How To | Monitor Ethernet interface state changes

Introduction

This document describes how to monitor Ethernet interface state changes on your Allied Telesyn routers.

Most interfaces that you are able to define on your router place output definitions and log messages showing port state changes. These in turn can then be sent through to a remote syslog.

For most VLAN and SYN/BRI interfaces you can do this using the following commands:

```
create log out=1 destin=syslog server=x.x.x.x
add log out=1 type=pint
```

However, this does not work for Ethernet interfaces, so to overcome this you can configure SNMP with link traps or use Allied Telesyn's triggers.

Examples of these methods are given in this document.

What information will you find in this document?

This document provides information on:

Which product and software version does this information apply to?

The information provided in this document applies to the following products:

- AR400 series routers
- AR700 series routers

running software release 2.6.1 and above.

Monitoring Ethernet interfaces using SNMP with linktraps

This configuration will cause an SNMP trap to be sent to the traphost every time the eth ports undergo a state change.

To monitor Ethernet interfaces via SNMP with linktraps, use the following configuration.

SNMP configuration

```
enable snmp
create snmp community=public open=on
enable snmp community=public trap
add snmp community=public traphost=10.33.27.24
```

Note: *You should change the community name to be unique due to security reasons.*

INTERFACE configuration

```
enable int=eth0 linktrap
enable int=eth1 linktrap
```

Monitoring Ethernet interfaces using triggers

To monitor Ethernet interfaces using triggers, use the following configuration.

```
enable trigger
create trigger=1 interface=eth1 event=down script=eth1down.scp
create trigger=2 interface=eth1 event=up script=eth1up.scp
```

where the content of the file eth1down.scp is:

```
eth1_down
```

and the content of the file eth1up.scp is:

```
eth1_up
```

This configuration places trigger activation log messages and error log messages when the trigger script is run, which gives you an `eth1_down` or `eth1_up` message in the log. You could then send these log messages to your syslog, using the commands:

```
create log output=1 destination=syslog server=10.33.27.24 secure=no
  messages=1

add log output=1 filter=2 module=CH
```

The log message sent to your syslog would look something like:

```
09-27-2004 16:58:29 User.Error 172.28.6.100 CH:MSG/ERROR,
Unknown command "eth1_UP"
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesyn.com

C613-16053-00 REV A