Quick Note 34

Configuring Syslog alerting on a TransPort

Digi Technical Support

September 2016

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 9

2.3 Configuring Syslog server 0 10

3 Syslog server software 12

4 Testing 13

5 Configuration Files 15

5.1 TransPort Configuration Files 15

5.2 TransPort Firmware Versions 17

1 INTRODUCTION

1.1 Outline

This document contains information regarding the configuration and use of syslog alerting.

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 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 Quick Note (QN) applies to:

Models shown: Digi TransPort WR21.

Other Compatible Models: All Digi TransPort products.

Firmware versions: 5.146 or newer.

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

1.3 Corrections

Requests for corrections or amendments to this QN are welcome and should be addressed to: tech.support@digi.com

Requests for new QNs can be sent to the same address.

1.4 Version & Revision History

Version Number	Status
0.1	Published
0.2	Updated screenshots for new web interface, rebranding (Sept 2016)

2 CONFIGURATION

2.1 Configuring the Event Logcodes

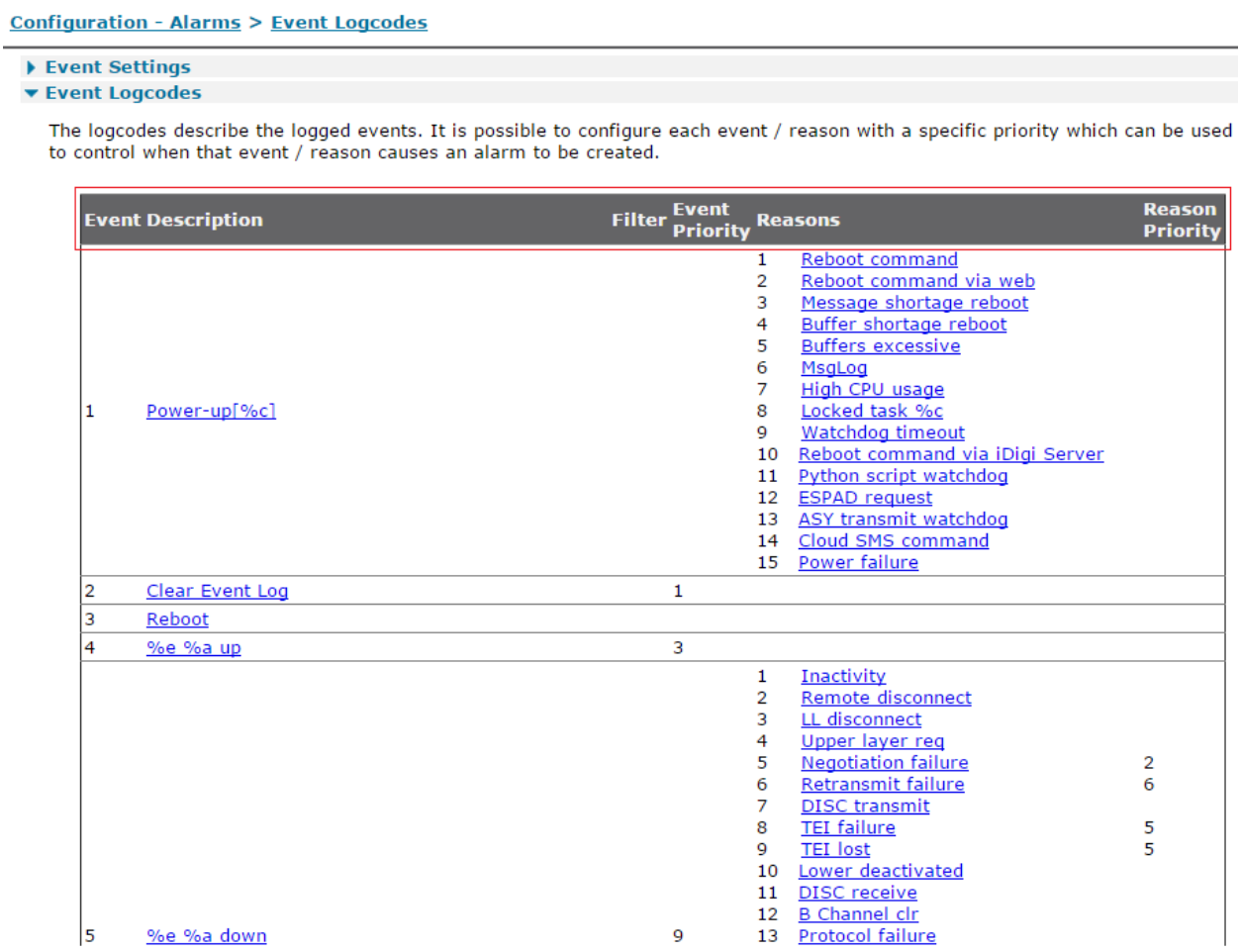
First it is necessary to choose which events should trigger the syslog alerts.

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.dao or logcodes.txt files, but are stored in the logcodes.dif file once the changes have been saved.

In order to send a syslog 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 a syslog alert when PPP 1 is down and Event 153 "PPP 1 up" will be used to trigger a syslog alert when PPP 1 is up.

Navigate to: **Configuration - Alarms > Event Logcodes**

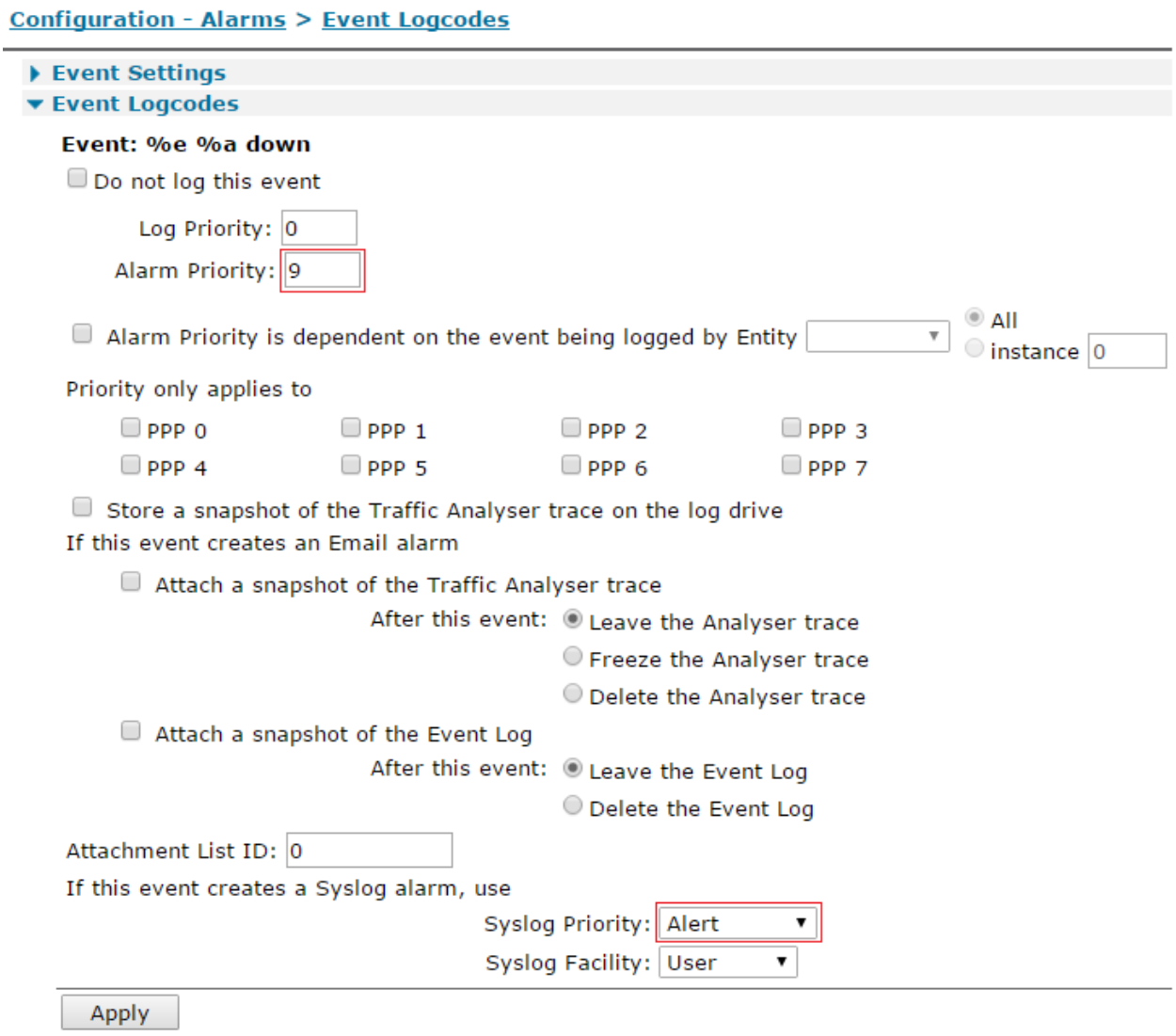


The following table describes the meaning of each column:

Parameter	Description
Event	A numerical value that represents the event
Description	The main description of the event
Filter	If the Filter is ON, this event will not be logged
Event Priority	The priority that the event currently has assigned. This is the alarm priority.
Reasons	The reason that the event is triggered
Reason Priority	The priority that the reason currently has assigned. This is the alarm priority

Click on the **%e %a down** event (Event number 5):

On the following page, configure the Alarm Priority and Syslog Priority. The Syslog Priority and Facility can be used to send different types of alerts to different Syslog servers based on priority and facility. This QN will only be sending alerts to one server, so the Syslog Priority is changed only for the purpose of showing the process.

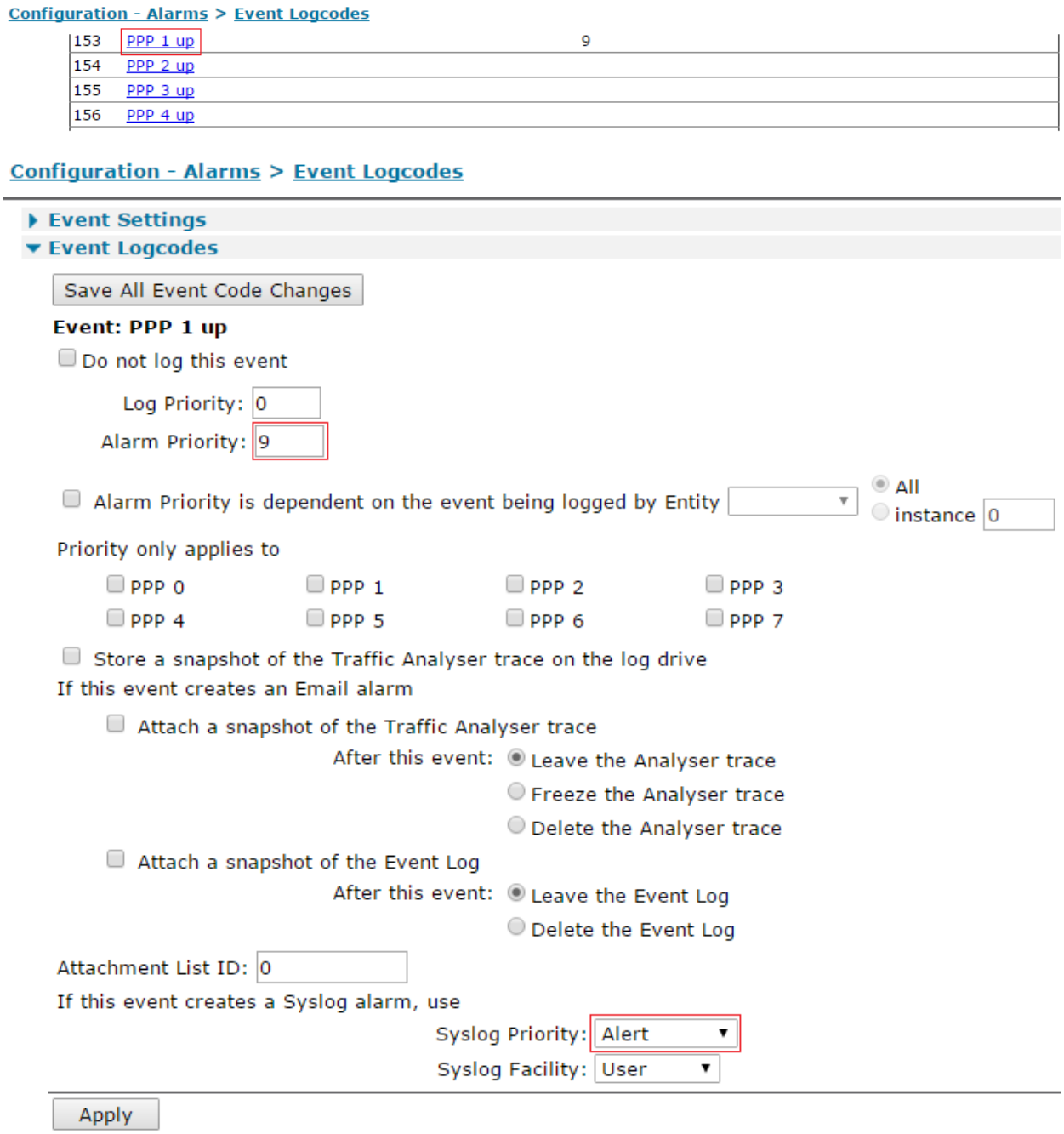


Click the **Apply** button.

NOTE: The Alarm Priority may already be defaulted to 9, depending on the TransPort firmware version.

Parameter	Setting	Description
Alarm Priority	9	Change the Alarm Priority to 9. This will be used later.
Syslog Priority	Alert	Change the Syslog Priority to Alert. This is in the info sent to the Syslog server.

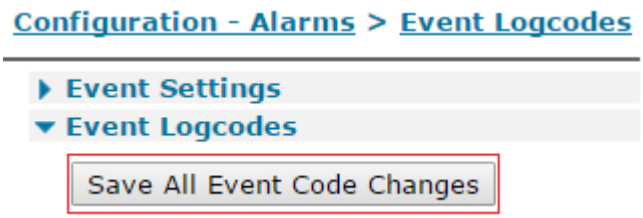
Repeat the process for Event 153, 'PPP 1 up':



Click the **Apply** button.

NOTE: The Alarm Priority may already be defaulted to 9, depending on the TransPort firmware version.

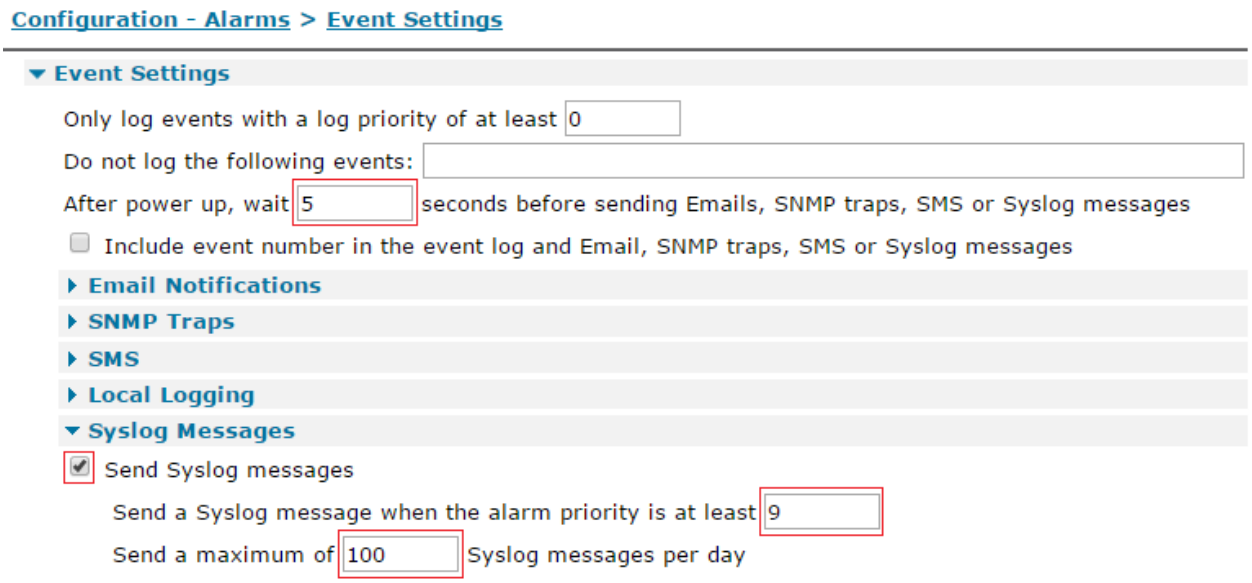
At the top of the screen, click 'Save All Event Code Changes' to save the changes to the logcodes.dif file:



2.2 Configuring the Event Settings

In the Event Handler, the syslog alarm priority (Send a Syslog message 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 Syslog Messages section and configure the following parameters:



Check the "Send Syslog messages" box to display the Syslog settings.

Parameter	Setting	Description
After power up, wait *nn* seconds before sending Emails, SNMP traps, SMS or Syslog messages	5	Delay in seconds, after power up, before alerts will be sent
Send Syslog messages	Checked	Enables syslog alerting
Send a Syslog message when the alarm priority is at least *nn*	9	Events with an alarm priority equal or greater than this number will trigger an alert
Send a maximum of *nn* Syslog messages per day	100	The maximum number of alerts to send per day. This counter is reset at midnight

After configuring these parameters, click the **Apply** button.

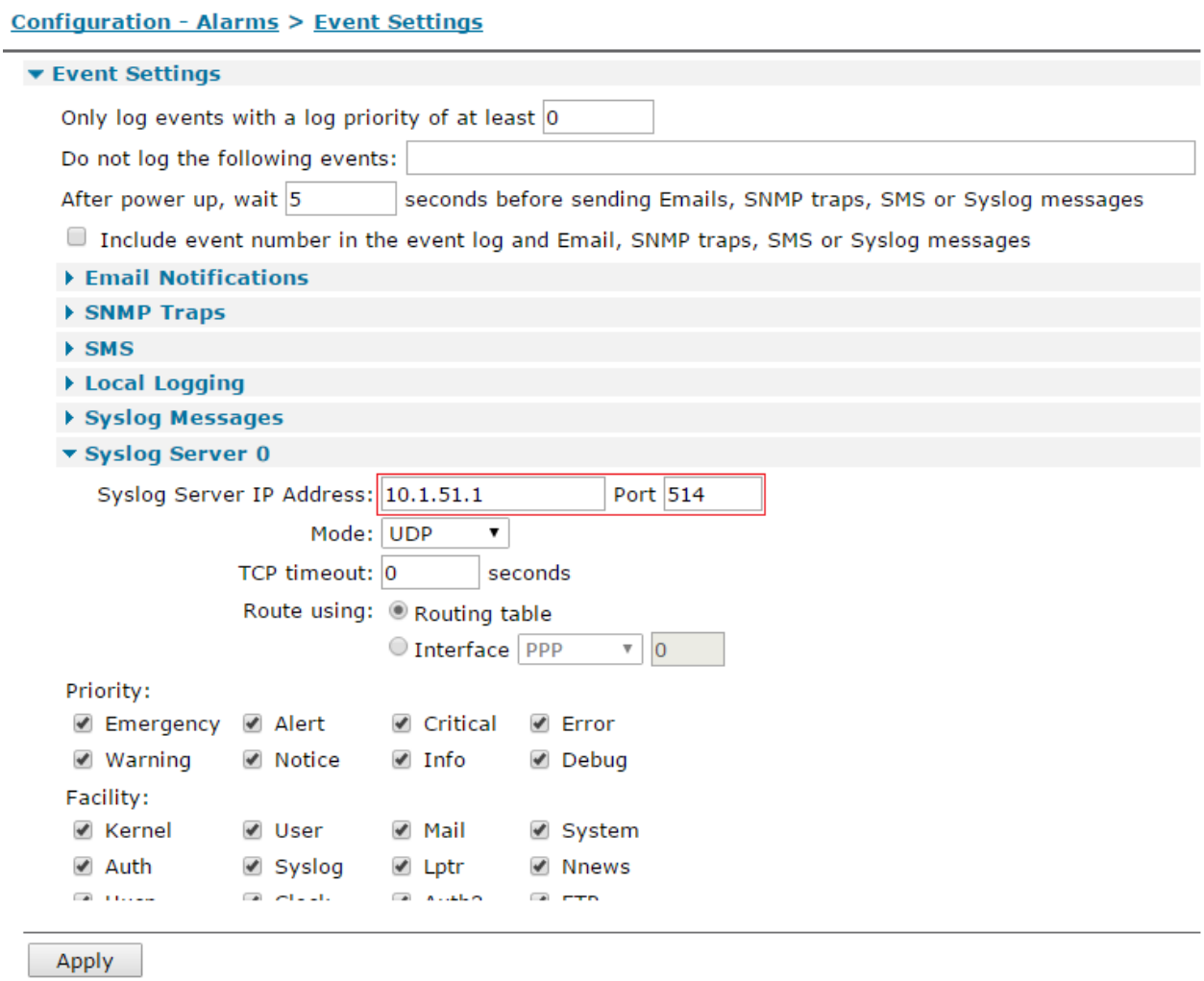
2.3 Configuring Syslog server 0

Scroll down the page a little and expand the section titled **Syslog Server 0**.

Configure the IP address of the Syslog server; this is where the alerts will be sent to. The port number for Syslog is UDP 514; this should be entered as 514 in the Port field.

Some TransPort routers also support TCP mode and RFC3195 mode; the options are not shown here.

If there were multiple Syslog servers available, it would be possible by using the tick boxes on this page to only alert the specified syslog server when the selected facilities and priorities match what was configured for the event in section 2.1. Since this QN only uses one syslog server, all boxes remain checked.



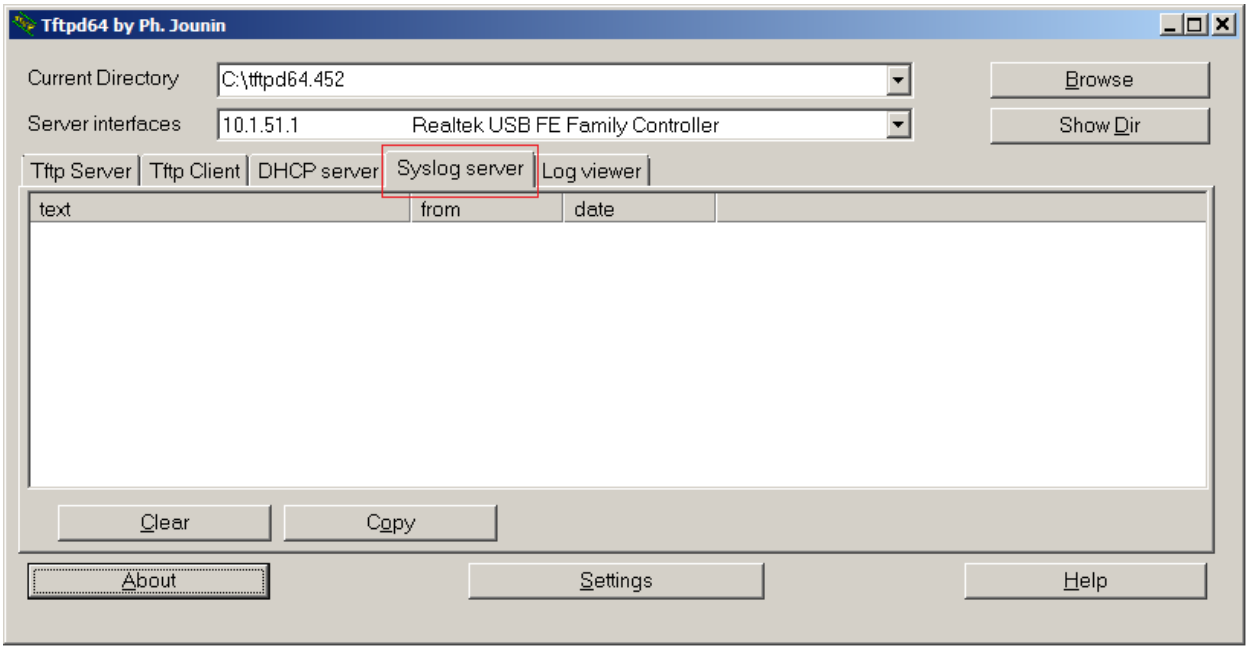
Parameter	Setting	Description
Syslog Server IP Address	10.1.51.1	The IP address of the syslog server
Port	514	The port that the syslog server is listening on

After configuring these parameters, click the **Apply** button, then **save the configuration to flash**.

3 SYSLOG SERVER SOFTWARE

There are plenty of network monitoring applications with syslog capabilities. The software used in this application note is Tftpd64 (there is also a 32 bit version called Tftpd32). This software has a bundled Syslog server.

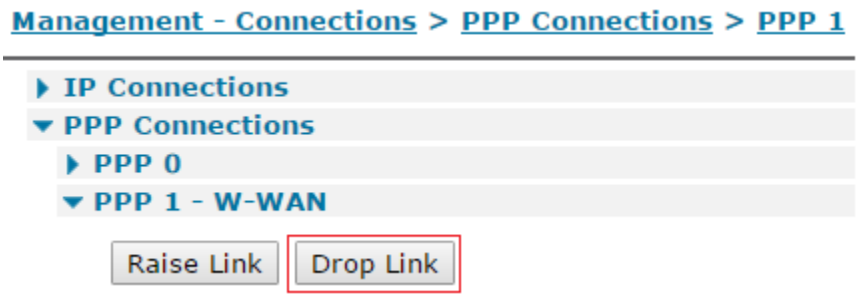
Run the syslog server software (Tftpd64 shown), ensure it is listening on port 514 and if there is a firewall configured on the PC, and make sure it is allowing inbound UDP 514 traffic.



4 TESTING

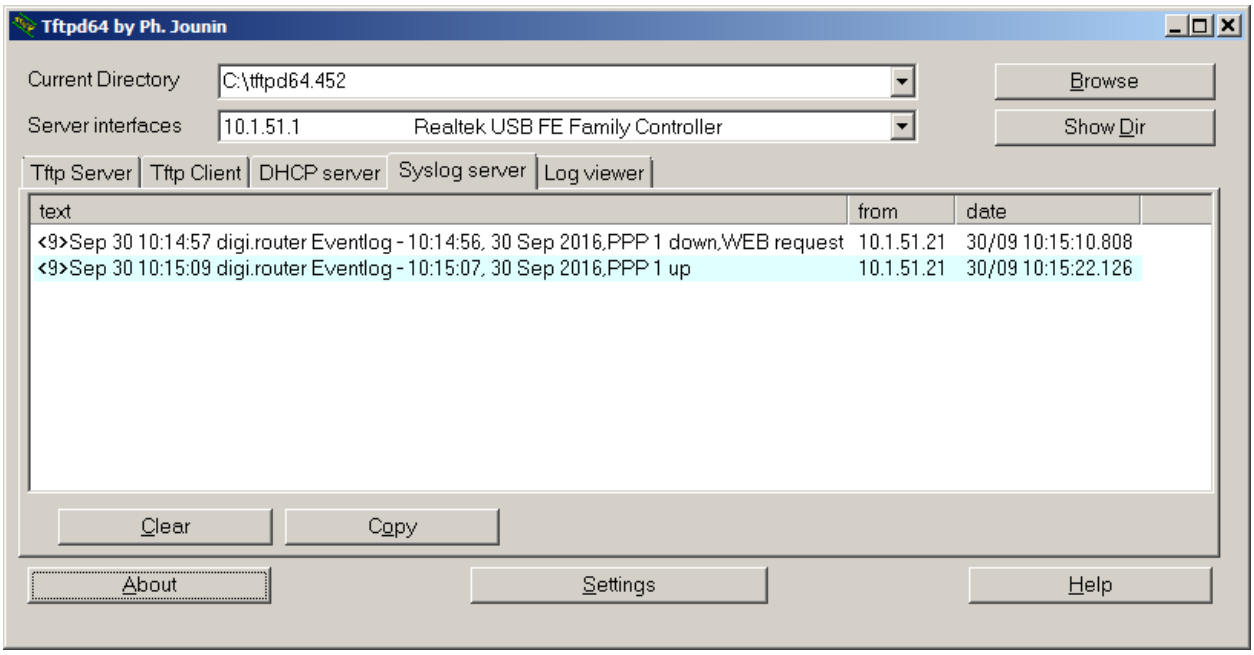
To test that the Digi TransPort is configured correctly, the PPP interface should be deactivated and allowed to reconnect.

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 a syslog alert will also be triggered. When the PPP link comes back up, another syslog alert will be sent.

This shows the syslog alerts on the syslog server, including the time stamp, the source IP address of the alert and the reason for the alert.



The events in **Management - Event Log** will look similar to below; 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.

10:15:07, 30 Sep 2016,Default Route 0 Available,Activation

10:15:07, 30 Sep 2016,PPP 1 Available,Activation

10:15:07, 30 Sep 2016,PPP 1 up

10:15:07, 30 Sep 2016,PPP 1 Start

10:15:07, 30 Sep 2016,Modem connected on asy 4

10:15:04, 30 Sep 2016,Modem dialing on asy 4 #:*98*1#

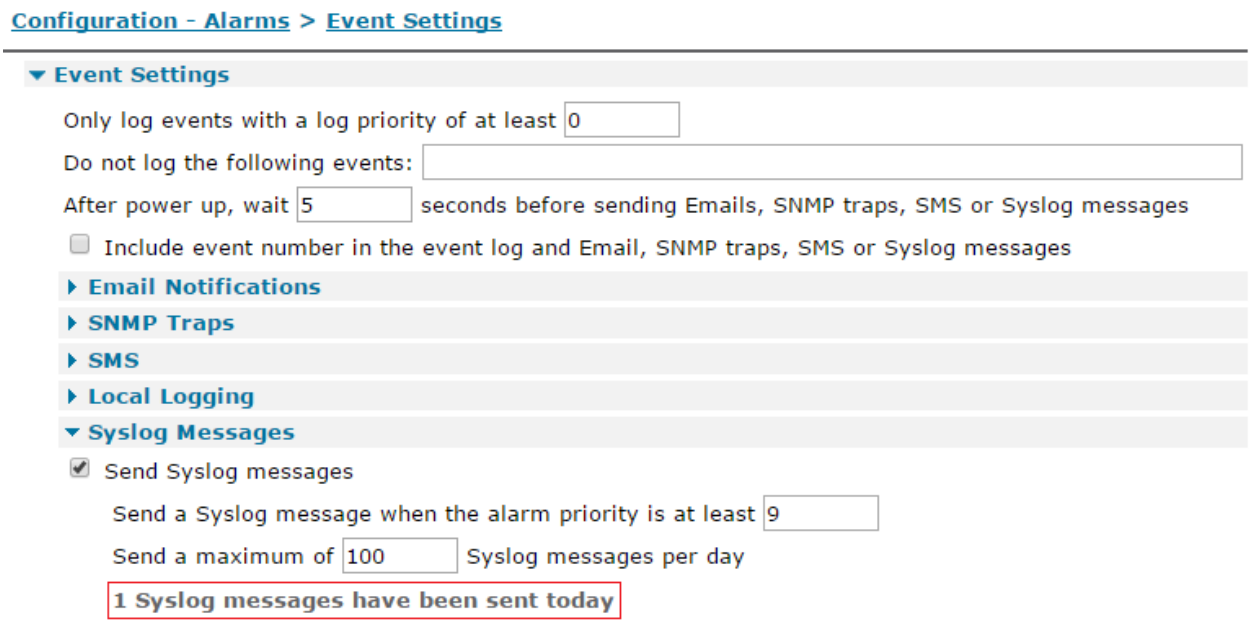
10:14:57, 30 Sep 2016,Modem disconnected on asy 4,1

10:14:56, 30 Sep 2016,Default Route 0 Out Of Service,Activation

10:14:56, 30 Sep 2016,PPP 1 Out Of Service,Activation

10:14:56, 30 Sep 2016,PPP 1 down,WEB request

The number of syslog messages 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 **Syslog Messages** section. This is the total number of alerts sent by all configured syslog instances, 0, 1, 2, 3 & 4 (if configured).



5 CONFIGURATION FILES

5.1 TransPort Configuration Files

```
Command: config c show
Command result

eth 0 IPaddr "10.1.51.21"
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
syslog 0 server "10.1.51.1"
syslog 0 port 514
syslog 0 mode "UDP"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
sntp 0 offset -8
sntp 0 dstonmon 3
sntp 0 dstonday 13
sntp 0 dstoffmon 11
sntp 0 dstoffday 6
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
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 "Your.APN.goes.here"
modemcc 0 link_retries 10
```

```
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
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
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "PDZxUxQeFB0="
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 syslog_max 100
event 0 syslog_trig 9
event 0 action_dly 5
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
templog 0 mo_autooff ON
cloud 0 ssl ON

Power Up Profile: 0
OK
```

Just below are the contents of the logcodes.dif file; manual configuration of the logcodes.dif is outside the scope of this QN.

```
E5,9 sp=1,
E153,9 sp=1,
```

If further instruction is required, please contact tech.support@digi.com

5.2 TransPort Firmware Versions

```
Command: ati5
Command result

Digi TransPort WR21-U81B-DE1-XX Ser#:xxxxxx HW Revision: 1201a
Software Build Ver5.2.15.6.  Aug 17 2016 17:42:05  WW
ARM Bios Ver 7.56u v43 454MHz B987-M995-F80-O0,0 MAC:00042d042ac6
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Ethernet Port Isolate 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
MultiTX                   Revision: 1.00
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
GPS                       Revision: 1.0
TELITUPD                  Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
CLOUDSMS                  Revision: 1.0
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 5.2
WEB                       Revision: 1.5
```

```
SMTP                        Revision: 1.1
FTP Client                  Revision: 1.5
FTP                         Revision: 1.4
IKE                         Revision: 1.0
PollANS                     Revision: 1.2
PPPOE                       Revision: 1.0
BRIDGE                      Revision: 1.1
MODEM CC (GOBI UMTS)        Revision: 5.2
FLASH Write                 Revision: 1.2
Command Interpreter         Revision: 1.38
SSLCLI                      Revision: 1.0
OSPF                        Revision: 1.0
BGP                         Revision: 1.0
QOS                         Revision: 1.0
PWRCTRL                     Revision: 1.0
RADIUS Client               Revision: 1.0
SSH Server                  Revision: 1.0
SCP                         Revision: 1.0
SSH Client                  Revision: 1.0
CERT                        Revision: 1.0
LowPrio                     Revision: 1.0
Tunnel                      Revision: 1.2
OVPN                        Revision: 1.2
TEMPLOG                     Revision: 1.0
QDL                         Revision: 1.0
OK
```