Precedencia de paquetes en QoS con DiffServ

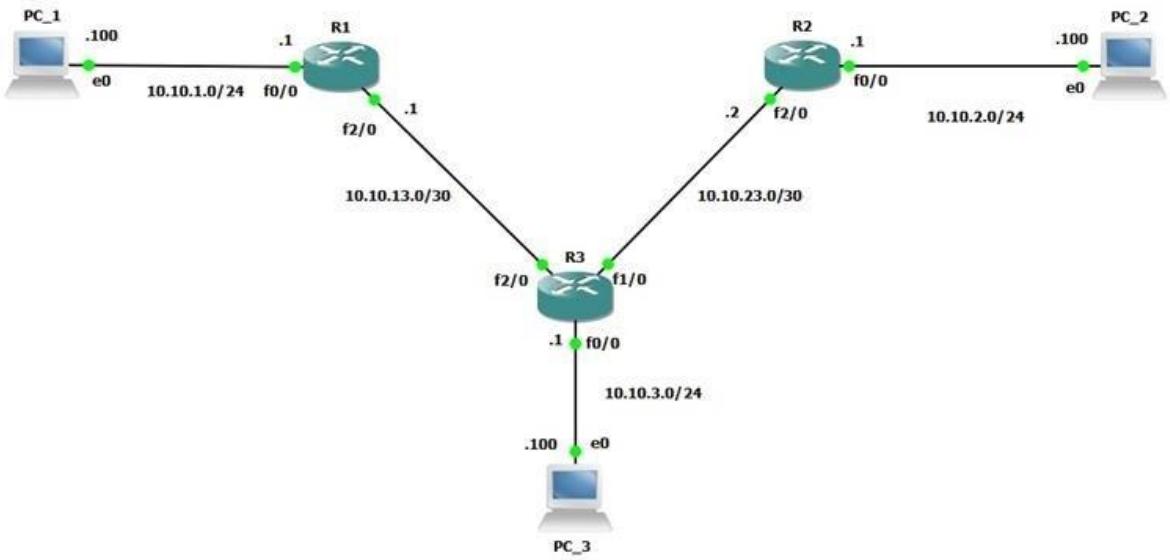
Introducción

Servicios diferenciados (DiffServ) es un nuevo modelo en el cual el tráfico es procesado a través de sistemas intermedios con prioridades relativas en base al campo Tipo de servicios (ToS). Definido en RFC 2474 y RFC 2475, el estándar DiffServ reemplaza la especificación original para definir la prioridad del paquete descrita en RFC 791.

DiffServ aumenta el número de niveles de prioridad definibles al reasignar los bits de un paquete de IP para que se les haga una marcación prioritaria. La arquitectura DiffServ define el campo DiffServ (DS), que reemplaza el campo ToS de IPv4 para tomar decisiones de comportamiento por salto (PHB), sobre la clasificación de paquetes y las funciones de condicionamiento del tráfico, tales como medición, marcado, forma y vigilancia. Los RFC no dictan la manera de implementar PHB; esta responsabilidad es del vendedor. Cisco implementa técnicas de colocación en cola que pueden basar su PHB en la precedencia de IP o en el valor DSCP del encabezado IP de un paquete. Sobre la base de la precedencia DSCP o IP, el tráfico se puede clasificar en una clase de servicio determinada. A los paquetes incluidos en una clase de servicio se los trata del mismo modo.

No es suficiente conocer las características del software, se necesita saber a qué plataformas son aplicables. Las funciones de QoS dependen mucho de la plataforma sobre la que se aplique. Algunas características se pueden aplicar solo a los enrutadores, otras solo a los switch y, algunos pueden ser diferentes entre miembros de la misma familia. Por ejemplo, no todas las características de QoS disponibles para Cisco 3560 son válidas para Cisco 3550.

La topología utilizada para esta práctica y para la simulación es la siguiente:



Objetivos

El propósito de la práctica es mostrarle cómo puede configurar QoS y verificar que se aplique correctamente.

Desarrollo

Se le ha asignado la tarea de configurar la siguiente política de QoS:

- Asignar al tráfico ICMP la precedencia de IP 1
- Asignar al tráfico HTTP la precedencia IP 3
- Asignar al tráfico OSPF la precedencia de IP 7
- Controla el tráfico ICMP a un máximo de 8 Kbps.
- Asigne un ancho de banda de 10Mbps para el tráfico HTTP
- Configure una prioridad estricta para el tráfico OSPF y asigne 1Mbps
- Deja el resto del tráfico en el mapa de clase predeterminado.

Una vez que se haya configurado la topología y se hayan encendido todos los dispositivos, deberá configurar las tres PC con direcciones IP y puerta de enlace predeterminada conforme a la topología.

Hay una cosa que no se muestra en el diagrama: R1, R2 y R3 ejecutan el protocolo OSPF para que todas las PC puedan alcanzarse entre sí, por lo que hay que levantarlo (todos en el área de backbone).

Esta es la tabla de enrutamiento de R2:

```
R2#show ip route | begin Gateway
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 5 subnets
O       10.10.1.0 [110/3] via 10.10.23.3, 00:40:27, FastEthernet2/0
C       10.10.2.0 is directly connected, FastEthernet0/0
O       10.10.3.0 [110/2] via 10.10.23.3, 00:40:27, FastEthernet2/0
O       10.10.13.0 [110/2] via 10.10.23.3, 00:40:27, FastEthernet2/0
C       10.10.23.0 is directly connected, FastEthernet2/0
R2#
```

Una vez que inicie los hosts, deberá configurar la dirección IP en eth0 de cada host y la puerta de enlace predeterminada que apunta al enrutador al que están conectados, como se muestra en el diagrama.

Puede pegar esta configuración en R1 para configurar los mapas de clase, las listas de acceso y los mapas de políticas y aplicarlos en las interfaces correctas:

```
R1#show running-config | section class-map
class-map match-all OSPF
 match protocol ospf
class-map match-all MATCH_HTTP
 match access-group 105
class-map match-all ICMP_A_NUCLEO
 match  precedence 1
```

```
class-map match-all HTTP_A_NUCLEO
 match  precedence 3
class-map match-all MATCH_ICMP
 match access-group 101
R1#show running-config | section policy-map
policy-map DESDE_HOST
 class MATCH_ICMP
  set precedence 1
 class MATCH_HTTP
  set precedence 3
policy-map A_NUCLEO
 class ICMP_A_NUCLEO
  bandwidth 8
  police cir 8000
    conform-action transmit
    exceed-action drop
 class HTTP_A_NUCLEO
  bandwidth 10000
 class OSPF
  set precedence 7
  priority 1000

R1#show  running-config | section access-list
access-list 101 permit icmp any any
access-list 101 remark "match icmp"
access-list 105 remark "match http"
access-list 105 permit tcp any any eq www
R1#show running-config interface f0/0
Building configuration...

Current configuration : 126 bytes
!
interface FastEthernet0/0
 ip address 10.10.1.1 255.255.255.0
 duplex auto
 speed auto
 service-policy input DESDE_HOST
end

R1#show running-config interface f2/0
Building configuration...

Current configuration : 126 bytes
!
interface FastEthernet2/0
 ip address 10.10.13.1 255.255.255.0
 duplex auto
 speed auto
 service-policy output A_NUCLEO
end

R1#
```

Las mismas listas de acceso, mapas de clase y mapas de políticas deben configurarse en R2 y R3. Solo preste atención a las interfaces a las que asigna los mapas de políticas y la dirección. Puede pegar esta configuración en R1 para configurar los mapas de clase, las listas de acceso y los mapas de políticas y aplicarlos en las interfaces correctas:

- El mapa de políticas A_NUCLEO debe aplicarse en la dirección de salida de una interfaz hacia otro enrutador.
- El mapa de políticas DESDE_HOST debe aplicarse en la dirección de entrada de una interfaz hacia una PC.

Verifiquemos si hubo algún paquete ICMP o HTTP enviado por PC_1. Observe que estoy verificando el mapa de políticas desde f0/0, donde se realiza la coincidencia:

```
R1#show policy-map interface f0/0
 FastEthernet0/0

  Service-policy input: DESDE_HOST

    Class-map: MATCH_ICMP (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      QoS Set
        precedence 1
          Packets marked 0

    Class-map: MATCH_HTTP (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 105
      QoS Set
        precedence 3
          Packets marked 0

    Class-map: class-default (match-any)
      3 packets, 981 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
R1#
```

Revisemos el mapa de políticas desde la interfaz f2/0 en R2. Este mapa de política debe aplicar los límites de ancho de banda en caso de que el tráfico supere el límite que configuramos:

```
R1#show policy-map interface f2/0
 FastEthernet2/0

  Service-policy output: A_NUCLEO

    Class-map: ICMP_A_NUCLEO (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 1
      Queueing
        Output Queue: Conversation 265
        Bandwidth 8 (kbps)Max Threshold 64 (packets)
```

```
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: HTTP_A_NUCLEO (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 3
      Queueing
        Output Queue: Conversation 266
        Bandwidth 10000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: OSPF (match-all)
      16 packets, 1504 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ospf
      QoS Set
        precedence 7
          Packets marked 16
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 1000 (kbps) Burst 25000 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: class-default (match-any)
      20 packets, 2051 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
R1#
```

Como puede ver, no hubo paquetes ICMP o HTTP, pero coincidimos con los paquetes OSPF. Hasta ahora, se habían enviado 16 paquetes y marcamos 16 con Precedencia de IP 7. Como también puede ver, se configuró la "prioridad estricta" para el tráfico OSPF con un ancho de banda de 1Mbps.

Simulemos una solicitud HTTP de R1 a R2. Haremos un telnet en el puerto 80 en R2. Debido a que no hay un servidor HTTP real ejecutándose en R2, la conexión será rechazada, pero, aun así, el paquete será tratado como un paquete HTTP.

```
tc@PC_1:~$ telnet 10.10.2.100 80
telnet: can't connect to remote host (10.10.2.100): Connection refused
tc@PC_1:~$
```

Revisemos R1 y veamos si coincidimos con algún paquete HTTP y lo marcamos con Precedencia de IP 3:

```
R1#show policy-map interface f0/0 input class MATCH_HTTP
 FastEthernet0/0

  Service-policy input: DESDE_HOST

    Class-map: MATCH_HTTP (match-all)
      1 packets, 74 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 105
      QoS Set
        precedence 3
          Packets marked 1
R1#
```

Como puede ver, hicimos coincidir un paquete HTTP y lo marcamos con IP Precedence 3.

Deberíamos ver que el mismo paquete coincida y sea establecido por R3 en la dirección de salida de la interfaz f1/0:

```
R3#show policy-map interface f1/0 output class HTTP_A_NUCLEO
 FastEthernet1/0

  Service-policy output: A_NUCLEO

    Class-map: HTTP_A_NUCLEO (match-all)
      1 packets, 74 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 3
      Queueing
        Output Queue: Conversation 266
        Bandwidth 10000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
R3#
```

Debido a que no estamos enviando a alta velocidad y porque no hay congestión, no alcanzaremos el límite de 10 Mbps asignados al tráfico HTTP.

Podemos probar la vigilancia policial utilizando el tráfico ICMP y ver cómo puede eliminar el paquete cuando alcanza el límite de ancho de banda asignado.

Actualmente, el tráfico ICMP se controla a 8 Kbps. Debido a que las PC no pueden enviar más de un paquete ICMP por segundo, no podremos alcanzar el límite. Sin embargo, podemos usar el ping rápido desde R1 y enviar paquetes ICMP con IP Precedence 1. Obtendremos una respuesta solo para algunos de los paquetes, porque algunos de ellos se eliminarán debido a la tasa de la policía.

Comencemos un ping extendido desde R1 hacia R2 y veamos cuántos paquetes se eliminaron y cuántos fueron transmitidos por R1 a R3 y luego a R2.

En el ping extendido, se le solicita que ponga el valor de TOS para la Precedencia de IP 1. Esto es 32 (00100000).

```
R1#ping
Protocol [ip]:
Target IP address: 10.10.23.2
Repeat count [5]: 100
Datagram size [100]: 1400
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.10.13.1
Type of service [0]: 32
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1400-byte ICMP Echos to 10.10.23.2, timeout is 2 seconds:
Packet sent with a source address of 10.10.13.1
Packet sent with the DF bit set
!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.
!.!.!.!.!.!.!.!.!.!.!.!.!.!.!.
Success rate is 50 percent (50/100), round-trip min/avg/max = 60/111/284
ms
R1#
```

Así que vamos a ver qué pasó en R1:

```
R1#show policy-map interface f2/0 output class ICMP_A_NUCLEO
 FastEthernet2/0

  Service-policy output: A_NUCLEO

    Class-map: ICMP_A_NUCLEO (match-all)
      100 packets, 141400 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 1
      Queueing
        Output Queue: Conversation 265
        Bandwidth 8 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 50/70700
        (depth/total drops/no-buffer drops) 0/0/0
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 50 packets, 70700 bytes; actions:
          transmit
        exceeded 50 packets, 70700 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps
R1#
```

Como puede ver, se suponía que se enviaran 100 paquetes; 50 fueron conformes (es decir, fueron transmitidos) y 50 fueron excedentes. Configuramos este mapa de políticas para eliminar

cualquier paquete excedente, de ahí el 50% de pérdida de paquetes. La mitad de los paquetes no fueron enviados por R1 a R3.

Así que veamos cuántos paquetes R3 se envían a R2:

```
R3#show policy-map interface f2/0 output class ICMP_TO_CORE
 FastEthernet2/0

  Service-policy output: A_NUCLEO

    Class-map: ICMP_TO_CORE (match-all)
      50 packets, 70700 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 1
      Queueing
        Output Queue: Conversation 265
        Bandwidth 8 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 50 packets, 70700 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps
R3#
```