Application Note 71

Cellular WAN failover to Ethernet with firewall monitoring

January 16
# Contents

1. Introduction ............................................................................................................. 4
   1.1 Outline .............................................................................................................. 4
   1.2 Assumptions ....................................................................................................... 4
   1.3 Corrections .......................................................................................................... 4
   1.4 Version ................................................................................................................ 4

2. Scenario .................................................................................................................... 5

3. Digi TransPort router configuration ........................................................................ 6
   3.1 LAN Settings ...................................................................................................... 6
   3.2 WAN Settings ..................................................................................................... 7
      3.2.1 Mobile settings .......................................................................................... 7
      3.2.2 PPP 1 Settings ......................................................................................... 8
   3.3 ETH 1 Backup WAN settings ............................................................................ 9
   3.4 Primary Default route 0 .................................................................................. 10
   3.5 Backup Default route 1 ................................................................................... 11
   3.6 Firewall settings ............................................................................................... 12
      3.6.1 Enabling the firewall on the WAN interfaces ........................................... 13

4. Testing ..................................................................................................................... 15
   4.1 Debug settings on TransPort ......................................................................... 15
   4.2 Testing the Cellular to Ethernet Failover ....................................................... 17
      4.2.1 Simulating the fault on PPP connection on the transport ...................... 17

5. Configuration file .................................................................................................... 25
   5.1 TransPort Firmware & Hardware .................................................................... 25
   5.2 TransPort Configuration File ........................................................................... 26
   5.3 Firewall rules .................................................................................................... 29
### Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1-1</td>
<td>LAN settings</td>
</tr>
<tr>
<td>3.2.1-1</td>
<td>Primary WAN settings - Mobile</td>
</tr>
<tr>
<td>3.2.2-2</td>
<td>Primary WAN settings – PPP1</td>
</tr>
<tr>
<td>3.3-1</td>
<td>Backup WAN settings</td>
</tr>
<tr>
<td>3.4-1</td>
<td>Primary route settings</td>
</tr>
<tr>
<td>3.5-1</td>
<td>Backup route settings</td>
</tr>
<tr>
<td>3.6-1</td>
<td>Firewall settings – PassAll rule</td>
</tr>
<tr>
<td>4.1-1</td>
<td>Analyser settings</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Outline

This Application Note gives a guide on configuring a TransPort router with a Cellular (Mobile) Primary WAN connectivity to failover to an Ethernet connection for Backup. This configuration can be useful when the Ethernet is, for example, a Satellite connection, so more expensive than Cellular and so used for Backup when the Mobile is not available or is experiencing issues.

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.

Preconditions: This guide assumes that the Digi TransPort router has a working Cellular connection and also an Ethernet one.

Models shown: Digi TransPort WR21

Other Compatible Models: All other Digi TransPort products with Cellular connection

Firmware versions: All Versions

Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

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

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
</tr>
<tr>
<td>1.0</td>
<td>Completed 7/2015</td>
</tr>
</tbody>
</table>
This application note will consider the following network scenario:
In order to configure the Digi TransPort, connect a PC to the ETH0 of the TransPort and log into the Web User Interface (WebUI) with a browser at the default address 192.168.1.1. Then follow the sections below.

### 3.1 LAN Settings

In this AN the LAN interface of the Transport is configured on ETH0 and left as default (192.168.1.1). The configuration can be checked going to the WEB UI at the section Configuration – Network > Interfaces > Ethernet > ETH0:

![LAN settings configuration page](image)

**Figure 3.1-1: LAN settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
<td>Specifies the IP address of this Ethernet port</td>
<td><code>eth o ipaddr 192.168.1.1</code></td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port</td>
<td><code>eth o mask 255.255.255.0</code></td>
</tr>
</tbody>
</table>
3.2  WAN Settings

In this Application note we will configure the Mobile as primary WAN connection as follows.

3.2.1  Mobile settings

In the WEB GUI, browse to the section Configuration - Network > Interfaces > Mobile and configure mobile settings as follows, then click Apply:

![Configuration - Network > Interfaces > Mobile screenshot]

**Figure 3.2.1-1: Primary WAN settings - Mobile**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Plan / APN</td>
<td>&lt;APN&gt;</td>
<td>Enter the APN (Access Point Name) given by the service provider</td>
<td><code>modemcc o apn &lt;APN&gt;</code></td>
</tr>
</tbody>
</table>
3.2.2 PPP 1 Settings

Browse to Configuration - Network > Interfaces > Advanced > PPP 1 > Advanced and configure the settings for the link monitor as described in the picture and table below, then click Apply:

![Configuration interface screenshot](image)

**Figure 3.2.2-2: Primary WAN settings – PPP1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate Ping packets on this interface</td>
<td>Ticked</td>
<td>This option will reveal the settings for ping generation on this interface</td>
<td></td>
</tr>
<tr>
<td>to IP host</td>
<td>&lt;IP to ping&gt;</td>
<td>Valid IP address to ping for link up/down testing.</td>
<td>ppp 1 pingip &quot;8.8.8.8&quot;</td>
</tr>
<tr>
<td>Every</td>
<td>10 Seconds</td>
<td>Interval in hours, minutes and seconds for the test pings to be sent</td>
<td>ppp 1 pingint 10</td>
</tr>
</tbody>
</table>
3.3 ETH 1 Backup WAN settings

In this AN the backup WAN is configured on ETH 1 and will obtain the IP settings via DHCP. Browse to Configuration - Network > Interfaces > Ethernet > ETH 1 and enable the DHCP client as follows, and click Apply:

![Configuration interface settings]

Figure 3.3-1: Backup WAN settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get an IP address automatically using DHCP</td>
<td>Ticked</td>
<td>This option will enable the DHCP client on ETH1</td>
<td><code>eth 1 dhcpcli ON</code></td>
</tr>
<tr>
<td>Enable NAT on this interface</td>
<td>Ticked</td>
<td>This option enable the NAT on the interface for the outgoing traffic</td>
<td><code>eth 1 do_nat 1</code></td>
</tr>
</tbody>
</table>
### 3.4 Primary Default route 0

Check the default route 0 is (as per default) configured to PPP 1 as outgoing interface, navigate to Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0:

![Configuration interface for Default Route 0](image)

**Figure 3.4-1: Primary route settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>PPP 1</td>
<td>Selects PPP 1 as the next available default route</td>
<td><code>def_route o ll_ent PPP</code>&lt;br&gt;<code>def_route o ll_add 1</code></td>
</tr>
</tbody>
</table>
### 3.5 Backup Default route 1

In order to configure the backup route through the ETH 1 interface, browse to **Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 1** and make the following changes:

![Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 1](image)

**Figure 3.5-1: Backup route settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
</table>
| Interface | ETH 1   | Selects ETH 1 | `def_route 1 ll_ent ETH`  
            |          |             | `def_route 1 ll_add 1` |

| Metric | 2 | Set this route as the second favourite route | `def_route 1 upmetric 2` |

| Advanced > Use metric <n> when the interface is down | 2 | Set this route as the second favourite route also when the interface down | `def_route 1 metric 2` |

The configuration of the gateway depends if the ETH scenario is static (in that case fill the Gateway field) or dynamic (in that case a DHCP server will assign it).

Click Apply.
3.6 Firewall settings

In order to have the backup mechanism working, the firewall will be configured in order to monitor the primary link.

Please note that if the firewall is enabled just for this purpose, it may be better add first of all the following rule in order to not lost the connection to the device when enabling the firewall on the interfaces, Navigate to: Configuration - Security > Firewall, click on “insert” and type/paste in the rule “pass break end”, then click OK:

![Image of firewall settings]

**Figure 3.6-1: Firewall settings – PassAll rule**

The next rule will enable the monitoring of the ICMP traffic exiting the PPP 1 interface. If the ICMP traffic fails then this interface will be taken out of service and the recovery ping process will verify when the test host is responding to test traffic again.

Click again on “insert” and type/paste in this rule (changing the monitoring IP address as per your scenario):  

`pass out break end on ppp 1 proto icmp from addr-ppp 1 to 8.8.8.8 icmp-type echo inspect-state oos 10 t=3 c=3 d=3 r=ping,3,3`

And click “OK” to add the rule:

![Image of firewall settings]

**Figure 3.6-2: Firewall settings – PPP1 Monitor rule**

Click “Save” button, to write the firewall rules to the fw.txt file on the router’s FLASH.
The firewall configuration should look like this for the 2 rules added in this section:

![Firewall settings – All the rules](image)

**Please note:** The IP address that is used in this AN for sending test pings to is not guaranteed to reply so it should be chosen an IP address within the ISP’s or a public IP address that can be controlled.

### 3.6.1 Enabling the firewall on the WAN interfaces

Scroll down to the Firewall configuration page to the Interface list and tick the boxes to enable the firewall on eth 1 and ppp 1:

![Firewall settings – Enabling the FW on PPP1](image)
Click the "Apply" button to enable the firewall on those two interfaces.

In order to have the settings taking effect on the cellular interface, the PPP should deactivated-reactivated:

Go to Management > Network Status > Interfaces > Advanced > PPP > PPP 1 and click first on "Drop link":

![Image of Management interface]

Figure 3.6-5: Drop PPP link to apply FW settings
TESTING

4.1 Debug settings on TransPort

In the phase of testing the functionality, it is very useful to set up the device in order to see the packets going through the primary/backup connection.

In order to configure it, on the TransPort, go to Management - Analyser > Settings and change the settings as shown below (uncheck everything else):

Figure 4.1-1: Analyser settings
### Cellular WAN failover to Ethernet with firewall monitoring

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Analyser</td>
<td>Selected</td>
<td>This checkbox is used to enable or disable the analyser.</td>
<td>ana 0 anon ON</td>
</tr>
<tr>
<td>Maximum packet capture size</td>
<td>1500</td>
<td>The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Common practice is to set it to 1500</td>
<td>ana 0 maxdata 1500</td>
</tr>
<tr>
<td>Log Size</td>
<td>180</td>
<td>The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Common practice is to set at this maximum (180). Notice that the data is compressed so more than 180Kb of trace data will be captured.</td>
<td>ana 0 logsize 180</td>
</tr>
<tr>
<td>Protocol layers</td>
<td>Layer 3 (Network)</td>
<td>Specify which protocol layers are captured and included in the analyser trace. For the purpose of this AN the Network Layer (Layer 3) is chosen</td>
<td>ana 0 l3on</td>
</tr>
<tr>
<td>IP Sources</td>
<td>ETH 0 ETH 1 PPP 1</td>
<td>Select the IP sources over which packets will be captured and included in the analyser trace</td>
<td>eth 0 ipanon on eth 1 ipanon on ppp 1 ipanon on</td>
</tr>
</tbody>
</table>
4.2 Testing the Cellular to Ethernet Failover

In order to test the failover, in this AN will be simulated two failures, one directly on the transport, for example removing the antenna and the other making the remote monitoring host unreachable, to simulate a failure somewhere in the network chain.

4.2.1 Simulating the fault on PPP connection on the transport

In the normal condition the routing table will look like this:

```
route print
Destination Gateway Metric Protocol Idx Interface Status
-----------------------------------------------
10.104.1.0/24 10.104.1.115 1 Local - ETH 1 UP
37.82.211.160/29 37.82.211.163 1 Local - PPP 1 UP
192.168.1.0/24 192.168.1.1 1 Local - ETH 0 UP
0.0.0.0/0 37.82.211.163 2 Static 0 PPP 1 UP
0.0.0.0/0 10.104.1.1 3 Static 1 ETH 1 UP
```

ICMP ECHO Request coming from ETH 0 and routed to PPP 1

```
----- 6-11-2014 10:05:57.650 ----- 
45 00 00 3C 15 97 00 00 80 01 57 12 C0 A8 01 64  EF.<......W....d
08 08 04 04 08 00 4D 54 00 01 00 07 61 62 63 64  ......MT....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69  uwwabcdefgh
IP (In) From REM TO LOC IFACE: ETH 0
45             IP Ver:        4
00             Hdr Len:       20
00             TOS:           Routine
00             Delay:         Normal
00             Throughput:    Normal
00             Reliability:   Normal
00 3C          Length:        60
15 97          ID:            5527
00 00          Frag Offset:   0
00             Congestion:    Normal
00             May Fragment
00             Last Fragment
80             TTL:           128
01             Proto:         ICMP
57 12          Checksum:      22290
C0 A8 01 64    Src IP:        192.168.1.100
08 08 04 04    Dest IP:       8.8.4.4
ICMP:
08             Type:         ECHO REQ
00             Code:         0
4D 54          Checksum:      21581
-----
----- 6-11-2014 10:05:57.650 ----- 
45 00 00 3C 15 97 00 00 7F 01 21 29 25 52 D3 A3  E..<......%!R..
08 08 04 04 08 00 4D 54 00 01 00 07 61 62 63 64  ......MT....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69  uwwabcdefgh
IP (Final) From LOC TO REM IFACE: PPP 1
45             IP Ver:        4
```
Cellular WAN failover to Ethernet with firewall monitoring

Hdr Len:       20
TOS:           Routine
Delay:         Normal
Throughput:    Normal
Reliability:   Normal
00 3C          Length:        60
15 97          ID:            5527
00 00          Frag Offset:   0
Congestion:    Normal
May Fragment
Last Fragment
7F             TTL:           127
01             Proto:         ICMP
21 29          Checksum:      8489
08 08 04 04    Src IP:        37.82.211.163
00             Dst IP:        8.8.4.4
ICMP:
08             Type:          ECHO REQ
00             Code:          0
4D 54          Checksum:      21581
----------

ICMP ECHO Reply coming on PPP 1 and routed to ETH 0

----- 6-11-2014 10:05:57.740 ------
45 00 00 3C 00 00 00 00 00 27 01 8E C0 08 08 04 04     E..<....'........
25 52 D3 A3 00 00 55 54 00 01 00 07 61 62 63 64     %R....UT....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efgijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi
IP (In) From REM TO LOC    IFACE: PPP 1
45             IP Ver:        4
00             Hdr Len:       20
00             TOS:           Routine
Delay:         Normal
Throughput:    Normal
Reliability:   Normal
00 3C          Length:        60
00 00          ID:            0
00 00          Frag Offset:   0
Congestion:    Normal
May Fragment
Last Fragment
27             TTL:           39
01             Proto:         ICMP
8E C0          Checksum:      36544
08 08 04 04    Src IP:        8.8.4.4
25 52 D3 A3    Dst IP:        37.82.211.163
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
4D 54          Checksum:      21589
----------

----- 6-11-2014 10:05:57.740 ------
45 00 00 3C 00 00 00 00 25 01 C7 A9 08 08 04 04     E..<....'........
C0 A8 01 64 00 00 55 54 00 01 00 07 61 62 63 64     %d....UT....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efgijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi
IP (Final) From LOC TO REM  IFACE: ETH 0
45             IP Ver:        4
00             Hdr Len:       20
00             TOS:           Routine
Delay:         Normal
Throughput:    Normal

Cellular WAN failover to Ethernet with firewall monitoring

To simulate the failure on PPP, let’s remove for example the antenna and check on the eventlogs, should appear logs as the following indicating that the PPP 1 and the default route 0 are set OOS by the firewall:

10:06:57, 06 Nov 2014, PPP 1 down, LL disconnect
10:06:57, 06 Nov 2014, Modem disconnected on asy 4, 26
10:06:55, 06 Nov 2014, Modem dialing on asy 4 #:*98*1#
10:06:52, 06 Nov 2014, GOBI 3000 running QCN D3200-STSUGN-1575
10:06:52, 06 Nov 2014, GOBI 3000 running FW D3200-STSUGN-1575
10:06:49, 06 Nov 2014, GPRS Registration Off
10:06:49, 06 Nov 2014, Modem disconnected on asy 4, 1
10:06:47, 06 Nov 2014, PPP 1 down, Firewall Request
10:06:47, 06 Nov 2014, Default Route 0 Out Of Service, Firewall
10:06:47, 06 Nov 2014, PPP 1 Out Of Service, Firewall
10:06:40, 06 Nov 2014, Network technology changed to WCDMA

In that condition the routing table becomes:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
<th>Protocol</th>
<th>Idx</th>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.104.1.0/24</td>
<td>10.104.1.115</td>
<td>1</td>
<td>Local</td>
<td>1</td>
<td>ETH 1</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>192.168.1.1</td>
<td>1</td>
<td>Local</td>
<td>1</td>
<td>ETH 0</td>
<td>UP</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>10.104.1.1</td>
<td>3</td>
<td>Static</td>
<td>1</td>
<td>ETH 1</td>
<td>UP</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>37.82.211.163</td>
<td>-</td>
<td>Static</td>
<td>0</td>
<td>PPP 1</td>
<td>OOS</td>
</tr>
</tbody>
</table>

And the same ping as before is now routed through the backup link on ETH 1:
Cellular WAN failover to Ethernet with firewall monitoring

00  TOS: Routine
    Delay: Normal
    Throughput: Normal
    Reliability: Normal
00 3C  Length: 60
24 98  ID: 9368
00 00  Frag Offset: 0
    Congestion: Normal
    May Fragment
    Last Fragment
80  TTL: 128
01  Proto: ICMP
48 11  Checksum: 18449
C0 A8 01 64  Src IP: 192.168.1.100
08 08 04 04 Dst IP: 8.8.4.4
ICMP:
  08  Type: ECHO REQ
  00  Code: 0
4D 53  Checksum: 21325
--------

-------- 6-11-2014 10:07:08.040 --------
45 00 00 3C 24 98 00 00 07 01 FF 42 0A 68 01 73 7E..<...B.h.s
08 08 04 04 08 00 4D 53 00 01 00 08 61 62 63 64 00MS....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efgijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69 uvwbcdefghi

IP (In) From LOC TO REM IFACE: ETH 1
45  IP Ver: 4
    Hdr Len: 20
00  TOS: Routine
    Delay: Normal
    Throughput: Normal
    Reliability: Normal
00 3C  Length: 60
24 98  ID: 9368
00 00  Frag Offset: 0
    Congestion: Normal
    May Fragment
    Last Fragment
7F  TTL: 127
01  Proto: ICMP
4F 42  Checksum: 65346
0A 68 01 73  Src IP: 10.104.1.115
08 08 04 04 Dst IP: 8.8.4.4
ICMP:
  08  Type: ECHO REQ
  00  Code: 0
4D 53  Checksum: 21325
--------

-------- 6-11-2014 10:07:08.060 --------
45 00 00 3C 00 00 00 00 00 30 01 72 DB 08 08 04 04 E..<...0.r.....
0A 68 01 73 00 00 55 53 00 01 00 08 61 62 63 64 .h.s..US....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efgijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69 uvwbcdefghi

IP (In) From REM TO LOC IFACE: ETH 1
45  IP Ver: 4
    Hdr Len: 20
00  TOS: Routine
    Delay: Normal
    Throughput: Normal
    Reliability: Normal
00 3C  Length: 60
00 00  ID: 0
00 00  Frag Offset: 0
    Congestion: Normal
Cellular WAN failover to Ethernet with firewall monitoring

---

<table>
<thead>
<tr>
<th>May Fragment</th>
<th>Last Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>TTL: 48</td>
</tr>
<tr>
<td>01</td>
<td>Proto: ICMP</td>
</tr>
<tr>
<td>72 DB</td>
<td>Checksum: 29403</td>
</tr>
<tr>
<td>08 08 04 04</td>
<td>Src IP: 8.8.4.4</td>
</tr>
<tr>
<td>0A 68 01 73</td>
<td>Dat IP: 10.104.1.115</td>
</tr>
<tr>
<td>ICMP:</td>
<td></td>
</tr>
<tr>
<td>00</td>
<td>Type: ECHO REPLY</td>
</tr>
<tr>
<td>00</td>
<td>Code: 0</td>
</tr>
<tr>
<td>55 53</td>
<td>Checksum: 21333</td>
</tr>
</tbody>
</table>
---

When the antenna is reconnected, and the PPP comes back online, on eventlog it will be showed like this:

10:08:01, 06 Nov 2014, Network technology changed to HSDPA/HSUPA
10:07:50, 06 Nov 2014, PPP 1 up
10:07:50, 06 Nov 2014, Default Route 0 Available, Activation
10:07:50, 06 Nov 2014, PPP 1 Available, Activation
10:07:50, 06 Nov 2014, PPP 1 Start
10:07:50, 06 Nov 2014, Modem connected on asy 4
10:07:36, 06 Nov 2014, GPRS Registration On
10:07:34, 06 Nov 2014, Modem dialing on asy 4 #*98*1#
10:07:12, 06 Nov 2014, GOBI 3000 running QCN D3200-STSUGN-1575
10:07:12, 06 Nov 2014, GOBI 3000 running FM D3200-STSUGN-1575
10:07:12, 06 Nov 2014, PPP 1 down, LL disconnect
10:07:12, 06 Nov 2014, GOBI 3000 running QCN D3200-STSUGN-1575
10:07:12, 06 Nov 2014, GOBI 3000 running FM D3200-STSUGN-1575
10:07:12, 06 Nov 2014, Modem disconnected on asy 4 #*98*1#
And the routing table will return to the normal one, with Default route 0 and PPP 1 UP again:

```
route print
Destination          Gateway   Metric   Protocol  Idx Interface  Status
------------------------------------------------------------------------------
10.104.1.0/24     10.104.1.115      1      Local   - ETH 1      UP
37.82.103.216/29   37.82.103.219      1      Local   - PPP 1      UP
192.168.1.0/24    192.168.1.1      1      Local   - ETH 0      UP
0.0.0.0/0         37.82.103.219      2      Static   0 PPP 1      UP
0.0.0.0/0         10.104.1.1      3      Static   1 ETH 1      UP
```

And the ping from the laptop is routed again to the primary connection on PPP1:

```
----- 6-11-2014 10:08:24.230 -----  
45 00 00 3C 2E 10 00 00 80 01 3E 99 C0 A8 01 64     E..<......>....d 
08 08 04 04 08 00 4D 52 00 01 00 09 61 62 63 64     .........abcd 
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efgijklmnopqrstuvwxyz 
75 76 77 61 62 63 64 65 66 67 68 69     uvwabcdefghi 
[IP (In) From REM TO LOC IFACE: ETH 0] 
45 00 00 3C 2E 10 00 00 80 01 3E 99 C0 A8 01 64     E..<......>....d 
08 08 04 04 08 00 4D 52 00 01 00 09 61 62 63 64     .........abcd 
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efgijklmnopqrstuvwxyz 
75 76 77 61 62 63 64 65 66 67 68 69     uvwabcdefghi 
[IP (Final) From LOC TO REM IFACE: PPP 1] 
45 00 00 3C 2E 10 00 00 7F 01 74 78 25 52 67 DB     E..<......tx%Rg. 
08 08 04 04 08 00 4D 52 00 01 00 09 61 62 63 64     .........abcd 
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efgijklmnopqrstuvwxyz 
75 76 77 61 62 63 64 65 66 67 68 69     uvwabcdefghi 
```
Cellular WAN failover to Ethernet with firewall monitoring

May Fragment
Last Fragment

<table>
<thead>
<tr>
<th>May Fragment</th>
<th>Last Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>7F</td>
<td>127</td>
</tr>
<tr>
<td>01</td>
<td>Proto: ICMP</td>
</tr>
<tr>
<td>74 78</td>
<td>Checksum: 29816</td>
</tr>
<tr>
<td>25 52 67 DB</td>
<td>Src IP: 37.82.103.219</td>
</tr>
<tr>
<td>08 04 04</td>
<td>Dest IP: 8.8.4.4</td>
</tr>
<tr>
<td>ICMP:</td>
<td></td>
</tr>
<tr>
<td>08</td>
<td>Type: ECHO REPLY</td>
</tr>
<tr>
<td>00</td>
<td>Code: 0</td>
</tr>
<tr>
<td>4D 52</td>
<td>Checksum: 21069</td>
</tr>
</tbody>
</table>

----------

6-11-2014 10:08:24.320

<table>
<thead>
<tr>
<th>IP (In) From REM TO LOC</th>
<th>IFACE: PPP 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>IP Ver: 4</td>
</tr>
<tr>
<td>00</td>
<td>Hdr Len: 20</td>
</tr>
<tr>
<td>00</td>
<td>TOS: Routine</td>
</tr>
<tr>
<td>00</td>
<td>Delay: Normal</td>
</tr>
<tr>
<td>00</td>
<td>Throughput: Normal</td>
</tr>
<tr>
<td>00 3C</td>
<td>Reliability: Normal</td>
</tr>
<tr>
<td>00 00</td>
<td>Length: 60</td>
</tr>
<tr>
<td>00 00</td>
<td>ID: 0</td>
</tr>
<tr>
<td>00 00</td>
<td>Frag Offset: 0</td>
</tr>
</tbody>
</table>

May Fragment
Last Fragment

<table>
<thead>
<tr>
<th>May Fragment</th>
<th>Last Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>TTL: 39</td>
</tr>
<tr>
<td>01</td>
<td>Proto: ICMP</td>
</tr>
<tr>
<td>FA 88</td>
<td>Checksum: 64136</td>
</tr>
<tr>
<td>08 04 04</td>
<td>Src IP: 8.8.4.4</td>
</tr>
<tr>
<td>25 52 67 DB</td>
<td>Dest IP: 37.82.103.219</td>
</tr>
<tr>
<td>ICMP:</td>
<td></td>
</tr>
<tr>
<td>00</td>
<td>Type: ECHO REPLY</td>
</tr>
<tr>
<td>00</td>
<td>Code: 0</td>
</tr>
<tr>
<td>55 52</td>
<td>Checksum: 21077</td>
</tr>
</tbody>
</table>

----------

6-11-2014 10:08:24.320

<table>
<thead>
<tr>
<th>IP (Final) From LOC TO REM</th>
<th>IFACE: ETH 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>IP Ver: 4</td>
</tr>
<tr>
<td>00</td>
<td>Hdr Len: 20</td>
</tr>
<tr>
<td>00</td>
<td>TOS: Routine</td>
</tr>
<tr>
<td>00</td>
<td>Delay: Normal</td>
</tr>
<tr>
<td>00</td>
<td>Throughput: Normal</td>
</tr>
<tr>
<td>00 3C</td>
<td>Reliability: Normal</td>
</tr>
<tr>
<td>00 00</td>
<td>Length: 60</td>
</tr>
<tr>
<td>00 00</td>
<td>ID: 0</td>
</tr>
<tr>
<td>00 00</td>
<td>Frag Offset: 0</td>
</tr>
</tbody>
</table>

May Fragment
Last Fragment

<table>
<thead>
<tr>
<th>May Fragment</th>
<th>Last Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TTL: 37</td>
</tr>
<tr>
<td>01</td>
<td>Proto: ICMP</td>
</tr>
<tr>
<td>C7 A9</td>
<td>Checksum: 51113</td>
</tr>
<tr>
<td>08 04 04</td>
<td>Src IP: 8.8.4.4</td>
</tr>
<tr>
<td>C0 A8 01 64</td>
<td>Dest IP: 192.168.1.100</td>
</tr>
<tr>
<td>ICMP:</td>
<td></td>
</tr>
<tr>
<td>00</td>
<td>Type: ECHO REPLY</td>
</tr>
<tr>
<td>00</td>
<td>Code: 0</td>
</tr>
</tbody>
</table>
5 CONFIGURATION FILE

5.1 TransPort Firmware & Hardware

This is the firmware and hardware information of the TransPort WR21 used in this Application:

<table>
<thead>
<tr>
<th>Description</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digi TransPort WR21-U82B-DE1-XX</td>
<td>Ser#: 237416</td>
</tr>
<tr>
<td>ARM Bios Ver 7.21u v43 454MHz</td>
<td>B987-M995-F80-08140,0 MAC: 00042d039f68</td>
</tr>
<tr>
<td>Async Driver</td>
<td>Revision: 1.19 Int clk</td>
</tr>
<tr>
<td>Firewall</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>EventEdit</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>Timer Module</td>
<td>Revision: 1.1</td>
</tr>
<tr>
<td>(B)USBHOST</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>L2TP</td>
<td>Revision: 1.10</td>
</tr>
<tr>
<td>PPTP</td>
<td>Revision: 1.00</td>
</tr>
<tr>
<td>TACPLUS</td>
<td>Revision: 1.00</td>
</tr>
<tr>
<td>MODBUS</td>
<td>Revision: 0.00</td>
</tr>
<tr>
<td>RealPort</td>
<td>Revision: 0.00</td>
</tr>
<tr>
<td>MultiTX</td>
<td>Revision: 1.00</td>
</tr>
<tr>
<td>LAPB</td>
<td>Revision: 1.12</td>
</tr>
<tr>
<td>X25 Layer</td>
<td>Revision: 1.19</td>
</tr>
<tr>
<td>MACRO</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>PAD</td>
<td>Revision: 1.4</td>
</tr>
<tr>
<td>X25 Switch</td>
<td>Revision: 1.7</td>
</tr>
<tr>
<td>V120</td>
<td>Revision: 1.16</td>
</tr>
<tr>
<td>TPAD Interface</td>
<td>Revision: 1.12</td>
</tr>
<tr>
<td>GPS</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>TELITUPD</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>SCRIBATS SK</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>BASTSK</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>PYTHON</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>CLOUDSMS</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>TCP</td>
<td>Revision: 1.14</td>
</tr>
<tr>
<td>TCP Util</td>
<td>Revision: 1.13</td>
</tr>
<tr>
<td>PPP</td>
<td>Revision: 1.19</td>
</tr>
<tr>
<td>WEB</td>
<td>Revision: 1.5</td>
</tr>
<tr>
<td>SMTP</td>
<td>Revision: 1.1</td>
</tr>
<tr>
<td>FTP Client</td>
<td>Revision: 1.5</td>
</tr>
<tr>
<td>FTP</td>
<td>Revision: 1.4</td>
</tr>
<tr>
<td>IKE</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>PollANS</td>
<td>Revision: 1.2</td>
</tr>
<tr>
<td>PPPOE</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>BRIDGE</td>
<td>Revision: 1.1</td>
</tr>
<tr>
<td>MODEM CC (GOBI UMTS)</td>
<td>Revision: 1.4</td>
</tr>
<tr>
<td>FLASH Write</td>
<td>Revision: 1.2</td>
</tr>
<tr>
<td>Command Interpreter</td>
<td>Revision: 1.38</td>
</tr>
<tr>
<td>SSLCLI</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>OSPF</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>BGP</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>QOS</td>
<td>Revision: 1.0</td>
</tr>
<tr>
<td>PWRCTRL</td>
<td>Revision: 1.0</td>
</tr>
</tbody>
</table>
5.2 TransPort Configuration File

This is the configuration used on the TransPort WR21 in this Application Note (main settings highlighted):

```
'config c show'
eth 0 IPaddr "192.168.1.1"
eth 0 ipanon ON
eth 1 dhcpcli ON
eth 1 mask ""
eth 1 do_nat 1
eth 1 ipanon ON
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
def_route 1 ll_ent "ETH"
def_route 1 ll_add 1
def_route 1 upmetric 2
def_route 1 metric 2
dhcp 0 IPmin "192.168.1.100"
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.etherios.com"
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 firewall ON
ppp 1 use_modem 1
```
Cellular WAN failover to Ethernet with firewall monitoring

```plaintext
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 pingip "8.8.8.8"
ppp 1 pingint 10
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 1 radiuscfg 0
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 "internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_concat 10
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
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdo 0
ana 0 lapbon 0
ana 0 maxdata 1500
ana 0 logsize 180
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 "KD5lSVJDVG="
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
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
```
Cellular WAN failover to Ethernet with firewall monitoring

<table>
<thead>
<tr>
<th>cloud</th>
<th>ssl</th>
<th>ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Up Profile</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.3 Firewall rules

Those are the Firewall rules used in this Application Notes (main rules highlighted):

```plaintext
pass out break end on ppp 1 proto icmp from addr-ppp 1 to 8.8.8.8 icmp-type echo inspect-state oos 10 t=3 c=3 d=3 r=ping,3,3

pass break end

# Allow outbound FTP traffic
pass out break end proto ftp from any to any port=ftpflags S!A inspect-state

# Allow any other outbound traffic and the replies back in
pass out break end inspect-state

# Allow incoming IPSEC
pass break end proto 50
pass in break end proto udp from any to any port=ike
pass in break end proto udp from any to any port=4500

# Allow any traffic within an IPSEC tunnel in both directions
pass break end oneroute any

# Allow incoming SSH and SFTP
pass in break end proto tcp from any to any port=22 flags S!A inspect-state

# Allow incoming HTTPS
pass in break end proto tcp from any to any port=443 flags S!A inspect-state

# Block and log everything else including incoming telnet, http and FTP
block log break end
```