Solutions | Products | Ordering | Support | Partners | Training | Corporate

Tech Notes

Quality of Service Order of Operation

TAC Notice: What's Changing on TAC Web

Contents

Introduction

This document illustrates the order in which Quality of Service (QoS) features are executed when applied inbound or outbound to an interface on a router running Cisco® IOS software. QoS policies are configured with the modular QoS Command Line Interface (MQC). This document also discusses IP header marking, like DSCP and IP Precedence, and the order in which the components of a QoS policy are evaluated by the router.

Prerequisites

Requirements

Readers of this document should have knowledge of:

- Basic QoS methodologies

Components Used

The example output in the Configurations section of this document was captured on a Cisco 7513 Series platform, running Cisco IOS Release 12.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Common Classification

Classification is the process of defining traffic classes that sort traffic into categories groups of flows. Classification defines the "match criteria" for each class of traffic that is to be treated by a QoS policy. More specifically, it defines the "traffic filter" that packets are checked against when a service-policy is applied.

Both distributed and non-distributed platforms match packets to a single class in a policy-map. Matching terminates at the first matching class. If two classes within a policy-map match the same IP precedence or IP address range, the packet always belongs to the first matching class. For this reason, class order within a policy-map is very important.

This classification approach is called "common classification" and has these benefits:

- Accurate accounting and the avoidance of double-accounting problems that were seen before "common classification".
- Reduces the impact of access control lists (ACLs) on the CPU since the ACL is checked once per class, rather than once per feature.
- Faster lookup of packet headers because of caching.

Common classification is enabled automatically when you attach an input or output policy-map with the **service-policy** command.

The table below illustrates the order of operation with common classification. It is important to understand from the table when classification occurs in the context of QoS features. On the inbound path, a packet is classified before it is switched. On the outbound path, a packet is classified after it is switched.

Inbound	Outbound
1. QoS Policy Propagation through Border Gateway Protocol (BGP) (QPPB) 2. Input common classification	1. CEF or Fast Switching 2. Output common classification

3. Input ACLs 4. Input marking (class-based marking or Committed Access Rate (CAR)) 5. Input policing (through a class-based policer or CAR) 6. IP Security (IPSec) 7. Cisco Express Forwarding (CEF) or Fast Switching	3. Output ACLs 4. Output marking 5. Output policing (through a class-based policer or CAR) 6. Queueing (Class-Based Weighted Fair Queueing (CBWFQ) and Low Latency Queueing (LLQ)), and Weighted Random Early Detection (WRED)

Note: Inbound Network-Based Application Recognition (NBAR) happens after ACLs and before policy-based routing.

Important changes have been implemented regarding feature ordering and remarked value usage. These changes include moving input CAR, input MAC, and IP precedence accounting functions to occur before MQC output classification:

- Input rate-limiting, or CAR, applies to packets following the process switching path and destined to the router. Previously, only packets switched through the router using CEF could be rate-limited.
- New IP precedence values set by input CAR or QPPB can be used for selecting a Virtual Circuit (VC) in an ATM VC bundle.
- IP precedence, Differentiated Services Code Points (DSCP), and QoS group values set by input CAR or QPPB can be used for MQC output packet classification.

Marking and Other QoS Actions on the Same Router

A frequent application of QoS is to remark a packet and then apply an action which considers the remarked value on the same interface or on the same router. You can configure both marking and other QoS actions with common classification.

You can remark packets with these QoS features:

- **set** command with class-based marking
- **police** command with class-based policing
- CAR

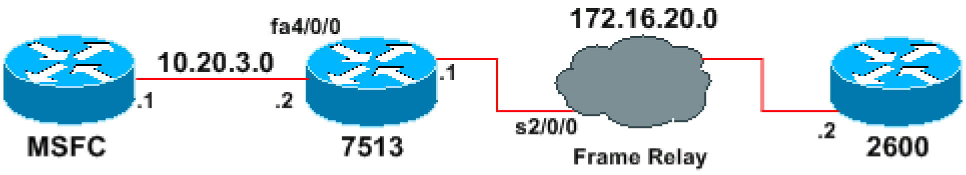
This table indicates whether or not a remarked value is considered by a QoS action in a service-policy.

Location of Policy	Value Used by the Outbound Policy Actions
Mark and apply QoS action in the same policy.	QoS actions use the original value of the packet when it is commonly classified. The packet will carry the new value when it is transmitted, and the next router uses the new value.
Mark with inbound policy and apply QoS action with outbound policy.	QoS actions use the new or remarked value when classifying traffic against the outbound policy.

On the outbound path, common classification happens before any QoS features are applied. A result of this approach is that any QoS features applied on the outbound policy act upon the original priority value. If you need to take actions based on a remarked value on the same router, then you must mark the packets on the incoming interface and apply other QoS actions based on this new priority on the outgoing interface.

Network Diagram

The configurations in this section uses this network diagram:



Note: The Multilayer Switch Feature Card (MSFC) is acting as a host.

Configurations

This example demonstrates how the order of operations can affect packet marking.

Separate Marking and Shaping Policy Configuration

```
class-map match-all In_Mark
   match any
policy-map In_Bound
  class In_Mark
    set ip precedence 5

!--- Use Private address below:

interface FastEthernet4/0/0
 ip address  10.20.3.2 255.255.255.0
ip route-cache distributed
 service-policy input In_Bound
```

```
!--- Apply the input policy for class-based marking.


class-map match-all Out_Shaper
match ip precedence 5
!
policy Map Outbound_Shaper
class one
    shape average 64000 256 256

!--- Use Private address below:

interface Serial2/0/0
 ip address 172.16.20.1 255.255.255.252
ip route-cache distributed
 service-policy output Outbound_Shaper

!--- Apply the output policy for class-based shaping.
```

Complete these steps to confirm the marking and shaping policies:

1. Use the **ping** command to the 172.16.20.2 destination address. The ping matches the criteria of the class-map named "In_Mark".

   ```
   msfc# ping 172.16.20.2

   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 40.1.44.2, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
   ```

2. Use the **show policy-map interface fast 4/0/0** command to view the match counters of the input class-based marking policy. The classification mechanism is successfully matched on the IP packets, and remarked the IP precedence value to five.

   ```
   7513# show policy-map interface fast 4/0/0
    FastEthernet4/0/0
     Service-policy input: In_Bound

       Class-map: In_Mark (match-all)
         5 packets, 570 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match: any
         QoS Set
           ip precedence 5
             Packets marked 5

       Class-map: class-default (match-any)
         0 packets, 0 bytes
         5 minute offered rate 0 BPS, drop rate 0 BPS
         Match: any
   ```

3. Use the **show policy-map interface serial 2/0/0** command to view the match counters of the outbound class-based shaping policy. The classification mechanism is successfully matched on

the remarked IP precedence value five in the packet header, and queued the packets to the correct class.

```
7513# show policy-map interface serial 2/0/0
 Serial2/0/0

  Service-policy output: Outbound_Shaper

    Class-map: Out_Shaper(match-all)
      5 packets, 520 bytes
      5 minute offered rate 0 BPS, drop rate 0 BPSMatch: ip precedence 5
      queue size 0, queue limit 16
      packets output 5, packet drops 0
      tail/random drops 0, no buffer drops 0, other drops 0
      Shape: cir 64000,  Bc 256,  Be 256
        output bytes 520, shape rate 0 BPS

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 BPS, drop rate 0 BPS
      Match: any  (1327)
```

You can see what happens when we configure a single service-policy that applies both shaping and marking to a class of traffic, as in the following example.

Single Marking and Shaping Policy Configuration

```
class-map match-all prec5
  match any
!
policy-map shape_five
  class prec5
    set ip precedence 5
    shape average 64000 256 256
int serial1/0/0
  service-policy out shape_five
```

The output from the **show policy-map interface serial 2/0/0** command shows that the router remarked the five ping packets, but the packets were queued to the class-default class. The QoS classification mechanisms on this router did not consider the remarked value in the IP precedence field.

```
7513# show policy-map interface serial 2/0/0
 Serial2/0/0

  Service-policy output: shape_five

    Class-map: prec5 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 BPS, drop rate 0 BPS
      Match: ip precedence 5  (1377)
      queue size 0, queue limit 16
      packets output 0, packet drops 0
      tail/random drops 0, no buffer drops 0, other drops 0
      QoS Set
        ip precedence 5
          Packets marked 5
      Shape: cir 64000,  BC 256,  Be 256
```

```
          output bytes 0, shape rate 0 BPS

      Class-map: class-default (match-any)
        5 packets, 520 bytes
        5 minute offered rate 0 BPS, drop rate 0 BPS
        Match: any
```

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for RP
Service Providers: MPLS
Provision SA probes - Apr 11, 2005 MPLS destroys my network - Apr 11, 2005 Minimum, Maximum threshold and mark threshold prob calculation - Apr 11, 2005 Targetted LDP sessions - Apr 10, 2005 VLAN no connection. - Apr 9, 2005
Virtual Private Networks: Services
PPTP problems after upgrade - Apr 11, 2005 Network Bandwidth Measurement - Apr 8, 2005 Maximum connections for VPN Concentrator behind a PIX - Apr 6, 2005 Cisco qdm 2.1 - Apr 5, 2005 Error Message - Apr 4, 2005
Virtual Private Networks: Security
Cisco VPN client via IPSEC - Apr 11, 2005 PIX 520 and OS 7.0 - Apr 11, 2005 VPN Client with PIX with auth from Microsoft CA - Apr 11, 2005 Ipsec - Packet Lost - Apr 11, 2005 NAT Traversal on pix site to site VPN - Apr 11, 2005

Related Information

- **Qos Support Page**
- **Technical Support - Cisco Systems**

Home | How to Buy | Login | Profile | Feedback | Site Map | Help