УДК 621.39

УПРАВЛІННЯ ПЕРЕВАНТАЖЕННЯМИ У МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ ЗА ДОПОМОГОЮ ОРГАНІЗАЦІЇ ЧЕРГ

Москвитіна А.А., Романов А.О.
Інститут телекомунікаційних систем НТУУ «КПІ»
Київський коледж зв'язку
E-mail: fuffypickly@gmail.com

Congestion management of data network using queue strategies
This article provides queue strategies as the one of the concepts of QoS. Also the example of organization of LLQ strategy is reviewed.

Будь-яка реальна мережа передачі даних схильна до перевантажень. Для відповідності параметрів якості зв'язку параметрам, заявленим в угоді про надання послуг, в мережу впроваджуються політики якості обслуговування (QoS, Quality of Service). По суті, QoS показує ймовірність проходження пакетів між двома точками мережі.

Одним з механізмів QoS є управління перевантаженнями мережі, що досягається організацією черги. Зазвичай використовується метод FIFO (перший прийшов - перший вийшов), однак при інтенсивному трафіку створюється «затор», і всі пакети, які не зайняли місце у буфері черги FIFO - губляться. Тому, оптимальніше використовувати «розумну» чергу, в якій пріоритет у пакетів залежить від типу сервісу. Найбільш широке застосування отримали механізми зважених справедливих черг CBWFQ і черг з малою затримкою LLQ (модифікація CBWFQ).

Налаштування черг включає конфігурацію класів (class-map), групування у policy-map і прив'язку визначеного інтерфейса до service-map.[1] Орієнтована структура призначення політик та класів показана на рис. 1:

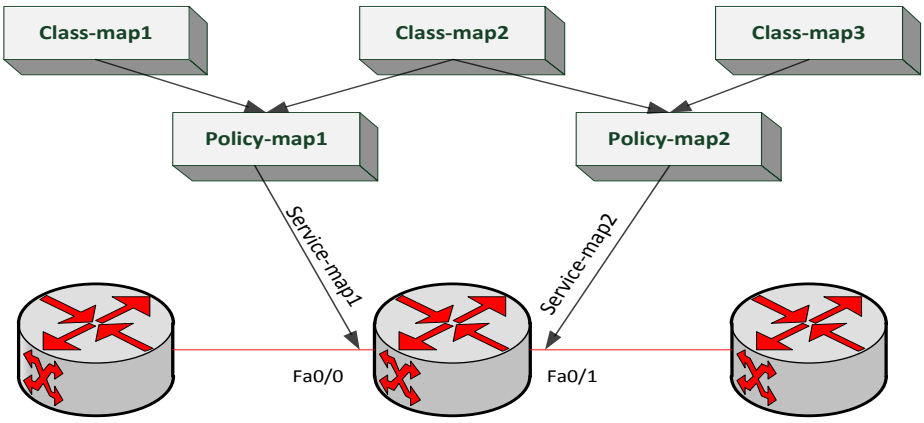

Рис. 1 Орієнтована структура призначення політик та класів

Поставимо задачу: Заборонити потік ICMP-пакетів від користувача VPCS1 до VPCS2 розміром більше 700 біт, а для ICMP-пакетів від 300 до 700 обмежити швидкість до 8000 bps. Змоделюємо стенд (див. рис. 2) в емуляторі GNS3.

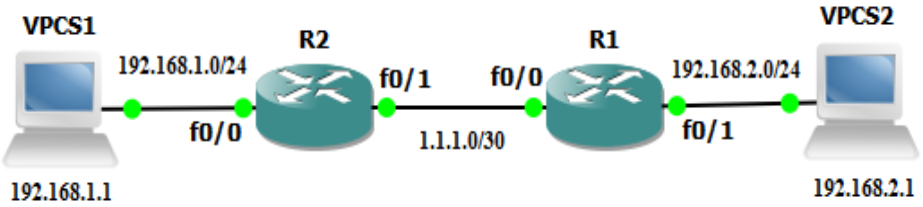

Рис. 2 Змодельований стенд

Проведемо налаштування відповідно до адресації, зазначеної на малюнку. R2(config)#access-list 1 permit 192.168.1.0 0.0.0.255. Налаштуємо на R2 class-mapicmp [2], для якого будемо задавати обмеження по швидкості і BIGicmp для заборони пакетів більше 700 біт. Атрибут [match-all | match-any] визначає порядок застосування правил класу [логічне І | логічне АБО] відповідно.

```
R2(config)#class-mapmatch-allicmp
R2(config-cmap)# matchaccess-group 1
R2(config-cmap)# matchprotocolicmp
R2(config-cmap)# matchpacketlengthmin 300 max 700
R2(config-cmap)#class-mapmatch-allBIGicmp
R2(config-cmap)# matchaccess-group 1
R2(config-cmap)# matchprotocolicmp
R2(config-cmap)# matchpacketlengthmin 701
```

Налаштуємо policy-mapPOLICYicmp [2], в якому задамо додаткові умови:

```
R2(config-cmap)# policy-mapPOLICYicmp
R2(config-pmap)# classicmp
R2(config-pmap-c)# policerate 8000 bps
R2(config-pmap-c-police)# conform-actiontransmit
R2(config-pmap-c-police)# exceed-actiondrop
R2(config-pmap)# classBIGicmp
R2(config-pmap-c)# drop
```

У директорії config-pmap-c задається основне правило політики для класу, в config-pmap-c-police задаються правила для даних, що потрапили в область класу.

Для того, щоб застосувати правила політики до певного інтерфейсу, вкажемоservice-map [2]

```
R2(config-pmap-c)#int fa0/1
R2(config-if)# service-policyoutputPOLICYicmp
```

Протестуємо створену конфігурацію утилітою PING. При цьому будемо задавати різні розміри пакетів даних. Результати перевірки зведені у таблицю 1.

```
   NAME    IP/MASK             GATEWAY             MAC          LPORT    RHOST:PORT
VPCS1   192.168.1.1/24      192.168.1.254     00:50:79:66:68:00  20000  127.0.0.1:30000
VPCS2   192.168.2.1/24      192.168.2.254     00:50:79:66:68:01  20001  127.0.0.1:30001
```

Таблиця 1. Результати перевірки конфігурації за допомогою утиліти PING

VPCS[1]>ping 192.168.2.1 -c 15 -l 299	VPCS[1]>ping 192.168.2.1 -c 15 -l 300
192.168.2.1 icmp_seq=1 ttl=62 time=49.003 ms	192.168.2.1 icmp_seq=1 timeout
192.168.2.1 icmp_seq=2 ttl=62 time=45.004 ms	192.168.2.1 icmp_seq=2 ttl=62 time=46.003 ms
192.168.2.1 icmp_seq=3 ttl=62 time=36.002 ms	192.168.2.1 icmp_seq=3 ttl=62 time=35.002 ms
192.168.2.1 icmp_seq=4 ttl=62 time=36.002 ms	192.168.2.1 icmp_seq=4 ttl=62 time=53.005 ms
192.168.2.1 icmp_seq=5 ttl=62 time=35.002 ms	192.168.2.1 icmp_seq=5 ttl=62 time=32.001 ms
192.168.2.1 icmp_seq=6 ttl=62 time=49.002 ms	192.168.2.1 icmp_seq=6 ttl=62 time=37.002 ms
192.168.2.1 icmp_seq=7 ttl=62 time=47.002 ms	192.168.2.1 icmp_seq=7 timeout
192.168.2.1 icmp_seq=8 ttl=62 time=37.003 ms	192.168.2.1 icmp_seq=8 ttl=62 time=30.001 ms
192.168.2.1 icmp_seq=9 ttl=62 time=14.003 ms	192.168.2.1 icmp_seq=9 ttl=62 time=61.003 ms
192.168.2.1 icmp_seq=10 ttl=62 time=34.002 ms	192.168.2.1 icmp_seq=10 ttl=62 time=33.002 ms
192.168.2.1 icmp_seq=11 ttl=62 time=36.002 ms	192.168.2.1 icmp_seq=11 ttl=62 time=58.003 ms
192.168.2.1 icmp_seq=12 ttl=62 time=31.002 ms	192.168.2.1 icmp_seq=12 ttl=62 time=33.001 ms
192.168.2.1 icmp_seq=13 ttl=62 time=34.002 ms	192.168.2.1 icmp_seq=13 timeout
192.168.2.1 icmp_seq=14 ttl=62 time=54.003 ms	192.168.2.1 icmp_seq=14 ttl=62 time=48.003 ms
192.168.2.1 icmp_seq=15 ttl=62 time=31.004 ms	192.168.2.1 icmp_seq=15 ttl=62 time=36.002 ms

Таблиця 1(продовження). Результати перевірки конфігурації за допомогою утиліти PING

```
VPCS[1]>ping 192.168.2.1 -c 15 -l 700
192.168.2.1 icmp_seq=1 timeout
192.168.2.1 icmp_seq=2 ttl=62 time=36.002 ms
192.168.2.1 icmp_seq=3 ttl=62 time=36.002 ms
192.168.2.1 icmp_seq=4 ttl=62 time=32.002 ms
192.168.2.1 icmp_seq=5 ttl=62 time=46.003 ms
192.168.2.1 icmp_seq=6 timeout
192.168.2.1 icmp_seq=7 ttl=62 time=21.005 ms
192.168.2.1 icmp_seq=8 timeout
192.168.2.1 icmp_seq=9 ttl=62 time=34.002 ms
192.168.2.1 icmp_seq=10 timeout
192.168.2.1 icmp_seq=11 ttl=62 time=47.004 ms
192.168.2.1 icmp_seq=12 ttl=62 time=38.004 ms
192.168.2.1 icmp_seq=13 timeout
192.168.2.1 icmp_seq=14 ttl=62 time=39.002 ms
192.168.2.1 icmp_seq=15 timeout
```

```
VPCS[1]>ping 192.168.2.1 -c 15 -l 701
192.168.2.1 icmp_seq=1 timeout
192.168.2.1 icmp_seq=2 timeout
192.168.2.1 icmp_seq=3 timeout
192.168.2.1 icmp_seq=4 timeout
192.168.2.1 icmp_seq=5 timeout
192.168.2.1 icmp_seq=6 timeout
192.168.2.1 icmp_seq=7 timeout
192.168.2.1 icmp_seq=8 timeout
192.168.2.1 icmp_seq=9 timeout
192.168.2.1 icmp_seq=10 timeout
192.168.2.1 icmp_seq=11 timeout
192.168.2.1 icmp_seq=12 timeout
192.168.2.1 icmp_seq=13 timeout
192.168.2.1 icmp_seq=14 timeout
192.168.2.1 icmp_seq=15 timeout
```

Перевіримо роботу заданої політики POLICY ICMP командою [3]:

```
#showpolicy-mapinterface [name]
R2#sh policy-mapinter fa0/1
 FastEthernet0/1
Service-policyoutput: POLICYicmp

###Для класу icmp:
Class-map: icmp (match-all)
      60 packets, 27500 bytes
      5 minuteofferedrate 0 bps, droprate 0
bps
Match: access-group 1
Match: protocolicmp
Match: packetlengthmin 300 max 700
police:
rate 8000 bps, burst 1500 bytes
conformed 60 packets, 27500 bytes; actions:
transmit
exceeded 9 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps

###Для класу BIGicmp:
Class-map: BIGicmp (match-all)
      40 packets, 29680 bytes
      5 minuteofferedrate 0 bps, droprate 0
bps
Match: access-group 1
Match: protocolicmp
Match: packetlengthmin 701
drop
Class-map: class-default (match-any)
      121 packets, 12560 bytes
      5 minuteofferedrate 0 bps, droprate 0
bps
Match: any
```

Результати перевірки показують, що алгоритм управління обслуговуванням пакетів працює справно.

Аналізуючи результати моделювання процесу обслуговування відповідно до заданих показників можна відзначити, що ICMP пакети до 299 біт проходять без затримок, минаючи політику класу. Пакети від 300 біт до 700 потрапляють під політику обмеження швидкості передачі інформації, тому відбуваються втрати пакетів (3/15 при розмірі пакета 300 біт, і 6/15 пакетів при розмірі пакета 700 біт). Пакети розміром більше 700 біт повністю втрачаються. Таким чином, в умовах перевантаження, є можливість знизити загальне навантаження на даній ділянці мережі

Література

1. Федоров С. Курс молодого бойца Cisco (v 1.1). Стаття. Електронна версія доступна за посиланням: http://groall.ru/wp-content/uploads/2011/05/YoungSoldierCisco.pdf.
2. Афонцев Э. Cisco QOS для начинающих. Стаття. Електронна версія доступна за посиланням: http://network.xsp.ru/3_11.php.
3. QOS в Cisco. Електронний ресурс: http://xgu.ru/wiki/QoS_%D0%B2_Cisco.