

Premier 3124FG Switch Common User Guide

Chapter #10





Chapter 10

상태 모니터링 및 통계

본 장은 현재 운영중인 Premier 3124FG 스위치의 상태를 파악하고, 로그의 정보를 화면에 표시하고, RMON(Remote Monitoring)을 통한 운영 관리 기능에 대하여 설명한다.

또한 Premier 3124FG 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.

상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. Premier 3124FG 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.

포트 통계

Premier 3124FG 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]
```

Premier 3124FG 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 down

type 100Base-TX

ifindex 0(k2) BROADCAST multicast

auto-negotiation

speed set auto

duplex set full

Last clearing of counters 17:31:00

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 down

type 100Base-TX

ifindex 1(k3) BROADCAST multicast

auto-negotiation

speed set auto

duplex set full

Last clearing of counters 17:31:00
 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
 - - More - -

표2. 포트 통계조회 조회 명령

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

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

Switch# **show port counter**

```

ifname I-Kbps O-Kbps InOctets InUpkt InNUpkt OutOctets OutUpkt OutNUpkt
-----
-----
fa1      0      0      0      0      0      0      0      0
fa2      0      0      0      0      0      0      0      0
fa3      0      0      0      0      0      0      0      0
fa4      0      0      0      0      0      0      0      0

```

fa5	0	0	0	0	0	0	0	0
fa6	0	0	0	0	0	0	0	0
fa7	0	0	0	0	0	0	0	0
fa8	0	0	0	0	0	0	0	0
fa9	0	0	0	0	0	0	0	0
fa10	0	0	0	0	0	0	0	0
fa11	0	0	0	0	0	0	0	0
fa12	0	0	0	0	0	0	0	0
fa13	0	0	0	0	0	0	0	0
fa14	0	0	0	0	0	0	0	0
fa15	0	0	0	0	0	0	0	0
fa16	0	0	0	0	0	0	0	0
fa17	0	0	0	0	0	0	0	0
fa18	0	0	0	0	0	0	0	0
fa19	0	0	0	0	0	0	0	0
fa20	0	0	0	0	0	0	0	0
fa21	0	0	0	0	0	0	0	0
fa22	0	0	0	0	0	0	0	0
fa23	0	224	2266323	11646	120	1779661246	19781	
1528642								
fa24	224	0	1779736598	20000	1528693	2279097	11857	
120								
fa25	0	0	0	0	0	0	0	0
fa26	0	0	0	0	0	0	0	0

Switch#

Switch#

Switch# **show port statistics fa24**

Last clearing of counters 17:31:45

	RX				TX		
	bits/s	bytes/s	pkts/s		bits/s	bytes/s	pkts/s
5sec :	222656	27832	23		0	0	0
1min :	223912	27989	23		40	5	0
5min :	222840	27855	23		80	10	0
Switch#							

또한 다음의 명령을 사용하여 show interface 시 보여주는 통계에 대한 설정을 바꾸거나 해당 인터페이스의 특정 기간의 High/Low threshold 값을 설정하여 log 로 남길수 있다.

표3. 포트 통계조회 설정 명령

명령어	설명	모드
load interval <5-100>	Show interface 시 보여주는 평균 값의 기간을 셋팅한다.	interface
no load interval	Show interface 시 보여주는 평균 값의 기간을 디폴트값으로 변경한다.(60 초)	interface
input-load-monitor <5-100> <1-1000> <1-1000>	해당 인터페이스의 특정 기간 동안의 low/high threash 설정하여 syslog, snmp trap 을 통해 보고한다.	interface
no input-load-monitor	Input-load-monitor 를 해제한다.	interface

다음 명령은 통계치에 대한 누적치를 초기화시키는 명령어이다.

표4. 포트 통계 초기화 명령

명령어	설명	모드
clear counters	시스템의 모든 인터페이스의 통계 누적치를 초기화한다.	privileged
clear counters <i>IFNAME</i>	특정 인터페이스의 통계누적치를 초기화한다.	privileged
clear counters snmp	시스템의 모든 인터페이스의 snmp 를 위한 통계누적치를 초기화한다.	privileged

Logging

Premier 3124FG 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.

Premier 3124FG 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.

Premier 3124FG 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

표 5. Premier 3124FG 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.

시스템 로그 메시지 내용

Premier 3124FG 스위치의 시스템 로그 메시지는 다음과 같은 내용을 제공한다.

- Timestamp

(Timestamp 는 이벤트가 발생한 월, 날짜, 연도 및 구체적인 시간 정보를 HH:MM:SS MM/DD/YYYY 과 같이 기록한다.

- Severity level

(<표 1>에서 정의한 Premier 3100 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
```

디폴트 Logging 설정 값

표 6. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	enabled
Telnet 세션으로의 로깅 출력	enabled.
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	Warnings(4)

표 7. 시스템 메시지 로깅 환경 설정 명령

명령어	설명
logging console { <i>enable/disable</i> }	• 콘솔로의 로깅 출력 여부 설정.
Logging session { <i>enable/disable</i> }	• 현 세션으로의 로깅 출력 여부 설정.
Logging session level <0 - 7>	• 현 세션으로 출력되는 로그 메시지의 레벨 설정
Logging server A.B.C.D	• 로깅서버를 지정한다.
Logging trap <logging level..>	• 로깅서버로 로깅할 로그레벨을 설정한다.
Logging facility <logging facility>	• 로깅서버로 로깅할 디바이스를 설정한다.
Show log [last] [number-of-message]	• 로깅 버퍼 출력 및 로깅 설정 확인.

■ RMON(Remote MONitoring)

시스템 운영자는 Premier 3124FG 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다.

다음 절에서는 RMON 개념 및 Premier 3124FG 스위치가 지원하는 RMON 서비스 기능에 대하여 자세히 설명한다.

RMON 개요

RMON은 IETF(Internet Engineering Task Force)의 RFC 1271와 RFC 1757에 정의되어 있는 국제 표준 규격으로 시스템 운영자가 네트워크를 원격으로 관리하는 기능을 제공한다. 일반적으로 RMON은 다음의 두 가지 구성 요소로 구성된다.

■ RMON probe

- 원격으로 제어되면서 지속적으로 LAN 세그먼트 또는 VLAN의 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 probe와 통신하면서 통계 정보를 수집
- 반드시 RMON probe와 동일한 네트워크에 있을 필요는 없으며, RMON probe를 in-band 또는 out-of-band 연결을 통하여 제어

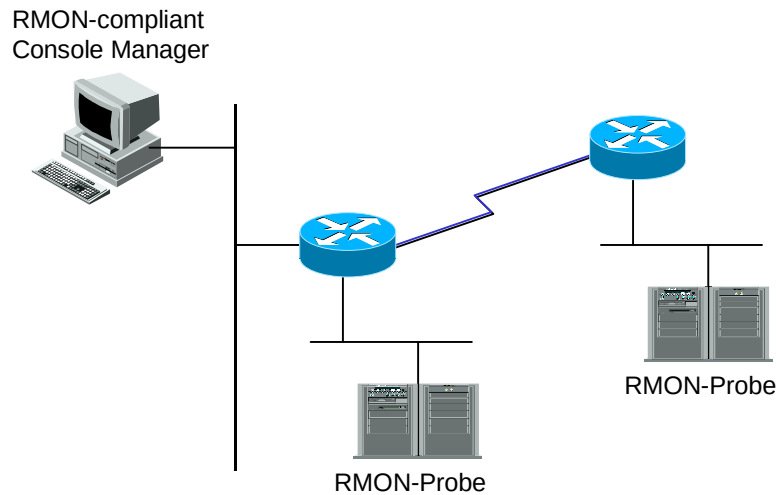


그림 1. RMON Manager 와 RMON Probe

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.

Premier 3124FG 스위치에서는 <표 >에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON 은 디폴트로 모든 설정이 disabled 이다.

표 8. 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 지속적인 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 호스트를 찾는다. - 관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 얻을 수 있다.
트래픽 매트릭스	- 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 알 수 있다. - 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없다.
필터	관리자가 특정한 패킷의 동향을 감시하기 위해서 이용한다.

패킷 수집	■ 세그먼트에 발생한 패킷을 수집해서 관리자가 분석.
사건	■ 특정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고 메시지를 보낸다. 트랩 발생 및 기록보관은 선택적이다.

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 9. RMON Alarm and Event 설정 명령

명령어	설명	모드
<code>rmon alarm <i>index</i> ifEntry <i>variable</i> ifIndex interval {delta absolute} rising-threshold <i>value</i> [event-number] falling-threshold <i>value</i> [event-number] [owner string]</code>	■ RMON 의 Alarm Table 에 Alarm 을 추가 ■ Index : 1 부터 65535 의 정수 값. ■ Variable 은 MIB object ■ interval 은 alarm variable 을 관찰한 시간 간격으로 초 단위 ■ delta 는 MIB variable 값의 샘플간의 값의 차이를 관찰함을 말하며, absolute 는 MIB variable 의 절대값을 말한다. ■ rising-threshold 와 falling-threshold 의 값을 각각 설정한다. ■ event 의 설정은 option 이며, alarm variable 의 delta 값이나 absolute 값이 rising-threshold 나 , falling threshold 값에 도달했을 때 각각 해당 Event 가 발생한다.	Config

	Alarm 의 owner 를 명시할 수 있다.	
rmon event <i>index</i> [log] [trap community <i>string</i>] [owner <i>string</i>] [description <i>string</i>]	- RMON Event table 에 Event 를 추가한다. - log 는 event 가 발생했을 때, RMON log 를 생성할 것인지를 명시한다. Trap 은 Event 가 발생했을 때, trap 을 보낼 것인지를 명시한다.	Config
no rmon alarm <i>alarm-index</i>	RMON Alarm table 에서 alarm 을 삭제한다.	Config
no rmon event <i>event-index</i>	RMON Event Table 에서 event 를 삭제한다.	Config
show rmon alarm	RMON alarm table 을 보여준다.	Privileged
show rmon event	RMON event table 을 보여준다.	Privileged
show rmon log	RMON log table 을 보여준다.	Privileged

Switch# **configure terminal**

Switch(config)# **rmon alarm 10 ifEntry inErrors 1 20 delta rising-threshold 15 1 falling-threshold 0 owner mijiok**

Switch(config)# **rmon event 1 log trap community rmonTrap owner mijiok 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         : mijiok

```

Switch# **show rmon event**

```

-----
                Event Configurations
-----

```

```

The Index of event : 1
eventDescription   : "Noti:TooMuchInErrors"
eventType          : log and trap
Community          : rmonTrap
eventOwner         : mijiok
Switch#

```

표 10. RMON Statistics And History 설정 명령

명령어	설명	모드
<code>rmon history <i>index</i> ifEntry <i>ifIndex</i> [buckets <i>bucket-number</i>] [interval seconds] [owner <i>string</i>]</code>	■ 명시된 bucket 의 수와 interval 간격으로 이력을 수집 ■ index 값은 1 부터 65535 까지 할당할 수 있다. ■ Bucket 의 default 개수는 50	Config
<code>no rmon history <i>index</i> ifEntry <i>ifIndex</i></code>	■ History 수집을 Disable 시킨다..	Config

show rmon history	■ RMON history table 을 보여준다. Privileged
show rmon statistics	■ RMON statistics table 을 보여준 Privileged 다.

Switch# **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                 : locus

```

```
The Index of stats : 2
Interface          : fa2
Drop Events        : 0
Total Octets       : 0
Total Packets      : 0
.....
Switch#
```

```
Switch# configure terminal
Switch#(config)# rmon history 1 ifEntry 1 buckets 20 interval 10 owner mijiok
Switch#(config)# exit
Switch# show rmon history
```

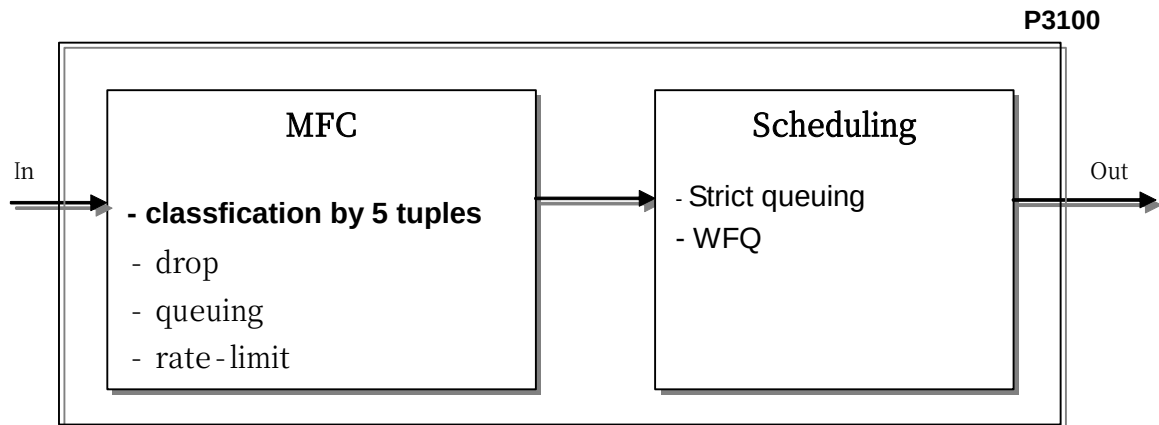
```
-----
                SHOW HISTORY
-----
```

```
===== fa1 =====
Control-index      : 1
ifindex            : 1
interval           : 10
buckets            : 20
owner              : hong
```

```
--- fa1 : bucket 1 ---
DropEvents         : 0
Octets             : 0
Pkts               : 0
BroadcastPkts      : 0
MulticastPkts      : 0
CRCAlignErrors     : 0
UndersizePkts      : 0
OversizePkts       : 0
```

Fragments	: 0
Jabbers	: 0
Collisions	: 0
Utilization	: 0
- - - fa1 : bucket 2 - - -	
DropEvents	: 0
Octets	: 0
Pkts	: 0
BroadcastPkts	: 0
MulticastPkts	: 0
CRCAAlignErrors	: 0
UndersizePkts	: 0
OversizePkts	: 0
Fragments	: 0
Jabbers	: 0
Collisions	: 0
Utilization	: 0
- - - fa1 : bucket 3 - - -	
DropEvents	: 0
Octets	: 0
Pkts	: 0
BroadcastPkts	: 0
MulticastPkts	: 0
CRCAAlignErrors	: 0

Qos 및 Packet Filtering



본 Premier 3124FG 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 우선 순위대로 처리하여 우선 순위가 높은 데이터를 빨리 처리되지만 우

선도가 낮은 데이터는 처리 순서가 밀린다. 만약 대역폭 전체가 우선 순위 높은 데이터로 채워지면 낮은 우선순위의 트래픽은 전혀 통과하지 못하고 대기 상태에 놓이는 단점을 지니고 있는 방식이다.

- WFQ(Weighted Fair Queuing Method)

일정 비율을 기반으로 데이터를 처리하는 방식으로 SPQ 방식의 단점을 보완할 수 있는 알고리즘으로서 큐에 일정한 크기의 처리율을 사용자가 자신의 환경에 맞게 설정할 수 있다.

MFC(Multi-Field Classifier)

Flow-Rule 설정/해제

패킷을 처리하는 정책을 설정하기 위해 적용할 대상이 되는 규칙을 설정하여야 하는데 이는 Flow-rule 을 classification 설정으로 가능하다.

Flow-rule 은 프로토콜, src/dest IP, UDP/TCP Port, dscp, Tcp sync 등의 지정된 값에 의해 다양하게 classification 할 수 있다. 또한, 특수 목적의 필터링을 위한 netbios-filter, nbt-filter, dhcp-filter 등의 classification 을 지원하는데 이는 다른 action 을 적용하지 못하며 오직 Filtering(drop)만을 위해 사용된다.

표11. Flow-rule Classification 명령

명령어	설명	모드
<code>flow-rule NAME classify { <0-255> icmp igmp ip ospf pim tcp udp } { SRCIP / MASK any } { DSTIP / MASK any }</code>	rule 이 적용된 포트의 특정 프로토콜에 대한 모든 혹은 지정된 src/dest ip 에 대해 적용	Config
<code>flow-rule NAME classify { tcp udp } { SRCIP MASK / any } { DSTIP /MASK / any } { <0-255> / SRCPORT } { <0-255> / DSTPORT }</code>	flow-rule 이 적용된 포트의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 에 대해 적용	Config

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.

표12. Flow-rule 정책 적용 명령

명령어	설명	모드
flow-rule <i>NAME</i> match drop	규칙과 일치하는 패킷을 불허한다.	Config
flow-rule <i>NAME</i> match queue <i>VALUE</i>	규칙과 일치하는 패킷의 해당값을 지정된 우선순위의 Queue 할당한다.	Config
flow-rule <i>NAME</i> match queuing-and-marking <i>VALUE</i>	규칙과 일치하는 패킷의 해당값을 지정된 우선순위의 Queue 할당하며, Queue 에 할당된 Cos 값으로 패킷에 marking 한다.	Config
flow-rule <i>NAME</i> match rate-limit <8-1000000>	규칙과 일치하는 패킷을 지정된 속도로 rate-limit 한다.	Config
rate-limit-aggregator <i>NAME</i> <8-1000000>	Rate-limit-aggregator 를 생성한다.	Config
flow-rule <i>NAME</i> match rate-limit aggregator <i>NAME</i>	Rate-limit 를 특정 Rate-limit-aggregator 를 이용해서 적용한다.	Config
no flow-rule <i>NAME</i> match	정책을 삭제한다.	Config
no rate-limit-aggregator <i>NAME</i>	Rate-limit-aggregator 를 삭제한다.	Config



Notice 위의 모든 정책은 flow-rule 에 하나만 적용된다.



Notice rate-limit 은 8kbps 단위로 설정이 가능하며, system wide 하게 7 개의 rate 값을 가질 수 있다.



Notice rate-limit-aggregator 는 여러 개의 flow-rule 에 해당하는 트래픽을 통합하여 rate-limit 을 걸려고 할 때 사용한다.

다음은 특정 flow-rule 을 삭제하는 명령어이다.

표13. flow-rule 삭제 명령

명령어	설명	모드
No flow-rule <i>NAME</i>	NAME 의 flow-rule 을 삭제한다.	Config

Flow-Rule 의 모드 설정

각 Flow-rule 은 그 특성에 따라 다음의 4 가지 모드를 셋팅할 수 있다.
이를 이용하여 Qos 의 선택조건이 되는 필드들을 바꾸지않고 그대로 보내거나, Qos mapping table(**show qos cos** 을 통해 확인 가능)의 값에 의해 Qos 필드들이 marking 될것인지, 혹은 유저에 의해 셋팅된 값에 의해 marking 할것인지 등을 결정한다. marking/remarking 에 대해서는 다음절에서 다시 설명된다.

policy-map 생성/추가

인터페이스에 Flow-rule 을 적용하기위해 Policy-map 을 만들어 적용하며, Policy-map 에는 다수의 Flow-rule 이 포함될수 있어, 한 인터페이스에 다수의 정책이 적용될수 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.

표14. Policy-map 생성 및 추가 명령

명령어	설명	모드
policy-map <i>PNAME</i> flow-	PNAME 이 없는 경우는 새로이 생	Config

rule FNAME	성하고 PNAME 의 policy 가 기존에 있는 경우는 FNAME 의 flow 가 마지막으로 추가된다.	
-------------------	--	--

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

표15. 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.

표16. policy-map 적용/해제 명령

명령어	설명	모드
service-policy IFNAME PNAME	특정 포트 인터페이스 (IFNAME) 에 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 적용 될 경우, drop 룰은 우선되어 적용된다.

다음의 명령을 사용하여 flow-rule 관련 설정을 조회할 수 있다.

표17. 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 돕기 위해 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 3 (highest) 및 marking
  
```

```

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 10.1.1.0/24 any
Switch(config)# flow-rule f2 match queuing 3
Switch(config)# flow-rule f3 classify tcp any any 23 any
Switch(config)# flow-rule f3 match queuing-and-marking 3
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**

Switch(config)#

예 2) fa2 포트에 다음과 같이 적용한다.

Tcp 4010 포트에 rate limit 10Mbps

tcp 5010, 5020 포트에 통합하여 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)# **rate-limit aggregator ra1 20000**

Switch(config)# **flow-rule f5 classify tcp any any 5010 any**

Switch(config)# **flow-rule f5 match rate-limit aggregator ra1**

Switch(config)# **flow-rule f6 classify tcp any any 5020 any**

Switch(config)# **flow-rule f6 match rate-limit aggregator ra1**

Switch(config)#

Switch(config)# **policy-map p2 flow-rule f4**

Switch(config)# **policy-map p2 flow-rule f5**

Switch(config)# **policy-map p2 flow-rule f6**

Switch(config)#

Switch(config)# **service-policy fa2 p2**

service-policy pol1

Switch#

Qos 관련 파라미터

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. Premier 3100 시리즈는 각 인터페이스별로 4 개의 queue 를 가지고 있으며, 이 둘 사이의 mapping table 을 system wide 하게 유지하고 있다. 이 테이블은 다음의 명령어를 통해 marking/remarking 될 값을 변경할수 있다.

표18. Qos관련 Marking/Remarking 테이블 셋팅 명령

명령어	설명	모드
qos cos-queue-map <i><0-7> <0-3></i>	규칙에 적용된 패킷의 cos 값에 의해 mapping 될 새로운 queue 값을 설정한다. 이는 show qos cos 로 확인 가능하다.	Config
qos cos-remarking <i><0-3> <0-7></i>	규칙에 적용된 패킷의 queue 값에 의해 remarking 될 새로운 Cos 값을 설정한다.	Config

표19. Qos관련 Marking/Remarking 테이블 조회명령

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

Scheduling

Premier 3124FG 스위치에서는 Scheduling 을 위해 SPQ(Strict Priority Queue) Method 와 WFQ(Weighted Fair Queing) Mothod 를 제공하며 디폴트는 SPQ 이다. 다음 그림은 SPQ 와 WFQ 의 차이점을 나타내고 있다.

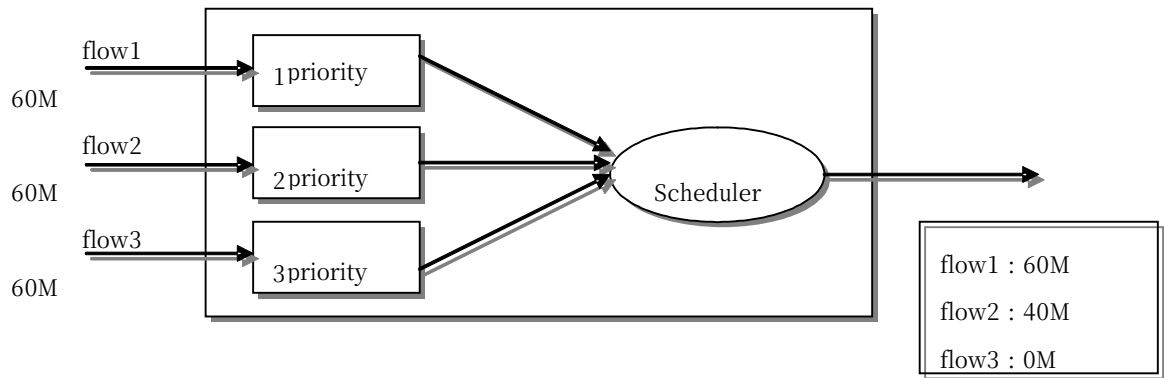


그림 2. SPQ(Strict Priority Queue) Method

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

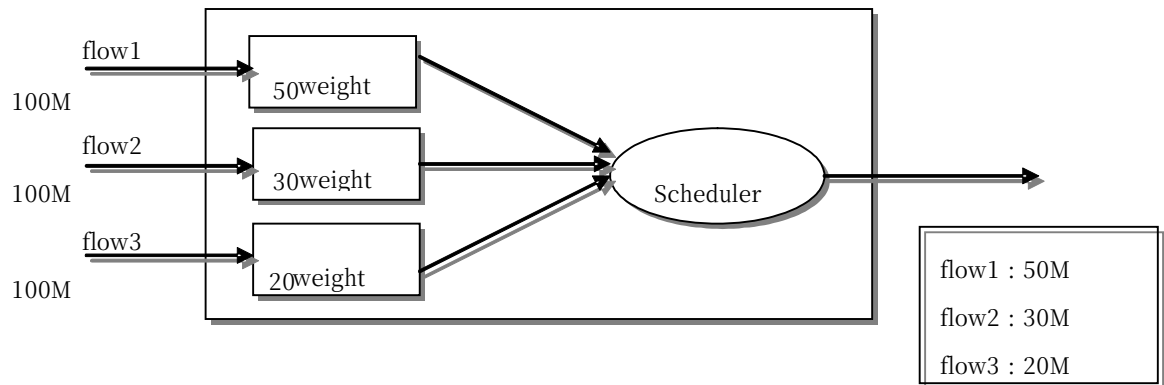


그림 3. WFQ(Weighted Fair Queing) Method

위의 그림은 WFQ(Weighted Fair Queing) Method 의 예인데 SPQ 와 달리 포트에 설정된 weight 를 기준으로 적당한 알고리즘에 의해 적당한 비율만큼 내보내게 된다. WFQ 는 WRR 과 유사하게 동작하지만, WRR 처럼 weight 에 따른 균등 분배는 아니기 때문에, 트래픽의 상태에 따라서 높은 우선순위의 Queue 에 weight 값

보다 더 많은 트래픽이 할당될 수 있다는 장점이 있다.

Premier 3124FG 스위치의 경우 4 개의 scheduling 을 위한 Queue 를 제공하며 다음은 특정 인터페이스의 Queue 방식을 결정하는 명령어이다.

표20. Queue-method 변경 명령

명령어	설명	모드
<code>queue-method <0-3> { strict wfq }</code>	해당 Interface 의 Queue-method 를 Strcint 방식 혹은 WFQ 방식으로 변경한다. Default 모드는 Strict 방식이다.	Interface



Notice SPQ 에서의 우선순위는 4 개 Queue 중 숫자가 높을수록 우선순위가 높다.

다음은 WFQ Method 로 설정되었을 경우에 해당 Queue 에 Weight 를 변경해주는 명령어이다.

표21. Wrr-method Queue weight 변경 명령

명령어	설명	모드
<code>wfq-profile weight-based</code>	Weight-based wfq 로 설정한다.	Interface
<code>no wfq-profile weight-based</code>	Weight-based wfq 를 해제한다.	Interface
<code>wfq-profile weight <0-3> <100-65534></code>	해당 Interface 의 지정된 Queue 의 weight 를 변경한다. 이는 해당 queue 가 WFQ 방식일때 의미가 있다. 변경후 이는 show port qos 명령으로 확인 가능하다.	Interface
<code>wfq-profile ratio <1-99> <1-99> <1-99> <1-99></code>	Ratio-based wfq 를 설정한다.	Interface

다음은 각 포트의 scheduling 관련 상태를 한눈에 알수 있게 하여준다.

표22. 전체 interface의 queue-method 및 weight 조회명령

명령어	설명	모드
show port qos	시스템의 모든 인터페이스의 queue-method 및 WRR 방식인 경우의 weight 값을 보여준다.	Interface

Congestion Avoidance

출력쪽의 큐에서 나타나는 혼잡은 실지 네트워크에서 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. Premier 3124FG 스위치는 Flow Classifier 나 Traffic Conditioner 에 의해서 마크된 높은 순위에 있는 패킷을 우선적으로 버린다. Premier 3124FG 에서 이를 위한 파라메타는 트래픽 종류에 따라 큐별로 서로 다르게 설정될 수 있다.

Filtering

보안을 위해서 netbios filtering 을 시스템에 적용할수 있다. Netbios 필터를 설정하면, Netbios / Netbeui / NBT / AppleTalk / Novell netware 프로토콜이 모두 차단된다.

Dhcp 필터는 개별 인터페이스 별로 설정이 가능하며, 이 필터를 설정하면 해당 인터페이스의 DHCP server 패킷이 차단된다.

명령어들은 다음과 같다.

표 23. 기타 Filtering 관련 명령

명령어	설명	모드
<code>filter netbios (allports downonly stacking-tx)</code>	시스템에 netbios 필터를 설정한다. Allports 는 모든 포트에 설정하는 것이며, downonly 는 fx 를 제외한 나머지 tx 포트에만 적용한다. Stacking-tx 는 stacking 을 위해서 사용되는 tx 포트도 필터링하지 않는다..	Config
<code>no filter netbios</code>	시스템에 netbios 필터를 해제한다.	Config
<code>filter dhcp IFNAME</code>	특정 인터페이스에 dhcp filtering 을 설정한다.	Config
<code>no filter dhcp IFNAME</code>	특정 인터페이스에 dhcp filtering 을 해제한다.	Config
<code>show filter</code>	Filtering 설정을 확인한다.	Privileged



Notice

P3124FG 에서 tx 포트에 stacking 을 사용하면서 동시에 netbios 를 적용하려 할때는 stacking port 는 fa23 , fa24 를 사용하여야 한다. 두가지 기능중 하나만 적용할때는 해당되지 않는다.