

**HUAWEI NetEngine80E/40E Router
V600R003C00**

Configuration Guide - QoS

Issue 02
Date 2011-09-10

HUAWEI TECHNOLOGIES CO., LTD.



Copyright © Huawei Technologies Co., Ltd. 2011. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
 Bantian, Longgang
 Shenzhen 518129
 People's Republic of China

Website: <http://www.huawei.com>

Email: support@huawei.com

About This Document

Purpose

This document describes the basic knowledge and configurations of QoS, including traffic policing, traffic shaping, congestion management and avoidance, and traffic classification and provides an introduction of QPPB, MPLS HQoS, ATM QoS, and HQoS.

This document can be used as a guide for QoS configurations.

NOTE

- This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.
- On NE80E/40E series excluding NE80E/40E-X1 and NE80E/40E-X2, line processing boards are called Line Processing Units (LPUs) and switching fabric boards are called Switching Fabric Units (SFUs). On the NE40E-X1 and NE40E-X2, there are no LPUs and SFUs, and NPUs implement the same functions of LPUs and SFUs to exchange and forward packets.

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
HUAWEI NetEngine80E/40E Router	V600R003C00

Intended Audience

This document is intended for:

- Commissioning engineer
- Data configuration engineer
- Network monitoring engineer
- System maintenance engineer

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
 WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
 CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
 TIP	Provides a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in previous issues.

Changes in Issue 02 (2011-09-10)

The second commercial release has the following updates.

- **Class-based QoS Configuration**
 - As defined in [4.2.5 Applying a Traffic Policy](#), the parameter **mpls-layer** can be specified in the **traffic-policy** command on upstream interfaces of specific LPUs.
 - The **qos phb enable** command can be configured on a downstream interface to enable PHB. The internal priorities of packets passing through the downstream interface are mapped to external priorities based on the PHB table.
- **ATM QoS Configuration**
 - As defined in [9.3.3 Configuring Forced ATM Traffic Classification](#), If the **traffic queue** and **difsserv-mode** commands are configured on an ATM interface, the priority and color configuration specified by the **difsserv-mode** command take effect.

Changes in Issue 01 (2011-05-30)

Initial commercial release.

Contents

About This Document..........ii

1 QoS Overview..........1

1.1 Introduction to QoS.....	2
1.1.1 Traditional Packets Transmission Application.....	2
1.1.2 New Applications Requirements.....	2
1.2 End-to-End QoS Model.....	3
1.2.1 Best-Effort Service Model.....	3
1.2.2 Integrated Service Model.....	3
1.2.3 Differentiated Service Model.....	4
1.3 Techniques Used for the QoS Application.....	9
1.3.1 Traffic Classification.....	10
1.3.2 Traffic Policing and Shaping.....	11
1.3.3 Congestion Avoidance Configuration.....	12
1.3.4 RSVP.....	13
1.3.5 Link Efficiency Mechanism.....	13
1.4 QoS Supported by the NE80E/40E.....	14

2 Traffic Policing and Shaping Configuration..........15

2.1 Introduction to Traffic Policing and Shaping.....	16
2.1.1 Traffic Policing.....	16
2.1.2 Traffic Shaping.....	18
2.1.3 Traffic Policing and Shaping Supported by NE80E/40E.....	20
2.2 Configuring Interface-based Traffic Policing.....	20
2.2.1 Establishing the Configuration Task.....	20
2.2.2 Configuring CAR on a Layer 3 Interface.....	21
2.2.3 Configuring CAR on a Layer 2 Port.....	22
2.2.4 Checking the Configuration.....	23
2.3 Configuring CTC-based Traffic Policing.....	24
2.3.1 Establishing the Configuration Task.....	24
2.3.2 Defining Traffic Classes.....	25
2.3.3 Defining a Behavior and Configuring Traffic Policing Actions.....	27
2.3.4 Configuring a Traffic Policy.....	28
2.3.5 Applying the Traffic Policy.....	29

2.3.6 Checking the Configuration.....	30
2.4 Configuring Traffic Shaping.....	32
2.4.1 Establishing the Configuration Task.....	32
2.4.2 Configuring Traffic Shaping.....	33
2.4.3 Checking the Configuration.....	34
2.5 Maintaining Traffic Policing and Shaping.....	34
2.5.1 Clearing Statistics of CAR.....	34
2.6 Configuration Examples.....	34
2.6.1 Example for Configuring Traffic Policing and Traffic Shaping.....	35
3 Congestion Avoidance Configuration.....	39
3.1 Introduction to Congestion Avoidance.....	40
3.1.1 Introduction to Congestion Avoidance.....	40
3.1.2 Congestion Avoidance Supported by NE80E/40E.....	42
3.2 Configuring WRED.....	42
3.2.1 Establishing the Configuration Task.....	42
3.2.2 Configuring WRED Parameters.....	43
3.2.3 Applying WRED.....	44
3.2.4 Checking the Configuration.....	45
3.3 Configuring Queue Scheduling for Low-Speed Links.....	46
3.3.1 Establishing the Configuration Task.....	47
3.3.2 Configuring PQ.....	47
3.3.3 Configuring WFQ.....	48
3.3.4 Checking the Configuration.....	48
3.4 Maintaining Congestion Avoidance.....	51
3.4.1 Clearing the Statistics on Class Queues.....	51
3.5 Configuration Examples.....	52
3.5.1 Example for Configuring Congestion Avoidance.....	52
3.5.2 Example for Configuring Queue Scheduling on Low-speed Links.....	58
4 Class-Based QoS Configuration.....	62
4.1 Class-Based QoS Overview.....	63
4.1.1 Introduction to Class-Based QoS.....	63
4.1.2 Class-Based QoS Supported by the NE80E/40E.....	65
4.2 Configuring a Traffic Policy Based on Complex Traffic Classification.....	65
4.2.1 Establishing the Configuration Task.....	65
4.2.2 Defining a Traffic Classifier.....	67
4.2.3 Defining a Traffic Behavior and Configuring Traffic Actions.....	70
4.2.4 Defining a Traffic Policy and Specifying a Traffic Behavior for a Traffic Classifier.....	74
4.2.5 Applying a Traffic Policy.....	74
4.2.6 Applying the Statistics Function of a Traffic Policy.....	76
4.2.7 Checking the Configuration.....	77
4.3 Configuring UCL-based Traffic Policies.....	79
4.3.1 Establishing the Configuration Task.....	79

4.3.2 Configuring a User Group.....	80
4.3.3 Configuring a UCL Rule.....	80
4.3.4 Defining a Traffic Classifier.....	81
4.3.5 Defining a Traffic Behavior and Configuring Actions.....	82
4.3.6 Defining a Traffic Policy.....	86
4.3.7 Applying UCL-based Traffic Policies.....	87
4.3.8 Specifying the Domain of a User.....	87
4.3.9 (Optional) Applying the Statistic Function of a Traffic Policy.....	88
4.3.10 Checking the Configuration.....	89
4.4 Configuring Precedence Mapping Based on Simple Traffic Classification.....	90
4.4.1 Establishing the Configuration Task.....	90
4.4.2 Configuring Priority Mapping for VLAN Packets.....	91
4.4.3 Configuring Priority Mapping for IP Packets.....	95
4.4.4 Configuring Priority Mapping for MPLS Packets.....	98
4.4.5 Configuring Priority Mapping for Control Packets.....	99
4.4.6 Configuring Priority Mapping for Multicast Packets.....	100
4.4.7 Configuring User Priority Mapping in a Domain.....	101
4.4.8 Checking the Configuration.....	103
4.5 Maintaining Class-based QoS.....	103
4.5.1 Clearing the Statistics About Traffic Policies.....	104
4.6 Configuration Examples.....	104
4.6.1 Example for Configuring a Traffic Policy Based on Complex Traffic Classification.....	104
4.6.2 Example for Configuring Complex Traffic Classification on a Sub-interface for QinQ VLAN Tag Termination.....	112
4.6.3 Example for Configuring Preference Mapping Based on Simple Traffic Classification for VLAN Packets	116
4.6.4 Example for Configuring Precedence Mapping Based on Simple Traffic Classification for MPLS Packets	121
5 QPPB Configuration.....	124
5.1 QPPB Overview.....	125
5.2 QPPB Supported by the NE80E/40E.....	125
5.3 Configuring Source-Based QPPB.....	127
5.3.1 Configuring Routing Policies on a BGP Route Sender.....	129
5.3.2 Configuring Routing Policies on a BGP Route Receiver.....	130
5.3.3 Configuring Traffic Behaviors on a Route Receiver.....	132
5.3.4 Configuring QPPB Local Policies on a BGP Route Receiver.....	132
5.3.5 Applying a QPPB Local Policy to an Interface.....	133
5.3.6 Checking the Configuration.....	134
5.4 Configuring Destination-Based QPPB.....	135
5.4.1 Configuring Routing Policies on a BGP Route Sender.....	136
5.4.2 Configuring Routing Policies on a BGP Route Receiver.....	137
5.4.3 Configuring Traffic Behaviors on a Route Receiver.....	139
5.4.4 Configuring QPPB Local Policies on a BGP Route Receiver.....	140

5.4.5 Applying a QPPB Local Policy to an Interface.....	140
5.4.6 Checking the Configuration.....	141
5.5 Maintaining QPPB.....	142
5.5.1 Clearing Statistics About a QPPB Policy.....	142
5.6 Configuration Examples.....	142
5.6.1 Example for Configuring QPPB.....	142
6 MPLS HQoS Configuration.....	148
6.1 Overview of MPLS HQoS.....	150
6.1.1 Introduction to MPLS HQoS.....	150
6.1.2 MPLS HQoS Supported by the NE80E/40E.....	151
6.2 Configuring QoS Template for VPN.....	151
6.2.1 Establishing the Configuration Task.....	151
6.2.2 (Optional) Configuring an FQ WRED Object.....	152
6.2.3 (Optional) Configuring Scheduling Parameters of an FQ.....	153
6.2.4 (Optional) Configuring a Mapping from an FQ to a CQ.....	154
6.2.5 (Optional) Configuring a Service Profile and Applying It to an Interface.....	154
6.2.6 Defining a QoS Template for VPN and Configuring Scheduling Parameters.....	155
6.2.7 Checking the Configuration.....	156
6.3 Configuring BGP/MPLS IP VPN QoS.....	157
6.3.1 Establishing the Configuration Task.....	157
6.3.2 Configuring BGP/MPLS IP VPN Instance-based QoS.....	158
6.3.3 Configuring BGP/MPLS IP VPN Peer QoS.....	159
6.3.4 Checking the Configuration.....	159
6.4 Configuring VLL QoS.....	160
6.4.1 Establishing the Configuration Task.....	160
6.4.2 Configuring VLL QoS.....	161
6.4.3 Checking the Configuration.....	162
6.5 Configuring PWE3 QoS.....	163
6.5.1 Establishing the Configuration Task.....	163
6.5.2 Configuring the Single-hop PWE3 QoS.....	164
6.5.3 Configuring Dynamic Multi-hop PWE3 QoS.....	165
6.5.4 Configuring QoS for the Mixed Multi-hop PWE3.....	166
6.5.5 Configuring the Static Multi-hop PWE3 QoS.....	166
6.5.6 Checking the Configuration.....	167
6.6 Configuring VPLS QoS.....	168
6.6.1 Establishing the Configuration Task.....	168
6.6.2 Configuring the VSI-based QoS.....	169
6.6.3 Configuring the VSI Peer-based QoS.....	170
6.6.4 Checking the Configuration.....	171
6.7 Configuring BGP/MPLS IP VPN Traffic Statistics.....	171
6.7.1 Establishing the Configuration Task.....	171
6.7.2 Configuring Traffic Statistics of BGP/MPLS IP VPN.....	172

6.7.3 Configuring Traffic Statistics of the BGP/MPLS IP VPN Peer.....	173
6.7.4 Checking the Configuration.....	173
6.8 Configuring Traffic Statistics of the Single-hop VLL.....	174
6.8.1 Establishing the Configuration Task.....	174
6.8.2 Enabling Statistics on the Single-hop VLL Traffic.....	175
6.8.3 Checking the Configuration.....	175
6.9 Configuring Traffic Statistics of the VPLS.....	176
6.9.1 Establishing the Configuration Task.....	176
6.9.2 Configuring the VSI-based Traffic Statistics.....	177
6.9.3 Configuring the VSI Peer-based Traffic Statistics.....	178
6.9.4 Checking the Configuration.....	179
6.10 Maintaining MPLS HQoS.....	180
6.10.1 Clearing Statistics on the QoS-enabled VPN Traffic.....	180
6.11 Configuration Examples of MPLS HQoS.....	180
6.11.1 Example for Configuring BGP/MPLS IP VPN QoS (LDP LSP at the Network Side).....	180
6.11.2 Example for Configuring BGP/MPLS IP VPN QoS (TE Tunnel at the Network Side).....	190
6.11.3 Example for Configuring MVPN QoS.....	201
6.11.4 Example for Configuring VLL QoS.....	211
6.11.5 Example for Configuring Dynamic Single-hop PWE3 QoS.....	219
6.11.6 Example for Configuring the Static Multi-hop PW QoS.....	226
6.11.7 Example for Configuring the Dynamic Multi-hop PW QoS.....	233
6.11.8 Example for Configuring the Mixed Multi-hop PW QoS.....	243
6.11.9 Example for Configuring Martini VPLS QoS.....	250
7 MPLS DiffServ-Mode Configuration.....	258
7.1 Introduction.....	259
7.1.1 MPLS DiffServ Models Overview.....	259
7.1.2 MPLS Pipe/Short Pipe supported by NE80E/40E.....	262
7.2 Configuring Uniform/Pipe Model for MPLS TE.....	262
7.2.1 Establishing the Configuration Task.....	262
7.2.2 Enabling MPLS TE to Support DiffServ Models.....	263
7.3 Configuring Pipe/Short Pipe Model Based on VPN.....	264
7.3.1 Establishing the Configuration Task.....	264
7.3.2 (Optional) Enabling BGP/MPLS IP VPN to Support DiffServ Models.....	265
7.3.3 (Optional) Enabling an VLL to Support DiffServ Models.....	265
7.3.4 (Optional) Enabling an VPLS to Support DiffServ Models.....	266
7.3.5 Checking the Configuration.....	267
7.4 Configuration Examples.....	268
7.4.1 Example for Configuring an MPLS DiffServ Mode.....	268
8 Link Efficiency Mechanisms.....	277
8.1 Introduction to Link Efficiency Mechanisms.....	278
8.1.1 Link Efficiency Mechanism Overview.....	278
8.1.2 RTP Header Compression(CRTP).....	278

8.1.3 Enhanced Compression RTP(ECRTP).....	280
8.2 Configuring IP Header Compression.....	281
8.2.1 Establishing the Configuration Task.....	281
8.2.2 Enabling IP Header Compression.....	282
8.2.3 Configuring the Maximum Number of Connections for RTP Header Compression.....	283
8.2.4 Configuring the Update Time for Sessions of Packet Header Compression.....	284
8.2.5 Configuring the Aging Time for a Session Environment.....	285
8.2.6 Checking the Configuration.....	285
8.3 Configuring Enhanced IP Header Compression.....	286
8.3.1 Establishing the Configuration Task.....	286
8.3.2 Configuring ECRTP.....	287
8.3.3 Configuring the Maximum Number of Connections for RTP Header Compression.....	287
8.3.4 Configuring the Update Time for Sessions of Packet Header Compression.....	288
8.3.5 (Optional) Configuring the Maximum Number of Consecutive Packet Drops Tolerable over the Link	289
8.3.6 (Optional) Configuring the No-Delta Compression Mode.....	289
8.3.7 Configuring the Aging Time for a Session Environment.....	290
8.3.8 Checking the Configuration.....	290
8.4 Maintaining Packet Header Compression.....	291
8.4.1 Clearing IP Header Compression.....	291
8.5 Configuration Examples.....	292
8.5.1 Example for Configuring IP Header Compression.....	292
8.5.2 Example for Configuring ECRTP.....	295
9 ATM QoS Configuration.....	299
9.1 ATM QoS Overview.....	301
9.1.1 Introduction to ATM QoS.....	301
9.1.2 ATM QoS Features Supported by the NE80E/40E.....	301
9.2 Configuring ATM Simple Traffic Classification.....	304
9.2.1 Establishing the Configuration Task.....	304
9.2.2 Enabling ATM Simple Traffic Classification.....	306
9.2.3 Configuring Mapping Rules for ATM QoS.....	307
9.2.4 Checking the Configuration.....	307
9.3 Configuring Forced ATM Traffic Classification.....	308
9.3.1 Establishing the Configuration Task.....	308
9.3.2 Configuring ATM Services.....	310
9.3.3 Configuring Forced ATM Traffic Classification.....	310
9.3.4 Checking the Configuration.....	311
9.4 Configuring ATM Complex Traffic Classification.....	311
9.4.1 Establishing the Configuration Task.....	311
9.4.2 Defining Traffic Classifiers.....	312
9.4.3 Defining Traffic Behaviors.....	313
9.4.4 Defining Traffic Policies.....	314

9.4.5 Applying Traffic Policies.....	314
9.4.6 Checking the Configuration.....	315
9.5 Configuring the ATM Traffic Shaping.....	316
9.5.1 Establishing the Configuration Task.....	316
9.5.2 Configuring ATM Traffic Shaping Parameters.....	317
9.5.3 Applying ATM Traffic Shaping Parameters.....	318
9.5.4 Checking the Configuration.....	319
9.6 Configuring the Priority of an ATM PVC.....	319
9.6.1 Establishing the Configuration Task.....	319
9.6.2 Configuring the Priority of an ATM PVC.....	320
9.7 Configuring Congestion Management of the ATM PVC.....	321
9.7.1 Establishing the Configuration Task.....	321
9.7.2 Configuring the Queue Scheduling of an ATM PVC.....	321
9.7.3 Checking the Configuration.....	322
9.8 Configuration Examples.....	323
9.8.1 Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission	324
9.8.2 Example for Configuring Simple Traffic Classification for 1-to-1 VPC ATM Transparent Transmission	331
9.8.3 Example for Configuring Simple Traffic Classification for AAL5 SDU ATM Transparent Transmission	337
9.8.4 Example for Configuring 1483R-based ATM Simple Traffic Classification.....	342
9.8.5 Example for Configuring 1483B-Based ATM Simple Traffic Classification.....	346
9.8.6 Example for Configuring Forced ATM Traffic Classification.....	350
9.8.7 Example for Configuring the ATM Complex Traffic Classification.....	355
9.8.8 Example for Configuring Queue Scheduling for an ATM PVC.....	359
10 HQoS Configuration.....	362
10.1 HQoS Overview.....	364
10.1.1 Introduction to HQoS.....	364
10.1.2 Related Concepts of HQoS.....	365
10.1.3 HQoS Supported by the NE80E/40E.....	366
10.2 Configuring HQoS on an Ethernet Interface.....	372
10.2.1 Establishing the Configuration Task.....	372
10.2.2 (Optional) Configuring an FQ WRED Object.....	374
10.2.3 (Optional) Configuring Scheduling Parameters of an FQ.....	375
10.2.4 (Optional) Configuring a Mapping from an FQ to a CQ.....	376
10.2.5 (Optional) Configuring Scheduling Parameters for a GQ.....	377
10.2.6 Configuring Scheduling Parameters of an SQ.....	378
10.2.7 (Optional) Configuring a CQ WRED Object.....	378
10.2.8 (Optional) Configuring Scheduling Parameters of a CQ.....	379
10.2.9 Checking the Configuration.....	380
10.3 Configuring HQoS on a QinQ Termination Sub-interface.....	382
10.3.1 Establishing the Configuration Task.....	383

10.3.2 (Optional) Configuring an FQ WRED Object.....	384
10.3.3 (Optional) Configuring Scheduling Parameters of an FQ.....	385
10.3.4 (Optional) Configuring a Mapping from an FQ to a CQ.....	385
10.3.5 (Optional) Configuring Scheduling Parameters for a GQ.....	386
10.3.6 Enabling QinQ on an Interface.....	387
10.3.7 Configuring QinQ on a Sub-interface.....	387
10.3.8 Configuring a VLAN Group.....	388
10.3.9 Configuring Scheduling Parameters of an SQ.....	389
10.3.10 (Optional) Configuring a CQ WRED Object.....	389
10.3.11 (Optional) Configuring Scheduling Parameters of a CQ.....	390
10.3.12 Checking the Configuration.....	391
10.4 Configuring Class-based HQoS.....	392
10.4.1 Establishing the Configuration Task.....	392
10.4.2 Defining a Traffic Classifier.....	393
10.4.3 (Optional) Configuring an FQ WRED Object.....	394
10.4.4 (Optional) Configuring Scheduling Parameters of an FQ.....	395
10.4.5 (Optional) Configuring a Mapping from an FQ to a CQ.....	396
10.4.6 (Optional) Configuring Scheduling Parameters for a GQ.....	396
10.4.7 Defining a Traffic Behavior and Configuring Scheduling Parameters for a Subscriber Queue.....	397
10.4.8 Defining a Traffic Policy and Applying It to an Interface.....	398
10.4.9 (Optional) Configuring a WRED Object for a Class Queue.....	399
10.4.10 (Optional) Configuring Scheduling Parameters for a Class Queue.....	399
10.4.11 Checking the Configuration.....	400
10.5 Configuring Profile-based HQoS.....	401
10.5.1 Establishing the Configuration Task.....	401
10.5.2 (Optional) Configuring an FQ WRED Object.....	405
10.5.3 (Optional) Configuring Scheduling Parameters of an FQ.....	406
10.5.4 (Optional) Configuring a Mapping from an FQ to a CQ.....	407
10.5.5 (Optional) Configuring Scheduling Parameters for a GQ.....	407
10.5.6 (Optional) Configuring a Service Profile and Applying It to an Interface.....	408
10.5.7 Defining a QoS Profile and Configuring Scheduling Parameters.....	409
10.5.8 Applying a QoS Profile.....	410
10.5.9 (Optional) Configuring a CQ WRED Object.....	411
10.5.10 (Optional) Configuring Scheduling Parameters of a CQ.....	412
10.5.11 Checking the Configuration.....	412
10.6 Configuring HQoS Scheduling for Family Users.....	414
10.6.1 Establishing the Configuration Task.....	415
10.6.2 Defining a QoS Profile and Configuring Scheduling Parameters.....	416
10.6.3 Configuring a Service Identification Policy.....	416
10.6.4 (Optional) Configuring the Service Traffic of Users in a Domain Not to Participate in the QoS Scheduling for Family Users.....	418
10.6.5 Binding a QoS Profile and a Service Identification Policy to a BAS Interface.....	419
10.6.6 (Optional) Configuring Dynamic Update of a QoS Profile.....	420

10.6.7 Checking the Configuration.....	421
10.7 Configuring HQoS Scheduling for Common Users.....	424
10.7.1 Establishing the Configuration Task.....	424
10.7.2 Defining a QoS Profile and Configuring Scheduling Parameters.....	425
10.7.3 Configuring the Rate Limit Mode for Common Users.....	426
10.7.4 (Optional) Configuring User Name-based Access Limit.....	426
10.7.5 Applying a QoS Profile to a Domain.....	427
10.7.6 (Optional) Configuring Dynamic Update of a QoS Profile.....	428
10.7.7 Checking the Configuration.....	429
10.8 Configuring HQoS Scheduling for Leased Line Users.....	431
10.8.1 Establishing the Configuration Task.....	432
10.8.2 Defining a QoS Profile and Configuring Scheduling Parameters.....	432
10.8.3 Configuring the Rate Limit Mode for Leased Line Users.....	433
10.8.4 Applying a QoS Profile to a Domain.....	434
10.8.5 Checking the Configuration.....	434
10.9 Maintaining HQoS.....	437
10.9.1 Clearing Queue Statistics.....	437
10.10 Configuration Examples.....	438
10.10.1 Example for Configuring HQoS on an Ethernet Interface.....	438
10.10.2 Example for Configuring QinQ HQoS.....	444
10.10.3 Example for Configuring Class-based HQoS.....	450
10.10.4 Example for Configuring Profile-based HQoS.....	457
10.10.5 Example for Configuring HQoS Scheduling for Leased Line Users.....	465
A Glossary.....	468
B Acronyms and Abbreviations.....	474

1 QoS Overview

About This Chapter

This chapter describes QoS basics and solutions, the DiffServ model, and relevant QoS technologies.

[1.1 Introduction to QoS](#)

This section describes the basic concepts of QoS, traditional packet delivery services, new demands resulting from new services, and QoS features supported by the device.

[1.2 End-to-End QoS Model](#)

Based on network quality and user requirements, QoS provides end-to-end services for users through different service models.

[1.3 Techniques Used for the QoS Application](#)

This section describes functions used for QoS implementation, such as traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance, RSVP, and the link efficiency mechanism.

[1.4 QoS Supported by the NE80E/40E](#)

The device supports unicast QoS, multicast QoS, IPv4 QoS, and IPv6 QoS.

1.1 Introduction to QoS

This section describes the basic concepts of QoS, traditional packet delivery services, new demands resulting from new services, and QoS features supported by the device.

Quality of service (QoS) is used to assess the ability of the supplier to meet the customer demands.

On the Internet, QoS is used to assess the ability of the network to transmit packets. As the network provides a wide variety of services, QoS should be assessed from different aspects. QoS generally refers to the analysis of the issues related to the process of sending packets such as, bandwidth, delay, jitter, and packet loss ratio.

1.1.1 Traditional Packets Transmission Application

The best-effort service, as a traditional service, does not give priority to the traffic that is delay- or jitter-sensitive, or requires a low packet loss ratio or high reliability. That is, all packets are treated in a uniform manner.

It is difficult to ensure QoS in the traditional IP network. Because routers in the network handle all the packets equally and adopt First In First Out (FIFO) method to transfer packets. Resources used for forwarding packets are allocated based on the arrival sequence of the packets.

All packets share the bandwidth of networks and routers. Resources are allocated according to the arrival time of the packets. This policy is called best effort (BE). The device in this mode tries its best to transmit packets to the destination. The BE mode, however, does not ensure any improvement in delay time, jitter, packet loss ratio, and high reliability.

The traditional BE mode applies only to services such as World Wide Web (WWW), file transfer, and email, which have no specific request for bandwidth and jitter.

1.1.2 New Applications Requirements

Compared with traditional QoS policies, newly developed QoS policies meet various requirements and provides differentiated services.

With the rapid development of the network, increasing number of networks are connected to the Internet. The Internet expands greatly in size, scope, and users. The use of the Internet as a platform for data transmission and implementation of various applications is on the rise. Further, the service providers also want to develop new services for more profits.

Apart from traditional applications such as WWW, email, and File Transfer Protocol (FTP), the Internet has expanded to accommodate other services such as E-learning, telemedicine, videophone, videoconference, and video on demand. Enterprise users want to connect their branches in different areas through VPN technologies to implement applications such as accessing corporate databases or managing remote devices through Telnet.

These new applications put forward special requirements for bandwidth, delay, and jitter. For example, videoconference and video on demand require high bandwidth, low delay, and low jitter. Telnet stresses on low delay and priority handling in the event of congestion.

As new services spring up, the number of requests for the service capability of IP networks has been on the rise. Users expect improved service transmission to the destination and also better quality of services. For example, IP networks are expected to provide dedicated bandwidth,

reduce packet loss ratio, avoid network congestion, control network flow, and set the preference of packets to provide different QoS for various services.

All these demand better service capability from the network, and QoS is just an answer to the requirements.

1.2 End-to-End QoS Model

Based on network quality and user requirements, QoS provides end-to-end services for users through different service models.

Different service models are provided for user services to ensure QoS according to users' requirements and the quality of the network. The common service models are as follows:

- Best-Effort service model
- Integrated service model
- Differentiated service model

1.2.1 Best-Effort Service Model

The BE service model is applicable to the services that are insensitive to the delay and has lower requirements for reliability. BE is realized through the FIFO mechanism.

Best-Effort is an indiscriminate and the simplest service model. Application programs can, without notifying the network or obtaining any approval from the network, send any number of packets at any time. For the Best-Effort service, the network tries its best to send packets, but cannot ensure the performance such as delay and reliability. The Best-Effort model is the default service model of the Internet and can be applied to most networks, such as FTP and email, through the First-in-First-out (FIFO) queue.

1.2.2 Integrated Service Model

In the integrated service model, the application program applies to the network for specific service, and does not send packets until the arrival of confirmation that the network has reserved resources for it.

The integrated service model is called Antiserum for short. Antiserum is an integrated service model and can meet various QoS requirements. In this service model, before sending packets, an application program needs to apply for specific services through signaling. The application program first notifies the network of its traffic parameters and the request for special service qualities such as bandwidth and delay. After receiving the confirmation of the network that resources have been reserved for packets, the application program begins sending packets. The sent packets are controlled within the range specified by the flow parameters.

After receiving the request for resources from the application program, the network checks the resource allocation. That is, based on the request and current available resources, the network determines whether to allocate resources for the application program or not. Once the network confirms that resources are allocated for the packets, and as long as the packets are controlled within the range specified by the flow parameters, the network is certain to meet the QoS requirements of the application program. The network maintains a state for each flow that is specified by the source and destination I addresses, interface number, and protocol number. Based on the state, the network classifies packets and performs traffic policing, queuing, and scheduling to fulfil its commitment to the application program.

Antiserum can provide the following services:

- Guaranteed service: provides the preset bandwidth and delay to meet the requirements of the application program. For example, a 10 Bit/s bandwidth and a delay less than one second can be provided for Voice over IP (VoIP) services.
- Controlled-load service: If network overload occurs, packets can still be provided with the service similar to that provided in the absence of network overload. That is, when traffic congestion occurs on the network, less delay and high pass rate are ensured for the packets of certain application programs.

1.2.3 Differentiated Service Model

In the differentiated service model, the application program does not need to send its request for network resources before sending packets. Instead, the application program notifies network nodes of its QoS requirements by setting QoS parameters in the IP header.

The differentiated service model is called DiffServ for short. In the model, the application program does not need to send its request for network resource before sending the packets. The application program informs network nodes of its demand for QoS by using QoS parameters in the IP packet header. Then routers along the path obtain the demand by analyzing the header of the packet.

To implement Diff-Serv, the access router classifies packets and marks the class of service (CoS) in the IP packet header. The downstream routers then identify the CoS and forward the packets on the basis of CoS. Diff-Serv is therefore a class-based QoS solution.

Diff-Serv Model in IP Network

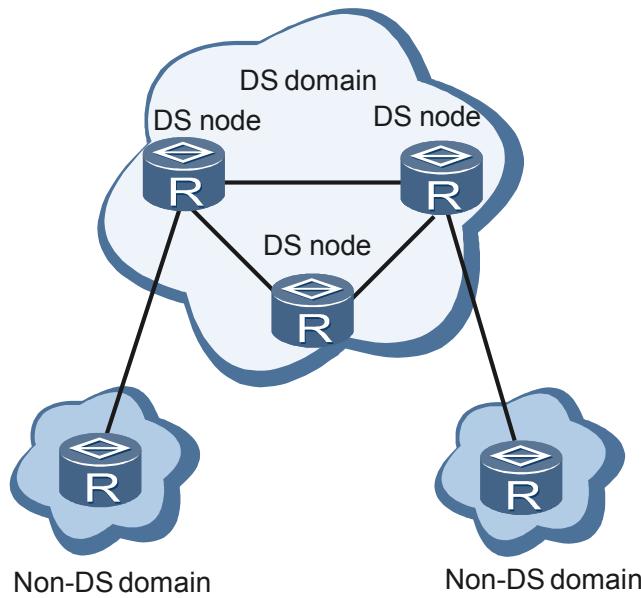
- Diff-Serv Networking

The network node that implements Diff-Serv is called a DS node. A group of DS nodes that adopt the same service policy and the same per-hop behavior (PHB) is called a DS domain. See [Figure 1-1](#).

DS nodes are classified into the following two modes:

- DS border node: Connects DS domain with non-DS domain. This node controls traffic and sets Differentiated Services CodePoint (DSCP) value in packets according to the Traffic Conditioning Agreement (TCA).
- DS interior node: Connects a DS border node with other interior nodes or connects interior nodes in a DS domain. This node carries out only the simple traffic classification and traffic control based on the DSCP value.

Figure 1-1 Diff-Serv networking diagram



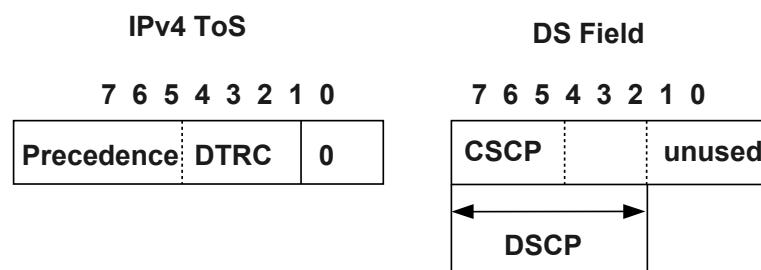
- DS Field and DSCP

The Type of Service (ToS) octet in IPv4 packet header is defined in RFC791, RFC134, and RFC1349. As shown in [Figure 1-2](#), the ToS octet contains the following fields: Precedence: It is of three bits (bits 5 through 7). It indicates the precedence of the IP packet. D bit: It is of one bit and indicates delay. T bit: It is of one bit and indicates throughput. R bit: It is of one bit and indicates reliability. C bit: It is of one bit and indicates cost. The lowest bit of ToS field has to be 0.

The router first checks the IP precedence of packets to implement QoS. The other bits are not fully used.

The ToS octet of IPv4 packet header is redefined in RFC2474, called DS field. As shown in [Figure 1-2](#): The leftmost 6 bits (from 7 through 2) in DS field are used as DSCP. The rightmost 2 bits (1 and 0) are the reserved bits. The leftmost 3 bits (from 7 through 5) are Class Selector CodePoint (CSCP), which indicate a type of DSCP. DS node selects PHB according to the DSCP value.

Figure 1-2 ToS field and DS field



The DSCP field within the DS field is capable of conveying 64 distinct codepoints. The codepoint space is divided into three pools as shown in [Table 1-1](#).

Table 1-1 Classification of DSCP

Code Pool	Code Space	Usage
1	xxxxx0	Standard action
2	xxxx11	EXP/LU (experiment or local use)
3	xxxx01	EXP/LU (can be used as the extended space for future standard action)

Code pool 1 (xxxxx0) is used for standard action, code pool 2 (xxxx11) and code pool 3 (xxxx01) are used for experiment or future extension.

- Standard PHB

The DS node implements the PHB behavior on the data flow. The network administrator can configure the mapping from DSCP to PHB. When a packet is received, the DS node detects its DSCP to find the mapping from DSCP to PHB. If no matching mapping is found, the DS node selects the default PHB (Best-Effort, DSCP=000000) to forward the packet. All the DS nodes support the default PHB.

The following are the four standard PHBs defined by the IETF: Class selector (CS), Expedited forwarding (EF), Assured forwarding (AF) and Best-Effort (BE). The default PHB is BE.

- CS PHB

Service levels defined by the CS are the same as the IP precedence used on the network.

The value of the DSCP is XXX00 where the value of "X" is either 1 or 0. When the value of DSCP is 000000, the default PHB is selected.

- EF PHB

EF means that the flow rate should never be less than the specified rate from any DS node. EF PHB cannot be re-marked in DS domain except on border node. New DSCP is required to meet EF PHB features.

EF PHB is defined to simulate the forwarding of a virtual leased line in the DS domain to provide the forwarding service with low drop ratio, low delay, and high bandwidth.

- AF PHB

AF PHB allows traffic of a user to exceed the order specification agreed by the user and the ISP. It ensures that traffic within the order specification is forwarded. The traffic exceeding the specification is not simply dropped, but is forwarded at lower service priorities.

Four classes of AF: AF1, AF2, AF3, and AF4 are defined. Each class of AF can be classified into three different dropping priorities. AF codepoint AFij indicates AF class is i ($1 \leq i \leq 4$) and the dropping priority is j ($1 \leq j \leq 3$). When providing AF service, the carrier allocates different bandwidth resource for each class of AF.

A special requirement for AF PHB is that the traffic control cannot change the packet sequence in a data flow. For instance, in traffic policing, different packets in a service flow are marked with different dropping priorities even if the packets belong to the same AF class. Although the packets in different service flows have different dropping ratio, their sequence remains unchanged. This mechanism is especially applicable to the transmission of multimedia service.

- BE PHB

BE PHB is the traditional IP packet transmission that focuses only on reachability. All routers support BE PHB.
- Recommended DSCP

Different DS domains can have self-defined mapping from DSCP to PHB. RFC2474 recommends code values for BE, EF, AFij, and Class Selector Codepoints (CSCP). CSCP is designed to be compatible with IPv4 precedence model.

 - BE: DSCP=000000
 - EF: DSCP=101110
 - AFij codepoint

AFij codepoint is shown in [Table 1-2](#).

Table 1-2 AF codepoint

Service Class	Low Dropping Priority, j=1	Medium Dropping Priority, j=2	High Dropping Priority, j=3
AF(i=4)	100010	100100	100110
AF(i=3)	011010	011100	011110
AF(i=2)	010010	010100	010110
AF(i=1)	001010	001100	001110

In traffic policing:

- If j=1, the packet color is marked as green.
- If j=2, the packet color is marked as yellow.
- If j=3, the packet color is marked as red.

The first three bits of the same AF class are identical. For example, the first three bits of AF1j are 001; that of AF3j are 011, that of AF4j are 100. Bit 3 and bit 4 indicate the dropping priority which has three valid values including 01, 10, and 11. The greater the Bit value, the higher the dropping priority.

- Class selector codepoint

In the Diff-Serv standard, the CSCP is defined to make the DSCP compatible with the precedence field of the IPv4 packet header. The routers identify the priority of the packets through IP precedence. The IP precedence and the CSCP parameters map with each other. The user should configure the values for these parameters. In CSCP, the higher the value of DSCP=xxx000 is, the lower the forwarding delay of PHB is.

The default mapping between CSCP and IPv4 precedence is shown in [Table 1-3](#).

Table 1-3 The default mapping between IPv4 precedence and CSCP

IPv4 Precedence	CSCP (in binary)	CSCP (in dotted decimal)	Service Class
0	000000	0	BE
1	001000	8	AF1
2	010000	16	AF2
3	011000	24	AF3
4	100000	32	AF4
5	101000	40	EF
6	110000	48	CS6
7	111000	56	CS7

- Other codepoints

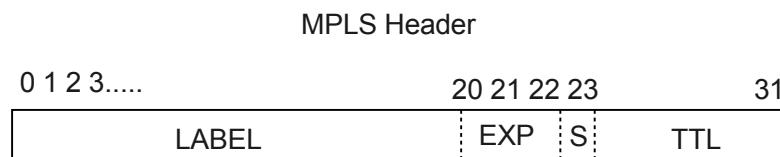
Besides the preceding DSCPs, other DSCPs correspond with BE services.

Diff-Serv Model in the MPLS Network

- EXP field

Defined in RFC3032, MPLS packet header is shown in [Figure 1-3](#). EXP field is of three bits. Its value ranges from 0 to 7 and indicates the traffic type. By default, EXP corresponds to IPv4 priority.

Figure 1-3 Position of EXP field



- Processing QoS Traffic in MPLS Domain

- Processing QoS Traffic on the Ingress Device

On the Ingress device of MPLS domain, you can limit the data flow by setting the Committed Access Rate (CAR) to ensure that the data flow complies with MPLS bandwidth regulations. Besides, you can assign different priorities to the IP packets according to certain policies.

One-to-one mapping can be achieved since the IP precedence field and the EXP field are both 3 bits. In Diff-Serv domain, however, the DSCP field of IP packet is 6 bits, which is different from the length of EXP and thus leads to many-to-one mapping. It is defined that the first 3 bits of DSCP (that is, CSCP) are mapped with EXP.

- Processing QoS Traffic on the Device in the MPLS Domain

When forwarding the MPLS label, the LSR in MPLS carries out queue scheduling according to the EXP field in the labels of packets that are received. This ensures that packets with higher priority enjoy better service.

- Processing QoS Traffic on the Egress Device

On the Egress device of MPLS domain, you need to map EXP field to DSCP field of IP packet. By standard, the first 3 bits of DSCP (that is, CSCP) take the value of EXP, and the last 3 bits take 0.

It should be noted that QoS is an end-to-end solution, while MPLS only ensures that data can enjoy the services regulated in SLA. After the data enters the IP network, IP network ensures QoS.

1.3 Techniques Used for the QoS Application

This section describes functions used for QoS implementation, such as traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance, RSVP, and the link efficiency mechanism.

The primary technologies for implementing DiffServ include:

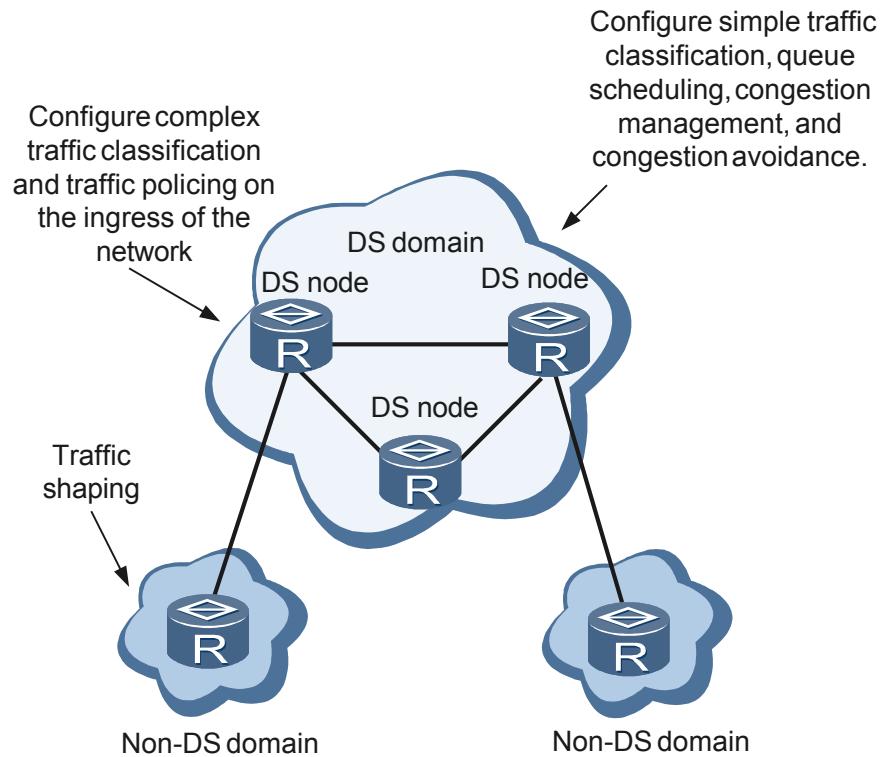
- Traffic classification
- Traffic policing
- Traffic shaping
- Congestion management
- Congestion avoidance

Traffic classification is the basis of the QoS application. With this technique, packets are identified based on certain mapping rules. This is a precondition for providing differentiated services. Traffic policing, traffic shaping, congestion management, and congestion avoidance control the network traffic and resource allocation from different aspects. They feature the DiffServ concept. The following describes these techniques in detail:

- Traffic classification: Identifies objects according to specific rules. It is the prerequisite of Diff-Serv and is used to identify packets according to defined rules.
- Traffic policing: Controls the traffic rate. The rate of the traffic that enters the network is monitored and the traffic exceeding its rate limit is restricted. Only a reasonable traffic range is allowed to pass through the network. This optimizes the use of network resources and protects the interests of the service providers.
- Traffic shaping: Actively adjusts the rate of outputting traffic. It adjusts the volume of output traffic according to the network resources that can be afforded by the downstream router to prevent dropping of packets and congestion.
- Congestion management: Handles resource allocation during network congestion. It stores packets in the queue first, and then takes a dispatching algorithm to decide the forwarding sequence of packets.
- Congestion avoidance: Monitors the usage of network resources, and actively drops packets in case of heavy congestion. This addresses the problem of network overload.

For the common QoS features in the DiffServ model, see [Figure 1-4](#).

Figure 1-4 Common QoS features in the DiffServ model



In the IntServ model, the Resource Reservation Protocol (RSVP) is used as signaling for the transmission of QoS requests. When a user needs QoS guarantee, the user sends a QoS request to the network devices through the RSVP signaling. The request may be a requirement for delay, bandwidth, or packet loss ratio. After receiving the RSVP request, the nodes along the transfer path perform admission control to check the validity of the user and the availability of resources. Then the nodes decide whether to reserve resources for the application program. The nodes along the transfer path meet the request of the user by allocating resources to the user. This ensures the QoS of the user services.

In addition, the link efficiency mechanism carries out packet header compression on low-rate links, which greatly improves the efficiency of links. The headers such as IP headers, and User Datagram Protocol (UDP) headers of packets transmitted on the link layer are compressed through the mechanism. This mechanism applies mainly to PPP link layers.

1.3.1 Traffic Classification

Consisting of complex traffic classification and simple traffic classification, traffic classification classifies packets so that the device can identify packets of various features.

When implementing QoS in Diff-Serv model, the router needs to identify each class of traffic. The following are the two methods for the router to classify traffic:

- Complex traffic classification: This classification is based on IP protocol domain, source IP address range, destination IP address range, DSCP, IP precedence, source port range, destination port range, type and code of ICPMP protocol, type of IGMP protocol.
- Simple traffic classification: This classification is based on IP precedence, DSCP, MPLS EXP, 802.1P precedence in packets. A collection of packets of the same class is called

Behavior Aggregate (BA). Generally, the core router in Diff-Serv domain performs only simple traffic classification.

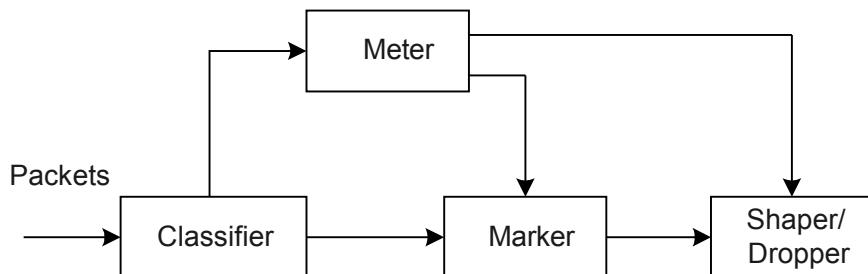
1.3.2 Traffic Policing and Shaping

Traffic policing is used to monitor the volume of the traffic that enters a network and keep it within a reasonable range. In addition, traffic policing optimizes network resources and protects the carriers' interests by restricting the traffic that exceeds the rate limit.

In a Diff-Serv domain, traffic policing, and traffic shaping is completed by the traffic conditioner. A traffic conditioner consists of four parts: Meter, Marker, Shaper, and Dropper as shown in **Figure 1-5**.

- Meter: Measures the traffic and judges whether the traffic complies with the specifications defined in TCS. Based on the result, the router performs other actions through Marker, Shaper, and Dropper.
- Marker: Re-marks the DSCP of the packet, and puts the re-marked packet into the specified BA. The available measures include lowering the service level of the packet flow which does not match the traffic specifications (Out-of-Profile) and maintaining the service level.
- Shaper: Indicates the traffic shaper. Shaper has buffer which is used to buffer the traffic received and ensures that packets are sent at a rate not higher than the committed rate.
- Dropper: Performs the traffic policing action, which controls the traffic by dropping packets so that the traffic rate conforms with the committed rate. Dropper can be implemented by setting the Shaper buffer to 0 or a small value.

Figure 1-5 Traffic policing and shaping



In Diff-Serv, routers must support traffic control on the inbound and outbound interfaces simultaneously. The functions of routers vary with their locations. The functions of a router are as follows:

- The border router processes the access of a limited number of low-speed users. In this way, traffic control on the border router can be completed efficiently. A large amount of traffic classification and traffic control are completed by the border router.
- The core router only performs PHB forwarding of BA to which packets flow belong. In this way, PHB forwarding can be completed with high efficiency, which also meets the requirements of high-speed forwarding by Internet core network.

1.3.3 Congestion Avoidance Configuration

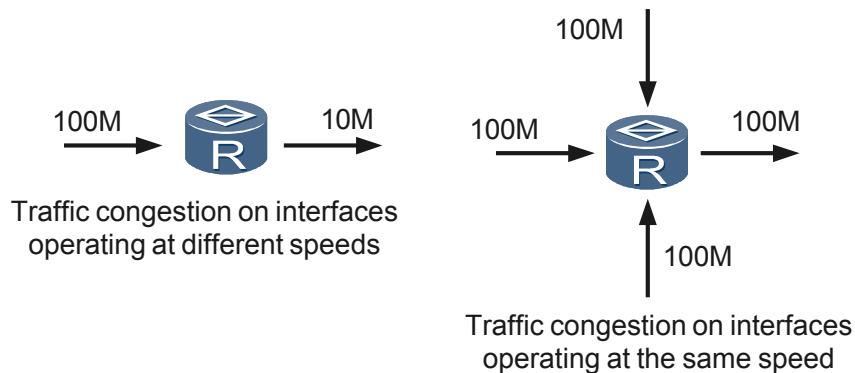
Congestion management creates queues, classifies packets, and places packets into different queues for scheduling. When congestion occurs or intensifies, congestion management allocates proper network resources to various services.

Low QoS in the traditional networks is mainly caused by network congestion. When the available resources temporarily fail to meet the requirements of the service transmission, the bandwidth cannot be ensured. As a result, service rate decreases, resulting in long delay and high jitter. This phenomenon is called congestion.

Causes of Congestion

Congestion often occurs in complex packet switching environment of the Internet. It is caused by the bandwidth bottleneck of two types of links, as shown in [Figure 1-6](#).

Figure 1-6 Schematic diagram of traffic congestion



- Packets enter the router at high rate through v1, and are forwarded at low rate through v2. Congestion occurs in the router because the rate of v1 is greater than that of v2.
- Packets from multiple links enter the router at the rate of v1, v2, and v3. They are forwarded at the same rate of v4 through a single link. Congestion occurs in the router because the total rate of v1, v2, and v3 is greater than that of v4.

Congestion also occurs due to the causes as follows:

- Packets enter the router at line speed.
- Resources such as available CPU time, buffer, or memory used for sending packets are insufficient.
- Packets that arrive at the router within a certain period of time are not well controlled. As a result, the network resources required to handle the traffic exceed the available resources.

Congestion Results

The impact of congestion is as follows:

- Increases the delay and the jitter in sending packets. Long delay can cause retransmission of packets.

- Reduces the efficiency of throughput of the network and result in waste of the network resources.
- Consumes more network resources, particularly storage resources when congestion is aggravated. If not properly allocated, the network resources may be exhausted, and the system may crash.

Congestion is the main cause of low QoS. It is very common in complex networks and must be solved to increase the efficiency of the network.

Congestion Solutions

When congestion occurs or aggravates, queue scheduling and packet discard policies can be used to allocate network resources for traffic of each service class. The commonly used packet discard policies are as follows:

- Tail Drop
When the queue is full, subsequent packets that arrive are discarded.
- Random Early Detection (RED)
When the queue reaches a certain length, packets are discarded randomly. This can avoid global synchronization due to slow TCP start.
- Weighted Random Early Detection (WRED)
When discarding packets, the router considers the queue length and packet precedence. The packets with low precedence are discarded first and are more likely to be discarded.

The NE80E/40E adopts WRED to avoid congestion problems.

1.3.4 RSVP

Through RSVP signaling, requests for resources are transmitted between nodes on the entire network. The nodes then allocate resources based on the priorities of requests.

RSVP is an end-to-end protocol.

Requests for resources are transmitted between nodes through RSVP. The nodes allocate resources at the requests. This is the process of resource reservation. Nodes check the requests against current network resources before determining whether to accept the requests. If the current network resources are quite limited, certain requests can be rejected.

Different priorities can be set for different requests for resources. Therefore, a request with a higher priority can preempt reserved resources when network resources are limited.

RSVP determines whether to accept requests for resources and promises to meet the accepted requests. RSVP itself, however, does not implement the promised service. Instead, it uses the techniques such as queuing to guarantee the requested service.

Network nodes need to maintain some soft state information for the reserved resource. Therefore, the maintenance cost is very high when RSVP is implemented on large networks. RSVP is therefore not recommended for the backbone network.

1.3.5 Link Efficiency Mechanism

The link efficiency mechanism reduces the network load by compressing IP headers before the packets are sent.

IP header compression (IPHC) improves the link efficiency by compressing IP headers of packets before the packets are sent. This mechanism effectively reduces the network load, speeds

up the transmission of Real-Time Transport Protocol (RTP) packets and UDP packets, and saves the bandwidth. IPHC supports the compression of RTP headers and UDP headers.

1.4 QoS Supported by the NE80E/40E

The device supports unicast QoS, multicast QoS, IPv4 QoS, and IPv6 QoS.

The NE80E/40E supports unicast QoS and multicast QoS. The mechanism of multicast QoS is similar to that of unicast QoS; the only difference between them is that multicast packets enter different queues for QoS processing. Therefore, you do not need to perform special configurations.

NE80E/40E supports IPv4 QoS and IPv6 QoS and can classify, re-mark service priorities of, and redirect IPv6 packets.

NE80E/40E supports the following QoS techniques:

- Traffic classification
- Traffic policing
- Traffic shaping
- Congestion avoidance
- Congestion management
- HQoS that enables more specific scheduling
- MPLS DiffServ, MPLS TE, and MPLS DS-TE that enable comprehensive combination between QoS and MPLS
- VPN QoS that enables VPN services with end-to-end QoS deployment

NE80E/40E supports ATM QoS, thus enabling QoS deployment on non-IP networks and delivery of QoS parameters between IP networks and non-IP networks.

2 Traffic Policing and Shaping Configuration

About This Chapter

Traffic policing and traffic shaping are used to monitor and control the volume of traffic on the network.

[2.1 Introduction to Traffic Policing and Shaping](#)

This section describes the basic concepts and implementation principle of traffic policing and traffic shaping.

[2.2 Configuring Interface-based Traffic Policing](#)

By means of traffic policing, the total traffic and burst traffic that enter or leave a network can be controlled. Interface-based traffic policing controls all traffic that is received by an interface without considering the types of packets.

[2.3 Configuring CTC-based Traffic Policing](#)

By means of traffic policing, the total traffic and burst traffic that enter or leave a network can be controlled. By applying complex traffic classification and traffic behaviors, traffic policing controls the volume of the traffic of one or more types within a reasonable range.

[2.4 Configuring Traffic Shaping](#)

Traffic shaping mainly buffers packets that are determined to be dropped by traffic policing by means of the buffer and token bucket.

[2.5 Maintaining Traffic Policing and Shaping](#)

You can clear the statistics on packets in traffic policing and traffic shaping.

[2.6 Configuration Examples](#)

This section provides examples for configuring traffic policing and traffic shaping, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

2.1 Introduction to Traffic Policing and Shaping

This section describes the basic concepts and implementation principle of traffic policing and traffic shaping.

2.1.1 Traffic Policing

Traffic policing is used to restrict the total traffic and burst traffic that enter a network, which provides basic QoS functions to ensure network stability.

Traffic policing (TP) is used to monitor the specifications of the traffic that enters a network and keep it within a reasonable range. In addition, TP optimizes network resources and protects the interests of carriers by restricting the traffic that exceeds the rate limit.

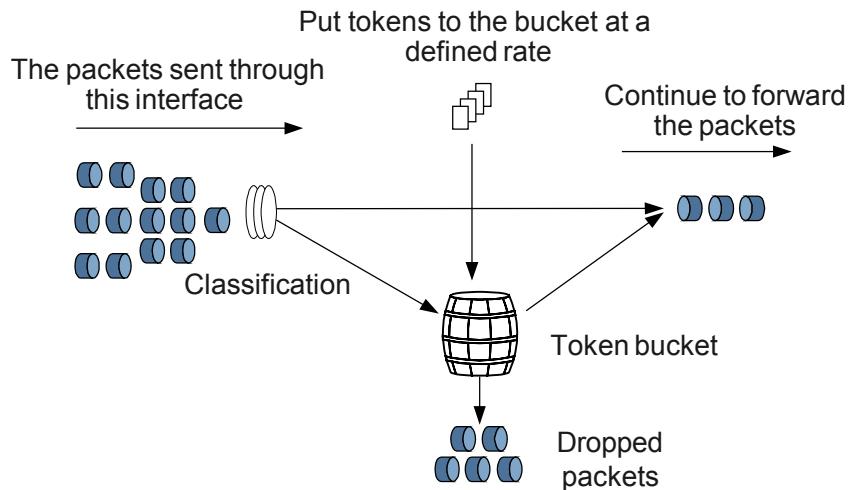
CAR

The Committed Access Rate (CAR) is applied to limit certain categories of traffic. For example, Hypertext Transfer Protocol (HTTP) packets can be kept from taking up more than 50% of the network bandwidth. Packets are first classified according to the pre-defined matching rules. Packets that comply with the specified rate limit are forwarded directly. Packets that exceed the specifications are dropped or have their priorities re-set.

Token Bucket

CAR uses token buckets (TBs) to implement traffic policing. As shown in [Figure 2-1](#), the token bucket is regarded as a container of tokens with a pre-defined capacity. The system puts tokens into the bucket at a defined rate. If the token bucket is full, no more tokens can be added.

Figure 2-1 Traffic policing according to CAR



The process is as follows:

1. If there are enough tokens in the bucket, packets are forwarded. At the same time, the amount of tokens in the bucket decreases based on the length of the packets.
2. If the token bucket does not hold enough tokens for sending packets, the packets are dropped or their priority values are re-set.

- Traffic policing with a single token bucket

A single token bucket can implement traffic measurement in simple situations. When a single token bucket is used, one token is used to forward one byte of data. If there are enough tokens available to forward a packet, the packet is regarded as compliant and is marked green. Otherwise, the packet is regarded as noncompliant or over the limit, and is marked red.

The following are the two parameters used in traffic policing with a single token bucket:

- Committed Information Rate: the rate of putting tokens into the bucket, that is, the permitted average traffic rate.
- Committed Burst Size : the capacity of the token bucket, that is, the maximum amount of traffic. The value of the CBS must be greater than that of the maximum packet size.

A new evaluation is made when a new packet arrives. If there are enough tokens in the bucket for each evaluation, it implies that the packet is within the range. In this case, the number of tokens taken equals the byte size of the forwarded packet.

- Traffic policing with two token buckets

You can use two token buckets to measure traffic in more complex conditions and implement more flexible traffic policing. These two buckets are called C bucket and P bucket. The C bucket places tokens at a rate of the Committed Information Rate (CIR) and its size is called Committed Burst Size (CBS). The P bucket places tokens at a rate of Peak Information Rate (PIR) and its size is called Peak Burst Size (PBS).

Each time the traffic is measured, the following rules are applied:

- If there are enough tokens in C bucket, packets are marked green.
- If there are not enough tokens in C bucket but enough tokens in P bucket, packets are marked yellow.
- If tokens in neither of the buckets are enough, packets are marked red.

The parameters used in traffic policing with two token buckets are described as follows:

- CIR: the rate of putting tokens into C bucket, that is, the permitted average traffic rate of C bucket.
- CBS: the capacity of the C bucket, that is, the maximum amount of traffic of C bucket.
- PIR: the rate of putting tokens into P bucket, that is, the permitted average traffic rate of P bucket.
- PBS: the capacity of the P bucket, that is, the maximum amount of traffic of P bucket.

The NE80E/40E uses two algorithms, srTCM and trTCM, in traffic policing with two token buckets. The algorithms have two working modes, Color-blind and Color-aware. The color-blind mode is more commonly used. For details, refer to "QoS Overview."

Traffic Policing Action

According to different evaluation results, TP implements the pre-configured policing actions, which are described as follows:

- Pass: Forwards the packets evaluated as "compliant" or re-forwards the service marked Differentiated Services Code Point (DSCP) for DiffServ.
- Discard: Drops the packets evaluated as "noncompliant."
- Remark: Changes the precedence of the packet that is evaluated as "partly compliant" and then forwards it.

Statistics Function

It is necessary to control and measure users' traffic on a network. The traditional method of statistics based on the interface has the following disadvantages:

- Of the upstream traffic, only the traffic before CAR operation can be measured. It is impossible to measure the actual traffic of users and the loss of packets that occurs when the traffic rate exceeds the bandwidth limit.
- Of the downstream traffic, only the interface traffic after CAR operation at the egress can be measured. Forwarded and dropped traffic cannot be measured.

To analyze how users' traffic exceeds the limit, carriers have to collect statistics again after CAR. Based on this statistic data, carriers can advise users to buy a higher bandwidth.

With the interface CAR statistics function, the NE80E/40E can measure and record the traffic after upstream CAR operation, that is, the actual access traffic of a company user or an Internet bar, as well as the forwarded and dropped packets after downstream CAR operation. This can help carriers know users' network traffic.

2.1.2 Traffic Shaping

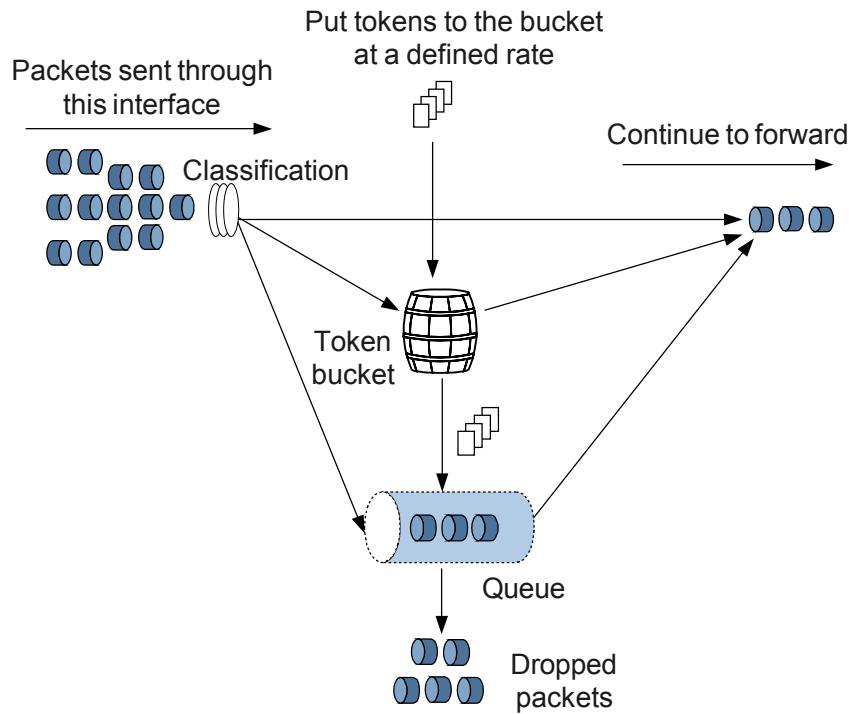
Traffic shaping is used to restrict the total traffic and burst traffic that leave a network, providing basic QoS functions to ensure network stability.

Traffic shaping (TS) is an active way to adjust the traffic output rate. A typical application of TS is to control the volume and burst of outgoing traffic based on the network connection. Thus, the packets can be transmitted at a uniform rate. TS is implemented by using the buffer and token bucket.

As shown in [Figure 2-2](#), after classification, packets are processed as follows:

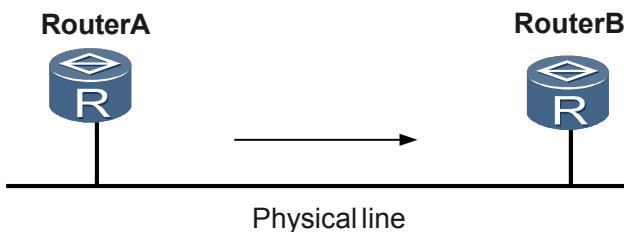
- For packets not involved in TS, the packets are forwarded directly.
- For packets involved in TS, when no General Traffic Shaping (GTS) queue exists, the length of packets is compared with the number of tokens in the token bucket. If there are sufficient tokens to send packets, packets are forwarded normally; if there are insufficient tokens, the GTS queue is enabled where packets are cached. Tokens are placed in the token bucket at a user-defined rate. Packets in the GTS queue are removed and sent periodically. As packets are sent, the number of tokens reduces based on the number of packets. During the course of sending packets, the number of packets is compared with the number of tokens in the token bucket. The number of tokens in the token bucket stops decreasing when all the packets in the GTS queue are sent or can no longer be sent.
- For packets involved in TS, packets enter the GTS queue to wait before being sent periodically, if the GTS queue is enabled.
- If the GTS queue is full when new packets arrive at the queue, the packets are dropped.

Figure 2-2 TS diagram



As shown in [Figure 2-3](#), Router A sends packets to Router B. Router B performs TP on the packets, and directly drops the packets over the traffic limits.

Figure 2-3 Application of traffic policing and shaping



To reduce the number of packets that are dropped, you can use TS on the output interface of Router A. The packets beyond the traffic limits of TS are cached in Router A. While sending the next batch of packets, TS gets the cached packets from the buffer or queues and sends them out. In this manner, all the packets sent to Router B abide by the traffic regulation of Router B.

The main difference between TS and TP is that TS buffers the packets which exceed the traffic limits. When there are enough tokens in the token bucket, these buffered packets are sent out at a uniform rate. Another difference is that TS may prolong delay but TP causes almost no extra delay.

2.1.3 Traffic Policing and Shaping Supported by NE80E/40E

Traffic policing and traffic shaping are implemented by means of the CAR, buffer, and token bucket. Using these methods, the device can buffer packets before traffic policing and traffic shaping are implemented.

NE80E/40E supports traffic policing and shaping. It includes:

- Interface-based traffic policing.
- Interface-based statistics function of CAR. It can measure the interface upstream traffic after CAR operation.
- CTC-based traffic policing. CoSs and color of packets can be re-marked after traffic policing.
- Traffic shaping on the outbound interface and the multicast tunnel interface (MTI) in distributed multicast VPN.



The LPUF-21 and LPUF-40, LPUI-41 and LPUS-41, LPUI-100 and LPUF-100 support distributed multicast VPN.

Multicast VPN transmits multicast data in the MPLS/BGP VPN. The NE80E/40E adopts the multicast domains (MD) mechanism to implement multicast VPN, which is called MD VPN for short. In an MD, private data is transmitted through the multicast tunnel (MT). The VPN instance delivers the private data through MTI, and then the remote end receives the private data through MTI.

For detailed explanation on multicast VPN and its configurations, refer to HUAWEI NetEngine80E/40E Router *Configuration Guide -- IP Multicast*.

2.2 Configuring Interface-based Traffic Policing

By means of traffic policing, the total traffic and burst traffic that enter or leave a network can be controlled. Interface-based traffic policing controls all traffic that is received by an interface without considering the types of packets.

Context



- This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.
- You can obtain CAR statistics of the following interfaces: Ethernet interfaces, POS interfaces, Ethernet sub-interfaces (excluding QinQ sub-interface), and Layer 2 Ethernet ports, GRE Tunnel interface, Eth-Trunk interface, Layer 2 Eth-Trunk interface, Eth-Trunk sub-interface, and IP-Trunk interface. Note that when you query the statistics of Layer 2 ports, you must specify a VLAN.
- Interface-based traffic policing does not differentiate unicast, multicast, or broadcast packets.

2.2.1 Establishing the Configuration Task

Before configuring interface-based traffic policing, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

If users' traffic is not limited, burst data from numerous users can make the network congested. To optimize the use of network resources, you need to limit users' traffic. Traffic policing is a

traffic control method that limits network traffic and control the usage of network resources by monitoring network specifications. Traffic policing can be implemented on both inbound interfaces and outbound interfaces.

Traffic policing based on the interface controls all traffic that enters an interface without differentiating types of packets. This method is used on core routers of a network.

Pre-configuration Tasks

Before configuring TP, complete the following tasks:

- Configuring the physical parameters of interfaces
- Configuring the link layer attributes of interfaces to ensure normal operation of the interfaces
- Configuring IP addresses for interfaces (This is done when you configure CAR on Layer 3 interfaces.)
- Enabling routing protocols and ensuring that routers interwork with each other (This is done when you configure CAR at Layer 3 interfaces.)

Data Preparation

To configure traffic policing, you need the following data:

No.	Data
1	CIR, PIR, CBS, and PBS
2	Interfaces where CAR and directions (inbound or outbound) are configured



NOTE

- When an interface is configured with both interface-based CAR and traffic classification-based CAR actions, the number of packets and bytes on which traffic classification-based CAR actions are performed is not counted in the interface-based CAR statistics.
- When a Layer 2 interface is configured with both interface-based CAR and suppression of broadcast, multicast, and unknown unicast traffic, the number of broadcast, multicast, and unknown unicast packets and bytes that are suppressed is not counted in the interface-based CAR statistics.
- When both the ACL-based CAR and the interface-based CAR are configured, only the ACL-based CAR statistics are collected; when both the broadcast suppression CAR and the interface-based CAR are configured, only the CAR statistics on broadcast suppression are collected; when CAR is configured for both packets sent to the CPU and packets sent to the interface, only the CAR statistics on packets sent to the CPU are collected.

2.2.2 Configuring CAR on a Layer 3 Interface

You can configure traffic policing in both inbound and outbound directions on Layer 3 main interfaces by using a single token bucket or double token buckets.

Context



NOTE

You can configure traffic policing for the NE80E/40E only on the Ethernet, POS, Ethernet (excluding QinQ), Eth-Trunk sub-interface or IP-Trunk interface.

The NE80E/40E supports configuration of traffic policing in both inbound and outbound directions on major Layer 3 interfaces. Traffic policing includes two types: STB traffic policing and DTB traffic policing.

- If the network traffic is simple, you can configure STB traffic policing with parameters **cir** and **cbs**.
- If the network traffic is complex, you need to configure DTB traffic policing with parameters **cir**, **pir**, **cbs**, and **pbs**.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
qos car { cir cir-value [ pir pir-value ] } [ cbs cbs-value pbs pbs-value ]
[ green { discard | pass [ service-class class color color ] } | yellow { discard
| pass [ service-class class color color ] } | red { discard | pass [ service-
class class color color ] } ]* { inbound | outbound }
```

The interface is configured with CAR.

Only LPUA, LPUG, LPUH, LPUF-10 support discard the green packets.

----End

Follow-up Procedure

If packets are re-marked to service classes of EF, BE, CS6, and CS7, these packets can only be re-marked green in color.

2.2.3 Configuring CAR on a Layer 2 Port

You can configure traffic policing in both inbound and outbound directions on Layer 2 main interfaces by using a single token bucket or double token buckets.

Context

The NE80E/40E supports configuration of traffic policing in both inbound and outbound directions on Layer 2 interfaces.

- To configure STB traffic policing, select parameters **cir** and **cbs**.
- To configure DTB traffic policing, select parameters **cir**, **pir**, **cbs** and **pbs**.
- To configure inbound traffic policing, select the parameter **inbound**.
- To configure outbound traffic policing, select the parameter **outbound**.



NOTE You can configure traffic policing for the NE80E/40E only on the physical GE and Ethernet interfaces.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface { ethernet | gigabitethernet } interface-number
```

The interface view is displayed.

Step 3 Run:

```
portswitch
```

The Layer 2 interface view is displayed.

Step 4 Run the following command as required:

- Run:

```
port default vlan vlan-id
```

A Layer 2 interface is added to a specified VLAN.



Please confirm the specified VLAN has been created before running this command.

- Run:

```
port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } & <1-10> | all }
```

The IDs of the VLANs allowed by the current interface are specified.

Step 5 Run:

```
qos car { cir cir-value [ pir pir-value ] } [ cbs cbs-value pbs pbs-value ] [ green
[ discard | pass [ service-class class color color ] ] | yellow { discard | pass
[ service-class class color color ] } | red { discard | pass [ service-class class
color color ] } ]* { inbound | outbound } [ vlan { vlan-id1 [ to vlan-id2 ]
&<1-10> } ]
```



CAR is configured on an interface. The parameter [vlan { vlan-id1 [to vlan-id2] &<1-10> }] takes effect only on layer 2 interfaces, and VLAN ID must be configured. When this command is configured on a layer 3 interface, however, VLAN ID cannot be configured.

Only LPUA, LPUG, LPUH, LPUF-10 support discard the green packets.

----End

Follow-up Procedure

If packets are re-marked to service classes of EF, BE, CS6, and CS7, these packets can only be re-marked green in color.

2.2.4 Checking the Configuration

After traffic policing is configured on an interface, you can view the CAR statistics on traffic in a specified direction on Layer 2 and 3 interfaces.

Context

Run the following commands to check the previous configuration.

Procedure

- Using the **display interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check the traffic information about an interface.
- Using the **display car statistics interface** *interface-type* *interface-number* [.*sub-interface*] { **inbound** | **outbound** } command to check the CAR statistics on a Layer 3 interface of a specified direction.
- Using the **display car statistics interface** *interface-type* *interface-number* **vlan** *vlan-id* { **inbound** | **outbound** } command to check the CAR statistics on a Layer 2 port of a specified direction.

----End

Example

Using the **display car statistics interface** *interface-type* *interface-number* [.*sub-interface*] { **inbound** | **outbound** } command, you can view the statistics on an interface of a specified direction. The statistics include the number of passed packets, number of passed bytes, and rate of passed packets; number of dropped packets, number of dropped bytes, and rate of dropped packets. For example:

```
<HUAWEI> display car statistics interface gigabitEthernet 6/0/0 outbound
interface GigabitEthernet6/0/0
    outbound
        Committed Access Rate:
        CIR 200(Kbps), PIR 0(Kbps), CBS 400(byte), PBS 500(byte)
        Conform Action: pass
        Yellow Action: pass
        Exceed Action: discard
        Passed: 840 bytes, 15 packets
        Dropped: 56 bytes, 1 packets
        Last 30 seconds passed rate: 0 bps, 0 pps
        Last 30 seconds dropped rate: 0 bps, 0 pps
```

2.3 Configuring CTC-based Traffic Policing

By means of traffic policing, the total traffic and burst traffic that enter or leave a network can be controlled. By applying complex traffic classification and traffic behaviors, traffic policing controls the volume of the traffic of one or more types within a reasonable range.

2.3.1 Establishing the Configuration Task

Before configuring traffic policing, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

There are a large number of users in the network and they send data constantly. This can cause network congestion and have a great impact on the operation and service quality of the network.

Therefore, to guarantee the bandwidth no matter the network is idle or congested, traffic control needs to be implemented on one or several types of packets. You can combine complex traffic

classification (CTC) and traffic control to configure the traffic policing policy based on complex traffic classification. Then, apply the policy to the inbound interface to restrict the traffic of the specific packets within a reasonable range. Therefore limited network resources are better utilized.

 **NOTE**

CTC means classifying packets based on the quintuple that includes the source address, source port number, protocol number, destination address, and destination address. It is usually implemented on the border routers in the network.

Pre-configuration Tasks

Before configuring CTC-based traffic policing, you need to complete the following pre-configuration tasks:

- Configure the physical parameters for related interfaces
- Configure the link layer attributes for related interfaces to ensure normal operation of the interfaces
- Configure IP addresses for related interfaces
- Enable the routing protocols for reachability

Data Preparation

The following data is necessary for configuring CTC-based traffic policing.

No.	Data
1	Class name
2	ACL number, source MAC address, destination MAC address, IP precedence, DSCP value, 802.1p value, and TCP flag value
3	Traffic behavior name
4	CIR, PIR, CBS, and PBS
5	Policy name
6	Interface type and number where the traffic policy is applied

2.3.2 Defining Traffic Classes

You need to define traffic classifiers before configuring complex traffic classification. Traffic can be classified based on ACL rules, IP precedence, MAC addresses, and multicast addresses used by protocols.

Context



NOTE

- If traffic classification is based on Layer 3 or Layer 4 information, the traffic policy can be applied to Layer 3 interface.
- If traffic classification is based on Layer 2 information, the traffic policy can be applied to both Layer 3 interface and Layer 2 port. To apply such a traffic policy to a Layer 2 port or a Layer 3 interface, specify the key word **link-layer** in the command line.

Procedure

- Defining traffic classification based on layer 3 or layer 4 information

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic classifier classifier-name [ operator { and | or } ]
```

A traffic classifier is defined and the view of the classifier is displayed.

3. Choose the desired matching rule according to your requirements:

- To set a matching rule to classify traffic based on the ACL number, Run:

```
if-match [ ipv6 ] acl { acl-number | name acl-name }
```

- To set a matching rule to classify traffic based on the DSCP value, Run:

```
if-match [ ipv6 ] dscp dscp-value
```

- To set a matching rule to classify traffic based on the TCP flag, Run:

```
if-match tcp syn-flag tcpflag-value
```

- To set a matching rule to classify traffic based on the IP precedence, Run:

```
if-match ip-precedence ip-precedence
```

- To match all packets, Run:

```
if-match [ ipv6 ] any
```

- To set a matching rule to classify traffic based on the source IPv6 address, Run:

```
if-match ipv6 source-address ipv6-address prefix-length
```

- To set a matching rule to classify traffic based on the destination IPv6 address, Run:
Run:

```
if-match ipv6 destination-address ipv6-address prefix-length
```

A matching rule is set to classify traffic.



NOTE

If both the **if-match [ipv6] acl acl-number** command and the **if-match [ipv6] any** command are configured, the command that is configured first takes effect before the other.

To match IPv6 packets, you must specify the key word **ipv6** when you choose a matching rule in Step 3. A matching rule defined to match packets based on source or destination addresses is valid only with IPv6 packets, but not with IPv4 packets.

If you set more than one matching rule for the same classifier, you can set their relations by specifying the parameter operator in step 2:

- Logic operator **and**: A packet belongs to the classifier only when it matches all the rules.

- Logic operator **or**: A packet belongs to the classifier if it matches one of the rules.
- By default, the logic operator of the rules is **or**.
- Defining traffic classification based on layer 2 information

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic classifier classifier-name [ operator { and | or } ]
```

A traffic classifier is defined and the view of the classifier is displayed.

3. Choose the desired matching rule according to your requirements:

- To set a matching rule to classify VLAN packets based on the value of the 802.1p field, Run:

```
if-match 8021p 8021p-value
```

- To set a matching rule to classify traffic based on the source MAC address, Run:

```
if-match source-mac mac-address
```

- To set a matching rule to classify traffic based on the destination MAC address, Run:

```
if-match destination-mac mac-address
```

- To set a matching rule to classify traffic based on MPLS EXP, Run:

```
if-match mpls-exp exp-value
```

If you set more than one matching rule for the same classifier, you can set their relations by specifying the parameter **operator** in step 2:

- Logic operator **and**: A packet belongs to the classifier only when it matches all the rules.
- Logic operator **or**: A packet belongs to the classifier if it matches one of the rules.
- By default, the logic operator of the rules is **or**.

----End

2.3.3 Defining a Behavior and Configuring Traffic Policing Actions

You can configure traffic policing actions for different traffic classifiers.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic behavior behavior-name
```

A traffic behavior is set and the behavior view is displayed.

Step 3 Run:

```
car { cir cir-value [ pir pir-value] } [ cbs cbs-value pbs pbs-value ] [ green
{ discard | pass [ service-class class color color ] } | yellow { discard | pass
[ service-class class color color ] } | red { discard | pass [ service-class class
color color ] } ]*
```

A traffic policing action is set for the traffic behavior.

In step 3, choose parameters according to your requirement:

- To set traffic policing with a single token bucket, select **cir** and **cbs**, and set the value of **pbs** to 0.
- To set traffic policing with double token buckets, select **cir**, **cbs**, and **pbs**.
- Use parameters **cir**, **pir**, **cbs**, and **pbs** to configure traffic policing with two rates and two token buckets.

----End

Follow-up Procedure

The NE80E/40E supports marking the priority and color of packets after traffic policing. If packets are re-marked as the service levels of ef, be, cs6, and cs7, the packet color can only be re-marked in green.

2.3.4 Configuring a Traffic Policy

After defining traffic classifiers and traffic behaviors, you need to configure a traffic policy in which the traffic classifiers and traffic behaviors are associated.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic policy policy-name
```

A policy is defined and the view of the policy is displayed.

Step 3 Run:

```
classifier traffic-class-name behavior behavior-name [ precedence precedence ]
```

The specified behavior and classifier are associated in the policy.

When the parameter **precedence precedence** is specified, the classifier is performed as the precedence. The small the value, the higher the precedence, meaning that the action of the classifier is preferentially performed.

----End

2.3.5 Applying the Traffic Policy

A class-based traffic policy takes effect only after being applied to an interface.

Procedure

- Applying Traffic Policies to Layer 3 Interfaces

 **NOTE**

- This product supports traffic policies on physical interfaces POS ports and GE ports, as well as logical interfaces, such as the sub-interface, ring-if, IP-Trunk and Eth-Trunk interface.
- Traffic policies cannot be directly applied to the VLANIF interface. They can be implemented by combining physical or Eth-trunk interfaces with VLAN IDs.
- If traffic is to be classified on a layer 3 interface based on layer 2 information 802.1p, the interface must be a sub-interface.

Do as follows on the router.

1. Run:

`system-view`

The system view is displayed.

2. Run:

`interface interface-type interface-number`

The specified interface view is displayed.

3. Run:

`traffic-policy policy-name { inbound | outbound } [link-layer | all-layer | mpls-layer]`

The specified traffic policy is applied to the interface.

If the parameter **all-layer** is specified, the system performs the complex classification according to Layer 2 information about packets. If the Layer 2 information about a packet fails to match the classification rules, the system goes on with the Layer 3 or Layer 4 information about the packet.

Only LPUA, LPUG, LPUH, LPUF-10 support to specify the parameter **all-layer**.

Only the LPUI-41, LPUS-41, LPUI-100, and LPUF-100 support to specify the parameter **mpls-layer**.

By default, the system performs the complex traffic classification according to Layer 3, Layer 4, or other information.

When applying a traffic policy to a Layer 3 interface, you can specify traffic classification based on Layer 2, Layer 3 or Layer 4 information about the packet.

In step 3, choose parameters according to your requirements:

- To configure complex classification of the incoming traffic, choose the parameter **inbound**.
- To configure complex classification of the outgoing traffic, choose the parameter **outbound**.

- Applying the Traffic Policy to Layer 2 Interfaces

Do as follows on the router.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface { ethernet | gigabitethernet | eth-trunk } interface-number
```

The specified interface view is displayed.

3. Run:

```
portswitch
```

The interface changes to a layer 2 interface.

4. Run:

```
traffic-policy policy-name { inbound | outbound } [ vlan vlan-id1 [ to  
vlan-id2 ] ] [ link-layer | all-layer | mpls-layer ]
```

The specified traffic policy is applied to the layer 2 port.

 **NOTE**

If you apply a traffic policy to the VLAN traffic on a Layer 2 interface, you need to configure the **port trunk allow-pass vlan { { vlan-id1 [to vlan-id2] } & <1-10> | all }** or the **port default vlan vlan-id** command on the Layer 2 interface.

If you apply a traffic policy without specifying a VLAN, the traffic policy is applied to the VLAN switch services that pass through the interface or the service traffic that is added to PBB-TE in interface mode.

When applying a traffic policy to VLAN switch services on a Layer 2 interface or the service traffic that is added to PBB-TE in interface mode, you do not need to specify a VLAN ID. You must, however, specify a VLAN ID when you apply a traffic policy to the VLAN traffic that goes through a Layer 2 interface.

If no VLAN is specified, a traffic policy is applied to the VLAN switch service traffic that flows through the interface.

You do not need to specify a VLAN ID if you apply a traffic policy to VLAN switch service traffic on a Layer 2 interface. You must, however, specify a VLAN ID if you apply a traffic policy to the VLAN traffic that goes through a Layer 2 interface.

Only LPUA, LPUG, LPUH, LPUF-10 support to specify the parameter **all-layer**.

Only the LPUI-41, LPUS-41, LPUI-100, and LPUF-100 support to specify the parameter **mpls-layer**.

If the parameter **link-layer** is not specified for the traffic policy applied to the upstream and downstream traffic on a Layer 2 interface of the LPUI-41, LPUS-41, LPUI-100, or LPUF-100, Layer 3 information can be used for traffic classification.

- To configure complex classification of the incoming traffic, use parameter **inbound**.
- To configure complex classification of the outgoing traffic, use parameter **outbound**.

----End

2.3.6 Checking the Configuration

After traffic policing based on complex traffic classification is configured, you can view information about the configured traffic classifiers, traffic behaviors, traffic policies in which the specified classifiers and behaviors are associated, and traffic statistics on interfaces.

Context

Use the following **display** commands to check the configuration.

Procedure

- Using the **display interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check the traffic of an interface.
- Using the **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] command to check the traffic behavior.
- Using the **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*] command to check the classifier.
- Using the **display traffic policy interface brief** [*interface-type* [*interface-number*]] command to check information about traffic policies configured on a specified interface or all interfaces.
- Using the **display traffic policy** { **system-defined** | **user-defined** } [*policy-name* [classifier *classifier-name*]] command to check the associated behavior and classifier in the traffic policy.

----End

Example

If the configuration succeeds,

- The name of the configured traffic behavior and the actions are displayed if you run the **display traffic behavior** command:

```
<HUAWEI> display traffic behavior user-defined
User Defined Behavior Information:
  Behavior: database
  Redirecting:
    Redirect Ip-NextHop 20.13.9.3
  RefedByPolicyNum : 0
  Behavior: huawei
  Marking:
    Remark IP Precedence 4
  Committed Access Rate:
    CIR 1000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 0 (byte)
    Conform Action:
  Committed Access Rate:
    CIR 1000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 0 (byte)
    Conform Action: pass
    Yellow Action: pass
    Exceed Action: discard
  RefedByPolicyNum : 1,
  PolicyName : test - test
```

- The name of the configured traffic classifier and its matching rules, as well as the logical operator of the rules are displayed if you run the **display traffic classifier** command:

```
<HUAWEI> display traffic classifier user-defined
User Defined Classifier Information:
  Classifier: database
  Operator: OR
  Rule(s) : if-match acl 3000
  RefedByPolicyNum : 0
  PolicyName : database
  Classifier: huawei
  Operator: AND
  Rule(s) : if-match ip-precedence 3
  RefedByPolicyNum : 0
  PolicyName : database
```

- The name of the configured traffic policy and the associated behavior and classifier are displayed if you run the **display traffic policy** command:

```
<HUAWEI> display traffic policy user-defined
```

```
User Defined Traffic Policy Information:  
Policy: test  
Share-mode  
Classifier: default-class  
Behavior: be  
-none-  
Classifier: huawei  
Behavior: huawei  
Marking:  
    Remark IP Precedence 4  
Committed Access Rate:  
    CIR 1000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 0 (byte)  
    Conform Action:  
        Committed Access Rate:  
        CIR 1000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 0 (byte)  
        Conform Action: pass  
        Yellow Action: pass  
        Exceed Action: discard
```

2.4 Configuring Traffic Shaping

Traffic shaping mainly buffers packets that are determined to be dropped by traffic policing by means of the buffer and token bucket.

2.4.1 Establishing the Configuration Task

Before configuring traffic shaping, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

When the traffic is heavy on the network, the packets that exceed specifications will be dropped. To avoid network congestion or loss of packets at the downstream network caused by too much traffic sent from the upstream network, you can configure traffic shaping on the outbound interface of the upstream router. Traffic shaping refers to restricting the packets of a specific connection flowing out of a network so that the packets are sent out at an even rate.

TS is usually carried out with cache buffer and token buckets. When the rate for sending packets is too high, packets are first placed in buffer queue, and then are forwarded steadily. The forwarding of packets is controlled by the token bucket, based on the priority of the queue. This can avoid retransmission of the packet.

Pre-configuration Tasks

Before configuring TS, you need to complete the tasks as follows:

- Configure the physical parameters of related interfaces
- Configure the link layer attributes of related interfaces to ensure normal operation of the interface
- Configure IP addresses for related interfaces
- Enable routing protocols so that routes are reachable

Data Preparation

To configure TS, you need the following data.

No.	Data
1	Interface to be configured with TS
2	TS rate

2.4.2 Configuring Traffic Shaping

You can configure traffic shaping to control the total traffic and burst traffic that leave the network. In this manner, traffic can be transmitted at an even rate, which is conducive to bandwidth allocation.

Context



You should configure traffic shaping for an interface in the interface view, and configure traffic shaping for an MTI that is bound to distributed multicast VPN in the slot view.

Procedure

- Configuring Traffic Shaping in the Interface View

Do as follows on the router:

At present, the NE80E/40E supports TS only on the outbound interface.

The NE80E/40E distributes resources to services of specific classes such as EF and AF through the pre-defined queue scheduling mechanism. Users need not configure queue management.

- Run:

```
system-view
```

The system view is displayed.

- Run:

```
interface interface-type interface-number
```

The specified interface view is displayed.

- Run:

```
port shaping shaping-value [ pbs pbs-value ]
```

TS is configured on the interface. You can perform TS for the outgoing traffic on the interface.

- Configuring Traffic Shaping for MTI in the Slot View

Do as follows on the router:

- Run:

```
system-view
```

The system view is displayed.

- Run:

```
slot slot-id
```

The slot view is displayed.

3. Run:

```
port shaping shaping-value bind mtunnel
```

Traffic shaping is configured for MTI that is bound to the distributed multicast VPN.

----End

2.4.3 Checking the Configuration

After traffic shaping is configured, you can view the traffic shaping configurations and relevant statistics on an interface.

Context

Run the following **display** commands to check the previous configuration.

Procedure

- Using the **display interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check information about traffic of an interface.

----End

2.5 Maintaining Traffic Policing and Shaping

You can clear the statistics on packets in traffic policing and traffic shaping.

2.5.1 Clearing Statistics of CAR

This section describes how to clear CAR statistics.

Context

To clear the CAR statistic information, run the following **reset** commands in the user view.

Procedure

- Run the **reset car statistics interface** *interface-type* *interface-number* [*.sub-interface*] { **inbound** | **outbound** } command to clear the CAR statistics of a Layer 3 interface in a direction.
- Run the **reset car statistics interface** *interface-type* *interface-number* **vlan** *vlan-id* { **inbound** | **outbound** } command to clear the CAR statistics of a Layer 2 port in a direction.

----End

2.6 Configuration Examples

This section provides examples for configuring traffic policing and traffic shaping, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

 NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

2.6.1 Example for Configuring Traffic Policing and Traffic Shaping

This section takes the traffic control scenario as an example to describe how to configure traffic policing and traffic shaping. The total traffic can be restricted through traffic policing and traffic shaping.

Networking Requirements

As shown in **Figure 2-4**, the POS3/0/0 of Router A is connected with the POS1/0/0 of Router B. Server, PC1 and PC2 can access the Internet through Router A and Router B.

Server, PC1 and the GE1/0/0 of Router A are on the same network segment. PC2 and the GE2/0/0 of Router A are on the same network segment.

The process to control traffic from Server and PC1 received by the GE1/0/0 of Router A is as follows:

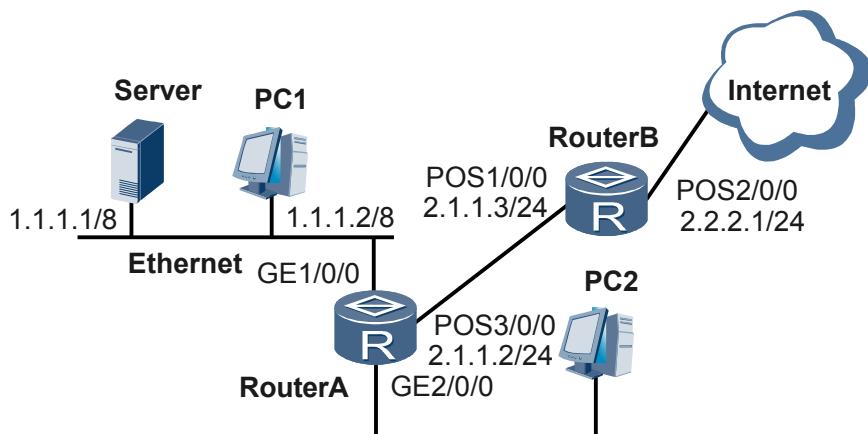
- A bandwidth of up to 6 Mbit/s is assured for traffic from Server. The default value is 5 Mbit/s and the maximum value is not more than 6 Mbit/s. For traffic whose rate is beyond 5 Mbit/s but is within the assured rate of 6 Mbit/s, packets are forwarded properly. When the traffic rate exceeds 6 Mbit/s, the packets are sent in the BE fashion.
- The rate-limit on traffic from PC1 is 2 Mbit/s. Traffic below this rate-limit can be transmitted properly. When the traffic exceeds this rate-limit, packets are dropped.

In addition, the POS3/0/0 and POS2/0/0 of Router A and Router B should meet the following requirements for sending and receiving packets:

- The rate-limit on the traffic that travels from the POS 3/0/0 of Router A to Router B is 20 Mbit/s. When the traffic exceeds this rate-limit, packets are dropped.
- The rate-limit on traffic going to the Internet through the POS2/0/0 of Router B is 30 Mbit/s. When the traffic exceeds this rate-limit, packets are dropped.

Networking Diagram

Figure 2-4 Networking diagram of TS



Configuration Roadmap

The configuration roadmap is as follows:

1. On the inbound interface GE 1/0/0 of Router A, perform traffic policing based on complex traffic classification on traffic from Server and PC1.
2. On the outbound interface POS 3/0/0 of Router A, configure traffic shaping and restrict the rate of the traffic that goes into Router B to 20 Mbit/s.
3. On the outbound interface POS 2/0/0 of Router B, configure traffic shaping and restrict the rate of the traffic that goes into the Internet to 30 Mbit/s.

Data Preparation

To complete the configuration, you need the following data:

- The ACL number, traffic classifier name, traffic behavior name, traffic policy name, and the interface where the traffic policy is applied, of Server and PC1
- CIR, PIR, CBS, and PBS
- Traffic rate for traffic shaping and the interface where traffic shaping is configured

Procedure

Step 1 Configure IP addresses for interfaces (The detailed configuration is not mentioned here).

Step 2 Configure Router A.

Configure an ACL for matching data flows from Server and PC1.

```
<RouterA> system-view
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[RouterA-acl-basic-2001] quit
[RouterA] acl number 2002
[RouterA-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
[RouterA-acl-basic-2002] quit
```

Configure traffic classes and define ACL-based class matching rules.

```
[RouterA] traffic classifier class1
[RouterA-classifier-class1] if-match acl 2001
[RouterA-classifier-class1] quit
[RouterA] traffic classifier class2
[RouterA-classifier-class2] if-match acl 2002
[RouterA-classifier-class2] quit
```

Define a behavior so that the default rate-limit on traffic from Server is 5 Mbit/s. Set the upper limit to 6 Mbit/s: When the traffic rate is higher than 5 Mbit/s but below 6 Mbit/s, packets are forwarded properly; when the traffic rate exceeds 6 Mbit/s, packets are sent in the BE fashion.

```
[RouterA] traffic behavior behavior1
[RouterA-behavior-behavior1] car cir 5000 pir 6000 green pass yellow pass red pass
service-class be color green
[RouterA-behavior-behavior1] quit
```

Define a behavior so that the rate-limit is 2 Mbit/s. When the traffic rate exceeds 2 Mbit/s, packets are dropped.

```
[RouterA] traffic behavior behavior2
```

```
[RouterA-behavior-behavior2] car cir 2000 green pass yellow discard red discard
[RouterA-behavior-behavior2] quit

# Define a policy to associate classes with behaviors.

[RouterA] traffic policy policy1
[RouterA-trafficpolicy-policy1] classifier class1 behavior behavior1
[RouterA-trafficpolicy-policy1] classifier class2 behavior behavior2
[RouterA-trafficpolicy-policy1] quit

# Apply the policy to GE1/0/0.

[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] traffic-policy policy1 inbound

# Configure TS on POS3/0/0 of Router A to shape the EF traffic on the interface (EF traffic beyond than 20 Mbit/s is dropped) to lower the packet loss ratio on POS1/0/0 of Router B.

[RouterA] interface pos 3/0/0
[RouterA-Pos3/0/0] undo shutdown
[RouterA-Pos3/0/0] port shaping 20
```

Step 3 Configure Router B.

Shape the traffic on POS2/0/0.

```
<RouterB> system-view
[RouterB] interface pos2/0/0
[RouterB-Pos2/0/0] undo shutdown
[RouterB-Pos2/0/0] port shaping 30
[RouterB-Pos2/0/0] return
```

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
acl number 2001
rule 5 permit source 1.1.1.1 0
acl number 2002
rule 5 permit source 1.1.1.2 0
#
traffic classifier class1
if-match acl 2001
traffic classifier class2
if-match acl 2002
#
traffic behavior behavior1
car cir 5000 pir 6000 green pass yellow pass red pass service-class be color
green
traffic behavior behavior2
car cir 2000 green pass yellow discard red discard
#
traffic policy policy1
classifier class1 behavior behavior1
classifier class2 behavior behavior2
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 1.1.1.3 255.255.255.0
traffic-policy policy1 inbound
#
interface Pos3/0/0
undo shutdown
```

```
ip address 2.1.1.2 255.255.255.0
port shaping 20
#
ospf 1
area 0.0.0.0
network 1.1.1.0 0.255.255.255
network 2.1.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
interface Pos 2/0/0
undo shutdown
ip address 2.2.2.1 255.255.255.0
port shaping 30
#
ospf 1
area 0.0.0.0
network 2.2.2.0 0.0.0.255
network 2.1.1.0 0.0.0.255
#
return
```

3 Congestion Avoidance Configuration

About This Chapter

You can adjust network traffic to prevent packet loss caused by network congestion and adopt a proper packet-dropping policy when network congestion occurs.

 **NOTE**

Queue Scheduling for Low-Speed Links cannot be configured on the X1 and X2 models of the NE80E/40E.

[3.1 Introduction to Congestion Avoidance](#)

This section describes traffic control policies.

[3.2 Configuring WRED](#)

Using WRED, you can set thresholds for random packet drop. This can prevent multiple TCP connections from reducing their transmitting rates at the same time and accordingly prevent global TCP synchronization.

[3.3 Configuring Queue Scheduling for Low-Speed Links](#)

On low-speed links, congestion is likely to occur due to limited network resources. To prevent packets from being indiscriminately dropped in the case of congestion, traffic flows need to be placed in different FQs for PQ and WFQ scheduling to ensure that higher-priority packets are forwarded ahead of lower-priority packets.

[3.4 Maintaining Congestion Avoidance](#)

This section describes how to clear the congestion avoidance statistics.

[3.5 Configuration Examples](#)

This section provides examples for configuring congestion avoidance, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

3.1 Introduction to Congestion Avoidance

This section describes traffic control policies.

3.1.1 Introduction to Congestion Avoidance

Congestion avoidance is a traffic control mechanism that uses traffic scheduling to prevent the network from being overloaded. With this mechanism, the device can monitor the usage of network resources such as queues and buffer areas in the memory and discard packets when network congestion is intensifying. The traditional packet drop policy uses the tail drop mechanism, which may lead to global TCP synchronization. RED and WRED, however, are introduced to prevent global TCP synchronization.

Congestion avoidance is a traffic control mechanism used to avoid network overload by adjusting network traffic. With this mechanism, the router can monitor the usage of network resources and discard packets when the network congestion gets heavier.

Compared with the end-to-end traffic control, congestion avoidance involves the traffic load of more service flows in the router. When dropping packets, however, the router can cooperate with traffic control actions on the source end, such as TCP traffic control, to adjust the load of the network to a reasonable state.

Traditional Packet-Dropping Policy

In the traditional tail-drop policy, all the newly received packets are dropped when a queue reaches its maximum length.

This policy may lead to global TCP synchronization. When queues drop the packets of several TCP connections at the same time, the TCP connections start to adjust their traffic simultaneously. There is a possibility that all the TCP connection sources begin the slow start process to perform congestion avoidance. Then, all the TCP connection sources start to build up traffic, causing the traffic to peak at a certain time. Therefore, traffic on the network fluctuates cyclically.

RED and WRED

To avoid global TCP synchronization, the following two algorithms are introduced:

- Random Early Detection (RED)
- Weighted Random Early Detection (WRED)

The RED algorithm sets the upper and lower limits for each queue and specifies the following rules:

- When the length of a queue below the lower limit, no packet is dropped.
- When the length of a queue exceeds the upper limit, all the incoming packets are dropped.
- When the length of a queue is between the lower and upper limits, the incoming packets are dropped randomly. A random number is set for each received packet. It is compared with the drop probability of the current queue. The packet is dropped when the random number is larger than the drop probability. The longer the queue, the higher the discard probability.

Unlike RED, the random number in WRED is based on the IP precedence of IP packets. WRED keeps a lower drop probability for the packet that has a higher IP precedence.

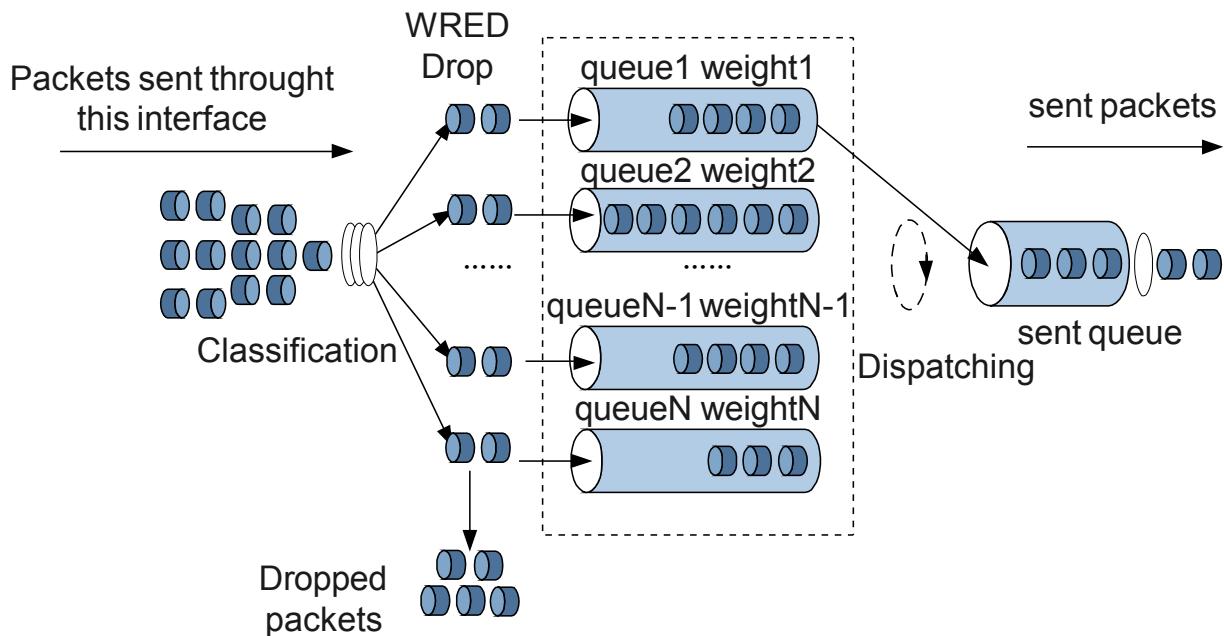
RED and WRED employ the random packet drop policy to avoid global TCP synchronization. When the packets of a TCP connection are dropped and sent at a lower rate, the packets of other TCP connections are still being sent at a relatively higher rate. There are always some TCP connections whose packets are sent at a relatively higher rate, improving the utilization of network bandwidth.

If packets are dropped by directly comparing the length of queues with the upper and lower limits (which set the absolute length of the queue threshold), the transmission of burst data stream is affected. The average queue length is hence used to set the relative value to compare the queue threshold and average queue length. The average length of a queue is the average length of the queues passing through a low pass filter. It reflects queue changes and is not affected by the burst change in queue length. This prevents adverse impact on the burst data stream.

Using Weighted Fair Queuing (WFQ), you can set the minimum threshold, maximum threshold and packet discard probability for every queue to provide different drop features for different classes of packets.

The relationship between WRED and queue mechanism is shown in [Figure 3-1](#).

Figure 3-1 Relationship between WRED and queue mechanism



Queue Scheduling

On the low-speed link, queue scheduling mechanisms are implemented based on the CoS values of traffic flows. Traffic flows enter eight flow queues (FQ) according to their CoS values, and then undergo Priority Queueing (PQ) and Weighted Fair Queueing (WFQ). After traffic flows enter their respective FQs, the Peak Information Rate (PIR) of traffic flows configured in the PQ mechanism is guaranteed first. Then, the remaining bandwidth resources are allocated among FQs according to the Committed Information Rate (CIR) configured in the WFQ mechanism.

Finally, bandwidth resources are allocated among FQs according to the PIR configured in the WFQ mechanism. In this way, PQ and WFQ provide traffic flows of various CoS values on the low-speed link with scheduling mechanisms of varying priorities.

3.1.2 Congestion Avoidance Supported by NE80E/40E

The congestion avoidance mechanism supported by the device is implemented through the WRED algorithm. WRED can identify QoS information contained in the packet header, including the IP precedence, DSCP value, and MPLS EXP value. In addition, the WRED algorithm can set the drop probability of a packet based on the IP precedence, DSCP value, or MPLS EXP value. In this manner, packets with different priorities are treated differently.

NE80E/40E adopts the Weighted Random Early Detection (WRED) algorithm to implement congestion avoidance in the outgoing traffic on interfaces. NE80E/40E also implements WRED on the MTI that is bound to the distributed multicast VPN.

 **NOTE**

Multicast VPN transmits multicast data in the MPLS/BGP VPN. The NE80E/40E adopts the multicast domains (MD) mechanism to implement multicast VPN, which is called MD VPN for short. In an MD, private data is transmitted through the multicast tunnel (MT). The VPN instance delivers the private data through MTI, and then the remote end receives the private data through MTI.

For detailed explanation on multicast VPN and its configurations, refer to HUAWEI NetEngine80E/40E Router *Configuration Guide -- IP Multicast*.

3.2 Configuring WRED

Using WRED, you can set thresholds for random packet drop. This can prevent multiple TCP connections from reducing their transmitting rates at the same time and accordingly prevent global TCP synchronization.

3.2.1 Establishing the Configuration Task

Before configuring WRED, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Due to limited memory resources, packets that exceed specifications are traditionally discarded in the case of network congestion. When a large number of TCP packets are discarded, TCP connections will time out. As a result, slow start of TCP connections and congestion avoidance are triggered so as to reduce the forwarding of TCP packets. When the packets of many TCP connections are discarded at the same time, slow start and congestion avoidance of the TCP connections occur simultaneously. This is called global TCP synchronization and it lowers the utilization of link bandwidth.

To avoid global TCP synchronization, you can set the queue to discard packets randomly using the WRED mechanism. Random packet discarding of WRED can prevent multiple TCP connections from reducing their transmit rates. As a result, global TCP synchronization is avoided. In addition, the bandwidth can be efficiently utilized.

 **NOTE**

The random packet discarding is usually used together with WFQ queue.

Pre-configuration Tasks

Before configuring WRED, you need to complete the following pre-configuration tasks:

- Configure physical parameters for related interfaces
- Configure link layer attributes for related interfaces
- Configure IP addresses for related interfaces
- Enable routing protocols to achieve reachable routes

Data Preparation

To configure WRED, you need the following data.

No	Data
1	WRED template name, lower limit and upper limit percentage, discarding probability, and color of packets in each queue
2	The interface where the WRED is applied and parameters for the class queue

3.2.2 Configuring WRED Parameters

You can define a discard policy rather than adopt the default tail drop policy, by setting upper and lower thresholds and discard probabilities for packets of different colors.

Context

With a WRED template, you can set the parameters for packets of three colors. Generally, the green packets have the smallest discarding probability and the highest thresholds; the yellow packets have the medium discarding probability and thresholds; the red packets have the highest discarding probability and the lowest thresholds.

By configuring a WRED template, you can set the upper limit, lower limit, and discarding probability for queues.

- When the length of a queue is below the lower percentage limit, no packet is dropped.
- When the length of a queue exceeds the upper percentage limit, all the incoming packets are dropped.
- When the length of a queue is between the lower and upper percentage limits, the incoming packets are dropped randomly. The longer the queue, the higher the discarding probability.
- You can configure limits and discarding probability for each color of packets.
- By default, the system can contain a maximum of eight class queue WRED templates. Among them, one is the default template (the lower percentage limit, the upper percentage limit and the discarding percentage are all 100) and seven templates can be created by users.

 NOTE

- For LPUI-41, LPUS-41, LPUI-100 and LPUF-100, if you do not configure a port-wred object, the system uses the WRED policy.
- You can configure the smallest upper and lower percentage limits for the queue containing red packets, medium upper and lower percentage limits for the queue containing yellow packets, and the highest upper and lower percentage limits for the queue containing green packets.
- In actual configuration, it is recommended that the lower percentage threshold for WRED starts from 50%; the thresholds for packets of different colors are then adjusted accordingly. It is recommended that the discarding probability is set to 100%.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
port-wred port-wred-name
```

A WRED object of a class queue is created and the WRED view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage
```

The lower percentage limit, upper percentage limit and discarding probability are set for different colors of packets.

----End

3.2.3 Applying WRED

A WRED template is applied to the service of a specific type.

Context

 NOTE

You should configure WRED for an interface in the interface view, and configure WRED for an MTI that is bound to distributed multicast VPN in the slot view.

Procedure

- Applying a WRED Template in the Interface View.

Currently, the WRED template can only be applied to the outgoing traffic on an interface.

Do as follows on the router where a WRED object is configured:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping
{ shaping-value | shaping-percentage shaping-percentage-value } | port-
wred wred-name } * outbound
```

The scheduling policy is set for the class queue with the specified CoS and the WRED object is applied in the scheduling policy.

The NE80E/40E can only support configure the scheduling policy on the outbound. The inbound class queue with the specified CoS is scheduled as the default scheduling policy.

- Applying a WRED Template for an MTI in the Slot View

Do as follows on the router where a WRED object is configured:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
slot slot-id
```

The slot view is displayed.

3. Run:

```
port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping
{ shaping-value | shaping-percentage shaping-percentage-value } | port-
wred wred-name } * outbound bind mtunnel
```

Scheduling policies are configured for multicast queues of different classes on the MTI that is bound to distributed multicast VPN, and the previously configured WRED objects are applied to these scheduling policies.

----End

3.2.4 Checking the Configuration

After WRED is configured, you can view the configurations of WRED.

Context

Run the following **display** command to check the previous configuration.

Procedure

- Using the **display interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check the traffic statistics on an interface.
- Using the **display port-wred configuration** [**verbose** [*port-wred-name*]] command to check the parameters for a WRED object of a class queue.
- Using the **display port-queue configuration** *interface* *interface-type* *interface-number* **outbound** command to check the detailed configuration of a class queue.
- Using the **display port-queue statistics** *interface* *interface-type* *interface-number* [*cos-value*] **outbound** command to check the statistics on a class queue.

- Using the **display port-queue configuration slot slot-id outbound bind Mtunnel** command to check the detailed configuration of a class queue about the multicast VPN.
- Using the **display port-queue statistics slot slot-id [cos-value] outbound bind Mtunnel** command to check the statistics on a class queue about the multicast VPN.

----End

Example

Running the **display port-wred configuration [verbose [port-wred-name]]** command, you can view the parameters for a WRED object of a class queue.

For example:

```
<HUAWEI> display port-wred configuration verbose pw
port-wred-name : pw
  color    low-limit      high-limit      discard-percent
  green      70            100            100
  yellow     60            90             100
  red        50            80             100
Reference relationships
  NULL
```

If the configuration succeeds, the following results can be obtained by running the preceding command:

- In the system view, you can see that the upper threshold, lower threshold, and discard probability of the WRED templates for all colors of packets are configured correctly.
- The WRED template is applied to packets with the specified class of service (CoS).

Running the **display port-queue statistics slot slot-id [cos-value] outbound bind Mtunnel** command, you can view the statistics on a class queue about the multicast VPN.

For example:

```
<HUAWEI> display port-queue statistics slot 10 be outbound bind mtunnel
slot 10 bind MTunnel outbound traffic statistics:
[be]
  Total pass:                      6,968,228 packets,          1,485,259,144 bytes
  Total discard:                   17,585,668 packets,          777,584,844 bytes
  Drop tail discard:              17,585,668 packets,          777,584,844 bytes
  Wred discard:                  0 packets,                      0 bytes
  Last 30 seconds pass rate:       0 pps,                         0 bps
  Last 30 seconds discard rate:   0 pps,                         0 bps
  Drop tail discard rate:         0 pps,                         0 bps
  Wred discard rate:              0 pps,                         0 bps
```

3.3 Configuring Queue Scheduling for Low-Speed Links

On low-speed links, congestion is likely to occur due to limited network resources. To prevent packets from being indiscriminately dropped in the case of congestion, traffic flows need to be placed in different FQs for PQ and WFQ scheduling to ensure that higher-priority packets are forwarded ahead of lower-priority packets.

3.3.1 Establishing the Configuration Task

Before configuring queue scheduling for low-speed links, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

On the links established on low-speed interfaces such as CPOS,E1/T1, and E3/T3, congestion is likely to occur due to limited network resources. To prevent packets from being indiscriminately dropped in the case of congestion, traffic flows need to be placed in different FQs for PQ and WFQ scheduling to ensure that higher priority packets are forwarded ahead of lower priority packets.

Pre-configuration Tasks

Before configuring queue scheduling on low-speed links, complete the following tasks:

- Configuring the physical parameters of relevant interfaces
- Configuring the link layer attributes of relevant interfaces to ensure their proper functioning
- Configuring IP addresses for relevant interfaces
- Enabling the routing protocol for communication between devices

Data Preparation

To configure queue scheduling on low-speed links, you need the following data.

No.	Data
1	Interface numbers for queue scheduling
2	PIR and the traffic shaping rate in percentage of the total bandwidth for PQ
3	CIR, PIR, and the traffic shaping rate in percentage of the total bandwidth for WFQ

3.3.2 Configuring PQ

On low-speed links, you can place different service flows into different FQs for PQ scheduling.

Context



Only EF, CS6, CS7, AF4, AF3, and AF2 flows support PQ.

The priority of PQ is higher than that of WFQ. If both PQ and WFQ are configured for packets in the same class queue, the one that is configured later takes effect.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.



NOTE
Queue scheduling on low-speed links can be configured only in the serial interface view, Trunk-serial interface view, Global-Mp-Group interface view, or the MP-Group interface view.

Step 3 Run:

```
port-queue cos-value pq shaping shaping-value shaping-percentage shaping-percentage-value
```

PQ parameters are set.

----End

3.3.3 Configuring WFQ

On low-speed links, you can place different service flows into different FQs for WFQ scheduling.

Context



NOTE
Except CS7 packets, all packets with other CoS values can be configured with WFQ.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-queue cos-value wfq shaping shaping-value shaping-percentage shaping-percentage-value
```

WFQ parameters are set.

----End

3.3.4 Checking the Configuration

After configuring queue scheduling for low-speed links, you can view the detailed configurations and statistics about class queues.

Context

Use the following **display** commands to check the previous configuration.

Procedure

- Run the **display interface [interface-type [interface-number]] [| { begin | exclude | include } regular-expression]** command to check traffic statistics on the interface.
- Run the **display ls-port-queue configuration interface interface-type interface-number outbound** command to check the configuration of the class queue.
- Run the **display ls-port-queue statistics interface interface-type interface-number [cos-value] outbound** command to check statistics on the class queue.

----End

Example

Using the **display ls-port-queue statistics interface serial3/0/0/2:0 outbound** command, you can view statistics on the class queues on interfaces on the low-speed interface card. For example:

```
<HUAWEI> display ls-port-queue statistics interface serial3/0/0/2:0 outbound
Serial3/0/0/2:0 outbound traffic statistics:
[be]

    Statistics last cleared:2008-10-09 17:17:23
    Total pass:                      0 packets,          0 bytes
    Drop tail discard:                0 packets,          0 bytes
    Free buffer pool discard:        0 packets
    MTU discard:                     0 packets
    Total pass rate:                 0 pps,            0 bps
    Drop tail discard rate:         0 pps,            0 bps
    Free buffer pool discard rate:  0 pps
    MTU discard rate:               0 pps

[af1]
    Statistics last cleared:2008-10-09 17:17:23
    Total pass:                      37446 packets,      3370140 bytes
    Drop tail discard:                38300 packets,      0 bytes
    Free buffer pool discard:        0 packets
    MTU discard:                     0 packets
    Total pass rate:                 2674 pps,         1925794 bps
    Drop tail discard rate:         2735 pps,         0 bps
    Free buffer pool discard rate:  0 pps
    MTU discard rate:               0 pps

[af2]
    Statistics last cleared:2008-10-09 17:17:23
    Total pass:                      0 packets,          0 bytes
    Drop tail discard:
```

```

          0 packets,          0 bytes
Free buffer pool discard:      0 packets
MTU discard:                  0 packets
Total pass rate:              0 pps,          0 bps
Drop tail discard rate:       0 pps,          0 bps
Free buffer pool discard rate: 0 pps
MTU discard rate:             0 pps
[af3]                         0 pps
Statistics last cleared:2008-10-09 17:17:23
Total pass:                   0 packets,          0 bytes
Drop tail discard:            0 packets,          0 bytes
Free buffer pool discard:     0 packets
MTU discard:                  0 packets
Total pass rate:              0 pps,          0 bps
Drop tail discard rate:       0 pps,          0 bps
Free buffer pool discard rate: 0 pps
MTU discard rate:             0 pps
[af4]                         0 pps
Statistics last cleared:2008-10-09 17:17:23
Total pass:                   0 packets,          0 bytes
Drop tail discard:            0 packets,          0 bytes
Free buffer pool discard:     0 packets
MTU discard:                  0 packets
Total pass rate:              0 pps,          0 bps
Drop tail discard rate:       0 pps,          0 bps
Free buffer pool discard rate: 0 pps
MTU discard rate:             0 pps
[ef]                           0 pps
Statistics last cleared:2008-10-09 17:17:23
Total pass:                   0 packets,          0 bytes
Drop tail discard:            0 packets,          0 bytes
Free buffer pool discard:     0 packets
MTU discard:                  0 packets
Total pass rate:              0 pps,          0 bps
Drop tail discard rate:       0 pps,          0 bps
Free buffer pool discard rate: 0 pps
MTU discard rate:             0 pps
[cs6]                         0 pps
Statistics last cleared:2008-10-09 17:17:23

```

```
Total pass:                                0 packets,          0 bytes
Drop tail discard:                          0 packets,          0 bytes
Free buffer pool discard:                  0 packets
MTU discard:                               0 packets
Total pass rate:                           0 pps,            0 bps
Drop tail discard rate:                   0 pps,            0 bps
Free buffer pool discard rate:           0 pps
MTU discard rate:                          0 pps
[cs7]
Statistics last cleared:2008-10-09 17:17:23
Total pass:                                5 packets,         107 bytes
Drop tail discard:                          0 packets,          0 bytes
Free buffer pool discard:                  0 packets
MTU discard:                               0 packets
Total pass rate:                           0 pps,            61 bps
Drop tail discard rate:                   0 pps,            0 bps
Free buffer pool discard rate:           0 pps
MTU discard rate:                          0 pps
```

3.4 Maintaining Congestion Avoidance

This section describes how to clear the congestion avoidance statistics.

3.4.1 Clearing the Statistics on Class Queues

This section describes the commands that are used to clear the statistics on class queues.

Context



CAUTION

Statistics cannot be restored after being cleared. Therefore, exercise caution when running the following commands.

After the confirmation, run the following **reset** commands in the user view to clear the specified statistics.

Procedure

- Step 1** Run the **reset port-queue statistics interface interface-type interface-number [cos-value] outbound** command to clear statistics on class queues on the specified interface.

Step 2 Run the **reset port-queue statistics slot slot-id [cos-value] outbound bind Mtunnel** command to clear the statistics on the port queue about multicast VPN.

----End

3.5 Configuration Examples

This section provides examples for configuring congestion avoidance, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

 **NOTE**

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

3.5.1 Example for Configuring Congestion Avoidance

This section provides an example for configuring congestion avoidance. The device monitors the usage of network resources and discards packets when congestion is intensifying.

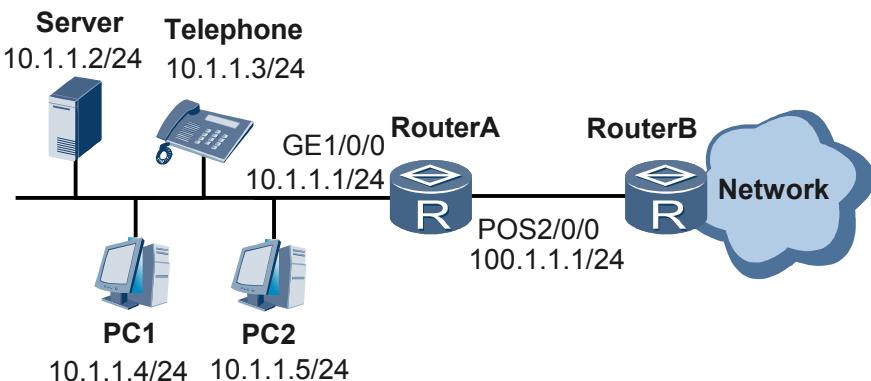
Networking Requirements

As shown in **Figure 3-2**, devices Server, Telephone, PC1 and PC2 all send data to the network through Router A. The data sent from Server is of critical traffic class; the data sent from Telephone is of voice services; the data from PC1 and PC2 is of normal services. Because the rate of the inbound interface GE 1/0/0 on Router A is greater than that of the outbound interface POS 2/0/0, congestion may occur on POS 2/0/0.

When network congestion occurs, the data sent by Server and Telephone must be transmitted first. Users PC1 and PC2 allow a little delay to the transmission of their data but they also require bandwidth guarantee because they are VIP users. Therefore, Router A must discard packets based on the priority of the packets when the network congestion intensifies.

Thus, WFQ and WRED must be both configured on Router A.

Figure 3-2 Networking diagram for configuring congestion avoidance



Configuration Roadmap

The configuration roadmap is as follows:

1. On GE 1/0/0 of Router A, mark the priority of different flows.
2. Configure a WRED object to set the lower and upper percentage limits for discarding packets as well as the discarding probability.
3. On POS 2/0/0, set the scheduling policy for the class queue and apply the WRED object in the scheduling policy.

Data Preparation

To complete the configuration, you need the following data:

- ACL number, traffic classifier name, traffic behavior name, priority of the service to be remarked and the traffic policy name
- WRED object name, lower percentage limit and upper percentage limit, discarding probability and packet color in each queue
- The interface where the packet discarding of WRED is applied and parameters for the class queue

Procedure

Step 1 Set ACL rules for packets that are sent from Server, Telephone, PC1 and PC2.

```
<RouterA> system-view
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 10.1.1.3 0.0.0.0
[RouterA-acl-basic-2001] quit
[RouterA] acl number 2002
[RouterA-acl-basic-2002] rule permit source 10.1.1.2 0.0.0.0
[RouterA-acl-basic-2002] quit
[RouterA] acl number 2003
[RouterA-acl-basic-2001] rule permit source 10.1.1.4 0.0.0.0
[RouterA-acl-basic-2001] quit
[RouterA] acl number 2004
[RouterA-acl-basic-2002] rule permit source 10.1.1.5 0.0.0.0
[RouterA-acl-basic-2002] return
```

Step 2 On GE 1/0/0 of Router A, configure the complex traffic classification to mark the priority of services.

```
<RouterA> system-view
[RouterA] traffic classifier aa
[RouterA-classifier-aa] if-match acl 2001
[RouterA-classifier-aa] quit
[RouterA] traffic classifier bb
[RouterA-classifier-bb] if-match acl 2002
[RouterA-classifier-bb] quit
[RouterA] traffic classifier cc
[RouterA-classifier-cc] if-match acl 2003
[RouterA-classifier-cc] quit
[RouterA] traffic classifier dd
[RouterA-classifier-dd] if-match acl 2004
[RouterA-classifier-dd] quit
[RouterA] traffic behavior aa
[RouterA-behavior-aa] remark ip-precedence 5
[RouterA-behavior-aa] quit
[RouterA] traffic behavior bb
[RouterA-behavior-bb] remark ip-precedence 4
[RouterA-behavior-bb] quit
[RouterA] traffic behavior cc
[RouterA-behavior-cc] remark ip-precedence 3
```

```
[RouterA-behavior-cc] quit
[RouterA] traffic behavior dd
[RouterA-behavior-dd] remark ip-precedence 2
[RouterA-behavior-dd] quit
[RouterA] traffic policy ee
[RouterA-trafficpolicy-ee] classifier aa behavior aa
[RouterA-trafficpolicy-ee] classifier bb behavior bb
[RouterA-trafficpolicy-ee] classifier cc behavior cc
[RouterA-trafficpolicy-ee] classifier dd behavior dd
[RouterA-trafficpolicy-ee] quit
[RouterA] interface gigabitethernet1/0/0
[RouterA-gigabitEthernet1/0/0] undo shutdown
[RouterA-gigabitEthernet1/0/0] traffic-policy ee inbound
[RouterA-gigabitEthernet1/0/0] return
```

Step 3 Configure a WRED object on Router A.

```
<RouterA> system-view
[RouterA] port-wred pw
[RouterA-port-wred-pw] color green low-limit 70 high-limit 100 discard-percentage
100
[RouterA-port-wred-pw] color yellow low-limit 60 high-limit 90 discard-percentage
100
[RouterA-port-wred-pw] color red low-limit 50 high-limit 80 discard-percentage 100
[RouterA-port-wred-pw] return
```

After the preceding configuration, run the **display port-wred configuration verbose** command to check the parameters set for the WRED object:

```
<RouterA> display port-wred configuration verbose pw
port-wred-name : pw
  color    low-limit      high-limit      discard-percent
  green     70            100            100
  yellow    60            90             100
  red       50            80             100
  reference relationships
  NULL
```

Step 4 On POS 2/0/0 of Router A, configure class queues and apply the WRED object pw.

```
<RouterA> system-view
[RouterA] interface pos2/0/0
[RouterA-POS2/0/0] undo shutdown
[RouterA-POS2/0/0] port-queue ef pq port-wred pw outbound
[RouterA-POS2/0/0] port-queue af4 wfq weight 15 shaping 100 port-wred pw outbound
[RouterA-POS2/0/0] port-queue af3 wfq weight 10 shaping 50 port-wred pw outbound
[RouterA-POS2/0/0] port-queue af2 wfq weight 10 shaping 50 port-wred pw outbound
[RouterA-POS2/0/0] return
```

After the preceding configuration, run the **display port-queue configuration interface** command to view the configuration of class queues:

```
<HUAWEI> display port-queue configuration interface pos 2/0/0 outbound
POS2/0/0
be current configuration:
  Arithmetic: wfq
  weight: 10
  tm weight: 3
  fact weight: 10.00
  shaping(mbps): NA
  port-wred name: NA
af1 current configuration:
  Arithmetic: wfq
  weight: 10
  tm weight: 3
  fact weight: 10.00
  shaping(mbps): NA
  port-wred name: NA
af2 current configuration:
  Arithmetic: wfq
```

```

        weight: 10
        tm weight: 3
        fact weight: 10.00
        shaping(mbps): 50
        port-wred name: pw
af3 current configuration:
    Arithmetic: wfq
    weight: 10
    tm weight: 3
    fact weight: 10.00
    shaping(mbps): 50
    port-wred name: pw
af4 current configuration:
    Arithmetic: wfq
    weight: 15
    tm weight: 2
    fact weight: 15.00
    shaping(mbps): 100
    port-wred name: pw
ef current configuration:
    Arithmetic: pq
    weight: NA
    tm weight: NA
    fact weight: NA
    shaping(mbps): NA
    port-wred name: pw
cs6 current configuration:
    Arithmetic: pq
    weight: NA
    tm weight: NA
    fact weight: NA
    shaping(mbps): NA
    port-wred name: NA
cs7 current configuration:
    Arithmetic: pq
    weight: NA
    tm weight: NA
    fact weight: NA
    shaping(mbps): NA
    port-wred name: NA

```

Step 5 Check the configuration.

When traffic transits the network, run the **display port-queue statistics** command on the outbound interface POS 2/0/0 of Router A. The output shows that the traffic volume of services EF, AF4, AF3, and AF2 increases rapidly.

When the traffic volume increases rapidly in the network, the output shows that the discarded traffic of services EF, AF4, AF3, and AF2 is also increasing. The traffic of AF4, AF3, and AF2 is forwarded using the configured bandwidth.

```

<HUAWEI> display port-queue statistics interface pos 2/0/0 outbound
Pos 2/0/0 outbound traffic statistics:
[be]
    Total pass:                                633,876,898 packets,      48,076,301,860 bytes
    Total discard:                             0 packets,                0 bytes
    Drop tail discard:                         0 packets,                0 bytes
    Wred discard:                            0 packets,                0 bytes
    Last 30 seconds pass rate:                 0 pps,                   0 bps
    Last 30 seconds discard rate:              0 pps,                   0 bps
    Drop tail discard:                         0 pps,                   0 bps

```

Wred discard:	0 pps,	0 bps
[af1]		
Total pass:	0 packets,	0 bytes
Total discard:	0 packets,	0 bytes
Drop tail discard:	0 packets,	0 bytes
Wred discard rate:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
Drop tail discard:	0 pps,	0 bps
Wred discard rate:	0 pps,	0 bps
[af2]		
Total pass:	58 packets,	5,684 bytes
Total discard:	24,478,662 packets,	1,860,378,312 bytes
Drop tail discard:	0 packets,	0 bytes
Wred discard rate:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
Drop tail discard:	0 pps,	0 bps
Wred discard rate:	0 pps,	0 bps
[af3]		
Total pass:	0 packets,	0 bytes
Total discard:	0 packets,	0 bytes
Drop tail discard:	0 packets,	0 bytes
Wred discard rate:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
Drop tail discard:	0 pps,	0 bps
Wred discard rate:	0 pps,	0 bps
[af4]		
Total pass:	0 packets,	0 bytes
Total discard:	0 packets,	0 bytes
Drop tail discard:	0 packets,	0 bytes
Wred discard rate:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
Drop tail discard:	0 pps,	0 bps
Wred discard rate:	0 pps,	0 bps

```

0 pps,          0 bps
[ef]
Total pass:      19,126,381 packets,      1,874,388,964 bytes
Total discard:   24,353,802 packets,      406,888,952 bytes
Drop tail discard: 0 packets,          0 bytes
Wred discard rate: 0 packets,          0 bytes
Last 30 seconds pass rate: 196,829 pps,      19,286,890 bps
Last 30 seconds discard rate:
Drop tail discard: 0 pps,          0 bps
Wred discard rate: 0 pps,          0 bps
0 pps,          0 bps
[cs6]
Total pass:      3,789 packets,      330,302 bytes
Total discard:   0 packets,          0 bytes
Drop tail discard: 0 packets,          0 bytes
Wred discard rate: 0 packets,          0 bytes
Last 30 seconds pass rate: 0 pps,          0 bps
Last 30 seconds discard rate:
Drop tail discard: 0 pps,          0 bps
Wred discard rate: 0 pps,          0 bps
0 pps,          0 bps
[cs7]
Total pass:      0 packets,          0 bytes
Total discard:   0 packets,          0 bytes
Drop tail discard: 0 packets,          0 bytes
Wred discard rate: 0 packets,          0 bytes
Last 30 seconds pass rate: 0 pps,          0 bps
Last 30 seconds discard rate:
Drop tail discard: 0 pps,          0 bps
Wred discard rate: 0 pps,          0 bps
0 pps,          0 bps

```

----End

Configuration Files

Configuration file on Router A

```

#
sysname RouterA
#
acl number 2001
rule permit source 10.1.1.3 0
#
acl number 2002
rule permit source 10.1.1.2 0
#
acl number 2003

```

```
rule permit source 10.1.1.4 0
#
acl number 2004
    rule permit source 10.1.1.5 0
#
traffic classifier cc operator or
    if-match acl 2003
traffic classifier dd operator or
    if-match acl 2004
traffic classifier aa operator or
    if-match acl 2001
traffic classifier bb operator or
    if-match acl 2002
#
traffic behavior cc
    remark ip-precedence 3
traffic behavior dd
    remark ip-precedence 2
traffic behavior aa
    remark ip-precedence 5
traffic behavior bb
    remark ip-precedence 4
#
traffic policy ee
    classifier aa behavior aa
    classifier bb behavior bb
    classifier cc behavior cc
    classifier dd behavior dd
#
port-wred pw
    color green low-limit 70 high-limit 100 discard-percentage 100
    color yellow low-limit 60 high-limit 90 discard-percentage 100
    color red low-limit 50 high-limit 80 discard-percentage 100
#
interface gigabitEthernet1/0/0
    undo shutdown
    ip address 10.1.1.1 0.0.0.255
    traffic-policy ee inbound
#
interface POS2/0/0
    undo shutdown
    ip address 100.1.1.1 0.0.0.255
    port-queue ef pq port-wred pw outbound
    port-queue af4 wfq weight 15 shaping 100 port-wred pw outbound
    port-queue af3 wfq weight 10 shaping 50 port-wred pw outbound
    port-queue af2 wfq weight 10 shaping 50 port-wred pw outbound
#
ospf 1
    area 0.0.0.0
        network 10.1.1.0 0.0.0.255
        network 100.1.1.0 0.0.0.255
#
return
```

3.5.2 Example for Configuring Queue Scheduling on Low-speed Links

This section provides an example for configuring queue scheduling on low-speed links. After queue scheduling is configured on low-speed links, queues with different priorities can be scheduled based on their CoSs when congestion occurs. In this manner, bandwidth is guaranteed for packets with a higher priority.

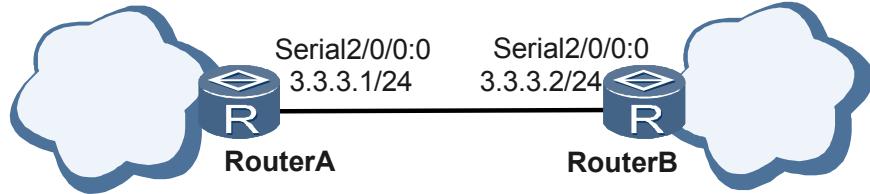
Networking Requirements



This configuration example cannot be configured on the X1 and X2 models of the NE80E/40E.

As shown in **Figure 3-3**, Router A and Router B are located in two networks, and are joined through a low-speed link with limited bandwidth resources. To ensure that packets of different priorities are allocated bandwidth resources based on their CoS values in the case of congestion, PQ and WFQ need to be configured on the interfaces on Router A.

Figure 3-3 Networking diagram of configuring queue scheduling on low-speed links



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the interfaces of the Router A and Router B to be UP.
2. Configure IP addresses for interfaces on Router A and Router B.
3. Configure PQ and WFQ on Router A.

Data Preparation

To complete the configuration, you need the following data.

- IP addresses of interfaces
- PIR and the traffic shaping rate in percentage of the total bandwidth for PQ
- CIR, PIR, and the traffic shaping rate in percentage of the total bandwidth for WFQ

Procedure

Step 1 Create the serial interfaces on Router A and Router B.

To be omitted. For details of the configuration, refer to the HUAWEI NetEngine80E/40E Router Configuration Guide *WAN Access*.

Step 2 Configure the interfaces of the Router A and Router B to be UP.

```
<RouterA> system view
[RouterA] interface serial 2/0/0:0
[RouterA(serial2/0/0:0)] undo shutdown
[RouterA(serial2/0/0:0)] return
<RouterB> system view
[RouterB] interface serial 2/0/0:0
[RouterB(serial2/0/0:0)] undo shutdown
[RouterB(serial2/0/0:0)] return
```

Step 3 Configure IP addresses for interfaces on Router A and Router B to ensure network connectivity.

The configuration is omitted here. For detailed configuration, refer to the *HUAWEI NetEngine80E/40E Router Configuration Guide - IP Routing*.

Step 4 Configure PQ and WFQ on Serial 2/0/0:0 on Router A.

```
<RouterA> system view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] port-queue ef pq shaping 60
[RouterA-serial2/0/0:0] port-queue af4 wfq shaping 40
[RouterA-serial2/0/0:0] port-queue af3 wfq shaping 40
[RouterA-serial2/0/0:0] port-queue af2 wfq shaping 30
[RouterA-serial2/0/0:0] return
```

After the preceding configurations, run the **display ls-port-queue configuration interface** command to view the detailed configuration of class queues:

```
<HUAWEI> display ls-port-queue configuration interface Serial2/0/0:0 outbound
Serial2/0/0:0 :
    be configuration:
        Arithmetic: wfq
        cir: 15%
        pir: 100%
    af1 configuration:
        Arithmetic: wfq
        cir: 15%
        pir: 100%
    af2 configuration:
        Arithmetic: wfq
        cir: 12
        pir: 30
    af3 configuration:
        Arithmetic: wfq
        cir: 15
        pir: 40
    af4 configuration:
        Arithmetic: wfq
        cir: 10
        pir: 40
    ef configuration:
        Arithmetic: pq
        cir: NA
        pir: 60
    cs6 configuration:
        Arithmetic: pq
        cir: NA
        pir: 100%
    cs7 configuration:
        Arithmetic: pq
        cir: NA
        pir: 100%
```

Step 5 Verify the configuration.

When traffic is being transmitted in the network, run the **display ls-port-queue statistics** command on the outbound interface Serial 2/0/0:0 of RouterA. The output shows that the EF, AF4, AF3, AF2, and BE flows are increasing rapidly.

When the traffic volume increases rapidly in the network, the output shows that a large number of the EF, AF4, AF3, AF2, and BE flows are discarded, and that the bandwidths are allocated to the AF4, AF3, and AF2 flows according to the configured weights.

----End

Configuration File

- The configuration file of Router A is as follows:

```
# 
Sysname RouterA
#
controller e1 2/0/0
channel-set 0 timeslot-list 1-31
```

```
undo shutdown
#
interface Serial2/0/0:0
undo shutdown
ip address 3.3.3.1 255.255.255.0
port-queue af2 wfq shaping 30
port-queue af3 wfq shaping 40
port-queue af4 wfq shaping 40
port-queue ef pq shaping 60
#
return
```

4 Class-Based QoS Configuration

About This Chapter

Using class-based QoS, you can implement traffic classification and traffic control on packets that enter a network and set the ToS values of packets.

[4.1 Class-Based QoS Overview](#)

This section describes basic techniques required for implementing class-based QoS, including traffic classification, re-marking, DSCP fields, and standard PHBs.

[4.2 Configuring a Traffic Policy Based on Complex Traffic Classification](#)

Traffic policies based on complex traffic classification allow the system to implement traffic policing, re-marking, packet filtering, policy-based routing, and traffic sampling on packets based on the traffic classifier to which the packets belong.

[4.3 Configuring UCL-based Traffic Policies](#)

By configuring UCL-based traffic policies, you can distinguish between users of different priorities and implement QoS on the traffic of users. In this manner, the CIR and PIR are guaranteed for users.

[4.4 Configuring Precedence Mapping Based on Simple Traffic Classification](#)

Precedence mapping based on simple traffic classification is used to map the priority of traffic on one network to that of traffic on another network. This allows traffic to be transmitted on another network based on the previous priority or the user-defined priority.

[4.5 Maintaining Class-based QoS](#)

This section describes how to clear statistics about traffic policies.

[4.6 Configuration Examples](#)

This section provides examples for configuring class-based QoS, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

4.1 Class-Based QoS Overview

This section describes basic techniques required for implementing class-based QoS, including traffic classification, re-marking, DSCP fields, and standard PHBs.

4.1.1 Introduction to Class-Based QoS

Class-based QoS defines traffic classifiers based on certain rules and associates traffic classifiers with certain traffic behaviors, forming certain traffic policies. After these policies are applied to interfaces, class-based traffic policing, traffic shaping, congestion management, and precedence re-marking are implemented.

The NE80E/40E supports DiffServ and provides standard forwarding services such as EF and AF for users by using the following traffic management measures:

- Traffic classification
- Traffic policing
- Traffic shaping
- Congestion avoidance

QoS of the NE80E/40E supports traffic policy with the above measures and mapping between the QoS fields in the IP header and the MPLS header.

The traffic policies in the NE80E/40E are as follows:

- Traffic policy based on complex traffic classification

The NE80E/40E carries out traffic policing, re-marking, filtering, policy-based routing and traffic sampling based on the class of the packet. Such a policy is usually applied to the border router of a DiffServ domain.
- Traffic policy based on simple traffic classification

The NE80E/40E re-sets the CoS, color and drop precedence of packets based on the mark fields in the packet. Such a traffic policy is usually configured on a router near the core of a network.
- Internal traffic policy in the router

The NE80E/40E uses the internal traffic policy to control the traffic sent from the LPU to the SRU so that the SRU remains in a stable state.

NOTE

- DiffServ is mainly used to guarantee the bandwidth for BA data flows. The NE80E/40E uses the pre-defined queuing mechanism to assign resources for EF, AF and other services. Users do not need to configure queue management.
- The precedence of complex traffic classification is higher than that of simple traffic classification.

Traffic Classification

Traffic classification is used to identify packets that have the same characters according to specific rules. It is the basis for providing differentiated services. Traffic classification consists of complex traffic classification and simple traffic classification:

- Simple traffic classification

The simple traffic classification refers to classifying packets according to the IP precedence or DSCP of the IP packet, the EXP of the MPLS packet, or the 802.1p field of the VLAN

packet. It is used to simply identify the traffic that has the specific precedence or class of service.

The protocol packets are configured with high priorities or CoSs and thus will not be dropped even in the case of traffic congestion.

- Complex traffic classification

The complex traffic classification refers to classifying packets according to more complex rules, for example, the combination of the link layer, the network layer, and the transport layer information.

Traffic Behavior

Traffic classification is meaningful only after it is associated with traffic control actions.

The NE80E/40E supports the following traffic actions and the combination of these traffic actions:

- Deny/Permit

It is the simplest traffic control action. It enables the NE80E/40E to control traffic by discarding packets or allowing packets to pass through.

- Mark

This traffic control action is used to set the precedence field in the packet. The precedence field in a packet varies with the network type. For example, the packet carries the 802.1p field in the VLAN, the DSCP field in the DiffServ network, and the EXP field in the MPLS network. Therefore, the router is required to mark the precedence of packets according to their network type.

Usually, devices at the border of a network marks the precedence of incoming packets. Devices in the core of the network provides corresponding QoS services according to the precedence marked by the border device, or re-mark the precedence according to its own standard.

- Redirection

It indicates that the router does not forward a packet according to the destination address in the packet but forwards it to another next hop or Label Distribution Path (LSP). This is policy-based routing.

- Traffic policing

It is a traffic control action used to limit the traffic and the resource used by the traffic by monitoring the specifications of the traffic. With traffic policing, the router can discard, re-mark the color or precedence of, or perform other QoS measures over packets that exceed the specifications.

- Security

It refers to performing such measures as Unicast Reverse Path Forwarding (URPF), port mirroring, or traffic statistics over packets.

Security actions are not QoS measures but can be used together with other QoS actions to improve the security of the network and packets.

Precedence Mapping

The precedence field in a packet varies with the network type. For example, the packet carries the 802.1p field in the VLAN, the DSCP field in the DiffServ network, and the EXP field in the MPLS network. When a packet passes through different networks, the mapping between the

precedence used in the networks must be set on the gateway that connects the networks to keep the precedence of the packet.

When the NE80E/40E serves as the gateway of different networks, the precedence fields (such as 802.1p, DSCP, and EXP fields) in the packets that go into the NE80E/40E are all mapped as the internal precedence of the router. When the NE80E/40E sends out the packet, the internal precedence is mapped back to the external precedence.

4.1.2 Class-Based QoS Supported by the NE80E/40E

The device supports class-based QoS that is implemented through traffic policing, traffic shaping, congestion management, and precedence re-marking.

The NE80E/40E supports class-based QoS to implement:

- Traffic policing based on complex traffic classification, re-marking, packet filtering, policy-based routing, load balancing, URPF, NetStream, and mirroring
- Mapping of priorities of services between networks based on simple traffic classification
- Traffic policing based on UCL

4.2 Configuring a Traffic Policy Based on Complex Traffic Classification

Traffic policies based on complex traffic classification allow the system to implement traffic policing, re-marking, packet filtering, policy-based routing, and traffic sampling on packets based on the traffic classifier to which the packets belong.

Context

NOTE

- The NE80E/40E supports complex traffic classification on POS, GE, and QinQ interfaces and their sub-interfaces, and logical interfaces such as RINGIF, IP-Trunk, and Eth-Trunk interfaces. For details about how to configure a QinQ interface, see "QinQ Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - LAN Access and MAN Access*.
- Traffic policies cannot be directly applied to VLANIF interfaces. The traffic policies can be applied to the physical interfaces and Layer 2 Eth-Trunk interfaces with VLAN IDs being specified.

4.2.1 Establishing the Configuration Task

Before configuring a traffic policy based on complex traffic classification, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To manage or limit the traffic that goes into or flows over a network according to the class of service, you need to configure QoS traffic policies based on complex traffic classification. That is, you need to provide differentiated services according to parameters such as DSCP, protocol type, IP address, or port number of the packet. In this way, different types of services, such as voice services, video services, and data services, as well as traffic from different users can be served differently in terms of bandwidth, delay, and precedence.

In normal circumstances, traffic policies based on complex traffic classification are applied to the router at the edge of the network; traffic policies based on simple traffic classification are applied to the router at the core of the network.

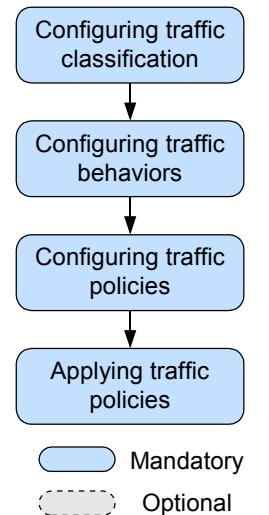
Pre-configuration Tasks

Before configuring a traffic policy based on complex traffic classification, complete the following tasks:

- Configuring physical parameters for interfaces
- Configuring link layer attributes for interfaces to ensure that the interfaces work normally
- Configuring IP addresses for interfaces
- Enabling routing protocols to ensure that routes are reachable

Configuration Procedures

Figure 4-1 Flowchart of configuring a traffic policy based on complex traffic classification



Data Preparation

To configure a traffic policy based on complex traffic classification, you need the following data.

No.	Data
1	Name of a traffic classifier
2	ACL number, DSCP value, 802.1p priority, and TCP flag value
3	Name of a traffic behavior
4	CIR, PIR, CBS, PBS, DSCP value, IP preference value, EXP value, 802.1p priority, next hop address, or outbound interface

No.	Data
5	Name of a traffic policy
6	Type and number of the interface where the traffic policy is applied

4.2.2 Defining a Traffic Classifier

You need to configure traffic classifiers before configuring class-based QoS. Traffic classifiers can be configured based on the ACL rules, IP precedence, MAC addresses, and protocol addresses.

Procedure

- Defining a traffic classifier based on Layer 3 or Layer 4 information

Do as follows on the router:

- Run:

```
system-view
```

The system view is displayed.

- Run:

```
traffic classifier classifier-name [ operator { and | or } ]
```

A traffic classifier is defined and the view of the classifier is displayed.

- Run the following command as required:

- To set a matching rule to classify traffic based on the ACL number, run:

```
if-match [ ipv6 ] acl { acl-number | name acl-name }
```

- To set a matching rule to classify traffic based on the DSCP value, run:

```
if-match [ ipv6 ] dscp dscp-value
```

- To set a matching rule to classify traffic based on the TCP flag, run:

```
if-match tcp syn-flag tcpflag-value
```

- To set a matching rule to classify traffic based on the IP precedence, run:

```
if-match ip-precedence ip-precedence
```

- To set a matching rule to classify traffic based on the MPLS EXP value, run:

```
if-match mpls-exp exp-value
```



The NE80E/40E supports complex traffic classification on upstream packets based on the MPLS EXP values of the outermost tags in packets. After classification, the packets only support the actions of deny, re-marking the MPLS EXP values, mirroring, and CAR.

- To match all packets, run:

```
if-match [ ipv6 ] any
```

- To set a matching rule for complex traffic classification based on the value of the next IPv6 header, run:

```
if-match ipv6 next-header header-number first-next-header
```

- To set a matching rule to classify traffic based on the source IPv6 address, run:

```
if-match ipv6 source-address ipv6-address prefix-length
```

- To set a matching rule to classify traffic based on the destination IPv6 address, run:

```
if-match ipv6 destination-address ipv6-address prefix-length
```

 **NOTE**

For IPv6 packets, you need to specify **ipv6** in Step 3. Source IP- and destination IP-based matching rules are applicable to only IPv6 packets rather than IPv4 packets.

ACL rules can be defined based on the protocol type, source address, destination address and ToS in packets. The **if-match acl** command filters packets according ACL rules defined in the **rule** command and then specific traffic actions will be performed.

If you set more than one matching rule for the same classifier, you can set their relationship by configuring **operator** in Step 2:

- Logical operator **and**: A packet belongs to the classifier only when it matches all rules.
 - Logical operator **or**: A packet belongs to the classifier if it matches any one of the rules.
 - By default, the logical operator of the rules is **or**.
- Defining a traffic classifier based on Layer 2 information

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic classifier classifier-name [ operator { and | or } ]
```

A traffic classifier is defined and the view of the classifier is displayed.

3. Run the following command as required:

- To set a matching rule to classify VLAN packets based on the 802.1p priority, run:

```
if-match 8021p 8021p-value
```

- To set a matching rule to classify traffic based on the source MAC address, run:

```
if-match source-mac mac-address
```

- To set a match rule to classify traffic based on the destination MAC address, run:

```
if-match destination-mac mac-address
```

If you set more than one matching rule for the same classifier, you can set their relationship by configuring **operator** in Step 2:

- Logic operator **and**: A packet belongs to the classifier only when it matches all rules.
- Logic operator **or**: A packet belongs to the classifier if it matches any one of the rules.
- By default, the logical operator of the rules is **or**.

If multiple matching rules are configured in one traffic policy, the traffic behaviors corresponding to the traffic classifiers are implemented in different orders.

- When multiple matching rules are configured to classify traffic based on different fields in IP packet, the traffic behavior corresponding to the traffic classifier that is first bound to a traffic policy is implemented.

For example, three matching rules are bound to policy1; classifier1 is configured first and classifier3 last, as shown in **Table 4-1**. If a packet matches all the three matching rules, the system performs behavior1, that is, re-marks the 802.1p priority as 1.

Table 4-1 Traffic classifiers and behaviors defined in policy1

Traffic Classifier Name	Matching Rule	Traffic Behavior Name	Action
classifier1	Matching traffic based on the destination MAC address	behavior1	Re-marking the 802.1p priority as 1
classifier2	Matching traffic based on the VLAN ID	behavior2	Re-marking the 802.1p priority as 2
classifier3	Matching traffic based on the source MAC address	behavior3	Re-marking the 802.1p priority as 3

- When multiple matching rules are configured to classify traffic based on the same field in IP packets, no packet can match all matching rules; as a result, the traffic behavior corresponding to the traffic classifier of packets that match a specific matching rule is performed.

For example, three traffic classifiers with their corresponding traffic behaviors are bound to policy2; classifier1 is configured first and classifier3 last, as shown in **Table 4-2**. Because the matching rules in traffic classifiers are configured to classify traffic based on the same IP packet field, a packet can match only one matching rule. As a result, the system performs the traffic behavior corresponding to the traffic classifier that matches the matching rule.

Table 4-2 Traffic classifiers and behaviors defined in policy2

Traffic Classifier Name	Matching Rule	Traffic Behavior Name	Action
classifier1	Matching traffic based on the destination MAC address 1-1-1	behavior1	Re-marking the 802.1p priority as 1
classifier2	Matching traffic based on the destination MAC address 2-2-2	behavior2	Re-marking the 802.1p priority as 2
classifier3	Matching traffic based on the destination MAC address 3-3-3	behavior3	Re-marking the 802.1p priority as 3

- Matching rules can be configured to classify traffic based on the same field or different fields in IP packets.
 - If traffic classifiers match the same field in IP packets, no conflict occurs.
 - If traffic classifiers match different fields in IP packets, the traffic behavior corresponding to the traffic classifier that is first bound to a traffic policy is performed.

For example, three traffic classifiers with their corresponding traffic behaviors are bundled into policy3; classifier1 is configured first and classifier3 last, as shown in **Table 4-3**. In this policy, classifier1 and classifier3 match the same field in IP packets, and no conflict occurs. When a packet matches both classifier1 and classifier2, the traffic behavior corresponding to classifier1 is performed. When a packet matches both classifier2 and classifier3, the traffic behavior corresponding to classifier2 is performed.

Table 4-3 Traffic classifiers and behaviors defined in policy3

Traffic Classifier Name	Traffic Rule	Traffic Behavior Name	Traffic Action
classifier1	Matching traffic based on the destination MAC address 1-1-1	behavior1	Re-marking the 802.1p priority as 1
classifier2	Matching traffic based on the source MAC address 2-2-2	behavior2	Re-marking the 802.1p priority as 2
classifier3	Matching traffic based on the destination MAC address 3-3-3	behavior3	Re-marking the 802.1p priority as 3

----End

4.2.3 Defining a Traffic Behavior and Configuring Traffic Actions

This section describes how to configure traffic behaviors.

Context

The NE80E/40E supports various types of traffic behaviors. You can choose one or more behaviors to meet your requirements.

Procedure

- Setting packet filtering actions

Do as follows on the router:

- Run:

```
system-view
```

The system view is displayed.

- Run:

```
traffic behavior behavior-name
```

A traffic behavior is defined and the traffic behavior view is displayed.

3. Run:

permit

Packets are allowed to pass.

Or run:

deny

Packets are discarded.

 **NOTE**

If you run both the **if-match any** and the **deny** commands to configure complex traffic classification, the device discards all packets, including protocol packets, that flow through an interface. Therefore, be cautious about configuring traffic classifiers and traffic behaviors by using the preceding commands.

If you set the permit or deny action in both the **rule** command and the traffic behavior view, the traffic action is implemented only on packets that are permitted by the **rule** command. If you configure the deny action in either the **rule** command or the traffic behavior view, all matched packets are denied.

If no traffic action is configured in the traffic behavior view, the default action is **permit**. The traffic that matches the rule in the traffic classifier is allowed to pass.

● Setting traffic policing actions

Do as follows on the router:

1. Run:

system-view

The system view is displayed.

2. Run:

traffic behavior behavior-name

A traffic behavior is set and the traffic behavior view is displayed.

3. Run:

```
car { cir cir-value [ pir pir-value ] [ cbs cbs-value pbs pbs-value ]  
[ green { discard | pass [ service-class class color color ] } | yellow  
{ discard | pass [ service-class class color color ] } | red { discard |  
pass [ service-class class color color ] } ]*
```

A traffic policing action is set in the traffic behavior.

After you configure a traffic policing action for a traffic policy, the traffic policy can be applied to both an inbound interface and an outbound interface.

If you configure a traffic policy with a traffic policing action on an interface, traffic policing defined by command parameters is implemented on the matched packets; traffic policing configured by the **qos car** command is implemented on the non-matched packets.

If you run this command for the same traffic policy more than once, the latest configuration takes effect.

 **NOTE**

If packets are re-marked as ef, be, cs6, and cs7, the packets can only be re-marked green.

● Defining a traffic behavior to set the precedence of packets

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is set and the traffic behavior view is displayed.

3. Run the following command as required.

- To re-configure the precedence of IP packets, run:

```
remark ip-precedence ip-precedence
```

- To re-configure the DSCP value of IPv6 packets, run:

```
remark [ ipv6 ] dscp dscp-value
```

- To re-configure the precedence of MPLS packets, run:

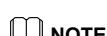
```
remark mpls-exp exp
```

- To re-configure the precedence of VLAN packets, run:

```
remark 8021p 8021p-value
```

- To re-configure the IP ToS value, run:

```
remark tos tos-value
```



NOTE

Run the **remark ipv6 dscp dscp-value** command to re-configure the DSCP value of IPv6 packets.

The **remark [ipv6] dscp dscp-value** command does not take effect on Layer 2 packets.

The **remark mpls-exp exp** command can be run only on the inbound interface of the router.

The 802.1p-based complex traffic classification does not support MPLS and DSCP re-marking. The traffic policy that defines the action of re-marking the 802.1p priority can be applied to only the outbound Ethernet sub-interface.

The LPUA, LPUF-10, LPUG, and LPUH support the re-marking of the 802.1p priority in the inner tag of packets in the outbound. The LPUB, LPUF-21 and LPUF-40 support the re-marking of the 802.1p priority in the inner tag of packets in the inbound.

- Defining a traffic behavior to set the class of service (CoS) in packets

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is set and the traffic behavior view is displayed.

3. Run:

```
service-class service-class color color
```

The CoS in packets is set.

Setting the CoS applies to only upstream packets. Specifying the CoS and drop precedence of packets allows matched packets to be placed in corresponding queues. In this case, the router does not need to look up the BA table according to the precedence field in the packets to determine the CoS. In addition, the packets can be transparently transmitted with no need to change the precedence field in the packet.

EF, BE, CS6, and CS7 packets cannot be re-marked yellow or red.

- Defining a traffic behavior to redirect packets



CAUTION

- Logical interfaces, such as VLANIF, RINGIF, and trunk interfaces, do not support redirection of packets to multiple next hops and outbound interfaces.
- Redirection to an LSP on the public network can be configured only on the ingress of the MPLS network.
- Redirection to an LSP on the public network applies to only packets with a single MPLS tag.

Do as follows on the router:

- Run:

```
system-view
```

The system view is displayed.

- Run:

```
traffic behavior behavior-name
```

A traffic behavior is set and the traffic behavior view is displayed.

- Run the following command as required.

- To forward packets directly instead of redirecting them, run (in the traffic behavior view):

```
permit
```

- To discard packets directly instead of redirecting them, run (in the traffic behavior view):

```
deny
```

- To re-configure a single next hop to be redirected, run:

```
redirect ip-nexthop ip-address [ interface interface-type ]
```

- To re-configure multiple next hops to be redirected, run:

```
redirect ipv4-multihop { nhp ip-address [ interface interface-type interface-number ] } &lt;2-4>
```

- To redirect IP data flows to a destination LSP on the public network, run:

```
redirect lsp public dest-ipv4-address [ nexthop-address | interface interface-type interface-number | secondary ]
```

- To redirect packets to a service instance, run:

```
redirect service-instance instance-name
```

- To redirect packets to a specified VPN group, run:

```
redirect vpn-group vpn-group-name
```



NOTE

To re-configure redirection of IPv6 packets to a single next hop, run **redirect ipv6-nexthop**.

To redirect IPv6 packets to a single multiple hop, run the **redirect ipv6-multihop** command.

When the **redirect ipv4-multihop** command is configured to redirect IPv4 packets to multiple next hops, if the outbound interface and VPN group are not specified, the command indicates a weak policy route.

The action **deny** and other traffic actions are mutually exclusive. For the traffic that is configured with the **deny** action, the traffic can be further processed only after it is configured with the **permit** action.

- Setting the load balancing mode

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is set and the traffic behavior view is displayed.

3. Run:

```
load-balance { flow | packet }
```

The load balancing mode is specified as flow by flow or packet by packet.

----End

4.2.4 Defining a Traffic Policy and Specifying a Traffic Behavior for a Traffic Classifier

After defining traffic classifiers and traffic behaviors, you need to configure a traffic policy in which the traffic classifiers and traffic behaviors are associated.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic policy policy-name
```

A traffic policy is defined and the traffic policy view is displayed.

Step 3 Run:

```
classifier classifier-name behavior behavior-name [ precedence precedence ]
```

A traffic behavior is specified for a traffic classifier in the traffic policy.

When **precedence** *precedence* is specified, the action of the classifier is preferentially performed. The small the value, the higher the precedence.

----End

4.2.5 Applying a Traffic Policy

A class-based traffic policy takes effect only after being applied to an interface.

Procedure

- Applying a traffic policy to Layer 3 interfaces



NOTE

- You can apply a traffic policy to the POS, GE, ATM (on the LPUF), QinQ, GRE tunnel/MTunnel, RINGIF, IP-Trunk, and Eth-Trunk interfaces or their sub-interfaces, and logical interfaces such as VE interfaces on the LPUF or LPUF-20.
- Traffic policies cannot be directly implemented on VLANIF interfaces. They can be applied to the physical interfaces or Layer 2 Eth-Trunk interfaces with VLAN IDs being specified.

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The specified interface view is displayed.

3. Run:

```
traffic-policy policy-name { inbound | outbound } [ link-layer | all-layer | mpls-layer ]
```

The specified traffic policy is applied to the interface.

If **link-layer** is configured, the NE80E/40E performs complex traffic classification based on Layer 2 information about the packets.

If **all-layer** is configured, when a traffic policy is applied to the interface, the system first matches packets against rules and performs the corresponding action based on Layer 2 information about packets. If Layer 2 information about packets fails to match traffic classification rules, the system matches the packets against rules and performs the corresponding action based on Layer 3 information about the packets.

If you specify the keyword **mpls-layer**, a router performs complex traffic classification based on the MPLS information of the packets.

By default, the NE80E/40E performs complex traffic classification based on Layer 3 or Layer 4 information about packets.

- Applying a traffic policy to Layer 2 interfaces

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The specified interface view is displayed.

3. Run:

```
portswitch
```

The interface is switched as a Layer 2 interface.

4. Run:

```
traffic-policy policy-name { inbound | outbound } [ vlan vlan-id1 [ to  
vlan-id2 ] ] [ link-layer | all-layer | mpls-layer ]
```

The specified traffic policy is applied to the Layer 2 interface.

 **NOTE**

You can apply traffic policies to Ethernet, GE, or Eth-Trunk interfaces that work in Layer 2 mode.

If you apply a traffic policy without specifying a VLAN, the traffic policy is applied to the VLAN switch services that flow through the interface or the service traffic that is added to a PBB-TE tunnel in interface mode.

To apply a traffic policy to VLAN switch services on a Layer 2 interface or the service traffic that is added to PBB-TE tunnel in interface mode, you do not need to specify a VLAN ID. You must, however, specify a VLAN ID if you apply a traffic policy to the VLAN traffic that goes through a Layer 2 interface.

If no VLAN is specified, a traffic policy is applied to the service traffic that flows through the interface.

You do not need to specify a VLAN ID if you apply a traffic policy to VLAN switch services on a Layer 2 interface. You must, however, specify a VLAN ID if you apply a traffic policy to the VLAN traffic that goes through a Layer 2 interface.

- Applying a traffic policy in the system view

 **NOTE**

Applying a traffic policy in the system view takes effect on only access users on the access interface.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic-policy policy-name inbound
```

The specified traffic policy is applied in the system view.

----End

4.2.6 Applying the Statistics Function of a Traffic Policy

You need to enable the statistics function before viewing the statistics about the traffic policy.

Context

Do as follows on the router where a traffic policy is applied:

Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

- Step 2** Run:

```
traffic-policy policy-name
```

The defined traffic policy view is displayed.

Step 3 Run:

```
statistics enable
```

The statistics function of a traffic policy is enabled.

Step 4 Run:

```
share-mode
```

The shared mode is specified for the traffic policy.



Step 3 is optional. To save memory, by default, the system does not enable the statistics function of a traffic policy. Before you can view the statistics about a traffic policy, you need to enable the statistics function of a traffic policy.

Step 4 is optional. The default attribute of a policy is shared.

- After a traffic policy is applied to an interface, you cannot change the shared or unshared mode of a traffic policy. Before changing the shared or unshared mode of a traffic policy, you must remove the application of the traffic policy from the interface.
- A traffic policy with the shared attribute: Although traffic policies are applied on different interfaces, statistics to be displayed are the final data obtained after calculation. Therefore, the original data on each interface is unidentified.
- A traffic policy with the unshared attribute: You can obtain the statistics about a traffic policy based on the interface where the traffic policy is applied.
- Inbound or outbound traffic is differentiated in traffic statistics, irrespective of whether the shared or unshared mode is specified.

----End

4.2.7 Checking the Configuration

After class-based QoS is configured, you can view information about the configured traffic classifiers, traffic behaviors, traffic policies in which the specified classifiers and behaviors are associated, and traffic statistics on interfaces.

Context

Run the following **display** commands to check the previous configurations.

Procedure

- Run the **display interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check information about the traffic on an interface.
- Run the **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] command to check information about the traffic behavior.
- Run the **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*] command to check information about the traffic classifier.
- Run the **display traffic policy** { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] command to check the classifier and behavior in the traffic policy.
- Using the **display traffic policy interface brief** [*interface-type* [*interface-number*]] command to check information about traffic policies configured on a specified interface or all interfaces.

- Run the **display traffic policy statistics interface interface-number [.sub-interface] { vlan vlan-id | pe-vid pe-vid ce-vid ce-vid } { inbound | outbound } [verbose { classifier-based | rule-based } [class class-name]]** command to check the statistics about the traffic policy on an interface.

----End

Example

If the configuration succeeds:

- Run the **display traffic behavior** command, and you can view the name of the configured traffic behavior and actions.
- Run the **display traffic classifier** command, and you can view the name of the configured traffic classifier and its matching rules, as well as the logic operator of the rules.
- Run the **display traffic policy** command, and you can view the name of the configured traffic policy and the associated behavior and classifier.
- Run the **display traffic policy interface brief** command, and you can view the statistics on traffic policies configured on interfaces. For example:

```
<HUAWEI> display traffic policy interface brief
      Interface           InboundPolicy        OutboundPolicy
      Ethernet2/1/0          tp3                  tp4
      Ethernet2/1/1          -                   tp6
      Ethernet2/1/1.1         -                   tp2
      GigabitEthernet3/2/0     tp1                  -
      Vlan 1 to 100          -                   tp4
      Vlan 200 to 300         tp3                  -
```

- Run the **display traffic policy statistics** command, and you can view the statistics on the traffic policy on an interface. For example:

```
<HUAWEI> display traffic policy statistics interface gigabitethernet 1/0/0
inbound
Interface: GigabitEthernet1/0/0
Traffic policy inbound: test
Traffic policy applied at 2007-08-30 18:30:20
Statistics enabled at 2007-08-30 18:30:20
Statistics last cleared: Never
Rule number: 7 IPv4, 1 IPv6
Current status: OK!
      Item            Packets          Bytes
      -----
      Matched          1,000       100,000
      +-+Passed        500        50,000
      +-+Dropped       500        50,000
      +-+Filter         100       10,000
      +-+URPF          0           0
      +-+CAR            300       30,000
      Missed          500        50,000
Last 30 seconds rate
      Item            pps            bps
      -----
      Matched          1,000       100,000
      +-+Passed        500        50,000
      +-+Dropped       500        50,000
      +-+Filter         100       10,000
      +-+URPF          0           0
      +-+CAR            300       30,000
      Missed          500        50,000
```

4.3 Configuring UCL-based Traffic Policies

By configuring UCL-based traffic policies, you can distinguish between users of different priorities and implement QoS on the traffic of users. In this manner, the CIR and PIR are guaranteed for users.

Context



User access cannot be configured on the X1 and X2 models of the NE80E/40E.

4.3.1 Establishing the Configuration Task

Before configuring UCL-based traffic policies, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

UCL refers to the user-based ACL. When access users are authorized, the traffic of some users needs to be restricted. For example, you may need to allow users to visit the specified websites, or to deny them the access to the specified websites. In this case, you can configure UCL-based traffic policies.

By configuring UCL-based traffic policies on the access device, you can distinguish between users of different priorities and implement QoS on traffic of the users, thus ensuring the Committed Information Rate (CIR) and Peak Information Rate (PIR) of users. Four types of UCLs are defined based on the configuration methods: user-to-network, user-to-user, network-to-network, and network-to-user. If an ACL specifies the source user group (UG), the type of the ACL is user-to-network; if the destination UG is specified, the type of the ACL is network-to-user; if both the source UG and destination UG are specified, the type of the ACL is user-to-user; if neither the source UG or destination UG is specified, the type of the ACL is network-to-network.



UCLs support the classifying of both IPv4 and IPv6 traffic. Note that with IPv6 traffic, classification is supported for only upstream traffic.

Pre-configuration Tasks

Before configuring UCL-based traffic policies, complete the following tasks:

- Configuring parameters of the link layer protocol and IP addresses for interfaces to ensure that the link layer protocol on the interfaces is Up
- Configuring a routing protocol on the backbone network to realize the IP interworking
- Configuring the access services to enable the users to access the Internet normally

Data Preparation

To configure UCL-based traffic policies, you need the following data.

No.	Data
1	User group name
2	Traffic classifier name
3	Number of the UCL and its rules
4	Traffic behavior name
5	Data in a traffic behavior, including the CIR, PIR, CBS, PBS, DSCP value, IP precedence, EXP value, 802.1p priority, next hop address, or outbound interface
6	Traffic policy name
7	Name of the domain to which users belong

4.3.2 Configuring a User Group

You need to create a user group before configuring UCL-based traffic policies.

Context

Do as follows on the router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-group group-name
```

A new user group is created.

----End

4.3.3 Configuring a UCL Rule

You can configure UCLs based on IP bearer protocol types.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

The UCL view is displayed.

The value of *acl-number* corresponding to the UCL ranges from 6000 to 9999.

Step 3 Configure the UCL according to actual networking requirements.

```
rule [ rule-id ] { deny | permit } protocol [ destination { any | ip-address { destination-ip-  
address destination-wildcard | any } | user-group { destination-group-name | any } } |  
destination-port operator port | fragment-type fragment-type-name | logging | source { any |  
ip-address { source-ip-address source-wildcard | any } | user-group { source-group-name |  
any } } | source-port operator port | syn-flag syn-flag | time-range time-name | dscp dscp |  
precedence precedence | tos tos | vpn-instance vpn-instance-name ] *
```

syn-flag *syn-flag* is applicable only when *protocol* is specified as TCP.

 **NOTE**

You can configure the UCL as required according to the protocol type. Parameters in the UCL vary with the protocol type. The combination of [**source-port** *operator port*] [**destination-port** *operator port*] is applicable to TCP and UDP only.

To add multiple rules to the UCL, you can repeat Step 3.

The sequence for matching multiple rules of the same UCL can be configured to depth-first (auto) or configuration-first (config). By default, multiple rules are matched according to the configuration-first principle. That is, the rule that is configured first is matched first.

Step 4 Run:

```
quit
```

Quit the UCL view.

----End

4.3.4 Defining a Traffic Classifier

Before configuring class-based QoS for the traffic on the network, you need to define a traffic classifier.

Context

Do as follows on the router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic classifier classifier-name [ operator { and | or } ]
```

A traffic classifier is defined and the traffic classifier view is displayed.

By default, if the operator is not specified, the logical relationship between matching rules in the traffic classifier is "OR".



NOTE

When a traffic classifier is defined for UCL, the logical relationship "and" between matching rules does not take effect.

Step 3 Run:

```
if-match [ ipv6 ] acl acl-number
```

A UCL-based complex traffic classification rule is configured.

In this configuration, the value of *acl-number* ranges from 6000 to 9999.

To configure multiple UCL-based complex traffic classification rules, you can repeat this step.

----End

4.3.5 Defining a Traffic Behavior and Configuring Actions

This section describes how to configure traffic behaviors.

Context

The NE80E/40E supports various types of traffic behaviors and traffic actions. You can choose one or more types of traffic behaviors and traffic actions as required.

Procedure

- Configuring a packet filtering action

Do as follows on the router:

- Run:

```
system-view
```

The system view is displayed.

- Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

- Do as follows to configure the traffic action deny or permit:

- To configure a deny action, run the **deny** [**packet-length** { **eq** length | **gt** length | **lt** length | **range** min-length max-length }] command.
- To configure a permit action, run the **permit** command.



NOTE

If both the **if-match any** and **deny** parameters are configured in the complex traffic classification rule, all packets, including protocol packets, are discarded by the interface. Therefore, use caution when configuring both the **if-match any** and **deny** parameters in a traffic classification rule.

If the permit and deny actions are configured in both the **rule** command and the traffic behavior view, only packets that are permitted by the **rule** command are further processed. If the deny action is configured in either the **rule** command or the traffic behavior view, all matched packets are discarded.

- Setting the random packet drop ratio

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Run:

```
random-discard discard-rate
```

The random packet drop ratio is configured.

- Configuring a traffic policing action

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Run:

```
car { cir cir-value [ pir pir-value ] } [ cbs cbs-value pbs pbs-value ]  
[ green { discard | pass [ service-class class color color ] } | yellow  
{ discard | pass [ service-class class color color ] } | red { discard |  
pass [ service-class class color color ] } ]*[ summary ]
```

A traffic policing action is configured.

This command is cyclic in nature. That is, if this command is configured for multiple times, only the last configuration takes effect. If the parameter **summary** is specified in the command, traffic policing is implemented on value-added services and basic services as a whole.



If the CoSs of packets are re-marked as EF, BE, CS6, and CS7, the colors of these packets can only be re-marked green.

- Setting the priority of packets

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Do as follows as required:

- To re-set the precedence of IP packets, run the **remark ip-precedence ip-precedence** command.

- To re-set the DSCP value of IP packets, run the **remark [ipv6] dscp *dscp-value*** command.
- To re-set the precedence of MPLS packets, run the **remark mpls-exp *exp*** command.
- To re-set the priority of VLAN packets, run the **remark 8021p 8021p-value** command.

 **NOTE**

To re-set the DSCP value of IPv6 packets, run the **remark ipv6 dscp *dscp-value*** command. This command does not take effect on Layer 2 traffic.

The remark **remark mpls-exp *exp*** can be applied to only upstream traffic on the router.

The 802.1p-based complex traffic classification does not support MPLS re-marking and DSCP re-marking.

● Setting the CoS of packets

Do as follows on the router:

1. Run:

system-view

The system view is displayed.

2. Run:

traffic behavior *behavior-name*

A traffic behavior is configured and the traffic behavior view is displayed.

3. Run:

service-class *service-class* color *color*

The CoS of packets is set.

Setting the CoS of packets applies to only upstream packets. It is used to specify the CoS and drop priority of packets so that the matched packets can enter the queues of the corresponding CoS values. In this manner, the device does not need to determine the CoS of packets by searching the BA table according to the precedence field in a packet header. Besides, this enables the device to implement transparent transmission of packets without changing the precedence fields of packets.

If the service class of packets is EF, BE, CS6, or CS7, the packets cannot be re-marked yellow or red.

● Setting a packet forwarding action



CAUTION

- Currently, for logical interfaces such as VLANIF, Ring-if and Trunk interfaces, multiple next-hop IP addresses and outbound interfaces are not supported for redirected packets.
 - Redirection of packets to the public network LSP can be configured only on the ingress node of the MPLS network, and cannot be configured on other nodes such as transit or egress.
 - Redirection of packets to the public network LSP can be configured for only single-tagged MPLS packets.
-

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Do as follows as required:

- To directly forward packets without redirecting them, run the **permit** command in the traffic behavior view.
- To directly drop packets without redirecting them, run the **deny** command in the traffic behavior view.
- To redirect packets to a single next hop, run the **redirect ip-nexthop ip-address [interface interface-type interface-number]** command.
- To re-configure multiple next hops to be re-directed, run:

```
redirect ipv4-multhp { nhp ip-address [ interface interface-type interface-number ] } &<2-4>
```
- To redirect IP packets to the public network LSP, run the **redirect lsp public dest-ipv4-address [nexthop-address | interface interface-type interface-number | secondary]** command.
- To redirect packets to a service instance, run the **redirect service-instance instance-name** command.
- To redirect packets to a specified VPN group, run the **redirect vpn-group vpn-group-name** command.

NOTE

To redirect IPv6 packets to a single next hop, run the **redirect ipv6-nexthop** command.

To redirect IPv6 packets to a single multiple hop, run the **redirect ipv6-multhp** command.

When the **redirect ipv4-multhp** command is configured to redirect IPv4 packets to multiple next hops, if the outbound interface and VPN group are not specified, the command indicates a weak policy route.

The action **deny** and other traffic actions are mutually exclusive. For the traffic that is configured with the **deny** action, the traffic can be further processed only after it is configured with the **permit** action.

- Setting the load balancing mode

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Run:

```
load-balance { flow | packet }
```

The load balancing mode is set to flow-by-flow or packet-by-packet.

- Setting the user queue scheduling

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Run:

```
user-queue cir cir-value [ [ pir pir-value ] | [ flow-queue flow-queue-name ] | [ flow-mapping mapping-name ] | [ user-group-queue group-name ] | [ service-template service-template-name ] ]*
```

User queue scheduling parameters are set.

The commands **user-queue** and **car** in one traffic behavior are mutually exclusive.

The commands **user-queue** can be configured on the inbound.

- Setting the traffic statistics method

Do as follows on the router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

3. Run:

```
traffic-statistic [ summary ]
```

```
traffic-statistic [ summary ]
```

If the parameter **summary** is specified in the command, traffic statistics are implemented on value-added services and basic services as a whole.

----End

4.3.6 Defining a Traffic Policy

After defining traffic classifiers and traffic behaviors, you need to configure a traffic policy in which the traffic classifiers and traffic behaviors are associated.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic policy policy-name
```

A traffic policy is defined and the traffic policy view is displayed.

Step 3 Run:

```
classifier classifier-name behavior behavior-name [ precedence precedence ]
```

A traffic behavior is specified for the specified traffic class in the traffic policy.

When the parameter **precedence** *precedence* is specified, the classifier is performed as the precedence. The small the value, the higher the precedence, meaning that the action of the classifier is preferentially performed.

----End

4.3.7 Applying UCL-based Traffic Policies

After the UCL-based traffic policies are applied, the traffic of all online users is classified according to the UCL rules.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic-policy policy-name { inbound | outbound }
```

A traffic policy is applied to online users.

After the UCL-based traffic policy is applied in the system view, the traffic of all online users is classified according to the UCL.

When traffic policies are configured in both the system view and the interface view, on the network side, the traffic policies that are configured in the interface view take effect, whereas on the user side, UCL-based traffic policies take effect.

----End

4.3.8 Specifying the Domain of a User

You need to create a domain to which a user group belongs and specify certain users for whom UCL-based traffic policies are implemented in the domain.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
domain
```

The AAA domain view is displayed.

Step 4 Run:

```
user-group user-group-name
```

The domain to which the user belongs is specified.

----End

4.3.9 (Optional) Applying the Statistic Function of a Traffic Policy

To view the statistics about a traffic policy, you need to enable the statistic function for the traffic policy.

Context

Do as follows on the router where a traffic policy is applied:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic policy policy-name
```

The defined policy view is displayed.

Step 3 Run:

```
statistics enable
```

The statistic function of a traffic policy is enabled.



Step 3 is optional. To save the memory, the system does not enable the statistic function of a traffic policy by default. To display the statistics of a traffic policy, you can enable the statistic function of a traffic policy.

----End

4.3.10 Checking the Configuration

After UCL-based traffic policies are configured, you can view the information about the traffic policies on a specified interface or all interfaces and statistics about UCL-based traffic policies.

Context

Use the following **display** commands to check the previous configuration.

Procedure

- Using the **display interface** [*interface-type* [*interface-number*]] [| {**begin** | **exclude**} **include** } *regular-expression*] command to check information about the traffic on an interface.
- Using the **display traffic behavior** { system-defined | user-defined } [*behavior-name*] command to check the traffic behavior.
- Using the **display traffic classifier** { system-defined | user-defined } [*classifier-name*] command to check the traffic classifier.
- Using the **display traffic policy** { system-defined | user-defined } [*policy-name* [*classifier classifier-name*]] command to check the class and the behavior in the traffic policy.
- Using the **display traffic policy interface brief** [*interface-type* [*interface-number*]] command to check information about traffic policies configured on a specified interface or all interfaces.
- Using the **display traffic policy statistics ucl** [slot *slot-id*] { **inbound** | **outbound** } [| **count**] [| {**begin** | **include** | **exclude**} *regular-expression*] [**verbose** { **classifier-based** | **rule-based** } [**class** *class-name*]] command to check the statistics about UCL-based Traffic Policies.

---End

Example

If the configuration succeeds:

- You can view the name of the configured traffic behavior and actions when you run the **display traffic behavior** command.
- You can view the name of the configured traffic classifier and its matching rules, as well as the logic operator of the rules when you run the **display traffic classifier** command.
- You can view the statistics about UCL-based Traffic Policies when you run the **display traffic policy statistics ucl** command.

```
<HUAWEI> display traffic policy statistics ucl slot 2 inbound
Traffic policy inbound: p1
Traffic policy applied at 2009-09-03 20:25:50
Statistics enabled at 2009-09-03 20:25:50
Statistics last cleared: Never
Rule number: 2 IPv4, 0 IPv6
Current status: OK!
      Item          Packets          Bytes
-----+
Matched          20,935,529    2,009,808,208
    +-Passed        543,363      52,178,560
    +-Dropped       20,392,166    1,957,629,648
    +-Filter           0              0
    +-URPF            0              0
```

Missed	20,392,166	0	1,957,629,648	0
Last 30 seconds rate				
Item	pps	bps	bps	
Matched	1,007,607	773,842,816		
+--Passed	26,326	20,225,840		
+--Dropped	981,281	753,616,976		
+--Filter	0	0		
+--URPF	0	0		
+--CAR	981,281	753,616,976		
Missed	0	0		

4.4 Configuring Precedence Mapping Based on Simple Traffic Classification

Precedence mapping based on simple traffic classification is used to map the priority of traffic on one network to that of traffic on another network. This allows traffic to be transmitted on another network based on the previous priority or the user-defined priority.

Context



The NE80E/40E supports simple traffic classification on POS, GE, and QinQ interfaces and their sub-interfaces, and logical interfaces such as RINGIF, IP-Trunk, and Eth-Trunk interfaces. For details about how to configure a QinQ interface, see "QinQ Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - LAN Access and MAN Access*.

Using the **qos default-service-class** command, you can configure the upstream traffic on the interface to enter the specific queues and provide service. By default, the traffic enters the queues with the service class as BE. After this command is run, other packets cannot be enabled to enter the queues, and simple traffic classification cannot be enabled.

4.4.1 Establishing the Configuration Task

Before configuring precedence mapping based on simple traffic classification, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Precedence mapping based on simple traffic classification is used to map the precedence of traffic on one type of network to another type. In this manner, the traffic is transmitted on another type of network based on its original precedence.

When the NE80E/40E serves as the border router of different networks, the precedence fields (802.1p, DSCP, and EXP fields) in the packets that enter the NE80E/40E are all mapped to the internal precedence (CoS and color) of the router. When the NE80E/40E sends out the packets, the internal precedence is mapped back to the external precedence.

Simple traffic classification is usually implemented on the core devices of the network. It can be implemented on both physical and logical interfaces. If being implemented on the logical interface, simple traffic classification can prevent traffic congestion on member interfaces of the logical interface and set the precedence of packets on the logical interface.

 **NOTE**

For GRE tunnel packets, only the precedence in the outer tunnel label can be changed. The inner IP precedence in the IP packets remains unchanged.

For precedence mappings in simple traffic classification, packets with the CoSs of BE, EF, CS6, and CS7 can only be marked green.

A DiffServ (DS) domain is a group of DiffServ nodes that adopt the same service policies and implement the same PHB.

The precedence of packets is usually accepted or re-defined on the core router. On the border router in the IP domain or MPLS domain, the DSCP and EXP values also need to be mapped.

Simple traffic classification can map the internal precedence to the external precedence, and the external precedence to the internal precedence. However, mapping between traffic of the same type, for example, IP traffic or MPLS traffic, is not supported.

Pre-configuration Tasks

Before configuring precedence mapping based on simple traffic classification, complete the following tasks:

- Configuring physical parameters for interfaces
- Configuring link layer attributes for interfaces to ensure that the interfaces work normally
- Configuring IP addresses for interfaces
- Enabling routing protocols to ensure that routes are reachable

Data Preparations

To configure precedence mapping based on simple traffic classification, you need the following data.

No.	Data
1	DS domain name
2	802.1p priorities and CoSs of inbound/outbound VLAN packets
3	DSCP values and CoSs of inbound/outbound IP packets
4	EXP values, CoSs, and colors of inbound/outbound MPLS packets
5	Type and number of the interface on which the DS domain is enabled

4.4.2 Configuring Priority Mapping for VLAN Packets

You can configure the mappings among the 802.1p priority, CoS, and color to implement QoS on VLAN packets.

Context

Do as follows on the router:



NOTE

If congestion occurs on the interface on the 8GE sub-interface of the LPUF-10, run the **set pic-forwarding** command to configure the scheduling priorities of the untagged packets or tagged packets on the interface. The packets with higher priorities are scheduled first. Those with lower priorities are buffered before being scheduled. In this manner, the transmission quality can be guaranteed for the packets with higher priorities. The 802.1p priorities must be specified for tagged packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
difffserv domain { ds-domain-name | default }
```

A DS domain is defined and the DS domain view is displayed.

Step 3 Run:

- **8021p-inbound** 8021p-code phb service-class [color]

Mapping from the 802.1p field to the COS value is set for incoming VLAN packets.

- **8021p-outbound** service-class color map 8021p-code

Mapping from the COS value to the 802.1p field is set for outgoing VLAN packets.

Following DS domain templates are pre-defined by the system for VLAN packets: the 5p3d domain template, and the default domain template.

- The 5p3d domain template describes mapping relations from the 802.1 priorities of VLAN packets to the QoS CoSs and colors, or from the QoS CoSs and colors to the 802.1 priorities. These mapping relations are not configurable. The 802.1p priorities of the packets from an upstream device are mapped to the QoS CoSs and colors. Their mapping relations are shown in **Table 4-4**. The QoS CoSs and colors of the packets going to a downstream device are mapped to the 802.1p priorities. Their mapping relations are shown in **Table 4-5**.

Table 4-4 Mappings from 802.1p priorities to QoS CoSs and colors in the 5p3d domain template

802.1p	CoS	Color	802.1p	CoS	Color
0	BE	Yellow	4	AF4	Yellow
1	BE	Green	5	AF4	Green
2	AF2	Yellow	6	CS6	Green
3	AF2	Green	7	CS7	Green

Table 4-5 Mappings from QoS CoSs and colors to 802.1p priorities in the 5p3d domain template

Service	Color	802.1p	Service	Color	802.1p
BE	Green	1	AF3	Yellow	2
AF1	Green	1	AF3	Red	2
AF1	Yellow	0	AF4	Green	5
AF1	Red	0	AF4	Yellow	4
AF2	Green	3	AF4	Red	4
AF2	Yellow	2	EF	Green	5
AF2	Red	2	CS6	Green	6
AF3	Green	3	CS7	Green	7

- The default domain template describes the default mapping relations from the 802.1p priorities of VLAN packets to the QoS services classes and colors, or from the QoS services classes and colors to the 802.1p priorities. You can change the mapping relations in the default domain template. The 802.1p priorities of the packets from an upstream device are mapped to the QoS CoSs and colors. Their mapping relations are shown in [Table 4-6](#). The QoS CoSs and colors of the packets going to a downstream device are mapped to the 802.1p priorities. Their mapping relations are shown in [Table 4-7](#).

Table 4-6 Mappings from 802.1p priorities to QoS CoSs and colors in the default domain template

802.1p	CoS	Color	802.1p	CoS	Color
0	BE	Green	4	AF4	Green
1	AF1	Green	5	EF	Green
2	AF2	Green	6	CS6	Green
3	AF3	Green	7	CS7	Green

Table 4-7 Mappings from QoS CoSs and colors to 802.1p priorities in the default domain template

CoS	Color	802.1p
BE	Green	0
AF1	Green, yellow, and red	1
AF2	Green, yellow, and red	2
AF3	Green, yellow, and red	3

CoS	Color	802.1p
AF4	Green, yellow, and red	4
EF	Green	5
CS6	Green	6
CS7	Green	7

Step 4 Run:

- Applying Traffic Policies for VLAN Packets to Layer-3 Interfaces

1. Run:

`system-view`

The system view is displayed.

2. Run:

`interface { ethernet | gigabitethernet } interface-number.subnumber`

The specified interface view is displayed.

3. Run:

`trust upstream { 5p3d | ds-domain-name | default }`

The interface is added in the DS domain.

4. Run:

`trust 8021p`

Traffic classification based on the 802.1p field is enabled.

 **NOTE**

- You can run the `trust 8021p` command only on the Ethernet (including Eth-trunk) sub-interface and the interface where you run the `portswitch` command .
- Before you run this command, you must add the interface to the DS domain first. Otherwise, the configuration does not take effect.

After an interface is added to a DS domain, the traffic policies defined in this domain can act on the incoming and outgoing traffic on this interface.

- Applying Traffic Policies for VLAN Packets to Layer-2 Interfaces

1. Run:

`system-view`

The system view is displayed.

2. Run:

`interface { ethernet | gigabitethernet } interface-number`

The specified interface view is displayed.

3. Run:

`portswitch`

The interface becomes a layer-2 interface.

4. Run:

`trust upstream { 5p3d | ds-domain-name | default | } [vlan { vlan-id1 [to vlan-id2] } <1-10>]`

The port is added to the specified DS domain.

5. Run:

`trust 8021p vlan { vlan-id1 [to vlan-id2] } <1-10>`

Traffic classification based on the 802.1p field is enabled.

 NOTE

If no VLAN ID is specified, the traffic policy of the simple traffic classification is applied to the VLAN switch packets that flow through the port.

You do not need to specify a VLAN ID if you apply a traffic policy to VLAN switch service packets on a layer-2 interface. You must, however, specify a VLAN ID if you apply a traffic policy to the VLAN packets that go through a layer-2 interface.

----End

4.4.3 Configuring Priority Mapping for IP Packets

You need to configure the mappings among the DSCP value, CoS, and color to implement QoS on IP packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
difffserv domain { ds-domain-name | default }
```

A DS domain is defined and the DS domain view is displayed.

Step 3 Run:

- `ip-dscp-inbound dscp-value phb service-class [color]`

Mapping from the DSCP value to the COS value is set for incoming IP packets.

- `ip-dscp-outbound service-class color map dscp-code`

Mapping from the COS value to the DSCP value is set for outgoing IP packets.

The default domain is pre-defined by the system for IP packets and cannot be deleted by users. If the precedence mapping in Step 3 is not set in the DS domain, the system uses the default mapping. The default domain template describes the default mapping relations from the DSCP of IP packets to the QoS services classes and colors, or from the QoS services classes and colors to the DSCP value. You can change the mapping relations in the default domain template. The DSCP values of the packets from an upstream device are mapped to the QoS CoSs and colors. Their mapping relations are shown in [Table 4-8](#). The QoS CoSs and colors of the packets going to a downstream device are mapped to the DSCP value. Their mapping relations are shown in [Table 4-9](#).

The default mapping between DSCP and CoS of IP packets is shown in [Table 4-8](#).

Table 4-8 Default mapping between DSCP value and COS value of IP packets

DSCP	Service	Color	DSCP	Service	Color
00	BE	Green	32	AF4	Green

DSCP	Service	Color	DSCP	Service	Color
01	BE	Green	33	BE	Green
02	BE	Green	34	AF4	Green
03	BE	Green	35	BE	Green
04	BE	Green	36	AF4	Yellow
05	BE	Green	37	BE	Green
06	BE	Green	38	AF4	Red
07	BE	Green	39	BE	Green
08	AF1	Green	40	EF	Green
09	BE	Green	41	BE	Green
10	AF1	Green	42	BE	Green
11	BE	Green	43	BE	Green
12	AF1	Yellow	44	BE	Green
13	BE	Green	45	BE	Green
14	AF1	Red	46	EF	Green
15	BE	Green	47	BE	Green
16	AF2	Green	48	CS6	Green
17	BE	Green	49	BE	Green
18	AF2	Green	50	BE	Green
19	BE	Green	51	BE	Green
20	AF2	Yellow	52	BE	Green
21	BE	Green	53	BE	Green
22	AF2	Red	54	BE	Green
23	BE	Green	55	BE	Green
24	AF3	Green	56	CS7	Green
25	BE	Green	57	BE	Green
26	AF3	Green	58	BE	Green
27	BE	Green	59	BE	Green
28	AF3	Yellow	60	BE	Green
29	BE	Green	61	BE	Green
30	AF3	Red	62	BE	Green

DSCP	Service	Color	DSCP	Service	Color
31	BE	Green	63	BE	Green

The default mapping between the CoS value and the DSCP value is shown in [Table 4-9](#).

Table 4-9 Default mapping between the CoS value and the DSCP value

Service	Color	DSCP
BE	Green	0
AF1	Green	10
AF1	Yellow	12
AF1	Red	14
AF2	Green	18
AF2	Yellow	20
AF2	Red	22
AF3	Green	26
AF3	Yellow	28
AF3	Red	30
AF4	Green	34
AF4	Yellow	36
AF4	Red	38
EF	Green	46
CS6	Green	48
CS7	Green	56

Step 4 Run:

`quit`

Return to the system view.

Step 5 Run:

`interface interface-type interface-number`

The specified interface view is displayed.

Step 6 Run:

`trust upstream { 5p3d | ds-domain-name | default }`

The interface is added in the DS domain and simple traffic classification is enabled.

----End

4.4.4 Configuring Priority Mapping for MPLS Packets

You need to configure the mappings among the EXP value, CoS, and color to implement QoS on MPLS packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
difffserv domain { ds-domain-name | default }
```

A DS domain is defined and the DS domain view is displayed.

Step 3 Run:

- `mpls-exp-inbound exp phb service-class [color]`

Mapping from the EXP value to the COS value is set for incoming MPLS packets.

- `mpls-exp-outbound service-class color map exp`

Mapping from the COS value to the EXP value is set for outgoing MPLS packets.

The default domain is pre-defined by the system. If the precedence mapping in Step 3 is not set in the DS domain, the system uses the default mapping. The default domain template describes the default mapping relations from the EXP of MPLS packets to the QoS services classes and colors, or from the QoS services classes and colors to the EXP value. You can change the mapping relations in the default domain template. The EXP of the packets from an upstream device are mapped to the QoS CoSs and colors. Their mapping relations are shown in [Table 4-10](#). The QoS CoSs and colors of the packets going to a downstream device are mapped to the DSCP value. Their mapping relations are shown in [Table 4-11](#).

The default mapping between the EXP value and the COS value of MPLS packets is shown in [Table 4-10](#).

Table 4-10 Default mapping between the EXP value and the COS value of MPLS packets

EXP	Service	Color	EXP	Service	Color
0	BE	Green	4	AF4	Green
1	AF1	Green	5	EF	Green
2	AF2	Green	6	CS6	Green
3	AF3	Green	7	CS7	Green

The default mapping between the CoS value and the EXP value is shown in **Table 4-11**.

Table 4-11 Default mapping between the CoS value and the EXP value

Service	Color	MPLS EXP
BE	Green	0
AF1	Green, Yellow, Red	1
AF2	Green, Yellow, Red	2
AF3	Green, Yellow, Red	3
AF4	Green, Yellow, Red	4
EF	Green	5
CS6	Green	6
CS7	Green	7

Step 4 Run:

`quit`

Return to the system view.

Step 5 Run:

`interface interface-type interface-number`

The specified interface view is displayed.

Step 6 Run:

`trust upstream { 5p3d | ds-domain-name | default }`

The interface is added in the DS domain and simple traffic classification is enabled.

----End

4.4.5 Configuring Priority Mapping for Control Packets

You need to configure the mappings among the control packet priority, CoS, and color to implement QoS on control packets.

Context

Control packets are usually forwarded with preference so that service interruption resulting from the loss of control packets due to network congestion is avoided.

By default, the system places control packets into the EF queue for being forwarded preferentially.

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`diffserv domain { ds-domain-name | default }`

A DS domain is created and the DS domain view is displayed.

Step 3 Run:

`ppp-inbound control phb service-class [color]`

To map the priorities of PPP control packets to the interior priorities of a router.

Step 4 Run:

`quit`

Return to the system view.

Step 5 Run:

`interface interface-type interface-number`

The specified interface view is displayed.

Step 6 Run:

`trust upstream { 5p3d | ds-domain-name | default }`

The interface is added in the DS domain and simple traffic classification is enabled.

----End

4.4.6 Configuring Priority Mapping for Multicast Packets

You need to configure the mappings among the IP multicast packet priority, CoS, and color to implement QoS on multicast packets.

Context

The NE80E/40E supports the simple traffic classification of multicast packets on its interfaces.

The NE80E/40E also supports simple traffic classification on the MTI that is bound to a distributed multicast VPN.



NOTE

Multicast VPN transmits multicast data on the MPLS/BGP VPN. The NE80E/40E adopts the multicast domains (MDs) mechanism to implement multicast VPN, which is called MD VPN for short. In an MD, private data is transmitted through the multicast tunnel (MT). The VPN instance delivers private data through MTI, which is then received by the remote end through the MTI.

For detailed explanation on multicast VPN and its configurations, refer to *Configuration Guide - IP Multicast*.

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

```
diffserv domain { ds-domain-name | default }
```

A DS domain is defined and the DS domain view is displayed.

Step 3 Select a command according to the type of multicast packets.

- To configure priority mapping for incoming multicast IP packets, run the **ip-multicast-dscp-inbound dscp-value phb service-class** command.
- To configure priority mapping for incoming multicast VLAN packets, run the **8021p-multicast-inbound 8021p-mcast-value phb service-class** command.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 6 Run:

```
trust upstream { ds-domain-name | default }
```

The DS domain is bound to the interface, and simple traffic classification is enabled on the interface.

Traffic policies for distributed multicast VPN packets must be configured on the MTI interface to which the distributed multicast VPN is bound. That is, you need to run the **interface mtunnel interface-number** command to access the MTunnel interface view, and then run the **trust upstream** command to add the MTI that is bound to the distributed multicast VPN to the DS domain and to enable the simple traffic classification.

----End

4.4.7 Configuring User Priority Mapping in a Domain

You need to configure the mappings among the user priority, CoS, and color to implement QoS on packets in a domain.

Context

You can configure the desired priorities for online users. To perform traffic scheduling according to the user priority, you can configure user priority mapping in a domain. After a user in this domain goes online, the priority of the user is mapped to the internal CoS of the device according to the configured mapping relationship.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

domain domain-name

The AAA domain view is displayed.

Step 4 Run:

user-priority { upstream | downstream } { priority | trust-8021p-inner | trust-8021p-outer | trust-dscp-outer | trust-dscp-inner | trust-exp-inner | trust-exp-outer | unchangeable }

The user priority is configured.

The methods for configuring user priorities are as follows:

- Directly specifying the user priority, which ranges from 0 to 7
- Using the internal or external 802.1p value of Layer 2 packets of the user as the user priority (not applicable to packets sent from the network side to the user side)
- Using the DSCP value of user packets as the user priority
- Using the EXP value of MPLS packets as the user priority

Step 5 Run:

diffserv domain { ds-domain-name | default }

A DS domain is defined and the DS domain view is displayed.

Step 6 Run:

user-priority priority phb service-class [color]

Priority mapping is configured for users in a domain.

Before configuring the user priority mapping by running the **user-priority phb** command, you must specify the user priority that needs to be mapped by running the **user-priority** command in the AAA domain. Otherwise, the mapping does not take effect.

If the CoS is CS6, CS7, EF or BE, packets can be marked only in green.

Table 4-12 Default mapping between user priorities and CoSs

User Priority	Service	Color
0	BE	Green
1	AF1	Green
2	AF2	Green
3	AF3	Green
4	AF4	Green
5	EF	Green
6	CS6	Green
7	CS7	Green

Step 7 Run:

`quit`

Return to the system view.

Step 8 Run:

`aaa`

The AAA view is displayed.

Step 9 Run:

`domain domain-name`

The AAA domain view is displayed.

Step 10 Select a command according to the type of packets.

- To configure priority mapping for IP packets, MPLS packets, and multicast packets of a domain, run the **trust upstream** command to enable simple traffic classification in the domain.
- To configure priority mapping for VLAN packets of a domain, run the **trust 8021p** command to enable simple traffic classification in the domain.



The **trust 8021p** command only takes effect on the outbound of the priority mapping.

----End

4.4.8 Checking the Configuration

After configuring precedence mapping based on simple traffic classification, you can view the name of the DiffServ domain, configurations of the traffic policies based on simple traffic classification in the DiffServ domain, and the traffic information on an interface.

Context

Use the following **display** command to check the previous configuration.

Procedure

- Run the **display diffserv domain** [*ds-domain-name*] command to check the DS domain name.

If the configuration succeeds, by running the **display diffserv domain** command, you can see that the traffic policy based on simple traffic classification is correctly configured in the DS domain.
- Run the **display interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check information about traffic on an interface.

----End

4.5 Maintaining Class-based QoS

This section describes how to clear statistics about traffic policies.

4.5.1 Clearing the Statistics About Traffic Policies

The statistics about traffic policies including historical data on Layer 2 and Layer 3 interfaces can be cleared.

Context



CAUTION

Statistics about traffic policies cannot be restored after you clear them. So, confirm the action before you use the **reset** command.

Procedure

Step 1 To clear the statistics about the traffic policy on an interface, run the **reset traffic policy statistics interface interface-type interface-number [. sub-interface] [vlan vlan-id] { inbound | outbound }** command in the user view.

---End

4.6 Configuration Examples

This section provides examples for configuring class-based QoS, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.



NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In actual situations, the actual interface numbers and link types may be different from those used in this document.

User access cannot be configured on the X1 and X2 models of the NE80E/40E.

4.6.1 Example for Configuring a Traffic Policy Based on Complex Traffic Classification

This section provides an example for configuring traffic classifiers and traffic behaviors and applying them in complex traffic classification.

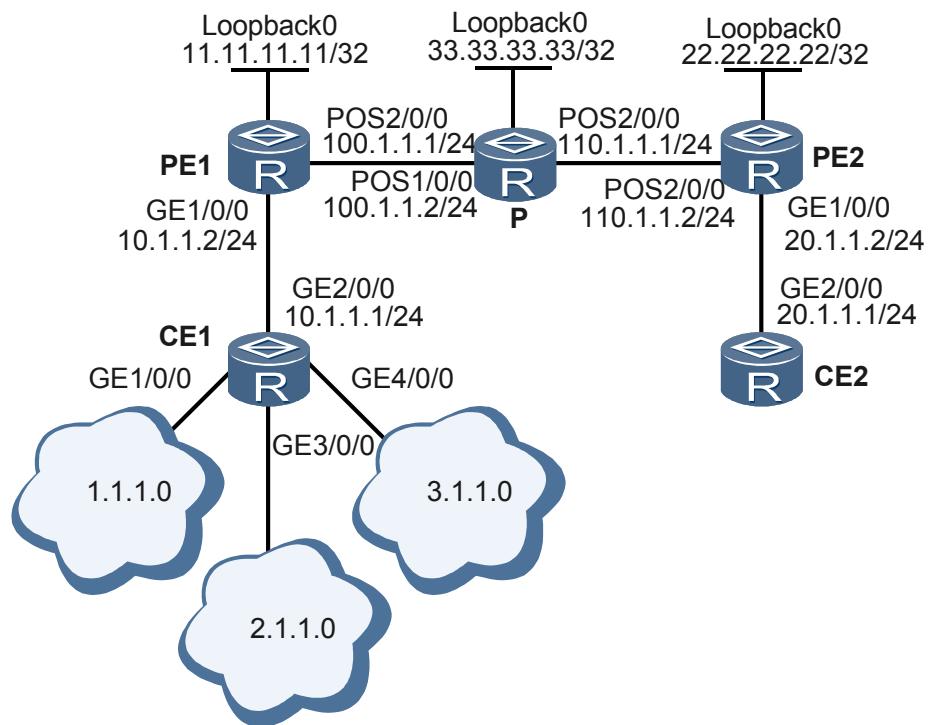
Networking Requirements

As shown in **Figure 4-2**, PE1, P, and PE2 are routers on an MPLS backbone network; CE1 and CE2 are access routers on the edge of the backbone network. Three users from the local network access the Internet through CE1.

- On CE1, the CIR of the users from the network segment 1.1.1.0 is limited to 10 Mbit/s and the CBS is limited to 150000 bytes.
- On CE1, the CIR of the users from the network segment 2.1.1.0 is limited to 5 Mbit/s and the CBS is limited to 100000 bytes.

- On CE1, the CIR of the users from the network segment 3.1.1.0 is limited to 2 Mbit/s and the CBS is limited to 100000 bytes.
- On CE1, the DSCP values of the service packets from the three network segments are marked to 40, 26, and 0.
- PE1 accesses the MPLS backbone network at the CIR of 15 Mbit/s, the CBS of 300000 bytes, the PIR of 20 Mbit/s, and the PBS of 500000 bytes.
- On CE1, the CIR of the UDP packets (except DNS, SNMP, SNMP Trap, and Syslog packets) is limited to 5 Mbit/s, the CBS is limited to 100000 bytes, and the PIR is limited to 15 Mbit/s.

Figure 4-2 Diagram for configuring a traffic policy based on complex traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure ACL rules.
2. Configure traffic classifiers.
3. Configure traffic behaviors.
4. Configure traffic policies.
5. Apply traffic policies to interfaces.

Data Preparation

To complete the configuration, you need the following data:

- ACL numbers 2001, 2002, 2003, 3001, and 3002
- DSCP values of the packets from the three network segments, which are re-marked to be 40, 26, and 0 respectively
- CIRs (10 Mbit/s, 5 Mbit/s, and 2 Mbit/s) and CBSs (150000 bytes, 100000 bytes, and 100000 bytes) of the traffic from the three network segments
- CIR (5 Mbit/s), CBS (100000 bytes), and PIR (15 Mbit/s) of the UDP packets (except DNS, SNMP, SNMP Trap, and Syslog packets) on CE1
- CIR (15 Mbit/s), CBS (300000 bytes), PIR (20 Mbit/s), and PBS (500000 bytes) of traffic on PE1
- Names of traffic classifiers, traffic behaviors, and traffic policies, and numbers of interfaces to which traffic policies are applied

Procedure

Step 1 Configure IP addresses of interfaces, routes, and basic MPLS functions. The detailed configurations are not mentioned.

Step 2 Configure complex traffic classification on CE1 to control the traffic that accesses CE1 from the three local networks.

Define ACL rules.

```
<CE1> system-view
[CE1] acl number 2001
[CE1-acl-basic-2001] rule permit source 1.1.1.0 0.0.0.255
[CE1-acl-basic-2001] quit
[CE1] acl number 2002
[CE1-acl-basic-2002] rule permit source 2.1.1.0 0.0.0.255
[CE1-acl-basic-2002] quit
[CE1] acl number 2003
[CE1-acl-basic-2003] rule permit source 3.1.1.0 0.0.0.255
[CE1-acl-basic-2003] quit
[CE1] acl number 3001
[CE1-acl-basic-3001] rule 0 permit udp destination-port eq dns
[CE1-acl-basic-3001] rule 1 permit udp destination-port eq snmp
[CE1-acl-basic-3001] rule 2 permit udp destination-port eq snmptrap
[CE1-acl-basic-3001] rule 3 permit udp destination-port eq syslog
[CE1-acl-basic-3001] quit
[CE1] acl number 3002
[CE1-acl-basic-3002] rule 4 permit udp
[CE1-acl-basic-3002] quit
```

Configure traffic classifiers and define ACL-based matching rules.

```
[CE1] traffic classifier a
[CE1-classifier-a] if-match acl 2001
[CE1-classifier-a] quit
[CE1] traffic classifier b
[CE1-classifier-b] if-match acl 2002
[CE1-classifier-b] quit
[CE1] traffic classifier c
[CE1-classifier-c] if-match acl 2003
[CE1-classifier-c] quit
[CE1] traffic classifier udplimit
[CE1-classifier-udplimit] if-match acl 3001
[CE1-classifier-udplimit] quit
[CE1] traffic classifier udplimit1
[CE1-classifier-udplimit1] if-match acl 3002
[CE1-classifier-udplimit1] quit
```

After the preceding configuration, you can run the **display traffic classifier** command to view the configuration of the traffic classifiers.

```
[CE1] display traffic classifier user-defined
User Defined Classifier Information:
    Classifier: a
        Operator: OR
        Rule(s): if-match acl 2001
    Classifier: c
        Operator: OR
        Rule(s): if-match acl 2003
    Classifier: b
        Operator: OR
        Rule(s): if-match acl 2002
    Classifier: udplimit
        Operator: OR
        Rule(s) : if-match acl 3001
    Classifier: udplimit1
        Operator: OR
        Rule(s) : if-match acl 3002

# Define traffic behaviors, configure traffic policing, and re-mark DSCP values.

[CE1] traffic behavior e
[CE1-behavior-e] car cir 10000 cbs 150000 pbs 0
[CE1-behavior-e] remark dscp 40
[CE1-behavior-e] quit
[CE1] traffic behavior f
[CE1-behavior-f] car cir 5000 cbs 100000 pbs 0
[CE1-behavior-f] remark dscp 26
[CE1-behavior-f] quit
[CE1] traffic behavior g
[CE1-behavior-g] car cir 2000 cbs 100000 pbs 0
[CE1-behavior-g] remark dscp 0
[CE1-behavior-g] quit
[CE1] traffic behavior udplimit
[CE1-behavior-udplimit] permit
[CE1-behavior-udplimit] quit
[CE1] traffic behavior udplimit1
[CE1-behavior-udplimit1] car cir 5000 cbs 100000 pbs 150000 green pass yellow
discard red discard
[CE1-behavior-udplimit1] quit
```

Define traffic policies and associate the traffic classifiers with the traffic behaviors.

```
[CE1] traffic policy 1
[CE1-trafficpolicy-1] classifier a behavior e
[CE1-trafficpolicy-1] quit
[CE1] traffic policy 2
[CE1-trafficpolicy-2] classifier b behavior f
[CE1-trafficpolicy-2] quit
[CE1] traffic policy 3
[CE1-trafficpolicy-3] classifier c behavior g
[CE1-trafficpolicy-3] quit
[CE1] traffic policy udplimit
[CE1-trafficpolicy-udplimit] classifier udplimit behavior udplimit
[CE1-trafficpolicy-udplimit] classifier udplimit1 behavior udplimit1
[CE1-trafficpolicy-3] quit
```

After the preceding configuration, run the **display traffic policy** command to view the configuration of the traffic policies, traffic classifiers defined in the traffic policies, and the traffic behaviors associated with traffic classifiers.

```
[CE1] display traffic policy user-defined
User Defined Traffic Policy Information:
Policy: 1
    Classifier: default-class
        Behavior: be
        -none-
    Classifier: a
        Behavior: e
        Committed Access Rate:
```

```

CIR 10000 (Kbps), PIR 0 (Kbps), CBS 15000 (byte), PBS 0 (byte)
Conform Action: pass
Yellow Action: pass
Exceed Action: discard
Marking:
    Remark DSCP cs5
Policy: 2
    Classifier: default-class
    Behavior: be
    -none-
Classifier: b
    Behavior: f
    Committed Access Rate:
        CIR 5000 (Kbps), PIR 0 (Kbps), CBS 100000 (byte), PBS 0 (byte)
        Conform Action: pass
        Yellow Action: pass
        Exceed Action: discard
Marking:
    Remark DSCP af31
Policy: 3
    Classifier: default-class
    Behavior: be
    -none-
Classifier: c
    Behavior: g
    Committed Access Rate:
        CIR 2000 (Kbps), PIR 0 (Kbps), CBS 100000 (byte), PBS 0 (byte)
        Conform Action: pass
        Yellow Action: pass
        Exceed Action: discard
Marking:
    Remark DSCP default
Policy: udplimit
    Classifier: default-class
    Behavior: be
    -none-
Classifier: udplimit
    Behavior: udplimit
    Firewall:
        permit
Classifier: udplimit1
    Behavior: udplimit1
    Committed Access Rate:
        CIR 5000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 15000 (byte)
        Conform Action: pass
        Yellow Action: discard
        Exceed Action: discard

```

Apply the traffic policies to the inbound interfaces.

```

[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] undo shutdown
[CE1-GigabitEthernet1/0/0] traffic-policy 1 inbound
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 3/0/0
[CE1-GigabitEthernet3/0/0] undo shutdown
[CE1-GigabitEthernet3/0/0] traffic-policy 2 inbound
[CE1-GigabitEthernet3/0/0] quit
[CE1] interface gigabitethernet 4/0/0
[CE1-GigabitEthernet4/0/0] undo shutdown
[CE1-GigabitEthernet4/0/0] traffic-policy 3 inbound
[CE1] interface gigabitethernet 2/0/0
[CE1-GigabitEthernet2/0/0] undo shutdown
[CE1-GigabitEthernet2/0/0] traffic-policy udplimit outbound

```

Step 3 Configure complex traffic classification on PE1 to control the traffic that goes to the MPLS backbone network.

Configure traffic classifiers and define matching rules.

```
<PE1> system-view
[PE1] traffic classifier pe
[PE1-classifier-pe] if-match any
[PE1-classifier-pe] quit
```

After the preceding configuration, you can run the **display traffic classifier** command to view the configuration of the traffic classifiers.

```
[PE1] display traffic classifier user-defined
User Defined Classifier Information:
  Classifier: pe
  Operator: OR
  Rule(s): if-match any

# Define traffic behaviors and configure traffic policing.

[PE1] traffic behavior pe
[PE1-behavior-pe] car cir 15000 pir 20000 cbs 300000 pbs 500000
[PE1-behavior-pe] quit
```

Define traffic policies and associate the traffic classifiers with the traffic behaviors.

```
[PE1] traffic policy pe
[PE1-trafficpolicy-pe] classifier pe behavior pe
[PE1-trafficpolicy-pe] quit
```

After the preceding configuration, you can run the **display traffic policy** command to view the configuration of the traffic policies, traffic classifiers defined in the traffic policies, and the traffic behaviors associated with the traffic classifiers.

```
[PE1] display traffic policy user-defined
User Defined Traffic Policy Information:
Policy: pe
  Classifier: default-class
  Behavior: be
    -none-
  Classifier: pe
  Behavior: pe
  Committed Access Rate:
  CIR 15000 (Kbps), PIR 20000 (Kbps), CBS 300000 (byte), PBS 500000 (byte)
    Conform Action: pass
    Yellow Action: pass
    Exceed Action: discard
```

Apply the traffic policies to the inbound interfaces.

```
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] undo shutdown
[PE1-GigabitEthernet1/0/0] traffic-policy pe inbound
[PE1-GigabitEthernet1/0/0] quit
```

Step 4 Verify the configuration.

Run the **display interface** command on CE1 and PE1. You can view that the traffic on the interfaces is controlled according to the configured traffic policies.

----End

Configuration Files

- Configuration file of CE1

```
#
sysname CE1
#
acl number 2001
  rule 5 permit source 1.1.1.0 0.0.0.255
acl number 2002
```

```
rule 5 permit source 2.1.1.0 0.0.0.255
acl number 2003
rule 5 permit source 3.1.1.0 0.0.0.255
acl number 3001
rule 0 permit udp destination-port eq dns
rule 1 permit udp destination-port eq snmp
rule 2 permit udp destination-port eq snmptrap
rule 3 permit udp destination-port eq syslog
acl number 3302
rule 4 permit udp
#
traffic classifier a operator or
if-match acl 2001
traffic classifier c operator or
if-match acl 2003
traffic classifier b operator or
if-match acl 2002
traffic classifier udp-limit operator or
if-match acl 3001
traffic classifier udp-limit1 operator or
if-match acl 3002
#
traffic behavior e
car cir 10000 cbs 150000 pbs 0 green pass red discard
remark dscp cs5
traffic behavior g
car cir 2000 cbs 100000 pbs 0 green pass red discard
remark dscp default
traffic behavior f
car cir 5000 cbs 100000 pbs 0 green pass red discard
remark dscp af31
traffic behavior udp-limit
traffic behavior udp-limit1
car cir 5000 cbs 100000 pbs 150000 green pass yellow discard red discard
#
traffic policy 3
classifier c behavior g
traffic policy 2
classifier b behavior f
traffic policy 1
classifier a behavior e
traffic policy udp-limit
classifier udp-limit behavior udp-limit
classifier udp-limit1 behavior udp-limit1
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 1.1.1.1 255.255.255.0
traffic-policy 1 inbound
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
traffic-policy udplimit outbound
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 2.1.1.1 255.255.255.0
traffic-policy 2 inbound
#
interface GigabitEthernet4/0/0
undo shutdown
ip address 3.1.1.1 255.255.255.0
traffic-policy 3 inbound
#
ospf 1
area 0.0.0.0
network 1.1.1.0 0.0.0.255
network 2.1.1.0 0.0.0.255
```

```
    network 3.1.1.0 0.0.0.255
    network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of PE1

```
#           sysname PE1
#
mpls lsr-id 11.11.11.11
mpls
#
mpls ldp
#
traffic classifier pe operator or
if-match any
#
traffic behavior pe
car cir 15000 pir 20000 cbs 300000 pbs 500000 green pass yellow pass red
discard
#
traffic policy pe
classifier pe behavior pe
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
traffic-policy pe inbound
#
interface Pos2/0/0
undo shutdown
ip address 100.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 11.11.11.11 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 100.1.1.0 0.0.0.255
network 11.11.11.11 0.0.0.0
#
return
```

- Configuration file of P

```
#           sysname P
#
mpls lsr-id 33.33.33.33
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
ip address 100.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
ip address 110.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 33.33.33.33 255.255.255.255
#
```

```
ospf 1
area 0.0.0.0
network 100.1.1.0 0.0.0.255
network 110.1.1.0 0.0.0.255
network 33.33.33.33 0.0.0.0
#
return

● Configuration file of PE2
#
sysname PE2
#
mpls lsr-id 22.22.22.22
mpls
#
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 20.1.1.2 255.255.255.0
#
interface Pos2/0/0
undo shutdown
ip address 110.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 22.22.22.22 255.255.255.255
#
ospf 10
area 0.0.0.0
network 110.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
network 22.22.22.22 0.0.0.0
#
return

● Configuration file of CE2
#
sysname CE2
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 20.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 20.1.1.0 0.0.0.255
#
return
```

4.6.2 Example for Configuring Complex Traffic Classification on a Sub-interface for QinQ VLAN Tag Termination

This section provides an example for configuring complex traffic classification on a sub-interface for QinQ VLAN tag termination.

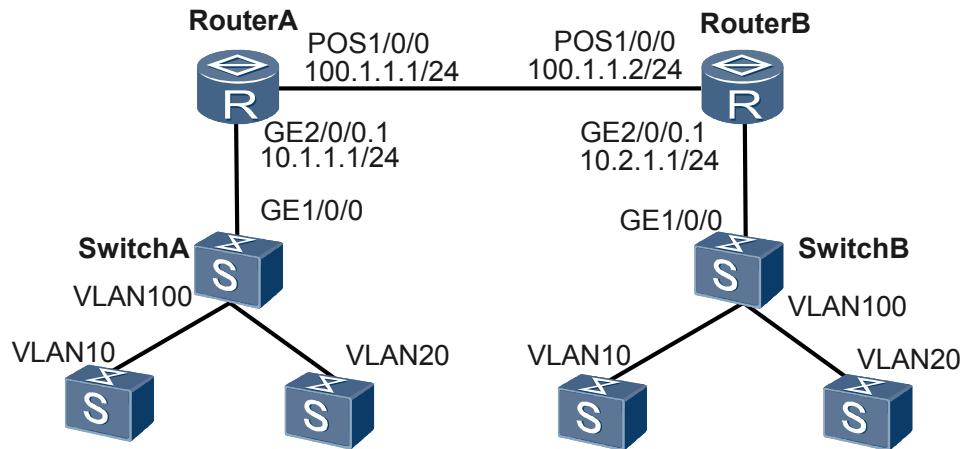
Networking Requirements

As shown in [Figure 4-3](#), Switch A and Switch B are connected to the carrier network through Router A and Router B. On the sub-interface for QinQ VLAN tag termination GE 2/0/0.1 on Router A, complex traffic classification is configured to limit the CIR to 10 Mbit/s and the CBS to 150000 bytes of user traffic on Switch A.

 NOTE

For details about how to configure QinQ interfaces, see "QinQ Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - LAN Access and MAN Access*.

Figure 4-3 Networking diagram for configuring complex traffic classification on a sub-interface for QinQ VLAN tag termination



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure GE2/0/0.1 on Router A and that on Router B to be sub-interfaces for QinQ VLAN tag termination.
2. Configure traffic policing based on complex traffic classification on the sub-interface for VLAN tag termination on Router A.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of interfaces
- Range of VLAN IDs to be terminated on the sub-interfaces for QinQ VLAN tag termination
- CIR (10 Mbit/s) and CBS (150000 bytes) for users attached to Switch A
- Names of traffic classifiers, traffic behaviors, and traffic policies, and numbers of the interfaces to which traffic policies are applied

Procedure

Step 1 Configure an IGP on the backbone network. In this example, OSPF is adopted.

Configure Router A.

```

<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
[RouterA-Pos1/0/0] ip address 100.1.1.1 24

```

```
[RouterA-Pos1/0/0] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

Configure Router B.

```
<HUAWEI> system-view
[HUAWEI] sysname RouterB
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] undo shutdown
[RouterB-Pos1/0/0] ip address 100.1.1.2 24
[RouterB-Pos1/0/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

Step 2 Configure sub-interfaces for QinQ VLAN tag termination.

Configure Router A.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] undo shutdown
[RouterA-GigabitEthernet2/0/0] mode user-termination
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterA-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10 to 20
[RouterA-GigabitEthernet2/0/0.1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterA-GigabitEthernet2/0/0.1] quit
```

Configure Router B.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] undo shutdown
[RouterB-GigabitEthernet2/0/0] mode user-termination
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] control-vid 1 qinq-termination
[RouterB-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10 to 20
[RouterB-GigabitEthernet2/0/0.1] ip address 10.2.1.1 24
[RouterB-GigabitEthernet2/0/0.1] arp broadcast enable
[RouterB-GigabitEthernet2/0/0.1] quit
```

Step 3 Configure complex traffic classification on the sub-interface for QinQ VLAN tag termination on Router A.

Configure a traffic classifier and define a matching rule.

```
[RouterA] traffic classifier cl
[RouterA-classifier-cl] if-match any
[RouterA-classifier-cl] quit
```

Define a traffic behavior.

```
[RouterA] traffic behavior b1
[RouterA-behavior-b1] car cir 10000 cbs 150000 pbs 0
[RouterA-behavior-b1] quit
```

Define a traffic policy and associate the traffic classifier with the traffic behavior.

```
[RouterA] traffic policy p1
[RouterA-trafficpolicy-p1] classifier cl behavior b1
```

```
[RouterA-trafficpolicy-p1] quit

# After the preceding configuration, run the display traffic policy command to view the
# configuration result, including the traffic policy, the traffic classifier defined in the traffic policy,
# and the traffic behavior associated with the traffic classifier.

[RouterA] display traffic policy user-defined
  User Defined Traffic Policy Information:
    Policy: p1
      Classifier: default-class
        Behavior: be
          -none-
    Classifier: c1
      Behavior: b1
      Committed Access Rate:
        CIR 10000 (Kbps), PIR 0 (Kbps), CBS 150000 (byte), PBS 0 (byte)
        Conform Action: pass
        Yellow Action: pass
        Exceed Action: discard

# Apply the traffic policy to the sub-interface.

[RouterA] interface gigabitethernet 2/0/0.1
[RouterA-GigabitEthernet2/0/0.1] traffic-policy p1 inbound
[RouterA-GigabitEthernet2/0/0.1] quit
```

Step 4 Verify the configuration.

After the preceding configuration, GE 2/0/0.1 on Router A only access 10 Mbit/s traffic. Packets that exceed the allowed traffic rate are discarded.

----End

Configuration Files

- Configuration file of Router A

```
# 
  sysname RouterA
#
  traffic classifier c1 operator and
    if-match any
#
  traffic behavior b1
    car cir 10000 cbs 150000 pbs 0 green pass yellow pass red discard
#
  traffic policy p1
    classifier c1 behavior b1
#
  interface GigabitEthernet2/0/0
    undo shutdown
    mode user-termination
#
  interface GigabitEthernet2/0/0.1
    control-vid 1 qinq-termination
      qinq termination pe-vid 100 ce-vid 10 to 20
      ip address 10.1.1.1 255.255.255.0
    traffic-policy p1 inbound
    arp broadcast enable
#
  interface Pos1/0/0
    undo shutdown
    link-protocol ppp
    ip address 100.1.1.1 255.255.255.0
#
  ospf 1
    area 0.0.0.0
      network 10.1.1.0 0.0.0.255
```

```
        network 100.1.1.0 0.0.0.255
#
return
● Configuration file of Router B
#
sysname RouterB
#
interface GigabitEthernet2/0/0
    undo shutdown
    mode user-termination
#
interface GigabitEthernet2/0/0.1
    control-vid 1 qinq-termination
    qinq termination pe-vid 100 ce-vid 10 to 20
    ip address 10.2.1.1 255.255.255.0
    arp broadcast enable
#
interface Pos1/0/0
    undo shutdown
    link-protocol ppp
    ip address 100.1.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
    network 10.2.1.0 0.0.0.255
    network 100.1.1.0 0.0.0.255
#
return
```

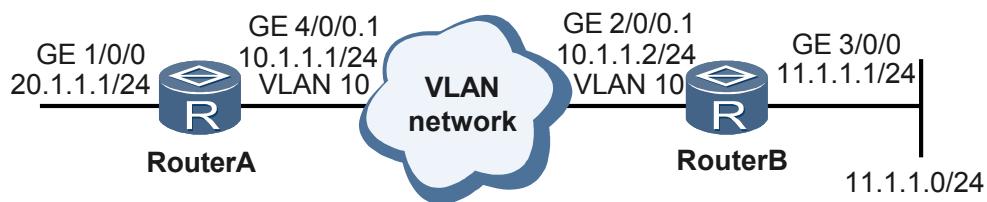
4.6.3 Example for Configuring Preference Mapping Based on Simple Traffic Classification for VLAN Packets

This section provides an example for configuring preference mapping based on simple traffic classification for VLAN packets.

Networking Requirements

As shown in **Figure 4-4**, Router A and Router B are connected to each other through a VLAN. When IP packets sent from Router A go into the VLAN, the DSCP value of the IP packets is mapped to the 802.1p priority of the VLAN packets according to the default mapping. When packets from the VLAN go into Router B, the 802.1p priority is mapped to the DSCP value of the IP packets according to precedence mapping for the DS domain set on Router B.

Figure 4-4 Networking diagram for configuring VLAN QoS



Configuration Roadmap

The configuration roadmap is as follows:

1. Set a VLAN and routes on Router A and Router B.
2. Configure the inbound interface on Router A to trust the precedence of packets from the upstream device.
3. Configure precedence mapping on simple traffic classification on the inbound interface of Router B.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID
- 802.1p priority, internal CoS and color on the router, and the IP DSCP value

Procedure

Step 1 Assign IP addresses for the interfaces. The detailed configuration is not mentioned.

Step 2 Configure a VLAN on Router A and Router B.

Create the sub-interface GE 4/0/0.1 and add it to the VLAN.

```
[RouterA] interface gigabitethernet 4/0/0.1
[RouterA-GigabitEthernet4/0/0.1] vlan-type dot1q 10
[RouterA-GigabitEthernet4/0/0.1] return
```

Create the sub-interface GE 2/0/0.1 and add it to the VLAN.

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0] vlan-type dot1q 10
[RouterB-GigabitEthernet2/0/0] return
```

Step 3 Configure a dynamic routing protocol on Router A and Router B. Take OSPF as an example.

Configure Router A.

```
<RouterA> system-view
[RouterA] ospf 1
[RouterA-ospf-1] area 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] return
```

Configure Router B.

```
<RouterB> system-view
[RouterB] ospf 1
[RouterB-ospf-1] area 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] return
```

Step 4 Enable simple traffic classification on GE 1/0/0 of Router A to map the precedence in IP packets to the 802.1p priority according to the default mapping.

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] trust upstream default
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 4/0/0.1
[RouterA-GigabitEthernet4/0/0.1] trust upstream default
[RouterA-GigabitEthernet4/0/0.1] trust 8021p
[RouterA-GigabitEthernet4/0/0.1] return
```

After the preceding configuration, the DSCP values in the IP packets from the upstream device are mapped to the 802.1p priorities in VLAN packets according to the default mapping on Router A.

- Step 5** On GE 2/0/0.1 of Router B, configure the mapping from the 802.1p priority to the IP DSCP value.

```
<RouterB> system-view
[RouterB] diffserv domain default
[RouterB-dsdomain-default] 8021p-inbound 2 phb ef green
[RouterB-dsdomain-default] ip-dscp-outbound ef green map 34
[RouterB-dsdomain-default] quit
[RouterB] interface gigabitethernet 2/0/0.1
[RouterB-GigabitEthernet2/0/0.1] trust upstream default
[RouterB-GigabitEthernet2/0/0.1] trust 8021p
[RouterB-GigabitEthernet2/0/0.1] return
```

After the preceding configuration, the VLAN packets whose 802.1p priority is 2 from the upstream device are converted to the IP packets whose DSCP value is 34, CoS is AF4, and color is green. The 802.1p priorities in other VLAN packets are mapped to the DSCP values according to the default mapping.

- Step 6** Verify the configuration.

On GE 3/0/0 of Router B, run the **display port-queue statistics interface gigabitethernet 3/0/0 outbound** command. The statistics about AF2 packets are not displayed because the mapping from the 802.1p priority 2 to the service priority EF of IP packets is configured on the inbound interface. The command output is as follows:

```
<RouterB> display port-queue statistics interface gigabitethernet 3/0/0 outbound
GigabitEthernet3/0/0 outbound traffic statistics:
[be]
Current usage percentage of queue: 0
Total pass: 18,466,135 packets, 1,735,817,160 bytes
Total discard: 0 packets, 0 bytes
Drop tail discard: 0 packets, 0 bytes
Wred discard: 0 pps, 0 bps
Last 30 seconds pass rate: 33,599 pps, 3,158,306 bps
Last 30 seconds discard rate: 0 pps, 0 bps
Drop tail discard rate: 0 pps, 0 bps
Wred discard rate: 0 pps, 0 bps
Peak rate: 0000-00-00 00:00:00 0 bps
[af1]
Current usage percentage of queue: 0
Total pass: 670,712 packets, 63,046,928 bytes
Total discard: 0 packets, 0 bytes
Drop tail discard: 0 packets, 0 bytes
Wred discard: 0 pps, 0 bps
Last 30 seconds pass rate: 33,600 pps, 3,158,400 bps
Last 30 seconds discard rate: 0 pps, 0 bps
Drop tail discard rate: 0 pps, 0 bps
```

```

Wred discard rate: 0 pps, 0 bps
Peak rate: 0000-00-00 00:00:00 0 bps
[af2]
Current usage percentage of queue: 0
Total pass: 58 packets, 5,684 bytes
Total discard: 24,478,662 packets, 1,860,378,312 bytes
Drop tail discard: 0 packets, 0 bytes
Wred discard: 0 pps, 0 bps
Last 30 seconds pass rate: 0 pps, 0 bps
Last 30 seconds discard rate: 0 pps, 0 bps
Drop tail discard rate: 0 pps, 0 bps
Wred discard rate: 0 pps, 0 bps
Peak rate: 0000-00-00 00:00:00 0 bps
[af3]
Current usage percentage of queue: 0
Total pass: 58 packets, 5,684 bytes
Total discard: 478,662 packets, 1,860,378,312 bytes
Drop tail discard: 0 packets, 0 bytes
Wred discard: 0 pps, 0 bps
Last 30 seconds pass rate: 33,599 pps, 3,158,306 bps
Last 30 seconds discard rate: 0 pps, 0 bps
Drop tail discard rate: 0 pps, 0 bps
Wred discard rate: 0 pps, 0 bps
Peak rate: 0000-00-00 00:00:00 0 bps
[af4]
Current usage percentage of queue: 0
Total pass: 670,709 packets, 63,046,646 bytes
Total discard: 0 packets, 0 bytes
Drop tail discard: 0 packets, 0 bytes
Wred discard: 0 pps, 0 bps
Last 30 seconds pass rate: 33,598 pps, 3,158,212 bps
Last 30 seconds discard rate: 0 pps, 0 bps
Drop tail discard rate: 0 pps, 0 bps
Wred discard rate: 0 pps, 0 bps
Peak rate: 0000-00-00 00:00:00 0 bps
[ef]
Current usage percentage of queue: 0
Total pass: 670,712 packets, 63,046,928 bytes
Total discard:

```

```

            353,802 packets,
Drop tail discard:                                406,888,952 bytes
            0 packets,
Wred discard:                                     0 bytes
            0 pps,
Last 30 seconds pass rate:                      0 bps
            33,600 pps,
Last 30 seconds discard rate:                   3,158,400 bps
            0 pps,
Drop tail discard rate:                         0 bps
            0 pps,
Wred discard rate:                            0 bps
            0 pps,
Peak rate:                                         0 bps
            0000-00-00 00:00:00

[cs6]
Current usage percentage of queue: 0
    Total pass:                                    12,667 bytes
            147 packets,
    Total discard:                               0 bytes
            0 packets,
    Drop tail discard:                         0 bytes
            0 packets,
    Wred discard:                             0 bytes
            0 pps,
Last 30 seconds pass rate:                      0 bps
            33,599 pps,
Last 30 seconds discard rate:                   3,158,306 bps
            0 pps,
Drop tail discard rate:                         0 bps
            0 pps,
Wred discard rate:                            0 bps
            0 pps,
Peak rate:                                         0 bps
            0000-00-00 00:00:00

[cs7]
Current usage percentage of queue: 0
    Total pass:                                    63,046,458 bytes
            670,708 packets,
    Total discard:                               0 bytes
            0 packets,
    Drop tail discard:                         0 bytes
            0 packets,
    Wred discard:                             0 bytes
            0 pps,
Last 30 seconds pass rate:                      0 bps
            33,599 pps,
Last 30 seconds discard rate:                   3,158,306 bps
            0 pps,
Drop tail discard rate:                         0 bps
            0 pps,
Wred discard rate:                            0 bps
            0 pps,
Peak rate:                                         0 bps
            0000-00-00 00:00:00

```

----End

Configuration Files

- Configuration file of Router A.

```

#
sysname RouterA
#
vlan batch 10
#
interface GigabitEthernet 1/0/0
undo shutdown

```

```
ip address 20.1.1.1 255.255.255.0
trust upstream default
#
interface GigabitEthernet 4/0/0.1
ip address 10.1.1.1 255.255.255.0
vlan-type dot1q 10
trust upstream default
trust 802.1p
#
ospf 1
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
vlan batch 10
#
diffserv domain default
8021p-inbound 2 phb ef green
ip-dscp-outbound ef green map 34
#
interface GigabitEthernet 2/0/0.1
ip address 10.1.1.2 255.255.255.0
vlan-type dot1q 10
trust upstream default
trust 802.1p
#
interface GigabitEthernet 3/0/0
undo shutdown
ip address 11.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 11.1.1.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return
```

4.6.4 Example for Configuring Precedence Mapping Based on Simple Traffic Classification for MPLS Packets

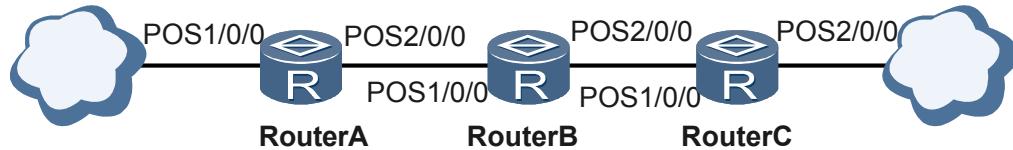
This section provides an example for configuring precedence mapping based on simple traffic classification for MPLS packets.

Networking Requirements

As shown in [Figure 4-5](#), Router A, Router B, and Router C establish MPLS neighbor relationships. When IP packets reach Router A, Router A adds MPLS headers to the packets to form MPLS packets. The MPLS packets are then transmitted from Router A to Router C. When the MPLS packets reach Router C, Router C removes the MPLS headers and the packets are sent out from Router C as IP packets.

It is required that Router A be able to change the priority of MPLS packets and Router C be able to change the priority of IP packets at any time.

Figure 4-5 Mapping from the DSCP value to MPLS EXP value



NOTE

- Assume that the three routers in this example have been configured to forward IP packets as MPLS packets from Router A to Router C, which are sent as IP packets when they flow out of Router C.
- This example lists only the commands related to QoS.

Configuration Roadmap

The configuration roadmap is as follows:

1. On the inbound interface POS 1/0/0 of Router A, set the mapping from the IP DSCP field to the MPLS EXP field and enable simple traffic classification.
2. On the inbound interface POS 1/0/0 of Router C, set the mapping from the MPLS EXP field to the IP DSCP field and enable simple traffic classification.

Data Preparation

To complete the configuration, you need the following data:

MPLS EXP value, internal CoS and color on the router, and IP DSCP value

Procedure

- Step 1** Configure basic MPLS functions and routes. The detailed configuration is not mentioned.

For details, see the chapter "Basic MPLS Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - MPLS*.

- Step 2** Set the mapping between the DSCP value and EXP value on POS 1/0/0 of Router A.

```
<RouterA> system-view
[RouterA] diffserv domain default
[RouterA-dsdomain-default] ip-dscp-inbound 18 phb af4 green
[RouterA-dsdomain-default] mpls-exp-outbound af4 green map 5
[RouterA-dsdomain-default] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] undo shutdown
[RouterA-Pos1/0/0] trust upstream default
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] undo shutdown
[RouterA-Pos2/0/0] trust upstream default
[RouterA-Pos2/0/0] quit
```

After the preceding configuration, the AF2 green service (DSCP value 18) is converted into the AF4 service on the inbound interface of Router A. On the outbound interface, the AF4 service is converted into the EF service of the MPLS service (MPLS EXP value 5).

- Step 3** Set the mapping from the MPLS EXP value to the DSCP value on POS1/0/0 on Router C.

```
<RouterC> system-view
[RouterC] diffserv domain default
```

```
[RouterC-dsdomain-default] mpls-exp-inbound 5 phb af3 green
[RouterC-dsdomain-default] ip-dscp-outbound af3 green map 32
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] undo shutdown
[RouterC-Pos1/0/0] trust upstream default
[RouterC] interface pos 2/0/0
[RouterC-Pos2/0/0] undo shutdown
[RouterC-Pos2/0/0] trust upstream default
[RouterC-Pos2/0/0] quit
```

Configure the mapping from the MPLS EXP value 5 to AF3 green service on the inbound interface of Router C and configure on the outbound interface the conversion from AF3 green service to the DSCP value 32. The traffic going out of Router C is of AF4.

Step 4 Verify the configuration.

After the preceding configuration, when POS 1/0/0 on Router A sends packets at 100 Mbit/s with the DSCP value of 18, Router C outputs packets with the DSCP value of 32 at 100 Mbit/s.

----End

Configuration Files

- Configuration file of Router A

```
#           sysname RouterA
#
diffserv domain default
    ip-dscp-inbound 18 phb af4 green
    mpls-exp-outbound af4 green map 5
#
interface Pos1/0/0
    undo shutdown
    ip address 2.2.2.1 255.255.255.0
    trust upstream default
#
interface Pos2/0/0
    undo shutdown
    ip address 3.3.3.1 255.255.255.0
    trust upstream default
#
return
```

- Configuration file of Router C

```
#           sysname RouterC
#
diffserv domain default
    ip-dscp-outbound af3 green map 32
    mpls-exp-inbound 5 phb af3 green
#
interface Pos1/0/0
    undo shutdown
    ip address 4.4.4.1 255.255.255.0
    trust upstream default
#
interface Pos2/0/0
    undo shutdown
    ip address 5.5.5.1 255.255.255.0
    trust upstream default
#
return
```

5 QPPB Configuration

About This Chapter

This chapter describes the basic principle and configuration procedures of QPPB, and provides configuration examples for QPPB.

[5.1 QPPB Overview](#)

QPPB enables a BGP route sender to classify routes by setting BGP attributes.

[5.2 QPPB Supported by the NE80E/40E](#)

QPPB configuration on the NE80E/40E involves destination-based QPPB and source-based QPPB.

[5.3 Configuring Source-Based QPPB](#)

Source-based QPPB differentiates routes from different sources and associates differentiated QoS policies with them.

[5.4 Configuring Destination-Based QPPB](#)

Destination-based QPPB differentiates the routes to different destinations and associates differentiated QoS policies with them.

[5.5 Maintaining QPPB](#)

This section describes how to clear statistics about a QPPB local policy.

[5.6 Configuration Examples](#)

This section provides examples for configuring QPPB, including the application scenario and configuration commands.

5.1 QPPB Overview

QPPB enables a BGP route sender to classify routes by setting BGP attributes.

On a large and complex network, a large number of complex traffic classification operations are required, and routes cannot be classified based on the community attribute, ACL, IP prefix, or AS_Path. When a network topology keeps changing, configuring or changing routing policies is difficult or even impossible to implement. Therefore, the QoS Policy Propagation Through the Border Gateway Protocol (QPPB) is introduced to reduce configuration workload by configuring or changing routing policies only on a BGP route sender.

After QPPB is deployed, a BGP route sender can classify routes and set attributes for BGP routes; a BGP route receiver accordingly applies different QoS policies to different types of BGP routes based on the set attributes.

QPPB is implemented as follows:

- Before sending BGP routes, a route sender sets a specific attribute, such as the AS_Path, community attribute, or extended community attribute, for BGP routes. These attributes are used to identify BGP routes.
 - After receiving the BGP routes, a route receiver performs the following operations:
 1. Maps each received BGP route to a QoS local ID, an IP preference and traffic behavior based on the AS_Path, community attribute, or extended community attribute.
 2. Performs different traffic behaviors for packets transmitted along the routes according to their mapped QoS local IDs, IP preference and traffic behavior.A route receiver can define traffic behaviors for the packets transmitted along the routes based on the following attributes:
 - ACL
 - AS-Path list
 - Community attribute list
 - Route cost
 - IP prefix list
3. Creates a QPPB local policy and define the mappings between BGP routes and QoS policies in it.
 4. Apply the QPPB local policy to all packets that meet the matching rules on interfaces.

5.2 QPPB Supported by the NE80E/40E

QPPB configuration on the NE80E/40E involves destination-based QPPB and source-based QPPB.

QPPB allows you to classify routes and set attributes for the classified routes on a route sender and configure QoS policies based on the route attributes on a route receiver. You can flexibly deploy destination-based or source-based QPPB.

Source-Based QPPB Local Policies

Traffic behaviors defined in a source-based QPPB local policy are applied to traffic transmitted along the route whose source address meets the matching rule. A source-based QPPB local policy

is applicable to the scenario where different traffic policies are required for traffic sent from different provider networks. You can view the statistics about the traffic that meets the matching rule. The keyword **source** indicates that traffic policies are applied to traffic along the route whose source address meets the matching rule; the keyword **destination** indicates that traffic policies are applied to traffic along the route whose destination address meets the matching rule.

Destination-Based QPPB Local Policies

Traffic behaviors defined in a destination-based QPPB local policy are applied to traffic transmitted along the route whose destination address meets the matching rule. A destination-based QPPB local policy is applicable to the scenario where different traffic policies are required for traffic sent to different providers. You can view the statistics about the traffic that meets the matching rule.

QPPB Applications

- QPPB application on an IPv4 network

Figure 5-1 QPPB application on an IPv4 network



As shown in **Figure 5-1**, Router B advertises a BGP route with community attribute 100:1 to Router A. After receiving this route, Router A performs the following operations:

1. Matches routes with community attribute 100:1 defined in the routing policy, sets QoS local ID 1 for the matched BGP route, and delivers QoS local ID 1 to the FIB table.
2. Configures a QoS policy and applies QoS behaviors to the traffic along the route that matches QoS local ID 1.
3. Creates a QPPB local policy and defines the mappings between BGP routes and QoS policies in it.
4. Applies the QPPB local policy to the inbound interface.

Router A checks the destination IP address of the packet destined for Router B and obtains mapped QoS local ID 1 from the FIB table. Then, Router A applies the QoS policy to the packet on the inbound interface and processes the packet by using relevant QoS behaviors.

- QPPB application on an L3VPN

Figure 5-2 QPPB application on an L3VPN

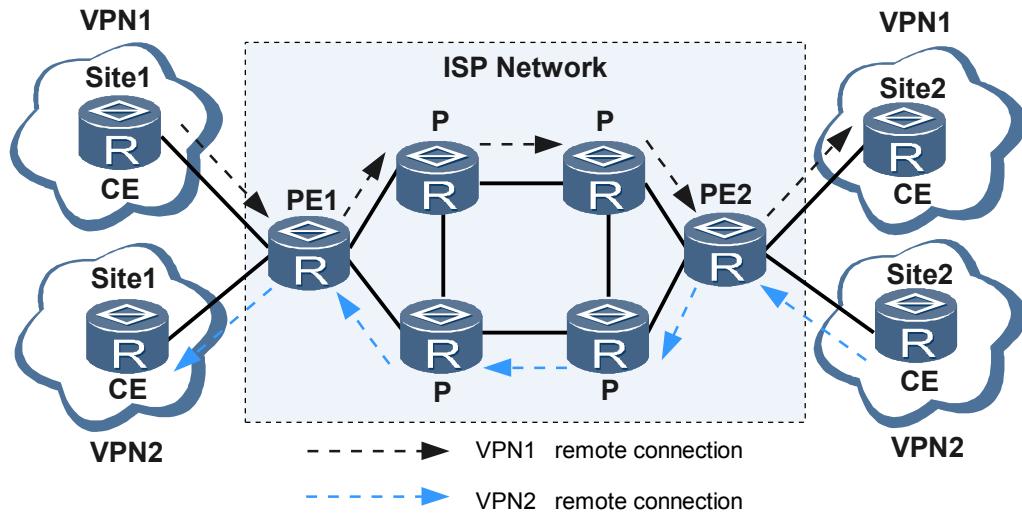


Figure 5-2 shows the QPPB application on an L3VPN. PE1 connects to multiple VPNs. PE1 can set route attributes, such as community attribute, for a specified VPN instance or all VPN instances on itself before advertising any route. After receiving routes, PE2 defines the mappings between routes and QoS parameters in the FIB table so that corresponding QoS policies can be applied to the traffic from CEs. In this manner, different VPNs are guaranteed with different qualities of services.

1. When advertising routes to PE2, PE1 sets community attribute 100:1 for the routes of VPN1.
2. After receiving the advertised routes, PE2 matches the routes with community attribute 100:1 defined in the routing policy, sets QoS local ID 1 for the matched BGP routes, and delivers QoS local ID 1 to the FIB table.
3. QoS policies are configured on the PE2 interfaces connected to CEs to perform the CAR action on the traffic when QoS local ID 1 is matched.
4. A QPPB local policy is created on PE2 and the mappings between BGP routes and QoS policies are defined in it.
5. QPPB is enabled on the PE2 interfaces connected to CEs.

When receiving a packet from CE4, PE3 checks the destination IP address of the packet and obtains mapped QoS local ID 1 from the FIB table. Then, PE3 applies the QoS policy to the packet on the inbound interface and processes the packet by using relevant QoS behaviors.

5.3 Configuring Source-Based QPPB

Source-based QPPB differentiates routes from different sources and associates differentiated QoS policies with them.

Applicable Environment

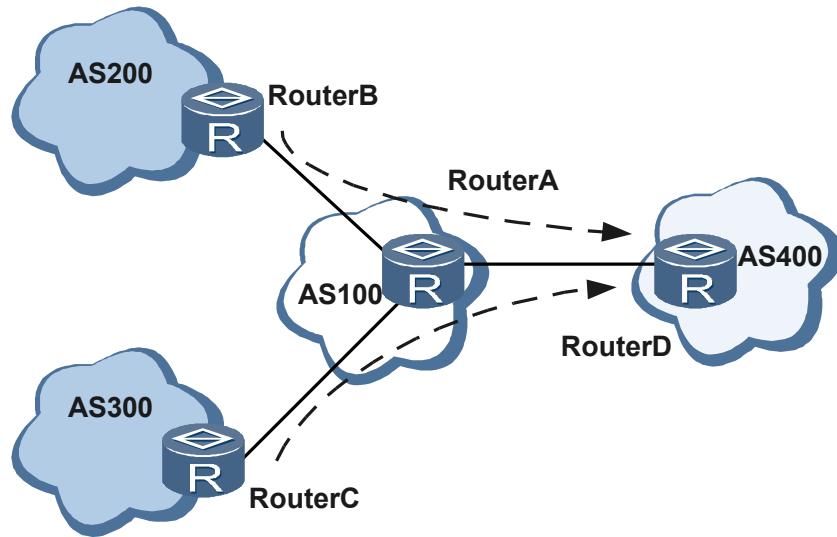
QPPB is applicable to both IBGP and EBGP and can be configured for one or more ASs.

As shown in **Figure 5-3**, traffic is transmitted from Router B (AS 200) and Router C (AS 300) to Router D (AS 400) through Router A (AS 100). Routers B and C function as BGP route senders and Router A functions as a BGP route receiver. Based on the traffic control policies signed between providers A, B, and C, Router A needs to implement the CAR action on the traffic sent from Routers B and C.

Routers B and C advertise BGP routes carrying the community attribute to Router A. After receiving the BGP routes, Router A matches the routes with the community list, ACL list, or AS_Path list, and configures QoS policy IDs and QoS behaviors for the routes. Source-based QPPB is enabled on the Router A interface that allows traffic to pass through. Therefore, QPPB local policies are applied to all traffic that passes through Router A.

Source-based QPPB is applicable to both incoming and outgoing traffic on a device.

Figure 5-3 Networking diagram for source-based QPPB configuration



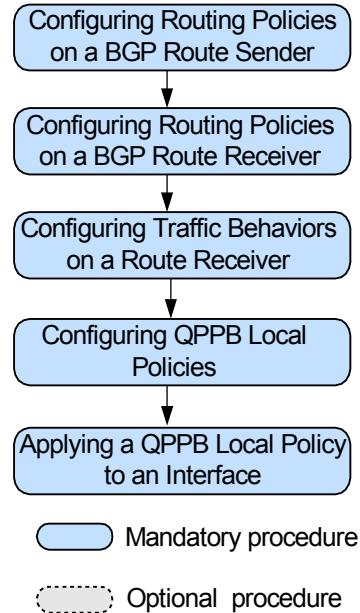
Pre-configuration Tasks

Before configuring source-based QPPB, complete the following tasks:

- Configuring basic BGP functions
- Configuring local network routes advertised by BGP
- Configuring interfaces for setting up a BGP connection

Configuration Procedures

Figure 5-4 Flowchart for QPPB configuration



5.3.1 Configuring Routing Policies on a BGP Route Sender

This section describes how to configure routing policies on a BGP route sender.

Context

Do as follows on a BGP route sender:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
route-policy route-policy-name { permit | deny } node node-number
```

The node of a routing policy is created, and the view of the routing policy is displayed.

Step 3 Run one of the following commands as required to configure a matching rule for the routing policy.

- To match an ACL, run the **if-match acl { acl-number | name acl-name }** command.



Only rules of ACLs 2000 to 2999 can be configured as matching rules in the routing policy.

- To match an AS_Path list, run the **if-match as-path-filter as-path-filter &<1-16>** command.

- To match the community attribute list, run the **if-match community-filter** { *basic-comm-filter-num* [**whole-match**] | *adv-comm-filter-num* } * &<1-16> or **if-match community-filter** *comm-filter-name* [**whole-match**] command.
- To match a route cost, run the **if-match cost** *cost* command.
- To match an IP prefix list, run the **if-match ip-prefix** *ip-prefix* command.

Step 4 Run one of the following commands as required to set route attributes.

- To set an AS_Path attribute, run the **apply as-path** *as-number* &<1-10> [**additive**] command.
- To set a community attribute, run the **apply community** { [*community-number* | *aa:nn*] &<1-32> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**] command.
- To set a route cost, run the **apply cost** { [*apply-type*] *cost* | **inherit** } command.

You can set one BGP attribute, such as the AS_Path, community attribute, or extended community attribute, for the matched BGP routes as required.

Step 5 Run:

quit

The system view is displayed.

Step 6 Run:

bgp *as-number*

The BGP view is displayed.

Step 7 Run:

peer { *ip-address* | *group-name* } **route-policy** *route-policy-name* **export**

The routing policy is applied to the routes that are to be advertised to the peer.



Ensure that BGP peer relationships have been set up before the routing policy is applied.

Step 8 Run:

peer *ip-address* **advertise-community**

The community attribute is advertised to the peer.

By default, the community attribute is not advertised to any peer. To allow the peer to configure QoS policies for the routes with the community attribute, advertise the community attribute to the peer.

----End

5.3.2 Configuring Routing Policies on a BGP Route Receiver

This section describes how to configure routing policies on a BGP route receiver.

Context

Do as follows on a BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
route-policy route-policy-name { permit | deny } node node-number
```

The node of a routing policy is created, and the view of the routing policy is displayed.

Step 3 Run one of the following commands as needed to configure a filtering rule for the routing policy on the BGP route receiver.

- To match an AS_Path list, run the **if-match as-path-filter** *as-path-acl-number &<1-16>* command.
- To match a community attribute list, run the **if-match community-filter** { *basic-comm-filter-num* [**whole-match**] | *ext-comm-filter-num* } &<1-16> command.
- To match a route cost, run the **if-match cost** *value* command.



NOTE

The route attribute configured for a BGP route must be the same as that of the route advertised by a BGP route sender.

Step 4 Perform the following steps as required:

When an LPUF-10, LPUI-41, LPUS-41, LPUI-100, LPUF-100 is used:

- Run the **apply qos-local-id** *qos-local-id* command to apply a QoS policy to the route that meets the matching rule in the routing policy.

When an LPUF-10 is used:

- Run the **apply behavior** *behavior-name* command to apply traffic behavior to the route that meets the matching rule in the routing policy.

A routing policy consists of multiple nodes. Each node comprises multiple **if-match** and **apply** clauses. The **if-match** clauses define matching rules of a node. The **apply** clauses define QoS behaviors to be performed on the routes that match the matching rule.

You can configure multiple **if-match** clauses for a node. The relationship between these rules is "AND". This means that a route passes the filtering only when it meets all the matching rules.

The relationship between routing policy nodes is "OR". That is, if a route matches a node of a routing policy, it matches the routing policy. If none of the routing policy nodes is matched, the route does not match the routing policy.

Step 5 Run:

```
quit
```

Return to the system view.

Step 6 Run:

```
bgp as-number
```

BGP is enabled and the BGP view is displayed.

Step 7 Run:

```
peer ip-address route-policy route-policy-name import
```

The routing policy is applied to the routes sent from the peer (route sender).

 **NOTE**

Ensure that BGP peer relationships have been set up before the routing policy is applied.

----End

5.3.3 Configuring Traffic Behaviors on a Route Receiver

You can configure different traffic behaviors for different traffic classifiers on a BGP receiver to implement differentiated services.

Context

Do as follows on the BGP route receiver:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`traffic behavior behavior-name`

A traffic behavior is configured and the traffic behavior view is displayed.

Step 3 Run one of the following commands as needed:

- To configure CAR actions, run the `car { cir cir-value [pir pir-value] } [cbs cbs-value pbs pbs-value] [green { discard | pass [service-class class color color] } | yellow { discard | pass [service-class class color color] } | red { discard | pass [service-class class color color] }]* [summary]` command.
- To re-mark the DSCP value of an IP packet, run the `remark dscp dscp-value` command.
- To reconfigure the IP preference of an IP packet, run the `remark ip-precedence ip-precedence` command.
- To allow all the packets that meet the matching rule to pass, run the `permit` command.
- To prevent all the packets that meet the matching rule from passing, run the `deny` command.

 **NOTE**

The device supports only five traffic behaviors: `permit`, `deny`, CAR, `remark dscp`, and `remark ip-precedence`.

----End

5.3.4 Configuring QPPB Local Policies on a BGP Route Receiver

QPPB allows QoS policies to be configured for routes that match the BGP community list, ACL, or BGP AS_Path list. After the QPPB local policy is applied to the inbound and outbound interfaces of traffic, relevant QoS policies are performed on the traffic.

Context

Do as follows on a BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
qppb local-policy policy-name
```

A QPPB local policy is created and the QPPB local policy view is displayed.

Step 3 Run:

```
qos-local-id qos-local-id behavior behavior-name
```

A QoS local policy ID is bound to a traffic behavior.

This step is needed only when an LPUF-10, LPUI-41, LPUS-41, LPUI-100 or LPUF-100 is used.



The device supports a maximum of 31 QPPB local policies. The maximum value of *qos-local-id* is 31.

----End

5.3.5 Applying a QPPB Local Policy to an Interface

After a QPPB local policy is applied to an interface, the associated traffic behavior is performed for the packets that meet the matching rule.

Context

You can apply a QPPB local policy to the incoming or outgoing traffic.

BGP routes in QPPB refer to only BGP routes on the public network. Private routes are involved in the QPPB application on the L3VPN.

Do as follows on a BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run one of the following commands as needed:

When an LPUI-41, LPUS-41, LPUI-100, LPUF-100 is used:

- To apply a QPPB local policy to the incoming traffic, run the **qppb-policy policy-name source inbound** command to apply a QPPB policy to an inbound interface.

- To apply a QPPB local policy to the outgoing traffic, run the **qppb-policy qos-local-id source inbound** and **qppb-policy policy-name outbound** commands to apply a QPPB policy to an inbound interface and an outbound interface.

When an LPUF-10 is used:

- To apply a QPPB local policy to the traffic behavior, run the **qppb-policy behavior source** command to apply a QPPB policy to the incoming traffic on an interface.

 **NOTE**

The keyword **source** indicates that policies are applied to traffic along the route whose source address meets the matching rule.

----End

5.3.6 Checking the Configuration

After QPPB is configured, you can view QPPB information.

Context

You can run the **display** commands in any view to check QPPB running information. For details about QPPB running information, see the chapter "QoS Commands" in the *HUAWEI NetEngine80E/40E Router Command Reference*.

Procedure

- Step 1** Run the **display qppb local-policy statistics interface interface-type interface-number [qos-local-id qos-local-id] { inbound | outbound }** command to check the statistics about a specific QPPB local policy.

----End

Example

After QPPB is configured successfully:

- Run the **display qppb local-policy statistics** command, you can view statistics about a specific QPPB local policy. For example:

```
<HUAWEI> display qppb local-policy statistics interface gigabitethernet 2/0/0
inbound
Interface: GigabitEthernet2/0/0
qppb local-policy inbound: policy1
qos-local-id 1
Item                                Packets          Bytes
-----                                -----
Matched                             0                 0

Current CAR statistics:
Item                                Packets          Bytes
-----                                -----
Green                               0                 0
Yellow                              0                 0
Red                                 0                 0
Passed                             0                 0
Dropped                            0                 0
```

5.4 Configuring Destination-Based QPPB

Destination-based QPPB differentiates the routes to different destinations and associates differentiated QoS policies with them.

Applicable Environment

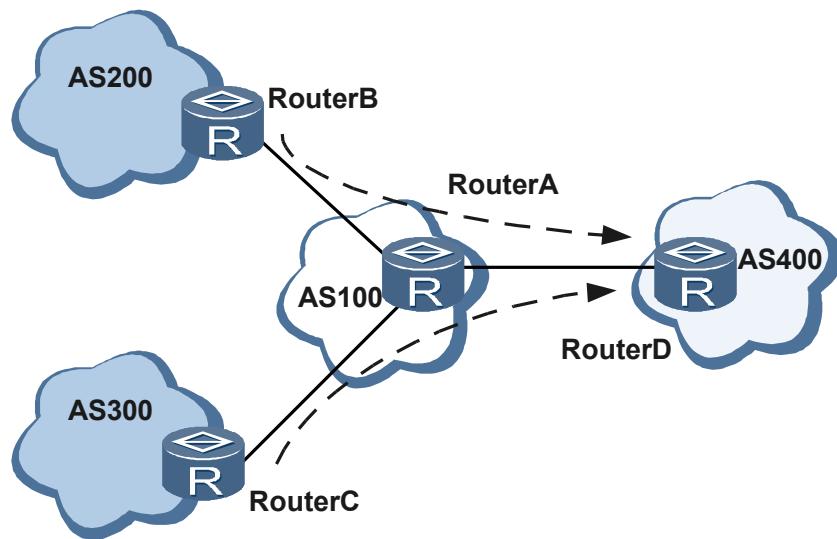
QPPB is applicable to both IBGP and EBGP and can be configured for one or more ASs.

As shown in **Figure 5-5**, traffic is transmitted from Router B (AS 200) and Router C (AS 300) to Router D (AS 400) through Router A (AS 100). Routers B and C function as BGP route senders and Router A functions as a BGP route receiver. Based on the traffic control policies that are signed between providers A and D, Router A needs to limit the rate of the traffic sent to Router D.

Routers B and C advertise BGP routes carrying the community attribute to Router A. After receiving the BGP routes, Router A matches the routes with the community list, ACL list, or AS_Path list, and associates QoS policy IDs with QoS behaviors for the routes. Destination-based QPPB is enabled on the Router A interface that allows traffic to pass through. Therefore, QPPB local policies are applied to all traffic that passes through Router A.

Destination-based QPPB is applicable to both incoming and outgoing traffic on a device.

Figure 5-5 Networking diagram for destination-based QPPB configuration



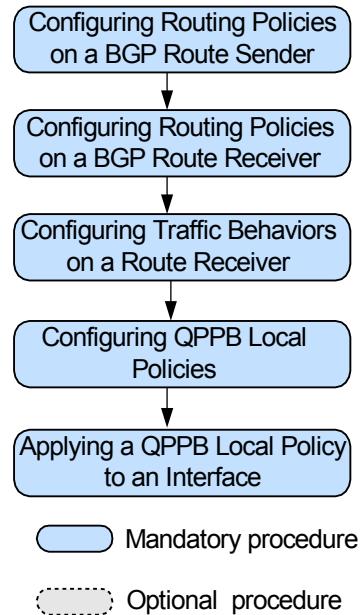
Pre-configuration Tasks

Before configuring QPPB, complete the following tasks:

- Configuring basic BGP functions
- Configuring local network routes advertised by BGP
- Configuring interfaces for setting up a BGP connection

Configuration Procedures

Figure 5-6 Flowchart for QPPB configuration



5.4.1 Configuring Routing Policies on a BGP Route Sender

This section describes how to configure routing policies on a BGP route sender.

Context

Do as follows on a BGP route sender:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
route-policy route-policy-name { permit | deny } node node-number
```

The node of a routing policy is created, and the view of the routing policy is displayed.

Step 3 Run one of the following commands as required to configure a matching rule for the routing policy.

- To match an ACL, run the **if-match acl { acl-number | name acl-name }** command.



Only rules of ACLs 2000 to 2999 can be configured as matching rules in the routing policy.

- To match an AS_Path list, run the **if-match as-path-filter as-path-filter &<1-16>** command.

- To match the community attribute list, run the **if-match community-filter** { *basic-comm-filter-num* [**whole-match**] | *adv-comm-filter-num* } * &<1-16> or **if-match community-filter** *comm-filter-name* [**whole-match**] command.
- To match a route cost, run the **if-match cost** *cost* command.
- To match an IP prefix list, run the **if-match ip-prefix** *ip-prefix* command.

Step 4 Run one of the following commands as required to set route attributes.

- To set an AS_Path attribute, run the **apply as-path** *as-number* &<1-10> [**additive**] command.
- To set a community attribute, run the **apply community** { [*community-number* | *aa:nn*] &<1-32> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**] command.
- To set a route cost, run the **apply cost** { [*apply-type*] *cost* | **inherit** } command.

You can set one BGP attribute, such as the AS_Path, community attribute, or extended community attribute, for the matched BGP routes as required.

Step 5 Run:

quit

The system view is displayed.

Step 6 Run:

bgp *as-number*

The BGP view is displayed.

Step 7 Run:

peer { *ip-address* | *group-name* } **route-policy** *route-policy-name* **export**

The routing policy is applied to the routes that are to be advertised to the peer.



Ensure that BGP peer relationships have been set up before the routing policy is applied.

Step 8 Run:

peer *ip-address* **advertise-community**

The community attribute is advertised to the peer.

By default, the community attribute is not advertised to any peer. To allow the peer to configure QoS policies for the routes with the community attribute, advertise the community attribute to the peer.

----End

5.4.2 Configuring Routing Policies on a BGP Route Receiver

This section describes how to configure routing policies on a BGP route receiver.

Context

Do as follows on a BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
route-policy route-policy-name { permit | deny } node node-number
```

The node of a routing policy is created, and the view of the routing policy is displayed.

Step 3 Run one of the following commands as needed to configure a matching rule for the routing policy on a BGP route receiver.

- To match an AS_Path list, run the **if-match as-path-filter** *as-path-acl-number &<1-16>* command.
- To match a community attribute list, run the **if-match community-filter** { *basic-comm-filter-num* [**whole-match**] | *ext-comm-filter-num* } &<1-16> command.
- To match a route cost, run the **if-match cost** *value* command.

 **NOTE**

The route attribute configured for a BGP route must be the same as that of the route advertised by the BGP route sender.

Step 4 Perform the following steps as required:

When an LPUF-10, LPUI-41, LPUS-41, LPUI-100, LPUF-100 is used:

- Run the **apply qos-local-id** *qos-local-id* command to apply a QoS policy to the route that meets the matching rule in the routing policy.

When an LPUF-21, LPUF-40 is used:

- Run the **apply ip-precedence** *ip-precedence* command to apply IP preference to the route that meets the matching rule in the routing policy.

When an LPUF-10 is used:

- Run the **apply behavior** *behavior-name* command to apply traffic behavior to the route that meets the matching rule in the routing policy.

 **NOTE**

You need to configure IP preference for the route that meets the matching rule in advance.

A routing policy consists of multiple nodes. Each node comprises multiple **if-match** and **apply** clauses. The **if-match** clauses define matching rules of a node. The **apply** clauses define QoS behaviors that are to be implemented for the routes that match the matching rule.

You can configure multiple **if-match** clauses on a node. The relationship between these rules is "AND". This means that a route passes the filtering only when it meets all the matching rules.

The relationship between routing policy nodes is "OR". That is, if a route matches a node of a routing policy, it matches the routing policy. If none of the routing policy nodes is matched, the route does not match the routing policy.

Step 5 Run:

```
bgp as-number
```

BGP is enabled and the BGP view is displayed.

Step 6 Run:

```
peer ip-address route-policy route-policy-name import
```

The routing policy configured on the route receiver is applied to the routes sent from the peer (route sender).



Ensure that BGP peer relationships have been set up before the routing policy is applied.

Step 7 Run:

```
commit
```

The configuration is committed.

----End

5.4.3 Configuring Traffic Behaviors on a Route Receiver

You can configure different traffic behaviors for different traffic classifiers on a BGP receiver to implement differentiated services.

Context

Do as follows on the BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

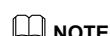
Step 2 Run:

```
traffic behavior behavior-name
```

A traffic behavior is configured and the traffic behavior view is displayed.

Step 3 Run one of the following commands as needed:

- To configure CAR actions, run the `car { cir cir-value [pir pir-value] } [cbs cbs-value pbs pbs-value] [green { discard | pass [service-class class color color] } | yellow { discard | pass [service-class class color color] } | red { discard | pass [service-class class color color] }]* [summary]` command.
- To re-mark the DSCP value of an IP packet, run the `remark dscp dscp-value` command.
- To reconfigure the IP preference of an IP packet, run the `remark ip-precedence ip-precedence` command.
- To allow all the packets that meet the matching rule to pass, run the `permit` command.
- To prevent all the packets that meet the matching rule from passing, run the `deny` command.



The device supports only five traffic behaviors: `permit`, `deny`, CAR, `remark dscp`, and `remark ip-precedence`.

----End

5.4.4 Configuring QPPB Local Policies on a BGP Route Receiver

QPPB allows QoS policies to be configured for routes that match the BGP community list, ACL, or BGP AS_Path list. After the QPPB local policy is applied to the inbound and outbound interfaces of traffic, relevant QoS policies are implemented on the traffic.

Context

Do as follows on a BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
qppb local-policy policy-name
```

A QPPB local policy is created and the QPPB local policy view is displayed.

Step 3 Run:

```
qos-local-id qos-local-id behavior behavior-name
```

A QoS policy is created and a traffic behavior is bound to the QoS local policy ID.

This step is needed only when an LPUF-10, LPUI-41, LPUS-41, LPUI-100 or LPUF-100 is used.



The device supports a maximum of 31 QPPB local policies. The maximum value of **qos-local-id** is 31.

----End

5.4.5 Applying a QPPB Local Policy to an Interface

After a QPPB local policy is applied to an interface, the associated traffic behavior is performed for the packets that meet the matching rule.

Context

You can apply a QPPB local policy to the incoming or outgoing traffic.

BGP routes in QPPB refer to only BGP routes on the public network. Private routes are involved in the QPPB application on the L3VPN.

Do as follows on a BGP route receiver:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run one of the following commands as needed to apply a QPPB local policy:

When an LPUI-41, LPUS-41, LPUI-100, LPUF-100 is used:

- To apply a QPPB local policy to the incoming traffic, run the **qppb-policy policy-name destination inbound** command.
- To apply a QPPB local policy to the outgoing traffic, run the **qppb-policy qos-local-id destination inbound** and **qppb-policy policy-name outbound** commands.

 **NOTE**

The keyword **destination** indicates that policies are applied to traffic along the route whose destination address meets the matching rule.

When an LPUF-21 or LPUF-40 is used:

To apply a QPPB local policy to the ip precedence, run the **qppb-policy ip-precedence destination** command.

When an LPUF-10 is used:

To apply a QPPB local policy to the traffic behavior, run the **qppb-policy behavior destination** command.

----End

5.4.6 Checking the Configuration

After QPPB is configured, you can view QPPB information.

Context

You can run the **display** commands in any view to check QPPB running information. For details about QPPB running information, see the chapter "QoS Commands" in the *HUAWEI NetEngine80E/40E Router Command Reference*.

Procedure

Step 1 Run the **display qppb local-policy statistics interface interface-type interface-number [qos-local-id qos-local-id] { inbound | outbound }** command to check the statistics about a specific QPPB local policy.

----End

Example

After QPPB is configured successfully:

- Run the **display qppb local-policy statistics** command, you can view statistics about a specific QPPB local policy. For example:

```
<HUAWEI> display qppb local-policy statistics interface gigabitethernet 2/0/0
inbound
Interface: GigabitEthernet2/0/0
qppb local-policy inbound: policy1
```

qos-local-id 1		
Item	Packets	Bytes
Matched	0	0
Current CAR statistics:		
Item	Packets	Bytes
Green	0	0
Yellow	0	0
Red	0	0
Passed	0	0
Dropped	0	0

5.5 Maintaining QPPB

This section describes how to clear statistics about a QPPB local policy.

5.5.1 Clearing Statistics About a QPPB Policy

This section describes how to clear statistics about a QPPB policy on an interface.

Context



CAUTION

Once deleted, statistics cannot be restored. Therefore, exercise caution when deleting statistics.

Procedure

- Step 1** Run the **reset qppb local-policy statistics interface interface-type interface-number [qos-local-id qos-local-id] { inbound | outbound }** command in the user view to clear statistics about a QPPB local policy on the specified interface.

---End

5.6 Configuration Examples

This section provides examples for configuring QPPB, including the application scenario and configuration commands.

5.6.1 Example for Configuring QPPB

This section provides an example for configuring QPPB.

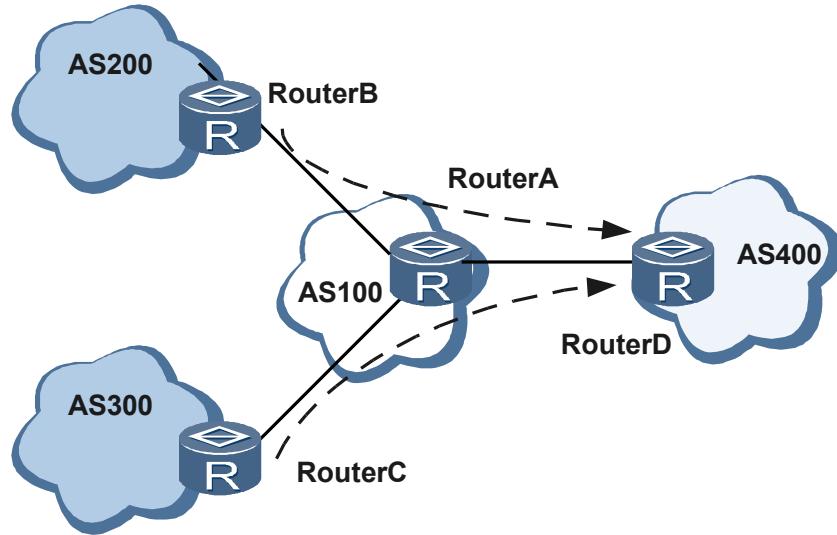
Networking Requirements

On the network shown in [Figure 5-7](#), Router B advertises BGP routes with community attributes to Router A, Router A matches the community attributes against the community list, associates traffic behaviors with QoS local IDs for the matched routes, and apply a QPPB local policy to the traffic transmitted along the routes.

Traffic is sent from Router B to Router C by passing Router A. Router B functions as a BGP route sender, and Router A functions as a BGP route receiver.

It is required that source-based QPPB be applied to the incoming traffic.

Figure 5-7 Networking diagram for configuring QPPB



Precautions

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic BGP functions.
2. Configure routing policies, set community attributes for the routes to be advertised, and advertise routes on Router B.
3. Apply routing policies, match route attributes, and set IP preference on Router A.
4. Configure QPPB and apply it to the incoming traffic on Router A.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface
- Routing policy name, matching rule, and route attribute
- QPPB policy name

Procedure

Step 1 Configure basic BGP functions on RouterA and RouterB.

Configure loopback interfaces on Router A and Router B.

```
<RouterA> system-view
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.255
[RouterA-LoopBack0] return
<RouterB> system-view
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 2.2.2.2 255.255.255.255
```

Configure interfaces connecting Router A and Router B and interfaces connecting Router A and Router C.

```
<RouterA> system-view
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] undo shutdown
[RouterA-Pos2/0/0] ip address 100.1.1.1 255.255.255.0
[RouterA-Pos2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] undo shutdown
[RouterA-GigabitEthernet1/0/0] ip address 200.1.1.2 255.255.255.0
[RouterA-GigabitEthernet1/0/0] return
<RouterB> system-view
[RouterB] interface pos 1/0/0
[RouterB-Pos2/0/0] undo shutdown
[RouterB-Pos2/0/0] ip address 100.1.1.2 255.255.255.0
[RouterB-Pos2/0/0] return
<RouterC> system-view
[RouterC] interface gigabitethernet1/0/0
[RouterC-GigabitEthernet1/0/0] undo shutdown
[RouterC-GigabitEthernet1/0/0] ip address 200.1.1.1 255.255.255.0
[RouterC-GigabitEthernet1/0/0] return
```

Enable OSPF and advertise route information containing the interface addresses.

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] return
<RouterB> system-view
[RouterB] ospf
[RouterB-ospf] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] return
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf] area 0
[RouterC-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] return
```

Configure BGP and set up EBGP peer relationships between Router A and Router B.

```
<RouterA> system-view
[RouterA] bgp 100
[RouterA-bgp] peer 2.2.2.2 as-number 200
[RouterA-bgp] peer 2.2.2.2 ebgp-max-hop 3
[RouterA-bgp] peer 2.2.2.2 connect-interface loopback 0
[RouterA-bgp] import-route direct
[RouterA-bgp] return
<RouterB> system-view
[RouterB] bgp 200
[RouterB-bgp] peer 1.1.1.1 as-number 100
[RouterB-bgp] peer 1.1.1.1 ebgp-max-hop 3
[RouterB-bgp] peer 1.1.1.1 connect-interface loopback 0
[RouterB-bgp] import-route direct
[RouterB-bgp] return
```

Configure BGP and set up an IBGP peer relationship between Router A and Router C.

```
<RouterA> system-view
[RouterA] bgp 100
[RouterA-bgp] peer 200.1.1.1 as-number 100
[RouterA-bgp] import-route direct
[RouterA-bgp] quit
<RouterC> system-view
[RouterC] bgp 100
[RouterC-bgp] peer 200.1.1.2 as-number 100
[RouterC-bgp] import-route direct
[RouterC-bgp] quit
```

After the configuration is complete, Router A can communicate with Router B and Router C.

Step 2 Configure and apply routing policies on Router B.

Configure an IP prefix on RouterB.

```
<RouterB> system-view
[RouterB] ip ip-prefix bb permit 66.1.1.1 32
[RouterB] return
```

Configure a routing policy on Router B.

```
<RouterB> system-view
[RouterB] route-policy aa permit node 10
[RouterB-route-policy] if-match ip-prefix bb
[RouterB-route-policy] apply community 10:10
[RouterB-route-policy] return
```

Configure a policy for advertising routes on Router B.

```
<RouterB> system-view
[RouterB] bgp 200
[RouterB-bgp] peer 1.1.1.1 route-policy aa export
[RouterB-bgp] peer 1.1.1.1 advertise-community
[RouterB-bgp] return
```

Step 3 Configure a policy for receiving routes on Router A, and apply traffic behaviors to the route that matches the route attribute.

Configure a traffic behavior.

```
<RouterA> system-view
[RouterA] traffic behavior dd
[RouterA-behavior-dd] remark dscp af11
[RouterA-behavior-dd] return
```

Configure a routing policy and apply the traffic behavior to the route that matches the route attribute.

```
<RouterA> system-view
[RouterA] ip community-filter 10 permit 10:10
[RouterA] route-policy aa permit node 10
[RouterA-route-policy] if-match community-filter 10
[RouterA-route-policy] apply qos-local-id 1
[RouterA-route-policy] return
```

Configure a QPPB local policy on Router A.

```
<RouterA> system-view
[RouterA] qppb local-policy ac
[RouterA-localpolicy-dd] qos-local-id 1 behavior dd
[RouterA-localpolicy-dd] return
```

Apply the routing policy to the routes sent from Router B on Router A.

```
<RouterA> system-view
```

```
[RouterA] bgp 100
[RouterA-bgp] peer 2.2.2.2 route-policy aa import
[RouterA-bgp] return
```

Step 4 Apply the QPPB local policy to the incoming traffic on Router A.

```
<RouterA> system-view
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] qppb-policy ac source inbound
[RouterA-Pos2/0/0] return
```

----End

Configuration Files

- Configuration file of Router A

```
#          sysname RouterA
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 200.1.1.2 255.255.255.0
#
interface Pos2/0/0
    undo shutdown
    link-protocol ppp
    qppb-policy ac source inbound
    ip address 100.1.1.1 255.255.255.0
#
interface LoopBack0
    ip address 1.1.1.1 255.255.255.255
#
bgp 100
    peer 2.2.2.2 as-number 200
    peer 2.2.2.2 ebgp-max-hop 3
    peer 2.2.2.2 connect-interface LoopBack0
    peer 200.1.1.1 as-number 100
#
ipv4-family unicast
    undo synchronization
    import-route direct
    peer 2.2.2.2 enable
    peer 2.2.2.2 route-policy aa import
    peer 200.1.1.1 enable
#
ospf 1
    area 0.0.0.0
    network 1.1.1.1 0.0.0.0
    network 100.1.1.0 0.0.0.255
    network 200.1.1.0 0.0.0.255
#
route-policy aa permit node 10
    if-match community-filter 10
    apply qos-local-id 1
#
    ip community-filter 10 permit 10:10
#
qppb local-policy ac
    qos-local-id 1 behavior dd
return
```

- Configuration file of Router B

```
#          sysname RouterB
#
interface Pos2/0/0
    undo shutdown
    link-protocol ppp
    ip address 100.1.1.2 255.255.255.0
```

```
#  
interface LoopBack0  
    ip address 2.2.2.2 255.255.255.255  
#  
interface LoopBack10  
    ip address 66.1.1.1 255.255.255.255  
#  
bgp 200  
    peer 1.1.1.1 as-number 100  
    peer 1.1.1.1 ebgp-max-hop 3  
    peer 1.1.1.1 connect-interface LoopBack0  
    #  
    ipv4-family unicast  
        undo synchronization  
        import-route direct  
        peer 1.1.1.1 enable  
        peer 1.1.1.1 route-policy aa export  
        peer 1.1.1.1 advertise-community  
        quit  
    #  
ospf 1  
    area 0.0.0.0  
        network 2.2.2.2 0.0.0.0  
        network 100.1.1.0 0.0.0.255  
    #  
    route-policy aa permit node 10  
        if-match ip-prefix bb  
        apply community 10:10  
    #  
    ip ip-prefix bb index 10 permit 66.1.1.1 32  
    #  
return
```

- Configuration file of Router C

```
#  
    sysname RouterC  
#  
interface gigabitethernet1/0/0  
    undo shutdown  
    ip address 200.1.1.1 255.255.255.0  
#  
bgp 100  
    peer 200.1.1.2 as-number 100  
    #  
    ipv4-family unicast  
        undo synchronization  
        import-route direct  
        peer 200.1.1.2 enable  
    #  
ospf 1  
    area 0.0.0.0  
        network 200.1.1.0 0.0.0.255  
    #  
return
```

6 MPLS HQoS Configuration

About This Chapter

In the deployment of a VPN, if the network structure is unstable and needs frequent modification, it is necessary to frequently modify the network configurations, which requires a lot of workload and may be difficult to implement. VPN QoS can implement both the forwarding policies of public network routes and the forwarding policies of VPN routes. This simplifies policy modification on the route receiver.

[6.1 Overview of MPLS HQoS](#)

This section provides an overview of VPN QoS, traffic statistics, QoS policy propagation via BGP, and the configuration of resource reserved VPN (RRVPN).

[6.2 Configuring QoS Template for VPN](#)

You can implement QoS scheduling for VPN users by defining various QoS profiles and applying them to VPN instances.

[6.3 Configuring BGP/MPLS IP VPN QoS](#)

VPN QoS can be configured to restrict and guarantee the bandwidths of VPN instances.

[6.4 Configuring VLL QoS](#)

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the VLL in the tunnel without affecting the QoS of other VPNs, VLL QoS needs to be configured.

[6.5 Configuring PWE3 QoS](#)

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the PWE3 in the tunnel without affecting the QoS of other VPNs, PWE3 QoS needs to be configured.

[6.6 Configuring VPLS QoS](#)

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the VPLS in the tunnel without affecting the QoS of other VPNs, VPLS QoS needs to be configured.

[6.7 Configuring BGP/MPLS IP VPN Traffic Statistics](#)

You can collect BGP/MPLS IP VPN traffic statistics in real time to check whether the QoS requirements of a VPN are met.

[6.8 Configuring Traffic Statistics of the Single-hop VLL](#)

You can collect traffic statistics on a single-hop VLL in real time to check whether the QoS requirements of the single-hop VLL are met.

[6.9 Configuring Traffic Statistics of the VPLS](#)

You can collect VPLS traffic statistics in real time to check whether the QoS requirements are met.

[6.10 Maintaining MPLS HQoS](#)

This sections describes the commands for maintaining VPN QoS, including the commands for clearing L3VPN statistics, VPLS statistics, and VLL statistics.

[6.11 Configuration Examples of MPLS HQoS](#)

This section provides examples for configuring VPN QoS, including application scenarios and configuration commands.

6.1 Overview of MPLS HQoS

This section provides an overview of VPN QoS, traffic statistics, QoS policy propagation via BGP, and the configuration of resource reserved VPN (RRVPN).

6.1.1 Introduction to MPLS HQoS

VPN QoS is a mechanism that makes sure that each type of traffic gets the specified bandwidth resources by means of bandwidth restriction and queue scheduling. In case of congestion, VPN QoS can implement queue scheduling of various types of traffic according to their class of service (CoS), and therefore ensures that higher priority queues are preferentially serviced.

MPLS HQoS

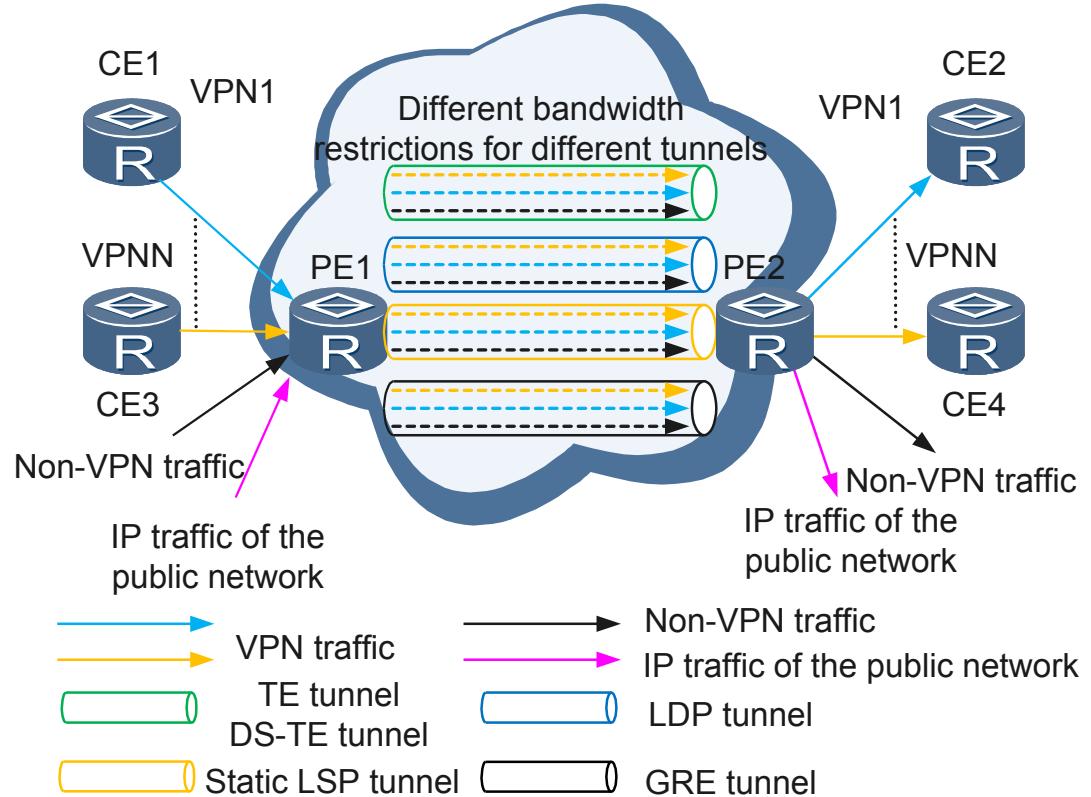
As shown in **Figure 6-1**, multiple types of tunnels, including the TE tunnel, DS-TE tunnel, LDP tunnel, static LSP tunnel, and GRE tunnel, are established between PE1 and PE2.

Data streams exchanged between the two nodes are as follows:

- Various types of traffic that enters the preceding tunnels
 - VPN traffic, for example, the traffic that goes from VPN1 to VPNN as shown in the following figure
 - Non-VPN traffic
- IP traffic in the Public network that does not enter the preceding tunnels

Amongst the preceding types of traffic, bandwidth contention occurs easily.

Figure 6-1 Networking diagram of MPLS HQoS



To meet the requirements for QoS, bandwidth restriction should be applied to the different types of traffic to ensure that each type of service is allocated the predefined bandwidth resources.

MPLS HQoS is just the mechanism that makes sure that each type of traffic gets the specified bandwidth resources by means of bandwidth restriction and queue scheduling. In this way, MPLS HQoS can implement queue scheduling of various types of traffic according to their class of service (CoS) in the case of congestion, and therefore ensures that higher priority queues are preferentially serviced.

6.1.2 MPLS HQoS Supported by the NE80E/40E

The NE80E/40E supports VPN QoS for the BGP/MPLS IP VPN, VLL, PWE3, VPLS, and MVPN. BGP/MPLS IP VPN, VLL, and VPLS can run over the LDP tunnel, static LSP tunnel, BGP LSP tunnel, and TE tunnel, whereas MVPN can run over the GRE tunnel.

The NE80E/40E can collect statistics on:

- QoS-enabled outgoing traffic on the BGP/MPLS IP VPN
- QoS-enabled outgoing traffic on the BGP/MPLS IP VPN Peer
- QoS-enabled outgoing traffic on the single-hop VLL
- QoS-enabled outgoing traffic on the VSI
- QoS-enabled outgoing traffic on the VSI peer

6.2 Configuring QoS Template for VPN

You can implement QoS scheduling for VPN users by defining various QoS profiles and applying them to VPN instances.

6.2.1 Establishing the Configuration Task

Before configuring a VPN-based QoS profile, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

QoS Template for VPN implements QoS scheduling management of VPN users mainly by defining various QoS templates and applying the QoS templates to VPN instances. A QoS template is the aggregate of QoS scheduling parameters. QoS Template for VPN includes templates for flow queues, templates for flow mapping and lengths for packet loss compensation of service templates. It implements uniform scheduling of traffic flows on multiple VPN users by defining QoS scheduling templates and applying the templates to different VPN instances.

Pre-configuration Tasks

Before configuring QoS Template for VPN, complete the following tasks:

- Configuring the physical parameters and link attributes of interfaces for them to work properly
- Assigning IP addresses to interfaces

- Configuring IP routes on the router to make devices on the link reachable

Data Preparation

To configure QoS Template for VPN, you need the following data.

No.	Data
1	Scheduling algorithms and related parameters in flow-queue
2	(Optional) CoS relations in flow-mapping
3	(Optional) Service-template name and parameters
4	QoS Template names

6.2.2 (Optional) Configuring an FQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a flow-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:



NOTE

- When no flow-wred objects are set, the system adopts the default tail-drop policy.
- The high and low limit percentages for red packets can be set to the minimum; those for yellow packets can be greater; those for green packets can be set to the maximum.
- In the actual configuration, the low limit percentage of WRED is recommended to begin with 50% and be adjusted based on different colors of packets. 100% is recommended for the drop probability.

By configuring a flow-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a FQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a FQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a FQ is greater than the high limit percentage, the system drops all subsequent packets.

You can create multiple flow-wred objects for being referenced by FQs as required. You can configure up to 511 flow-wred objects in the system.

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

```
flow-wred flow-wred-name
```

The flow-wred is created and the flow-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage-value
```

The high and low limit percentages and the drop probability are set for different colors of packets.

Step 4 (Optional) Run:

```
queue-depth queue-depth-value
```

The depth is set for the FQs in the flow-wred objects to decrease the delay.

----End

6.2.3 (Optional) Configuring Scheduling Parameters of an FQ

You can define an FQ profile rather than adopt the default profile to configure WFQ scheduling weights, traffic shaping, the shaping rate, and the way of dropping packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-queue flow-queue-name
```

The FQ view is displayed.

Step 3 Run:

```
queue cos-value { { pq | wfq weight weight-value | lpq } | { shaping { shaping-value | shaping-percentage shaping-percentage-value } [ pbs pbs-value ] } | flow-wred wred-name } *
```

A queue scheduling policy for a class is set.

 **NOTE**

You can configure scheduling parameters in one flow queue profile for the eight FQs of a subscriber respectively.

If you do not configure a flow queue, the system uses the default flow queue profile.

- By default, the system performs PQ scheduling on the FQs with the priorities of EF, CS6, and CS7.
- The system defaults the FQs with the priorities of BE, AF1, AF2, AF3, and AF4 to WFQ. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The default discarding policy is the tail drop.

----End

6.2.4 (Optional) Configuring a Mapping from an FQ to a CQ

You can define a mapping from an FQ to a CQ rather than adopt the default mapping to set the priority of a type of service in an SQ entering a CQ.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`flow-mapping mapping-name`

The flow mapping view is displayed.

Step 3 Run:

`map flow-queue cos-value to port-queue cos-value`

The priority mapping from a flow queue to a CQ is set.

 **NOTE**

You can configure eight mappings from flow queues to port queues in one flow queue mapping profile.

When no mapping from the flow queue to the CQ is set, the system defaults the one-to-one mapping.

Users can create multiple flow-mapping profiles for being referenced by SQs as required. You can configure up to 15 flow-mapping profiles in the system.

----End

6.2.5 (Optional) Configuring a Service Profile and Applying It to an Interface

Applying a service profile to an interface and configuring packet loss compensation achieve precise flow control by compensating a processed packet with a certain length.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
service-template service-template-name [ slot slot-id ]
```

The service profile view is displayed.

Step 3 Run:

```
network-header-length network-header-length { inbound | outbound }
```

The packet loss compensation length of the service profile is specified.

 **NOTE**

After packets enter the device, there is a difference between the length of a processed packet and the original packet. Packet loss compensation is a method to achieve precise traffic control by compensating a processed packet with a certain length.

Step 4 Run:

```
quit
```

The system view is displayed.

Step 5 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 6 Run:

```
shaping service-template service-template-name
```

The service profile is applied to the interface.

 **NOTE**

By default, the system has 14 service profiles. You can select the service profile as required.

----End

6.2.6 Defining a QoS Template for VPN and Configuring Scheduling Parameters

You can define the FQ profile, FQ mapping object, service profile, and user group queue in a QoS profile.

Context

Do as follows to configure MPLS HQoS on the router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
qos-profile qos-profile-name
```

A QoS template for VPN is defined and the qos-profile view is displayed.

Step 3 Run:

```
mpls-hqos flow-queue flow-queue-name [ flow-mapping flow-mapping-name | service-template service-template-name | user-group-queue group-name ]
```

Flow queue scheduling parameters for VPN users in QoS template are configured.



NOTE

The service template specified in command must be a globally configured template rather than a board-specific service template.

This command cannot be configured concurrently with the **car** command or the **user-queue** command in the QoS profile.

----End

6.2.7 Checking the Configuration

After a VPN-based QoS profile is configured, you can view the configurations of an FQ profile, configurations of a QoS profile, and applications of a QoS profile.

Context

Run the following **display** commands to check the previous configuration.

Procedure

- Using the **display flow-mapping configuration** [**verbose** [*mapping-name*]] command to check the configurations of a FQ mapping object and the referential relations of the object.
- Using the **display flow-queue configuration** [**verbose** [*flow-queue-name*]] command to check the configurations of the flow queue template.
- Using the **display qos-profile configuration** [*profile-name*] command to check the configurations of a QoS template.
- Using the **display qos-profile application** *profile-name* command to check the applications of a QoS template.

----End

Example

- Using the **display qos-profile configuration** [*profile-name*] command, you can view the detailed configurations of a QoS template.

```
<HUAWEI> display qos-profile configuration test
qos-profile: test
    inbound:
```

```
outbound:  
both:  
    mpls-hqos flow-queue test flow-mapping test user-group-queue test service-  
templa  
te test  
<HUAWEI> display qos-profile configuration  
[qos-profile brief information]  
total number : 4  
qos-profile-name           is-used  
a                         no  
test                      yes  
asdasd                   no  
ddd                      no
```

- Using the **display qos-profile application profile-name** command, you can view the applications of a QoS template.

```
<HUAWEI> display qos-profile application test  
qos-profile test:  
Reference relationship:  
Eth-Trunk1.1  
GigabitEthernet4/0/0.1  
Vpn-instance test peer 1.1.1.1  
<HUAWEI> display qos-profile application test  
qos-profile test:  
GigabitEthernet4/0/0.1
```

6.3 Configuring BGP/MPLS IP VPN QoS

VPN QoS can be configured to restrict and guarantee the bandwidths of VPN instances.

6.3.1 Establishing the Configuration Task

Before configuring BGP/MPLS IP VPN QoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

MPLS HQoS is a special QoS service for VPN users, and is able to implement bandwidth restriction and other QoS-related functions on VPN traffic.

The NE80E/40E supports VPN instance-based QoS and peer-based QoS for L3VPN.

- VPN instance-based QoS implements overall bandwidth restriction and guarantee for the network-side traffic going from a VPN instance on a PE to all the other PE devices.
- Peer-based QoS, by comparison, restricts the traffic going from a VPN on a PE to a specified PE device.

NOTE

VPN instance-based QoS and peer-based QoS are mutually exclusive on the same VPN, but can be configured on different VPN instances. That is, one VPN instance can be configured with VPN instance-based QoS, whereas another VPN instance can be configured with peer-based QoS.

Pre-configuration Tasks

Before configuring BGP/MPLS IP VPN QoS, complete the following task:

- Configuring the BGP/MPLS IP VPN to ensure the connectivity of networks

- (Optional) Configuring the QoS profile

 **NOTE**

For details about the configuration of QoS-profile, refer to [6.2 Configuring QoS Template for VPN](#)

Data Preparation

To configure BGP/MPLS IP VPN QoS, you need the following data.

No.	Data
1	Committed Information Rate(CIR)
2	Peak Information Rate(PIR)
3	(Optional) Name of the QoS profile
4	(Optional) IP address of the peer to which MPLS HQoS is applied

6.3.2 Configuring BGP/MPLS IP VPN Instance-based QoS

By configuring BGP/MPLS IP VPN instance-based QoS, you can provide QoS treatments for the total traffic from a VPN to other PEs.

Context

VPN instance-based QoS implements overall bandwidth restriction and guarantee for the network-side traffic going from a VPN instance to all PE devices.

Do as follows on the PE.

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`ip vpn-instance vpn-instance-name`

The VPN instance view is displayed.

Step 3 Run:

`ipv4-family`

The VPN instance IPv4 address family view is displayed.

Step 4 Run:

`qos cir cir [pir pir] [qos-profile qos-profile-name]`

VPN instance-based QoS is configured.

To reference a QoS profile, you should ensure that the QoS profile is already configured.

----End

6.3.3 Configuring BGP/MPLS IP VPN Peer QoS

By configuring BGP/MPLS IP VPN instance-based QoS, you can provide QoS treatment for the traffic from a VPN to the specified PE.

Context

Peer-based QoS restricts the traffic going from a VPN to a specified PE device.

Do as follows on the PE.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip vpn-instance vpn-instance-name
```

The VPN instance view is displayed.

Step 3 Run:

```
ipv4-family
```

The VPN instance IPv4 address family view is displayed.

Step 4 Run:

```
qos cir cir [ pir pir ] [ qos-profile qos-profile-name ] [ peer ipv4-address &lt;1-10> ]
```

VPN peer-based QoS is configured.

Using the **qos cir** command, you can specify up to 10 PE peers at a time.

To reference a QoS profile, you should ensure that the QoS profile is already configured.

----End

6.3.4 Checking the Configuration

After BGP/MPLS IP VPN QoS is successfully configured, you can view information about tunnels, VPN instances that reference the specified QoS profile, and the VPN QoS configurations of VPNs.

Prerequisite

All BGP/MPLS IP VPN QoS configurations are complete.

Procedure

- Run the **display tunnel-info { tunnel-id tunnel-id | all | statistics [slots] }** command to view the established tunnels.
- Run the **display tec sub-tunnel-info { all | peer ip-address | protocol { { bgp | gre | ldp | mpls-local-ifnet | static } [token | out-interface interface-type interface-number] | }**

l3vpn [vpn-instance-name] [peer ip-address] | te [tunnel-interface interface-type interface-number] } | tunnel-id tunnel-id } command to view the established sub-tunnels.

- Run the **display tcm statistics { global | token | tunnel-interface interface-type interface-number }** command to view statistics on sub-tunnels that are established on the main tunnels.
- If a QoS profile is referenced by VPN instances, run the **display ip vpn-qos l3vpn-instance-list refer qos-profile qos-profile-name** command to view the VPN instances that reference the QoS profile.
- Run the **display ip vpn-instance vpn-instance-name** command to view the QoS configurations of VPN instances.

----End

Example

- Run the **display tcm sub-tunnel-info all** command to view the CIR, PIR, and the type of QoS of each sub-tunnel.
- Run the **display tcm statistics** command to view the total number of sub-tunnels and the sum of CIR for all the sub-tunnels on a main tunnel.

```
<HUAWEI> display tcm statistics 1014
Main LSP-token : 0x1014
Sub-tunnel Num With Qos : 2
Sub-tunnel Num Without Qos : 0
Total Used CIR(kbps) : 13000
```

- If a VPN instance is configured with QoS, run the **display ip vpn-instance verbose** command to view the QoS configurations of the VPN instance.

```
<HUAWEI> display ip vpn-instance verbose vpnb
VPN-Instance Name and ID : vpnb, 2
Address family ipv4
Create date : 2009/03/27 12:13:14
Up time : 0 days, 04 hours, 10 minutes and 17 seconds
Route Distinguisher : 3:2
Export VPN Targets : 200:1
Import VPN Targets : 200:1
Label policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe
The VPN QoS configuration information : based on peer
<1>CIR: 4000 PIR: 6000
Peer List: 1.1.1.1
Tunnel Policy : p3
Log Interval : 5
Interfaces : GigabitEthernet1/0/0
```

6.4 Configuring VLL QoS

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the VLL in the tunnel without affecting the QoS of other VPNs, VLL QoS needs to be configured.

6.4.1 Establishing the Configuration Task

Before configuring VLL QoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In the L2VPN, multiple VPNs may share one tunnel, which leads to bandwidth contention between VPNs. As a result, the forwarding or discarding of VPN traffic cannot be implemented based on the priorities of services within VPNs, and in the tunnel, non-VPN traffic may preempt the bandwidth resources of VPN traffic.

Because different VPNs in the tunnel have different resource requirements, it is necessary to configure VLL QoS in order to meet the resource requirements of the VLL in the tunnel without reducing the QoS for services in the other VPNs.

Pre-configuration Tasks

Before configuring VLL QoS, complete the following tasks:

- Configuring the VLL and ensuring the connectivity of the network.
- (Optional)Configuring the QoS-Profile.



For details about the configuration of QoS-profile, refer to [6.2 Configuring QoS Template for VPN](#)

Data Preparation

To configure VLL QoS, you need the following data.

No.	Data
1	Committed information rate (CIR)
2	Peak information rate (PIR)
3	Name of the QoS-Profile

6.4.2 Configuring VLL QoS

Configuring VLL QoS can solve QoS issues such as bandwidth allocation and resource usage on a Layer 2 VPN.

Context

Do as follows on the router:

Procedure

- Configure VLL QoS on the interface.

1. Run:

`system-view`

The system view is displayed.

2. Run:

`interface interface-type interface-number[.subinterface-number]`

The interface view is displayed.

3. Run:

```
mpls l2vpn qos cir cir [ pir pir ] [ qos-profile qos-profile-name ]  
[ secondary ]
```

Bandwidth resources are configured for the VLL.

 **NOTE**

- CCC VLL does not support VLL QoS.
- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

● Configure VLL QoS in the PW template view.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
pw-template template-name
```

A PW template is created, and the PW template view is displayed.

3. Run:

```
qos cir cir [ pir pir ] [ qos-profile qos-profile-name ]
```

Bandwidth resources are configured for the VLL.

 **NOTE**

- SVC VLL, LDP VLL and single-hop PWE3 support the configuring of VLL QoS in the PW template view.
- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

4. Run:

```
quit
```

The system view is displayed.

5. Run:

```
interface interface-type interface-number [.subinterface-number ]
```

The interface view is displayed.

6. Run:

```
mpls static-l2vc { { destination ip-address | pw-template pw-template-  
name vc-id } * | destination ip-address [ vc-id ] } transmit-vpn-label  
transmit-label-value receive-vpn-label receive-label-value [ tunnel-  
policy tnl-policy-name | [ control-word | no-control-word ] | [ raw |  
tagged | ip-interworking ] ] *
```

An SVC VLL connection is established.

----End

6.4.3 Checking the Configuration

After VLL QoS is successfully configured, you can view the VLL QoS configuration of an interface and the VLL QoS configuration of a PW template.

Prerequisite

All VLL QoS configurations are complete.

Procedure

- Running the **display mpls l2vpn qos interface** *interface-type interface-number [secondary]* command displays VLL QoS configurations of the specified interface.
- Running the **display mpls l2vpn qos pw-template** *pw-template regular-expression [*] command displays VLL QoS configurations in the PW template.

----End

Example

To view VLL QoS configurations of an interface, run the **display mpls l2vpn qos interface** command. For example:

```
<HUAWEI> display mpls l2vpn qos interface gigabitethernet 1/0/0 secondary
Using IntfName GigabitEthernet 1/0/0 Display Interface VLL SVC QoS:
-----
L2VPN QoS CIR value      : 2000
L2VPN QoS PIR value      : 3000
L2VPN QoS qos-profile name : qp1
```

To view VLL QoS configurations of the PW template, run the **display mpls l2vpn qos pw-template** command. For example:

```
<HUAWEI> display mpls l2vpn qos pw-template test
Using PWTName test Display PWT QoS:
-----
L2VPN QoS CIR value      : 2000
L2VPN QoS PIR value      : 3000
L2VPN QoS qos-profile name : qp1
```

6.5 Configuring PWE3 QoS

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the PWE3 in the tunnel without affecting the QoS of other VPNs, PWE3 QoS needs to be configured.

6.5.1 Establishing the Configuration Task

Before configuring PWE3 QoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In the L2VPN, multiple VPNs may share one tunnel, which leads to bandwidth contention between VPNs. As a result, the forwarding or discarding of VPN traffic cannot be implemented based on the priorities of services within VPNs, and non-VPN traffic may preempt the bandwidth resources of VPN traffic.

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the PWE3 in the tunnel without affecting the QoS of other VPNs, PWE3 QoS needs to be configured.

You can configure the single-hop PWE3 QoS and multi-hop PWE3 QoS for the single-hop PWE3 and multi-hop PWE3 respectively.

Pre-configuration Tasks

Before configuring PWE3 QoS, complete the following tasks:

- Configuring the PWE3 and ensuring the connectivity of the network.
- (Optional)Configuring the QoS-Profile.

 **NOTE**

For details about the configuration of QoS-profile, refer to [6.2 Configuring QoS Template for VPN](#)

Data Preparation

To configure PWE3 QoS, you need the following data.

No.	Data
1	Committed information rate (CIR)
2	Peak information rate (PIR)
3	Name of the QoS-Profile
4	Name of the tunnel policy

6.5.2 Configuring the Single-hop PWE3 QoS

This part describes how to configure QoS for a single-hop PWE3.

Context

Do as follows on the router:

Procedure

- Configure the single-hop PWE3 QoS on the interface.
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`interface interface-type interface-number[.subinterface-number]`
The interface view is displayed.
 3. Run:
`mpls l2vpn qos cir cir [pir pir] [qos-profile qos-profile-name] [secondary]`
Bandwidth resources are configured for the PWE3.

 NOTE

- Only the NE80E/40E support the configuring of the QoS-Profile.
 - A QoS-Profile that is in use cannot be deleted.
- Configure the single-hop PWE3 QoS in the PW template view.

1. Run:

`system-view`

The system view is displayed.

2. Run:

`pw-template template-name`

A PW template is created, and the PW template view is displayed.

3. Run:

`qos cir cir [pir pir] [qos-profile qos-profile-name]`

Bandwidth resources are configured for the PWE3.

 NOTE

- SVC VLL, LDP VLL and single-hop PWE3 support the configuring of VLL QoS in the PW template view.
- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

4. Run:

`quit`

The system view is displayed.

5. Run:

`interface interface-type interface-number[.subinterface-number]`

The interface view is displayed.

6. Run the following commands to create a static or a dynamic single-hop PWE3 connection.

- To create a static PWE3 connection, run the `mpls static-l2vc { { destination ip-address | pw-template pw-template-name vc-id } * | destination ip-address [vc-id] } transmit-vpn-label transmit-label-value receive-vpn-label receive-label-value [tunnel-policy tnl-policy-name | [control-word | no-control-word] | [raw | tagged | ip-interworking]] *` command.
- To create a dynamic PWE3 connection, run the `mpls l2vc { ip-address | pw-template pw-template-name } * vc-id [[group-id group-id]] | [tunnel-policy policy-name] | [{ control-word | no-control-word }] | [ip-interworking | ip-layer2 | { raw | tagged }] | [secondary]` command.

----End

6.5.3 Configuring Dynamic Multi-hop PWE3 QoS

This part describes how to configure QoS for a dynamic multi-hop PWE3.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls switch-l2vc ip-address vc-id [ [ cir cir [ [ pir pir ] | [ qos-profile qos-profile-name ] ] ] | [ tunnel-policy policy-name ] ] between ip-address vc-id [ [ cir cir [ [ pir pir ] | [ qos-profile qos-profile-name ] ] ] | [ tunnel-policy policy-name ] ] encapsulation encapsulation-type
```

Bandwidth resources are configured for the dynamic multi-hop PWE3.

- The multi-hop PWE3 supports the configuring of tunnel policies so that the PWE3 traffic enters the TE tunnel. In this way, the PWE3 traffic can be properly forwarded.
- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

----End

6.5.4 Configuring QoS for the Mixed Multi-hop PWE3

This part describes how to configure QoS for a mixed multi-hop PWE3.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls switch-l2vc ip-address vc-id [ [ cir cir [ [ pir pir ] | [ qos-profile qos-profile-name ] ] ] | [ tunnel-policy policy-name ] ] between ip-address vc-id trans trans-label recv received-label [ [ cir cir [ [ pir pir ] | [ qos-profile qos-profile-name ] ] ] | [ tunnel-policy policy-name ] ] encapsulation encapsulation-type [ mtu mtu ] { control-word [ cc { cw | alert }* cv lsp-ping ] }
```

Bandwidth resources are configured for the mixed multi-hop PWE3 (consisting of both the static PWE3 and dynamic PWE3).

- The multi-hop PWE3 supports the configuring of tunnel policies so that the PWE3 traffic enters the TE tunnel. In this way, the PWE3 traffic can be properly forwarded.
- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

----End

6.5.5 Configuring the Static Multi-hop PWE3 QoS

This part describes how to configure QoS for a static multi-hop PWE3.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls switch-l2vc ip-address vc-id trans trans-label recv received-label [ [ cir cir [ [ pir pir ] | [ qos-profile qos-profile-name ] ] ] | [ tunnel-policy policy-name ] ] between ip-address vc-id trans trans-label recv received-label [ [ cir cir [ [ pir pir ] | [ qos-profile qos-profile-name ] ] ] | [ tunnel-policy policy-name ] ] encapsulation encapsulation-type { control-word [ cc { cw | alert }* cv lsp-ping ] }
```

Bandwidth resources are configured for the static multi-hop PWE3.

- The multi-hop PWE3 supports the configuring of tunnel policies so that the PWE3 traffic enters the TE tunnel. In this way, the PWE3 traffic can be properly forwarded.
- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

----End

6.5.6 Checking the Configuration

After PWE3 QoS is successfully configured, you can view the single-hop PWE3 QoS configuration, multi-hop PWE3 QoS configuration, and the QoS configuration of a PW template.

Prerequisite

All PWE3 QoS configurations are complete.

Procedure

- Running the **display mpls l2vpn qos interface** *interface-type interface-number* [**secondary**] command displays the single-hop PWE3 QoS configurations in the interface view.
- Running the **display mpls l2vpn qos pw-template** *pw-template* command displays the QoS configurations in the PW template view.
- Running the **display mpls l2vpn qos vc-id** *vc-id* **vc-type** *vc-type* command displays the multi-hop PWE3 QoS configurations.

----End

Example

To view the single-hop PWE3 QoS configurations in the interface view, run the **display mpls l2vpn qos interface** command. For example:

```
<HUAWEI> display mpls l2vpn qos interface gigabitethernet 1/0/0 secondary
Using IntfName GigabitEthernet 1/0/0GigabitEthernet 1/0/0 Display Interface VLL SVC
```

QoS:

```
-----  
L2VPN QoS CIR value      : 2000  
L2VPN QoS PIR value      : 3000  
L2VPN QoS qos-profile name : qp1
```

To view QoS configurations in the PW template view, run the **display mpls l2vpn qos pw-template** command. For example:

```
<HUAWEI> display mpls l2vpn qos pw-template test  
Using PWTName test Display PWT QoS:  
-----  
L2VPN QoS CIR value      : 2000  
L2VPN QoS PIR value      : 3000  
L2VPN QoS qos-profile name : qp1
```

To view the PWE3 QoS configurations, run the **display mpls l2vpn qos vc-id** command. For example:

```
<HUAWEI> display mpls l2vpn qos vc-id 100 vc-type vlan  
Using VC ID 100 VC Type vlan Display LDP Peer QoS:  
-----  
L2VPN QoS CIR value      : 2000  
L2VPN QoS PIR value      : 3000  
L2VPN QoS qos-profile name : qp1
```

6.6 Configuring VPLS QoS

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the VPLS in the tunnel without affecting the QoS of other VPNs, VPLS QoS needs to be configured.

6.6.1 Establishing the Configuration Task

Before configuring VPLS QoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In the L2VPN, multiple VPNs may share one tunnel, which leads to bandwidth contention between VPNs. As a result, the forwarding or discarding of VPN traffic cannot be implemented based on the priorities of services within VPNs, and non-VPN traffic may preempt the bandwidth resources of VPN traffic.

In the tunnel, different VPNs demand different resources. To meet the demands for resources of the VPLS in the tunnel without affecting the QoS of other VPNs, VPLS QoS needs to be configured.



VPLS QoS is available in two forms: the VSI-based QoS and the VSI peer-based QoS.

- The VSI-based QoS is configured on the local PE in order to implement bandwidth control on all VSIs.
- The VSI peer-based QoS is configured on the local PE in order to implement bandwidth control on a peer VSI.
- The VPLS in LDP mode supports both VSI-based QoS and VSI peer-based QoS while the VPLS in BGP mode supports only VSI-based QoS.

For details about the configuration of QoS-profile, refer to [6.2 Configuring QoS Template for VPN](#)

Pre-configuration Tasks

Before configuring VPLS QoS, complete the following tasks:

- Configuring the VPLS and ensuring the connectivity of the network.
- (Optional) Configuring the QoS-profile.

Data Preparation

To configure VPLS QoS, you need the following data.

No.	Data
1	Committed information rate (CIR)
2	Peak information rate (PIR)
3	Name of the QoS-profile
4	Name of the VSI
5	ID of the VSI
6	IP address of the peer
7	Name of the PW view

6.6.2 Configuring the VSI-based QoS

This part describes how to configure VSI-based QoS to control the total bandwidths of a VSI.

Context



The VSI-based QoS and the VSI peer-based QoS cannot be both configured on the LDP VSI.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vsi vsi-name [ auto | static ]
```

The VSI view is displayed.

Step 3 Run:

```
qos cir cir [ pir pir ] [ qos-profile qos-profile-name ]
```

The VSI-based QoS is configured.

 **NOTE**

Only the NE80E/40E support the configuring of the QoS-Profile.
A QoS-Profile that is in use cannot be deleted.

----End

6.6.3 Configuring the VSI Peer-based QoS

This part describes how to configure VSI-peer-based QoS to control the total bandwidths of a VSI peer.

Context

 **NOTE**

The VSI-based QoS and the VSI peer-based QoS cannot be both configured on the LDP VSI.

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`vsi vsi-name [static]`

The VSI view is displayed.

Step 3 Run:

`pwsignal ldp`

The signaling mode is configured for the VSI.

 **NOTE**

The VSI peer-based QoS can be configured only on the LDP VSI.

Step 4 Run:

`vsi-id vsi-id`

The ID of the VSI is configured.

Step 5 Run:

`peer peer-address [negotiation-vc-id vc-id] [tnl-policy policy-name] [upe]
pw pw-name`

The VSI peer is configured, and the PW view is displayed.

Step 6 Run:

`qos cir cir [pir pir] [qos-profile qos-profile-name]`

The VSI peer-based QoS is configured.

 NOTE

- Only the NE80E/40E support the configuring of the QoS-Profile.
- A QoS-Profile that is in use cannot be deleted.

----End

6.6.4 Checking the Configuration

After VPLS QoS is successfully configured, you can view configurations of VPLS QoS.

Prerequisite

All VPLS QoS configurations are complete.

Procedure

- Step 1** Running the **display mpls l2vpn qos vsi-name vsi-name [peer peer-ip-address] [pw-id pw-id]** command displays the VPLS QoS configurations.

----End

Example

To view the VPLS QoS configurations, run the **display mpls l2vpn qos vsi-name** command.

For example:

```
<HUAWEI> display mpls l2vpn qos vsi-name vsi1 peer 2.2.2.2
Using VSIName: vsi1 LDP Peer IP: 2.2.2.2 Display VSI QoS:
-----
L2VPN QoS CIR value      : 2000
L2VPN QoS PIR value      : 3000
L2VPN QoS qos-profile name : qp1
```

6.7 Configuring BGP/MPLS IP VPN Traffic Statistics

You can collect BGP/MPLS IP VPN traffic statistics in real time to check whether the QoS requirements of a VPN are met.

6.7.1 Establishing the Configuration Task

Before configuring BGP/MPLS IP VPN traffic statistics, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To view the status of various kinds of traffic in real time and to set up a traffic model in a VPN, you can enable the traffic statistics function.

Where QoS is already configured, after the traffic statistics function is enabled, you can check whether traffic configurations meet the QoS requirements by viewing the status of various kinds of traffic in real time.

Pre-configuration Tasks

To configure traffic statistics of the BGP/MPLS IP VPN, complete the following tasks:

- Configuring the BGP/MPLS IP VPN and ensuring the connectivity of networks.

Data Preparation

To configure traffic statistics of the BGP/MPLS IP VPN, you need the following data.

No.	Data
1	Name of the VPN instance
2	IP address of the peer

6.7.2 Configuring Traffic Statistics of BGP/MPLS IP VPN

After BGP/MPLS IP VPN traffic statistics are configured, you can view the total bandwidth usage in real time.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`ip vpn-instance vpn-instance-name`

The VPN instance view is displayed.

Step 3 Run:

`ipv4-family`

The VPN instance IPv4 address family view is displayed.

Step 4 (Optional) Run:

`qos cir cir [pir pir] [qos-profile qos-profile-name]`

The BGP/MPLS IP VPN QoS is enabled.

- If BGP/MPLS IP VPN QoS is enabled, statistics will be produced on the QoS-enabled traffic at the network side.
- If BGP/MPLS IP VPN QoS is not enabled, statistics will be produced on all the traffic at the AC side.

Step 5 Run:

`traffic-statistics enable`

Statistics are enabled on the BGP/MPLS IP VPN traffic.

----End

6.7.3 Configuring Traffic Statistics of the BGP/MPLS IP VPN Peer

After BGP/MPLS IP VPN peer traffic statistics are configured, you can view the traffic statistics of the peer in real time.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip vpn-instance vpn-instance-name
```

The VPN instance view is displayed.

Step 3 Run:

```
ipv4-family
```

The VPN instance IPv4 address family view is displayed.

Step 4 Run:

```
qos cir cir [ pir pir ] [ qos-profile qos-profile-name ]
```

The BGP/MPLS IP VPN QoS is enabled.

When statistics are enabled on the traffic of the BGP/MPLS IP VPN peer, statistics are produced only on the QoS-enabled traffic of the peer.

Step 5 Run:

```
traffic-statistics peer ip-address enable
```

Statistics are enabled on the traffic of the BGP/MPLS IP VPN peer.

----End

6.7.4 Checking the Configuration

After BGP/MPLS IP VPN traffic statistics are successfully configured, you can view the traffic statistics of the BGP/MPLS IP VPN.

Prerequisite

All traffic statistics configurations of the BGP MPLS IP VPN are complete.

Procedure

Step 1 Running the **display traffic-statistics vpn-instance** *vpn-instance-name* [**qos**] [**peer peer-address**] command displays the traffic statistics on the BGP MPLS IP VPN

----End

Example

To view the traffic statistics on the BGP MPLS IP VPN, run the **display traffic-statistics vpn-instance** command. For example:

```
<HUAWEI> display traffic-statistics vpn-instance vpn1 qos peer 1.1.1.1
Vpn-instance name : vpn1
Peer-address : 1.1.1.1
Statistics last cleared : never
Last 300 seconds QoS statistics rate : 0 bits/sec, 0 packets/sec
QoS statistics output: 16 bytes, 16 packets
PacketRate : Last 300 seconds packets rate(packets/sec)
ByteRate : Last 300 seconds bytes rate(bits/sec)
Passed traffic statistics :
  Queue Packets      Bytes      PacketRate     ByteRate
  ----- -----
  be    0            0          0            0
  af1   0            0          0            0
  af2   0            0          0            0
  af3   0            0          0            0
  af4   0            0          0            0
  ef    0            0          0            0
  cs6   0            0          0            0
  cs7   0            0          0            0
  -----
Discarded traffic statistics :
  Queue Packets      Bytes      PacketRate     ByteRate
  ----- -----
  be    0            0          0            0
  af1   0            0          0            0
  af2   0            0          0            0
  af3   0            0          0            0
  af4   0            0          0            0
  ef    0            0          0            0
  cs6   0            0          0            0
  cs7   0            0          0            0
  -----
```

6.8 Configuring Traffic Statistics of the Single-hop VLL

You can collect traffic statistics on a single-hop VLL in real time to check whether the QoS requirements of the single-hop VLL are met.

6.8.1 Establishing the Configuration Task

Before configuring single-hop VLL traffic statistics, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To view the status of various kinds of traffic in real time and to set up a traffic model in a VPN, you can enable the traffic statistics function.

Where QoS is already configured, after the traffic statistics function is enabled, you can check whether traffic configurations meet the QoS requirements by viewing the status of various kinds of traffic in real time.

Pre-configuration Tasks

Before configuring traffic statistics of the single-hop VLL, complete the following tasks:

- Configuring the VLL network and ensuring the connectivity of the network.
- Enabling VLL QoS.



With the single-hop VLL traffic statistics, traffics can be produced only on the QoS-enabled VLL traffic.

Data Preparation

To configure traffic statistics of the single-hop VLL, you need the following data.

No.	Data
1	Interface name

6.8.2 Enabling Statistics on the Single-hop VLL Traffic

You can enable traffic statistics on single-hop VLLs and view the traffic statistics of a single-hop VLL in real time.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface interface-type interface-number`

The interface view is displayed.

Step 3 Run:

`mpls l2vpn pw traffic-statistics enable [secondary]`

Statistics are enabled on the single-hop VLL traffic.

----End

6.8.3 Checking the Configuration

After traffic statistics on single-hop VLLs are successfully configured, you can view the collected traffic statistics.

Prerequisite

All configurations of the VLL traffic statistics are complete.

Procedure

- Step 1** Running the **display traffic-statistics l2vpn pw interface interface-type interface-number [secondary]** command displays traffic statistics of the VLL.

----End

Example

To view traffic statistics of the VLL, run the **display traffic-statistics l2vpn pw interface** command. For example:

```
<HUAWEI> display traffic-statistic l2vpn pw interface gigabitethernet 1/0/0
Interface name : GigabitEthernet 1/0/0
Statistics last cleared : never
Last 300 seconds QoS statistics rate : 0 bits/sec, 0 packets/sec
QoS statistics output : 0 bytes, 0 packets
PacketRate : Last 300 seconds packets rate(packets/sec)
ByteRate : Last 300 seconds bytes rate(bits/sec)
Queue Packets      Bytes      PacketRate   ByteRate
-----
be    0          0          0          0
af1   0          0          0          0
af2   0          0          0          0
af3   0          0          0          0
af4   0          0          0          0
ef    0          0          0          0
cs6   0          0          0          0
cs7   0          0          0          0
-----
Discarded traffic statistics :
Queue Packets      Bytes      PacketRate   ByteRate
-----
be    0          0          0          0
af1   0          0          0          0
af2   0          0          0          0
af3   0          0          0          0
af4   0          0          0          0
ef    0          0          0          0
cs6   0          0          0          0
cs7   0          0          0          0
-----
```

6.9 Configuring Traffic Statistics of the VPLS

You can collect VPLS traffic statistics in real time to check whether the QoS requirements are met.

6.9.1 Establishing the Configuration Task

Before configuring VPLS traffic statistics, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In the VPLS, in order to be able to view the status of various kinds of traffic in real time and to set up a traffic model, you can enable the traffic statistics function.

Where QoS is already configured, after the traffic statistics function is enabled, you can check whether traffic configurations meet the QoS requirements by viewing the status of various kinds of traffic in real time.

Pre-configuration Tasks

Before configuring traffic statistics of the VPLS, complete the following tasks:

- Configuring the VPLS and ensuring the connectivity of the network.

Data Preparation

To configure traffic statistics of the VPLS, you need the following data.

No.	Data
1	Name of the VSI
2	IP address of the peer
3	ID of the VSI
4	negotiation-vc-id or remote-site

6.9.2 Configuring the VSI-based Traffic Statistics

After VSI-based traffic statistics are configured, you can view the total bandwidth usage of a VSI in real time.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`vsi vsi-name [auto | static]`

The VSI view is displayed.

Step 3 Run:

`qos cir cir [pir pir] [qos-profile qos-profile-name]`

The VSI-based QoS is enabled.

 NOTE

Before enabling the VSI-based traffic statistics, you must enable the VSI-based QoS. Otherwise, the traffic statistics do not take effect.

Step 4 Run:

```
traffic-statistics enable
```

The VSI-based traffic statistics are enabled.

----End

6.9.3 Configuring the VSI Peer-based Traffic Statistics

After VSI-peer-based traffic statistics are configured, you can view the traffic statistics of the VSI peer in real time.

Context

Do as follows on the router:

Procedure

- Configure the LDP mode of VSI peer-based traffic statistics.
 1. Run:

```
system-view
```

The system view is displayed.
 2. Run:

```
vsi vsi-name [ static ]
```

The VSI view is displayed.
 3. Run:

```
pwsignal ldp
```

The signaling mode of the VSI is configured to be the LDP.
 4. Run:

```
traffic-statistics peer peer-address [ negotiation-vc-id vc-id ] enable
```

The LDP mode of VSI peer-based traffic statistics are enabled.
 - If the LDP mode of VSI peer-based QoS is enabled, statistics are produced on the QoS-enabled traffic of the VSI peer.
 - If the LDP mode of VSI peer-based QoS is not enabled, statistics are produced on all the traffic of the VSI peer.
- Configure the BGP mode of VSI peer-based traffic statistics.
 1. Run:

```
system-view
```

The system view is displayed.
 2. Run:

```
vsi vsi-name [ auto ]
```

The VSI view is displayed.

3. Run:

pwsignal bgp

The signaling mode of the VSI is configured to be the BGP.

4. Run:

traffic-statistics peer peer-address remote-site site-id enable

The BGP mode of VSI peer-based traffic statistics are enabled.

----End

6.9.4 Checking the Configuration

After VPLS traffic statistics are successfully configured, you can view the collected VPLS traffic statistics.

Prerequisite

All configurations of the VPLS traffic statistics are complete.

Procedure

- Running the **display traffic-statistics vsi vsi-name [qos] [peer peer-address [negotiation-vc-id vc-id]]** command displays the traffic statistics of the VPLS.

----End

Example

To view traffic statistics of the VPLS, run the **display traffic-statistics vsi** command. For example:

```
<HUAWEI> display traffic-statistic vsi vsi1 qos
VSI name : vsi1
Statistics last cleared : never
Last 300 seconds QoS statistics rate : 0 bits/sec, 0 packets/sec
QoS statistics output: 16 bytes, 16 packets
PacketRate : Last 300 seconds packets rate(packets/sec)
ByteRate : Last 300 seconds bytes rate(bits/sec)
Passed traffic statistics :
  Queue  Packets    Bytes   PacketRate  ByteRate
  -----  -----
  be      0          0        0           0
  af1     0          0        0           0
  af2     0          0        0           0
  af3     0          0        0           0
  af4     0          0        0           0
  ef      0          0        0           0
  cs6     0          0        0           0
  cs7     0          0        0           0
  -----
Discarded traffic statistics :
  Queue  Packets    Bytes   PacketRate  ByteRate
  -----  -----
  be      0          0        0           0
  af1     0          0        0           0
  af2     0          0        0           0
  af3     0          0        0           0
  af4     0          0        0           0
  ef      0          0        0           0
  cs6     0          0        0           0
  cs7     0          0        0           0
  -----
```

6.10 Maintaining MPLS HQoS

This section describes the commands for maintaining VPN QoS, including the commands for clearing L3VPN statistics, VPLS statistics, and VLL statistics.

6.10.1 Clearing Statistics on the QoS-enabled VPN Traffic

This part describes how to reset statistics on the QoS-enabled VPN traffic so that statistics can be re-collected on VPN traffic.

Context



CAUTION

Statistics cannot be restored after being cleared. Therefore, confirm the action before you run the following commands.

Procedure

- After confirming that you need to clear traffic statistics of the Layer 3 VPN, run the **reset traffic-statistics vpn-instance { name vpn-instance-name [peer peer-address] | all }** command in the user view.
- After confirming that you need to clear traffic statistics of the VLL, run the **reset traffic-statistics l2vpn pw { all | interface interface-type interface-number [secondary] }** command in the user view.
- After confirming that you need to clear traffic statistics of the VPLS, run the **reset traffic-statistics vsi { name vsi-name | all }** command in the user view.

----End

6.11 Configuration Examples of MPLS HQoS

This section provides examples for configuring VPN QoS, including application scenarios and configuration commands.



NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

6.11.1 Example for Configuring BGP/MPLS IP VPN QoS (LDP LSP at the Network Side)

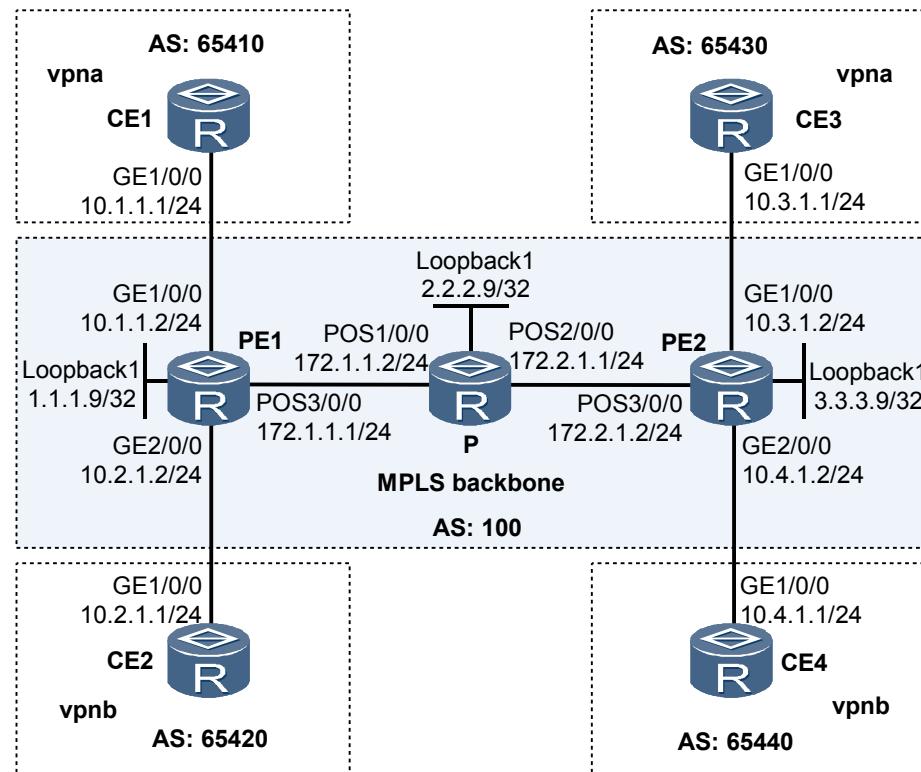
This part describes how to configure BGP/MPLS IP VPN QoS to implement bandwidth restriction and assurance for VPNs.

Networking Requirements

As shown in [Figure 6-2](#), PE1 and PE2 are configured with VPN instances named vpna and vpnb respectively. MPLS HQoS needs to be configured for the two VPN instances so that bandwidths are guaranteed for traffic of the VPN instances going from PE1 to PE2. Such QoS-enabled traffic should be carried by LDP LSPs.

In the event of congestion, packets should be dropped according to the WRED discard parameters configured for flow queues. The traffic shaping rates of flow queues AF1 and EF are 500 kbit/s and 1000 kbit/s respectively, and the traffic of flow queue AF1 is mapped to class queue EF.

Figure 6-2 Networking diagram of configuring BGP/MPLS IP VPN QoS



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure BGP/MPLS IP VPN
2. Configure the QoS-profile and the scheduling parameters.
3. Configure peer-based MPLS HQoS for vpna
4. Configure peer-based MPLS HQoS for vpnb

Data Preparation

To complete the configuration, you need the following data:

- VPN instance name, RD, and VPN target

- The parameters of flow-wred, flow-queue, and the value of network-header-length in the QoS-profile
- Committed Information Rate for VPN instances
- Committed Burst Size for VPN instances

Procedure

Step 1 Configure BGP/MPLS IP VPN. For details, refer to "Example for Configuring BGP/MPLS IP VPN" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - VPN*.

After the configuration, run the **display mpls ldp lsp** command, and you can view the established LDP LSPs.

Take the display on PE1 as an example.

```
<PE1> display mpls ldp lsp
LDP LSP Information
-----
DestAddress/Mask   In/OutLabel   UpstreamPeer   NextHop   OutInterface
-----
1.1.1.9/32        3/NULL       2.2.2.9        127.0.0.1  InLoop0
*1.1.1.9/32       Liberal      -              172.1.1.2   Pos3/0/0
2.2.2.9/32        NULL/3       -              172.1.1.2   Pos3/0/0
2.2.2.9/32        1024/3       2.2.2.9        172.1.1.2   Pos3/0/0
3.3.3.9/32        NULL/1025    -              172.1.1.2   Pos3/0/0
3.3.3.9/32        1025/1025   2.2.2.9        172.1.1.2   Pos3/0/0
-----
TOTAL: 5 Normal LSP(s) Found.
TOTAL: 1 Liberal LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
```

Run the **display ip routing-table vpn-instance** command on the PEs, and you can view the routes to the peer CEs.

Take the display on PE1 as an example.

```
<PE1> display ip routing-table vpn-instance vpna
Route Flags: R - relied, D - download to fib
-----
Routing Tables: vpna
  Destinations : 3      Routes : 3
  Destination/Mask Proto Pre Cost   Flags NextHop   Interface
    10.1.1.0/24   Direct 0   0     D   10.1.1.2   GigabitEthernet1/0/0
    10.1.1.2/32   Direct 0   0     D   127.0.0.1   InLoopBack0
    10.3.1.0/24   BGP    255  0     RD   3.3.3.9   Pos3/0/0
<PE1> display ip routing-table vpn-instance vpnb
Route Flags: R - relied, D - download to fib
-----
Routing Tables: vpnb
  Destinations : 3      Routes : 3
  Destination/Mask Proto Pre Cost   Flags NextHop   Interface
    10.2.1.0/24   Direct 0   0     D   10.2.1.2   GigabitEthernet2/0/0
    10.2.1.2/32   Direct 0   0     D   127.0.0.1   InLoopBack0
    10.4.1.0/24   BGP    255  0     RD   3.3.3.9   Pos3/0/0
```

Step 2 Configure the QoS-profile and the scheduling parameters.

Configure packet dropping parameters of flow-wred.

```
[PE1] flow-wred test
[PE1-flow-wred-test] color green low-limit 70 high-limit 100 discard-percentage 100
[PE1-flow-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage 100
[PE1-flow-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
```

```
[PE1-flow-wred-test] return
```

After the preceding configuration, you can run the **display flow-wred configuration verbose** command to view the configured parameters of the flow WRED object.

```
<PE1> display flow-wred configuration verbose test
Flow wred name : test
-----
Color    Low-limit   High-limit   Discard-percent
-----
green    70          100          100
yellow   60          90           100
red      50          80           100
Queue Depth : 1000
Reference relationships : test
```

Configure the scheduling algorithms, WRED parameters, and shaping values for flow queues.

```
<PE1> system view
[PE1] flow-queue test
[PE1-flow-queue-template-test] queue af1 lpq flow-wred test shaping 500
[PE1-flow-queue-template-test] queue ef pq flow-wred test shaping 1000
```

After the preceding configuration, you can run the **display flow-queue configuration verbose** command to view the configurations of the flow queue template.

```
<PE1> display flow-queue configuration verbose test
Codes: Arith(Schedule algorithm)
        U-Weight(Schedule weight configured by users)
        I-Weight(Inverse schedule weight used by TM)
        A-Weight(Actual schedule weight obtained by users)
        Shp(Shaping value, the percentage of subscriber queue's PIR)
        Drop-Arith(The name of the WRED object used by the flow queue)
```

```
Flow Queue Template : test
-----
Cos  Arith   U-Weight  I-Weight  A-Weight  Shp     Pct  Drop-Arith
-----
be   wfq    10        3         10.00    -       -     Tail Drop
af1  lpq    -         -         -         500    -     test
af2  wfq    10        3         10.00    -       -     Tail Drop
af3  wfq    15        2         15.00    -       -     Tail Drop
af4  wfq    15        2         15.00    -       -     Tail Drop
ef   pq     -         -         -         -       1000   -     test
cs6  pq     -         -         -         -       -     Tail Drop
cs7  pq     -         -         -         -       -     Tail Drop
Reference relationships : NULL
```

Configure the CoS mapping between flow queues and class queues.

```
<PE1> system view
[PE1] flow-mapping test
[PE1-flow-mapping-test] map flow-queue af1 to port-queue ef
[PE1-flow-mapping-test] return
```

After the preceding configuration, run the **display flow-mapping configuration verbose** command to view the configured parameters of the flow queue mapping object and the referential relations of the object.

```
<PE1> display flow-mapping configuration verbose test
flow-mapping-name : test
fq-cosvalue to pq-cosvalue
be          to be
af1         to ef
af2         to af2
af3         to af3
af4         to af4
ef          to ef
```

```

cs6      to cs6
cs7      to cs7
[reference relationship]
NULL

# Configure service-template and network-header-length.

<PE1> system view
[PE1] service-template test
[PE1-service-template-test] network-header-length 12 outbound
[PE1-service-template-test] quit

```

After the preceding configuration, you can run the **display service-template configuration verbose** command to view the configurations of the service template, the value of network-header-length, and the referential relations of the service template.

```

<PE1> display service-template configuration verbose
[service-template detail information]
total number : 1
slot all     : 1
service-template-name : test
slot : all
[current configuration]
inbound network-header-length: NA
outbound network-header-length: 12
[reference relationship]
NULL

```

Configure scheduling parameters for user-queue and suppression rate of broadcast packets in the QoS template.

```

<PE1> system view
[PE1] qos-profile test
[PE1-qos-profile-test] mpls-hqos flow-queue test flow-mapping test service-
template test
[PE1-qos-profile-test] quit

```

Step 3 On PE1, configure peer-based MPLS HQoS for vpna and vpnb.

Configure the CIR and PIR of vpna to be 2000 kbit/s and 5000 kbit/s respectively.



QoS cannot be configured for a VPN instance whose routing table is empty.

```

[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] qos cir 2000 pir 5000 peer 3.3.3.9
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] qos cir 2000 pir 5000 qos-profile test peer 3.3.3.9
[PE1-vpn-instance-vpna] quit

```

Configure the CIR and PIR of vpnb to be 3000 kbit/s and 5000 kbit/s respectively.

```

[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] qos cir 3000 pir 5000 peer 3.3.3.9
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] qos cir 3000 pir 5000 qos-profile test peer 3.3.3.9
[PE1-vpn-instance-vpnb] quit

```

Step 4 After the configuration, run the **display tcm sub-tunnel-info l3vpn** command on PE1 to view information about the sub-tunnels that carry L3VPN traffic.

```

<PE1> display tcm sub-tunnel-info l3vpn
-----
                                         Sub-tunnel information: LSP sub-tunnel
-----
Sub-tunnel Type    : LDP LSP
Qos Token         : 0x1016

```

```

Main LSP-token      : 0x1014
Out-interface       : Pos3/0/0
Indirect ID         : 0x9
N-Key                : 0x1
CIR Value            : 2000
PIR Value            : 5000
Qos Profile Name    : ---
VPN Qos Type      : Base on peer
VPN Type             : L3VPN
VPN Name              : vpna
Peer IP              : 3.3.3.9
Time Stamp           : 13078

Sub-tunnel Type     : LDP LSP
Qos Token            : 0x101b
Main LSP-token      : 0x1014
Out-interface       : Pos3/0/0
Indirect ID         : 0xd
N-Key                : 0x1
CIR Value            : 3000
PIR Value            : 5000
Qos Profile Name    : ---
VPN Qos Type      : Base on peer
VPN Type             : L3VPN
VPN Name              : vpnb
Peer IP              : 3.3.3.9
Time Stamp           : 15084

```

The preceding display shows that the sub-tunnels that carry the QoS-enabled traffic of vpna and vpnb belong to the same primary LSP.

Step 5 Run the **display ip vpn-instance verbose** command to view the QoS configurations of VPN instances.

```

<PE1> display ip vpn-instance verbose vpna
VPN-Instance Name and ID : vpna, 2
Address family ipv4
Create date : 2009/03/27 12:13:14
Up time : 0 days, 04 hours, 10 minutes and 17 seconds
Route Distinguisher : 100:1
Export VPN Targets : 111:1
Import VPN Targets : 111:1
Label policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe
The VPN QoS configuration information : based on peer

<1>CIR: 2000 PIR: 5000 QoS-profile name: test
Peer List: 3.3.3.9
Log Interval : 5
Interfaces : GigabitEthernet1/0/0

<PE1> display ip vpn-instance verbose vpnb
VPN-Instance Name and ID : vpnb, 3
Address family ipv4
Create date : 2009/03/27 12:13:30
Up time : 0 days, 04 hours, 10 minutes and 01 seconds
Route Distinguisher : 100:2
Export VPN Targets : 222:2
Import VPN Targets : 222:2
Label policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe
The VPN QoS configuration information : based on peer

<1>CIR: 3000 PIR: 5000 QoS-profile name: test
Peer List: 3.3.3.9
Log Interval : 5
Interfaces : GigabitEthernet2/0/0

```

The displayed QoS information about a VPN includes its peer-based QoS configurations, CIR, PIR, and IP address of the peer PE.

----End

Configuration Files

- Configuration file of PE1

```
#  
    sysname PE1  
#  
    ip vpn-instance vpna  
        ipv4-family  
            route-distinguisher 100:1  
            vpn-target 111:1 export-extcommunity  
            vpn-target 111:1 import-extcommunity  
            qos cir 2000 pir 5000 qos-profile test peer 3.3.3.9  
#  
    ip vpn-instance vpnb  
        ipv4-family  
            route-distinguisher 100:2  
            vpn-target 222:2 export-extcommunity  
            vpn-target 222:2 import-extcommunity  
            qos cir 3000 pir 5000 qos-profile test peer 3.3.3.9  
#  
    mpls lsr-id 1.1.1.9  
    mpls  
        lsp-trigger all  
#  
    mpls ldp  
#  
    flow-wred test  
        color green low-limit 70 high-limit 100 discard-percentage 100  
        color yellow low-limit 60 high-limit 90 discard-percentage 100  
        color red low-limit 50 high-limit 80 discard-percentage 100  
#  
    flow-mapping test  
        map flow-queue afl to port-queue ef  
#  
    flow-queue test  
        queue afl lpq shaping 500 flow-wred test  
        queue ef pq shaping 1000 flow-wred test  
#  
    service-template test  
        network-header-length 12 outbound  
#  
    qos-profile test  
        mpls-hqos flow-queue test flow-mapping test service-template test  
#  
interface GigabitEthernet1/0/0  
    undo shutdown  
    ip binding vpn-instance vpna  
    ip address 10.1.1.2 255.255.255.0  
#  
interface GigabitEthernet2/0/0  
    undo shutdown  
    ip binding vpn-instance vpnb  
    ip address 10.2.1.2 255.255.255.0  
#  
interface Pos3/0/0  
    link-protocol ppp  
    undo shutdown  
    ip address 172.1.1.1 255.255.255.0  
    mpls  
    mpls ldp  
#  
interface LoopBack1  
    ip address 1.1.1.9 255.255.255.255
```

```

#
bgp 100
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 3.3.3.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 3.3.3.9 enable
#
ipv4-family vpn-instance vpna
peer 10.1.1.1 as-number 65410
import-route direct
#
ipv4-family vpn-instance vpnb
peer 10.2.1.1 as-number 65420
import-route direct
#
ospf 1
area 0.0.0.0
network 172.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
return

```

- Configuration file of P

```

#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 172.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 172.2.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 172.1.1.0 0.0.0.255
network 172.2.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return

```

- Configuration file of PE2

```

#
sysname PE2
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 200:1

```

```

vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpnb
 ipv4-family
  route-distinguisher 200:2
  vpn-target 222:2 export-extcommunity
  vpn-target 222:2 import-extcommunity
#
  mpls lsr-id 3.3.3.9
  mpls
    lsp-trigger all
#
mpls ldp
#
interface GigabitEthernet1/0/0
  undo shutdown
  ip binding vpn-instance vpna
  ip address 10.3.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
  undo shutdown
  ip binding vpn-instance vpnb
  ip address 10.4.1.2 255.255.255.0
#
interface Pos3/0/0
  link-protocol ppp
  undo shutdown
  ip address 172.2.1.2 255.255.255.0
  mpls
  mpls ldp
#
interface LoopBack1
  ip address 3.3.3.9 255.255.255.255
#
bgp 100
  peer 1.1.1.9 as-number 100
  peer 1.1.1.9 connect-interface LoopBack1
  #
  ipv4-family unicast
    undo synchronization
    peer 1.1.1.9 enable
  #
  ipv4-family vpngv4
    policy vpn-target
    peer 1.1.1.9 enable
  #
  ipv4-family vpn-instance vpna
    peer 10.3.1.1 as-number 65430
    import-route direct
  #
  ipv4-family vpn-instance vpnb
    peer 10.4.1.1 as-number 65440
    import-route direct
  #
ospf 1
  area 0.0.0.0
  network 172.2.1.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
return

```

- Configuration file of CE1

```

#
sysname CE1
#
interface GigabitEthernet1/0/0
  undo shutdown
  ip address 10.1.1.1 255.255.255.0
#

```

```
bgp 65410
  peer 10.1.1.2 as-number 100
  #
  ipv4-family unicast
    undo synchronization
    import-route direct
    peer 10.1.1.2 enable
  #
  return
```

- Configuration file of CE2

```
#
  sysname CE2
#
interface GigabitEthernet1/0/0
  undo shutdown
  ip address 10.2.1.1 255.255.255.0
#
bgp 65420
  peer 10.2.1.2 as-number 100
  #
  ipv4-family unicast
    undo synchronization
    import-route direct
    peer 10.2.1.2 enable
  #
  return
```

- Configuration file of CE3

```
#
  sysname CE3
#
interface GigabitEthernet1/0/0
  undo shutdown
  ip address 10.3.1.1 255.255.255.0
#
bgp 65430
  peer 10.3.1.2 as-number 100
  #
  ipv4-family unicast
    undo synchronization
    import-route direct
    peer 10.3.1.2 enable
  #
  return
```

- Configuration file of CE4

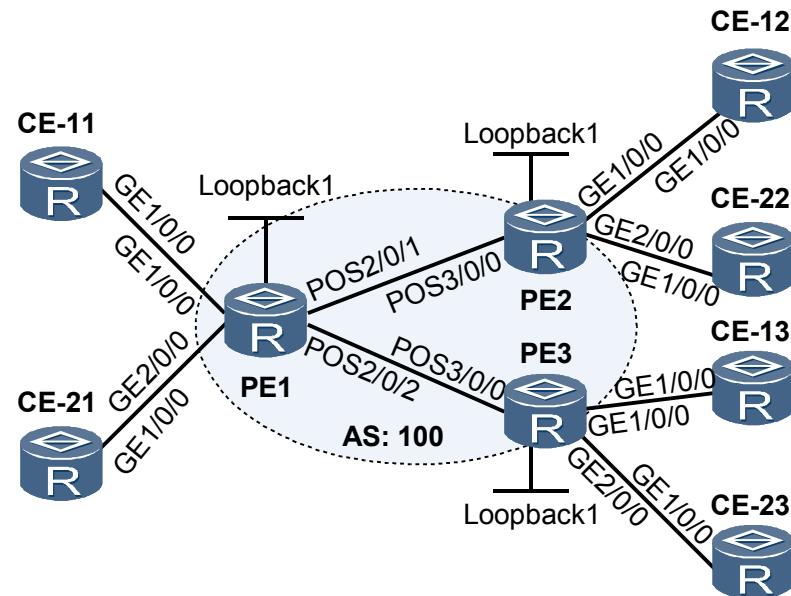
```
#
  sysname CE4
#
interface GigabitEthernet1/0/0
  undo shutdown
  ip address 10.4.1.1 255.255.255.0
#
bgp 65440
  peer 10.4.1.2 as-number 100
  #
  ipv4-family unicast
    undo synchronization
    import-route direct
    peer 10.4.1.2 enable
  #
  return
```

6.11.2 Example for Configuring BGP/MPLS IP VPN QoS (TE Tunnel at the Network Side)

Networking Requirements

As shown in [Figure 6-3](#), both vpna and vpnb are deployed on PE1, PE2, and PE3. CE-11, CE-12, and CE-13 belong to vpna, whereas CE-21, CE-22, and CE-23 belong to vpnb. The public network uses TE tunnels that are not configured with bandwidth restriction to transport VPN traffic. To meet service requirements, bandwidth of traffic on the public network side of L3VPN must be restricted. VPN instance-based QoS needs to be configured to limit the peak bandwidth so that the overall volume of public network traffic from PE1 to PE2 and from PE1 to PE3 that belong to the same VPN does not exceed the configured peak bandwidth value.

[Figure 6-3](#) Networking diagram of configuring BGP/MPLS IP VPN QoS



Device	Interface	IP Address
CE-11	GE1/0/0	10.1.1.1/24
CE-21	GE1/0/0	10.2.1.1/24
PE1	Loopback1	1.1.1.9/32
	GE1/0/0	10.1.1.2/24
	GE2/0/0	10.2.1.2/24
	POS2/0/1	172.1.1.1/24
	POS2/0/2	172.2.1.1/24
CE-12	GE1/0/0	10.3.1.1/24
CE-22	GE1/0/0	10.4.1.1/24
PE2	Loopback1	2.2.2.9/32
	GE1/0/0	10.3.1.2/24
	GE2/0/0	10.4.1.2/24
	POS3/0/0	172.1.1.2/24
CE-13	GE1/0/0	10.5.1.1/24
CE-23	GE1/0/0	10.6.1.1/24
PE3	Loopback1	3.3.3.9/32

GE1/0/0	10.5.1.2/24
GE2/0/0	10.6.1.2/24
POS3/0/0	172.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure BGP/MPLS IP VPN.
2. Apply tunnel policies to VPNs so that VPN traffic is carried over TE tunnels.
3. Configure VPN instance-based QoS for vpna.
4. Configure VPN instance-based QoS for vpnb.

Data Preparation

To complete the configuration, you need the following data:

- VPN instance name, RD, and VPN target
- TE Tunnel policy name and TE tunnel interface
- Committed Information Rate for VPN instances
- Committed Burst Size for VPN instances

Procedure

Step 1 Configure IGP on the MPLS backbone network so that PEs can learn the loopback route of each other. In this example, Open Shortest Path First (OSPF) is used. For details, see the following configuration files.

After the configuration, run the **display ip routing-table protocol ospf** command on PEs. The result shows that PEs have learnt the loopback route of each other through OSPF.

```
<PE1> display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
-----
Public routing table : OSPF
    Destinations : 5          Routes : 5

OSPF routing table status :<Active>
    Destinations : 2          Routes : 2

    Destination/Mask      Proto  Pre  Cost          Flags NextHop      Interface
    2.2.2.9/32      OSPF   10    1              D  172.1.1.2      Pos2/0/1
    3.3.3.9/32      OSPF   10    1              D  172.2.1.2      Pos2/0/2

OSPF routing table status : <Inactive>
    Destinations : 3          Routes : 3

    Destination/Mask      Proto  Pre  Cost          Flags NextHop      Interface
    1.1.1.9/32      OSPF   10    0              1.1.1.9        LoopBack1
    172.1.1.0/24     OSPF   10    1              172.1.1.1        Pos2/0/1
    172.2.1.0/24     OSPF   10    1              172.2.1.1        Pos2/0/2
```

Step 2 Set up the MP IBGP peer relationship between PEs.

```
# Configure PE1.

[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface LoopBack1
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface LoopBack1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 2.2.2.9 enable
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

After the configuration, run the **display bgp vpnv4 all peer** command on PEs. The result shows that MP-IBGP peer relationship is in the **Established** state. Take the display on PE1 as an example.

```
<PE1> display bgp vpnv4 all peer

BGP local router ID : 172.2.1.1
Local AS number : 100
Total number of peers : 2                               Peers in established state : 2

Peer          V      AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv

2.2.2.9        4      100      52      47      0 00:36:04 Established  2
3.3.3.9        4      100      50      49      0 00:35:35 Established  0
```

Step 3 Configure MPLS and MPLS TE on the MPLS backbone and interfaces, and set up TE tunnels between PE1 and PE2, and between PE1 and PE3.

Configure MPLS and MPLS TE on the MPLS backbone and interfaces, and enable OSPF TE.

Configure PE1.

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] mpls te
[PE1-mpls] mpls rsvp-te
[PE1-mpls] mpls te cspf
[PE1-mpls] quit
[PE1] interface pos2/0/1
[PE1-Pos2/0/1] mpls
[PE1-Pos2/0/1] mpls te
[PE1-Pos2/0/1] mpls rsvp-te
[PE1-Pos2/0/1] quit
[PE1] interface pos2/0/2
[PE1-Pos2/0/2] mpls
[PE1-Pos2/0/2] mpls te
[PE1-Pos2/0/2] mpls rsvp-te
[PE1-Pos2/0/2] quit
[PE1] ospf 1
[PE1-ospf-1] opaque-capability enable
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] mpls-te enable
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

Set up TE tunnels on PEs so that VPN traffic is carried over TE tunnels.

Configure PE1.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
```

```
[PE1-Tunnel1/0/0] ip address unnumbered interface LoopBack1
[PE1-Tunnel1/0/0] destination 2.2.2.9
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
[PE1-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[PE1-Tunnel1/0/0] mpls te commit
[PE1-Tunnel1/0/0] quit
[PE1] interface tunnel 2/0/0
[PE1-Tunnel2/0/0] tunnel-protocol mpls te
[PE1-Tunnel2/0/0] ip address unnumbered interface LoopBack1
[PE1-Tunnel2/0/0] destination 3.3.3.9
[PE1-Tunnel2/0/0] mpls te tunnel-id 200
[PE1-Tunnel2/0/0] mpls te signal-protocol rsvp-te
[PE1-Tunnel2/0/0] mpls te commit
[PE1-Tunnel2/0/0] quit
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

After the configuration, run the **display interface tunnel** command on PEs to check whether TE tunnels are set up. If the status of the TE tunnel is Up, it indicates that a TE tunnel has been set up. Take the display on PE1 as an example.

```
<PE1> display interface Tunnel1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2009-09-28 13:28:51

Description:HUAWEI, Tunnel1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack1.1.1.9.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 2.2.2.9
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x2008005, secondary tunnel id is 0x0
    300 seconds output rate 0 bits/sec, 0 packets/sec
    64 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output, 0 bytes
    0 output error
```

Step 4 Configure VPN instances on PEs to connect CEs to PEs.

Configure PE1.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] route-distinguisher 100:2
[PE1-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 both
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] ip binding vpn-instance vpna
[PE1-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] ip binding vpn-instance vpnb
[PE1-GigabitEthernet2/0/0] ip address 10.2.1.2 24
[PE1-GigabitEthernet2/0/0] quit
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] ipv4-family vpn-instance vpnb
```

```
[PE1-bgp-vpnbg] import-route direct
[PE1-bgp-vpnbg] quit
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

Step 5 Apply tunnel policies to VPNs so that VPN traffic is carried over TE tunnels.

Configure PE1.

```
[PE1] tunnel-policy p1
[PE1-tunnel-policy-p1] tunnel select-seq cr-lsp load-balance-number 1
[PE1-tunnel-policy-p1] quit
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] tnl-policy p1
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] tnl-policy p1
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

Step 6 Configure VPN instance-based QoS for VPNs.

Configure the CIR and CBS of vpna to be 5000 kbit/s and 8000 kbit/s respectively.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] qos cir 5000 pir 8000
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
```

Configure the CIR and CBS of vpnb to be 3000 kbit/s and 8000 kbit/s respectively.

```
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] qos cir 3000 pir 8000
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
```

After the configuration, run the **display ip vpn-instance verbose** command on PEs to view the QoS configurations of the VPN instance. Take the display on PE1 as an example.

```
<PE1> display ip vpn-instance verbose vpna
VPN-Instance Name and ID : vpna, 1
Address family ipv4
Create date : 2009/09/28 14:25:19
Up time : 0 days, 00 hours, 21 minutes and 57 seconds
Route Distinguisher : 100:1
Export VPN Targets : 111:1
Import VPN Targets : 111:1
Label Policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe
The VPN QoS configuration information : based on VPN
CIR: 5000 PIR: 8000
Tunnel Policy : p1
Log Interval : 5
Interfaces : GigabitEthernet1/0/0
```

Step 7 Verify the configuration.

Run the **display tcm sub-tunnel-info l3vpn** command on PEs to view information about the sub-tunnels that carry L3VPN traffic. Take the display on PE1 as an example.

```
<PE1> display tcm sub-tunnel-info 13vpn
-----
                                         Sub-tunnel information: TE sub-tunnel
-----
Sub-tunnel Type      : TE
Sub-Tunnel ID        : 0xc2060402
Qos Token            : 0x80014000
Backup Qos Token     : 0x80014001
Tunnel-interface   : Tunnel1/0/0
Indirect ID          : 0x2
N-Key                 : 0x1
CIR Value          : 5000
PIR Value          : 8000
Qos Profile Name     : ---
VPN Qos Type       : Base on VPN
VPN Type              : L3VPN
VPN Name              : vpna
Peer IP               : 2.2.2.9
Time Stamp             : 98872

Sub-tunnel Type      : TE
Sub-Tunnel ID        : 0xc2060403
Qos Token            : 0x80014002
Backup Qos Token     : 0x80014003
Tunnel-interface   : Tunnel1/0/0
Indirect ID          : 0x3
N-Key                 : 0x1
CIR Value          : 3000
PIR Value          : 8000
Qos Profile Name     : ---
VPN Qos Type       : Base on VPN
VPN Type              : L3VPN
VPN Name              : vpnb
Peer IP               : 2.2.2.9
Time Stamp             : 98878

Sub-tunnel Type      : TE
Sub-Tunnel ID        : 0xc4060404
Qos Token            : 0x80014004
Backup Qos Token     : 0x80014005
Tunnel-interface   : Tunnel12/0/0
Indirect ID          : 0x5
N-Key                 : 0x4
CIR Value          : 5000
PIR Value          : 8000
Qos Profile Name     : ---
VPN Qos Type       : Base on VPN
VPN Type              : L3VPN
VPN Name              : vpna
Peer IP               : 3.3.3.9
Time Stamp             : 98890

Sub-tunnel Type      : TE
Sub-Tunnel ID        : 0xc4060405
Qos Token            : 0x80014006
Backup Qos Token     : 0x80014007
Tunnel-interface   : Tunnel12/0/0
Indirect ID          : 0x6
N-Key                 : 0x4
CIR Value          : 3000
PIR Value          : 8000
Qos Profile Name     : ---
VPN Qos Type       : Base on VPN
VPN Type              : L3VPN
VPN Name              : vpnb
Peer IP               : 3.3.3.9
Time Stamp             : 98896
```

The preceding information shows that the QoS-enabled VPN traffic is carried over TE tunnels, and that the traffic of vpna and vpnb bound for the same peer PE is carried on the same primary TE tunnel.

Run the **display tcm statistics tunnel-interface** command to view statistics on sub-tunnels on the TE tunnel that carry QoS-enabled traffic. Take the display on PE1 as an example.

```
<PE1> display tcm statistics tunnel-interface Tunnel 1/0/0
    Tunnel-interface : Tunnel1/0/0
    Sub-tunnel Num With Qos : 2
    Sub-tunnel Num Without Qos : 0
    Total Used CIR(kbps) : 8000
<PE1> display tcm statistics tunnel-interface Tunnel 2/0/0
    Tunnel-interface : Tunnel2/0/0
    Sub-tunnel Num With Qos : 2
    Sub-tunnel Num Without Qos : 0
    Total Used CIR(kbps) : 8000
```

----End

Configuration Files

- Configuration file of CE-11

```
#           sysname CE-11
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 10.1.1.1 255.255.255.0
#
return
```

- Configuration file of CE-12.

```
#           sysname CE-12
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 10.2.1.1 255.255.255.0
#
return
```

- Configuration file of PE1

```
#           sysname PE1
#
ip vpn-instance vpna
    ipv4-family
        route-distinguisher 100:1
        tnl-policy p1
        vpn-target 111:1 export-extcommunity
        vpn-target 111:1 import-extcommunity
        qos cir 5000 pir 8000
ip vpn-instance vpnb
    ipv4-family
        route-distinguisher 200:1
        tnl-policy p1
        vpn-target 222:2 export-extcommunity
        vpn-target 222:2 import-extcommunity
        qos cir 3000 pir 8000
#
    mpls lsr-id 1.1.1.9
    mpls
        mpls te
        mpls rsvp-te
```

```
mpls te cspf
#
interface GigabitEthernet1/0/0
undo shutdown
ip binding vpn-instance vpna
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip binding vpn-instance vpnb
ip address 10.2.1.2 255.255.255.0
#
interface Pos2/0/1
undo shutdown
ip address 172.1.1.1 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface Pos2/0/2
undo shutdown
ip address 172.2.1.1 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 2.2.2.9
mpls te tunnel-id 100
mpls te commit
#
interface Tunnel2/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.9
mpls te tunnel-id 200
mpls te commit
#
tunnel-policy p1
tunnel select-seq cr-lsp load-balance-number 1
#
bgp 100
peer 2.2.2.9 as-number 100
peer 2.2.2.9 connect-interface LoopBack1
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 2.2.2.9 enable
peer 3.3.3.9 enable
#
ipv4-family vpng4
policy vpn-target
peer 2.2.2.9 enable
peer 3.3.3.9 enable
#
ipv4-family vpn-instance vpna
import-route direct
#
ipv4-family vpn-instance vpnb
import-route direct
#
ospf 1
```

```
opaque-capability enable
area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 172.2.1.0 0.0.0.255
  mpls-te enable
#
return

● Configuration file of PE2

#
  sysname PE2
#
  ip vpn-instance vpna
    ipv4-family
      route-distinguisher 100:1
      tnl-policy p1
      vpn-target 111:1 export-extcommunity
      vpn-target 111:1 import-extcommunity
      qos cir 5000 pir 8000
  ip vpn-instance vpnb
    ipv4-family
      route-distinguisher 200:1
      tnl-policy p1
      vpn-target 222:2 export-extcommunity
      vpn-target 222:2 import-extcommunity
      qos cir 3000 pir 8000
#
  mpls lsr-id 2.2.2.9
  mpls
    mpls te
    mpls rsvp-te
    mpls te cspf
#
  interface GigabitEthernet1/0/0
    undo shutdown
    ip binding vpn-instance vpna
    ip address 10.3.1.2 255.255.255.0
#
  interface GigabitEthernet2/0/0
    undo shutdown
    ip binding vpn-instance vpnb
    ip address 10.4.1.2 255.255.255.0
#
  interface Pos3/0/0
    undo shutdown
    ip address 172.1.1.2 255.255.255.0
    mpls
    mpls te
    mpls rsvp-te
#
  interface LoopBack1
    ip address 2.2.2.9 255.255.255.255
#
  interface Tunnel1/0/0
    ip address unnumbered interface LoopBack1
    tunnel-protocol mpls te
    destination 1.1.1.9
    mpls te tunnel-id 100
    mpls te commit
#
  tunnel-policy p1
    tunnel select-seq cr-lsp load-balance-number 1
#
  bgp 100
    peer 1.1.1.9 as-number 100
    peer 1.1.1.9 connect-interface LoopBack1
#
    ipv4-family unicast
```

```
undo synchronization
peer 1.1.1.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 1.1.1.9 enable
#
ipv4-family vpn-instance vpna
import-route direct
#
ipv4-family vpn-instance vpnb
import-route direct
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 172.1.1.0 0.0.0.255
mpls-te enable
#
return
```

- Configuration file of CE-21

```
#
sysname CE-21
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.3.1.1 255.255.255.0
#
return
```

- Configuration file of CE-22

```
#
sysname CE-22
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.4.1.1 255.255.255.0
#
return
```

- Configuration file of PE3

```
#
sysname PE3
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 100:1
tnl-policy p1
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
qos cir 5000 pir 8000
ip vpn-instance vpnb
ipv4-family
route-distinguisher 200:1
tnl-policy p1
vpn-target 222:2 export-extcommunity
vpn-target 222:2 import-extcommunity
qos cir 3000 pir 8000
#
mpls lsr-id 3.3.3.9
mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface GigabitEthernet1/0/0
```

```
undo shutdown
ip binding vpn-instance vpna
ip address 10.5.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip binding vpn-instance vpnb
ip address 10.6.1.2 255.255.255.0
#
interface Pos3/0/0
undo shutdown
ip address 172.2.1.2 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.9
mpls te tunnel-id 100
mpls te commit
#
tunnel-policy p1
tunnel select-seq cr-lsp load-balance-number 1
#
bgp 100
peer 1.1.1.9 as-number 100
peer 1.1.1.9 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 1.1.1.9 enable
#
ipv4-family vpng4
policy vpn-target
peer 1.1.1.9 enable
#
ipv4-family vpn-instance vpna
import-route direct
#
ipv4-family vpn-instance vpnb
import-route direct
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 172.2.1.0 0.0.0.255
mpls-te enable
#
return
```

- Configuration file of CE-13

```
#
sysname CE-13
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.5.1.1 255.255.255.0
#
return
```

- Configuration file of CE-23

```
#
```

```

sysname CE-23
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.6.1.1 255.255.255.0
#
return

```

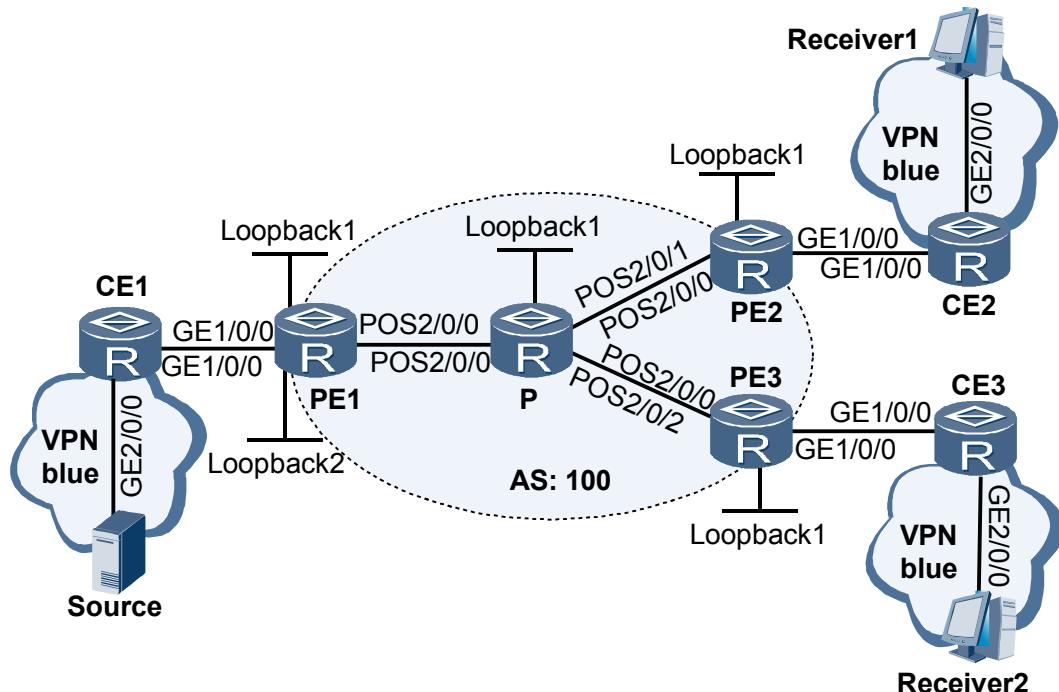
6.11.3 Example for Configuring MVPN QoS

Networking Requirements

MVPN QoS needs to be configured on PEs to implement traffic policing and bandwidth restriction on multicast traffic that reaches the network side. After the configuration, multicast traffic can be forwarded at a rate not higher than the configured CIR.

As shown in **Figure 6-4**, a multicast source is connected to CE1. Each of CE2 and CE3 has a multicast traffic receiver. PEs are connected to the same VPN instance, forming a multicast domain (MD). MVPN QoS needs to be configured on PE1 so that traffic is sent from the source to the receiver at a rate not higher than the configured peak bandwidth value.

Figure 6-4 Networking diagram for configuring MVPN QoS



Device	Interface	IP address
CE1	GE1/0/0	192.168.10.2/24
	GE2/0/0	192.168.40.1/24
PE1	Loopback1	1.1.1.1/32
	Loopback2	8.8.8.8/32
	GE1/0/0	192.168.10.1/24
	POS2/0/0	10.1.1.1/24
P	Loopback1	4.4.4.4/32
	POS2/0/0	10.1.1.2/24

	POS2/0/1	20.1.1.1/24
	POS2/0/2	30.1.1.1/24
CE2	GE1/0/0	192.168.20.2/24
	GE2/0/0	192.168.50.1/24
PE2	Loopback1	2.2.2.2/32
	GE1/0/0	192.168.20.1/24
	POS2/0/0	20.1.1.2/24
CE3	GE1/0/0	192.168.30.2/24
	GE2/0/0	192.168.60.1/24
PE3	Loopback1	3.3.3.3/32
	GE1/0/0	192.168.30.1/24
	POS2/0/0	30.1.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a unicast BGP/MPLS VPN. Ensure that the VPN network works normally and unicast routes are reachable.
2. Enable multicast and Protocol Independent Multicast (PIM) globally. VPN multicast traffic is forwarded from CEs to PEs. Then, PEs forward the VPN multicast traffic to the public network.
3. Configure identical share-group address, MTI, and switch-address-pool range of Switch-MDT for the same VPN instance on each PE.
4. Configure the MTI address of each PE as the IBGP peer interface address on the public network, and enable PIM on the MTI.
5. Configure MVPN QoS to restrict the total bandwidth for MVPN traffic.

Data Preparation

To complete the configuration, you need the following data:

- MVPN instance name, RD, and VPN target
- Share-group address, switch-group address, and MTI interface number
- CIR for MVPN instances
- CBS for MVPN instances

Procedure

- Step 1** Configure IGP on the MPLS backbone network so that PEs can learn the loopback route of each other. In this example, Open Shortest Path First (OSPF) is used. For details, see the following configuration files.

After the configuration, run the **display ip routing-table** command on PE1. The result shows that PEs have learnt the loopback route of each other through OSPF.

```
[PE1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
```

Destinations : 13			Routes : 13			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
2.2.2.2/32	OSPF	10	2	D	10.1.1.2	Pos2/0/0
3.3.3.3/32	OSPF	10	2	D	10.1.1.2	Pos2/0/0
4.4.4.4/32	OSPF	10	1	D	10.1.1.2	Pos2/0/0
10.1.1.0/24	Direct	0	0	D	10.1.1.1	Pos2/0/0
10.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.1.1.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
20.1.1.0/24	OSPF	10	2	D	10.1.1.2	Pos2/0/0
30.1.1.0/24	OSPF	10	2	D	10.1.1.2	Pos2/0/0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

Step 2 Set up MP-IBGP peer relationships between PEs.

Configure PE1.

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.2 as-number 100
[PE1-bgp] peer 2.2.2.2 connect-interface LoopBack1
[PE1-bgp] peer 3.3.3.3 as-number 100
[PE1-bgp] peer 3.3.3.3 connect-interface LoopBack1
[PE1-bgp] ipv4-family vpng4
[PE1-bgp-af-vpng4] peer 2.2.2.2 enable
[PE1-bgp-af-vpng4] peer 3.3.3.3 enable
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

After the configuration, run the **display bgp vpng4 all peer** command on PEs. The result shows that MP-IBGP peer relationship is in the **Established** state. Take the display on PE1 as an example.

```
<PE1> display bgp vpng4 all peer

BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 2                               Peers in established state : 2

Peer          V      AS  MsgRcvd  MsgSent  OutQ  Up/Down       State
PrefRcv

2.2.2.2        4     100      52      47      0 00:36:04 Established  2
3.3.3.3        4     100      50      49      0 00:35:35 Established  2
```

Step 3 Enable MPLS and MPLS LDP on the MPLS backbone so that LDP LSP sessions are established between PEs.

Configure PE1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos2/0/0
[PE1-Pos2/0/0] mpls
[PE1-Pos2/0/0] mpls ldp
[PE1-Pos2/0/0] quit
```

The configurations of PE2, PE3, and P are the same as the configuration of PE1, and are not mentioned here.

After the configuration, run the **display mpls ldp session** command on PEs. The result shows that the status of the LDP session is **Operational**.

```
<PE1> display mpls ldp session
LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
A '*' before a session means the session is being deleted.
-----
PeerID          Status      LAM  SsnRole   SsnAge      KASent/Rcv
-----
4.4.4.4:0       Operational DU   Passive   0000:00:50  201/201
-----
TOTAL: 1 session(s) Found.
```

Step 4 Configure VPN instances on PEs to connect CEs to PEs.

Create VPN instances on PEs and bind the VPN instances to private network interfaces.

Configure PE1.

```
[PE1] ip vpn-instance blue
[PE1-vpn-instance-blue] ipv4-family
[PE1-vpn-instance-blue-af-ipv4] route-distinguisher 100:1
[PE1-vpn-instance-blue-af-ipv4] vpn-target 100:1 both
[PE1-vpn-instance-blue-af-ipv4] quit
[PE1-vpn-instance-blue] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] ip binding vpn-instance blue
[PE1-GigabitEthernet1/0/0] ip address 192.168.10.1 24
[PE1-GigabitEthernet1/0/0] quit
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

Configure RIP multi-instances on PEs to exchange routes between PEs and CEs.

Configure PE1.

```
[PE1] rip 2 vpn-instance blue
[PE1-rip-2] network 192.168.10.0
[PE1-rip-2] import-route bgp cost 3
[PE1-rip-2] quit
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance blue
[PE1-bgp-blue] import-route rip 2
[PE1-bgp-blue] import-route direct
[PE1-bgp-blue] quit
[PE1-bgp] quit
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

Configure CE1.

```
[CE1] rip 2
[CE1-rip-2] network 192.168.10.0
[CE1-rip-2] network 192.168.40.0
[CE1-rip-2] import-route direct
```

The configurations of CE2 and CE3 are the same as the configuration of CE1, and are not mentioned here.

After the configuration, CEs can ping through each other. This indicates that the unicast BGP/MPLS VPN has been established.

Step 5 Enable multicast globally and enable and PIM Sparse Mode (PIM-SM) on interfaces.

Configure PE1.

```
[PE1] multicast routing-enable
[PE1] interface pos 2/0/0
[PE1-Pos2/0/0] pim sm
[PE1-Pos2/0/0] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] pim sm
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

The configurations of PE2, PE3, and P are the same as the configuration of PE1, and are not mentioned here.

Configure CE1.

```
[CE1] multicast routing-enable
[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] ip address 192.168.10.2 24
[CE1-GigabitEthernet1/0/0] pim sm
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 2/0/0
[CE1-GigabitEthernet2/0/0] ip address 192.168.40.1 24
[CE1-GigabitEthernet2/0/0] pim sm
[CE1-GigabitEthernet2/0/0] quit
```

The configurations of CE2 and CE3 are the same as the configuration of CE1, and are not mentioned here.

Configure loopback1 on P as the C-BSR and C-RP for the public network.

```
[P] pim
[P-pim] c-bsr loopback1
[P-pim] c-rp loopback1
[P-pim] quit
```

Configure loopback2 on PE1 as the C-BSR and C-RP for VPNA blue.

```
[PE1] interface loopback2
[PE1-Loopback2] ip binding vpn-instance blue
[PE1-Loopback2] ip address 8.8.8.8 32
[PE1-Loopback2] pim sm
[PE1-Loopback2] quit
[PE1] pim vpn-instance blue
[PE1-pim-blue] c-bsr loopback2
[PE1-pim-blue] c-rp loopback2
[PE1-pim-blue] quit
```

Step 6 Configure share-group addresses and switch-group addresses for MVPN.

Configure PE1.

```
[PE1] ip vpn-instance blue
[PE1-vpn-instance-blue] ipv4-family
[PE1-vpn-instance-blue-af-ipv4] multicast routing-enable
[PE1-vpn-instance-blue-af-ipv4] multicast-domain share-group 239.1.1.1 binding
mtunnel 0
[PE1-vpn-instance-blue-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28
[PE1-vpn-instance-blue-af-ipv4] quit
[PE1-vpn-instance-blue] quit
[PE1] interface mtunnel 0
[PE1-MTunnel0] ip address 1.1.1.1 32
[PE1-MTunnel0] pim sm
[PE1-MTunnel0] quit
```

The configurations of PE2 and PE3 are the same as the configuration of PE1, and are not mentioned here.

Step 7 Configure MVPN QoS to restrict the total bandwidth for MVPN traffic.

Configure the CIR and CBS of MVPN to be 5000 kbit/s and 8000 kbit/s respectively.

```
[PE1] ip vpn-instance blue
[PE1-vpn-instance-blue-af-ipv4] ipv4-family
[PE1-vpn-instance-blue-af-ipv4] qos cir 5000 pir 8000
[PE1-vpn-instance-blue-af-ipv4] quit
[PE1-vpn-instance-blue] quit
```

After the configuration, run the **display ip vpn-instance verbose** command on PEs to view the QoS configurations of the VPN instance. Take the display on PE1 as an example.

```
<PE1> display ip vpn-instance verbose blue
VPN-Instance Name and ID : blue, 2
Address family ipv4
Create date : 2009/10/09 20:18:41
Up time : 0 days, 01 hours, 33 minutes and 11 seconds
Route Distinguisher : 100:1
Export VPN Targets : 100:1
Import VPN Targets : 100:1
Label Policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe
The VPN QoS configuration information : based on VPN
CIR: 5000 PIR: 8000
Log Interval : 5
Interfaces : MTunnel0
GigabitEthernet1/0/0
```

Step 8 Verify the configuration.

After the preceding configurations, Receiver 1 and Receiver 2 can receive multicast traffic from Source. When Source sends traffic at a rate higher than 8000 kbit/s, the data that reaches the receivers is incomplete. That is, some data is discarded.

----End

Configuration Files

- Configuration file of CE1

```
# 
sysname CE1
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 192.168.10.2 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 192.168.40.1 255.255.255.0
pim sm
#
rip 2
network 192.168.10.0
network 192.168.40.0
import-route direct
#
return
```

- Configuration file of PE1

```
# 
sysname PE1
#
router id 1.1.1.1
```

```
#  
multicast routing-enable  
#  
multicast-vpn slot 4  
#  
mpls lsr-id 1.1.1.1  
mpls  
#  
mpls ldp  
#  
ip vpn-instance blue  
ipv4-family  
route-distinguisher 100:1  
vpn-target 100:1 export-extcommunity  
vpn-target 100:1 import-extcommunity  
multicast routing-enable  
multicast-domain share-group 239.1.1.1 binding MTunnel 0  
multicast-domain switch-group-pool 225.2.2.0 255.255.255.240  
#  
interface Pos2/0/0  
undo shutdown  
ip address 10.1.1.1 255.255.255.0  
pim sm  
mpls  
mpls ldp  
#  
interface GigabitEthernet1/0/0  
undo shutdown  
ip binding vpn-instance blue  
ip address 192.168.10.1 255.255.255.0  
pim sm  
#  
interface LoopBack1  
ip address 1.1.1.1 255.255.255.255  
pim sm  
#  
interface LoopBack2  
ip address 8.8.8.8 255.255.255.255  
pim sm  
#  
pim vpn-instance blue  
c-bsr LoopBack2  
c-rp LoopBack2  
#  
interface MTunnel0  
ip binding vpn-instance blue  
ip address 1.1.1.1 255.255.255.255  
pim sm  
#  
bgp 100  
peer 2.2.2.2 as-number 100  
peer 2.2.2.2 connect-interface loopback1  
peer 3.3.3.3 as-number 100  
peer 3.3.3.3 connect-interface loopback1  
#  
ipv4-family unicast  
undo synchronization  
peer 2.2.2.2 enable  
peer 3.3.3.3 enable  
#  
ipv4-family vpnv4  
policy vpn-target  
peer 2.2.2.2 enable  
peer 3.3.3.3 enable  
#  
ipv4-family vpn-instance blue  
import-route rip 2  
import-route direct  
#
```

```
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 10.1.1.0 0.0.0.255
#
rip 2 vpn-instance blue
network 192.168.10.0
import-route bgp cost 3
#
return
```

- Configuration file of P

```
#
sysname P
#
multicast routing-enable
#
mpls lsr-id 4.4.4.4
mpls
#
mpls ldp
#
interface Pos2/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
pim sm
mpls
mpls ldp
#
interface Pos2/0/1
undo shutdown
ip address 20.1.1.1 255.255.255.0
pim sm
mpls
mpls ldp
#
interface Pos2/0/2
undo shutdown
ip address 30.1.1.1 255.255.255.0
pim sm
mpls
mpls ldp
#
interface LoopBack1
ip address 4.4.4.4 255.255.255.255
pim sm
#
pim
c-bsr Loopback1
c-rp Loopback1
#
ospf 1
area 0.0.0.0
network 4.4.4.4 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
#
return
```

- Configuration file of PE2

```
#
sysname PE2
#
router id 2.2.2.2
#
multicast routing-enable
#
multicast-vpn slot 4
#
```

```

mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
ip vpn-instance blue
 ipv4-family
 route-distinguisher 200:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
 multicast routing-enable
 multicast-domain share-group 239.1.1.1 binding MTunnel 0
 multicast-domain switch-group-pool 225.2.2.0 255.255.255.240
#
interface Pos2/0/0
 undo shutdown
 ip address 20.1.1.2 255.255.255.0
 pim sm
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip binding vpn-instance blue
 ip address 192.168.20.1 255.255.255.0
 pim sm
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface MTunnel0
 ip binding vpn-instance blue
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface loopback1
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface loopback1
#
ipv4-family unicast
 undo synchronization
 peer 1.1.1.1 enable
 peer 3.3.3.3 enable
#
ipv4-family vpng4
 policy vpn-target
 peer 1.1.1.1 enable
 peer 3.3.3.3 enable
#
ipv4-family vpn-instance blue
 import-route rip 2
 import-route direct
#
ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 20.1.1.0 0.0.0.255
#
rip 2 vpn-instance blue
 network 192.168.20.0
 import-route bgp cost 3
#
return
● Configuration file of CE2
#
sysname CE2

```

```
#  
    multicast routing-enable  
#  
interface GigabitEthernet1/0/0  
undo shutdown  
ip address 192.168.20.2 255.255.255.0  
pim sm  
#  
interface GigabitEthernet2/0/0  
undo shutdown  
ip address 192.168.50.1 255.255.255.0  
pim sm  
igmp enable  
#  
rip 2  
network 192.168.20.0  
network 192.168.50.0  
import-route direct  
#  
return
```

- Configuration file of PE3

```
#  
    sysname PE3  
#  
    router id 3.3.3.3  
#  
    multicast routing-enable  
#  
multicast-vpn slot 4  
#  
mpls lsr-id 3.3.3.3  
mpls  
#  
mpls ldp  
#  
ip vpn-instance blue  
ipv4-family  
route-distinguisher 300:1  
vpn-target 100:1 export-extcommunity  
vpn-target 100:1 import-extcommunity  
multicast routing-enable  
multicast-domain share-group 239.1.1.1 binding MTunnel 0  
multicast-domain switch-group-pool 225.2.2.0 255.255.255.240  
#  
interface Pos2/0/0  
undo shutdown  
ip address 30.1.1.2 255.255.255.0  
pim sm  
mpls  
mpls ldp  
#  
interface GigabitEthernet1/0/0  
undo shutdown  
ip binding vpn-instance blue  
ip address 192.168.30.1 255.255.255.0  
pim sm  
#  
interface LoopBack1  
ip address 3.3.3.3 255.255.255.255  
pim sm  
#  
interface MTunnel0  
ip binding vpn-instance blue  
ip address 3.3.3.3 255.255.255.255  
pim sm  
#  
bgp 100  
peer 1.1.1.1 as-number 100  
peer 1.1.1.1 connect-interface loopback1
```

```

peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface loopback1
#
ipv4-family unicast
undo synchronization
peer 1.1.1.1 enable
peer 2.2.2.2 enable
#
ipv4-family vpnv4
policy vpn-target
peer 1.1.1.1 enable
peer 2.2.2.2 enable
#
ipv4-family vpn-instance blue
import-route rip 2
import-route direct
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 30.1.1.0 0.0.0.255
#
rip 2 vpn-instance blue
network 192.168.30.0
import-route bgp cost 3
#
return

```

- Configuration file of CE3

```

#
sysname CE3
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 192.168.30.2 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 192.168.60.1 255.255.255.0
pim sm
igmp enable
#
rip 2
network 192.168.30.0
network 192.168.60.0
import-route direct
#
return

```

6.11.4 Example for Configuring VLL QoS

This part describes how to configure VLL QoS to provide QoS handling in terms of bandwidth allocation and resource usage on an L2VPN.

Networking Requirements

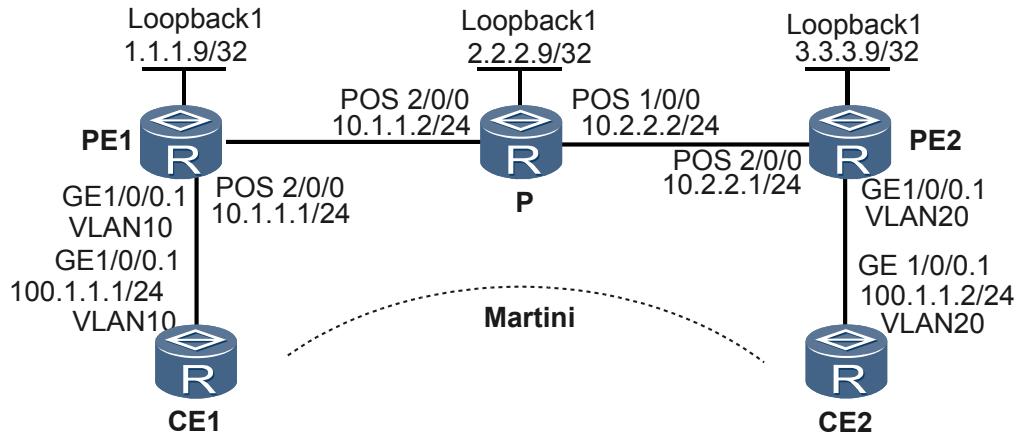
As shown in [Figure 6-5](#), CE1 and CE2 are connected to PE1 and PE2 respectively through VLANs.

A Martini VLL is set up between CE1 and CE2.

To meet the QoS requirements for the VLL, traffic policing needs to be implemented on the incoming traffic at the user side of PE2 to limit the bandwidth. The CIR for traffic going from CE2 to CE1 should be 2000 kbit/s, and the PIR should be 3000 kbit/s.

Congestion avoidance and flow queue scheduling need to be carried out in the event of congestion. That is, when congestion occurs, packets should be dropped according to the WRED discard parameters configured for flow queues. The traffic shaping rates of flow queues AF1 and EF are 500 kbit/s and 1000 kbit/s respectively, and the traffic of flow queue AF1 is mapped to class queue EF.

Figure 6-5 Networking diagram for configuring Martini VLL



Configuration Roadmap

The configuration roadmap is as follows:

1. On the backbone devices (PEs and the P), configure a routing protocol to achieve connectivity and enable MPLS.
2. Use the default tunnel policy to set up LSPs for transmitting user data.
3. Enable MPLS L2VPN on PEs and establish VCs.
4. Configure VLAN sub-interfaces on PEs so that CEs can access PEs through VLANs.
5. Configure the QoS-profile and the scheduling parameters.
6. Configure QoS parameters on sub-interface GE 1/0/0.1 on PE2.

Data Preparation

To complete the configuration, you need the following data:

- VLAN sub-interface numbers
- Name of each remote PE peer
- VC ID
- The parameters of flow-wred, flow-queue, and the value of network-header-length in the QoS-profile
- CIR
- PIR

Procedure

Step 1 Configure CEs.

Configure CE1.

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] undo shutdown
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 1/0/0.1
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE1-GigabitEthernet1/0/0.1] ip address 100.1.1.1 24
[CE1-GigabitEthernet1/0/0.1] quit
```

Configure CE2.

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface gigabitethernet 1/0/0
[CE2-GigabitEthernet1/0/0] undo shutdown
[CE2-GigabitEthernet1/0/0] quit
[CE2] interface gigabitethernet 1/0/0.1
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 20
[CE2-GigabitEthernet1/0/0.1] ip address 100.1.1.2 24
[CE2-GigabitEthernet1/0/0.1] quit
```

Step 2 Configure IGP on the MPLS backbone. In this example, OSPF is adopted.

As shown in [Figure 6-5](#), configure IP addresses for interfaces on PEs and the P. Note that when configuring OSPF, IP addresses with 32-bit masks of loopback interfaces of PE1, the P, and PE2, which are used as LSR IDs, should be advertised.

The configuration details are not mentioned here.

After the configuration, OSPF neighbor relationship should have been set up between PE1, P, and PE2. Run the **display ospf peer** command, and you can view that the neighbor status is Full. Run the **display ip routing-table** command, and you can view that the PEs learn from each other the route to each other's loopback1 interface.

Step 3 Configure the basic MPLS capability and LDP on the MPLS backbone.

Configure PE1.

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos 2/0/0
[PE1-Pos2/0/0] mpls
[PE1-Pos2/0/0] mpls ldp
[PE1-Pos2/0/0] quit
```

Configure the P.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface pos 1/0/0
[P-Pos1/0/0] mpls
[P-Pos1/0/0] mpls ldp
[P-Pos1/0/0] quit
[P] interface pos 2/0/0
```

```
[P-Pos2/0/0] mpls
[P-Pos2/0/0] mpls ldp
[P-Pos2/0/0] quit

# Configure PE2.

[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos 2/0/0
[PE2-Pos2/0/0] mpls
[PE2-Pos2/0/0] mpls ldp
[PE2-Pos2/0/0] quit
```

Step 4 Establish remote LDP sessions between PEs.

Configure PE1.

```
[PE1] mpls ldp remote-peer 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] quit
```

Configure PE2.

```
[PE2] mpls ldp remote-peer 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] remote-ip 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] quit
```

After the preceding configurations, run the **display mpls ldp session** command on PE1 to view how LDP sessions are established. You can find that remote LDP sessions with PE2 are established on PE1.

Take the display on PE1 as an example.

```
<PE1> display mpls ldp session
      LDP Session(s) in Public Network
-----
Peer-ID          Status       LAM   SsnRole   SsnAge      KA-Sent/Rcv
-----
2.2.2.9:0        Operational DU    Passive  000:00:09  40/40
3.3.3.9:0        Operational DU    Passive  000:00:09  37/37
-----
TOTAL: 2 session(s) Found.
      LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Step 5 Enable MPLS L2VPN on PEs and establish VCs.

Configure PE1: create a VC on GE 1/0/0.1 that connects PE1 to CE1.

```
[PE1] mpls 12vpn
[PE1-12vpn] mpls 12vpn default martini
[PE1-12vpn] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] undo shutdown
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 1/0/0.1
[PE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[PE1-GigabitEthernet1/0/0.1] mpls 12vc 3.3.3.9 101
[PE1-GigabitEthernet1/0/0.1] quit
```

Configure PE2: create a VC on GE 1/0/0.1 that connects PE2 to CE2.

```
[PE2] mpls 12vpn
[PE2-12vpn] mpls 12vpn default martini
[PE2-12vpn] quit
[PE2] interface gigabitethernet 1/0/0
[PE2-GigabitEthernet1/0/0] undo shutdown
```

```
[PE2-GigabitEthernet1/0/0] quit
[PE2] interface gigabitethernet 1/0/0.1
[PE2-GigabitEthernet1/0/0.1] vlan-type dot1q 20
[PE2-GigabitEthernet1/0/0.1] mpls 12vc 1.1.1.9 101
[PE2-GigabitEthernet1/0/0.1] quit
```

Step 6 Configure the QoS-profile and the scheduling parameters. See[Example for Configuring BGP/MPLS IP VPN QoS step 2.](#)

Step 7 Configure QoS policies on GE 1/0/0.1 on PE2 to ensure the bandwidth of VLL.

Configure QoS parameters.

```
[PE2] interface gigabitethernet 1/0/0.1
[PE2-GigabitEthernet1/0/0.1] mpls 12vpn qos cir 2000 pir 3000 qos-profile test
[PE2-GigabitEthernet1/0/0.1] quit
```

Enable traffic statistics of the VLL so that VLL traffic transmission can be easily viewed.

```
[PE2] interface gigabitethernet 1/0/0.1
[PE2-GigabitEthernet1/0/0.1] mpls 12vpn pw traffic-statistic enable
[PE2-GigabitEthernet1/0/0.1] quit
```

Step 8 Verify the configuration.

On PEs, check the L2VPN connections. You can find that an L2VC is set up and is in the Up state.

Take the display on PE21 as an example.

```
<PE2> display mpls 12vc interface gigabitethernet 1/0/0.1
*client interface      : GigabitEthernet1/0/0.1 is up
  session state       : up
  AC status           : up
  VC state            : up
  VC ID               : 101
  VC type             : VLAN
  destination         : 1.1.1.9
  local group ID     : 0          remote group ID   : 0
  local VC label      : 21504    remote VC label   : 21504
  local AC OAM State : up
  local PSN State     : up
  local forwarding state: forwarding
  remote AC OAM state: up
  remote PSN state   : up
  remote forwarding state: forwarding
  BFD for PW          : disable
  manual fault        : not set
  active state        : active
  forwarding entry    : exist
  link state          : up
  local VC MTU        : 1500     remote VC MTU     : 1500
  local VCCV          : Disable
  remote VCCV         : Disable
  local control word  : disable   remote control word : disable
  tunnel policy name  : --
  traffic behavior name: --
  PW template name   : --
  primary or secondary: primary
  VC tunnel/token info: 1 tunnels/tokens
    NO.0 TNL type : lsp , TNL ID : 0x2002003
    create time    : 0 days, 0 hours, 4 minutes, 19 seconds
    up time        : 0 days, 0 hours, 2 minutes, 40 seconds
    last change time: 0 days, 0 hours, 2 minutes, 40 seconds
  VC last up time : 2009/04/22 12:31:31
  VC total up time: 0 days, 2 hours, 12 minutes, 51 seconds
  CKey              : 2
  NKey              : 1
```

```
L2VPN QoS CIR value : 2000
L2VPN QoS PIR value : 3000
L2VPN QoS qos-profile name: test
```

CE1 and CE2 can ping through each other.

Take the display on CE1 as an example.

```
<CE1> ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=5 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=2 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=28 ms
--- 100.1.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 2/15/31 ms
```

View traffic statistics of the VLL.

```
<PE2> display traffic-statistics l2vpn pw interface gigabitethernet1/0/0.1
Interface name : GigabitEthernet 1/0/0.1
Statistics last cleared : never
Last 300 seconds QoS statistics rate : 0 bits/sec, 0 packets/sec
QoS statistics output : 0 bytes, 0 packets
PacketRate : Last 300 seconds packets rate(packets/sec)
ByteRate : Last 300 seconds bytes rate(bits/sec)
Queue Packets      Bytes      PacketRate   ByteRate
-----
be    0            0           0           0
af1   0            0           0           0
af2   0            0           0           0
af3   0            0           0           0
af4   0            0           0           0
ef    0            0           0           0
cs6   0            0           0           0
cs7   0            0           0           0
-----
Discarded traffic statistics :
Queue Packets      Bytes      PacketRate   ByteRate
-----
be    0            0           0           0
af1   0            0           0           0
af2   0            0           0           0
af3   0            0           0           0
af4   0            0           0           0
ef    0            0           0           0
cs6   0            0           0           0
cs7   0            0           0           0
-----
```

----End

Configuration Files

- Configuration file of CE1

```
#          sysname CE1
#
interface GigabitEthernet1/0/0
    undo shutdown
#
interface GigabitEthernet1/0/0.1
    vlan-type dot1q 10
    ip address 100.1.1.1 255.255.255.0
```

```
#  
return  


- Configuration file of PE1



```

 sysname PE1

 mpls lsr-id 1.1.1.9
 mpls

 mpls l2vpn
 mpls l2vpn default martini

 mpls ldp

 mpls ldp remote-peer 3.3.3.9
 remote-ip 3.3.3.9

interface GigabitEthernet1/0/0
 undo shutdown

interface GigabitEthernet1/0/0.1
 vlan-type dot1q 10
 mpls 12vc 3.3.3.9 101

interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp

interface LoopBack1
 ip address 1.1.1.9 255.255.255.255

ospf 1
 area 0.0.0.0
 network 1.1.1.9 0.0.0.0
 network 10.1.1.0 0.0.0.255

return
```


```

- Configuration file of the P

```
#  
    sysname P  
#  
    mpls lsr-id 2.2.2.9  
    mpls  
#  
    mpls ldp  
#  
interface Pos1/0/0  
    link-protocol ppp  
    undo shutdown  
    ip address 10.2.2.2 255.255.255.0  
    mpls  
    mpls ldp  
#  
interface Pos2/0/0  
    link-protocol ppp  
    undo shutdown  
    ip address 10.1.1.2 255.255.255.0  
    mpls  
    mpls ldp  
#  
interface LoopBack1  
    ip address 2.2.2.9 255.255.255.255  
#  
ospf 1  
    area 0.0.0.0
```

```
        network 2.2.2.9 0.0.0.0
        network 10.1.1.0 0.0.0.255
        network 10.2.2.0 0.0.0.255
#
return
```

- Configuration file of PE2

```
#           sysname PE2
#
#           mpls lsr-id 3.3.3.9
#           mpls
#
#           mpls l2vpn
#           mpls l2vpn default martini
#
#           mpls ldp
#
#           mpls ldp remote-peer 1.1.1.9
#           remote-ip 1.1.1.9
#
#           flow-wred test
#           color green low-limit 70 high-limit 100 discard-percentage 100
#           color yellow low-limit 60 high-limit 90 discard-percentage 100
#           color red low-limit 50 high-limit 80 discard-percentage 100
#
#           flow-mapping test
#           map flow-queue af1 to port-queue ef
#
#           flow-queue test
#           queue af1 lpq shaping 500 flow-wred test
#           queue ef pq shaping 1000 flow-wred test
#
#           service-template test
#           network-header-length 12 outbound
#
#           qos-profile test
#           mpls-hqos flow-queue test flow-mapping test service-template test
#
#           interface GigabitEthernet1/0/0
#           undo shutdown
#
#           interface GigabitEthernet1/0/0.1
#           vlan-type dot1q 20
#           mpls 12vc 1.1.1.9 101
#           mpls 12vpn qos cir 2000 pir 3000 qos-profile test
#           mpls 12vpn pw traffic-statistic enable
#
#           interface Pos2/0/0
#           link-protocol ppp
#           undo shutdown
#           ip address 10.2.2.1 255.255.255.0
#           mpls
#           mpls ldp
#
#           interface LoopBack1
#           ip address 3.3.3.9 255.255.255.255
#
#           ospf 1
#           area 0.0.0.0
#           network 3.3.3.9 0.0.0.0
#           network 10.2.2.0 0.0.0.255
#
#           return
```

- Configuration file of CE2

```
#           sysname CE2
#
#           interface GigabitEthernet1/0/0
```

```
undo shutdown
#
interface GigabitEthernet1/0/0.1
  vlan-type dot1q 20
  ip address 100.1.1.2 255.255.255.0
#
return
```

6.11.5 Example for Configuring Dynamic Single-hop PWE3 QoS

This part describes how to provide bandwidth assurance for a single-hop PWE3 by configuring single-hop PWE3 QoS.

Networking Requirements

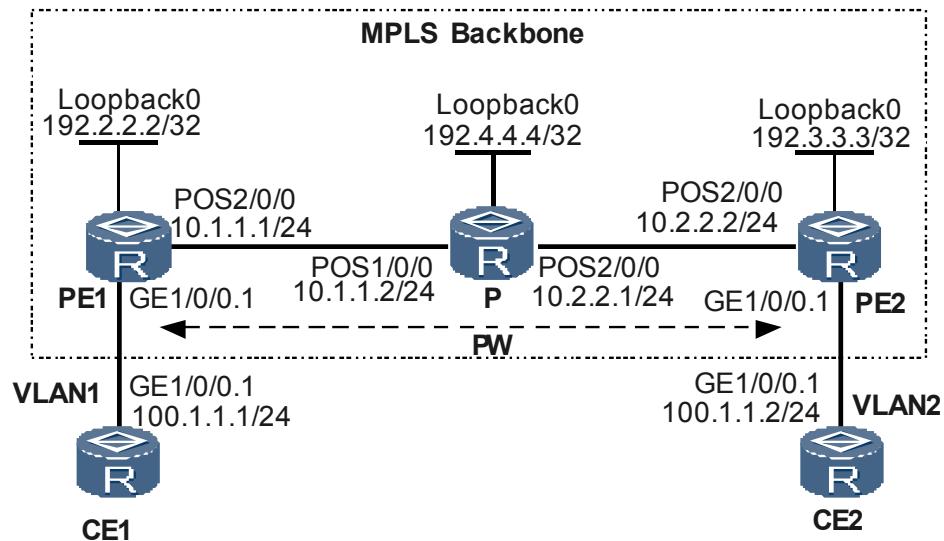
As shown in **Figure 6-6**, CE1 and CE2 are connected to PE1 and PE2 respectively through VLANs. PE1 and PE2 are connected over an MPLS backbone.

An LSP tunnel is needed to set up a dynamic PW between PE1 and PE2.

Traffic policing needs to be implemented on the incoming traffic at the user side of PE1 to limit the bandwidth. The CIR for traffic going from CE1 to CE2 should be 2000 kbit/s, and the PIR should be 4000 kbit/s.

Congestion avoidance and flow queue scheduling need to be carried out in the event of congestion. That is, when congestion occurs, packets should be dropped according to the WRED discard parameters configured for flow queues. The traffic shaping rates of flow queues AF1 and EF are 500 kbit/s and 1000 kbit/s respectively, and the traffic of flow queue AF1 is mapped to class queue EF.

Figure 6-6 Networking diagram for configuring a single-hop dynamic PW (LSP tunnel adopted)



Configuration Roadmap

The configuration roadmap is as follows:

1. Run IGP on the backbone to achieve connectivity between devices over the backbone.
2. Enable basic MPLS capabilities, set up an LSP tunnel on the backbone, and establish remote MPLS LDP peer relationship between the PEs at two ends of the PW.
3. Create MPLS L2VCs on PEs.
4. Configure the QoS-profile and the scheduling parameters.
5. Configure QoS policies on PE1 to ensure the bandwidth of PWE3.

Data Preparation

To complete the configuration, you need the following data:

- Identical L2VC IDs for PEs on both ends of the PW
- MPLS LSR IDs for PEs and the P
- IP address of the remote PE peer
- The parameters of flow-wred, flow-queue, and the value of network-header-length in the QoS-profile
- CIR
- PIR

Procedure

Step 1 Assign IP addresses to interfaces on CEs that connect CEs to PEs.

Configure CE1.

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] undo shutdown
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 1/0/0.1
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 1
[CE1-GigabitEthernet1/0/0.1] ip address 100.1.1.1 24
[CE1-GigabitEthernet1/0/0.1] quit
```

Configure CE2.

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface gigabitethernet 1/0/0
[CE2-GigabitEthernet1/0/0] undo shutdown
[CE2-GigabitEthernet1/0/0] quit
[CE2] interface gigabitethernet 1/0/0.1
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 2
[CE2-GigabitEthernet1/0/0.1] ip address 100.1.1.2 24
[CE2-GigabitEthernet1/0/0.1] quit
```

Step 2 Configure IGP on the MPLS backbone. In this example, OSPF is adopted.

The configuration details are not mentioned here.

After the configuration, run the **display ip routing-table** command. You can find that PE1 and PE2 have learnt the IP route to each other's loopback0 interface through OSPF, and that PE1 and PE2 can ping through each other.

```
<PE1> display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
```

```

Destinations : 9      Routes : 9
Destination/Mask Proto Pre Cost Flags NextHop      Interface
10.1.1.0/24 Direct 0   0       D  10.1.1.1      Pos2/0/0
10.1.1.1/32 Direct 0   0       D  127.0.0.1     InLoopBack0
10.1.1.2/32 Direct 0   0       D  10.1.1.2      Pos2/0/0
10.2.2.0/24 OSPF   10   2       D  10.1.1.2      Pos2/0/0
127.0.0.0/8 Direct 0   0       D  127.0.0.1     InLoopBack0
127.0.0.1/32 Direct 0   0       D  127.0.0.1     InLoopBack0
192.2.2.2/32 Direct 0   0       D  127.0.0.1     InLoopBack0
192.3.3.3/32 OSPF   10   3       D  10.1.1.2      Pos2/0/0
192.4.4.4/32 OSPF   10   2       D  10.1.1.2      Pos2/0/0

<PE1> ping 192.3.3.3
PING 192.3.3.3: 56 data bytes, press CTRL_C to break
Reply from 192.3.3.3: bytes=56 Sequence=1 ttl=254 time=230 ms
Reply from 192.3.3.3: bytes=56 Sequence=2 ttl=254 time=120 ms
Reply from 192.3.3.3: bytes=56 Sequence=3 ttl=254 time=120 ms
Reply from 192.3.3.3: bytes=56 Sequence=4 ttl=254 time=120 ms
Reply from 192.3.3.3: bytes=56 Sequence=5 ttl=254 time=90 ms
--- 192.3.3.3 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 90/136/230 ms

```

Step 3 Enable MPLS, and set up LSP tunnels and remote LDP sessions.

Enable MPLS on the backbone, set up an LSP tunnel and remote LDP sessions between the PEs.

The configuration details are not mentioned here.

After the configuration, you can find that LDP sessions are established between PEs and between PEs and the P, with the status being Operational.

Take the display on PE1 as an example.

```

<PE1> display mpls ldp session
          LDP Session(s) in Public Network
-----
Peer-ID      Status      LAM    SsnRole    SsnAge      KA-Sent/Rcv
-----
192.3.3.3:0  Operational DU    Passive  000:00:04  18/18
192.4.4.4:0  Operational DU    Passive  000:00:05  21/21
-----
TOTAL: 2 session(s) Found.
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM

```

Step 4 Create VCs.

Enable MPLS L2VPN on PE1 and PE2, and then create a VC on each PE.

NOTE

PWE3 does not support P2MP. Therefore, when you create an MPLS L2VC on an ATM sub-interface, the ATM sub-interface must be of the point-to-point (P2P) type. In the case of transparent transmission of ATM cells, however, the ATM sub-interface does not have to be of the P2P type.

Configure PE1.

```

[PE1] mpls l2vpn
[PE1-l2vpn] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] undo shutdown
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 1/0/0.1
[PE1-GigabitEthernet1/0/0.1] vlan-type dot1q 1
[PE1-GigabitEthernet1/0/0.1] mpls 12vc 192.3.3.3 100
[PE1-GigabitEthernet1/0/0.1] quit

```

Configure PE2.

```
[PE2] mpls l2vpn
[PE2-l2vpn] quit
[PE2] interface gigabitethernet 1/0/0
[PE2-GigabitEthernet1/0/0] undo shutdown
[PE2-GigabitEthernet1/0/0] quit
[PE2] interface gigabitethernet1/0/0.1
[PE2-GigabitEthernet1/0/0.1] vlan-type dot1q 2
[PE2-GigabitEthernet1/0/0.1] mpls 12vc 192.2.2.2 100
[PE2-GigabitEthernet1/0/0.1] quit
```

Step 5 Configure the QoS-profile and the scheduling parameters. See[Example for Configuring BGP/MPLS IP VPN QoS step 2.](#)

Step 6 Configure PWE3 QoS.

Configure QoS parameters on PE1, and enable traffic statistics.

```
[PE1] interface gigabitethernet 1/0/0.1
[PE1-GigabitEthernet1/0/0.1] mpls 12vpn qos cir 2000 pir 4000 qos-profile test
[PE1-GigabitEthernet1/0/0.1] mpls 12vpn pw traffic-statistic enable
[PE1-GigabitEthernet1/0/0.1] quit
```

Step 7 Verify the configuration.

On PEs, check the L2VPN connections. You can find that an L2VC is set up and is in the Up state.

Take the display on PE1 as an example.

```
<PE1> display mpls 12vc interface gigabitethernet 1/0/0.1
*client interface      : GigabitEthernet1/0/0.1 is up
  session state       : up
  AC status           : up
  VC state            : up
  VC ID               : 100
  VC type             : VLAN
  destination         : 192.3.3.3
  local group ID     : 0          remote group ID   : 0
  local VC label      : 21504    remote VC label   : 21504
  local AC OAM State : up
  local PSN State    : up
  local forwarding state: forwarding
  remote AC OAM state: up
  remote PSN state   : up
  remote forwarding state: forwarding
  BFD for PW          : unavailable
  manual fault        : not set
  active state        : active
  forwarding entry    : exist
  link state          : up
  local VC MTU        : 1500     remote VC MTU     : 1500
  local VCCV          : Disable
  remote VCCV         : Disable
  local control word  : disable   remote control word : disable
  tunnel policy        : --
  traffic behavior    : --
  PW template name   : --
  primary or secondary: primary
  VC tunnel/token info: 1 tunnels/tokens
    NO.0 TNL type : lsp , TNL ID : 0x2002003
  create time          : 0 days, 0 hours, 7 minutes, 16 seconds
  up time              : 0 days, 0 hours, 5 minutes, 6 seconds
  last change time    : 0 days, 0 hours, 5 minutes, 6 seconds
  VC last up time    : 2009/04/22 12:31:31
  VC total up time   : 0 days, 2 hours, 12 minutes, 51 seconds
  CKey                : 2
  NKey                : 1
```

```
L2VPN QoS CIR value : 2000
L2VPN QoS PIR value : 4000
L2VPN QoS qos-profile name: test
```

CE1 and CE2 can ping through each other.

Take the display on CE1 as an example.

```
<CE1> ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=5 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=2 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=28 ms
--- 100.1.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 2/15/31 ms
```

View traffic statistics of the PWE3.

```
<PE1> display traffic-statistics l2vpn pw interface gigabitethernet1/0/0.1
Interface name : GigabitEthernet 1/0/0.1
Statistics last cleared : never
Last 300 seconds QoS statistics rate : 0 bits/sec, 0 packets/sec
QoS statistics output : 0 bytes, 0 packets
PacketRate : Last 300 seconds packets rate(packets/sec)
ByteRate : Last 300 seconds bytes rate(bits/sec)
Queue Packets      Bytes      PacketRate   ByteRate
-----
be    0            0           0           0
af1   0            0           0           0
af2   0            0           0           0
af3   0            0           0           0
af4   0            0           0           0
ef    0            0           0           0
cs6   0            0           0           0
cs7   0            0           0           0
-----
Discarded traffic statistics :
Queue Packets      Bytes      PacketRate   ByteRate
-----
be    0            0           0           0
af1   0            0           0           0
af2   0            0           0           0
af3   0            0           0           0
af4   0            0           0           0
ef    0            0           0           0
cs6   0            0           0           0
cs7   0            0           0           0
-----
```

----End

Configuration Files

- Configuration file of CE1

```
#          sysname CE1
#
interface GigabitEthernet1/0/0
    undo shutdown
#
interface GigabitEthernet1/0/0.1
    vlan-type dot1q 1
    ip address 100.1.1.1 255.255.255.0
```

```
#  
return  


- Configuration file of PE1



```

 sysname PE1

 mpls lsr-id 192.2.2.2
 mpls

 mpls l2vpn

 mpls ldp

 mpls ldp remote-peer 192.3.3.3
 remote-ip 192.3.3.3

flow-wred test
 color green low-limit 70 high-limit 100 discard-percentage 100
 color yellow low-limit 60 high-limit 90 discard-percentage 100
 color red low-limit 50 high-limit 80 discard-percentage 100

flow-mapping test
 map flow-queue af1 to port-queue ef

flow-queue test
 queue af1 lpq shaping 500 flow-wred test
 queue ef pq shaping 1000 flow-wred test

service-template test
 network-header-length 12 outbound

qos-profile test
 mpls-hqos flow-queue test flow-mapping test service-template test

interface GigabitEthernet1/0/0
 undo shutdown

interface GigabitEthernet1/0/0.1
 vlan-type dot1q 1
 mpls 12vc 192.3.3.3 100
 mpls 12vpn qos cir 2000 pir 3000 qos-profile test
 mpls 12vpn pw traffic-statistic enable

interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp

interface LoopBack0
 ip address 192.2.2.2 255.255.255.255

ospf 1
area 0.0.0.0
 network 192.2.2.2 0.0.0.0
 network 10.1.1.0 0.0.0.255

return

- Configuration file of the P


```
#  
    sysname P  
#  
    mpls lsr-id 192.4.4.4  
    mpls  
#  
    mpls ldp  
#
```


```


```

```
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 192.4.4.4 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.4.4.4 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.2.0 0.0.0.255
#
return
```

- Configuration file of PE2

```
#
sysname PE2
#
mpls lsr-id 192.3.3.3
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 192.2.2.2
remote-ip 192.2.2.2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.2.2.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet 1/0/0.1
vlan-type dot1q 2
mpls l2vc 192.2.2.2 100
#
interface LoopBack0
ip address 192.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 192.3.3.3 0.0.0.0
network 10.2.2.0 0.0.0.255
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
interface GigabitEthernet1/0/0
undo shutdown
#
```

```

interface GigabitEthernet1/0/0.1
  vlan-type dot1q 2
  ip address 100.1.1.2 255.255.255.0
#
return

```

6.11.6 Example for Configuring the Static Multi-hop PW QoS

This part describes how to provide bandwidth assurance for a static PWE3 by configuring static PW QoS.

Networking Requirements

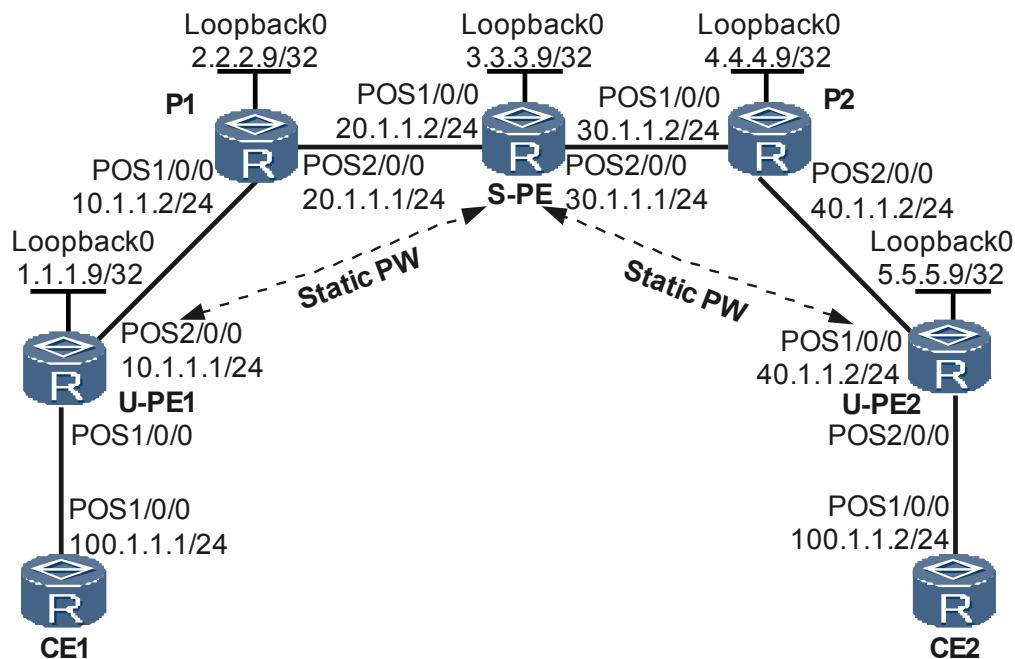
As shown in **Figure 6-7**, CE1 and CE2 are connected to U-PE1 and U-PE2 respectively through PPP.

MPLS L2VPN needs to be set up between U-PE1 and U-PE2 by using static PWs. The static PW has two hops, and uses S-PE as the switching node.

Traffic policing needs to be implemented on the S-PE to limit the bandwidth. The required CIR for the two-hop PW is 3000 kbit/s, and the required PIR is 4000 kbit/s.

Congestion avoidance and flow queue scheduling need to be carried out in the event of congestion. That is, when congestion occurs, packets should be dropped according to the WRED discard parameters configured for flow queues. The traffic shaping rates of flow queues AF1 and EF are 500 kbit/s and 1000 kbit/s respectively, and the traffic of flow queue AF1 is mapped to class queue EF.

Figure 6-7 Networking diagram of configuring the static multi-hop PW



Configuration Roadmap

The configuration roadmap is as follows:

1. Run a common routing protocol on the backbone to achieve connectivity between devices on the backbone.
2. Enable basic MPLS capabilities over the backbone and set up LSP tunnels.
3. Establish static MPLS L2VC connections on U-PeEs.
4. Set up a switching PW on the switching node S-PE.
5. Configure the QoS-profile and the scheduling parameters.
6. Configure QoS parameters for the two-hop PW on S-PE.

Data Preparation

To complete the configuration, you need the following data:

- L2VC IDs of U-PE1 and U-PE2
- MPLS LSR IDs of U-PE1, S-PE, and U-PE2
- Names and parameters of the PW templates to be configured on U-PeEs
- VC label values that are required for configuring the static PW (note the mapping between the VC label values on both ends)
- Encapsulation type of the switching PW on S-PE
- The parameters of flow-wred, flow-queue, and the value of network-header-length in the QoS-profile
- CIR
- PIR

Procedure

Step 1 Configure CEs.

Configure CE1.

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface pos 1/0/0
[CE1-Pos1/0/0] ip address 100.1.1.1 24
[CE1-Pos1/0/0] undo shutdown
[CE1-Pos1/0/0] quit
```

Configure CE2.

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface pos 1/0/0
[CE2-Pos1/0/0] ip address 100.1.1.2 24
[CE2-Pos1/0/0] undo shutdown
[CE2-Pos1/0/0] quit
```

Step 2 Configure IGP on the MPLS backbone.

Configure IGP on the MPLS backbone. In this example, OSPF is adopted.

Assign IP addresses to interfaces on U-PeEs, S-PE, and the P routers, as shown in [Figure 6-7](#). When configuring OSPF, advertise the 32-bit IP addresses of loopback interfaces on U-PE1, S-PE, and U-PE2.

The configuration details are not mentioned here.

Step 3 Configure basic MPLS capabilities and set up LSP tunnels.

Enable basic MPLS capabilities on the MPLS backbone, and set up LSP tunnels between U-PE1 and S-PE, and between SPE and U-PE2. The configuration details are not mentioned here.

Step 4 Create VCs.

Enable MPLS L2VPN on U-PE1, U-PE2, and S-PE, and set up VCs on U-PE1 and U-PE2.

 **NOTE**

PWE3 does not support P2MP. Therefore, when you create an MPLS L2VC on an ATM sub-interface, the ATM sub-interface must be of the point-to-point (P2P) type. In the case of transparent transmission of ATM cells, however, the ATM sub-interface does not have to be of the P2P type.

Configure U-PE1.

```
[U-PE1] mpls l2vpn
[U-PE1-l2vpn] quit
[U-PE1] pw-template pwt
[U-PE1-pw-template-pwt] peer-address 3.3.3.9
[U-PE1-pw-template-pwt] quit
[U-PE1] interface pos 1/0/0
[U-PE1-Pos1/0/0] mpls static-l2vc pw-template pwt 100 transmit-vpn-label 100
receive-vpn-label 100
[U-PE1-Pos1/0/0] undo shutdown
[U-PE1-Pos1/0/0] quit
```

Configure S-PE.

```
[S-PE] mpls l2vpn
[S-PE-l2vpn] quit
```

Configure U-PE2.

```
[U-PE2] mpls l2vpn
[U-PE2-l2vpn] quit
[U-PE2] pw-template pwt
[U-PE2-pw-template-pwt] peer-address 3.3.3.9
[U-PE2-pw-template-pwt] quit
[U-PE2] interface pos 2/0/0
[U-PE2-Pos2/0/0] mpls static-l2vc pw-template pwt 100 transmit-vpn-label 200
receive-vpn-label 200
[U-PE2-Pos2/0/0] undo shutdown
[U-PE2-Pos2/0/0] quit
```

 **NOTE**

The transmit-vpn-label configured on the U-PE must be consistent with the recv label on the S-PE and the receive-vpn-label configured on the U-PE must be consistent with the trans label on the S-PE. Otherwise, CEs cannot communicate.

Step 5 Configure the QoS-profile and the scheduling parameters. See[Example for Configuring BGP/MPLS IP VPN QoS step 2.](#)

Step 6 Configure QoS parameters on S-PE.

```
[S-PE] mpls switch-l2vc 5.5.5.9 100 trans 200 recv 200 cir 3000 pir 4000 qos-
profile test between 1.1.1.9 100 trans 100 recv 100 cir 3000 pir 4000 qos-profile
test encapsulation ppp
```

Step 7 Verify the configuration.

View L2VPN QoS configurations on PEs.

Take the display on S-PE as an example.

```
<S-PE> display mpls switch-l2vc
Total Switch VC : 1, 1 up, 0 down
```

```

*Switch-l2vc type : SVC<---->SVC
Peer IP Address : 5.5.5.9, 1.1.1.9
VC ID : 100, 100
VC Type : PPP
VC State : up
In/Out Label : 200/200, 100/100
Control Word : Disable, Disable
VCCV Capability : Disable, Disable
Switch-l2vc tunnel info :
    1 tunnels for peer 5.5.5.9
    NO.0 TNL Type : lsp , TNL ID : 0x2002006
    1 tunnels for peer 1.1.1.9
    NO.0 TNL Type : lsp , TNL ID : 0x1002000
CKey : 5, 6
NKey : 1, 3
L2VPN QoS CIR value : 3000, 3000
L2VPN QoS PIR value : 4000, 4000
L2VPN QoS qos-profile name : test
Create time : 0 days, 0 hours, 12 minutes, 13 seconds
UP time : 0 days, 0 hours, 5 minutes, 16 seconds
Last change time : 0 days, 0 hours, 5 minutes, 16 seconds
VC last up time : 2009/04/22 12:31:31
VC total up time: 0 days, 2 hours, 12 minutes, 51 seconds

```

CE1 and CE2 can ping through each other.

Take the display on CE1 as an example.

```

<CE1> ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=188 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=187 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=187 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=188 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=188 ms
--- 100.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 187/187/188 ms

```

----End

Configuration Files

- Configuration file of CE1

```

#
sysname CE1
#
interface Pos1/0/0
    link-protocol ppp
    undo shutdown
    ip address 100.1.1.1 255.255.255.0
#
return

```

- Configuration file of U-PE1

```

#
sysname U-PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
pw-template pwt
peer-address 3.3.3.9
#

```

```
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
mpls static-l2vc pw-template pwt 100 transmit-vpn-label 100 receive-vpn-label
100
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
return
```

- Configuration file of P1

```
#
sysname P1
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return
```

- Configuration file of S-PE

```
#
sysname S-PE
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
```

```

#
mpls switch-l2vc 5.5.5.9 100 trans 200 recv 200 cir 3000 pir 4000 qos-profile
test between 1.1.1.9 100 trans 100 recv 100 cir 3000 pir 4000 qos-profile test
encapsulation ppp
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
#
mpls ldp remote-peer 5.5.5.9
remote-ip 5.5.5.9
#
flow-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
flow-mapping test
map flow-queue af1 to port-queue ef
#
flow-queue test
queue af1 lpq shaping 500 flow-wred test
queue ef pq shaping 1000 flow-wred test
#
service-template test
network-header-length 12 outbound
#
qos-profile test
mpls-hqos flow-queue test flow-mapping test service-template test
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
network 3.3.3.9 0.0.0.0
#
return

```

- Configuration file of P2

```

#
sysname P2
#
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.2 255.255.255.0
mpls

```

```
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 40.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 4.4.4.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 4.4.4.9 0.0.0.0
network 30.1.1.0 0.0.0.255
network 40.1.1.0 0.0.0.255
#
return
```

- Configuration file of U-PE2

```
#
sysname U-PE2
#
mpls lsr-id 5.5.5.9
mpls
#
mpls l2vpn
#
pw-template pwt
peer-address 3.3.3.9
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 40.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
mpls static-l2vc pw-template pwt 100 transmit-vpn-label 200 receive-vpn-label
200
#
interface LoopBack0
ip address 5.5.5.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 5.5.5.9 0.0.0.0
network 40.1.1.0 0.0.0.255
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 100.1.1.2 255.255.255.0
#
```

return

6.11.7 Example for Configuring the Dynamic Multi-hop PW QoS

This part describes how to provide bandwidth assurance for a dynamic PWE3 by configuring dynamic multi-hop PWE QoS.

Networking Requirements

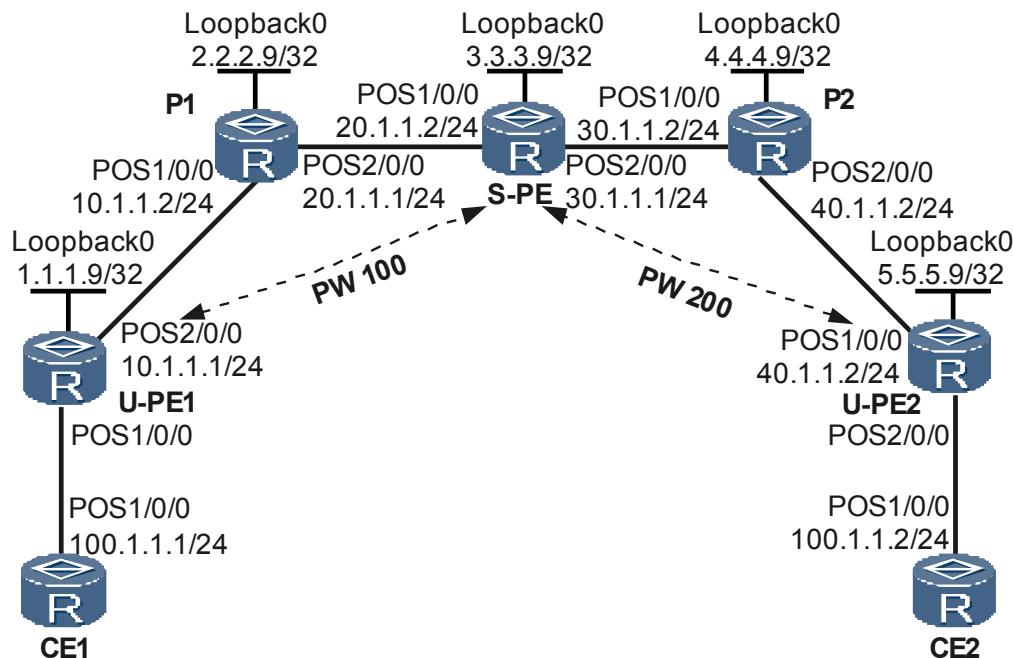
As shown in [Figure 6-8](#), CE1 and CE2 are connected to U-PE1 and U-PE2 respectively through PPP. U-PE1 and U-PE2 are connected through the MPLS backbone. A dynamic multi-hop PW is set up between U-PE1 and U-PE2 through the LSP tunnel, with S-PE functioning as the switching node.

Traffic policing needs to be implemented on the S-PE to limit the bandwidth. The required CIR for the two-hop PW is 3000 kbit/s, and the required PIR is 4000 kbit/s.

NOTE

QoS-Profile can be configured as requirement. For details of the configurations, refer to [Example for Configuring the Static Multi-hop PW QoS](#)

Figure 6-8 Networking diagram of configuring the dynamic multi-hop PW



Configuration Roadmap

The configuration roadmap is as follows:

1. Run IGP on the backbone to achieve connectivity between devices over the backbone.
2. Enable basic MPLS capabilities over the backbone and set up LSP tunnels. Establish remote MPLS LDP peer relationship between U-PE1 and S-PE, and between U-PE2 and S-PE.

3. Create PW templates, and enable the control word and LSP Ping.
4. Set up an MPLS L2VC between the U-PEs.
5. Set up a switching PW on the switching node S-PE.
6. Configure QoS parameters on S-PE.

Data Preparation

To complete the configuration, you need the following data:

- L2VC IDs of U-PE1 and U-PE2 (the two IDs must be different)
- MPLS LSR IDs of U-PE1, S-PE, and U-PE2
- IP address of the remote peer
- Encapsulation type of the switching PW
- Names and parameters of the PW templates to be configured on U-PEs
- CIR
- PIR

Procedure

Step 1 Assign IP addresses to interfaces on CEs that connect CEs to PEs.

Configure CE1.

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface pos 1/0/0
[CE1-Pos1/0/0] ip address 100.1.1.1 24
[CE1-Pos1/0/0] undo shutdown
[CE1-Pos1/0/0] quit
```

Configure CE2.

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface pos 1/0/0
[CE2-Pos1/0/0] ip address 100.1.1.2 24
[CE2-Pos1/0/0] undo shutdown
[CE2-Pos1/0/0] quit
```

Step 2 Configure IGP on the MPLS backbone.

Configure IGP on the MPLS backbone. In this example, OSPF is adopted.

Assign IP addresses to interfaces on U-PEs, S-PE, and the P. When configuring OSPF, advertise the 32-bit IP addresses of loopback interfaces on U-PE1, S-PE, and U-PE2.

Configure U-PE1.

```
[U-PE1] interface loopback 0
[U-PE1-LoopBack0] ip address 1.1.1.9 32
[U-PE1-LoopBack0] quit
[U-PE1] interface pos 2/0/0
[U-PE1-Pos2/0/0] ip address 10.1.1.1 24
[U-PE1-Pos2/0/0] undo shutdown
[U-PE1-Pos2/0/0] quit
[U-PE1] ospf 1
[U-PE1-ospf-1] area 0.0.0.0
[U-PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[U-PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
```

```
[U-PE1-ospf-1-area-0.0.0.0] quit
[U-PE1-ospf-1] quit

# Configure P1.

[P1] interface loopback 0
[P1-LoopBack0] ip address 2.2.2.9 32
[P1-LoopBack0] quit
[P1] interface pos 1/0/0
[P1-Pos1/0/0] ip address 10.1.1.2 24
[P1-Pos1/0/0] undo shutdown
[P1-Pos1/0/0] quit
[P1] interface pos 2/0/0
[P1-Pos2/0/0] ip address 20.1.1.1 24
[P1-Pos2/0/0] undo shutdown
[P1-Pos2/0/0] quit
[P1] ospf 1
[P1-ospf-1] area 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

Configure S-PE.

```
[S-PE] interface loopback 0
[S-PE-LoopBack0] ip address 3.3.3.9 32
[S-PE-LoopBack0] quit
[S-PE] interface pos 1/0/0
[S-PE-Pos1/0/0] ip address 20.1.1.2 24
[S-PE-Pos1/0/0] undo shutdown
[S-PE-Pos1/0/0] quit
[S-PE] interface pos 2/0/0
[S-PE-Pos2/0/0] ip address 30.1.1.1 24
[S-PE-Pos2/0/0] undo shutdown
[S-PE-Pos2/0/0] quit
[S-PE] ospf 1
[S-PE-ospf-1] area 0.0.0.0
[S-PE-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[S-PE-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[S-PE-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[S-PE-ospf-1-area-0.0.0.0] quit
[S-PE-ospf-1] quit
```

Configure P2.

```
[P2] interface loopback 0
[P2-LoopBack0] ip address 4.4.4.9 32
[P2-LoopBack0] quit
[P2] interface pos 1/0/0
[P2-Pos1/0/0] ip address 30.1.1.2 24
[P2-Pos1/0/0] undo shutdown
[P2-Pos1/0/0] quit
[P2] interface pos 2/0/0
[P2-Pos2/0/0] ip address 40.1.1.1 24
[P2-Pos2/0/0] undo shutdown
[P2-Pos2/0/0] quit
[P2] ospf 1
[P2-ospf-1] area 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

Configure U-PE2.

```
[U-PE2] interface loopback 0
[U-PE2-LoopBack0] ip address 5.5.5.9 32
```

```
[U-PE2-LoopBack0] quit
[U-PE2] interface pos 1/0/0
[U-PE2-Pos1/0/0] ip address 40.1.1.2 24
[U-PE2-Pos1/0/0] undo shutdown
[U-PE2-Pos1/0/0] quit
[U-PE2] ospf 1
[U-PE2-ospf-1] area 0.0.0.0
[U-PE2-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[U-PE2-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[U-PE2-ospf-1-area-0.0.0.0] quit
[U-PE2-ospf-1] quit
```

After the configuration, run the **display ip routing-table** command on U-PEs, Ps and S-PE. You can find that these devices have learnt the route to each other. Take the display on S-PE as an example.

```
<S-PE> display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
    Destinations : 15      Routes : 15
Destination/Mask Proto Pre Cost     Flags NextHop      Interface
1.1.1.9/32    OSPF  10  3          D  20.1.1.1      Pos1/0/0
2.2.2.9/32    OSPF  10  2          D  20.1.1.1      Pos1/0/0
            3.3.3.9/32 Direct 0  0          D  127.0.0.1    InLoopBack0
4.4.4.9/32    OSPF  10  2          D  30.1.1.2      Pos2/0/0
5.5.5.9/32    OSPF  10  3          D  30.1.1.2      Pos2/0/0
            10.1.1.0/24 OSPF  10  2          D  20.1.1.1      Pos1/0/0
            20.1.1.0/24 Direct 0  0          D  20.1.1.2      Pos1/0/0
            20.1.1.1/32 Direct 0  0          D  20.1.1.1      Pos1/0/0
            20.1.1.2/32 Direct 0  0          D  127.0.0.1    InLoopBack0
            30.1.1.0/24 Direct 0  0          D  30.1.1.1      Pos2/0/0
            30.1.1.1/32 Direct 0  0          D  127.0.0.1    InLoopBack0
            30.1.1.2/32 Direct 0  0          D  30.1.1.2      Pos2/0/0
            40.1.1.0/24 OSPF  10  2          D  30.1.1.2      Pos2/0/0
            127.0.0.0/8  Direct 0  0          D  127.0.0.1    InLoopBack0
            127.0.0.1/32 Direct 0  0          D  127.0.0.1    InLoopBack0
```

U-PEs can ping through each other. Take the display on U-PE1 as an example.

```
<U-PE1> ping 40.1.1.2
PING 40.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 40.1.1.2: bytes=56 Sequence=1 ttl=252 time=160 ms
    Reply from 40.1.1.2: bytes=56 Sequence=2 ttl=252 time=120 ms
    Reply from 40.1.1.2: bytes=56 Sequence=3 ttl=252 time=150 ms
    Reply from 40.1.1.2: bytes=56 Sequence=4 ttl=252 time=150 ms
    Reply from 40.1.1.2: bytes=56 Sequence=5 ttl=252 time=160 ms
--- 40.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 120/148/160 ms
```

Step 3 Enable MPLS, and set up LSP tunnels and remote LDP sessions.

Configure basic MPLS capabilities on the MPLS backbone, and set up LSP tunnels and remote LDP sessions between U-PE1 and S-PE, and between S-PE and U-PE2.

Configure U-PE1.

```
[U-PE1] mpls lsr-id 1.1.1.9
[U-PE1] mpls
[U-PE1-mpls] quit
[U-PE1] mpls ldp
[U-PE1-mpls-ldp] quit
[U-PE1] interface pos 2/0/0
[U-PE1-Pos2/0/0] mpls
[U-PE1-Pos2/0/0] mpls ldp
[U-PE1-Pos2/0/0] quit
```

```
[U-PE1] mpls ldp remote-peer 3.3.3.9
[U-PE1-mpls-ldp-remote-3.3.3.9] remote-ip 3.3.3.9
[U-PE1-mpls-ldp-remote-3.3.3.9] quit
```

Configure P1.

```
[P1] mpls lsr-id 2.2.2.9
[P1] mpls
[P1-mpls] quit
[P1] mpls ldp
[P1-mpls-ldp] quit
[P1] interface pos 1/0/0
[P1-Pos1/0/0] mpls
[P1-Pos1/0/0] mpls ldp
[P1-Pos1/0/0] quit
[P1] interface pos 2/0/0
[P1-Pos2/0/0] mpls
[P1-Pos2/0/0] mpls ldp
[P1-Pos2/0/0] quit
```

Configure S-PE.

```
[S-PE] mpls lsr-id 3.3.3.9
[S-PE] mpls
[S-PE-mpls] quit
[S-PE] mpls ldp
[S-PE-mpls-ldp] quit
[S-PE] interface pos 1/0/0
[S-PE-Pos1/0/0] mpls
[S-PE-Pos1/0/0] mpls ldp
[S-PE-Pos1/0/0] quit
[S-PE] interface pos 2/0/0
[S-PE-Pos2/0/0] mpls
[S-PE-Pos2/0/0] mpls ldp
[S-PE-Pos2/0/0] quit
[S-PE] mpls ldp remote-peer 1.1.1.9
[S-PE-mpls-ldp-remote-1.1.1.9] remote-ip 1.1.1.9
[S-PE-mpls-ldp-remote-1.1.1.9] quit
[S-PE] mpls ldp remote-peer 5.5.5.9
[S-PE-mpls-ldp-remote-5.5.5.9] remote-ip 5.5.5.9
[S-PE-mpls-ldp-remote-5.5.5.9] quit
```

Configure P2.

```
[P2] mpls lsr-id 4.4.4.9
[P2] mpls
[P2-mpls] quit
[P2] mpls ldp
[P2-mpls-ldp] quit
[P2] interface pos 1/0/0
[P2-Pos1/0/0] mpls
[P2-Pos1/0/0] mpls ldp
[P2-Pos1/0/0] quit
[P2] interface pos 2/0/0
[P2-Pos2/0/0] mpls
[P2-Pos2/0/0] mpls ldp
[P2-Pos2/0/0] quit
```

Configure U-PE2.

```
[U-PE2] mpls lsr-id 5.5.5.9
[U-PE2] mpls
[U-PE2-mpls] quit
[U-PE2] mpls ldp
[U-PE2-mpls-ldp] quit
[U-PE2] interface pos 1/0/0
[U-PE2-Pos1/0/0] mpls
[U-PE2-Pos1/0/0] mpls ldp
[U-PE2-Pos1/0/0] quit
[U-PE2] mpls ldp remote-peer 3.3.3.9
```

```
[U-PE2-mpls-ldp-remote-3.3.3.9] remote-ip 3.3.3.9
[U-PE2-mpls-ldp-remote-3.3.3.9] quit
```

After the preceding configuration, run the **display mpls ldp session** command on U-PEs, Ps, or S-PE, and you can find that the value of the Session State field is **Operational**. Run the **display mpls ldp peer** command, and you can view how LDP sessions are set up. Run the **display mpls lsp** command, and you can view the setup of the LSP. Take the display on S-PE as an example.

```
<S-PE> display mpls ldp session
      LDP Session(s) in Public Network
-----
Peer-ID          Status       LAM   SsnRole   SsnAge      KA-Sent/Rcv
-----
1.1.1.9:0        Operational DU    Active    000:00:14  57/57
2.2.2.9:0        Operational DU    Active    000:00:14  56/56
4.4.4.9:0        Operational DU    Passive   000:00:05  22/22
5.5.5.9:0        Operational DU    Passive   000:00:12  52/52
-----
TOTAL: 4 session(s) Found.
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
<S-PE> display mpls ldp peer
      LDP Peer Information in Public network
-----
Peer-ID          Transport-Address  Discovery-Source
-----
1.1.1.9:0        1.1.1.9           Remote Peer : 1.1.1.9
2.2.2.9:0        2.2.2.9           Pos1/0/0
4.4.4.9:0        4.4.4.9           Pos2/0/0
5.5.5.9:0        5.5.5.9           Remote Peer : 5.5.5.9
-----
TOTAL: 4 Peer(s) Found.
<S-PE> display mpls lsp
      LSP Information: LDP LSP
-----
FEC              In/Out Label  In/Out IF          Vrf Name
3.3.3.9/32       3/NULL     --/--                -
1.1.1.9/32       NULL/1024  --/Pos1/0/0
1.1.1.9/32       1024/1024 --/Pos1/0/0
2.2.2.9/32       NULL/3     --/Pos1/0/0
2.2.2.9/32       1025/3    --/Pos1/0/0
4.4.4.9/32       NULL/3     --/Pos2/0/0
4.4.4.9/32       1027/3    --/Pos2/0/0
5.5.5.9/32       NULL/1027  --/Pos2/0/0
5.5.5.9/32       1026/1027 --/Pos2/0/0
```

Step 4 Create and configure PW templates.

Create PW templates on U-PEs, and enable the control word and LSP Ping.

Configure U-PE1.

```
[U-PE1] mpls 12vpn
[U-PE1-12vpn] quit
[U-PE1] pw-template pwt
[U-PE1-pw-template-pwt] peer-address 3.3.3.9
[U-PE1-pw-template-pwt] quit
```

Configure U-PE2.

```
[U-PE2] mpls 12vpn
[U-PE2-12vpn] quit
[U-PE2] pw-template pwt
[U-PE2-pw-template-pwt] peer-address 3.3.3.9
[U-PE2-pw-template-pwt] quit
```

 NOTE

You can also configure a dynamic PW without using the PW template. If you choose not to use the PW template, when you verify the configuration (as shown in Step 7), you are unable to detect the connectivity of the PW or collect path information about the PW. That is, you cannot run the **ping vc** or **tracert vc** command.

Step 5 Create VCs.

Enable MPLS L2VPN on U-PE1, U-PE2, and S-PE.

Configure dynamic PWs on U-PEs, and configure S-PE to function as the switching node for the dynamic PWs.

 NOTE

PWE3 does not support P2MP. Therefore, when you create an MPLS L2VC on an ATM sub-interface, the ATM sub-interface must be of the point-to-point (P2P) type. In the case of transparent transmission of ATM cells, however, the ATM sub-interface does not have to be of the P2P type.

Configure U-PE1.

```
[U-PE1] interface pos 1/0/0
[U-PE1-Pos1/0/0] mpls l2vc pw-template pwt 100
[U-PE1-Pos1/0/0] undo shutdown
[U-PE1-Pos1/0/0] quit
```

Configure S-PE.

```
[S-PE] mpls l2vpn
[S-PE-l2vpn] quit
```

Configure U-PE2.

```
[U-PE2] interface pos 2/0/0
[U-PE2-Pos2/0/0] mpls l2vc pw-template pwt 200
[U-PE2-Pos2/0/0] undo shutdown
[U-PE2-Pos2/0/0] quit
```

Step 6 Configure QoS parameters on S-PE.

```
[S-PE] mpls switch-l2vc 1.1.1.9 100 cir 3000 pir 4000 between 5.5.5.9 200 cir 3000
pir 4000 encapsulation ppp
```

Step 7 Verify the configuration.

1. Run the **display mpls switch-l2vc** command on S-PE to check L2VPN connections, and you can find that an L2VC is set up and is in the Up state.

```
<S-PE> display mpls switch-l2vc
Total Switch VC : 1, 1 up, 0 down
*Switch-l2vc type          : LDP<---->LDP
Peer IP Address        : 5.5.5.9, 1.1.1.9
VC ID                 : 200, 100
VC Type               : PPP
VC State              : up
VC StatusCode          | PSN | OAM | FW |
-Local VC :| UP | UP | UP |      | UP | UP | UP |
-Remote VC:| UP | UP | UP |      | UP | UP | UP |
Session State         : up, up
Local/Remote Label    : 21504/21504, 21505/21504
Local/Remote MTU       : 4470/4470, 4470/4470
Local/Remote Control Word : Enable/Enable, Enable/Enable
Local/Remote VCCV Capability : cw lsp-ping/cw lsp-ping, cw lsp-ping/cw lsp-
ping
Switch-l2vc tunnel info   :
                           1 tunnels for peer 5.5.5.9
                           NO.0 TNL Type : lsp , TNL ID : 0x2002006
                           1 tunnels for peer 1.1.1.9
```

```

NO.0 TNL Type : lsp , TNL ID : 0x1002000
CKey : 7, 8
NKey : 1, 3
L2VPN QoS CIR value : 3000, 3000
L2VPN QoS PIR value : 4000, 4000
L2VPN QoS qos-profile name : --, --
Tunnel policy : --, --
Create time : 0 days, 0 hours, 13 minutes, 1 seconds
UP time : 0 days, 0 hours, 3 minutes, 58 seconds
Last change time : 0 days, 0 hours, 3 minutes, 58 seconds
VC last up time : 2009/04/22 12:31:31
VC total up time: 0 days, 2 hours, 12 minutes, 51 seconds

```

2. Check the connectivity between CEs and information about the path between CEs.

CE1 and CE2 can ping through each other.

```

<CE1> ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=180 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=120 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=160 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=160 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=130 ms
--- 100.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 120/150/180 ms

```

Run the **display mpls switch-l2vc** command to view information about the path from CE1 to CE2.

```

[CE1] traceroute 100.1.1.2
traceroute to 100.1.1.2 (100.1.1.2), max hops: 30, packet length: 40, press
CTRL_C to break
    1 100.1.1.2 250 ms 220 ms 130 ms

```

----End

Configuration Files

- Configuration file of CE1

```

#
sysname CE1
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 100.1.1.1 255.255.255.0
#
return

```

- Configuration file of U-PE1

```

#
sysname U-PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls l2vpn
#
pw-template pwt
peer-address 3.3.3.9
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#

```

```
interface Pos1/0/0
link-protocol ppp
undo shutdown
mpls 12vc pw-template pwt 100
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
return
```

- Configuration file of P1

```
#
sysname P1
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
#
return
```

- Configuration file of S-PE

```
#
sysname S-PE
#
mpls lsr-id 3.3.3.9
mpls
#
mpls 12vpn
#
mpls switch-12vc 1.1.1.9 100 cir 3000 pir 4000 between 5.5.5.9 200 cir 3000 pir
4000 encapsulation ppp
#
mpls ldp
#
```

```
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
#
mpls ldp remote-peer 5.5.5.9
remote-ip 5.5.5.9
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 20.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 20.1.1.0 0.0.0.255
network 30.1.1.0 0.0.0.255
#
return
```

- Configuration file of P2

```
#
sysname P2
#
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 30.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 40.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack0
ip address 4.4.4.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 4.4.4.9 0.0.0.0
network 30.1.1.0 0.0.0.255
network 40.1.1.0 0.0.0.255
#
return
```

- Configuration file of U-PE2

```
#
sysname U-PE2
#
mpls lsr-id 5.5.5.9
```

```
mpls
#
mpls 12vpn
#
pw-template pwt
  peer-address 3.3.3.9
#
mpls ldp
#
  mpls ldp remote-peer 3.3.3.9
  remote-ip 3.3.3.9
#
interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ip address 40.1.1.2 255.255.255.0
  mpls
  mpls ldp
#
interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  mpls 12vc pw-template pwt 200
#
interface LoopBack0
  ip address 5.5.5.9 255.255.255.255
#
ospf 1
  area 0.0.0.0
    network 5.5.5.9 0.0.0.0
    network 40.1.1.0 0.0.0.255
#
return
```

- Configuration file of CE2

```
#
  sysname CE2
#
interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ip address 100.1.1.2 255.255.255.0
#
return
```

6.11.8 Example for Configuring the Mixed Multi-hop PW QoS

This part describes how to provide bandwidth assurance for a mixed PWE3 by configuring mixed multi-hop PW QoS.

Networking Requirements

As shown in [Figure 6-9](#), CE1 and CE2 are connected to U-PE1 and U-PE2 respectively through PPP.

U-PE1 and U-PE2 are connected through the MPLS backbone.

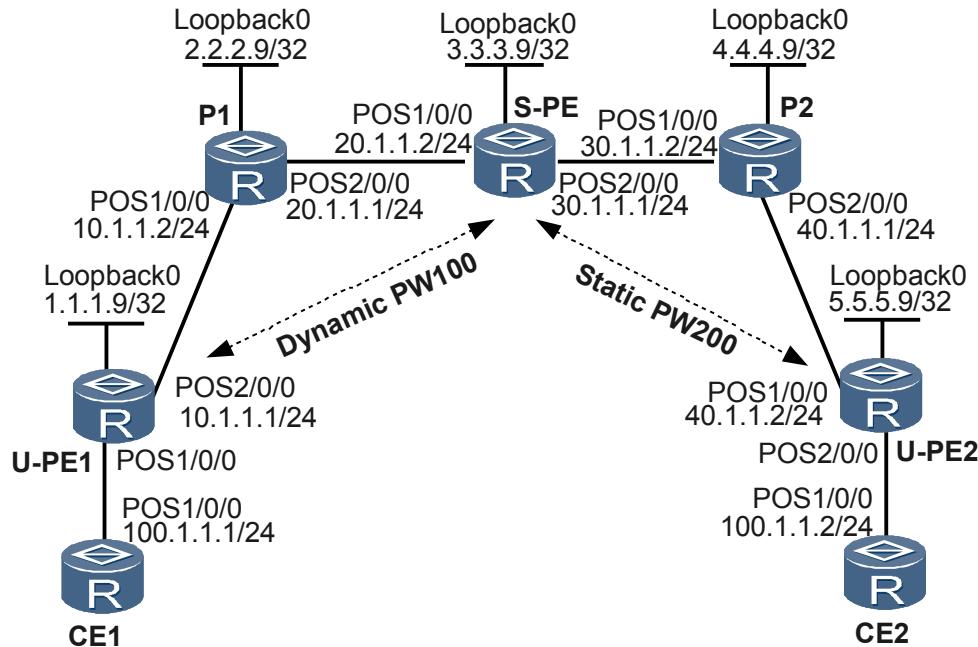
A mixed multi-hop PW (with hops consisting of both the static PW and the dynamic PW) needs to be set up between U-PE1 and U-PE2, with S-PE functioning as the switching node.

Traffic policing needs to be implemented on the S-PE to limit the bandwidth. The required CIR for the two-hop PW is 3000 kbit/s, and the required PIR is 4000 kbit/s.

 NOTE

QoS-Profile can be configured as requirement. For details of the configurations, refer to [Example for Configuring the Static Multi-hop PW QoS](#)

Figure 6-9 Networking diagram of configuring the mixed multi-hop PW



Configuration Roadmap

The configuration roadmap is as follows:

1. Run IGP on the backbone to achieve connectivity between devices on the backbone.
2. Enable basic MPLS capabilities over the backbone and set up LSP tunnels.
3. Set up remote LDP sessions between U-PEs and S-PE.
4. Set up static and/or dynamic MPLS L2VC connections on U-PEs.
5. Set up a switching PW on the switching node S-PE.
6. Configure QoS parameters for the two-hop PW on S-PE.

Data Preparation

To complete the configuration, you need the following data:

- L2VC IDs of U-PE1 and U-PE2 (the two IDs must be different)
- MPLS LSR IDs of U-PE1, S-PE, and U-PE2
- VC label values that are required for configuring the static PW on U-PE2 (note the mapping between the VC label values on both ends)
- Encapsulation type of the PW
- Names and parameters of the PW template to be configured on U-PE2

- CIR
- PIR

Procedure

Step 1 Configure CEs.

Configure CE1.

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] interface pos 1/0/0
[CE1-Pos1/0/0] ip address 100.1.1.1 24
[CE1-Pos1/0/0] undo shutdown
[CE1-Pos1/0/0] quit
```

Configure CE2.

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] interface pos 1/0/0
[CE2-Pos1/0/0] ip address 100.1.1.2 24
[CE2-Pos1/0/0] undo shutdown
[CE2-Pos1/0/0] quit
```

Step 2 Configure IGP on the MPLS backbone. In this example, OSPF is adopted.

Assign IP addresses to interfaces on U-PEs, S-PE, and the P, as shown in [Figure 6-9](#). When configuring OSPF, advertise the 32-bit IP addresses of loopback interfaces on U-PE1, S-PE, and U-PE2.

The configuration details are not mentioned here.

Step 3 Enable MPLS, set up tunnels, and set up a remote LDP session between U-PE1 and S-PE.

Configure basic MPLS capabilities and tunnels on the MPLS backbone. In this example, the LSP tunnel is adopted.

Note that a remote LDP session needs to be set up between U-PE1 and S-PE.

The configuration details are not mentioned here.

Step 4 Create VCs.

Enable MPLS L2VPN on U-PE1, U-PE2, and S-PE.

Configure a dynamic VC on U-PE1 and a static VC on U-PE2, and configure S-PE to be the switching node of the mixed PW.

NOTE

PWE3 does not support P2MP. Therefore, when you create an MPLS L2VC on an ATM sub-interface, the ATM sub-interface must be of the point-to-point (P2P) type. In the case of transparent transmission of ATM cells, however, the ATM sub-interface does not have to be of the P2P type.

Configure U-PE1.

```
[U-PE1] mpls l2vpn
[U-PE1-l2vpn] quit
[U-PE1] interface pos 1/0/0
[U-PE1-Pos1/0/0] mpls 12vc 3.3.3.9 100
[U-PE1-Pos1/0/0] undo shutdown
[U-PE1-Pos1/0/0] quit
```



NOTE

When configuring the mixed PW, note the difference between the value of *ip-address vc-id* before the key word **between** and the value of *ip-address vc-id* after the key word **between**. The two cannot be mistaken for each other because the one before the key word **between** corresponds to the dynamic PW, whereas the one after the key word **between** corresponds to the static PW.

Configure S-PE.

```
[S-PE] mpls 12vpn
[S-PE-12vpn] quit
```

Configure U-PE2.

```
[U-PE2] mpls 12vpn
[U-PE2-12vpn] quit
[U-PE2] pw-template pwt
[U-PE2-pw-template-pwt] peer-address 3.3.3.9
[U-PE2-pw-template-pwt] quit
[U-PE2] interface pos 2/0/0
[U-PE2-Pos2/0/0] mpls static-l2vc pw-template pwt 200 transmit-vpn-label 100
receive-vpn-label 200
[U-PE2-Pos2/0/0] undo shutdown
[U-PE2-Pos2/0/0] quit
```

Step 5 Configure QoS parameters on S-PE.

```
[S-PE] mpls switch-l2vc 1.1.1.9 100 cir 3000 pir 4000 between 5.5.5.9 200 trans 200
recv 100 cir 3000 pir 4000 encapsulation ppp mtu 4470
```

Step 6 Verify the configuration.

Run the related command on S-PE to check L2VPN connections, and you can find that an L2VC is set up and is in the Up state.

```
<S-PE> display mpls switch-l2vc
Total Switch VC : 1, 1 up, 0 down
*Switch-l2vc type : LDP<---->SVC
Peer IP Address : 1.1.1.9, 5.5.5.9
VC ID : 100, 200
VC Type : PPP
VC State : up
Session State : up, None
Local(In)/Remote(Out) Label : 21504/21504, 100/200
Local/Remote MTU : 4470/4470, 4470
Local/Remote Control Word : Disable/Disable, Disable
Local/Remote VCCV Capability : Disable/Disable, Disable
Switch-l2vc tunnel info :
    1 tunnels for peer 1.1.1.9
    NO.0 TNL Type : lsp , TNL ID : 0x1002000
    1 tunnels for peer 5.5.5.9
    NO.0 TNL Type : lsp , TNL ID : 0x2002006
CKey : 2, 4
NKey : 1, 3
L2VPN QoS CIR value : 3000, 3000
L2VPN QoS PIR value : 4000, 4000
L2VPN QoS qos-profile name : --, --
Tunnel policy : --, --
Create time : 0 days, 13 hours, 1 minutes, 59 seconds
UP time : 0 days, 12 hours, 55 minutes, 45 seconds
Last change time : 0 days, 12 hours, 55 minutes, 45 seconds
VC last up time : 2008/07/24 12:31:31
VC total up time: 0 days, 2 hours, 12 minutes, 51 seconds
```

CE1 and CE2 can ping through each other.

Take the display on CE1 as an example.

```
<CE1> ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
```

```
Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=270 ms
Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=220 ms
Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=190 ms
Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=190 ms
Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=160 ms
--- 100.1.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 160/206/270 ms
```

----End

Configuration Files

- Configuration file of CE1

```
#           sysname CE1
#
interface Pos1/0/0
    link-protocol ppp
    undo shutdown
    ip address 100.1.1.1 255.255.255.0
#
return
```

- Configuration file of U-PE1

```
#           sysname U-PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls 12vpn
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface Pos1/0/0
    link-protocol ppp
    undo shutdown
    mpls 12vc 3.3.3.9 100
#
interface Pos2/0/0
    link-protocol ppp
    undo shutdown
    ip address 10.1.1.1 255.255.255.0
    mpls
    mpls ldp
#
interface LoopBack0
    ip address 1.1.1.9 255.255.255.255
#
ospf 1
    area 0.0.0.0
    network 10.1.1.0 0.0.0.255
    network 1.1.1.9 0.0.0.0
#
return
```

- Configuration file of P1

```
#           sysname P1
#
mpls lsr-id 2.2.2.9
mpls
```

```
#  
mpls ldp  
#  
interface Pos1/0/0  
link-protocol ppp  
undo shutdown  
ip address 10.1.1.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface Pos2/0/0  
link-protocol ppp  
undo shutdown  
ip address 20.1.1.1 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack0  
ip address 2.2.2.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
network 10.1.1.0 0.0.0.255  
network 20.1.1.0 0.0.0.255  
network 2.2.2.9 0.0.0.0  
#  
return
```

- Configuration file of S-PE

```
#  
Sysname S-PE  
#  
mpls lsr-id 3.3.3.9  
mpls  
#  
mpls l2vpn  
#  
mpls switch-l2vc 1.1.1.9 100 cir 3000 pir 4000 between 5.5.5.9 200 trans 200  
recv 100 cir 3000 pir 4000 encapsulation ppp mtu 4470  
#  
mpls ldp  
#  
mpls ldp remote-peer 1.1.1.9  
remote-ip 1.1.1.9  
#  
mpls ldp remote-peer 5.5.5.9  
remote-ip 5.5.5.9  
#  
interface Pos1/0/0  
link-protocol ppp  
undo shutdown  
ip address 20.1.1.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface Pos2/0/0  
link-protocol ppp  
undo shutdown  
ip address 30.1.1.1 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack0  
ip address 3.3.3.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
network 20.1.1.0 0.0.0.255  
network 30.1.1.0 0.0.0.255  
network 3.3.3.9 0.0.0.0
```

```
#  
return
```

- Configuration file of P2

```
#  
sysname P2  
#  
mpls lsr-id 4.4.4.9  
mpls  
#  
mpls ldp  
#  
interface Pos1/0/0  
link-protocol ppp  
undo shutdown  
ip address 30.1.1.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface Pos2/0/0  
link-protocol ppp  
undo shutdown  
ip address 40.1.1.1 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack0  
ip address 4.4.4.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
network 4.4.4.9 0.0.0.0  
network 30.1.1.0 0.0.0.255  
network 40.1.1.0 0.0.0.255  
#  
return
```

- Configuration file of U-PE2

```
#  
sysname U-PE2  
#  
mpls lsr-id 5.5.5.9  
mpls  
#  
mpls l2vpn  
#  
pw-template pwt  
peer-address 3.3.3.9  
#  
mpls ldp  
#  
mpls ldp remote-peer 3.3.3.9  
remote-ip 3.3.3.9  
#  
interface Pos1/0/0  
link-protocol ppp  
undo shutdown  
ip address 40.1.1.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface Pos2/0/0  
link-protocol ppp  
undo shutdown  
mpls static-l2vc pw-template pwt 200 transmit-vpn-label 100 receive-vpn-label  
200  
#  
interface LoopBack0  
ip address 5.5.5.9 255.255.255.255  
#
```

```

ospf 1
area 0.0.0.0
network 5.5.5.9 0.0.0.0
network 40.1.1.0 0.0.0.255
#
return
● Configuration file of CE2
#
sysname CE2
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 100.1.1.2 255.255.255.0
#
return

```

6.11.9 Example for Configuring Martini VPLS QoS

This part describes how to provide bandwidth assurance for VPLS by configuring QoS on VSIs.

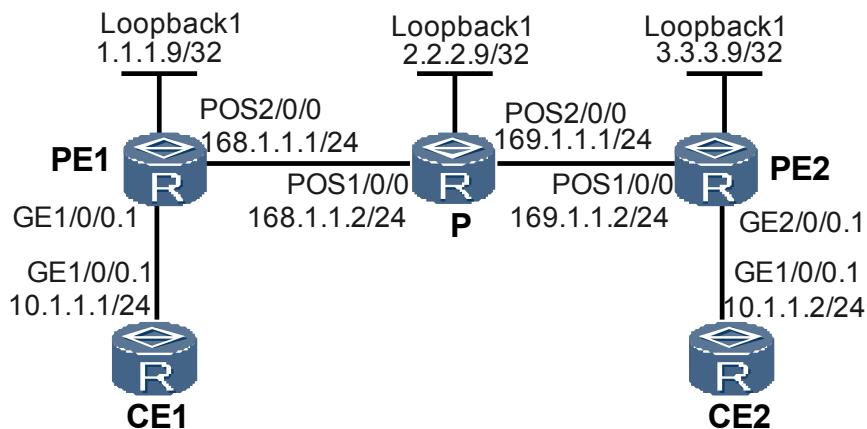
Networking Requirements

As shown in [Figure 6-10](#), VPLS needs to be enabled on PE1 and PE2. CE1 should be attached to PE1, and CE2 to PE2. CE1 and CE2 are on the same VPLS network. PWs should be established by using LDP as the VPLS signaling, and VPLS should be configured to achieve connectivity between CE1 and CE2.

Traffic policing needs to be implemented on the incoming traffic at the user side of PE2 to limit the bandwidth. The required CIR for the traffic going from CE2 to CE1 is 3000 kbit/s, and the required PIR is 4000 kbit/s.

Congestion avoidance and flow queue scheduling need to be carried out in the event of congestion. That is, when congestion occurs, packets should be dropped according to the WRED discard parameters configured for flow queues. The traffic shaping rates of flow queues AF1 and EF are 500 kbit/s and 1000 kbit/s respectively, and the traffic of flow queue AF1 is mapped to class queue EF.

Figure 6-10 Networking diagram for configuring Martini VPLS



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a routing protocol on the backbone to achieve connectivity between devices.
2. Set up remote LDP sessions between PEs.
3. Establish tunnels between PEs for transmitting user data.
4. Enable MPLS L2VPN on PEs.
5. Create VSIs on PEs, configure the signaling protocol to be LDP, and bind VSIs to AC interfaces.
6. Configure the QoS-profile and the scheduling parameters.
7. Configure QoS parameters on PE2.

Data Preparation

To complete the configuration, you need the following data:

- Name and ID of the VSI
- IP addresses of peers and tunnel policies used for setting up peer relationship
- Interface to which the VSI is bound
- The parameters of flow-wred, flow-queue, and the value of network-header-length in the QoS-profile
- CIR
- PIR

Procedure

- Step 1** Assign an IP address to each interface on the PEs and the P, as shown in [Figure 6-10](#). In this example, OSPF is adopted.

Note that when configuring OSPF, you need to advertise 32-bit loopback interface addresses (LSR IDs) of PE1, the P, and PE2.

After the configuration, run the **display ip routing-table** command on PE1, the P, and PE2. You can find that PE1, the P, and PE2 have learnt the route to each other.

For detailed configuration procedures, see the following configuration files.

- Step 2** Configure basic MPLS capabilities and LDP.

For detailed configuration procedures, see the following configuration files.

After the configuration, run the **display mpls ldp session** command on PE1, the P, and PE2. You can find that the status of the peer relationship between PE1 and the P, or between PE2 and the P is **Operational**, which indicates that the peer relationship is established. Run the **display mpls lsp** command, and you can view the setup of the LSP.

- Step 3** Establish remote LDP sessions between PEs.

Configure PE1.

```
[PE1] mpls ldp remote-peer 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] quit
```

Configure PE2.

```
[PE2] mpls ldp remote-peer 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] remote-ip 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] quit
```

After the configuration, run the **display mpls ldp session** on PE1 or PE2. You can find that the status of the peer relationship between PE1 and PE2 is **Operational**, which indicates that the peer relationship is established.

Step 4 Enable MPLS L2VPN on PEs.

Configure PE1.

```
[PE1] mpls l2vpn
```

Configure PE2.

```
[PE2] mpls l2vpn
```

Step 5 Configure VSIs on PEs.

Configure PE1.

```
[PE1] vsi a2 static
[PE1-vsi-a2] pwsignal ldp
[PE1-vsi-a2-ldp] vsi-id 2
[PE1-vsi-a2-ldp] peer 3.3.3.9
```

Configure PE2.

```
[PE2] vsi a2 static
[PE2-vsi-a2] pwsignal ldp
[PE2-vsi-a2-ldp] vsi-id 2
[PE2-vsi-a2-ldp] peer 1.1.1.9
```

Step 6 Bind VSIs to interfaces on PEs.

Configure PE1.

```
[PE1] interface gigabitethernet1/0/0.1
[PE1-GigabitEthernet1/0/0.1] shutdown
[PE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[PE1-GigabitEthernet1/0/0.1] 12 binding vsi a2
[PE1-GigabitEthernet1/0/0.1] undo shutdown
[PE1-GigabitEthernet1/0/0.1] quit
```

Configure PE2.

```
[PE2] interface gigabitethernet2/0/0.1
[PE2-GigabitEthernet2/0/0.1] shutdown
[PE2-GigabitEthernet2/0/0.1] vlan-type dot1q 10
[PE2-GigabitEthernet2/0/0.1] 12 binding vsi a2
[PE2-GigabitEthernet2/0/0.1] undo shutdown
[PE2-GigabitEthernet2/0/0.1] quit
```

Step 7 Configure CEs.

Configure CE1.

```
<HUAWEI> sysname CE1
[CE1] interface gigabitethernet1/0/0.1
[CE1-GigabitEthernet1/0/0.1] shutdown
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE1-GigabitEthernet1/0/0.1] ip address 10.1.1.1 255.255.255.0
[CE1-GigabitEthernet1/0/0.1] undo shutdown
[CE1-GigabitEthernet1/0/0.1] quit
```

Configure CE2.

```
<HUAWEI> sysname CE2
[CE2] interface gigabitethernet1/0/0.1
[CE2-GigabitEthernet1/0/0.1] shutdown
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE2-GigabitEthernet1/0/0.1] ip address 10.1.1.2 255.255.255.0
[CE2-GigabitEthernet1/0/0.1] undo shutdown
[CE2-GigabitEthernet1/0/0.1] quit
```

Step 8 Configure the QoS-profile and the scheduling parameters. See [Example for Configuring BGP/MPLS IP VPN QoS step 2.](#)

Step 9 # Configure QoS parameters on PE2, and enable traffic statistics.

```
[PE2] vsi a2 static
[PE2-vsi-a2] qos cir 3000 pir 4000 qos-profile test
[PE2-vsi-a2] traffic-statistics enable
```

Step 10 Verify the configuration.

After the preceding configurations, run the **display vsi name a2 verbose** command on PE2, and you can view that the VSI named a2 has established a PW to PE1, and the status of the VSI is Up.

```
<PE2> display vsi name a2 verbose
***VSI Name : a2
Administrator VSI : no
Isolate Spoken : disable
VSI Index : 0
PW Signaling : ldp
Member Discovery Style : static
PW MAC Learn Style : unqualify
Encapsulation Type : vlan
MTU : 1500
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : 255
Domain Name :
Ignore AcState : disable
Create Time : 0 days, 3 hours, 30 minutes, 31 seconds
VSI State : up
L2VPN QoS CIR value : 3000
L2VPN QoS PIR value : 4000
L2VPN QoS qos-profile name: test
VSI ID : 2
*Peer Router ID : 1.1.1.9
VC Label : 23552
Peer Type : dynamic
Session : up
Tunnel ID : 0x2002001,
Broadcast Tunnel ID : 0x2002001
CKey : 2
NKey : 1
Interface Name : GigabitEthernet1/0/0.1
State : up
Last Up Time : 2008-08-15 15:41:59
Total Up Time : 0 days, 0 hours, 1 minutes, 2 seconds
***PW Information:
*Peer Ip Address : 1.1.1.9
PW State : up
Local VC Label : 23552
Remote VC Label : 23552
PW Type : label
Tunnel ID : 0x2002001,
Broadcast Tunnel ID : 0x2002001
Ckey : 0x2
Nkey : 0x1
Main PW Token : 0x2002001
```

```

Slave PW Token      : 0x0
Tnl Type           : LSP
OutInterface       : Pos1/0/0
Stp Enable         : 0
Mac Flapping       : 0
PW Last Up Time   : 2009-04-22 15:41:59
PW Total Up Time  : 0 days, 0 hours, 1 minutes, 3 seconds

```

CE1 (10.1.1.1) can ping through CE2 (10.1.1.2).

```

<CE1> ping 10.1.1.2
PING 10.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=90 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=77 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=255 time=34 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=255 time=46 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=255 time=94 ms
--- 10.1.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 34/68/94 ms

```

On PE2, view traffic statistics of the VPLS.

```

<PE2> display traffic-statistics vsi a2 qos
VSI name : a2
Statistics last cleared : never
Last 300 seconds QoS statistics rate : 0 bits/sec, 0 packets/sec
QoS statistics output: 16 bytes, 16 packets
PacketRate : Last 300 seconds packets rate(packets/sec)
ByteRate : Last 300 seconds bytes rate(bits/sec)
Passed traffic statistics :
  Queue Packets     Bytes     PacketRate   ByteRate
  ----- -----
  be      0          0          0          0
  af1     0          0          0          0
  af2     0          0          0          0
  af3     0          0          0          0
  af4     0          0          0          0
  ef      0          0          0          0
  cs6     0          0          0          0
  cs7     0          0          0          0
  -----
Discarded traffic statistics :
  Queue Packets     Bytes     PacketRate   ByteRate
  ----- -----
  be      0          0          0          0
  af1     0          0          0          0
  af2     0          0          0          0
  af3     0          0          0          0
  af4     0          0          0          0
  ef      0          0          0          0
  cs6     0          0          0          0
  cs7     0          0          0          0
  -----

```

----End

Configuration Files

- Configuration file of CE1

```

#
sysname CE1
#
interface GigabitEthernet1/0/0.1
  undo shutdown
  vlan-type dot1q 10

```

```
ip address 10.1.1.1 255.255.255.0
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
return
```

- Configuration file of PE1

```
#
sysname PE1
#
mpls lsr-id 1.1.1.9
mpls
#
mpls 12vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 3.3.3.9
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface GigabitEthernet1/0/0.1
undo shutdown
vlan-type dot1q 10
12 binding vsi a2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 168.1.1.0 0.0.0.255
#
return
```

- Configuration file of the P

```
#
sysname P
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 168.1.1.2 255.255.255.0
mpls
```

```
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 168.1.1.0 0.0.0.255
network 169.1.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return
```

- Configuration file of PE2

```
#
sysname PE2
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
flow-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
flow-mapping test
map flow-queue af1 to port-queue ef
#
flow-queue test
queue af1 lpq shaping 500 flow-wred test
queue ef pq shaping 1000 flow-wred test
#
service-template test
network-header-length 12 outbound
#
qos-profile test
mpls-hqos flow-queue test flow-mapping test service-template test
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 1.1.1.9
qos cir 3000 pir 4000 qos-profile test
traffic-statistics enable
#
mpls ldp
#
mpls ldp remote-peer 1.1.1.9
remote-ip 1.1.1.9
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 169.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface GigabitEthernet2/0/0.1
undo shutdown
vlan-type dot1q 10
12 binding vsi a2
```

```
#  
interface LoopBack1  
    ip address 3.3.3.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
    network 3.3.3.9 0.0.0.0  
    network 169.1.1.0 0.0.0.255  
#  
return
```

7

MPLS DiffServ-Mode Configuration

About This Chapter

The MPLS DiffServ model defines two factors for the packets that are transmitted over an MPLS network: the manner in which the DSCP field and the EXP field are propagated and the PHB such as the CoS and color after the packet leaves the MPLS network. In this manner, differentiated QoS is guaranteed for packets.

[7.1 Introduction](#)

This section describes three MPLS DiffServ modes: Uniform, Pipe, and Short Pipe.

[7.2 Configuring Uniform/Pipe Model for MPLS TE](#)

On an MPLS network, to provide differentiated priorities for MPLS TE services, you need to configure the Uniform/Pipe mode to implement queue scheduling according to different CoSs.

[7.3 Configuring Pipe/Short Pipe Model Based on VPN](#)

Multiple VPNs may share one MPLS TE tunnel. To provide differentiated priorities for VPN services, you need to configure Pipe/Short Pipe mode for VPN to implement queue scheduling according to CoSs.

[7.4 Configuration Examples](#)

This section provides examples for configuring MPLS DiffServ, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

7.1 Introduction

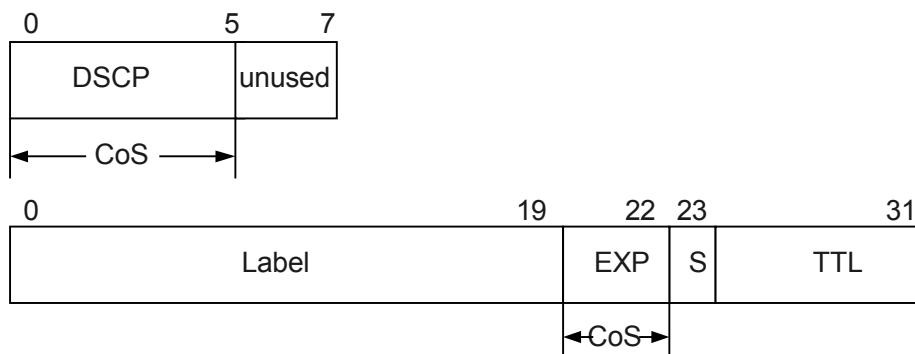
This section describes three MPLS DiffServ modes: Uniform, Pipe, and Short Pipe.

7.1.1 MPLS DiffServ Models Overview

The MPLS DiffServ model defines two factors for the packets that are transmitted over an MPLS network: the manner in which the DSCP field and the EXP field are propagated and the PHB such as the CoS and color after the packet leaves the MPLS network. In this manner, differentiated QoS is guaranteed for transmission.

The DSCP field (6 bits) in the header of the IP packet is used to define the Class of Service (CoS). In the MPLS label, the EXP field (3 bits) is also used to define the CoS. See [Figure 7-1](#).

Figure 7-1 The DSCP field in the IP packet and the EXP field in the MPLS packet



In the MPLS DiffServ model, packets are processed in the following steps:

- When a packet enters the MPLS network, a label is added to the packet. The DSCP field in the packet is copied to the EXP field.
- In the MPLS network, the PHB is chosen according to the EXP value in the packet. Each EXP value is mapped with a PHB.
- When the packet leaves the MPLS network, the label is stripped. Then, the PHB is chosen according to the DSCP or EXP field. Each DSCP value is also mapped with a PHB.

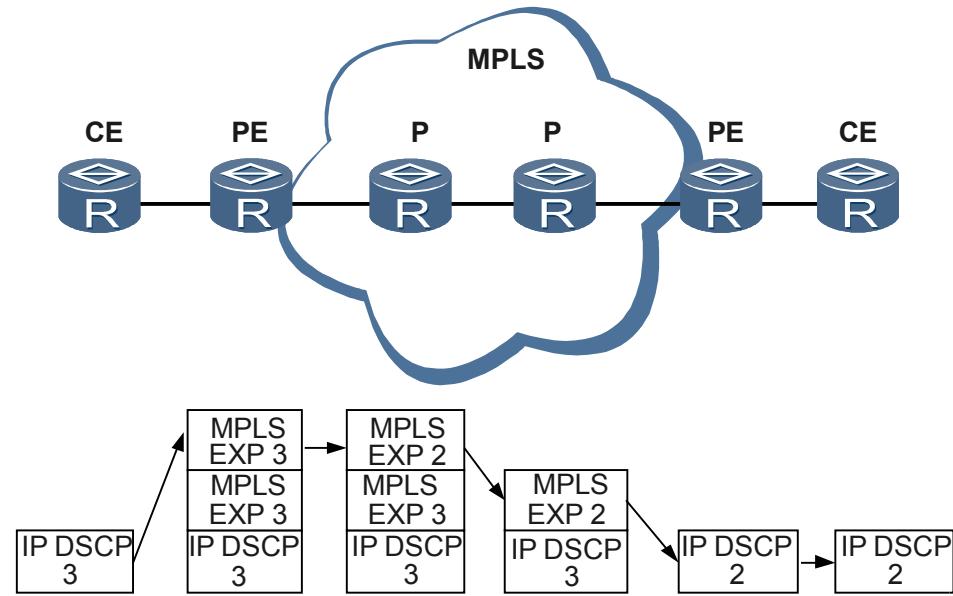
The MPLS DiffServ model defines the following factors for the packets that pass through an MPLS network: the manner in which the DSCP field and the EXP field are propagated and PHB such as CoS and color after the packet leaves the MPLS network. Thus, transmission with differentiated QoS is carried out.

In the RFC 3270, three MPLS DiffServ models are defined: Uniform, Pipe, and Short Pipe.

Uniform Model

The ingress PE adds a label to the packet by copying the DSCP value to the EXP field. If the EXP value is changed in the MPLS network, the change affects the PHB adopted when the packet leaves the MPLS network. That is, the egress PE adopts the PHB according to the EXP value. See [Figure 7-2](#).

Figure 7-2 Uniform model



Pipe Model

In the Pipe model, the user-defined CoS and color together determine the EXP value that is added to the MPLS label by the ingress PE. The default mapping between the CoS value and the EXP value is shown in [Table 7-1](#). If the EXP value is changed in the MPLS network, the change is valid only in the MPLS network. The egress PE selects the PHB according to the EXP value. When the packet leaves the MPLS network, the DSCP value becomes effective again. See [Figure 7-3](#).

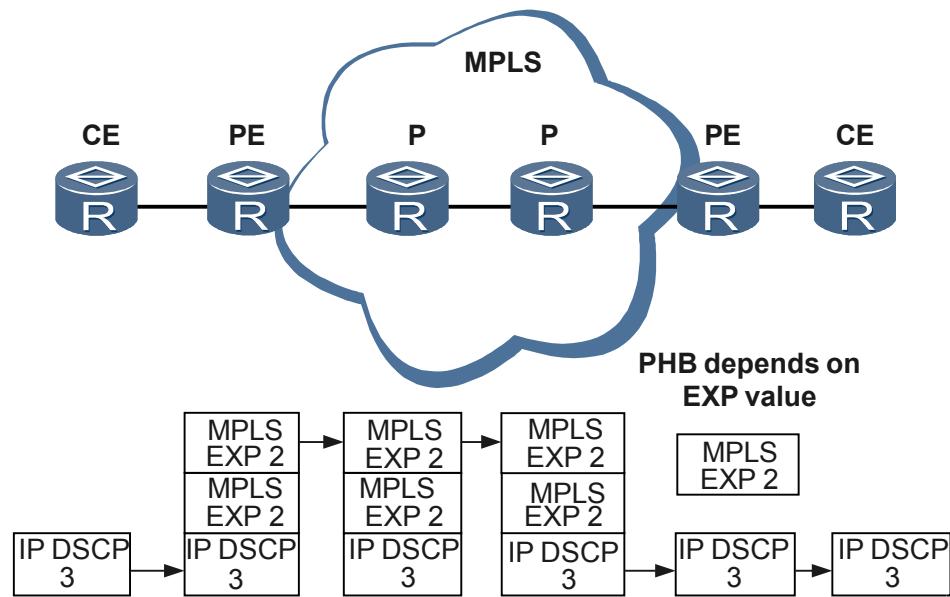
NOTE

The Pipe model does not support the Penultimate Hop Popping of the MPLS label.

Table 7-1 Default mapping between the CoS value and the EXP value

CoS	Color	MPLS EXP
BE	Green	0
AF1	Green, Yellow, Red	1
AF2	Green, Yellow, Red	2
AF3	Green, Yellow, Red	3
AF4	Green, Yellow, Red	4
EF	Green	5
CS6	Green	6
CS7	Green	7

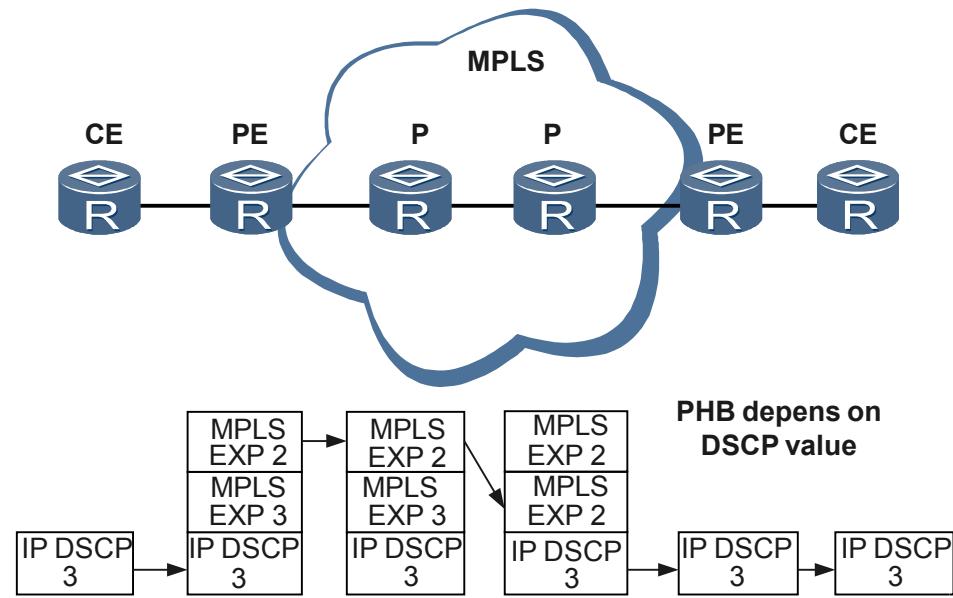
Figure 7-3 Pipe model



Short Pipe Model

In the Short Pipe model, the user-defined CoS and color together determine the EXP value that is added to the MPLS label by the ingress PE. If the EXP value is changed in the MPLS network, the change is valid only in the MPLS network. The egress PE selects the PHB according to the DSCP value. When the packet leaves the MPLS network, the DSCP value becomes effective again. See [Figure 7-4](#).

Figure 7-4 Short Pipe model



7.1.2 MPLS Pipe/Short Pipe supported by NE80E/40E

The MPLS DiffServ modes supported by the TE, L3VPN, and VLL can be configured on the device.

The MPLS Pipe/Short Pipe supports the queue scheduling according to eight priorities and implements the following functions:

- TE supports to configure uniform and Pipe models.
- L3VPN supports to configure uniform, Pipe and Short Pipe models.
- VPLS supports to configure uniform, Pipe and Short Pipe models.
- VLL supports to configure uniform, Pipe and Short Pipe models.

7.2 Configuring Uniform/Pipe Model for MPLS TE

On an MPLS network, to provide differentiated priorities for MPLS TE services, you need to configure the Uniform/Pipe mode to implement queue scheduling according to different CoSs.

7.2.1 Establishing the Configuration Task

Before configuring the Uniform/Pipe mode for MPLS TE, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In the MPLS public network, to ensure the priorities of different MPLS TE services, you need to configure the Uniform/Pipe mode to implement queue scheduling according to different service classes.

Pre-configuration Tasks

Before configuring uniform/Pipe model for MPLS TE, complete the following tasks:

- Configuring the physical parameters and link attributes to ensure normal operation of the interfaces
- Configuring an MPLS TE tunnel between PEs. For details, refer to "MPLS TE Configuration" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - MPLS*.



Before configuring the MPLS TE uniform/Pipe mode, you need to confirm that the MPLS TE is Up.

Data Preparation

To configure uniform/Pipe model for MPLS TE, you need the following data.

No.	Data
1	CoS and color of IP packets in DiffServ model

7.2.2 Enabling MPLS TE to Support DiffServ Models

On an interface enabled with MPLS TE, you can configure Uniform/Pipe mode for MPLS TE.

Context

Do as follows on the Tunnel interface on the user side of an ingress PE.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel interface-number
```

The Tunnel interface view of the user side is displayed.



MPLS TE must be enabled on the interface and the state is UP.

Step 3 Run:

```
diffserv-mode { pipe service-class color | uniform }
```

A DiffServ model for MPLS TE is set.

----End

7.3 Configuring Pipe/Short Pipe Model Based on VPN

Multiple VPNs may share one MPLS TE tunnel. To provide differentiated priorities for VPN services, you need to configure Pipe/Short Pipe mode for VPN to implement queue scheduling according to CoSs.

7.3.1 Establishing the Configuration Task

Before configuring Pipe/Short Pipe mode for a VPN, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In VPN environment, sometimes multiple VPNs share one MPLS TE tunnel. This may result in the following problems: VPNs compete for resources. To ensure the priorities of different VPN services, you need to configure MPLS Pipe/Short Pipe to implement queue scheduling according to different service classes.

Pre-configuration Tasks

Before configuring MPLS Pipe/Short Pipe model, complete the following tasks:

- Configuring the physical parameters and link attributes to ensure normal operation of the interfaces.
- Configuring an MPLS TE tunnel between PEs. For details, refer to "MPLS TE Configuration" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - MPLS*.
- Configuring L3VPN or L2VPN to enable normal communications. For details, refer to HUAWEI NetEngine80E/40E Router *Configuration Guide - VPN*.
- Configuring the simple traffic classification or complex traffic classification on the interface on the user side of the ingress PE. For details, refer to "Class-based QoS Configuration" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - QoS*.



NOTE

- If both the simple traffic classification and the Pipe (or Short Pipe) model are configured on the interface on the user side of an ingress PE, the VPN prefers the Pipe (or Short Pipe) model.
- If you have configured the L3VPN to support the Pipe model, you are unnecessary to configure the simple traffic classification.

Data Preparation

To configure Pipe/Short Pipe model based on VPN, you need the following data.

No.	Data
1	CoS and color of IP packets in DiffServ models

7.3.2 (Optional) Enabling BGP/MPLS IP VPN to Support DiffServ Models

You can configure Pipe/Short Pipe mode for a VPN instance to implement queue scheduling according to CoSs.

Context

Do as follows on the ingress PE device:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip vpn-instance vpn-instance-name
```

A VPN instance is created and the VPN instance view is displayed.

Step 3 Run:

```
diffserv-mode { pipe service-class color | short-pipe service-class color [ domain ds-name ] | uniform }
```

A DiffServ model for a VPN instance is set.



If the DiffServ model is set to Uniform, you need to configure simple traffic classification. Otherwise, this configuration does not take effect.

----End

7.3.3 (Optional) Enabling an VLL to Support DiffServ Models

When multiple VPNs share one MPLS TE tunnel, you need to configure Pipe/Short Pipe mode for a VPN to implement queue scheduling according to CoSs. You can enable a VLL to support the DiffServ mode on the L2VPN-bound user-side interface.

Context

Do as follows on the interface on the user side of the ingress PE device where resources are reserved:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on the user side is displayed.

 NOTE

This interface is a user-side interface configured with L2VPN services.

Step 3 Run:

```
diffserv-mode { pipe service-class color | uniform }
```

A DiffServ model in the VLL networking mode is set.

 NOTE

If the DiffServ model is set to Uniform, you need to configure simple traffic classification. Otherwise, this configuration does not take effect.

----End

7.3.4 (Optional) Enabling an VPLS to Support DiffServ Models

When multiple VPNs share one MPLS TE tunnel, you need to configure Pipe/Short Pipe mode for a VPN to implement queue scheduling according to CoSs. You can enable a VPLS to support the DiffServ mode in a VSI instance.

Context

 NOTE

- Enabling the VPN to support the DiffServ model is an optional setting. You can perform this configuration according to the actual conditions of networks. If you do not enable VPNs to support a specific DiffServ model, the system defaults the Uniform model.
- When both the simple traffic classification and the Pipe or Short Pipe model are configured, the Pipe or Short Pipe model takes effect.

The three DiffServ models are Pipe, Short Pipe, and Uniform.

- If the Pipe model is set for a VPN, the EXP value of the MPLS label pushed on the ingress PE device is determined by both the class of service (CoS) and the color specified by users. After an MPLS label is popped out by the egress PE device, the DSCP value of an IP packet is not changed. Then the EXP value of the MPLS label determines the packet forwarding behavior of the egress node.
- If the Short Pipe model is set for a VPN, the EXP value of the MPLS label pushed on the ingress PE device is determined by both the CoS and the color specified by users. After an MPLS label is popped out by the egress PE, the DSCP value of an IP packet is not changed. Then the DSCP value of the IP packet determines the packet forwarding behavior of the egress node.
- If the Uniform model is set for a VPN, the EXP value of the MPLS label pushed on the ingress PE is determined by the mapped DSCP value of an IP packet. After an MPLS label is popped out by the egress PE, the EXP value is mapped as the DSCP value of an IP packet. Then the mapped DSCP value of the IP packet determines the packet forwarding behavior of the egress node. The default model is Uniform.

When you configure a DiffServ model,

- If you want the MPLS network to differentiate service priorities, you can choose the Uniform model.
- If you do not want the MPLS network to differentiate service priorities, you can choose the Pipe or Short Pipe model.

Do as follows on the ingress PE device where resources are reserved:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vsi vsi-name [ auto | static ]
```

A virtual switching instance (VSI) is created and the VSI view is displayed.

Step 3 Run:

```
diffserv-mode { pipe service-class color | short-pipe service-class color [ domain ds-name ] | uniform }
```

The DiffServ model for a VSI is set.



If the DiffServ model is set to Uniform, you need to configure simple traffic classification. Otherwise, this configuration does not take effect.

----End

7.3.5 Checking the Configuration

After MPLS DiffServ information is configured, you can view the information about MPLS DiffServ.

Context

Run the following commands to check the previous configuration.

Procedure

- Using the **display ip vpn-instance [verbose] [vpn-instance-name]** command to check information about the MPLS DiffServ in the BGP/MPLS IP VPN.
- Using the **display vsi [vsi-name] [verbose]** command to check information about the VPLS MPLS DiffServ.

----End

Example

Run the **display ip vpn-instance [verbose] [vpn-instance-name]** command, and you can view information about the MPLS DiffServ in the BGP/MPLS IP VPN.

```
<HUAWEI>display ip vpn-instance verbose
Total VPN-Instances configured : 1
VPN-Instance Name and ID : vpna, 1
Create date : 2008/04/26 22:31:05
Up time : 0 days, 03 hours, 35 minutes and 20 seconds
Label policy : label per route
The diffserv-mode Information is : Pipe af1 green
The ttl-mode Information is : Pipe
```

Run the **display vsi [vsi-name] [verbose]** command, and you can view information about the MPLS DiffServ in the VPLS.

```
<PE1> display vsi verbose
```

```
***VSI Name          : a2
Administrator VSI   : no
Isolate Spoken      : disable
VSI Index           : 0
PW Signaling        : ldp
Member Discovery Style: static
PW MAC Learn Style : unqualify
Encapsulation Type : vlan
MTU                 : 1500
Mode                : Pipe
Service Class       : af3
Color               : green
DomainId            :
Domain Name         :
Tunnel Policy Name : policy1
VSI State           : up
VSI ID              : 2
*Peer Router ID    : 3.3.3.9
VC Label             :
Peer Type            : dynamic
Session              : up
Tunnel ID            : 0x60018000,
Interface Name       : GigabitEthernet2/0/0.1
State               : up
**PW Information:
*Peer Ip Address   : 3.3.3.9
PW State             : up
Local VC Label      : 117760
Remote VC Label     : 117759
PW Type              : label
Tunnel ID            : 0x60618013
```

7.4 Configuration Examples

This section provides examples for configuring MPLS DiffServ, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

 **NOTE**

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

7.4.1 Example for Configuring an MPLS DiffServ Mode

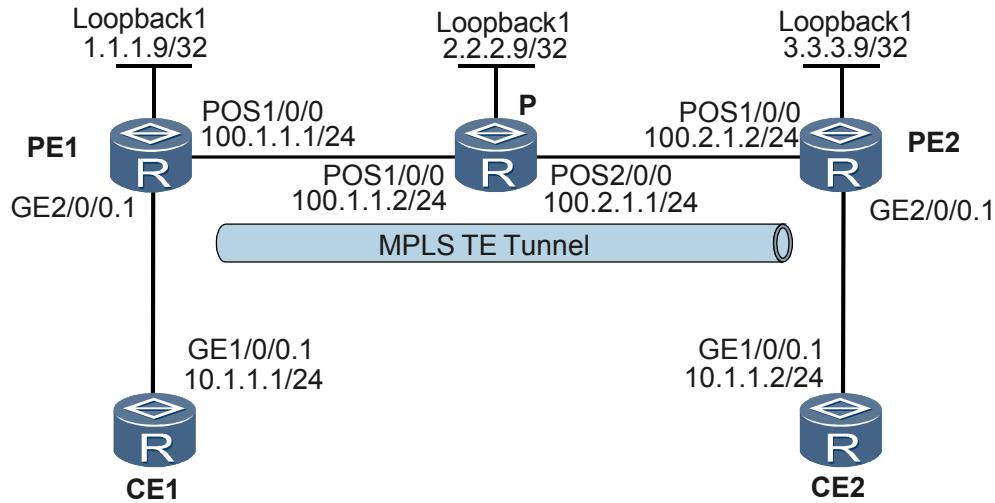
This section describes how to configure MPLS DiffServ.

Networking Requirements

As shown in [Figure 7-5](#), CE1 and CE2 belong to the same VPLS and access the MPLS backbone network respectively through PE1 and PE2. In the MPLS backbone network, OSPF is used as the IGP protocol.

On PE1, the bandwidth for VPN traffic of CE1 is 1 Mbit/s. The Pipe mode needs to be configured on PE1 to implement the MPLS DiffServ. VPN services are forwarded in the MPLS network with the priority configured by the service carrier. The egress router of the MPLS network does not change the 8021p value of the packet and only implements queue scheduling according to the EXP value in the MPLS label.

Figure 7-5 Networking diagram for configuring an MPLS DiffServ model



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure routing protocols and enable MPLS on the PE and P devices
2. Create the MPLS TE tunnel and configure tunnel policies. For detailed configuration, refer to the "MPLS TE Configuration" in the HUAWEI NetEngine80E/40E Router Configuration Guide - MPLS
3. Configure VPLS over TE. For detailed configuration, refer to the "VPLS Configuration" in the HUAWEI NetEngine80E/40E Router Configuration Guide - VPN.
4. Configure traffic policing on PE1 based on the complex traffic classification.
5. Configure the MPLS DiffServ mode on PE1.

Data Preparations

To complete the configuration, you need the following data:

- Names of traffic classifiers, traffic behaviors, and traffic policies
- CIR used in traffic policing
- CoS values and colors of IP packets in the Pipe mode

Procedure

Step 1 Configure IP addresses for the interfaces and configure OSPF.

The detailed configuration is not mentioned here.

Step 2 Enable MPLS, MPLS TE, MPLS RSVP-TE, and MPLS CSPF. Configure OSPF TE.

On the nodes along the MPLS TE tunnel, enable MPLS, MPLS TE, and MPLS RSVP-TE both in the system view and the interface view. On the ingress node of the tunnel, enable MPLS CSPF in the MPLS view.

Configure PE1.

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] mpls te
[PE1-mpls] mpls rsvp-te
[PE1-mpls] mpls te cspf
[PE1-mpls] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] undo shutdown
[PE1-Pos1/0/0] mpls
[PE1-Pos1/0/0] mpls te
[PE1-Pos1/0/0] mpls rsvp-te
[PE1-Pos1/0/0] quit
[PE1] ospf
[PE1-ospf-1] opaque-capability enable
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] mpls-te enable
[PE1-ospf-1-area-0.0.0.0] quit
```

Configure the P.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] mpls te
[P-mpls] mpls rsvp-te
[P-mpls] quit
[P] interface pos1/0/0
[P-Pos1/0/0] undo shutdown
[P-Pos1/0/0] mpls
[P-Pos1/0/0] mpls te
[P-Pos1/0/0] mpls rsvp-te
[P-Pos1/0/0] quit
[P] interface pos2/0/0
[P-Pos2/0/0] undo shutdown
[P-Pos2/0/0] mpls
[P-Pos2/0/0] mpls te
[P-Pos2/0/0] mpls rsvp-te
[P-Pos2/0/0] quit
[P] ospf
[P-ospf-1] opaque-capability enable
[P-ospf-1] area 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 100.2.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] mpls-te enable
[P-ospf-1-area-0.0.0.0] quit
```

Configure PE2.

The configuration of PE2 is similar to that of PE1, and is not mentioned here.

Step 3 Configure the Tunnel interface.

Create tunnel interfaces on the PE devices. Set the tunneling protocol to be MPLS TE and the signaling protocol to be RSVP-TE.

Configure PE1.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface loopback1
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[PE1-Tunnel1/0/0] destination 3.3.3.9
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
[PE1-Tunnel1/0/0] mpls te reserved-for-binding
[PE1-Tunnel1/0/0] mpls te commit
```

Configure PE2.

```
[PE2] interface tunnel 1/0/0
[PE2-Tunnel1/0/0] ip address unnumbered interface loopback1
[PE2-Tunnel1/0/0] tunnel-protocol mpls te
[PE2-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[PE2-Tunnel1/0/0] destination 1.1.1.9
[PE2-Tunnel1/0/0] mpls te tunnel-id 100
[PE2-Tunnel1/0/0] mpls te reserved-for-binding
[PE2-Tunnel1/0/0] mpls te commit
```

After the preceding configuration, run the **display this interface** command in the tunnel interface view. The command output shows that the value of **Line protocol current state** is UP. It indicates that the MPLS TE tunnel is set up successfully. Take the display on PE1 for an example:

```
[PE1-Tunnel1/0/0] display this interface
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Description: Tunnel1/0/0 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1(1.1.1.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 3.3.3.9
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x1002003, secondary tunnel id is 0x0
    5 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets output, 0 bytes
    0 output error
```

Step 4 Set up LDP sessions.

Set up LDP sessions between PE1 and PE2.

Configure PE1.

```
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] mpls ldp remote-peer 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-3.3.3.9] quit
```

Configure PE2.

```
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] mpls ldp remote-peer 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] remote-ip 1.1.1.9
[PE2-mpls-ldp-remote-1.1.1.9] quit
```

After the above configuration, the LDP session should be set up between the PE devices.

Take the display on PE1 for an example:

```
[PE1] display mpls ldp session
      LDP Session(s) in Public Network
-----
Peer-ID          Status        LAM   SsnRole   SsnAge       KA-Sent/Rcv
-----
3.3.3.9:0        Operational DU    Passive   000:00:06   26/26
-----
TOTAL: 1 session(s) Found.
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Step 5 Create VSIs on the PE devices and configure tunnel policies.

Configure PE1.

```
[PE1] tunnel-policy policy1
[PE1-tunnel-policy-policy1] tunnel binding destination 3.3.3.9 te tunnel1/0/0
```

```
[PE1-tunnel-policy-policy1] quit
[PE1] mpls l2vpn
[PE1] vsi a2 static
[PE1-vsi-a2] pwsignal ldp
[PE1-vsi-a2-ldp] vsi-id 2
[PE1-vsi-a2-ldp] peer 3.3.3.9
[PE1-vsi-a2-ldp] quit
[PE1-vsi-a2] tnl-policy policy1

# Configure PE2.

[PE2] tunnel-policy policy1
[PE2-tunnel-policy-policy1] tunnel binding destination 1.1.1.9 to tunnell1/0/0
[PE2-tunnel-policy-policy1] quit
[PE2] mpls l2vpn
[PE2] vsi a2 static
[PE2-vsi-a2] pwsignal ldp
[PE2-vsi-a2-ldp] vsi-id 2
[PE2-vsi-a2-ldp] peer 1.1.1.9
[PE2-vsi-a2-ldp] quit
[PE2-vsi-a2] tnl-policy policy1
```

Step 6 Bind VSIs to the interfaces on the PEs.

Configure PE1.

```
[PE1] interface gigabitethernet2/0/0.1
[PE1-GigabitEthernet2/0/0.1] vlan-type dot1q 10
[PE1-GigabitEthernet2/0/0.1] 12 binding vsi a2
```

Configure PE2.

```
[PE2] interface gigabitethernet2/0/0.1
[PE2-GigabitEthernet2/0/0.1] vlan-type dot1q 10
[PE2-GigabitEthernet2/0/0.1] 12 binding vsi a2
```

Configure CE1.

```
<HUAWEI> sysname CE1
[CE1] interface gigabitethernet1/0/0.1
[CE1-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE1-GigabitEthernet1/0/0.1] ip address 10.1.1.1 255.255.255.0
```

Configure CE2.

```
<HUAWEI> sysname CE2
[CE2] interface gigabitethernet1/0/0.1
[CE2-GigabitEthernet1/0/0.1] vlan-type dot1q 10
[CE2-GigabitEthernet1/0/0.1] ip address 10.1.1.2 255.255.255.0
```

Step 7 On PE1, configure traffic policing for VPN traffic of CE1.

```
<PE1> system-view
[PE1] traffic classifier car
[PE1-classifier-car] if-match any
[PE1-classifier-car] quit
[PE1] traffic behavior car
[PE1-behavior-car] car cir 1000 green pass red discard
[PE1-behavior-car] quit
[PE1] traffic policy car
[PE1-trafficpolicy-car] classifier car behavior car
[PE1-trafficpolicy-car] quit
[PE1] interface gigabitethernet2/0/0.1
[PE1-GigabitEthernet2/0/0.1] undo shutdown
[PE1-GigabitEthernet2/0/0.1] traffic-policy car inbound
[PE1-GigabitEthernet2/0/0.1] quit
```

Step 8 Set the MPLS DiffServ model on PE1 and PE2.

Configure PE1.

```
[PE1] vsi a2
[PE1-vsi-a2] diffserv-mode pipe af3 green
[PE1-vsi-a2] quit
[PE1] mpls
[PE1-mpls] label advertise non-null
[PE1-mpls] quit

# Configure PE1.

[PE2] vsi a2
[PE2-vsi-a2] diffserv-mode pipe af3 green
[PE2-vsi-a2] quit
[PE2] mpls
[PE2-mpls] label advertise non-null
[PE2-mpls] quit
```

Step 9 Verify the configuration.

Run the **display vsi verbose** command on PE1. The command output shows that the MPLS DiffServ mode is Pipe.

```
<PE1> display vsi verbose
***VSI Name : a2
    Administrator VSI : no
    Isolate Spoken : disable
    VSI Index : 0
    PW Signaling : ldp
    Member Discovery Style : static
    PW MAC Learn Style : unqualify
    Encapsulation Type : vlan
    MTU : 1500
    Mode : pipe
    Service Class : af3
    Color : green
    DomainId : 0
    Domain Name :
    Tunnel Policy Name : policy1
    VSI State : up
    VSI ID : 2
    *Peer Router ID : 3.3.3.9
    VC Label : 117760
    Peer Type : dynamic
    Session : up
    Tunnel ID : 0x60018000,
    Interface Name : GigabitEthernet2/0/0.1
    State : up
    Last Up Time : 2008/08/15 15:41:59
    Total Up Time : 0 days, 0 hours, 1 minutes, 2 seconds
**PW Information:
    *Peer Ip Address : 3.3.3.9
    PW State : up
    Local VC Label : 117760
    Remote VC Label : 117759
    PW Type : label
    Tunnel ID : 0x60618013
    PW Last Up Time : 2008/08/15 15:41:59
    PW Total Up Time : 0 days, 0 hours, 1 minutes, 3 seconds
```

----End

Configuration Files

- Configuration file of PE1

```
# sysname PE1
#
mpls lsr-id 1.1.1.9
mpls
```

```

mpls te
mpls rsvp-te
mpls te cspf
label advertise non-null
#
mpls l2vpn
#
vsi a2 static
pwsignal ldp
vsi-id 2
peer 3.3.3.9
tnl-policy policy1
diffserv-mode pipe af3 green
#
mpls ldp
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
traffic classifier car
if-match any
#
traffic behavior car
car cir 1000 cbs 10000 pbs 0 green pass red discard
#
traffic policy car
classifier car behavior car
#
mpls ldp remote-peer 3.3.3.9
remote-ip 3.3.3.9
#
interface Pos1/0/0
undo shutdown
link-protocol ppp
ip address 100.1.1.1 255.255.255.0
mpls
mpls te
mpls rsvp-te
#
interface GigabitEthernet2/0/0
undo shutdown
#
interface GigabitEthernet2/0/0.1
vlan-type dot1q 10
l2 binding vsi a2
traffic-policy car inbound
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 3.3.3.9
mpls te tunnel-id 100
mpls te reserved-for-binding
mpls te commit
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 100.1.1.0 0.0.0.255
mpls-te enable
#
tunnel-policy policy1
tunnel binding destination 3.3.3.9 te tunnel1/0/0
#
return

```

- Configuration file of the P

```
#  
    sysname P  
#  
    mpls lsr-id 2.2.2.9  
    mpls  
        mpls te  
        mpls rsvp-te  
#  
    interface Pos1/0/0  
    undo shutdown  
    link-protocol ppp  
        ip address 100.1.1.2 255.255.255.0  
    mpls  
        mpls te  
        mpls rsvp-te  
#  
    interface Pos2/0/0  
    undo shutdown  
    link-protocol ppp  
        ip address 100.2.1.1 255.255.255.0  
    mpls  
        mpls te  
        mpls rsvp-te  
#  
    interface LoopBack1  
        ip address 2.2.2.9 255.255.255.255  
#  
ospf 1  
    opaque-capability enable  
area 0.0.0.0  
    network 2.2.2.9 0.0.0.0  
    network 100.1.1.0 0.0.0.255  
    network 100.2.1.0 0.0.0.255  
    mpls-te enable  
#  
return
```

- Configuration file of PE2

```
#  
    sysname PE2  
#  
    mpls lsr-id 3.3.3.9  
    mpls  
        mpls te  
        mpls rsvp-te  
        mpls te cspf  
        label advertise non-null  
#  
    mpls l2vpn  
#  
vsi a2 static  
    pwsignal ldp  
        vsi-id 2  
        peer 1.1.1.9  
        tnl-policy policy1  
        diffserv-mode pipe af3 green  
#  
    mpls ldp  
#  
        mpls ldp remote-peer 1.1.1.9  
        remote-ip 1.1.1.9  
#  
    interface Pos1/0/0  
    undo shutdown  
    link-protocol ppp  
        ip address 100.2.1.2 255.255.255.0  
    mpls  
        mpls te
```

```
mpls rsvp-te
mpls te cspf
#
interface GigabitEthernet2/0/0
undo shutdown
#
interface GigabitEthernet2/0/0.1
vlan-type dot1q 10
12 binding vsi a2
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
interface Tunnel1/0/0
ip address unnumbered interface LoopBack1
tunnel-protocol mpls te
destination 1.1.1.9
mpls te tunnel-id 100
mpls te reserved-for-binding
mpls te commit
#
ospf 1
opaque-capability enable
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 100.2.1.0 0.0.0.255
mpls-te enable
#
tunnel-policy policy1
tunnel binding destination 1.1.1.9 te tunnel1/0/0
#
return
```

- Configuration file of CE1

```
#
sysname CE1
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.1 255.255.255.0
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
vlan-type dot1q 10
ip address 10.1.1.2 255.255.255.0
#
return
```

8 Link Efficiency Mechanisms

About This Chapter

This chapter describes how to improve link efficiency through link fragmentation and interleaving and IP header compression.

 **NOTE**

Link Efficiency Mechanisms cannot be configured on the X1 and X2 models of the NE80E/40E.

[8.1 Introduction to Link Efficiency Mechanisms](#)

This section describes the basic concepts and applications of IP header compression and link fragmentation and interleaving.

[8.2 Configuring IP Header Compression](#)

IP header compression improves the link efficiency by reducing the length of packets to be transmitted over the link.

[8.3 Configuring Enhanced IP Header Compression](#)

By shortening the length of packets, EC RTP improves the efficiency of transmitting user data over the link. Therefore, EC RTP is applicable to the low-speed link over which long delay, frequent packet loss, and packet reordering occur.

[8.4 Maintaining Packet Header Compression](#)

This section describes the maintenance commands of the link efficiency mechanism, including commands for clearing statistics on header compression and commands for debugging IP header compression.

[8.5 Configuration Examples](#)

This section provides examples for configuring the link efficiency mechanism, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

8.1 Introduction to Link Efficiency Mechanisms

This section describes the basic concepts and applications of IP header compression and link fragmentation and interleaving.

8.1.1 Link Efficiency Mechanism Overview

The link efficiency mechanism is used to improve link performance and accordingly upgrade QoS on a network by shortening the delay in packet transmission and adjusting available bandwidth.

IP header compression improves the link efficiency by compressing IP headers before packets are sent. This mechanism effectively reduces the network load, speeds up the transmission of Real-Time Transport Protocol (RTP) packets, and UDP packets and saves the bandwidth resources.

The NE80E/40E supports two types of basic IPHC: RTP header compression and UDP header compression. This chapter describes the RTP header compression.

In the Next Generation Network (NGN) carrier network, many operators have to face the shortage of transmission resources. In IP NGN services, an IP/UDP/RTP header is about 40 bytes. The voice data in an actual packet (if an effective voice compression algorithm is used), however, is usually smaller than 30 bytes. In such a case, the overhead is too large and the link efficiency is low.

To solve this problem, the IETF proposes a series of RFCs. RFC 2508 proposes the compressed real-time protocol (CRTP), which can compress an RTP/UDP/IP header of 40 bytes to 2 to 4 bytes. This effectively addresses the problem of transmission resources shortage.

NOTE

CRTP specifies how multi-media data is transmitted over unicast or multicast networks in real time. It is a technology that can cut the overall length of an RTP packet by compressing the IP/UDP/RTP header of the RTP packet.

At present, the NE80E/40E supports the compression of the RTP/UDP/IP header.

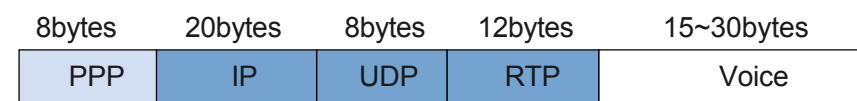
- Two compression methods are available: Compressed Real-Time Protocol (CRTP) and Enhanced Compressed Real-Time Protocol (ECRTP).
- Header compression of Point-to-Point Protocol (PPP) packets is also supported.
- Interfaces that support header compression include the Serial interface and MP-Group interface channelized from the CE1, CPOS, CT1, and CT3 interfaces.

8.1.2 RTP Header Compression(CRTP)

This section describes the principle of RTP header compression, format of a CRTP packet, and process of compressing an RTP packet.

In traditional networks, the IP protocol carries voice through RTP. Assume that RTP data is transmitted over a PPP link. [Figure 8-1](#) shows the frame format.

Figure 8-1 Format of an encapsulated RTP packet



During a call, the headers of a frame change as follows:

- Certain fields in the IP, UDP, and RTP packet headers, such as the source IP address, destination IP address, source port ID, destination port ID, and RTP load type, remain the same.
- Certain fields are redundant. Although these fields change during the call, their original values can be calculated after the decapsulation of other information. For example, the value of the length field in a UDP header can be calculated based on the length information contained in an IP header. The value of the length field of the IP header can be calculated based on the length information contained in a link-layer header. In addition, the link layer can detect errors, such as through the Cyclic Redundancy Check (CRC) in PPP. The IP head checksum can also be ignored.
- Although certain fields change during the transmission, the differences between packets are invariable. Therefore, the quadratic differential is 0.

The CRTP compression algorithm compresses packet headers based on the rules of the changes in the headers of the packets that carry voice services.

Figure 8-2 shows the format of a compressed and encapsulated CRTP packet.

Figure 8-2 Format of an encapsulated CRTP packet



CRTP defines four new packet formats, not IPv4 or IPv6, at the link layer.

- FULL_HEADER: transmits the uncompressed headers and data. The difference between a FULL_HEADER packet and an IPv4 or IPv6 packet is that a FULL_HEADER packet must carry a Context Identifier (CID) and a 4-bit sequence number to synchronize the compressor router and decompressor router. To avoid the lengthening of the head, the CID and sequence number are inserted into the length fields of the IP and UDP headers.

 **NOTE**

Each packet, compressed or uncompressed, must carry the CID and sequence number. Thus, packets lost during the transmission can be detected.

- COMPRESSED_UDP: carries the compressed IP and UDP headers. These headers are followed by uncompressed RTP header and data. This format is adopted when changes occur on the fields, of which the values should be constants, in the RTP header.
- COMPRESSED_RTP: carries compressed RTP, UDP, and IP headers. If the quadratic differential of a changing field in the RTP header is 0, this packet type is adopted. The decompressor router can restore the original header by adding the simple differential result to the uncompressed header of the previous packet.
- CONTEXT_STATE: It is a special packet sent from the decompressor router to the compressor router. A CONTEXT_STATE packet is used to transmit the CID that may lose or has already lost synchronization and request the update of context. This packet is transmitted only on point-to-point (P2P) links without carrying the IP header.

Figure 8-3 shows how an RTP header is compressed.

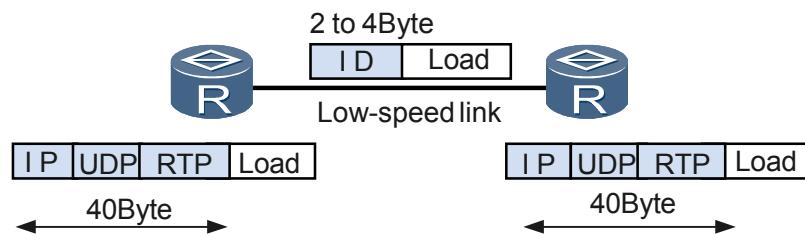
1. The compressor router sends a FULL_HEADER packet to the decompressor router. Then the compressor router removes the fields that remain the same and redundant fields in the packet header when compressing a packet and performs differential coding on changed fields. The compressed packet contains a CID to indicate the context to which it belongs.

 **NOTE**

CRTP uses a CID to indicate the combination of the source IP address, destination IP address, source UDP port, destination UDP port, and synchronous source (SSRC) field. This combination of fields is called context.

2. When the decompressor router receives the compressed packet, it searches the context list based on the CID and obtains the context information of the compressed packet. Assume that no information is lost, the decompressor router adds the differential result to the header of the previous uncompressed packet header and the packet header of the compressed packet can be obtained.
3. If the compressed packet is lost or damaged during the transmission on the link, the decompressor router drops the damaged packet and sends a CONTEXT_STATE packet to request the compressor router to resend the packet in the FULL_HEADER format.

Figure 8-3 Process of RTP header compression



8.1.3 Enhanced Compression RTP(ECRTP)

CRTP has to send synchronization packets frequently over the links. ECRTP resolves this problem, and thus reduces the impact of link quality on the compression efficiency.

CRTP has to send synchronization packets frequently on the links with the following problems: great jitter, high packet loss ratio, and disorder in packets. This affects the efficiency of compression to a great extent. RFC 3545 proposes ECRTP to strengthen the CRTP functions. ECRTP can reduce the impacts of link quality on the efficiency of compression.

ECRTP changes the fashion in which the compressor router requests the decompressor router to update the context. In this manner, CRTP becomes more adaptable to the changes in link quality in the following aspects:

- The compressor router regularly sends extended COMPRESSED_UDP packets to update the context of the decompressor router. Thus, the context of the two routers can be synchronized. The format of the packet is extended to carry more information about the changes in the header.
- If no UDP checksum is carried, the CRTP head checksum field is added. The decompressor router can determine whether errors occur during decompression according to the CRTP head checksum and make a second try. This can reduce the packets lost owing to the asynchronous state between the two routers.

- The compressor router sends N+1 synchronization packets continuously. As a result, if a synchronization packet is lost, the contexts of two routers still keep synchronous. The value of N can be configured depending on the quality of the link.

CRTTP applies to reliable P2P links with a short delay. ECRTTP applies to low-rate links of poor quality with the following problems: the rather long delay, high packet loss ratio, and disorder in packets.

8.2 Configuring IP Header Compression

IP header compression improves the link efficiency by reducing the length of packets to be transmitted over the link.

Context



NOTE

Currently, only the serial and MP-group interfaces support IPHC at the PPP link layer.

After IPHC is configured, the IP Compression Protocol (IPCP) needs to re-negotiate compression parameters and the link becomes Down and then Up. Therefore, be cautious before you use the following commands:

- **ppp compression iphc**
- **ppp compression iphc rtp-connections**

MP fragmentation must be configured first if you intend to configure packet header compression on the MP-group interface enabled with IS-IS; otherwise, packets are disordered or discarded.

The maximum link bandwidth cannot exceed the bandwidth of 51 E1 interfaces when CRTTP is configured on the MP-group interface.

8.2.1 Establishing the Configuration Task

Before configuring IP header compression, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To reduce the consumption of bandwidth during the real-time transmission on the network, you can configure the IPHC function on the low-speed link to reduce the total length of the packet and improve the packets transmission efficiency.

Pre-configuration Tasks

Before configuring the IPHC, complete the following tasks:

- Configuring the physical parameters for the interface
- Configuring the link layer attributes for the interface
- Configuring the IP address for the interface

Data Preparations

To configure IPHC, you need the following data.

No.	Data
1	Type and number of an interface where packet header compression is enabled
2	(Optional) Maximum number of RTP connections for packet header compression
3	(Optional) Update time for sessions of packet header compression
4	(Optional) Aging time of a session environment

8.2.2 Enabling IP Header Compression

Before configuring IP header compression, you need to enable IP header compression.

Context

Do as follows on the routers of the compressor and the decompressor:



CAUTION

You must configure commands containing the same parameters for RTP header compression at both ends of a link.

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface interface-type interface-number`

The interface view is displayed.

Step 3 Run:

`link-protocol ppp`

The link layer protocol is set to be PPP.

Step 4 Run:

`ppp compression iphc [nonstandard | udp-only | udpandrtp | static]`

IP header compression is enabled.

 NOTE

nonstandard: indicates the non-standard compatible encapsulation format.

udp-only: indicates that only UDP header compression is implemented. This means that the UDP header compression is implemented for even RTP packets.

udpandrtp: indicates that RTP header compression is implemented on the packets that meet the specified conditions for RTP header compression; otherwise, UDP header compression is implemented.

static: indicates that IP/UDP/RTP compression is statically specified without the PPP negotiation. If the parameter **static** is configured, errors may occur on the compression connections at both ends of the link during the compression due to the difference in parameters.

Step 5 (Option) Run:

```
priority { high | normal }
```

The forwarding priority of the packets received on the MP-Group interface is configured.

The command can only be configured on the MP-Group interface view.

When compressed RTP (CRTP) is configured on an MP-group interface consisting of 126 E1 interfaces and excessive packets are to be transmitted through the MP-group interface, you can configure the forwarding priority for the packets received on the MP-group interface. In this manner, packets on the MP-group interface can be normally transmitted.

Step 6 (Option) Run:

```
packet-reassembly queue depth depth-value
```

The depth of the packet reassembly queue on an MP-group interface is configured.

When data packets of different sizes (such as IS-IS packets and voice data) are transmitted through the same MP-group interface, you can configure the depth of the packet reassembly queue on the MP-group interface according to the actual interface bandwidth and the difference between the largest-size packet and the smallest-size packet. This can avoid the disorder and loss of data packets caused by insufficient depth of the packet reassembly queue on the MP-group interface.

---End

8.2.3 Configuring the Maximum Number of Connections for RTP Header Compression

To implement IP header compression over a PPP link, you must set the maximum number of RTP header compression connections on both ends of the PPP link.

Context

Do as follows on the routers of the compressor and the decompressor:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp compression iphc rtp-connections number [ static ]
```

The maximum RTP connections for header compression are configured.



static: indicates that the maximum number of connections for RTP compression is statically specified without the PPP negotiation. If the parameter **static** is configured, errors may occur at both ends of the link during the compression due to the difference in parameters. The maximum number of connections for RTP compression can be statically specified only when the header compression mode is set to **Static**.

If the compressor and the decompressor are configured with different maximum numbers of connections for RTP header compression, the smaller value is chosen as the valid one after IPCP negotiation.

By default, the maximum number of connections for RTP header compression is 16. This means that if the **ppp compression iphc rtp-connections** command is not configured, when the number of connections over the line exceeds 16, the exceeding number of connections are not compressed. The recommended number of connections for CRTP header compression is more than or equal to the number of connections over the line.

----End

8.2.4 Configuring the Update Time for Sessions of Packet Header Compression

You can set the update time for sessions of packet header compression to synchronize the compressing end with the decompressing end regularly. In this manner, the compressing end is prevented from frequently sending decompressed IP packets, which saves bandwidth.

Context

Do as follows on the compressor router and the decompressor router.

Procedure

Step 1 Run:

```
system-view
```

The system view is entered.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is entered.

Step 3 Run:

```
ppp compression iphc max-time number
```

The update time of sessions for packet header compression is configured.

By default, the period of time between two automatic session update events is 5 seconds. If the value is set to 0 second, it indicates that no update is performed.

----End

8.2.5 Configuring the Aging Time for a Session Environment

When the aging time of a compression session expires on the compressing end, the session is updated.

Context

Do as follows on the compressor router.

Procedure

Step 1 Run:

`system-view`

The system view is entered.

Step 2 Run:

`slot slot-id`

The slot view is displayed.

Step 3 Run:

`iphc aging-time time`

The aging time for a session environment is configured at the compressor router.



The aging time only takes effect at the compressor router. By default, the aging time on the compressor router is set to 10s. The value 0 indicates that the session context is not aged.

----End

8.2.6 Checking the Configuration

After IP header compression is configured, you can view the statistics on TCP header compression and RTP header compression.

Procedure

Step 1 Using the `display ppp compression iphc rtp [interface interface-type interface-number]` command to check the statistics of IPHC.

----End

Example

Using the `display ppp compression iphc rtp [interface interface-type interface-number]` command, you can view the statistics about RTP header compression. The statistics include

- The number of received packets and the decompressed packets on the router when acting as the decompressor.
- The number of compressed packets and the compression ratio on the router when acting as the compressor.

For example:

```
<HUAWEI> display ppp compression iphc rtp interface serial 13/0/0/1:0
```

```
IPHC: RTP/UDP/IP header compression
Interface: Serial13/0/0/1:0
Received:
  Receive/Decompress/Fail/Discard: 28926/28900/1/25 (Packets)
Sent:
  Compress/Send: 28796/28914 (Packets)
  Send/Save/Total: 1709112/777492/2486604 (Bytes)
  Compression Success Ratio(Compress/Send) : 99%
Connect:
  Rx/Tx: 100/100
```

8.3 Configuring Enhanced IP Header Compression

By shortening the length of packets, ECRTT improves the efficiency of transmitting user data over the link. Therefore, ECRTT is applicable to the low-speed link over which long delay, frequent packet loss, and packet reordering occur.

Context



NOTE

Currently, only the serial and MP-group interfaces support IPHC at the PPP link layer.

After IPHC is configured, the IP Compression Protocol (IPCP) needs to re-negotiate compression parameters and the link becomes Down and then Up. Therefore, be cautious before you use the following commands:

- [ppp compression iphc](#)
- [ppp compression iphc rtp-connections](#)

8.3.1 Establishing the Configuration Task

Before configuring ECRTT, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Enhanced Compressed Real-Time Transport Protocol (ECRTT) changes the way that the compressor updates the session context at the decompressor. With such an enhanced feature, Compressed Real-Time Transport Protocol (CRTP) performs well over links with frequent packet loss, packet reordering and long delay.

Pre-configuration Tasks

Before configuring the enhanced IPHC, complete the following tasks:

- Configuring the physical parameters for the interface
- Configuring the link layer attributes for the interface
- Configuring the IP address for the interface

Data Preparations

To configure enhanced IPHC, you need the following data.

No.	Data
1	Type and number of an interface where ECRTP is enabled
2	(Optional) Maximum number of RTP connections for packet header compression
3	(Optional) Update time for sessions of packet header compression
4	(Optional) Maximum number of packet drops tolerable over the link
5	(Optional) Aging time of a session context

8.3.2 Configuring ECRTP

Before configuring IP header compression, you need to enable IP header compression.

Context

Do as follows on the compressor router and the decompressor router.

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface interface-type interface-number`

The interface view is displayed.

Step 3 Run:

`link-protocol ppp`

The link layer protocol is set to be PPP.

Step 4 Run:

`ppp compression iphc enhanced`

ECRTP is enabled.

You must configure commands containing the same parameters for ECRTP at both ends of a link.

----End

8.3.3 Configuring the Maximum Number of Connections for RTP Header Compression

To implement IP header compression over a PPP link, you must set the maximum number of RTP header compression connections on both ends of the PPP link.

Context

Do as follows on the routers of the compressor and the decompressor:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp compression iphc rtp-connections number [ static ]
```

The maximum RTP connections for header compression are configured.



static: indicates that the maximum number of connections for RTP compression is statically specified without the PPP negotiation. If the parameter **static** is configured, errors may occur at both ends of the link during the compression due to the difference in parameters. The maximum number of connections for RTP compression can be statically specified only when the header compression mode is set to **Static**.

If the compressor and the decompressor are configured with different maximum numbers of connections for RTP header compression, the smaller value is chosen as the valid one after IPCP negotiation.

By default, the maximum number of connections for RTP header compression is 16. This means that if the **ppp compression iphc rtp-connections** command is not configured, when the number of connections over the line exceeds 16, the exceeding number of connections are not compressed. The recommended number of connections for CRTP header compression is more than or equal to the number of connections over the line.

----End

8.3.4 Configuring the Update Time for Sessions of Packet Header Compression

You can set the update time for sessions of packet header compression to synchronize the compressing end with the decompressing end regularly. In this manner, the compressing end is prevented from frequently sending decompressed IP packets, which saves bandwidth.

Context

Do as follows on the compressor router and the decompressor router.

Procedure

Step 1 Run:

```
system-view
```

The system view is entered.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is entered.

Step 3 Run:

```
ppp compression iphc max-time number
```

The update time of sessions for packet header compression is configured.

By default, the period of time between two automatic session update events is 5 seconds. If the value is set to 0 second, it indicates that no update is performed.

----End

8.3.5 (Optional) Configuring the Maximum Number of Consecutive Packet Drops Tolerable over the Link

You can configure the allowed maximum number of consecutive packet drops for a link on an EC RTP-capable interface.

Context

Do as follows on the compressor router and the decompressor router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp compression iphc enhanced n-value n-value
```

The maximum number of consecutive packet drops tolerable over the link is set.

By default, the maximum number of consecutive packet drops tolerable over the link is 1.

----End

8.3.6 (Optional) Configuring the No-Delta Compression Mode

By default, the system adopts the delta compression mode. If the no-delta compression mode is configured, IPv4 ID, RTP Time Stamp, and RTP Sequence Number in packet headers are not compressed when the packets are sent.

Context

Do as follows on the compressor router and the decompressor router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp compression iphc enhanced no-delta
```

The no-delta compression mode is configured.

By default, the system adopts the delta compression mode. If the no-delta compression mode is configured, IPv4 ID, RTP Time Stamp, and RTP Sequence number in packet headers are always sent without being compressed.

----End

8.3.7 Configuring the Aging Time for a Session Environment

When the aging time of a compression session expires on the compressing end, the session is updated.

Context

Do as follows on the compressor router.

Procedure

Step 1 Run:

```
system-view
```

The system view is entered.

Step 2 Run:

```
slot slot-id
```

The slot view is displayed.

Step 3 Run:

```
iphc aging-time time
```

The aging time for a session environment is configured at the compressor router.



The aging time only takes effect at the compressor router. By default, the aging time on the compressor router is set to 10s. The value 0 indicates that the session context is not aged.

----End

8.3.8 Checking the Configuration

After IP header compression is configured, you can view the statistics on TCP header compression and RTP header compression.

Procedure

Step 1 Using the **display ppp compression iphc rtp [interface interface-type interface-number]** command to check statistics about the RTP header compression.

----End

Example

```
<RouterA> display ppp compression iphc rtp interface serial13/0/0/1:0
IPHC: RTP/UDP/IP header compression
Interface: Serial13/0/0/1:0
Received:
    Recieve/Decompress/Fail/Discard: 28926/28900/1/25 (Packets)
Sent:
    Compress/Send: 28796/28914 (Packets)
    Send/Save/Total: 1709112/777492/2486604 (Bytes)
    Compression Success Ratio(Compress/Send) : 99%
Connect:
    Rx/Tx: 100/100
```

8.4 Maintaining Packet Header Compression

This section describes the maintenance commands of the link efficiency mechanism, including commands for clearing statistics on header compression and commands for debugging IP header compression.

8.4.1 Clearing IP Header Compression

You can delete the tables storing the invalid context of IP header compression or decompression and clear the statistics about IP header compression.

Context



CAUTION

Running the **reset ppp compression iphc** command to clear the cached entries of IPHC may make some node unreachable.

Procedure

Step 1 To clear the running information of IPHC, run the **reset ppp compression iphc interface interface-type interface-number** command in the user view.

This command is used to clear the ineffective IPHC, decapsulate the storage lists or clear the related statistic.

----End

8.5 Configuration Examples

This section provides examples for configuring the link efficiency mechanism, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

 **NOTE**

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

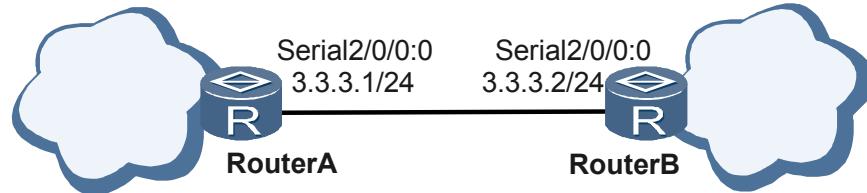
8.5.1 Example for Configuring IP Header Compression

This section provides an example for IP header compression. You can learn how to compress an RTP packet to improve the bandwidth usage.

Networking Requirements

As shown in **Figure 8-4**, Router A and Router B are devices on two networks. The two routers are connected through a low-speed link and the bandwidth resources are less. To improve the bandwidth utilization, you can enable the IPHC function on the low-speed link that connects Router A and Router B so that data packets that travel between Router A and Router B are compressed.

Figure 8-4 Networking diagram for configuring RTP header compression



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the link between Router A and Router B to be in PPP encapsulation.
2. Configure the IP addresses of the interfaces on Router A and Router B.
3. Enable IPHC on Router A and Router B.
4. Configure the maximum number of connections for RTP header compression on Router A and Router B.
5. Configure the update time for sessions of IPHC on Router A and Router B.
6. Configure the aging time for the session environment on Router A.

 **NOTE**

The aging time only takes effect at the compressor router.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the interfaces
- Maximum number of connections for the RTP header compression, the update time for the compressing sessions, and the aging time for the session environment.

Procedure

Step 1 Create the serial interfaces on Router A and Router B.

To be omitted. For details of the configuration, refer to the HUAWEI NetEngine80E/40E Router Configuration Guide *WAN Access*.

Step 2 Configure the link encapsulation protocol on Router A and Router B to PPP.

```
<RouterA> system view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] undo shutdown
[RouterA-serial2/0/0:0] link-protocol ppp
[RouterA-serial2/0/0:0] return
<RouterB> system view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] undo shutdown
[RouterB-serial2/0/0:0] link-protocol ppp
[RouterB-serial2/0/0:0] return
```

Step 3 Configure the IP addresses of the interfaces on Router A and Router B to ensure normal communications of the network.

To be omitted. For details of the configuration, refer to the HUAWEI NetEngine80E/40E Router Configuration Guide *IP Routing*.

Step 4 Enable the IPHC function on Serial 2/0/0:0 of Router A and Serial 2/0/0:0 of Router B.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc
[RouterB-serial2/0/0:0] return
```

Step 5 Configure the maximum number of connections for RTP header compression to 100 on Router A and Router B.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc rtp-connections 100
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc rtp-connections 100
[RouterB-serial2/0/0:0] return
```

Step 6 Configure the update time for the sessions to 8 seconds on Router A and Router B.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc max-time 8
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc max-time 8
[RouterB-serial2/0/0:0] return
```

Step 7 Configure the aging time for the RTP session environment to 20 seconds on Router A.

```
<RouterA> system-view
[RouterA] slot 2
[RouterA-slot-2] iphc aging-time 20
[RouterA-slot-2] return
```

Step 8 Verify the configuration.

```
<RouterA> display ppp compression iphc rtp interface serial 2/0/0:0
IPHC: RTP/UDP/IP header compression
  Interface: Serial2/0/0:0
    Received:
      Recieve/Decompress/Fail/Discard: 28926/28900/1/25 (Packets)
    Sent:
      Compress/Send: 28796/28914 (Packets)
      Send/Save/Total: 1709112/777492/2486604 (Bytes)
      Compression Success Ratio(Compress/Send) : 99%
    Connect:
      Rx/Tx: 100/100
<RouterB> display ppp compression iphc rtp interface serial 2/0/0:0
IPHC: RTP/UDP/IP header compression
  Interface: Serial2/0/0:0
    Received:
      Recieve/Decompress/Fail/Discard: 28940/28912/1/27 (Packets)
    Sent:
      Compress/Send: 28784/28900 (Packets)
      Send/Save/Total: 1691900/793500/2485400 (Bytes)
      Compression Success Ratio(Compress/Send) : 99%
    Connect:
      Rx/Tx: 100/100
```

After the configuration, RTP packets sent from Router A are compressed; these packets are decompressed by Router B, which receives the packets.

----End

Configuration Files

● Configuration file of Router A

```
# 
  sysname RouterA
#
  controller e1 2/0/0
    channel-set 0 timeslot-list 1-31
    undo shutdown
#
  interface Serial2/0/0:0
    undo shutdown
    link-protocol ppp
    ip address 3.3.3.1 255.255.255.0
    ppp compression iphc
    ppp compression iphc rtp-connections 100
    ppp compression iphc max-time 8
#
  slot 2
    iphc aging-time 20
#
  return
```

● Configuration file of Router B

```
# 
  sysname RouterB
#
  controller e1 2/0/0
    channel-set 0 timeslot-list 1-31
    undo shutdown
#
  interface Serial2/0/0:0
```

```
undo shutdown
link-protocol ppp
ip address 3.3.3.2 255.255.255.0
ppp compression iphc
ppp compression iphc rtp-connections 100
ppp compression iphc max-time 8
#
return
```

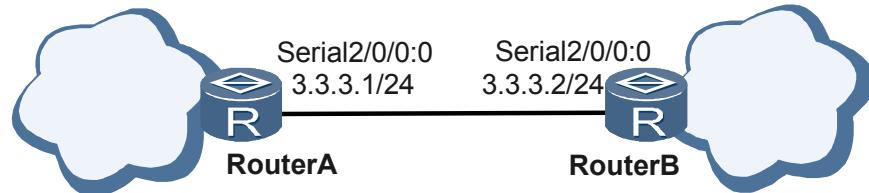
8.5.2 Example for Configuring EC RTP

This section provides an example for enhanced IP header compression. You can learn how to compress an RTP packet to improve the usage of bandwidth.

Networking Requirements

As shown in **Figure 8-5**, Router A and Router B are located in the same network and are joined through the low-speed link with long delay, high packet loss ratio, and frequent reordering. This requires that enhanced header compression be configured over the link. This requires that data packets over the link between Router A and Router B be compressed.

Figure 8-5 Networking diagram of configuring IP header compression



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure PPP encapsulation for the link between Router A and Router B.
2. Configure IP addresses for interfaces on Router A and Router B.
3. Enable EC RTP on Router A and Router B.
4. Configure the maximum number connections for the RTP header compression on Router A and Router B.
5. Configure the update interval for the compression session on Router A and Router B.
6. Configure the maximum number of consecutive packet drops tolerable on the link between Router A and Router B.
7. Configure the no-delta compression mode on Router A and Router B.
8. Configure the aging time of the session context on Router A.



You can configure aging time only on the compressor. The decompressor adopts the default aging time of the system, which cannot be configured.

Data Preparation

To complete the configuration, you need the following data.

- IP addresses of interfaces
- Maximum number of connections for the RTP header compression, update interval for the compression session, maximum number of consecutive packet drops tolerable over the link, and the aging time for the session context

Procedure

Step 1 Create the serial interfaces on Router A and Router B.

To be omitted. For details of the configuration, refer to the HUAWEI NetEngine80E/40E Router Configuration Guide *WAN Access*.

Step 2 Configure PPP encapsulation for the link between Router A and Router B.

```
<RouterA> system view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] undo shutdown
[RouterA-serial2/0/0:0] link-protocol ppp
[RouterA-serial2/0/0:0] return
<RouterB> system view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] undo shutdown
[RouterB-serial2/0/0:0] link-protocol ppp
[RouterB-serial2/0/0:0] return
```

Step 3 Configure IP addresses for interfaces on Router A and Router B to ensure network connectivity.

The configuration is omitted here. For detailed configuration, refer to the *HUAWEI NetEngine80E/40E Router Configuration Guide - IP Routing*.

Step 4 Enable ECRTP on Serial 2/0/0:0 on Router A and on Serial 2/0/0:0 on Router B.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc enhanced
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc enhanced
[RouterB-serial2/0/0:0] return
```

Step 5 Set the maximum number of connections for the RTP header compression on Router A and Router B to 100.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc rtp-connections 100
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc rtp-connections 100
[RouterB-serial2/0/0:0] return
```

Step 6 Set the update interval for session compressions on Router A and Router B to 8s.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc max-time 8
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc max-time 8
[RouterB-serial2/0/0:0] return
```

Step 7 Set the maximum number of consecutive packet drops tolerable on Router A and Router B to 2.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc enhanced n-value 2
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc enhanced n-value 2
[RouterB-serial2/0/0:0] return
```

Step 8 Set the compression mode on Router A and Router B to be no-delta.

```
<RouterA> system-view
[RouterA] interface serial 2/0/0:0
[RouterA-serial2/0/0:0] ppp compression iphc enhanced no-delta
[RouterA-serial2/0/0:0] return
<RouterB> system-view
[RouterB] interface serial 2/0/0:0
[RouterB-serial2/0/0:0] ppp compression iphc enhanced no-delta
[RouterB-serial2/0/0:0] return
```

Step 9 Set the aging time for the RTP session context on Router A to 20s.

```
<RouterA> system-view
[RouterA] slot 2
[RouterA-slot-2] iphc aging-time 20
```

Step 10 Verify the configuration.

```
<RouterA> display ppp compression iphc rtp interface serial 2/0/0:0
IPHC: RTP/UDP/IP header compression
  Interface: Serial2/0/0:0
    Received:
      Recieve/Decompress/Fail/Discard: 28926/28900/1/25 (Packets)
    Sent:
      Compress/Send: 28796/28914 (Packets)
      Send/Save/Total: 1709112/777492/2486604 (Bytes)
      Compression Success Ratio(Compress/Send) : 99%
    Connect:
      Rx/Tx: 100/100
<RouterB> display ppp compression iphc rtp interface serial 2/0/0:0
IPHC: RTP/UDP/IP header compression
  Interface: Serial2/0/0:0
    Received:
      Recieve/Decompress/Fail/Discard: 28940/28912/1/27 (Packets)
    Sent:
      Compress/Send: 28784/28900 (Packets)
      Send/Save/Total: 1691900/793500/2485400 (Bytes)
      Compression Success Ratio(Compress/Send) : 99%
    Connect:
      Rx/Tx: 100/100
```

After the preceding configurations, compressed RTP packets are sent from Router A, and Router B decompresses these RTP packets.

----End

Configuration Files

- Configuration file of Router A

```
#          sysname RouterA
#
#          controller e1 2/0/0
#          channel-set 0 timeslot-list 1-31
#          undo shutdown
#
#          interface Serial2/0/0:0
```

```
undo shutdown
link-protocol ppp
ip address 3.3.3.1 255.255.255.0
ppp compression iphc
ppp compression iphc rtp-connections 100
ppp compression iphc max-time 8
ppp compression iphc enhanced
ppp compression iphc enhanced n-value 2
ppp compression iphc enhanced no-delta
#
slot 2
    iphc aging-time 20
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
controller e1 2/0/0
    channel-set 0 timeslot-list 1-31
    undo shutdown
#
interface Serial2/0/0:0
    undo shutdown
    link-protocol ppp
    ip address 3.3.3.2 255.255.255.0
    ppp compression iphc
    ppp compression iphc rtp-connections 100
    ppp compression iphc max-time 8
    ppp compression iphc enhanced
    ppp compression iphc enhanced n-value 2
    ppp compression iphc enhanced no-delta
#
return
```

9 ATM QoS Configuration

About This Chapter

End-to-end QoS policies, including congestion management and traffic policing, must be applied to ATM PVCs on the ATM bearer network.

 **NOTE**

ATM QoS cannot be configured on the X1 and X2 models of the NE80E/40E.

[**9.1 ATM QoS Overview**](#)

This section describes the ATM QoS configuration. To ensure the quality of the data transmission service on an ATM network, every VC must be configured with ATM QoS parameters. You can ensure service quality by applying ATM QoS policies to the VCs and ATM interfaces.

[**9.2 Configuring ATM Simple Traffic Classification**](#)

This section describes how to apply simple traffic classification to an ATM network.

[**9.3 Configuring Forced ATM Traffic Classification**](#)

ATM forced traffic classification can be configured on an upstream sub-interface, a PVP, or a PVC to classify traffic, mark the traffic with specific color, and perform queue scheduling based on the classification and color.

[**9.4 Configuring ATM Complex Traffic Classification**](#)

ATM complex traffic classification can be configured to classify and manage traffic that enters an ATM network or that is transmitted over an ATM network, and then provide differentiated services.

[**9.5 Configuring the ATM Traffic Shaping**](#)

Configuring ATM traffic shaping limits the volume of outgoing traffic on an ATM network within a reasonable range, preventing a large number of burst data that from affecting normal operation of the network.

[**9.6 Configuring the Priority of an ATM PVC**](#)

You can set priorities for ATM PVC traffic to define the priorities of ATM users. In this manner, traffic can be scheduled and guaranteed based on the priorities.

[**9.7 Configuring Congestion Management of the ATM PVC**](#)

By configuring queues on ATM PVCs, you can schedule packets into different queues based on a certain algorithm and discard excess packets to implement congestion management.

9.8 Configuration Examples

This section provides examples for configuring ATM QoS, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

9.1 ATM QoS Overview

This section describes the ATM QoS configuration. To ensure the quality of the data transmission service on an ATM network, every VC must be configured with ATM QoS parameters. You can ensure service quality by applying ATM QoS policies to the VCs and ATM interfaces.

9.1.1 Introduction to ATM QoS

To ensure the quality of the data transmission service on an ATM network, every PVC must be configured with ATM QoS parameters. You can ensure service quality by applying ATM QoS policies to PVCs and ATM interfaces.

The Asynchronous Transfer Mode (ATM) is a conventional multi-service bearing technology that is used on the backbone network. It is used to bear IP, FR, voice, conference call, and ISDN/DSL with powerful QoS capability. The existing ATM networks are used to bear crucial services.

Limited by the transfer mode and class of services, however, the ATM nowadays is inferior to the IP network in terms of scalability, upgradeability, and compatibility. In the process of network upgrade, the ATM faces the problem of how to use existing resources to combine the ATM network with the Packet Switched Network (PSN).

The ATM network has powerful QoS capability. In combination with the PSN network, the QoS capability of the ATM network must be remained and the mapping between the IP precedence, MPLS precedence, VLAN precedence and the ATM priority must be set so that packets are transmitted with the same priority in the two networks.

Combination of the ATM network and the PSN network applies to the following two situations:

- Transparent transmission of ATM cells: In the transition from the ATM network to the PSN network, the MPLS tunnel is used as the PW to join the ATM networks at both ends. Over the PW, AAL5 data frames or ATM cells are encapsulated and transparently transmitted through MPLS encapsulation.
- IPoEoA encapsulated through 1483B and IPoA encapsulated through 1483R: The router is located at the edge of the ATM network to provide access to the IP network. When data packets are transmitted over the ATM network, they are encapsulated in AAL5 frames. The router performs ATM termination to forward IP packets to other types of interfaces or forward Layer 2 Ethernet frames to the Ethernet interface.



To configure the data described in this chapter, you need to be familiar with the ATM and QoS knowledge. For information about the ATM concept and the ATM configuration, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - WAN Access*. This chapter describes the ATM QoS configuration only.

9.1.2 ATM QoS Features Supported by the NE80E/40E

IP QoS and ATM QoS can be combined to support individual PVCs or PVC groups.

When the ATM network is being transformed to the PSN network or serves as the bearer plane of the IP network, QoS of the ATM network and QoS of the IP network should be integrated to provide end to end QoS.

ATM Simple Traffic Classification

ATM QoS supports simple traffic classification in three modes, that is, ATM transparent transmission, 1483R, and 1483B. The product supports the configuration and mapping of the ATM simple traffic classification on the ATM sub-interface, VE interface or PVC, and PVP.

ATM transparent transmission consists of transparent transmission of ATM cells and ATM frames.

- VCC and VPC transparent transmission modes are for ATM cells. In these two modes, the basic transmission unit is ATM cell with a fixed size, 53 bytes. This corresponds with the transmission unit over standard ATM links.
- SDU transparent transmission is for ATM frames. The basic transmission unit is frame and the size depends on the user-defined MTU and the packet received by the upstream PE.

The 1483R protocol is used to encapsulate IP packets to carry out IPoA service. The 1483B protocol is used to encapsulate Ethernet packets to carry out IPoEoA service.

- Principle of ATM simple traffic classification for transparent transmission

On the AC side of the ingress PE in the MPLS network, the CoS and CLP values of the ATM network are mapped to the internal priority of the router. On the PW side of the ingress PE in the MPLS network, the internal priority is mapped back to the EXP value. Thus, QoS parameters of the ATM network can be transmitted in the MPLS network. (For SDU transparent transmission, the CLP in the SDU is 1 only if any one of the CLP value is 1 on the AC side of the ingress PE on the MPLS network. Otherwise, the CLP in the SDU is 0. The CLP value, in combination with the CoS of PVC, is mapped to the internal priority of the router. On the PW side of the ingress PE, the CLP value is the same as that in transparent transmission of other modes.)

On the PW side of the egress PE in the MPLS network, the router forwards packets according to the MPLS EXP field. On the AC side of the egress PE in the MPLS network, the router forwards packets according to the priority of the ATM cells. (On the PW side of the egress PE, the transparent transmission of SDU is the same as that of other modes. On the AC side of the egress PE in the MPLS network, if the CLP is 1, the CLP values of all ATM cells are set to 1. Otherwise, the CLP values of all ATM cells are set to 0.)

Based on the simple traffic classification described here, the QoS parameters of the ATM network are transparently transmitted from one ATM network to another through the PSN network.

- Principle of 1483R and 1483B simple traffic classification

At the edge of the ATM network, simple traffic classification is enabled to set the mapping from the DSCP field to the ATM priority on the router that provides access to the IP network.

On the upstream PVC of the access router, the precedence of the 1483R and 1483B packets depends on the encapsulated DSCP value.

On the downstream PVC of the access router, the internal priority inside the router is mapped to the ATM CLP to map the DSCP values to ATM priority.

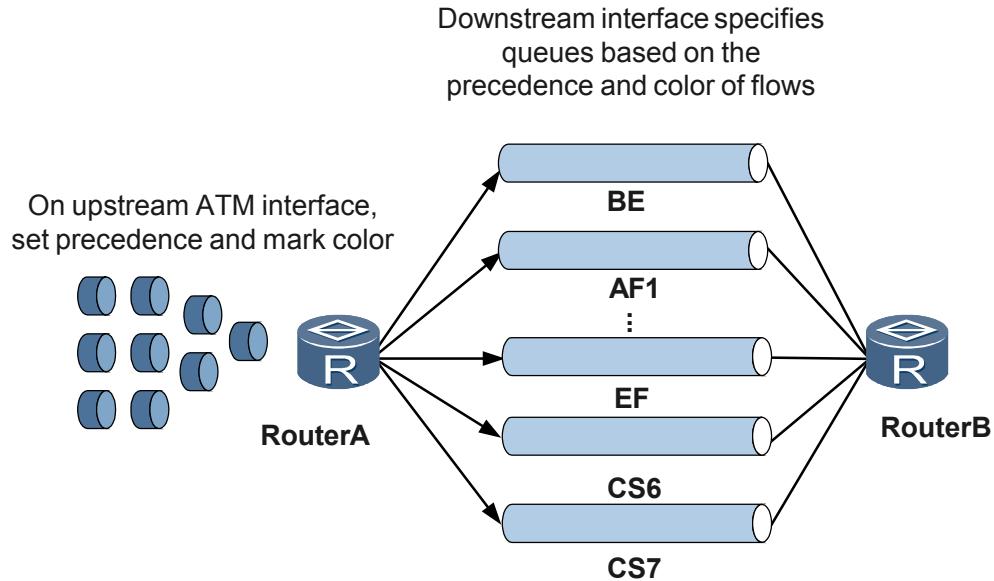
Forced ATM Traffic Classification

Although ATM cells in the ATM network hold the precedence information, it is very difficult to carry out IPoA, transparent transmission of cells and IWF simple traffic classification based on the precedence information. Forced ATM traffic classification does not involve the service type and precedence. On the upstream interface on the router at the ATM network edge, you can

configure forcible traffic classification to set the precedence and color for IP packets of a PVC, an interface (either a main interface or a sub-interface), or a PVP. You can also apply QoS policies to the downstream interface of the router at the ATM network edge.

As shown in **Figure 9-1**, you can set the precedence and color for a specific flow on the upstream ATM interface of Router A. Then, the downstream interface can specify the queue and scheduling mode for the flow according to the precedence and the color. In this way, ATM QoS is implemented.

Figure 9-1 Forced ATM traffic classification



ATM physical interface, ATM sub-interface, ATM PVC, ATM PVP and Virtual Ethernet (VE) interface all support forced traffic classification.

ATM Complex Traffic Classification

In the deployment of IP over ATM (IPoA) or IP over Ethernet over AAL5 (IPoEoA) services, sometimes you need to classify and limit the traffic that enters an ATM network or that flows in an ATM network, for example:

- To differentiate packet types, such as voice packets, video packets, and data packets and to provide different bandwidths and latencies for those types of packet
- To handle traffic coming from different users and provide different bandwidths and priorities for those types of packet

To do so, you need to classify packets according to parameters such as the DSCP value, the protocol type, the IP address, or the port number, provide differentiated services, and configure QoS traffic policies based on the ATM complex traffic classification.

The ATM complex traffic classification is implemented through the application of QoS traffic policies. To provide QoS assurance on an ATM interface, you can define a QoS policy that contains traffic classifiers associated with traffic behaviors and then apply the QoS policy to the ATM interface.

To do so, perform the following steps:

1. Define traffic classifiers.
2. Define traffic behaviors.
3. Define traffic policies and associate the traffic classifiers with the traffic behaviors.
4. Apply the traffic policies to the ATM interfaces (or sub-interfaces) or VE interfaces.



The NE80E/40E does not support the ATM complex traffic classification of IPv6 packets or IPv4 multicast packets because ATM does not support the IPv6 protocol or the IPv4 multicast protocol.

ATM Traffic Shaping

When an ATM network is congested so that the traffic rate exceeds the threshold, the subsequent excessive packets are discarded. To prevent a downstream network from being congested or from directly dropping a large number of packets due to too heavy traffic on an upstream network, you can configure ATM traffic shaping (TS) on the outbound interface of the upstream router. TS limits the traffic rate and burst size of traffic that goes out of a network so that this type of packets are sent out at a uniform rate. This benefits the bandwidth conformity between an upstream network and a downstream network.

To configure ATM TS, perform the following steps:

- Configure the ATM service type and shaping parameters in the system view. You can configure the service types of the Constant Bit Rate (CBR), Non Real Time-Variable Bit Rate (NRT-VBR), or Real Time-Variable Bit Rate (RT-VBR).
- Specify a ATM service type on a PVC or a PVP and apply the TS parameters.

Congestion Management of ATM PVC

On an ATM network, when the traffic rate exceeds the threshold, the excessive packets are buffered rather than discarded. When the network is not busy, the buffered packets are then forwarded. With the congestion management of ATM PVC, the packets are organized into eight PVC queues according to a specified algorithm. The packets then are forwarded according to the queue scheduling mechanism. The configuration of ATM PVC queues involves the PQ configuration and the WFQ configuration.

9.2 Configuring ATM Simple Traffic Classification

This section describes how to apply simple traffic classification to an ATM network.

9.2.1 Establishing the Configuration Task

Before configuring ATM simple traffic classification, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

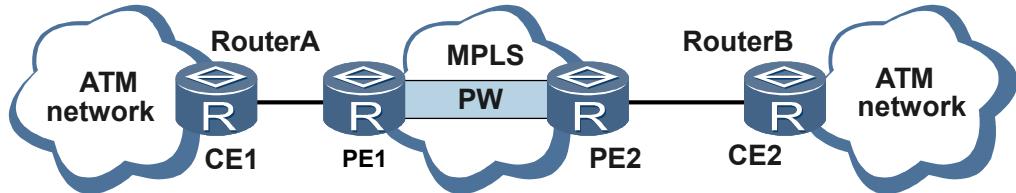
Applicable Environments

ATM simple traffic classification is mainly applied to the following two situations:

- Two ATM networks are connected through the PSN network (ATM transparent transmission)

As shown in **Figure 9-2**, Router A and Router B are the edge routers of two ATM networks. The existing ATM networks are used to bear crucial services. The two ATM networks are connected through the PSN backbone network. An MPLS tunnel serves as the PW to connect the two ATM networks. Over the PW, MPLS packets are used to encapsulate AAL5 data frames or ATM cells.

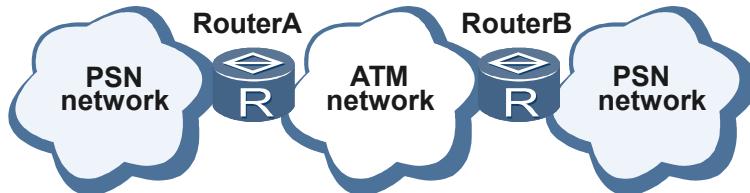
Figure 9-2 Networking diagram for connecting two ATM networks with the PSN network



- Ethernet or IP packets are carried over the existing ATM network (1483R or 1483B transparent transmission)

As shown in **Figure 9-3**, Router A and Router B are edge routers of two ATM networks to provide access to the IP network. On the ATM network, IP packets are transmitted in AAL5 frames. When IP packets are sent out of the ATM network, the router performs ATM termination and forwards IP packets to other types of interfaces or forwards Layer 2 Ethernet frames to the Ethernet interface.

Figure 9-3 Networking diagram for transmitting Ethernet or IP packets over the ATM network



You can configure ATM simple traffic classification on an interface, or on a PVC or PVP. Note that:

- If ATM simple traffic classification is configured on an interface, it takes effect on all the PVCs or PVPs under the interface.
- If ATM simple traffic classification is configured not on the interface but only on a specific PVC or PVP, it takes effect only on the PVC or PVP.
- If a PVC is bound to a VE interface, ATM simple traffic classification takes effect only when it is configured on both the PVC and the VE interface.
- If ATM simple traffic classification is configured on both ATM interface (or VE interface) and PVC or PVP, the configuration on PVC or PVP preferentially takes effect.

Pre-configuration Tasks

Before configuring ATM simple traffic classification, complete the following tasks:

- Configuring link attributes of the interface
- Allocating IP addresses for the interface
- Configuring PVC or PVP and the related parameters
- Configuring ATM services (ATM transparent transmission, IPoA, or IPoEoA)

Data Preparation

To configure ATM simple traffic classification, you need the following data.

No.	Data
1	Number of the interface, PVC, or PVP that is enabled with the ATM simple traffic classification
2	Mapping rules for ATM simple traffic classification

9.2.2 Enabling ATM Simple Traffic Classification

ATM simple traffic classification can be enabled only on ATM sub-interfaces, PVCs/PVPs, or VE interfaces.

Context

Do as follows on the router on which ATM simple traffic classification is required:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Do as follows on the router as required:

- To create an ATM sub-interface and enter the view of the ATM sub-interface, run:

```
interface atm atm-number.sub-interface
```

- To create a PVC or PVP and enter the PVC or PVP view, on the sub-interface view, run:

```
pvc [ pvc-name ] vpi/vci
```

or

```
pvp vpi
```

- To create a VE interface and enter the view of the VE interface, run:

```
interface virtual-ethernet ve-name
```

Step 3 Run:

```
trust upstream { ds-domain-name | default }
```

The specified DS domain is bound to the interface and the simple traffic classification is enabled.

----End

9.2.3 Configuring Mapping Rules for ATM QoS

The system maps the CoS and CLP values of incoming ATM cells to the internal priorities of the device and colors the ATM cells.

Context

Do as follows on the router that is enabled with the ATM simple traffic classification:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
diffserv domain { ds-domain-name | default }
```

A DS domain is defined and the DS domain view is displayed.

Step 3 Do as follows on the router as required:

- To set ATM simple traffic classification for upstream ATM cells, run:

```
atm-inbound service-type clp-value phb service-class [ color ]
```

- To set ATM simple traffic classification for downstream ATM cells, run:

```
atm-outbound service-class [ color ] map clp-value
```

- To define mapping rules for simple traffic classification of ATM control cells, run:

```
atm-inbound cam-cell phb service-class [ color ]
```

CLP is a bit indicating the cell priority in an ATM cell header. A cell with CLP being 0 is of normal priority. A cell with CLP being 1 is of low priority which is given the first opportunity to be discarded in the case of congestion. ATM defines five services types, namely, CBR, rt-VBR, nrt-VBR, ABR, and UBR. The ATM simple traffic classification supports traffic classification on the basis of ATM service types and CLP.

----End

9.2.4 Checking the Configuration

After ATM simple traffic classification is configured, you can view configurations of priority mapping in the DS domain.

Procedure

Step 1 Use the **display diffserv domain** [*ds-domain-name*] command to check the configuration of the DS domain.

If the preceding configuration succeeds, you can run this command to check the configuration of the precedence mapping for simple traffic classification in the DS domain.

----End

9.3 Configuring Forced ATM Traffic Classification

ATM forced traffic classification can be configured on an upstream sub-interface, a PVP, or a PVC to classify traffic, mark the traffic with specific color, and perform queue scheduling based on the classification and color.

9.3.1 Establishing the Configuration Task

Before configuring ATM forced traffic classification, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environments

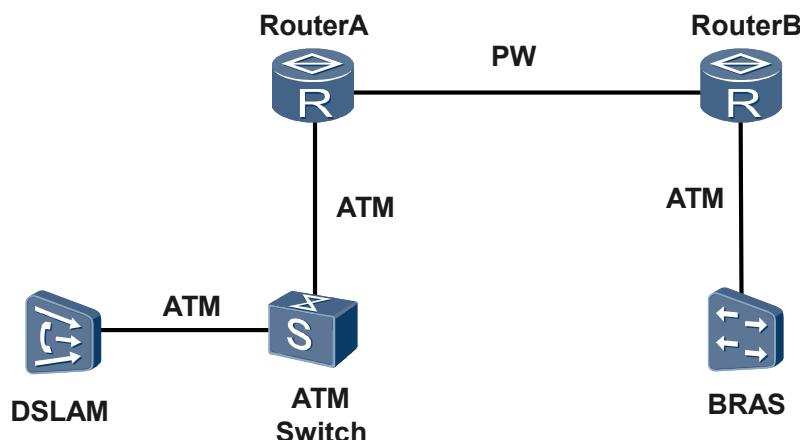
Forced ATM traffic classification can be applied to the following situations:

- Transparent transmission of ATM cells

As shown in [Figure 9-4](#), transparent transmission of ATM cells needs to be set on Router A and Router B for ATM traffic accessed through DSLAM. Router A transmits the received ATM cells to Router B over a PW. Router B continues to forward the ATM cells over its ATM links.

On the upstream sub-interface, PVP or PVC of Router A, forced traffic classification can be set to classify traffic and mark the traffic with specific color. Then the downstream interface, PVP or PVC of Router A can schedule queues on the basis of the forced classification and coloring.

Figure 9-4 Forced traffic classification for transparent transmission of ATM cells

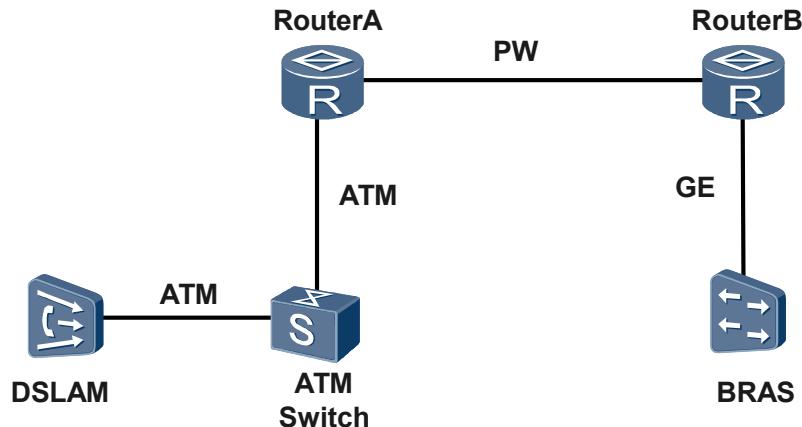


- 1483B traffic access

As shown in [Figure 9-5](#), the DSLAM provides access for the 1483B traffic. The outbound interface of Router B is an Ethernet port. According to the design of ATM-Ethernet IWF, configure IWF function on Router A and Router B. This allows you to map VPN to the outer VLAN ID and map VCI to inner VLAN ID. The 1483B-based ATM cells are transparently transmitted to the BRAS over the Ethernet link through the PW between Router A and Router B.

In the upstream sub-interface view of Router A, set forced traffic classification and color marking. Then the downstream interface of Router A can perform queue scheduling based on the forced traffic classification and coloring.

Figure 9-5 Forced traffic classification of 1483B traffic



NOTE

- Forced traffic classification based on PVC supports such services as transparent transmission of ATM cells, IPoA and IPoEoA.
- Forced traffic classification based on PVP supports such services as transparent transmission of ATM cells.
- Forced traffic classification based on sub-interface supports such services as transparent transmission of ATM cells, IPoA, and ATM IWF.
- Forced traffic classification based on the main interface is valid to only PVC or PVP of the interface and supports transparent transmission of ATM cells and IPoA.

Pre-configuration Tasks

Before configuring forced ATM traffic classification, complete the following tasks:

- Configuring an L2VPN between PEs at both ends and binding the L2VPN to the two PEs' interfaces that connect to CEs
- Configuring PVCs on CEs and configuring transparent cell transmission or IWF at the ATM side on PEs

Data Preparation

To configure forced ATM traffic classification, you need the following data.

No.	Data
1	Priorities and colors for PVCs

9.3.2 Configuring ATM Services

The ATM service can be transmitted through ATM cell relay, IWF, or IPoA.

Context

ATM services may be cell transmission, IWF or IPoA.

Procedure

- Step 1** To configure ATM cell transmission, see the chapter "PWE3 Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - VPN*.
- Step 2** To configure ATM IWF, see the chapter "ATM IWF Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - VPN*.
- Step 3** To configure IPoA, see the chapter "ATM Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - WAN Access*.

---End

9.3.3 Configuring Forced ATM Traffic Classification

ATM forced traffic classification can be configured on ATM interfaces, ATM sub-interfaces, or PVCs/PVPs.

Context

Do as follows on the upstream interface of the router on which forced ATM traffic classification is required:

Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

- Step 2** Do as follows as required:

- To enter the ATM interface, view, run:

```
interface atm interface-number
```

- To create an ATM sub-interface and enter the sub-interface view, run:

```
interface atm interface-number.sub-interface
```

- To create a PVC or PVP and enter the PVC or PVP view, run the following command in the sub-interface view:

```
pvc [ pvc-name ] vpi/vci
```

or

```
pvp vpi
```

- Step 3** Run

```
traffic queue service-class { green | red | yellow }
```

or

Forced traffic classification is set on the upstream ATM interface of the PE.

 **NOTE**

- If the service class is AF1, AF2, AF3 or AF4, you must specify the color of the packets.
- If the service class is CS7, CS6, EF or BE, you cannot specify the color of the packets.
- **green**: indicates the actions to the data packet when the packet traffic complies with the committed information rate (CIR). The default value is **pass**.
- **yellow**: indicates the actions to the data packet when the packet traffic complies with the peak information rate (PIR). The default value is **pass**.
- **red**: indicates the actions to the data packet when the packet traffic exceeds the PIR. The default value is **discard**.

----End

9.3.4 Checking the Configuration

After ATM forced traffic classification is configured, you can view that traffic is classified as defined.

Procedure

Step 1 Use the **ping ip-address** command to check the intercommunication between CEs.

If the preceding configuration is successful, the following results are obtained when you run the preceding command:

- CEs at both the ends can ping through each other.
- Traffic is classified according to the specified service class.

----End

9.4 Configuring ATM Complex Traffic Classification

ATM complex traffic classification can be configured to classify and manage traffic that enters an ATM network or that is transmitted over an ATM network, and then provide differentiated services.

9.4.1 Establishing the Configuration Task

Before configuring ATM complex traffic classification, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

You are required to classify and limit the traffic that enters an ATM network or that flows in an ATM network, for example:

- To differentiate packet types such as voice packets, video packets, and data packets, and provide different bandwidths and latencies for those types of packets
- To handle traffic coming from different users and provide different bandwidths and priorities for those types of packets

You can classify packets according to parameters such as the DSCP value, the protocol type, the IP address, or the port number, and then provide differentiated services and configure QoS traffic policies based on the ATM complex traffic classification.

Pre-configuration Tasks

Before configuring the ATM complex traffic classification, complete the following tasks:

- Configuring the link attributes of ATM interfaces
- Configuring IP addresses for ATM interfaces or VE interfaces
- Configuring PVC or PVP parameters
- Configuring IPoA or IPoEoA services

 **NOTE**

An ATM interface configured with IPoA or IPoEoA services supports the ATM complex traffic classification whereas an ATM interface configured with ATM transparent cell transmission services or IWF does not support the ATM complex traffic classification.

Data Preparation

To configure the ATM complex traffic classification, you need the following data.

No.	Data
1	Names of traffic classifiers
2	Data for matching rules
3	Names of traffic behaviors
4	Data for traffic behaviors
5	Names of traffic policies
6	Types and numbers of the interfaces to which traffic policies are applied

9.4.2 Defining Traffic Classifiers

Before configuring complex traffic classification, you need to define a traffic classifier.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic classifier classifier-name [ operator { and | or } ]
```

A traffic classifier is defined and the traffic classifier view is displayed.

Step 3 Run the following command as required to define a traffic classifier.

- To define an ACL matching rule, run:

```
if-match acl acl-number
```

 **NOTE**

Only ACLs that match packets based on the Layer 3 or Layer 4 information are supported.

- To define a DSCP matching rule, run:

```
if-match dscp dscp-value
```

- To define a TCP flag matching rule, run:

```
if-match tcp syn-flag tcpflag-value
```

- To define a matching rule based on IP precedence, run:

```
if-match ip-precedence ip-precedence
```

- To define a rule for matching all packets, run:

```
if-match any
```

- To define a rule for matching packets based on the MPLS EXP value, run:

```
if-match mpls-exp exp-value
```

---End

9.4.3 Defining Traffic Behaviors

This section describes traffic behaviors and how to configure them.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic behavior behavior-name
```

A traffic behavior is defined and the traffic behavior view is displayed.

Step 3 Run one of the following commands as required.

- To allow packets to pass the device, run:

```
permit
```

- To discard matched packets, run:

```
deny
```

- To re-configure traffic shaping, run:

```
car { cir cir-value [ pir pir-value] } [ cbs cbs-value pbs pbs-value ] [ green
{ discard | pass [ service-class class color color ] } | yellow { discard |
pass [ service-class class color color ] } | red { discard | pass [ service-
class class color color ] } ]*
```

- To re-configure the IP precedence of an IP packet, run:

- To re-configure the DSCP value of an IP packet, run:
`remark ip-precedence ip-precedence`
 - To re-configure the priority of an MPLS packet, run:
`remark mpls-exp exp`
-  **NOTE**
The `remark mpls-exp` command can be applied to only upstream traffic on a router.
- To configure the Class of Service (CoS) of packets, run:
`service-class service-class color color`
 - To configure a load-balancing mode (per flow or per packet) of packets, run:
`load-balance { flow | packet }`
 - To configure redirecting of packets to a single next hop device, run:
`redirect ip-nexthop ip-address [interface interface-type interface-number]`
 - To redirect IP packets to a target LSP on the public network, run:
`redirect lsp public dest-ipv4-address [nexthop-address | interface interface-type interface-number | secondary]`

----End

9.4.4 Defining Traffic Policies

After defining traffic classifiers and traffic behaviors, you need to configure traffic policies by associating traffic classifiers with traffic behaviors.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`traffic policy policy-name`

A traffic policy is defined and the policy view is displayed.

Step 3 Run:

`classifier classifier-name behavior behavior-name`

A traffic behavior is associated with a specified traffic classifier in the traffic policy.

----End

9.4.5 Applying Traffic Policies

Class-based traffic policies take effect only after they are applied to interfaces.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run one of the following commands as required.

- To enter the ATM interface (or sub-interface) view, run:

```
interface atm interface-number [.sub-interface ]
```

- To enter the VE interface view, run:

```
interface virtual-ethernet interface-number
```

Step 3 Run:

```
traffic-policy policy-name { inbound | outbound }
```

A traffic policy is applied to the interface.



NOTE

- After a traffic policy is applied to an interface, you cannot modify the **shared** or **unshared** mode of the traffic policy. Before modifying the **shared** or **unshared** mode of a traffic policy, you must cancel the application of the traffic policy from the interface.
- A traffic policy with the **shared** attribute: For a traffic policy that is applied to different interfaces, the statistics displayed for an individual interface is the sum of the statistics of all interfaces to which the traffic policy is applied. Therefore, the original data for each individual interface is not identifiable.
- A traffic policy with the **unshared** attribute: You can identify the statistics of a traffic policy according to the interface where the traffic policy is applied.
- Whether a traffic policy is **shared** or **unshared** depends on the PAF file. The inbound and outbound attributes can be identified in traffic statistics, no matter a policy is of the **shared** attribute or the **unshared** attribute.
- An ATM interface configured with ATM transparent cell transport services or IWF does not support the ATM complex traffic classification or this command.

----End

9.4.6 Checking the Configuration

After class-based QoS is configured, you can view information about the configured traffic classifiers, traffic behaviors, traffic policies formed by the specified classifiers and behaviors, and traffic statistics on interfaces.

Context

Run the following commands to check the previous configurations.

Procedure

- Use the **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] command to check the configuration of a traffic behavior.
- Use the **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*] command to check the configuration of a traffic classifier.
- Use the **display traffic policy** { **system-defined** | **user-defined** } [*policy-name* [*classifier classifier-name*]] command to check information about the associations of all

traffic classifiers with traffic behaviors, or information about the association of a particular traffic classifier with a traffic behavior.

- Use the **display traffic policy statistics interface interface-type interface-number [.sub-interface] { inbound | outbound } [verbose { classifier-based | rule-based } [class class-name]]** command to check information about the traffic policy statistics on an interface.

----End

Example

- Run the **display traffic behavior** command. If correct traffic behaviors are displayed, it means that the configuration succeeds.
- Run the **display traffic classifier** command. If correct rules for traffic classifier are displayed, it means that the configuration succeeds.
- Run the **display traffic policy** command. If correct traffic policy names and the binding relations between traffic classifiers and traffic behaviors are displayed, it means that the configuration succeeds.
- Run the **display traffic policy statistics** command. If correct statistics about the specified interface defined in a traffic policy are displayed, it means that the configuration succeeds.

For example:

```
<HUAWEI> display traffic policy statistics interface atm 1/0/0 inbound
Interface: Atm1/0/0
Traffic policy inbound: test
Traffic policy applied at 2007-08-30 18:30:20
Statistics enabled at 2007-08-30 18:30:20
Statistics last cleared: Never
Rule number: 7 IPv4, 0 IPv6
Current status: OK!
      Item          Packets          Bytes
-----+
Matched           1,000       100,000
    +-Passed        500        50,000
    +-Dropped        500        50,000
    +-Filter         100       10,000
    +-CAR            300       30,000
Missed            500        50,000
Last 30 seconds rate
      Item          pps          bps
-----+
Matched           1,000       100,000
    +-Passed        500        50,000
    +-Dropped        500        50,000
    +-Filter         100       10,000
    +-CAR            300       30,000
Missed            500        50,000
```

9.5 Configuring the ATM Traffic Shaping

Configuring ATM traffic shaping limits the volume of outgoing traffic on an ATM network within a reasonable range, preventing a large number of burst data that from affecting normal operation of the network.

9.5.1 Establishing the Configuration Task

Before configuring ATM traffic shaping, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To keep the traffic over an ATM network within a reasonable scope to avoid abnormal operation of the network in the case of heavy and bursting traffic, you can configure ATM traffic shaping to limit the outgoing traffic rate. The configuration can better utilize the network resources.

Pre-configuration Tasks

Before configuring the ATM traffic shaping, complete the following tasks:

- Configuring the physical parameters of ATM interfaces to ensure normal operation of the interfaces
- Configuring IP addresses for the ATM interfaces

Data Preparation

To configure ATM traffic shaping, you need the following data:

No.	Data
1	Names of service types and service type on the PVC
2	Peak Cell Rate, Sustainable Cell Rate, Maximum Burst Size, and Cell Delay Variation Tolerance
3	VPI or VCI of PVC used for traffic shaping

9.5.2 Configuring ATM Traffic Shaping Parameters

You must specify the service type and parameters related to the service type for PVCs or PVPs to limit the volume of outgoing traffic on an ATM network.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
atm service service-name { cbr output-pcr cdvt-value | nrt-vbr output-pcr output-scr output-mbs cdvt-value | rt-vbr output-pcr output-scr output-mbs cdvt-value }
```

The PVC or PVP service types and related parameters are configured.

To configure PVC service types, you need to create service types in the system view; then, apply the service types to specific PVCs.

The default PVC service type is UBR and therefore, you do not need to create the service type of UBR.

----End

9.5.3 Applying ATM Traffic Shaping Parameters

ATM traffic shaping parameters are applied to ATM interfaces or ATM sub-interfaces.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface atm interface-number[.subinterface]`

The ATM interface view or sub-interface view is displayed.

Step 3 Run the following command as required:

- To create PVP and display the PVP view, run:

`pvp vpi`

- To create PVC and display the PVC view, run:

`pvc { pvc-name vpi/vci | vpi/vci }`



● PVP can be configured on ATM sub-interfaces only.

● PVP and PVC should not coexist on the same ATM sub-interface.

Step 4 Run:

`shutdown`

The PVC or PVP is shut down.

Step 5 Run:

`service output service-name`

The service type of PVC or PVP is specified and the traffic shaping parameters are applied to the PVC or PVP.



To specify a service type of PVC or PVP with the `service output` command, you need to run the `shutdown` command to shut down the PVC or PVP and then run the `undo shutdown` command to re-enable the PVC or PVP. In this manner, the configuration can be ensured to take effect.

Step 6 Run:

`undo shutdown`

Traffic shaping is enabled on the PVC or PVP.

----End

9.5.4 Checking the Configuration

After ATM traffic shaping is configured, you can view traffic shaping parameters.

Context

Run the following command to check the previous configuration.

Procedure

- Use the **display atm service [service-name]** command to check the configuration of traffic shaping parameters.

----End

Example

Run the **display atm service [service-name]** command. If correct configuration of the traffic shaping parameters is displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display atm service
Atm Service Config:
    Service Name: cbr
    State: VALID
    Index: 0
    ServiceType: CBR
    PCR: 111
    SCR: 0
    MBS: 0
    CDVT: 111
    Traffic Type: Shaper
```

9.6 Configuring the Priority of an ATM PVC

You can set priorities for ATM PVC traffic to define the priorities of ATM users. In this manner, traffic can be scheduled and guaranteed based on the priorities.

9.6.1 Establishing the Configuration Task

Before configuring priorities for ATM PVC traffic, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To ensure the bandwidth for user services with different priorities in an ATM network, you can configure the priorities of the traffic in ATM PVCs so that traffic scheduling is performed based on the priorities.

Pre-configuration Tasks

Before configuring the priority of an ATM PVC, complete the following task:

- Configuring the physical parameters of ATM interfaces to ensure normal operation of the interfaces

- Configuring IP addresses of the ATM interfaces

Data Preparation

To configure the priority of an ATM PVC, you need the following data.

No.	Data
1	The VPI and VCI of the PVC to be configured with a priority
2	Priority of the PVC

9.6.2 Configuring the Priority of an ATM PVC

By setting priorities for ATM PVC traffic, you can schedule traffic on the PVCs with different priorities.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface atm interface-number.sub-interface`

The ATM sub-interface view is displayed.



NOTE

To configure the priorities of all PVCs in the interface view, you can run the `service output priority` command on the interface.

Step 3 Run:

`pvc { pvc-name [vpi/vci] | vpi/vci }`

The PVC view is displayed.

Step 4 Run:

`service output priority priority`

The priority of the PVC or PVP is specified.



NOTE

You can use this command to configure priorities of only UBR-type PVCs. Thus, the system can schedule the traffic in the PVCs with different priorities.

----End

9.7 Configuring Congestion Management of the ATM PVC

By configuring queues on ATM PVCs, you can schedule packets into different queues based on a certain algorithm and discard excess packets to implement congestion management.

9.7.1 Establishing the Configuration Task

Before configuring congestion management for ATM PVCs, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

On an ATM network, when the traffic rate exceeds the threshold, the exceeding packets are buffered instead of being discarded. When the network is not busy, the buffered packets are forwarded. After the congestion management of ATM PVC is configured, the packets are organized into queues according to a specified algorithm. The packets then are forwarded according to the queue scheduling mechanism.

The configuration of ATM PVC queues involves the PQ configuration and the WFQ configuration.

Pre-configuration Tasks

Before configuring the traffic shaping of the ATM PVC, complete the following task:

- Configuring the physical parameters of ATM interfaces to ensure normal operation of the interfaces
- Configuring IP addresses for the ATM interfaces
- Configuring a PVC
- Configuring the traffic shaping of the ATM PVC

Data Preparation

To configure congestion management of the ATM PVC, you need the following data.

No.	Data
1	Interface type and ID, PVC name, and VPI or VCI number
2	Queue names for queue scheduling
3	(Optional) WFQ weights. (If the queue scheduling is configured to be PQ, this parameter is not required.)

9.7.2 Configuring the Queue Scheduling of an ATM PVC

When the network is congested, you can buffer the packets that exceed the PVC bandwidth and then send the packets out when the network becomes idle.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number [.sub-interface ]
```

The ATM interface view or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

The PVC view is displayed.

Step 4 Run:

```
shutdown
```

The PVC is shut down.

Step 5 Run:

```
pvc-queue cos-value { pq | wfq weight weight } outbound
```

The queue scheduling parameter of the ATM PVC is configured.



NOTE

- Of the eight queues for a PVC, only one queue can be configured with the PQ scheduling.
- If one PVC queue is configured with the PQ or WFQ scheduling, the rest queues are configured with the WFQ scheduling by default. The default scheduling parameter is 20.
- Queue scheduling of ATM PVCs can be configured only for downstream packets.

Step 6 Run:

```
undo shutdown
```

The queue scheduling parameter for the PVC is enabled.

By default, the ATM PVC is not configured with a queue scheduling algorithm. Before configuring the queue scheduling parameter of an ATM PVC, you must run the **shutdown** command to shut down the PVC.

----End

9.7.3 Checking the Configuration

After congestion management is configured for ATM PVCs, you can view information about queues and packet statistics on ATM interfaces.

Procedure

- Use the **display atm pvc-queue [interface interface-type interface-number [.sub-interface] [pvc vpi/vci]]** command to check queue scheduling information on all PVCs or one PVC on an ATM interface.

- Use the **display atm pvc-info [interface atm interface-number [pvc { pvc-name [vpi/vci] | vpi/vci }]]** command to check information of PVCs on an ATM interface.

----End

Example

Run the **display atm pvc-queue** command. If correct queue scheduling information on all PVCs or one PVC on an ATM interface is displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display atm pvc-queue interface atm 4/0/1
Show CBQ PVC configuration of interface Atm4/0/1 PVC 0/1:
  be distribute OutBound wfq Weight 20
  af1 distribute OutBound pq
  af2 distribute OutBound wfq Weight 50
  af3 distribute OutBound wfq Weight 20
  af4 distribute OutBound wfq Weight 20
  ef  distribute OutBound wfq Weight 20
  cs6 distribute OutBound wfq Weight 20
  cs7 distribute OutBound wfq Weight 20
Show CBQ PVC configuration of interface Atm4/0/1 PVC 0/2:
  be distribute OutBound wfq Weight 20
  af1 distribute OutBound pq
  af2 distribute OutBound wfq Weight 20
  af3 distribute OutBound wfq Weight 20
  af4 distribute OutBound wfq Weight 20
  ef  distribute OutBound wfq Weight 20
  cs6 distribute OutBound wfq Weight 20
```

Run the **display atm pvc-info** command after queue scheduling of PVCs is configured. The information about PVCs is displayed, including information about traffic queues. For example:

```
<HUAWEI> display atm pvc-info interface atm 7/1/3.24 pvc 24/24
Atm7/1/3.24, VPI: 24, VCI: 24, INDEX: 275
AAL5 Encaps: SNAP, Protocol: IP
OAM interval: 0 sec(disabled), OAM retry interval: 0 sec
OAM retry count (up/down): 0/0
  input pkts: 0, input bytes: 0, input pkt errors: 0
  output pkts: 0, output bytes: 0, output pkt errors: 0
  [be]    output pkts: 2222123, output bytes: 0
  [af1]   output pkts: 0, output bytes: 0
  [af2]   output pkts: 0, output bytes: 0
  [af3]   output pkts: 0, output bytes: 0
  [af4]   output pkts: 0, output bytes: 0
  [ef]    output pkts: 0, output bytes: 0
  [cf6]   output pkts: 0, output bytes: 0
  [cf7]   output pkts: 0, output bytes: 0
Interface State: DOWN, PVC State: DOWN
```

9.8 Configuration Examples

This section provides examples for configuring ATM QoS, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.



NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

9.8.1 Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission

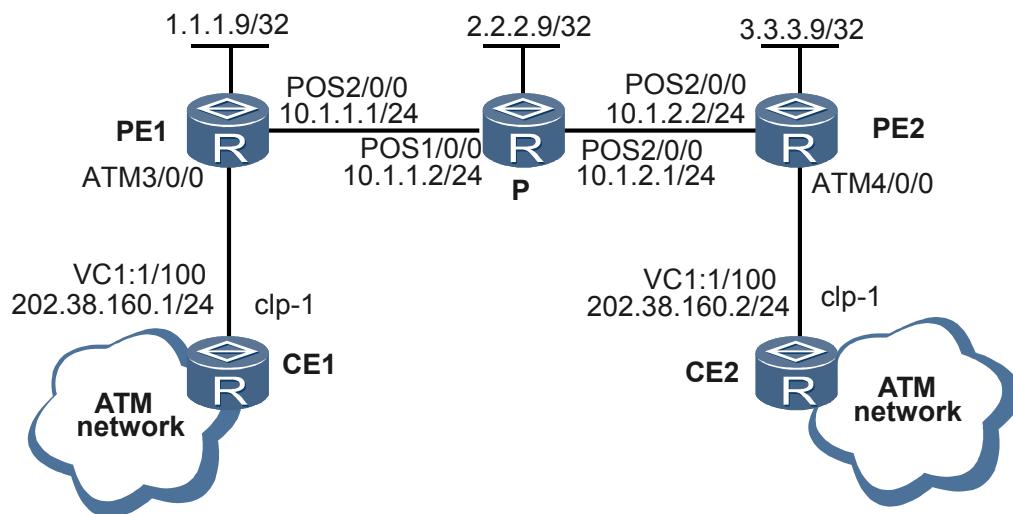
This section provides an example for configuring ATM simple traffic classification in 1-to-1 VCC ATM cell relay networking.

Networking Requirements

As shown in **Figure 9-6**, the ATM interface of CE1 connects to the MPLS network through PE1, and connects to CE2 through PE2. A VC is established between CE1 and CE2 over the MPLS network.

Simple traffic classification is required for the upstream traffic on PE1. PE1 maps the PVC service type and the CLP of upstream traffic to its internal precedence. For downstream traffic, PE1 maps the internal precedence to the MPLS EXP field. The precedence of ATM cells is transmitted transparently over the MPLS network.

Figure 9-6 Networking diagram for configuring ATM simple traffic classification for 1-to-1 VCC ATM transparent transmission



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and PVC parameters for the interfaces.
2. Configure IGP on the P and PE devices on the MPLS network to achieve IP connectivity.
3. Configure basic MPLS functions on the P and PE devices.
4. Configure MPLS LDP on the P and PE devices.
5. Establish remote LDP sessions between the two PEs.
6. Enable MPLS L2VPN on the PE devices.
7. Configure 1-to-1 VCC ATM transparent transmission.
8. Configure mapping rules for ATM simple traffic classification.

9. Enable simple traffic classification.

Data Preparation

To complete the configuration, you need the following data:

- Data for configuring OSPF
- Name of the remote PE peer
- VC ID
- VPI/VCI value on the CE
- Service type and CLP value

Procedure

Step 1 Configure ATM interfaces on the CEs.

Configure CE1.

```
<CE1> system-view
[CE1] interface atm 1/0/0
[CE1-Atm1/0/0] undo shutdown
[CE1-Atm1/0/0] quit
[CE1] interface atm 1/0/0.1
[CE1-Atm1/0/0.1] ip address 202.38.160.1 24
[CE1-Atm1/0/0.1] pvc 1/100
[CE1-atm-pvc-Atm1/0/0.1-1/100] map ip 202.38.160.2
[CE1-atm-pvc-Atm1/0/0.1-1/100] return
```

Configure CE2.

```
<CE2> system-view
[CE2] interface atm 2/0/0
[CE2-Atm2/0/0] undo shutdown
[CE2-Atm2/0/0] quit
[CE2] interface atm 2/0/0.1
[CE2-Atm2/0/0.1] ip address 202.38.160.2 24
[CE2-Atm2/0/0.1] pvc 1/100
[CE2-atm-pvc-Atm2/0/0.1-1/100] map ip 202.38.160.1
[CE2-atm-pvc-Atm2/0/0.1-1/100] return
```

Step 2 Configure IGP on the MPLS network (In this example, OSPF is used).

Assign IP addresses for the interfaces on the PE1, PE2, and P devices (Details omitted).

Configure PE1.

```
<PE1> system-view
[PE1] ospf 1 router-id 1.1.1.9
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure the P.

```
<P> system-view
[P] ospf 1 router-id 2.2.2.9
[P-ospf-1] area 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configure PE2.

```
<PE2> system-view
[PE2] ospf 1 router-id 3.3.3.9
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Step 3 Configure basic MPLS functions and LDP on the MPLS network.

Configure PE1.

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos 2/0/0
[PE1-Pos2/0/0] undo shutdown
[PE1-Pos2/0/0] mpls
[PE1-Pos2/0/0] mpls ldp
[PE1-Pos2/0/0] return
```

Configure the P.

```
<P> system-view
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] lsp-trigger all
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface pos 1/0/0
[P-Pos1/0/0] undo shutdown
[P-Pos1/0/0] mpls
[P-Pos1/0/0] mpls ldp
[P-Pos1/0/0] quit
[P] interface pos 2/0/0
[P-Pos2/0/0] undo shutdown
[P-Pos2/0/0] mpls
[P-Pos2/0/0] mpls ldp
[P-Pos2/0/0] quit
```

Configure PE2.

```
<PE2> system-view
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos 2/0/0
[PE2-Pos2/0/0] undo shutdown
[PE2-Pos2/0/0] mpls
[PE2-Pos2/0/0] mpls ldp
[PE2-Pos2/0/0] quit
```

Step 4 Establish remote LDP sessions between the two PEs.

Configure PE1.

```
<PE1> system-view
[RouterC] mpls ldp remote-peer 1
[PE1-mpls-ldp-remote-1] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-1] return
```

```
# Configure PE2.  
  
<PE2> system-view  
[PE2] mpls ldp remote-peer 1  
[PE2-mpls-ldp-remote-1] remote-ip 1.1.1.9  
[PE2-mpls-ldp-remote-1] return
```

Step 5 On PEs, enable MPLS L2VPN and configure 1-to-1 VCC ATM transmission.

```
# Configure PE1.  
  
<PE1> system-view
```

```
[PE1] mpls 12vpn  
[PE1-12vpn] quit  
[PE1] interface atm 3/0/0  
[PE1-Atm3/0/0] undo shutdown  
[PE1-Atm3/0/0] quit  
[PE1] interface atm 3/0/0.1 p2p  
[PE1-Atm3/0/0.1] atm cell transfer  
[PE1-Atm3/0/0.1] pvc 1/100  
[PE1-atm-pvc-Atm3/0/0.1-1/100] quit  
[PE1-Atm3/0/0.1] mpls 12vc 3.3.3.9 101  
[PE1-Atm3/0/0.1] return
```

```
# Configure PE2.  
  
<PE2> system-view
```

```
[PE2] mpls 12vpn  
[PE2-12vpn] quit  
[PE2] interface atm 4/0/0  
[PE2-Atm4/0/0] undo shutdown  
[PE2-Atm4/0/0] quit  
[PE2] interface atm 4/0/0.1 p2p  
[PE2-Atm4/0/0.1] atm cell transfer  
[PE2-Atm4/0/0.1] pvc 1/100  
[PE2-atm-pvc-Atm4/0/0.1-1/100] quit  
[PE2-Atm4/0/0.1] mpls 12vc 1.1.1.9 101  
[PE2-Atm4/0/0.1] return
```

Step 6 Set the service type for the ATM PVC on PE1.

```
<PE1> system-view  
[PE1] atm service cbr-name cbr 100 2000  
[PE1] interface atm 3/0/0.1  
[PE1-Atm3/0/0.1] pvc 1/100  
[PE1-atm-pvc-Atm3/0/0.1-1/100] shutdown  
[PE1-atm-pvc-Atm3/0/0.1-1/100] service output cbr-name  
[PE1-atm-pvc-Atm3/0/0.1-1/100] undo shutdown  
[PE1-atm-pvc-Atm3/0/0.1-1/100] return
```

 **NOTE**

Before configuring the **service output** command on a PVC or PVP, run the **shutdown** command to shut down it. Otherwise, the configuration does not take effect.

Step 7 On PE1, configure mapping rules for ATM simple traffic classification and enable simple traffic classification.

```
<PE1> system-view  
[PE1] diffserv domain default  
[PE1-dsdomain-default] atm-inbound cbr 0 phb af2 green  
[PE1-dsdomain-default] quit  
[PE1] interface atm 3/0/0.1  
[PE1-Atm3/0/0.1] pvc 1/100  
[PE1-atm-pvc-Atm3/0/0.1-1/100] trust upstream default  
[PE1-atm-pvc-Atm3/0/0.1-1/100] quit  
[PE1-Atm3/0/0.1] quit  
[PE1] interface pos 2/0/0  
[PE1-pos2/0/0] trust upstream default  
[PE1-pos2/0/0] return
```

 **NOTE**

Because network traffic is bi-directional, on PE2, you also need to configure ATM simple traffic classification for the reverse traffic. The configuration is similar to that on PE1 and is not mentioned in this example.

Step 8 Verify the configuration.

- On the PE devices, view the L2VPN connections. The output shows that an L2VC is set up and the status is Up.

Take PE1 for an example:

```
[PE1] display mpls l2vc
Total ldp vc : 1      1 up      0 down
*Client Interface      : Atm3/0/0.1
Session State        : up
AC Status            : up
VC State             : up
VC ID                : 101
VC Type              : atm 1to1 vcc
Destination          : 3. 3. 3.9
Local VC Label       : 138240
Remote VC Label      : 138240
Control Word         : Disable
Local VC MTU         : 1500
Remote VC MTU        : 0
Tunnel Policy Name   : --
Traffic Behavior Name: --
PW Template Name     : --
Create time          : 0 days, 0 hours, 5 minutes, 22 seconds
UP time              : 0 days, 0 hours, 5 minutes, 22 seconds
Last change time     : 0 days, 0 hours, 5 minutes, 22 seconds
VC last up time     : 2008/07/24 12:31:31
VC total up time    : 0 days, 2 hours, 12 minutes, 51 seconds
```

- CE1 and CE2 can ping through each other.
- Traffic mapping succeeds.

```
[PE1] display port-queue statistics interface pos 2/0/0 af2 outbound
[af2]
    Total pass:                      271004559 packets,           20596342912 bytes
    Total discard:                   0 packets,                  0 bytes
    Drop tail discard:              0 packets,                  0 bytes
    Wred discard:                   0 packets,                  0 bytes
    Last 30 seconds pass rate:     118647 pps,           9017172 bps
    Last 30 seconds discard rate:  0 pps,                     0 bps
    Drop tail discard rate:       0 pps,                     0 bps
    Wred discard rate:            0 pps,                     0 bps
    bps
```

----End

Configuration Files

- Configuration file of CE1

```
#          sysname CE1
#
#          interface Atm1/0/0
#          undo shutdown
```

```
#  
interface Atm1/0/0.1  
pvc 1/100  
    map ip 202.38.160.2  
    ip address 202.38.160.1 255.255.255.0  
#  
return
```

- Configuration file of CE2

```
#  
    sysname CE2  
#  
interface Atm2/0/0  
    undo shutdown  
#  
interface Atm2/0/0.1  
pvc 1/100  
    map ip 202.38.160.1  
    ip address 202.38.160.2 255.255.255.0  
#  
return
```

- Configuration file of PE1

```
#  
    sysname PE1  
#  
    atm service cbr-name cbr 100 2000  
#  
    mpls lsr-id 1.1.1.9  
    mpls  
        lsp-trigger all  
        mpls 12vpn  
#  
    mpls ldp  
#  
    mpls ldp remote-peer 1  
        remote-ip 3.3.3.9  
#  
    diffserv domain default  
        atm-inbound cbr 0 phb af2 green  
#  
    interface Atm3/0/0  
        undo shutdown  
#  
    interface Atm3/0/0.1 p2p  
        atm cell transfer  
        pvc 1/100  
            trust upstream default  
            service output cbr-name  
            mpls 12vc 3.3.3.9 101  
#  
    interface Pos2/0/0  
        undo shutdown  
        link-protocol ppp  
        ip address 10.1.1.1 255.255.255.0  
        mpls  
        mpls ldp  
            trust upstream default  
#  
    interface LoopBack1  
        ip address 1.1.1.9 255.255.255.255  
#  
    ospf 1  
        area 0.0.0.0  
        network 1.1.1.9 0.0.0.0  
        network 10.1.1.0 0.0.0.255  
#  
return
```

- Configuration file of P

```
#  
    sysname P  
#  
    mpls lsr-id 2.2.2.9  
    mpls  
        lsp-trigger all  
#  
    mpls ldp  
#  
    interface Pos1/0/0  
        undo shutdown  
        link-protocol ppp  
        ip address 10.1.1.2 255.255.255.0  
        mpls  
        mpls ldp  
#  
    interface Pos2/0/0  
        undo shutdown  
        link-protocol ppp  
        ip address 10.1.2.1 255.255.255.0  
        mpls  
        mpls ldp  
#  
    interface LoopBack1  
        ip address 2.2.2.9 255.255.255.255  
#  
ospf 1  
    area 0.0.0.0  
        network 2.2.2.9 0.0.0.0  
        network 10.1.1.0 0.0.0.255  
        network 10.1.2.0 0.0.0.255  
#  
return
```

- Configuration file of PE2

```
#  
    sysname PE2  
#  
    mpls lsr-id 3.3.3.9  
    mpls  
        lsp-trigger all  
        mpls 12vpn  
#  
    mpls ldp  
#  
    mpls ldp remote-peer 1  
        remote-ip 1.1.1.9  
#  
    interface Atm4/0/0  
        undo shutdown  
#  
    interface Atm4/0/0.1 p2p  
        atm cell transfer  
        pvc 1/100  
        mpls 12vc 1.1.1.9 101  
#  
    interface Pos2/0/0  
        undo shutdown  
        ip address 10.1.2.2 255.255.255.0  
        mpls  
        mpls ldp  
#  
    interface LoopBack1  
        ip address 3.3.3.9 255.255.255.255  
#  
ospf 1  
    area 0.0.0.0  
        network 3.3.3.9 0.0.0.0
```

```
network 10.1.2.0 0.0.0.255
#
return
```

9.8.2 Example for Configuring Simple Traffic Classification for 1-to-1 VPC ATM Transparent Transmission

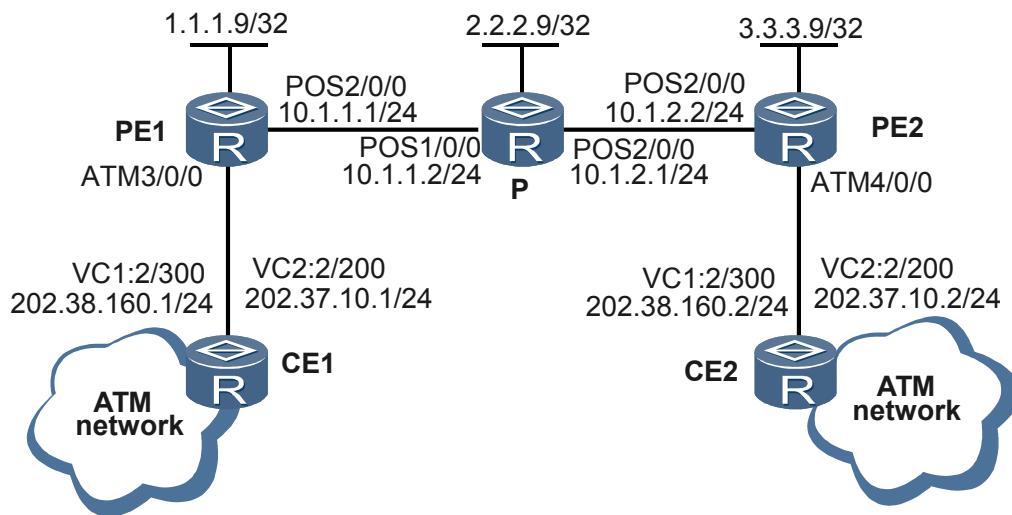
This section provides an example for configuring ATM simple traffic classification in 1-to-1 VPC ATM cell relay networking.

Networking Requirements

As shown in [Figure 9-7](#), the ATM interface of CE1 connects to the MPLS network through PE1, and connects to CE2 through PE2. A VP is established between CE1 and CE2 over the MPLS network. Two VCs are established in the VP.

Simple traffic classification is required for the upstream traffic on PE1. PE1 maps the PVC service type and the CLP of upstream traffic to its internal precedence. For downstream traffic, PE1 maps the internal precedence to the MPLS EXP field. The precedence of ATM cells is transmitted transparently over the MPLS network.

Figure 9-7 Networking diagram for configuring simple traffic classification for 1-to-1 VPC ATM transparent transmission



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and PVC parameters for the interfaces.
2. Configure IGP on the P and PE devices on the MPLS network to achieve IP connectivity.
3. Configure basic MPLS functions on the P and PE devices.
4. Configure MPLS LDP on the P and PE devices.
5. Establish remote LDP sessions between the two PEs.
6. Enable MPLS L2VPN on the PE devices.

7. Configure 1-to-1 VPC ATM transparent transmission.
8. Configure mapping rules for ATM simple traffic classification.
9. Enable simple traffic classification.

Data Preparation

To complete the configuration, you need the following data:

- Data for configuring OSPF
- Name of the remote PE peer
- VC ID
- VPI/VCI value on the CE
- Service type and CLP value

Procedure

Step 1 Configure the ATM interfaces on the CEs.

Configure CE1.

```
<CE1> system-view
[CE1] interface atm 1/0/0
[CE1-Atm1/0/0] undo shutdown
[CE1-Atm1/0/0] quit
[CE1] interface atm 1/0/0.1
[CE1-Atm1/0/0.1] ip address 202.38.160.1 24
[CE1-Atm1/0/0.1] pvc 2/300
[CE1-atm-pvc-Atm1/0/0.1-2/300] map ip 202.38.160.2
[CE1-atm-pvc-Atm1/0/0.1-2/300] quit
[CE1-Atm1/0/0.1] quit
[CE1] interface atm 1/0/0.2
[CE1-Atm1/0/0.2] ip address 202.37.10.1 24
[CE1-Atm1/0/0.2] pvc 2/200
[CE1-atm-pvc-Atm1/0/0.2-2/200] map ip 202.37.10.2
[CE1-atm-pvc-Atm1/0/0.2-2/200] return
```

Configure CE2.

```
<CE2> system-view
[CE2] interface atm 2/0/0
[CE2-Atm2/0/0] undo shutdown
[CE2-Atm2/0/0] quit
[CE2] interface atm 2/0/0.1
[CE2-Atm2/0/0.1] ip address 202.38.160.2 24
[CE2-Atm2/0/0.1] pvc 2/300
[CE2-Atm2/0/0.1-2/300] map ip 202.38.160.1
[CE2-Atm2/0/0.1-2/300] quit
[CE2-Atm2/0/0.1] interface atm 2/0/0.2
[CE2-Atm2/0/0.2] ip address 202.37.10.2 24
[CE2-Atm2/0/0.2] pvc 2/200
[CE2-Atm2/0/0.2-2/200] map ip 202.37.10.1
[CE2-Atm2/0/0.2-2/200] quit
```

Step 2 Configure IGP on the MPLS network (In this example, OSPF is used).

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 2](#).

Step 3 Configure basic MPLS functions and LDP on the MPLS network.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 3](#).

Step 4 Establish remote LDP sessions between the two PEs.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 4](#).

Step 5 On PEs, enable MPLS L2VPN and configure 1-to-1 VPC ATM transmission.

Configure PE1.

```
<PE1> system-view
[PE1] mpls l2vpn
[PE1-l2vpn] quit
[PE1] interface atm 3/0/0
[PE1-Atm3/0/0] undo shutdown
[PE1-Atm3/0/0] quit
[PE1] interface atm 3/0/0.1 p2p
[PE1-Atm3/0/0.1] atm cell transfer
[PE1-Atm3/0/0.1] pvp 2
[PE1-atm-pvp-Atm3/0/0.1-2] quit
[PE1-Atm3/0/0.1] mpls 12vc 3.3.3.9 101
[PE1-Atm3/0/0.1] return
```

Configure PE2.

```
<PE2> system-view
[PE2] mpls l2vpn
[PE2-l2vpn] quit
[PE2] interface atm 4/0/0
[PE2-Atm4/0/0] undo shutdown
[PE2-Atm4/0/0] quit
[PE2] interface atm 4/0/0.1 p2p
[PE2-Atm4/0/0.1] atm cell transfer
[PE2-Atm4/0/0.1] pvp 2
[PE2-atm-pvp-Atm4/0/0.1-2] quit
[PE2-Atm4/0/0.1] mpls 12vc 1.1.1.9 101
[PE2-Atm4/0/0.1] return
```

Step 6 On PE1, set the CoS of the PVP.

```
<PE1> system-view
[PE1] atm service cbr-name cbr 100 2000
[PE1] interface atm 3/0/0.1
[PE1-Atm3/0/0.1] pvp 2
[PE1-atm-pvp-Atm3/0/0.1-2] shutdown
[PE1-atm-pvp-Atm3/0/0.1-2] service output cbr-name
[PE1-atm-pvp-Atm3/0/0.1-2] undo shutdown
[PE1-atm-pvp-Atm3/0/0.1-2] return
```

 **NOTE**

Before configuring the **service output** command on a PVC or PVP, run the **shutdown** command to shut down it. Otherwise, the configuration does not take effect.

Step 7 On PE1, configure mapping rules for ATM simple traffic classification and enable simple traffic classification.

```
<PE1> system-view
[PE1] diffserv domain default
[PE1-dsdomain-default] atm-inbound cbr 0 phb af2 green
[PE1-dsdomain-default] quit
[PE1] interface atm 3/0/0.1
[PE1-Atm3/0/0.1] pvp 2
[PE1-atm-pvc-Atm3/0/0.1-2/0] trust upstream default
[PE1-atm-pvc-Atm3/0/0.1-2/0] quit
[PE1-Atm3/0/0.1] quit
[PE1] interface pos 2/0/0
[PE1-pos2/0/0] undo shutdown
```

```
[PE1-pos2/0/0] trust upstream default
[PE1-pos2/0/0] return
```

 **NOTE**

Because network traffic is bi-directional, on PE2, you also need to configure ATM simple traffic classification for the reverse traffic. The configuration is similar to that on PE1 and is not mentioned in this example.

Step 8 Verify the configuration.

- On the PE devices, view the L2VPN connections. The output shows that an L2VC is set up and the status is Up.

Take PE1 for an example:

```
[PE1] display mpls l2vc
Total ldp vc : 1      1 up      0 down
*Client Interface      : Atm3/0/0.1
Session State        : up
AC Status            : up
VC State             : up
VC ID                : 101
VC Type              : atm 1to1 vpc
Destination          : 3. 3. 3.9
local VC label       : 138240      remote VC label      : 138240
Control Word          : Disable
Local VC MTU         : 1500
Remote VC MTU        : 0
Tunnel Policy Name   : --
Traffic Behavior Name: --
PW Template Name     : --
Create time          : 0 days, 0 hours, 5 minutes, 22 seconds
UP time              : 0 days, 0 hours, 5 minutes, 22 seconds
Last change time     : 0 days, 0 hours, 5 minutes, 22 seconds
VC last up time     : 2008/07/24 12:31:31
VC total up time    : 0 days, 2 hours, 12 minutes, 51 seconds
```

- CEs (Router A and Router B) can ping through each other.
- Traffic mapping succeeds.

```
[PE1] display port-queue statistics interface Pos 2/0/0 af2 outbound
[af2]
    Total pass:                      271004559 packets,           20596342912 bytes
    Total discard:                   0 packets,           0 bytes
    Drop tail discard:              0 packets,           0 bytes
    Wred discard:                   0 packets,           0 bytes
    Last 30 seconds pass rate:     118647 pps,           9017172 bps
    Last 30 seconds discard rate:  0 pps,           0 bps
    Drop tail discard rate:       0 pps,           0 bps
    Wred discard rate:            0 pps,           0 bps
                                bps
```

----End

Configuration Files

- Configuration file of CE1

```
#           sysname CE1
#
```

```
interface Atm1/0/0
    undo shutdown
#
interface Atm1/0/0.1
    pvc 2/300
        map ip 202.38.160.2
        ip address 202.38.160.1 255.255.255.0
#
interface Atm1/0/0.2
    pvc 2/200
        map ip 202.37.10.2
        ip address 202.37.10.1 255.255.255.0
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
interface Atm2/0/0
    undo shutdown
#
interface Atm2/0/0.1
    pvc 2/300
        map ip 202.38.160.1
        ip address 202.38.160.2 255.255.255.0
#
interface Atm2/0/0.2
    pvc 2/200
        map ip 202.37.10.1
        ip address 202.37.10.2 255.255.255.0
#
return
```

- Configuration file of PE1

```
#
sysname PE1
#
atm service cbr-name cbr 100 2000
#
mpls lsr-id 1.1.1.9
mpls
    lsp-trigger all
    mpls 12vpn
#
mpls ldp
#
mpls ldp remote-peer 1
    remote-ip 3.3.3.9
#
diffserv domain default
    atm-inbound cbr 0 phb af2 green
#
interface Atm3/0/0
    undo shutdown
#
interface Atm3/0/0.1
    atm cell transfer
    pvp 2
        trust upstream default
        service output cbr-name
        mpls 12vc 3.3.3.9 101
#
interface Pos2/0/0
    undo shutdown
    link-protocol ppp
    ip address 10.1.1.1 255.255.255.0
    mpls
    mpls ldp
    trust upstream default
```

```
#  
interface LoopBack1  
ip address 1.1.1.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
    network 1.1.1.9 0.0.0.0  
    network 10.1.1.0 0.0.0.255  
#  
return
```

- Configuration file of P

```
#  
sysname P  
#  
mpls lsr-id 2.2.2.9  
mpls  
    lsp-trigger all  
#  
mpls ldp  
#  
interface Pos1/0/0  
undo shutdown  
link-protocol ppp  
ip address 10.1.1.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface Pos2/0/0  
undo shutdown  
link-protocol ppp  
ip address 10.1.2.1 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack1  
ip address 2.2.2.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
    network 2.2.2.9 0.0.0.0  
    network 10.1.1.0 0.0.0.255  
    network 10.1.2.0 0.0.0.255  
#  
return
```

- Configuration file of PE2

```
#  
sysname PE2  
#  
mpls lsr-id 3.3.3.9  
mpls  
    lsp-trigger all  
    mpls 12vpn  
#  
mpls ldp  
#  
mpls ldp remote-peer 1  
    remote-ip 1.1.1.9  
#  
interface Atm4/0/0  
undo shutdown  
#  
interface Atm4/0/0.1  
atm cell transfer  
pvp 2  
mpls 12vc 1.1.1.9 101  
#  
interface Pos2/0/0  
undo shutdown
```

```
ip address 10.1.2.2 255.255.255.0
mpls
mpls ldp
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.1.2.0 0.0.0.255
#
return
```

9.8.3 Example for Configuring Simple Traffic Classification for AAL5 SDU ATM Transparent Transmission

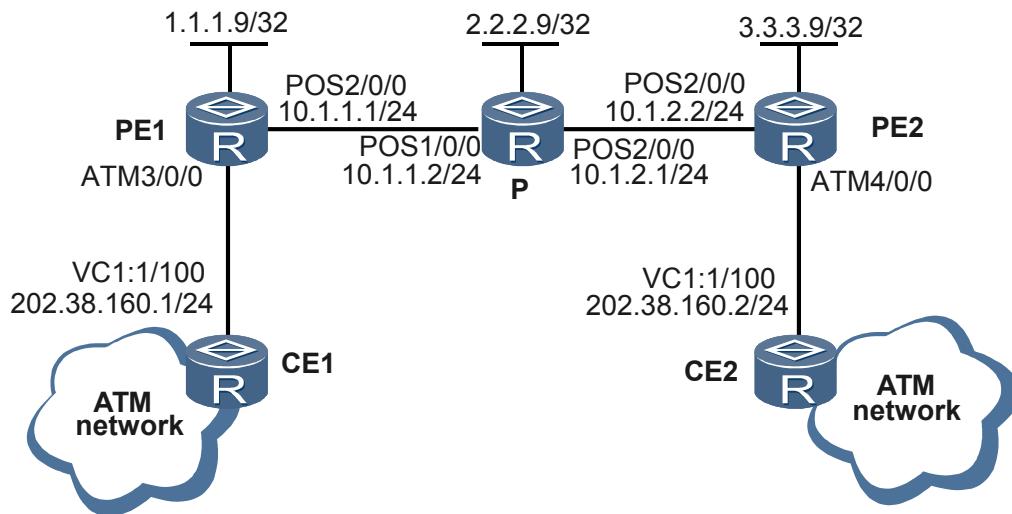
This section provides an example for configuring ATM simple traffic classification in AAL5 SDU ATM cell relay networking.

Networking Requirements

As shown in [Figure 9-8](#), the ATM interface of CE1 connects to the MPLS network through PE1, and connects to CE2 through PE2. A VC is established between Router A and Router B over the MPLS network.

Simple traffic classification is required for the upstream traffic on PE1. PE1 maps the PVC service type and the CLP of upstream traffic to its internal precedence. For downstream traffic, PE1 maps the internal precedence to the MPLS EXP field. The precedence of ATM cells is transmitted transparently over the MPLS network.

Figure 9-8 Networking diagram for configuring simple traffic classification for AAL5 SDU ATM transparent transmission



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and PVC parameters for the interfaces.
2. Configure IGP on the P and PE devices ON the MPLS network to achieve IP connectivity.
3. Configure basic MPLS functions on the P and PE devices.
4. Configure MPLS LDP on the P and PE devices.
5. Establish remote LDP sessions between the two PEs.
6. Enable MPLS L2VPN on the PE devices.
7. Configure AAL5 SDU ATM transparent transmission.
8. Configure mapping rules for ATM simple traffic classification.
9. Enable simple traffic classification.

Data Preparation

To complete the configuration, you need the following data:

- Data for configuring OSPF
- Name of the remote PE peer
- VC ID
- VPI/VCI value on the CE
- Service type and CLP value

Procedure

Step 1 Configure ATM interfaces on the CEs.

Configure CE1.

```
<CE1> system-view
[CE1] interface atm 1/0/0
[CE1-Atm1/0/0] undo shutdown
[CE1-Atm1/0/0] quit
[CE1] interface atm 1/0/0.1
[CE1-Atm1/0/0.1] ip address 202.38.160.1 24
[CE1-Atm1/0/0.1] pvc 1/100
[CE1-atm-pvc-Atm1/0/0.1-1/100] map ip 202.38.160.2
[CE1-atm-pvc-Atm1/0/0.1-1/100] return
```

Configure CE2.

```
<CE2> system-view
[CE2] interface atm 2/0/0
[CE2-Atm2/0/0] undo shutdown
[CE2-Atm2/0/0] quit
[CE2] interface atm 2/0/0.1
[CE2-Atm2/0/0.1] ip address 202.38.160.2 24
[CE2-Atm2/0/0.1] pvc 1/100
[CE2-atm-pvc-Atm2/0/0.1-1/100] map ip 202.38.160.1
[CE2-atm-pvc-Atm2/0/0.1-1/100] return
```

Step 2 Configure IGP on the MPLS network (In this example, OSPF is used).

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 2](#).

Step 3 Configure basic MPLS functions and LDP on the MPLS network.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 3](#).

Step 4 Establish remote LDP sessions between the two PEs.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 4](#).

Step 5 On the PE, enable MPLS L2VPN and configure transparent transmission of AAL5 SDU frames.

Configure PE1.

```
<PE1> system-view
[PE1] mpls l2vpn
[PE1-l2vpn] quit
[PE1] interface atm 3/0/0
[PE1-Atm3/0/0] undo shutdown
[PE1-Atm3/0/0] quit
[PE1] interface atm 3/0/0.1 p2p
[PE1-Atm3/0/0.1] pvc 1/100
[PE1-atm-pvc-Atm3/0/0.1-1/100] quit
[PE1-Atm3/0/0.1] mpls l2vc 3.3.3.9 101 no-control-word
[PE1-Atm3/0/0.1] return
```

Configure PE2.

```
<PE2> system-view
[PE2] mpls l2vpn
[PE2-l2vpn] quit
[PE2] interface atm 4/0/0
[PE2-Atm4/0/0] undo shutdown
[PE2-Atm4/0/0] quit
[PE2] interface atm 4/0/0.1 p2p
[PE2-Atm4/0/0.1] pvc 1/100
[PE2-atm-pvc-Atm4/0/0.1-1/100] quit
[PE2-Atm4/0/0.1] mpls l2vc 1.1.1.9 101 no-control-word
[PE2-Atm4/0/0.1] return
```

Step 6 On PE1, set the CoS of the PVC.

```
<PE1> system-view
[PE1] atm service cbr-name cbr 100 2000
[PE1] interface atm 3/0/0.1
[PE1-Atm3/0/0.1] pvc 1/100
[PE1-atm-pvc-Atm3/0/0.1-1/100] shutdown
[PE1-atm-pvc-Atm3/0/0.1-1/100] service output cbr-name
[PE1-atm-pvc-Atm3/0/0.1-1/100] undo shutdown
[PE1-atm-pvc-Atm3/0/0.1-1/100] return
```

NOTE

Before configuring the **service output** command on a PVC or PVP, run the **shutdown** command to shut down it. Otherwise, the configuration does not take effect.

Step 7 On PE1, configure mapping rules for ATM simple traffic classification and enable simple traffic classification.

```
<PE1> system-view
[PE1] diffserv domain default
[PE1-dsdomain-default] atm-inbound cbr 0 phb af2 green
[PE1-dsdomain-default] quit
[PE1] interface atm 3/0/0.1
[PE1-Atm3/0/0.1] pvc 1/100
[PE1-atm-pvc-Atm3/0/0.1-1/100] trust upstream default
[PE1-atm-pvc-Atm3/0/0.1-1/100] quit
[PE1-Atm3/0/0.1] quit
[PE1] interface pos 2/0/0
[PE1-pos 2/0/0] undo shutdown
[PE1-pos 2/0/0] trust upstream default
[PE1-pos 2/0/0] return
```

 NOTE

Because network traffic is bi-directional, on PE2, you also need to configure ATM simple traffic classification for the reverse traffic. The configuration is similar to that on PE1 and is not mentioned in this example.

Step 8 Verify the configuration.

- On the PE devices, view information about the L2VPN connection. The output shows that an L2VC is set up and the status is Up.

Take PE1 for an example:

```
[PE1] display mpls l2vc
Total ldp vc : 1      1 up      0 down
*Client Interface      : Atm3/0/0.1
  Session State       : up
  AC Status           : up
  VC State            : up
  VC ID               : 101
  VC Type             : atm aal5 sdu
  Destination         : 3. 3. 3.9
  local VC label      : 138240      remote VC label      : 138240
  Control Word         : Disable
  Local VC MTU        : 1500
  Remote VC MTU       : 1500
  Tunnel Policy Name  : --
  Traffic Behavior Name: --
  PW Template Name    : --
  Create time          : 0 days, 0 hours, 5 minutes, 22 seconds
  UP time              : 0 days, 0 hours, 5 minutes, 22 seconds
  Last change time    : 0 days, 0 hours, 5 minutes, 22 seconds
  VC last up time     : 2008/07/24 12:31:31
  VC total up time    : 0 days, 2 hours, 12 minutes, 51 seconds
```

- CEs (Router A and Router B) can ping through each other.
- Traffic mapping succeeds.

----End

Configuration Files

- Configuration file of CE1

```
# 
sysname CE1
#
interface Atm1/0/0
  undo shutdown
#
interface Atm1/0/0.1
  pvc 1/100
    map ip 202.38.160.2
    ip address 202.38.160.1 255.255.255.0
#
return
```

- Configuration file of CE2

```
# 
sysname CE2
#
interface Atm2/0/0
  undo shutdown
#
interface Atm2/0/0.1
  pvc 1/100
    map ip 202.38.160.1
    ip address 202.38.160.2 255.255.255.0
#
```

```
return
● Configuration file of PE1
#
  sysname PE1
#
atm service cbr-name cbr 100 2000
#
  mpls lsr-id 1.1.1.9
  mpls
    lsp-trigger all
  mpls 12vpn
#
  mpls ldp
#
  mpls ldp remote-peer 1
    remote-ip 3.3.3.9
#
  diffserv domain default
    atm-inbound cbr 0 phb af2 green
#
  interface Atm3/0/0
    undo shutdown
#
  interface Atm3/0/0.1 p2p
    pvc 1/100
      trust upstream default
      service output cbr-name
    mpls 12vc 3.3.3.9 101 no-control-word
#
  interface Pos2/0/0
    undo shutdown
    link-protocol ppp
    ip address 10.1.1.1 255.255.255.0
    mpls
    mpls ldp
      trust upstream default
#
  interface LoopBack1
    ip address 1.1.1.9 255.255.255.255
ospf 1
  area 0.0.0.0
    network 1.1.1.9 0.0.0.0
    network 10.1.1.0 0.0.0.255
    network 202.38.160.0 0.0.0.255
#
return
```

● Configuration file of P

```
#
  sysname P
#
  mpls lsr-id 2.2.2.9
  mpls
    lsp-trigger all
#
  mpls ldp
#
  interface Pos1/0/0
    undo shutdown
    link-protocol ppp
    ip address 10.1.1.2 255.255.255.0
    mpls
    mpls ldp
#
  interface Pos2/0/0
    undo shutdown
    link-protocol ppp
    ip address 10.1.2.1 255.255.255.0
    mpls
```

```
mpls ldp
#
interface LoopBack1
    ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
#
return
```

- Configuration file of PE2

```
#
sysname PE2
#
mpls lsr-id 3.3.3.9
mpls
    lsp-trigger all
    mpls 12vpn
#
mpls ldp
#
mpls ldp remote-peer 1
    remote-ip 1.1.1.9
#
interface Atm4/0/0
    undo shutdown
#
interface Atm4/0/0.1 p2p
pvc 1/100
    mpls 12vc 1.1.1.9 101 no-control-word
#
interface Pos2/0/0
    undo shutdown
ip address 10.1.2.2 255.255.255.0
mpls
    mpls ldp
#
interface LoopBack1
    ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 10.1.2.0 0.0.0.255
network 202.38.160.0 0.0.0.255
#
return
```

9.8.4 Example for Configuring 1483R-based ATM Simple Traffic Classification

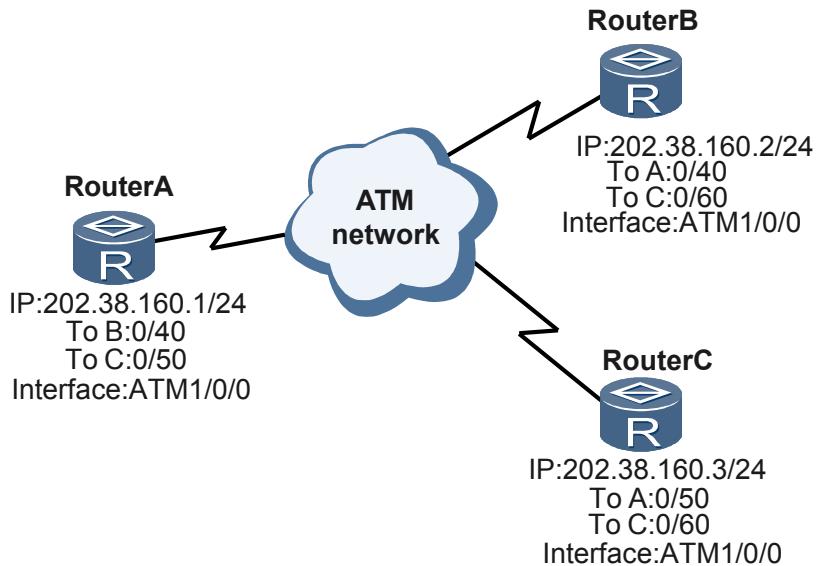
This section provides an example for configuring 1483R-based ATM simple traffic classification.

Networking Requirements

As shown in **Figure 9-9**, Router A, Router B, and Router C are located at the edge of the ATM network to provide IP network access. The three routers connect the three PSN networks that are separated by the ATM network. On the ATM network, IP packets are transmitted in AAL5 frames. When IP packets are sent out of the ATM network, the routers perform ATM termination and forward the packets to other types of interfaces.

- The IP addresses for the ATM interfaces of the three routers are 202.38.160.1/24, 202.38.160.2/24, and 202.38.160.3/24 respectively.
- On the ATM network, the VPI and VCI of Router A are 0/40 and 0/50, which are connected to Router B and Router C respectively; the VPI and VCI of Router B are 0/40 and 0/60, which are connected to Router A and Router C respectively; the VPI and VCI of Router C are 0/50 and 0/60, which are connected to Router A and Router B.
- All the PVCs on the ATM interfaces of the three routers adopt IPoA.
- On the outbound interface of Router A, enable simple traffic classification, and map the DSCP field of IP packets to the CLP of ATM cells. (In this manner, the QoS capability of the ATM network can serve IP applications.)

Figure 9-9 Networking diagram of configuring 1483R-based ATM simple traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses for interfaces.
2. Configure IPoA mapping on the PVC of each interface.
3. Configure mapping rules for ATM simple traffic classification.
4. Enable simple traffic classification.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses for the ATM interfaces of the three routers, which are 202.38.160.1/24, 202.38.160.2/24, and 202.38.160.3/24 respectively
- VPI/VCI of Router A: 0/40 and 0/50 that are connected to Router B and Router C respectively

- VPI/VCI of Router B: 0/40 and 0/60 that are connected to Router A and Router C respectively
- VPI/VCI of Router C: 0/50 and 0/60 that are connected to Router A and Router B respectively
- Service type and CLP value

Procedure

Step 1 Assign an IP address to the ATM interface and enable simple traffic classification on the interface.

```
<RouterA> system-view
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] undo shutdown
[RouterA-Atm1/0/0] ip address 202.38.160.1 255.255.255.0
[RouterA-Atm1/0/0] return
<RouterB> system-view
[RouterB] interface atm 1/0/0
[RouterB-Atm1/0/0] undo shutdown
[RouterB-Atm1/0/0] ip address 202.38.160.2 255.255.255.0
[RouterB-Atm1/0/0] return
<RouterC> system-view
[RouterC] interface atm 1/0/0
[RouterC-Atm1/0/0] undo shutdown
[RouterC-Atm1/0/0] ip address 202.38.160.3 255.255.255.0
[RouterC-Atm1/0/0] return
```

Step 2 Create a PVC and set the IPoA mapping for the PVC.

```
<RouterA> system-view
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc to_b 0/40
[RouterA-atm-pvc-Atm1/0/0-0/40-to_b] map ip 202.38.160.2
[RouterA-atm-pvc-Atm1/0/0-0/40-to_b] quit
[RouterA-Atm1/0/0] pvc to_c 0/50
[RouterA-atm-pvc-Atm1/0/0-0/50-to_c] map ip 202.38.160.3
[RouterA-atm-pvc-Atm1/0/0-0/50-to_c] return
<RouterB> system-view
[RouterB] interface atm 1/0/0
[RouterB-Atm1/0/0] pvc to_a 0/40
[RouterB-atm-pvc-Atm1/0/0-0/40-to_a] map ip 202.38.160.1
[RouterB-atm-pvc-Atm1/0/0-0/40-to_a] quit
[RouterB-Atm1/0/0] pvc to_c 0/60
[RouterB-atm-pvc-Atm1/0/0-0/60-to_c] map ip 202.38.160.3
[RouterB-atm-pvc-Atm1/0/0-0/60-to_c] return
<RouterC> system-view
[RouterC] interface atm 1/0/0
[RouterC-Atm1/0/0] pvc to_a 0/50
[RouterC-atm-pvc-Atm1/0/0-0/50-to_a] map ip 202.38.160.1
[RouterC-atm-pvc-Atm1/0/0-0/50-to_a] quit
[RouterC-Atm1/0/0] pvc to_b 0/60
[RouterC-atm-pvc-Atm1/0/0-0/60-to_b] map ip 202.38.160.2
[RouterC-atm-pvc-Atm1/0/0-0/60-to_b] return
```

Step 3 Configure mapping rules for ATM simple traffic classification and enable simple traffic classification.

NOTE

If you do not set mapping rules for the downstream, the router uses the rule in the default domain. If another DS domain is applied to the interface, the router uses the rule in the user-defined domain.

- For the traffic that enters the ATM network, set ATM mapping rules for simple traffic classification and enable simple traffic classification on Router A, Router B, and Router C.

```
<RouterA> system-view
[RouterA] diffserv domain default
```

```
[RouterA-dsdomain-default] atm-outbound af1 green map 0
[RouterA-dsdomain-default] quit
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] trust upstream default
[RouterA-Atm1/0/0] return
<RouterB> system-view
[RouterB] diffserv domain default
[RouterB-dsdomain-default] atm-outbound af1 green map 0
[RouterB-dsdomain-default] quit
[RouterB] interface atm 1/0/0
[RouterB-Atm1/0/0] trust upstream default
[RouterB-Atm1/0/0] return
<RouterC> system-view
[RouterC] diffserv domain default
[RouterC-dsdomain-default] atm-outbound af1 green map 0
[RouterC-dsdomain-default] quit
[RouterC] interface atm 1/0/0
[RouterC-Atm1/0/0] trust upstream default
[RouterC-Atm1/0/0] return
```

- Because IPoA service is configured for the traffic that comes out of the ATM network, Router A, Router B, and Router C can automatically recover the IP packets and forward them to other interfaces.

Step 4 Check the configuration.

View the status of the PVC on Router A.

```
[RouterA] display atm pvc-info
VPI/VCI | STATE | PVC-NAME | INDEX | ENCAP | PROT | INTERFACE
-----+-----+-----+-----+-----+-----+-----+
 0/40 | UP   | to_b    | 0     | SNAP  | IP   | Atm1/0/0 (UP)
 0/50 | UP   | to_c    | 1     | SNAP  | IP   | Atm1/0/0 (UP)
```

View the mapping rule for the PVC on Router A.

```
[RouterA] display atm map-info
Atm1/0/0, PVC 0/40, IP, State UP
 202.38.160.2, vlink 393217
Atm1/0/0, PVC 0/50, IP, State UP
 202.38.160.3, vlink 393218
```

Similarly, you can view the status of the PVC and the mapping rule on Router B and Router C.

On Router A, run the **ping** command to ping Router B. Router A can ping through Router B.

```
[RouterA] ping 202.38.160.2
PING 202.38.160.2: 56 data bytes, press CTRL_C to break
  Reply from 202.38.160.2: bytes=56 Sequence=1 ttl=255 time=62 ms
  Reply from 202.38.160.2: bytes=56 Sequence=2 ttl=255 time=31 ms
  Reply from 202.38.160.2: bytes=56 Sequence=3 ttl=255 time=31 ms
  Reply from 202.38.160.2: bytes=56 Sequence=4 ttl=255 time=31 ms
  Reply from 202.38.160.2: bytes=56 Sequence=5 ttl=255 time=31 ms
--- 202.38.160.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 31/37/62 ms
```

Similarly, Router A can ping through Router C; Router B can ping through Router A and Router C; Router C can ping through Router A and Router B.

----End

Configuration Files

- Configuration file of Router A.

#

```
    sysname RouterA
#
interface Atm1/0/0
undo shutdown
trust upstream default
pvc to_b 0/40
map ip 202.38.160.2
pvc to_c 0/50
map ip 202.38.160.3
ip address 202.38.160.1 255.255.255.0
#
diffserv domain default
atm-outbound afl green map 0
#
return
```

- Configuration file of Router B.

```
    #
    sysname RouterB
#
interface Atm1/0/0
undo shutdown
trust upstream default
pvc to_a 0/40
map ip 202.38.160.1
pvc to_c 0/60
map ip 202.38.160.3
ip address 202.38.160.2 255.255.255.0
#
diffserv domain default
atm-outbound afl green map 0
#
return
```

- Configuration file of Router C.

```
    #
    sysname RouterC
#
interface Atm1/0/0
undo shutdown
trust upstream default
pvc to_a 0/50
map ip 202.38.160.1
pvc to_b 0/60
map ip 202.38.160.2
ip address 202.38.160.3 255.255.255.0
#
diffserv domain default
atm-outbound afl green map 0
#
return
```

9.8.5 Example for Configuring 1483B-Based ATM Simple Traffic Classification

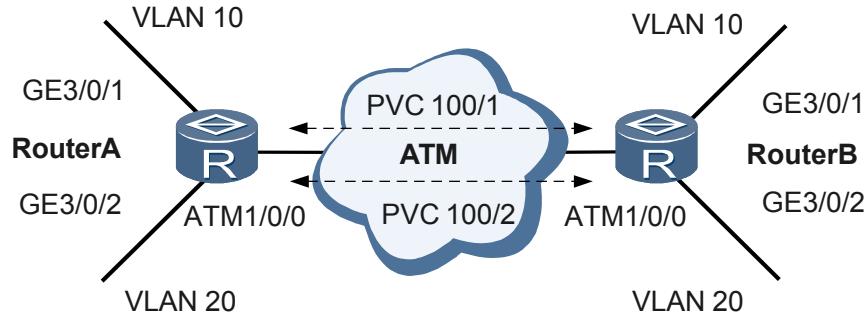
This section provides an example for configuring 1483B-based ATM simple traffic classification.

Networking Requirements

As shown in **Figure 9-10**, Router A and Router B are located at the edge of the ATM network to provide IP network access. The intranets of an enterprise are in two different locations. The ATM interfaces of the routers are used to transparently transmit Ethernet frames for the intranets. The enterprise has two departments, whose VLAN IDs are 10 and 20 respectively. ATM bridging function is enabled on the routers so that users in the same VLAN can communicate as if they

are in the same LAN. On the outbound interfaces of Router A and Router B, simple traffic classification is used to apply IP QoS to the ATM network.

Figure 9-10 Networking diagram of configuring 1483B-based ATM simple traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add GE ports into the VLANs.
2. Create VE interfaces and add the VE interface to VLANs.
3. Create a PVC and set IPoEoA mapping for the PVC.
4. Configure mapping rules for ATM simple traffic classification.
5. Enable simple traffic classification.

Data Preparation

To complete the configuration, you need the following data:

- Number of the interface that is added to the VLAN
- ID of the VLAN that is connected to the ATM network
- VPI/VCI of the PVC that is used to transparently transmit Layer 2 packets
- Service type and CLP value

Procedure

Step 1 On Router A and Router B, create VLANs and add the GE interfaces to the VLANs.

NOTE

The configuration of Router B is same with the Router A.

```

<RouterA> system view
[RouterA] vlan 10
[RouterA-vlan10] quit
[RouterA] vlan 20
[RouterA-vlan20] quit
[RouterA] interface gigabitethernet3/0/1
[RouterA-GigabitEthernet3/0/1] undo shutdown
[RouterA-GigabitEthernet3/0/1] portswitch
[RouterA-GigabitEthernet3/0/1] port default vlan 10
[RouterA-GigabitEthernet3/0/1] quit
  
```

```
[RouterA] interface gigabitethernet3/0/2
[RouterA-GigabitEthernet3/0/2] undo shutdown
[RouterA-GigabitEthernet3/0/2] portswitch
[RouterA-GigabitEthernet3/0/2] port default vlan 20
[RouterA-GigabitEthernet3/0/2] quit
[RouterA] quit
```

Step 2 On Router A and Router B, create VE interfaces and add the VE interfaces to VLANs.

```
<RouterA> system view
[RouterA] interface virtual-ethernet1/0/0
[RouterA-Virtual-Ethernet1/0/0] portswitch
[RouterA-Virtual-Ethernet1/0/0] port default vlan 10
[RouterA-Virtual-Ethernet1/0/0] quit
[RouterA] interface virtual-ethernet1/0/1
[RouterA-Virtual-Ethernet1/0/1] portswitch
[RouterA-Virtual-Ethernet1/0/1] port default vlan 20
[RouterA-Virtual-Ethernet1/0/1] quit
[RouterA] quit
```

Step 3 On Router A and Router B, create PVCs and set IPoEoA mapping for the PVC.

```
<RouterA> system view
[RouterA] interface atm1/0/0
[RouterA-Atm1/0/0] undo shutdown
[RouterA-Atm1/0/0] pvc 100/1
[RouterA-atm-pvc-Atm1/0/0-100/1-1] encapsulation aal5snap
[RouterA-atm-pvc-Atm1/0/0-100/1-1] map bridge virtual-ethernet1/0/0
[RouterA-atm-pvc-Atm1/0/0-100/1-1] quit
[RouterA-Atm1/0/0] pvc 100/2
[RouterA-atm-pvc-Atm1/0/0-100/2-2] encapsulation aal5snap
[RouterA-atm-pvc-Atm1/0/0-100/2-2] map bridge virtual-ethernet1/0/1
[RouterA-atm-pvc-Atm1/0/0-100/2-2] quit
[RouterA] quit
```

Step 4 Configure mapping rules for ATM simple traffic classification and enable simple traffic classification.

 **NOTE**

If you do not set mapping rules for the downstream, the router uses the rule in the default domain. If another DS domain is applied to the interface, the router uses the rule in the user-defined domain.

- For the traffic that enters the ATM network, set ATM mapping rules for simple traffic classification and enable simple traffic classification on Router A and Router B.

```
<RouterA> system-view
[RouterA] diffserv domain default
[RouterA-dsdomain-default] atm-outbound af1 green map 0
[RouterA-dsdomain-default] quit
[RouterA] interface atm1/0/0
[RouterA-Atm1/0/0] pvc 100/1
[RouterA-atm-pvc-Atm1/0/0-100/1-1] trust upstream default
[RouterA-Atm1/0/0] pvc 100/2
[RouterA-atm-pvc-Atm1/0/0-100/2-2] trust upstream default
[RouterA-atm-pvc-Atm1/0/0-100/2-2] return
```

- Because IPoEoA service is configured for the traffic that is sent out of the ATM network, A and Router B can automatically recover the IP packets and forward them to Ethernet interfaces.

Step 5 Verify the configuration.

View the status of the PVC on Router A and Router B.

```
[RouterA] display atm pvc-info
VPI/VCI | STATE | PVC-NAME | INDEX | ENCAP | PROT | INTERFACE
-----+-----+-----+-----+-----+-----+
100/1 | UP | | 0 | SNAP | GE | Atm3/0/1 (UP)
100/2 | UP | | 1 | SNAP | GE | Atm3/0/2 (UP)
```

PCs connected to Router A and B can ping through each other.

----End

Configuration Files

- Configuration file of Router A.

```
#  
    sysname RouterA  
#  
vlan batch 10 20  
#  
interface Atm1/0/0  
    undo shutdown  
pvc 100/1  
    map bridge Virtual-Ethernet1/0/0  
    trust upstream default  
pvc 100/2  
    map bridge Virtual-Ethernet1/0/1  
    trust upstream default  
#  
interface Gigabitethernet3/0/1  
    undo shutdown  
    portswitch  
    port default vlan 10  
#  
interface Gigabitethernet3/0/2  
    undo shutdown  
    portswitch  
    port default vlan 20  
#  
interface Virtual-Ethernet1/0/0  
    portswitch  
    port default vlan 10  
#  
interface Virtual-Ethernet1/0/1  
    portswitch  
    port default vlan 20  
#  
diffserv domain default  
    atm-outbound af1 green map 0  
#  
return
```

- Configuration file of Router B.

```
#  
    sysname RouterB  
#  
vlan batch 10 20  
#  
interface Atm1/0/0  
    undo shutdown  
pvc 100/1  
    map bridge Virtual-Ethernet1/0/0  
    trust upstream default  
pvc 100/2  
    map bridge Virtual-Ethernet1/0/1  
    trust upstream default  
#  
interface Gigabitethernet3/0/1  
    undo shutdown  
    portswitch  
    port default vlan 10  
#  
interface Gigabitethernet3/0/2  
    undo shutdown  
    portswitch  
    port default vlan 20
```

```

#
interface Virtual-Ethernet1/0/0
  portswitch
  port default vlan 10
#
interface Virtual-Ethernet1/0/1
  portswitch
  port default vlan 20
#
diffserv domain default
  atm-outbound afl green map 0
#
return

```

9.8.6 Example for Configuring Forced ATM Traffic Classification

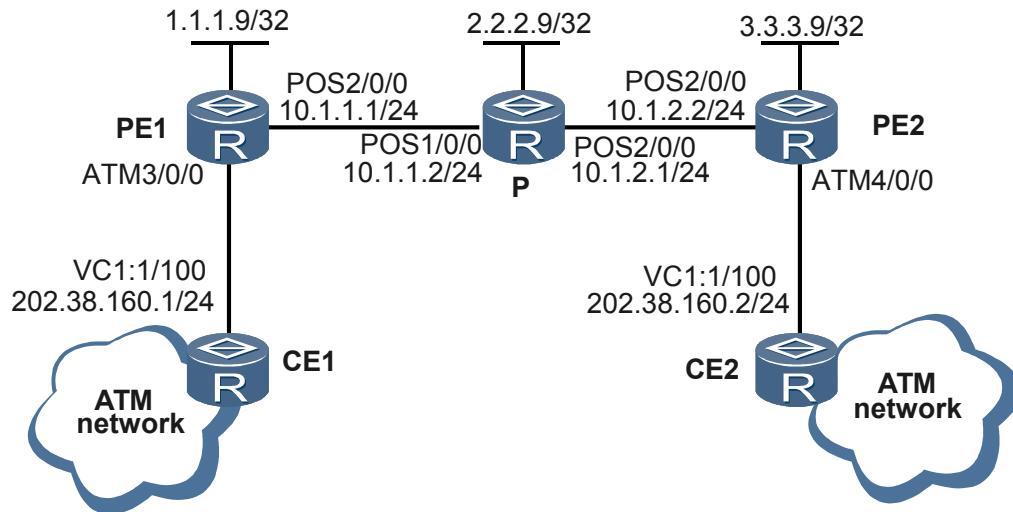
This section provides an example for configuring ATM forced traffic classification.

Networking Requirements

As shown in [Figure 9-11](#), when PE1 receives ATM cells from CE1, it transparently transmits the ATM cells over PW to PE2. PE2 then transmits the ATM cells over the ATM link.

L2VPN needs to be configured between PE1 and PE2 to implement forced traffic classification of the traffic flowing from CE1 to CE2.

Figure 9-11 Networking diagram for forced ATM traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and PVC parameters for the interfaces.
2. Configure IGP on the P and PE devices in the MPLS network to achieve IP connectivity.
3. Configure basic MPLS functions on the P and PE devices.
4. Configure MPLS LDP on the P and PE devices.
5. Establish remote LDP sessions between the two PEs.

6. Enable MPLS L2VPN on the PE devices.
7. Configure transparent transmission of ATM cells on the PE devices.
8. Configure forced ATM traffic classification on the upstream interface ATM 3/0/0 of PE1.

Data Preparation

To complete the configuration, you need the following data:

- Data for configuring OSPF
- Name of the remote PE peer
- VC ID
- VPI/VCI value on the CE
- CoS and color of IP packets on the PVC for forced ATM traffic classification

Procedure

Step 1 Configure ATM interfaces of the CEs.

Configure CE1.

```
<CE1> system-view
[CE1] interface atm 1/0/0
[CE1-Atm1/0/0] undo shutdown
[CE1-Atm1/0/0] quit
[CE1] interface atm 1/0/0.1
[CE1-Atm1/0/0.1] ip address 202.38.160.1 24
[CE1-Atm1/0/0.1] pvc 1/100
[CE1-atm-pvc-Atm1/0/0.1-1/100] map ip 202.38.160.2
[CE1-atm-pvc-Atm1/0/0.1-1/100] return
```

Configure CE2.

```
<CE2> system-view
[CE2] interface atm 2/0/0
[CE2-Atm2/0/0] undo shutdown
[CE2-Atm2/0/0] quit
[CE2] interface atm 2/0/0.1
[CE2-Atm2/0/0.1] ip address 202.38.160.2 24
[CE2-Atm2/0/0.1] pvc 1/100
[CE2-atm-pvc-Atm2/0/0.1-1/100] map ip 202.38.160.1
[CE2-atm-pvc-Atm2/0/0.1-1/100] return
```

Step 2 Configure IGP on the MPLS network (In this example, OSPF is used).

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 2](#).

Step 3 Configure based MPLS and LDP on the MPLS network.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 3](#).

Step 4 Establish LDP sessions between the two PE devices.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 4](#).

Step 5 Enable MPLS L2VPN on PEs, and then configure ATM cell relay in 1-to-1 VCC mode.

See [Example for Configuring Simple Traffic Classification for 1-to-1 VCC ATM Transparent Transmission step 5](#).

Step 6 Configure forced ATM traffic classification on PE1.

```
<PE1> system-view
[PE1] interface atm 3/0/0
[PE1-Atm3/0/0] undo shutdown
[PE1-Atm3/0/0] quit
[PE1] interface atm 3/0/0.1
[PE1-Atm3/0/0.1] traffic queue af4 green
[PE1-Atm3/0/0.1] quit
[PE1] interface pos 2/0/0
[PE1-pos2/0/0] undo shutdown
[PE1-pos2/0/0] trust upstream default
[PE1-pos2/0/0] return
```

 **NOTE**

Because network traffic is bi-directional, on PE2, you also need to configure ATM simple traffic classification for the reverse traffic. The configuration is similar to that on PE1 and is not mentioned in this example.

Step 7 Verify the configuration.

On the PE devices, view the L2VPN connections. The output shows that an L2VC is set up and the status is Up.

```
<PE1> display mpls l2vc
Total ldp vc : 1      1 up      0 down

*Client Interface      : POS2/0/0
Session State          : up
AC Status               : up
VC State                : up
VC ID                  : 1
VC Type                 : ip-interworking
Destination             : 3.3.3.9
local VC label          : 138240      remote VC label      : 138240
Control Word            : Disable
Local VC MTU            : 1500
Remote VC MTU           : 1500
Tunnel Policy Name      : --
Traffic Behavior Name   : --
PW Template Name         : --
Create time              : 0 days, 0 hours, 0 minutes, 29 seconds
UP time                  : 0 days, 0 hours, 0 minutes, 26 seconds
Last change time          : 0 days, 0 hours, 0 minutes, 26 seconds
VC last up time          : 2008/07/24 12:31:31
VC total up time          : 0 days, 2 hours, 12 minutes, 51 seconds
```

The output shows that the Session State, AC Status, and VC State are Up. This indicates that the L2VPN has been configured successfully.

From the CE, run the **ping** command to ping the other CE. The two CEs should be able to ping through each other.

----End

Configuration Files

- Configuration file of CE1

```
#          sysname CE1
#
#          interface Atm1/0/0
#          undo shutdown
```

```
#  
interface Atm1/0/0.1  
    pvc 1/100  
    map ip 202.38.160.2  
    ip address 202.38.160.1 255.255.255.0  
#  
return
```

- Configuration file of CE2

```
#  
    sysname CE2  
#  
interface Atm2/0/0  
    undo shutdown  
#  
interface Atm2/0/0.1  
    pvc 1/100  
    map ip 202.38.160.1  
    ip address 202.38.160.2 255.255.255.0  
#  
return
```

- Configuration file of PE1

```
#  
    sysname PE1  
#  
mpls lsr-id 1.1.1.9  
    mpls  
        lsp-trigger all  
    mpls 12vpn  
#  
mpls ldp  
#  
mpls ldp remote-peer 1  
    remote-ip 3.3.3.9  
#  
interface Atm3/0/0  
    undo shutdown  
#  
interface Atm3/0/0.1  
    traffic queue af4 green  
    atm cell transfer  
    pvc 1/100  
    mpls 12vc 3.3.3.9 101 no-control-word  
#  
interface Pos2/0/0  
    undo shutdown  
    ip address 10.1.1.1 255.255.255.0  
    trust upstream default  
    mpls  
    mpls ldp  
#  
interface LoopBack1  
    ip address 1.1.1.9 255.255.255.255  
#  
ospf 1  
    area 0.0.0.0  
    network 1.1.1.9 0.0.0.0  
    network 10.1.1.0 0.0.0.255  
    network 202.38.160.0 0.0.0.255  
#  
return
```

- Configuration file of P

```
#  
    sysname P  
#  
mpls lsr-id 2.2.2.9  
    mpls  
        lsp-trigger all
```

```
#  
mpls ldp  
#  
interface Pos1/0/0  
undo shutdown  
link-protocol ppp  
ip address 10.1.1.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface Pos2/0/0  
undo shutdown  
link-protocol ppp  
ip address 10.1.2.1 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack1  
ip address 2.2.2.9 255.255.255.255  
#  
ospf 1  
area 0.0.0.0  
network 2.2.2.9 0.0.0.0  
network 10.1.1.0 0.0.0.255  
network 10.1.2.0 0.0.0.255  
#  
return
```

- Configuration file of PE2

```
#  
sysname PE2  
#  
mpls lsr-id 3.3.3.9  
mpls  
lsp-trigger all  
mpls 12vpn  
#  
mpls ldp  
#  
mpls ldp remote-peer 1  
remote-ip 1.1.1.9  
#  
interface Atm1/0/0  
undo shutdown  
#  
interface Atm4/0/0.1  
traffic queue af4 green  
atm cell transfer  
pvc 1/100  
mpls 12vc 1.1.1.9 101 no-control-word  
#  
interface Pos2/0/0  
undo shutdown  
ip address 10.1.2.2 255.255.255.0  
mpls  
mpls ldp  
#  
interface LoopBack1  
ip address 3.3.3.9 255.255.255.255  
ospf 1  
area 0.0.0.0  
network 3.3.3.9 0.0.0.0  
network 10.1.2.0 0.0.0.255  
network 202.38.160.0 0.0.0.255  
#  
return
```

9.8.7 Example for Configuring the ATM Complex Traffic Classification

This section provides an example for configuring ATM complex traffic classification.

Networking Requirements

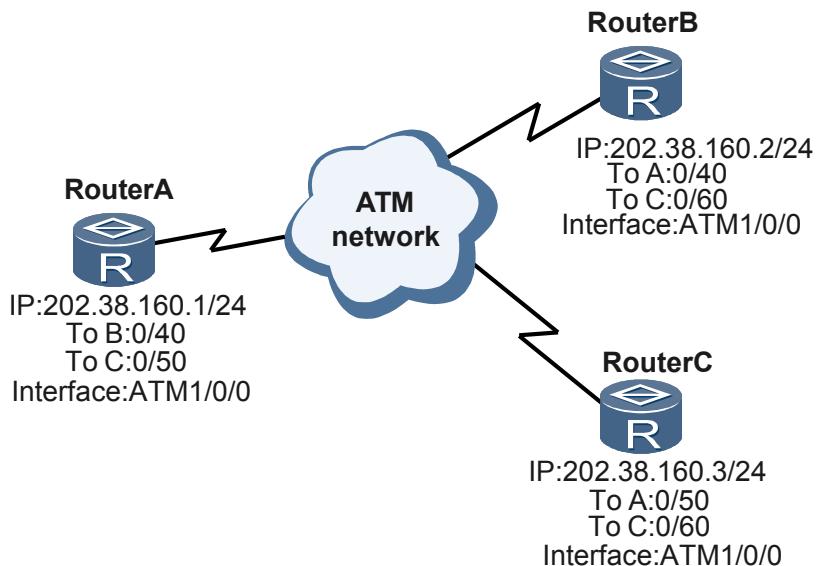
As shown in **Figure 9-12**, Router A, Router B, and Router C are at the edge of the ATM network. They provide IP network access, enabling communications between the three separated packet switched networks (PSNs). IP packets are encapsulated into AAL5 frames when they are transmitted over the ATM network. The service is therefore called the IPoA service. When the packets leave the ATM network, the AAL5 frame headers are removed on the router before the packets are forwarded to other types of interfaces.

- The IP addresses of the ATM interfaces of the three routers are 202.38.160.1/24, 202.38.160.2/24, and 202.38.160.3/24.
- On the ATM network, the VPIs/VCIs of Router A are 0/40 and 0/50, which connect Router B and Router C respectively; the VPIs/VCIs of Router B are 0/40 and 0/60, which connect Router A and Router C respectively; the VPIs/VCIs of Router C are 0/50 and 0/60 respectively, which connect Router A and Router B respectively.
- All PVCs on the ATM interfaces of the three routers are in IPoA mode.

The specific requirements are as follows:

The downstream ATM 1/0/0 on Router A is enabled with the complex traffic classification. All ATM cells carrying the IP packets with the IP precedence of 5, 6, and 7 can pass; the ATM cells carrying the IP packets with the IP precedence of 4 are guaranteed a bandwidth of 2 Mbit/s.

Figure 9-12 Networking diagram for configuring the ATM complex traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses for the interfaces.
2. Configure traffic classifiers.
3. Configure traffic behaviors.
4. Configure traffic policies.
5. Apply traffic policies to the ATM interfaces.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the ATM interfaces of the three routers: 202.38.160.1/24, 202.38.160.2/24, and 202.38.160.3/24.
- VPIs/VCIs of Router A: 0/40 and 0/50, which connect Router B and Router C respectively
- VPIs/VCIs of Router B: 0/40 and 0/60, which connect Router A and Router C respectively
- VPIs/VCIs of Router C: 0/50 and 0/60, which connect Router A and Router B respectively
- Parameters for the ATM complex traffic classification: names of traffic classifiers, IP precedence, names of traffic behaviors, guaranteed bandwidths, the name of a traffic policy, and interfaces to which the policy is applied

Procedure

Step 1 Enter the system view and configure IP addresses for the ATM interfaces of the routers.

```
<RouterA> system-view
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] undo shutdown
[RouterA-Atm1/0/0] ip address 202.38.160.1 255.255.255.0
[RouterA-Atm1/0/0] return
<RouterB> system-view
[RouterB] interface atm 1/0/0
[RouterB-Atm1/0/0] undo shutdown
[RouterB-Atm1/0/0] ip address 202.38.160.2 255.255.255.0
[RouterB-Atm1/0/0] return
<RouterC> system-view
[RouterC] interface atm 1/0/0
[RouterC-Atm1/0/0] undo shutdown
[RouterC-Atm1/0/0] ip address 202.38.160.3 255.255.255.0
[RouterC-Atm1/0/0] return
```

Step 2 Create PVCs and configure IPoA mappings for the PVCs.

```
<RouterA> system-view
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc to_b 0/40
[RouterA-atm-pvc-Atm1/0/0-0/40-to_b] map ip 202.38.160.2
[RouterA-atm-pvc-Atm1/0/0-0/40-to_b] quit
[RouterA-Atm1/0/0] pvc to_c 0/50
[RouterA-atm-pvc-Atm1/0/0-0/50-to_c] map ip 202.38.160.3
[RouterA-atm-pvc-Atm1/0/0-0/50-to_c] return
<RouterB> system-view
[RouterB] interface atm 1/0/0
[RouterB-Atm1/0/0] pvc to_a 0/40
[RouterB-atm-pvc-Atm1/0/0-0/40-to_a] map ip 202.38.160.1
[RouterB-atm-pvc-Atm1/0/0-0/40-to_a] quit
[RouterB-Atm1/0/0] pvc to_c 0/60
[RouterB-atm-pvc-Atm1/0/0-0/60-to_c] map ip 202.38.160.3
[RouterB-atm-pvc-Atm1/0/0-0/60-to_c] return
<RouterC> system-view
[RouterC] interface atm 1/0/0
[RouterC-Atm1/0/0] pvc to_a 0/50
[RouterC-atm-pvc-Atm1/0/0-0/50-to_a] map ip 202.38.160.1
```

```
[RouterC-atm-pvc-Atm1/0/0-0/50-to_a] quit
[RouterC-Atm1/0/0] pvc to_b 0/60
[RouterC-atm-pvc-Atm1/0/0-0/60-to_b] map ip 202.38.160.2
[RouterC-atm-pvc-Atm1/0/0-0/60-to_b] return
```

Step 3 Configure the ATM complex traffic classification.

Create traffic classifiers and define matching rules.

```
[RouterA] traffic classifier a
[RouterA-classifier-a] if-match ip-precedence 7
[RouterA-classifier-a] if-match ip-precedence 6
[RouterA-classifier-a] if-match ip-precedence 5
[RouterA-classifier-a] quit
[RouterA] traffic classifier b
[RouterA-classifier-b] if-match ip-precedence 4
[RouterA-classifier-b] quit
```

After the preceding configuration, you can run the **display** command to view the configuration of the traffic classifiers.

```
[RouterA] display traffic classifier user-defined
User Defined Classifier Information:
    Classifier: b
    Operator: OR
Rule(s): if-match ip-precedence 4
    Classifier: a
    Operator: OR
Rule(s) : if-match ip-precedence 7
    if-match ip-precedence 6
    if-match ip-precedence 5
```

Define traffic behaviors.

```
[RouterA] traffic behavior a
[RouterA-behavior-a] permit
[RouterA-behavior-a] quit
[RouterA] traffic behavior b
[RouterA-behavior-b] car cir 2000
[RouterA-behavior-b] quit
```

After the preceding configuration, you can run the **display** command to view the configuration of the traffic classifiers.

```
[PE1] display traffic behavior user-defined
User Defined Behavior Information:
    Behavior: b
        Committed Access Rate:
            CIR 2000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 0 (byte)
            Conform Action: pass
            Yellow Action: pass
            Exceed Action: discard
    Behavior: a
        Firewall:
            permit
```

Define a traffic policy and associate the traffic classifiers with the traffic behaviors.

```
[RouterA] traffic policy p
[RouterA-trafficpolicy-a] classifier a behavior a
[RouterA-trafficpolicy-a] classifier b behavior b
[RouterA-trafficpolicy-a] quit
```

Apply the traffic policy to the outbound interface.

```
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] undo shutdown
[RouterA-Atm1/0/0] traffic-policy p outbound
[RouterA-Atm1/0/0] quit
```

Step 4 Verify the configuration.

Run the **display traffic policy** command. You can view the configuration of the traffic policies, traffic classifiers defined in the traffic policies, and the traffic behaviors associated with traffic classifiers.

```
[RouterA] display traffic policy user-defined
User Defined Traffic Policy Information:
Policy: p
    Classifier: default-class
        Behavior: be
        -none-
    Classifier: a
        Behavior: a
        Firewall:
            permit
    Classifier: b
        Behavior: b
        Committed Access Rate:
            CIR 2000 (Kbps), PIR 0 (Kbps), CBS 10000 (byte), PBS 0 (byte)
        Conform Action: pass
        Yellow Action: pass
        Exceed Action: discard
```

Run the **display interface** command on Router A. You can view that the traffic on the interfaces are controlled according to the specified requirements.

----End

Configuration Files

- Configuration file of Router A

```
#           sysname RouterA
#
traffic classifier a
    if-match ip-precedence 7
    if-match ip-precedence 6
    if-match ip-precedence 5
traffic classifier b
    if-match ip-precedence 4
#
traffic behavior a
    permit
traffic behavior b
    car cir 2000 cbs 10000 pbs 0 green pass red discard
#
traffic policy p
    classifier a behavior a
    classifier b behavior b
#
interface Atm1/0/0
    undo shutdown
    pvc to_b 0/40
        map ip 202.38.160.2
    pvc to_c 0/50
        map ip 202.38.160.3
    ip address 202.38.160.1 255.255.255.0
    traffic-policy p outbound
#
return
```

- Configuration file of Router B

```
#           sysname RouterB
#
interface Atm1/0/0
```

```
undo shutdown
pvc to_a 0/40
    map ip 202.38.160.1
pvc to_c 0/60
    map ip 202.38.160.3
ip address 202.38.160.2 255.255.255.0
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface Atm1/0/0
    undo shutdown
pvc to_a 0/50
    map ip 202.38.160.1
pvc to_b 0/60
    map ip 202.38.160.2
ip address 202.38.160.3 255.255.255.0
#
return
```

9.8.8 Example for Configuring Queue Scheduling for an ATM PVC

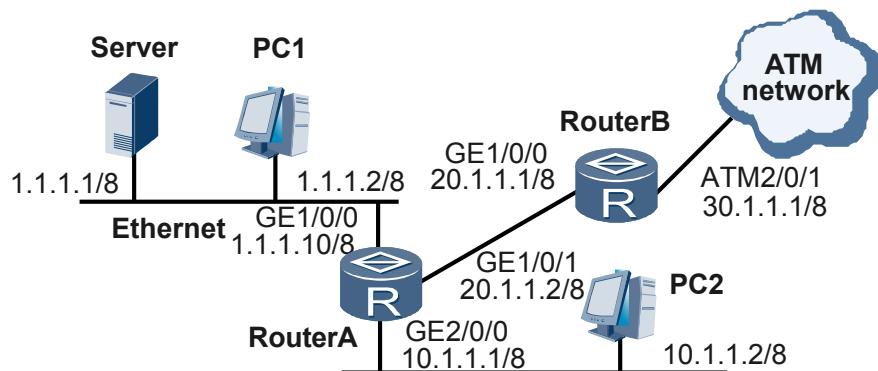
This section provides an example for configuring queue scheduling on ATM PVCs.

Networking Requirements

As shown in **Figure 9-13**, GE 1/0/1 of Router A connects to GE 1/0/0 of Router B. Server, PC1, and PC2 can access the Internet through Router A and Router B. Server, PC1, and GE1/0/0 of Router A are in the same network segment. PC2 and GE 2/0/0 of Router A are in the same network segment.

To avoid congestion when huge traffic enters the ATM network, it is required that traffic shaping and queue scheduling be configured on ATM 2/0/1 of Router B.

Figure 9-13 Networking diagram for configuring queue scheduling of ATM PVCs



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses for interfaces and the route.
2. Configure IPoA on Router B.
3. Configure the traffic shaping for the ATM PVC on ATM 2/0/1 of Router B.
4. Configure the queue scheduling for the ATM PVC on ATM 2/0/1 of Router B.

Data Preparation

To complete the configuration, you need the following data:

- PVC name and VPI or VCI number
- Traffic shaping rate
- Queue name, queue scheduling type, and WFQ weight

Procedure

Step 1 Configure IP addresses and routes to ensure normal operation of the network (omitted).

Step 2 Create a PVC and configure IPoA mapping of the PVC (omitted).

For details of the configurations, refer to "ATM Configuration" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - WAN Access*.

Step 3 Configure the simple traffic classification on GE 1/0/0 of Router B.

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 20.1.1.1 255.0.0.0
[RouterB-GigabitEthernet1/0/0] trust upstream default
[RouterB-GigabitEthernet1/0/0] return
```

Step 4 Configure the traffic shaping and queue scheduling for the ATM PVC on Router B.

```
<RouterB> system-view
[RouterB] atm service cbr-name cbr 100 2000
[RouterB] interface atm 2/0/1
[RouterB-Atm2/0/1] pvc 0/40
[RouterB-atm-pvc-Atm2/0/1-0/40] shutdown
[RouterB-atm-pvc-Atm2/0/1-0/40] service output cbr-name
[RouterB-atm-pvc-Atm2/0/1-0/40] pvc-queue ef pq outbound
[RouterB-atm-pvc-Atm2/0/1-0/40] pvc-queue af4 wfq 50 outbound
[RouterB-atm-pvc-Atm2/0/1-0/40] undo shutdown
[RouterB-atm-pvc-Atm2/0/1-0/40] return
```

Step 5 Verify the configuration.

Run the **display atm pvc-queue** command on Router B and view the queue scheduling information about PVC 0/40 on ATM 4/0/1. For example:

```
<RouterB> display atm pvc-queue interface atm 4/0/1 pvc 0/40
Show CBQ PVC configuration of interface Atm4/0/1 PVC 0/40:
    be distribute OutBound wfq Weight 20
    af1 distribute OutBound wfq Weight 20
    af2 distribute OutBound wfq Weight 20
    af3 distribute OutBound wfq Weight 20
    af4 distribute OutBound wfq Weight 50
    ef distribute OutBound pq
    cs6 distribute OutBound wfq Weight 20
    cs7 distribute OutBound wfq Weight 20
```

----End

Configuration Files

- Configuration file of Router A

```
#  
    sysname RouterA  
#  
    interface gigabitEthernet1/0/0  
        undo shutdown  
        ip address 1.1.1.10 255.0.0.0  
#  
    interface gigabitEthernet1/0/1  
        undo shutdown  
        ip address 20.1.1.2 255.0.0.0  
#  
    interface gigabitEthernet2/0/0  
        undo shutdown  
        ip address 10.1.1.1 255.0.0.0  
#  
ospf 1  
area 0.0.0.0  
    network 1.0.0.0 0.255.255.255  
    network 10.0.0.0 0.255.255.255  
network 20.0.0.0 0.255.255.255  
#  
return
```

- Configuration file of Router B

```
#  
    sysname RouterB  
#  
    atm service cbr-name cbr 100 2000  
#  
    interface GigabitEthernet1/0/0  
        undo shutdown  
        ip address 20.1.1.1 255.0.0.0  
        trust upstream default  
#  
    interface Atm2/0/1  
        undo shutdown  
        ip address 30.1.1.1 255.0.0.0  
        pvc 0/40  
            map ip 202.38.160.2  
        service output cbr-name  
        pvc-queue ef pq outbound  
        pvc-queue af4 wfq 50 outbound  
#  
ospf 1  
area 0.0.0.0  
    network 20.0.0.0 0.255.255.255  
network 30.0.0.0 0.255.255.255  
#  
return
```

10 HQoS Configuration

About This Chapter

Conventional QoS performs interface-based queue scheduling in which different users and different types of services of the same user cannot be identified. HQoS performs queue scheduling for user-specific traffic.

NOTE

HQoS Scheduling for Family Users cannot be configured on the X1 and X2 models of the NE80E/40E.

HQoS Scheduling for Leased Line Users cannot be configured on the X1 and X2 models of the NE80E/40E.

[10.1 HQoS Overview](#)

HQoS offers refined QoS for advanced users. This section provides basic concepts and principle of HQoS.

[10.2 Configuring HQoS on an Ethernet Interface](#)

In HQoS, multiple sub-interfaces are configured for an Ethernet main interface. In this case, each user can access the network through an Ethernet sub-interface, better utilizing the interface bandwidth.

[10.3 Configuring HQoS on a QinQ Termination Sub-interface](#)

After HQoS is configured on a sub-interface for QinQ VLAN tag termination, packets from different VLANs can be differentiated when they enter the ISP network.

[10.4 Configuring Class-based HQoS](#)

Class-based HQoS classifies users in the case of a limited number of interfaces and performs hierarchical scheduling for traffic from different users.

[10.5 Configuring Profile-based HQoS](#)

Profile-based HQoS places traffic from multiple interfaces into an SQ for scheduling. It implements uniform scheduling for traffic on multiple interfaces by defining QoS profiles and applying the profiles to different interfaces.

[10.6 Configuring HQoS Scheduling for Family Users](#)

HQoS for family users performs uniform scheduling for an entire family rather than individual terminals.

[10.7 Configuring HQoS Scheduling for Common Users](#)

HQoS for common users identifies services by priority and then performs uniform scheduling.

10.8 Configuring HQoS Scheduling for Leased Line Users

Leased line users share the same SQ and HQoS performs uniform scheduling for leased line users.

10.9 Maintaining HQoS

This section describes how to clear HQoS statistics.

10.10 Configuration Examples

This section provides examples for configuring HQoS, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

10.1 HQoS Overview

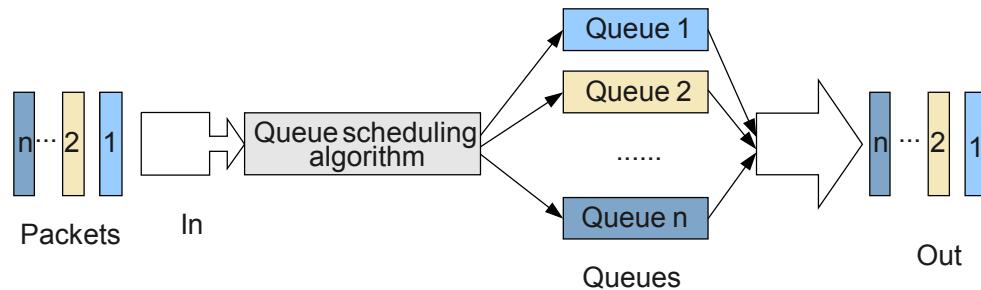
HQoS offers refined QoS for advanced users. This section provides basic concepts and principle of HQoS.

10.1.1 Introduction to HQoS

Different from conventional QoS that performs queue scheduling based on interfaces, HQoS identifies different users and different services of the same user on a single interface.

Traditional QoS performs traffic scheduling on the basis of the interface. A single interface can distinguish service priorities but cannot identify users or services of the same user. Packets of the same priority go to the same interface queue and compete for resources in the same queue. As a result, the traditional QoS is unable to identify packets from a specific user on an interface and to provide differentiated services for this type of packets. [Figure 10-1](#) shows the queue scheduling principle of traditional QoS.

Figure 10-1 Principle of traditional QoS queue scheduling



For example, two users want to send AF4 packets at the same time: user 1 sends packets at 10 Mbit/s and user 2 sends packets at 1 Gbit/s. The traffic rate of AF4 flows is limited to 10 Mbit/s.

Traditional QoS does not identify users. Because user 2 sends AF4 packets at a higher rate, these packets are more likely to enter the queue whereas packets from user 1 have a higher chance of being discarded.

This mechanism results in the fact that user 1's traffic is easily affected by other users' traffic. This is unfavorable for a telecommunication carrier to develop user-specific services for enterprises and subscribers. The reason is that a carrier is unable to ensure the quality of service for traffic of all users; as a result, the carrier is unable to attract more users to buy its products and services.

Nowadays, network users and services are expanding continuously. Users and service providers both expect user-specific and differentiated services so that users can obtain better quality of service and service providers can reap in more profits. HQoS can provide better user-specific quality of service for advanced users and save cost in network operation and maintenance, and therefore has huge market demands.

10.1.2 Related Concepts of HQoS

Basic concepts of HQoS include the flow queue (FQ), subscriber queue (SQ), subscriber group queue (GQ), class queue (CQ), and low priority queue (LPQ).

Flow Queue

HQoS enables the router to perform user-specific queue scheduling. You can restrict the bandwidth of a user by setting the PIR. A user's services can be classed into eight FQs. You can configure PQ, WFQ or LPQ scheduling and WRED for each flow queue and configure the traffic rate for traffic shaping.

Subscriber Queue

A subscriber queue (SQ) is a virtual queue, meaning that there is no buffer for the queue. Data enters or leaves the queue without any delay. The queue is only one level participating in hierarchical scheduling for output packets.

Each SQ is mapped to eight types of FQ priority and can be configured with one to eight FQs. The idle queues of an SQ cannot be used by other SQs, that is, one to eight FQs share the total bandwidth of the SQ. Each SQ corresponds to one user, which is either a VLAN or a VPN. Each user can use one to eight FQs, and the CIR and PIR of an SQ are configurable.

Group Queue

One group queue (GQ) consists of multiple SQs that are bundled to carry out Level-3 queue scheduling.

A GQ functions to limit the traffic rate of a group of users as a whole. Setting the shaping value to a value not less than the sum of CIRs of SQs in the GQ is recommended. Otherwise, the traffic rate of an SQ in the GQ cannot be guaranteed.

A GQ is also a virtual queue. Each SQ can be in only one GQ. If it is not in any GQ, the router skips Level-3 queue scheduling.

A GQ can be used to perform traffic shaping. You can set the traffic shaping rate for a GQ.

Class Queue

In HQoS scheduling, packets of FQs, after CQ scheduling, enter CQs on the interface together with common packets. For packets of an FQ entering a CQ, the router supports two priority mapping models:

- Uniform

The eight levels of FQs of each SQ map the eight CQs on an interface. The mapping relationships are pre-defined by the system.

- Pipe

The mapping between the eight levels of FQs of the SQ and the eight CQs on the interface can be configured manually. The pipe model, however, does not affect the priority of packets.

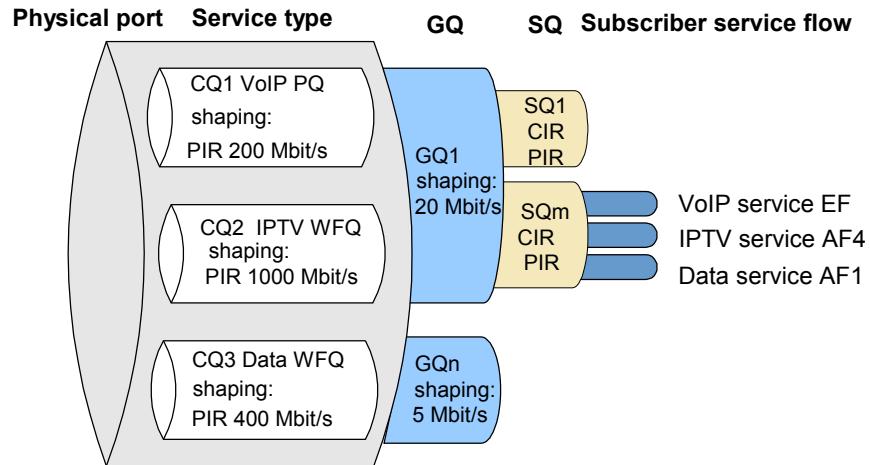
10.1.3 HQoS Supported by the NE80E/40E

HQoS features supported by the device include Ethernet interface-based HQoS, class-based HQoS, profile-based HQoS, and HQoS for multi-play services.

HQoS Implementation on an Ethernet Interface

The router performs five-level HQoS scheduling on an Ethernet interface for upstream traffic and downstream traffic, and in this manner delivers rich QoS services to users. [Figure 10-2](#) shows the principle of HQoS scheduling on an Ethernet interface.

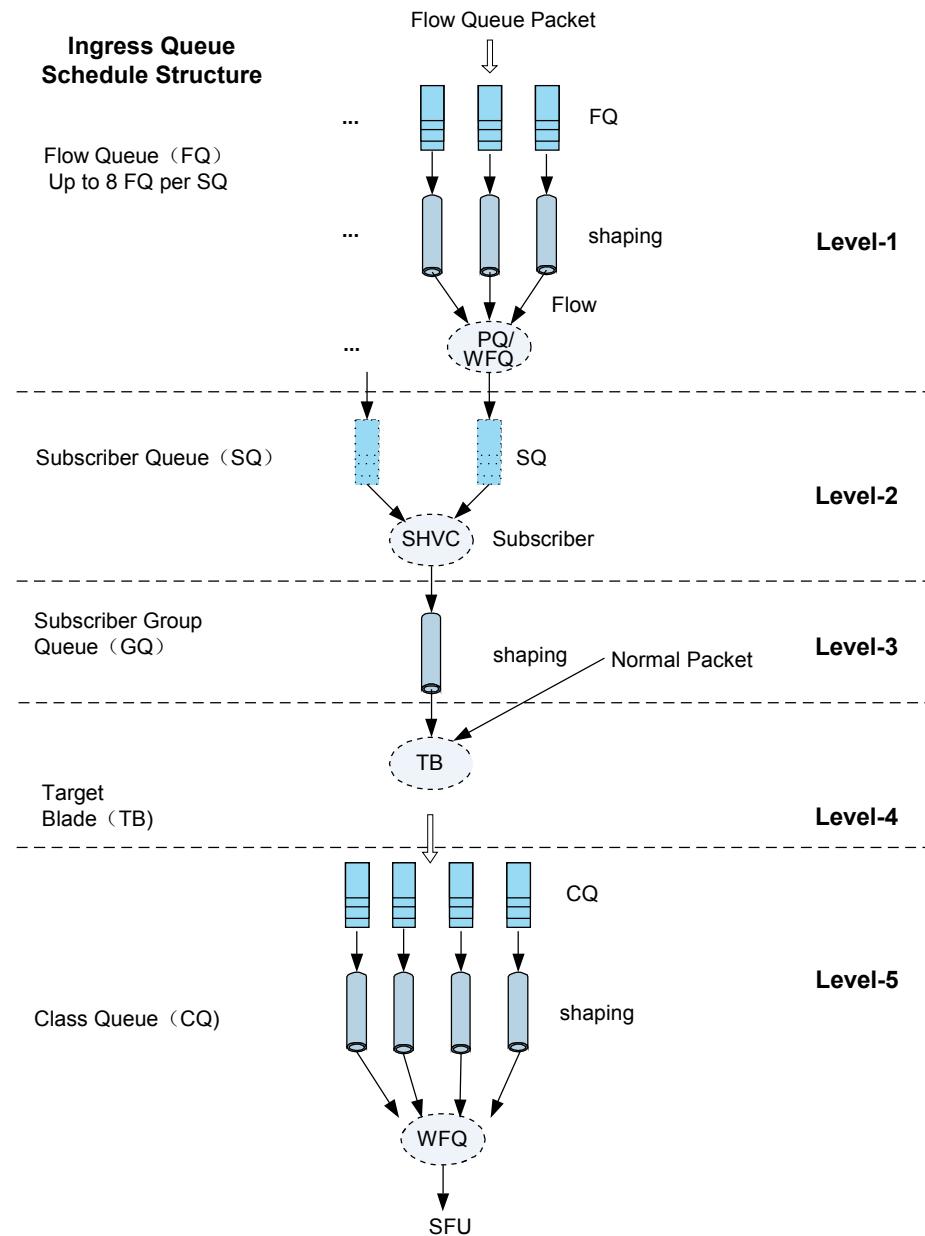
Figure 10-2 Principle of HQoS scheduling on an Ethernet interface



- Upstream HQoS

Upstream HQoS is available at five levels: Flow Queue (FQ) - Subscriber Queue (SQ) - Group Queue (GQ) - Target Blade (TB) - Class Queue (CQ), as shown in [Figure 10-3](#).

Figure 10-3 Upstream HQoS scheduling on an Ethernet interface



1. Level-1 queue scheduling: FQ

An FQ is a physical queue, which is identified by the priority of a user service and which is used for storing the data of each flow temporarily. A delay occurs when data enters or leaves the queue. You can set the scheduling weight, shaping value, and flow-wred object for each FQ. The mapping between two levels of physical queues, namely FQ and CQ, can be implemented based on the customized flow mapping template.

2. Level-2 queue scheduling: SQ

The SQ is a virtual queue, meaning that there is no buffer for the queue. Data enters or leaves the queue without any delay. The queue serves only as one level participating in the hierarchical scheduling for output scheduling. You can set the scheduling

weight, CIR, and PIR for each SQ; you can also set the FQ, flow mapping, and GQ object that are referenced by the SQ.

One SQ is mapped to eight types of FQs. You can choose to use up to eight FQs based on actual conditions. The idle queues of an SQ cannot be used by other SQs, that is, one to eight FQs share the total bandwidth of the SQ. In application, each SQ corresponds to one user, which is either a VLAN or a VPN. Each user can use one to eight FQs with different service priorities. An SQ can reference up to one GQ, or it can reference no GQ at all.

3. Level-3 queue scheduling: GQ

A GQ is also a virtual queue. One GQ consists of multiple SQs that are bundled to carry out the third-level queue scheduling. You can set the shaping value for each GQ. A GQ performs virtual scheduling and can only limit the traffic rate. Each SQ can be in only one GQ. If it is not in any GQ, the router does not perform the third-level queue scheduling. One GQ can schedule multiple SQs.

4. Level-4 queue scheduling: TB

TB performs queue scheduling among boards. A TB has four buffer queues, which correspond to four service CQs. This level of scheduling is pre-defined by the system and is not configurable.

5. Level-5 queue scheduling: CQ

A CQ is a physical queue. Each physical interface for upstream HQoS corresponds to four CQs that identify users' upstream service flows. You can set the scheduling weight, shaping value, and port-wred object for each CQ. After CQ scheduling, users' data is forwarded at a high rate through the switching fabric card (SFC). Upstream HQoS scheduling of CQs is pre-defined by the system and is not configurable.

● Processing of upstream HQoS on Ethernet interfaces

1. The router performs simple traffic classification of packets and marks each packet with one of the eight service priorities.
2. Classified packets are identified as belonging to a certain SQ or GQ on the interface. Then they enter the eight FQs of the SQ based on the service priority.
 - To shape the FQ, a user can set the FQ congestion avoidance parameters and queue scheduling policy; a user can also set the mapping relationship between a certain service in an SQ and a CQ.

 **NOTE**

You can set the PQ, WFQ, or LPQ scheduling mode for an FQ.

The three queue scheduling modes are in the following sequence of priorities (from high to low):

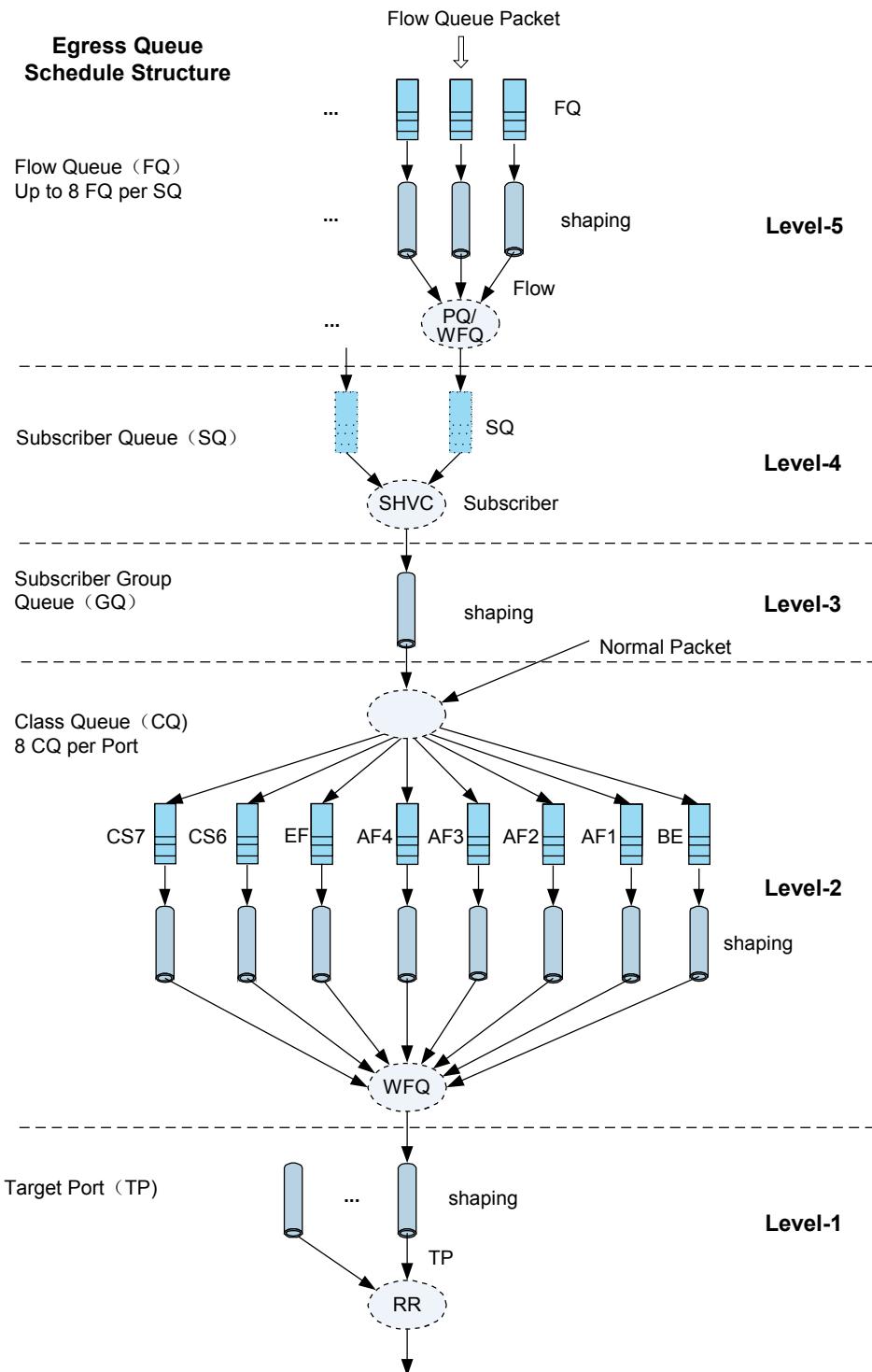
PQ > WFQ > LPQ

A queue of a higher priority can preempt the bandwidth of a queue of a lower priority.

- Users can set the bandwidth for an SQ, the GQ name, and the FQ referential relationship. Each SQ can be in no more than one GQ, or no GQ at all. If an SQ is not in any GQ, the router does not perform the third-level queue scheduling on the SQ.
 - Users can set the bandwidth for a GQ.
3. In queue scheduling, the scheduler first checks whether the GQ has sufficient bandwidth.
 - If the GQ has sufficient bandwidth resources, the router forwards the SQ packets in the GQ at the configured bandwidth.

- If the GQ does not have sufficient bandwidth resources, packets in the GQ are discarded.
 - 4. The system checks whether the SQs in the GQ have sufficient bandwidth resources.
 - If the SQs have sufficient bandwidth resources, the router forwards the FQ packets in the SQ at the configured bandwidth.
 - If the SQs do not have sufficient bandwidth resources, the packets in the SQ are discarded.
 - 5. The packets in FQs are given TB scheduling. These packets then enter CQs based on the mappings between FQs and CQs.
 - 6. The packets are then forwarded through the SFC after CQ scheduling.
- Downstream HQoS
- Downstream HQoS scheduling is available at five levels: Flow Queue - Subscriber Queue (virtual queue) - Group Queue (virtual queue) - Class Queue - target port, as shown in [Figure 10-4](#).

Figure 10-4 Downstream HQoS scheduling on an Ethernet interface



The first three levels of queue scheduling, namely, Level-1 queue scheduling (FQ), Level-2 queue scheduling (SQ), and Level-3 queue scheduling (GQ) are the same as those of upstream HQoS scheduling.

Level-4 queue scheduling: CQ. A CQ is a physical queue. Each physical interface for downstream HQoS corresponds to eight CQs, which identify users' downstream service flows based on service priorities. You can set the scheduling weight, shaping value, and port-wred object for each CQ. Users' data is mapped to the CQ for scheduling based on the configured mapping between the FQ and the CQ.

Level-5 queue scheduling: TP. TP schedules data among the interfaces. TP has buffer queues, which correspond to eight CQ service queues. After TP scheduling, users' data is forwarded through the corresponding interface. This scheduling is pre-defined by the system and is not configurable.

The processing of downstream HQoS is similar to that of upstream HQoS and is not described here. The only difference is that users can set the congestion avoidance parameters and queue scheduling policy to shape the CQ.

HQoS may be required either on the user side or the network side. To meet the requirement, the product is able to deliver both upstream and downstream HQoS. You can deploy HQoS based on users' requirements and choose to implement HQoS either in one direction, or in both.

You can configure the five-level HQoS scheduling on the Ethernet, GE, or Eth-Trunk, or the corresponding sub-interfaces.

Class-based HQoS

Class-based HQoS is an extension of interface-based HQoS, which combines complex traffic classification (CTC) and HQoS.

Interface-based HQoS takes the traffic on an interface or a sub-interface as belonging to only one user. In actual networking, however, operators hope to use an interface or a sub-interface to deliver hierarchical traffic scheduling to multiple users. Interface-based HQoS, however, is incapable of further classifying users based on the traffic on one interface.

By integrating the classification function of the CTC and the queue scheduling function of HQoS, class-based HQoS enables refined traffic classification and hierarchical scheduling of classified traffic.

The device carries out class-based HQoS in the following manner:

- Classifies traffic that needs HQoS scheduling through the CTC.
- Configures HQoS parameters by taking all the packets that match a classifying rule as belonging to one user. The system then distributes resources based on the configured HQoS parameters for HQoS scheduling.

NOTE

- To configure interface-based HQoS, you need to directly configure Subscriber Queues (SQs) on an interface; you also need to specify the parameter **inbound** or **outbound** to configure upstream HQoS scheduling or downstream HQoS scheduling on the interface.
- To configure class-based HQoS, you need to configure SQs in a traffic behavior. The HQoS configuration takes effect after you apply the traffic policy that contains the traffic behavior to an interface.
- Class-based HQoS is valid to upstream traffic only.
- For the interface-based HQoS and class-based HQoS, the configurations of Flow Queues (FQs), Group Queues (GQs), and Class Queues (CQs) are the same.
- The interior scheduling mechanism for class-based HQoS is exactly the same as that for interface-based HQoS.

Class-based HQoS supports the Ethernet interface, GE interface, Eth-Trunk interface, and the Layer 2 interface and sub-interface of the preceding three types of interfaces. Class-based HQoS also supports the POS interface, IP-Trunk interface, RINGIF interface, and tunnel interface.

Profile-based HQoS

Profile-based HQoS implements QoS scheduling management of access users mainly by defining various QoS templates and applying the QoS templates to interfaces. A QoS template is the aggregate of QoS scheduling parameters. Configurable scheduling parameters for user queues include assured bandwidth, peak bandwidth, templates for flow queues, and lengths for packet loss compensation of service templates.

Profile-based HQoS binds the five-level HQoS resource scheduling to users, which satisfies the varying demands for traffic control of the same user that accesses through different interfaces. This can better implement HQoS scheduling based on user levels in an all-round way.

HQoS Scheduling for the Multi-Play Service

HQoS scheduling for the Multi-Play service includes HQoS scheduling for family users, common users, and leased line access users.

With the development of the Multi-Play service, a family may have several terminals to implement various services, such as the voice service, video service, and data service. In a family, different services have different requirements for the delay, jitter, and bandwidth. In addition, resources must be ensured for the preferential service when network resources are insufficient. Therefore, QoS scheduling must take a family but not a terminal as a unit; otherwise, the quality of special services (such as the voice service) cannot be guaranteed when multiple services are implemented at the same time for a family.

10.2 Configuring HQoS on an Ethernet Interface

In HQoS, multiple sub-interfaces are configured for an Ethernet main interface. In this case, each user can access the network through an Ethernet sub-interface, better utilizing the interface bandwidth.

Context



Configuring upstream HQoS on an Ethernet interface is independent from configuring downstream HQoS. They do not affect each other.

Currently you can configure only FQ, SQ, and GQ for upstream HQoS on an Ethernet interface. CQ, however, is pre-defined by the system and is not configurable. With downstream HQoS, you can configure all FQ, SQ, GQ, PQ, and CQ on an Ethernet interface.

It is recommended that you configure FQ, SQ, and GQ for upstream HQoS, and CQ for downstream HQoS on the Ethernet interface. CQ, however, is not mandatory for downstream HQoS.

10.2.1 Establishing the Configuration Task

Before configuring HQoS on an Ethernet interface, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

HQoS is mostly used on the user side of

- A PE device of a backbone network
- An access router of an access network.

In the case of multiple user access and multiple service access, HQoS can differentiate users (VLAN users or VPN users) in a network for priority scheduling and bandwidth guarantee. In addition, HQoS can also save the costs in network operation and maintenance.

To differentiate users and provide hierarchical QoS for them, HQoS divides a GE interface into multiple sub-interfaces. Each user occupies one GE sub-interface for service access. In this manner, the interface bandwidth can be better utilized. [Figure 10-5](#) provides a typical networking diagram for VLAN user access through sub-interfaces. [Figure 10-6](#) provides a typical networking diagram for VPN user access through sub-interfaces.

The procedures of configuring HQoS in the two environments are the same.

Figure 10-5 Typical networking diagram for VLAN user access through sub-interfaces

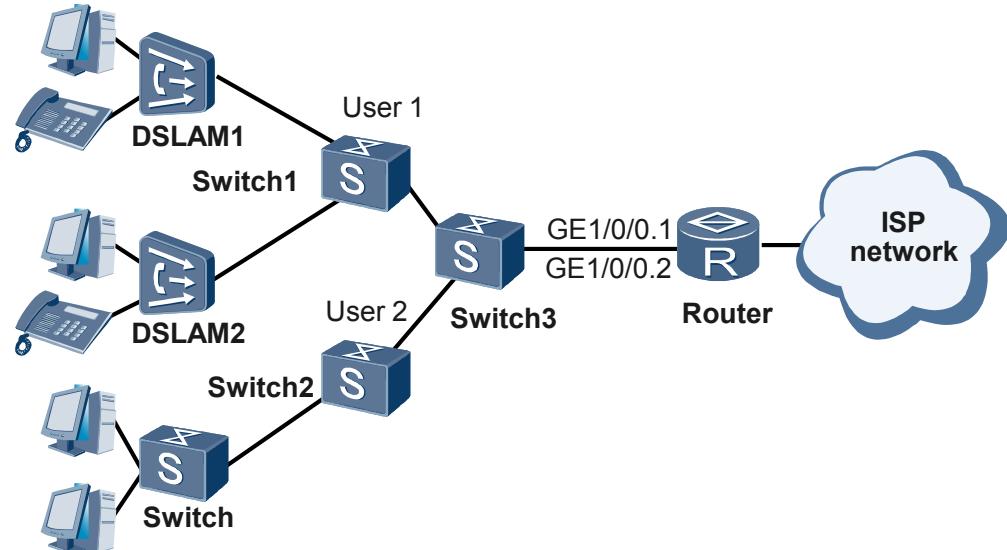
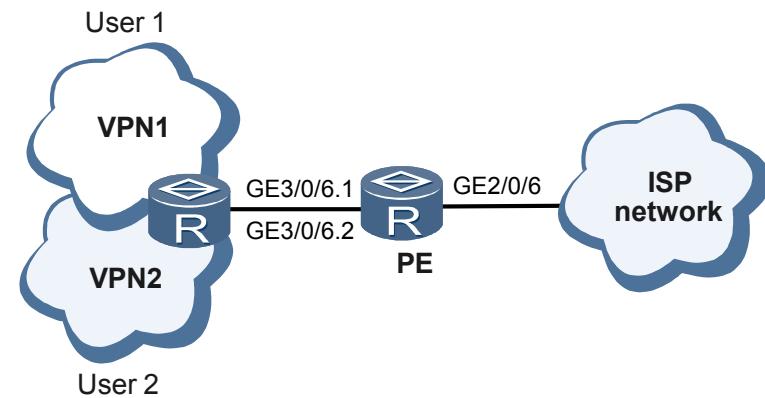


Figure 10-6 Typical networking diagram for VPN user access through sub-interfaces



Pre-configuration Tasks

Before configuring HQoS, complete the following tasks:

- Configuring IP addresses for the interfaces
- Configuring IP routing protocol on the routers and ensure that the link works normally
- Configuring simple traffic classification

 **NOTE**

Before you configure the HQoS function, it is recommended that you configure the simple traffic classification or complex traffic classification; otherwise, in FQ scheduling all traffic is considered BE by default.

Data Preparation

To configure HQoS, you need the following data.

No.	Data
1	VLAN IDs
2	(Optional) Parameters of flow-wred packet discarding
3	(Optional) Algorithms for flow-queue scheduling and related parameters
4	(Optional) Service class mappings for flow-mapping
5	(Optional) A value of user-group-queue shaping
6	Values of CIR, PIR, and network-header-length
7	(Optional) Parameters of port-wred referenced by port-queue scheduling
8	(Optional) Algorithms for port-queue scheduling and related parameters, and the shaping value

10.2.2 (Optional) Configuring an FQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a flow-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:

 NOTE

- When no flow-wred objects are set, the system adopts the default tail-drop policy.
- The high and low limit percentages for red packets can be set to the minimum; those for yellow packets can be greater; those for green packets can be set to the maximum.
- In the actual configuration, the low limit percentage of WRED is recommended to begin with 50% and be adjusted based on different colors of packets. 100% is recommended for the drop probability.

By configuring a flow-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a FQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a FQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a FQ is greater than the high limit percentage, the system drops all subsequent packets.

You can create multiple flow-wred objects for being referenced by FQs as required. You can configure up to 511 flow-wred objects in the system.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-wred flow-wred-name
```

The flow-wred is created and the flow-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage-value
```

The high and low limit percentages and the drop probability are set for different colors of packets.

Step 4 (Optional) Run:

```
queue-depth queue-depth-value
```

The depth is set for the FQs in the flow-wred objects to decrease the delay.

----End

10.2.3 (Optional) Configuring Scheduling Parameters of an FQ

You can define an FQ profile rather than adopt the default profile to configure WFQ scheduling weights, traffic shaping, the shaping rate, and the way of dropping packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-queue flow-queue-name
```

The FQ view is displayed.

Step 3 Run:

```
queue cos-value { { pq | wfq weight weight-value | lpq } | { shaping { shaping-value | shaping-percentage shaping-percentage-value } [ pbs pbs-value ] } | flow-wred wred-name } *
```

A queue scheduling policy for a class is set.



NOTE

You can configure scheduling parameters in one flow queue profile for the eight FQs of a subscriber respectively.

If you do not configure a flow queue, the system uses the default flow queue profile.

- By default, the system performs PQ scheduling on the FQs with the priorities of EF, CS6, and CS7.
- The system defaults the FQs with the priorities of BE, AF1, AF2, AF3, and AF4 to WFQ. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The default discarding policy is the tail drop.

----End

10.2.4 (Optional) Configuring a Mapping from an FQ to a CQ

You can define a mapping from an FQ to a CQ rather than adopt the default mapping to set the priority of a type of service in an SQ entering a CQ.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-mapping mapping-name
```

The flow mapping view is displayed.

Step 3 Run:

```
map flow-queue cos-value to port-queue cos-value
```

The priority mapping from a flow queue to a CQ is set.

 NOTE

You can configure eight mappings from flow queues to port queues in one flow queue mapping profile.
When no mapping from the flow queue to the CQ is set, the system defaults the one-to-one mapping.

Users can create multiple flow-mapping profiles for being referenced by SQs as required. You can configure up to 15 flow-mapping profiles in the system.

----End

10.2.5 (Optional) Configuring Scheduling Parameters for a GQ

The shaping rate can be set for a GQ to limit the volume of GQ traffic and prevent GQ traffic burst. In this case, traffic can be evenly sent.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`user-group-queue group-name`

The specified GQ view is displayed.

Step 3 Run:

`shaping shaping-value [pbs pbs-value] { inbound | outbound }`

The shaping value is set for the GQ.

 NOTE

When traffic shaping is not configured for the GQ, the system performs no traffic shaping by default.

Step 4 (Option) Run:

`mode template`

The GQ shares QoS resources according to the keyword **group** in the **qos-profile** (interface view) command.

 NOTE

The **mode template** command is valid only for interface-based HQoS.

After a GQ is created, the GQ applies for QoS resources only when the **user-queue** command is run in the interface view. If the **mode template** command is configured, GQs consume resources based on the keyword **group** of the **qos-profile** (interface view) command in the interface view; if the **mode template** command is not configured, GQs share the same QoS resources. Even though **group** is defined differently in multiple **qos-profile** (interface view) commands in the interface view, GQs share the same QoS resources.

For example, the **qos-profile test inbound group group1** command is configured on GE 1/0/0 and the **qos-profile test inbound group group2** command is configured on GE 1/0/1. If the **mode template** command is configured, GQs apply for two QoS resources; if the **mode template** command is not configured, GQs share the same QoS resources.

----End

10.2.6 Configuring Scheduling Parameters of an SQ

You can set the CIR, PIR, FQ profile, FQ mapping object, GQ name, name of the applied service profile, and the inbound or outbound direction.

Context

Do as follows on the upstream interface of the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number[ sub-interface-number ]
```

View of the specified interface is displayed.

Step 3 Run:

```
user-queue cir cir-value [ [ pir pir-value ] | [ flow-queue flow-queue-name ] | [ flow-mapping mapping-name ] | [ user-group-queue group-name ] ] *{ inbound | outbound } [ service-template service-template-name ]
```

Queue scheduling parameters are set for SQ and HQoS is enabled.



NOTE

To set the presion scheduling length for a service template run the command **network-header-length** in the service-template view.

----End

10.2.7 (Optional) Configuring a CQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a port-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
port-wred port-wred-name
```

A port-wred object is created, and the port-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-value high-limit high-limit-
value discard-percentage discard-percentage-value
```

The low limit percentage, high limit percentage, and drop probability are set.

 **NOTE**

When no port-wred objects are set, the system adopts the default wred.

By configuring a port-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a CQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a CQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a CQ is greater than the high limit percentage, the system drops all subsequent packets.

Users can create multiple port-wred objects for being referenced by CQs as required. The system provides one default port-wred object. You can configure a maximum of seven port-wred objects.

Step 4 (Option) Run:

```
queue-depth queue-depth-value
```

The depth is set for the CQs in the port-wred objects to decrease the delay.

----End

10.2.8 (Optional) Configuring Scheduling Parameters of a CQ

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system. To prevent congestion on the backbone network, you need to configure the downstream CQ on the Ethernet interface.

Context



CAUTION

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system and is not configured by users.

Configuring the downstream CQ on an Ethernet interface is recommended so that the backbone network is not congested.

Do as follows on the downstream interface of the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping { shaping-value | shaping-percentage shaping-percentage-value [ pbs pbs-value ] } } | port-wred wred-name } * outbound
```

A queue scheduling policy for different CQs is set.

 **NOTE**

You can configure eight CQ scheduling parameters respectively on one interface.

When no CQ is configured, the system adopts the default CQ profile.

- By default, the system performs PQ on the flow queues with the priorities of EF, CS6, and CS7.
- By default, the system performs WFQ on the flow queues with the priorities of BE, AF1, AF2, AF3, and AF4. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The discarding policy defaults to WRED drop.

----End

10.2.9 Checking the Configuration

After HQoS is configured on an Ethernet interface, you can view the configuration parameters of an FQ mapping object and the referential relations of the object, configuration parameters of a GQ and the referential relations, and statistics about the SQ, GQ, and CQ on specified interfaces.

Procedure

- Using the **display flow-mapping configuration** [**verbose** [*mapping-name*]] command to check the configured parameters of a flow queue mapping object and the referential relations of the object.
- Using the **display flow-queue configuration** [**verbose** [*flow-queue-name*]] command to check the configuration of a flow queue template.
- Using the **display flow-wred configuration** [**verbose** [*flow-wred-name*]] command to check the configured parameters of a flow queue WRED object.
- Using the **display user-queue configuration** **interface** *interface-type interface-number* [**inbound** | **outbound**] command to check the HQoS configuration on interfaces.
- Using the **display user-group-queue configuration** [**verbose** [*group-name*]] command to check the configuration of a GQ and the referential relations.
- Using the **display port-wred configuration** [**verbose** [*port-wred-name*]] command to check the configured parameters of a CQ WRED object.
- Using the **display port-queue configuration** **interface** *interface-type interface-number* **outbound** command to check the detailed configuration of a CQ.
- Using the **display user-queue statistics** **interface** *interface-type interface-number* { **inbound** | **outbound** } command to check the statistics of SQs on a specified interface.
- Using the **display user-group-queue** *group-name* **statistics** [**slot slot-id**] { **inbound** | **outbound** } command to check the statistics of a GQ.

- Using the **display port-queue statistics interface interface-type interface-number [cos-value] outbound** command to check the statistics of a CQ.

----End

Example

Running the **display user-queue statistics interface interface-type interface-number { inbound | outbound }** command, you can view the statistics of an SQ on a specified interface. The statistic information covers that of every service of an SQ. For example:

```
<HUAWEI> display user-queue statistics interface gigabitethernet 6/0/0 inbound
GigabitEthernet6/0/0 inbound traffic statistics:
[be]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af1]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af2]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af3]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af4]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[ef]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs6]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs7]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
```

```
Last 5 minutes discard rate:          0 pps,          0 bps
[total]
Pass:                                0 packets,        0 bytes
Discard:                             0 packets,        0 bytes
Last 5 minutes pass rate:           0 pps,
Last 5 minutes discard rate:        0 pps,          0 bps
```

Running the **display user-group-queue group-name statistics [slot slot-id] { inbound | outbound }** command, you can view the statistics of a GQ. For example:

```
<HUAWEI> display user-group-queue test statistics inbound
test inbound traffic statistics:
[slot 6]
  total:
    Pass:          855,444 packets,      88,193,994 bytes
    Discard:       22,815,639 packets,   2,467,264,575 bytes
[slot all]
  total:
    Pass:          855,444 packets,      88,193,994 bytes
    Discard:       22,815,639 packets,   2,467,264,575 bytes
```

Running the **display port-queue statistics interface interface-type interface-number [cos-value] outbound** command, you can view the statistics of a CQ. For example: Display the statistics of the AF1 queue on GE 2/0/1.

```
<HUAWEI> display port-queue statistics interface gigabitethernet 2/0/1 af1 outbound
[af1]
  Total pass:          27,697,521 packets,      2,006,796,750 bytes
  Total discard:        0 packets,          0 bytes
  --Drop tail discard: 0 packets,          0 bytes
  --Wred discard:       0 packets,          0 bytes
  Last 30 seconds pass rate: 0 pps,          0 bps
  Last 30 seconds discard rate: 0 pps,          0 bps
  --Drop tail discard rate: 0 pps,          0 bps
  --Wred discard rate:   0 pps,          0 bps
```

10.3 Configuring HQoS on a QinQ Termination Sub-interface

After HQoS is configured on a sub-interface for QinQ VLAN tag termination, packets from different VLANs can be differentiated when they enter the ISP network.

Context

For details of the QinQ principle and configuration, refer to "QinQ Configuration" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - LAN Access and MAN Access*.

10.3.1 Establishing the Configuration Task

Before configuring HQoS on a sub-interface for QinQ VLAN tag termination, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

The QinQ HQoS technology is mostly used on the user side of the edge PE in a backbone network.

When packets of multiple VLAN users, after users' two-layer tags being terminated on the QinQ termination sub-interface, enter the ISP network, the ISP network can identify only the service types of packets instead of users.

The HQoS function configured on a QinQ termination sub-interface enables the system to identify both services and users in the network when packets of multiple VLAN users enter the ISP network. After this, the system performs priority scheduling and provides bandwidth guarantee for services of high priority.

You need to configure HQoS features of a QinQ termination sub-interface in the vlan-group view of the QinQ termination sub-interface.

Pre-configuration Tasks

Before configuring HQoS, complete the following tasks:

- Configuring the physical parameters and link attributes to ensure normal operation of the interfaces
- Configuring IP addresses of the interfaces
- Configuring the IP routes on the router and keeping the link be connected
- Configuring simple traffic classification

 **NOTE**

Before you configure the HQoS function, it is recommended that you configure the simple traffic classification or complex traffic classification; otherwise, in FQ scheduling all traffic is considered BE by default.

Data Preparation

To configure HQoS on a QinQ termination sub-interface, you need the following data.

No.	Data
1	VLAN-group ID
2	QinQ termination sub-interface number
3	(Optional) Parameters of flow-wred
4	(Optional) Algorithms for flow-queue scheduling and related parameters
5	(Optional) Service class mappings for flow-mapping
6	(Optional) A value of user-group-queue shaping

No.	Data
7	Values of CIR, PIR, and network-header-length
8	(Optional) port-wred parameters of port-queue
9	(Optional) Algorithms for port-queue scheduling and related parameters and shaping values

10.3.2 (Optional) Configuring an FQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a flow-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:



- When no flow-wred objects are set, the system adopts the default tail-drop policy.
- The high and low limit percentages for red packets can be set to the minimum; those for yellow packets can be greater; those for green packets can be set to the maximum.
- In the actual configuration, the low limit percentage of WRED is recommended to begin with 50% and be adjusted based on different colors of packets. 100% is recommended for the drop probability.

By configuring a flow-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a FQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a FQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a FQ is greater than the high limit percentage, the system drops all subsequent packets.

You can create multiple flow-wred objects for being referenced by FQs as required. You can configure up to 511 flow-wred objects in the system.

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`flow-wred flow-wred-name`

The flow-wred is created and the flow-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-
percentage discard-percentage discard-percentage-value
```

The high and low limit percentages and the drop probability are set for different colors of packets.

Step 4 (Optional) Run:

```
queue-depth queue-depth-value
```

The depth is set for the FQs in the flow-wred objects to decrease the delay.

----End

10.3.3 (Optional) Configuring Scheduling Parameters of an FQ

You can define an FQ profile rather than adopt the default profile to configure WFQ scheduling weights, traffic shaping, the shaping rate, and the way of dropping packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-queue flow-queue-name
```

The FQ view is displayed.

Step 3 Run:

```
queue cos-value { { pq | wfq weight weight-value | lpq } | { shaping { shaping-
value | shaping-percentage shaping-percentage-value } [ pbs pbs-value ] } | flow-
wred wred-name } *
```

A queue scheduling policy for a class is set.

 **NOTE**

You can configure scheduling parameters in one flow queue profile for the eight FQs of a subscriber respectively.

If you do not configure a flow queue, the system uses the default flow queue profile.

- By default, the system performs PQ scheduling on the FQs with the priorities of EF, CS6, and CS7.
- The system defaults the FQs with the priorities of BE, AF1, AF2, AF3, and AF4 to WFQ. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The default discarding policy is the tail drop.

----End

10.3.4 (Optional) Configuring a Mapping from an FQ to a CQ

You can define a mapping from an FQ to a CQ rather than adopt the default mapping to set the priority of a type of service in an SQ entering a CQ.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-mapping mapping-name
```

The flow mapping view is displayed.

Step 3 Run:

```
map flow-queue cos-value to port-queue cos-value
```

The priority mapping from a flow queue to a CQ is set.



NOTE

You can configure eight mappings from flow queues to port queues in one flow queue mapping profile.

When no mapping from the flow queue to the CQ is set, the system defaults the one-to-one mapping.

Users can create multiple flow-mapping profiles for being referenced by SQs as required. You can configure up to 15 flow-mapping profiles in the system.

----End

10.3.5 (Optional) Configuring Scheduling Parameters for a GQ

The shaping rate can be set for a GQ to limit the volume of GQ traffic and prevent GQ traffic burst. In this case, traffic can be evenly sent.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-group-queue group-name
```

The specified GQ view is displayed.

Step 3 Run:

```
shaping shaping-value [ pbs pbs-value ] { inbound | outbound }
```

The shaping value is set for the GQ.

 **NOTE**

When traffic shaping is not configured for the GQ, the system performs no traffic shaping by default.

Step 4 (Option) Run:

```
mode template
```

The GQ shares QoS resources according to the keyword **group** in the **qos-profile** (interface view) command.

 **NOTE**

The **mode template** command is valid only for interface-based HQoS.

After a GQ is created, the GQ applies for QoS resources only when the **user-queue** command is run in the interface view. If the **mode template** command is configured, GQs consume resources based on the keyword **group** of the **qos-profile** (interface view) command in the interface view; if the **mode template** command is not configured, GQs share the same QoS resources. Even though **group** is defined differently in multiple **qos-profile** (interface view) commands in the interface view, GQs share the same QoS resources.

For example, the **qos-profile test inbound group group1** command is configured on GE 1/0/0 and the **qos-profile test inbound group group2** command is configured on GE 1/0/1. If the **mode template** command is configured, GQs apply for two QoS resources; if the **mode template** command is not configured, GQs share the same QoS resources.

----End

10.3.6 Enabling QinQ on an Interface

Before configuring HQoS on a sub-interface for QinQ VLAN tag termination, you need to configure user termination and QinQ on the main interface.

Context

Do as follows on the upstream interface of the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the specified interface is displayed.

Step 3 Run:

```
mode user-termination
```

The interface is set to work in user termination mode and QinQ is enabled on the master interface.

----End

10.3.7 Configuring QinQ on a Sub-interface

This section describes how to create a QinQ sub-interface and configure the sub-interface to terminate double-tagged packets.

Context

Do as follows on the QinQ sub-interface of the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number.sub-interface
```

A QinQ sub-interface is created and the QinQ sub-interface view is displayed.

Step 3 Run:

```
control-vid vid qinq-termination
```

The VLAN encapsulation mode is set to QinQ.

Step 4 Run:

```
qinq termination pe-vid pe-vid ce-vid low-ce-vid [ to high-ce-vid ] [ vlan-group group-id ]
```

The QinQ sub-interface termination is configured.

Step 5 Run:

```
quit
```

Exit from the QinQ sub-interface view.

----End

10.3.8 Configuring a VLAN Group

This section describes how to create a VLAN group and apply different QoS policies to different user groups.

Context

Do as follows on the master QinQ interface of the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number.sub-interface
```

The view of the specified QinQ sub-interface is displayed.

Step 3 Run:

```
vlan-group vlan-group-id
```

A VLAN group is created and the view of the VLAN group is displayed.

Step 4 Run:

`quit`

Exit from the VLAN group view.

----End

10.3.9 Configuring Scheduling Parameters of an SQ

You can set the CIR, PIR, FQ profile, FQ mapping object, GQ name, name of the applied service profile, and the inbound or outbound direction for a VLAN group.

Context

Do as follows on the vlan-group view of the QinQ sub-interface of the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface interface-type interface-number[sub-interface-number]`

View of the specified sub-interface is displayed.

Step 3 Run:

`vlan-group vlan-group-id`

The view of the specified VLAN group is displayed.

Step 4 Run:

`user-queue cir cir-value [[pir pir-value] | [flow-queue flow-queue-name] | [flow-mapping mapping-name] | [user-group-queue group-name]] *{ inbound | outbound }[service-template service-template-name]`

The parameters of the SQ scheduling are set and HQoS is enabled on the sub-interface.



To set the presion scheduling length for a service template run the command `network-header-length` in the service-template view.

----End

10.3.10 (Optional) Configuring a CQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a port-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
port-wred port-wred-name
```

A port-wred object is created, and the port-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-value high-limit high-limit-value discard-percentage discard-percentage-value
```

The low limit percentage, high limit percentage, and drop probability are set.



NOTE

When no port-wred objects are set, the system adopts the default wred.

By configuring a port-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a CQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a CQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a CQ is greater than the high limit percentage, the system drops all subsequent packets.

Users can create multiple port-wred objects for being referenced by CQs as required. The system provides one default port-wred object. You can configure a maximum of seven port-wred objects.

Step 4 (Option) Run:

```
queue-depth queue-depth-value
```

The depth is set for the CQs in the port-wred objects to decrease the delay.

----End

10.3.11 (Optional) Configuring Scheduling Parameters of a CQ

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system. To prevent congestion on the backbone network, you need to configure the downstream CQ on the Ethernet interface.

Context



CAUTION

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system and is not configured by users.

Configuring the downstream CQ on an Ethernet interface is recommended so that the backbone network is not congested.

Do as follows on the downstream interface of the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`interface interface-type interface-number`

The interface view is displayed.

Step 3 Run:

`port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping { shaping-value | shaping-percentage shaping-percentage-value [pbs pbs-value] } } | port-wred wred-name } * outbound`

A queue scheduling policy for different CQs is set.



NOTE

You can configure eight CQ scheduling parameters respectively on one interface.

When no CQ is configured, the system adopts the default CQ profile.

- By default, the system performs PQ on the flow queues with the priorities of EF, CS6, and CS7.
- By default, the system performs WFQ on the flow queues with the priorities of BE, AF1, AF2, AF3, and AF4. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The discarding policy defaults to WRED drop.

----End

10.3.12 Checking the Configuration

After HQoS is configured on a sub-interface for QinQ VLAN tag termination, you can view the configuration parameters of an FQ mapping object and the referential relations of the object, configuration parameters of a GQ and the referential relations, and statistics about the SQ, GQ, and CQ on specified interfaces.

Procedure

- Using the **display flow-mapping configuration [verbose [mapping-name]]** command to check the configured parameters of an FQ mapping object and the referential relations of the object.
- Using the **display flow-queue configuration [verbose [flow-queue-name]]** command to check the configuration of an FQ template.
- Using the **display flow-wred configuration [verbose [flow-wred-name]]** command to check the configured parameters of an FQ WRED object.
- Using the **display user-group-queue configuration [verbose [group-name]]** command to check the configuration of a GQ and the referential relations.
- Using the **display statistic user-queue qinq-termination interface interface-type interface-number pe-vid pe-vid ce-vid ce-vid { inbound | outbound }** command to check the SQ statistics on a specified interface.
- Using the **display user-group-queue group-name statistics [slot slot-id] { inbound | outbound }** command to check the statistics of a GQ.

----End

10.4 Configuring Class-based HQoS

Class-based HQoS classifies users in the case of a limited number of interfaces and performs hierarchical scheduling for traffic from different users.

10.4.1 Establishing the Configuration Task

Before configuring class-based QoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

HQoS is mostly used on the user side of:

- A PE on a backbone network
- An access router on an access network

In the case of multiple user access and multiple service access, HQoS can differentiate users (VLAN users) in a network for priority scheduling and bandwidth guarantee. In addition, HQoS can also save the costs in network operation and maintenance.

To further divide users on a small number of interfaces and perform hierarchical scheduling over traffic of multiple users, you need to deploy class-based HQoS. Class-based HQoS integrates the classification function of the CTC and the queue scheduling function of HQoS. The system first classifies traffic that needs HQoS scheduling through the CTC. Then, it configures HQoS parameters by taking all the packets that match a classifying rule as one user.

Pre-configuration Tasks

Before configuring class-based HQoS, complete the following tasks:

- Configuring physical parameters and link attributes to ensure normal operation of the interfaces
- Configuring IP addresses for interfaces
- Configuring IP routes on routers to ensure normal operation of the link
- Configuring simple traffic classification

Data Preparation

To configure class-based HQoS, you need the following data.

No.	Data
1	Matching rule, names of the traffic classifier, traffic behavior, traffic policy, and the interface where the traffic policy is applied
2	(Optional) Parameters for packet drop in flow-wred
3	(Optional) Scheduling algorithms and related parameters in flow-queue
4	(Optional) CoS relationships in flow-mapping
5	(Optional) Shaping value in user-group-queue
6	CIR, PIR, and network-header-length of user-queue
7	(Optional) Port-wred parameters used in port-queue
8	(Optional) Scheduling algorithms, related parameters, and shaping values in port-queue

10.4.2 Defining a Traffic Classifier

Before configuring class-based QoS, you need to define a traffic classifier.

Context



NOTE

In configuration of class-based HQoS, the purpose of defining a traffic classifier is to single out the packets through the CTC for further HQoS scheduling.

Do as follows on the router to configure class-based HQoS:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`traffic classifier classifier-name [operator { and | or }]`

A traffic classifier is defined, and the traffic classifier view is displayed.

Step 3 Run the following command as required to define a traffic policy.

- To define an ACL rule, run the **if-match acl *acl-number*** command.
- To define a DSCP rule, run the **if-match dscp *dscp-value*** command.
- To define a TCP flag rule, run the **if-match tcp syn-flag *tcpflag-value*** command.
- To define a matching rule based on the IP precedence, run the **if-match ip-precedence *ip-precedence*** command.
- To define a rule for matching all packets, run the **if-match any** command.
- To define a rule for matching VLAN packets based on the 802.1p priority, run the **if-match 8021p *8021p-value*** command.
- To define a rule for matching packets based on the source MAC address, run the **if-match source-mac *mac-address*** command.
- To define a rule for matching packets based on the destination MAC address, run the **if-match destination-mac *mac-address*** command.
- To define a rule for matching packets based on the MPLS EXP value, run the **if-match mpls-exp *exp-value*** command.

If multiple matching rules are configured for one traffic classifier, you can set the relationship among the matching rules by specifying the parameter **operator** in Step 2 with the command **traffic classifier *classifier-name* [**operator** { **and** | **or** }]**, where,

- **and**: is an operator indicating that the matching rules are in the logical **AND** relationship. This means that the packets are of the specified class only when all rules are matched.
- **or**: is an operator indicating that the matching rules are in the logical **OR** relationship. This means that the packets are of the specified class when any of the rules is matched.

If the parameter **operator** is not specified, the default relationship among matching rules is logical **OR**.

----End

10.4.3 (Optional) Configuring an FQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a flow-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:



NOTE

- When no flow-wred objects are set, the system adopts the default tail-drop policy.
- The high and low limit percentages for red packets can be set to the minimum; those for yellow packets can be greater; those for green packets can be set to the maximum.
- In the actual configuration, the low limit percentage of WRED is recommended to begin with 50% and be adjusted based on different colors of packets. 100% is recommended for the drop probability.

By configuring a flow-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a FQ is less than the low limit percentage, the system does not drop packets.

- When the percentage of the actual length of a queue over the length of a FQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a FQ is greater than the high limit percentage, the system drops all subsequent packets.

You can create multiple flow-wred objects for being referenced by FQs as required. You can configure up to 511 flow-wred objects in the system.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-wred flow-wred-name
```

The flow-wred is created and the flow-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage-value
```

The high and low limit percentages and the drop probability are set for different colors of packets.

Step 4 (Optional) Run:

```
queue-depth queue-depth-value
```

The depth is set for the FQs in the flow-wred objects to decrease the delay.

----End

10.4.4 (Optional) Configuring Scheduling Parameters of an FQ

You can define an FQ profile rather than adopt the default profile to configure WFQ scheduling weights, traffic shaping, the shaping rate, and the way of dropping packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-queue flow-queue-name
```

The FQ view is displayed.

Step 3 Run:

```
queue cos-value { { pq | wfq weight weight-value | lpq } | { shaping { shaping-  
value | shaping-percentage shaping-percentage-value } [ pbs pbs-value ] } | flow-  
wred wred-name } *
```

A queue scheduling policy for a class is set.

 **NOTE**

You can configure scheduling parameters in one flow queue profile for the eight FQs of a subscriber respectively.

If you do not configure a flow queue, the system uses the default flow queue profile.

- By default, the system performs PQ scheduling on the FQs with the priorities of EF, CS6, and CS7.
- The system defaults the FQs with the priorities of BE, AF1, AF2, AF3, and AF4 to WFQ. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The default discarding policy is the tail drop.

----End

10.4.5 (Optional) Configuring a Mapping from an FQ to a CQ

You can define a mapping from an FQ to a CQ rather than adopt the default mapping to set the priority of a type of service in an SQ entering a CQ.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-mapping mapping-name
```

The flow mapping view is displayed.

Step 3 Run:

```
map flow-queue cos-value to port-queue cos-value
```

The priority mapping from a flow queue to a CQ is set.

 **NOTE**

You can configure eight mappings from flow queues to port queues in one flow queue mapping profile.

When no mapping from the flow queue to the CQ is set, the system defaults the one-to-one mapping.

Users can create multiple flow-mapping profiles for being referenced by SQs as required. You can configure up to 15 flow-mapping profiles in the system.

----End

10.4.6 (Optional) Configuring Scheduling Parameters for a GQ

The shaping rate can be set for a GQ to limit the volume of GQ traffic and prevent GQ traffic burst. In this case, traffic can be evenly sent.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-group-queue group-name
```

The specified GQ view is displayed.

Step 3 Run:

```
shaping shaping-value [ pbs pbs-value ] { inbound | outbound }
```

The shaping value is set for the GQ.



NOTE

When traffic shaping is not configured for the GQ, the system performs no traffic shaping by default.

Step 4 (Option) Run:

```
mode template
```

The GQ shares QoS resources according to the keyword **group** in the **qos-profile** (interface view) command.



NOTE

The **mode template** command is valid only for interface-based HQoS.

After a GQ is created, the GQ applies for QoS resources only when the **user-queue** command is run in the interface view. If the **mode template** command is configured, GQs consume resources based on the keyword **group** of the **qos-profile** (interface view) command in the interface view; if the **mode template** command is not configured, GQs share the same QoS resources. Even though **group** is defined differently in multiple **qos-profile** (interface view) commands in the interface view, GQs share the same QoS resources.

For example, the **qos-profile test inbound group group1** command is configured on GE 1/0/0 and the **qos-profile test inbound group group2** command is configured on GE 1/0/1. If the **mode template** command is configured, GQs apply for two QoS resources; if the **mode template** command is not configured, GQs share the same QoS resources.

----End

10.4.7 Defining a Traffic Behavior and Configuring Scheduling Parameters for a Subscriber Queue

You can set the high threshold percentage, low threshold percentage, and drop probability for an SQ. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router to configure class-based HQoS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic behavior behavior-name
```

A traffic behavior is defined, and the traffic behavior view is displayed.

Step 3 Run:

```
user-queue cir cir-value [ [ pir pir-value ] | [ flow-queue flow-queue-name ] | [ flow-mapping mapping-name ] | [ user-group-queue group-name ] | [ service-template service-template-name ] ]*
```

The scheduling parameters of a subscriber queue are configured, and HQoS is enabled on the interface.



NOTE

To set the precision scheduling length for a service profile, run the **network-header-length** command in the service-template view.

----End

10.4.8 Defining a Traffic Policy and Applying It to an Interface

After defining traffic classifiers and traffic behaviors, you need to configure traffic policies by associating traffic classifiers with traffic behaviors, and then apply traffic policies to interfaces.

Context

Do as follows on the router to configure class-based HQoS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
traffic policy policy-name
```

A traffic policy is defined, and the policy view is displayed.

Step 3 Run:

```
classifier classifier-name behavior behavior-name
```

A traffic behavior is associated with a specified traffic classifier in the traffic policy.

Step 4 Run:

```
quit
```

The device returns to the system view.

Step 5 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 6 Run:

```
traffic-policy policy-name inbound
```

The traffic policy is applied to the interface.

----End

10.4.9 (Optional) Configuring a WRED Object for a Class Queue

You can set the high threshold percentage, low threshold percentage, and drop probability for a port-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router to configure class-based HQoS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
port-wred port-wred-name
```

A port-wred object is created, and the port-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-value high-limit high-limit-value discard-percentage discard-percentage-value
```

The upper limit (in percentage), lower limit (in percentage), and drop probability are set for different colors of packets.



NOTE

If you do not configure a WRED object for a CQ (that is, a port-wred object), the system uses the default tail-drop policy.

----End

10.4.10 (Optional) Configuring Scheduling Parameters for a Class Queue

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system. To prevent congestion on the backbone network, you need to configure the downstream CQ on the Ethernet interface.

Context



CAUTION

In the HQoS scheduling for upstream HQoS on an Ethernet interface, CQs adopt the default scheduling setting of the system and requires no configuration.

Configuring the downstream CQ on an Ethernet interface is recommended so that the backbone network is not congested.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping { shaping-value | shaping-percentage shaping-percentage-value } | port-wred wred-name } *  
outbound
```

A scheduling policy is set for queues of different priorities.

NOTE

You can configure scheduling parameters for eight CQs on one interface.

If you do not configure a CQ, the system uses the default CQ profile.

- By default, the system performs PQ on the FQs with the priorities of EF, CS6, and CS7.
- WFQ is the default tool of the system for scheduling the FQs with the priorities of BE, AF1, AF2, AF3, and AF4. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system does not perform traffic shaping.
- The default discarding policy is the tail-drop policy.

----End

10.4.11 Checking the Configuration

After class-based HQoS is configured, you can view the configuration parameters of an FQ mapping object and the referential relationships of the object and configurations and statistics about a CQ.

Procedure

- Run the **display flow-mapping configuration [verbose [mapping-name]]** command to check the configured parameters of a flow-mapping object and the referential relationships of the object.

- Run the **display flow-queue configuration [verbose [flow-queue-name]]** command to check the configuration of an FQ profile.
- Run the **display flow-wred configuration [verbose [flow-wred-name]]** command to check the configured parameters of a flow-wred object.
- Run the **display user-group-queue configuration [verbose [group-name]]** command to check the configuration of a GQ and the referential relationships.
- Run the **display port-wred configuration [verbose [port-wred-name]]** command to check the configured parameters of the WRED object for a CQ.
- Run the **display port-queue configuration interface interface-type interface-number outbound** command to check the detailed configurations of a CQ.
- Run the **display user-group-queue statistics group-name [slot slot-id] { inbound | outbound }** command to check the statistics on a GQ.
- Run the **display port-queue statistics interface interface-type interface-number [cos-value] outbound** command to check the statistics on a CQ.
- Run the **display traffic policy { system-defined | user-defined } [policy-name [classifier classifier-name]]** command to check the classifier and behavior in the traffic policy.
- Run the **display traffic behavior user-defined behavior-name** command to check the configurations of a traffic behavior.
- Run the **display traffic classifier user-defined classifier-name** command to check the configurations of a traffic classifier.

----End

10.5 Configuring Profile-based HQoS

Profile-based HQoS places traffic from multiple interfaces into an SQ for scheduling. It implements uniform scheduling for traffic on multiple interfaces by defining QoS profiles and applying the profiles to different interfaces.

Context



Only the LPUF-20/21, LPUF-40, LPUF-10 and LPUG support SQs.

Only the LPWA , LPUF-10 support traffic suppression in both inbound and outbound directions.

The LPUF-20/21 and LPUF-40 support traffic suppression in inbound direction on all interfaces and traffic suppression in outbound direction on all interfaces except QinQ interfaces.

10.5.1 Establishing the Configuration Task

Before configuring profile-based HQoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To achieve uniform scheduling of incoming traffic flows on multiple interfaces, you need to implement traffic management by user levels. Interface-based HQoS only supports classifying traffic flows on one interface into an SQ for scheduling. It does not support uniform scheduling

of traffic flows on multiple interfaces. Profile-based HQoS, by comparison, supports classifying traffic flows on multiple interfaces into an SQ for scheduling. It implements uniform scheduling of traffic flows on multiple interfaces by defining QoS scheduling profiles and applying the profiles to different interfaces. The profile-based HQoS technique is used mainly on the access devices deployed at the edge of a MAN.

The difference between the complex traffic classification-based traffic policy and the profile-based HQoS is as follows:

The traffic policy based on complex traffic classification identifies the quintuple information of packets and performs traffic policing, traffic shaping, traffic statistics, and information modification for packets in a certain direction. In this manner, the direction of the traffic and the bandwidth consumed by the traffic are controlled. The configuration of queue scheduling is not involved. Traffic policing identifies and matches the quintuple information of packets to restrict the volume of the incoming traffic within a reasonable range and discard the excess traffic. In this manner, the network resources and the interests of carriers can be protected. Traffic policing is unaware of users and service priorities. This method is applicable to the case where traffic in only one direction is to be restricted.

Profile-based HQoS adjusts the scheduling policy and traffic control of various services in different queues and at different scheduling levels by configuring a QoS profile to control the bandwidth and priorities of packets from different users and interfaces. This method is applicable to the case where differentiated services are required by users.

The differences between the traffic policy and QoS profile are as follows:

Compared Item	Traffic Policy	QoS Profile
Identification of packets	In-depth identification of the quintuple information of packets, such as the source/destination MAC address, source/destination IP address, user group number, protocol type, and TCP/UDP port number of the application program.	Identification of users and packet types.
Action taken on the packets	Various actions, including packet filtering, traffic policing, re-marking of packet priorities, re-marking of packet types, setting forwarding actions, and load balancing.	Traffic policing, traffic shaping, and queue scheduling.
Traffic control	There is no cache; the excess packets are discarded; traffic scheduling is implemented in a uniform manner.	Packets in different queues are hierarchically scheduled and then cached. Traffic is scheduled and restricted in a more granular manner.
Applied object	Traffic that is in the same direction and shares the same quintuple information.	Traffic that is sent by different users and belongs to different services.

Compared Item	Traffic Policy	QoS Profile
Applied interface	This function is configured on the inbound interface.	This function can be configured on both upstream and downstream interfaces and is mostly configured on the outbound interface.
Association with packet suppression	Traffic policing and packet suppression cannot be configured on an inbound interface at the same time.	Traffic policing and packet suppression can be configured at the same time through the configuration of the QoS profile.

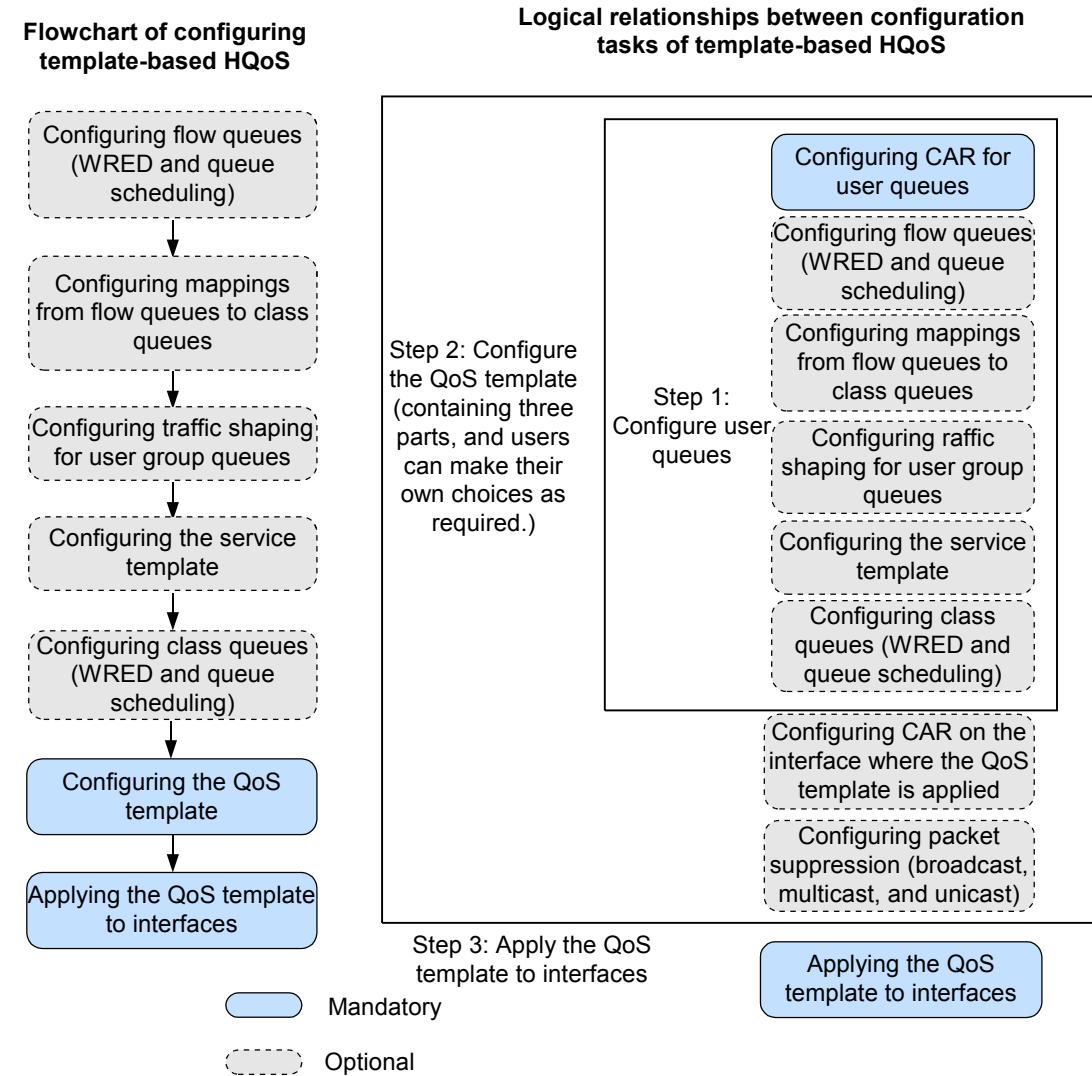
Pre-configuration Tasks

Before configuring profile-based HQoS, complete the following tasks:

- Configuring the physical parameters and link attributes of interfaces for them to work properly
- Assigning IP addresses to interfaces
- Configuring IP routes on the router to make devices on the link reachable

Configuration Procedures

Figure 10-7 Flowchart of configuring the profile-based HQoS



Data Preparation

To configure profile-based HQoS, you need the following data.

No.	Data
1	(Optional) Parameters for packet drop in flow-wred
2	(Optional) Scheduling algorithms and related parameters in flow-queue
3	(Optional) CoS relationships in flow-mapping
4	(Optional) Shaping value in user-group-queue

No.	Data
5	QoS profile names
6	<ul style="list-style-type: none"> ● Values of CIR, PIR, and network-header-length in the user-queue command ● CIR, PIR, CBS, and PBS of the car command
7	Interfaces, VLAN ID, PE VLAN ID, and CE VLAN ID to which the QoS profile is applied
8	(Optional) Port-wred parameters used in port-queue
9	(Optional) Scheduling algorithms, relevant parameters, and shaping values in port-queue

10.5.2 (Optional) Configuring an FQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a flow-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:



NOTE

- When no flow-wred objects are set, the system adopts the default tail-drop policy.
- The high and low limit percentages for red packets can be set to the minimum; those for yellow packets can be greater; those for green packets can be set to the maximum.
- In the actual configuration, the low limit percentage of WRED is recommended to begin with 50% and be adjusted based on different colors of packets. 100% is recommended for the drop probability.

By configuring a flow-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a FQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a FQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a FQ is greater than the high limit percentage, the system drops all subsequent packets.

You can create multiple flow-wred objects for being referenced by FQs as required. You can configure up to 511 flow-wred objects in the system.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

```
flow-wred flow-wred-name
```

The flow-wred is created and the flow-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage-value
```

The high and low limit percentages and the drop probability are set for different colors of packets.

Step 4 (Optional) Run:

```
queue-depth queue-depth-value
```

The depth is set for the FQs in the flow-wred objects to decrease the delay.

----End

10.5.3 (Optional) Configuring Scheduling Parameters of an FQ

You can define an FQ profile rather than adopt the default profile to configure WFQ scheduling weights, traffic shaping, the shaping rate, and the way of dropping packets.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-queue flow-queue-name
```

The FQ view is displayed.

Step 3 Run:

```
queue cos-value { { pq | wfq weight weight-value | lpq } | { shaping { shaping-value | shaping-percentage shaping-percentage-value } [ pbs pbs-value ] } | flow-wred wred-name } *
```

A queue scheduling policy for a class is set.



You can configure scheduling parameters in one flow queue profile for the eight FQs of a subscriber respectively.

If you do not configure a flow queue, the system uses the default flow queue profile.

- By default, the system performs PQ scheduling on the FQs with the priorities of EF, CS6, and CS7.
- The system defaults the FQs with the priorities of BE, AF1, AF2, AF3, and AF4 to WFQ. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The default discarding policy is the tail drop.

----End

10.5.4 (Optional) Configuring a Mapping from an FQ to a CQ

You can define a mapping from an FQ to a CQ rather than adopt the default mapping to set the priority of a type of service in an SQ entering a CQ.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
flow-mapping mapping-name
```

The flow mapping view is displayed.

Step 3 Run:

```
map flow-queue cos-value to port-queue cos-value
```

The priority mapping from a flow queue to a CQ is set.



NOTE

You can configure eight mappings from flow queues to port queues in one flow queue mapping profile.

When no mapping from the flow queue to the CQ is set, the system defaults the one-to-one mapping.

Users can create multiple flow-mapping profiles for being referenced by SQs as required. You can configure up to 15 flow-mapping profiles in the system.

----End

10.5.5 (Optional) Configuring Scheduling Parameters for a GQ

The shaping rate can be set for a GQ to limit the volume of GQ traffic and prevent GQ traffic burst. In this case, traffic can be evenly sent.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-group-queue group-name
```

The specified GQ view is displayed.

Step 3 Run:

```
shaping shaping-value [ pbs pbs-value ] { inbound | outbound }
```

The shaping value is set for the GQ.

 **NOTE**

When traffic shaping is not configured for the GQ, the system performs no traffic shaping by default.

Step 4 (Option) Run:

```
mode template
```

The GQ shares QoS resources according to the keyword **group** in the **qos-profile** (interface view) command.

 **NOTE**

The **mode template** command is valid only for interface-based HQoS.

After a GQ is created, the GQ applies for QoS resources only when the **user-queue** command is run in the interface view. If the **mode template** command is configured, GQs consume resources based on the keyword **group** of the **qos-profile** (interface view) command in the interface view; if the **mode template** command is not configured, GQs share the same QoS resources. Even though **group** is defined differently in multiple **qos-profile** (interface view) commands in the interface view, GQs share the same QoS resources.

For example, the **qos-profile test inbound group group1** command is configured on GE 1/0/0 and the **qos-profile test inbound group group2** command is configured on GE 1/0/1. If the **mode template** command is configured, GQs apply for two QoS resources; if the **mode template** command is not configured, GQs share the same QoS resources.

----End

10.5.6 (Optional) Configuring a Service Profile and Applying It to an Interface

Applying a service profile to an interface and configuring packet loss compensation achieve precise flow control by compensating a processed packet with a certain length.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
service-template service-template-name [ slot slot-id ]
```

The service profile view is displayed.

Step 3 Run:

```
network-header-length network-header-length { inbound | outbound }
```

The packet loss compensation length of the service profile is specified.

 **NOTE**

After packets enter the device, there is a difference between the length of a processed packet and the original packet. Packet loss compensation is a method to achieve precise traffic control by compensating a processed packet with a certain length.

Step 4 Run:

`quit`

The system view is displayed.

Step 5 Run:

`interface interface-type interface-number`

The interface view is displayed.

Step 6 Run:

`shaping service-template service-template-name`

The service profile is applied to the interface.

 **NOTE**

By default, the system has 14 service profiles. You can select the service profile as required.

----End

10.5.7 Defining a QoS Profile and Configuring Scheduling Parameters

A QoS profile is the aggregate of QoS scheduling parameters. Configurable scheduling parameters for SQs include the CIR, PIR, FQ profiles, and lengths for packet loss compensation of service profiles.

Context

Do as follows to configure HQoS on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`qos-profile qos-profile-name`

A QoS profile is defined, and its view is displayed.

Step 3 You can choose to configure user queue scheduling parameters or traffic assurance for users based on actual needs.

- To configure user queue scheduling parameters to implement HQoS for user services, run:

`user-queue cir cir-value [pir pir-value] [flow-queue flow-queue-name] [flow-mapping flow-mapping-name] [user-group-queue user-group-queue name] [service-template service-template-name] [inbound | outbound]`

- To configure a committed access rate (CAR) for users, run:

`car { cir cir-value [pir pir-value] } [cbs cbs-value pbs pbs-value] [green { discard | pass [service-class class color color] } | yellow { discard |`

```
pass [ service-class class color color ] } | red { discard | pass [ service-class class color color ] } ]* [ inbound | outbound ]
```

- To limit the rate of broadcast packets in the QoS profile, run:

```
broadcast-suppression cir cir-value [ cbs cbs-value ][ inbound | outbound ]
```

- To limit the rate of multicast packets in the QoS profile, run:

```
multicast-suppression cir cir-value [ cbs cbs-value ][ inbound | outbound ]
```

- To limit the rate of unknown unicast packets in the QoS profile, run:

```
unknown-unicast-suppression cir cir-value [ cbs cbs-value ][ inbound | outbound ]
```

NOTE

- In addition, if you configure the **qos-profile** command on an interface, you cannot configure the **user-queue** command, or the **car** command, or the traffic suppression function for the same direction on the interface.
- Only a global service profile can be applied in profile-based HQoS.

----End

10.5.8 Applying a QoS Profile

Different QoS profiles can be defined and then applied to different interfaces to perform QoS scheduling for user traffic.

Context

Do as follows to configure HQoS on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number [ .sub-interface ]
```

The interface view is displayed.

Step 3 (Optional) Run:

```
qos committed-bandwidth check outbound enable
```

Check on the total bandwidth of SQs is enabled.

Step 4 Choose the matched command line to apply QoS profiles on different types of interfaces.

- To apply the QoS profile on the GE interface, Eth-Trunk interface, Ethernet sub-interface, GE sub-interface, and Eth-Trunk sub-interface, run:

```
qos-profile qos-profile-name { inbound | outbound } [ identifier none | option82 ] [ group group-name ]
```

- To apply the QoS profile on the Layer 2 GE interface, Layer 2 Eth-Trunk interface, and dot1q termination sub-interface, run:

```
qos-profile qos-profile-name { inbound | outbound } vlan vlan-id1 [to vlan-id2] identifier { vlan-id | none | option82 } [ group group-name ]
```

- To apply the QoS profile on the QinQ termination sub-interface and QinQ mapping interface, run:

```
qos-profile qos-profile-name { inbound | outbound } pe-vid pe-vlan-id ce-vid ce-vlan-id1 [to ce-vlan-id2] identifier { pe-vid | ce-vid | pe-ce-vid | none | option82 } [ group group-name ]
```

----End

10.5.9 (Optional) Configuring a CQ WRED Object

You can set the high threshold percentage, low threshold percentage, and drop probability for a port-wred object. In this case, when the queue length exceeds the threshold, the device randomly discards packets by using the WRED mechanism.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
port-wred port-wred-name
```

A port-wred object is created, and the port-wred view is displayed.

Step 3 Run:

```
color { green | yellow | red } low-limit low-limit-value high-limit high-limit-value discard-percentage discard-percentage-value
```

The low limit percentage, high limit percentage, and drop probability are set.



NOTE

When no port-wred objects are set, the system adopts the default wred.

By configuring a port-wred object, users can set the high limit percentage, low limit percentage, and drop probability for queues.

- When the percentage of the actual length of a queue over the length of a CQ is less than the low limit percentage, the system does not drop packets.
- When the percentage of the actual length of a queue over the length of a CQ is between the low limit percentage and the high limit percentage, the system drops packets through the WRED mechanism. The longer the queue length, the higher the drop probability.
- When the percentage of the actual length of a queue over the length of a CQ is greater than the high limit percentage, the system drops all subsequent packets.

Users can create multiple port-wred objects for being referenced by CQs as required. The system provides one default port-wred object. You can configure a maximum of seven port-wred objects.

Step 4 (Option) Run:

```
queue-depth queue-depth-value
```

The depth is set for the CQs in the port-wred objects to decrease the delay.

----End

10.5.10 (Optional) Configuring Scheduling Parameters of a CQ

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system. To prevent congestion on the backbone network, you need to configure the downstream CQ on the Ethernet interface.

Context



CAUTION

In upstream HQoS scheduling on an Ethernet interface, CQs adopt the default scheduling setting of the system and is not configured by users.

Configuring the downstream CQ on an Ethernet interface is recommended so that the backbone network is not congested.

Do as follows on the downstream interface of the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-queue cos-value { { pq | wfq weight weight-value | lpq } | shaping { shaping-value | shaping-percentage shaping-percentage-value [ pbs pbs-value ] } | port-wred wred-name } * outbound
```

A queue scheduling policy for different CQs is set.



You can configure eight CQ scheduling parameters respectively on one interface.

When no CQ is configured, the system adopts the default CQ profile.

- By default, the system performs PQ on the flow queues with the priorities of EF, CS6, and CS7.
- By default, the system performs WFQ on the flow queues with the priorities of BE, AF1, AF2, AF3, and AF4. The scheduling weight proportion is 10:10:10:15:15.
- By default, the system performs no traffic shaping.
- The discarding policy defaults to WRED drop.

----End

10.5.11 Checking the Configuration

After profile-based HQoS is configured on an ATM interface, you can view information about queues and packet statistics on the ATM interface.

Procedure

- Run the **display flow-mapping configuration [verbose [mapping-name]]** command to check the configurations of an FQ mapping object and the referential relationships of the object.
- Using the **display flow-queue configuration [verbose [flow-queue-name]]** command to check the configurations of the flow queue template.
- Run the **display flow-wred configuration [verbose [flow-wred-name]]** command to check the configurations of a flow queue's WRED object.
- Run the **display user-group-queue configuration [verbose [group-name]]** command to check the configurations of a user group queue and its referential relationships.
- Run the **display port-wred configuration [verbose [port-wred-name]]** command to check the configurations of a class queue's WRED object.
- Run the **display port-queue configuration interface interface-type interface-number outbound** command to check the configurations of a class queue.
- Run the **display qos-profile configuration [profile-name]** command to check the configurations of a QoS profile.
- Run the **display qos-profile application profile-name** command to check the applications of a QoS profile.
- Run the **display qos-profile statistics interface interface-type interface-number [[vlan vlan-id] | [pe-vid pe-vid ce-vid ce-vid]] { inbound | outbound }** command to check the statistics about a QoS profile.

----End

Example

- Run the **display qos-profile configuration [profile-name]** command, and you can view the detailed configurations of a QoS profile.

```
<HUAWEI> display qos-profile configuration test
qos-profile: test
  inbound:
  outbound:
  both:
    car cir 6000 pir 10000 cbs 10000 pbs 10000 green pass yellow pass red
    discard
  Reference relationship:
    GigabitEthernet1/0/0.1
```
- Run the **display qos-profile application profile-name** command, and you can view the applications of a QoS profile.

```
<HUAWEI> display qos-profile application test
qos-profile test:
  GigabitEthernet4/0/0.1
```
- Run the **display qos-profile statistics interface interface-type interface-number [[vlan vlan-id] | [pe-vid pe-vid ce-vid ce-vid]] { inbound | outbound }** command, and you can view the statistical information about a QoS profile on an interface.

```
<HUAWEI> display qos-profile statistics interface gigabitethernet 4/0/7
outbound
GigabitEthernet4/0/7 outbound traffic statistics:
  [be]
  Pass:                      0 packets,          0 bytes
  Discard:                    0 packets,          0 bytes
  Last 5 minutes pass rate:   0 pps,            0 bps
```

Last 5 minutes discard rate:	0 pps,	0 bps
[af1]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af2]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af3]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af4]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[ef]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[cs6]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[cs7]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[total]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps

10.6 Configuring HQoS Scheduling for Family Users

HQoS for family users performs uniform scheduling for an entire family rather than individual terminals.

10.6.1 Establishing the Configuration Task

Before configuring HQoS for family users, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

A family may use multiple terminals to demand various services, such as VoIP, IPTV, and HSI. These services have different requirements for delay, jitter, and bandwidth. In addition, requirements of high-priority services must be satisfied preferentially when network resources are insufficient. Therefore, QoS scheduling must be performed based on a family rather than on each separate terminal.

After users log in, the NE80E/40E identifies services based on inner or outer VLAN IDs, 802.1p values, DSCP values, or DHCP-Option 60 information carried in user packets. The packets matching the identification condition are mapped to a domain and are authenticated.

After user authentication succeeds, if the interface is configured with a QoS profile and the access information of user packets matches the scheduling defined in the QoS profile, the access users are considered as family users; otherwise, they are considered as common users.



The services on a BAS interface or different sub-interfaces can participate in uniform QoS scheduling for family users if they have the same family attributes.

Pre-configuration Tasks

Before configuring HQoS scheduling for family users, complete the following tasks:

Configuring the BRAS function for the NE80E/40E so that users can successfully access the network (For details, refer to the *HUAWEI NetEngine80E/40E Router Configuration Guide - User Access*.)

Data Preparation

To configure HQoS scheduling for family users, you need the following data.

No.	Data
1	Family profile name and family identification policy
2	QoS profile name and scheduling parameters
3	Number of the interface through which the user accesses the network
4	Service identification policy name and service identification mode
5	Name of the domain to which a user belongs



If the parameters about the family profile and the service identification policy are changed after a family or a user logs in, the changed parameters take effect only after next login.

10.6.2 Defining a QoS Profile and Configuring Scheduling Parameters

A QoS profile is the aggregate of QoS scheduling parameters. Configurable scheduling parameters for SQs include CIR, PIR, FQ profiles, and lengths for packet loss compensation of service profiles.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
qos-profile qos-profile-name
```

A QoS profile is defined and the QoS profile view is displayed.

Step 3 You can choose to configure user queue scheduling and traffic assurance for users as required.

- To configure user queue scheduling parameters to implement HQoS for user services, run the **user-queue cir cir-value [pir pir-value] [flow-queue flow-queue-name] [flow-mapping flow-mapping-name] [user-group-queue user-group-queue name] [service-template service-template-name] [inbound | outbound]** command.
- To configure the CAR function to implement traffic assurance for users, run the **car { cir cir-value [pir pir-value] } [cbs cbs-value pbs pbs-value] [green { discard | pass [service-class class color color] } | yellow { discard | pass [service-class class color color] } | red { discard | pass [service-class class color color] }]* [inbound | outbound]** command.

 **NOTE**

- The **car** command and the **user-queue** command cannot be configured together with the **qos-profile** command in the same direction of an interface.
- When configuring the **user-queue** command, you can apply only the global service profile.

----End

10.6.3 Configuring a Service Identification Policy

Service identification enables the system to determine which authentication domain is used based on the information about some fields carried in user packets.

Context

Service identification enables the NE80E/40E to determine which authentication domain is used based on the information about some fields carried in user packets. Currently, service identification is applicable to the IPoE access users. For PPPoE access users, the NE80E/40E can resolve the information about the authentication domain based on the user names carried in user packets.

The NE80E/40E supports the following service identification modes. You can select the mode as required.

- Service identification based on VLAN IDs in inner or outer VLAN tags
- Service identification based on 802.1p values in inner or outer VLAN tags
- Service identification based on DSCP values
- Service identification based on DHCP Option 60 information

Procedure

- Configuring service identification based on VLAN IDs in inner or outer VLAN tags
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`service-identify-policy policy-name`
A service identification policy is created and the service identification policy view is displayed.
By default, no service identification policy is configured.
 3. Run:
`service-identify { inner-vlan | outer-vlan }`
The service identification mode is configured.
 4. Run:
`vlan start-vlan-id [to end-vlan-id] domain domain-name`
The packets with a specified VLAN ID are mapped a domain.
- Configuring service identification based on 802.1p values in inner or outer VLAN tags
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`service-identify-policy policy-name`
A service identification policy is created and the service identification policy view is displayed.
By default, no service identification policy is configured.
 3. Run:
`service-identify 8021p { inner-vlan | outer-vlan }`
The service identification mode is configured.
 4. Run:
`8021p start-8021p-value [end-8021p-value] domain domain-name`
The packets with a specified 802.1p value in the inner or outer VLAN tag are mapped to a domain.
- Configuring service identification based on DSCP values
 1. Run:

system-view

The system view is displayed.

2. Run:

service-identify-policy policy-name

A service identification policy is created and the service identification policy view is displayed.

By default, no service identification policy is configured.

3. Run:

service-identify dscp

The service identification mode is configured.

4. Run:

dscp start-dscp-value [end-dscp-value] domain domain-name

The packets with a specified DSCP value are mapped to a domain.

- Configuring service identification based on DHCP Option 60 information

1. Run:

system-view

The system view is displayed.

2. Run:

service-identify-policy policy-name

A service identification policy is created and the service identification policy view is displayed.

By default, no service identification policy is configured.

3. Run:

service-identify dhcp-option60

The service identification mode is configured.

4. (Optional) Run:

option60 partial-match

Partial matching of the DHCPv4 OPTION60 information is configured.

By default, the service identification mode is domain included, that is, strictly matching the domain name.

5. (Optional) Run:

option60 encrypt

Encrypt the Option 60 field value is configured.

----End

10.6.4 (Optional) Configuring the Service Traffic of Users in a Domain Not to Participate in the QoS Scheduling for Family Users

You can exclude the traffic of users in a domain from the family-based traffic scheduling. Instead, service-specific bandwidth management is implemented on the traffic of these users.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
domain domain-name
```

A domain is created and the AAA domain view is displayed.

Step 4 Run:

```
session-group-exclude { car | user-queue } { inbound | outbound }
```

The service traffic of users in a domain is configured not to participate in the QoS scheduling for family users.

- Using the **session-group-exclude car** command, you can exclude the service traffic of users in a domain from participating in the CAR operation for family users.
- Using the **session-group-exclude user-queue** command, you can exclude the service traffic of users in a domain from participating in SQ scheduling for family users.

----End

10.6.5 Binding a QoS Profile and a Service Identification Policy to a BAS Interface

You can apply a QoS profile to a type of user packets on an interface to perform HQoS for the user packets based on the scheduling parameters. You can also bind a service identification policy to the interface so that packets that meet specified conditions can be mapped to the domain for authentication.

Context



NOTE

Applying a QoS profile to an interface functions differently from applying a QoS profile to a domain. The parameters about the bandwidth allocated to family users are obtained through the QoS profile applied to the interface while the parameters about the bandwidth allocated based on service types are obtained through the QoS profile applied to the domain.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 (Option) Run:

```
qos committed-bandwidth check outbound enable
```

Check on the total bandwidth of SQs is enabled.

Step 4 Run:

```
bas
```

The BAS interface view is displayed.

Step 5 Choose the matched command line to apply QoS profiles based on types of user packets.

- Run the **qos-profile** *qos-profile-name* { **inbound** | **outbound** } [**identifier none** | **option82**] [**group group-name**] command to apply a QoS profile to Layer 3 user packets and specify a family user identification mode.
- Run the **qos-profile** *qos-profile-name* { **inbound** | **outbound** } [**vlan vlan-id1** [**to vlan-id2**]] **identifier** { **vlan-id** | **none** | **option82** } [**group group-name**] [**session-limit max-session-number**] command to apply a QoS profile to VLAN user packets and specify a family user identification mode.
- Run the **qos-profile** *qos-profile-name* { **inbound** | **outbound** } [**pe-vid pe-vlan-id ce-vid ce-vlan-id1** [**to ce-vlan-id2**]] **identifier** { **pe-vid** | **ce-vid** | **pe-ce-vid** | **none** | **option82** } [**group group-name**] [**session-limit max-session-number**] command to apply a QoS profile to QinQ user packets and specify a family user identification mode.

Step 6 Run:

```
service-identify-policy policy-name
```

A service identification policy is bound to the BAS interface.

----End

10.6.6 (Optional) Configuring Dynamic Update of a QoS Profile

When the QoS profile applied by online users is changed, the previously configured QoS profile for the domain to which the online users belong does not take effect.

Context

To enable an online user to modify the in-use QoS profile, you need to configure dynamic update of the QoS profile. After this function is configured, the QoS profile being used by the user is changed to the profile defined in the **update qos-profile** command and the original QoS profile applied to the user domain no longer takes effect.

Dynamic update of the QoS profile takes effect for only service traffic of the user. The QoS profile for family users cannot be updated. That is only the QoS profile applied in domain can be updated but the QoS profile applied in interface cannot be updated.

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
update qos-profile user-id user-id profile qos-profile-name { inbound | outbound }
```

Dynamic update of the QoS profile is configured.

----End

10.6.7 Checking the Configuration

After HQoS is configured for family users, you can view information about the online users with specified IDs and the bandwidth consumed by them and applications of the QoS profile.

Context

Run the following commands to check the previous configuration.

Procedure

Step 1 Run the **display qos user-id user-id** command to check the traffic statistics on the eight subscriber queues (SQs) of a specified user.

Step 2 Run the **display qos-profile configuration [profile-name]** command to check the configuration about a QoS profile.

Step 3 Run the **display qos-profile application profile-name** command to check applications of a QoS profile.

Step 4 Run the **display access-user user-id user-id** command to check QoS information after a user goes online.

----End

Example

- Run the **display qos user-id user-id** command, and you can view information about the online users with specified IDs.

```
<HUAWEI> display qos user-id 1 inbound
user-id 1 inbound user-queue statistics:
[be]
Current usage percentage of queue: 1
  Pass:          0 packets,          0 bytes
  Discard:       0 packets,          0 bytes
  Last 5 minutes pass rate:      0 pps,          0 bps
  Last 5 minutes discard rate:   0 pps,          0 bps
[af1]
```

```

Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af2]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af3]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af4]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[ef]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs6]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs7]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[total]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

```

- Run the **display qos-profile configuration [profile-name]** command, and you can view the detailed configuration about a QoS profile.

```
<HUAWEI> display qos-profile configuration test
qos-profile: test
inbound:
outbound:
```

```
both:  
    car cir 6000 pir 10000 cbs 10000 pbs 10000 green pass yellow pass red  
discard  
Reference relationship:  
    GigabitEthernet1/0/0.1
```

- Run the **display qos-profile application profile-name** command, and you can view applications of a QoS profile.

```
<HUAWEI> display qos-profile application test  
qos-profile test:  
    GigabitEthernet4/0/0.1
```

- Run the **display qos-profile statistics interface interface-type interface-number [[vlan vlan-id] | [pe-vid pe-vid ce-vid ce-vid]] { inbound | outbound }** command, and you can view statistics about a QoS profile applied to an interface.

```
<HUAWEI> display qos-profile statistics interface gigabitethernet4/0/7 outbound  
GigabitEthernet4/0/7 outbound traffic statistics:  
    [be]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [af1]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [af2]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [af3]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [af4]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [ef]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [cs6]  
        Pass: 0 packets, 0 bytes  
        Discard: 0 packets, 0 bytes  
        Last 5 minutes pass rate: 0 pps, 0 bps  
        Last 5 minutes discard rate: 0 pps, 0 bps  
    [cs7]  
        Pass: 0 packets, 0 bytes
```

Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[total]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps

10.7 Configuring HQoS Scheduling for Common Users

HQoS for common users identifies services by priority and then performs uniform scheduling.

Context

After user authentication succeeds, if the interface is configured with a QoS profile and the access information of user packets matches the scheduling defined in the QoS profile, the access users are considered as family users; otherwise, they are considered as common users.

10.7.1 Establishing the Configuration Task

Before configuring HQoS for common users, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

If the access user is a IPoE user, family identification is not required. Such an access is considered as a single user access and such a user is called a common user. The IPoE users are identified according to IP addresses. In addition, common users may demand various types of services. The demanded services need be differentiated according to priorities. The system obtains QoS information about common users from the QoS profile applied to the authentication domain.

NOTE

You can configure the RADIUS server to dynamically deliver QoS parameters during the authentication of common users. In such a case, configuring QoS parameter delivery on the NE80E/40E is not required.

After user authentication succeeds, if the interface is configured with a QoS profile and the access information of user packets matches the scheduling defined in the QoS profile, the access users are considered as family users; otherwise, they are considered as common users.

Pre-configuration Tasks

Before configuring HQoS scheduling for common users, complete the following tasks:

Configuring the BRAS function for the NE80E/40E so that users can successfully access the network (For details, refer to the *Configuration Guide - User Access*.)

Data Preparation

To configure HQoS scheduling for common users, you need the following data.

No.	Data
1	QoS profile name and scheduling parameters
2	Rate limit mode for common users
3	Service identification policy name and service identification mode
4	Name of the domain to which a user belongs

10.7.2 Defining a QoS Profile and Configuring Scheduling Parameters

A QoS profile is the aggregate of QoS scheduling parameters. Configurable scheduling parameters for SQs include CIR, PIR, FQ profiles, and lengths for packet loss compensation of service profiles.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
qos-profile qos-profile-name
```

A QoS profile is defined and the QoS profile view is displayed.

Step 3 You can choose to configure user queue scheduling and traffic assurance for users as required.

- To configure user queue scheduling parameters to implement HQoS for user services, run the **user-queue cir cir-value [pir pir-value] [flow-queue flow-queue-name] [flow-mapping flow-mapping-name] [user-group-queue user-group-queue name] [service-template service-template-name] [inbound | outbound]** command.
- To configure the CAR function to implement traffic assurance for users, run the **car { cir cir-value [pir pir-value] } [cbs cbs-value pbs pbs-value] [green { discard | pass [service-class class color color] } | yellow { discard | pass [service-class class color color] } | red { discard | pass [service-class class color color] }]*[inbound | outbound]** command.

NOTE

- The **car** command and the **user-queue** command cannot be configured together with the **qos-profile** command in the same direction of an interface.
- When configuring the **user-queue** command, you can apply only the global service profile.

----End

10.7.3 Configuring the Rate Limit Mode for Common Users

The system schedules traffic from common users by obtaining CAR and SQ parameters defined in the QoS profile based on the rate limit mode configured for the common users.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
domain domain-name
```

A domain is created and the AAA domain view is displayed.

Here, *domain-name* specifies the domain to which the service is mapped.

Step 4 Run:

```
qos rate-limit-mode { car | user-queue } { inbound | outbound }
```

The rate limit mode for common users is configured.

When a QoS profile is applied in an AAA domain, if the QoS profile contains both the **car** and **user-queue** parameters, the system determines whether the **qos rate-limit-mode** command is configured in the domain. If the **qos rate-limit-mode** command is configured in the domain, the system performs traffic scheduling according to the CAR parameter in the QoS profile. If the **qos rate-limit-mode user-queue** command is configured in the domain, the system performs traffic scheduling according to the SQ parameter in the QoS profile.

----End

10.7.4 (Optional) Configuring User Name-based Access Limit

By configuring user name-based access limit, you can limit the total number of access users with the same user account. If the number of access users exceeds the upper limit, subsequent access users are denied.

Context

To guarantee the processing performance of the NE80E/40E, you can limit the total number of access users with the same account. If the number of users reaches the upper limit, new access users are denied.

By configuring user name-based access limit, you can control the number of sessions set up by users with the same account (user name), thereby restricting the total bandwidth. After the user name-based access limit function is configured, the users with the same user name share QoS

resources. If there are users already online before this function is configured, the online users are allocated QoS resources separately. Only the users going online after the **user-max-session** is configured share QoS resources.

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`aaa`

The AAA view is displayed.

Step 3 Run:

`domain domain-name`

The AAA domain view is displayed.

Step 4 Run:

`user-max-session max-session-number`

The maximum number of sessions that can be set up by users with the same account is set.

By default, the number of sessions is not limited.

----End

10.7.5 Applying a QoS Profile to a Domain

You can define a QoS profile and then apply it to the AAA domain to perform QoS scheduling for access user traffic.

Context



NOTE

Applying a QoS profile to an interface functions differently from applying a QoS profile to a domain. The parameters about the bandwidth allocated to family users are obtained through the QoS profile applied to the interface while the parameters about the bandwidth allocated based on service types are obtained through the QoS profile applied to the domain.

The system performs traffic scheduling on common online users in a domain by directly adopting the parameters in the QoS profile applied to the domain. For family users, however, the system adopts only the parameters in the **car** command that is configured in the view of the QoS profile applied to the domain for traffic rate limit.

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`aaa`

The AAA view is displayed.

Step 3 Run:

`domain domain-name`

A domain is created and the AAA domain view is displayed.

Here, *domain-name* specifies the domain to which the service needs to be mapped.

Step 4 Run:

`qos-profile qos-profile-name { inbound | outbound } [lns-gts]`

The QoS profile is applied to the domain.

You can configure the parameter **lns-gts** only when you need to perform QoS scheduling on user services on an LNS. That is, the **lns-gts** parameter takes effect for only L2TP users.

----End

10.7.6 (Optional) Configuring Dynamic Update of a QoS Profile

When the QoS profile applied by online users is changed, the previously configured QoS profile for the domain to which the online users belong does not take effect.

Context

To enable an online user to modify the in-use QoS profile, you need to configure dynamic update of the QoS profile. After this function is configured, the QoS profile being used by the user is changed to the profile defined in the **update qos-profile** command and the original QoS profile applied to the user domain no longer takes effect.

Dynamic update of the QoS profile takes effect for only service traffic of the user. The QoS profile for family users cannot be updated. That is only the QoS profile applied in domain can be updated but the QoS profile applied in interface cannot be updated.

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

`aaa`

The AAA view is displayed.

Step 3 Run:

`update qos-profile user-id user-id profile qos-profile-name { inbound | outbound }`

Dynamic update of the QoS profile is configured.

----End

10.7.7 Checking the Configuration

After HQoS is configured for common users, you can view information about the online users with specified IDs and the bandwidth consumed by them and applications of the QoS profile.

Context

Run the following commands to check the previous configuration.

Procedure

- Step 1 Run the **display qos user-id user-id** command to check the traffic statistics on the eight subscriber queues (SQs) of a specified user.
- Step 2 Run the **display qos-profile configuration [profile-name]** command to check the configuration about a QoS profile.
- Step 3 Run the **display qos-profile application profile-name** command to check the applications of a QoS profile.

----End

Example

- Run the **display qos user-id user-id** command, and you can view information about the online users with specified IDs.

```
<HUAWEI> display qos user-id 1 inbound
user-id 1 inbound user-queue statistics:
[be]
Current usage percentage of queue: 1
  Pass:          0 packets,          0 bytes
  Discard:       0 packets,          0 bytes
  Last 5 minutes pass rate:      0 pps,          0 bps
  Last 5 minutes discard rate:   0 pps,          0 bps
[af1]
Current usage percentage of queue: 1
  Pass:          0 packets,          0 bytes
  Discard:       0 packets,          0 bytes
  Last 5 minutes pass rate:      0 pps,          0 bps
  Last 5 minutes discard rate:   0 pps,          0 bps
[af2]
Current usage percentage of queue: 1
  Pass:          0 packets,          0 bytes
  Discard:       0 packets,          0 bytes
  Last 5 minutes pass rate:      0 pps,          0 bps
  Last 5 minutes discard rate:   0 pps,          0 bps
[af3]
Current usage percentage of queue: 1
  Pass:          0 packets,          0 bytes
  Discard:       0 packets,          0 bytes
  Last 5 minutes pass rate:      0 pps,          0 bps
  Last 5 minutes discard rate:   0 pps,          0 bps
[af4]
Current usage percentage of queue: 1
  Pass:          0 packets,          0 bytes
```

```

Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[ef]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs6]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs7]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[total]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

```

- Run the **display qos-profile configuration [profile-name]** command, and you can view the detailed configuration about a QoS profile.

```
<HUAWEI> display qos-profile configuration test
qos-profile: test
inbound:
outbound:
both:
    car cir 6000 pir 10000 cbs 10000 pbs 10000 green pass yellow pass red
discard
Reference relationship:
    GigabitEthernet1/0/0.1
```

- Run the **display qos-profile application profile-name** command, and you can view applications of a QoS profile.

```
<HUAWEI> display qos-profile application test
qos-profile test:
    GigabitEthernet4/0/0.1
```

- Run the **display qos-profile statistics interface interface-type interface-number [[vlan vlan-id] | [pe-vid pe-vid ce-vid ce-vid]] { inbound | outbound }** command, and you can view statistics about a QoS profile applied to an interface.

```
<HUAWEI> display qos-profile statistics interface gigabitethernet4/0/7 outbound
GigabitEthernet4/0/7 outbound traffic statistics:
[be]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
```

```
[af1]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[af2]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[af3]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[af4]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[ef]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[cs6]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[cs7]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps

[total]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
```

10.8 Configuring HQoS Scheduling for Leased Line Users

Leased line users share the same SQ and HQoS performs uniform scheduling for leased line users.

10.8.1 Establishing the Configuration Task

Before configuring HQoS for leased line users, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

All Layer 2 or Layer 3 access users belong to the same enterprise. They access the network through one sub-interface and are accounted and allocated bandwidth uniformly. These users are called leased line users. Leased line users share the same SQ and the SQ scheduling parameters are obtained from the QoS profile applied to the authentication domain.

NOTE

Service identification is not applicable to leased line users.

Pre-configuration Tasks

Before configuring HQoS scheduling for leased line users, complete the following tasks:

Configuring the BRAS function for the NE80E/40E so that users can successfully access the network (For details, refer to the *Configuration Guide - User Access*.)

Data Preparation

To configure HQoS scheduling for leased line users, you need the following data.

No.	Data
1	QoS profile name and scheduling parameters
2	Rate limit mode for leased line users
3	Name of the domain to which a user belongs

10.8.2 Defining a QoS Profile and Configuring Scheduling Parameters

A QoS profile is the aggregate of QoS scheduling parameters. Configurable scheduling parameters for SQs include CIR, PIR, FQ profiles, and lengths for packet loss compensation of service profiles.

Context

Do as follows on the router:

Procedure

Step 1 Run:

`system-view`

The system view is displayed.

Step 2 Run:

```
qos-profile qos-profile-name
```

A QoS profile is defined and the QoS profile view is displayed.

Step 3 You can choose to configure user queue scheduling and traffic assurance for users as required.

- To configure user queue scheduling parameters to implement HQoS for user services, run the **user-queue cir cir-value [pir pir-value] [flow-queue flow-queue-name] [flow-mapping flow-mapping-name] [user-group-queue user-group-queue name] [service-template service-template-name] [inbound | outbound]** command.
- To configure the CAR function to implement traffic assurance for users, run the **car { cir cir-value [pir pir-value] } [cbs cbs-value pbs pbs-value] [green { discard | pass [service-class class color color] } | yellow { discard | pass [service-class class color color] } | red { discard | pass [service-class class color color] }]* [inbound | outbound]** command.

 **NOTE**

- The **car** command and the **user-queue** command cannot be configured together with the **qos-profile** command in the same direction of an interface.
- When configuring the **user-queue** command, you can apply only the global service profile.

----End

10.8.3 Configuring the Rate Limit Mode for Leased Line Users

The system obtains SQ parameters about leased line users from the QoS profile applied to the authentication domain. You can configure the rate limit mode for leased line users and perform flow control for leased line users based on the CAR and SQ parameters defined in the QoS profile.

Context

Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaaaaa
```

The AAA view is displayed.

Step 3 Run:

```
domain domain-name
```

A domain is created and the AAA domain view is displayed.

Here, *domain-name* specifies the domain to which the service is mapped.

Step 4 Run:

```
qos rate-limit-mode { car | user-queue } { inbound | outbound }
```

The rate limit mode for leased line users is configured.

When a QoS profile is applied in an AAA domain, if the QoS profile contains both the **car** and **user-queue** parameters, the system judges whether the **qos rate-limit-mode** command is configured in the domain. If the **qos rate-limit-mode** command is configured in the domain, the system performs traffic scheduling according to the CAR parameter in the QoS profile. If the **qos rate-limit-mode user-queue** command is configured in the domain, the system performs traffic scheduling according to the SQ parameter in the QoS profile.

----End

10.8.4 Applying a QoS Profile to a Domain

Context



Applying a QoS profile to an interface functions differently from applying a QoS profile to a domain. The parameters about the bandwidth allocated to family users are obtained through the QoS profile applied to the interface while the parameters about the bandwidth allocated based on service types are obtained through the QoS profile applied to the domain.

The system performs traffic scheduling on common online users in a domain by directly adopting the parameters in the QoS profile applied to the domain. For family users, however, the system adopts only the parameters in the **car** command that is configured in the view of the QoS profile applied to the domain for traffic rate limit.

Do as follows on the router:

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

domain domain-name

A domain is created and the AAA domain view is displayed.

Here, *domain-name* specifies the domain to which the service needs to be mapped.

Step 4 Run:

qos-profile qos-profile-name { inbound | outbound }

The QoS profile is applied to the domain.

----End

10.8.5 Checking the Configuration

After HQoS is configured for leased line users, you can view information about the online users with specified IDs and the bandwidth consumed by them and applications of a QoS profile.

Context

Run the following commands to check the previous configuration.

Procedure

- Step 1** Run the **display qos user-id user-id** command to check the traffic statistics on the eight subscriber queues (SQs) of a specified user.
- Step 2** Run the **display qos-profile configuration [profile-name]** command to check the configuration about a QoS profile.
- Step 3** Run the **display qos-profile application profile-name** command to check applications of a QoS profile.
- Step 4** Run the **display access-user user-id user-id** command to check QoS information after a user goes online.

----End

Example

- Run the **display qos user-id user-id** command, and you can view information about the online users with specified IDs.

```
<HUAWEI> display qos user-id 1 inbound
user-id 1 inbound user-queue statistics:
[be]
Current usage percentage of queue: 1
    Pass:          0 packets,          0 bytes
    Discard:       0 packets,          0 bytes
    Last 5 minutes pass rate:      0 pps,          0 bps
    Last 5 minutes discard rate:   0 pps,          0 bps
[af1]
Current usage percentage of queue: 1
    Pass:          0 packets,          0 bytes
    Discard:       0 packets,          0 bytes
    Last 5 minutes pass rate:      0 pps,          0 bps
    Last 5 minutes discard rate:   0 pps,          0 bps
[af2]
Current usage percentage of queue: 1
    Pass:          0 packets,          0 bytes
    Discard:       0 packets,          0 bytes
    Last 5 minutes pass rate:      0 pps,          0 bps
    Last 5 minutes discard rate:   0 pps,          0 bps
[af3]
Current usage percentage of queue: 1
    Pass:          0 packets,          0 bytes
    Discard:       0 packets,          0 bytes
    Last 5 minutes pass rate:      0 pps,          0 bps
    Last 5 minutes discard rate:   0 pps,          0 bps
[af4]
Current usage percentage of queue: 1
    Pass:          0 packets,          0 bytes
    Discard:       0 packets,          0 bytes
    Last 5 minutes pass rate:      0 pps,          0 bps
```

```
Last 5 minutes discard rate: 0 pps, 0 bps
[ef]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs6]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs7]
Current usage percentage of queue: 1
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[total]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
```

- Run the **display qos-profile configuration [profile-name]** command, and you can view the detailed configuration about a QoS profile.

```
<HUAWEI> display qos-profile configuration test
qos-profile: test
inbound:
outbound:
both:
car cir 6000 pir 10000 cbs 10000 pbs 10000 green pass yellow pass red
discard
Reference relationship:
GigabitEthernet1/0/0.1
```

- Run the **display qos-profile application profile-name** command, and you can view applications of a QoS profile.

```
<HUAWEI> display qos-profile application test
qos-profile test:
GigabitEthernet4/0/0.1
```

- Run the **display qos-profile statistics interface interface-type interface-number [[vlan vlan-id] | [pe-vid pe-vid ce-vid ce-vid]] { inbound | outbound }** command, and you can view statistics about a QoS profile applied to an interface.

```
<HUAWEI> display qos-profile statistics interface gigabitethernet4/0/7 outbound
GigabitEthernet 4/0/7 outbound traffic statistics:
[be]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af1]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
```

Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af2]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af3]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af4]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[ef]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[cs6]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[cs7]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[total]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps

10.9 Maintaining HQoS

This section describes how to clear HQoS statistics.

10.9.1 Clearing Queue Statistics

This section describes how to clear statistics about a specified GQ, a specified SQ on a specified interface, a QoS profile on a specified interface, and SQs of the eight priorities of a specified user.

Context



CAUTION

Queue statistics cannot be restored after you clear it. So, confirm the action before you use the command.

Make sure that you would clear the queue statistics and run the **reset** command in the user view to clear the existing queue statistics.

Procedure

- Run the **reset user-group-queue group-name statistics slot { slot-id | all } { inbound | outbound }** command to clear statistics on a specified GQ.
- Run the **reset user-queue statistics interface interface-type interface-number { inbound | outbound }** command to clear statistics of a specified SQ on a specified interface.
- Run the **reset qos-profile statistics interface interface-type interface-number [[vlan vlan-id] | [pe-vid pe-vid ce-vid ce-vid]] { inbound | outbound }** command to clear statistics of the QoS template on a specified interface.
- Run the **reset qos user-id user-id { inbound | outbound }** command to clear eight SQ statistics of a specified user.

---End

10.10 Configuration Examples

This section provides examples for configuring HQoS, including the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

NOTE

This document takes interface numbers and link types of the NE40E-X8 for example. In working situations, the actual interface numbers and link types may be different from those used in this document.

10.10.1 Example for Configuring HQoS on an Ethernet Interface

This section provides an example for configuring HQoS on an Ethernet interface in the networking where users access the network through Ethernet sub-interfaces.

Networking Requirements

To differentiate users and provide hierarchical QoS for them, HQoS divides a GE master interface into multiple sub-interfaces for access by users. For the purpose of better utilization of the bandwidth of the GE interface, each user accesses the network through a GE sub-interface. The packets of all users are then converged to the backbone network by the router.

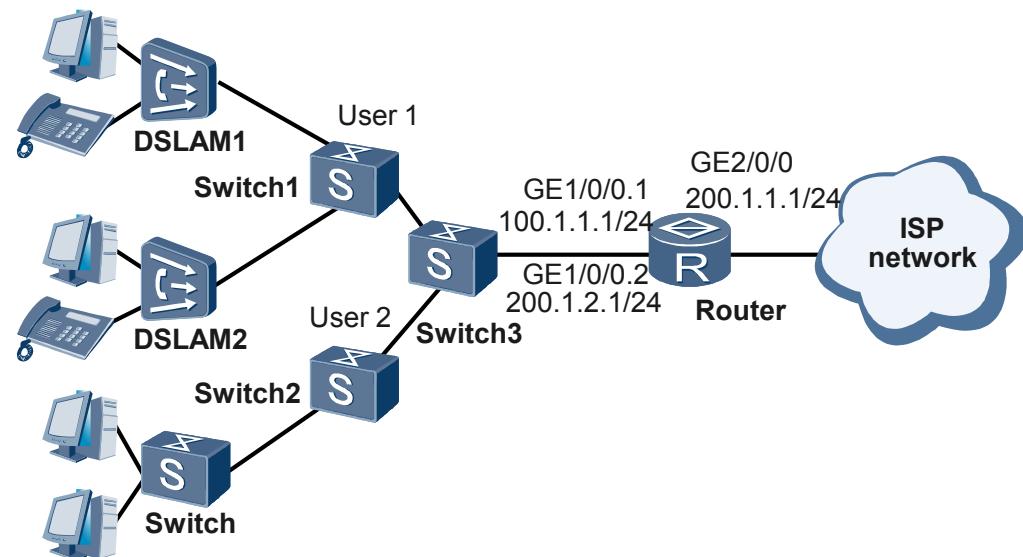
As shown in **Figure 10-8**, router is an access device to the backbone network. The router connects Layer 2 switches. User1 and User2 access the network through GigabitEthernet1/0/0.1 and GigabitEthernet1/0/0.2 of router. User1 is guaranteed with a bandwidth of 100 Mbit/s; User2, 200 Mbit/s. The bandwidth of the EF flow of User1 is 30 Mbit/s; that of the AF1 flow, 10 Mbit/s.

s. The bandwidth of the EF flow of User2 is 50 Mbit/s. User1 and User2 are in the same subscriber group. The bandwidth of the group queue is 500 Mbit/s. On the downstream interface of router, the traffic rate of EF flow is no more than 100 Mbit/s.

 **NOTE**

Home users carry out broadband access through home service gateways. A home service gateway adds VLAN tags to service packets of home users to identify the users' VLAN and the 802.1 priorities of services. Home users' packets with VLAN tags are forwarded at Layer 2 through DSLAMs and switches. VLAN tags are terminated on the sub-interface of router and then the packets go to the ISP network.

Figure 10-8 Networking diagram for configuring SQ



Configuration Roadmap



CAUTION

In upstream HQoS scheduling on an Ethernet interface, CQ adopts the default scheduling setting and is not configured by users.

It is recommended that users configure downstream CQ on an Ethernet interface so that the backbone network is not congested.

The configuration roadmap is as follows:

1. Configuring parameters of packet dropping for the FQ WRED object.
2. Configuring algorithms for flow queue scheduling and related parameters.
3. Configuring service class mappings from FQs to CQs.
4. Configuring values of GQ shaping.
5. Configuring SQs on the upstream interface of the access router.

6. Configuring parameters of packet dropping for a CQ WRED object.
7. Configuring CQs on the downstream interface of the access router.

Data Preparation

To complete the configuration, you need the following data:

- VLAN IDs of sub-interfaces
- Parameters of flow-wred packet dropping
- Algorithms for flow-queue scheduling and related parameters
- Service class mappings for flow-mapping
- Values of user-group-queue shaping
- Values of user-queue CIR, PIR, and network-header-length
- Parameters of port-wred referenced by port-queue
- Algorithms for port-queue scheduling and related parameters and shaping values

Procedure

Step 1 Configure a WRED object referenced by FQs.

Configure parameters of flow-wred packet dropping.

```
<HUAWEI> system view
[HUAWEI] flow-wred test
[HUAWEI-flow-wred-test] color green low-limit 70 high-limit 100 discard-percentage
100
[HUAWEI-flow-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage
100
[HUAWEI-flow-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-flow-wred-test] return
```

After the preceding configuration, you can run the **display flow-wred configuration verbose** command to view the configured parameters of the FQ WRED object.

```
<HUAWEI> display flow-wred configuration verbose test
flow-wred-name : test
-----
          color    low-limit    high-limit    discard-percent
-----
          green      70          100          100
          yellow     60          90          100
          red        50          80          100
Queue Depth : 32768
Reference relationships : test
```

Step 2 Configure algorithms for queue scheduling and related parameters of FQs.

Configure the scheduling algorithms, WRED parameters, and shaping values for FQs.

```
<HUAWEI> system view
[HUAWEI] flow-queue test1
[HUAWEI-flow-queue-template-test1] queue af1 lpq flow-wred test shaping 10000
[HUAWEI-flow-queue-template-test1] queue ef pq flow-wred test shaping 30000
[HUAWEI-flow-queue-template-test1] quit
[HUAWEI] flow-queue test2
[HUAWEI-flow-queue-template-test2] queue ef pq flow-wred test shaping 25000
[HUAWEI-flow-queue-template-test2] return
```

After the preceding configuration, you can run the **display flow-queue configuration verbose** command to view the configuration of the FQ template.

```
<HUAWEI> display flow-queue configuration verbose test1
Codes: Arith(Schedule algorithm)
        U-Weight(Schedule weight configured by users)
        I-Weight(Inverse schedule weight used by TM)
        A-Weight(Actual schedule weight obtained by users)
        Shp(Shaping value, the percentage of subscriber queue's PIR)
        Drop-Arith(The name of the WRED object used by the flow queue)
```

```
Flow Queue Template : test1
-----
Cos  Arith   U-Weight  I-Weight  A-Weight  Shp    Pct  Drop-Arith
-----
be   wfq     10        3         10.00    -       -     Tail Drop
af1  lpq     -         -         -         10000   -     test
af2  wfq     10        3         10.00    -       -     Tail Drop
af3  wfq     15        2         15.00    -       -     Tail Drop
af4  wfq     15        2         15.00    -       -     Tail Drop
ef   pq      -         -         -         30000   -     test
cs6  pq      -         -         -         -       -     Tail Drop
cs7  pq      -         -         -         -       -     Tail Drop
```

Reference relationships : NULL

```
<HUAWEI> display flow-queue configuration verbose test2
Codes: Arith(Schedule algorithm)
        U-Weight(Schedule weight configured by users)
        I-Weight(Inverse schedule weight used by TM)
        A-Weight(Actual schedule weight obtained by users)
        Shp(Shaping value, the percentage of subscriber queue's PIR)
        Drop-Arith(The name of the WRED object used by the flow queue)
```

```
Flow Queue Template : test2
-----
Cos  Arith   U-Weight  I-Weight  A-Weight  Shp    Pct  Drop-Arith
-----
be   wfq     10        3         10.00    -       -     Tail Drop
af1  wfq     10        3         10.00    -       -     Tail Drop
af2  wfq     10        3         10.00    -       -     Tail Drop
af3  wfq     15        2         15.00    -       -     Tail Drop
af4  wfq     15        2         15.00    -       -     Tail Drop
ef   pq      -         -         -         25000   -     test
cs6  pq      -         -         -         -       -     Tail Drop
cs7  pq      -         -         -         -       -     Tail Drop
```

Reference relationships : NULL

Step 3 Configure service class mappings from FQs to CQs.

```
<HUAWEI> system view
[HUAWEI] flow-mapping test1
[HUAWEI-flow-mapping-test1] map flow-queue af1 to port-queue ef
[HUAWEI-flow-mapping-test1] return
```

After the preceding configuration, you can run the **display flow-mapping configuration verbose** command to view the configured parameters of the FQ mapping object and the referential relations of the object.

```
<HUAWEI> display flow-mapping configuration verbose test1
flow-mapping-name : test1
  fq-cosvalue to pq-cosvalue
  be          to be
  af1         to ef
  af2         to af2
  af3         to af3
  af4         to af4
  ef          to ef
  cs6         to cs6
  cs7         to cs7
  [reference relationship]
NULL
```

Step 4 Configure the value for the GQ shaping.

```
# Configure user-group-queue.  
  
<HUAWEI> system view  
[HUAWEI] user-group-queue test  
[HUAWEI-user-group-queue-test-slot-all] shaping 500000 inbound  
[HUAWEI-user-group-queue-test-slot-all] return
```

After the preceding configuration, you can run the **display user-group-queue configuration verbose** command to view the configuration of the GQ and the referential relations.

```
<HUAWEI> display user-group-queue configuration verbose test  
user-group-queue-name : test  
slot : 3  
[current configuration]  
inbound  
shaping-value <kbps> : 500000  
pbs-value <byte> : 524288  
outbound  
shaping-value <kbps> : NA  
pbs-value <byte> : NA  
[reference relationship]  
NULL  
[unsuccessful slot]  
NULL
```

Step 5 Configure an SQ on the upstream interface of the access router.

```
<HUAWEI> system view  
[HUAWEI] service-template st1  
[HUAWEI-service-template-st1-slot-all] network-header-length 10 inbound  
[HUAWEI-service-template-st1-slot-all] quit  
[HUAWEI] interface gigabitethernet 1/0/0  
[HUAWEI-GigabitEthernet1/0/0] undo shutdown  
[HUAWEI-GigabitEthernet1/0/0] quit  
[HUAWEI] interface gigabitethernet 1/0/0.1  
[HUAWEI-GigabitEthernet1/0/0.1] trust upstream default  
[HUAWEI-GigabitEthernet1/0/0.1] trust 8021p  
[HUAWEI-GigabitEthernet1/0/0.1] vlan-type dot1q 1  
[HUAWEI-GigabitEthernet1/0/0.1] ip address 100.1.1.1 24  
[HUAWEI-GigabitEthernet1/0/0.1] user-queue cir 100000 pir 100000 flow-queue test1  
flow-mapping test1 user-group-queue test inbound service-template st1  
[HUAWEI-GigabitEthernet1/0/0.1] return  
[HUAWEI] interface gigabitethernet 1/0/0.2  
[HUAWEI-GigabitEthernet1/0/0.2] trust upstream default  
[HUAWEI-GigabitEthernet1/0/0.2] trust 8021p  
[HUAWEI-GigabitEthernet1/0/0.2] vlan-type dot1q 2  
[HUAWEI-GigabitEthernet1/0/0.2] ip address 200.1.2.1 24  
[HUAWEI-GigabitEthernet1/0/0.2] user-queue cir 200000 pir 200000 flow-queue test2  
flow-mapping test1 user-group-queue test inbound service-template st1  
[HUAWEI-GigabitEthernet1/0/0.2] return
```

After the preceding configuration, you can run the **display user-queue configuration interface** command to view the detailed HQoS configuration on the interface.

```
<HUAWEI> display user-queue configuration interface gigabitethernet 1/0/0.1 inbound  
user-queue configuration infomation show :  
GigabitEthernet1/0/0.1 Inbound:  
    CirValue<kbps>: 100000  
    PirValue<kbps>: 100000  
    FlowQueue: test1  
    FlowMapping: test1  
    GroupQueue: test  
    service-template: NULL  
<HUAWEI> display user-queue configuration interface gigabitethernet 1/0/0.2 inbound  
user-queue configuration infomation show :  
GigabitEthernet1/0/0.2 Inbound:  
    CirValue<kbps>: 200000  
    PirValue<kbps>: 200000
```

```
FlowQueue: test2
FlowMapping: test1
GroupQueue: test
service-template: NULL
```

Step 6 Configure a WRED object referenced by CQs.

```
# Configure the parameters of port-wred packet dropping referenced by CQs.
```

```
<HUAWEI> system view
[HUAWEI] port-wred test
[HUAWEI-port-wred-test] color green low-limit 70 high-limit 100 discard-percentage 100
[HUAWEI-port-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage 100
[HUAWEI-port-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-port-wred-test] return
```

After the preceding configuration, you can run the **display port-wred configuration verbose** command to view the configured parameters of the CQ WRED object.

```
<HUAWEI> display port-wred configuration verbose test
Port wred name : test
-----
Color      Low-limit      High-limit      Discard-percent
-----
green      70            100            100
yellow     60            90             100
red        50            80             100
Reference relationships : NULL
```

Step 7 Verify the configuration.

When packets are available in the network, you can find that packets of User1's AF1 and EF flows and User2's EF flow are forwarded at the guaranteed bandwidth.

Running the **display port-queue statistics** command on the downstream GE 2/0/0 of router, you can see that the packets of the CS7 flow increases rapidly.

```
<HUAWEI> display port-queue statistics interface gigabitethernet 2/0/0 ef outbound
[ef]
    Total pass:                      104,762,039 packets,          10,251,481,862 bytes
    Total discard:                   0 packets,                  0 bytes
    --Drop tail discard:           0 packets,                  0 bytes
    --Wred discard:                0 pps,                     0 bps
    Last 30 seconds pass rate:   0 pps,                     0 bps
    Last 30 seconds discard rate: 0 pps,                     0 bps
    --Drop tail discard rate:    0 pps,                     0 bps
    --Wred discard rate:         0 pps,                     0 bps
```

----End

Configuration Files

Configuration file of router

```
#  
sysname HUAWEI  
#
```

```
flow-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
flow-mapping test1
map flow-queue af1 to port-queue ef
#
flow-queue test1
queue af1 lpq shaping 10000 flow-wred test
queue ef pq shaping 30000 flow-wred test
#
flow-queue test2
queue ef pq shaping 25000 flow-wred test
#
user-group-queue test
shaping 500000 inbound
#
service-template st1
network-header-length 10 inbound
#
interface GigabitEthernet1/0/0
undo shutdown
#
interface GigabitEthernet1/0/0.1
trust upstream default
trust 8021p
vlan-type dot1q 1
ip address 100.1.1.1 255.255.255.0
user-queue cir 100000 pir 100000 flow-queue test1 flow-mapping test1 user-group-
queue test inbound service-template st1
#
interface GigabitEthernet1/0/0.2
trust upstream default
trust 8021p
vlan-type dot1q 2
ip address 200.1.2.1 255.255.255.0
user-queue cir 200000 pir 200000 flow-queue test2 flow-mapping test1 user-group-
queue test inbound service-template st1
#
port-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 200.1.1.1 255.255.255.0
port-queue ef pq shaping 100 port-wred test outbound
#
osfp 10
area 0.0.0.0
network 200.1.1.0 0.0.0.255
network 200.1.2.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#
return
```

10.10.2 Example for Configuring QinQ HQoS

This section provides an example for configuring HQoS on a sub-interface for QinQ VLAN tag termination.

Networking Requirements

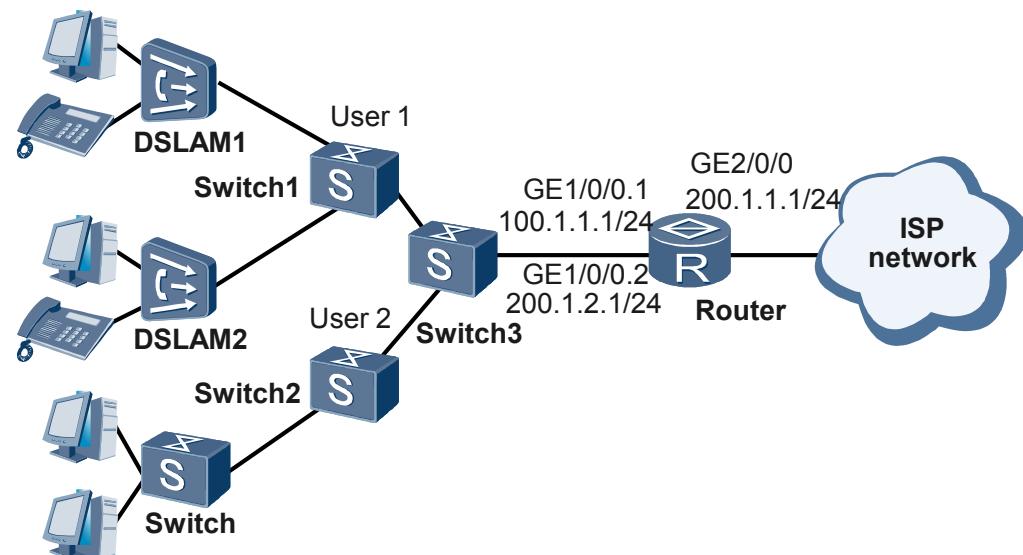
As shown in [Figure 10-9](#), router is an edge device of the backbone network. The router connects Layer 2 switches. User1 and User2 access the network through the VLAN group of the two QinQ

termination sub-interfaces GigabitEthernet1/0/0.1 and GigabitEthernet1/0/0.2 of router. User1 is guaranteed with a bandwidth of 100 Mbit/s; User2, 200 Mbit/s. The bandwidth of the EF flow of User1 is 30 Mbit/s; that of the AF1 flow, 10 Mbit/s. The bandwidth of the EF flow of User2 is 50 Mbit/s. User1 and User2 are in the same subscriber group. The bandwidth of the group queue is 500 Mbit/s. On the downstream interface of router, the traffic rate of CS7 flow is no more than 100 Mbit/s.

 **NOTE**

Home users carry out broadband access through home service gateways. A home service gateway adds VLAN tags to service packets of home users to identify the users' VLAN and the 802.1 priorities of services. According to the QinQ technology, DSLAM can also encapsulate an outer tag over a VLAN tag in a home user's packet. This makes it easy to manage internal VLAN users. For example, the inner VLAN tag marks a home user and the outer VLAN tag marks a cell; or the inner VLAN tag marks a cell and the outer VLAN tag marks a service. In this manner, home users' packets with two-layer VLAN tags are forwarded at Layer 2 through DSLAMs and switches. The VLAN tags are terminated on the sub-interface of router and then the packets go to the ISP network.

Figure 10-9 Networking diagram for configuring QinQ HQoS



Configuration Roadmap

The configuration roadmap is as follows:

1. Configuring parameters of packet dropping for flow queue WRED objects.
2. Configuring algorithms for flow queue scheduling and related parameters.
3. Configuring service class mappings from FQs to CQs.
4. Configuring values of GQ shaping.
5. Enabling QinQ on the master interface.
6. Creating and configuring QinQ sub-interfaces.
7. Creating VLAN groups.
8. Configuring SQs on the upstream interface of the PE1.

 NOTE

In this procedure, HQoS is configured only on a QinQ termination sub-interface. You do not need to configure upstream HQoS CQs. You can configure HQoS on the downstream interface of a router or configure only CQs according to the actual network traffic to prevent network congestion.

Data Preparation

To complete the configuration, you need the following data:

- QinQ termination sub-interface numbers and vlan-group IDs
- Parameters of flow-wred packet dropping
- Algorithms for flow-queue scheduling and related parameters
- Service class mappings for flow-mapping
- Value of user-group-queue shaping
- Values of user-queue CIR and PIR

Procedure

Step 1 Configure a WRED object referenced by a flow queue.

Configure parameters of flow-wred packet dropping.

```
<HUAWEI> system view
[HUAWEI] flow-wred test
[HUAWEI-flow-wred-test] color green low-limit 70 high-limit 100 discard-percentage
100
[HUAWEI-flow-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage
100
[HUAWEI-flow-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-flow-wred-test] return
```

After the preceding configuration, you can run the **display flow-wred configuration verbose** command to view the configured parameters of the FQ WRED object.

```
<HUAWEI> display flow-wred configuration verbose test
flow-wred-name : test
-----
color      low-limit    high-limit   discard-percent
-----
green      70           100          100
yellow     60           90           100
red        50           80           100
Queue Depth : 1000
Reference relationships : test
```

Step 2 Configure algorithms for flow queue scheduling and related parameters.

Configure the scheduling algorithms, WRED parameters, and shaping values for FQs.

```
<HUAWEI> system view
[HUAWEI] flow-queue test1
[HUAWEI-flow-queue-template-test] queue af1 lpq flow-wred test shaping 10000
[HUAWEI-flow-queue-template-test] queue ef pq flow-wred test shaping 30000
[HUAWEI-flow-queue-template-test] quit
[HUAWEI] flow-queue test2
[HUAWEI-flow-queue-template-test] queue ef pq flow-wred test shaping 25000
[HUAWEI-flow-queue-template-test] return
```

After the preceding configuration, you can run the **display flow-queue configuration verbose** command to view the configuration of the FQ template.

```
<HUAWEI> display flow-queue configuration verbose test1
```

```

Codes: Arith(Schedule algorithm)
       U-Weight(Schedule weight configured by users)
       I-Weight(Inverse schedule weight used by TM)
       A-Weight(Actual schedule weight obtained by users)
       Shp(Shaping value, the percentage of subscriber queue's PIR)
       Drop-Arith(The name of the WRED object used by the flow queue)

```

```
Flow Queue Template : test1
-----
Cos  Arith   U-Weight  I-Weight  A-Weight  Shp      Pct  Drop-Arith
-----
```

Cos	Arith	U-Weight	I-Weight	A-Weight	Shp	Pct	Drop-Arith
be	wfq	10	3	10.00	-	-	Tail Drop
af1	lpq	-	-	-	10000	-	test
af2	wfq	10	3	10.00	-	-	Tail Drop
af3	wfq	15	2	15.00	-	-	Tail Drop
af4	wfq	15	2	15.00	-	-	Tail Drop
ef	pq	-	-	-	30000	-	test
cs6	pq	-	-	-	-	-	Tail Drop
cs7	pq	-	-	-	-	-	Tail Drop

Reference relationships : NULL

<HUAWEI> **display flow-queue configuration verbose test2**

```

Codes: Arith(Schedule algorithm)
       U-Weight(Schedule weight configured by users)
       I-Weight(Inverse schedule weight used by TM)
       A-Weight(Actual schedule weight obtained by users)
       Shp(Shaping value, the percentage of subscriber queue's PIR)
       Drop-Arith(The name of the WRED object used by the flow queue)

```

```
Flow Queue Template : test2
-----
Cos  Arith   U-Weight  I-Weight  A-Weight  Shp      Pct  Drop-Arith
-----
```

Cos	Arith	U-Weight	I-Weight	A-Weight	Shp	Pct	Drop-Arith
be	wfq	10	3	10.00	-	-	Tail Drop
af1	wfq	10	3	10.00	-	-	Tail Drop
af2	wfq	10	3	10.00	-	-	Tail Drop
af3	wfq	15	2	15.00	-	-	Tail Drop
af4	wfq	15	2	15.00	-	-	Tail Drop
ef	pq	-	-	-	25000	-	test
cs6	pq	-	-	-	-	-	Tail Drop
cs7	pq	-	-	-	-	-	Tail Drop

Reference relationships : NULL

Step 3 Configure service class mappings from FQs to CQs.

```

<HUAWEI> system view
[HUAWEI] flow-mapping test1
[HUAWEI-flow-mapping-test1] map flow-queue af1 to port-queue ef
[HUAWEI-flow-mapping-test1] quit

```

After the preceding configuration, you can run the **display flow-mapping configuration verbose** command to view the configured parameters of the FQ mapping objects and the referential relations of the objects.

```

<HUAWEI> display flow-mapping configuration verbose test1
flow-mapping-name : test1
fq-cosvalue to pq-cosvalue
be          to be
af1         to ef
af2         to af2
af3         to af3
af4         to af4
ef          to ef
cs6         to cs6
cs7         to cs7
[reference relationship]
NULL

```

Step 4 Configure a value of a GQ shaping.

```
# Configure user-group-queue

<HUAWEI> system view
[HUAWEI] user-group-queue test
[HUAWEI-user-group-queue-test-slot-all] shaping 500000 inbound
[HUAWEI-user-group-queue-test-slot-all] return
```

After the preceding configuration, you can run the **display user-group-queue configuration verbose** command to view the configuration of the GQ and the referential relations.

```
<HUAWEI> display user-group-queue configuration verbose test
user-group-queue-name : test
slot : 3
[current configuration]
inbound
shaping-value <kbps> : 500000
pbs-value <byte> : 524288
outbound
shaping-value <kbps> : NA
pbs-value <byte> : NA
[reference relationship]
NULL
[unsuccessful slot]
NULL
```

Step 5 Configure the master interface to enable the user termination mode.

```
# Configure the user termination mode.
```

```
[HUAWEI] interface gigabitethernet 1/0/0
[HUAWEI-GigabitEthernet1/0/0] undo shutdown
[HUAWEI-GigabitEthernet1/0/0] mode user-termination
[HUAWEI-GigabitEthernet1/0/0] quit
```

Step 6 Create QinQ termination sub-interfaces and configure QinQ termination.

```
[HUAWEI] interface gigabitethernet 1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] control-vid 1 qinq-termination
[HUAWEI-GigabitEthernet1/0/0.1] vlan-group 1
[HUAWEI-GigabitEthernet1/0/0.1] qinq termination pe-vid 100 ce-vid 600 vlan-group 1
[HUAWEI] interface gigabitethernet 1/0/0.2
[HUAWEI-GigabitEthernet1/0/0.2] control-vid 2 qinq-termination
[HUAWEI-GigabitEthernet1/0/0.2] vlan-group 1
[HUAWEI-GigabitEthernet1/0/0.2] qinq termination pe-vid 100 ce-vid 700 vlan-group 1
```

Step 7 Create a VLAN group and configure SQs of the VLAN group.

```
<HUAWEI> system view
[HUAWEI] interface gigabitethernet 1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] trust upstream default
[HUAWEI-GigabitEthernet1/0/0.1] ip address 100.1.1.1 24
[HUAWEI-GigabitEthernet1/0/0.1] vlan-group 1
[HUAWEI-GigabitEthernet1/0/0.1-vlangroup1] user-queue cir 100000 pir 100000 flow-
queue test1 flow-mapping test1 user-group-queue test inbound
[HUAWEI-GigabitEthernet1/0/0.1-vlangroup1] quit
[HUAWEI-GigabitEthernet1/0/0.1] quit
[HUAWEI] interface gigabitethernet 1/0/0.2
[HUAWEI-GigabitEthernet1/0/0.2] trust upstream default
[HUAWEI-GigabitEthernet1/0/0.2] ip address 200.1.1.1 24
[HUAWEI-GigabitEthernet1/0/0.2] vlan-group 1
[HUAWEI-GigabitEthernet1/0/0.2-vlangroup1] user-queue cir 200000 pir 200000 flow-
queue test2 flow-mapping test1 user-group-queue test inbound
[HUAWEI-GigabitEthernet1/0/0.2-vlangroup1] quit
[HUAWEI-GigabitEthernet1/0/0.1] return
```

Step 8 Verify the configuration.

When packets are available in the network, you can find that packets of User1's AF1 and EF flows and User2's EF flow are forwarded at the guaranteed bandwidth.

Running the **display port-queue statistics** command on the downstream GE 2/0/0 of router, you can see that the packets of the CS7 flow increases rapidly.

```
<HUAWEI> display port-queue statistics interface gigabitethernet 2/0/0 ef outbound
[ef]
    Total pass:                                104,762,039 packets,          10,251,481,862 bytes
    Total discard:                             0 packets,                  0 bytes
    --Drop tail discard:                      0 packets,                  0 bytes
    --Wred discard:                           0 pps,                     0 bps
    Last 30 seconds pass rate:                0 pps,                     0 bps
    Last 30 seconds discard rate:             0 pps,                     0 bps
    --Drop tail discard rate:                 0 pps,                     0 bps
    --Wred discard rate:                     0 pps,                     0 bps
```

----End

Configuration File

Configuration file of router:

```
#  
sysname HUAWEI  
#  
flow-wred test  
    color green low-limit 70 high-limit 100 discard-percentage 100  
    color yellow low-limit 60 high-limit 90 discard-percentage 100  
    color red low-limit 50 high-limit 80 discard-percentage 100  
flow-mapping test1  
    map flow-queue af1 to port-queue ef  
#  
flow-queue test1  
    queue af1 lpq shaping 10000 flow-wred test  
    queue ef pq shaping 30000 flow-wred test  
#  
flow-queue test2  
    queue ef pq shaping 25000 flow-wred test  
#  
user-group-queue test  
    shaping 500000 inbound  
#  
interface GigabitEthernet1/0/0  
    undo shutdown  
    mode user-termination  
#  
interface GigabitEthernet1/0/0.1  
    control-vid 1 qinq-termination  
    vlan-group 1  
        user-queue cir 100000 pir 100000 flow-queue test1 flow-mapping test1 user-group-  
queue test inbound  
        qinq termination pe-vid 100 ce-vid 600 vlan-group 1  
        ip address 100.1.1.1 255.255.255.0  
        trust upstream default  
#  
interface GigabitEthernet1/0/0.2  
    control-vid 2 qinq-termination  
    vlan-group 1  
        user-queue cir 200000 pir 200000 flow-queue test2 flow-mapping test1 user-group-  
queue test inbound  
        qinq termination pe-vid 100 ce-vid 700 vlan-group  
        ip address 200.1.2.1 255.255.255.0
```

```
trust upstream default
#
interface GigabitEthernet2/0/0
  undo shutdown
  ip address 200.1.1.1 255.255.255.0
#
osfp 10
  area 0.0.0.0
  network 200.1.1.0 0.0.0.255
  network 200.1.2.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
return
```

10.10.3 Example for Configuring Class-based HQoS

This section provides an example for configuring class-based HQoS to identify users based on the source IP addresses of user packets.

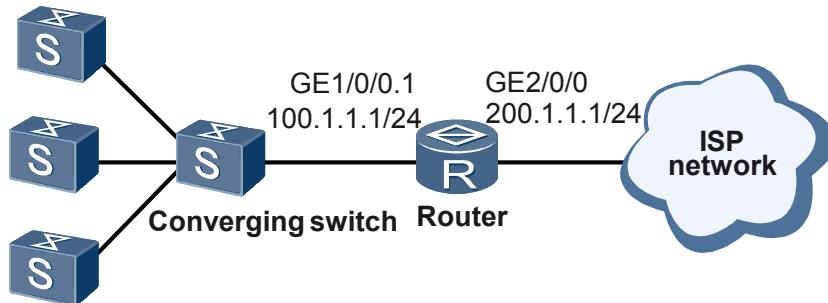
Networking Requirements

As shown in **Figure 10-10**, packets of multiple VLANs are converged on the converging switch. GE 1/0/1 admits packets of VLANs 1 to 1000. Configure the sub-interface for dot1q termination and class-based HQoS on GE 1/0/0.1. Packets are identified based on their source IP addresses. Totally there are 10 users; the Committed Information Rate (CIR) of each user is 10 Mbit/s and the Peak Information Rate (PIR), 100 Mbit/s. The 10 users share the total bandwidth of 100 Mbit/s.

 **NOTE**

The following example is about the configuration of the router only.

Figure 10-10 Networking diagram for configuring class-based HQoS



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a dot1q termination sub-interface on GE 1/0/0.1 of the router.
2. Configure traffic classifiers.
3. Configure packet drop parameters for flow-wred objects.
4. Configure scheduling algorithms and parameters for FQs.

5. Configure CoS mappings between FQs and CQs.
6. Configure shaping values for GQs.
7. Configure SQs in traffic behaviors.
8. Configure traffic policies and apply them to GE 1/0/0.1.
9. Configure packet drop parameters for port-wred objects.
10. Configure CQs on downstream GE 2/0/0 of the router.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the 10 users: from 10.110.1.0/24 to 10.110.10.0/24
- Control VLAN ID of the dot1q termination sub-interface
- Flow-wred drop parameters
- Algorithms of flow-queue scheduling and related parameters
- Flow-mapping of CoS
- Shaping values of user-group-queue
- Values of user-queue CIR, and PIR. CIR and PIR of each user: 10 Mbit/s and 100 Mbit/s
- Port-wred parameters used in port-queue
- Algorithms of port-queue scheduling and related parameters, and shaping values

Procedure

Step 1 Configure the sub-interface for dot1q termination.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/0
[HUAWEI-GigabitEthernet1/0/0] undo shutdown
[HUAWEI-GigabitEthernet1/0/0] mode user-termination
[HUAWEI-GigabitEthernet1/0/0] quit
[HUAWEI] interface gigabitethernet 1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] control-vid 1 dot1q-termination
[HUAWEI-GigabitEthernet1/0/0.1] dot1q termination vid 1 to 1000
[HUAWEI-GigabitEthernet1/0/0.1] ip address 100.1.1.1 24
[HUAWEI-GigabitEthernet1/0/0.1] trust upstream default
[HUAWEI-GigabitEthernet1/0/0.1] trust 8021p
[HUAWEI-GigabitEthernet1/0/0.1] quit
```

Step 2 Configure classifiers to identify the 10 users to be applied with class-based HQoS.

Configure the classifier c1.

```
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule permit ip source 10.110.1.0 0.0.0.255
[HUAWEI-acl-adv-3000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 3000
[HUAWEI-classifier-c1] quit
```

Configure the classifier c2.

```
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit ip source 10.110.2.0 0.0.0.255
[HUAWEI-acl-adv-3001] quit
[HUAWEI] traffic classifier c2
[HUAWEI-classifier-c2] if-match acl 3001
[HUAWEI-classifier-c2] quit
```

The configurations of the classifiers **c3** to **c10** are similar to that of **c1**, and therefore, are not mentioned.

Step 3 Configure a flow-wred object.

```
[HUAWEI] flow-wred test
[HUAWEI-flow-wred-test] color green low-limit 70 high-limit 100 discard-percentage
100
[HUAWEI-flow-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage
100
[HUAWEI-flow-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-flow-wred-test] quit
```

Step 4 Configure scheduling algorithms and parameters for FQs.

```
[HUAWEI] flow-queue test
[HUAWEI-flow-queue-template-test] queue af1 lpq flow-wred test shaping 1000
[HUAWEI-flow-queue-template-test] queue ef pq flow-wred test shaping 3000
[HUAWEI-flow-queue-template-test] quit
```

Step 5 Configure CoS mappings from FQs to CQs.

```
[HUAWEI] flow-mapping test
[HUAWEI-flow-mapping-test] map flow-queue af1 to port-queue ef
[HUAWEI-flow-mapping-test] quit
```

Step 6 Configure shaping values for GQs.

```
[HUAWEI] user-group-queue test
[HUAWEI-user-group-queue-test-slot-all] shaping 100000 inbound
[HUAWEI-user-group-queue-test-slot-all] quit
```

Step 7 Configure traffic behaviors, that is, the SQ scheduling parameters of the 10 users.

Configure the behavior **b1**.

```
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] user-queue cir 10000 pir 100000 flow-queue test flow-mapping
test user-group-queue test
[HUAWEI-behavior-b1] quit
```

Configure the behavior **b2**.

```
[HUAWEI] traffic behavior b2
[HUAWEI-behavior-b2] user-queue cir 10000 pir 100000 flow-queue test flow-mapping
test user-group-queue test
[HUAWEI-behavior-b2] quit
```

The configurations of the behaviors **b3** to **b10** are similar to that of **b1**, and therefore are not mentioned.

 **NOTE**

You need to configure traffic behaviors one by one for the 10 users even though the HQoS scheduling parameters of the 10 users are the same. Otherwise, the system considers that all packets that match any of the 10 traffic classifiers correspond to one user, by default.

Step 8 Configure a traffic policy and apply it to GE 1/0/0.1.

```
[HUAWEI] traffic policy p
[HUAWEI-trafficpolicy-p] share-mode
[HUAWEI-trafficpolicy-p] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p] classifier c2 behavior b2
[HUAWEI-trafficpolicy-p] classifier c3 behavior b3
[HUAWEI-trafficpolicy-p] classifier c4 behavior b4
[HUAWEI-trafficpolicy-p] classifier c5 behavior b5
[HUAWEI-trafficpolicy-p] classifier c6 behavior b6
[HUAWEI-trafficpolicy-p] classifier c7 behavior b7
[HUAWEI-trafficpolicy-p] classifier c8 behavior b8
[HUAWEI-trafficpolicy-p] classifier c9 behavior b9
[HUAWEI-trafficpolicy-p] classifier c10 behavior b10
```

```
[HUAWEI-trafficpolicy-p] quit
[HUAWEI] interface gigabitethernet 1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] traffic-policy P inbound
[HUAWEI-GigabitEthernet1/0/0.1] quit
```

Step 9 Configure CQs.

Configure a port-wred object.

```
[HUAWEI] port-wred test
[HUAWEI-port-wred-test] color green low-limit 70 high-limit 100 discard-percentage 100
[HUAWEI-port-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage 100
[HUAWEI-port-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-port-wred-test] quit
```

Configure the scheduling algorithms, WRED parameters, and shaping values for CQs.

```
[HUAWEI] interface gigabitethernet 2/0/0
[HUAWEI-GigabitEthernet2/0/0] undo shutdown
[HUAWEI-GigabitEthernet2/0/0] port-queue ef pq shaping 100 port-wred test outbound
[HUAWEI-GigabitEthernet2/0/0] return
```

Step 10 Verify the configuration.

Run the **display traffic classifier user-defined classifier-name** command. You can view the configuration of a classifier.

```
<HUAWEI> display traffic classifier user-defined cl
User Defined Classifier Information:
  Classifier: cl
  Operator: OR
Rule(s) : if-match acl 3000
```

Run the **display traffic behavior user-defined behavior-name** command. You can view the configuration of a traffic behavior.

```
<HUAWEI> display traffic behavior user-defined b1
User Defined Behavior Information:
  Behavior: b1
  User-queue:
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test network-
header-length default user-group-queue test
```

Run the **display user-queue statistics** command. You can view the statistics on an SQ.

```
<HUAWEI> display user-queue statistics interface gigabitethernet 1/0/0.1 inbound
GigabitEthernet1/0/0.1 inbound traffic statistics:
[be]
  Pass: 0 packets, 0 bytes
  Discard: 0 packets, 0 bytes
  Last 5 minutes pass rate: 0 pps, 0 bps
  Last 5 minutes discard rate: 0 pps, 0 bps
[af1]
  Pass: 193385 packets, 18951730 bytes
  Discard: 3876689 packets, 399298967 bytes
  Last 5 minutes pass rate: 0 pps, 0 bps
  Last 5 minutes discard rate: 0 pps, 0 bps
[af2]
  Pass: 0 packets, 0 bytes
  Discard: 0 packets, 0 bytes
  Last 5 minutes pass rate: 0 pps, 0 bps
  Last 5 minutes discard rate: 0 pps, 0 bps
```

[af3]	0 pps,	0 bps
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[af4]	0 pps,	0 bps
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[ef]	0 pps,	0 bps
Pass:	581216 packets,	56959168 bytes
Discard:	3490089 packets,	359479167 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[cs6]	0 pps,	0 bps
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[cs7]	0 pps,	0 bps
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps
[total]	0 pps,	0 bps
Pass:	774601 packets,	75910898 bytes
Discard:	7366778 packets,	758778134 bytes
Last 5 minutes pass rate:	0 pps,	0 bps
Last 5 minutes discard rate:	0 pps,	0 bps

Run the **display port-queue statistics** command on GE 2/0/0. You can view the port-queue statistics. Because the CoS AF1 is mapped to EF, no packets with the CoS AF1 are in the CQ on the interface; meanwhile, the number of EF packets increases greatly.

```
<HUAWEI> display port-queue statistics interface gigabitethernet 2/0/0 outbound
GigabitEthernet2/0/2 outbound traffic statistics:
[be]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 30 seconds pass rate: 0 pps, 0 bps
Last 30 seconds discard rate: 0 pps, 0 bps
[af1]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 30 seconds pass rate: 0 pps, 0 bps
Last 30 seconds discard rate: 0 pps, 0 bps
[af2]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 30 seconds pass rate: 0 pps, 0 bps
```

Last 30 seconds discard rate:	0 pps,	0 bps
[af3]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
[af4]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
[ef]		
Pass:	60,716,995 packets,	5,707,379,530 bytes
Discard:	0 packets,	0 bytes
Last 30 seconds pass rate:	99,534 pps,	93,561,596 bps
Last 30 seconds discard rate:	0 pps,	0 bps
[cs6]		
Pass:	257 packets,	18,504 bytes
Discard:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps
[cs7]		
Pass:	0 packets,	0 bytes
Discard:	0 packets,	0 bytes
Last 30 seconds pass rate:	0 pps,	0 bps
Last 30 seconds discard rate:	0 pps,	0 bps

----End

Configuration Files

```

#
Sysname HUAWEI
#
acl number 3000
rule 5 permit ip source 10.110.1.0 0.0.0.255
#
acl number 3001
rule 5 permit ip source 10.110.2.0 0.0.0.255
#
acl number 3002
rule 5 permit ip source 10.110.3.0 0.0.0.255
#
acl number 3003
rule 5 permit ip source 10.110.4.0 0.0.0.255
#
acl number 3004
rule 5 permit ip source 10.110.5.0 0.0.0.255
#
acl number 3005
rule 5 permit ip source 10.110.6.0 0.0.0.255
#
acl number 3006
rule 5 permit ip source 10.110.7.0 0.0.0.255
#
acl number 3007
rule 5 permit ip source 10.110.8.0 0.0.0.255
#

```

```
acl number 3008
    rule 5 permit ip source 10.110.9.0 0.0.0.255
#
acl number 3009
    rule 5 permit ip source 10.110.10.0 0.0.0.255
#
port-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
flow-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
flow-mapping test1
    map flow-queue afl to port-queue ef
#
flow-queue test1
    queue afl lpq shaping 1000 flow-wred test
    queue ef pq shaping 3000 flow-wred test
#
user-group-queue group
    shaping 100000 inbound
#
traffic classifier c1 operator or
    if-match acl 3000
traffic classifier c2 operator or
    if-match acl 3001
traffic classifier c3 operator or
    if-match acl 3002
traffic classifier c4 operator or
    if-match acl 3003
traffic classifier c5 operator or
    if-match acl 3004
traffic classifier c6 operator or
    if-match acl 3005
traffic classifier c7 operator or
    if-match acl 3006
traffic classifier c8 operator or
    if-match acl 3007
traffic classifier c9 operator or
    if-match acl 3008
traffic classifier c10 operator or
    if-match acl 3009
#
traffic behavior b1
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b2
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b3
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b4
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b5
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b6
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b7
    user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b8
```

```
user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b9
user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
traffic behavior b10
user-queue cir 10000 pir 100000 flow-queue test flow-mapping test user-group-queue
test
#
traffic policy p
share-mode
classifier c1 behavior b1
classifier c2 behavior b2
classifier c3 behavior b3
classifier c4 behavior b4
classifier c5 behavior b5
classifier c6 behavior b6
classifier c7 behavior b7
classifier c8 behavior b8
classifier c9 behavior b9
classifier c10 behavior b10
#
diffserv domain default
#
interface GigabitEthernet1/0/0
undo shutdown
mode user-termination
#
interface GigabitEthernet1/0/0.1
control-vid 1 dot1q-termination
dot1q termination vid 1 to 1000
ip address 100.1.1.1 24
traffic-policy P inbound
trust upstream default
trust 8021p
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 200.1.1.1 255.255.255.0
port-queue ef pq shaping 100 port-wred test outbound
#
Ospf 10
area 0.0.0.0
network 200.1.1.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#
return
```

10.10.4 Example for Configuring Profile-based HQoS

This section provides an example for configuring profile-based HQoS so that service traffic of different types are transmitted through different sub-interfaces.

Networking Requirements

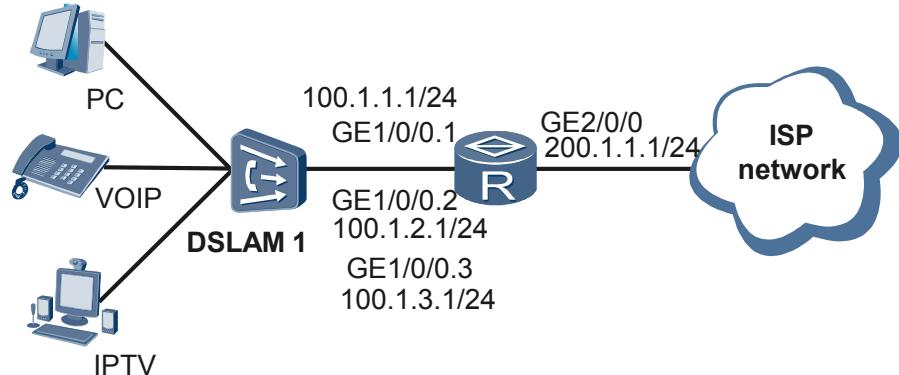
As shown in [Figure 10-11](#), users need to access the router through the DSLAM. The router functions as the access device of the backbone network.

Three types of services of the users are to be mapped to three PVCs of the DSLAM. The traffic flows of the same user access the router through sub-interfaces GE 1/0/0.1, GE 1/0/0.2, and GE 1/0/0.3 respectively, with different types of traffic flowing through different sub-interfaces.

When reaching the router, traffic flows carry double tags. The inner tag indicates the user, and the outer tag indicates the service type. Uniform scheduling of user traffic needs to be implemented with 100 Mbit/s assured bandwidth. The bandwidth for EF flows should be 20 Mbit/s, and the bandwidth for AF1 flows should be 10 Mbit/s. The bandwidth for the user group

to which the users belong should be 500 Mbit/s. On the downstream interface of the router, the traffic rate of EF flows should not be higher than 120 Mbit/s.

Figure 10-11 Networking diagram of profile-based HQoS



Service Name	Inner VLAN Tag	Outer VLAN Tag
PC	1	1 - 100
VOIP	2	1 - 100
IPTV	3	1 - 100

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure packet drop parameters for flow WRED objects.
2. Configure scheduling algorithms and parameters for the flow queues.
3. Configure CoS mappings between flow queues and class queues.
4. Configure the shaping value for the user group queues.
5. Configure the length for packet loss compensation of the service profile.
6. Configure scheduling parameters and the CIR value of the user queues.
7. Configure packet drop parameters for class WRED objects.
8. Configure class queues on the downstream interface of the access router.

Data Preparation

To complete the configuration, you need the following data:

- Packet drop parameters for flow-wred
- Algorithms of flow-queue scheduling and related parameters
- Flow-mapping of CoS
- Shaping value for user group queues
- Values of CIR, PIR, and network-header-length in the **user-queue** command in the QoS profile
- Interface to which the QoS profile is applied
- Port-wred parameters that are referenced by port-queue

- Algorithms, related parameters, and shaping values for port-queue scheduling

Procedure

Step 1 Configure a WRED object referenced by a flow queue.

Configure packet dropping parameters of flow-wred.

```
<HUAWEI> system view
[HUAWEI] flow-wred test
[HUAWEI-flow-wred-test] color green low-limit 70 high-limit 100 discard-percentage
100
[HUAWEI-flow-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage
100
[HUAWEI-flow-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-flow-wred-test] return
```

After the preceding configuration, you can run the **display flow-wred configuration verbose** command to view the configured parameters of the flow WRED object.

```
<HUAWEI> display flow-wred configuration verbose test
flow-wred-name : test
-----
color    low-limit    high-limit    discard-percent
-----
green      70          100          100
yellow     60          90          100
red        50          80          100
Queue Depth : 1000
Reference relationships : NULL
```

Step 2 Configure scheduling algorithms and parameters for flow queues.

Configure the scheduling algorithms, WRED parameters, and shaping values for flow queues.

```
<HUAWEI> system view
[HUAWEI] flow-queue test
[HUAWEI-flow-queue-template-test] queue af1 lpq flow-wred test shaping 10000
[HUAWEI-flow-queue-template-test] queue ef pq flow-wred test shaping 30000
```

After the preceding configuration, you can run the **display flow-queue configuration verbose** command to view the configurations of the flow queue profile.

```
<HUAWEI> display flow-queue configuration verbose test
Codes: Arith(Schedule algorithm)
       U-Weight(Schedule weight configured by users)
       I-Weight(Inverse schedule weight used by TM)
       A-Weight(Actual schedule weight obtained by users)
       Shp(Shaping value, the percentage of subscriber queue's PIR)
       Drop-Arith(The name of the WRED object used by the flow queue)
```

```
Flow Queue Template : test
-----
Cos  Arith   U-Weight   I-Weight   A-Weight   Shp      Pct   Drop-Arith
-----
be   wfq     10         3          10.00     -        -      Tail Drop
af1  lpq     -          -          -          10000   -      test
af2  wfq     10         3          10.00     -        -      Tail Drop
af3  wfq     15         2          15.00     -        -      Tail Drop
af4  wfq     15         2          15.00     -        -      Tail Drop
ef   pq      -          -          -          30000   -      test
cs6  pq      -          -          -          -        -      Tail Drop
cs7  pq      -          -          -          -        -      Tail Drop
Reference relationships : NULL
```

Step 3 Configure CoS mappings between flow queues and class queues.

```
<HUAWEI> system view
[HUAWEI] flow-mapping test
[HUAWEI-flow-mapping-test] map flow-queue af1 to port-queue ef
[HUAWEI-flow-mapping-test] return
```

After the preceding configuration, run the **display flow-mapping configuration verbose** command to view the configured parameters of the flow queue mapping object and the referential relationships of the object.

```
<HUAWEI> display flow-mapping configuration verbose test
flow-mapping-name : test
fq-cosvalue to pq-cosvalue
be to be
af1 to ef
af2 to af2
af3 to af3
af4 to af4
ef to ef
cs6 to cs6
cs7 to cs7
[reference relationship]
NULL
```

Step 4 Configure the shaping value for user group queues.

```
<HUAWEI> system view
[HUAWEI] user-group-queue test
[HUAWEI-user-group-queue-test-slot-all] shaping 500000 inbound
[HUAWEI-user-group-queue-test-slot-all] return
```

After the preceding configuration, run the **display user-group-queue configuration verbose** command to view the configurations and the referential relationships of the user group queue.

```
<HUAWEI> display user-group-queue configuration verbose test
user-group-queue-name : test
slot : 3
[current configuration]
inbound
shaping-value <kbps> : 500000
pbs-value <byte> : 524288
outbound
shaping-value <kbps> : NA
pbs-value <byte> : NA
[reference relationship]
NULL
[unsuccessful slot]
NULL
```

Step 5 Configure the length for packet loss compensation of the service profile.

Configure the service profile and network-header-length.

```
<HUAWEI> system view
[HUAWEI] service-template test
[HUAWEI-service-template-test-slot-all] network-header-length 12 inbound
[HUAWEI-service-template-test-slot-all] quit
```

After the preceding configuration, you can run the **display service-template configuration verbose** command to view the configurations of the service profile, the value of network-header-length, and the referential relationships of the service profile.

```
<HUAWEI> display service-template configuration verbose
[service-template detail information] total number : 1 slot all      : 1
service-template-name : test slot : all [current configuration] inbound network-
header-length: 12
outbound network-header-length: NA
```

```
[reference relationship] NULL
```

Step 6 Configure scheduling parameters in the QoS profile and apply the parameters to interfaces.

```
# Configure scheduling parameters for user-queue and suppression rate of broadcast packets in the QoS profile.
```

```
<HUAWEI> system view
[HUAWEI] qos-profile test
[HUAWEI-qos-profile-test] user-queue cir 100000 flow-queue test flow-mapping test
user-group-queue test service-template test
```

```
# Configure the master interface to enable the user termination mode.
```

```
[HUAWEI] interface gigabitethernet 1/0/0
[HUAWEI-GigabitEthernet1/0/0] undo shutdown
[HUAWEI-GigabitEthernet1/0/0] mode user-termination
[HUAWEI-GigabitEthernet1/0/0] quit
```

```
# Create QinQ termination sub-interfaces and configure QinQ termination. Then apply the QoS profile to GE 1/0/0.1, GE 1/0/0.2, and GE 1/0/0.3.
```

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/0.1
[HUAWEI-GigabitEthernet1/0/0.1] control-vid 1 qinq-termination
[HUAWEI-GigabitEthernet1/0/0.1] qinq termination pe-vid 1 ce-vid 1 to 100
[HUAWEI-GigabitEthernet1/0/0.1] ip address 100.1.1.1 24
[HUAWEI-GigabitEthernet1/0/0.1] qos-profile test inbound pe-vid 1 ce-vid 1 to 100
group group1
[HUAWEI-GigabitEthernet1/0/0.1] quit
[HUAWEI] interface gigabitethernet 1/0/0.2
[HUAWEI-GigabitEthernet1/0/0.2] control-vid 2 qinq-termination
[HUAWEI-GigabitEthernet1/0/0.2] qinq termination pe-vid 2 ce-vid 1 to 100
[HUAWEI-GigabitEthernet1/0/0.2] ip address 100.1.2.1 24
[HUAWEI-GigabitEthernet1/0/0.2] qos-profile test inbound pe-vid 2 ce-vid 1 to 100
group group1
[HUAWEI-GigabitEthernet1/0/0.2] quit
[HUAWEI] interface gigabitethernet 1/0/0.3
[HUAWEI-GigabitEthernet1/0/0.3] control-vid 3 qinq-termination
[HUAWEI-GigabitEthernet1/0/0.3] qinq termination pe-vid 3 ce-vid 1 to 100
[HUAWEI-GigabitEthernet1/0/0.3] ip address 100.1.3.1 24
[HUAWEI-GigabitEthernet1/0/0.3] qos-profile test inbound pe-vid 3 ce-vid 1 to 100
group group1
[HUAWEI-GigabitEthernet1/0/0.3] quit
```

After the preceding configuration, you can run the **display qos-profile configuration test** and **display qos-profile application test group group1 slot 1 inbound** commands to view the configurations of the QoS profile and its applications.

```
<HUAWEI> display qos-profile configuration test
qos-profile : test
inbound :
outbound :
both :
    user-queue cir 100000 pir 100000 flow-queue test flow-mapping test user-group-
queue test service-template test
        Reference relationship:
        GigabitEthernet1/0/0.1
        GigabitEthernet1/0/0.2
        GigabitEthernet1/0/0.3
<HUAWEI> display qos-profile application test group group1 slot 1 inbound
qos-profile test + group group1:
    interface GigabitEthernet1/0/0.1, pe-vid 1, ce-vid 1 to 100
    interface GigabitEthernet1/0/0.2, pe-vid 2, ce-vid 1 to 100
    interface GigabitEthernet1/0/0.3, pe-vid 3, ce-vid 1 to 100
```

You can run the **display qos-profile statistics interface gigabitethernet1/0/0.1 pe-vid 1 ce-vid 1 inbound** command to view statistics about the QoS profile on GE 1/0/0.1.

```
<HUAWEI> display qos-profile statistics interface gigabitethernet1/0/0.1 pe-vid 1
ce-vid 1 inbound
GigabitEthernet1/0/0.1 pe-vid 1 ce-vid 1 inbound traffic statistics:
[be]
Pass: 38,226,678 packets, 3,784,441,122 bytes
Discard: 183,848,703 packets, 18,201,021,597 bytes
Last 5 minutes pass rate: 112,576 pps, 89,160,656 bps
Last 5 minutes discard rate: 223,089 pps, 176,686,608 bps
[af1]
Pass: 9,940,098 packets, 984,069,702 bytes
Discard: 721,620,432 packets, 71,440,422,768 bytes
Last 5 minutes pass rate: 11,962 pps, 9,474,208 bps
Last 5 minutes discard rate: 323,664 pps, 256,341,960 bps
[af2]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af3]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[af4]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[ef]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs6]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[cs7]
Pass: 0 packets, 0 bytes
Discard: 0 packets, 0 bytes
Last 5 minutes pass rate: 0 pps, 0 bps
Last 5 minutes discard rate: 0 pps, 0 bps
[total]
Pass: 48,166,776 packets, 4,768,510,824 bytes
Discard: 905,469,135 packets, 89,641,444,365 bytes
Last 5 minutes pass rate: 124,538 pps, 98,634,864 bps
Last 5 minutes discard rate: 546,753 pps, 433,028,568 bps
```

Step 7 Configure a WRED object referenced by the class queue.

Configure the port-wred packet dropping parameters referenced by the class queue.

```
<HUAWEI> system view
[HUAWEI] port-wred test
[HUAWEI-port-wred-test] color green low-limit 70 high-limit 100 discard-percentage
100
[HUAWEI-port-wred-test] color yellow low-limit 60 high-limit 90 discard-percentage
100
[HUAWEI-port-wred-test] color red low-limit 50 high-limit 80 discard-percentage 100
[HUAWEI-port-wred-test] return
```

After the preceding configuration, you can run the **display port-wred configuration verbose** command to view the configurations of the class WRED object.

```
<HUAWEI> display port-wred configuration verbose test
Port wred name : test
-----
Color Low-limit High-limit Discard-percent
-----
green 70 100 100
yellow 60 90 100
red 50 80 100
Reference relationships : NULL
```

Step 8 Configure a class queue.

Configure the scheduling algorithms, WRED parameters, and shaping values for port-queue.

```
<HUAWEI> system view
[HUAWEI] interface gigabitethernet 2/0/0
[HUAWEI-GigabitEthernet2/0/0] undo shutdown
[HUAWEI-GigabitEthernet2/0/0] port-queue ef pq shaping 100 port-wred test outbound
[HUAWEI-GigabitEthernet2/0/0] return
```

After the preceding configuration, you can run the **display port-queue configuration interface** command to view the configurations of the class queue.

```
<HUAWEI> display port-queue configuration interface gigabitethernet 2/0/0 outbound
GigabitEthernet2/0/0
be current configuration:
    Arithmetic: wfq
    weight: 10
    tm weight: 3
    fact weight: 10.00
    shaping(mbps): NA
    port-wred name: NA
af1 current configuration:
    Arithmetic: wfq
    weight: 10
    tm weight: 3
    fact weight: 10.00
    shaping(mbps): NA
    port-wred name: NA
af2 current configuration:
    Arithmetic: wfq
    weight: 10
    tm weight: 3
    fact weight: 10.00
    shaping(mbps): NA
    port-wred name: NA
af3 current configuration:
    Arithmetic: wfq
    weight: 15
    tm weight: 2
    fact weight: 15.00
    shaping(mbps): NA
    port-wred name: NA
af4 current configuration:
    Arithmetic: wfq
    weight: 15
    tm weight: 2
```

```

fact weight: 15.00
shaping(mbps): NA
port-wred name: NA
ef current configuration:
    Arithmetic: pq
    weight: NA
    tm weight: NA
    fact weight: NA
    shaping(mbps): 100
    port-wred name: test
cs6 current configuration:
    Arithmetic: pq
    weight: NA
    tm weight: NA
    fact weight: NA
    shaping(mbps): NA
    port-wred name: NA
cs7 current configuration:
    Arithmetic: pq
    weight: NA
    tm weight: NA
    fact weight: NA
    shaping(mbps): NA
    port-wred name: NA

```

Step 9 Verify the configuration.

When there are flows on the network, you can observe that packets of User1's AF1 and EF flows and User2's EF flows are forwarded at the assured bandwidth.

Running the **display port-queue statistics** command on the downstream interface GE 2/0/0 of the router, you can see that EF packets increase rapidly.

```
<HUAWEI> display port-queue statistics interface gigabitethernet 2/0/0 ef outbound
[ef]
    Total pass:                                5,097,976 packets,          458,817,750 bytes
    Total discard:                             0 packets,                  0 bytes
    Drop tail discard:                         0 packets,                  0 bytes
    Wred discard:                            0 packets,                  0 bytes
    Last 30 seconds pass rate:                12,030 pps,            8,661,600 bps
    Last 30 seconds discard rate:             0 pps,                      0 bps
    Drop tail discard rate:                  0 pps,                      0 bps
    Wred discard rate:                       0 pps,                      0 bps
```

----End

Configuration Files

Configuration file of the router.

```

#
sysname HUAWEI
#
flow-wred test
color green low-limit 70 high-limit 100 discard-percentage 100
color yellow low-limit 60 high-limit 90 discard-percentage 100
color red low-limit 50 high-limit 80 discard-percentage 100
#
flow-mapping test
map flow-queue af1 to port-queue ef

```

```
#  
flow-queue test  
    queue af1 lpq shaping 10000 flow-wred test  
    queue ef pq shaping 30000 flow-wred test  
#  
user-group-queue test  
    shaping 500000 inbound  
#  
service-template test  
    network-header-length 12 inbound  
#  
qos-profile test  
    user-queue cir 100000 pir 100000 flow-queue test flow-mapping test user-group -  
queue test service-template test  
#  
port-wred test  
    color green low-limit 70 high-limit 100 discard-percentage 100  
    color yellow low-limit 60 high-limit 90 discard-percentage 100  
    color red low-limit 50 high-limit 80 discard-percentage 100  
#  
interface GigabitEthernet1/0/0.1  
    control-vid 1 qinq-termination  
        qinq termination pe-vid 1 ce-vid 1 to 100  
        ip address 100.1.1.1 255.255.255.0  
        qos-profile test inbound pe-vid 1 ce-vid 1 to 100 group group1  
#  
interface GigabitEthernet1/0/0.2  
    control-vid 2 qinq-termination  
        qinq termination pe-vid 2 ce-vid 1 to 100  
        ip address 100.1.2.1 255.255.255.0  
        qos-profile test inbound pe-vid 2 ce-vid 1 to 100 group group1  
#  
interface GigabitEthernet1/0/0.3  
    control-vid 3 qinq-termination  
        qinq termination pe-vid 3 ce-vid 1 to 100  
        ip address 100.1.3.1 255.255.255.0  
        qos-profile test inbound pe-vid 3 ce-vid 1 to 100 group group1  
#  
interface GigabitEthernet2/0/0  
    undo shutdown  
    ip address 200.1.1.1 255.255.255.0  
    port-queue ef pq shaping 100 port-wred test outbound  
#  
osfp 10  
    area 0.0.0.0  
    network 200.1.1.0 0.0.0.255  
    network 100.1.1.0 0.0.0.255  
    network 100.1.2.0 0.0.0.255  
    network 100.1.3.0 0.0.0.255  
#  
return
```

10.10.5 Example for Configuring HQoS Scheduling for Leased Line Users

This section provides an example for configuring HQoS for Ethernet Layer 3 leased line users.

Networking Requirements



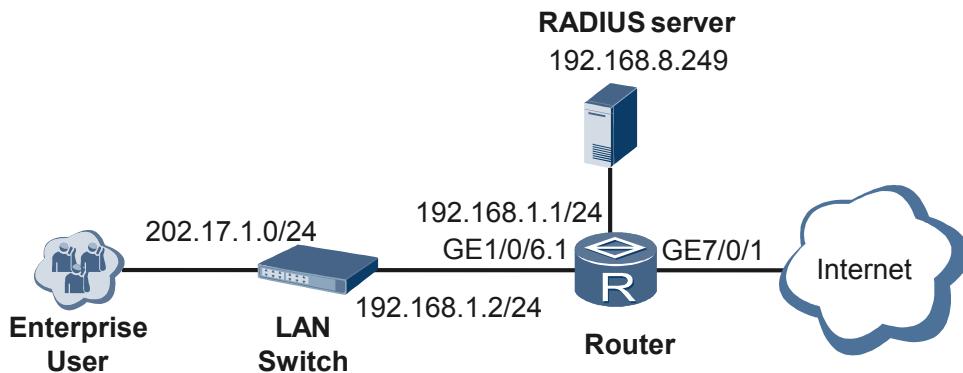
This Configuration Example cannot be configured on the X1 and X2 models of the NE80E/40E.

As shown in [Figure 10-12](#), the enterprise user accesses the Internet in Ethernet Layer 3 leased line mode. The networking requirements are as follows:

- The user accesses the Internet through GE 1/0/6.1 on the router through the Ethernet Layer 3 leased line.
- The user name of the leased line is layer3lease1@isp1.
- The network segment for the Layer 3 leased line user is 202.17.1.0/24.
- RADIUS authentication and RADIUS accounting are used. The IP address of the RADIUS server is 192.168.7.249. The authentication port number is 1645 and the accounting port number is 1646. The RADIUS+1.1 protocol is adopted, with the shared key being itellin.
- The network-side interface is GE 7/0/1.

HQoS is required for the leased line users to guarantee total bandwidth and service bandwidth of the enterprise.

Figure 10-12 Networking diagram of configuring HQoS scheduling for leased line users



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the access mode for the enterprise user.
2. Define a QoS profile and configure scheduling parameters.
3. Configure the rate limit mode for leased line users.
4. Apply the QoS profile to a domain.

Data Preparation

To complete the configuration, you need the following data:

- QoS profile name and scheduling parameters
- Rate limit mode for leased line users
- Domain to which the QoS profile is applied

Procedure

Step 1 Configure the BRAS service on the router so that the enterprise user can successfully access the Internet through the Ethernet Layer 3 lease line.

For the detailed configuration procedure, refer to the *HUAWEI NetEngine80E/40E Router Configuration Guide - User Access*.

Step 2 Define a QoS profile and configure scheduling parameters.

```
[HUAWEI] qos-profile test
[HUAWEI-qos-profile-test] car cir 1000 pir 2000 cbs 10000 pbs 20000 green pass
yellow pass red discard
[HUAWEI-qos-profile-test] quit
```

Step 3 Configure the rate limit mode for leased line users.

```
[HUAWEI] aaa
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-ispl] qos rate-limit-mode car inbound
```

Step 4 Apply the QoS profile to the lease line user in a domain.

```
[HUAWEI-aaa-domain-ispl] qos-profile test inbound
```

----End

Configuration Files

Configuration file of the router

```
#  
sysname HUAWEI  
#  
radius-server group rdl  
radius-server authentication 192.168.7.249 1645 weight 0  
radius-server accounting 192.168.7.249 1646 weight 0  
radius-server shared-key itellin  
radius-server type plus11  
radius-server traffic-unit kbyte  
#  
interface GigabitEthernet1/0/6  
undo shutdown  
mode user-termination  
#  
interface GigabitEthernet1/0/6.1  
user-vlan 1  
ip address 192.168.1.1 255.255.255.0  
bas  
access-type layer3-leased-line user-name layer3lease1 hello default-domain  
authentication ispl  
#  
interface GigabitEthernet7/0/1  
ip address 192.168.7.1 255.255.255.0  
#  
qos-profile test  
car cir 1000 pir 2000 cbs 10000 pbs 20000 green pass yellow pass red discard  
#  
aaa  
authentication-scheme auth1  
accounting-scheme acct1  
#  
domain default0  
domain default1  
domain default_admin  
domain isp1  
authentication-scheme auth1  
accounting-scheme acct1  
radius-server group rdl  
qos-profile test inbound  
qos rate-limit-mode car inbound  
#
```

A Glossary

This appendix collates frequently used glossaries in this document.

Glossary

A

AAA	Authentication, Authorization and Accounting.
Access Control List	A list composed of multiple sequential permit/deny statements. In firewall, after ACL is applied to an interface on the router, the router decides which packet can be forwarded and which packet should be denied. In QoS, ACL is used to classify traffic.
Assured Service	A kind of service that enables the user to obtain more service amount than what has subscribed. As with the case that the ensured service amount that is less than what has subscribed, good forwarding quality is ensured; as with the excess service, they are forwarded with a lower forwarding quality but not be discarded directly.
ATM	An asynchronous Transfer Mode. It is a data transmission technology in which data (files, voice and video) is transferred in cells with a fixed length (53 Bytes). The fixed length makes the cell be processed by the hardware. The object of ATM is to make good use of high-speed transmission medium such as E3, SONET and T3.

B

Bandwidth	An average transmission rate of data during a specified period. It is in bit/s.
Best-Effort	A traditional packet posting service. It features processing packets based on the sequence they reach the router (First In First Out rule). Packets from all users share the network resource and the bandwidth. The amount of the resource the packet gets depending on the time they reach the router. Best-Effort does not take effect on posting delay, jitter delay, packet loss ratio and reliability.

Glossary

Border Gateway Protocol An exterior gateway protocol. The function of this protocol is to exchange routing information (without loop) between autonomous systems.

C

Class-Based Queuing To allocate a single First In First Out queue for each user-defined traffic class to cache the data of the same class. When the network congestion occurs, CBQ matches the output packet with the user-defined rule and places it in the corresponding queue. Before being placed in the queue, congestion avoidance mechanism such as Tail-Drop or WRED and bandwidth restriction check should be performed. When the packet is to be sent out from the queue, packets in corresponding queues are equally scheduled.

Committed Access Rate An instance of traffic policing. Three parameters can be defined in CAR: Committed Information Rate (CIR), Committed Burst Size (CBS) and Excess Burst Size (EBS). These parameters can be used to estimate the traffic. CAR also can be used in traffic classification and traffic policing behavior definition.

Committed Burst Size A maximum size of the burst traffic. It indicates the capacity of the token bucket. The maximum burst size should be larger than the packet length.

Committed Information Rate A rate of placing tokens to the token bucket. It is in bit/s. Commonly, the traffic rate should be slower than the committed information rate.

Congestion A phenomenon of degraded service. It is because the capacity of the network is exceeded by the data rate of the input to the network. Congestion affects the quality of service.

Congestion Avoidance A traffic control mechanism in which packets are automatically discarded when network congestion occurs and becomes intensive. This mechanism can adjust the network traffic by monitoring the network resource occupancy so as to prevent the network overload.

Congestion Management A traffic control measure used to cache the packet when the network congestion occurs. It adopts some scheduling policy to define the forwarding order of each packet.

Custom Edge A terminator at one end of a layer connection within a Service Access Point. It is used in the MPLS VPN network. CE can be a router, a switch or a host.

Custom Queue A queuing policy allocating resources based on the user-defined bandwidth proportion.

D

Data Circuit-terminating Equipment An equipment providing interfaces for the communication between DTE and the network.

Glossary

Delay	An average time taken by the service data to transmit across the network.
Differentiated Service	A QoS model that classifies the service level according the packet precedence field (IP Precedence and DSCP), the source IP address and the destination IP address. Packets with different levels can be provided with different service levels. It is commonly used to provide end-to-end QoS for specified application programs.
Differentiated Services Code Point	A basis of traffic classification. It marks the priorities of packets through specifying ToS field.
Data terminal Equipment	A device working as a data sender or a data receiver. It connects with network through a Data Circuit-terminating Equipment (DCE).

E

Expedited Forwarding	A mechanism in which messages from any DS node should be sent at an equal or more rate than what has specified. This can ensure little delay and enough bandwidth.
----------------------	--

F

Fair Queue	A mechanism for queue scheduling in which network resource is allocated equally and delay and jitter time of all traffic are optimized.
File Transfer Protocol	An application layer protocol based on TCP/IP. It is used to transfer large amounts of data reliably between the user and the remote host. FTP is implemented based on corresponding file system.
First In First Out Queuing	A queuing policy that features that the packet reaching earlier can be allocated resource firstly.

G

Generic Traffic Shaping	A kind of traffic shaping measure. It adopts the queuing policy WFQ.
-------------------------	--

I

Integrated Service	An integrated service model that needs to reserve the network resource. It ensures the bandwidth, limits the delay and provides service and payload control for the packet as defined by traffic parameters.
IP-Precedence	A basis of traffic classification. It is three bits long carried in the ToS field of the IP packet.

Glossary

J

Jitter Refers to the interval for sending two adjacent packets minus the interval for receiving the two packets.

L

Limit Rate A traffic management technology used to limit the total rate of packet sending on a physical interface or a Tunnel interface. LR is directly enabled on the interface to control the traffic passing the interface.

Link Fragmentation and Interleaving To fragment large-size frames to small-size frames and send them with other small fragments so that the delay and jitter time of the frames transmitted across the low-speed link is decreased. The fragmented frames are reassembled when reaching the destination.

Local Area Network A network intended to serve a small geographic area, (few square kilometers or less), a single office or building, or a small defined group of users. It features high speed and little errors. Ethernet, FDDI and Token Ring are three technologies implemented in LAN.

Loss Rate A rate of the lost packet during packet transmission.

M

Maximum Transmission Unit A maximum size of packets that an interface can process. It is in bytes.

Media Access Control It is in the data link layer in OSI and is next to the physical layer.

MultiLink PPP A link generated by binding multiple PPP links for increasing bandwidth.

Multiprotocol Label Switching It is derived from IPv4 and its core technology can be extended to multiple network protocols. Packet is marked with a short and predetermined label. Based on routing protocol and control protocol, it provides a connection-oriented data exchange. MPLS enhances the network performance, optimizes the network extensibility, and provides more flexible routing.

O

Open Shortest Path First An interior gateway protocol developed by IETF. It is based on Link-State.

P

Glossary

Permanent Virtual Circuit	A permanent communication circuit that can be generated though no data is transmitted. PVC applies to stable communication systems or communication systems with frequent data exchange.
Point to Point Protocol	A transport serial link between two devices.
Priority Queuing	A queuing policy based on packet priorities. It features that the packet with a higher priority is allocated resource firstly.
Provider Edge	In an MPLS VPN network, PE is in the backbone network, engaged in managing VPN users, setting up LSPs and route designating for users in the same VPN.

Q

QoS	An estimation of the ability of service providers to meet the requirements of the user. It focuses on estimating the delay, jitter delay and packet loss ratio.
-----	---

R

Real-Time Protocol	A host-to-host protocol that is used in multi-media services such as Voice over IP and video.
Random Early Detection	A packet loss algorithm used in congestion avoidance. It discards the packet according to the specified higher limit and lower limit of a queue so that global TCP synchronization resulted in traditional Tail-Drop can be prevented.
Resource Reservation Protocol	A protocol that prearranges the network resource for an application. In the Intserv model, the application program should inform the router to apply QoS before sending out packets to reserve the network resource.

S

Service Level Agreement	An agreement between the user and the network carrier in which the treatment of the user's traffic that needs to be transmitted across the network is defined. The agreement covers the information of technology and commercial. Commonly, SLA is used to indicate a certain QoS.
-------------------------	--

T

Tail-Drop	A mechanism for queue discarding. When the length of the queue reaches the maximum, the subsequently received packets are all discarded.
-----------	--

Glossary

Traffic Engineering	A traffic control measure that dynamically monitors the network traffic and load of each network entity. It adjusts the traffic management parameters, routes parameters, and resource restriction parameters in real time to optimize the network operation status and the resource occupancy. In this way, congestion that is resulted from unbalanced load can be prevented.
Traffic Classifier	A basis and precondition to provide differentiated service. It identifies packets according to certain matching rules.
Traffic policing	A traffic control measure that monitors the size of the traffic that reach the router. If the traffic size exceeds the maximum, some restriction measures so as to protect the benefits of the carrier and the network resource.
Traffic Shaping	A traffic control measure that auto adjusts the output rate of traffic. It aims at making the traffic adapt the network resource that the downstream can provide and avoiding packet loss and congestion.
Throughput	Supposing that no packet is discarded, it indicates the number of packets that passed in a specified time.
Tunnel	In VPN, it is a transport tunnel set up between two entities to prevent interior users from interrupting and ensure security.

V

Versatile Routing Platform	Versatile Routing Platform. It is a versatile operating system platform developed by Huawei.
Virtual Local Area Network	Virtual LAN. A LAN is divided into several logical LANs. Each virtual LAN is a broadcast area. Communication between hosts in a virtual is just like the host communication is a LAN. VLANs can be divided according to the function, department and application despite of device location.
Virtual Private Network	Provision of an apparent single private network (as seen by the user), over a number of separate public and private networks. It is a newly developed technology as the Internet becomes widely used. "Virtual" indicates the network is logical.

W

Weighted Fair Queuing	It features automatic traffic classification and balances the delay and jitter time of each traffic. Compared with Fair Queue (FQ), it benefits the high-priority packet.
Weighted Random Early Detection	A packet loss algorithm used on congestion avoidance. It can prevent the global synchronization resulted in traditional Tail-Drop and features benefiting the high-priority packet with high-quality service during calculating the packet loss rate.

B Acronyms and Abbreviations

This appendix collates frequently used acronyms and abbreviations in this document.

Acronyms and Abbreviations

Numerics

3G	The Third Generation
3GPP2	3rd Generation Partnership Project 2

A

ACL	Access Control List
AF	Assured Forwarding
ATM	Asynchronous Transfer Mode

B

BE	Best-Effort
BW	Band Width

C

CAR	Committed Access List
CBQ	Class-based Queue
CBS	Committed Burst Size
CE	Customer Edge
CIR	Committed information Rate
CoS	Class of Service

**Acronyms and
Abbreviations**

CQ Custom Queue

D

DCE Data Circuit-terminating Equipment
Diff-Serv Different-service
DSCP Differentiated Services Codepoint
DTE Data Terminal Equipment

E

EBS Excess Buret Size
EF Expedited Forwarding

F

FECN Forwarding Explicit Congestion Notification
FIFO First In First Out
FQ Fair Queue
FR Frame Relay
FTP File Transfer Protocol

G

GTS Generic Traffic Shaping

H

HDLC High Level Data Link Control
HTTP Hyper Text Transport Protocol

I

ILM Incoming Label Map
IP Internet Protocol
IPX Internet Packet Exchange
ISDN Integrated Services Digital Network

Acronyms and Abbreviations

L

LAN	Local Area Network
LFI	Link Fragmentation and Interleaving
LR	Limit Rate
LSP	Label Switch Path

M

MIC	Media Access Control
MP	Multilink PPP
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit

O

OSPF	Open Shortest Path First
------	--------------------------

P

P2P	Point to Point
PE	Provider Edge
PPP	Point-to-Point Protocol
PQ	Priority Queuing
PVC	Permanent Virtual Circuit

Q

QoS	Quality of Service
-----	--------------------

R

RED	Random Early Detection
RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol

Acronyms and Abbreviations

T

TCP	Transmission Control Protocol
TE	Traffic Engineering
ToS	Type of Service
TP	Traffic Policing
TS	Traffic Shaping

U

UDP	User Datagram Protocol
-----	------------------------

V

VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VRP	Versatile Routing Platform

W

WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WWW	World Wide Web