SNMP Traps

The T:LAN can be configured to generate SNMP traps once a certain set of conditions arises. The configuration of these traps is controlled through the Protocols/SNMP Menu.

Overview

Simple Network Management Protocol (SNMP) is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It is used to monitor network-attached devices for conditions that warrant administrative attention.

The idea behind trap-directed notification is that if a manager is responsible for a large number of devices, it is impractical for the manager to request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as an event trap.

After the manager receives the event trap, the manager can take corrective action, as required. Trap-directed notifications can reduce network costs and agent resources by eliminating frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap if the device has had a catastrophic outage.

Types of SNMP Traps

The T:LAN distinguishes between eight different classes of SNMP traps. Each class can be individually enabled or disabled for each trap recipient. They include:

- Coldstart Trap
- Warmstart Trap
- WAN1 LinkUp/LinkDown Traps
- WAN2 LinkUp/LinkDown Traps
- LAN LinkUp/LinkDown Traps
- PPP LinkUp/LinkDown Traps
- Authentication Failure Traps
- Enterprise Specific Traps

When SNMP Traps Are Sent

The following table identifies when specific SNMP Traps are sent:

SNMP Trap Type	Condition
coldStart	Power cycling/Cold boot, or when the Reset button is pressed by the operator.
warmStart	OS upgrades, or when user initiated reboot through the General Menu.
linkDown	**WAN INTERFACES:** Cabling error/disconnect. Loss of Signal (LOS). Loss of Framing/Synchronization (LOF). Remote Alarm Indication (RAI) (remote lost RX). Optima Link:Guard reporting link is down. **LAN INTERFACES:** LAN1-4 port down events. Optima Link:Guard reporting link is down. **PPP INTERFACE:** Cabling error/disconnect. Modem reports carrier lost. PPP time-out. PPP communication failure. Optima MDL/PPP being wound down. Optima Link:Guard reporting link is down.
linkUp	**WAN INTERFACES:** SYNC. Optima Link:Guard reporting link is up. **LAN INTERFACES:** LAN1-4 port up events. Optima Link:Guard reporting link is up. **PPP INTERFACE:** Optima MDL/PPP reports link is up. Optima Link:Guard reporting link is up.
authenticationFailure	T:LAN received a SNMP transaction request with an invalid community string.
enterpriseSpecific	Various. See MIB documentation.

Link Up/Link Down Traps

The T:LAN will send WAN Link Up/Down traps under the following conditions:

Admin State Condition	Operation State Condition	Action Taken
Down	Transitions from UP to DOWN	None (Reporting disabled)

Admin State Condition	Operation State Condition	Action Taken
Down	Transitions from DOWN to UP	None (Reporting disabled)
Up	Transitions from UP to DOWN	Send link down trap
Up	Transitions from DOWN to UP	Send link up trap
Transitions from UP to DOWN	State is DOWN	Send link down trap
Transitions from Up to DOWN	State is UP	Send link down trap
Transitions from DOWN to UP	State is UP	Send link up trap

Additional Variable Bindings

The following table lists some additional variable bindings that may appear in Link Up/Link Down SNMP Traps:

Variable	Description
OID1	ifIndex OID (1.3.6.1.2.1.2.2.1.1.x) Identifies the interface that caused the linkUp/linkDown trap. Only present for linkUp/linkDown traps.
OID2	ifAdminStatus OID (1.3.6.1.2.1.2.2.1.7.x) Shows the administrative status of the interface causing the linkUp/linkDown trap. Only present for linkUp/linkDown traps.
OID3	ifOperStatus OID (1.3.6.1.2.1.2.2.1.7.x) Shows the operative status of the interface causing the linkUp/linkDown trap. Only present for linkUp/linkDown traps.
OID4	sysLocation OID (1.3.6.1.2.1.1.6.0) As defined by the user in the GENERAL menu.
OID5	sysName OID (1.3.6.1.2.1.1.5.0) As defined by the user in the GENERAL menu.
OID6	sysContact OID (1.3.6.1.2.1.1.4.0) As defined by the user in the GENERAL menu.

Refer to the "RIO User Guide" for information on the RIO SNMP Notifications.