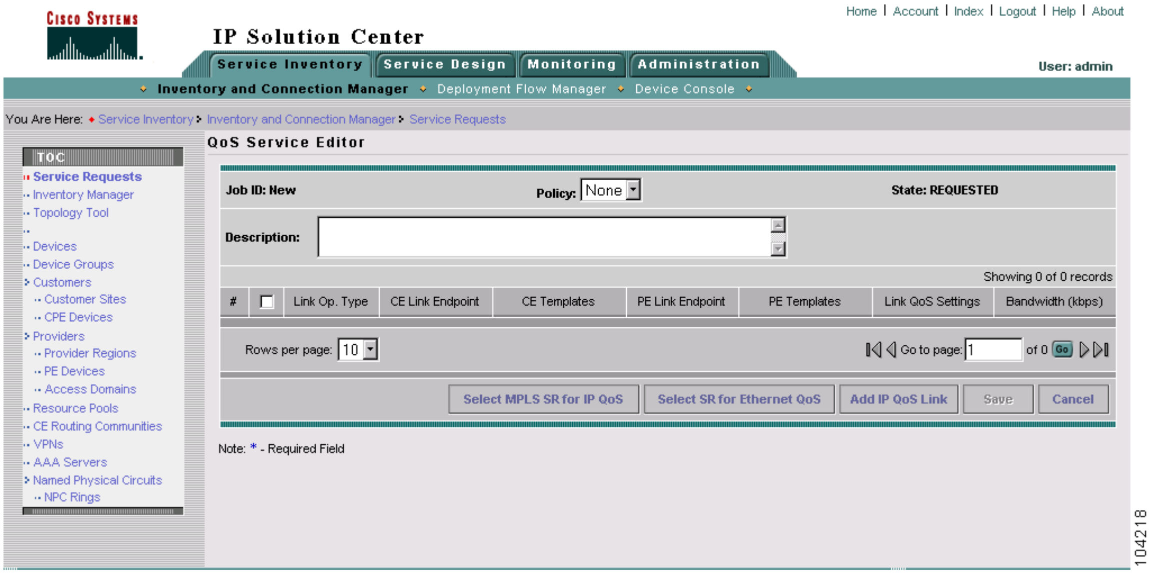
Showing 1-2 of 2 records

| # | □ | Name |
|---|---|---|
| 1. | □ | Customer1 |
| 2. | □ | Customer2 |

Rows per page: 10  Go to page: 1 of 1

The QoS Service Editor window appears (Figure 7-21).

*Figure 7-21 QoS Service Editor*



QoS Service Editor

Job ID: New Policy: None State: REQUESTED

Description:

Showing 0 of 0 records

| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|

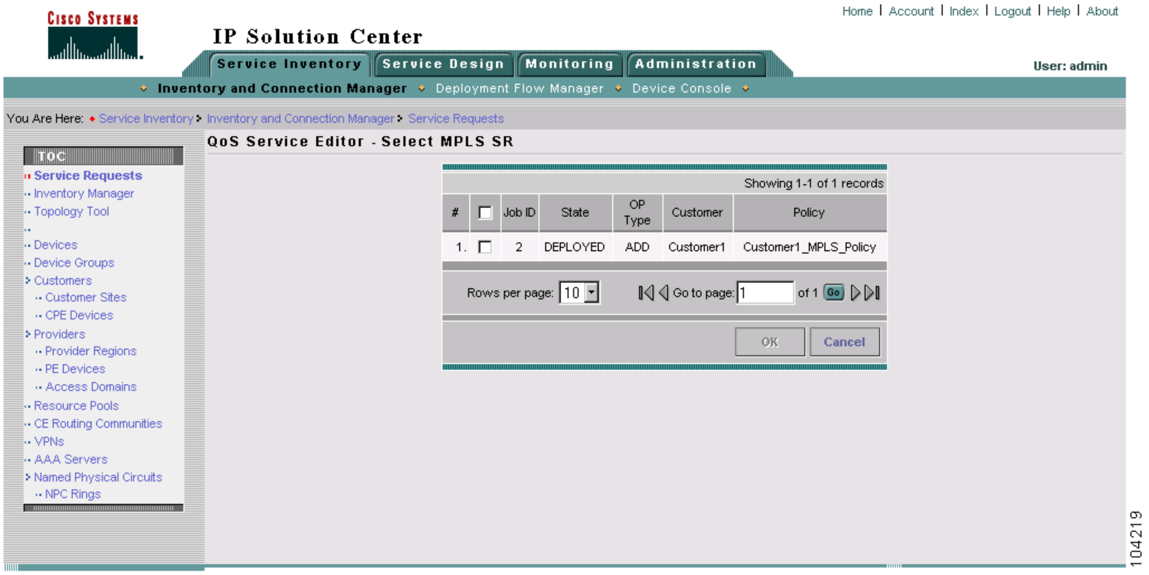
Note: * - Required Field

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

- Link Op. Type—The link operation type for this CPE-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, 4.0* 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, 4.0* for information on creating templates
- Link QoS Settings—Previously configured link QoS setting to use for this CPE-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 7-22).

*Figure 7-22 Select MPLS Service Request for QoS*



QoS Service Editor - Select MPLS SR

Showing 1-1 of 1 records

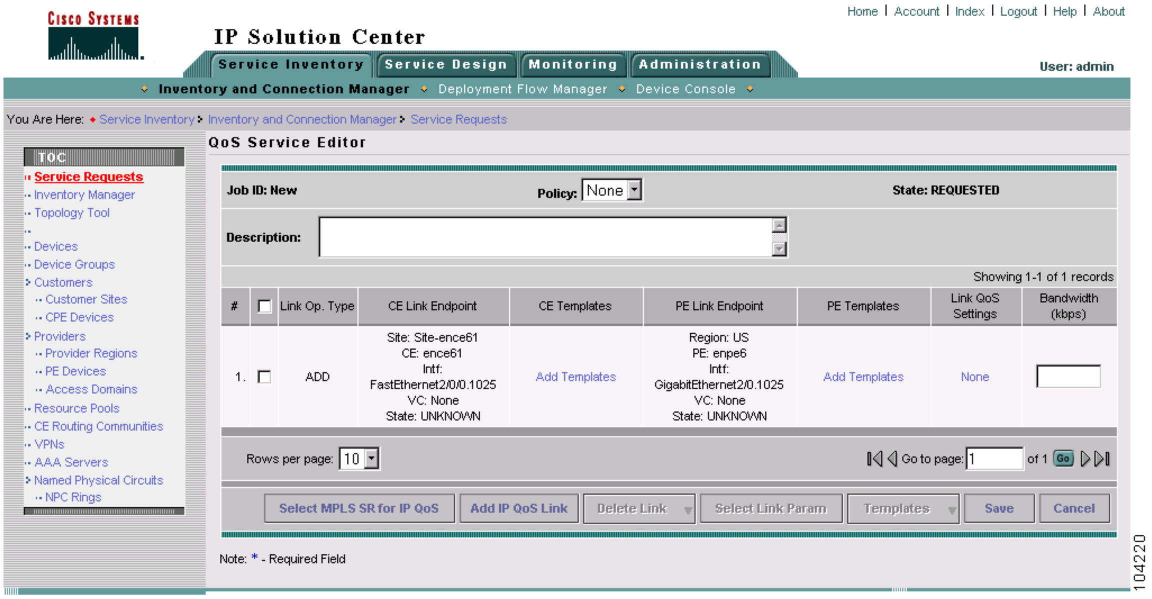
| # | □ | Job ID | State | OP Type | Customer | Policy |
|---|---|---|---|---|---|---|
| 1. | □ | 2 | DEPLOYED | ADD | Customer1 | Customer1_MPLS_Policy |

Rows per page: 10 Go to page: 1 of 1

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 7-23).

*Figure 7-23 QoS Service Editor*



QoS Service Editor

Job ID: New Policy: None State: REQUESTED

Description:

Showing 1-1 of 1 records

| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|
| 1. | □ | ADD | Site: Site-ence61<br>CE: ence61<br>Intf: FastEthernet2/0/0.1025<br>VC: None<br>State: UNKNOWN | Add Templates | Region: US<br>PE: enpe6<br>Intf: GigabitEthernet2/0.1025<br>VC: None<br>State: UNKNOWN | Add Templates | None | |

Rows per page: 10 Go to page: 1 of 1

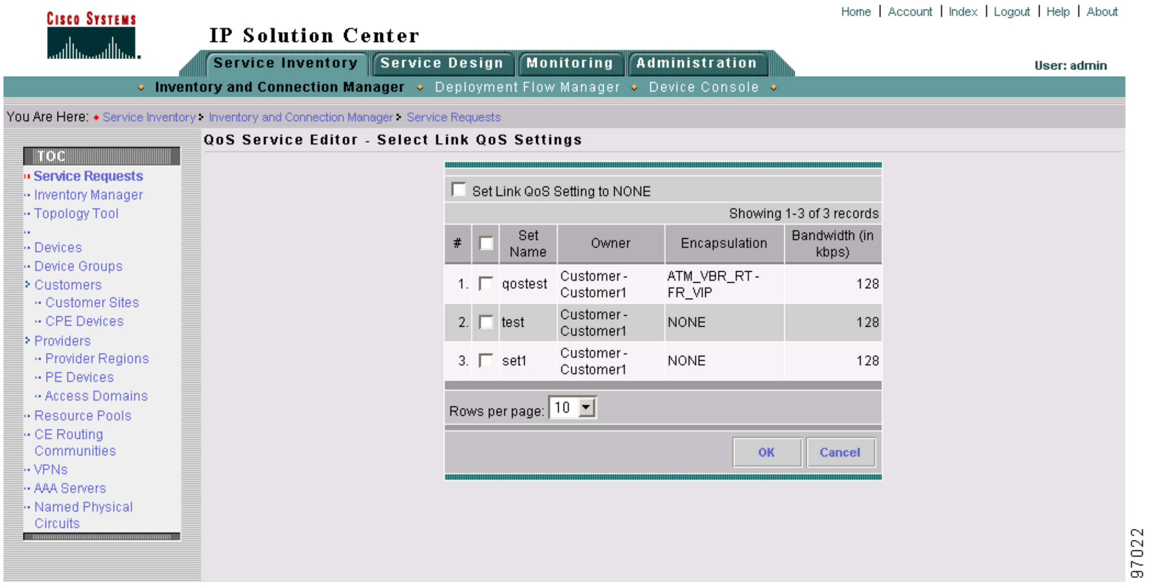
Note: * - Required Field

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, 4.0*.

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 Param**. Alternately, you can click **None** in the Link QoS Settings column. The QoS Service Editor–Select Link QoS settings appears (Figure 7-24).

*Figure 7-24 QoS Service Editor Select—Link QoS Settings*



QoS Service Editor - Select Link QoS Settings

□ Set Link QoS Setting to NONE

Showing 1-3 of 3 records

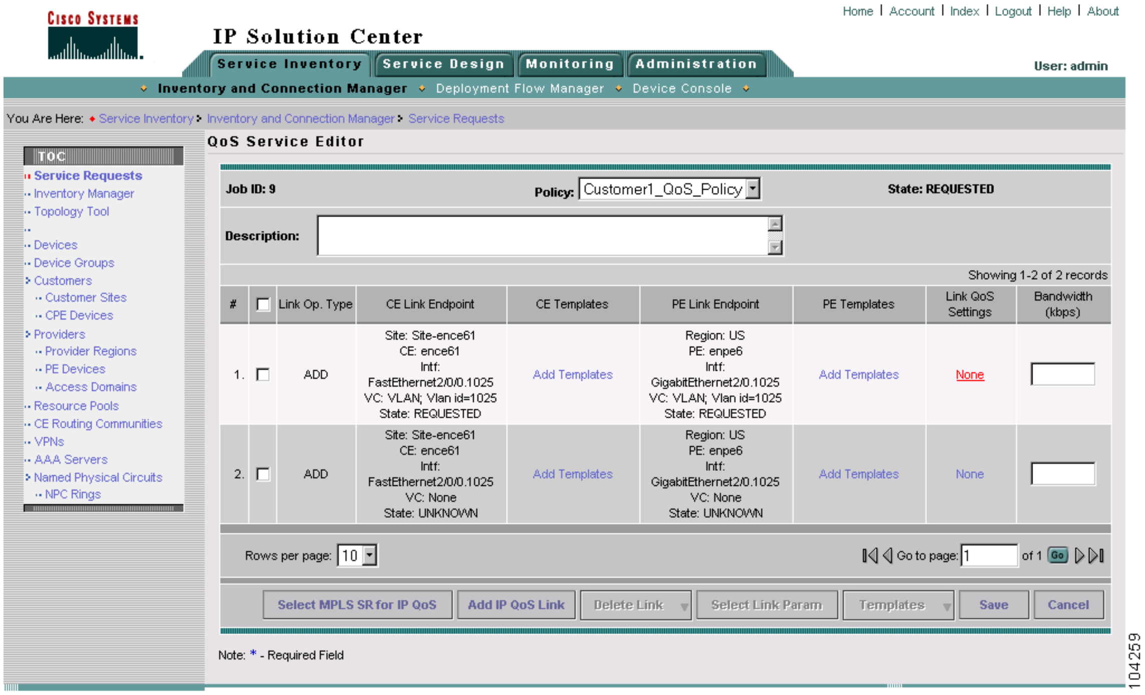
| # | □ | Set Name | Owner | Encapsulation | Bandwidth (in kbps) |
|---|---|---|---|---|---|
| 1. | □ | qostest | Customer - Customer1 | ATM_VBR_RT - FR_VIP | 128 |
| 2. | □ | test | Customer - Customer1 | NONE | 128 |
| 3. | □ | set1 | Customer - Customer1 | NONE | 128 |

Rows per page: 10

This window lists all set names (link QoS settings) previously defined in the link level QoS policy. See Defining the Link Level QoS Policy, page 5-15 for more information.

**Step 7** Select the link QoS setting (set name) to apply to this CPE-PE link and click **OK**. You return to the QoS Service Editor window (Figure 7-25).

*Figure 7-25 Completed QoS SR from MPLS SR*



You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests

QoS Service Editor

Job ID: 9 Policy: Customer1_QoS_Policy State: REQUESTED

Description:

Showing 1-2 of 2 records

| # | □ | Link Op. Type | CE Link Endpoint | CE Templates | PE Link Endpoint | PE Templates | Link QoS Settings | Bandwidth (kbps) |
|---|---|---|---|---|---|---|---|---|
| 1. | □ | ADD | Site: Site-ence61<br>CE: ence61<br>Intf: FastEthernet2/0/0.1025<br>VC: VLAN; Vlan id=1025<br>State: REQUESTED | Add Templates | Region: US<br>PE: enpe6<br>Intf: GigabitEthernet2/0.1025<br>VC: VLAN; Vlan id=1025<br>State: REQUESTED | Add Templates | None | |
| 2. | □ | ADD | Site: Site-ence61<br>CE: ence61<br>Intf: FastEthernet2/0/0.1025<br>VC: None<br>State: UNKNOWN | Add Templates | Region: US<br>PE: enpe6<br>Intf: GigabitEthernet2/0.1025<br>VC: None<br>State: UNKNOWN | Add Templates | None | |

Rows per page: 10 Go to page: 1 of 1 Go

Note: * - Required Field

The CPE-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 8-3.

CHAPTER 8

# 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, page 8-1
- QoS Service Requests, page 8-3
- QoS Task Logs, page 8-14

## 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.

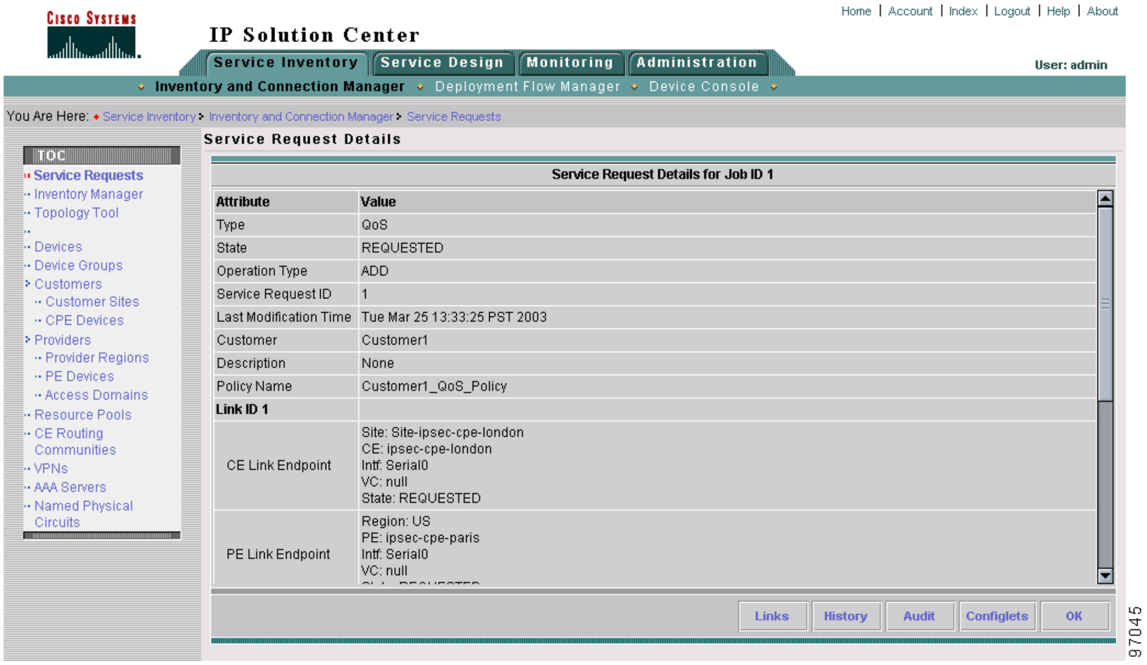
This section describes how to manually generate a configuration audit and view the audit report.

To manually generate a configuration audit:

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

**Step 2** Select a QoS service request for the configuration audit and click **Details**. The Service Request Details window appears as shown in Figure 8-1.

***Figure 8-1 Service Request Details***



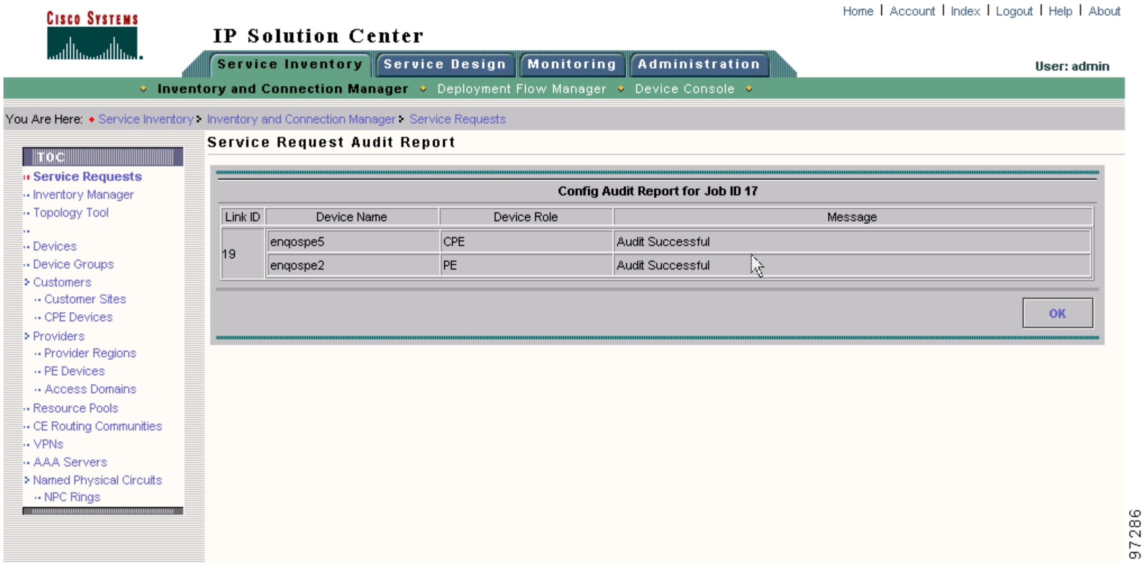
Service Request Details

Service Request Details for Job ID 1

| Attribute | Value |
|---|---|
| Type | QoS |
| State | REQUESTED |
| Operation Type | ADD |
| Service Request ID | 1 |
| Last Modification Time | Tue Mar 25 13:33:25 PST 2003 |
| Customer | Customer1 |
| Description | None |
| Policy Name | Customer1_QoS_Policy |
| **Link ID 1** | |
| CE Link Endpoint | Site: Site-ipsec-cpe-london<br>CE: ipsec-cpe-london<br>Intf: Serial0<br>VC: null<br>State: REQUESTED |
| PE Link Endpoint | Region: US<br>PE: ipsec-cpe-paris<br>Intf: Serial0<br>VC: null |

**Step 3** Click **Audit**. The Service Request Audit Report window appears. Figure 8-2 shows an example of a successful configuration audit.

***Figure 8-2 Service Request Audit Report—Successful***



Service Request Audit Report

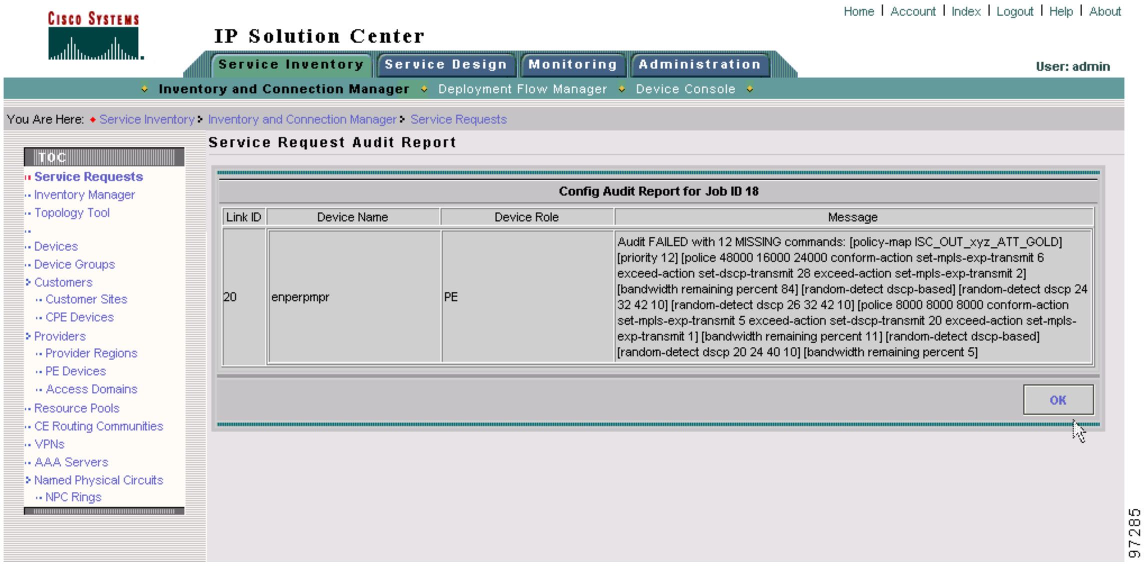
Config Audit Report for Job ID 17

| Link ID | Device Name | Device Role | Message |
|---|---|---|---|
| 19 | enqospe5 | CPE | Audit Successful |
| | enqospe2 | PE | Audit 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 8-3 shows an example of a failed audit message for a QoS service request.

*Figure 8-3 Service Request Audit Report—Failed*



Service Request Audit Report

Config Audit Report for Job ID 18

| Link ID | Device Name | Device Role | Message |
|---|---|---|---|
| 20 | enperpmpr | PE | Audit FAILED with 12 MISSING commands: [policy-map ISC_OUT_xyz_ATT_GOLD] [priority 12] [police 48000 16000 24000 conform-action set-mpls-exp-transmit 6 exceed-action set-dscp-transmit 28 exceed-action set-mpls-exp-transmit 2] [bandwidth remaining percent 84] [random-detect dscp-based] [random-detect dscp 24 32 42 10] [random-detect dscp 26 32 42 10] [police 8000 8000 8000 conform-action set-mpls-exp-transmit 5 exceed-action set-dscp-transmit 20 exceed-action set-mpls-exp-transmit 1] [bandwidth remaining percent 11] [random-detect dscp-based] [random-detect dscp 20 24 40 10] [bandwidth remaining percent 5] |

The audit failure message indicates missing commands and configuration issues. 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

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 8-4

Verifying QoS Service Requests, page 8-5

Service Request States, page 8-5

Service Request States, page 8-5

Changing Service Request Parameters, page 8-8

**Note** See Creating the QoS Service Request, page 5-18 and Deploying the QoS Service Request, page 5-26 for more information on the create and deploy operations.

# Managing QoS Service Requests

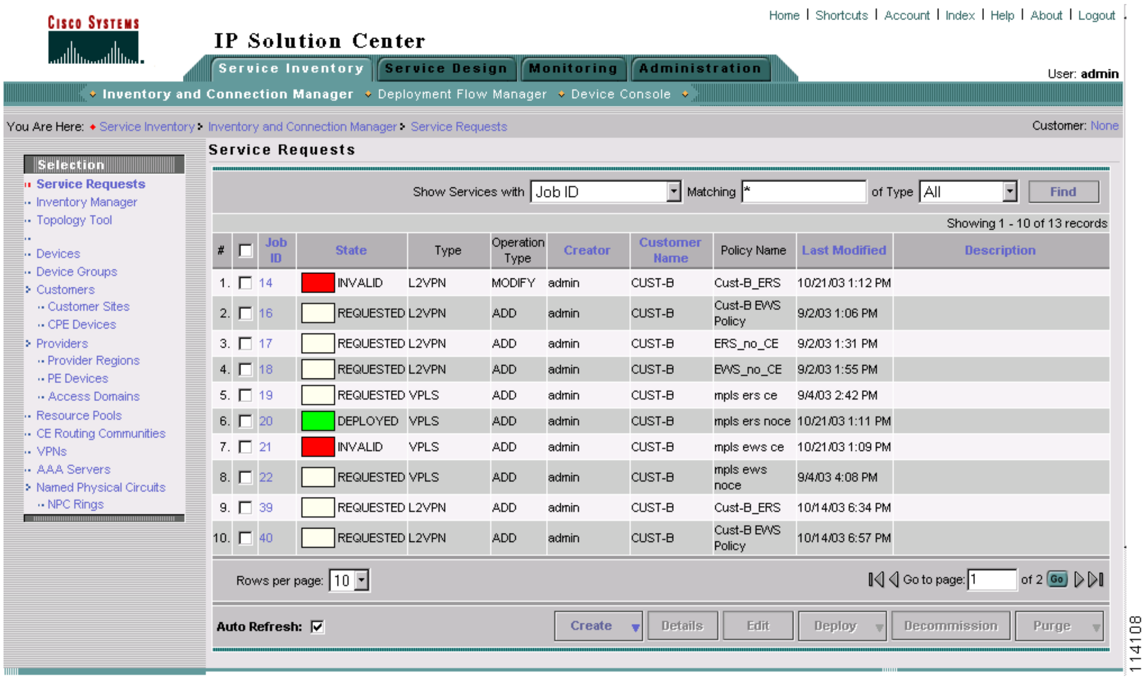
To manage QoS service request, select **Service Inventory > Inventory and Connection Manager > Service Requests**.

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

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

Figure 8-4 shows an example of the Service Requests window.

***Figure 8-4 Service Requests List***



Show Services with Job ID Matching * of Type All

Showing 1 - 10 of 13 records

| # | □ | Job ID | State | Type | Operation Type | Creator | Customer Name | Policy Name | Last Modified | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | □ | 14 | 🟥 INVALID | L2VPN | MODIFY | admin | CUST-B | Cust-B_ERS | 10/21/03 1:12 PM | |
| 2. | □ | 16 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B EWS Policy | 9/2/03 1:06 PM | |
| 3. | □ | 17 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | ERS_no_CE | 9/2/03 1:31 PM | |
| 4. | □ | 18 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | EWS_no_CE | 9/2/03 1:55 PM | |
| 5. | □ | 19 | □ REQUESTED | VPLS | ADD | admin | CUST-B | mpls ers ce | 9/4/03 2:42 PM | |
| 6. | □ | 20 | 🟩 DEPLOYED | VPLS | ADD | admin | CUST-B | mpls ers noce | 10/21/03 1:11 PM | |
| 7. | □ | 21 | 🟥 INVALID | VPLS | ADD | admin | CUST-B | mpls ews ce | 10/21/03 1:09 PM | |
| 8. | □ | 22 | □ REQUESTED | VPLS | ADD | admin | CUST-B | mpls ews noce | 9/4/03 4:08 PM | |
| 9. | □ | 39 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B_ERS | 10/14/03 6:34 PM | |
| 10. | □ | 40 | □ REQUESTED | L2VPN | ADD | admin | CUST-B | Cust-B EWS Policy | 10/14/03 6:57 PM | |

Rows per page: 10 Go to page: 1 of 2 Go

Auto Refresh: ☑

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

- JobID—The job number assigned to the service request by ISC. Table 8-1 describes ISC service request states.
- State—The transition state for the service request. See Service Request States, page 8-5 for more information.
- Type—The type of service request. For example, QoS, MPLS, IPsec, L2VPN, NAT, or Firewall. **- IPsec, NAT, and Firewall are not supported in this release. -**
- Operation Type—The operation type for the service request. For example, ADD means that you are adding this service request, and DELETE means 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 8-5 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 8-8 for more information.
- Task Logs—Access the task logs from the Monitoring tab to help you troubleshoot a failed service request or to view more details about a service request. See QoS Task Logs, page 8-14 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 8-1 describes the transition states for an ISC service request.

*Table 8-1* ***Cisco IP Solution Center Service Request States***

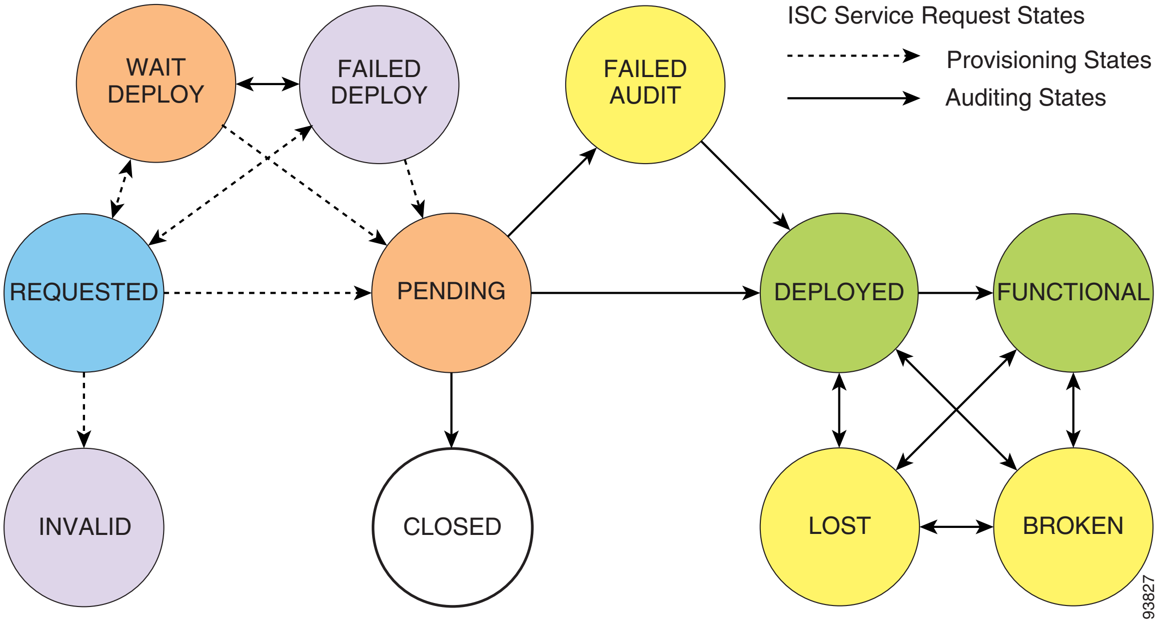
| Service Request Type | Description |
|---|---|
| **Requested** | If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains ***Requested***, the service is in an error state. |
| **Invalid** | ***Invalid*** indicates that the service request 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 engine cannot generate configuration updates to service this request. |
| **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.<br>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. |
| **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). |
| **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. |
| **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. Once a service request is deployed successfully, it cannot re-enter the ***Failed Audit*** state (except if the service request is redeployed). |
| **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. |
| **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***. |

*Table 8-1 Cisco IP Solution Center Service Request States (continued)*

| Service Request Type | Description |
|---|---|
| Functional<br>(does not apply to QoS service requests) | 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.<br>An IPsec service request moves to *Functional* when the auditor finds that the router is configured properly and the IPsec traffic is flowing (ping is used to determine if IPsec traffic is flowing). **- IPsec is not supported in this release. -** |
| Broken<br>(does not apply to QoS service requests) | The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example).<br>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.<br>An IPsec service request moves to ***Broken*** if a ping fails for all the remote peers of the current device. **- IPsec is not supported in this release. -** |
| **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. |

Figure 8-5 illustrates which service request states relate to the QoS configuration auditing process, and which states relate to the provisioning process.

*Figure 8-5 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 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.

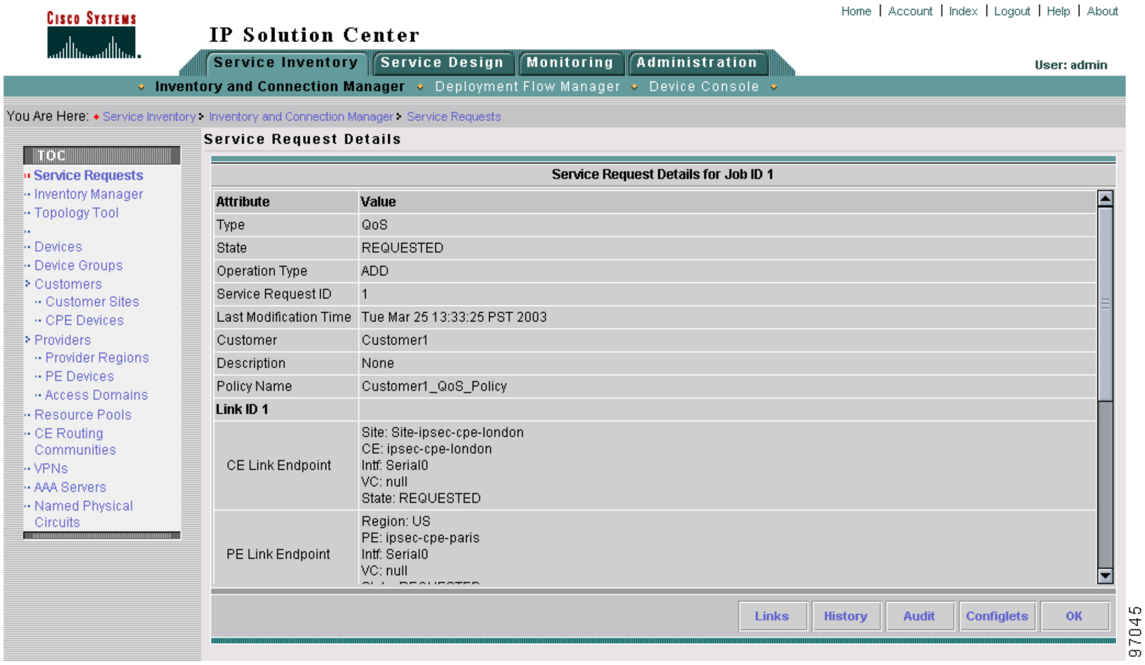
This section describes how to view the details of a QoS service request, including the history, link details, and QoS configlets.

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 8-6. See Figure 8-6 for Attribute details and Figure 8-7 for Link ID details.

*Figure 8-6 QoS Service Request Details—Attributes*



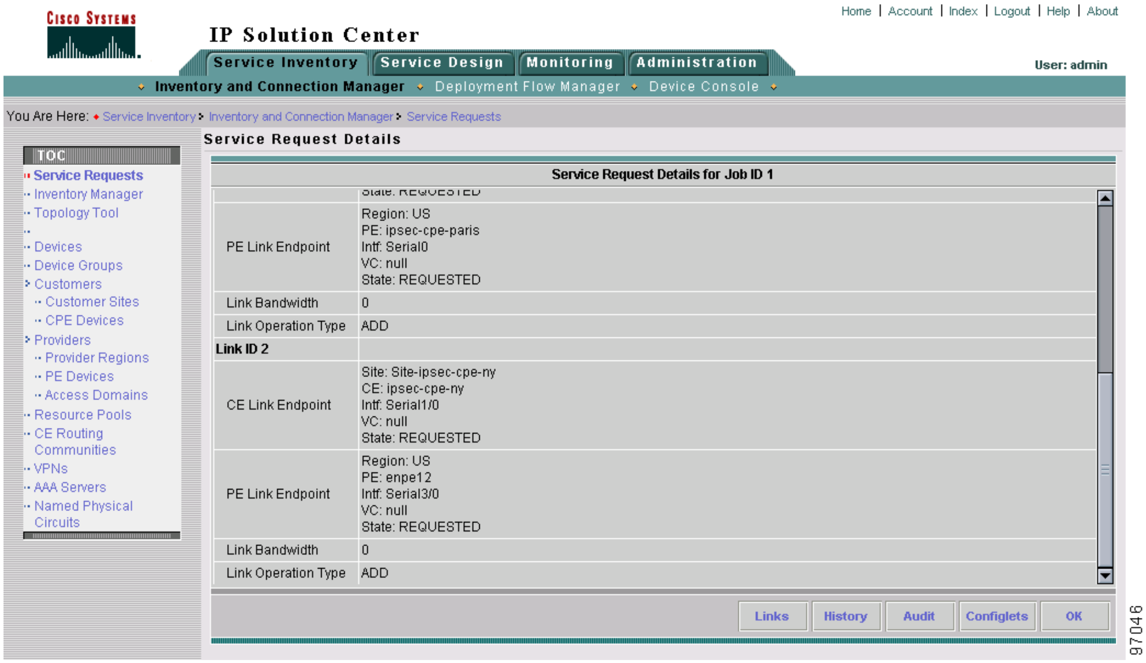
Service Request Details

Service Request Details for Job ID 1

| Attribute | Value |
|---|---|
| Type | QoS |
| State | REQUESTED |
| Operation Type | ADD |
| Service Request ID | 1 |
| Last Modification Time | Tue Mar 25 13:33:25 PST 2003 |
| Customer | Customer1 |
| Description | None |
| Policy Name | Customer1_QoS_Policy |
| **Link ID 1** | |
| CE Link Endpoint | Site: Site-ipsec-cpe-london<br>CE: ipsec-cpe-london<br>Intf: Serial0<br>VC: null<br>State: REQUESTED |
| PE Link Endpoint | Region: US<br>PE: ipsec-cpe-paris<br>Intf: Serial0<br>VC: null |

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

*Figure 8-7 QoS Service Request Details—Link ID*



Service Request Details

Service Request Details for Job ID 1

| | |
|---|---|
| | State: REQUESTED |
| PE Link Endpoint | Region: US<br>PE: ipsec-cpe-paris<br>Intf: Serial0<br>VC: null<br>State: REQUESTED |
| Link Bandwidth | 0 |
| Link Operation Type | ADD |
| **Link ID 2** | |
| CE Link Endpoint | Site: Site-ipsec-cpe-ny<br>CE: ipsec-cpe-ny<br>Intf: Serial1/0<br>VC: null<br>State: REQUESTED |
| PE Link Endpoint | Region: US<br>PE: enpe12<br>Intf: Serial3/0<br>VC: null<br>State: REQUESTED |
| Link Bandwidth | 0 |
| Link Operation Type | ADD |

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:

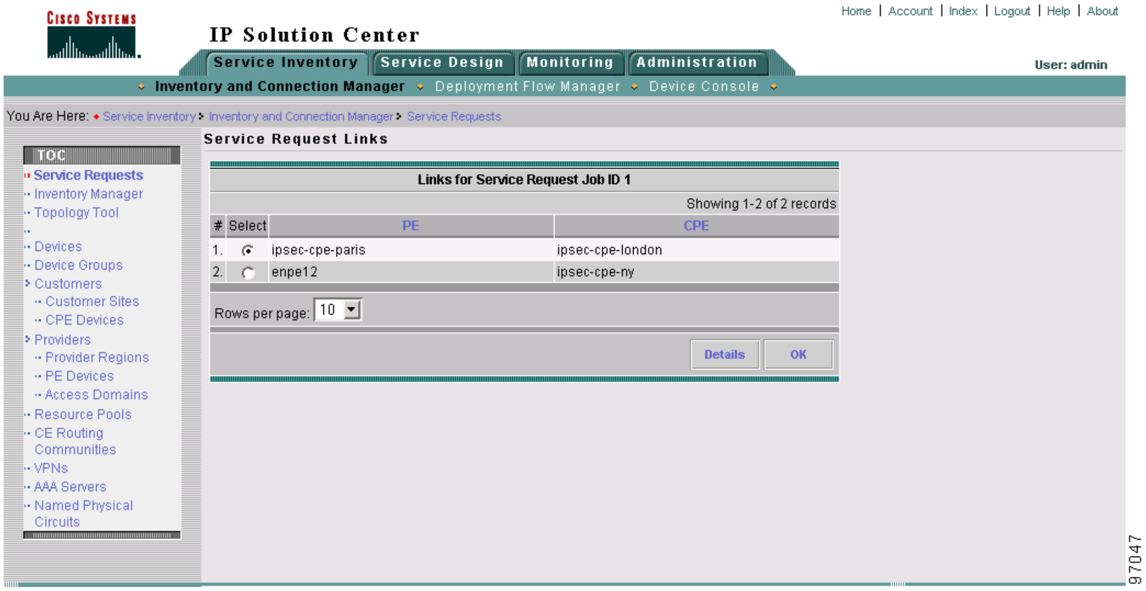
- Links—The link endpoint details.
- History—Service request history report
- Audit—Audit reports for the link IDs
- Configlets—View the ISC generated configlet for the QoS service request

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 8-1.

## Links

Figure 8-8 shows the Service Request Links window.

***Figure 8-8 QoS Service Request Links***



Service Request Links

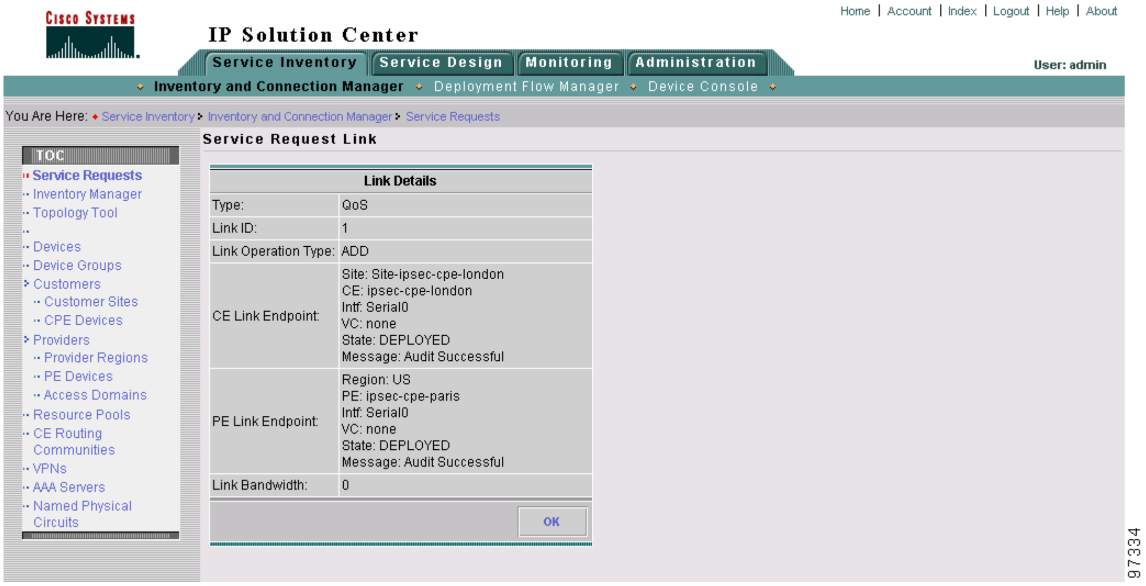
Links for Service Request Job ID 1

Showing 1-2 of 2 records

| # | Select | PE | CPE |
|---|---|---|---|
| 1. | ● | ipsec-cpe-paris | ipsec-cpe-london |
| 2. | ○ | enpe12 | ipsec-cpe-ny |

Click **Details** to display the devices marked with link QoS settings for this service request (Figure 8-9).

*Figure 8-9 Service Request Link Details*



Service Request Link

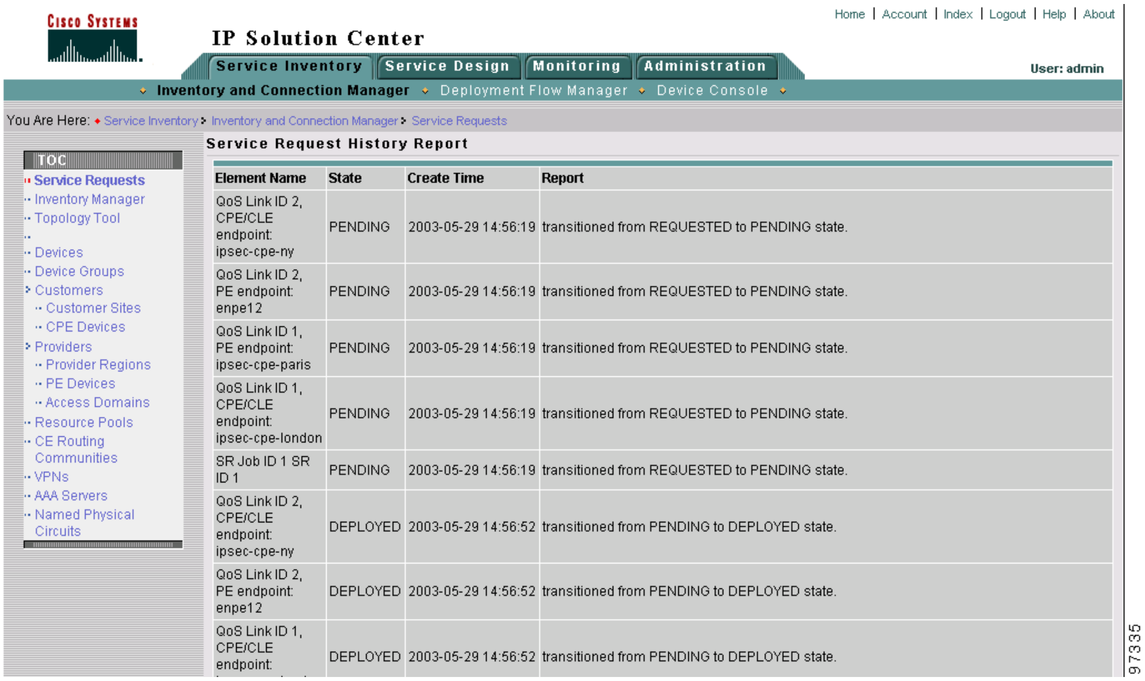
| Link Details | |
|---|---|
| Type: | QoS |
| Link ID: | 1 |
| Link Operation Type: | ADD |
| CE Link Endpoint: | Site: Site-ipsec-cpe-london<br>CE: ipsec-cpe-london<br>Intf: Serial0<br>VC: none<br>State: DEPLOYED<br>Message: Audit Successful |
| PE Link Endpoint: | Region: US<br>PE: ipsec-cpe-paris<br>Intf: Serial0<br>VC: none<br>State: DEPLOYED<br>Message: Audit Successful |
| Link Bandwidth: | 0 |

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

## History

Figure 8-10 shows the Service Request History Report window.

*Figure 8-10 Service Request History Report*



Service Request History Report

| Element Name | State | Create Time | Report |
|---|---|---|---|
| QoS Link ID 2, CPE/CLE endpoint: ipsec-cpe-ny | PENDING | 2003-05-29 14:56:19 | transitioned from REQUESTED to PENDING state. |
| QoS Link ID 2, PE endpoint: enpe12 | PENDING | 2003-05-29 14:56:19 | transitioned from REQUESTED to PENDING state. |
| QoS Link ID 1, PE endpoint: ipsec-cpe-paris | PENDING | 2003-05-29 14:56:19 | transitioned from REQUESTED to PENDING state. |
| QoS Link ID 1, CPE/CLE endpoint: ipsec-cpe-london | PENDING | 2003-05-29 14:56:19 | transitioned from REQUESTED to PENDING state. |
| SR Job ID 1 SR ID 1 | PENDING | 2003-05-29 14:56:19 | transitioned from REQUESTED to PENDING state. |
| QoS Link ID 2, CPE/CLE endpoint: ipsec-cpe-ny | DEPLOYED | 2003-05-29 14:56:52 | transitioned from PENDING to DEPLOYED state. |
| QoS Link ID 2, PE endpoint: enpe12 | DEPLOYED | 2003-05-29 14:56:52 | transitioned from PENDING to DEPLOYED state. |
| QoS Link ID 1, CPE/CLE endpoint: | DEPLOYED | 2003-05-29 14:56:52 | transitioned from PENDING to DEPLOYED state. |

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

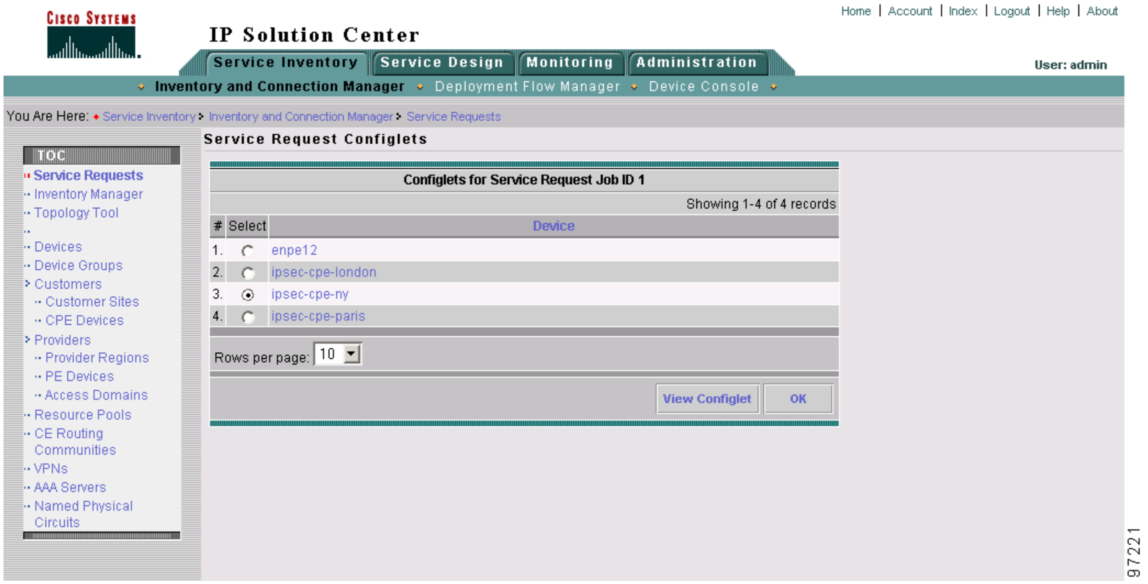
- Element name—The device, interface, and subinterfaces participating in this service request.
- State—The transition states the element has gone through.
- Create Time—The time the element was created for this service request.
- Report—The action taken by ISC for the element in this service request.

## Configlets

To view QoS configlets:

**Step 1** Click **Configlets** on the Service Request Details window. The Service Request Configlets window appears (Figure 8-11).

*Figure 8-11 Service Request Configlets*



Configlets for Service Request Job ID 1

Showing 1-4 of 4 records

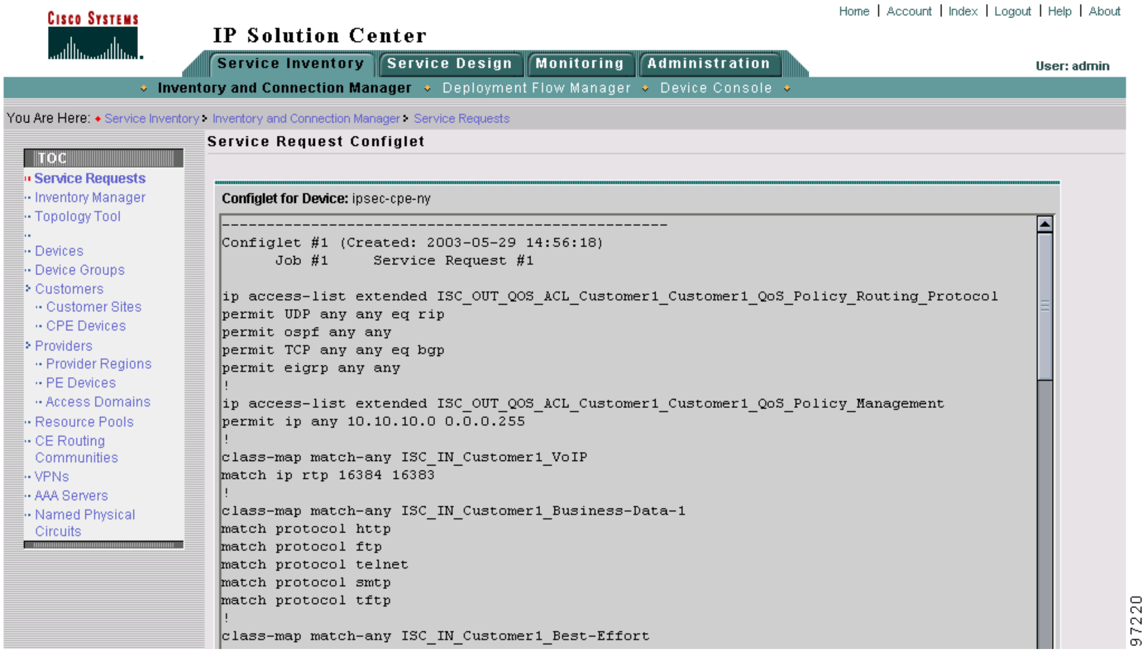
| # | Select | Device |
|---|---|---|
| 1. | ○ | enpe12 |
| 2. | ○ | ipsec-cpe-london |
| 3. | ● | ipsec-cpe-ny |
| 4. | ○ | ipsec-cpe-paris |

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 8-12).

*Figure 8-12 QoS Configlet Example*



Service Request Configlet

**Configlet for Device:** ipsec-cpe-ny

```
--------------------------------------------------
Configlet #1 (Created: 2003-05-29 14:56:18)
      Job #1     Service Request #1

ip access-list extended ISC_OUT_QOS_ACL_Customer1_Customer1_QoS_Policy_Routing_Protocol
permit UDP any any eq rip
permit ospf any any
permit TCP any any eq bgp
permit eigrp any any
!
ip access-list extended ISC_OUT_QOS_ACL_Customer1_Customer1_QoS_Policy_Management
permit ip any 10.10.10.0 0.0.0.255
!
class-map match-any ISC_IN_Customer1_VoIP
match ip rtp 16384 16383
!
class-map match-any ISC_IN_Customer1_Business-Data-1
match protocol http
match protocol ftp
match protocol telnet
match protocol smtp
match protocol tftp
!
class-map match-any ISC_IN_Customer1_Best-Effort
```

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

**Note** For Ethernet QoS, class-maps 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 class-maps 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.

To access the task logs:

**Step 1** From the Monitoring tab, click **Task Manager**.

**Step 2** Click **Logs** under the TOC heading.

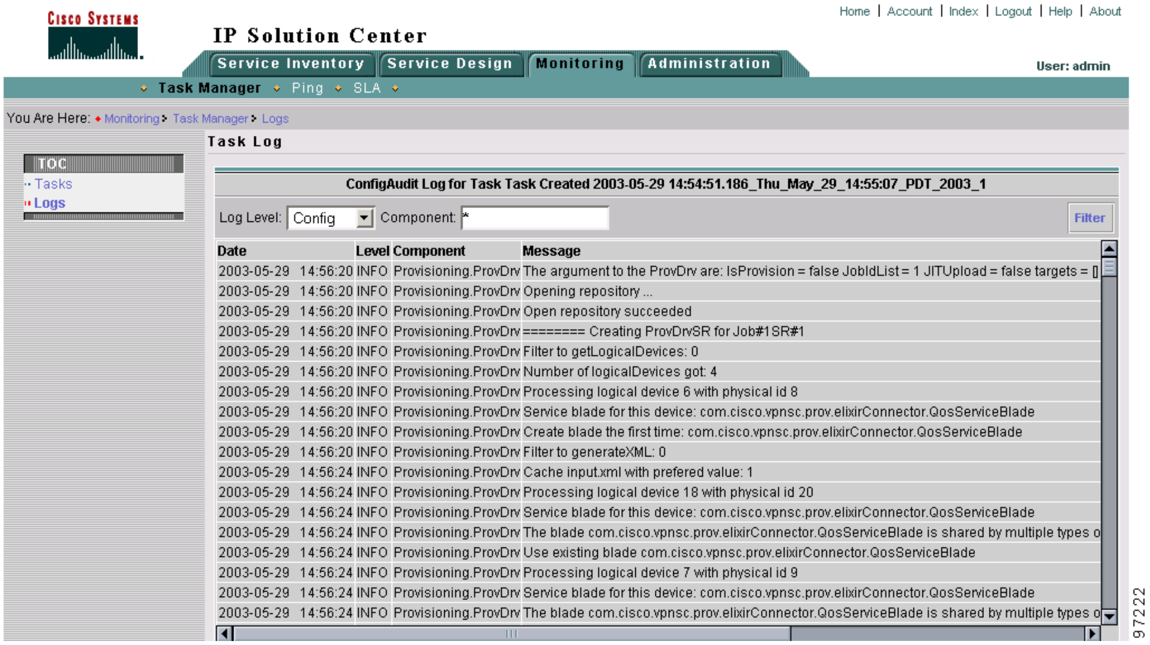
**Step 3** Select the task to view the logs for and click **Instances**.

**Step 4** Select the log to view and click **Log**. The Task Log window appears.

**Step 5** 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 8-13 shows an example of the information contained in an ISC task log.

*Figure 8-13 Task Log Example*



Task Log

ConfigAudit Log for Task Task Created 2003-05-29 14:54:51.186_Thu_May_29_14:55:07_PDT_2003_1

Log Level: Config Component: *

| Date | Level | Component | Message |
|---|---|---|---|
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | The argument to the ProvDrv are: IsProvision = false JobIdList = 1 JITUpload = false targets = [] |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Opening repository ... |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Open repository succeeded |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | ======== Creating ProvDrvSR for Job#1SR#1 |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Filter to getLogicalDevices: 0 |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Number of logicalDevices got: 4 |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Processing logical device 6 with physical id 8 |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Service blade for this device: com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Create blade the first time: com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade |
| 2003-05-29 14:56:20 | INFO | Provisioning.ProvDrv | Filter to generateXML: 0 |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | Cache input.xml with prefered value: 1 |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | Processing logical device 18 with physical id 20 |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | Service blade for this device: com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | The blade com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade is shared by multiple types o |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | Use existing blade com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | Processing logical device 7 with physical id 9 |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | Service blade for this device: com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade |
| 2003-05-29 14:56:24 | INFO | Provisioning.ProvDrv | The blade com.cisco.vpnsc.prov.elixirConnector.QosServiceBlade is shared by multiple types o |

**Step 6** For example, this window shows all log entries related to the device configuration.

**Step 7** To exit from task logs, you must click **Task Manager** above the TOC for this window.

# Sample Configurations

This appendix lists sample configurations and contains the following sections:

- ISC-Generated Configlets, page A-1
- Device Configurations, page A-7

# ISC-Generated Configlets

The following are examples of configlets generated by Cisco IP Solution Center (ISC) for the network example used in Chapter 5, "Provisioning Process for IP QoS."

## 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 5, “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

## PE-CLE QoS Cofiguration (Cisco Catalyst 3550)

**Note** ISC treats the global **mls qos** command as a prerequisite for Metro Ethernet QoS deployment. You must use this command to enable QoS on the Catalyst 3550. ISC does not automatically provision the **mls qos** command but requires it to be part of the initial configuration.

The **mls qos** command has a global effect on the switch and is not ever disabled by ISC. If you do not enable the QoS switch on the Catalyst 3550 with the **mls qos** command, all the QoS commands provisioned by ISC do download to the switch and the QoS service request does go to the DEPLOYED state. However QoS is not in effect until it is enabled with the **mls qos** command.

### Ingress per vlan policing / Trust DSCP / Match DSCP / Set CoS to 5 and 2

```
mls qos aggregate-policer aggr-vlan1701-d 5000000 250000 exceed-action drop
mls qos aggregate-policer aggr-vlan1701-v 1000000 250000 exceed-action drop
class-map match-all vlan1701-voice
  match vlan  1701
  match class-map voice-traffic
class-map match-all vlan1701-voice-ctrl
  match vlan  1701
  match class-map voice-control
class-map match-all vlan1701-data
  match vlan  1701
  match class-map data-traffic
class-map match-all vlan1701-l2
  match vlan  1701
  match class-map l2-traffic
policy-map pol-giga01
 description Input policy for Port Giga 0/1
  class vlan1701-voice
    police aggregate aggr-vlan1701-v
    trust dscp
    set cos 5
  class vlan1701-voice-ctrl
    police aggregate aggr-vlan1701-v
    trust dscp
    set cos 3
  class vlan1701-data
    police aggregate aggr-vlan1701-d
    trust dscp
    set cos 2
  class vlan1701-l2
    police aggregate aggr-vlan1701-d
    set cos 2
interface GigabitEthernet0/1
 description 802.1Q trunk connected to Customer A1
 service-policy input pol-giga01
```

### Egress Queuing at the Customer UNI in a PE-CLE: Egress Traffic Assigned to Respective Queue

```
interface GigabitEthernet0/11
```

```
 wrr-queue bandwidth 30 60 10 0
 wrr-queue queue-limit 20 40 20 20
 wrr-queue cos-map 1 0 1 4
 wrr-queue cos-map 2 2
 wrr-queue cos-map 3 3 6 7
 wrr-queue cos-map 4 5
 priority-queue out
```

### Egress Queueing at the PE-POP Facing Port in a PE-CLE

```
interface GigabitEthernet0/11
 wrr-queue bandwidth 30 60 10 0
 wrr-queue queue-limit 20 40 20 20
 wrr-queue cos-map 1 0 1 4
 wrr-queue cos-map 2 2
 wrr-queue cos-map 3 3 6 7
 wrr-queue cos-map 4 5
 priority-queue out
```

# PE-POP QoS Configuration (Cisco 7600)

## No DSCP Rewrite / Copy MPLS exp to 802.1p / Egress Queueing

```
mls qos queueing-only

interface GigabitEthernet3/1
 wrr-queue queue-limit 50 50
 wrr-queue random-detect min-threshold 1 100 100
 wrr-queue random-detect min-threshold 2 100 100
 wrr-queue random-detect max-threshold 1 100 100
 wrr-queue random-detect max-threshold 2 100 100
 wrr-queue cos-map 1 1 0 1 3 4
 wrr-queue cos-map 2 1 2
 priority-queue cos-map 1 5 6 7
```

INDEX