



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

Figure 3.1-1: LAN settings	6
Figure 3.2.1-1: Primary WAN settings - Mobile	7
Figure 3.2.2-2: Primary WAN settings – PPP1	8
Figure 3.3-1: Backup WAN settings	9
Figure 3.4-1: Primary route settings	10
Figure 3.5-1: Backup route settings	11
Figure 3.6-1: Firewall settings –PassAll rule	12
Figure 4.1-1: Analyser settings	15

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

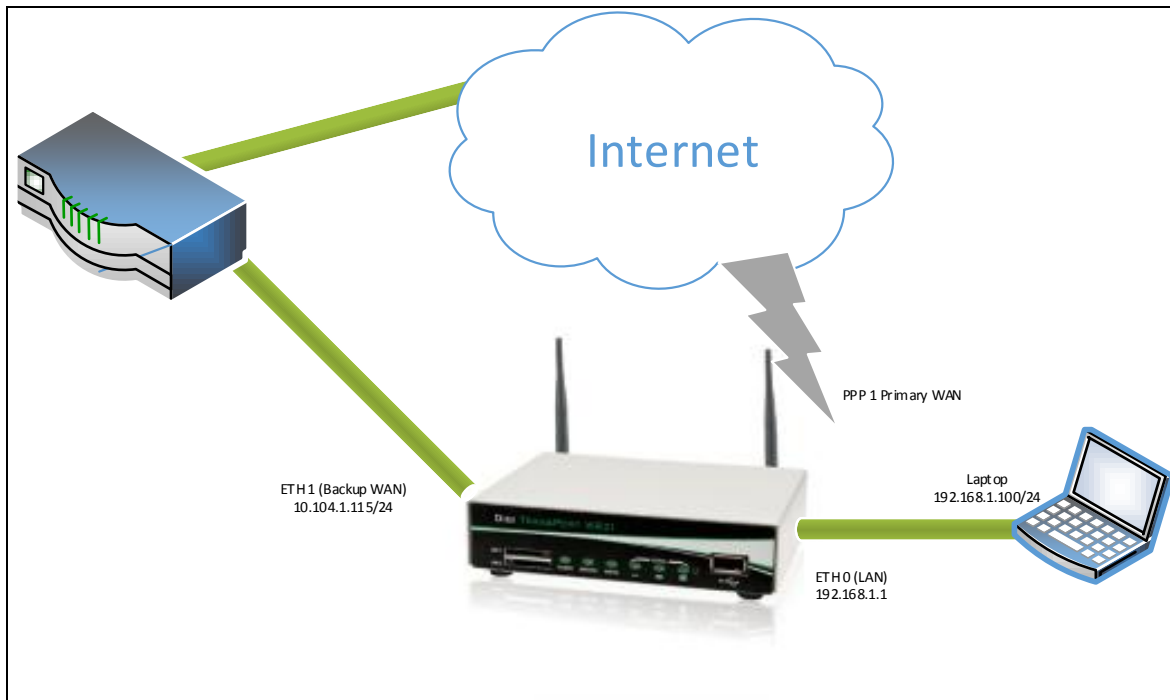
Requests for new application notes can be sent to the same address.

1.4 Version

Version Number	Status
0.1	Draft
1.0	Completed 7/2015

2 SCENARIO

This application note will consider the following network scenario:



3 DIGITRANSPORT ROUTER CONFIGURATION

In order to configure the Digi TransPort, connect a PC to the ETHo 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 ETH 0 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 > ETH 0:

Configuration - Network > Interfaces > Ethernet > ETH 0

▼ Interfaces

▼ Ethernet

▼ ETH 0

Description:

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address:

Mask:

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

► Advanced

► QoS

► VRRP

Figure 3.1-1: LAN settings

Parameter	Setting	Description	CLI command
IP Address	192.168.1.1	Specifies the IP address of this Ethernet port	<i>eth 0 ipaddr 192.168.1.1</i>
Mask	255.255.255.0	Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port	<i>eth 0 mask 255.255.255.0</i>

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:

The screenshot shows the 'Configuration - Network > Interfaces > Mobile' web page. The 'Service Plan / APN' field is highlighted with a red box. The 'Apply' button at the bottom is also highlighted with a red box.

Configuration - Network > Interfaces > Mobile

Interfaces

- Ethernet**
- Mobile**

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: **1 (PPP 1)**

IMSI: 262010050359784

Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: **Internet-01-00**

☐ Use backup APN: Retry the main APN after minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

☐ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☒ Enable NAT on this interface

☒ IP address ☐ IP address and Port

☐ Enable IPsec on this interface

☐ Enable the firewall on this interface

SIM Selection

Advanced

SMS Settings

Apply

Figure 3.2.1-1: Primary WAN settings - Mobile

Parameter	Setting	Description	CLI command
Service Plan / APN	<APN>	Enter the APN (Access Point Name) given by the service provider	<i>modemcc o apn <APN></i>

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:

The screenshot shows the 'Configuration - Network > Interfaces > Advanced > PPP 1 > Advanced' page. The 'Advanced' tab is selected. The 'Metric' is set to 1. The 'Allow this PPP interface to settle for' is set to 0 x 100 milliseconds. The 'Enable "Always On" mode of this interface' is checked, with 'On' selected. The 'Attempt to re-connect after' is set to 0 seconds. The 'Wait' time after power-up is set to 0 seconds. The 'Keep this interface up for at least' is set to 0 seconds. The 'Click here to assign a timeband to this interface' link is present. The 'Add a route to' checkbox is unchecked. The 'Enable DNS inbound blocking' checkbox is unchecked. The 'Forward IP broadcasts over this interface if this interface is on the same IP network as an Ethernet interface' checkbox is unchecked. The 'Send LCP echo request packet to the remote peer' checkbox is unchecked. The 'Generate Heartbeats on this interface' checkbox is unchecked. The 'Generate Ping packets on this interface' checkbox is checked. The 'Send' field is set to 0 byte pings to IP host 8.8.8.8 every 0 hrs 0 mins 10 secs. The 'Send pings every' field is set to 0 hrs 0 mins 0 seconds if ping responses are not being received. The 'Switch to sending pings to IP host' field is set to 3 failures. The 'Ping responses are expected within' field is set to 0 seconds. The 'Only send Pings when this interface is "In Service"' checkbox is unchecked. The 'New connections to resume with previous Ping interval' checkbox is unchecked. The 'Reset the link if no response is received within' field is set to 0 seconds. The 'Use the ETH 0 IP address as the source IP address' checkbox is unchecked. The 'Defer sending pings if IP traffic is being received' checkbox is unchecked.

Figure 3.2.2-2: Primary WAN settings – PPP1

Parameter	Setting	Description	CLI command
Generate Ping packets on this interface	Ticked	This option will reveal the settings for ping generation on this interface	---
to IP host	<IP to ping>	Valid IP address to ping for link up/down testing.	<i>ppp 1 pingip "8.8.8.8"</i>
Every	10 Seconds	Interval in hours, minutes and seconds for the test pings to be sent	<i>ppp 1 pingint 10</i>

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:

Figure 3.3-1: Backup WAN settings

Parameter	Setting	Description	CLI command
Get an IP address automatically using DHCP	Ticked	This option will enable the DHCP client on ETH1	<i>eth 1 dhcpcli ON</i>
Enable NAT on this interface	Ticked	This option enable the NAT on the interface for the outgoing traffic	<i>eth 1 do_nat 1</i>

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:

Figure 3.4-1: Primary route settings

Parameter	Setting	Description	CLI command
Interface	PPP 1	Selects PPP 1 as the next available default route	<i>def_route 0 ll_ent PPP</i> <i>def_route 0 ll_add 1</i>

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:

Figure 3.5-1: Backup route settings

Parameter	Setting	Description	CLI command
Interface	ETH 1	Selects ETH 1	<i>def_route 1 ll_ent ETH def_route 1 ll_add 1</i>
Metric	2	Set this route as the second favourite route	<i>def_route 1 upmetric 2</i>
Advanced > Use metric <n> when the interface is down	2	Set this route as the second favourite route also when the interface down	<i>def_route 1 metric 2</i>

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:

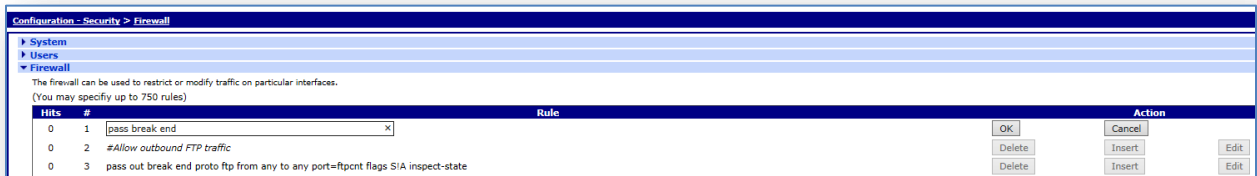


Figure 3.6-1: Firewall settings –PassAll rule

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:

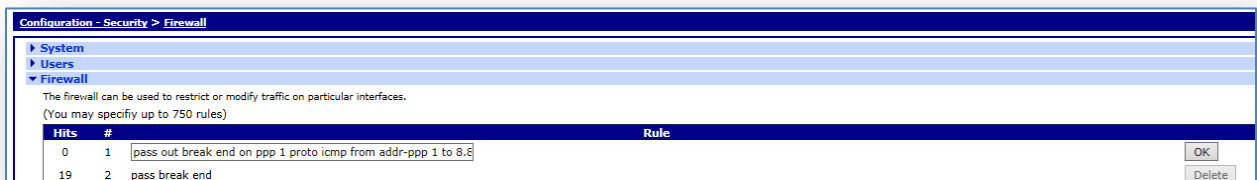


Figure 3.6-2: Firewall settings – PPP1 Monitor rule

Click “**Save**” button, to write the firewall rules to the fw.txt file on the router’s FLASH.

Cellular WAN failover to Ethernet with firewall monitoring

The firewall configuration should look like this for the 2 rules added in this section:



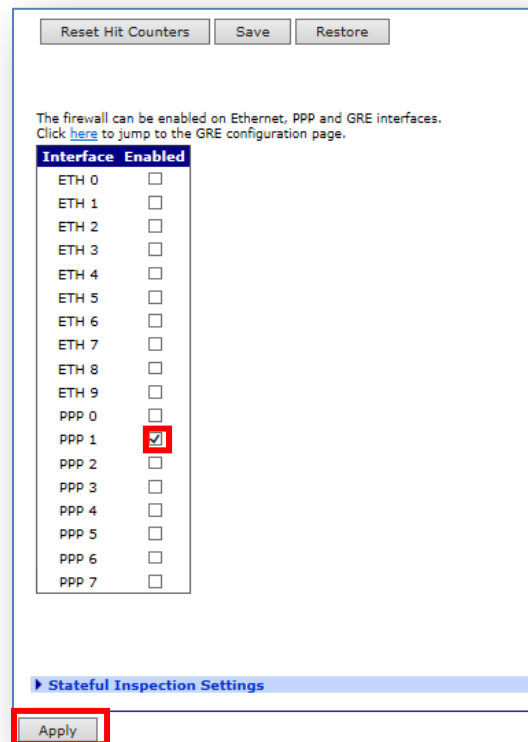
Hits	#	Rule	Action
2	1	pass out break end on ppp 1 proto icmp from addr-ppp 1 to 8.8.8.8 icmp-type echo inspect-state oos 10 t=3 c=3 d=3 r=ping,3,3	Delete Insert Edit
148	2	pass break end	Delete Insert Edit

Figure 3.6-3: Firewall settings – All the rules

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:



Reset Hit Counters Save Restore

The firewall can be enabled on Ethernet, PPP and GRE interfaces.
Click [here](#) to jump to the GRE configuration page.

Interface	Enabled
ETH 0	<input type="checkbox"/>
ETH 1	<input type="checkbox"/>
ETH 2	<input type="checkbox"/>
ETH 3	<input type="checkbox"/>
ETH 4	<input type="checkbox"/>
ETH 5	<input type="checkbox"/>
ETH 6	<input type="checkbox"/>
ETH 7	<input type="checkbox"/>
ETH 8	<input type="checkbox"/>
ETH 9	<input type="checkbox"/>
PPP 0	<input type="checkbox"/>
PPP 1	<input checked="" type="checkbox"/>
PPP 2	<input type="checkbox"/>
PPP 3	<input type="checkbox"/>
PPP 4	<input type="checkbox"/>
PPP 5	<input type="checkbox"/>
PPP 6	<input type="checkbox"/>
PPP 7	<input type="checkbox"/>

Stateful Inspection Settings

Apply

Figure 3.6-4: Firewall settings – Enabling the FW on PPP1

Cellular WAN failover to Ethernet with firewall monitoring

Parameter	Setting	Description	CLI command
Interface	PPP 1	Selects ETH 1	<i>def_route 1 ll_ent ETH def_route 1 ll_add 1</i>

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”:

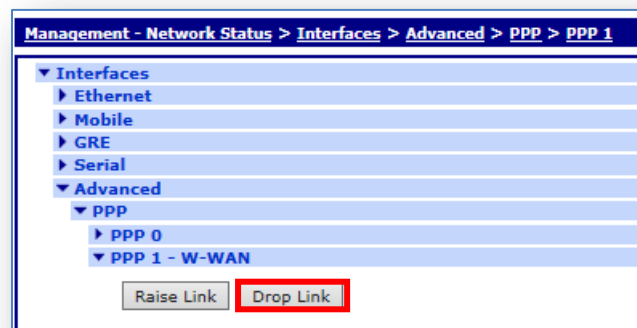


Figure 3.6-5: Drop PPP link to apply FW settings

4 TESTING

4.1 Debug settings on TransPort

In the phase of testing the functionality, 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):

The screenshot shows the 'Management - Analyser > Settings' window. The 'Settings' section is expanded. The following settings are highlighted with red boxes:

- ☒ Enable Analyser
- Maximum packet capture size: 12000 bytes
- Log size: 128 Kbytes
- ☒ Layer 3 (Network) (under Protocols)
- ☒ OVPN 0 (under IP Sources)
- Apply button at the bottom.

Other visible settings include:

- ☐ Layer 1 (Physical)
- ☐ Layer 2 (Link)
- ☐ xOT
- ☐ Enable IKE debug
- ☐ Enable QMI trace
- LAPB Links**
 - ☐ LAPB 0
 - ☐ LAPB 1
- Serial Interfaces**
 - ☐ ASY 0 to ☐ ASY 17
 - ☐ W-WAN
 - Clear all Serial Interfaces
- Ethernet Interfaces**
 - ☐ ETH 0 to ☐ ETH 9
 - Clear all Ethernet Interfaces
- PPP Interfaces**
 - ☐ PPP 0 to ☐ PPP 7
 - Clear all PPP Interfaces
- IP Sources**
 - ☒ ETH 0, ☒ ETH 1, ☐ ETH 2 to ☐ ETH 9
 - ☐ OVPN 0, ☐ OVPN 1, ☐ OVPN 2
 - ☐ PPP 0 to ☐ PPP 7
 - Clear all IP Sources
- IP Options**
 - ☐ Trace discarded packets
 - ☐ Trace loopback packets
- Ethernet Packet Filters**
 - MAC Addresses:
- IP Packet Filters**
 - TCP/UDP Ports:
 - IP Protocols:
 - IP Addresses:
- Discarded IP Packet Filters**
 - TCP/UDP Ports:
 - IP Protocols:
 - IP Addresses:

Figure 4.1-1: Analyser settings

Cellular WAN failover to Ethernet with firewall monitoring

Parameter	Setting	Description	CLI command
Enable Analyser	Selected	This checkbox is used to enable or disable the analyser.	ana o anon ON
Maximum packet capture size	1500	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	ana o maxdata 1500
Log Size	180	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.	ana o logsize 180
Protocol layers	Layer 3 (Network)	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	ana o l3on
IP Sources	ETH 0 ETH 1 PPP 1	Select the IP sources over which packets will be captured and included in the analyser trace	eth 0 ipanon on eth 1 ipanon on ppp 1 ipanon on

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 E..<.....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 uvwabcdefghi
```

```
IP (In) From REM TO LOC IFACE: ETH 0
45 IP Ver: 4
Hdr Len: 20
00 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
80 TTL: 128
01 Proto: ICMP
57 12 Checksum: 22290
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 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 uvwabcdefghi
```

```
IP (Final) From LOC TO REM IFACE: PPP 1
45 IP Ver: 4
```

Cellular WAN failover to Ethernet with firewall monitoring

```
00          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
25 52 D3 A3 Src IP:     37.82.211.163
08 08 04 04 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 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  efghijklmnopqrst
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
          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
55 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  efghijklmnopqrst
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
          Hdr Len:      20
00          TOS:         Routine
          Delay:         Normal
          Throughput:    Normal
```

Cellular WAN failover to Ethernet with firewall monitoring

```

Reliability: Normal
00 3C Length: 60
00 00 ID: 0
00 00 Frag Offset: 0
Congestion: Normal
May Fragment
Last Fragment
25 TTL: 37
01 Proto: ICMP
C7 A9 Checksum: 51113
08 08 04 04 Src IP: 8.8.4.4
C0 A8 01 64 Dst IP: 192.168.1.100
ICMP:
00 Type: ECHO REPLY
00 Code: 0
55 54 Checksum: 21589

```

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:

```

route print
-----
Destination          Gateway             Metric    Protocol    Idx Interface    Status
-----
10.104.1.0/24        10.104.1.115       1         Local      -    ETH 1         UP
192.168.1.0/24       192.168.1.1        1         Local      -    ETH 0         UP

0.0.0.0/0            10.104.1.1         3         Static     1    ETH 1         UP
0.0.0.0/0            37.82.211.163      -         Static     0    PPP 1         OOS

```

And the same ping as before is now routed through the backup link on ETH 1:

```

----- 6-11-2014 10:07:08.040 -----
45 00 00 3C 24 98 00 00 80 01 48 11 C0 A8 01 64 E..<$.....H....d
08 08 04 04 08 00 4D 53 00 01 00 08 61 62 63 64 .....MS....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 uvwabcdeefghi

IP (In) From REM TO LOC IFACE: ETH 0
45 IP Ver: 4
Hdr Len: 20

```

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 7F 01 FF 42 0A 68 01 73   E..<$.....B.h.s
08 08 04 04 08 00 4D 53 00 01 00 08 61 62 63 64   .....MS....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               uvwabcdefghi
```

```
IP (Final) 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
FF 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 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   efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69               uvwabcdefghi
```

```
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

```

May Fragment
Last Fragment
30          TTL:          48
01          Proto:        ICMP
72 DB       Checksum:     29403
08 08 04 04 Src IP:      8.8.4.4
0A 68 01 73 Dst IP:      10.104.1.115
ICMP:
00          Type:         ECHO REPLY
00          Code:         0
55 53       Checksum:     21333
-----

----- 6-11-2014 10:07:08.060 -----
45 00 00 3C 00 00 00 00 2E 01 BE A9 08 08 04 04  E...<.....
C0 A8 01 64 00 00 55 53 00 01 00 08 61 62 63 64  ...d..US....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              uvwabcdefghi

IP (Final) From LOC TO REM IFACE: ETH 0
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
          May Fragment
          Last Fragment
2E          TTL:          46
01          Proto:        ICMP
BE A9       Checksum:     48809
08 08 04 04 Src IP:      8.8.4.4
C0 A8 01 64 Dst IP:      192.168.1.100
ICMP:
00          Type:         ECHO REPLY
00          Code:         0
55 53       Checksum:     21333

```

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#
10:07:29, 06 Nov 2014,GOBI 3000 running QCN D3200-STUGN-1575
10:07:29, 06 Nov 2014,GOBI 3000 running FW D3200-STUGN-1575
10:07:26, 06 Nov 2014,PPP 1 down,LL disconnect
10:07:26, 06 Nov 2014,Modem disconnected on asy 4,26
10:07:24, 06 Nov 2014,Modem dialing on asy 4 #:*98*1#
10:07:20, 06 Nov 2014,GOBI 3000 running QCN D3200-STUGN-1575
10:07:20, 06 Nov 2014,GOBI 3000 running FW D3200-STUGN-1575

```

Cellular WAN failover to Ethernet with firewall monitoring

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    .....MR....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                uvwabcdefghi
```

```
IP (In) From REM TO LOC IFACE: ETH 0
45          IP Ver:      4
          Hdr Len:      20
00          TOS:         Routine
          Delay:         Normal
          Throughput:    Normal
          Reliability:   Normal
00 3C       Length:      60
2E 10       ID:          11792
00 00       Frag Offset: 0
          Congestion:   Normal
          May Fragment
          Last Fragment
80          TTL:         128
01          Proto:       ICMP
3E 99       Checksum:    16025
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 52       Checksum:    21069
-----
```

```
----- 6-11-2014 10:08:24.230 -----
 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    .....MR....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                uvwabcdefghi
```

```
IP (Final) From LOC TO REM IFACE: PPP 1
45          IP Ver:      4
          Hdr Len:      20
00          TOS:         Routine
          Delay:         Normal
          Throughput:    Normal
          Reliability:   Normal
00 3C       Length:      60
2E 10       ID:          11792
00 00       Frag Offset: 0
          Congestion:   Normal
```

Cellular WAN failover to Ethernet with firewall monitoring

```

May Fragment
Last Fragment
7F          TTL:          127
01          Proto:        ICMP
74 78       Checksum:     29816
25 52 67 DB Src IP:      37.82.103.219
08 08 04 04 Dst IP:      8.8.4.4
ICMP:
08          Type:         ECHO REQ
00          Code:         0
4D 52       Checksum:     21069
-----

```

```

----- 6-11-2014 10:08:24.320 -----
45 00 00 3C 00 00 00 00 27 01 FA 88 08 08 04 04  E..<....'.....
25 52 67 DB 00 00 55 52 00 01 00 09 61 62 63 64  %Rg...UR....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             uvwabcdefghi

```

```

IP (In) From REM TO LOC IFACE: PPP 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
          May Fragment
          Last Fragment
27          TTL:         39
01          Proto:        ICMP
FA 88       Checksum:     64136
08 08 04 04 Src IP:      8.8.4.4
25 52 67 DB Dst IP:      37.82.103.219
ICMP:
00          Type:         ECHO REPLY
00          Code:         0
55 52       Checksum:     21077
-----

```

```

----- 6-11-2014 10:08:24.320 -----
45 00 00 3C 00 00 00 00 25 01 C7 A9 08 08 04 04  E..<....%.....
C0 A8 01 64 00 00 55 52 00 01 00 09 61 62 63 64  ...d..UR....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             uvwabcdefghi

```

```

IP (Final) From LOC TO REM IFACE: ETH 0
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
          May Fragment
          Last Fragment
25          TTL:         37
01          Proto:        ICMP
C7 A9       Checksum:     51113
08 08 04 04 Src IP:      8.8.4.4
C0 A8 01 64 Dst IP:      192.168.1.100
ICMP:
00          Type:         ECHO REPLY
00          Code:         0

```

Cellular WAN failover to Ethernet with firewall monitoring

55 52

Checksum: 21077

5 CONFIGURATION FILE

5.1 TransPort Firmware & Hardware

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

```
Digi TransPort WR21-U82B-DE1-XX Ser#:237416
Software Build Ver5246. Aug 15 2014 12:20:23 WW
ARM Bios Ver 7.21u v43 454MHz B987-M995-F80-08140,0 MAC:00042d039f68
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 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
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
Device Cloud	Revision: 2.0
OK	

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 respdels 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
```

```

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 lapdon 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 "KD51SVJDVg="
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

```
cloud 0 ssl ON
```

```
Power Up Profile: 0  
OK
```

5.3 Firewall rules

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

```
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=ftpcnt flags 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
```