Quick Note 36

Configuring SNMP Trap alerting on a TransPort router

TransPort Support
March 2013
## Contents

1  Introduction ................................................................................................................................. 3
   1.1  Outline ................................................................................................................................. 3
   1.2  Assumptions .......................................................................................................................... 3
   1.3  Corrections ............................................................................................................................. 3
   1.4  Version & Revision History ................................................................................................. 3
2  Configuration .................................................................................................................................. 4
   2.1  Configuring the Event Logcodes ............................................................................................. 4
   2.2  Configuring the Event Settings ............................................................................................. 8
   2.3  Configure SNMP ..................................................................................................................... 8
3  SNMP Trap receiver software ......................................................................................................... 10
4  Testing .......................................................................................................................................... 10
5  Configuration Files ......................................................................................................................... 12
   5.1  Digi TransPort Configuration Files ....................................................................................... 12
   5.2  Digi TransPort Firmware Versions ....................................................................................... 13
1 INTRODUCTION

1.1 Outline
This document contains information regarding the configuration and use of SNMP traps.

All Digi TransPort products contain an event log. Whenever the Digi TransPort firmware does any significant operation an event is stored in the event log. Each event can be used to trigger an automatic email, SNMP trap, syslog alert or on products with GPRS/WCDMA an SMS message.

1.2 Assumptions
This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

This application note applies to:
Models shown: Digi TransPort WR21.

Other Compatible Models: All Digi TransPort products.

Firmware versions: 5.146 or newer.

Configuration: This Application Note assumes that the Digi TransPort product has a PPP instance configured to connect to the Internet and is connected to a LAN. SNMP traps will be configured to notify a LAN connected SNMP management server when the PPP connection on the WAN interface changes its UP/DOWN status.

1.3 Corrections
Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com
Requests for new application notes can be sent to the same address.

1.4 Version & Revision History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Published</td>
</tr>
</tbody>
</table>
2 CONFIGURATION

2.1 Configuring the Event Logcodes

First it is necessary to choose which events should trigger the SNMP traps.

The Event logcodes are configured from Configuration - Alarms > Event Logcodes. The list of events and trigger priorities is held in a file called logcodes.txt, when the event logcodes are changed the changes will not appear in the config.da0 or logcodes.txt files, but are stored in the logcodes.dif file once the changes have been saved.

In order to send an SMS alert when a particular event occurs, the Alarm Priority for the event should be changed. There can be a number of reasons for each event. Each event can be configured with a global Alarm Priority which applies to all the reasons. It is also possible to override the global event Alarm Priority with a different Alarm Priority for each reason.

In the example below the Event 5 “%e %a down” will be used to trigger an SNMP trap when PPP 1 is down and Event 153 “PPP 1 up” will be used to trigger an SNMP trap when PPP 1 is up.

Navigate to Configuration - Alarms > Event Logcodes

The following table describes the meaning of each column.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>A numerical value that represents the event</td>
</tr>
<tr>
<td>Description</td>
<td>The main description of the event.</td>
</tr>
<tr>
<td>Filter</td>
<td>If the Filter is ON, this event will not be logged.</td>
</tr>
<tr>
<td>Event Priority</td>
<td>The priority that the event currently has assigned. This is the alarm priority.</td>
</tr>
<tr>
<td>Reasons</td>
<td>The reason that the event is triggered.</td>
</tr>
<tr>
<td>Reason Priority</td>
<td>The priority that the reason currently has assigned. This is the alarm priority.</td>
</tr>
</tbody>
</table>
Click on the %e %a down event (event number 5).

On the following page, configure the Alarm Priority.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Priority</td>
<td>9</td>
<td>Change the Alarm Priority to 9, this will be used later.</td>
</tr>
</tbody>
</table>

Click Apply
Repeat the process for Event 153, ‘PPP 1 up’.

Click Apply
Optional step
If required, alerts can be locked to a specific PPP interface by using the parameter **Alarm Priority** is dependent on the event being logged by Entity and configuring it as the PPP interface in use.

When all changed to the logcodes are complete, scroll up to the top of the screen, click ‘Save All Event Code Changes’ to save the changes to the logcodes.dif file.
2.2 Configuring the Event Settings

In the Event Handler, the SNMP Trap priority (Send a SNMP Trap when the alarm priority is at least) should be set to a number the same or higher than the alarm priority configured for the event in the previous steps. If the alarm priority on the Event Settings page is set to 9, then every event (or event reason) with an alarm priority of 9=> will trigger a syslog alert. i.e. 9, 10, 11, 12....

Navigate to Configuration - Alarms > Event Settings, expand the SNMP Traps section and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After power up, wait nn seconds before sending Emails, SNMP traps, SMS or Syslog messages</td>
<td>5</td>
<td>Delay in seconds, after power up, before alerts will be sent.</td>
</tr>
<tr>
<td>Send SNMP Traps</td>
<td>Checked</td>
<td>Enables SNMP trap alerting</td>
</tr>
<tr>
<td>if the alarm priority is at least nn</td>
<td>9</td>
<td>Events with an alarm priority equal or greater than this number will trigger an alert.</td>
</tr>
<tr>
<td>Send a maximum of nn SMS messages per day</td>
<td>100</td>
<td>The maximum number of alerts to send per day, this counter is reset at midnight.</td>
</tr>
</tbody>
</table>

After configuring these parameters, click Apply.

2.3 Configure SNMP

Navigate to Configuration - Remote Management > SNMP
The SNMP modes that are shown are only applicable to inbound SNMP management & monitoring access to the router, these have no effect on SNMP trap alerts.

SNMP users & SNMP filters are also used for inbound SNMP management & monitoring access to the router, these have no effect on SNMP trap alerts.

Navigate to Configuration - Remote Management > SNMP > SNMP Traps
Enable all the trap generation types that are required.

Navigate to Configuration - Remote Management > SNMP > SNMP Traps > SNMP Trap Server 0
This configuration must match the settings on the SNMP Trap receiver/management server.

Configure the trap server IP address, this is the IP address of the SNMP trap receiver. The default destination port number for sending SNMP traps is 162, if the receiver is listening on a different port number, change this to match.
The SNMP version number must match what is in use on the SNMP trap receiver.
Configure the community string to match the SNMP trap receiver community. If SNMPv3 is required, also configure the authentication and encryption options.

If the SNMP trap receiver/management server expects to receive Inform Requests instead of SNMP traps, the option 'Send "Inform Request" message' should be enabled. Since Inform Requests are expected to be
acknowledged by the receiver, enabling this option on the router but not on the receiver will cause multiple alerts to be sent for each event because the router is expecting an acknowledgement.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate Enterprise traps</td>
<td>Checked</td>
<td>Enables event generated SNMP traps</td>
</tr>
<tr>
<td>Generate Generic traps</td>
<td>Not checked</td>
<td>Disables these traps</td>
</tr>
<tr>
<td>Generate Authentication Failure traps</td>
<td>Not checked</td>
<td>Disables these traps</td>
</tr>
<tr>
<td>Generate VRRP traps</td>
<td>Not checked</td>
<td>Disables these traps</td>
</tr>
<tr>
<td>Trap Server IP Address</td>
<td>IP address of Trap receiver</td>
<td>The IP address of the SNMP Trap receiver, this is where the traps will be sent to.</td>
</tr>
<tr>
<td>Port</td>
<td>162</td>
<td>The port number the trap receiver is listening on</td>
</tr>
<tr>
<td>Use interface</td>
<td>Ethernet 0</td>
<td>The source IP address to use for SNMP traps</td>
</tr>
<tr>
<td>Use SNMP Version</td>
<td>v2c</td>
<td>The SNMP protocol version enabled on the trap receiver</td>
</tr>
<tr>
<td>Community / Confirm Community</td>
<td>netman</td>
<td>The SNMP community name</td>
</tr>
</tbody>
</table>

After configuring these parameters, click Apply.
3 SNMP TRAP RECEIVER SOFTWARE

There are plenty of SNMP network monitoring and management applications that are capable of receiving traps and performing actions based on traps received. The software used in this application note is ManageEngine MIB Browser 5. This software has a bundled SNMP Trap receiver.

Run the SNMP trap receiver software (MIB Browser 5 shown), ensure the correct community is configured, it is listening on port 162 and if there is a firewall configured on the PC make sure it is allowing inbound UDP 162 traffic.

4 TESTING

To test that the Digi TransPort is configured correctly, the PPP interface should be deactivated and allowed to reconnect.

Navigate to Management - Connections > PPP Connections > PPP 1 and click on Drop Link. Note that the connection to the internet will disconnect for a few seconds.
When the PPP link is dropped, this will create an event in the event log and an SNMP Trap will also be triggered. When the PPP link comes back up, another SNMP Trap will be sent. This shows the SNMP Trap on the SNMP Trap receiver, including the time stamp, the source IP address of the alert and the SNMP message.

Clicking the ‘Show Details’ button gives more information and lists the reason for the SNMP trap.

The events in Management - Event Log will look similar to this, the 2 events that triggered the syslog alert are shown in red for clarification, colouring of text in the actual event log does not happen.

15:36:40, 15 Mar 2013, PPP 1 Available, Activation
15:36:40, 15 Mar 2013, PPP 1 up
15:36:37, 15 Mar 2013, iDigi disconnected
15:36:37, 15 Mar 2013, iDigi reconnect timer expired
15:36:36, 15 Mar 2013, PPP 1 Start IPCP
15:36:36, 15 Mar 2013, PPP 1 Start AUTHENTICATE
15:36:36, 15 Mar 2013, PPP 1 Start LCP
15:36:36, 15 Mar 2013, PPP 1 Start
15:36:36, 15 Mar 2013, Modem connected on asy 4
15:36:35, 15 Mar 2013, Modem dialing on asy 4 #:*98*1#
15:36:32, 15 Mar 2013, Modem disconnected on asy 4, Normal Breakdown
15:36:30, 15 Mar 2013, Default Route 0 Out Of Service, Activation
15:36:30, 15 Mar 2013, PPP 1 Out Of Service, Activation
15:36:30, 15 Mar 2013, PPP 1 down, CLI request

The number of SNMP traps sent by the router since midnight can be checked by navigating to Configuration - Alarms > Event Settings, the number of messages sent is shown in the SNMP Traps section. This is the total number of alerts sent by all configured SNMP Trap server instances.
5 CONFIGURATION FILES

5.1 Digi TransPort Configuration Files

This is the relevant parts of the config.da0 file:

```
ss237424>config c show
eth 0 IPaddr "10.1.51.21"
eth 0 mask "255.255.0.0"
eth 0 gateway "10.1.2.100"
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
snmp 0 v1enable OFF
snmp 0 v2cenable OFF
snmp 0 v3enable OFF
snmp 0 name "BG WR21"
snmp 0 contact "Ben"
snmp 0 location "Bens desk"
snmp 0 vrrptraps OFF
snmp 0 tacacs_auth OFF
snmptrap 0 IPaddr "10.1.51.1"
snmptrap 0 version "v2c"
snmptrap 0 community "netman"
snmptrap 0 ipent "ETH"
snmptrap 0 ipadd "0"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 username "bt"
ppp 1 epassword "Ois=
ppp 1 IPaddr "0.0.0.0"
ppp 1 ans ON
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 1
ppp 3 defpak 16
modemcc 0 asy_add 4
modemcc 0 info_asy_add 2
modemcc 0 init_str "+CGQREQ=1"
```
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "btmobile.bt.com"
modemcc 0 link_retries 11
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_cmd_sep "%"
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
CMD 0 unitid "ss%s>
CMD 0 cmdnua "99"
CMD 0 hostname "digi.router"
CMD 0 asyled_mode 2
CMD 0 ent_name "sarian"
CMD 0 tremto 1200
USER 0 access 0
USER 1 name "username"
USER 1 epassword "KD51SVJDVVg="
USER 1 access 0
USER 2 access 0
USER 3 access 0
USER 4 access 0
USER 5 access 0
USER 6 access 0
USER 7 access 0
USER 8 access 0
USER 9 access 0
LOCAL 0 transaccess 2
EVENT 0 trap_max 100
EVENT 0 trap_trig 9
EVENT 0 action_dly 5
SSH 0 hostkey1 "privSSH.pem"
SSH 0 nb_listen 5
SSH 0 v1 OFF

OK

This is the contents of the logcodes.dif file, manual configuration of the logcodes.dif is outside the scope of this application note, if further instruction is required please contact tech.support@digi.com:

E5,9,
E153,9,

5.2 Digi TransPort Firmware Versions

This is the firmware \ hardware information from the unit:
Digi TransPort WR21-U82B-DE1-XX Ser#:237424
Software Build Ver5169. Feb 27 2013 02:47:07 WW
ARM Bios Ver 6.91u v43 454MHz B987-M995-F80-08001_0 MAC:00042d039f70
Async Driver Revision: 1.19 Int clk
Ethernet Hub Driver Revision: 1.11
Firewall Revision: 1.0
EventEdit Revision: 1.0
Timer Module Revision: 1.1
(B)USBHOST Revision: 1.0
L2TP Revision: 1.10
PPTP Revision: 1.00
TACPLUS Revision: 1.00
MODBUS Revision: 0.00
RealPort Revision: 0.00
<table>
<thead>
<tr>
<th>Component</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>MultiTX</td>
<td>1.00</td>
</tr>
<tr>
<td>LAPB</td>
<td>1.12</td>
</tr>
<tr>
<td>X25 Layer</td>
<td>1.19</td>
</tr>
<tr>
<td>MACRO</td>
<td>1.0</td>
</tr>
<tr>
<td>PAD</td>
<td>1.4</td>
</tr>
<tr>
<td>X25 Switch</td>
<td>1.7</td>
</tr>
<tr>
<td>TPAD Interface</td>
<td>1.12</td>
</tr>
<tr>
<td>GPS</td>
<td>1.0</td>
</tr>
<tr>
<td>SCRIBATSK</td>
<td>1.0</td>
</tr>
<tr>
<td>BASTSK</td>
<td>1.0</td>
</tr>
<tr>
<td>PYTHON</td>
<td>1.0</td>
</tr>
<tr>
<td>IDIGISMS</td>
<td>1.0</td>
</tr>
<tr>
<td>TCP</td>
<td>1.14</td>
</tr>
<tr>
<td>TCP Util</td>
<td>1.13</td>
</tr>
<tr>
<td>PPP</td>
<td>1.19</td>
</tr>
<tr>
<td>WEB</td>
<td>1.5</td>
</tr>
<tr>
<td>SMTP</td>
<td>1.1</td>
</tr>
<tr>
<td>FTP Client</td>
<td>1.5</td>
</tr>
<tr>
<td>FTP</td>
<td>1.4</td>
</tr>
<tr>
<td>IKE</td>
<td>1.0</td>
</tr>
<tr>
<td>PollANS</td>
<td>1.2</td>
</tr>
<tr>
<td>PFPoE</td>
<td>1.0</td>
</tr>
<tr>
<td>BRIDGE</td>
<td>1.1</td>
</tr>
<tr>
<td>MODEM CC (GOBI UMTS)</td>
<td>1.4</td>
</tr>
<tr>
<td>FLASH Write</td>
<td>1.2</td>
</tr>
<tr>
<td>Command Interpreter</td>
<td>1.38</td>
</tr>
<tr>
<td>SSLCLI</td>
<td>1.0</td>
</tr>
<tr>
<td>OSPPF</td>
<td>1.0</td>
</tr>
<tr>
<td>BGP</td>
<td>1.0</td>
</tr>
<tr>
<td>QOS</td>
<td>1.0</td>
</tr>
<tr>
<td>PWRCTRL</td>
<td>1.0</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>1.0</td>
</tr>
<tr>
<td>SSH Server</td>
<td>1.0</td>
</tr>
<tr>
<td>SCP</td>
<td>1.0</td>
</tr>
<tr>
<td>CERT</td>
<td>1.0</td>
</tr>
<tr>
<td>LowPrio</td>
<td>1.0</td>
</tr>
<tr>
<td>Tunnel</td>
<td>1.2</td>
</tr>
<tr>
<td>OVPN</td>
<td>1.2</td>
</tr>
<tr>
<td>QDL</td>
<td>1.0</td>
</tr>
<tr>
<td>WiMax</td>
<td>1.0</td>
</tr>
<tr>
<td>iDigi</td>
<td>2.0</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>