Application Note 70

Wi-Fi-to-Cellular Failover

Digi Technical Support

October 2016

Contents

1 INTRODUCTION

1.1 Outline

This Application Note (AN) gives a guide on configuring a TransPort router to have a WAN connection through Wi-Fi with a failover to a Cellular/Mobile connectivity using a monitoring on the link via Firewall rules.

This method can be very useful to detect some kind of failures on the Access Point (AP) to which the TransPort is connected to, as for example, a failure on the WAN connectivity of the AP. Without the monitoring method, this failure cannot be detected on the Client as the Wi-Fi connection to the AP will still be UP, but the client has effectively not access to the outside network as the AP cannot provide it in this situation. With the monitoring via firewall rules, this kind of failure can be easily detected allowing the TransPort to use the Backup link until the failure on the AP is recovered.

Obviously, using this method, it will always be possible to detect failure on the Wi-Fi itself. In that case, the primary route will go Out Of Service/back online due to the failure/rollback of Wi-Fi itself and not due to firewall monitoring.

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 a TransPort can be connected working AP that can provide Internet access.

Models shown: Digi TransPort WR44v2

Other Compatible Models: All other Digi TransPort products with Wi-Fi features.

Firmware versions: All Versions

Configuration: This AN 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 AN are welcome and should be addressed to: tech.support@digi.com

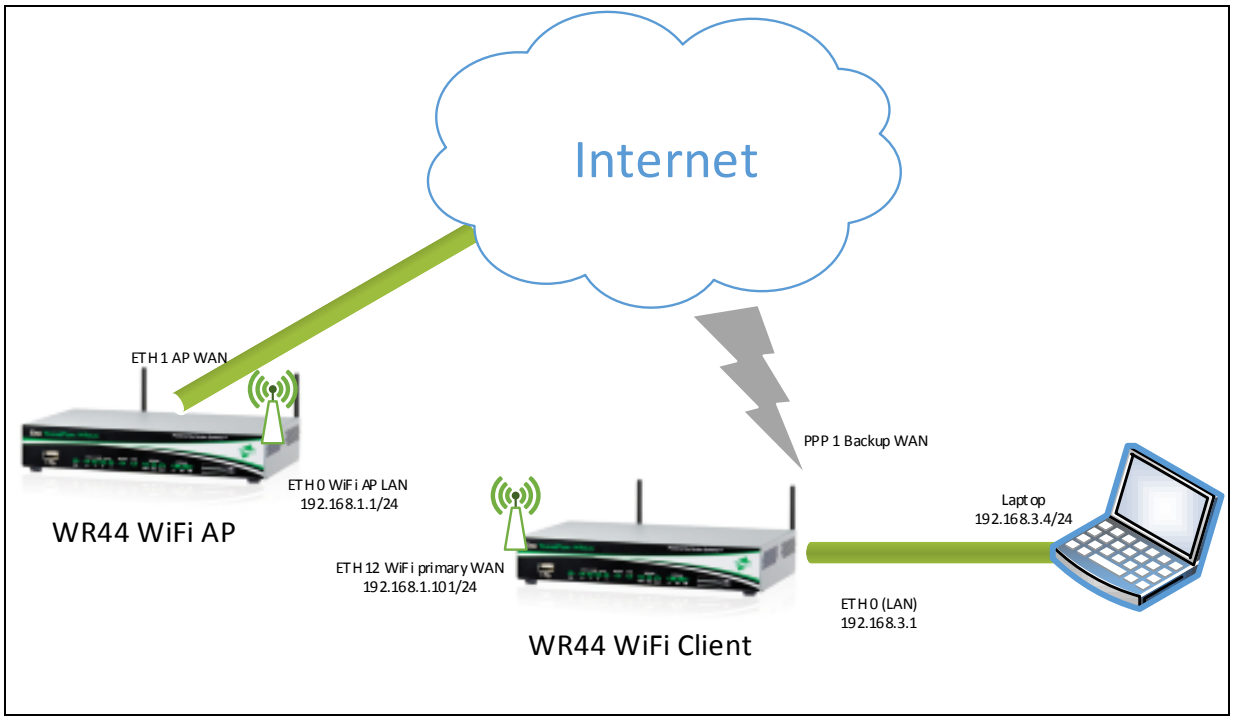
Requests for new ANs can be sent to the same address.

1.4 Version

Version Number	Status
0.1	Draft
1.0	Completed 7/2015
1.1	Updated screenshots and instructions for new web interface, rebranding (July 2016)

2 SCENARIO

This AN will consider the following scenario:



NOTE: This AN applies to the configuration of the rightmost TransPort, the Wi-Fi Client. In this this example, the leftmost TransPort represents the AP, which may be an entirely different product.

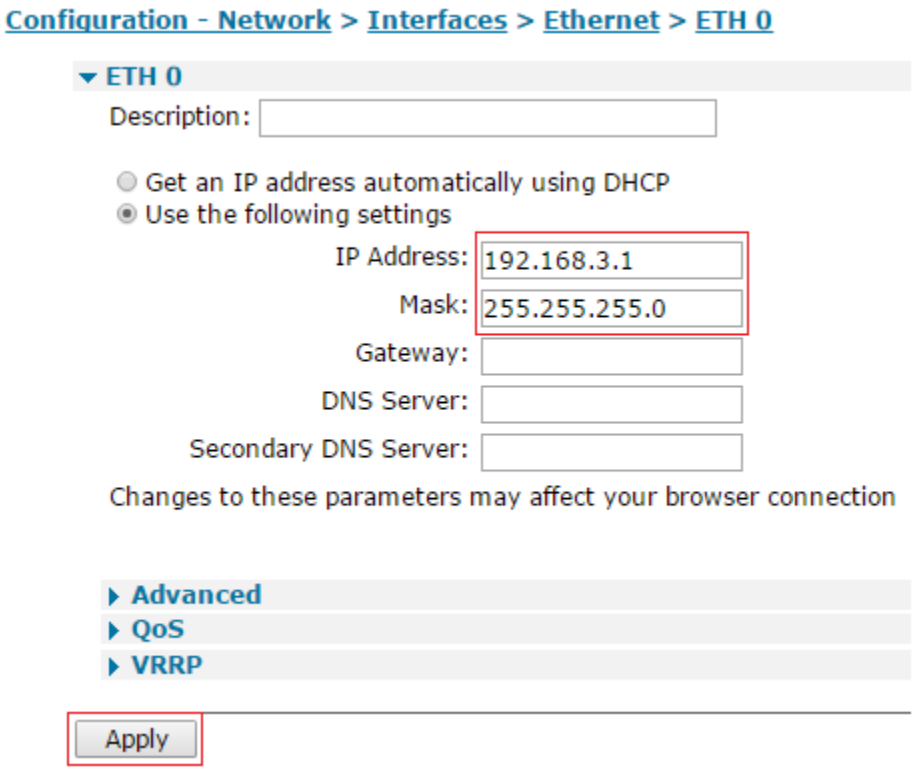
The failure and rollback will be simulated disconnecting/reconnecting the ETH cable on the AP and also disabling/enabling the Wi-Fi on the AP.

3 TRANSPORT ROUTER CONFIGURATION

In order to configure the TransPort, connect a PC to the ETHo of the TransPort and log into the web interface with a browser at the default address 192.168.1.1. Then follow the sections below.

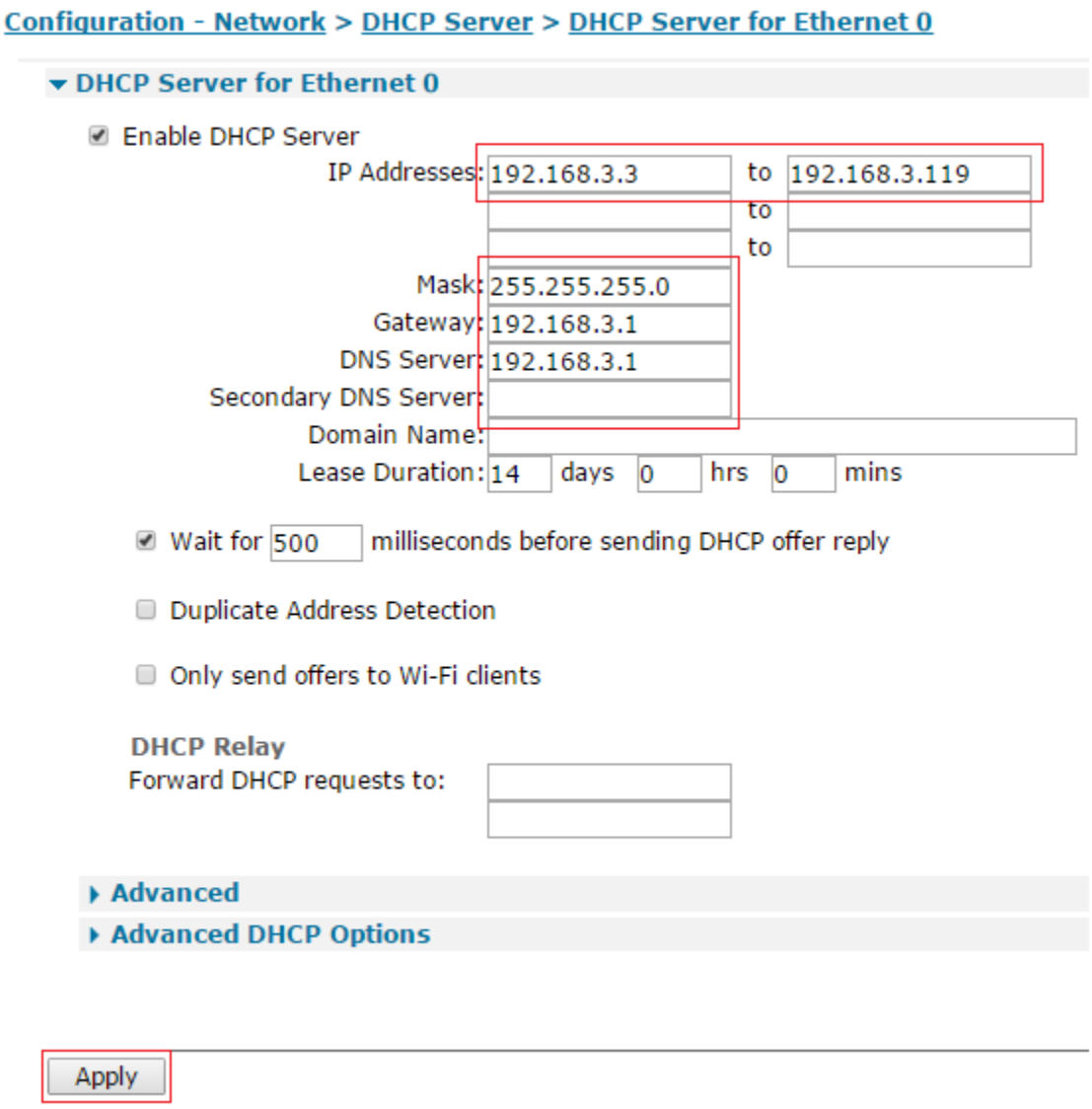
3.1 LAN Settings

In this AN the LAN interface of the TransPort is configured on ETH o and for setup purpose is set as 192.168.3.1/24 as IP address/Mask. The configuration can be changed going to the web interface at the section Configuration – Network > Interfaces > Ethernet > ETH o following the picture/table below:



Parameter	Setting	Description	CLI command
IP Address	192.168.3.1	Specifies the IP address of this Ethernet port	*eth o ipaddr 192.168.3.1*
Mask	255.255.255.0	Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port	*eth o mask 255.255.255.0*

Having changed the ETH o configuration respect to the default, also the DHCP server for ETH o should be changed as follows:



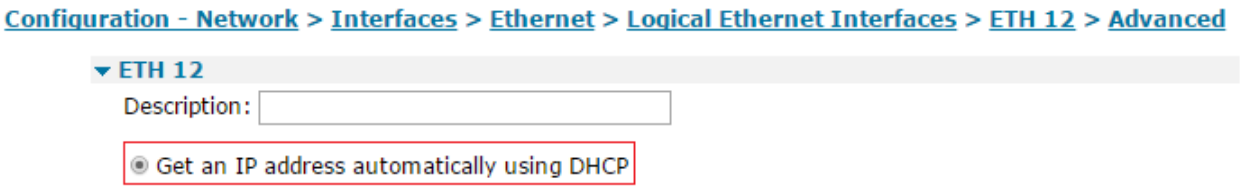
Parameter	Setting	Description	CLI command
IP Addresses <> to <>	192.168.3.3 to 192.168.3.119	The values in these specify the starting and ending addresses for the range of IP addresses that will be handed out by the DHCP server. Each of the three rows can be used to specify a different IP address pool, all pools should be within the same subnet	*dhcp o IPmin "192.168.3.3"* *dhcp o IPrange 117*
Mask	255.255.255.0	specifies the subnet mask used to on the network to which the router is connected	*dhcp o mask "255.255.255.0"*
Gateway	192.168.3.1	The value in this text box specifies the IP address of the gateway (which is usually the IP address of the router itself as configured by the IP address of the Ethernet interface associated with this DHCP instance).	*dhcp o gateway "192.168.3.1"*
DNS Server	192.168.3.1	The value in this text box specifies the IP address of the primary DNS server to be used by clients on the LAN. This will usually be the IP address of the route itself.	*dhcp o DNS "192.168.3.1"*

3.2 Primary WAN Settings: Wi-Fi

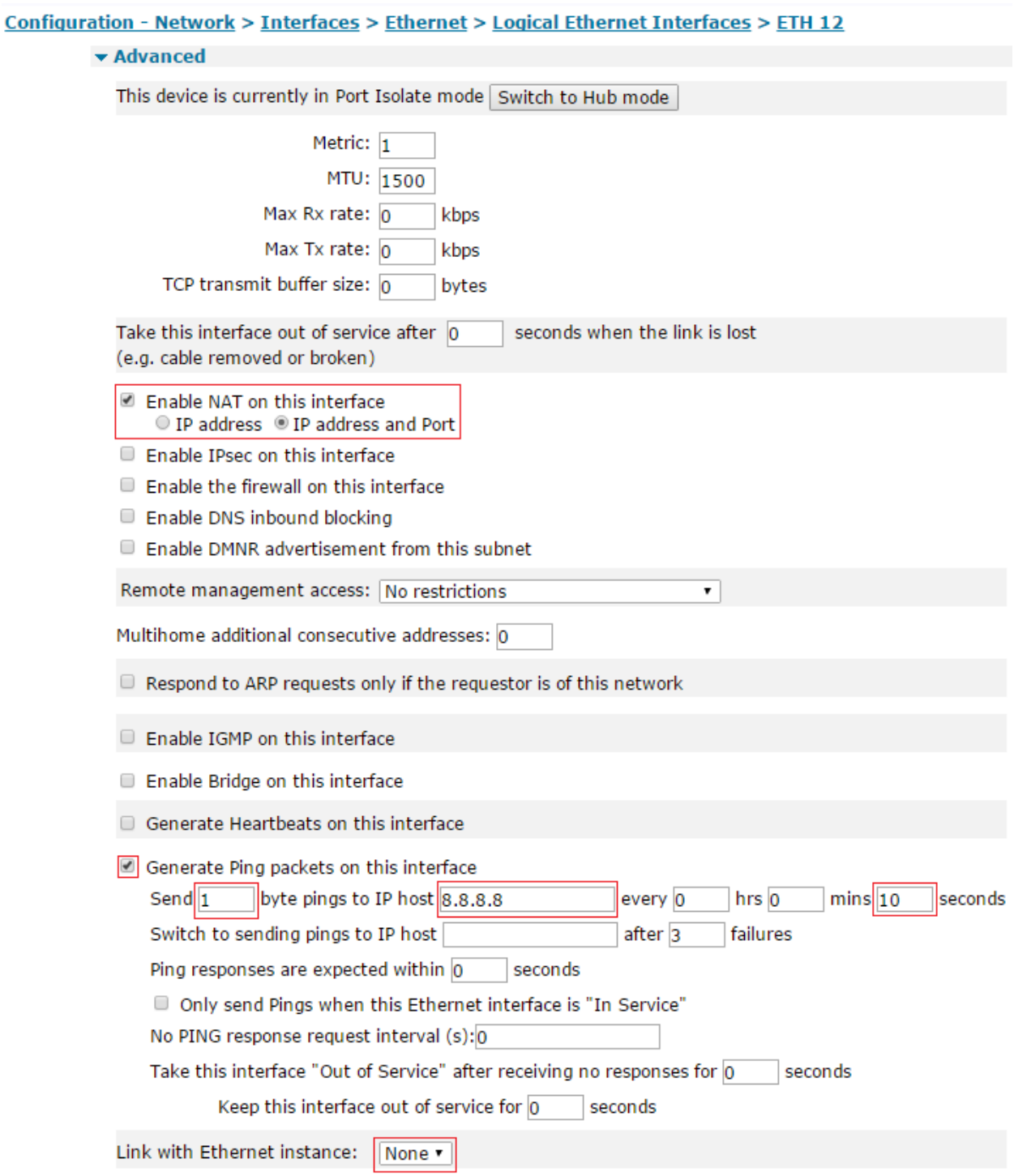
In this AN, the primary WAN connection is the Wi-Fi. In order to configure it, an ETH interface needs to be configured with DHCP client enabled and linked to the Wi-Fi interface set as Client mode. The following sub-sections will explains how to do this configuration.

3.2.1 Logical Ethernet Settings

In this AN, Logical Ethernet 12 has been used for the Wi-Fi connection. Basically, the ETH 12 interface will be configured in order to get the IP configuration via DHCP through the Wi-Fi client connection and to generate a periodic ping that will be used for the firewall monitoring of the link. In order to configure it, browse to **Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces > ETH 12 > Advanced**, follow the settings below, and then click the Apply button.



Parameter	Setting	Description	CLI command
Get an IP address automatically using DHCP	Selected	Selecting this option enables the DHCP client on this interface. The TransPort will get the IP configuration from the DHCP server through the Wi-Fi connection	*eth 12 dhcpcli "ON"*


Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces > ETH 12
Advanced
This device is currently in Port Isolate mode
Switch to Hub mode
Metric: 1
MTU: 1500
Max Rx rate: 0 kbps
Max Tx rate: 0 kbps
TCP transmit buffer size: 0 bytes
Take this interface out of service after 0 seconds when the link is lost
(e.g. cable removed or broken)
Enable NAT on this interface
IP address
IP address and Port
Enable IPsec on this interface
Enable the firewall on this interface
Enable DNS inbound blocking
Enable DMNR advertisement from this subnet
Remote management access: No restrictions
Multihome additional consecutive addresses: 0
Respond to ARP requests only if the requestor is of this network
Enable IGMP on this interface
Enable Bridge on this interface
Generate Heartbeats on this interface
Generate Ping packets on this interface
Send 1 byte pings to IP host 8.8.8.8 every 0 hrs 0 mins 10 seconds
Switch to sending pings to IP host after 3 failures
Ping responses are expected within 0 seconds
Only send Pings when this Ethernet interface is "In Service"
No PING response request interval (s): 0
Take this interface "Out of Service" after receiving no responses for 0 seconds
Keep this interface out of service for 0 seconds
Link with Ethernet instance: None

Parameter	Setting	Description	CLI command
Enable NAT on this interface	Selected / IP address and Port	As this Logical ETH will be the WAN interface, NAT needs to be enabled on it	*eth 12 do_nat "2"*
Link with Ethernet instance	None	This logical interface will be linked to the Wi-Fi node, so it should not be linked to an ETH instance	*eth 12 physadd "-1"*
Generate Ping packets on this interface	Ticked	This option will reveal the settings for ping generation on this interface. This ping will be used for the firewall monitoring	*N/A*
Send <n> byte pings	1	Size of ICMP packet to send	*eth 12 pingsiz "1"*
to IP host	<IP to ping>	Valid IP address to ping for link up/down testing.	*eth 12 pingip "8.8.8.8"*
Every	10 (seconds)	Interval in hours, minutes and seconds for the test pings to be sent	*eth 12 pingint "10"*

3.2.2 Global Wi-Fi Settings

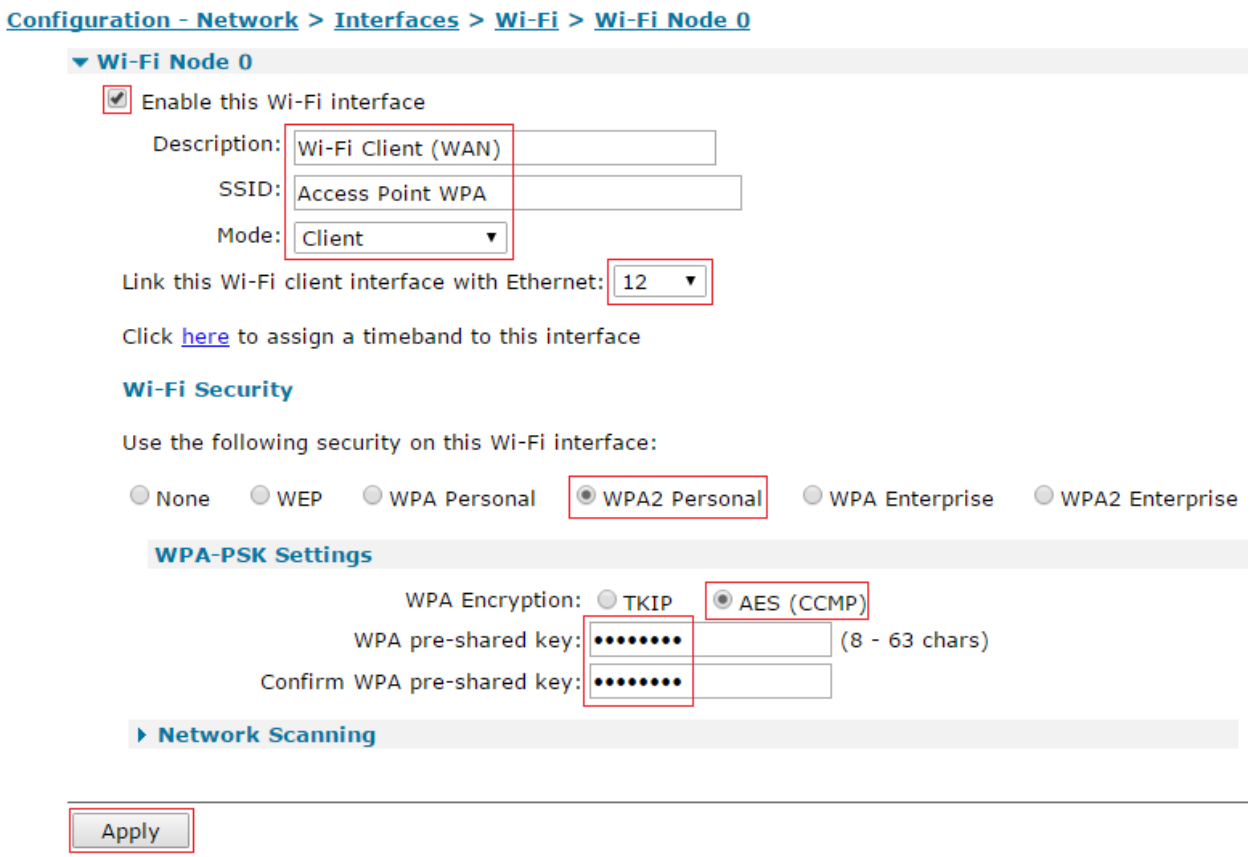
Browse to **Configuration - Network > Interfaces > Wi-Fi > Global Wi-Fi Settings** and follow the screenshot and table below to configure the general settings for the Wi-Fi Module, then click the Apply button.

Basically, only the "Country" field needs to be configured; the other settings can be left as default.

Parameter	Setting	Description	CLI command
Country	United States	Selecting a country from the drop down list will restrict the channels that the router will use. Refer to the Digi TransPort User Guide for more info on licensed channels.	*wifi o country "United States"*

3.2.3 Wi-Fi Node 0 Settings

In order to configure the Wi-Fi client settings, browse to **Configuration - Network > Interfaces > Wi-Fi > Wi-Fi Node 0** and refer to the following picture and table, then click Apply:

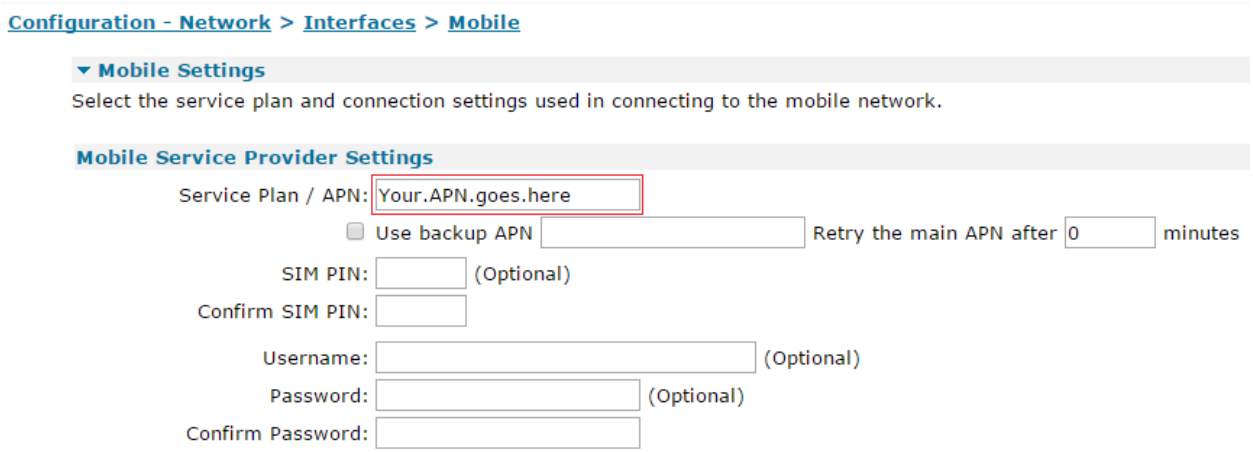


Parameter	Setting	Description	CLI command
Enable	Selected	Enable the Wi-Fi interface and reveals the options	---
Description	Wi-Fi Client (WAN)	A descriptive name for the Wi-Fi interface to make it easier to identify [optional]	*wifinode 0 descr "WiFi Client (WAN)"*
SSID		When the Wi-Fi interface is configured to be a Client, this is the SSID of the AP you wish to connect to	*wifinode 0 ssid "Access Point WPA"*
Mode	Client	Select the "Client" mode from the drop-down menu	*wifinode 0 mode "client"*
Link this Wi-Fi client	12	When the Wi-Fi interface is configured to	*eth 12 wificli*

interface with Ethernet <n>		be a client, it must be bridged to a particular Ethernet interface. In this AN ETH12 is the Ethernet interface used for the Wi-Fi Client.	*"ON"*
Use the following security on this Wi-Fi interface	WPA2 Personal	Selects the security that is used on this Wi-Fi interface. In this AN the AP to which the TransPort is connecting uses WPA2 Personal Security type	*wifinode 0 security "wpa2psk"*
WPA Encryption	AES (CCMP)	The encryption algorithm to use. The AP for this AN uses the AES (CCMP) algorithm	*wifinode 0 wpatype "aes"*
WPA Pre-Shared Key / Confirm	********	The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.	*wifinode 0 esharedkey "PDZxUoFFQFU="*

3.3 Backup WAN Settings: Cellular

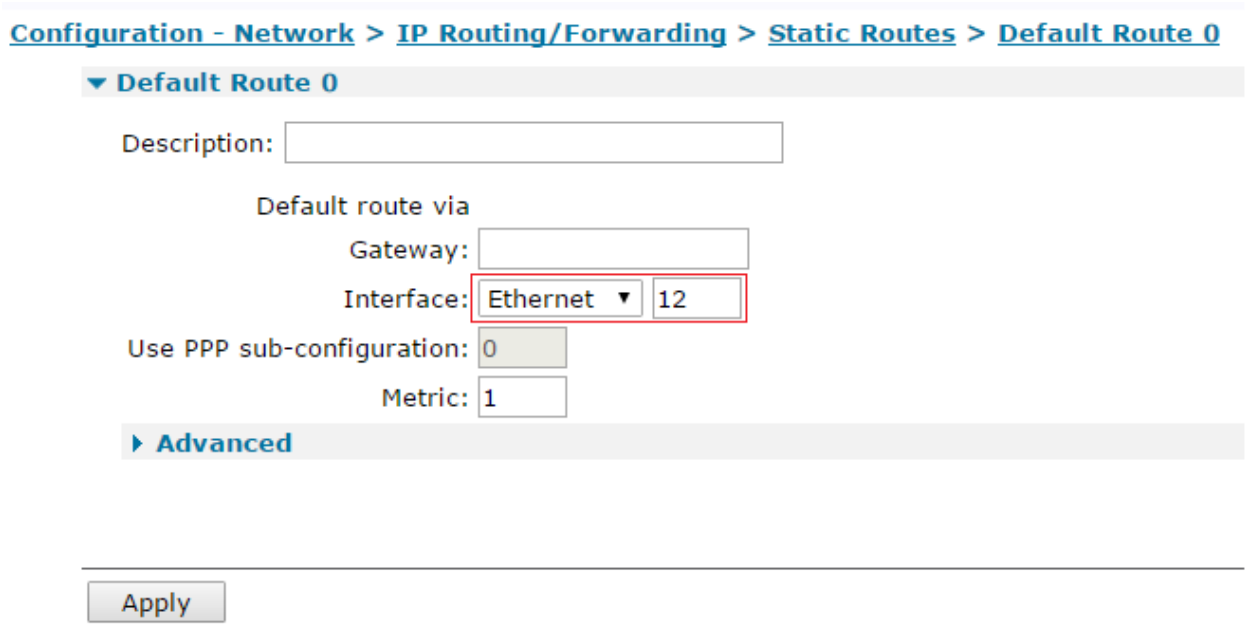
In order to configure the PPP interface that will act as Backup connection, browse to **Configuration - Network > Interfaces > Mobile** and go in the **Mobile Settings** section, then follow the settings/table below:



Parameter	Setting	Description	CLI command
Service Plan/APN	Your.APN.goes.here	Enter the APN (Access Point Name) given by the service provider.	*modemcc o apn "Your.APN.goes.here"*

3.4 Primary Default Route via Wi-Fi

Browse to **Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0** and set the primary route to point at ETH 12 as follows:

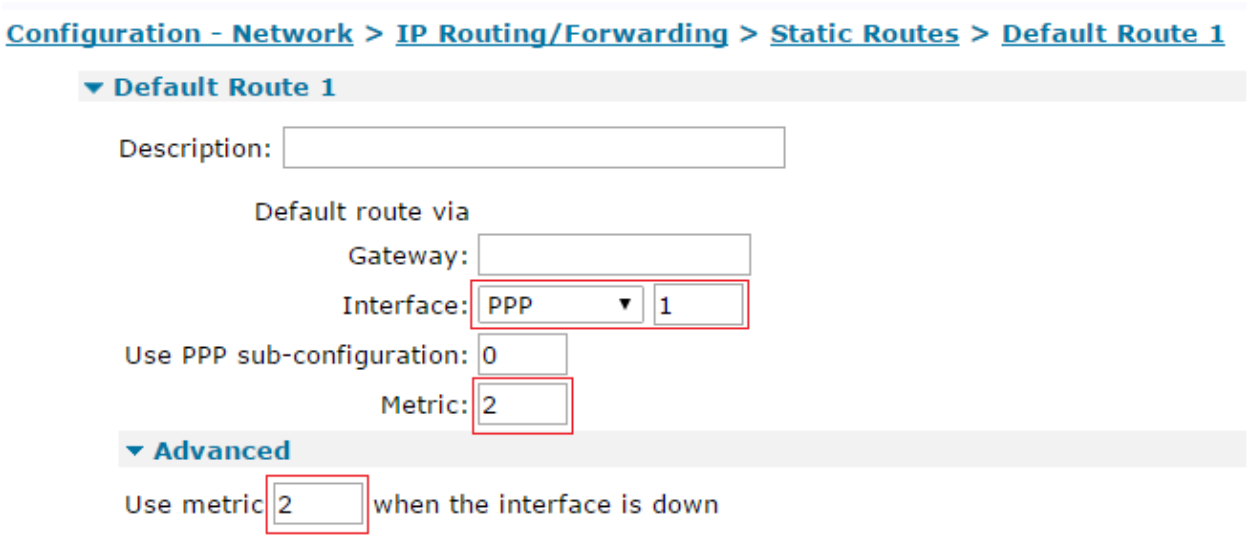


Click the Apply button.

Parameter	Setting	Description	CLI command
Interface	Ethernet 12	The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box	*def_route 0 ll_ent "ETH"* *def_route 0 ll_add "12"*

3.5 Backup Default Route via Cellular

Browse to **Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 1** and set the primary route to point at ETH 12 as follows:



Click the Apply button.

Parameter	Setting	Description	CLI command
Interface	PPP 1	The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box. This route is the backup via PPP 1.	*def_route 1 ll_ent "PPP"* *def_route 1 ll_add "1"*
Metric	2	The value in this text box is the routing metric to use when the interface is connected (connected metric). This should have a value between 1 and 16 and is used to select which route should be used when the subnet for a packet matches more than one of the IP route entries. As the route via PPP 1 is the backup, the metric needs to be higher than the primary, so set to 2.	*def_route 1 upmetric "2"*
Advanced > Use metric <> when the interface is down	2	The value in this text box specifies the routing metric to use when the interface is not active (disconnected metric). This is usually set equal to the connected metric.	*def_route 1 metric "2"*

3.6 Firewall Configuration

In order to enable the firewall monitoring on the primary link, a rule needs to be configured on the firewall. This rule has to match the periodic ping configured on the ETH 12; this will allow the firewall to detect the failure and put the ETH12 and the route as OOS (Out of Service) and also to detect the recovery, putting the ETH and route back in the UP state.

Please note that if the firewall is enabled just for this purpose, as in this example, it may be better to first add of all the following rules in order to not lose 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:

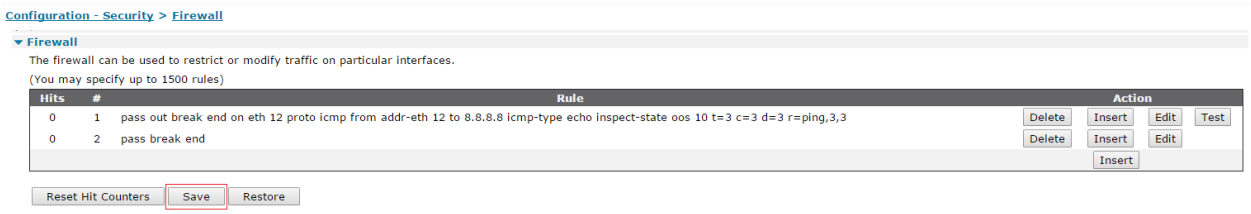
pass break end

Then click OK.

After that, click the "Insert" button to the right of the new first rule (which will add a new rule to the top), and type the following rule for the monitoring:

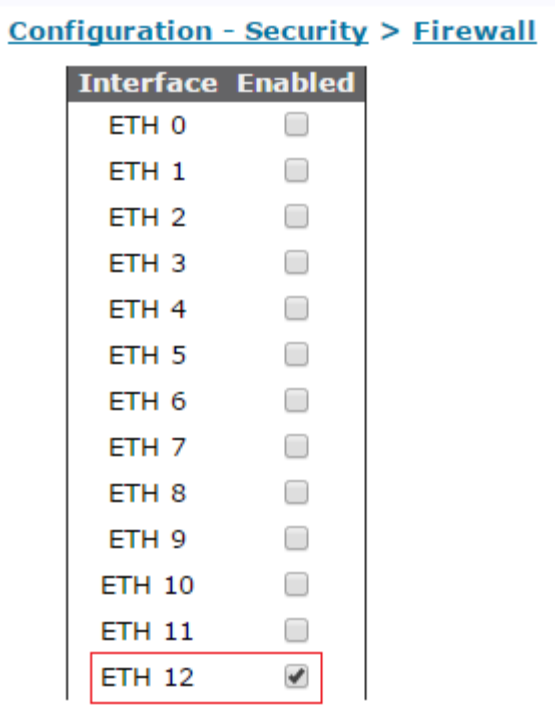
pass out break end on eth 12 proto icmp from addr-eth 12 to 8.8.8.8 icmp-type echo inspect-state oos 10 t=3 c=3 d=3 r=ping,3,3

Click OK, confirm the firewall rule looks like the image below, and then click the "Save" button.



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

In order to have this effectively applied, the firewall needs to be then enabled on the ETH 12 interface. To do this, scroll down to the Firewall configuration page to the Interface list and tick the boxes to enable the firewall on ETH 12, the click the Apply button:

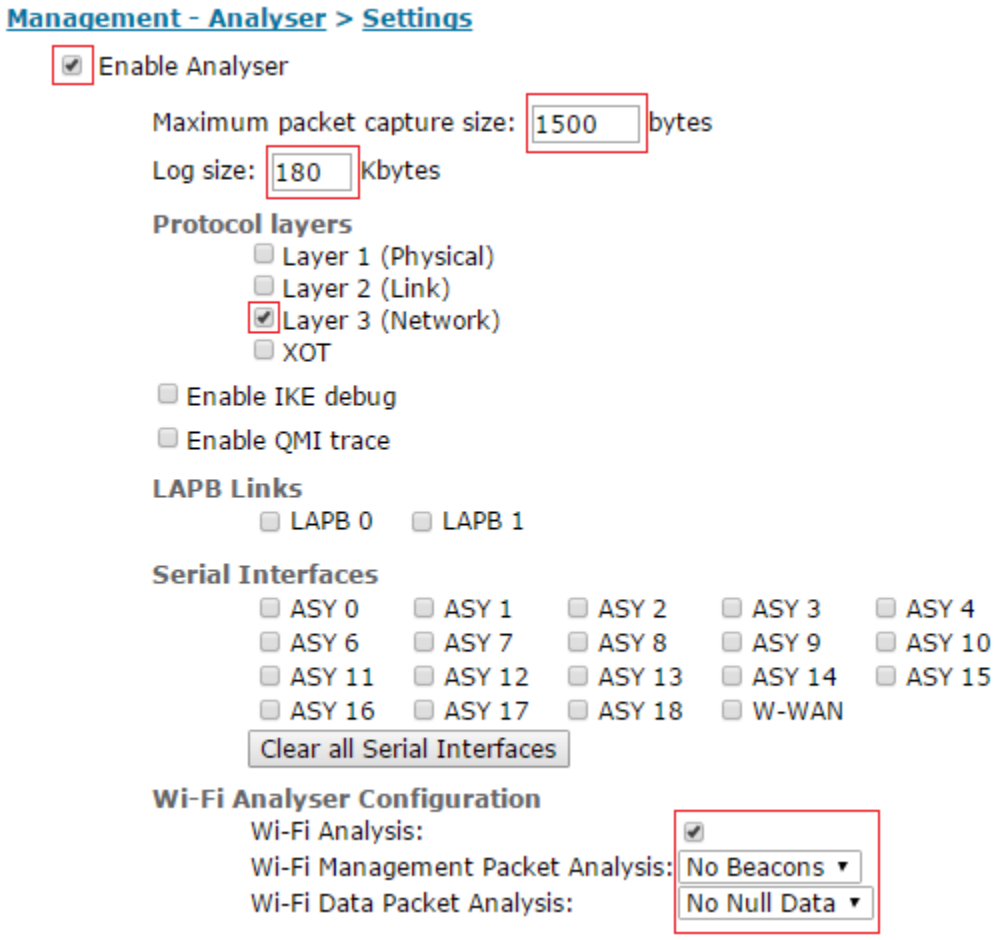

Configuration - Security > Firewall
Interface
Enabled
ETH 0
ETH 1
ETH 2
ETH 3
ETH 4
ETH 5
ETH 6
ETH 7
ETH 8
ETH 9
ETH 10
ETH 11
ETH 12

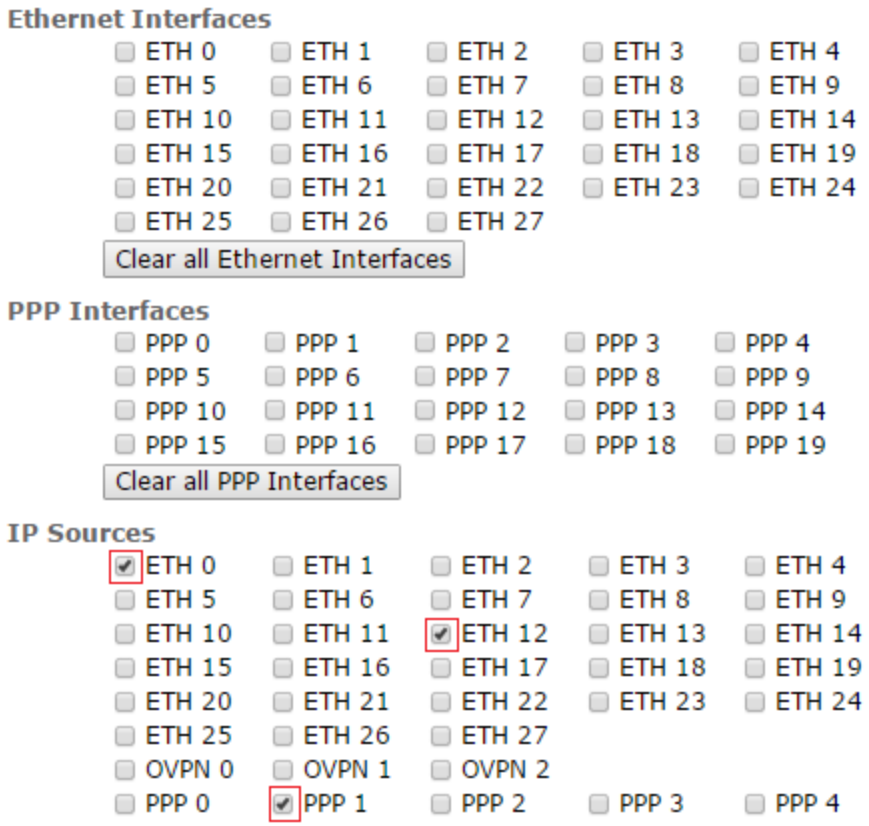
4 TESTING

4.1 Debug Settings on TransPort

In many cases, it is very useful configure the device to have a debug trace for the IKE negotiation in case of issues setting up the VPN, and to check that the traffic is correctly tunnelled.

On the TransPort, go to **Management - Analyser > Settings** and change the settings as shown below (uncheck everything else):





Click the Apply button.

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	*ana o logsize "180"*

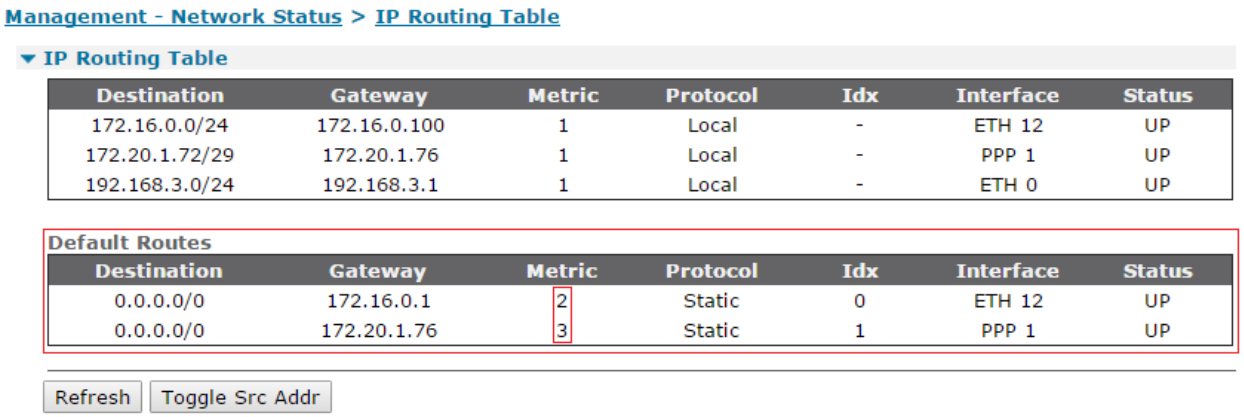
		of trace data will be captured.	
Protocol layers	Layer 3 (Network)	Specify which protocol layers are captured and included in the analyser trace. For the purpose of this AN the Network Layer (Layer 3) is chosen	*ana o "l3on"*
Wi-Fi analysis	Ticked	Enable the Wi-Fi trace on the module	*wifi o wifianon "ON"*
Wi-Fi management packer analysis	No beacons	Select the level of management packet analysis, in that case we need the trace only to check the routing of the data so we can avoid t have beacon frames in the trace	*wifi o anamgmt "nobeacons"*
Wi-Fi data packet analysis	No Null data	Select the level of datapacket analysis, in that case we need the trace only to check the routing of the data (Ping) so we can avoid t have null data frames in the trace	*wifi o anadata "nonull"*
IP Sources	ETH 0 ETH 12 PPP 1	Select the IP sources over which packets will be captured and included in the analyser trace	*eth 0 ipanon "on"* *eth 12 ipanon "on"* *ppp 1 ipanon "on"*

4.2 Testing Failover with Firewall Monitoring: AP's WAN Failure

In this section, a simple test of the failover mechanism and rollback using the firewall monitoring will be provided. In order to perform it, a laptop connected to the LAN interface of the TransPort is needed.

4.2.1 Normal Condition: Primary Route Active

Once the Wi-Fi client is connected to the AP, the routing table should look like the following, showing that the primary route is the one pointing to ETH 12. In the routing table, the backup route to PPP 1 is also shown (as UP), and it will be not used while the primary is UP due to metric priority.



In order to check if the traffic is effectively routed through the primary route via Wi-Fi, an easy method is to make a ping to an Internet address from a laptop connected to the LAN interface of the TransPort and then check the TransPort Analyser trace by browsing to: **Management - Analyser > Trace**.

The trace will show that the ICMP ECHO REQ is received on ETH 0, routed to ETH 12, correctly "NAT'ed" and then finally transmitted via the Wi-Fi module:

```
-----   11-12-2014  12:39:13.690   -----
   45 00 00 3C 0B 2C 00 00 80 01 5F DD C0 A8 03 04     E..<.,...._.....
   08 08 04 04 08 00 4D 41 00 01 00 1A 61 62 63 64     ......MA....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
   0B 2C          ID:            2860
   00 00          Frag Offset:   0
```

```
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   80             TTL:           128
   01             Proto:         ICMP
   5F DD          Checksum:      24541
   C0 A8 03 04    Src IP:        192.168.3.4
   08 08 04 04    Dst IP:        8.8.8.8
   ICMP:
   08             Type:          ECHO REQ
   00             Code:          0
   4D 41          Checksum:      19777
   ----------
-----   11-12-2014  12:39:13.690   -----
45 00 00 3C 0B 2C 00 00 7F 01 62 7C C0 A8 01 65     E..<.,....b|...e
08 08 04 04 08 00 4D 41 00 01 00 1A 61 62 63 64     ......MA....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 12
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
0B 2C          ID:            2860
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
7F             TTL:           127
01             Proto:         ICMP
62 7C          Checksum:      25212
C0 A8 01 65    Src IP:        192.168.1.101
08 08 04 04    Dst IP:        8.8.8.8
ICMP:
08             Type:          ECHO REQ
00             Code:          0
4D 41          Checksum:      19777
----------
-----   11-12-2014  12:39:13.690   -----
08 41 28 00 04 F0 21 0C 9B 18 00 0E 8E 23 14 85     .A(...!......#..
00 04 2D 04 B4 4C E0 05 00 20 5B 20 00 00 00 00     ..-..L... [ ....
AA AA 03 00 00 00 08 00 45 00 00 3C 0B 2C 00 00     ........E..<.,..
7F 01 62 7C C0 A8 01 65 08 08 04 04 08 00 4D 41     ..b|...e......MA
00 01 00 1A 61 62 63 64 65 66 67 68 69 6A 6B 6C     ....abcdefghijkl
6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65     mnopqrstuvwabcde
66 67 68 69                                         fghi

Wi-Fi From LOC To REM                       IFACE: Wi-Fi Module 0
08 41                  Version:             0
                       Type:                Data
                       Subtype:             Data
                       Flags:               STA -> AP, Protected
28 00                  Duration:            40
04 F0 21 0C 9B 18      BSS ID
00 0E 8E 23 14 85      Src. MAC
00 04 2D 04 B4 4C      Dst. MAC
05 E0                  Fragment:            0
                       Sequence:            94
00 20 5B 20 00 00 00 00  TKIP Security Param
AA AA 03 00 00 00      LLC SNAP
08 00                  Type:                IP
IP:
45             IP Ver:        4
```

```
              Hdr Len:       20
00            TOS:           Routine
              Delay:         Normal
              Throughput:    Normal
              Reliability:   Normal
00 3C         Length:        60
0B 2C         ID:            2860
00 00         Frag Offset:   0
              Congestion:    Normal
                             May Fragment
                             Last Fragment
7F            TTL:           127
01            Proto:         ICMP
62 7C         Checksum:      25212
C0 A8 01 65   Src IP:        192.168.1.101
08 08 04 04   Dst IP:        8.8.8.8
----------
```

Then, the ECHO REPLY is received via the Wi-Fi module on ETH 12 and routed back to ETH 0:

```
   -----   11-12-2014  12:39:13.700   -----
   08 02 2C 00 00 0E 8E 23 14 85 04 F0 21 0C 9B 18     ..,....#....!...
   00 04 2D 04 B4 4C 10 10 AA AA 03 00 00 00 08 00     ..-..L..........
   45 00 00 3C 3D AB 00 00 34 01 7A FD 08 08 04 04     E..<=...4.z.....
   C0 A8 01 65 00 00 55 41 00 01 00 1A 61 62 63 64     ...e..UA....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 B1 29 06 80     uvwabcdefghi.)..
   15 AF D0 9B                                         ....

   Wi-Fi From REM To LOC                       IFACE: Wi-Fi Module 0
   08 02                    Version:           0
                            Type:              Data
                            Subtype:           Data
                            Flags:             AP -> STA
   2C 00                    Duration:          44
   00 0E 8E 23 14 85        Dst. MAC
   04 F0 21 0C 9B 18        BSS ID
   00 04 2D 04 B4 4C        Src. MAC
   10 10                    Fragment:          0
                            Sequence:          257
   AA AA 03 00 00 00        LLC SNAP
   08 00                    Type:              IP
   IP:
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   3D AB          ID:            15787
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   34             TTL:           52
   01             Proto:         ICMP
   7A FD          Checksum:      31485
   08 08 04 04    Src IP:        8.8.8.8
   C0 A8 01 65    Dst IP:        192.168.1.101
   ----------
   -----   11-12-2014  12:39:13.700   -----
   45 00 00 3C 3D AB 00 00 34 01 7A FD 08 08 04 04     E..<=...4.z.....
   C0 A8 01 65 00 00 55 41 00 01 00 1A 61 62 63 64     ...e..UA....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 B1 29 06 80     uvwabcdefghi.)..
   15 AF D0 9B                                         ....

   IP (In) From REM TO LOC       IFACE: ETH 12
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   3D AB          ID:            15787
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   34             TTL:           52
   01             Proto:         ICMP
   7A FD          Checksum:      31485
   08 08 04 04    Src IP:        8.8.8.8
   C0 A8 01 65    Dst IP:        192.168.1.101
   ICMP:
   00             Type:          ECHO REPLY
   00             Code:          0
   55 41          Checksum:      21825
   ----------
-----   11-12-2014  12:39:13.700   -----
45 00 00 3C 3D AB 00 00 32 01 7B 5E 08 08 04 04     E..<=...2.{^....
C0 A8 03 04 00 00 55 41 00 01 00 1A 61 62 63 64     ......UA....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
3D AB          ID:            15787
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
32             TTL:           50
01             Proto:         ICMP
7B 5E          Checksum:      31582
08 08 04 04    Src IP:        8.8.8.8
C0 A8 03 04    Dst IP:        192.168.3.4
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
55 41          Checksum:      21825
```

4.2.2 Failure on Access Point WAN Connection

In order to test the failover to Cellular using firewall monitoring, an easy way is to simulate the failure of the AP, for example by disconnecting the WAN connection of it.

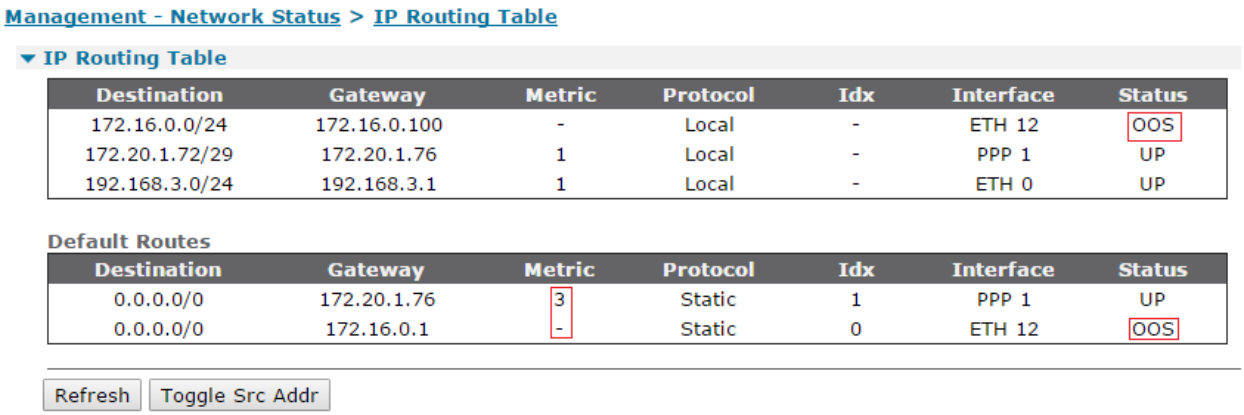
In this AN, the AP is also a TransPort, with ETH WAN connectivity, so disconnecting the ETH cable will simulate the failure, as the Client will be not able to reach the outside network. As already explained,

this kind of failure cannot be detected without the firewall monitoring, as, for the client, the Wi-Fi connection to the AP is still UP (and so the primary route on the routing table), but actually it has no more connection to Internet.

To do the test, disconnect the ETH cable on the AP and then check the TransPort Event Log by navigating to **Management - Event Log**:

```
11:56:39, 29 Jul 2016,Default Route 0 Out Of Service,Firewall
11:56:39, 29 Jul 2016,ETH 12 Out Of Service,Firewall
```

The Event Log shows that the Firewall monitoring fails and so the ETH12 and the Primary route are set to OOS. Also by checking the routing table, it shows that the primary route is now OOS, and so the default route that will be used now is the PPP one:



Management - Network Status > IP Routing Table

IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.16.0.0/24	172.16.0.100	-	Local	-	ETH 12	OOS
172.20.1.72/29	172.20.1.76	1	Local	-	PPP 1	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	172.20.1.76	3	Static	1	PPP 1	UP
0.0.0.0/0	172.16.0.1	-	Static	0	ETH 12	OOS

Refresh | Toggle Src Addr

To check that the traffic is been routed via the backup Cellular connection, make, as before, a ping from a laptop connected to the LAN interface of the TransPort to an Internet address and check the Analyser trace navigating to **Management - Analyser > Trace**.

The trace will show that the ICMP ECHO REQ is received on ETH 0, routed and transmitted through PPP 1, correctly "NAT'ed":

```
-----   11-12-2014  12:40:41.000   -----
 45 00 00 3C 13 ED 00 00 80 01 57 1C C0 A8 03 04     E..<......W.....
 08 08 04 04 08 00 4D 3F 00 01 00 1C 61 62 63 64     ......M?....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
   13 ED          ID:            5101
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   80             TTL:           128
   01             Proto:         ICMP
   57 1C          Checksum:      22300
   C0 A8 03 04    Src IP:        192.168.3.4
   08 08 04 04    Dst IP:        8.8.8.8
   ICMP:
   08             Type:          ECHO REQ
   00             Code:          0
   4D 3F          Checksum:      19775
   ----------
-----   11-12-2014  12:40:41.000   -----
45 00 00 3C 13 ED 00 00 7F 01 F5 36 25 54 01 3E     E..<.......6%T.>
08 08 04 04 08 00 4D 3F 00 01 00 1C 61 62 63 64     ......M?....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
13 ED          ID:            5101
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
7F             TTL:           127
01             Proto:         ICMP
F5 36          Checksum:      62774
25 54 01 3E    Src IP:        37.84.1.62
08 08 04 04    Dst IP:        8.8.8.8
ICMP:
08             Type:          ECHO REQ
00             Code:          0
4D 3F          Checksum:      19775
----------
```

Then, the ECHO REPLY is received via PPP 1 and routed back to ETH 0:

```
   -----   11-12-2014  12:40:41.060   -----
   45 00 00 3C 56 EA 00 00 2E 01 03 3A 08 08 04 04     E..<V......:....
   25 54 01 3E 00 00 55 3F 00 01 00 1C 61 62 63 64     %T.>..U?....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
```

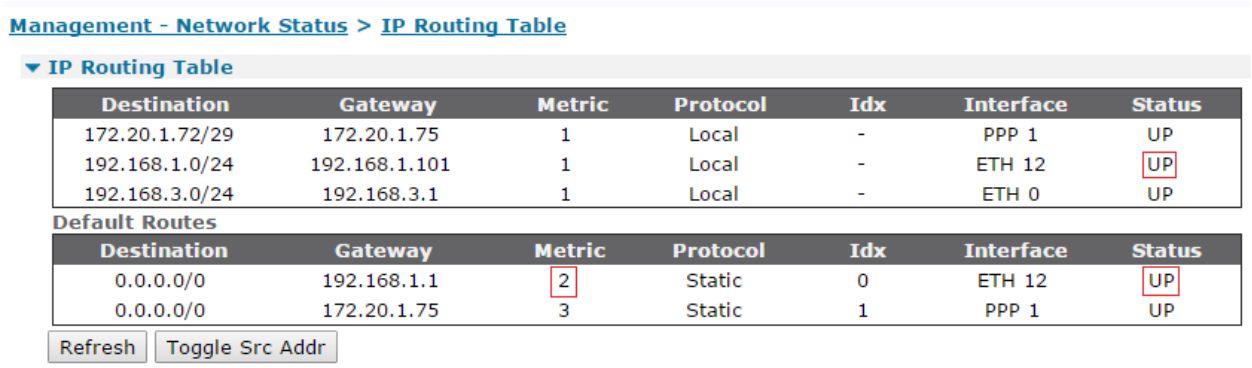
```
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   56 EA          ID:            22250
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   2E             TTL:           46
   01             Proto:         ICMP
   03 3A          Checksum:      826
   08 08 04 04    Src IP:        8.8.8.8
   25 54 01 3E    Dst IP:        37.84.1.62
   ICMP:
   00             Type:          ECHO REPLY
   00             Code:          0
   55 3F          Checksum:      21823
   ----------
-----   11-12-2014  12:40:41.060   -----
45 00 00 3C 56 EA 00 00 2C 01 68 1F 08 08 04 04     E..<V...,.h.....
C0 A8 03 04 00 00 55 3F 00 01 00 1C 61 62 63 64     ......U?....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
56 EA          ID:            22250
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
2C             TTL:           44
01             Proto:         ICMP
68 1F          Checksum:      26655
08 08 04 04    Src IP:        8.8.8.8
C0 A8 03 04    Dst IP:        192.168.3.4
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
55 3F          Checksum:      21823
----------
```

4.2.3 Recovery and Rollback to Wi-Fi

In order to simulate the recovery of the fault, reconnect the ETH cable on the AP and check the Event Log again.

```
12:00:59, 29 Jul 2016,Default Route 0 Available,Oos timer
12:00:59, 29 Jul 2016,ETH 12 Available,Recovery
12:00:59, 29 Jul 2016,ETH 12 Recovery Completed,PING
```

The Event Log will show that the PING recovery is performed by the firewall and that the ETH 12 and the Primary Route go back UP. It can also be checked looking at the routing table:



Management - Network Status > IP Routing Table

IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	1	Local	-	ETH 12	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	192.168.1.1	2	Static	0	ETH 12	UP
0.0.0.0/0	172.20.1.75	3	Static	1	PPP 1	UP

Refresh | Toggle Src Addr

Performing again the ping from the laptop on the LAN, the trace will show that the traffic is now routed again on the Primary Link:

```
-----   11-12-2014  12:43:32.510   -----
   45 00 00 3C 16 4B 00 00 80 01 54 BE C0 A8 03 04     E..<.K....T.....
   08 08 04 04 08 00 4D 3E 00 01 00 1D 61 62 63 64     ......M>....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
   16 4B          ID:            5707
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   80             TTL:           128
   01             Proto:         ICMP
   54 BE          Checksum:      21694
   C0 A8 03 04    Src IP:        192.168.3.4
   08 08 04 04    Dst IP:        8.8.8.8
   ICMP:
   08             Type:          ECHO REQ
```

```
   00             Code:          0
   4D 3E          Checksum:      19774
   ----------
-----   11-12-2014  12:43:32.510   -----
45 00 00 3C 16 4B 00 00 7F 01 57 5D C0 A8 01 65     E..<.K....W]...e
08 08 04 04 08 00 4D 3E 00 01 00 1D 61 62 63 64     ......M>....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 12
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
16 4B          ID:            5707
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
7F             TTL:           127
01             Proto:         ICMP
57 5D          Checksum:      22365
C0 A8 01 65    Src IP:        192.168.1.101
08 08 04 04    Dst IP:        8.8.8.8
ICMP:
08             Type:          ECHO REQ
00             Code:          0
4D 3E          Checksum:      19774
----------
-----   11-12-2014  12:43:32.510   -----
08 41 28 00 04 F0 21 0C 9B 18 00 0E 8E 23 14 85     .A(...!......#..
00 04 2D 04 B4 4C F0 08 00 20 8C 20 00 00 00 00     ..-..L... . ....
AA AA 03 00 00 00 08 00 45 00 00 3C 16 4B 00 00     ........E..<.K..
7F 01 57 5D C0 A8 01 65 08 08 04 04 08 00 4D 3E     ..W]...e......M>
00 01 00 1D 61 62 63 64 65 66 67 68 69 6A 6B 6C     ....abcdefghijkl
6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65     mnopqrstuvwabcde
66 67 68 69                                         fghi

Wi-Fi From LOC To REM                    IFACE: Wi-Fi Module 0
08 41                  Version:          0
                       Type:             Data
                       Subtype:          Data
                       Flags:            STA -> AP, Protected
28 00                  Duration:         40
04 F0 21 0C 9B 18      BSS ID
00 0E 8E 23 14 85      Src. MAC
00 04 2D 04 B4 4C      Dst. MAC
08 F0                  Fragment:         0
                       Sequence:         143
00 20 8C 20 00 00 00 00  TKIP Security Param
AA AA 03 00 00 00      LLC SNAP
08 00                  Type:             IP
IP:
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
16 4B          ID:            5707
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
```

```
                              Last Fragment
7F              TTL:          127
01              Proto:        ICMP
57 5D           Checksum:     22365
C0 A8 01 65     Src IP:       192.168.1.101
08 08 04 04     Dst IP:       8.8.8.8
----------
```

And also the reply:

```
   -----   11-12-2014  12:43:32.520   -----
   08 02 2C 00 00 0E 8E 23 14 85 04 F0 21 0C 9B 18     ..,....#....!...
   00 04 2D 04 B4 4C 10 11 AA AA 03 00 00 00 08 00     ..-..L..........
   45 00 00 3C 3E 4D 00 00 34 01 7A 5B 08 08 04 04     E..<>M..4.z[....
   C0 A8 01 65 00 00 55 3E 00 01 00 1D 61 62 63 64     ...e..U>....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 AA 01 A3 09     uvwabcdefghi....
   31 19 A4 2C                                         1..,

   Wi-Fi From REM To LOC                          IFACE: Wi-Fi Module 0
   08 02                    Version:              0
                            Type:                 Data
                            Subtype:              Data
                            Flags:                AP -> STA
   2C 00                    Duration:             44
   00 0E 8E 23 14 85        Dst. MAC
   04 F0 21 0C 9B 18        BSS ID
   00 04 2D 04 B4 4C        Src. MAC
   11 10                    Fragment:             0
                            Sequence:             273
   AA AA 03 00 00 00        LLC SNAP
   08 00                    Type:                 IP
   IP:
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   3E 4D          ID:            15949
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   34             TTL:           52
   01             Proto:         ICMP
   7A 5B          Checksum:      31323
   08 08 04 04    Src IP:        8.8.8.8
   C0 A8 01 65    Dst IP:        192.168.1.101
   ----------
   -----   11-12-2014  12:43:32.520   -----
   45 00 00 3C 3E 4D 00 00 34 01 7A 5B 08 08 04 04     E..<>M..4.z[....
   C0 A8 01 65 00 00 55 3E 00 01 00 1D 61 62 63 64     ...e..U>....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 AA 01 A3 09     uvwabcdefghi....
   31 19 A4 2C                                         1..,

   IP (In) From REM TO LOC        IFACE: ETH 12
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
```

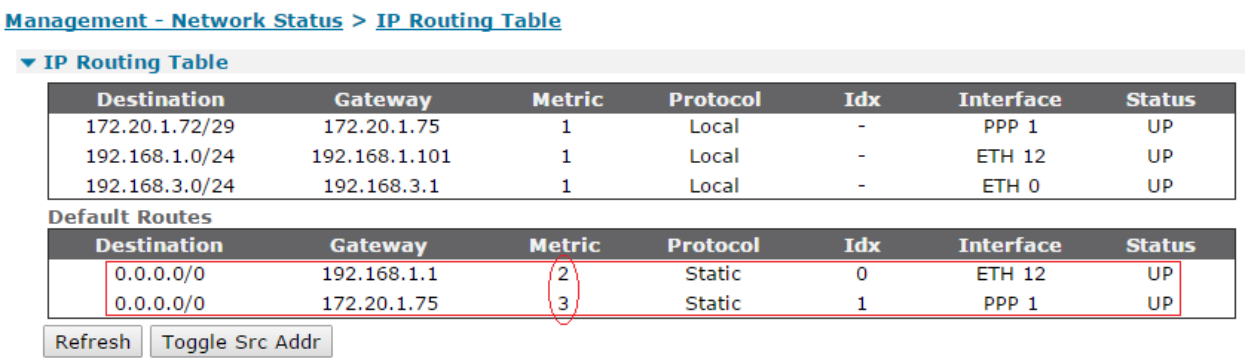
```
   00 3C          Length:        60
   3E 4D          ID:            15949
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   34             TTL:           52
   01             Proto:         ICMP
   7A 5B          Checksum:      31323
   08 08 04 04    Src IP:        8.8.8.8
   C0 A8 01 65    Dst IP:        192.168.1.101
   ICMP:
   00             Type:          ECHO REPLY
   00             Code:          0
   55 3E          Checksum:      21822
   ----------
-----   11-12-2014  12:43:32.520   -----
45 00 00 3C 3E 4D 00 00 32 01 7A BC 08 08 04 04     E..<>M..2.z.....
C0 A8 03 04 00 00 55 3E 00 01 00 1D 61 62 63 64     ......U>....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
3E 4D          ID:            15949
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
32             TTL:           50
01             Proto:         ICMP
7A BC          Checksum:      31420
08 08 04 04    Src IP:        8.8.8.8
C0 A8 03 04    Dst IP:        192.168.3.4
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
55 3E          Checksum:      21822
----------
```

4.3 Testing Failover without Firewall Monitoring: Wi-Fi Link Failure

This section will demonstrate how the failover is performed in case of a failure on the Wi-Fi connection.

This kind of failure will not use the firewall monitoring, so in order to have it working, Section 3.6 and the "Generate Ping" settings of Section 3.2 1 are optional. But if present, as in this example, these optional settings should not cause issues.

As shown in section 4.2.1, once the Wi-Fi client is connected to the AP, the routing table should look like the following, showing that the primary route is the one pointing to ETH 12. In the routing table, the backup route to PPP 1 (which is UP) will be not used while the primary is UP due to metric priority.


Management - Network Status > IP Routing Table

IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	1	Local	-	ETH 12	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	192.168.1.1	2	Static	0	ETH 12	UP
0.0.0.0/0	172.20.1.75	3	Static	1	PPP 1	UP

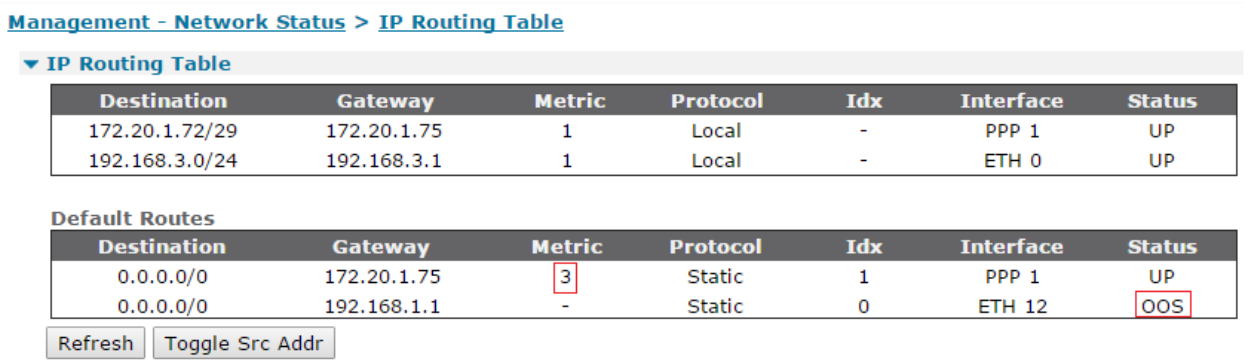
Refresh Toggle Src Addr

In this condition, the traffic is routed to the Primary Wi-Fi connection.

When a failure on the Wi-Fi link occurs, for example disabling the Wi-Fi on the AP side, the ETH 12 and the primary route will go immediately OOS (again, without using the firewall monitoring) and the Event Log should look like the following:

```
12:21:23, 29 Jul 2016,Default Route 0 Out Of Service,Activation
12:21:23, 29 Jul 2016,ETH 12 Out Of Service,Activation
12:21:23, 29 Jul 2016,Wi-Fi client 0 probing Access Point WPA
12:21:23, 29 Jul 2016,Wi-Fi Node 0 disconnected from Access Point WPA,Remote out of
range
```

The routing table will now look like this (and so the traffic will pass through the PPP link):


Management - Network Status > IP Routing Table

IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	172.20.1.75	3	Static	1	PPP 1	UP
0.0.0.0/0	192.168.1.1	-	Static	0	ETH 12	OOS

Refresh Toggle Src Addr

Enabling again the Wi-Fi on the AP side will bring UP ETH 12 and the primary route. In this case, the Event Log and the routing table will look like the following:

```
12:28:21, 29 Jul 2016,Default Route 0 Available,Oos timer
12:28:13, 29 Jul 2016,ETH 12 Available,Activation
12:28:07, 29 Jul 2016,Wi-Fi Node 0 connected to Access Point WPA, RSSI:66
12:28:03, 29 Jul 2016,Wi-Fi client 0 probing Access Point WPA
```

Management - Network Status > IP Routing Table

▼ IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	1	Local	-	ETH 12	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	192.168.1.1	2	Static	0	ETH 12	UP
0.0.0.0/0	172.20.1.75	3	Static	1	PPP 1	UP

Refresh Toggle Src Addr

5 TRANSPORT CONFIGURATION FILES

5.1 Configuration File

This is the configuration used on the TransPort in this AN; relevant CLI lines are highlighted:

```
Command: config c show
Command result

wifi 0 country "United States"
wifinode 0 descr "Wi-Fi Client (WAN)"
wifinode 0 ssid "Access Point WPA"
wifinode 0 mode "client"
wifinode 0 security "wpa2psk"
wifinode 0 wpatype "aes"
wifinode 0 esharedkey "********"
eth 0 IPaddr "192.168.3.1"
eth 12 dhcpcli ON
eth 12 mask ""
eth 12 do_nat 2
eth 12 firewall ON
eth 12 pingip "8.8.8.8"
eth 12 pingint 10
eth 12 pingsiz 1
eth 12 wificli ON
eth 12 physadd -1
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 "ETH"
def_route 0 ll_add 12
def_route 1 ll_ent "PPP"
def_route 1 ll_add 1
def_route 1 upmetric 2
def_route 1 metric 2
dhcp 0 IPmin "192.168.3.3"
dhcp 0 IPrange 117
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.3.1"
dhcp 0 DNS "192.168.3.1"
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"
snmp 0 v1enable OFF
snmp 0 v2cenable OFF
snmp 0 v3enable OFF
services 0 telnet OFF
services 0 http OFF
services 0 https ON
services 0 ssh OFF
services 0 ftp OFF
services 0 asytcp OFF
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*5#"
ppp 1 epassword "KD5lSVJDVVg="
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 pwr_dly 40
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpcli 0 hostname "ftp1.digi.com"
ftpcli 0 directory "support/firmware/transport/MC7354_carrier_firmware"
modemcc 0 info_asy_add 7
modemcc 0 apn "Your.APN.goes.here"
modemcc 0 link_retries 30
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 30
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
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 tremto 1200
user 0 access 0
user 1 name "username"
user 1 epassword "********"
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
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
cloud 0 ssl ON

Power Up Profile: 0
OK
```

5.2 Firewall Rules

The firewall rules used in this AN are the following:

```
pass out break end on eth 12 proto icmp from addr-eth 12  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
```

5.3 Hardware and Firmware

The hardware and firmware used for this AN are reported below:

```
Command: ati5
Command result

Digi TransPort WR44-L500-NE1-SU Ser#:xxxxxx HW Revision: 2202a
Software Build Ver5.2.15.4.  Jun 22 2016 12:24:12  LW
ARM Bios Ver 7.56u v45 800MHz B995-M1003-F80-O0,0 MAC:00042d080153
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Wi-Fi                     Revision: 2.0
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
MySQL                     Revision: 0.01
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
ARM Sync Driver            Revision: 1.18
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 (SIERRA LTE)      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
```