

RMON

Feature Overview and Configuration Guide

Introduction

The guide describes the Remote Network MONitoring (RMON) service on the switch, and describes a configuration example showing how to set up an RMON alarm.

This RMON alarm configuration example described creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch port exceeds a threshold, and creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch drops below a lower threshold. RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support RMON, running version **5.4.4** or later.

From version 5.4.9-1.1 onwards, RMON includes enabling this feature over tunnel interfaces.

From version 5.5.0-2.1 onwards, you can create alarms for history entries as well as statistics.

To see whether your product supports RMON, see the following documents:

- The [product's Datasheet](#)
- The product's [Command Reference](#)

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Content

Introduction 1

 Products and software version that apply to this guide 1

Overview.....3

RMON Configuration Example4

Overview

The Remote Network MONitoring (RMON) MIB (RFC2819) was developed by the IETF to support monitoring and protocol analysis of LANs with a focus on Layer 1 and 2 information in networks. RMON is an industry standard that provides the functionality for network analyzers.

RMON is a process that runs within Alliedware Plus, to collect and store certain statistics (primarily, counters on Ethernet ports). The collected statistics can then be gathered from the switch by a network management station. The values stored by RMON can be accessed as SNMP Objects. The OID values for these objects are defined in the RMON MIB.

In the language of RMON, the Alliedware Plus device that is collecting the RMON statistics is referred to as a **probe**.

RMON is mainly used for 'flow-based' monitoring, while SNMP is mainly used for 'device-based' management. Data collected by RMON deals mainly with traffic patterns on the network, and data collected by SNMP usually deals with the status of individual devices on the network.

One disadvantage of flow based monitoring is that remote devices have much more of the management burden, and require more resources. AlliedWare Plus minimizes the management and resources burden by implementing a subset of the RMON MIB group to provide a minimal RMON agent implementation supporting statistics, history, alarms, and events.

The RMON groups supported in AlliedWare Plus are:

- **Statistics** - collects Ethernet statistics on a switch port, such as utilization and collisions.
- **History** - collects a history of Ethernet statistics on a switch port.
- **Alarms** - monitor a MIB object for a specified interval, trigger an alarm at a specified value (the 'rising threshold'), and resets the alarm at another value (the '**falling threshold**'). Alarms are used with events to trigger alarms, which generate logs or SNMP traps.
- **Events** - specify the action to take when an event is triggered by an alarm.

The action of an event can generate a log or an SNMP trap.

You can create alarms:

- for statistics and (from 5.5.0-2.1 onwards) history entries
- on switch ports
- and on eth ports and (from 5.4.9-1.1 onwards) tunnel interfaces on AR series devices.

RMON Configuration Example

This configuration example sets up an RMON alarm to create SNMP traps and log messages. This RMON alarm creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch port exceeds a threshold, and creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch port drops below a lower threshold.

Step 1: Set up an RMON collection on the switch port that is being monitored.

Use the following commands to configure this functionality:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# rmon collection stats 4
```

This will cause the software to build a table in which it stores statistics relating to the switch port.

Step 2: Define an RMON event that will be called by the alarm when the thresholds are passed.

Create this as a 'trap and log' event, so that both an SNMP trap and a log message will be generated. The trap will be sent to the SNMP community named 'public'. Use the following command to configure this functionality:

```
awplus# configure terminal
awplus(config)# rmon event 10 log trap public
```

Step 3: Create the RMON alarm.

Every 5 seconds, the alarm checks the broadcast packet counter in RMON collection stats 4. If the change in the value of that counter over the 5 second interval exceeds 5000 (1000 broadcasts per second), the alarm will trigger the event defined in step 2 above. Additionally, when the rate broadcast falls below 500 broadcasts per 5 seconds, then the alarm will trigger the event defined in step 2 above again.

Use the below command to configure this functionality:

```
awplus# configure terminal
awplus(config)# rmon alarm 5 etherStatsBroadcastPkts.4 interval 5
delta rising-threshold 5000 event 10 falling-threshold 500 event 10
alarmstartup 3
```

For the variable '**etherStatsBroadcastPkts.4**' in this command, note that '**.4**' refers to the index number of the RMON collection stats 4 as defined on port1.0.4 in step 1.

So, '**etherStatsBroadcastPkts.4**' refers to 'Received broadcasts' in RMON collection stats 4. Further counters for RMON are defined in section 5 of RFC 2819.

Step 4: Enable RMON traps.

To ensure that the SNMP trap is sent, you need to enable RMON traps, and you need to define a trap host in SNMP. Use the below commands to configure this functionality:

```
awplus# configure terminal
awplus(config)# snmp-server
awplus(config)# snmp-server enable trap rmon
awplus(config)# snmp-server community public
awplus(config)# snmp-server host 192.168.2.254 version 2c public
```

Note that the resulting log message will be of the form listed below:

```
RMON [1024]: Alarm Index 5 alarm Rising Threshold 5000 alarm Value 5117
alarm Rising event Index 10 event description RMON_SNMP
```