Application Note 70

Wi-Fi-to-Cellular Failover

Digi Technical Support

October 2016
Contents

1 Introduction ........................................................................................................................................ 3
  1.1 Outline ......................................................................................................................................... 3
  1.2 Assumptions .................................................................................................................................. 3
  1.3 Corrections .................................................................................................................................... 4
  1.4 Version ......................................................................................................................................... 4
2 Scenario ............................................................................................................................................. 4
3 TransPort Router Configuration .......................................................................................................... 5
  3.1 LAN Settings ................................................................................................................................ 5
  3.2 Primary WAN Settings: Wi-Fi ......................................................................................................... 8
    3.2.1 Logical Ethernet Settings ........................................................................................................ 8
    3.2.2 Global Wi-Fi Settings ............................................................................................................. 11
    3.2.3 Wi-Fi Node 0 Settings ............................................................................................................. 12
  3.3 Backup WAN Settings: Cellular ..................................................................................................... 14
  3.4 Primary Default Route via Wi-Fi ..................................................................................................... 15
  3.5 Backup Default Route via Cellular ................................................................................................. 16
  3.6 Firewall Configuration .................................................................................................................... 17
4 Testing .................................................................................................................................................. 19
  4.1 Debug Settings on TransPort ......................................................................................................... 19
  4.2 Testing Failover with Firewall Monitoring: AP’s WAN Failure ...................................................... 22
    4.2.1 Normal Condition: Primary Route Active .............................................................................. 22
    4.2.2 Failure on Access Point WAN Connection ............................................................................ 25
    4.2.3 Recovery and Rollback to Wi-Fi ............................................................................................. 29
  4.3 Testing Failover without Firewall Monitoring: Wi-Fi Link Failure ............................................... 33
5 TransPort Configuration Files ........................................................................................................... 35
  5.1 Configuration File .......................................................................................................................... 35
  5.2 Firewall Rules ................................................................................................................................ 37
  5.3 Hardware and Firmware .................................................................................................................. 37
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

<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>
<tr>
<td>1.1</td>
<td>Updated screenshots and instructions for new web interface, rebranding (July 2016)</td>
</tr>
</tbody>
</table>

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 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 ETH0 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 ETH0 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 > ETH0 following the picture/table below:

<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>192.168.3.1</td>
<td>Specifies the IP address of this Ethernet port</td>
<td><code>eth o ipaddr 192.168.3.1</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>
Having changed the ETH 0 configuration respect to the default, also the DHCP server for ETH 0 should be changed as follows:

**Configuration - Network > DHCP Server > DHCP Server for Ethernet 0**

- **Enable DHCP Server**
  - IP Addresses: 192.168.3.3 to 192.168.3.119
  - Mask: 255.255.255.0
  - Gateway: 192.168.3.1
  - DNS Server: 192.168.3.1
  - Secondary DNS Server: 
  - Domain Name: 
  - Lease Duration: 14 days 0 hrs 0 mins

- **Wait for 500 milliseconds before sending DHCP offer reply**
- **Duplicate Address Detection**
- **Only send offers to Wi-Fi clients**

**DHCP Relay**
- Forward DHCP requests to: 

**Advanced**
- **Advanced DHCP Options**

---

Apply
Wi-Fi to Cellular Failover

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
</table>
| IP Addresses    | 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 explain 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.

<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>Selected</td>
<td>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.</td>
<td><code>eth 12 dhcpcli &quot;ON&quot;</code></td>
</tr>
</tbody>
</table>
### Wi-Fi to Cellular Failover

#### Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces > ETH 12

- **Advanced**

  - 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 hours 0 minutes 1.0 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]

---

Page | 9
## Wi-Fi to Cellular Failover

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NAT on this interface</td>
<td>Selected / IP address and Port</td>
<td>As this Logical ETH will be the WAN interface, NAT needs to be enabled on it</td>
<td><code>eth 12 do_nat “2”</code></td>
</tr>
<tr>
<td>Link with Ethernet instance</td>
<td>None</td>
<td>This logical interface will be linked to the Wi-Fi node, so it should not be linked to an ETH instance</td>
<td><code>eth 12 physadd “-1”</code></td>
</tr>
<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. This ping will be used for the firewall monitoring</td>
<td>N/A</td>
</tr>
<tr>
<td>Send &lt;n&gt; byte pings to IP host</td>
<td>1</td>
<td>Size of ICMP packet to send</td>
<td><code>eth 12 pingsiz “1”</code></td>
</tr>
<tr>
<td></td>
<td>&lt;IP to ping&gt;</td>
<td>Valid IP address to ping for link up/down testing.</td>
<td><code>eth 12 pingip “8.8.8.8”</code></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><code>eth 12 pingint “10”</code></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>United States</td>
<td>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.</td>
<td><code>wifi 0 country “United States”</code></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Selected</td>
<td>Enable the Wi-Fi interface and reveals the options</td>
<td>---</td>
</tr>
<tr>
<td>Description</td>
<td>Wi-Fi Client (WAN)</td>
<td>A descriptive name for the Wi-Fi interface to make it easier to identify [optional]</td>
<td><code>wifinode o descr &quot;WiFi Client (WAN)&quot;</code></td>
</tr>
<tr>
<td>SSID</td>
<td></td>
<td>When the Wi-Fi interface is configured to be a Client, this is the SSID of the AP you wish to connect to</td>
<td><code>wifinode o ssid &quot;Access Point WPA&quot;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Client</td>
<td>Select the “Client” mode from the drop-down menu</td>
<td><code>wifinode o mode &quot;client&quot;</code></td>
</tr>
<tr>
<td>Link this Wi-Fi client</td>
<td>12</td>
<td>When the Wi-Fi interface is configured to</td>
<td><code>eth 12 wificli</code></td>
</tr>
<tr>
<td>Interface with Ethernet &lt;n&gt;</td>
<td>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.</td>
<td>“ON”</td>
<td></td>
</tr>
<tr>
<td>Use the following security on this Wi-Fi interface</td>
<td>WPA2 Personal</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>WPA Encryption</td>
<td>AES (CCMP)</td>
<td>The encryption algorithm to use. The AP for this AN uses the AES (CCMP) algorithm</td>
<td></td>
</tr>
<tr>
<td>WPA Pre-Shared Key / Confirm</td>
<td>*******</td>
<td>The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.</td>
<td></td>
</tr>
</tbody>
</table>

Use the following security on this Wi-Fi interface:
- WPA2 Personal
- AES (CCMP)

The pre-shared key (PSK) to use. It must be between 8 and 63 characters long:
```
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:

<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>Your.APN.goes.here</td>
<td>Enter the APN (Access Point Name) given by the service provider.</td>
<td><code>modem cc o apn &quot;Your.APN.goes.here&quot;</code></td>
</tr>
</tbody>
</table>
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:

![Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0](image)

Click the **Apply** button.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
</table>
| 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 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.

![Firewall Rule Configuration](image)

**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:
Wi-Fi to Cellular Failover

**Configuration - Security > Firewall**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH 0</td>
<td></td>
</tr>
<tr>
<td>ETH 1</td>
<td></td>
</tr>
<tr>
<td>ETH 2</td>
<td></td>
</tr>
<tr>
<td>ETH 3</td>
<td></td>
</tr>
<tr>
<td>ETH 4</td>
<td></td>
</tr>
<tr>
<td>ETH 5</td>
<td></td>
</tr>
<tr>
<td>ETH 6</td>
<td></td>
</tr>
<tr>
<td>ETH 7</td>
<td></td>
</tr>
<tr>
<td>ETH 8</td>
<td></td>
</tr>
<tr>
<td>ETH 9</td>
<td></td>
</tr>
<tr>
<td>ETH 10</td>
<td></td>
</tr>
<tr>
<td>ETH 11</td>
<td></td>
</tr>
<tr>
<td>ETH 12</td>
<td>✔️</td>
</tr>
</tbody>
</table>
4 TESTING

4.1 Debug Settings on TransPort

In many cases, it is very useful to 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):

**Management - Analyser > Settings**

- Enable Analyser
- Maximum packet capture size: **1500** bytes
- Log size: **180** Kbytes
- Protocol layers:
  - Layer 1 (Physical)
  - Layer 2 (Link)
  - Layer 3 (Network)
  - XOT
- Enable IKE debug
- Enable QMI trace

**LAPB Links**

- LAPB 0  
- LAPB 1

**Serial Interfaces**

- ASY 0  
- ASY 1  
- ASY 2  
- ASY 3  
- ASY 4  
- ASY 6  
- ASY 7  
- ASY 8  
- ASY 9  
- ASY 10  
- ASY 11  
- ASY 12  
- ASY 13  
- ASY 14  
- ASY 15  
- ASY 16  
- ASY 17  
- ASY 18  
- W-WAN

**Clear all Serial Interfaces**

**Wi-Fi Analyser Configuration**

- Wi-Fi Analysis:
- Wi-Fi Management Packet Analysis: **No Beacons**
- Wi-Fi Data Packet Analysis: **No Null Data**
Click the Apply button.

<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><code>ana o anon &quot;ON&quot;</code></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><code>ana o maxdata &quot;1500&quot;</code></td>
</tr>
<tr>
<td>Log Size</td>
<td>180</td>
<td>The maximum size of the pseudo file &quot;ana.txt&quot; 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</td>
<td><code>ana o logsize &quot;180&quot;</code></td>
</tr>
</tbody>
</table>
### Wi-Fi to Cellular Failover

| 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 wifion "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 "nonnull"
| 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.

<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>172.16.0.0/24</td>
<td>172.16.0.100</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 12</td>
<td>UP</td>
</tr>
<tr>
<td>172.20.1.72/29</td>
<td>172.20.1.76</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>192.168.3.1</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 0</td>
<td>UP</td>
</tr>
</tbody>
</table>

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:
Wi-Fi to Cellular Failover

<table>
<thead>
<tr>
<th>Congestion: Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>May Fragment</td>
</tr>
<tr>
<td>Last Fragment</td>
</tr>
<tr>
<td>00</td>
</tr>
<tr>
<td>TTL:</td>
</tr>
<tr>
<td>128</td>
</tr>
<tr>
<td>01</td>
</tr>
<tr>
<td>Proto: ICMP</td>
</tr>
<tr>
<td>5F DD</td>
</tr>
<tr>
<td>Checksum: 24541</td>
</tr>
<tr>
<td>C0 A8 03 04</td>
</tr>
<tr>
<td>Src IP: 192.168.3.4</td>
</tr>
<tr>
<td>08 08 04 04</td>
</tr>
<tr>
<td>Dst IP: 8.8.8.8</td>
</tr>
</tbody>
</table>

ICMP:
| 08 Type: ECHO REQ |
| 00 Code: 0         |
| 4D 41 Checksum: 19777 |

IP (Final) From LOC TO REM IFACE: ETH 12
| 45 IP Ver: 4 |
| 00 Hdr Len: 20 |
| 00 TOS: Routine |
| 00 Delay: Normal |
| 00 Throughput: Normal |
| 00 Reliability: Normal |
| 00 3C Length: 60 |
| 08 2C ID: 2860 |
| 00 00 Frag Offset: 0 |
| Congestion: Normal |

IP Ver: 4

| Version: 0 |
| Type: Data |
| Subtype: Data |
| Flags: STA -> AP, Protected |
| Duration: 48 |

TKIP Security Param

IP:
| 45 IP Ver: 4 |
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  ..-.........  
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 00 1A 61 62 63 64  ...e..UA....abcd  
75 76 77 61 62 63 64 65 66 67 68 69 81 29 06 80  uvwabcdefghi)...)  
15 AF D0 9B  ....  

Wi-Fi From REM To LOC  
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  
LiC 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 00 1A 61 62 63 64  ...e..UA....abcd
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,
Wi-Fi to Cellular Failover

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 |

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**

<table>
<thead>
<tr>
<th>IP Routing Table</th>
<th>Gateway</th>
<th>Metric</th>
<th>Protocol</th>
<th>Idx</th>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.0/24</td>
<td>172.16.0.100</td>
<td>-</td>
<td>Local</td>
<td>-</td>
<td>ETH 12</td>
<td>OOS</td>
</tr>
<tr>
<td>172.20.1.72/29</td>
<td>172.20.1.76</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>192.168.3.1</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 0</td>
<td>UP</td>
</tr>
</tbody>
</table>

**Default Routes**

<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>0.0.0.0/0</td>
<td>172.20.1.76</td>
<td>3</td>
<td>Static</td>
<td>1</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>172.16.0.1</td>
<td>-</td>
<td>Static</td>
<td>0</td>
<td>ETH 12</td>
<td>OOS</td>
</tr>
</tbody>
</table>

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 03 13 ED 00 00 80 01 57 1C C0 A8 03 04     E..<......W.....
08 08 04 04 08 00 4D 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 78 61 62 63 64 65 66 67 68 69             uwabcdefghi

IP (In) From REM TO LOC IFACE: ETH 0
45  IP Ver:  4
Hdr Len: 20
00  TOS:  Routine
Delay: Normal
Throughput: Normal
Then, the ECHO REPLY is received via PPP 1 and routed back to ETH 0:
Wi-Fi to Cellular Failover

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   -----   E..<V...,h......
45 00 00 3C 56 EA 00 00 2C 01 68 1F 08 08 04 04  ......U?....abcd
c0 a8 03 04 00 00 55 3F 00 01 00 1C 61 62 63 64  efgihklmnopqrst
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 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**

<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>172.20.1.72/29</td>
<td>172.20.1.75</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>192.168.1.101</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 12</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>192.168.3.1</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 0</td>
<td>UP</td>
</tr>
</tbody>
</table>

**Default Routes**

<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>0.0.0.0/0</td>
<td>192.168.1.1</td>
<td>2</td>
<td>Static</td>
<td>0</td>
<td>ETH 12</td>
<td>UP</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>172.20.1.75</td>
<td>3</td>
<td>Static</td>
<td>1</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
</tbody>
</table>

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 48 00 00 08 01 54 BE C0 A8 03 04   E..<K....T....
08 08 04 04 08 00 0D 3E 00 01 00 0D 61 62 63 64   ......M>......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   uwwwabcddefghi

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
00 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
```
Wi-Fi to Cellular Failover

IP (Final) From LOC TO REM
IFACE: ETH 12

<table>
<thead>
<tr>
<th>Code</th>
<th>Length</th>
<th>ID</th>
<th>Type</th>
<th>Seq</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>08</td>
<td>00</td>
<td>04</td>
<td>04</td>
<td>00</td>
<td>40</td>
</tr>
</tbody>
</table>

IP:
- Ver: 4
- Hdr Len: 20
- TOS: Routine
- Delay: Normal
- Throughput: Normal
- Reliability: Normal

Checksum: 19774

Wi-Fi From LOC To REM
IFACE: Wi-Fi Module 0

<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Subtype</th>
<th>Flags</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>08</td>
<td>41</td>
<td>Data</td>
<td>STA</td>
<td>40</td>
</tr>
</tbody>
</table>

Version: 0
Type: Data
Subtype: Data
Flags: STA -> AP, Protected

TKIP Security Param

Checksum: 19774
Wi-Fi to Cellular Failover

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 | Version: | 0 |
00 0E | Type: | Data |
| 0E | Subtype: | Data |
| 00 | Flags: | AP -> STA |
| 2C 00 | Duration: | 44 |
| 00 0E | Dst. MAC | 8E 23 14 05 |
| 04 | BSS ID | F0 21 0C 98 18 |
| 00 04 | Src. MAC | 04 B4 4C |
| 11 10 | Fragment: | 0 |
| AA AA 03 00 00 00 | Sequence: | 273 |
| 08 00 | LLC SNAP | 0 |

Wi-Fi From REM To LOC | IFACE: Wi-Fi Module 0

| 08 02 | IP Ver: | 4 |
| 00 | Hdr Len: | 20 |
| 00 | TOS: | Routine |
| 00 | Delay: | Normal |
| 00 | Throughput: | Normal |
| 00 3C | Reliability: | Normal |
| 3E 4D | Length: | 60 |
| 00 | ID: | 15949 |
| 00 00 | Frag Offset: | 0 |
| 00 | Congestion: | Normal |
| 34 | May Fragment | 52 |
| 01 | TTL: | 52 |
| 7A 5B | Proto: | ICMP |
| 08 08 04 04 | Src IP: | 192.168.1.101 |

------ 11-12-2014 12:43:32.520 ------

IP (In) From REM TO LOC | IFACE: ETH 12

| 45 | IP Ver: | 4 |
| 00 | Hdr Len: | 20 |
| 00 | TOS: | Routine |
| 00 | Delay: | Normal |
| 00 | Throughput: | Normal |
| 00 | Reliability: | Normal |
Wi-Fi to Cellular Failover

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 01 00 0D 61 62 63 64 .........abcd
65 66 67 68 69 6A 68 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](image)

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, 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](image)
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**

<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>172.20.1.72/29</td>
<td>172.20.1.75</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.1.24</td>
<td>192.168.1.101</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 12</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.3.24</td>
<td>192.168.3.1</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 0</td>
<td>UP</td>
</tr>
</tbody>
</table>

**Default Routes**

<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>0.0.0.0/0</td>
<td>192.168.1.1</td>
<td>2</td>
<td>Static</td>
<td>0</td>
<td>ETH 12</td>
<td>UP</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>172.20.1.75</td>
<td>3</td>
<td>Static</td>
<td>1</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
</tbody>
</table>
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 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
snpt 0 dstonmon 3
snpt 0 dstonday 13
snpt 0 dstoffmon 11
snpt 0 dstoffday 6
```
Wi-Fi to Cellular Failover

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 "KD5lSVJIVg="
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 sm_interval 1
modemcc 0 sm_access 1
modemcc 0 sm_concat 0
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 30
modemcc 0 stat_retries_2 30
modemcc 0 sm_interval_2 1
modemcc 0 sm_access_2 1
modemcc 0 sm_concat_2 0
ana 0 anon ON
ana 0 x2on 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%>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
user 0 access 0
user 1 name "username"
user 1 epassword "*******"
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:

<table>
<thead>
<tr>
<th>Command: ati5</th>
<th>Command result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digi TransPort WR44-L500-NE1-SU Ser#:xxxxxx HW Revision: 2202a</td>
<td></td>
</tr>
<tr>
<td>Software Build Ver5.2.15.4. Jun 22 2016 12:24:12 LW</td>
<td></td>
</tr>
<tr>
<td>ARM Bios Ver 7.56u v45 800MHz B995-M1003-F00-00,0 MAC:00042d080153</td>
<td></td>
</tr>
<tr>
<td>Power Up Profile: 0</td>
<td></td>
</tr>
<tr>
<td>Async Driver</td>
<td>Revision: 1.19 Int clk</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Revision: 2.0</td>
</tr>
<tr>
<td>Ethernet Port Isolate Driver</td>
<td>Revision: 1.11</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>MySQL</td>
<td>Revision: 0.01</td>
</tr>
<tr>
<td>RealPort</td>
<td>Revision: 0.00</td>
</tr>
<tr>
<td>Component</td>
<td>Revision</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>MultiTX</td>
<td>1.00</td>
</tr>
<tr>
<td>LAPB</td>
<td>1.12</td>
</tr>
<tr>
<td>X25 Layer</td>
<td>1.19</td>
</tr>
<tr>
<td>MACRO</td>
<td>1.0</td>
</tr>
<tr>
<td>PAD</td>
<td>1.4</td>
</tr>
<tr>
<td>X25 Switch</td>
<td>1.7</td>
</tr>
<tr>
<td>V120</td>
<td>1.16</td>
</tr>
<tr>
<td>TPAD Interface</td>
<td>1.12</td>
</tr>
<tr>
<td>GPS</td>
<td>1.0</td>
</tr>
<tr>
<td>TELITUPD</td>
<td>1.0</td>
</tr>
<tr>
<td>SCRIBATSK</td>
<td>1.0</td>
</tr>
<tr>
<td>BASTSK</td>
<td>1.0</td>
</tr>
<tr>
<td>PYTHON</td>
<td>1.0</td>
</tr>
<tr>
<td>CLOUDSMS</td>
<td>1.0</td>
</tr>
<tr>
<td>ARM Sync Driver</td>
<td>1.18</td>
</tr>
<tr>
<td>TCP (HASH mode)</td>
<td>1.14</td>
</tr>
<tr>
<td>TCP Utils</td>
<td>1.13</td>
</tr>
<tr>
<td>PPP</td>
<td>5.2</td>
</tr>
<tr>
<td>WEB</td>
<td>1.5</td>
</tr>
<tr>
<td>SMTP</td>
<td>1.1</td>
</tr>
<tr>
<td>FTP Client</td>
<td>1.5</td>
</tr>
<tr>
<td>FTP</td>
<td>1.4</td>
</tr>
<tr>
<td>IKE</td>
<td>1.0</td>
</tr>
<tr>
<td>PollANS</td>
<td>1.2</td>
</tr>
<tr>
<td>PPPOE</td>
<td>1.0</td>
</tr>
<tr>
<td>BRIDGE</td>
<td>1.1</td>
</tr>
<tr>
<td>MODEM CC (SIERRA LTE)</td>
<td>5.2</td>
</tr>
<tr>
<td>FLASH Write</td>
<td>1.2</td>
</tr>
<tr>
<td>Command Interpreter</td>
<td>1.38</td>
</tr>
<tr>
<td>SSLCLI</td>
<td>1.0</td>
</tr>
<tr>
<td>OSPF</td>
<td>1.0</td>
</tr>
<tr>
<td>BGP</td>
<td>1.0</td>
</tr>
<tr>
<td>QOS</td>
<td>1.0</td>
</tr>
<tr>
<td>PWRCTRL</td>
<td>1.0</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>1.0</td>
</tr>
<tr>
<td>SSH Server</td>
<td>1.0</td>
</tr>
<tr>
<td>SCP</td>
<td>1.0</td>
</tr>
<tr>
<td>SSH Client</td>
<td>1.0</td>
</tr>
<tr>
<td>CERT</td>
<td>1.0</td>
</tr>
<tr>
<td>LowPrio</td>
<td>1.0</td>
</tr>
<tr>
<td>Tunnel</td>
<td>1.2</td>
</tr>
<tr>
<td>OVPN</td>
<td>1.2</td>
</tr>
<tr>
<td>TEMPLOG</td>
<td>1.0</td>
</tr>
<tr>
<td>QDL</td>
<td>1.0</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>