Application Note 52

Configuring Syslog alerting on a TransPort router

TransPort Support

November 2015

Contents

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 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. 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 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

Version Number	Status
1.0	Published

2 CONFIGURATION

2.1 Configuring the Event Logcodes

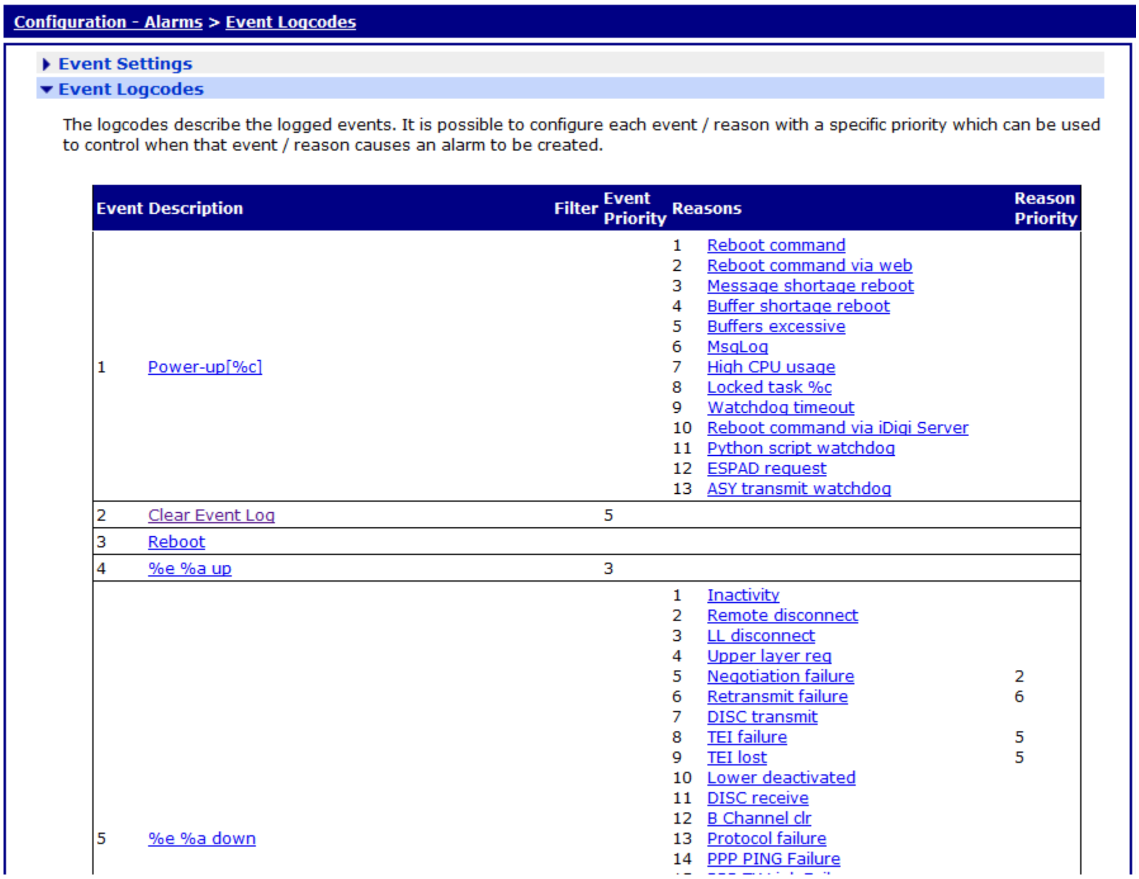
First it is necessary to choose which events should trigger the syslog alerts.

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.da0 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**



Configuration - Alarms > Event Logcodes

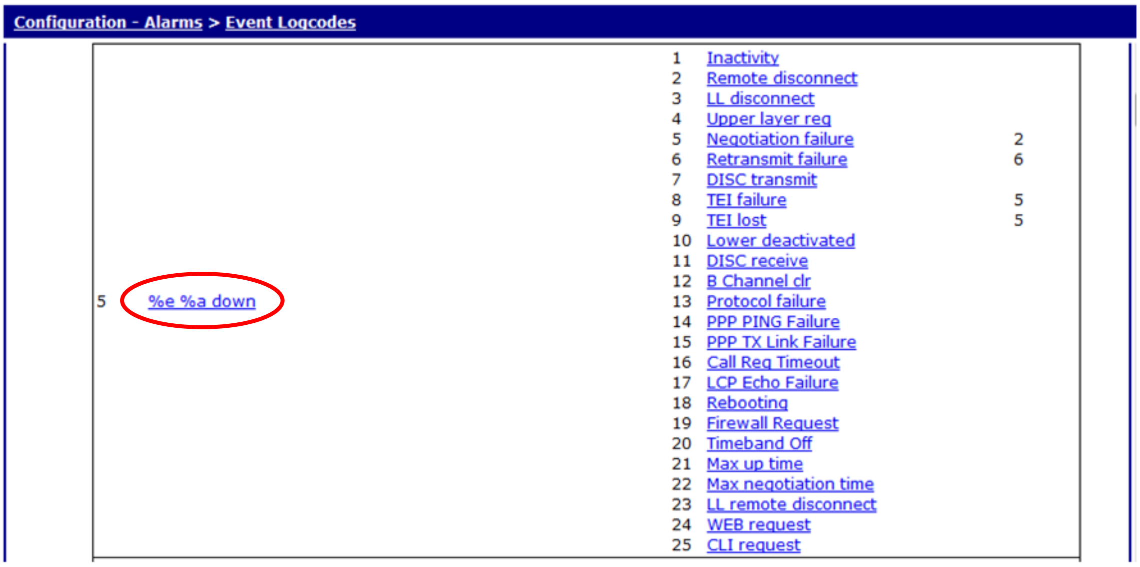
The logcodes describe the logged events. It is possible to configure each event / reason with a specific priority which can be used to control when that event / reason causes an alarm to be created.

Event Description		Filter	Event Priority	Reasons		Reason Priority
1	Power-up[%c]			1	Reboot command	
				2	Reboot command via web	
				3	Message shortage reboot	
				4	Buffer shortage reboot	
				5	Buffers excessive	
				6	MsgLog	
				7	High CPU usage	
				8	Locked task %c	
				9	Watchdog timeout	
				10	Reboot command via iDigi Server	
				11	Python script watchdog	
				12	ESPAD request	
				13	ASY transmit watchdog	
2	Clear Event Log		5			
3	Reboot					
4	%e %a up		3			
5	%e %a down			1	Inactivity	
				2	Remote disconnect	
				3	LL disconnect	
				4	Upper layer req	
				5	Negotiation failure	2
				6	Retransmit failure	6
				7	DISC transmit	
				8	TEI failure	5
				9	TEI lost	5
				10	Lower deactivated	
				11	DISC receive	
				12	B Channel clr	
				13	Protocol failure	
				14	PPP PING Failure	

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.

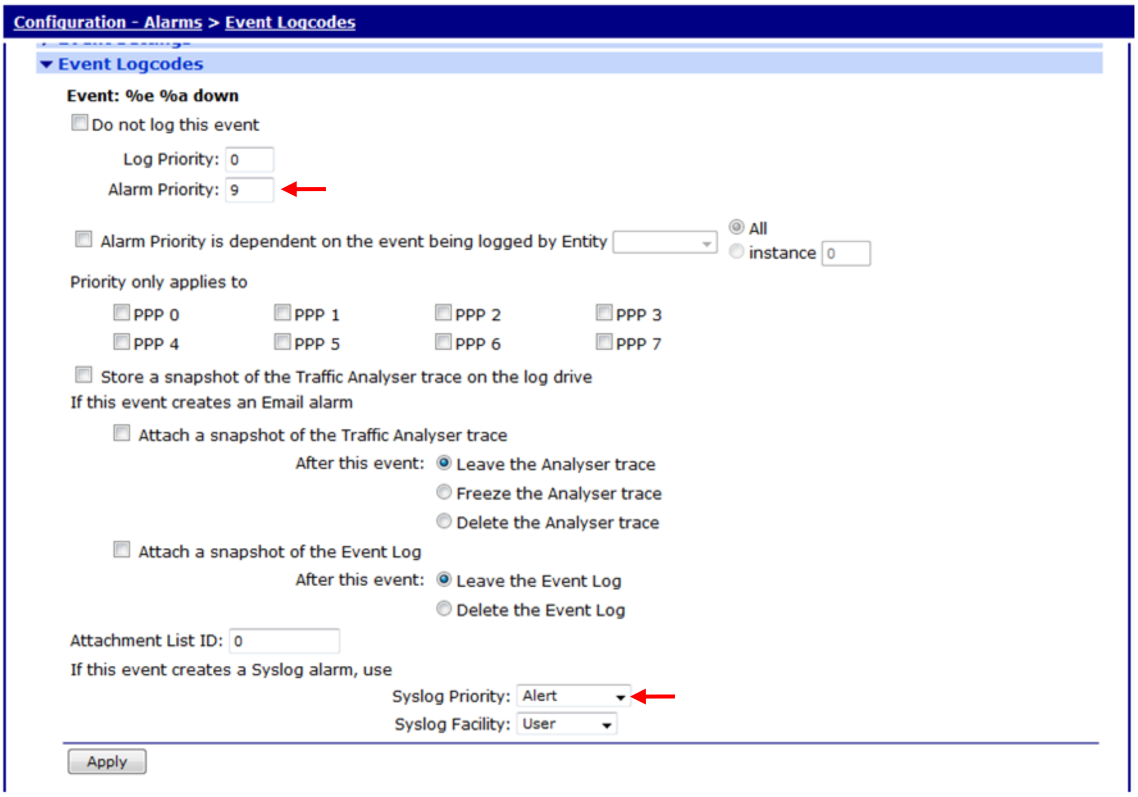
Click on the **%e %a down** event (event number 5).



Configuration - Alarms > Event Logcodes

5	%e %a down	1	Inactivity	
		2	Remote disconnect	
		3	LL disconnect	
		4	Upper layer req	
		5	Negotiation failure	2
		6	Retransmit failure	6
		7	DISC transmit	
		8	TEI failure	5
		9	TEI lost	5
		10	Lower deactivated	
		11	DISC receive	
		12	B Channel clr	
		13	Protocol failure	
		14	PPP PING Failure	
		15	PPP TX Link Failure	
		16	Call Req Timeout	
		17	LCP Echo Failure	
		18	Rebooting	
		19	Firewall Request	
		20	Timeband Off	
		21	Max up time	
		22	Max negotiation time	
		23	LL remote disconnect	
		24	WEB request	
		25	CLI request	

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 application note will only be sending alerts to one server, so the Syslog Priority is changed only for the purpose of showing the process.



Configuration - Alarms > Event Logcodes

Event Logcodes

Event: %e %a down

□ Do not log this event

Log Priority: 0

Alarm Priority: 9

□ Alarm Priority is dependent on the event being logged by Entity ● All ○ instance 0

Priority only applies to

□ PPP 0	□ PPP 1	□ PPP 2	□ PPP 3
□ PPP 4	□ PPP 5	□ PPP 6	□ PPP 7

□ Store a snapshot of the Traffic Analyser trace on the log drive

If this event creates an Email alarm

□ Attach a snapshot of the Traffic Analyser trace

After this event: ● Leave the Analyser trace ○ Freeze the Analyser trace ○ Delete the Analyser trace

□ Attach a snapshot of the Event Log

After this event: ● Leave the Event Log ○ Delete the Event Log

Attachment List ID: 0

If this event creates a Syslog alarm, use

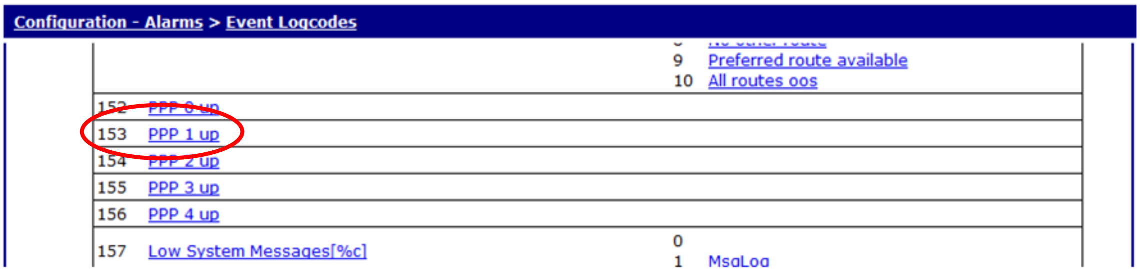
Syslog Priority: Alert

Syslog Facility: User

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

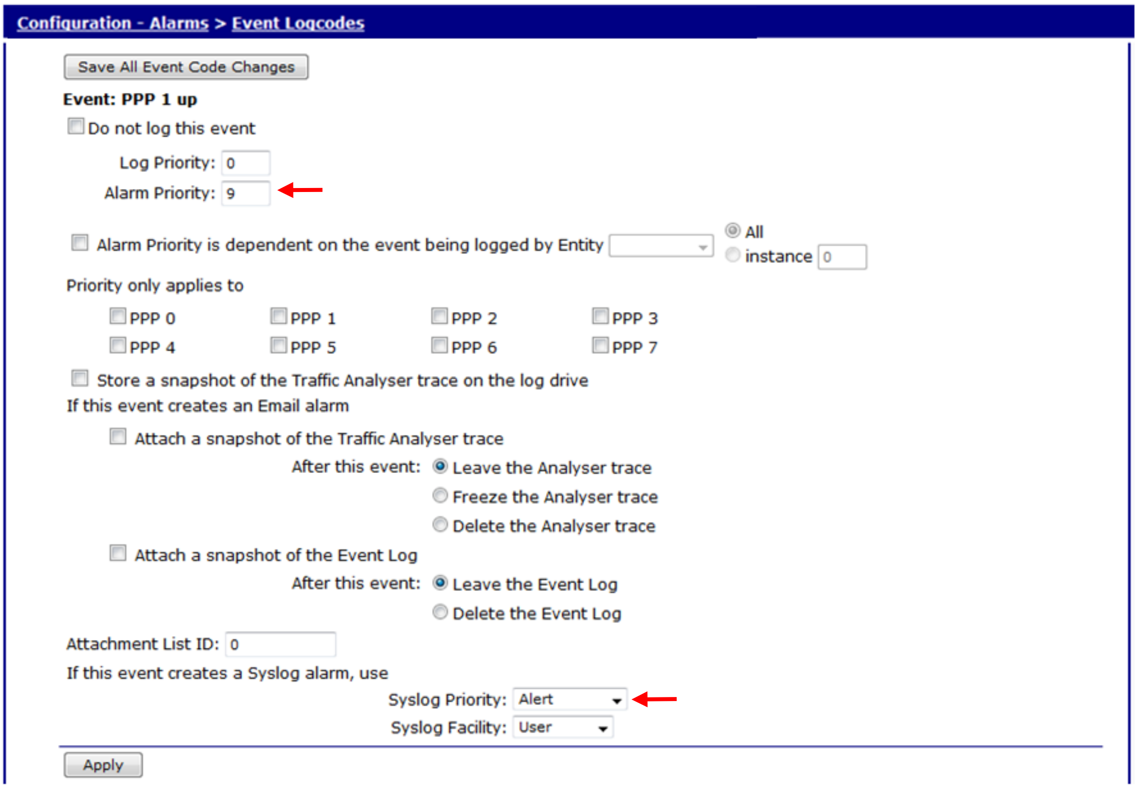
Click Apply

Repeat the process for Event 153, ‘PPP 1 up‘



Configuration - Alarms > Event Logcodes

		9 10	Preferred route available All routes oos
152	PPP 0 up		
153	PPP 1 up		
154	PPP 2 up		
155	PPP 3 up		
156	PPP 4 up		
157	Low System Messages[%c]	0 1	 MsgLog



Configuration - Alarms > Event Logcodes

Event: PPP 1 up

□ Do not log this event

Log Priority: 0

Alarm Priority: 9

□ Alarm Priority is dependent on the event being logged by Entity ● All ○ instance 0

Priority only applies to

□ PPP 0	□ PPP 1	□ PPP 2	□ PPP 3
□ PPP 4	□ PPP 5	□ PPP 6	□ PPP 7

□ Store a snapshot of the Traffic Analyser trace on the log drive

If this event creates an Email alarm

□ Attach a snapshot of the Traffic Analyser trace

After this event: ● Leave the Analyser trace ○ Freeze the Analyser trace ○ Delete the Analyser trace

□ Attach a snapshot of the Event Log

After this event: ● Leave the Event Log ○ Delete the Event Log

Attachment List ID: 0

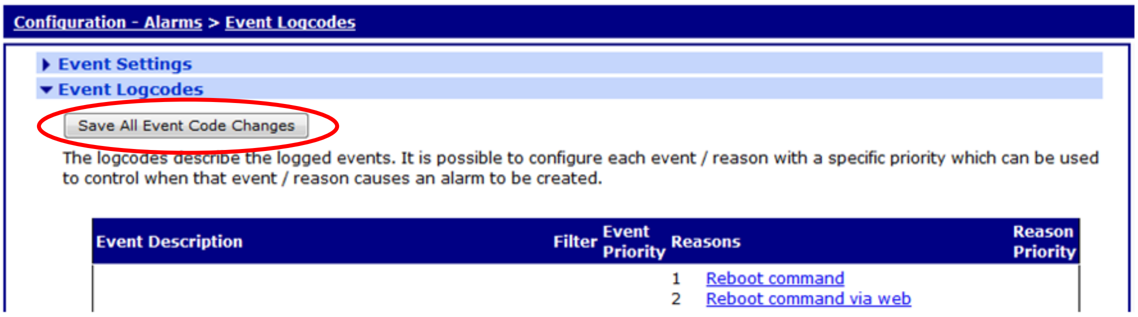
If this event creates a Syslog alarm, use

Syslog Priority: Alert

Syslog Facility: User

Click Apply

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



Configuration - Alarms > Event Logcodes

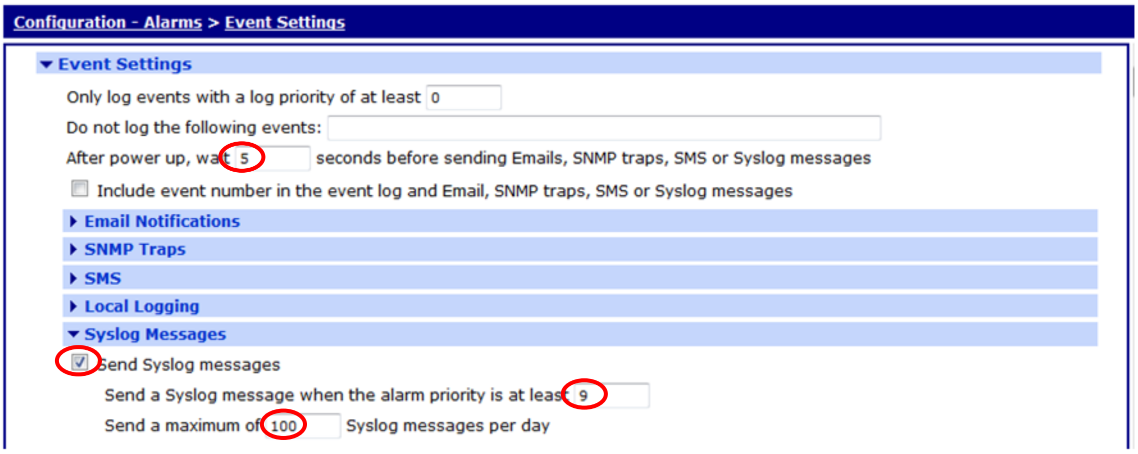
The logcodes describe the logged events. It is possible to configure each event / reason with a specific priority which can be used to control when that event / reason causes an alarm to be created.

Event Description	Filter	Event Priority	Reasons	Reason Priority
		1	Reboot command	
		2	Reboot command via web	

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:



Configuration - Alarms > Event Settings

▼ Event Settings

Only log events with a log priority of at least 0

Do not log the following events:

After power up, wait 5 seconds before sending Emails, SNMP traps, SMS or Syslog messages

□ Include event number in the event log and Email, SNMP traps, SMS or Syslog messages

▶ Email Notifications

▶ SNMP Traps

▶ SMS

▶ Local Logging

▼ Syslog Messages

☑ Send Syslog messages

Send a Syslog message when the alarm priority is at least 9

Send a maximum of 100 Syslog messages per day

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 Apply.

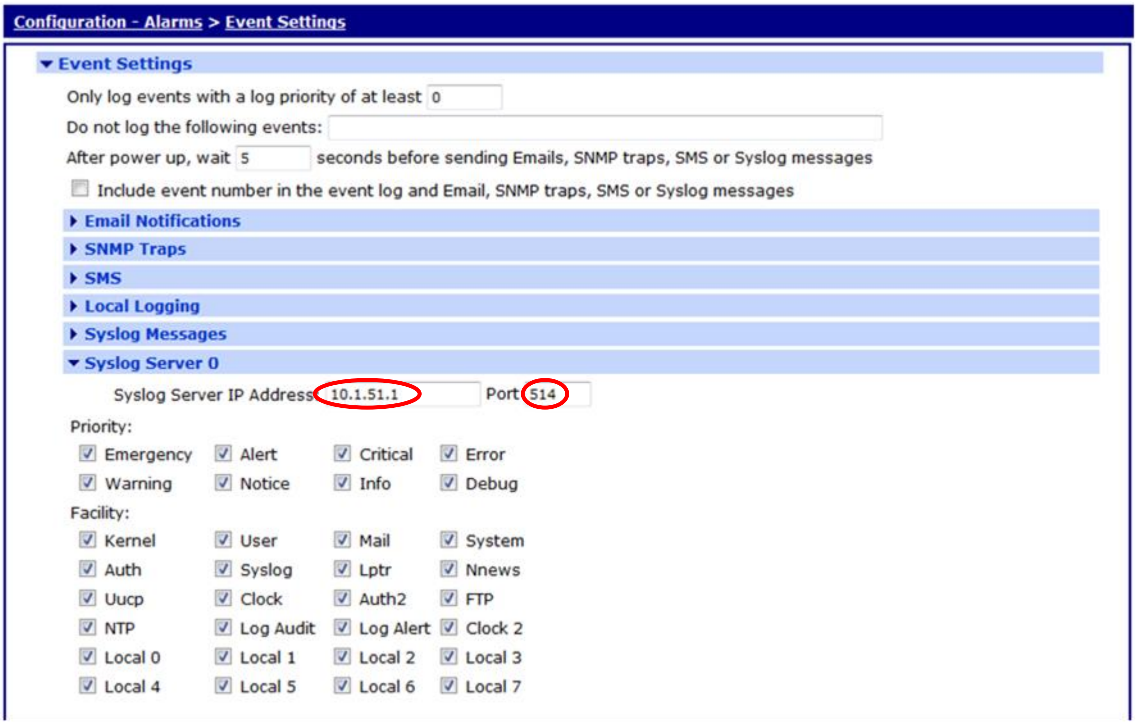
2.3 Configure Syslog server 0

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 application note only uses one syslog server, all boxes remain checked.



Configuration - Alarms > Event Settings

▾ Event Settings

Only log events with a log priority of at least 0

Do not log the following events:

After power up, wait 5 seconds before sending Emails, SNMP traps, SMS or Syslog messages

□ Include event number in the event log and Email, SNMP traps, SMS or Syslog messages

▸ Email Notifications

▸ SNMP Traps

▸ SMS

▸ Local Logging

▸ Syslog Messages

▾ Syslog Server 0

Syslog Server IP Address 10.1.51.1 Port 514

Priority:

☑ Emergency ☑ Alert ☑ Critical ☑ Error
☑ Warning ☑ Notice ☑ Info ☑ Debug

Facility:

☑ Kernel ☑ User ☑ Mail ☑ System
☑ Auth ☑ Syslog ☑ Lptr ☑ Nnews
☑ Uucp ☑ Clock ☑ Auth2 ☑ FTP
☑ NTP ☑ Log Audit ☑ Log Alert ☑ Clock 2
☑ Local 0 ☑ Local 1 ☑ Local 2 ☑ Local 3
☑ Local 4 ☑ Local 5 ☑ Local 6 ☑ Local 7

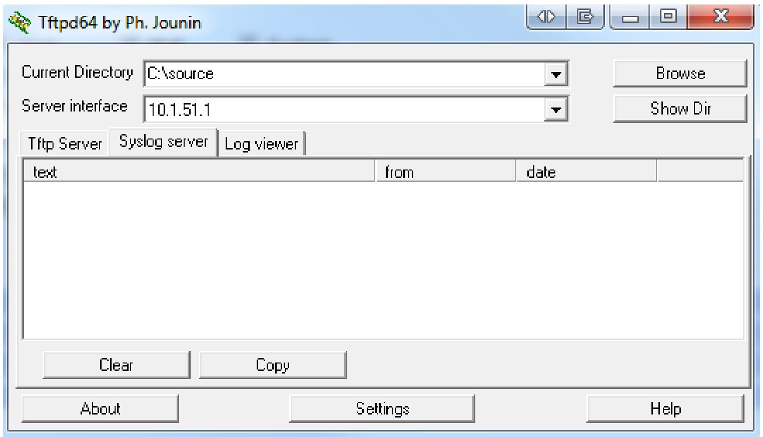
Parameter	Setting	Description
Syslog Server IP Address	10.1.51.1	The IP address of the syslog server.
Port	514	The port that the syslog server is listening on.

After configuring these parameters, click Apply, 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 make sure it is allowing inbound UDP 514 traffic.



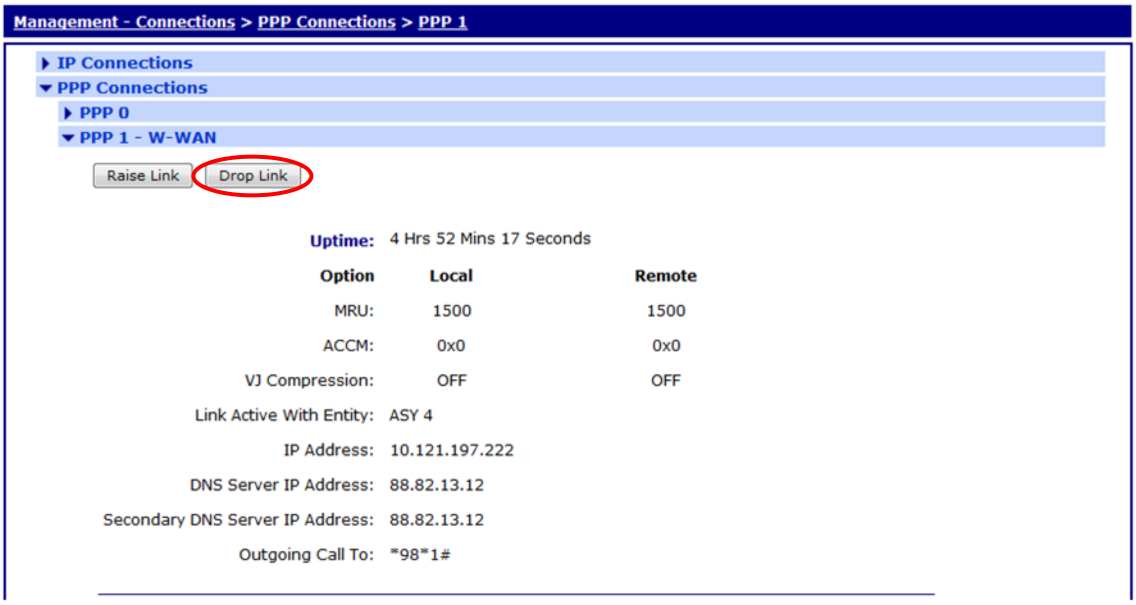
Current Directory: C:\source

Server interface: 10.1.51.1

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.



Uptime: 4 Hrs 52 Mins 17 Seconds

Option	Local	Remote
MRU:	1500	1500
ACCM:	0x0	0x0
VJ Compression:	OFF	OFF

Link Active With Entity: ASY 4

IP Address: 10.121.197.222

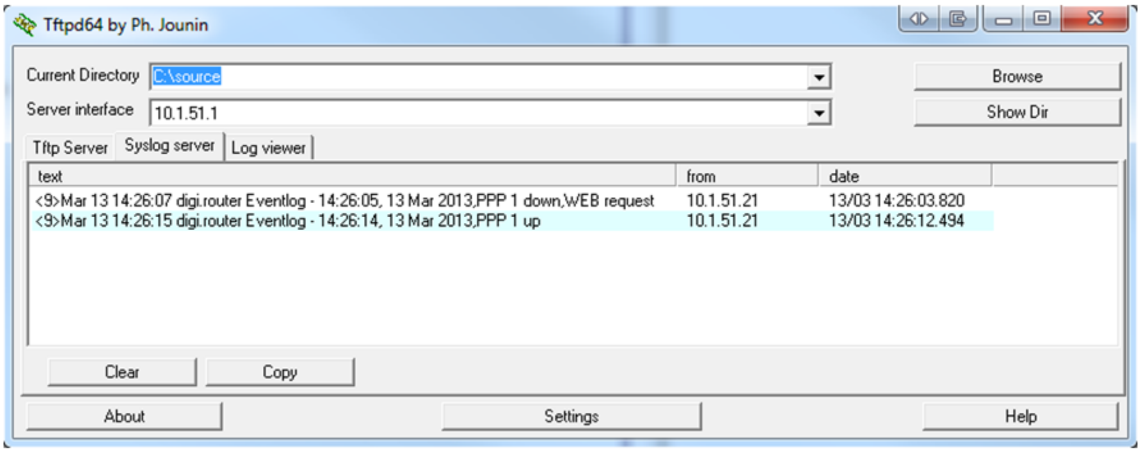
DNS Server IP Address: 88.82.13.12

Secondary DNS Server IP Address: 88.82.13.12

Outgoing Call To: *98*1#

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.



Current Directory: C:\source

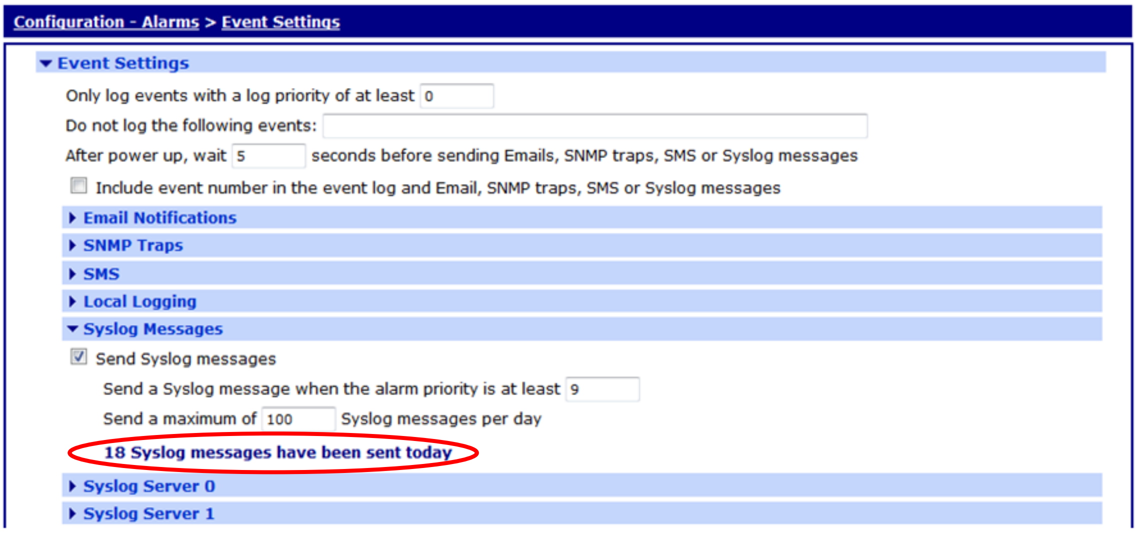
Server interface: 10.1.51.1

text	from	date
<9>Mar 13 14:26:07 digi.router Eventlog - 14:26:05, 13 Mar 2013,PPP 1 down,WEB request	10.1.51.21	13/03 14:26:03.820
<9>Mar 13 14:26:15 digi.router Eventlog - 14:26:14, 13 Mar 2013,PPP 1 up	10.1.51.21	13/03 14:26:12.494

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.

```
14:26:14, 13 Mar 2013,Default Route 0 Available,Activation
14:26:14, 13 Mar 2013,PPP 1 Available,Activation
14:26:14, 13 Mar 2013,PPP 1 up
14:26:11, 13 Mar 2013,PPP 1 Start IPCP
14:26:11, 13 Mar 2013,PPP 1 Start AUTHENTICATE
14:26:11, 13 Mar 2013,PPP 1 Start LCP
14:26:11, 13 Mar 2013,PPP 1 Start
14:26:11, 13 Mar 2013,Modem connected on asy 4
14:26:11, 13 Mar 2013,Modem dialing on asy 4 #:*98*1#
14:26:08, 13 Mar 2013,Modem disconnected on asy 4,Normal Breakdown
14:26:06, 13 Mar 2013,Default Route 0 Out Of Service,Activation
14:26:06, 13 Mar 2013,PPP 1 Out Of Service,Activation
14:26:05, 13 Mar 2013,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).



Configuration - Alarms > Event Settings

▼ Event Settings

Only log events with a log priority of at least 0

Do not log the following events:

After power up, wait 5 seconds before sending Emails, SNMP traps, SMS or Syslog messages

□ Include event number in the event log and Email, SNMP traps, SMS or Syslog messages

▶ Email Notifications

▶ SNMP Traps

▶ SMS

▶ Local Logging

▼ Syslog Messages

☑ Send Syslog messages

Send a Syslog message when the alarm priority is at least 9

Send a maximum of 100 Syslog messages per day

18 Syslog messages have been sent today

▶ Syslog Server 0

▶ Syslog Server 1

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
syslog 0 server "10.1.51.1"
syslog 0 port 514
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 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 16
ppp 4 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 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 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
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 "KD5lSVJDVVg="
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
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF

Power Up Profile: 0
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 sp=1,
E153,9 sp=1,
```

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-O8001,0 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
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
TPAD Interface            Revision: 1.12
GPS                       Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
IDIGISMS                  Revision: 1.0
TCP                       Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.19
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: 1.4
```

```
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
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
OVPN                      Revision: 1.2
QDL                       Revision: 1.0
WiMax                     Revision: 1.0
iDigi                     Revision: 2.0
OK
```