

**H-QoS**  
**Technology White Paper**



***Ruijie***

## Copyright Statement

Ruijie Networks©2000-2017

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

## Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.


## Obtaining Technical Assistance

- Ruijie Networks Website: <http://www.ruijienetworks.com/>
- Service Email: [service\\_rj@ruijienetworks.com](mailto:service_rj@ruijienetworks.com)
- Technical Support: <http://www.ruijienetworks.com/service.aspx>
- Technical Support Hotline: +86-4008-111-000

## Documentation Conventions


The symbols used in this document are defined as follows:

---

 This symbol brings your attention to some helpful suggestions and references.

---

---

 This symbol means that you must be extremely careful not to do some things that may damage the switch or cause data loss.

---

# Contents

<b>Abstract</b> .....	4
<b>Keywords</b> .....	4
<b>Terms</b> .....	4
<b>Overview</b> .....	4
Background.....	5
Development.....	6
Prospect.....	8
<b>Technical Principle</b> .....	8
Class of Service.....	8
Traffic Classification .....	9
Simple Traffic Classification .....	9
Complex Traffic Classification.....	12
Queue Scheduling.....	14
QoS Basics .....	14
H-QoS Queues.....	16
H-QoS Multi-level Scheduling.....	16
<b>Typical Application</b> .....	20
Applications.....	20
Configuration .....	21
Test Result.....	30
<b>Implementation Analysis</b> .....	31
Advantage and Disadvantage .....	31
Platform.....	31
Constraints.....	31
Risks .....	31
<b>Comparison</b> .....	31
H3C H-QoS.....	32
Cisco H-QoS.....	34
<b>Conclusion</b> .....	36
<b>References</b> .....	36

## Abstract

Based on TR-051 and TR-101 developed by DSL Forum and the implementation of Hierarchical QoS (H-QoS) presented by other enterprises, this document not only details H-QoS, but outputs the Ruijie H-QoS technical model and implementation policies and features.

## Keywords

QoS, H-QoS

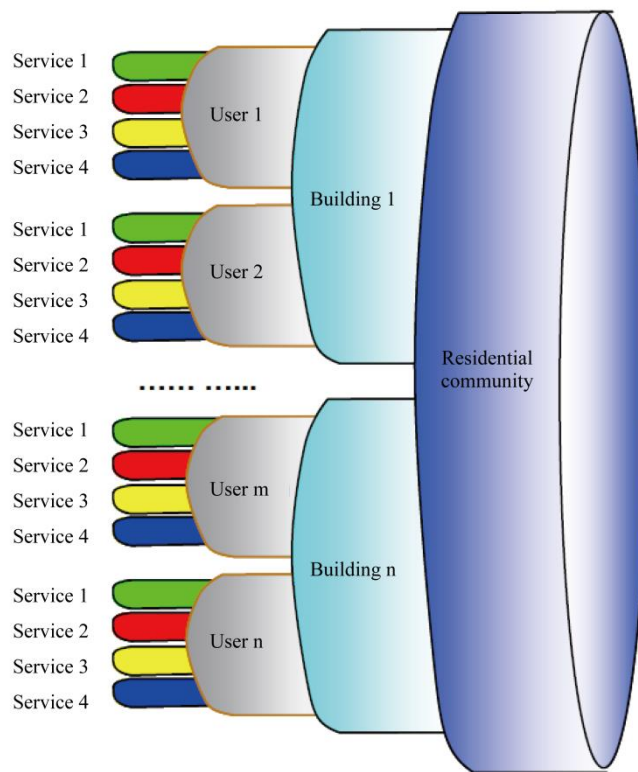
## Terms

Terminology	Description
QoS	Quality of Service
H-QoS	Hierarchical Quality of Service
PHB	Per-Hop Behavior
BRAS	Broadband Remote Access Server
NSP	Network Service Provider
ASP	Application Service Provider
RG	Routing Gateway
LP	Loop Provider
ANP	Access Network Provider
RNP	Regional Network Provider

## Overview

H-QoS stands for hierarchical QoS. Unlike conventional service-specific single-level QoS, H-QoS provides multi-level QoS for data traffic in a pyramid hierarchy consisting of services, users, buildings, and residential communities. The bottom-level QoS implements per-user, multi-service QoS; the second-bottom-level QoS implements per-building, multi-user QoS, et cetera. In such way, H-QoS provides a high degree of granularity of QoS for data convergence devices, thereby improving the QoS for the entire network.

Figure 1 User + User Service Scheduling Model



## Background

The conventional Differentiated Services (DiffServ) QoS categorizes service traffic and specifies different processing policies to meet the transmission requirements for bandwidth, delays and so on. Typical applications include Priority Queuing (PQ), Class-based Weighted Fair Queuing (CBWFQ), and Low Latency Queuing (LLQ). For DiffServ QoS domains are deployed based on Per-Hop Behaviors (PHBs), a unified policy is necessarily implemented on all devices to achieve the required network transmission.

In existing Digital Subscriber Line (DSL), a large number of access devices (such as Layer 2 switches and various converters) do not support complex QoS based on Differentiated Services Code Point (DSCP). Though the egress devices maximize the QoS assurance for transmission services, they cannot differentiate QoS based on users or user groups. To improve the service quality and attract more customers, service providers must provide more specific QoS. In such background, DSL Forum proposed H-QoS deployed on Broadband Remote Access Servers (BRASs) to improve QoS for network access.

Figure 2 Many-to-many Access Network Based on Regional/Access Network

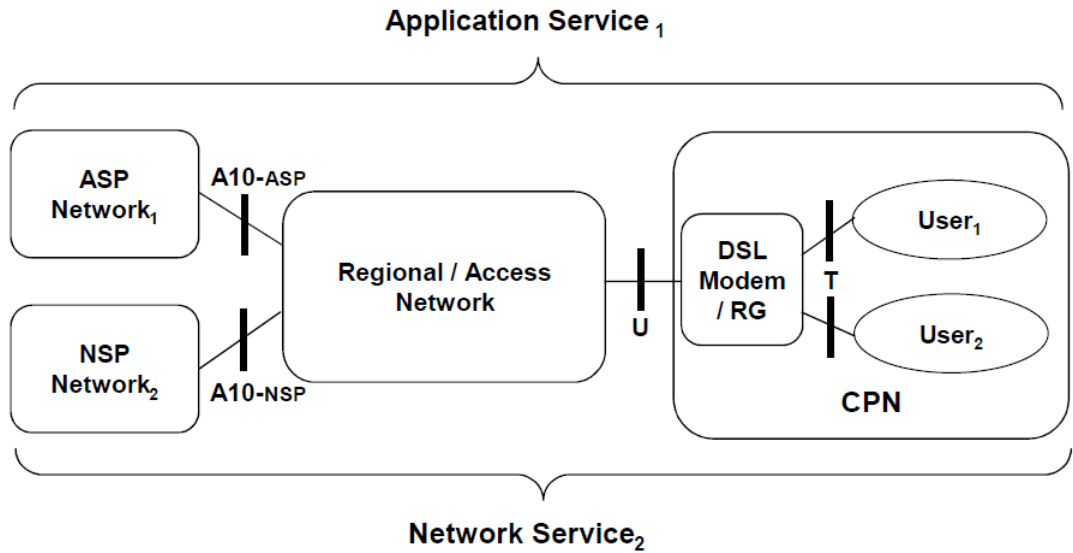
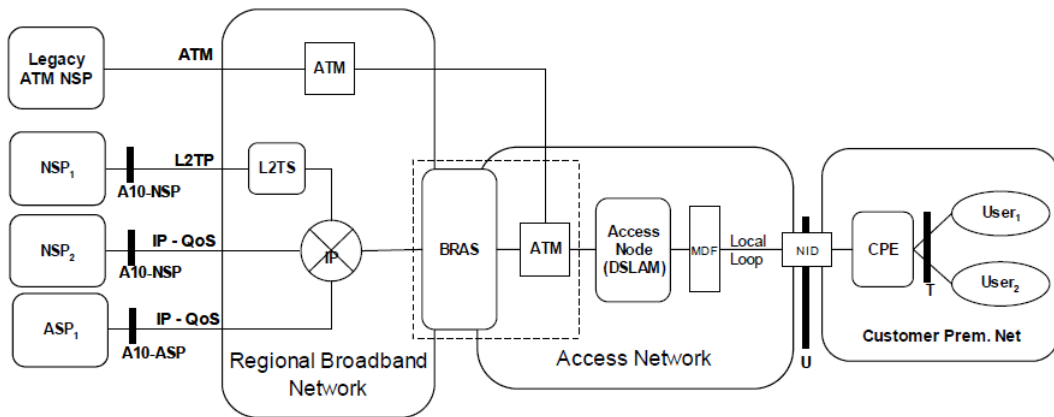


Figure 3 Enabling QoS in IP-enabled Regional/Access Network



## Development

Broadband Forum strives to advance broadband access. It focuses on the home-to-core network and management solutions. It has launched three releases of BroadbandSuite. Both BroadbandSuite Release 1.0 and BroadbandSuite Release 3.0 described the QoS requirements of DSL.

BroadbandSuite Release 1.0 focused on ATM-based DSL network architecture: TR-059 proposed H-QoS and focuses on the deployment of QoS for the DSL networks; it defined the H-QoS function for the BRAS devices that support IP service convergence and ATM link convergence in the access networks, as shown below.

Figure 4 Topology of a BRAS Device in an IP-enabled ATM Network

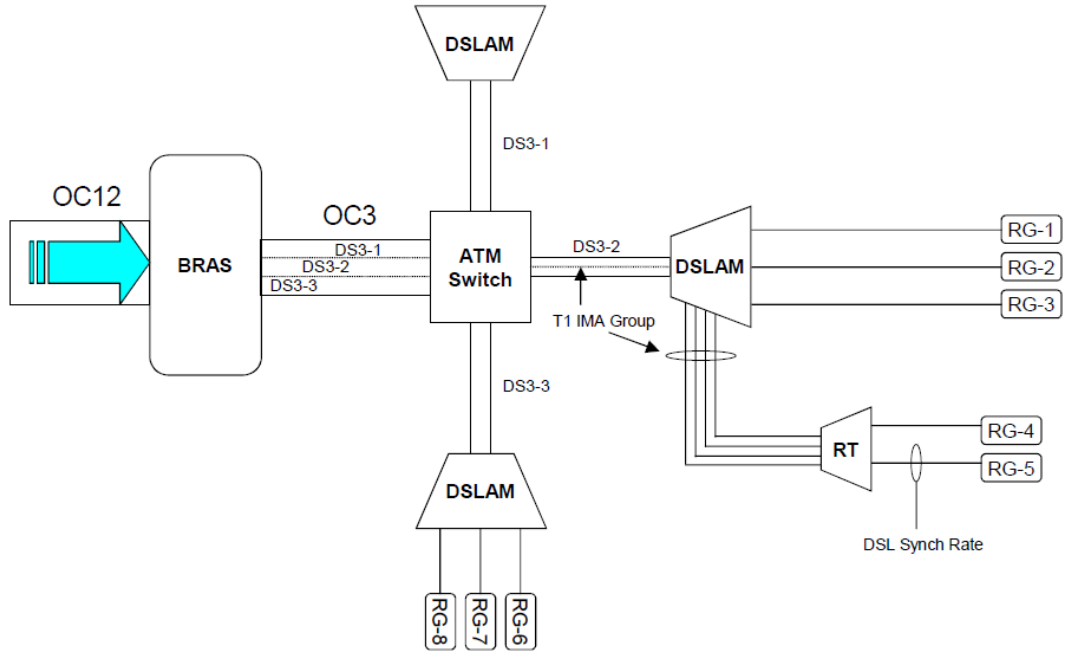
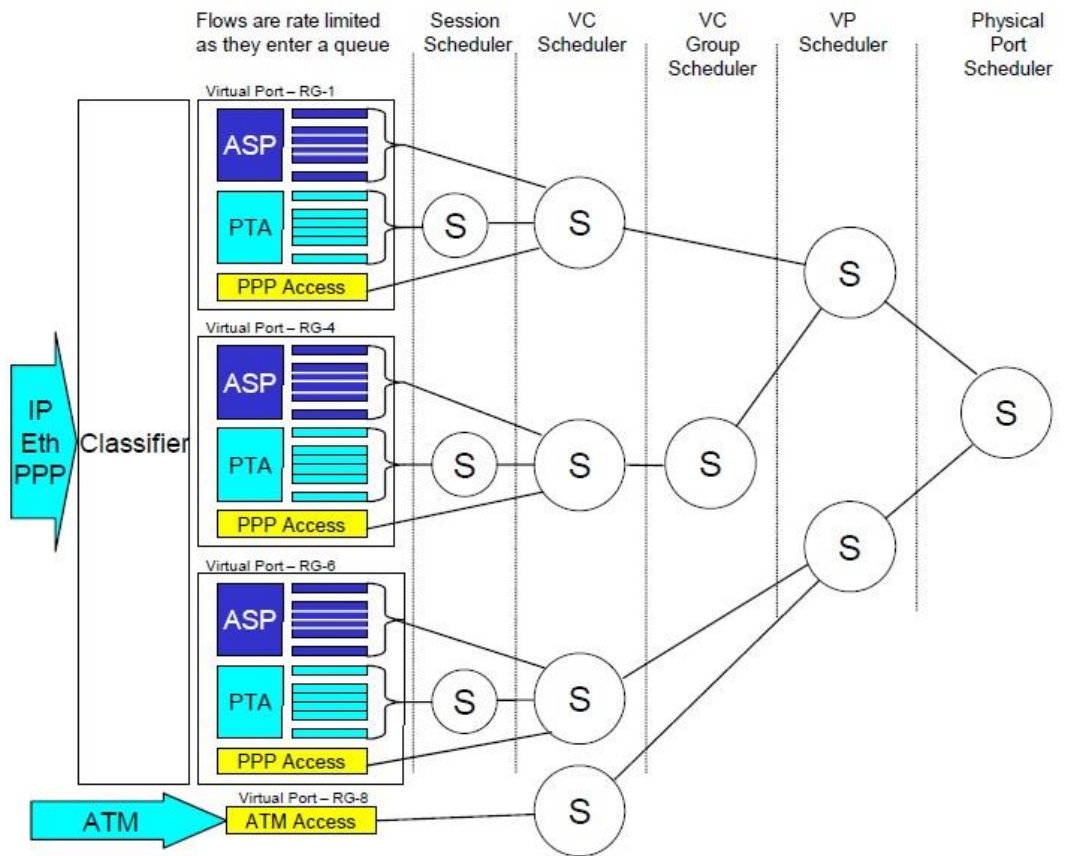


Figure 5 H-QoS for a BRAS Device in an IP-enabled ATM Network



ASP – Application Service Provider  
 ATM – Asynchronous Transfer Mode  
 PTA – PPP Terminated Aggregation  
 PPP – Point-to-Point Protocol  
 S – Scheduler

In BroadbandSuite Release 3.0, TR-101 revised the QoS descriptions for Ethernet-based DSL: In an Ethernet-based network, hierarchical services are primarily differentiated by using QinQ tag in IEEE 802.1ad.

Cisco, Huawei, and H3C have realized H-QoS implementation. Both Huawei and H3C follow the framework defined in the DSL documents, while Cisco develops Hierarchical Queuing Framework simply by extending traditional LLQ and CBWFQ to implement H-QoS functions defined in the DSL documents.

## Prospect

Based on the current network development, H-QoS is primarily required in BRAS devices and broadband network gateways in DSL networks. In common campus networks and core networks, the conventional DiffServ/InterServ QoS and MPLS TE are deployed. Therefore, H-QoS will be primarily used in carriers' networks and large enterprise networks.

In both ATM-based DSL networks and Ethernet-based DSL networks, H-QoS can be deployed on the convergence devices to implement the QoS assurance function. The H-QoS simplifies the QoS deployment in the DSL networks, reduces the QoS deployment costs, and improves the QoS assurance for multi-level user services in the DSL networks.

The H-QoS is ideal for the convergence devices in the DSL networks. However, the centralized H-QoS significantly affect the system performance of the devices. If necessary, the hardware-based H-QoS function needs to be implemented to meet the service requirements.

## Technical Principle

### Class of Service

The data traffic entering a system must be differentiated to ensure service quality. Therefore, the data traffic is classified by using the preset Classes of Service (CoS) as below.

Table 1 Definition of CoS

No.	Cos	Description
7	CS7	Defines the class of in-band control packets with the highest precedence.
6	CS6	Defines the class of control-plane protocol packets, such as routing protocol packets and BFD packets.
5	Expedited Forwarding (EF)	Defines the class of packets sensitive to delay, jitter and packet loss rate, such as VoIP and TDM.
4	AF4	Defines the class of other types of packets which can be discarded according to the discarding priority when the maximum allowable bandwidth is exceeded. This CoS is divided into four subclasses, and each subclass is allocated different bandwidth.
3	AF3	
2	AF2	
1	AF1	
0	Best Effort (BE)	Defines the class of packets insensitive to delay, jitter, and packet loss rate, such as Web, FTP, and other Internet services.

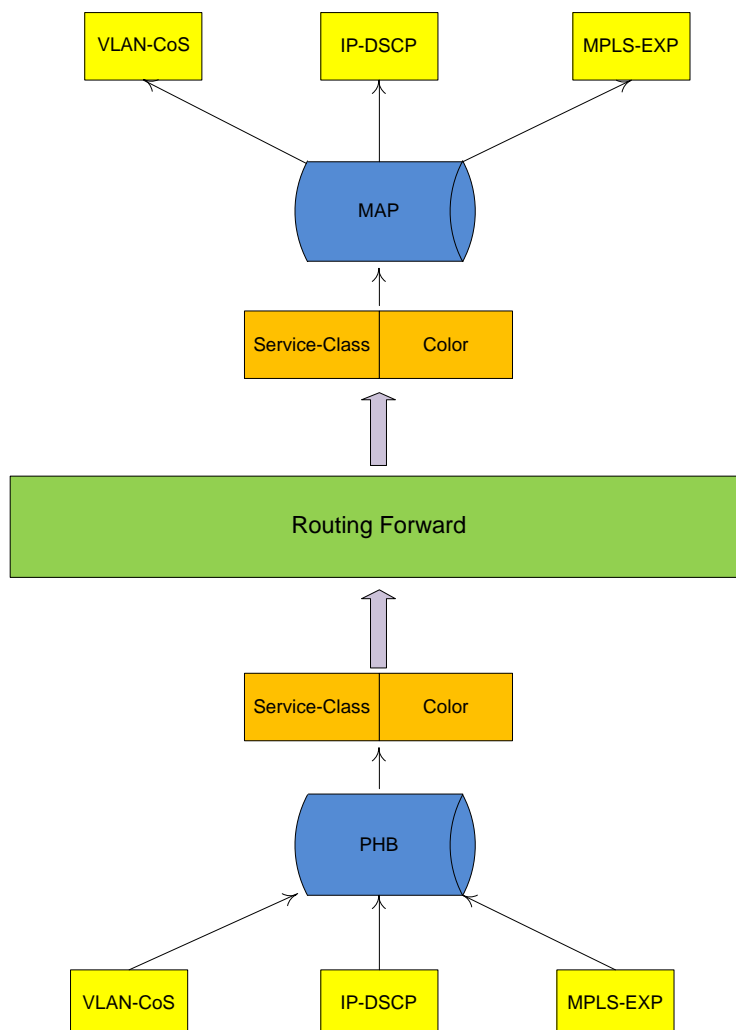


## Traffic Classification

### Simple Traffic Classification

Simple traffic classification refers to that packets are classified based on the priority fields carried in them. The priority fields include VLAN-CoS, MPLS-EXP, and IP-DSCP. When the ingress and egress of the packets are in different differentiated service domains, simple traffic classification maps packet priorities in the ingress domain to packet priorities in the egress domain. The mapping process is implemented by modifying the priority values in the packets.

Figure 6 Flowchart of Simple Traffic Classification



In the ingress direction, simple traffic classification maps a packet priority to an internal CoS based on the priority information carried in the packet according to the predefined PHB mapping rules.

In the egress direction, simple traffic classification converts the CoS to a priority based on the predefined mapping rules.

For the simple traffic classification, default rules are available for mapping a packet priority to an internal CoS and for mapping an internal CoS to a packet priority.

Table 2 Default Mapping Rules for Mapping an IP-DSCP to an Internal CoS

IP-DSCP	CoS	Color
0-7, 9, 11, 13, 15, 17, 19, 21, 23, 24, 27, 29, 31, 33, 35, 37, 39, 41-45, 47, 49-55, 57-63	BE	Green
8, 10	AF1	Green
12	AF1	Yellow
14	AF1	Red
16, 18	AF2	Green
20	AF2	Yellow
22	AF2	Red
24, 26	AF3	Green
28	AF3	Yellow
30	AF3	Red
32, 34	AF4	Green
36	AF4	Yellow
38	AF4	Red
40, 46	EF	Green
48	CS6	Green
56	CS7	Green

Table 3 Default Mapping Rules for Mapping an MPLS-DSCP to an Internal CoS

MPLS-EXP	CoS	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

Table 4 Default Mapping Rules for Mapping a VLAN-CoS to an Internal CoS

VLAN-CoS	CoS	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

Table 5 Default Mapping Rules for Mapping an Internal CoS to an IP-DSCP

CoS	Color	IP-DSCP
BE	Green, Yellow, and Red	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, Yellow, and Red	46
CS6	Green, Yellow, and Red	48
CS7	Green, Yellow, and Red	56

Table 6 Default Mapping Rules for Mapping an Internal CoS to an MPLS-EXP

CoS	Color	MPLS-EXP
BE	Green, Yellow, and Red	0
AF1	Green, Yellow, and Red	1
AF2	Green, Yellow, and Red	2
AF3	Green, Yellow, and Red	3

AF4	Green, Yellow, and Red	4
EF	Green, Yellow, and Red	5
CS6	Green, Yellow, and Red	6
CS7	Green, Yellow, and Red	7

Table 7 Default Mapping Rules for Mapping an Internal CoS to a VLAN-CoS

CoS	Color	VLAN-CoS
BE	Green, Yellow, and Red	0
AF1	Green, Yellow, and Red	1
AF2	Green, Yellow, and Red	2
AF3	Green, Yellow, and Red	3
AF4	Green, Yellow, and Red	4
EF	Green, Yellow, and Red	5
CS6	Green, Yellow, and Red	6
CS7	Green, Yellow, and Red	7

## Complex Traffic Classification

Complex traffic classification refers to that packets are classified by using complex rules based on information in link layer, network layer, and transmission layer (such as source and destination MAC addresses, source and destination IP addresses, user group IDs, protocol types, or TCP/UDP port IDs of applications).

Complex traffic classification per layer only focuses on the traffic matching policy and traffic behavior policy used at the layer, as shown below.

Table 8 Complex Traffic Classification Rules

CoS		Color	VLAN-CoS
Layer 3	IPv4	ACL-ID	remark dscp remark ip-prec
		DSCP	
		IP-Precedence	
		Any	
Layer 3	IPv6	ACL-Name	remark dscp
		DSCP	
		Any	
Layer 2.5	MPLS	EXP	remark mpls-exp
Layer 2	Ethernet	VLAN-CoS	remark cos
		Source MAC	

		Destination MAC	
--	--	-----------------	--

#### ■ Traffic matching

Traffic matching checks whether packets conform to the self-defined matching rules. As shown in Figure 5–8, different network layers have different matching criteria, which should be flexibly configured as required.

#### ■ Traffic behavior

Traffic behavior sets packet priorities, internal CoSs, and User Queues (UQs), and child policies for packets successfully matching the contract.

Packet priorities can be modified as shown in Table 5–8. For different layers, the priority fields for the corresponding layer in the packets can be modified after the traffic matching succeeds.

The basis of H-QoS is to set internal CoSs to differentiate services.

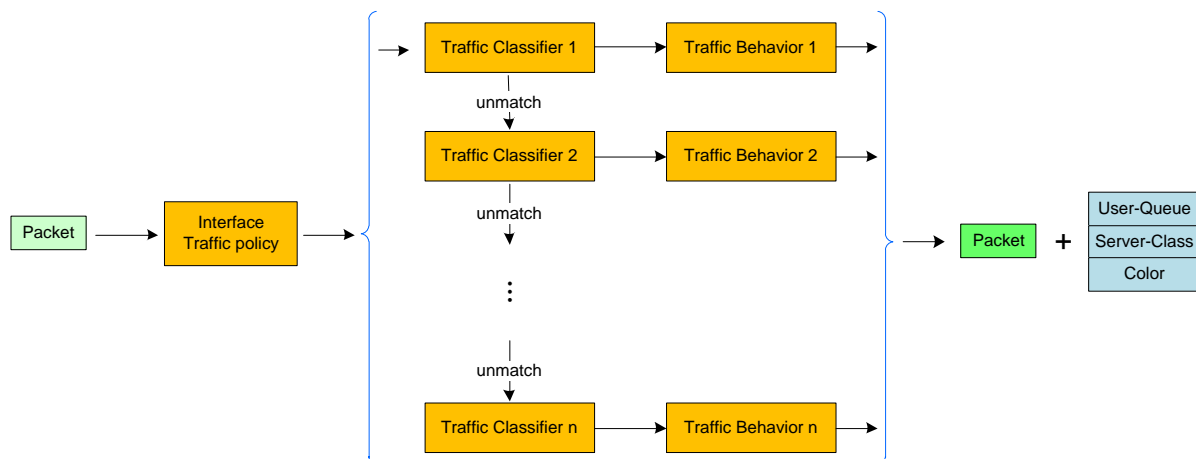
UQs are set so that H-QoS can distinguish between different data traffic, identify user of the data traffic, and take different bandwidth policies for different users.

Child policies provide a simplified configuration manner. With sub-policies, multiple channels of traffic are provided with a same traffic behavior.

#### ■ Traffic policy

A traffic policy specifies a certain traffic behavior for the data traffic in concert with a certain traffic matching criteria. A traffic policy can specify multiple criteria of traffic matching and traffic behavior. The higher-priority traffic takes precedence in matching. Only if the matching fails, lower-priority traffic matching gets the handoff. When the traffic matching succeeds, corresponding traffic behavior is implemented. After the processing is complete, packets with modified priorities and CoSs are obtained. See Figure 7.

Figure 7 Flowchart of Complex Traffic Classification



#### ■ Traffic Classification Features

When the simple traffic classification is used on an interface, traffic in the uplink and downlink direction is not differentiated. That is, the simple traffic classification works on both directions. In addition, the simple traffic classification works on all the network layers. In contrast, complex traffic classification varies with traffic transport direction and network layers on an interface. In the uplink direction, the simple traffic classification works on lower network layers. For example, after Layer 2 VLAN-CoS is mapped to an internal CoS, the mapping of the Layer 3 IP-DSCP will not be performed. While complex traffic classification works on higher network layers in the uplink direction but on lower network layers in the downlink direction.

When both the simple traffic classification and the complex traffic classification are applied on the same network layer in the same direction, complex traffic classification takes the lead.

## Queue Scheduling

### QoS Basics

H-QoS still preserves QoS theories and concepts. The following describes QoS basics.

#### ■ Traffic policing

Traffic policing restricts the traffic transmission rate on an ingress or egress interface for a router.

Traffic policing adopts Committed Access Rate (CAR). When network congestion occurs, packets that do not conform to the traffic features will be discarded. The CAR technology is implemented by using the token bucket algorithm.

Traffic shaping is used on an egress interface to shape some traffic for a router. It helps reduce the packet loss for efficient capacity utilization.

Traffic shaping applies Generic Traffic Shaping (GTS). After the traffic shaping is implemented, the data traffic is output at a predefined rate. The GTS technology is implemented by using a token bucket and a buffer.

#### ■ Congestion avoidance

Congestion avoidance selectively discards packets based on the queue status to avoid data overloading, thereby avoiding network congestion.

The tail-drop is one conventional congestion avoidance method. When a network is congested, subsequent packets that enter the queue will be discarded.

Ruijie H-QoS provides the Weighted Random Early Detection (WRED) algorithm for congestion avoidance.

In the WRED algorithm, a lower limit and a higher limit are set for each queue. The WRED algorithm is implemented as follows:

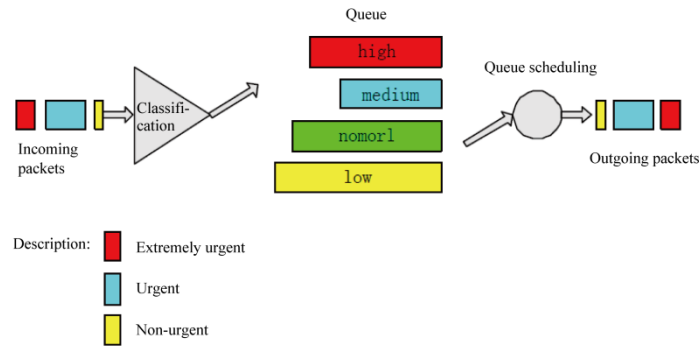
- 1) When the queue size is less than the lower limit, all incoming packets are retained.
- 2) When the queue size is greater than the higher limit, all incoming packets are discarded.
- 3) When the queue size ranges between the lower limit and the higher limit, incoming packets are randomly discarded. Specifically, a random number is generated for each incoming packet. If the random number is greater than the discarding probability, the packet is discarded. The larger the queue size is, the higher the drop probability will be.

#### ■ Congestion management

When a network is congested, congestion management must be performed. Congestion management can be implemented by using queuing strategies. The following describes three common queuing strategies.

#### **PQ**

Figure 8 Principle of PQ



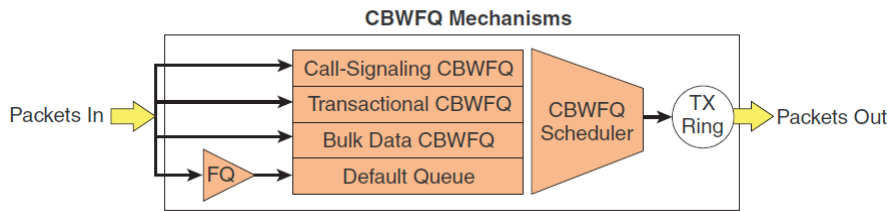
Principle: PQ classifies data traffic in a network into four priorities and sends data traffic in order by strictly following the priorities.

Advantage: As the oldest QoS congestion management policy, PQ is used to process the data traffic in the network.

Disadvantage: Because the PQ is implemented strictly following queuing strategy, low-priority data traffic may not be transmitted, and the bandwidth for each queue is not guaranteed.

**CBWFQ**

Figure 9 Principle of CBWFQ



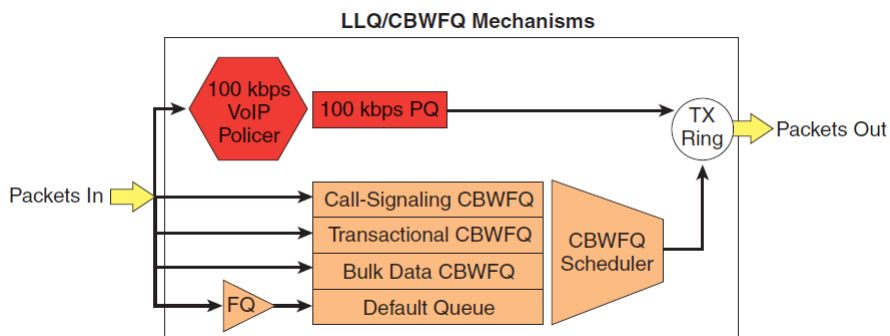
Principle: Based on PQ, CBWFQ uses the user bandwidth assurance mechanism to guarantee the bandwidth for different data traffic.

Advantage: CBWFQ provides flexible service matching rules and bandwidth assurance to meet complex service and bandwidth requirements in the data service network.

Disadvantage: It has no priority-based mechanism and cannot satisfy real-time services.

**LLQ**

Figure 10 Principle of LLQ



Principle: LLQ is a combination of CBWFQ and PQ. In the LLQ, high-priority queues are added to the implementation framework to CBWFQ to ensure a low delay for real-time services.

Advantage: It provides flexible bandwidth allocation and preferential processing of real-time services.

Disadvantage: It does not support H-QoS in the multi-level service model such as “user (level 1) + service (level 2)” or “service (level 1) + user (level 2)”.

## H-QoS Queues

### ■ Flow Queue (FQ)

A flow queue refers to a service queue of a user. Each user has eight flow queues (with different CoS including BE, AF1, AF2, AF3, AF4, EF, CS6, and CS7). PQ, WFQ, and LPQ scheduling can be configured for the FQs. Each FQ supports WRED and traffic shaping.

### ■ User Queue (UQ)

Here a user generally refers to a VLAN, a VPN, or the like. Users can be classified by interfaces, sub-interfaces, and ACL. Traffic of each user is one UQ, which aggregates the eight FQs. The transmission rate of each UQ can be limited for best bandwidth utilization.

### ■ Group Queue (GQ)

Several users can be bound to a user group, and traffic of each user group is one GQ. Traffic shaping can be implemented for the GQ so as to control the traffic of the users in the group.

### ■ Virtual Output Queue (VoQ)

The VoQs are divided into four groups, which correspond to four service types. In each service group, one VoQ queue is set for each destination device, and Round-Robin Scheduling is implemented between the VoQ queues. The scheduling of a VoQ is controlled by a credit point. The VoQ can participate in the scheduling only when the credit is sufficient. The credit point is allocated by a destination device.

### ■ Class Queue (CQ)

Each destination interface has eight CQs. Similar to FQs, the eight CQs correspond to eight service types. The eight queues can be configured with Strict-Priority (SP) and WFQ. Each CQ supports WRED and traffic shaping.

CQ on a destination device can be deemed as CQ on a destination outgoing interface. They are essentially the same. The difference is that CQ on the destination device is to be transmitted to a carrier board rather than a network interface. Each destination device has four CQs, which correspond to four service types. The four CQs are scheduled by using SP.

### ■ Low Priority Queue (LPQ)

There are three queuing manners of H-QoS: PQ, WFQ, and LPQ. Their scheduling precedence is: PQ > WFQ > LPQ. In case of network congestion, PQ and WFQ can preempt the bandwidth of LPQ. In applications, LPQ is generally implemented on BE services.

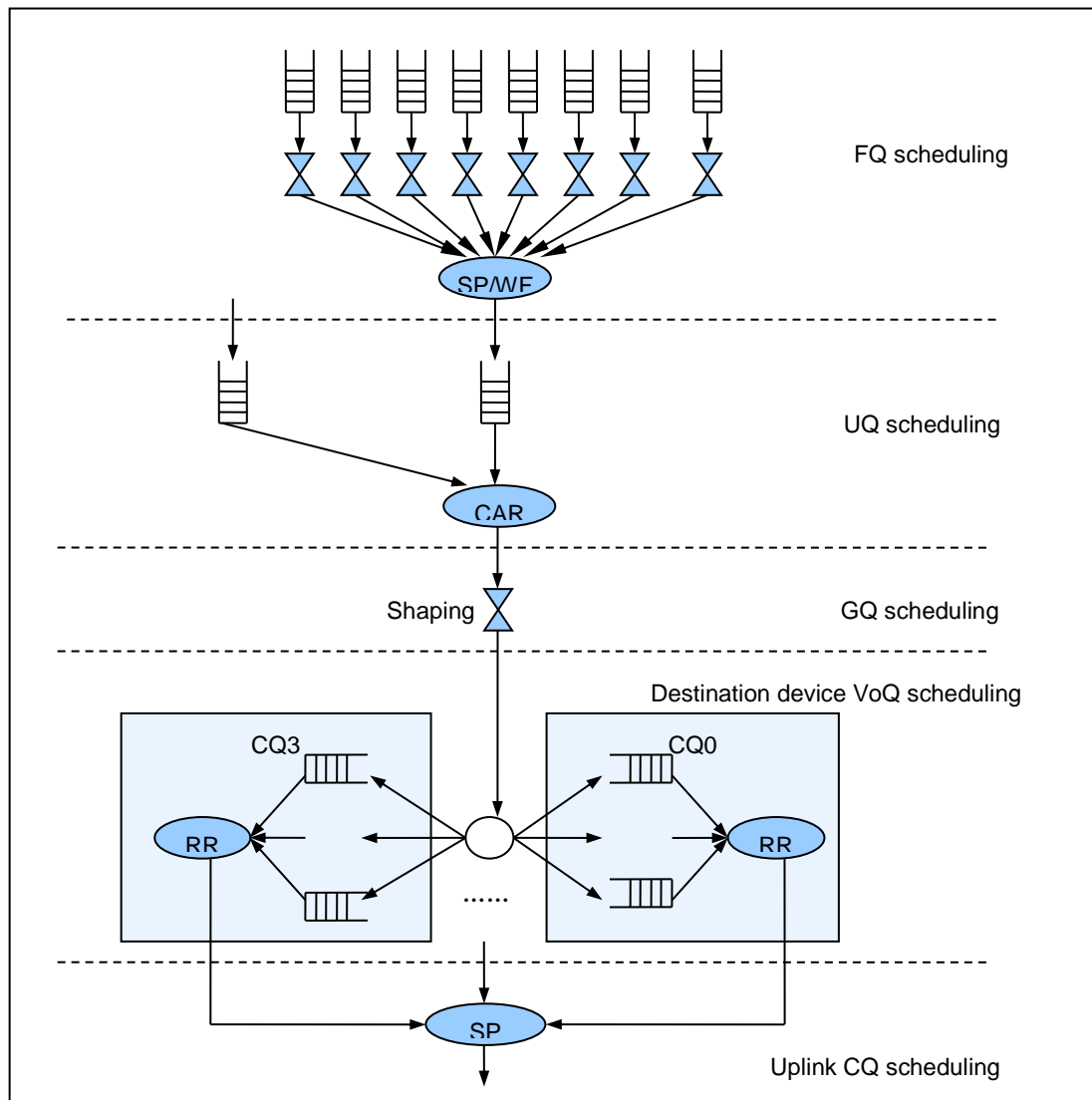
## H-QoS Multi-level Scheduling

### ■ 5-level uplink scheduling



The 5-level uplink scheduling applies in different precedence: FQ > UQ > GQ > VoQ > Uplink CQ, as shown below.

Figure 11 H-QoS Uplink Scheduling Model



Level-1 scheduling is FQ scheduling. A FQ is a physical queue which buffers packets. FQ includes FQ WRED, FQ shaping, and FQ scheduling. Before packets enter the FQ, WRED is first implemented for congestion avoidance. The system discards packets according to priority colors: red, yellow, and green. Red indicates the highest discarding priority, yellow the medium, and green the lowest. In each FQ, the lower and higher discarding limits and discarding probability are set for each discarding priority. The higher the discarding priority is, the larger the lower and higher limits are, and the higher the discarding probability is. After WRED is implemented for FQ, traffic shaping is implemented by using a token bucket. Finally, FQs are scheduled by using SP and WFQ. SP includes PQ and LPQ; that is, CS7, CS6, EF, AF, and BE are scheduled based on the priorities. When a higher-priority queue has no packets, a lower-priority queue is scheduled. AF falls into four types, and fair scheduling is implemented according to their weights.

Level-2 scheduling is UQ scheduling. A UQ is a virtual queue which buffers no packet and is only scheduled as a level-1 queue. Each UQ contains eight FQs, which share the bandwidth of the UQ. The UQ supports only the rate limiting function. Each UQ can use only one GQ. It is acceptable if the UQ does not use any GQ.

Level-3 scheduling is GQ scheduling. A GQ is a virtual queue. Multiple UQs can be bound as GQ for scheduling. The GQ supports only the traffic shaping function. If no UQ is bound to the GQ, the GQ scheduling will not be implemented.

Level-4 scheduling is VoQ scheduling. VoQ scheduling is to schedule traffic between line cards in the uplink direction. The VoQs are divided into four groups based on the service priorities. Each destination device in each group has one queue. After UQ scheduling is implemented for the packets, the packets enter different VoQs based on the destination devices and priorities. The VoQ scheduling is implemented inside the system, so it does not need to be configured by the user. The system provides commands for enabling and disabling the VoQ function.

Level-5 scheduling is CQ scheduling. A CQ is a virtual queue which buffers no packet. However, each CQ has information like scheduling priority and scheduling weight, and supports SP/WFQ scheduling. In the uplink H-QoS, the CQ scheduling is configured by the system instead of users.

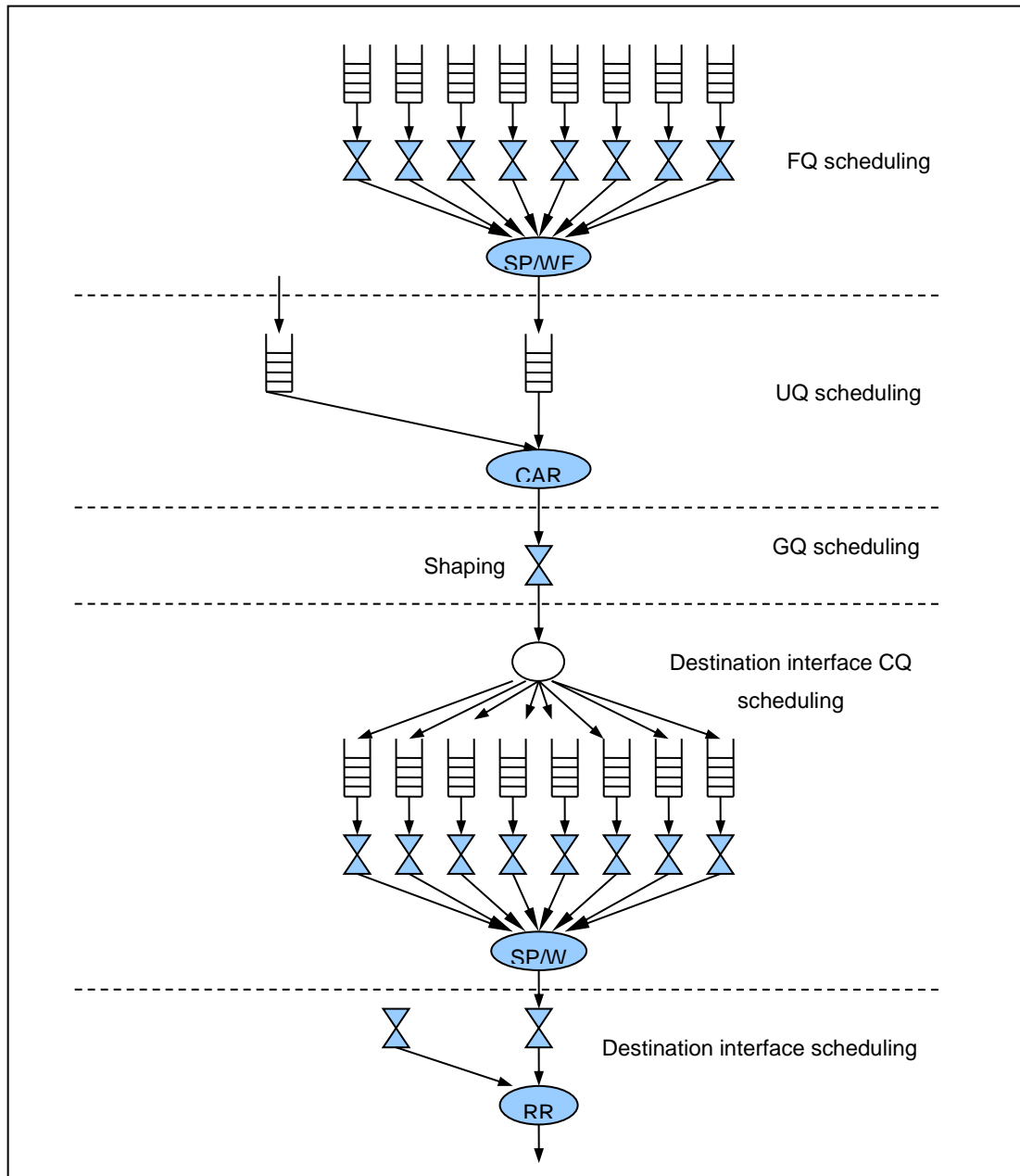
■ Class-based uplink H-QoS processing:

- 1) Perform traffic classification based on the configured traffic classification rules, and mark eight packet priorities.
- 2) Determine the UQs, GQs, WRED parameters, and scheduling policies of the packets based on the traffic behavior criteria. Then, add the packets to the corresponding FQs.
  - During FQ scheduling, congestion avoidance can be implemented based on user configuration.
  - FQ scheduling can be implemented based on queues: PQ, WFQ, and LPQ. PQ and WFQ can preempt the bandwidth of LPQ.
- 3) Check the idle bandwidth of GQ. If the idle bandwidth of GQ is insufficient, the UQ included in the GQ will not be scheduled; if the free bandwidth of GQ is sufficient, the UQ included in the GQ will be scheduled. The bandwidth of the GQ can be set by the user.
- 4) Check the free bandwidth of UQ. If the free bandwidth of UQ is insufficient, the FQ included in the UQ will not be scheduled; if the free bandwidth of UQ is sufficient, the FQ included in the UQ will be scheduled. The bandwidth of the UQ can be set by the user.
- 5) After FQ scheduling is implemented for the packets, the packets enter the VoQs of the destination device.
- 6) Implement CQ scheduling. During the CQ scheduling, four queues are scheduled by using the SP manner. After the CQ scheduling is implemented, the packets are forwarded.

■ 5-level downlink scheduling

The scheduling for downlink H-QoS is also divided into five levels: FQ > UQ > GQ > destination interface CQ > destination interface queues, as shown below.

Figure 12 5-Level Downlink Scheduling Model



The level-1 FQ scheduling, level-2 UQ scheduling, and level-3 GQ scheduling are the same as those in uplink H-QoS.

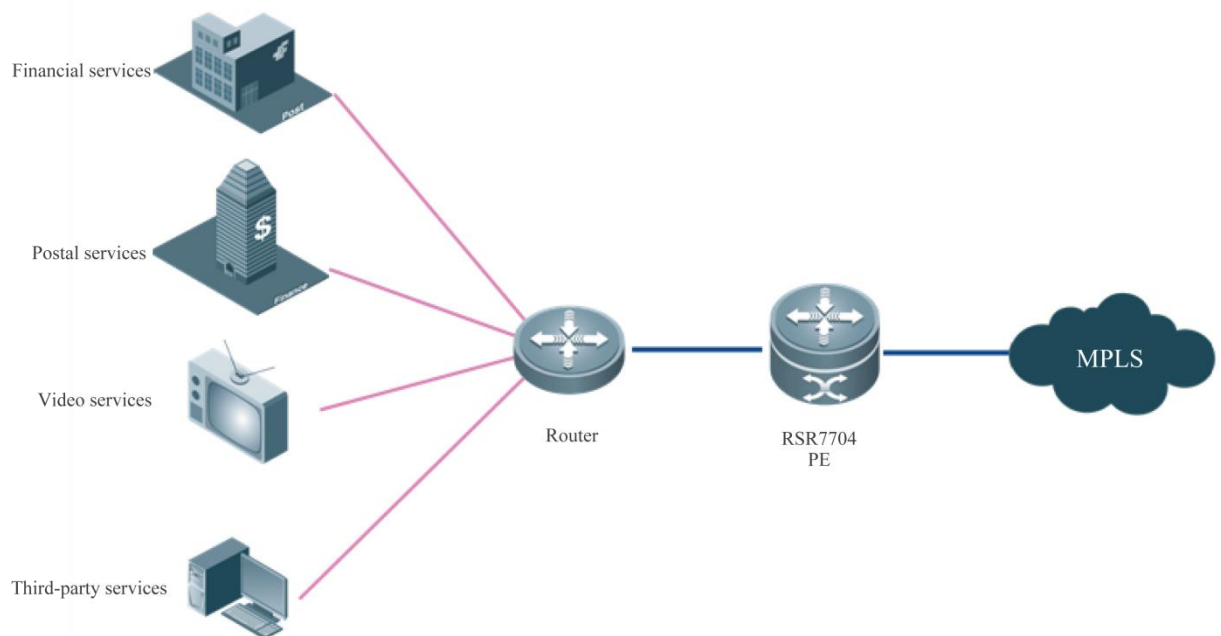
Level-4 scheduling is CQ scheduling. Each interface has eight CQs, which correspond to eight service priorities. Unlike the CQ in the uplink H-QoS, the congestion avoidance parameters and traffic shaping values for the CQ can be configured by the user. The CQ scheduling is implemented by using SP and WFQ.

Level-5 scheduling is destination interface scheduling. The system schedules the interfaces by using the Round-Robin Scheduling algorithm. The CQ scheduling is implemented inside the system instead of users.

# Typical Application

## Applications

Figure 13 Application Topology



### Description:

- 1) In case of network congestion, the assured bandwidth for four services should be allocated as follows: 4 Mbps for postal services, 6 Mbps for financial services, 7 Mbps for video OA services, 3 Mbps for third-party communication services; PQ scheduling is used in financial and video applications guarantees low delay.
- 2) In case of network congestion, the bandwidth for postal services is allocated as follows: 0.5 Mbps for the electronic branch operations system, 2 Mbps for the electronic remittance system, 0.5 Mbps for the network operations system, and 1 Mbps for EMS; PQ scheduling used in electronic remittance services guarantees low delay.
- 3) In case of network congestion, the bandwidth for financial services is allocated as follows: 3 Mbps for savings service, 1 Mbps for agency and insurance, and 2 Mbps for public services; PQ scheduling used in the savings service guarantees low delay.
- 4) In case of network congestion, the bandwidth for video OA services is allocated as follows: 4 Mbps for high-definition video service, 1 Mbps for OA, and 2 Mbps for VoIP; PQ scheduling used on high-definition video and VoIP services guarantees low delay.
- 5) In case of network congestion, the bandwidth for third-party communication services is allocated as follows: The third-party communication subservices are not distinguished, and they fairly contend for the bandwidth.
- 6) If the network is not congested, any services can contend for all the free bandwidth. For example, if only video service is transmitted at a moment, and the traffic of the video service is 18 Mbps, transmission of all the traffic of the video service must be guaranteed.
- 7) The uplink network is MPLS network, and a MPLS-EXP value must be set for the corresponding traffic.

**Analysis:**

Table 9 Application Requirements

Service Type	Subservice Name	Subservice Code	Network Segment	Bandwidth (totally 20 Mbps)	QoS Description	Queue	EXP
Postal	Electronic branch operation system	DZHZJ	81.1.1.0/24	0.5 Mbps	PQ	AF3	5
	Electronic remittance system	DZHD	81.1.2.0/24	2 Mbps		AF4	6
	Network operations system	WYXT	81.1.3.0/24	0.5 Mbps		AF2	5
	EMS	EMS	81.1.4.0/24	1 Mbps		AF1	2
Financial	Savings	CC	81.2.1.0/24	3 Mbps	PQ	AF4	6
	Agency and insurance	DLBX	81.2.2.0/24	1 Mbps		AF3	5
	Public service	DG	81.2.3.0/24	2 Mbps		AF2	4
Video OA	High-definition video	GQSP	81.3.1.0/24	4 Mbps	PQ	AF4	6
	OA	OA	81.3.2.0/24	1 Mbps		AF3	5
	VoIP	VoIP	81.3.3.0/24	2 Mbps		AF2	6
Third-party communication	External communication	DSFWL	81.4.1.0/24	3 Mbps	PQ	BE	1

## Configuration

## 1) Configuring traffic classification policies

## 1) Configure ACLs.

```

!
ip access-list extended 101
 10 permit ip 81.1.1.0 0.0.0.255 any
!
ip access-list extended 102
 10 permit ip 81.1.2.0 0.0.0.255 any
!
ip access-list extended 103
 10 permit ip 81.1.3.0 0.0.0.255 any
!
ip access-list extended 104
 10 permit ip 81.1.4.0 0.0.0.255 any
!
ip access-list extended 105

```

```
10 permit ip 81.2.1.0 0.0.0.255 any
!
ip access-list extended 106
10 permit ip 81.2.2.0 0.0.0.255 any
!
ip access-list extended 107
10 permit ip 81.2.3.0 0.0.0.255 any
!
ip access-list extended 108
10 permit ip 81.2.4.0 0.0.0.255 any
!
ip access-list extended 109
10 permit ip 81.3.1.0 0.0.0.255 any
!
ip access-list extended 110
10 permit ip 81.3.2.0 0.0.0.255 any
!
ip access-list extended 111
10 permit ip 81.3.3.0 0.0.0.255 any
!
ip access-list extended 112
10 permit ip 81.3.4.0 0.0.0.255 any
!
ip access-list extended 113
10 permit ip 81.4.1.0 0.0.0.255 any
!
ip access-list extended 114
10 permit ip 81.4.2.0 0.0.0.255 any
!
ip access-list extended 115
10 permit ip 81.4.3.0 0.0.0.255 any
!
ip access-list extended 116
10 permit ip 81.4.4.0 0.0.0.255 any
!
```

## 2) Configure the simple traffic classification.

```
!
diffserv domain JSYZ
mpls-exp-outbound be green map 1
mpls-exp-outbound af1 green map 2
mpls-exp-outbound af2 green map 4
mpls-exp-outbound af3 green map 5
mpls-exp-outbound cs7 green map 6
!
```

## 3) Configure the complex traffic classification.

```
!
```

```
traffic classifier tcy1 or
  if-match acl 101
!
traffic classifier tcy2 or
  if-match acl 102
!
traffic classifier tcy3 or
  if-match acl 103
!
traffic classifier tcy4 or
  if-match acl 104
!
traffic classifier tcj1 or
  if-match acl 105
!
traffic classifier tcj2 or
  if-match acl 106
!
traffic classifier tcj3 or
  if-match acl 107
!
traffic classifier tcj4 or
  if-match acl 108
!
traffic classifier tcv1 or
  if-match acl 109
!
traffic classifier tcv2 or
  if-match acl 110
!
traffic classifier tcv3 or
  if-match acl 111
!
traffic classifier tcv4 or
  if-match acl 112
!
traffic classifier tcw1 or
  if-match acl 113
!
traffic classifier tcw2 or
  if-match acl 114
!
traffic classifier tcw3 or
  if-match acl 115
!
traffic classifier tcw4 or
  if-match acl 116
!
```

```
traffic classifier DZHZJ or
  if-match acl 101
!
traffic classifier DZHD or
  if-match acl 102
!
traffic classifier WYXT or
  if-match acl 103
!
traffic classifier EMS or
  if-match acl 104
!
traffic classifier CC or
  if-match acl 105
!
traffic classifier DLBX or
  if-match acl 106
!
traffic classifier DG or
  if-match acl 107
!
traffic classifier GQSP or
  if-match acl 109
!
traffic classifier OA or
  if-match acl 110
!
traffic classifier VoIP or
  if-match acl 111
!
traffic classifier DSFWL or
  if-match acl 113
!
traffic classifier tc_high or
  if-match mpls-exp 6
!
traffic classifier tc_1 or
  if-match mpls-exp 6
!
traffic classifier tc_2 or
  if-match mpls-exp 5
!
traffic classifier tc_3 or
  if-match mpls-exp 2
!
traffic classifier tc_4 or
  if-match mpls-exp 1
!
```



## 4) Configure traffic behavior criteria.

```
!  
traffic behavior DZHZJ  
  user-queue YZZH inbound  
  service-class be color green  
  remark dscp 11  
!  
traffic behavior DZHD  
  user-queue YZZH inbound  
  service-class af4 color green  
  remark dscp 12  
!  
traffic behavior WYXT  
  user-queue YZZH inbound  
  service-class af2 color green  
  remark dscp 13  
!  
traffic behavior EMS  
  user-queue YZZH inbound  
  service-class af1 color green  
  remark dscp 14  
!  
traffic behavior CC  
  user-queue JR inbound  
  service-class af4 color green  
  remark dscp 15  
!  
traffic behavior DLBX  
  user-queue JR inbound  
  service-class af3 color green  
  remark dscp 16  
!  
traffic behavior DG  
  user-queue JR inbound  
  service-class af2 color green  
  remark dscp 17  
!  
traffic behavior GQSP  
  user-queue OA inbound  
  service-class af4 color green  
  remark dscp 18  
!  
traffic behavior OA  
  user-queue OA inbound  
  service-class af3 color green  
  remark dscp 19  
!
```

```

traffic behavior VoIP
  user-queue OA inbound
  service-class af4 color green
  remark dscp 20
!
traffic behavior DSFWL
  user-queue DSFWL inbound
  service-class be color green
  remark dscp 21
!
traffic behavior DZHHD
  remark dscp 11
!
traffic behavior tb1
  user-queue others inbound
  service-class af4 color green
!
traffic behavior tb2
  user-queue others inbound
  service-class af3 color green
!
traffic behavior tb3
  user-queue others inbound
  service-class af2 color green
!
traffic behavior tb4
  user-queue others inbound
  service-class af1 color green
!

```

#### 5) Configure traffic policies.

```

!
traffic policy YZZH
  classifier DZHJ behavior DZHJ precedence 1
  classifier DZHD behavior DZHD precedence 2
  classifier WYXT behavior WYXT precedence 3
  classifier EMS behavior EMS precedence 4
!
traffic policy JR
  classifier CC behavior CC precedence 1
  classifier DLBX behavior DLBX precedence 2
  classifier DG behavior DG precedence 3
!
traffic policy OA
  classifier GQSP behavior GQSP precedence 1
  classifier OA behavior OA precedence 2
  classifier VoIP behavior VoIP precedence 3
!

```

```

traffic policy DSFWL
 classifier DSFWL behavior DSFWL precedence 1
!
traffic policy tp_other
 classifier tc_4 behavior tb4 precedence 1
 classifier tc_2 behavior tb2 precedence 2
 classifier tc_3 behavior tb3 precedence 3
 classifier tc_1 behavior tb1 precedence 4
!

```

## 2) Configuring queue scheduling

### 1) Configure user queues.

```

!
user-queue YZZH inbound
 cir 4000 pir 20000
 flow-queue YZZH
 user-group-queue JSYZ
 flow-mapping YZZH
!
user-queue JR inbound
 cir 6000 pir 20000
 flow-queue JR
 user-group-queue JSYZ
 flow-mapping JR
!
user-queue OA inbound
 cir 7000 pir 20000
 flow-queue OA
 user-group-queue JSYZ
 flow-mapping OA
!
user-queue DSFWL inbound
 cir 3000 pir 20000
 flow-queue DSFWL
 user-group-queue JSYZ
!
user-queue others inbound
 cir 14000 pir 20000
 flow-queue other
 user-group-queue JSYZ
 flow-mapping other
!

```

### 2) Configure a user group.

```

!
user-group-queue JSYZ inbound
 shaping 20000

```

!

## 3) Configure traffic queues.

```
!  
flow-queue YZZH  
queue be wfq weight 50  
queue af1 wfq weight 100  
queue af2 wfq weight 50  
queue af3 wfq weight 15  
queue af4 wfq weight 200  
queue ef pq  
queue cs6 pq  
queue cs7 pq  
!  
flow-queue JR  
queue be wfq weight 10  
queue af1 wfq weight 100  
queue af2 wfq weight 40  
queue af3 wfq weight 20  
queue af4 wfq weight 60  
queue ef pq  
queue cs6 pq  
queue cs7 pq  
!  
flow-queue OA  
queue be wfq weight 10  
queue af1 wfq weight 10  
queue af2 wfq weight 10  
queue af3 wfq weight 20  
queue af4 wfq weight 120  
queue ef pq  
queue cs6 pq  
queue cs7 pq  
!  
flow-queue DSFWL  
queue be wfq weight 10  
queue af1 wfq weight 10  
queue af2 wfq weight 10  
queue af3 wfq weight 15  
queue af4 wfq weight 15  
queue ef pq  
queue cs6 pq  
queue cs7 pq  
!  
flow-queue other  
queue be wfq weight 10  
queue af1 wfq weight 30  
queue af2 wfq weight 10
```

```

queue af3 wfq weight 20
queue af4 wfq weight 80
queue ef pq
queue cs6 pq
queue cs7 pq
!

```

#### 4) Configure traffic mapping rules.

```

!
flow-mapping YZZH
map flow-queue af3 to port-queue cs7
!
flow-mapping JR
map flow-queue af4 to port-queue cs7
!
flow-mapping OA
map flow-queue af4 to port-queue cs7
!
flow-mapping other
map flow-queue af4 to port-queue cs7
!

```

#### 5) Configure interface queues.

```

!
port-queue jsyz
queue be wfq weight 10
queue af1 wfq weight 10
queue af2 wfq weight 10
queue af3 wfq weight 15
queue af4 wfq weight 15
queue ef pq
queue cs6 pq
queue cs7 pq
!

```

### 3) Configuring interface applications

#### 1) Configuring ingress interfaces.

```

!
interface GigabitEthernet 1/1/3.1
 encapsulation dot1Q 1
 ip address 81.1.1.1 255.255.255.0
 traffic-policy YZZH inbound
!
interface GigabitEthernet 1/1/3.2
 encapsulation dot1Q 2
 ip address 81.2.1.1 255.255.255.0
 traffic-policy JR inbound

```

```

!
interface GigabitEthernet 1/1/3.3
 encapsulation dot1Q 3
 ip address 81.3.1.1 255.255.255.0
 traffic-policy OA inbound
!
interface GigabitEthernet 1/1/3.4
 encapsulation dot1Q 4
 ip address 81.4.1.1 255.255.255.0
 traffic-policy DSFWL inbound
!
    
```

2) Configure egress interfaces.

```

!
interface GigabitEthernet 1/1/1
 port-queue jsyz
 trust upstream JSYZ
 traffic-policy tp_other inbound
!
    
```

## Test Result

Figure 14 Test Results for Postal applications

Chassis: 192.168.50.200, Card: 02, Port: 12									
PGID	Total # Frames	Latency Cut	Latency Cut	Latency Cut	Latency Cut	Bit Rate (/sec)	Byte Count	Byte Rate (/sec)	Frame Rate (/sec)
Traffic of financial services									
5	5,546,010	37,601,860	37,937,440	335,579.94	37,629,835	2,946,640	2,839,557,	368,330	719
6	1,848,621	37,749,165	38,653,564	904,398.74	37,827,507	967,948	946,493,95	120,993	236
7	3,697,391	37,642,937	38,121,899	478,962.00	37,679,323	1,958,210	1,893,064,	244,776	478
Traffic of postal, OA, and external communication services									
9	505,956	38,309,698	39,028,555	718,856.86	38,612,053	660,061	259,049,47	82,507	161
10	1,956,957	37,658,026	38,088,352	430,326.02	37,822,859	2,002,174	1,001,961,	250,271	488
11	443,424	38,309,565	39,726,234	1,416,668.	38,721,222	548,901	227,033,08	68,612	134
12	866,482	37,905,330	39,178,731	1,273,400.	38,166,265	1,076,971	443,638,78	134,621	262
13	2,777,679	37,692,009	37,876,958	184,948.98	37,742,196	3,233,276	1,422,171,	404,159	789
14	717,727	38,185,082	38,591,506	406,424.12	38,293,217	807,625	367,476,22	100,953	197
15	1,396,510	37,862,515	38,108,144	245,628.88	37,932,463	1,586,191	715,013,12	198,273	387
16	3,788,666	37,638,399	38,110,925	472,526.40	37,691,270	4,214,823	1,939,796,	526,852	1,029

The test results show that the H-QoS multi-level scheduling policies meet the requirements of service-specific bandwidth and priority when networks are in congestion.

# Implementation Analysis

## Advantage and Disadvantage

Technically speaking, no technical solution that is similar to or can replace the H-QoS is launched.

Advantage: H-QoS provides end-to-end QoS assurance.

Disadvantage: Because H-QoS processes data services in a centralized manner, it imposes a high requirement on the processing capacity of the system.

## Platform

H3C H-QoS is hardware-dependently implemented by using ASIC-based QoS. Its implementation is dependent upon hardware structures.

Cisco H-QoS is software-dependent. Its implementation is independent of hardware.

Ruijie H-QoS is purely software-dependent. The implementation of all functions of Ruijie H-QoS is independent of hardware.

## Constraints

The standards focus on hierarchical scheduling and traffic shaping. The hierarchical scheduling focuses on bandwidth assurance (CB) and priority assurance (LLQ/Priority). Manufacturers have not implemented hierarchical functions for PQ, CQ, RTPQ, and WFQ, so the implementation of these scheduling functions is not considered temporarily.

## Risks

In terms of related standards, DSL Forum described the H-QoS support for an ATM-based network in BroadbandSuite 1.0 (TR-059, 2003.11), and described the H-QoS support for an Ethernet-based network in BroadbandSuite 3.0 (TR-101, 2006.04). Therefore, the standards were released many years ago.

From the perspective of manufacturers, Shanghai Bell launched products that support H-QoS in 2004; Huawei NE series routers and Multi-Service Control Gateway (MSCG) provided relatively mature support for H-QoS; and Cisco began to support H-QoS in July 2008 (IOS 12.4(20)T).

Ruijie H-QoS is relatively mature and is independently implemented by using command lines similar to Huawei. It does not depend upon existing QoS functions and softwares.

## Comparison

Huawei, H3C, and Cisco have implemented related functions. Because Huawei H-QoS is similar to H3C H-QoS, the following only presents the implementation of H3C H-QoS and Cisco H-QoS.

## H3C H-QoS

### Function description

Figure 15 Principle of H-QoS (1)

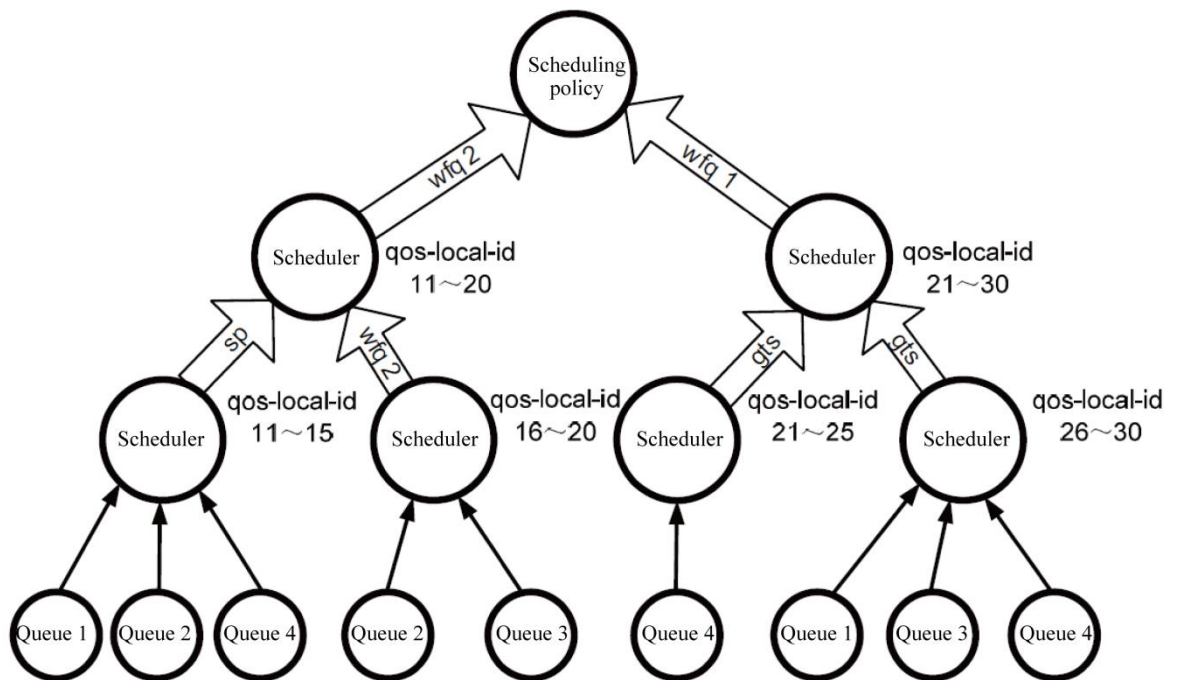


Figure 7-1 shows the principle of the H-QoS. The **qos-local-id** range beside each node is the classification rule of the node. "SP", "WFQ", or "GTS" in an arrow pointing to an upstream node indicates the control parameter of the node. When the scheduling policy in the upper part of the figure is applied to an interface, multi-level classification and management can be implemented for the traffic entering the interface.

The biggest difference between the H-QoS and the conventional single-layer QoS is that, the former can divide the scheduling queues into multiple scheduling levels with different features, such as physical level, logical level, and application level or service level. For example, the physical level is used to manage the bandwidth of all the physical interfaces; the logical level can be used to manage the bandwidth of each user on the interfaces; and the service level can be used to manage the bandwidth of different services of a user. In this way, multi-level queue scheduling is performed to implement hierarchical traffic management, thereby helping carriers to implement multi-user and multi-service management.

### Configuration examples

The key feature of the QoS-Local-ID mode is to identify different service types by using different qos-local-ids. The services connected to the backbone router fall into four types: VoIP, VoD, VPN, and Internet. Different IP address segments are used to bear different service types and distinguish between users, so as to perform control operations, such as rate limiting and bandwidth management, for the traffic of different services.

#### 1. Networking requirements

##### 1) Requirements analysis

The rate of the ingress interface is limited to 1,000 Mbps.

VoIP service requirement: IP preferences: 6 and 7; absolute preferential scheduling; rate limit: 100 Mbps; and two user groups evenly share the bandwidth.



VoD service requirement: IP preferences: 4 and 5; bandwidth-assured scheduling; higher-priority queue scheduling; rate limit: 450 Mbps; and three user groups share the bandwidth according to 2:2:1.

VPN service requirement: IP preferences: 2 and 3; bandwidth-assured scheduling; medium-priority queue scheduling; rate limit: 300 Mbps; and all user groups evenly share the bandwidth. When there are less than three user groups, the rate limit for each user group is 100 Mbps; when there are three or more user groups, all the user groups evenly share the bandwidth.

Internet service requirement: IP preferences: 0 and 1; lowest scheduling authority; low-priority queue scheduling; free network bandwidth is recycled; and five user groups evenly share the bandwidth. Because the rates of other services are limited, the assured bandwidth for the Internet service is 150 Mbps, and the minimum bandwidth for each user group is 30 Mbps. The total bandwidth for the Internet service is not limited, but the maximum bandwidth for each user group is limited to 36 Mbps.

## 2) Allocation of source IP addresses

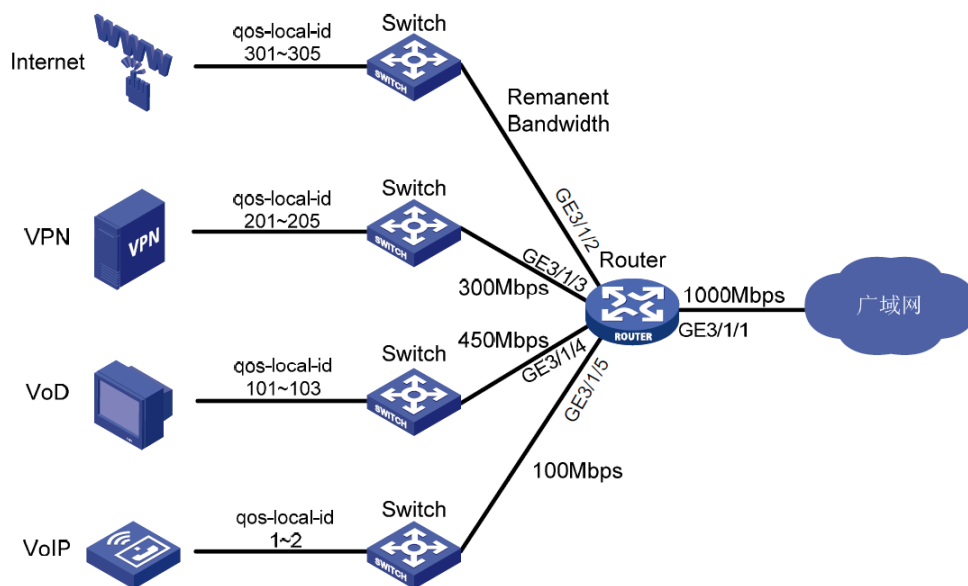
VoIP: 10.1.1.X and 10.1.2.X for bearing two user groups.

VoD: 20.1.1.X, 20.1.2.X, and 20.1.3.X for bearing user groups.

VPN: 30.1.1.X, 30.1.2.X, 30.1.3.X, 30.1.4.X, and 30.1.5.X for bearing five user groups.

Internet: 40.1.1.X, 40.1.2.X, 40.1.3.X, 40.1.4.X, and 40.1.5.X for bearing five user groups.

Figure 16 Principle of H-QoS (2)



## 2. Configuration

The IP preferences for the VoIP traffic are 6 and 7, so the VoIP traffic is mapped to the predefined forwarding class NC. The IP preferences for the VoD traffic are 4 and 5, so the VoD traffic is mapped to the predefined forwarding class EF. The IP preferences for the VPN traffic are 2 and 3, so the VPN traffic is mapped to the predefined forwarding class AF; and the IP preferences for the Internet traffic are 0 and 1, so the Internet traffic is mapped to the predefined forwarding class BE.

The traffic of VoIP, VoD, VPN, and Internet traffic is implemented by using forwarding groups. QoS-Local-ID mapping is performed based on source IP addresses of the users, and the mapping of QoS-Local-ID to a forwarding group is performed during the instantiation operation.

The classification of VoIP, VoD, VPN, and Internet traffic is implemented by instantiation.

## Cisco H-QoS

### Function description

Hierarchical Queuing Framework (HQF) is an MQC-based software QoS function that Cisco began to support in IOS Software Release 12.4(20)T. The HQF extended the original MQC framework, and supports auxiliary policy-map, and the police, shape, bandwidth, and priority functions that are based on the policy-map, so as to configure hierarchical QoS. The HQF brings the following advantages to the customers :

- 1) Software-based MQC, which supports all Cisco routers
- 2) Hierarchical queue scheduling
- 3) Hierarchical shaping and queuing
- 4) Class-based fair queuing and discarding policy

### Configure examples

HQF support list:

#### 1. Hierarchical queuing

```
policy-map child
  class child-c1
    bandwidth 400
  class child-c2
    bandwidth 400
policy-map parent
  class parent-c1
    bandwidth 1000
    service-policy child
  class parent-c2
    bandwidth 2000
    service-policy child
```

#### 2. Class-based fair queuing

```
policy-map p1
  class c1
    bandwidth 1000
    fair-queue
```

#### 3. ATM PVC-based shaping

#### 4. Rate-unlimited SP

```
policy-map p1
  class c1
    priority
  class c2
    bandwidth remaining percent 20
```

## 5. Rate-limited SP

```

policy-map p1
  class c1
    priority
    police cir 1000000 conform-action transmit exceed-action drop

```

## 6. WRED based on class-default

```

policy-map p1
  class class-default
    random-detect precedence-based
    random-detect precedence 0 40 80

```

## 7. Extended WRED

**random-detect atm-clp-based Command**

```

policy-map p1
  class c1
    bandwidth 1000
    random-detect atm-clp-based
    random-detect clp 0 <min> <max> <mark-probability>

```

**random-detect cos-based Command**

```

policy-map p1
  class c1
    bandwidth 1000
    random-detect cos-based
    random-detect cos 0 <min> <max> <mark-probability>

```

**random-detect thresholds set in bytes**

```

policy-map p1
  class c1
    bandwidth 1000
    random-detect precedence-based
    random-detect precedence 0 100 bytes 400 bytes 100

```

**random-detect thresholds set in milliseconds**

```

policy-map p1
  class c1
    bandwidth 1000
    random-detect precedence-based
    random-detect precedence 0 200 ms 800 ms 100

```

## 8. ms-based queue depth configuration

```

policy-map p1
  class c1
    bandwidth 1000
    queue-limit 1000 bytes
  class c2
    bandwidth 1000
    queue-limit 500 bytes

```

## Conclusion

H-QoS is an important enhancement and supplement to the conventional QoS solution. The conventional DiffServ QoS deployment solution relies on multi-level devices to implement end-to-end service assurance, whereas H-QoS are centralizedly deployed to implement end-to-end assurance.

## References

- [1] Technical Report DSL Forum TR-059 DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services
- [2] Technical Report DSL Forum TR-101 Migration to Ethernet-Based DSL Aggregation



**H-QoS**  
Technology White Paper

[www.ruijienetworks.com](http://www.ruijienetworks.com)