

Application Note 055

WiFi to Cellular Failover

July 2015

Contents

1	Intr	oduction					
	1.1	Outline					
	1.2	Assumptions					
	1.3	Corrections					
	1.4	Version					
2	Scei	nario					
3	Digi	TransPort router configuration					
	3.1	LAN Settings					
	3.2	Primary WAN Settings: WiFi					
	3.2.	1 Logical Ethernet Settings					
	3.2.	2 Global Wi-Fi Settings					
	3.2.	3 WiFi Node 0 Settings					
	3.3	Backup WAN Settings: Cellular12					
	3.4	Primary Default Route via WiFi12					
	3.5	Backup default Route via Cellular13					
	3.6	Firewall Configuration14					
4	Test	ting1(
	4.1	Debug settings on TransPort16					
	4.2	Testing Failover with Firewall Monitoring: AP's WAN failure18					
	4.2.	1 Normal condition: Primary Route active18					
	4.2.	2 Failure on Access Point WAN connection					
	4.2.	3 Recovery and rollback to WiFi25					
	4.3	Testing failover without Firewall Monitoring: WiFi link failure					
5	Trar	nsPort Configuration files					
	5.1	Configuration File					
	5.2	Firewall Rules					
	5.3	Hardware and Firmware					

1 INTRODUCTION

1.1 Outline

This Application Note gives a guide on configuring a TransPort router to have a WAN connection through WiFi 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 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 WiFi connection to the AP wil 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 WiFi itself. In that case, the primary route will go Out Of Service/back online due to the failure/rollback of WiFi 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 Digi TransPort can be connected working Access Point that can provide Internet access.

Models shown: Digi TransPort WR44

Other Compatible Models: All other Digi TransPort products with WIFi features.

Firmware versions: All Versions

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

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com

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

1.4 Version

Version Number	Status
0.1	Draft
1.0	Completed 7/2015

2 SCENARIO

This application note will consider the following scenario:



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

3 DIGI TRANSPORT ROUTER CONFIGURATION

In order to configure the Digi TransPort, connect a PC to the ETHO of the TransPort and log into the Web User Interface (WebUI) with a browser at the default address **192.168.1.1**. Then follow the sections below.

3.1 LAN Settings

In this AN the LAN interface of the Transport is configured on ETH 0 and for setup purpose is set as 192.168.3.1/24 as IP address/Mask. The configuration can be changed going to the WEB UI at the section **Configuration – Network > Interfaces > Ethernet > ETH 0** following the picture/table below:

' Inte	erfaces
▼ Ei	thernet
•	ETH 0
	Description:
	\bigcirc Get an IP address automatically using DHCP
	Use the following settings
	IP Address: 192.168.3.1
	Mask: 255.255.255.0
	Gateway:
	DNS Server:
	Secondary DNS Server:
	Changes to these parameters may affect your browser connection
	Advanced
	V V V V V V V V V V V V V V V V V V V
	/ YIMF

Figure 3.1-1: LAN settings

Parameter	Setting	Description	CLI command
IP Address	192.168.3.1	Specifies the IP address of this Ethernet port	eth 0 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 0 mask 255.255.255.0

Having changed the ETH 0 configuration respect to the default, also the DHCP server should be changed as follows:

Serial		
Advanced		
HCP Server		
DHCP Server for	· Ethernet 0	
Enable DHCP S	Server	
	IP Addresses: .92.168.3.3 to .92.168.3.119	
	to	
	to	
	Mask: 255.255.255.0	
	Gateway: 192.168.3.1	
	DNS Server: 192.168.3.1	
Seco	ndary DNS Server:	
	Domain Name:	
	Lease Duration: 14 days 0 hrs 0 mins	
Wait for 5	i00 milliseconds before sending DHCP offer reply	
Duplicate	Address Detection	
Only send	offers to Wi-Fi clients	
DHCP Relay		
Forward DHCP	requests to:	
► Advanced		
Advanced DHC	P Options	
Apply		
жрріу		

Figure 3.1-2: DHCP Server settings

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 0 IPmin "192.168.3.3" dhcp 0 IPrange 117
Mask	255.255.255.0	specifies the subnet mask used to on the network to which the router is connected	dhcp 0 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 0 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 0 DNS "192.168.3.1"

3.2 Primary WAN Settings: WiFi

In this Application note the primary WAN connection is the WiFi. In order to configure it, an ETH interface needs to be configured with DCHP client enabled and linked to the WiFi 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 WiFi connection. Basically, The ETH 12 interface will be configured in order to get the IP configuration via DHCP through the WiFi 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 <u>Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces > ETH 12</u> and <u>then > Advanced</u>, and follow the picture and table below, then click Apply.

ETH 12	
Description:	
Override these DHCP server vi	cally using DHCP
Mask:	
Gateway:	
DNS Server:	
Secondary DNS Server:	
Use the MAC address as the c OUse the following settings	ient ID
Changes to these parameters may	affect your browser connection
▼ Advanced	
This interfere is consisted with	- W6 E 0
This device is associated with	in made. Switch to Bast Jackta made
Ethernet Hub group:	
Metri	= <u>1</u>
MTI	1: 1500
Max Rx rat	E kbps
Max Tx rat	E 0 kbps
TCP transmit buffer siz	: O bytes
Take this interface out of servic (e.g. cable removed or broken)	e after 0 seconds when the link is lost
Enable NAT on this interfac O IP address	ess and Port
Enable IPsec on this interface	ce
Enable the firewall on this i	nterface
Enable DNS inbound blocki	19
Li chable DMink advertisemer	
Remote management acces	e addresses: 0
Respond to ARP requests o	nly if the requestor is of this network
Enable IGMP on this interfa	28
Enable Bridge on this interf	sce
Generate Heartbeats on thi	s interface
enerate Ping packets on t	his interface
Send 1 byte pings to	IP hos 8.8.8 very 0 hrs 0 min 10 seconds
Switch to sending pings to	IP host after 3 failures
Ping responses are expecte	d within 0 seconds
Only send Pings when	his 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 V

Figure 3.2-1: WAN settings – Logical Eth 12

Parameter	Setting	Description	CLI command
Get an IP address automatically using DHCP	Selected	Selecting this option enables the DHCP client on this interface. In this AN is selected as the TransPort will get the IP configuration from the DHCP server through the WiFi connection	eth 12 dhcpcli on
Enable NAT on this interface	Selected / IP address and Port	As this Logical Eth will be the WAN interface, NAPT needs to be enabled on it	eth 12 do_nat 2
Link with Ethernet instance	None	This logical interface will be linked to the WiFi 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	eth 12 pingis ON
Send <n> byte pings</n>	1	Size of ICMP packet to send	eth 12 pingsiz 1
to IP host	<ip ping="" to=""></ip>	Valid IP address to ping for link up/down testing.	eth 12 pingip "8.8.8.8"
Every	10	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 <u>Configuration - Network > Interfaces > Wi-Fi > Global Wi-Fi Settings</u> and follow the picture and table below to configure the general settings for the WiFi Module, then click Apply.

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

Interfaces					
Ethernet					
▼ Wi-Fi					
Global \	Ni-Fi Settii	ngs			
Rem	ote managem Net	Country: nent access: twork Mode: Channel:	Germany No restrictio B/G ✓ Auto ✓	∨ Ins	 ~
Adva	nced				
Wi-Fi	Hotspot				
Wi-Fi	Filtering				
Apply					

Figure 3.2-2: WAN settings – WiFi Global Settings

Parameter	Setting	Description	CLI command
Country	Germany	Selecting a country from the drop down list will restrict the channels that the router will use. See table on page 51 on the User Manual (<u>http://ftp1.digi.com/support/documentation/90</u> 001019_K.pdf) for more info on licensed channels.	wifi 0 country "Germany"

3.2.3 WiFi Node 0 Settings

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

Inte	ces mat	
- Wi	net	
•	bal Wi-Fi Settings	
•	Fi Node 0 - WiFi Client (WAN)	
	Enable this Wi-Fi interface	
	Description: WiFi Client (WAN)	
	SSID: Access Point WPA	
	ink this Wi-Fi client interface with Ethernet: 12 💙	
	lick <u>here</u> to assign a timeband to this interface	
	Vi-Fi Security	
	Ise the following security on this Wi-Fi interface:	
	○None ○WEP ●WPA-PSK ○WPA2-PSK ○WPA-802.1X ○WPA2-802.1X	
	WPA-PSK Settings	
	WPA pre-shared key:	
	Network Scanning	

Figure 3.2-3: WAN settings – WiFi Client Settings

Parameter	Setting	Description	CLI command
Enable	Selected	Enable the WiFi interface and reveals the options	
Description	WiFi 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 Access Point 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 interface with Ethernet <n></n>	12	When the Wi-Fi interface is configured to be a client, it must be bridged to a particular Ethernet interface. In this AN ETH12 is the Ethernet interface used for the WiFi Client.	eth 12 wificli ON
Use the following security on this Wi-Fi interface	WPA-PSK	Selects the security that is used on this Wi-Fi interface. In this AN the AP to which the TransPort is connecting uses WPA-PSK Security type	wifinode 0 security "wpapsk"
WPA Encryption	TKIP	The encryption algorithm to use. The AP for this AN uses TKIP algorithm	wifinode 0 wpatype "tkip"
WPA Pre-Shared Key / Confirm	*****	The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.	wifinode 0 esharedkey "PDZxU0FFQFU="

3.3 Backup WAN Settings: Cellular

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

nterfaces
• Ethernet
• Wi-Fi
f Mobile
Select a SIM to configure from the list below
Settings on this page apply to the selected SIM
SIM: 1 (PPP 1) V
IMSI: Unknown
▼ Mobile Settings
Select the service plan and connection settings used in connecting to the mobile network.
Mobile Service Provider Settings
Service Plan / APN internet.t-d1.de
Use backup APN Retry the main APN after minutes
SIM PIN: (Optional)
Confirm SIM PIN:
Username: (Optional)
Password: (Optional)
Confirm Password:

Figure 3-1: Backup WAN settings – Mobile

Parameter	Setting	Description	CLI command
Service Plan/APN	internet.t-d1.de	Enter the APN (Access Point Name) given by the service provider.	modemcc 0 apn "internet.t-d1.de"

3.4 Primary Default Route via WiFi

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

Routes 10 -	19
Routes 20 -	29
Poutes 40 -	- 40
Default Rou	ite 0
Description:	
De	fault route via
	Gateway:
	Interface: Ethernet 💙 12
Use PPP sub-	configuration: 0
	Metric: 1
Advance	d
Apply	

Figure 3.4-1: Primary Route via WiFi ETH 12

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 II_ent "ETH" def_route 0 II_add 12

3.5 Backup default Route via Cellular

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

onriguration - Network > <u>1P Routing/Forwarding</u> > <u>Static Routes</u> > <u>Default Route 1</u>	
Advanced	
DHCP Server	
Network Services	
DNS Servers	
Dynamic DNS	
▼ IP Routing/Forwarding	
P IP Routing	
Static Routes	
Proutes 10 - 10	
 Routes 10 - 19 Routes 20 - 20 	
 Routes 20 - 25 Poutes 30 - 30 	
Poutes 40 - 49	
Default Route 0	
▼ Default Route 1	
Description:	
Default route via	
Gateway:	
Interface PPP V 1	
Use PPP sub-configuration: 0	
Metric: 2	
✓ Advanced	
Use metric 2 when the interface is down	

Figure 3.5-2: Backup Route via PPP 1

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 II_ent "PPP" def_route 1 II_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). Usually is 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 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 add first of all the following rule in order to not lost the connection to the device when enabling the firewall on the interfaces, Navigate to: <u>Configuration - Security > Firewall</u>, click on "insert" and type/paste in the rule:

pass break end

then click OK.

After that, click on "insert" again and type the rule for the monitoring. In this AN is used the following rule:

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 and the FW rule should look like the following picture. Click "Save" in order to save the fw file:

Users				
Firewall	an natioular interfaces			
(You may specify up to 750 rules)	on particular interfaces.			
Hits #	Rule		Action	
0 1 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	Delete	Insert Edit	Test
0 2 pass break end		Delete	Insert Edit	i
			Insert	
Reset Hit Counters Save Restor	e			

Figure 3.6-1: Firewall Rules

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

In order to have this effectively applied, the FW 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 Apply:

Reset Hit Counters Save Restore The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click here to jump to the GRE configuration page. Interface Enabled ETH 0 ETH 1 ETH 2 ETH 3 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12	iguration - Se	curity > <u>Firewall</u>	
Reset Hit Counters Save Restore The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click here to jump to the GRE configuration page. Interface Enabled ETH 0 ETH 1 ETH 2 ETH 3 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 2			
Reset Hit Counters Save Restore The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click here to jump to the GRE configuration page. Interface Enabled ETH 0 ETH 1 ETH 2 ETH 3 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12			
The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click here to jump to the GRE configuration page. 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 11 ETH 12	Reset Hit	Counters Save Restore	
The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click here to jump to the GRE configuration page. Interface Enabled ETH 0 ETH 1 ETH 2 ETH 3 ETH 4 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 11 ETH 12			
The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click here to jump to the GRE configuration page. Interface Enabled ETH 0 ETH 1 ETH 2 ETH 3 ETH 4 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 11 ETH 12 V			
Click here to jump to the GRE configuration page. Interface Enabled ETH 0	The firewall ca	be enabled on Ethernet, PPP and GRE inte	erfaces.
Interface Enabled ETH 0	Click <u>here</u> to ju	np to the GRE configuration page.	
ETH 1 ETH 2 ETH 2 ETH 3 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12 V	Interface I		
ETH 1 ETH 2 ETH 2 ETH 3 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12 V			
ETH 2 C			
ETH 4 ETH 4 ETH 5 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12 V	ETH 3		
ETH 5 ETH 6 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12 V	ETH 4		
ETH 6 ETH 6 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12 ETH 12	ETH 5		
ETH 7 ETH 7 ETH 8 ETH 9 ETH 10 ETH 11 ETH 12 ETH 1	ETH 6		
ETH 8 □ ETH 9 □ ETH 10 □ ETH 11 □ ETH 12 ☑	ETH 7		
ETH 9 ETH 10 ETH 11 ETH 12 V	ETH 8		
ETH 10 ETH 11 ETH 12 V	ETH 9		
ETH 11 ETH 12	ETH 10		
ETH 12 🗹	ETH 11		
	ETH 12		

Figure 3.6-2: Enabling Firewall

4 TESTING

4.1 Debug settings on TransPort

In many cases is very useful configure the device in order to have a debug trace for the IKE negotiation in case of issues of setting up the VPN and for 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):

▼ Settings											
Maximum packet capture size: 1500 bytes											
Log size: 180 Kbytes											
Protocol layers											
Layer 2 (Link)											
Mayer 3 (Network)											
Enable QMI trace											
LAPB Links											
LAPB 0 LAPB 1											
Serial Interfaces											
□ ASY 0 □ ASY 1 □ ASY 2 □ ASY 3 □ ASY 4											
□ ASY 5 □ ASY 6 □ ASY 8 □ ASY 9 □ ASY 10											
ASY 11 ASY 12 ASY 13 ASY 14 ASY 15											
Clear all Serial Interfaces											
Wi-Fi Analyser Configuration											
Wi-Fi Analysis:											
Wi-Fi Management Packet Analysis <mark>No Beacons ♥</mark>											
Wi-Fi Data Packet Analysis: No Null Data 💙											
Ethernet Interfaces											
□ ETH 20 □ ETH 21 □ ETH 22 □ ETH 23											
Clear all Ethernet Interfaces											
PPP Interfaces											
□ PPP 0 □ PPP 1 □ PPP 2 □ PPP 3 □ PPP 4											
Clear all PPP Interfaces											
1P Sources											
🗆 ЕТН 10 🗌 ЕТН 11 🗹 ЕТН 12 🗌 ЕТН 13 🗌 ЕТН 14											
□ ETH 15 □ ETH 16 □ ETH 17 □ ETH 18 □ ETH 19											
□ PPP 5 □ PPP 6 □ PPP 7											
Clear all IP Sources											

Figure 4.1-1: Analyser settings

Parameter	Setting	Description	CLI command
Enable Analyser	Selected	This checkbox is used to enable or disable the analyser.	ana 0 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 0 maxdata 1500
Log Size	180	The maximum size of the pseudo file "ana.txt" that is used to store the captured data packets. Common practice is to set at this maximum (180). Notice that the data is compressed so more than 180Kb of trace data will be captured.	ana 0 logsize 180
Protocol layers	Layer 3 (Network)	Specify which protocol layers are captured and included in the analyser trace. For the purpose of this AN the Network Layer (Layer 3) is chosen	ana 0 I3on
Wi-Fi analysis	Ticked	Enable the WiFi trace on the module	wifi 0 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 0 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 0 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 WiFi client is connected to the AP, the routing table should looks like the following, showing that the primary route is the one pointing to ETH 12. In the routing table is also shown the backup route to PPP 1 (as UP), that will be not used while the primary is UP due to metric priority. The routing table can be checked browsing to <u>Management - Network Status > IP Routing Table:</u>

• Ethernet						
Wi-Fi						
• Mobile						
GRE						
Serial						
Advanced						
IP Statistics						
IP Routing Table						
Destination	Gateway	Metric	Protocol	Idx	Interface	Status
37.84.1.60/30	37.84.1.62	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 Deutee						
Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0/0	192.168.1.1	2	Static	0	ETH 12	UP
0.0.0/0	37.84.1.62	3	Static	1	PPP 1	UP

Figure 4.2-1: Routing Table in Normal Condition

In order to check if the traffic is effectively routed through the primary route via WiFi, 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 analyser trace browsing to: <u>Management - Analyser > Trace.</u>

The trace will show that the ICMP ECHO REQ is received on ETH 0, routed to ETH 12, correctly natted and then finally transmitted via the WiFi module:

	-	11-1	12-2	2014	1 1	L2:3	39:1	13.0	590	-						
45	00	00	3C	0B	2C	00	00	80	01	5F	DD	С0	A8	03	04	E<.,
08	08	04	04	08	00	4D	41	00	01	00	1A	61	62	63	64	MAabcd
65	66	67	68	69	6A	6В	6C	6D	6E	6F	70	71	72	73	74	efghijklmnopqrst
75	76	77	61	62	63	64	65	66	67	68	69					uvwabcdefghi

IP (Ir	n) I	From	REM TO LOC	IFACE: ETH 0
5			IP Ver:	4
			Hdr Len:	20
0			TOS:	Routine
			Delay:	Normal
			Throughput:	Normal
			Reliability:	Normal
0 3C			Length:	60
B 2C			ID:	2860
0 00			Frag Offset:	0
			Congestion:	Normal
				May Fragment
				Last Fragmen
0			TTL:	128
1			Proto:	ICMP
FDD			Checksum:	24541
0 A8	03	04	Src IP:	192.168.3.4
8 08	04	04	Dst IP:	8.8.4.4
CMP:				
8(Type:	ECHO REQ
0			Code:	0
D 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 08 08 04 04 08 00 4D 41 00 01 00 1A 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 uvwabcdefghi

ΙP	(F:	inai	l) 1	From	n L(DC 1	FO I	REM		IFZ	ACE :	E.	ГН 1	12	
45					ΙP	Ve	r:			4					
					Hdi	r Le	en:			20					
00					TOS	3:				Roi	utir	ne			
					De	lay	:			Noi	rmal	L			
					Th	roug	ghpı	it:		Noi	rmal	L			
					Re	liak	oil:	ity	:	Noi	rmal	L			
00	3C				Lei	ngtl	n:			60					
0B	2C				ID	:				286	60				
00	00				Fra	ag (Off	set	:	0					
					Coi	nges	stic	on:		Noi	rmal	L			
										Ma	y Fi	cagr	nent	t	
										Las	st E	raq	gmei	nt	
7F					TTI	L:				12	7				
01					Pro	oto	:			ICI	ИР				
62	'/C		6.5		Che	ecks	sum	:		252	212			0.0	
CO	A8	10	65		Sro		2:			192	2.10	. 80	Ι.Ι(υL	
08	80	04	04		DS1	t 11	2:			8.8	3.4.	. 4			
TC	MP:									DOI					
08					TY	pe:				ECI	10 1	KEQ			
10	11				Ch	ue: Doku				10					
40	41				CIIE	CKS	suii	•		19					
			 11-'	12-	2014	1 -	12.	39.	13	690	_				
0.8	41	28	00	04	F0	21	00	9R	18	00	0E	8E	23	14	1
00	04	2D	04	B4	4C	EO	05	00	20	5B	20	00	00	0.0	1 J
AA	AA	03	00	00	0.0	0.8	00	45	00	00	3C	0B	2C	00))
7 F	01	62	7C	C0	A8	01	65	0.8	0.8	04	04	08	00	4 T	5
00	01	00	1A	61	62	63	64	65	66	67	68	69	6A	61	3
6D	6E	6F	70	71	72	73	74	75	76	77	61	62	63	6	4
66	67	68	69												

Wi-	-Fi	Fro	m I	COC	То	REM		IFACE:	Wi-Fi	Module 0
08	41						Version:	0		
							Type:	Data		
							Subtype:	Data		
							Flags:	STA ->	AP, P	rotected
28	00						Duration:	40		
04	FO	21	0C	9B	18		BSS ID			
00	0E	8E	23	14	85		Src. MAC			

00	04	2D	04	В4	4C		Dst.	MAC	
05	ΕO						Frag	ment:	0
							Sequ	ience:	94
00	20	5B	20	00	00 00	00 0	TKIF	Security Param	
AA	AA	03	00	00	00		LLC	SNAP	
80	00						Туре	:	ΙE
IP:	:								
45					IP Ve	er:		4	
					Hdr 1	len:		20	
00					TOS:			Routine	
					Delay	/:		Normal	
					Throu	ighpu	t:	Normal	
					Relia	abili	ty:	Normal	
00	3C				Lengt	ch:		60	
0в	2C				ID:			2860	
00	00				Frag	Offs	et:	0	
					Conge	estio	n:	Normal	
								May Fragment	
								Last Fragment	
7F					TTL:			127	
01					Proto	:		ICMP	
62	7C				Checl	sum:		25212	
С0	A8	01	65		Src 1	[P:		192.168.1.101	
08	08	04	04		Dst 1	[P:		8.8.4.4	

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

			11-1	12-2	2014	1 1	L2:3	39:1	13.7	700							
08	02	2C	00	00	0E	8E	23	14	85	04	FO	21	0C	9B	18	,#!	
00	04	2D	04	В4	4C	10	10	AA	AA	03	00	00	00	08	00	L	
45	00	00	3C	ЗD	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	eUAabcd	
65	66	67	68	69	6A	6В	6C	6D	6E	6F	70	71	72	73	74	efghijklmnopqrst	
75	76	77	61	62	63	64	65	66	67	68	69	В1	29	06	80	uvwabcdefghi.)	
15	AF	D0	9B														
		_			-		~										
W1	-11	F, L	om I	REM	Ίo	LOC	2	ττ.			_				1 FACE	: Wi-Fi Module O	
08	02							V 6	ers.		:				Data		
								1 <u>-</u>	ype vh+v	me					Data Data		
								ਹ ਸ		, pe	•				ND =>	S T N	
20	00							г. П	irət	- 1 - 1	. .				AF	SIA	
00	0E	8E	23	14	85				3±01	MA	~						
04	FO	21	00	9B	18			B	35.		0						
00	04	2D	04	в4	4C			S	rc.	MA	С						
10	10							F	ragi	nent	t:				0		
								Se	∋que	ence	e:				257		
AA	AA	03	00	00	00			LI	LĊS	SNA	P						
08	00							T	ype						IP		
ΙP	:																
45					ΙP	Vei	::			4							
					Hdı	r Le	en:			20							
00					TOS	5:				Roi	utii	ne					
					De	lay	:			No:	rma.	L					
					Th	roug	ghpι	it:		No:	rma.	L					
0.0	29				Re.	Liak	2113	Lty	•	NO:	rma.	L					
00	30				Lei	ngti	1:			60							
30	AB				ID:	:		- -	_	15	/8/						
00	00				FIG Cov	ag () 1 1 5	set:		U	~~~ ~ ·	1					
					COI	iges	SLIC)II :		Mai	LINA.	L	nont	-			
										La	y r. st 1	- ayı Tra	mer	nt.			
34					וידיד					52			Juici	10			
01					Pro					TCI	ИР						
77	ΕD				Che	ecks	311m :			31	485						

	08 C0	08 A8	04 01	04 65		Sro Dst	o Il t Il	P: P:			8. 19	8.4 2.1	.4 68.1	1.1(01	
	45 C0 65 75 15	00 A8 66 76 AF	00 01 67 77 D0	 3C 65 68 61 9B	12-2 3D 00 69 62	2014 AB 00 6A 63	1 (00 55 6B 64	12: 00 41 6C 65	39:1 34 00 6D 66	13. 01 01 6E 67	700 7A 00 6F 68	FD 1A 70 69	08 61 71 B1	08 62 72 29	04 63 73 06	04 64 74 80
	ΙP	(II	n) 1	Fror	n RI	EM 1	ro i	LOC			IF	ACE	: E1	ГН 1	12	
	45					ΙP	Ve	r:			4					
	00					Hdi TOS De	r Le 3: lay	en:			20 Roi No:	uti: rma	ne 1			
	00 3D 00	3C AB 00				Thi Re Ler ID Fra Cor	roue lia ngtl ngt nge:	ghp oil: h: Off: stie	ut: ity: set: on:	:	No: No: 60 15 0 No: Mo:	rma rma 787 rma	1	nond	_	
											La	y r st :	Frag	gmei	nt	
	34					TTI	L:				52			_		
	01 7A	FD				Pro	oto eck:	: sum	:		ICI 31	MP 485				
	08	08	04	04		Sro		P:			8.	8.4	.4			
	C0	A8 vd•	01	65		Dst	t II	P:			19:	2.1	68.1	1.10	01	
	00					Тур	pe:				EC	HO	REPI	LY		
	00	11				Coo	de:		_		0	0 2 5				
						CII	SCK:	Sum	•		21	020				
			11-1	12-2	2014	1 1	12:	39:	13.	700						
45 C0	00 A8	00	3C 04	3D 00	AB 00	00 55	00 41	32	01	00 /B	5E 1A	08 61	08 62	04 63	04 64	
65	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74	
75	76	77	61	62	63	64	65	66	67	68	69					
ΙP	(F:	inal	1)]	From	n LO	DC I	ro i	REM		IFZ	ACE	: E	ГН (D		
45					IP	Vei	r:			4						
00					TOS	ст. З:	=11.			Roi	uti	ne				
					Del	Lay	:			Noi	rma	1				
					Thi Re	roug liab	gnp: cil	ut: it.v	:	Noi	rma. rma	1 1				
00	3C				Ler	ngtl	n:	1	•	60		_				
3D	AB				ID:	:) f f	+		15	787					
00	00				Cor	ig (iges	sti	on:	•	Noi	rma	1				
						-				Ma	y F	ragi	ment	t		
32					ΨΨT					Las	st i	Fra	gmei	nt		
01					Pro	oto	:			ICI	ЧР					
7B	5E	~ •			Che	ecks	sum	:		315	582					
C0	08 A8	04	04		Dst					8.8	3.4 2.1	•4 68	3.4			
ICN	4P:	0.5	гU		231					1) .	- • I					
00					Тур	pe:				ECI	HO I	REP	LY			
55	41				Coc	ae: ecks	sum	:		218	325					

E..<=...4.z.... ...e..UA....abcd efghijklmnopqrst uvwabcdefghi.)..

E..<=...2.{^....UA....abcd efghijklmnopqrst uvwabcdefghi

4.2.2 Failure on Access Point WAN connection

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

In this AN the AP is a Digi TransPort with an 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 FW monitoring, as, for the client, the WiFi 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 after a while check the evenlog on the TransPort going to <u>Management - Event Log</u>:

```
12:40:24, 11 Dec 2014, Default Route 0 Out Of Service, Firewall 12:40:24, 11 Dec 2014, ETH 12 Out Of Service, Firewall
```

The eventlog shows that the Firewall monitoring fails and so the ETH12 and the Primary route are set to OOS. Checking also the routing table going to <u>Management - Network Status > IP Routing Table</u>, it shows that the primary route is now OOS, and so the default route that wil be used now is the PPP one:

Ethernet						
Wi-Fi						
Mobile						
GRE						
Serial						
Advanced						
IP Statistics						
(P Routing Table						
Destination	Gateway	Metric	Protocol	Idx	Interface	Status
37.84.1.60/30	37.84.1.62	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	-	Local	-	ETH 12	005
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	37.84.1.62	3	Static	1	PPP 1	UP
0.0.0/0	192.168.1.1	Ŀ	Static	0	ETH 12	005

Figure 4.2-2: Routing Table after a failure on AP

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 browsing to <u>Management - Analyser > Trace</u>.

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

	45 08 65 75	00 08 66 76	11 00 04 67 77	-12 3C 04 68 61	2-20 13 08 69 62)14 ED 00 6A 63	12 00 4D 6B 64	2:40 00 3F 6C 65	9:41 80 00 6D 66	1.00 01 01 6E 67	00 57 00 6F 68	1C 1C 70 69	C0 61 71	- A8 62 72	03 63 73	04 64 74	E <w M?abcd efghijklmnopqrst uvwabcdefghi</w
	ΙP	(Ir	1) E	ron	n RE	EM 1	I OI	COC			IF	ACE	: E	ГН ()		
	45					IP	Vei	::			4						
	0.0					Hdi	î L∈	en:			20 Da						
	00					Del Thr	ay: Lay: couc	; ghpi	1t:		No: No:	rma rma	ne 1 1 1				
	00	3C				Ler	nath) 1:	LUY.	•	60	Lilla	T				
	13	ED				ID:	:				51	01					
	00	00				Fra	ag ()ffs	set	:	0		-				
						Cor	nges	stic	on:		No: Ma	rma. v F	L ram	nent	-		
											La	st	Frag	gmer	nt		
	80					TTI	:				12	8					
	01 57	10				Pro	oto:	: : 11m -			1CI	MP 300					
	C0	A8	03	04		Sro	C II	2:	•		19	2.1	68.3	3.4			
	08	08	04	04		Dst	: IH	?:			8.	8.4	.4				
	ICN 0.8	4P:				Ͳ៶៸r					ECI	HO 1	REO				
	00					Coc	de:				0		ιшų				
	4D	ЗF				Che	ecks	sum:	:		19	775					
			 1-1	2-2	014	1 1	2:4	10:4	11.(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 67	4D	3F	00 6 D	01 6 E	00 6 E	1C	61	62	63 72	64		M?abcd
75	76	77	61	62	63	ов 64	65	66	67	68	69	/ 1	12	15	/4		uvwabcdefghi
		_	· · · -	_							~-						
1P 45	(E'J	Inal	L)	ron	n L(IP	Vei Vei	10 F	(EM		4	ACE	: P.	PP.	L			
					Hdı	c Le	en:			20							
00					TOS	3: 				Roi	uti	ne					
					Th:	couc	ihpu	it:		Noi	rma.	1					
					Re	Liak	bili	Lty:	:	Noi	rma	1					
00	3C				Ler	ngtł	1:			60 51(1						
00	00				Fra	i ag (Offs	set:	:	0	JI						
					Cor	nges	stic	on:		Noi	rma	1					
										Ma	y F	ragi	ment	t			
7F					וידיד					12	ร่เ. 7	ra	gmei	10			
01					Pro	oto:				ICI	ЧР						
F5	36	0.1			Che	ecks	sum:			62	774	1	<u> </u>				
25 08	54 08	01	3E 04		Dst	с 1В - тя				37	.84 3.4	. 1 .	62				
ICI	4P:	0 1	0 1		200	1				~.(
80					Тур	pe:				ECI	IO I	REQ					
00 4 D	੨ਛ				Coc	le:	21170			0	775						
10	9 E				CITE	CAS	Juni.			1)	, , ,						

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

		1	11-1	2-2	2014	1 1	2:4	10:4	11.0	060	-				
45	00	00	3C	56	ΕA	00	00	2E	01	03	ЗA	08	08	04	04
25	54	01	ЗE	00	00	55	ЗF	00	01	00	1C	61	62	63	64
65	66	67	68	69	6A	6В	6C	6D	6E	6F	70	71	72	73	74
75	76	77	61	62	63	64	65	66	67	68	69				

E..<V....:.... %T.>..U?....abcd efghijklmnopqrst 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:	8.8.4.4
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....</td>

 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

ΙP	(F	lna	l) From	n 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	ΕA			ID:	22250
00	00			Frag Offset:	0
				Congestion:	Normal
					May Fragment
					Last Fragment
2C				TTL:	44
01				Proto:	ICMP
68	1F			Checksum:	26655
80	08	04	04	Src IP:	8.8.4.4
С0	A8	03	04	Dst IP:	192.168.3.4
ICN	4P:				
00				Туре:	ECHO REPLY
00				Code:	0
55	ЗF			Checksum:	21823

4.2.3 Recovery and rollback to WiFi

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

12:42:05, 11 Dec 2014,Default Route 0 Available,Recovery
12:42:04, 11 Dec 2014,ETH 12 Available,Recovery
12:42:04, 11 Dec 2014,ETH 12 Recovery Completed,PING
12:40:57, 11 Dec 2014,Network technology changed to WCDMA
12:40:37, 11 Dec 2014,Network technology changed to HSDPA/HSUPA

The eventlog 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:

Ethernet						
▶ Wi-Fi						
Mobile						
GRE						
Serial						
Advanced						
IP Statistics						
IP Routing Table						
Destination	Gateway	Metric	Protocol	Idx	Interface	Status
37.84.1.60/30	37.84.1.62	1	Local	-	PPP 1	UP
			Local	-	ETH 12	UP
192.168.1.0/24	192.168.1.101	1	Local		E111 12	
192.168.1.0/24 192.168.3.0/24	192.168.1.101 192.168.3.1	1	Local	-	ETH 0	UP
192.168.1.0/24 192.168.3.0/24	192.168.1.101 192.168.3.1	1	Local	-	ETH 0	UP
192.168.1.0/24 192.168.3.0/24 Default Routes	192.168.1.101 192.168.3.1	1	Local	-	ETH 0	UP
192.168.1.0/24 192.168.3.0/24 Default Routes Destination	192.168.1.101 192.168.3.1 Gateway	1 1 Metric	Local	- Idx	ETH 0	UP
192.168.1.0/24 192.168.3.0/24 Default Routes Destination 0.0.0.0/0	192.168.1.101 192.168.3.1 Gateway 192.168.1.1	1 1 Metric 2	Local Protocol Static	- Idx 0	ETH 12 ETH 0 Interface ETH 12	UP Status UP

Figure 4.2-3: Routing Table after Rollback to WiFi

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:

	-	11-1	12-2	2014	1 1	2:4	13:3	32.5	510	-						
45	00	00	3C	16	4B	00	00	80	01	54	ΒE	С0	A8	03	04	E<.KT
08	08	04	04	08	00	4D	3E	00	01	00	1D	61	62	63	64	M>abcd
65	66	67	68	69	6A	6В	6C	6D	6E	6F	70	71	72	73	74	efghijklmnopqrst
75	76	77	61	62	63	64	65	66	67	68	69					uvwabcdefghi
ΙP	(Ir	n) I	Fron	n RE	CM 7	I OI	COC			IFA	ACE :	: E1	ГН ()		
45					ΙP	Vei	::			4						
					Hdı	: Le	en:			20						

	00 00 16 00	3C 4B 00				TO: De: Th: Re: Lei ID Fra Coi	S: lay roug lia ngtl ag (nge:	: pil: n: Off: stic	ut: ity set on:	:	Roi No: No: 60 57 0 No: Ma	utin rma rma 07 rma y F	ne l l l ragr	nent	5			
	80 01					TTI Pro	L: oto				La: 12 ICI	st 1 8 MP	Fraq	gmer	ıt			
	54	BE	0.0	0.4		Che	ecks	sum:	:		21	694	<u> </u>					
	08	A8 08	03	04		Dst	t II	2:			8.	8.4	.4	. 4				
	ICN 08	4P:				Ту	pe:				EC	HO I	REQ					
	00 4D	3E				Coo Che	de: ecks	sum	:		0 19	774						
			 11-1	 12-2	2014	1 .	12•4	13.1	32 1	510								
45 08 65 75	00 08 66 76	00 04 67 77	3C 04 68 61	16 08 69 62	4B 00 6A 63	00 4D 6B 64	00 3E 6C 65	7F 00 6D 66	01 01 6E 67	57 00 6F 68	5D 1D 70 69	C0 61 71	A8 62 72	01 63 73	65 64 74	E< efgh uvwa	(.KW]e M>abcd nijklmnopqrst abcdefghi	ì
IP 45	(Fi	Ina	l) I	Fror	n LO		FO I	REM		IF	ACE	: E?	ГН 1	L <mark>2</mark>				
45 00					Hdi TOS	ve: r Le S:	r: en:			4 20 Roi	uti	ne						
					Th:	rou	; ghpı	it:		NO: NO:	rma.	1						
00	3C				Ler	ngtl	n:	LUY	:	NO: 60	rma.	T						
16 00	4B 00				ID: Fra	: ag (Off	set	:	57) 0	07							
					Cor	nge	sti	on:		No: Ma	rma y Fi	l ragi	nent	5				
7F					TTI	L:				La: 12	st : 7	Fra	gmer	nt				
01 57	5D				Pro Che	oto eck:	: sum			ICI 223	MP 365							
C0 08	A8 08	01 04	65 04		Sro Dst	C II t TI	P: P:			19:	2.1 8.4	68.: .4	1.1()1				
ICN 08	4P:				TTT					FCI								
00	2.				Coc	de:				0		<u>NDQ</u>						
4D)도 				Cne	eck:	sum	•		19	//4							
08	41	28	11-1 00	12-2 04	2014 F0	4 : 21	12:4 0C	43:3 9B	32. 18	510 00	0E	8E	23	14	85	.A(.		
00 AA	04 AA	2D 03	04 00	В4 00	4C 00	F0 08	08 00	00 45	20 00	8C 00	20 3C	00 16	00 4B	00 00	00 00	· · - ·	.L	
7F 00	01 01	57 00	5D 1D	C0 61	A8 62	01 63	65 64	08 65	08 66	04 67	04 68	08 69	00 6A	4D 6B	3E 6C	W]	abcdefghijkl	> L
6D 66	6E 67	6F 68	70 69	71	72	73	74	75	76	77	61	62	63	64	65	mnop fahi	oqrstuvwabcde	4
Wi-	-Fi	Fre	om 1	. <u></u>	To	REI	vī								TFACE	• Wi-	Fi Module O	
08	41							Ve Tr	ers	ion •	:				0 Data			
								Su	ibt:	ype	:				Data		Drotocted	
28	00	0.1	0	0-	1.0			E. Di	irat	s: tio	n:				40	AP,	FIOLECTED	
04 00	F0 0E	21 8E	0C 23	9B 14	18 85			BS S1	SS : rc.	LD MA(С							
	01	2D	04	B4	4C			Ds	st.	MA	С							

08 F0 Fragment: Sequence: 00 20 8C 20 00 00 00 00 TKIP Security Param

0 143

08 00 Type: IP IP: IP Ver: 4 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 TF TTL: 127 01 Proto: ICMP	AA	03	00	00	00	LLC S	SNAP	
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	00					Туре	:	1P
Hdr Len:2000TOS:RoutineDelay:NormalThroughput:NormalReliability:Normal00 3CLength:6016 4BID:570700 00Frag Offset:0Congestion:NormalMay FragmentLast Fragment7FTTL:12701Proto:ICMP					IP Ver:		4	
00TOS:RoutineDelay:NormalThroughput:NormalReliability:Normal00 3CLength:6016 4BID:570700 00Frag Offset:0Congestion:NormalMay FragmentLast Fragment7FTTL:12701Proto:ICMP					Hdr Len:		20	
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					TOS:		Routine	
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					Delay:		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					Throughput	z:	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					Reliabilit	cy:	Normal	
16 4B ID: 5707 00 00 Frag Offset: 0 Congestion: Normal May Fragment Last Fragment 7F TTL: 127 01 Proto: ICMP	3C				Length:		60	
00 00 Frag Offset: 0 Congestion: Normal May Fragment Last Fragment 7F TTL: 127 01 Proto: ICMP	4B				ID:		5707	
Congestion: Normal May Fragment Last Fragment 7F TTL: 127 01 Proto: ICMP	00				Frag Offse	et:	0	
May Fragment Last Fragment 7F TTL: 127 01 Proto: ICMP					Congestion	n:	Normal	
Last Fragment7FTTL:12701Proto:ICMP							May Fragment	
7F TTL: 127 01 Proto: ICMP							Last Fragment	
01 Proto: ICMP					TTL:		127	
					Proto:		ICMP	
57 5D Checksum: 22365	5D				Checksum:		22365	
CO A8 01 65 Src IP: 192.168.1.101	A8 (01	65	5	Src IP:		192.168.1.101	
08 08 04 04 Dst IP: 8.8.4.4	08	04	04	1	Dst IP:		8.8.4.4	

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[.... CO 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 uvwabcdefghi.... 75 76 77 61 62 63 64 65 66 67 68 69 AA 01 A3 09 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 OE 8E 23 14 85 Dst. MAC 04 F0 21 OC 9B 18 BSS ID Src. MAC 00 04 2D 04 B4 4C 11 10 Fragment: 0 273 Sequence: AA AA 03 00 00 00 LLC SNAP 08 00 ΙP Type: IP: IP Ver: 45 4 20 Hdr Len: 00 TOS: Routine Delay: Normal Normal Throughput: Reliability: Normal 00 3C Length: 60 3E 4D ID: 15949 Frag Offset: 00 00 0 Congestion: Normal May Fragment Last Fragment 34 TTL: 52 ICMP 01 Proto: 7A 5B Checksum: 31323 08 08 04 04 8.8.4.4 Src IP: CO A8 01 65 192.168.1.101 Dst IP: ----- 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[....

CO A8 01 65 00 00 55 3E 00 01	00 1D 61 62 63 64
65 66 67 68 69 6A 6B 6C 6D 6E	6F /0 /1 /2 /3 /4
75 76 77 61 62 63 64 65 66 67	68 69 AA 01 A3 09
31 19 A4 2C	
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:	8.8.4.4
CO 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
 32
 01
 7A
 BC
 08
 04
 04

 C0
 A8
 03
 04
 00
 00
 32
 01
 7A
 BC
 08
 04
 04

 C0
 A8
 03
 04
 00
 00
 55
 3E
 00
 01
 00
 1D
 61
 62
 63
 64

 65
 66
 67
 68
 69
 6A
 6B
 6C
 6D
 6E
 6F
 70
 71
 72
 73
 74

 75
 76
 77
 61
 62
 63
 64
 65
 66
 67
 68
 69

ΙP	(Fi	nal	L) From	n 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
ЗE	4D			ID:	15949
00	00			Frag Offset:	0
				Congestion:	Normal
					May Fragment
					Last Fragment
					Last Llagment
32				TTL:	50
32 01				TTL: Proto:	50 ICMP
32 01 7A	BC			TTL: Proto: Checksum:	50 ICMP 31420
32 01 7A 08	BC 08	04	04	TTL: Proto: Checksum: Src IP:	1030 1109MeHe 50 1CMP 31420 8.8.4.4
32 01 7A 08 C0	BC 08 A8	04 03	04 04	TTL: Proto: Checksum: Src IP: Dst IP:	1030 110gmente 50 ICMP 31420 8.8.4.4 192.168.3.4
32 01 7A 08 C0 ICN	BC 08 A8 4P:	04 03	04 04	TTL: Proto: Checksum: Src IP: Dst IP:	1000 1100 1100 1100 1000 1000 1000 100
32 01 7A 08 C0 ICN 00	BC 08 A8 4P:	04 03	04 04	TTL: Proto: Checksum: Src IP: Dst IP: Type:	50 ICMP 31420 8.8.4.4 192.168.3.4 ECHO REPLY
32 01 7A 08 C0 ICN 00 00	BC 08 A8 4P:	04 03	04 04	TTL: Proto: Checksum: Src IP: Dst IP: Type: Code:	1100000000000000000000000000000000000
32 01 7A 08 C0 IC1 00 00 55	BC 08 A8 4P: 3E	04 03	04 04	TTL: Proto: Checksum: Src IP: Dst IP: Type: Code: Checksum:	1100000000000000000000000000000000000

E..<>M..2.z....U>....abcd efghijklmnopqrst uvwabcdefghi

...e..U>....abcd efghijklmnopqrst

uvwabcdefghi....

1...

4.3 Testing failover without Firewall Monitoring: WiFi link failure

In this section will be provided a quick test on how is performed the failover in case of a failure on the WiFi connection.

This kind of failure will not use the FW monitoring, so in order to have it working the section "3.6 Firewall Configuration" and the "Generate Ping" section of the ETH 12 configuration (see Figure 3.2 1) are optional (but, if present as in this example, don't cause issues).

As shown in section 4.2.1, once the WiFi client is connected to the AP, the routing table should looks like the following, showing that the primary route is the one pointing to ETH 12. In the routing table is also shown the backup route to PPP 1 (as UP), that will be not used while the primary is UP due to metric priority. The routing table can be checked browsing to <u>Management - Network Status > IP Routing Table:</u>

Ethernet							
Wi-Fi							
Mobile							
GRE							
Serial							
Advanced							
IP Statistics							
IP Routing Table							
Destination	Gateway	Metric	Protocol	Idx	Interface	Status	
37.82.42.80/30	37.82.42.82	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	192.168.1.1	2	Static	0	ETH 12	UP	
	07.00.40.00	(3)	Static	1	PPP 1	UP	

Figure 4.3-1: Routing Table in Normal Condition

In this condition the traffic is routed to the Primary WiFi connection.

When a failure on the WiFi link occurs, for example disabling the WiFi on the AP side, the ETH 12 and the primary route will go immediately OOS (without using the FW monitoring) and the eventlog should look like the following:

```
11:15:54, 11 Dec 2014,Default Route 0 Out Of Service,Activation
11:15:54, 11 Dec 2014,ETH 12 Out Of Service,Activation
11:15:54, 11 Dec 2014,Wi-Fi client 0 probing Access Point WPA
11:15:54, 11 Dec 2014,Wi-Fi Node 0 disconnected from Access Point WPA,Remote
out of range
```

```
11:15:50, 11 Dec 2014, Wi-Fi Node 0 reassociating with Access Point WPA, RSSI:36
11:15:27, 11 Dec 2014, Clear Event Log
```

The routing table will be then:

A Ethornot						
> Wi-Ei						
Mohile						
CRE						
 Serial 						
Advanced						
IP Statistics						
IP Routing Table						
Destination	Gateway	Metric	Protocol	Idx	Interface	Status
37.82.42.80/30	37.82.42.82	1	Local	-	PPP 1	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP
Default Routes	C - 1		Destand	x .1	T-1-5-	C1 -1
Destination	Gateway	Merric	Protocol	Tax	Interrace	Status
	37.82.42.82	3	Static	1	PPP 1	
0.0.0/0				•	FTH 12	005

Figure 4.3-2: Routing Table after failure on WiFi link

And so the traffic will pass through the PPP link.

Enabling again the WIFi on the AP side will bring UP ETH 12 and the primary route. In this case the eventlog and the routing table will look like the following:

```
11:17:15, 11 Dec 2014,ETH 12 up
11:17:15, 11 Dec 2014,Default Route 0 Available,Activation
11:17:15, 11 Dec 2014,ETH 12 Available,Activation
11:17:15, 11 Dec 2014,Wi-Fi Node 0 connected to Access Point WPA, RSSI:42
11:17:12, 11 Dec 2014,Wi-Fi client 0 probing Access Point WPA
11:17:10, 11 Dec 2014,Wi-Fi client 0 probing Access Point WPA
11:17:07, 11 Dec 2014,Wi-Fi client 0 probing Access Point WPA
```

Ethernet						
Wi-Fi						
Mobile						
GRE						
Serial						
Advanced						
Statistics						
Routing Table						
Destination	Gateway	Metric	Protocol	Idx	Interface	Status
37.82.42.80/30	37.82.42.82	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
fault Routes						
Destination	Gateway	Moterc	Protocol	Idx	Interface	Status
0.0.0/0	192.168.1.1	2	Static	0	ETH 12	UP
0.0.0/0	37.82.42.82	3	Static	1	PPP 1	UP

Figure 4.3-3: Routing Table after Rollback to WiFi

5 TRANSPORT CONFIGURATION FILES

5.1 Configuration File

This is the configuration used on the TransPort in this Application Note, relevant CLI lines are highlighted:

```
'config c show'
wifi 0 country "Germany"
wifi 0 wifianon ON
wifi 0 anamgmt "nobeacons"
wifi 0 anadata "nonull"
wifinode 0 descr "WiFi Client (WAN)"
wifinode 0 ssid "Access Point WPA"
wifinode 0 mode "client"
wifinode 0 security "wpapsk"
wifinode 0 esharedkey "PDZxU0FFQFU="
eth 0 IPaddr "192.168.3.1"
eth 0 ipanon ON
eth 1 pingip "8.8.8.8"
eth 1 pingsiz 1
eth 1 pingis ON
eth 12 dhcpcli ON
eth 12 mask ""
eth 12 do nat 1
eth 12 firewall ON
eth 12 ipanon ON
eth 12 pingip "8.8.8.8"
eth 12 pingint 10
eth 12 pingsiz 1
eth 12 pingis ON
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
gps 0 asy add 1
qps 0 qpson ON
ip 0 cidr ON
def route 0 11 ent "ETH"
def route 0 11 add 12
def route 1 11 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.etherios.com" ppp 0 timeout 300 ppp 1 name "W-WAN" ppp 1 phonenum "*98*1#" ppp 1 IPaddr "0.0.0.0" ppp 1 timeout 0 ppp 1 use_modem 1 ppp 1 aodion 1 ppp 1 autoassert 1 ppp 1 ipanon ON ppp 1 r_chap OFF ppp 3 defpak 16 ppp 4 defpak 16 web 0 prelogin info ON modemcc 0 asy add 7 modemcc 0 info asy add 5 modemcc 0 init str "+CGQREQ=1" modemcc 0 init str1 "+CGQMIN=1" modemcc 0 apn "internet.t-d1.de" modemcc 0 link retries 10 modemcc 0 stat retries 30 modemcc 0 sms access 1 modemcc 0 sms concat 0 modemcc 0 init str 2 "+CGQREQ=1" modemcc 0 init str1 2 "+CGQMIN=1" modemcc 0 apn 2 "Your.APN.goes.here" modemcc 0 link retries 2 10 modemcc 0 stat retries 2 30 ana 0 anon ON ana 0 12on OFF ana 0 xoton OFF ana 0 lapdon 0 ana 0 lapbon 0 ana 0 maxdata 1500 ana 0 logsize 180 cmd 0 unitid "ss%s>" cmd 0 cmdnua "99" cmd 0 hostname "digi.router" cmd 0 asyled mode 1 cmd 0 tremto 1200 cmd 0 rcihttp ON cmd 1 autocmd "ats31=7" cmd 1 gpson ON user 0 access 0 user 1 name "username" user 1 epassword "KD51SVJDVVg=" user 1 access 0 user 2 access 0 user 3 access 0 user 4 access 0 user 5 access 0 user 6 access 0 user 7 access 0

```
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
ssh 0 hostkey1 "privTsa.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:

```
Digi TransPort WR44-U8G1-WE5-XX Ser#:149353
Software Build Ver5271. Oct 30 2014 06:10:52 SW
ARM Bios Ver 7.24u v39 400MHz B512-M512-F80-O0,0 MAC:00042d024769
Async Driver
                       Revision: 1.19 Int clk
Wi-Fi
                        Revision: 2.0
IX
                        Revision: 1.0
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
                       Revision: 1.00
TACPLUS
MODBUS
                        Revision: 0.00
                        Revision: 0.01
MySOL
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
```

SCRIBATSK	Revision:	1.0
BASTSK	Revision:	1.0
PYTHON	Revision:	1.0
CLOUDSMS	Revision:	1.0
ARM Sync Driver	Revision:	1.18
TCP	Revision:	1.14
TCP Utils	Revision:	1.13
PPP	Revision:	1.19
WEB	Revision:	1.5
SMTP	Revision:	1.1
FTP Client	Revision:	1.5
FTP	Revision:	1.4
IKE	Revision:	1.0
PollANS	Revision:	1.2
PPPOE	Revision:	1.0
BRIDGE	Revision:	1.1
MODEM CC (GOBI UMTS)	Revision:	1.4
FLASH Write	Revision:	1.2
Command Interpreter	Revision:	1.38
SSLCLI	Revision:	1.0
OSPF	Revision:	1.0
BGP	Revision:	1.0
QOS	Revision:	1.0
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
QDL	Revision:	1.0
WiMax	Revision:	1.0
OK		