

Configuring MAC Usage Alarm Threshold

- [Introduction](#)
- [Configuring MAC address table usage Alarm Threshold](#)
- [Configuration Example](#)
 - [Procedure](#)
 - [Verify the Configuration](#)

Introduction

MAC address table usage is an important indicator used to evaluate device performance. A high MAC address table usage will cause service faults. During data processing, if the device can generate an SNMP Trap alarm when high MAC address table usage occurs, you can effectively monitor MAC address table usage and optimize system performance to ensure system stability.

- MAC address table usage limit threshold and duration: When the MAC address table usage exceeds the limit threshold for a continuous period of time, the system sends an SNMP Trap alarm message.

New PICA8 Private MIB Information

OID	Object Name	Description
1.3.6.1.4.1.3509 8.1.15.1.0	oidMacThresh oldStatus	This object is in configuration information node. The value of this object identifies whether the function of monitoring the switch MAC address table usage is enabled. The value could be 0 or 1. 0: disable. 1: enable.
1.3.6.1.4.1.3509 8.1.15.2.0	oidMacThresh oldValue	This object is in configuration information node. The value of this object identifies the limit threshold for MAC address table usage monitoring. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 50.
1.3.6.1.4.1.3509 8.1.15.3.0	oidMacThresh oldPeriod	This object is in configuration information node. The value of this object identifies the time duration when the MAC address table usage continues to exceed the limit threshold. The value is an integer, in seconds, that ranges from 5 to 4294967295. The default value is 300s.
1.3.6.1.4.1.3509 8.1.15.4.0	oidMacMonitor Value	This object is in configuration information node. The value of this object identifies the MAC address table usage when the system sends the last SNMP Trap message.
1.3.6.1.4.1.3509 8.21.5.1	oidMacThresh old	This object is used in the syslog and SNMP Trap message, indicating the MAC address table usage exceeds the limit threshold over a continuous time period. The system then sends an SNMP Trap alarm message.

Configuring MAC address table usage Alarm Threshold

Step1 Enable the function of monitoring the switch MAC address table usage.

```
set protocols snmp trap-group event mac-threshold enable <true | false>
```

Step2 Set the limit threshold for MAC address table usage monitoring to send SNMP Trap messages.

```
set protocols snmp trap-group event mac-threshold limit <limit-value>
```

Step3 Configure the time duration when the MAC address table usage continues to exceed the limit threshold.

```
set protocols snmp trap-group event mac-threshold interval <interval>
```

The system samples MAC address table usage one time every 10 seconds, if the MAC address table usage exceed the limit threshold over this interval time, a SNMP trap message will be sent. But once MAC address table usage falls back below the threshold when the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Configuration Example

Procedure

Step1 Configure the target host with IP address 10.10.50.16 for receiving SNMP traps.

```
admin@Xorplus#set protocols snmp community public
admin@Xorplus#set protocols snmp trap-group targets 10.10.50.16 security-name public
```

Step2 Enable the function of monitoring the switch MAC address table usage.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold enable true
```

Step3 Set the limit threshold for MAC address table usage monitoring to send SNMP Trap messages.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold limit 50
```

Step4 Configure the time duration when the MAC address table usage continues to exceed the limit threshold, and an SNMP Trap message will be sent.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold interval 300
```

Step5 Enable SNMP traceoptions for checking the SNMP syslogs.

```
admin@Xorplus# set protocols snmp traceoptions flag all disable false
```

Step6 Commit the configuration.

```
admin@Xorplus# commit
```

Verify the Configuration

- User can check the syslog when the MAC address table usage monitoring continuously exceeds the limit threshold.

2001-01-01 06:27:44.86 Xorplus [local0.info](#) : [SNMP]Trap: send v2 trap, community name public, oid: 1.3.6.1.4.1.35098.21.5.1, to:10.10.50.16/162