

Application Note 70

Wi-Fi-to-Cellular Failover

Digi Technical Support

October 2016

Contents

1	Intr	oduction
	1.1	Outline
	1.2	Assumptions
	1.3	Corrections
	1.4	Version4
2	Sce	nario4
3	Trai	nsPort Router Configuration5
	3.1	LAN Settings5
	3.2	Primary WAN Settings: Wi-Fi8
	3.2.	1 Logical Ethernet Settings8
	3.2.	2 Global Wi-Fi Settings 11
	3.2.	3 Wi-Fi Node o Settings 12
	3.3	Backup WAN Settings: Cellular14
	3.4	Primary Default Route via Wi-Fi15
	3.5	Backup Default Route via Cellular16
	3.6	Firewall Configuration17
4	Tes	ting19
	4.1	Debug Settings on TransPort19
	4.2	Testing Failover with Firewall Monitoring: AP's WAN Failure
	4.2.	1 Normal Condition: Primary Route Active
	4.2.	2 Failure on Access Point WAN Connection 25
	4.2.	3 Recovery and Rollback to Wi-Fi
	4.3	Testing Failover without Firewall Monitoring: Wi-Fi Link Failure
5	Trai	nsPort Configuration Files
	5.1	Configuration File
	5.2	Firewall Rules
	5.3	Hardware and Firmware

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

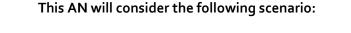
Requests for corrections or amendments to this AN are welcome and should be addressed to: <u>tech.support@digi.com</u>

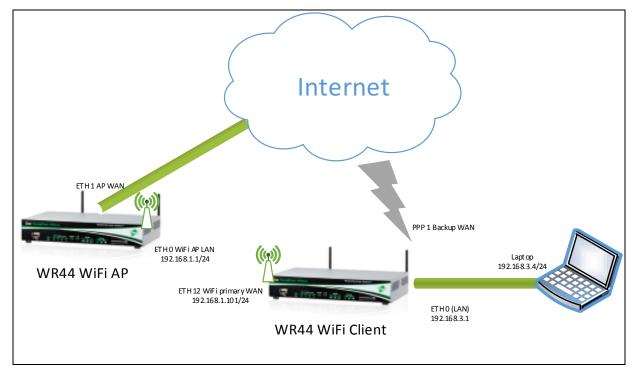
Requests for new ANs can be sent to the same address.

1.4 Version

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

2 SCENARIO





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

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

3 TRANSPORT ROUTER CONFIGURATION

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

3.1 LAN Settings

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

<u>Configuration - Network</u> > <u>Interfac</u>	<u>es</u> > <u>Ethernet</u> > <u>ETH 0</u>			
▼ ETH 0				
Description:				
 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:				
character the theory manufacture of				

Changes to these parameters may affect your browser connection

Advance	ed			
QoS				
► VRRP				
Apply				

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

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

Configuration - Network	< >	DHCP Server >	- [DHCP	Server	for	Ethernet (0
contraction nection		Differ Derrer P	_		001001		Etherniet (-

Enable DHCP Server ID Addresses	:192.168.3.3	to	192.168.3.119
IF Addresses	.192.108.3.3		192.108.3.119
		to	
		to	
	255.255.255.0		
	192.168.3.1		
	192.168.3.1		
Secondary DNS Server			
Domain Name			
Lease Duration	:14 days 0 h	rs () mins
 Duplicate Address Detection Only send offers to Wi-Fi contraction 			
DHCP Relay			
DHCP Relay			

Apply

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

3.2 Primary WAN Settings: Wi-Fi

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

3.2.1 Logical Ethernet Settings

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

<u>Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces > ETH 12 > Advanced</u>

▼ ETH 12

Description:

In the second second

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

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

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

3.2.2 Global Wi-Fi Settings

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

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

<u>Configuration - Network</u> > <u>Interfac</u>	<u>es</u> > <u>Wi-Fi</u> > <u>Global Wi-Fi Settings</u>
▼ Global Wi-Fi Settings	
Country:	United States 🔻
Remote management access:	No restrictions
Network Mode:	B/G ▼
Channel:	Auto 🔻
Antenna:	Auto 🔻
Advanced	
Wi-Fi Hotspot	
Wi-Fi Filtering	
Apply	

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

3.2.3 Wi-Fi Node o Settings

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

<u> Configuration - Network > Interfaces > Wi-Fi > Wi-Fi Node 0</u>
▼ Wi-Fi Node 0
Enable this Wi-Fi interface
Description: Wi-Fi Client (WAN)
SSID: Access Point WPA
Mode: Client
Link this Wi-Fi client interface with Ethernet: 12 🔻
Click <u>here</u> to assign a timeband to this interface
Wi-Fi Security
Use the following security on this Wi-Fi interface:
◎ None ◎ WEP ◎ WPA Personal ● WPA2 Personal ◎ WPA Enterprise ◎ WPA2 Enterprise
WPA-PSK Settings
WPA Encryption: TKIP (CCMP)
WPA pre-shared key: (8 - 63 chars)
Confirm WPA pre-shared key:
Network Scanning
Apply

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

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

3.3 Backup WAN Settings: Cellular

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

onfiguration - Network > Interfaces > Mobile
▼ Mobile Settings
Select the service plan and connection settings used in connecting to the mobile network.
Mobile Service Provider Settings
Service Plan / APN: Your.APN.goes.here
Use backup APN Retry the main APN after 0 minutes
SIM PIN: (Optional)
Confirm SIM PIN:
Username: (Optional)
Password: (Optional)
Confirm Password:

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

3.4 Primary Default Route via Wi-Fi

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

<u>Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0</u>
▼ Default Route 0
Description:
Default route via
Gateway:
Interface: Ethernet 🔻 12
Use PPP sub-configuration: 0
Metric: 1
► Advanced
Apply

Click the Apply button.

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

Configuration - Network > IP Routing/For	warding > <u>Static Routes</u> > <u>Default Route 1</u>
--	---

 Default Route 1 	
Description:	
Default route	via
Gatew	ay:
Interfa	ace: PPP 🔻 1
Use PPP sub-configurat	ion: 0
Met	tric: 2
Advanced	
Use metric 2 whe	n the interface is down

Click the Apply button.

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

3.6 Firewall Configuration

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

Please note that if the firewall is enabled just for this purpose, as in this example, it may be better to first add of all the following rules in order to not lose the connection to the device when enabling the firewall on the interfaces. Navigate to: **Configuration - Security > Firewall**, click on "Insert" and type/paste in the rule:

pass break end

Then click OK.

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

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

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



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

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

Conf	figuration ·	- Security	> <u>Firewall</u>
	Interface	Enabled	
	ETH 0		
	ETH 1		
	ETH 2		
	ETH 3		
	ETH 4		
	ETH 5		
	ETH 6		
	ETH 7		
	ETH 8		
	ETH 9		
	ETH 10		
	ETH 11		
	ETH 12		

4 TESTING

4.1 Debug Settings on TransPort

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

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

Management - Analyser > Settings

🗷 Ena	ble Analy	/ser	_												
	Maximu	m packet cap	oture size: 1	500 by	tes										
	Log size	: 180 Kby	/tes												
	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 I	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	3 🗌 ASY 14	ASY 15									
		ASY 16	ASY 17	ASY 18	B 🔲 W-WAN										
		Clear all Ser	rial Interfaces	5											
		-	is:	-	✓ No Beacons No Null Data										

Ethernet Interfaces													
0	ETH 0	🔲 ETH 1	ETH 2	🔲 ETH 3	🔲 ETH 4								
0	ETH 5	🔲 ETH 6	ETH 7	🔲 ETH 8	ETH 9								
0	ETH 10	🔲 ETH 11	🔲 ETH 12	🔲 ETH 13	🔲 ETH 14								
0	ETH 15	🔲 ETH 16	🔲 ETH 17	🔲 ETH 18	🔲 ETH 19								
0	ETH 20	🔲 ETH 21	🔲 ETH 22	ETH 23	🔲 ETH 24								
0	ETH 25	🔲 ETH 26	🔲 ETH 27										
C	lear all Eth	nernet Interf	aces										
PPP Inte	rfaces												
0	PPP 0	PPP 1	PPP 2	PPP 3	PPP 4								
0	PPP 5	PPP 6	PPP 7	PPP 8	PPP 9								
0	PPP 10	PPP 11	PPP 12	PPP 13	PPP 14								
0	PPP 15	PPP 16	PPP 17	PPP 18	PPP 19								
C	lear all PP	P Interfaces											
IP Sourc	es												
	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	🗆 ETH 13	🗆 ETH 14								
	ETH 15	🗆 ETH 16	🔲 ETH 17	🗆 ETH 18	🗆 ETH 19								
0	ETH 20	🔲 ETH 21	ETH 22	🔲 ETH 23	🗆 ETH 24								
0	ETH 25	🔲 ETH 26	🔲 ETH 27										
0	OVPN 0	OVPN 1	OVPN 2										
	PPP 0	PPP 1	PPP 2	PPP 3	PPP 4								

Click the Apply button.

Parameter	Setting	Description	CLI command
Enable Analyser	Selected	This checkbox is used to enable or disable the analyser.	ana o anon "ON″
Maximum packet capture size	1500	The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Common practice is to set it to 1500	ana o maxdata "1500″
Log Size	180	The maximum size of the pseudo file "ana.txt" that is used to store the captured data packets. Common practice is to set at this maximum (180). Notice that the data is compressed so more than 180Kb	ana o logsize "180″

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

IP Routing Table														
Destination	Gateway	Metric	Protocol	Idx	Interface	Status								
172.16.0.0/24	172.16.0.100	1	Local	-	ETH 12	UP								
172.20.1.72/29	172.20.1.76	1	Local	-	PPP 1	UP								
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP								
efault Routes														
Destination	Gateway	Metric	Protocol	Idx	Interface	Status								
0.0.0/0	172.16.0.1	2	Static	0	ETH 12	UP								
0.0.0/0	172.20.1.76	3	Static	1	PPP 1	UP								

Management - Network Status > IP Routing Table

Refresh Toggle Src Addr

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 o, routed to ETH 12, correctly "NAT'ed" and then finally transmitted via the Wi-Fi module:

11-12-2014 12:39:13.690	
45 00 00 3C 0B 2C 00 00 80 01 5F DD C0 A8 03 04 E	
08 08 04 04 08 00 4D 41 00 01 00 1A 61 62 63 64MAabcd	
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efghijklmnopqrst	
75 76 77 61 62 63 64 65 66 67 68 69 uvwabcdefghi	
IP (In) From REM TO LOC IFACE: ETH 0	
45 IP Ver: 4	
Hdr Len: 20	
00 TOS: Routine	
Delay: Normal	
Throughput: Normal	
Reliability: Normal	
00 3C Length: 60	
0B 2C ID: 2860	
00 00 Frag Offset: 0	

					Con	iges [.]	tion:		Мау	mal Fr	agr						
	80				TTL				128								
	01					oto:			ICM								
	5F I		2 01						245		0	<u>л</u>					
			3 04 4 04			: IP : IP				.16 .8.		5.4					
	ICM		+ 0+				•		0.0		0						
	08				Тур	e:			ECH	IO R	EQ						
	00				Cod	le:			0		-						
	4D 4	41			Che	ecks	um:		197	77							
				201		2.2	0.12	c 0 0									
 15	 00						9:13. 7F 01		-	 C0	- ^Q	Q1	65		E<.,b e		
							00 01								MAabcd		
							6D 6E								fghijklmnopqrst		
75	76	77 6	1 62	63	64	65	66 67	68	69						wabcdefghi		
	(Fi	nal)	Fro				EM		ACE:	ET	Ή :	12					
45					Ver r Le			4 20									
00				TOS					utin	e							
					Lay:				rmal								
					-	ghpu	t:	Nor	rmal								
				Re]	liab	oili [.]	ty:	Nor	rmal								
00					ngth	1:		60									
0B				ID:		محد	~+ ·	286	60								
00	00				-)ffs stio		0 Nor	rmal								
				0	iges	,			/ Fr		ient	t					
								-	st F	_							
7F				TTL	.:			127	7								
01					oto:			ICN									
62		51 C	-		ecks				212	0 1	1/	21					
	A8 (: IP t IP				2.16 3.8.		. . т	<u>91</u>					
ICN		54 0	•	050		•		0.0		0							
08				Тур	be:			ECH	IO R	EQ							
00				Сос	le:			0									
4D	41			Che	ecks	sum:		197	777								
		11	-12-2	201	1 1	2.2	9:13.	600									
							9815. 9B 18		0F	8F	23	14	85		A(#		
							00 20								L [
							45 00								E		
							08 08								.b eMA		
							65 66								abcdefghijkl		
	6E (72	/3	/4	75 76	//	61	62	63	64	65		nopqrstuvwabcde ghi		
00	07	50 0	9											'	BUT		
Wi-	Fi	rom	LOC	То	REM	1							IFACE	E:	Wi-Fi Module 0		
 08							Vers	ion:					0				
							Туре						Data				
							Subt						Data				
28	aa						Flag Dura		. .				40 STA -	->	AP, Protected		
		21 0	С 9В	18			BSS		••				40				
			3 14				Src.		2								
00	04	2D Ø	4 B4	4C			Dst.										
05	EØ						Frag						0				
00	20	- D - 2	2 00	00	00	00	Sequ			+	De		94				
			00 6 00 6		00	00	TKIP			сy	Pai	am					
08		55 0	00	50			Туре						IP				
IP:							770										
45				IP	Ver	·:		4									

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

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

11-12-3	2014 12:39:13.7	700		
		04 F0 21 0C 9B :	18	,#!
		03 00 00 00 08 0		····L·····
		7A FD 08 08 04 0		E<=4.z
		00 1A 61 62 63 0		eUAabcd
		6F 70 71 72 73		efghijklmnopqrst
		68 69 B1 29 06		uvwabcdefghi.)
15 AF DØ 9B	05 01 05 00 07	00 09 01 29 00 0	50	
15 / 00 50				
Wi-Fi From REM			IFACE:	: Wi-Fi Module 0
08 02	Versi	ion:	0	
	Type:	:	Data	
	Subty	/pe:	Data	
	Flags	5:	AP ->	STA
2C 00	Durat	tion:	44	
00 0E 8E 23 14	85 Dst.	MAC		
04 F0 21 0C 9B				
00 04 2D 04 B4				
10 10	Fragn		0	
	Seque		257	
AA AA 03 00 00	00 LLC S	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		
11-12-2			~ ~	_
45 00 00 3C 3D	AB 00 00 34 01	7A FD 08 08 04 (04	E<=4.z
		00 1A 61 62 63 0	- A	eUAabcd

			of the international states of
		6E 6F 70 71 72 73 74 67 68 69 B1 29 06 80	efghijklmnopqrst uvwabcdefghi.)
15 AF DØ 9B		07 00 05 01 25 00 00	
	m REM TO LOC	IFACE: ETH 12	
45	IP Ver:	4	
00	Hdr Len:	20 Davitina	
00	TOS: Delay:	Routine Normal	
	Throughput:	Normal	
	Reliability		
00 3C	Length:	60	
3D AB	ID:	15787	
00 00	Frag Offset		
	Congestion:	Normal May Enggment	
		May Fragment Last Fragment	
34	TTL:	52	
01	Proto:	ICMP	
7A FD	Checksum:	31485	
08 08 04 04		8.8.8.8	
C0 A8 01 65	Dst IP:	192.168.1.101	
ICMP: 00	Type:	ECHO REPLY	
00	Code:	0	
55 41	Checksum:	21825	
	2014 12:39:13.		
		7B 5E 08 08 04 04 00 1A 61 62 63 64	E<=2.{^ UAabcd
		6F 70 71 72 73 74	efghijklmnopqrst
	63 64 65 66 67		uvwabcdefghi
IP (Final) Fro		IFACE: ETH 0	
45	IP Ver: Hdr Len:	4 20	
00	TOS:	Routine	
	Delay:	Normal	
	Throughput:	Normal	
	Reliability:	Normal	
00 3C	Length:	60	
3D AB 00 00	ID: Frag Offset:	15787 0	
00 00	Congestion:	Normal	
	0	May Fragment	
		Last Fragment	
32	TTL:	50	
01 78 FF	Proto:	ICMP	
7B 5E 08 08 04 04	Checksum: Src IP:	31582 8.8.8.8	
C0 A8 03 04	Dst IP:	192.168.3.4	
ICMP:			
00	Type:	ECHO REPLY	
00 55 41	Code: Checksum:	0	
	(hocksum ·	21825	

4.2.2 Failure on Access Point WAN Connection

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

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

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

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

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

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

Management - Network Status > IP Routing Table

IP Routing Table														
Destination	Gateway	Metric	Protocol	Idx	Interface	Status								
172.16.0.0/24	172.16.0.100	-	Local	-	ETH 12	00S								
172.20.1.72/29	172.20.1.76	1	Local	-	PPP 1	UP								
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP								
6 H B I														
efault Routes														
Destination	Gateway	Metric	Protocol	Idx	Interface	Status								
0.0.0/0	172.20.1.76	3	Static	1	PPP 1	UP								
0.0.0/0	172.16.0.1		Static	0	ETH 12	005								

Refresh Toggle Src Addr

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

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

		11	L-12	2-26	914	12	2:40	9:41	1.00	90			-					
45	00	00	3C	13	ED	00	00	80	01	57	1C	C0	A8	03	04		E <w< td=""><td></td></w<>	
08	08	04	04	08	00	4D	3F	00	01	00	1C	61	62	63	64		M?abcd	
65	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74		efghijklmnopqrst	
75	76	77	61	62	63	64	65	66	67	68	69						uvwabcdefghi	
																	-	
IP	(Ir	1) F	ron	n RE	EM 1	ΓΟ Ι	-0C			IFACE: ETH 0								
45					IΡ	Ver	r:			4								
					Hdr	۲ Le	en:			20								
00	00 TOS:						Rou	ıtir	ne									
Delay:							Normal											
Throughput:										Normal								

00 3C 13 ED 00 00	Reliability: Length: ID: Frag Offset: Congestion:	Normal 60 5101 0 Normal May Fragment Last Fragment	
80	TTL:	128	
01	Proto:	ICMP	
57 1C	Checksum:	22300	
C0 A8 03 04 08 08 04 04	Src IP: Dst IP:	192.168.3.4 8.8.8.8	
ICMP:		0.0.0	
08	Type:	ECHO REQ	
00	Code:	0	
4D 3F	Checksum:	19775	
11-12-2	2014 12:40:41.00	0	
	ED 00 00 7F 01 F		E<6%T.>
	00 4D 3F 00 01 00 6A 6B 6C 6D 6E 6		<pre>M?abcd efghijklmnopgrst</pre>
	63 64 65 66 67 68		uvwabcdefghi
			U
IP (Final) From 45	n LOC TO REM II IP Ver: 4	ACE: PPP 1	
45	Hdr Len: 20		
00		outine	
	,	ormal	
	01	ormal ormal	
00 3C	Length: 60		
13 ED		101	
00 00	Frag Offset: 0 Congestion: No	ormal	
	-	ay Fragment	
	La	ast Fragment	
7F		27 MD	
01 F5 36		CMP 2774	
25 54 01 3E		7 <mark>.84.1.62</mark>	
08 08 04 04	Dst IP: 8	<mark>.8.8.8</mark>	
ICMP: 08	Type: E	CHO REQ	
00	Code: 0		
4D 3F	Checksum: 19	9775	

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

11-12-2014 12:40:41.	060	
45 00 00 3C 56 EA 00 00 2E 01 25 54 01 3E 00 00 55 3F 00 01 65 66 67 68 69 6A 6B 6C 6D 6E 75 76 77 61 62 63 64 65 66 67	00 1C 61 62 63 64 6F 70 71 72 73 74	E <v %T.>U?abcd efghijklmnopqrst uvwabcdefghi</v
IP (In) From REM TO LOC 45 IP Ver: Hdr Len:	IFACE: PPP 1 4 20	

00	TOS: Delay: Throughput: Reliability:	Routine Normal Normal Normal
00 3C	Length:	60
56 EA	ID:	22250
00 00	Frag Offset:	0
00 00	Congestion:	Normal
	congeseroni	May Fragment
		Last Fragment
2E	TTL:	46
01	Proto:	ICMP
03 3A	Checksum:	826
08 08 04 04		8.8.8.8
25 54 01 3E		37.84.1.62
ICMP:		
00	Type:	ECHO REPLY
00	Code:	0
55 3F	Checksum:	21823
11-12-2014	4 12:40:41.060	
45 00 00 3C 56 EA	00 00 2C 01 68	1F 08 08 04 04 E
C0 A8 03 04 00 00		
65 66 67 68 69 6A		
75 76 77 61 62 63	64 65 66 67 68	69 uvw

E <v,.h< th=""><th></th></v,.h<>	
U?abcd	
efghijklmnopqrst	
uvwabcdefghi	

IP (Final) Fro	m 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:

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	1	Local	-	ETH 12	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP
efault Routes						
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	172.20.1.75	3	Static	1	PPP 1	UP

Management - Network Status > IP Routing Table

Refresh Toggle Src Addr

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

	2-2014 12:43:32.510		
	3C 16 4B 00 00 80 01		E<.KT
	04 08 00 4D 3E 00 01		M>abcd
	68 69 6A 6B 6C 6D 6E		efghijklmnopqrst
/5 /6 //	61 62 63 64 65 66 67	68 69	uvwabcdefghi
IP (In) F	rom REM TO LOC	IFACE: ETH 0	
45	IP Ver:	4	
45			
	Hdr Len:	20	
00	TOS:	Routine	
	Delay:	Normal	
	Throughput:	Normal	
	Reliability:	Normal	
00 3C	Length:	60	
16 4B	ID:	5707	
00 00	Frag Offset:	0	
	Congestion:	Normal	
		May Fragment	
		Last Fragment	
80	TTL:	128	
01	Proto:	ICMP	
54 BE	Checksum:	21694	
CØ A8 Ø3	04 Src IP:	192.168.3.4	
08 08 04	04 Dst IP:	8.8.8	
ICMP:			
08	Type:	ECHO REQ	

	00 4D	3E				Code: Check	sum:		0 19774	1				
		1	11-1	L2-2	2014	12:	43:32	2.510						
45	00	00	3C	16	4B	00 00	7F 6	91 57	5D C	8A 6	01	65	E<.KW]e	
80	80	04	04	08	00	4D 3E	00 0	00 10	1D 63	1 62	63	64	M>abcd	
65	66	67	68	69	6A	6B 6C	6D 6	5E 6F	70 7	1 72	73	74	efghijklmnopqrst	
75	76	77	61	62	63	64 65	66 6	67 68	69				uvwabcdefghi	
													-	
	(Fi	inal	L) F	ron		ос то	REM		ACE: I	ETH 1	12			
45						Ver:		4						
						Len:		20						
00					TOS				utine					
						ay:			rmal					
						oughp			rmal					
						iabil	ity:		rmal					
00						ngth:		60						
16					ID:			576	97					
00	00					ng Off		0	,					
					Cor	ngesti	on:		rmal					
								-	/ Frag	-				
7F					TTL			127	st Fra 7	agiliei	IL.			
01						to:		IC						
57	5D					cksum	•		" 365					
		01	65			IP:	•		2.168	.1.10	91			
		04				IP:			3.8.8					
ICN	1P:													
08					Тур	e:		ECł	IO RE	2				
00					Coc	le:		0						
4D	3E				Che	cksum	:	197	774					
	41				2014			2.510			11	0.5	A/ I #	
						21 OC							.A(#	
						F0 08 08 00							EE<.K	
						01 65							W]eM>	
						63 64								
			10	<u> </u>									abcdetghijkl	
			70	71		73 74					64		<pre>abcdefghijkl mnopgrstuvwabcde</pre>	
	67			71		73 74					64		mnopqrstuvwabcde	
	67	6F		71		73 74					64		• . • .	
		6F 68	69		72	73 74 REM					64	65	mnopqrstuvwabcde	
	·Fi	6F 68	69		72		75 7		61 63		64	65	mnopqrstuvwabcde fghi	
Wi-	·Fi	6F 68	69		72		75 7 Ver Typ	rsion	61 63		64	65 IFACE Ø Data	mnopqrstuvwabcde fghi	
Wi-	·Fi	6F 68	69		72		75 7 Ver Typ Sub	rsion be: otype	61 63		64	65 IFACE Ø Data Data	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
<mark>Wi-</mark> 08	<mark>·Fi</mark> 41	6F 68	69		72		75 Ver Typ Sub Fla	rsion be: otype ags:	61 6: :		64	65 IFACE Ø Data Data STA -:	mnopqrstuvwabcde fghi	
<mark>Wi-</mark> 08 28	• <mark>Fi</mark> 41	6F 68 Fro	69 om L	.OC	72 To		75 Ver Typ Sub Fla Dur	rsion be: otype ags: ration	61 6: :		64	65 IFACE Ø Data Data	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
<mark>Wi</mark> - 08 28 04	• <mark>Fi</mark> 41 00 F0	6F 68 Fro	69 om L 0C	.OC 9B	72 To 18		Ver Typ Sub Fla Dur BSS	rsion be: btype ags: ration 5 ID	61 6: : :		64	65 IFACE Ø Data Data STA -:	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00	•Fi 41 00 F0 0E	6F 68 Frc 21 8E	69 0m L 0C 23	-OC 9B 14	72 To 18 85		Ver Typ Sub Fla Dur BSS Sro	rsion be: btype ags: ration 5 ID c. MAG	61 6: : :: :		64	65 IFACE Ø Data Data STA -:	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 00	•Fi 41 00 F0 0E 04	6F 68 Fro	69 0m L 0C 23	-OC 9B 14	72 To 18 85		Ver Typ Sub Fla Dur BSS Sro Dst	nsion be: btype ags: nation 5 ID c. MAG	61 6: : ::		64	65 IFACE Ø Data Data STA -: 40	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00	•Fi 41 00 F0 0E 04	6F 68 Frc 21 8E	69 0m L 0C 23	-OC 9B 14	72 To 18 85		Ver Typ Sub Fla Dur BSS Sro Dst Fra	rsion be: btype ags: ration 5 ID c. MAG t. MAG	61 6:		64	65 IFACE Ø Data Data STA -: 40	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 00 08	Fi 41 00 F0 0E 04 F0	6F 68 Frc 21 8E 2D	69 om l 0C 23 04	9B 14 B4	72 To 18 85 4C	REM	Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec	rsion be: btype ags: ration 5 ID c. MAG t. MAG agment quence	61 6:	2 63		65 IFACE Ø Data Data STA -: 40	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 08 08	Fi 41 00 F0 0E 04 F0 20	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00		Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec TKI	rsion be: btype ags: ration 5 ID c. MAG t. MAG agment quence IP Sec	61 6:	2 63		65 IFACE Ø Data Data STA -: 40	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 08 08	Fi 41 00 F0 0E 04 F0 20 AA	6F 68 Frc 21 8E 2D	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00	REM	Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec TKI	rsion be: btype ags: ration 5 ID c. MAG t. MAG agment quence IP Sec 5 SNAF	61 6:	2 63		65 IFACE Ø Data Data STA -: 40	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 00 08 00 AA	Fi 41 00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00	REM	Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec TKI	rsion be: btype ags: ration 5 ID c. MAG t. MAG agment quence IP Sec 5 SNAF	61 6:	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08	Fi 41 00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00	REM	Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec TKI	rsion be: btype ags: ration 5 ID c. MAG t. MAG agment quence IP Sec 5 SNAF	61 6:	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 IP:	Fi 41 00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP	REM 00 00	Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec TKI	rsion be: btype ags: btion 5 ID c. MAG agment fuence IP Sec 5 SNAF be:	61 6:	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 IP:	Fi 41 00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP	REM 00 00 Ver: `Len:	Ver Typ Sub Fla Dur BSS Sro Dst Fra Sec TKI	rsion pe: otype ags: ration 5 ID c. MAG t. MAG t. MAG c. SNAF pe: 4 20 Rou	61 63	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 00 08 00 AA 08 IP: 45	Fi 41 00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del	REM 00 00 Ver: Len: : : .ay:	Ver Typ Sub Fla Dur BSSS Src Dst Fra See TK1 LLC Typ	rsion pe: ptype ags: ration 5 ID 1. MAG 10 SNAF 20 SNAF 20 Rou Nor	61 63	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 28 04 00 00 08 00 AA 08 IP: 45	Fi 41 00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del Thr	REM 00 00 Ver: Len: ay: roughp	Ver Typ Sub Fla Dur BSS Src Dst Fra Sec TKI LLC Typ	76 77 rsion pe: ptype ags: ration 5 ID c. MAG t. MAG agment quence SNAF pe: 4 20 Rou Non Non	61 63	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 1P: 45 00	00 F0 0E 04 F0 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del Thr Rel	REM 00 00 Ver: Len: ay: roughp .iabil	Ver Typ Sub Fla Dur BSS Src Dst Fra Sec TKI LLC Typ	76 77 rsion pe: ptype ags: ration 5 ID c. MAG t. MAG agment quence SNAF pe: 4 20 Rou Non Non	61 63	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 1P: 45 00	 Fi 41 00 F0 04 F0 20 AA 00 30 	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del Thr Rel Ler	REM 00 00 Ver: Len: ay: roughp iabil agth:	Ver Typ Sub Fla Dur BSS Src Dst Fra Sec TKI LLC Typ	76 77 rsion pe: ptype ags: ration 5 ID 5 ID	61 6: :: :: :: :: :: :: :: :: ::	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 1P: 45 00 00 16	Fi 41 00 F0 0E 04 F0 20 AA 00 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del Thr Rel Ler ID:	REM 00 00 Ver: Len: ay: oughp iabil	Ver Typ Sut Fla Dur BSS Src Dst Fra Sec TK1 LLC Typ	rsion be: btype ags: ration 5 ID 5. MAG 10 SNAF 00 5 SNAF 00 5 SNAF 00 5 SNAF 00 8 OU 8 OU 8 OU 8 OU 8 OU 8 OU 8 OU 8 OU	61 6: :: :: :: :: :: :: :: :: ::	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 1P: 45 00	Fi 41 00 F0 0E 04 F0 20 AA 00 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del Thr Rel Ler ID: Fra	REM 00 00 Ver: Len: ay: oughp iabil gth: ag Off	Ver Typ Sub Fla Dur BSS Srcc TKI LLC Typ ut: ity:	76 77 rsion pe: ptype ags: ration 5 ID C. MAG t. MAG agment quence SNAF pe: 4 20 Rou Non Non 60 570 0	61 6: 	2 63		65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	
Wi- 08 04 00 00 08 00 AA 08 1P: 45 00 00 16	Fi 41 00 F0 0E 04 F0 20 AA 00 20 AA 00	6F 68 Frc 21 8E 2D 8C	69 om l 0C 23 04 20	9B 14 B4	72 To 18 85 4C 00 00 IP Hdr TOS Del Thr Rel Ler ID: Fra	REM 00 00 Ver: Len: ay: oughp iabil	Ver Typ Sub Fla Dur BSS Srcc TKI LLC Typ ut: ity:	76 77 rsion pe: ptype ags: ration 5 ID 5 ID 5 C 4 20 Rou Non Non 60 570 0 Non	61 6: :: :: :: :: :: :: :: :: ::	2 63	∽am	65 IFACE Ø Data Data STA -: 40 Ø 143	mnopqrstuvwabcde fghi : Wi-Fi Module 0	

		Last Fragment
7F	TTL:	127
01	Proto:	ICMP
57 5D	Checksum:	22365
C0 A8 01 65	Src IP:	192.168.1.10
08 08 04 04	Dst IP:	8.8.8

And also the reply:

----11-12-2014 12:43:32.520 - - -08 02 2C 00 00 0E 8E 23 14 85 04 F0 21 0C 9B 18 ...,....#....!... 00 04 2D 04 B4 4C 10 11 AA AA 03 00 00 00 08 00 ..-..L....... 45 00 00 3C 3E 4D 00 00 34 01 7A 5B 08 08 04 04 E..<>M..4.z[.... C0 A8 01 65 00 00 55 3E 00 01 00 1D 61 62 63 64 ...e..U>....abcd 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efghijklmnopqrst 75 76 77 61 62 63 64 65 66 67 68 69 AA 01 A3 09 uvwabcdefghi.... 31 19 A4 2C 1.., Wi-Fi From REM To LOC IFACE: Wi-Fi Module 0 Version: 08 02 0 Type: Data Subtype: Data Flags: AP -> STA 2C 00 Duration: 44 00 0E 8E 23 14 85 Dst. MAC BSS ID 04 F0 21 0C 9B 18 00 04 2D 04 B4 4C Src. MAC 11 10 Fragment: 0 273 Sequence: AA AA 03 00 00 00 LLC SNAP IΡ 08 00 Type: IP: IP Ver: 45 4 Hdr Len: 20 TOS: Routine 00 Delay: Normal Throughput: Normal Reliability: Normal 00 3C Length: 60 3E 4D 15949 ID: 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 Src IP: 8.8.8.8 C0 A8 01 65 Dst IP: 192.168.1.101 ----11-12-2014 12:43:32.520 45 00 00 3C 3E 4D 00 00 34 01 7A 5B 08 08 04 04 E..<>M..4.z[.... C0 A8 01 65 00 00 55 3E 00 01 00 1D 61 62 63 64 ...e..U>....abcd 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efghijklmnopqrst 75 76 77 61 62 63 64 65 66 67 68 69 AA 01 A3 09 uvwabcdefghi.... 31 19 A4 2C 1.., IP (In) From REM TO LOC IFACE: ETH 12 IP Ver: 45 4 Hdr Len: 20 Routine 00 TOS: Delay: Normal Throughput: Normal Reliability: Normal

	00 3C 3E 4D	Length: ID:	60 15949	
	00 00	Frag Offset:	0	
	00 00	Congestion:	Normal	
		congestion	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	
	11-12-20	14 12:43:32.5	20	
4			7A BC 08 08 04 04	E<>M2.z
			00 1D 61 62 63 64	U>abcd
6	5 66 67 68 69 6	A 6B 6C 6D 6E	6F 70 71 72 73 74	efghijklmnopqrst
7	5 76 77 61 62 63	3 64 65 66 67	68 69	uvwabcdefghi
	P (Final) From		IFACE: ETH 0	
4		P Ver:	4	
~		dr Len:	20	
0			Routine Normal	
		elay: hroughput:	Normal	
		eliability:	Normal	
0		ength:	60	
		D:	15949	
0	0 00 Fi	rag Offset:	0	
	C	ongestion:	Normal	
			May Fragment	
			Last Fragment	
3		TL:	50	
0		roto:	ICMP	
		hecksum:	31420	
			8.8.8.8 192.168.3.4	
	0 A8 05 04 <mark>D</mark> CMP:	St 17.	192.100.3.4	

ECHO REPLY 0 21822

ICMP: 00 00 55 3E <mark>Type:</mark> Code: Checksum: - -

---_ _

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.

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	1	Local	-	ETH 12	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP
efault Routes						
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	172.20.1.75	3	Static	1	PPP 1	UP

Management - Network Status > IP Routing Table

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

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

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

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

Management - Network Status > IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
100 100 0 0/04	100 100 0 1		the sector		ETU O	110
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP
	Gateway	ı Metric	Protocol	Idx	Interface	Statu
efault Routes		I Metric 3				

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

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
172.20.1.72/29	172.20.1.75	1	Local	-	PPP 1	UP
192.168.1.0/24	192.168.1.101	1	Local	-	ETH 12	UP
192.168.3.0/24	192.168.3.1	1	Local	-	ETH 0	UP
efault Routes						
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	172.20.1.75	3	Static	1	PPP 1	UP

Refresh Toggle Src Addr

5 TRANSPORT CONFIGURATION FILES

5.1 Configuration File

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

```
Command: config c show
Command result
wifi 0 country "United States"
wifinode 0 descr "Wi-Fi Client (WAN)"
wifinode 0 ssid "Access Point WPA"
wifinode 0 mode "client"
wifinode 0 security "wpa2psk"
wifinode 0 wpatype "aes"
wifinode 0 esharedkey "*******"
eth 0 IPaddr "192.168.3.1"
eth 12 dhcpcli ON
eth 12 mask ""
eth 12 do nat 2
eth 12 firewall ON
eth 12 pingip "8.8.8.8"
eth 12 pingint 10
eth 12 pingsiz 1
eth 12 wificli ON
eth 12 physadd -1
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def route 0 11 ent "ETH"
def_route 0 ll_add 12
def_route 1 ll_ent "PPP"
def_route 1 ll_add 1
def_route 1 upmetric 2
def_route 1 metric 2
dhcp 0 IPmin "192.168.3.3"
dhcp 0 IPrange 117
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.3.1"
dhcp 0 DNS "192.168.3.1"
sntp 0 server "time.devicecloud.com"
sntp 0 offset -8
sntp 0 dstonmon 3
sntp 0 dstonday 13
sntp 0 dstoffmon 11
sntp 0 dstoffday 6
```

dyndns 0 ifent "default" snmp 0 v1enable OFF snmp 0 v2cenable OFF snmp 0 v3enable OFF services 0 telnet OFF services 0 http OFF services 0 https ON services 0 ssh OFF services 0 ftp OFF services 0 asytcp OFF ppp 0 timeout 300 ppp 1 name "W-WAN" ppp 1 phonenum "*98*5#" ppp 1 epassword "KD5lSVJDVVg=" ppp 1 IPaddr "0.0.0.0" ppp 1 timeout 0 ppp 1 use_modem 1 ppp 1 aodion 1 ppp 1 autoassert 1 ppp 1 pwr_dly 40 ppp 1 r_chap OFF ppp 3 defpak 16 ppp 4 defpak 16 web 0 prelogin info ON ftpcli 0 hostname "ftp1.digi.com" ftpcli 0 directory "support/firmware/transport/MC7354_carrier_firmware" modemcc 0 info asy add 7 modemcc 0 apn "Your.APN.goes.here" modemcc 0 link_retries 30 modemcc 0 stat_retries 30 modemcc 0 sms_interval 1 modemcc 0 sms access 1 modemcc 0 sms concat 0 modemcc 0 apn_2 "Your.APN.goes.here" modemcc 0 link_retries_2 30 modemcc 0 stat retries 2 30 modemcc 0 sms_interval_2 1 modemcc 0 sms_access_2 1 modemcc 0 sms_concat_2 0 ana 0 anon ON ana 0 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 tremto 1200 user 0 access 0 user 1 name "username" user 1 epassword "*******" user 1 access 0

```
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
cloud 0 ssl ON
Power Up Profile: 0
OK
```

5.2 Firewall Rules

The firewall rules used in this AN are the following:

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

pass break end

5.3 Hardware and Firmware

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

```
Command: ati5
Command result
```

```
Digi TransPort WR44-L500-NE1-SU Ser#:xxxxxx HW Revision: 2202a
Software Build Ver5.2.15.4. Jun 22 2016 12:24:12 LW
ARM Bios Ver 7.56u v45 800MHz B995-M1003-F80-O0,0 MAC:00042d080153
Power Up Profile: 0
Async Driver
                          Revision: 1.19 Int clk
Wi-Fi
                          Revision: 2.0
Ethernet Port Isolate Driver Revision: 1.11
Firewall
                          Revision: 1.0
                          Revision: 1.0
EventEdit
Timer Module
                          Revision: 1.1
(B)USBHOST
                          Revision: 1.0
L2TP
                          Revision: 1.10
PPTP
                          Revision: 1.00
                          Revision: 1.00
TACPLUS
                          Revision: 0.00
MODBUS
                          Revision: 0.01
MySQL
RealPort
                          Revision: 0.00
```

MultiTX	Revision:	
LAPB	Revision:	1.12
X25 Layer	Revision:	1.19
MACRO	Revision:	1.0
PAD	Revision:	1.4
X25 Switch	Revision:	1.7
V120	Revision:	
TPAD Interface	Revision:	
GPS	Revision:	
TELITUPD	Revision:	
SCRIBATSK	Revision:	
BASTSK	Revision:	
PYTHON	Revision:	
CLOUDSMS	Revision:	
ARM Sync Driver	Revision:	1.18
TCP (HASH mode)	Revision:	
TCP Utils	Revision:	
PPP	Revision:	
WEB	Revision:	
SMTP	Revision:	
FTP Client	Revision:	
FTP	Revision:	
IKE	Revision:	
PollANS	Revision:	
PPPOE	Revision:	
BRIDGE	Revision:	
-	Revision:	
FLASH Write	Revision:	
Command Interpreter	Revision:	
SSLCLI	Revision:	
OSPF	Revision:	
BGP	Revision:	
QOS	Revision:	
PWRCTRL	Revision:	
RADIUS Client	Revision:	
SSH Server	Revision:	
SCP	Revision:	
SSH Client	Revision:	
CERT	Revision:	
LowPrio	Revision:	
Tunnel	Revision:	
OVPN	Revision:	
TEMPLOG	Revision:	
QDL	Revision:	
OK		1.0