ubiQuoss

VP5200 Series Switch

Common User Guide

Chapter #10

ubiQuoss

목 차

표 목차

그림 목차

10

통계 모니터링 및 Qos

본 장은 현재 운영중인 VP5200 Series 스위치의 상태를 파악하고, 로그의 정보를 화면에 표시하고, RMON(Remote Monitoring)을 통한 운영 관리 기능에 대하여 설명한다.

또한 VP5200 Series 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 한다. 만일 주기적으로 통계 데이터를 관리한다면, 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있다.

10.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. VP5200 Series 스위치는 show 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공한다.

표 1. 상태 모니터링 명령어

명령어	설명
show log	■ 시스템이 현재 관리하고 있는 로그를 보여 준다. ■ 최대 500 개까지의 로그를 저장할 수 있다.
show memory usage	■ 현재 시스템의 메모리 사용 상태를 보여 준다.
show cpu usage	■ 현재 CPU 점유율을 보여 준다.
show version	■ 스위치의 H/W 와 S/W 의 버전 정보를 보여 준다.

10.2. 포트 통계

VP5200 Series 스위치는 포트의 통계 정보를 제공한다. 포트의 통계 정보는 시스템의 현재 운용 중인 모듈의 각 포트의 현재 카운터 값을 보여준다.

포트 통계를 보기 위해서는 다음의 명령을 사용한다.

`show interface [`*`interface name`*`]`

VP5200 Series 스위치는 운용자에게 다음의 포트 통계 정보를 제공한다.

- **Link Status** – 링크의 현재 상태
- **Received Packet Count (Rx Pkt Count)** – The total number of good packets that have been received by the port.
- **Received Byte Count (Rx Byte Count)** – The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- **Transmit Packet Count (Tx Pkt Count)** – The number of packets that have been successfully transmitted by the port.
- **Transmit Byte Count (Tx Byte Count)** – The total number of data bytes successfully transmitted by the port.
- **Received Broadcast (Rx Bcast)** – The total number of frames received by the port that are addressed to a broadcast address.
- **Received Multicast (Rx Mcast)** – The total number of frames received by the port that are addressed to a multicast address.
- **Transmit Collisions (Tx Coll)** – The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Received Bad CRC Frames (RX CRC)** – The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Oversize)** – The total number of good frames received by the ports that were of greater than the supported maximum length of 1,522 bytes.
- **Receive Dropped Frames (Rx Drop)** – The total number of dropped frames due to lack of system resources.

`Show interface` 명령을 사용하면 다음과 같이 다양한 통계 데이터를 확인할 수 있다.

```
Switch# show interface
fa1 is link down.
 type 100Base-TX
```

```
  auto-negotiation
  speed set auto
  duplex set full
  cpu-mac-filter disable

  Last clearing of counters 02:47:05
  1 minutes input rate 0 bytes/sec, 0 packets/sec
  1 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 multicasts
    0 CRC, 0 oversize, 0 dropped
    0 packets output, 0 bytes
    Sent 0 broadcasts, 0 multicasts

 fa2 is link down.
  type 100Base-TX
  auto-negotiation
  speed set auto
  duplex set full
  cpu-mac-filter disable

  Last clearing of counters 02:47:05
  1 minutes input rate 0 bytes/sec, 0 packets/sec
  1 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 multicasts
    0 CRC, 0 oversize, 0 dropped
    0 packets output, 0 bytes
    Sent 0 broadcasts, 0 multicasts
 --More--
```

표 2. 포트 통계조회 조회 명령

명령어	설명	모드
show port counter	시스템의 모든 인터페이스의 In/Out packet 의 누적치를 보여준다.	privileged
show port counter detail	시스템의 모든 인터페이스의 In/Out packet 과 octet 의 누적치를 보여준다.	privileged
Show port statistics *IFNAME*	해당 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bit/s, bytes/s, pkts/s 를 보여준다.	privileged
Show port statistics allports	모든 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bit/s, bytes/s, pkts/s 를 보여준다.	privileged

다음은 show port counter 를 이용하여 전체 포트의 패킷 누적치와 특정 인터페이스(fa1)의 5 초, 1 분, 5 분 통계치를 보여준다.

```
Switch# show port counter

 ifname I-Kbps O-Kbps        InUpkt       InNUpkt       OutUpkt      OutNUpkt
-------------------------------------------------------------------------------
 fa1         0      0             0             0             0             0
 fa2         0      0             0             0             0             0
 fa3         0      0             0             0             0             0
 fa4         0      0             0             0             0             0
 fa5         0      0             0             0             0             0
 fa6         0      0             0             0             0             0
 fa7         0      0             0             0             0             0
 fa8         0      0             0             0             0             0
 fa9         0      0             0             0             0             0
 fa10        0      0             0             0             0             0
 fa11        0      0             0             0             0             0
 fa12        0      0             0             0             0             0
 fa13        0      0             0             0             0             0
 fa14        0      0             0             0             0             0
 fa15        0      0             0             0             0             0
 fa16        0      0             0             0             0             0
 fa17        0      0             0             0             0             0
 fa18        0      0             0             0             0             0
 fa19        0      0             0             0             0             0
 fa20        0      0             0             0             0             0
 fa21        0      0             0             0             0             0
 fa22        0      0             0             0             0             0
 fa23        0      0             0             0             0             0
 fa24        0      0             0             0             0             0
-------------------------------------------------------------------------------
Switch#
Switch#
Switch# show port statistics fa24

Last clearing of counters :  0 days and 00:06:24 before

-----------------------------------------------------------------
                                TX |                        RX
                  bits/s       pkts/s |     bits/s       pkts/s
-----------------------------------------------------------------
     5sec :            0            0            0            0
     1min :            0            0            0            0
     5min :            0            0            0            0
-----------------------------------------------------------------
Switch#
```

다음 명령은 통계치에 대한 누적치를 초기화시키는 명령어이다.

표 4. 포트 통계 초기화 명령

명령어	설명	모드
clear counters	시스템의 모든 인터페이스의 통계누적치를 초기화한다.	privileged
clear counters *IFNAME*	특정 인터페이스의 통계누적치를 초기화한다.	privileged
clear counters snmp	시스템의 모든 인터페이스의 snmp 를 위한 통계누적치를 초기화한다.	privileged

10.3. CPU 트래픽 통계

VP5200 series 스위치는 cpu 로 올라오는 수많은 packet 을 모니터링 하기 위해 CPU Packet Counter 를 사용하여 어떤 종류의 packet 이 얼마나 올라오는지 확인할 수 있다.
CPU Packet Counter 는 packet 의 ether type 에 따라, IP protocol 에 따라, TCP port 에 따라, UDP port 에 따라 분류하며, 최근 5 초동안의 CPU packet count, 최근 1 분 동안의 CPU packet count, 최근 5 분 동안의 CPU packet count 를 보여 준다.

10.3.1. CPU Packet Counter 설정

이 절에서는 스위치에 새로운 packet type 을 추가하거나 삭제하는 방법을 설명한다.
Packet Counter 는 설정된 packet type 에 따라 CPU 로 들어오는 packet 을 분류하며 default 로 설정된 packet type 과 user 에 의해 새로 추가된 packet type 을 지원한다.

CPU Packet Counter 는 default packet type list 를 가지며 이 type 들은 항상 적용되고, list 에서 삭제할 수 없다. Default packet type 은 ethertype, IP protocol, TCP port, UDP port 로 나눌 수 있다.

Ethertype

```
ETHERTYPE_IP        0x0800  /* IP protocol */
ETHERTYPE_ARP       0x0806  /* Addr. resolution protocol */
ETH_P_IPX   0x8137  /* IPX over DIX        */
```

IP Protocol

```
IPPROTO_IP = 0,       /* Dummy protocol for TCP       */
IPPROTO_ICMP = 1,     /* Internet Control Message Protocol    */
IPPROTO_IGMP = 2,     /* Internet Group Management Protocol   */
```

IPPROTO_TCP = 6, /* Transmission Control Protocol */
IPPROTO_UDP = 17, /* User Datagram Protocol */
IPPROTO_IPV6 = 41, /* IPv6-in-IPv4 tunnelling */
IPPROTO_PIM = 103, /* Protocol Independent Multicast */
IPPROTO_RAW = 255, /* Raw IP packets */

TCP Port

20 : ftp-data
21 : ftp
22 : ssh
23 : telnet
25 : smtp
42 : nameserver
53 : domain
80 : www
137 : netbios-ns
138 : netbios-dgm
139 : netbios-ssn
TCP SYN

UDP Port

53 : domain
67 : BOOTP server
68 : BOOTP client
69 : tftp
123 : ntp
137 : netbios-ns
138 : netbios-dgm
139 : netbios-ssn
161 : snmp
162 : snmp-trap

User 가 추가할 수 있는 Packet type 은 default 로 지정된 packet type 을 포함하여 다음과 같이 정해진 수 까지 추가 가능하다. ()안은 default 로 설정된 값이다.

Ether type : 10 (default 4)
IP protocol : 15 (default 8)
TCP/UDP port : 15 (tcp 11, udp 10)

Default 로 설정된 packet type 과는 별도로 사용자의 필요에 의해 새로운 packet type 을 지정하여 count 를 볼 수 있다. 이렇게 추가된 packet type 은 삭제 가능하다.

표 5. packet type 추가

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입한다.
Step2a	**cpu-packet-counter ethertype** *ETHERTYPE*	새로운 ethertype 추가
Step2b	**cpu-packet-counter ip_protocol** *IP_PROTO*	새로운 IP protocol 추가
Step2c	**cpu-packet-counter tcp_port** *PORT_NUM*	새로운 TCP port 추가
Step2d	**cpu-packet-counter udp_port** *PORT_NUM*	새로운 UDP port 추가
Step3	**end**	Privilideged 모드로 진입한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

다음은 TCP port 222 를 추가하는 것을 보여준다.

```
Switch# configure terminal
Switch(config)# cpu-packet-counter tcp_port 222
Switch(config)# end
Switch#
```

Note Ethertype 은 "unsigned short", IP protocol 은 "unsigned char", TCP/UDP port 는 "unsigned short" 값으로 입력해야 한다.

User 가 추가할 수 있는 Packet type 은 default 로 지정된 packet type 을 포함하여 다음과 같이 정해진 수 까지 추가 가능하다. ()안은 default 로 설정된 값이다.

Ether type : 10 (default 4)
IP protocol : 15 (default 8)
TCP/UDP port : 15 (tcp 11, udp 10

Default 로 설정된 packet type 과는 별도로 사용자의 필요에 의해 새로운 packet type 을 지정하여 count 를 볼 수 있다. 이렇게 추가된 packet type 은 삭제 가능하다.

표 6. packet type 삭제

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입한다.
Step2a	**no cpu-packet-counter**	User 가 입력한 ethertype 삭제

	ethertype *ETHERTYPE*	
Step2b	**no cpu-packet-counter ip_protocol** *IP_PROTO*	User 가 입력한 IP protocol 삭제
Step2c	**no cpu-packet-counter tcp_port** *PORT_NUM*	User 가 입력한 TCP port 삭제
Step2d	**no cpu-packet-counter udp_port** *PORT_NUM*	User 가 입력한 UDP port 삭제
Step3	**end**	Privilideged 모드로 진입한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

10.3.2. Displaying CPU Packet Counter

User 에 의해 설정된 packet type 을 조회하려면 privileged EXEC 명령 "show running-config"나 show packet-counter type-list"를 사용하라.
CPU packet counter 조회에 관련된 command 는 다음과 같다.

표 7. display cpu packet counter

Command	Purpose
show cpu-packet-counter	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 보여준다.
show cpu-packet-counter *IFNAME*	저정된 interface 의 Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 cpu packet count 를 보여준다.
show cpu-packet-counter bps	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 bps 로 보여준다.
show cpu-packet-counter bps *IFNAME*	저정된 interface 의 Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 cpu packet count 를 bps 로 보여준다.
show cpu-packet-counter pps	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 pps 로 보여준다.
show cpu-packet-counter pps *IFNAME*	저정된 interface 의 Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 cpu packet count 를 pps 로 보여준다.
show cpu-packet-counter total	CPU 로 올라온 모든 packet count 를 보여준다.
show cpu-packet-counter ethertype *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 ethertype 별로 보여준다.
show cpu-packet-counter ip_protocol *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 IP protocol 별로 보여준다.

show cpu-packet-counter tcp_port *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 TCP port 별로 보여준다.
show cpu-packet-counter udp_port *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 UDP port 별로 보여준다.
show cpu-packet-counter type-list	CPU 로 올라오는 모든 packet 을 count 하기 위해 가지고 있는 모든 packet 의 type 을 보여준다.
clear cpu-packet-counter	저장된 모든 cpu packet count 를 clear 한다.

10.4. Logging

VP5200 series 스위치 로그는 모든 환경 설정 정보와 경보 발생 정보를 보여 준다. 시스템 메시지 로깅 소프트웨어는 스위치의 메모리에 로그 메시지를 저장하며, 다른 디바이스로 메시지를 보낼 수 있다. 시스템 메시지 로깅 기능은 다음을 지원한다.

- ✓ 사용자에게 수집할 로깅 타입을 선택할 수 있도록 한다.
- ✓ 사용자에게 수집한 로깅을 보낼 디바이스를 선택할 수 있도록 한다.

VP5200 series 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI 를 사용하여 로깅되는 시스템 메시지를 제어할 수 있다. 최대 500 개의 로그 메시지를 시스템 버퍼에 저장한다. 시스템 운영자는 시스템 메시지를 Telnet 이나 콘솔을 통해서, 또는 Syslog server 의 로그를 봄으로써 원격으로 모니터 할 수 있다.

VP5200 series 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

표 8. VP5200 series 스위치의 로그 레벨

Severity 레벨	설명
Emergencies (0)	시스템 사용 불가.
Alerts (1)	즉각적인 조치가 필요한 상태
Critical (2)	Critical 상태.
Errors (3)	에러 메시지.
Warnings (4)	경고 메시지.

Notifications (5)	정상적인 상태지만 중요한 정보.
Informational (6)	사용자에게 제공하는 정보 메시지.
Debugging (7)	디버깅 메시지.

10.4.1. 시스템 로그 메시지 내용

VP5200 series 스위치의 시스템 로그 메시지는 다음과 같은 내용을 제공된다.

- ✓ Timestamp
  - Timestamp 는 이벤트가 발생한 월, 날짜, 연도 및 구체적인 시간 정보를 Month Day HH:MM:SS 와 같이 기록한다.
- ✓ Severity level
  - <표 1>에서 정의한 VP5200 스위치의 로그 메시지의 레벨
  - 0~7 까지의 숫자
- ✓ Log description
  - 발생한 이벤트에 대한 상세한 정보를 포함하는 텍스트 문자열

다음은 시스템 부팅 시의 로그 메시지 이다.

```
May  6 11:53:48  [5] %REMOTE-CONNECT: login from console as lns
May  6 11:54:01  [5] IFM-NOTICE: Rate limit ra creation
May  7 02:10:24  [5] %REMOTE-CONNECT: login from console as lns
May  7 02:10:40  [5] IFM-NOTICE: Flow xx classified
May  7 02:10:48  [5] IFM-NOTICE: Flow xx match rate 10
May  7 05:17:56  [5] %REMOTE-CONNECT: login from console as lns
May  7 05:23:10  [5] IFM-NOTICE: Service pa add interface fa1
```

10.4.2. 디폴트 Logging 설정 값.

표 9. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	enabled
Telnet 세션으로의 로깅 출력	disabled.
로깅 버퍼 사이즈	250kb
Time-Stamp 출력	enabled
Logging Server	disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings(4)
콘솔의 Severity	Debuggings(7)
Telnet 의 Severity	info(6)
Flash 로의 로깅 저장	disable
Flash 버퍼 사이즈	25KB

표 10. 시스템 메시지 로깅 환경 설정 명령

명령어	설명
`logging console {enable|disable|level}`	■ 콘솔로의 로깅 출력 여부 설정 및 환경 설정.
`logging facility {auth|cron|daemon|kernel|local0| local1|local2local3|local4|local5| local6|local7|lpr|mail|news|syslog| user|uucp}`	■ syslog 메시지를 보낼 Facility parameter 를 설정.
logging flash `{enable|disable|level|size}`	■ syslog 메시지를 flash 에 저장할지의 여부 설정 및 환경 설정.
logging server `A.B.C.D`	■ syslog 메시지를 외부 syslog 서버에 보낼지 설정

logging session {*enable*|*disable*|*level* }	■ 현 세션으로의 로깅 출력 여부 설정.
logging size BYTE	■ 저장할 syslog 의 size 설정
logging source-ip *A.B.C.D*	■ syslog packet 의 source ip 를 설정
logging trap {<*0-7*>|*alert*|*crit*|*debug*|*emerg*|*err*| info|notice|warn}	■ syslog server 의 logging level 설정
show logging {<*0-7*>|*back*|*flash* }	■ 로깅 버퍼 출력 및 로깅 configuration 확인.

10.4.3. Logging 설정 예.

Console 로 접속한 경우 Log level notice(5) 이하의 log message 만을 console 로 출력하고자 할 때 다음과 같이 설정한다. console 로 log message 출력을 중단하고자 할 경우 “logging console disable” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging console enable
Switch(config)# logging console level notice
Switch(config)#
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# logging console disable
Switch(config)#
```

Telnet 으로 접속한 경우 Log level warn(4) 이하의 log message 만을 telnet session 에 출력하고자 할 때 다음과 같이 설정한다. Telnet session 으로 log message 출력을 중단하고자 할 경우 “logging session disable” command 를 사용한다.

```
Switch#
Switch# configure terminal
Switch(config)# logging session enable
Switch(config)# logging session level warn
Switch(config)#
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# logging session disable
Switch(config)#
```

Log level err(3) 이하의 log message 를 flash 에 저장하고자 할 경우 다음과 같이 설정한다. flash 에 log message 의 저장을 중단하고자 할 경우 “logging flash disable” command 를 사용한다.

```
Switch#
Switch# configure terminal
Switch(config)# logging flash enable
Switch(config)# logging flash level err
Switch(config)#
Switch (config)# end
Switch# configure terminal
Switch(config)# logging flash disable
Switch(config)#
```

Log server 100.10.1.1 에 이 switch 에서 발생하는 log 중 Log level err(5) 이하의 log message 를 보내고자 할 경우 다음과 같이 설정한다. log server 로 log message 보내는 것을 중단하고자 할 경우 “no logging server” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging server 100.10.1.1
Switch(config)# logging trap err 100.10.1.1
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging server 100.10.1.1
Switch(config)#
```

10.5. RMON(Remote MONitoring)

시스템 운영자는 VP5200 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다.

다음 절에서는 RMON 개념 및 VP5200 Series 스위치가 지원하는 RMON 서비스 기능에 대하여 자세히 설명한다.

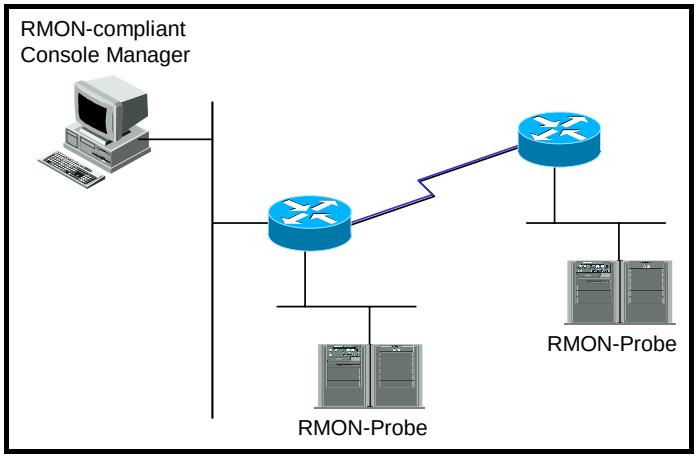
10.5.1. RMON 개요

RMON 은 IETF(Internet Engineering Task Force)의 RFC 1271 와 RFC 1757 에 정의되어 있는 국제

표준 규격으로 시스템 운영자가 네트워크를 원격으로 관리하는 기능을 제공한다. 일반적으로 RMON 은 다음의 두 가지 구성 요소로 구성된다.

- **RMON probe**
  - 원격으로 제어되면서 지속적으로 LAN 세그먼트 또는 VLAN 의 통계 정보를 수집하는 지능형 디바이스 또는 소프트웨어 agent
  - 수집한 정보를 운영자의 요구가 있을 때 또는 미리 정의한 환경에 따라서 자동으로 관리 호스트에게 전송

- **RMON Manager**
  - RMON probe 와 통신하면서 통계 정보를 수집
  - 반드시 RMON probe 와 동일한 네트워크에 있을 필요는 없으며, RMON probe 를 in-band 또는 out-of-band 연결을 통하여 제어



- 그림 1. RMON Manager 와 RMON Probe

기존의 SNMP MIBs 가 SNMP agent 가 탑재된 장비 자체를 관리 대상으로 보고 있는데 반하여 RMON MIBs 는 관리 대상을 장비에 연결된 LAN 세그먼트로 한다. 즉 LAN 세그먼트의 전체 발생 트래픽, 세그먼트에 연결된 각 호스트의 트래픽, 호스트들 사이의 트래픽 발생 현황을 알려준다.

RMON Agent 는 전체 통계 데이터, 이력 데이터, 호스트 관련 데이터, 호스트 매트릭스와 사전에 문제 예측 및 제거를 위해서 특정 패킷을 필터링하는 기능과 임계치를 설정, 이에 도달하면 자동으로 알려주는 경보 기능 및 사건 발생 기능을 보유하고 있어야 한다.

VP5200 Series 스위치에서는 <표 11.RMON 항목> 에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON 의 모든 설정은 기본적으로 비활성화 상태이다.

표 11. RMON 항목

항목	설명
통계	■ 한 세그먼트에서 발생한 패킷/바이트 수, 브로드캐스트/멀티캐스트 수, 충돌 수 및 패킷 길이별 수 그리고 각종 오류(fragment, CRC Alignment, jabber, 길이 미달, 길이 초과)에 대한 통계를 제공.
이력	■ 관리자가 설정한 시간 간격 내에 발생한 각종 트래픽 및 오류에 대한 정보를 제공 ■ 기본적으로 단기/장기적으로 간격을 설정 가능하고 1-3.600 초를 간격으로 제한 ■ 이 자료를 통해 시간대별 이용 현황 및 다른 세그먼트와 비교 가능
경보	■ 주기적으로 특정한 값을 체크 해 기준치에 도달하면 관리자에 보고하고 대리인이 자신의 기록을 보유 ■ 기준치는 절대값 및 상대값으로 정할 수 있고 계속적인 경보 발생을 막기 위해서 상/하한치를 설정해서 넘나드는 경우에만 경보가 발생.
호스트	■ 세그먼트에 연결된 각 장비가 발생시킨 트래픽, 오류 수를 호스트별로 관리
상위 n 개의 호스트	■ 위 호스트 테이블에 발견될 호스트 중에서 일정시간 동안 가장 많은 트래픽을 발생시킨 호스트 검색 ■ 관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 수집
트래픽 메트릭스	■ 데이터 링크 계층, 즉 MAC 어드레스를 기준으로 두 호스트간에 발생한 트래픽 및 오류에 대한 정보를 수집 ■ 이 정보를 이용해서 특정 호스트에 가장 많은 이용자가 누구인지를 어느 정도는 판별 가능함 ■ 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없음.
필터	■ 관리자가 특정한 패킷의 동향을 감시하기 위해서 이용.
패킷 수집	■ 세그먼트에 발생한 패킷을 수집해서 관리자가 분석.
사건	■ 특정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고를 전송. 트랩 발생 및 기록보관은 선택적임.

10.5.2. RMON 의 Alarm 과 Event 그룹 설정.

사용자는 CLI 또는 SNMP Manager 에 의해서 RMON 의 Configuration 을 설정할 수 있다. 이는

Privileged 모드에서 설정되며, 명령어는 다음과 같다.

표 12. RMON Alarm and Event 설정 명령

명령어	설명	모드
`rmon alarm` *`index`* `ifEntry` *`variable ifIndex interval`* `{delta|absolute} rising-threshold` *`value`* `[`*`event-number`*`] falling-threshold` *`value`* `[`*`event-number`*`] [owner` *`string`*`]`	■ RMON 의 alarm table 에 alarm 을 추가 ■ *Index*: alarm table 의 유일한 인덱스 ■ *Variable*: alarm variable 을 관찰할 MIB object ■ *IfIndex*: 알람 발생을 감시할 물리적 인테페이스 ■ *interval*: alarm variable 을 관찰한 시간 간격으로 초 단위로 지정 ■ Delta: MIB variable 값의 샘플간의 값의 차이 값 ■ Absolute: MIB variable 의 절대값 ■ Rising-threshold, falling-threshold *value*: alarm 을 발생시킬 설정 값 ■ *Event-number*: alarm variable 의 delta 값이나 absolute 값이 rising-threshold 또는 falling threshold 값에 도달했을 때 발생할 Event number ■ Owner *string*: Alarm 의 owner	Config
`rmon event` *`index`* `[log] [trap community` *`string`*`] [owner` *`string`*`] [description` *`string`*`]`	■ RMON event table 에 event 를 추가 ■ log: event 가 발생했을 때, RMON log 를 생성할 것인지를 명시 ■ Trap community: event 가 발생했을 때, trap 과 함께 전송할 community *string* ■ Owner *string*: Event 의 owner ■ Description *string:* Event 에 대한 설명	Config
`no rmon alarm` *`alarm-index`*	■ RMON alarm table 에서 alarm 을 삭제	Config
`no rmon event` *`event-index`*	■ RMON event table 에서 event 를 삭제	Config
`show rmon alarm`	■ RMON alarm table 을 출력	Privileged
`show rmon event`	■ RMON event table 을 출력	Privileged
`show rmon log`	■ RMON log table 을 출력	Privileged

```
Switch# configure terminal
Switch(config)# rmon alarm 10 ifEntry inErrors 1 20 delta rising-threshold 15 1
falling-threshold 0 owner hong
Switch(config)# rmon event 1 log trap community rmontrap owner hong description
"Noti : Too Much InErrors"
Switch(config)# exit
Switch# show rmon alarm
-------------------------------------
         Alarm Configurations
-------------------------------------

The index of alarm    : 10
The interval          : 20
The type of Packets   : inErrors
The interface         : fa1
The type of Sample    : deltaValue
alarmValue            : 0
The status of starting: RISING_FALLING_ALARM
alarmRisingThreshold  : 15
alarmFallingThreshold : 0
alarmRisingEventIndex  : 1
alarmFallingEventIndex : 1
alarmOwner            : hong

Switch# show rmon event
-------------------------------------
         Event Configurations
-------------------------------------

The Index of event : 1
eventDescription   : "Noti:TooMuchInErrors"
eventType          : log and trap
Community          : rmontrap
eventOwner         : hong
Switch#
```

표 13. RMON History 설정 And Statistics 명령

명령어	설명	모드
rmon history *index* ifEntry *ifIndex* [buckets *bucket-number*] [interval seconds] [owner *string*]	■ 물리적 인터페이스에 대하여 이력을 수집 ■ *Index*: history table 의 유일한 인덱스 ■ Buckets *bucket-number*: 수집할 이력의 수	Config

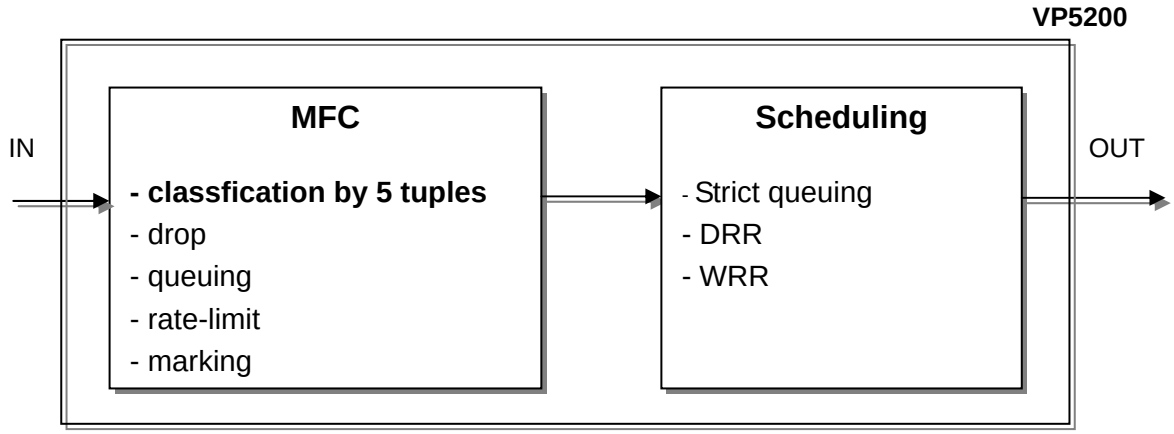
	■ IfEntry *ifIndex*: 이력을 수집할 물리적 인터페이스 ■ Interval *seconds*: 이력을 수집할 시간 간격으로 초 단위로 지정 ■ Owner *string:* History 의 owner	
`no rmon history` *`index`* `ifEntry` *`ifindex`*	■ History 수집을 Disable 함.	Config
`show rmon history`	■ RMON history table 을 출력	Privileged
`show rmon statistics` [*IFNAME*]	■ RMON statistics table 을 출력. ■ *IFNAME:* 특정 인터페이스를 지정	Privileged
`show port statistics rmon` [IFNAME]	■ RMON statistics table 을 출력. ■ *IFNAME:* 특정 인터페이스를 지정	Privileged

Notice ‘show rmon statistics’ 명령은 ‘show port statistics rmon’명령과 동일한 내용을 출력한다.

```
Switch# configure terminal
Switch(config)# rmon history 1 ifEntry 9 buckets 100 interval 5 owner park
Swtich(config)# end
Switch# show rmon history
--------------------------------------
         SHOW HISTORY
--------------------------------------


====== gi2/1 ======
Control-index     : 1
ifindex           : 9
interval          : 5
buckets           : 50
owner             : park

--- gi2/1 : bucket 1 ---
DropEvents        : 0
Octets            : 0
       (생략)
P808FG_85# show rmon statistics
--------------------------------------
         SHOW STATISTICS
--------------------------------------
```

```
The Index of stats   : 1
Interface            : fa1
Drop Events          : 0
Total Octets         : 0
Total Packets        : 0
Broadcast Packets    : 0
Multicast Packets    : 0
CRC errors           : 0
Under Size Packets   : 0
Over Size Packets    : 0
Fragments            : 0
Jabbers              : 0
Collisions           : 0
Pkts 64 Octets       : 0
Pkts 65 to 127 Oct   : 0
Pkts 128 to 255 Oct  : 0
Pkts 256 to 511 Oct  : 0
Pkts 512 to 1023 Oct : 0
Pkts 1024 to 1518 Oct: 0
Owner                : ubiquoss
      (생략)
Switch# show rmon statistics fa2
--------------------------------------------------------------------------------
         RMON STATISTICS
--------------------------------------------------------------------------------

The Index of stats   : 3 (fa2)
DropEvents           :               0  Jabbers             :               0
Octets               :               0  Collisions          :               0
Pkts                 :               0  Pkts64Octets        :               5
BroadcastPkts        :               0  Pkts65to127Octets   :           10562
MulticastPkts        :               0  Pkts128to255Octets  :               0
CRCAlignErrors       :               0  Pkts256to511Octets  :               0
UndesizePkts         :               0  Pkts512to1023Octets :               0
OversizePkts         :               0  Pkts1024to1518Octets:               0
Fragments            :               0
--------------------------------------------------------------------------------
```

10.6. Qos 및 Packet Filtering



본 VP5200 Series 스위치에서는 Qos 와 Packet filtering 을 위해 다음과 같은 기능을 수행을 한다.

- **MFC(Multi-Field Classifier)**

  프로토콜, src/dest IP, UDP/TCP Port 등의 지정된값에 의해 다양하게 classification 하여 flow-rule 을 결정한후 drop, queuing, rate-limit, marking 등의 특정 정책(action)을 수행할 수 있다. 또한 이를 이용하여 다양하게 filtering 기능을 수행하는데 이용되기도 한다.

- **Scheduling**

  트래픽이 과부하가 일어났을 경우 이를 위한 처리 방식으로 Scheduling 알고리즘을 이용하여 트래픽의 조건에 따라 처리순서를 다르게 하는 방식이다.

  - Strict Queuing Method

  이 알고리즘은 중요한 데이터를 가장 빨리 처리하려고 할 때 사용된다. 모든 데이터를 우선순위대로 처리하여 우선 순위가 높은 데이터를 빨리 처리되지만 우선도가 낮은 데이터는 처리 순서가 밀린다. 만약 대역폭 전체가 우선 순위 놓은 데이터로 채워지면 낮은 우선순위의 트래픽은 전혀 통과하지 못하고 대기 상태에 놓이는 단점을 지니고 있는 방식이다.

  - WRR(Weighted Round Robin Method)

  일정 비율을 기반으로 데이터를 처리하는 방식으로 SPQ 방식의 단점을 보완할수 있는 알고리즘으로서 사용자가 자신의 환경에 맞게 설정한 큐에 지정된 비율에 따라 데이터를 처리한다.

- DRR(Deficit Round Robin Method)

일정 비율을 기반으로 데이터를 처리하는 방식으로 SPQ 방식의 단점을 보완할수 있는 알고리즘으로서 큐에 변화하는 size 의 패킷들을 고려해서 일정한 크기의 처리율을 사용자가 자신의 환경에 맞게 설정할 수 있다.

10.6.1. MFC(Multi-Field Classifier)

10.6.1.1. Flow-Rule 설정/해제

패킷을 처리하는 정책을 설정하기 위해 적용할 대상이되는 규칙을 설정하여야 하는데 이는 Flow-rule 을 classification 설정으로 가능하다. Flow-rule 은 src/dest mac, vlan, cos, ethertype, 프로토콜, src/dest IP, UDP/TCP Port, dscp, tos, Tcp sync 등의 지정된 값에 의해 다양하게 classification 할수 있다.

표 15. Flow-rule Classification 명령

명령어	설명	모드
flow-rule NAME classify { <0-255> | icmp | igmp | ip | ospf | pim | tcp | udp } { *SRCIP/M* **| any } {** *DSTIP/M* **| any }**	flow-rule 이 적용된 인터페이스의 특정 프로토콜에 대한 모든 혹은 지정된 src/dest ip 에 대해 적용(L3 기본 classify)	Config
flow-rule NAME classify <0-255> mask MASK *SRCIP/M DSTIP/M*	flow-rule 이 적용된 인터페이스의 특정 range 의 프로토콜에 대한 지정된 src/dest ip 에 대해 적용(L3 기본 classify)	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP/M* | **any** } { *DSTIP/M* | **any** } { *<0-65535>* | *SRCPORT* } { *<0-65535>* | *DSTPORT*}	flow-rule 이 적용된 인터페이스의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 에 대해 적용(L3 기본 classify)	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP/M* | **any** } { *DSTIP/M* | **any** } **mask** *SRCPORT SPORTMASK DSTPORT DSTPORTMASK*	flow-rule 이 적용된 인터페이스의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 mask range 의 src/dest port 에 대하여 적용. 이 경우 Port 도 16 진수로 입력해야 함(L3 기본 classify) * Mask-calculator 참조	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP/M* | **any** } { *DSTIP/M* | **any** } { *l4port-range-checker*	flow-rule 이 적용된 인터페이스의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip	Config

<1-16> | *SRCPORT* } { *l4port-range-checker <1-16>* | *DSTPORT*}	와 모든 혹은 지정된 src/dest port 에 대해 적용(L3 기본 classify). 이 경우 port 의 classification 을 l4port-range-checker 을 사용.	
flow-rule *NAME* **classify** { *H.H.H* | **any** } { *H.H.H* | **any** }	flow-rule 이 적용된 인터페이스의 모든 혹은 지정된 src/dest Mac address 에 대하여 적용(L2 기본 classify)	Config
flow-rule *NAME* **classify** *H.H.H* **mask** *H.H.H H.H.H* **mask** *H.H.H*	flow-rule 이 적용된 인터페이스의 모든 혹은 지정된 mask range 의 src/dest Mac address 에 대하여 적용(L2 기본 classify)	Config
flow-rule *NAME* **classify tcp-control** *{ack|fin|psh|rst|syn|urg|VALUE MASK}*	Tcp control flag 를 이용한 classification 설정	Config
(no) flow-rule *NAME* **classify dscp** *VALUE*	flow-rule 이 적용된 인터페이스의 해당 dscp 값의 패킷에 대하여 적용/해제	Config
(no) flow-rule *NAME* **classify tos** *VALUE*	flow-rule 이 적용된 인터페이스의 해당 tos 값의 패킷에 대하여 적용/해제	Config
(no) flow-rule *NAME* **classify cos** *VALUE*	flow-rule 이 적용된 인터페이스의 해당 cos 값의 패킷에 대하여 적용	Config
(no) flow-rule *NAME* **classify vlan <1-4094>**	Vlan 을 이용한 classification 설정	Config
(no) flow-rule *NAME* **classify ethertype** *VALUE*	flow-rule 이 적용된 인터페이스의 특정 ethertype 패킷에 대하여 적용	Config
(no) flow-rule *NAME* **classify ethertype** *VALUE* **mask** *MASK*	flow-rule 이 적용된 인터페이스의 특정 ethertype mask range 패킷에 대하여 적용	Config
(no) flow-rule *NAME* **classify tag-type (tagged | untagged)**	flow-rule 이 적용된 인터페이스의 패킷이 untagged packet 혹은 tagged packet 에 대하여 적용	Config

Notice Marking dscp , marking tos , cos-to-tos 는 동시에 적용되지 않으며, 동시 설정시 dscp , tos , cos-to-tos 의 우선순위로 한가지만 설정된다.

각 조건에 의해 Classification 된 Flow-Rule 에 특정 정책(action)을 적용시킬 수가 있다.
Qos 를 위해 Cos, Queue 필드를 marking 할수도 있으며, rate-limit 등의 정책을 적용할수도 있다.

표 16. Flow-rule 정책 적용 명령

명령어	설명	모드
flow-rule *NAME* **match drop**	규칙과 일치하는 패킷을 불허한다.	Config
flow-rule *NAME* **match queuing <0-7>**	규칙과 일치하는 패킷을 지정된 우선순위의 Queue 에 할당한다.	Config
flow-rule *NAME* **match marking cos <0-7>**	규칙과 일치하는 패킷의 해당값을 할당된 Cos 값으로 패킷에 marking 한다.	Config
flow-rule *NAME* **match marking dscp <0-63>**	규칙과 일치하는 패킷의 해당값을 할당된 dscp 값으로 패킷에 marking 한다.	Config
flow-rule *NAME* **match marking tos <0-7>**	규칙과 일치하는 패킷의 해당값을 할당된 tos 값으로 패킷에 marking 한다.	Config
flow-rule *NAME* **match cos-to-tos**	규칙과 일치하는 패킷의 tos 값을 패킷의 cos 값을 참조하여 패킷에 marking 한다.	Config
flow-rule *NAME* **match tos-to-cos**	규칙과 일치하는 패킷의 cos 값을 패킷의 tos 값을 참조하여 패킷에 marking 한다.	Config
flow-rule *NAME* **match mirror**	규칙과 일치하는 패킷을 지정된 mirror 포트에 복사한다.	Config
flow-rule *NAME* **match redirect {all|unicast|broadcast|BPDU|DLF|known-multicast|unknown-multicast}** *INTERFACE* **{ tag | untag }**	규칙과 일치하는 패킷을 지정된 INTERFACE 로 redirect 한다.	Config
flow-rule *NAME* **match trap-cpu**	규칙과 일치하는 패킷을 CPU 로 트랩시킨다.	Config
flow-rule *NAME* **match control-cpu-trap**	규칙과 일치하는 패킷을 CPU 에 high priority 로 트랩시키며, 동시에 drop 시킨다.	Config
flow-rule *NAME* **match drop-precedence**	규칙과 일치하는 패킷에 drop-precedence 를 부여한다.	Config
flow-rule *NAME* **match dynamic-nat**	규칙과 일치하는 패킷에 dynamic-nat 을 적용한다.	Config
flow-rule *NAME* **match metering**	규칙과 일치하는 패킷을 카운팅한다.	Config
flow-rule *NAME* **match rate-limit** <64-1048576>	규칙과 일치하는 패킷에 rate-limit 를 적용한다.	Config
flow-rule *NAME* **match cpu-queuing** *<1-6>*	규칙과 일치하는 패킷에 cpu-queuing 값을 지정한 값을 할당한다.	Config
no flow-rule *NAME* **match drop**	규칙과 일치하는 패킷을 불허를 취소한다.	Config
no flow-rule *NAME* **match dynamic-nat**	규칙과 일치하는 패킷의 dynamic-nat 를 취소한다.	Config
no flow-rule *NAME* **match queuing**	규칙과 일치하는 패킷의 queuing 을 취소한다.	Config
no flow-rule *NAME* **match marking cos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match marking dscp**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config

no flow-rule *NAME* **match marking tos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match cos-to-tos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match tos-to-cos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match mirror**	규칙과 일치하는 패킷의 mirror 를 취소한다.	Config
no flow-rule *NAME* **match redirect**	규칙과 일치하는 패킷의 redirect 를 취소한다.	Config
no flow-rule *NAME* **match trap-cpu**	규칙과 일치하는 패킷의 trap-cpu 를 취소한다.	Config
no flow-rule *NAME* **match control-cpu-trap**	규칙과 일치하는 패킷의 trap-cpu 를 취소한다.	Config
no flow-rule *NAME* **match drop-precedence**	규칙과 일치하는 패킷의 drop-precedence 를 취소한다.	Config
no flow-rule *NAME* **match metering**	규칙과 일치하는 패킷의 metering 를 취소한다.	Config
no flow-rule *NAME* **match rate-limit**	규칙과 일치하는 패킷의 rate-limit 를 취소한다.	Config
no flow-rule *NAME* **match cpu-queuing**	규치과 일치하는 패킷의 cpu-queuing 을 취소한다.	Config

Notice 위의 모든 정책은 flow-rule 에 여러 개를 동시에 적용이 가능하지만, action 에 따라서 동시에 적용되지 않을수 있다. 예를 들면 queuing 과 marking cos 는 동시에 적용이 가능하지만, drop 과 queuing 은 한가지로만 동작한다. Action 의 우선 순위는 Broadcom 칩셋을 따른다.

Notice control-cpu-trap 은 해당 패킷을 cpu 의 high-priority 로 trap 하면서, 동시에 drop 을 수행한다. Igmp snooping 을 수행하기 위해서는 해당 packet 에 대해서 이 trap 을 설정해 주는 것을 권장한다.

10.6.1.2. mask-calculator

flow-rule *NAME* **classify l4port mask** 명령을 사용하기 위해서는 복잡한 16 진수 mask 계산이 필요한 데 이를 쉽게 해결해 주는 명령이다. L4port 의 시작 값과 끝 값을 주면 이에 필요한 mask 개수와 설정에 필요한 mask 값을 출력해 준다.

표 17. mask-calculator 명령

명령어	설명	모드
mask-calculator <0-65535> <0-65535>	시작값과 끝값을 주면 필요한 mask 값을 출력한다.	Privileged

이해를 돕기위해 다음의 조건을 만족시키기 위한 한가지 예를 나타내었다.

예 1) port number 4000~4100 까지 100 개의 port 에 대해서 classification 하기 위한 mask 계산

```
Switch# mask-calculator 4000 4100

  mask 0fa0 ffe0 :   4000 ~   4031 ( 6)
  mask 0fc0 ffc0 :   4032 ~   4095 ( 7)
  mask 1000 fffc :   4096 ~   4099 ( 3)
  mask 1004 ffff :   4100 ~   4100 ( 1)

Required number of mask = 4

Switch#
```

위와 같이 출력된 4 개의 mask 를 이용해서 classification rule 을 적용하면 된다.

10.6.1.3. port range checker

port range checker 는 L4port range 를 classification 하는 경우 쉽게 할 수 있도록 지원하는 기능이다. L4port range 를 classification 하기 전에 먼저 port range 를 다음 명령어를 통해 정의 한다.

표 18 port range checker 명령어

명령어	설명	모드
flow-rule l4port-range-checker *<1-16>* (*src*|*dst*) *<0-65535> <0-65535>*	L4port-range-checker 의 identify 는 1-16 이고 port 의 direction, range 를 설정한다.	Privileged

l4port-range-checker 는 최대 16 개까지 정의 할 수 있다. 그리고 각 l4pot-range-checker 는 source port 또는 destination port 둘 중에 하나만 설정 할 수 있다.

이해를 돕기위해 다음의 조건을 만족시키기 위한 한가지 예를 나타내었다.

예 1) fa1 포트에 다음과 같이 적용한다.
tcp src 6000~10000 번 포트 drop

```
Switch#configure terminal
Switch(config)# flow-rule l4port-range-checker 1 src 6000 10000
Switch(config)# flow-rule f1 classify tcp any any l4port-range-checker 1 any
Switch(config)# flow-rule f1 match drop
Switch(config)#
Switch(config)# policy-map p1 flow-rule f1
Switch(config)#
Switch(config)# service-policy fa1 ingress p1
Switch(config)#
```

10.6.1.4. policy-map 생성/추가

인터페이스에 Flow-rule 을 적용하기위해 Policy-map 을 만들어 적용하며, Policy-map 에는 다수의 Flow-rule 이 포함될 수 있어, 한 인터페이스에 다수의 정책이 적용될 수 있으며 Policy-map 에 추가되는 순서에 의해 Flow-rule 이 적용되므로 그 순서가 대단히 중요하다.
적용된 순서는 **show flow-rule** 을 통해 확인할 수 있다.

표 19. Policy-map 생성 및 추가 명령

명령어	설명	모드
policy-map *PNAME* **flow-rule** *FNAME*	PNAME 이 없는 경우는 새로이 생성하고 PNAM 의 policy 가 기존에 있는 경우는 FNAME 의 flow 가 마지막으로 추가된다.	Config

Policy-map 전체를 삭제하거나, 적용된 하나의 Flow-rule 을 삭제하기 위해서는 다음의 명령어들이 사용된다.

표 20. Policy-map 삭제 및 특정 flow-rule 삭제 명령

명령어	설명	모드
No policy-map *PNAME*	PNAME 의 policy-map 을 삭제한다.	Config
No policy-map *PNAME* **flow-rule** *FNAME*	PNAME 의 policy-map 에서 FNAME 의 특정 flow-rule 를 삭제한다.	Config

생성된 policy-map 을 vlan 인터페이스에 적용/해제하는 명령어는 다음과 같다.

표 21. policy-map 적용/해제 명령

명령어	설명	모드
service-policy *IFNAME* **ingress** *PNAME*	특정 포트 인터페이스의 해당 direction 으로 PNAME 의 policy-map 을 적용한다.	Config
no service-policy *IFNAME*	해당 인터페이스 적용된 policy-map 을 해제한다.	Config

Notice policy-map 은 포트 인터페이스에 내려지며 하나의 포트 인터페이스에는 하나의 policy-map 만이 적용되므로 순서에 주의하면서 다수의 flow-rule 을 적용가능한 policy-map 을 생성하여야 한다.

Notice policy-map 의 flow-rule 중에 drop 과 그 이외의 match rule 이 동시에 적용될 경우, drop 룰은 우선되어 적용된다.

다음의 명령을 사용하여 flow-rule 관련 설정을 조회할수 있다.

표 22. Flow-rule 조회 명령

명령어	설명	모드
show flow-rule	flow-rule 및 policy-map 의 정보를 보여준다.	Config
show service-policy	현재 적용되어있는 policy-map 을 vlan 인터페이스와 함께 보여준다.	Config

이해를 돕기위해 다음의 조건을 만족시키기 위한 두가지 예를 나타내었다.

예 1) fa1 포트에 다음과 같이 적용한다.
tcp 6000 번 포트 drop
Src ip 20.1.1.0/24 queuing 2
Tcp 23 포트에 queuing 7

```
Switch#configure terminal
Switch(config)# flow-rule f1 classify tcp any any 6000 any
Switch(config)# flow-rule f1 match drop
Switch(config)# flow-rule f2 classify ip 20.1.1.0/24 any
Switch(config)# flow-rule f2 match queuing 2
Switch(config)# flow-rule f3 classify tcp any any 23 any
Switch(config)# flow-rule f3 match queuing 7
Switch(config)#
Switch(config)# policy-map p1 flow-rule f1
```

```
Switch(config)# policy-map p1 flow-rule f2
Switch(config)# policy-map p1 flow-rule f3
Switch(config)#
Switch(config)# service-policy fa1 ingress p1
Switch(config)#
```

예 2) fa2 포트에 다음과 같이 적용한다.

tcp 4010 포트에 rate limit 10Mbps
tcp 5010 포트에 rate limit 20Mbps

```
Switch# conf t
Switch(config)# flow-rule f4 classify tcp any any 4010 any
Switch(config)# flow-rule f4 match rate-limit 10000
Switch(config)# flow-rule f5 classify tcp any any 5010 any
Switch(config)# flow-rule f5 match rate-limit 20000
Switch(config)#
Switch(config)# policy-map p2 flow-rule f4
Switch(config)# policy-map p2 flow-rule f5
Switch(config)#
Switch(config)# service-policy fa2 ingress p2
Switch#
```

10.6.2. Qos 관련 파라메터

IEEE 802.1p 규약에 의해서 tag 정보를 가지는 L2 패킷에는 패킷 우선순위를 가지는 cos 값이 있고, 이를 이용해서 queuing 할수 있어야 한다. 또한, 적당한 방법에 의해서 cos 값을 설정/재설정이 가능해야 한다. 이 값은 0 부터 7 사이의 값을 가진다.
또한, L3 패킷에는 dscp 값이 있으며, 이에 따른 적당한 queuing 역시 가능해야 한다.
VP5200 시리즈는 각 인터페이스별로 8 개의 queue 를 가지고 있으며, 이들 사이의 mapping table 을 system wide 하게 유지하고 있다.

이 테이블은 다음의 명령어를 통해 marking/remarking 될 값을 변경할 수 있다.

표 23. Qos 관련 Marking/Remarking 테이블 셋팅 명령

명령어	설명	모드

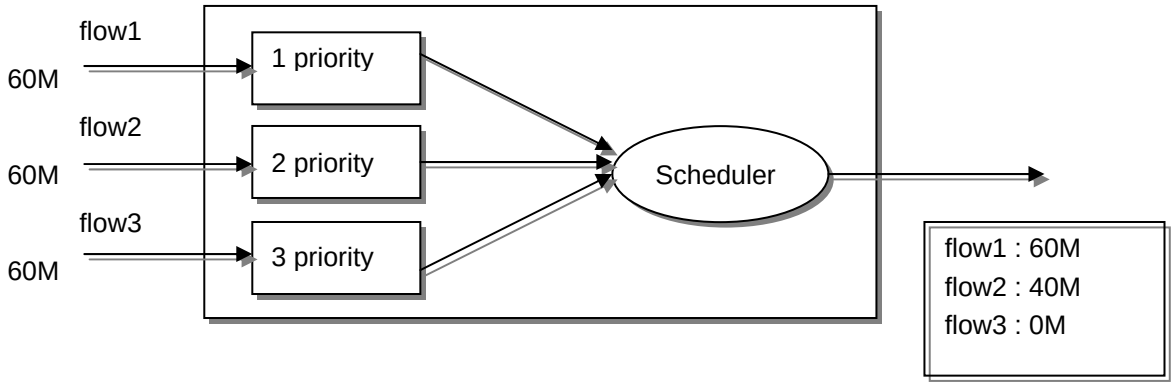
qos cos-queue-map <*0-7*> <*0-7*>	규칙에 적용된 패킷의 cos 값에 의해 mapping 될 새로운 queue 값을 설정한다. 이는 **show qos cos** 로 확인 가능하다.	Config
qos cos-remarking <*0-7*> <*0-7*>	규칙에 적용된 패킷의 queue 값에 의해 remarking 될 새로운 Cos 값을 설정한다.	Config
qos dscp-dp-map <*0-63*> <*0-1*>	규칙에 적용된 패킷의 dscp 값에 의해 mapping 될 새로운 dp 값을 설정한다. 이는 show qos dscp 로 확인 가능하다.	Config
qos dscp-pri-map <*0-63*> <*0-7*>	규칙에 적용된 패킷의 dscp 값에 의해 mapping 될 새로운 pri 값을 설정한다. 이는 show qos dscp 로 확인 가능하다.	Config

표 24. Qos 관련 Marking/Remarking 테이블 조회명령

명령어	설명	모드
show qos cos	규칙에 적용된 패킷의 cos 값에 의해 mapping/remaking 테이블을 보여준다.	Privileged
show qos dscp	규칙에 적용된 패킷의 dscp 값에 의해 mapping 테이블을 보여준다.	Privileged

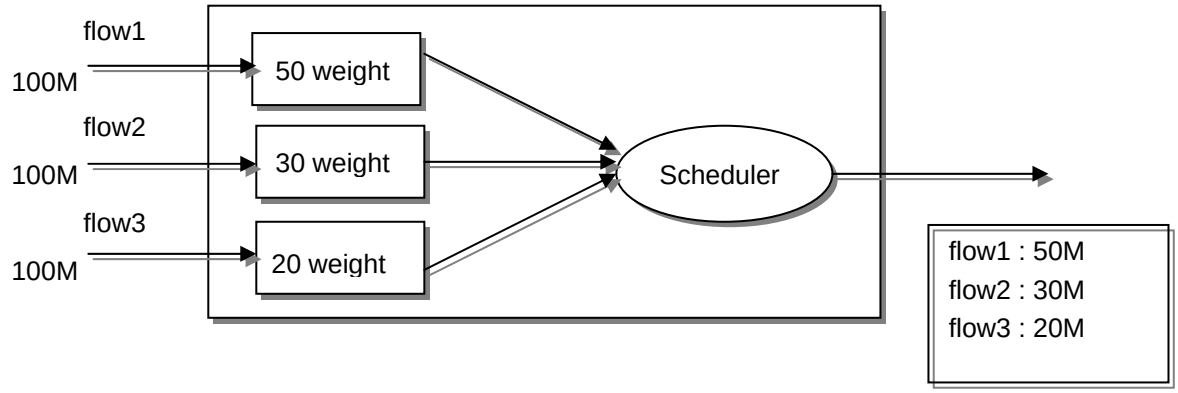
10.6.3. Scheduling

VP5200 Series 스위치에서는 Scheduling 을 위해 SPQ(Strict Priority Queue) Method 와 DRR(Deficit Round Robin), WRR(Weighted Round Robin) Mothod 를 제공하며 디폴트는 SPQ 이다. 다음 그림은 SPQ 와 WRR 의 차이점을 나타내고 있다.



■ 그림 2. SPQ(Strict Priority Queue) Method

SPQ(Strict Priority Queue) Method 인경우 우선순위가 높은 패킷을 우선적으로 처리하기 때문에 flow1 과 같은 경우는 모든 패킷이 전달되지만 가장 낮은순위의 flow3 의 패킷은 하나도 전달되지 않는 경우가 발생한다.



■ 그림 3. DRR / WRR Method

위의 그림은 WRR 과 DRR Method 의 예인데 SPQ 와 달리 포트에 설정된 weight 를 기준으로 적당한 알고리즘에 의해 적당한 비율만큼 내보내게 된다. DRR 는 WRR 과 유사하게 동작하지만, 변화하는 size 의 packet 들을 고려해서 대역폭 할당 scheduring 을 한다.
VP5200 Series 스위치의 경우 8 개의 sheduling 을 위한 Queue 를 제공하며 다음은 특정 인터페이스의 Queue 방식을 결정하는 명령어이다.

표 25. Queue-mode 변경 명령

명령어	설명	모드
queueing-mode { **strict | drr | wrr** }	해당 Interface 의 Queue-mode 를 Strict 방식 혹은 DRR / WRR 방식으로 변경한다. Default 모드는 Strict 방식이다.	Interface
queueing-method <*0-7*> **{ strict | drr | wrr }**	DRR 또는 WRR 로 설정한 interface 의 특정 queue 를 strict 로 설정하거나 해제 하기 위해서 사용한다.	Interface

Notice SPQ 에서의 우선순위는 8 개 Queue 중 숫자가 높을수록 우선순위가 높다.

Notice Queuing-mode 설정은 FX / Giga 포트의 경우 개별 설정이 가능하다. 하지만 TX 포트 인 경우는 8 개 단위로만 설정이 가능하며, 8 포트중 제일 첫번째 포트에 설정하면 8 개의 포트에 모두 적용이 된다. 예를 들어 fa1 에 설정하면 fa1 ~ fa8 까지 모두 설정된다.

다음은 DRR / WRR mode 로 설정되었을 경우에 해당 Queue 에 Weight 를 변경해주는 명령어이다.

표 26. Wrr-method Queue weight 변경 명령

명령어	설명	모드
queueing-profile drr-weight ***<0-7> <1-15>***	해당 포트가 drr 모드 일 때, 지정된 queue 의 drr weight 값을 지정한다.	Interface
no queueing-profile drr-weight	해당 포트가 drr 모드 일 때, 지정된 queue 의 drr weight 값을 디폴트 값으로 설정한다.	Interface
queueing-profile wrr-weight ***<0-7> <1-15>***	해당 포트가 wrr 모드 일 때, 지정된 queue 의 wrr weight 값을 지정한다.	Interface
no queueing-profile wrr-weight	해당 포트가 wrr 모드 일 때, 지정된 queue 의 wrr weight 값을 디폴트 값으로 설정한다.	Interface

다음은 각 포트의 scheduling 관련 상태를 한눈에 알수 있게 하여준다.

표 27. 전체 interface 의 queue-method 및 weight 조회명령

명령어	설명	모드
show port qos	시스템의 모든 인터페이스의 queue-method 및 weight 값을 보여준다.	Privileged

10.6.4. Congestion Avoidance

출력쪽의 큐에서 나타나는 혼잡은 실지 네트웍에서 입력 링크와 출력 링크사이에서 속도의 불협화로 출력쪽의 큐가 넘치면서 빈번히 발생한다. 큐의 혼잡이 발생했을 때 버퍼의 자원을 가용하게 하기 위해서 버퍼안에 있는 패킷을 버리는 것과 패킷의 지연시간이 원하는 값 이하로 유지하도록 하는 것이 중요하다.
VP5200 Series 스위치는 Flow Classifier 나 Traffic Conditioner 에 의해서 마크된 높은 순위에 있는 패기할 패킷을 우선적으로 버린다. VP5200 Series 에서 이를 위한 파라메타은 트래픽 종류에 따라 큐별로 서로 다르게 설정될 수 있다.

10.6.5. Filtering

Netbios 필터는 개별 인터페이스 별로 설정이 가능하며,. Netbios 필터를 설정하면, Netbios / Netbeui / NBT 프로토콜이 모두 차단된다. Dhcp 필터는 개별 인터페이스 별로 설정이 가능하며, 이 필터를 설정하면 해당 인터페이스의 DHCP server 패킷이 차단된다. 또한, 사설 IP 와 loopback IP 를 차단할 수 있다.

명령어들은 다음과 같다.
설정된 내용은 show interface 로 확인이 가능하다.

표 28. 기타 **Filtering** 관련 명령

명령어	설명	모드
filter netbios	특정 인터페이스에 netbios 필터를 설정한다...	Interface
no filter netbios	특정 인터페이스에 netbios 필터를 해제한다.	Interface
filter dhcp	특정 인터페이스에 dhcp filtering 을 설정한다.	Interface
no filter dhcp	특정 인터페이스에 dhcp fltering 을 해제한다.	Interface
filter lltd	특정 인터페이스에 lltd filtering 을 설정한다.	Interface
no filter lltd	특정 인터페이스에 lltd fltering 을 해제한다.	Interface
filter private-ip [10|172|192|all]	특정 인터페이스에 사설 IP filtering 을 설정한다.	Interface
no filter private-ip [10|172|192|all]	특정 인터페이스에 사설 IP filtering 을 해제한다.	Interface
filter src-ip-all-f	특정 인터페이스에 src IP 가 all f (255.255.255.255) 인 패킷의 filtering 을 설정한다.	Interface
no filter src-ip-all-f	특정 인터페이스에 src IP 가 all f (255.255.255.255) 인 패킷의 filtering 을 해제한다.	Interface
filter src-ip-loopback	특정 인터페이스에 loopback ip (127.0.0.0/8) 인 패킷의 filtering 을 설정한다.	Interface
no filter src-ip-loopback	특정 인터페이스에 loopback ip (127.0.0.0/8) 인 패킷의 fltering 을 해제한다.	Interface