Application Note 7

How to configure TransPort WR for Cellular Problem Detection and Recovery using Sure Link Wizard

September 2020

Contents

1 Introduction 3

1.1 Outline 3

1.2 Assumptions 4

1.3 Corrections 4

1.4 Version 4

2 Cellular module problem detection 5

2.1 Cellular Modem Module Reset due to unsuccessful connection attempts 5

2.2 Cellular Module reset due to status retrieval failures 7

2.3 TransPort reboot due to connection failures 11

3 Dead Cellular Link detection & recovery using the Sure Link Wizard 8

3.1 Passive Techniques 10

3.1.1 Stateful Route Inspection: TCP/UDP/ICMP monitoring with Firewall 14

3.1.1.1 TCP Traffic Monitoring: configuration and testing 15

3.1.1.2 UDP Traffic Monitoring: configuration and testing 17

3.1.1.3 ICMP traffic Monitoring: configuration and testing 20

3.1.2 Deactivate PPP via Unanswered TX packets 23

3.1.3 Deactivate PPP via No traffic received for a certain period of time 26

3.2 Active Techniques 29

3.2.1 Deactivate cellular link via PING failure detection (no firewall) 30

3.2.2 Generate & monitor traffic with the firewall 33

3.2.2.1 Generate & monitor UDP traffic 33

3.2.2.2 Generate & monitor ICMP traffic 37

3.2.3 Dead link detected using IPsec tunnel DPD 40

1 INTRODUCTION

1.1 Outline

This document will consider a TransPort WR router with a W-WAN PPP link to the Internet Network:

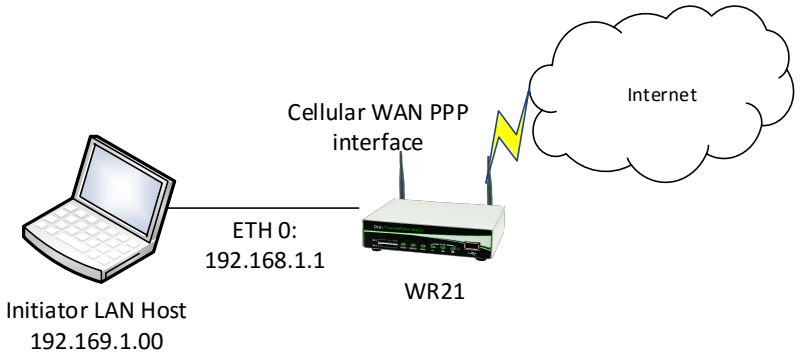


Figure 1-1: Overview Diagram

Cellular Wireless WAN (W-WAN) technologies have proven to be extremely reliable. However, the consequences of losing contact with a remote unit are so severe in terms of recovery costs (site visits, etc.) that it warrants extra precautions.

Such a problem might occur on very rare occasions due to power spikes, interference, or the network blocking the current connection due to some error or failure.

TransPorts WR offer a number of built-in features that are designed to recover from any cellular modem module or network problems that may occur without user intervention, if this is possible.

Some of these options are Passive:

- They work simply by monitoring traffic on the cellular network and spotting problems.

Some of these options are Active:

- They work by actually generating traffic on the cellular network. The Active options have the advantage of working even when the hosts on the TransPort's Ethernet network are not sending packets to the cellular network. The disadvantage is that data charges may be incurred by your cellular provider.

NOTE: If a speedy recovery from the problem is not required then the amount of traffic generated for the active options can be set so low as to be of negligible cost.

Almost all those methods are easily configurable via the SureLink wizard in a step by step and clearly explained procedure that will be shown in this document.

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.

Configuration: This application note assumes that the TransPort will be connecting to a cellular network, i.e. GPRS, EDGE, 3G, HSDPA, HSUPA, CDMA or 4G LTE.

Model used for testing: Digi TransPort WR21.

Other Compatible Models: All other Digi TransPort WR products (SarOS) with cellular connectivity.

Firmware versions: All versions

Configuration: This Application Note (AN) assumes that the TransPort WR has basic mobile settings configured (APN, username/password, PIN/PUCK).

About "Cellular": Within this AN, the term cellular may be used interchangeably with Mobile or W-WAN.

1.3 Corrections

Requests for corrections or amendments to this Application Note (AN) 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
1.0	Published: this substitutes old AN007 on Cellular recovering (October 2017)
1.1	Added date, minor fix (September 2020)

2 CELLULAR MODULE PROBLEM DETECTION

In this section, two basic Cellular module problem detection methods will be shown.

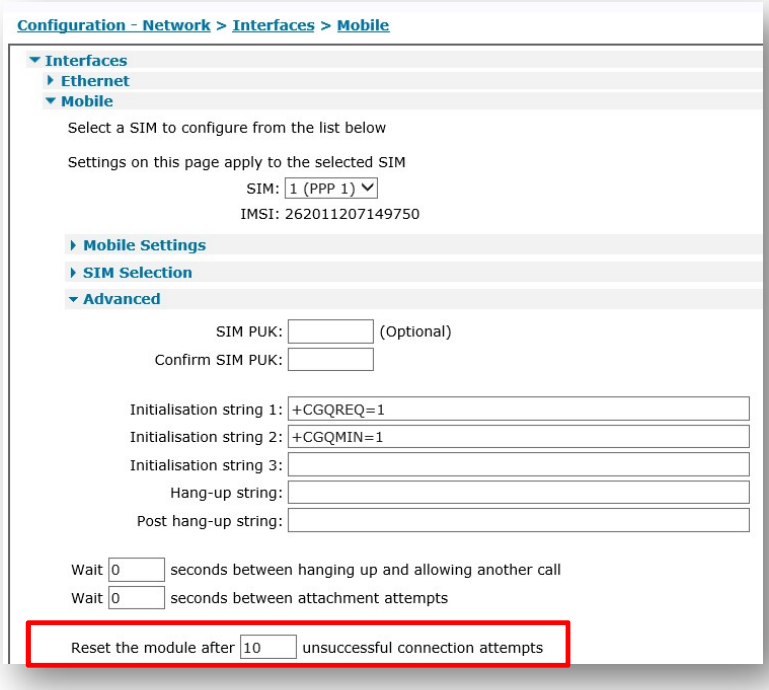
Please note that while the features described in this section can technically be used alone, we recommend that they are used in conjunction with cellular link problem detection techniques, configurable via the SureLink Wizard, which deactivate the cellular link if it stops working, shown in the section 3.

2.1 Cellular Modem Module Reset due to unsuccessful connection attempts

By default all TransPorts WR are shipped with a configuration that will power cycle the TransPort's cellular modem module if 10 or 30 (module dependent) attempts at a Mobile connection in a row fail. This is useful not only because it can recover from an error condition in the module itself, but because it causes the module to re-register with the cellular network. Re-registering with the network is sometimes required to recover from a connection problem.

Configuration: To check if this feature is enabled and what the settings are, navigate to:

CONFIGURATION - NETWORK > INTERFACES > MOBILE > ADVANCED



Check the "**Reset the module after n unsuccessful connection attempts**" parameter: if this is set to a non-zero value "n", this means that after "n" unsuccessful attempts at activating a cellular link, the module (not the TransPort itself) will be power cycled.

Testing:

This feature can be tested by deliberately "sabotaging" the TransPort's attempts to connect to the cellular network, for example, by using an incorrect APN. Next, deactivate the cellular link and then inspect the TransPort's Event Log. Check for an entry like the "GPRS Link Failed → power cycle,Link Retries" entry just below. In this example, the value is 10, so the module reset occurred after 10 failed attempts at connecting.

MANAGEMENT - EVENT LOG

```
14:27:23, 06 Mar 2017,GPRS link failed -> power cycling m,Link Retries
14:27:23, 06 Mar 2017,Modem disconnected on asy 4,26
14:27:22, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:27:12, 06 Mar 2017,PPP 1 down,LL disconnect
14:27:12, 06 Mar 2017,Modem disconnected on asy 4,26
14:27:11, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:27:01, 06 Mar 2017,PPP 1 down,LL disconnect
14:27:01, 06 Mar 2017,Modem disconnected on asy 4,26
14:27:00, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:26:50, 06 Mar 2017,PPP 1 down,LL disconnect
14:26:50, 06 Mar 2017,Modem disconnected on asy 4,26
14:26:49, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:26:39, 06 Mar 2017,PPP 1 down,LL disconnect
14:26:39, 06 Mar 2017,Modem disconnected on asy 4,26
14:26:38, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:26:28, 06 Mar 2017,PPP 1 down,LL disconnect
14:26:28, 06 Mar 2017,Modem disconnected on asy 4,26
14:26:26, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:26:16, 06 Mar 2017,PPP 1 down,LL disconnect
14:26:16, 06 Mar 2017,Modem disconnected on asy 4,26
14:26:15, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:26:05, 06 Mar 2017,PPP 1 down,LL disconnect
14:26:05, 06 Mar 2017,Modem disconnected on asy 4,26
14:26:04, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:25:54, 06 Mar 2017,PPP 1 down,LL disconnect
14:25:54, 06 Mar 2017,Modem disconnected on asy 4,26
14:25:53, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:25:43, 06 Mar 2017,PPP 1 down,LL disconnect
14:25:43, 06 Mar 2017,Modem disconnected on asy 4,26
14:25:42, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:25:32, 06 Mar 2017,PPP 1 down,LL disconnect
14:25:32, 06 Mar 2017,Modem disconnected on asy 4,26
14:25:30, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
14:25:20, 06 Mar 2017,PPP 1 down,LL disconnect
14:25:20, 06 Mar 2017,Modem disconnected on asy 4,26
14:25:19, 06 Mar 2017,Modem dialing on asy 4 #:*98*1#
```

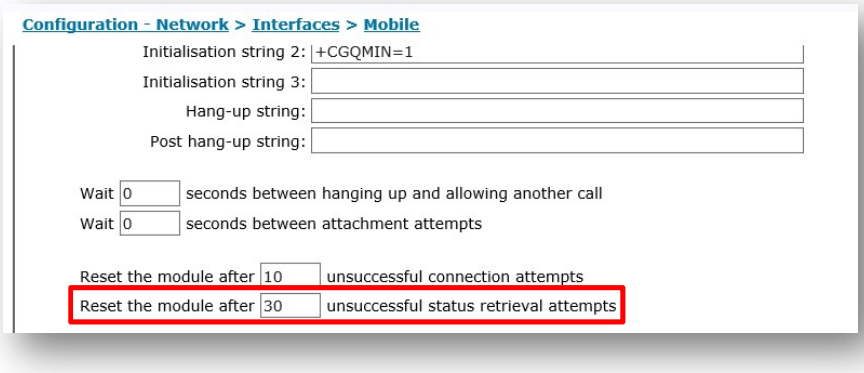
2.2 Cellular Module reset due to status retrieval failures

Additionally, all TransPorts are shipped with a setting that will cause the TransPort to power cycle the cellular module (not the TransPort itself) if 30 attempts at checking the status of the module (e.g. reading the signal strength) fail.

Configuration:

To check if this feature is enabled and what the settings are, navigate to:

CONFIGURATION - NETWORK > INTERFACES > MOBILE > ADVANCED



Check the "**Reset the module after n unsuccessful status retrieval attempts**"parameter: if this is set to a non-zero value "n", this means that after "n" unsuccessful attempts at retrieving the status of the module, the module (not the TransPort itself) will be power cycled.

Testing:

It is not very easy to test this feature as it would be needed to get the module in a state where it doesn't reply to status retrieval attempts. Just for information, below is shown the event that can be found on eventlog section when this setting triggers the power cycle of the module:

MANAGEMENT - EVENT LOG

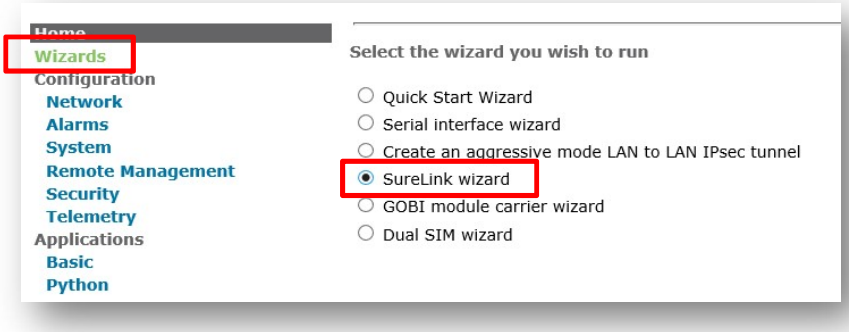
```
12:23:42, 14 Mar 2017,GPRS link failed -> power cycling m,Status request failed
```

3 DEAD CELLULAR LINK DETECTION & RECOVERY USING THE SURE LINK WIZARD

The Sure Link Wizard will help to configure TransPort router to stay connected to the W-WAN (Wireless Wide Area Network) under adverse conditions. This can be achieved by a variety of features designed to recover from network and other problems.

In the previous section, has been shown how the automatic power cycling of the internal Wireless WAN radio will occur if ever the PPP link to the network cannot be established. In the event of a problem occurring when the PPP link is already up, some other mechanisms must be employed to detect the "dead link" and deactivate it. This wizard will help to configure the most appropriate dead link detection technique.

To access to the wizard, navigate to the “Wizards” section from the left main menu on the WEB User Interface:



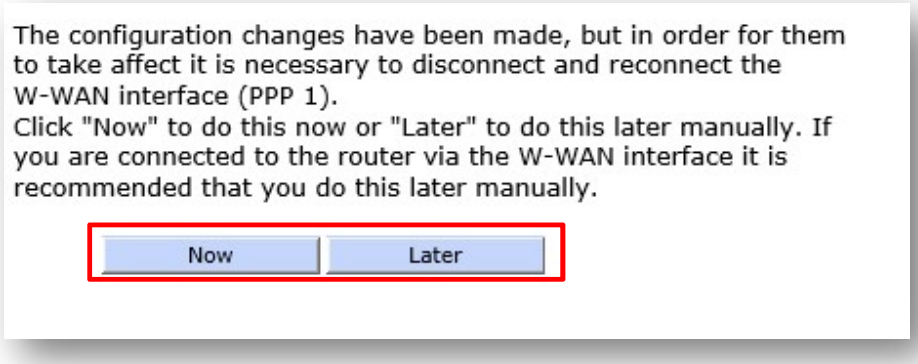
Select “Surelink Wizard” and click on “Next”.

The first 3 pages displayed after selecting the SureLink wizard are for information only and explain what the SureLink wizard is used for and the differences between the Active and Passive link failure detection methods (those details will be reported later on this document), click on “next” to proceed.

After that, a choice is to be made between passive or active types of dead link detection techniques, all of them will be explained in the following sections.

In general, when an option is selected, the wizard will prompt for configuration parameters that relate to the chosen option.

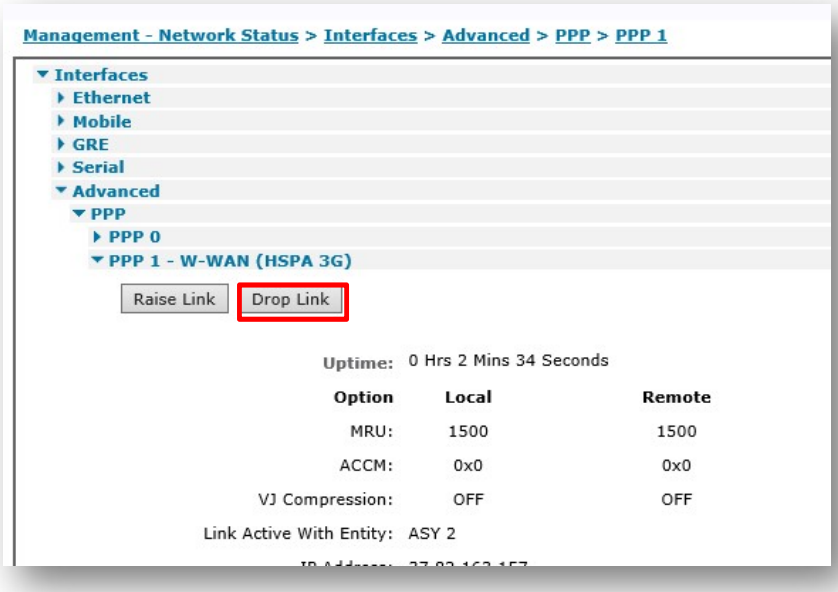
Note: when the wizard will perform changes on the PPP interface, it will be asked to re-activate the PPP interface in order to have the configuration changes taking effect:



In order to test immediately this function, click on “Now”.

If, instead, you prefer to do it later (for example if you are connected to the router via the cellular interface) click on “Later”. In this case, you will need to do this manually later, after the wizard procedure is completed, going to Management - Network Status > Interfaces > Advanced > PPP > PPP 1 and click on “Drop Link” (and then, eventually, on “Raise Link” if the PPP is not configured as default to automatically reconnect):

MANAGEMENT - NETWORK STATUS > INTERFACES > ADVANCED > PPP > PPP 1



Then, the Wizard will also ask to save settings, so, follow the link and save the configuration:

3.1 Passive Techniques

Passive techniques work by monitoring data that would be sent over the W-WAN network anyway. As it is necessary for data to be sent in order to detect a problem, these techniques are only suitable if the equipment on the router's LAN (Local Area Network) regularly sends data over the W-WAN.

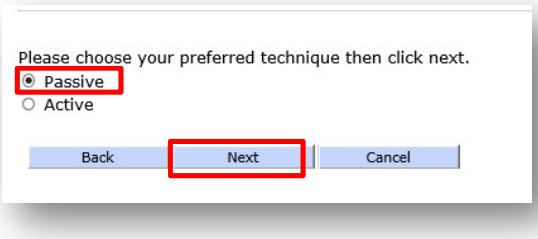
The main advantages of passive techniques are:

- No additional data charges (if your mobile operator charges you for data)
- In a hub and spoke deployment, no additional load will be placed on equipment at the hub

The main disadvantages are:

- If the equipment on the LAN does not send data and a problem with the connection manifests, it will not be possible to connect to the router or the router's LAN remotely until the equipment on the LAN sends data.
- As equipment on the LAN needs to send data before some problems can be detected, if a problem does occur, the equipment on the LAN will be subject to delays when it first tries to send data. This is because it will take the router a certain amount of time to detect and recover from the network problem.

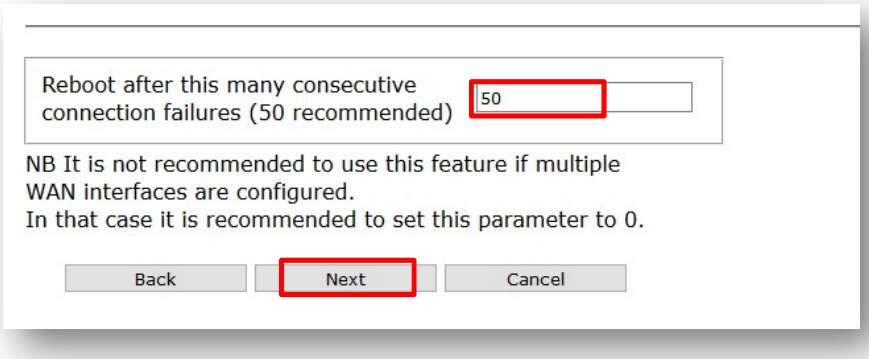
In order to proceed with one of the Passive Techniques, click on “Passive” and, again, on “Next”:



The different options for Passive Techniques will be shown in the next screens and will be discussed in the following sections.

3.1.1 TransPort WR reboot due to connection failures

The first passive option shown is the following:



Under some very rare circumstances, it may be necessary to reboot the TransPort itself to recover from a serious cellular issue. This has been shown to help in situations where the extra time required to reboot the router can help the mobile operator to recover from a problem in their network (i.e. the network "objects" to rapid re-registrations).

This is a passive error detection technique designed to be used if the automatic W-WAN module power cycle technique fails. THIS IS NORMALLY NOT REQUIRED AND NORMALLY NOT RECOMMENDED, in particular if there are multiple WAN interfaces configured. In that case that parameter should be set to 0.

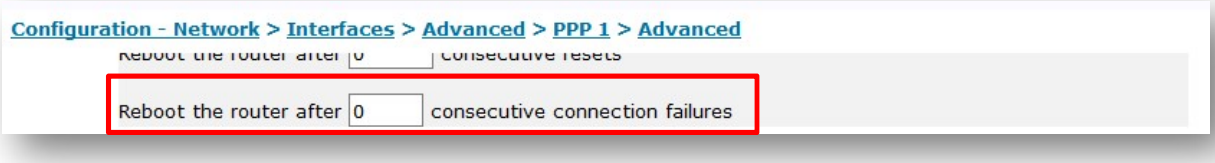
When used, that value should be enough high, for the purpose if testing we set it as 10 but the suggested value is 50 as shown in the Wizard.

Note: this value MUST ALWAYS be significantly larger than the "Reset the module after n unsuccessful connection attempts" value (if used) explained in the previous section.

Clicking "next" will direct to other passive techniques that can be used in conjunctions with that one. When finish the Wizard with another technique configured, this setting will be applied.

If you need just to configure or change this setting, that can be found on the WEB UI:

CONFIGURATION - NETWORK > INTERFACES > ADVANCED > PPP 0-9 > PPP 1 – W-WAN > ADVANCED



To activate the configuration changes, navigate to PPP connection status page (**Management - Connections > PPP connections > PPP 1 – W-Wan**) and click on the "Drop Link" button. The cellular link will automatically attempt to re-activate (subject to the unit containing a default configuration).

Testing:

The correct functioning of this facility can be tested by entering an incorrect APN into the TransPort, saving this

change, then dropping the cellular PPP link and inspecting the Event Log. In the example below), the router is configured to reset the module after 3 failed attempts, and to reboot the router after 10 connection failures ((low values used just for testing purpose):

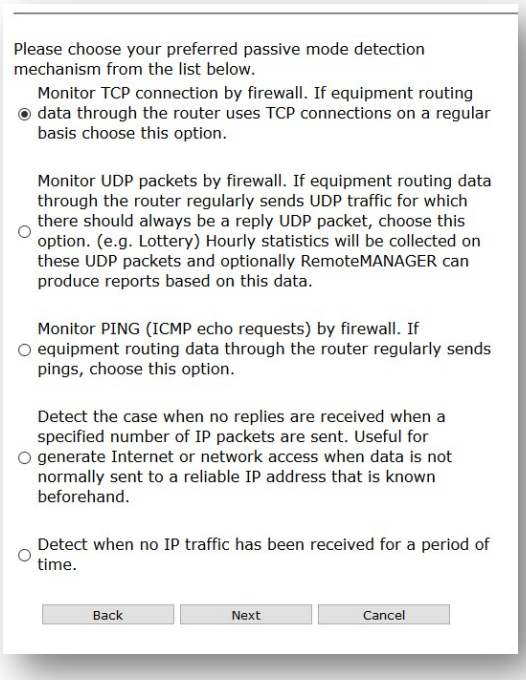
```
13:27:40, 24 Mar 2017,Default Route 0 Available,Activation
13:27:40, 24 Mar 2017,PPP 1 up
13:27:40, 24 Mar 2017,PPP 1 Start
13:27:40, 24 Mar 2017,Modem connected on asy 4
13:27:36, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:27:31, 24 Mar 2017,GPRS Registration On
13:27:31, 24 Mar 2017,GPRS Attachment On
13:27:29, 24 Mar 2017,GOBI 3000 running QCN D3200-STSUGN-1575
13:27:29, 24 Mar 2017,GOBI 3000 running FW D3200-STSUGN-1575
13:27:26, 24 Mar 2017,Default Route 0 Out Of Service,Activation
13:27:26, 24 Mar 2017,PPP 1 down,LL disconnect
13:27:26, 24 Mar 2017,Modem disconnected on asy 4,18
13:27:23, 24 Mar 2017,ASY 5 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:27:23, 24 Mar 2017,ASY 4 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:27:23, 24 Mar 2017,ASY 3 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:27:23, 24 Mar 2017,QMI interface attached to MODEM:0
13:27:23, 24 Mar 2017,USB-2 device 2 connected: Huawei EM680 w/Gobi Technology
13:27:22, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:27:17, 24 Mar 2017,DNS Query on [time.devicecloud.com]
13:27:17, 24 Mar 2017,IP Act_Rq to PPP 1-0: s_ip[0.0.0.0] d_ip[0.0.0.0]
d_port[53]
13:27:10, 24 Mar 2017,ETH 0 cable connect
13:27:07, 24 Mar 2017,USB-2 device 1 connected: EHCI root hub
13:27:07, 24 Mar 2017,USB-1 device 1 connected: EHCI root hub
13:27:07, 24 Mar 2017,Power control profile 0 activated
13:27:07, 24 Mar 2017,Power-up[],Reboot command
13:27:07, 24 Mar 2017,GPRS using SIM 1 (present)
13:27:06, 24 Mar 2017,Eventlog Counters Reset
13:26:57, 24 Mar 2017,Reboot
13:26:55, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:26:45, 24 Mar 2017,GOBI 3000 running QCN D3200-STSUGN-1575
13:26:45, 24 Mar 2017,GOBI 3000 running FW D3200-STSUGN-1575
13:26:45, 24 Mar 2017,PPP 1 failed -> reboot
13:26:45, 24 Mar 2017,PPP 1 down,LL disconnect
13:26:45, 24 Mar 2017,Modem disconnected on asy 4,18
13:26:44, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:26:34, 24 Mar 2017,PPP 1 down,LL disconnect
13:26:34, 24 Mar 2017,Modem disconnected on asy 4,18
13:26:33, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:26:31, 24 Mar 2017,ASY 5 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:26:31, 24 Mar 2017,ASY 4 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:26:31, 24 Mar 2017,ASY 3 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:26:31, 24 Mar 2017,QMI interface attached to MODEM:0
13:26:31, 24 Mar 2017,USB-2 device 2 connected: Huawei EM680 w/Gobi Technology
13:26:31, 24 Mar 2017,QMI interface detached
13:26:31, 24 Mar 2017,USB-2 device 2 disconnected: Has devices attached
13:26:30, 24 Mar 2017,DTR Down ASY 5
13:26:30, 24 Mar 2017,DTR Down ASY 4
13:26:30, 24 Mar 2017,DTR Down ASY 3
13:26:30, 24 Mar 2017,ASY 5 unassigned
13:26:30, 24 Mar 2017,ASY 4 unassigned
13:26:30, 24 Mar 2017,ASY 3 unassigned
```

```
13:26:11, 24 Mar 2017,GPRS link failed -> power cycling m,Link Retries
13:26:11, 24 Mar 2017,PPP 1 down,LL disconnect
13:26:11, 24 Mar 2017,Modem disconnected on asy 4,26
13:26:08, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:25:58, 24 Mar 2017,PPP 1 down,LL disconnect
13:25:58, 24 Mar 2017,Modem disconnected on asy 4,26
13:25:56, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:25:49, 24 Mar 2017,GPRS Registration On
13:25:47, 24 Mar 2017,GOBI 3000 running QCN D3200-STSUGN-1575
13:25:47, 24 Mar 2017,GOBI 3000 running FW D3200-STSUGN-1575
13:25:46, 24 Mar 2017,PPP 1 down,LL disconnect
13:25:46, 24 Mar 2017,Modem disconnected on asy 4,18
13:25:46, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:25:36, 24 Mar 2017,PPP 1 down,LL disconnect
13:25:36, 24 Mar 2017,Modem disconnected on asy 4,18
13:25:35, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:25:33, 24 Mar 2017,ASY 5 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:25:33, 24 Mar 2017,ASY 4 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:25:33, 24 Mar 2017,ASY 3 assigned to usb-2-1 (Huawei EM680 w/Gobi Technology
13:25:33, 24 Mar 2017,QMI interface attached to MODEM:0
13:25:33, 24 Mar 2017,USB-2 device 2 connected: Huawei EM680 w/Gobi Technology
13:25:33, 24 Mar 2017,QMI interface detached
13:25:33, 24 Mar 2017,USB-2 device 2 disconnected: Has devices attached
13:25:32, 24 Mar 2017,DTR Down ASY 5
13:25:32, 24 Mar 2017,DTR Down ASY 4
13:25:32, 24 Mar 2017,DTR Down ASY 3
13:25:32, 24 Mar 2017,ASY 5 unassigned
13:25:32, 24 Mar 2017,ASY 4 unassigned
13:25:32, 24 Mar 2017,ASY 3 unassigned
13:25:13, 24 Mar 2017,PPP 1 down,LL disconnect
13:25:13, 24 Mar 2017,GPRS link failed -> power cycling m,Link Retries
13:25:13, 24 Mar 2017,Modem disconnected on asy 4,26
13:25:11, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:25:01, 24 Mar 2017,PPP 1 down,LL disconnect
13:25:01, 24 Mar 2017,Modem disconnected on asy 4,26
13:24:59, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:24:49, 24 Mar 2017,PPP 1 down,LL disconnect
13:24:49, 24 Mar 2017,Modem disconnected on asy 4,26
13:24:46, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:24:36, 24 Mar 2017,PPP 1 down,LL disconnect
13:24:36, 24 Mar 2017,Modem disconnected on asy 4,26
13:24:34, 24 Mar 2017,Modem dialing on asy 4 #:*98*1#
13:24:33, 24 Mar 2017,GOBI 3000 running QCN D3200-STSUGN-1575
13:24:33, 24 Mar 2017,GOBI 3000 running FW D3200-STSUGN-1575
13:24:27, 24 Mar 2017,Modem disconnected on asy 4,1
13:24:26, 24 Mar 2017,Default Route 0 Out Of Service,Activation
13:24:26, 24 Mar 2017,PPP 1 Out Of Service,Activation
13:24:26, 24 Mar 2017,PPP 1 down,WEB request
13:24:18, 24 Mar 2017,Par change by username, modemcc 0 apn to incorrectAPN
13:23:39, 24 Mar 2017,Par change by username, modemcc 0 link_retries to 3
13:23:30, 24 Mar 2017,Par change by username, ppp 1 rebootfails to 10
```

In the log entries is shown that the configuration is changed with the mentioned parameters for reset the module and reboot the router, and the APN is changed to an incorrect one, then the PPP is manually reset to have the changes taking effect. After that, the connection attempts will fail, triggering some power cycles before and the reboot of the router at the end after 10 PPP link connection failing attempts. After the reboot the PPP comes up correctly.

3.1.2 Stateful Route Inspection: TCP/UDP/ICMP monitoring with Firewall

Clicking Next after the previous option, the other available Passive Techniques will be shown:



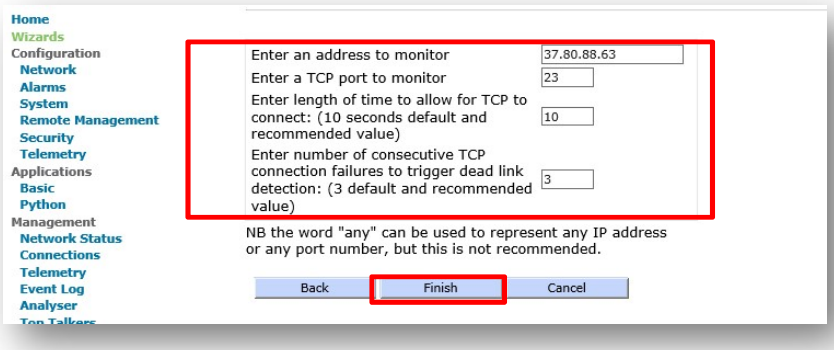
The first three Passive Options use the SRI or Stateful Route Inspection technique. Most TransPort WR models contain a powerful Stateful firewall facility. In addition to blocking unauthorized traffic, the firewall can be used to monitor traffic on a particular interface and flag routes as OOS (Out Of Service) or even deactivate cellular links. In the context of cellular problem detection, this facility can be used to deactivate the cellular link to the cellular network (usually PPP instance 1) and cause it to re-negotiate, thus potentially fixing the problem identified. It can also be used to cause the TransPort to send the data through a backup interface, but this will not be detailed in this AN.

This first technique is only suitable if some equipment routing through the TransPort via the cellular interface initiates traffic on a regular basis, i.e. some device local to the TransPort is required to generate the traffic in the first place.

The traffic that can be monitored by the firewall can be TCP, UDP or PING (ICMP echo request).

3.1.2.1 TCP Traffic Monitoring: configuration and testing

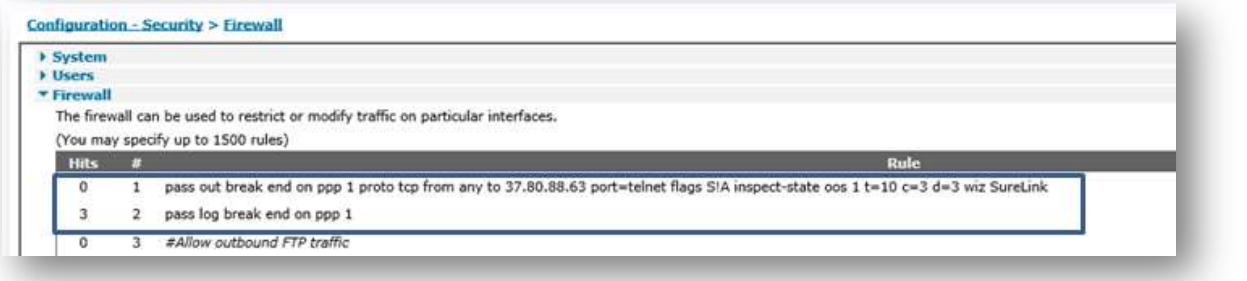
Configuration: Choosing the first option and clicking “Next”, the following screen will be shown:

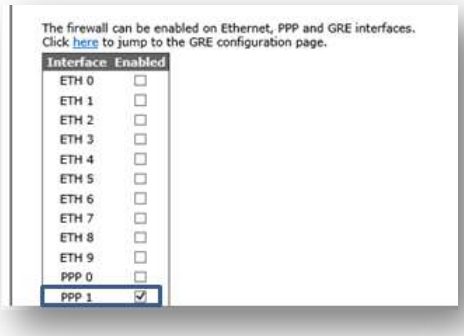


Enter the IP address of the remote peer to monitor as well as other parameters and then click “Finish” to complete the wizard.

At this point, the inserted configuration can be checked going in the Firewall section:

CONFIGURATION – SECURITY > FIREWALL

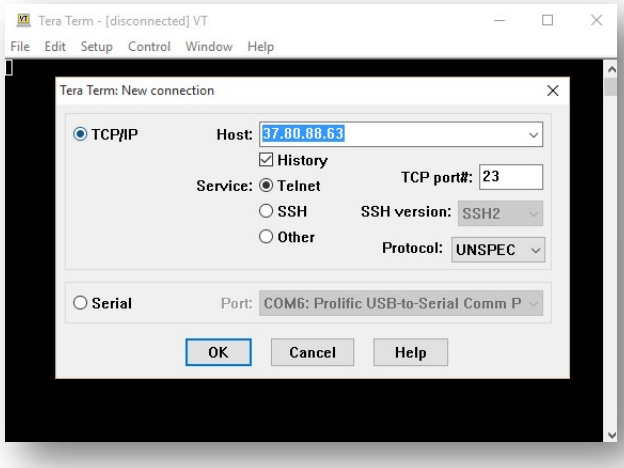


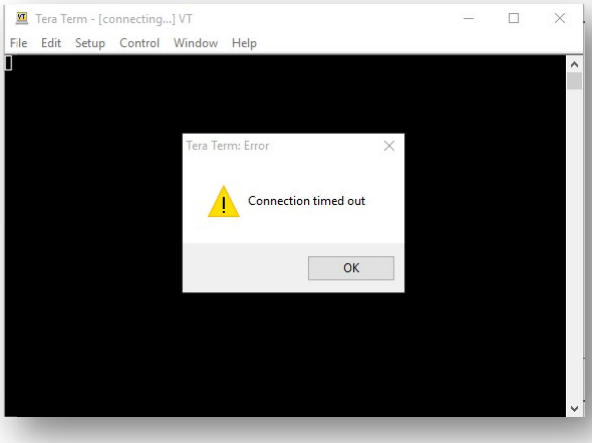


You will see that two Firewall rules are added in order to monitor the TCP traffic configured, and the Firewall is now enabled on the PPP 1 Interface.

Testing: A simple way to test if this feature is working as desired, is generating “failing” traffic to trigger the firewall and checking that the cellular link deactivates itself and then re-activates itself as expected.

As an example, basing on what has been configured in the previous steps, some telnet sessions to the configured address can be attempted (being sure that the remote device will not reply):





To check what happens to the cellular link, browse to the Eventlog section:

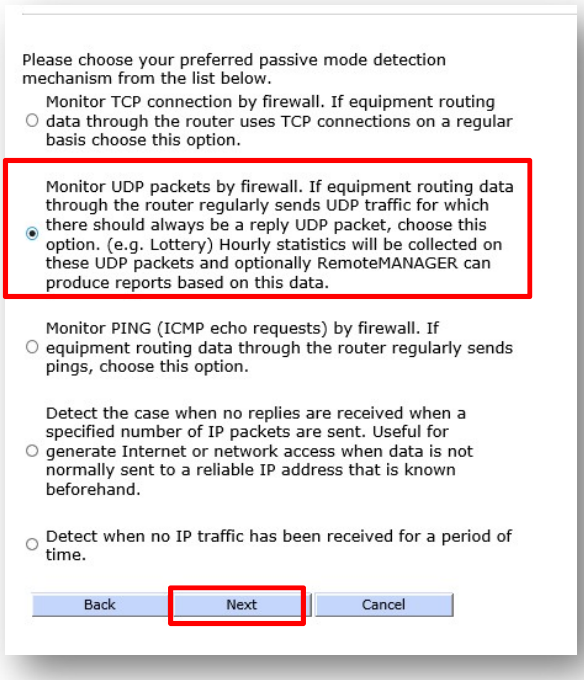
MANAGEMENT – EVENTLOG

```
12:21:40, 21 Feb 2017,Default Route 0 Available,Activation
12:21:40, 21 Feb 2017,PPP 1 Available,Activation
12:21:40, 21 Feb 2017,PPP 1 up
12:21:40, 21 Feb 2017,PPP 1 Start
12:21:40, 21 Feb 2017,Modem connected on asy 4
12:21:37, 21 Feb 2017,Modem dialing on asy 4 #:*98*1#
12:21:31, 21 Feb 2017,Modem disconnected on asy 4,1
12:21:29, 21 Feb 2017,PPP 1 down,Firewall Request
12:21:29, 21 Feb 2017,Default Route 0 Out Of Service,Firewall
12:21:29, 21 Feb 2017,PPP 1 Out Of Service,Firewall
```

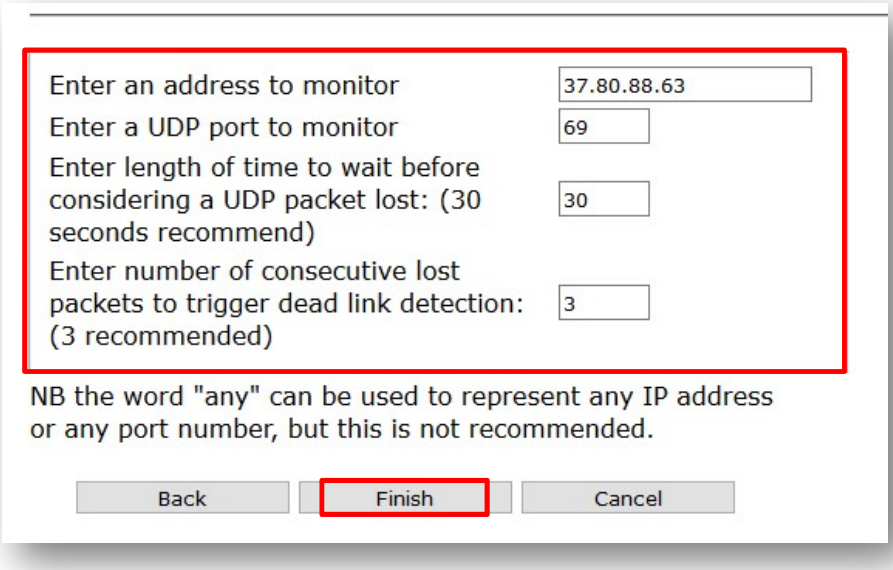
There will be entries showing that the PPP 1 (and related default route) has been marked as OOS by the firewall monitoring. The PPP then goes down due to the firewall and, as it is configured as default to automatically reconnect, it attempts again the connection and goes back up.

3.1.2.2 UDP Traffic Monitoring: configuration and testing

Configuration: In the Passive Techniques screen, choose the second option and click “Next”:



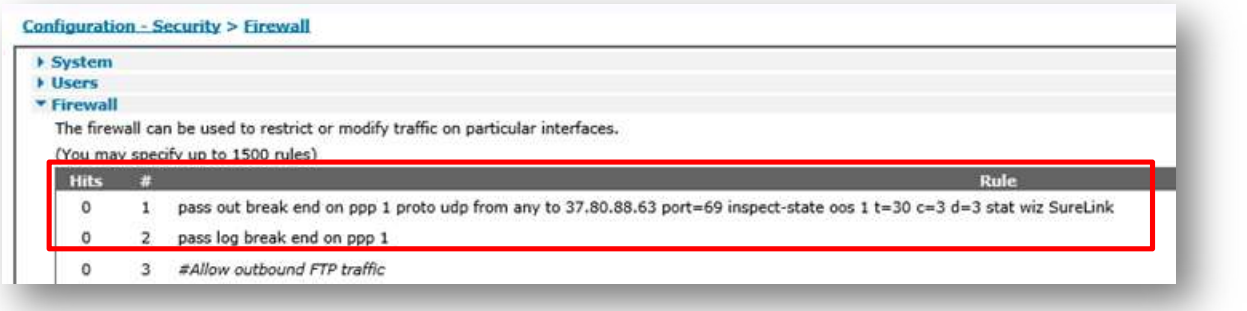
The following screen will be shown:

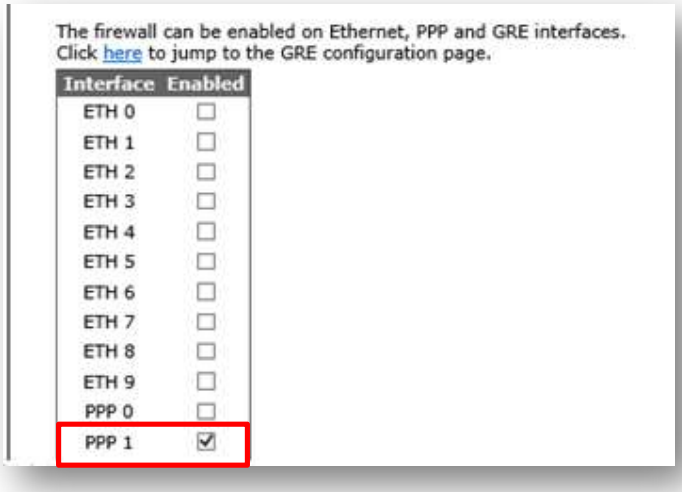


Enter the IP address of the remote peer to monitor as well as other parameters and then click “Finish” to complete the wizard.

At this point, the inserted configuration can be checked going in the Firewall section:

CONFIGURATION – SECURITY > FIREWALL

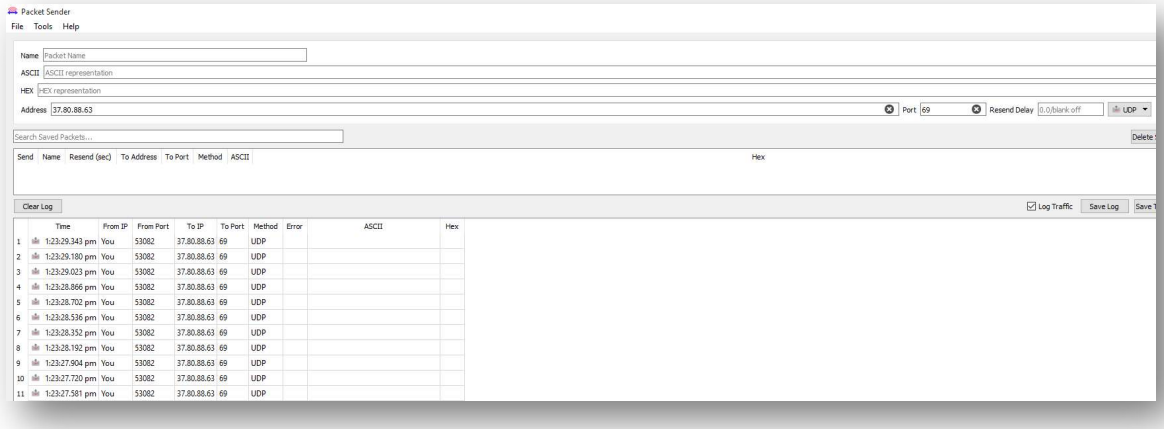




You will see that two Firewall rules are added in order to monitor the UDP traffic configured, and the Firewall is now enabled on the PPP 1 Interface.

Testing: A simple way to test if this feature is working as desired, is generating “failing” traffic to trigger the firewall and checking that the cellular link deactivates itself and then re-activates itself as expected.

As an example, basing on what has been configured in the previous steps, UDP connection attempts can be made to the configured address and port (in this example a simulator has been used to generate traffic on port 69):



To check what happens to the cellular link, browse to the Eventlog section:

MANAGEMENT – EVENTLOG

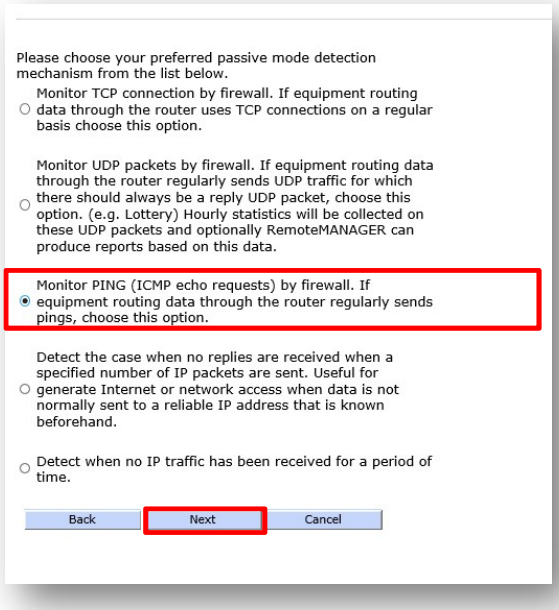
```
13:24:08, 21 Feb 2017,Network technology changed to HSDPA/HSUPA
13:24:03, 21 Feb 2017,Default Route 0 Available,Activation
13:24:03, 21 Feb 2017,PPP 1 Available,Activation
13:24:03, 21 Feb 2017,PPP 1 up
13:24:03, 21 Feb 2017,PPP 1 Start
13:24:03, 21 Feb 2017,Modem connected on asy 4
13:24:00, 21 Feb 2017,Modem dialing on asy 4 #:*98*1#
13:23:53, 21 Feb 2017,Modem disconnected on asy 4,NO CARRIER
13:23:52, 21 Feb 2017,PPP 1 down,Firewall Request
13:23:52, 21 Feb 2017,Default Route 0 Out Of Service,Firewall
13:23:52, 21 Feb 2017,PPP 1 Out Of Service,Firewall
```

There will be entries showing that the PPP 1 (and related default route) has been marked as OOS by the firewall monitoring. The PPP then goes down due to the firewall and, as it is configured as default to automatically reconnect, it attempts again the connection and goes back up.

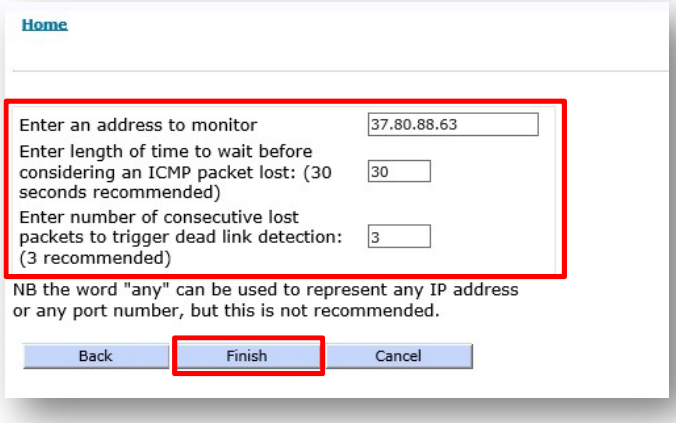
NOTE: It can be completely OK for some protocols that use UDP not to receive a reply; this rule should only be used for UDP based protocols that expect a reply.

3.1.2.3 ICMP traffic Monitoring: configuration and testing

Configuration: In the Passive Techniques screen, choose the third option and click “Next”:



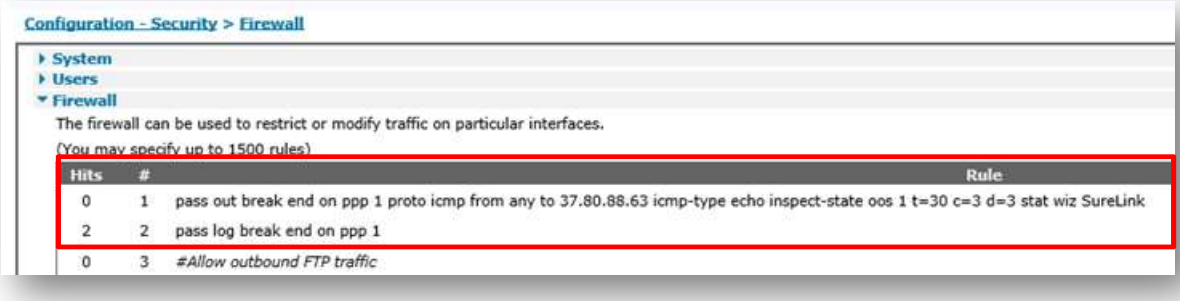
The following screen will be shown:

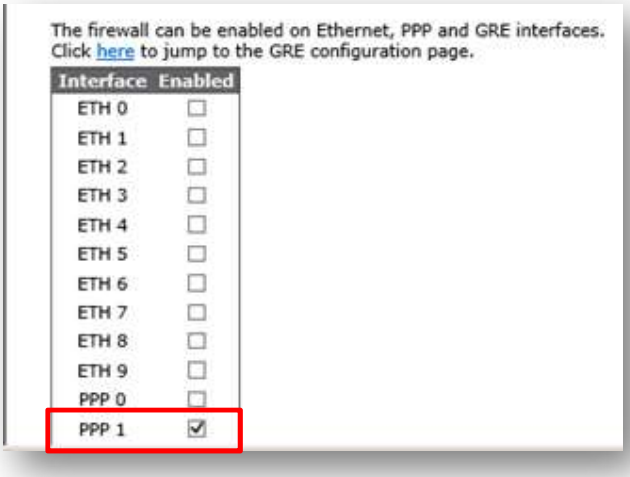


Enter the IP address of the remote peer to monitor as well as other parameters and then click “Finish” to complete the wizard.

At this point, the inserted configuration can be checked going in the Firewall section:

CONFIGURATION – SECURITY > FIREWALL

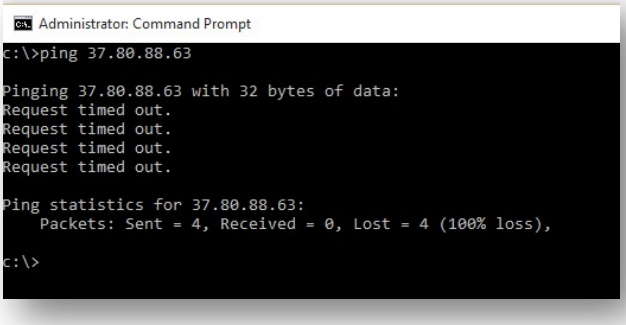




You will see that two Firewall rules are added in order to monitor the ICMP traffic configured, and the Firewall is now enabled on the PPP 1 Interface.

Testing: A simple way to test if this feature is working as desired, is generating “failing” traffic to trigger the firewall and checking that the cellular link deactivates itself and then re-activates itself as expected.

As an example, basing on what has been configured in the previous steps, ICMP requests are sent to the configured not responding address.



To check what happens to the cellular link, browse to the Eventlog section:

MANAGEMENT – EVENTLOG

```
aaa13:43:03, 21 Feb 2017,Default Route 0 Available,Activation
13:43:03, 21 Feb 2017,PPP 1 Available,Activation
13:43:03, 21 Feb 2017,PPP 1 up
13:43:03, 21 Feb 2017,PPP 1 Start
13:43:03, 21 Feb 2017,Modem connected on asy 4
13:43:00, 21 Feb 2017,Modem dialing on asy 4 #:*98*1#
13:42:53, 21 Feb 2017,Modem disconnected on asy 4,1
13:42:52, 21 Feb 2017,PPP 1 down,Firewall Request
13:42:52, 21 Feb 2017,Default Route 0 Out Of Service,Firewall
13:42:52, 21 Feb 2017,PPP 1 Out Of Service,Firewall
```

There will be entries showing that the PPP 1 (and related default route) has been marked as OOS by the firewall monitoring. The PPP then goes down due to the firewall and, as it is configured as default to automatically reconnect, it attempts again the connection and goes back up.

3.1.3 Deactivate PPP via Unanswered TX packets

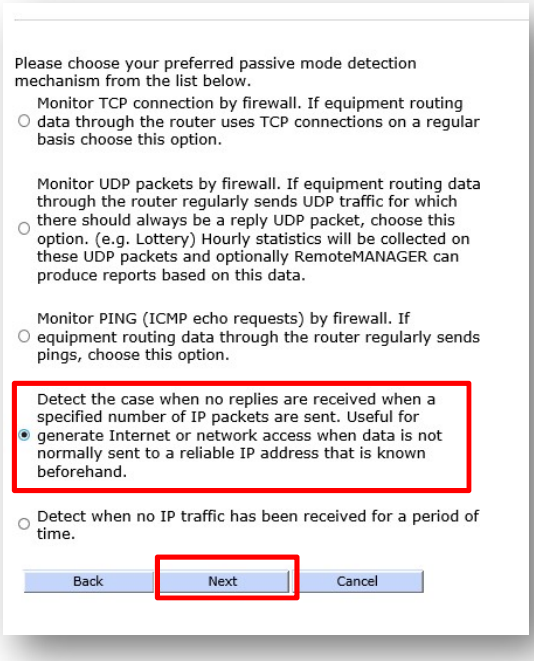
The TransPort can be configured to deactivate an interface if a number of packets are transmitted consecutively with no packets received.

This is not suitable for all situations because sometimes there are legitimate cases where a large number of packets will be sent and no reply is expected (e.g. streaming audio or video)

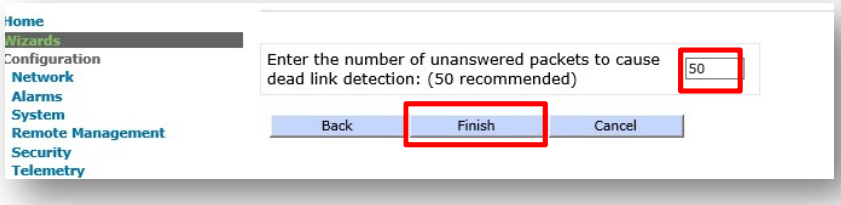
As other Passive methods, this is only suitable if some equipment routing through the TransPort via the cellular interface initiates traffic on a regular basis, i.e. some device local to the TransPort is required to generate the traffic in the first place. This method is very useful when generating Internet traffic and reliable IP address is not known beforehand.

Configuration:

In the Passive Techniques screen, choose the fourth option and click “Next”:



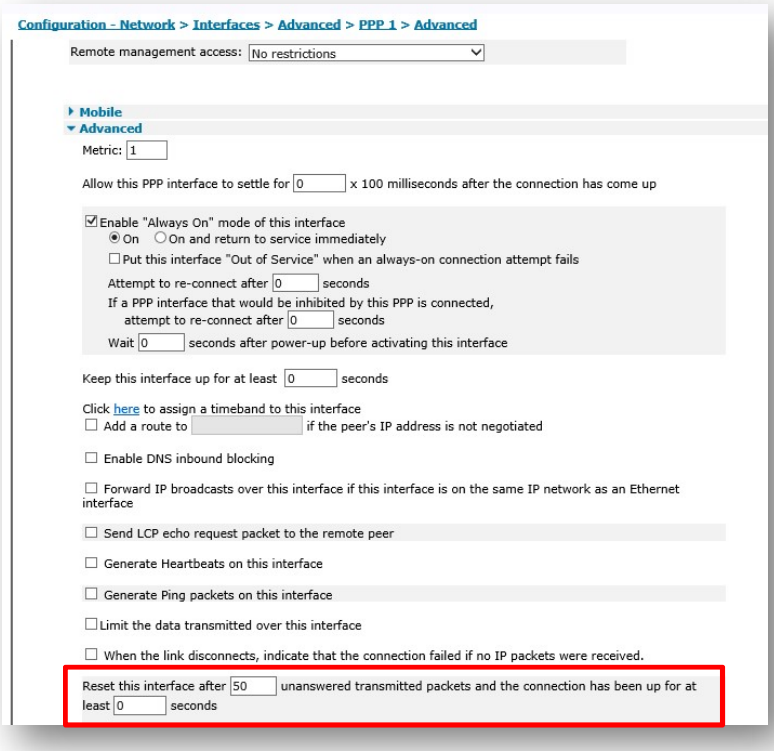
The following screen will be shown:



Enter the number of unanswered packets that you want to cause the link to reactivate. Note: A “large” value such as 50 unanswered packets is required because it is quite normal for a number of packets to be transmitted without any reply being received. It is reasonably unlikely that in most cases (e.g. any cases where TCP is used) 50 packets will be sent in a row without a reply.

In order to check what changes have been made by the wizard, navigate to the Advanced section of the PPP 1 settings page and check the following parameter:

CONFIGURATION - NETWORK > INTERFACES > ADVANCED > PPP 1 > ADVANCED



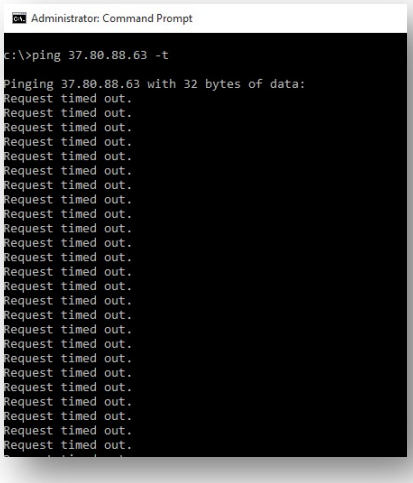
You can also see the changes and the PPP reactivation events in the eventlog section:

MANAGEMENT – EVENTLOG

```
12:53:21, 21 Feb 2017,Default Route 0 Available,Activation
12:53:21, 21 Feb 2017,PPP 1 Available,Activation
12:53:21, 21 Feb 2017,PPP 1 up
12:53:21, 21 Feb 2017,PPP 1 Start
12:53:21, 21 Feb 2017,Modem connected on asy 4
12:53:18, 21 Feb 2017,Modem dialing on asy 4 #:*98*1#
12:53:10, 21 Feb 2017,Modem disconnected on asy 4,NO CARRIER
12:53:10, 21 Feb 2017,Default Route 0 Out Of Service,Activation
12:53:10, 21 Feb 2017,PPP 1 Out Of Service,Activation
12:53:10, 21 Feb 2017,PPP 1 down,CLI request
12:53:07, 21 Feb 2017,Par change by PYTHON 22, ppp 1 sscnt to 50
```

Testing:

In order to test this Passive Method, some traffic to a not responding peer (doesn't matter which in this case) needs to be generated. In this example we sent a continuous ping to a not responding IP address:



To check what happens to the cellular link, browse to the Eventlog section:

MANAGEMENT – EVENTLOG

```
13:04:40, 21 Feb 2017,Default Route 0 Available,Activation
13:04:40, 21 Feb 2017,PPP 1 Available,Activation
13:04:40, 21 Feb 2017,PPP 1 up
13:04:40, 21 Feb 2017,PPP 1 Start
13:04:40, 21 Feb 2017,Modem connected on asy 4
13:04:37, 21 Feb 2017,Modem dialing on asy 4 #:*98*1#
13:04:30, 21 Feb 2017,Modem disconnected on asy 4,NO CARRIER
13:04:29, 21 Feb 2017,Default Route 0 Out Of Service,Activation
13:04:29, 21 Feb 2017,PPP 1 Out Of Service,Activation
13:04:29, 21 Feb 2017,PPP 1 down,PPP TX Link Failure
```

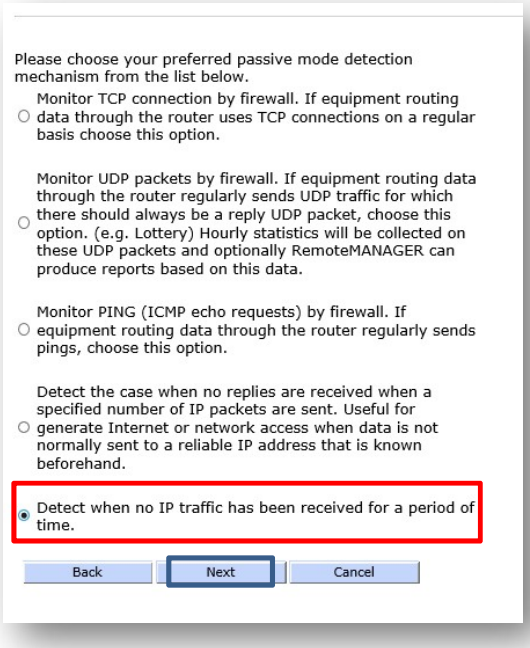
There will be entries showing that the PPP 1 (and then the related default route) has been deactivated due to "PPP TX Link Failure". After that, as configured as default to automatically reconnect, the PPP comes UP again.

3.1.4 Deactivate PPP via No traffic received for a certain period of time

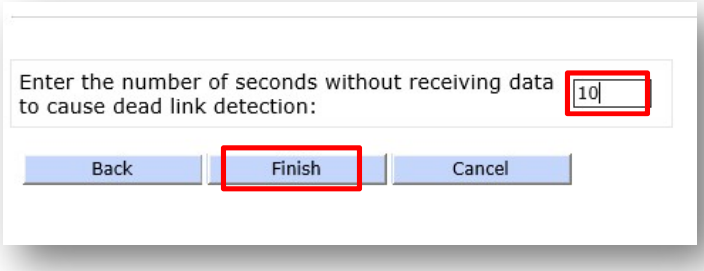
The last passive method provided by the wizard is to deactivate the PPP link if no traffic is received at all for a certain period of time. This method does not consider if/how many packets are sent from the PPP interface, it just checks if traffic is received on the interface (no matter what is sent). If traffic is not received in the configured period of time, the PPP link will be considered as "dead" and reactivated.

Configuration:

In the Passive Techniques screen, choose the fourth option and click "Next":



The following screen will be shown:

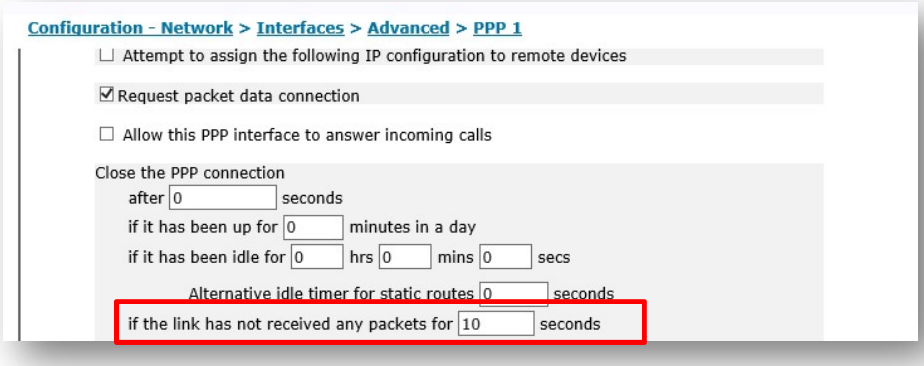


Configure the desired Interval of time of no traffic received to consider the link dead, and click "Finish".

Note: In this example a value of 10 is set just for testing purpose. In real scenario, higher values (as for example 300) are recommended.

In order to check what changes have been made by the wizard, navigate to the PPP 1 settings page and check the following parameter:

CONFIGURATION - NETWORK > INTERFACES > ADVANCED > PPP 1



You can also see the changes and the PPP reactivation events in the eventlog section:

MANAGEMENT – EVENTLOG

```
11:08:55, 24 Feb 2017,Default Route 0 Available,Activation
11:08:55, 24 Feb 2017,PPP 1 Available,Activation
11:08:55, 24 Feb 2017,PPP 1 up
11:08:55, 24 Feb 2017,PPP 1 Start
11:08:55, 24 Feb 2017,Modem connected on asy 4
11:08:52, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
11:08:45, 24 Feb 2017,Modem disconnected on asy 4,NO CARRIER
11:08:44, 24 Feb 2017,Default Route 0 Out Of Service,Activation
11:08:44, 24 Feb 2017,PPP 1 Out Of Service,Activation
11:08:44, 24 Feb 2017,PPP 1 down,CLI request
11:08:06, 24 Feb 2017,Par change by PYTHON 22, ppp 1 rxtimeout to 10
```

Testing:

In order to test this method, no traffic needs to be made for at least the period of time configured (so no management traffic using the PPP interface, no Internet traffic from devices behind the router etc). When the configured interval expired, in the eventlog section will be shown something as follows:

MANAGEMENT – EVENTLOG

```
11:09:29, 24 Feb 2017,Default Route 0 Available,Activation
11:09:29, 24 Feb 2017,PPP 1 Available,Activation
```

```
11:09:29, 24 Feb 2017,PPP 1 up
11:09:28, 24 Feb 2017,PPP 1 Start
11:09:28, 24 Feb 2017,Modem connected on asy 4
11:09:24, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
11:09:14, 24 Feb 2017,PPP 1 down,LL disconnect
11:09:14, 24 Feb 2017,Modem disconnected on asy 4,26
11:09:13, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
11:09:12, 24 Feb 2017,Network technology changed to HSDPA/HSUPA
11:09:06, 24 Feb 2017,Modem disconnected on asy 4,1
11:09:05, 24 Feb 2017,Default Route 0 Out Of Service,Activation
11:09:05, 24 Feb 2017,PPP 1 Out Of Service,Activation
11:09:05, 24 Feb 2017,PPP 1 down,Inactivity
```

There will be entries showing that the PPP 1 (and then the related default route) has been deactivated due to “Inactivity”. After that, as configured as default to automatically reconnect, the PPP comes UP again.

3.2 Active Techniques

Active techniques work by sending data to test the link. For example, a ping, UDP packet or IPsec keep-alive (Dead Peer Detection) packet.

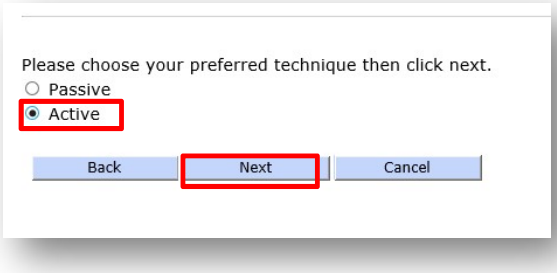
The main advantages of active techniques are:

- Problems are detected promptly and the availability of remote access to the router or its LAN is maximised
- Problems can be repaired BEFORE equipment on the router's LAN needs to use the W-WAN resulting in no delays sending data

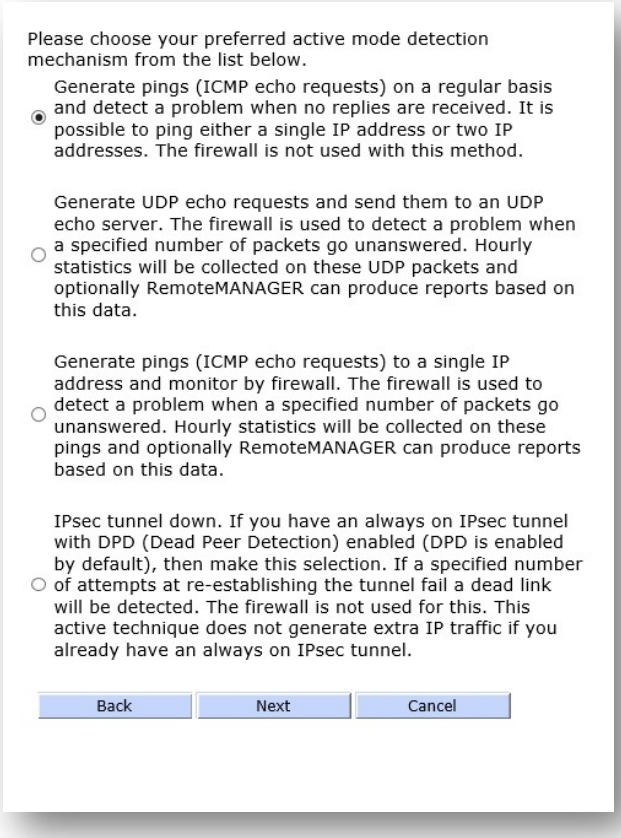
The main disadvantages are:

- Some mobile operators charge for the data sent to test the link
- In a hub and spoke deployment, addition load will be placed on equipment at the hub end by the test data

In order to configure one of the active techniques with the Sure Link wizard, select “Active” and click next:



The following options will be shown, and they all explained in next sections of this document:



3.2.1 Deactivate cellular link via PING failure detection (no firewall)

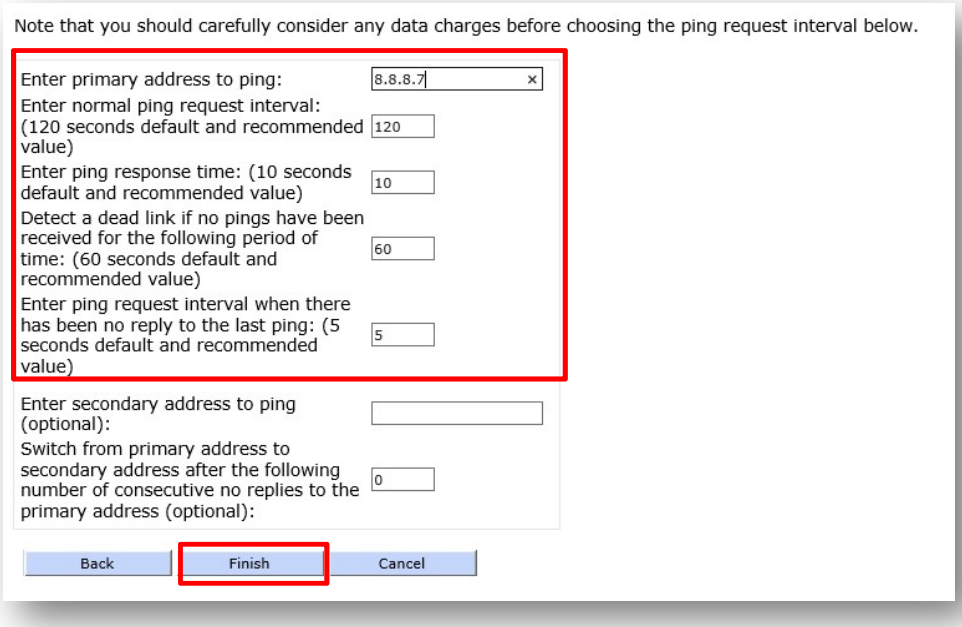
The TransPort can be configured to automatically generate pings at a specified interval and send them to a destination IP address. If the TransPort receives no reply to these pings in a specified amount of time then the unit will deactivate the cellular link.

NOTE: On some cellular networks, PING packets are blocked, so this technique should not be used then.

Configuration:

From the Active Techniques options screen, choose the first one and click on “Next”.

The following screen will be shown:



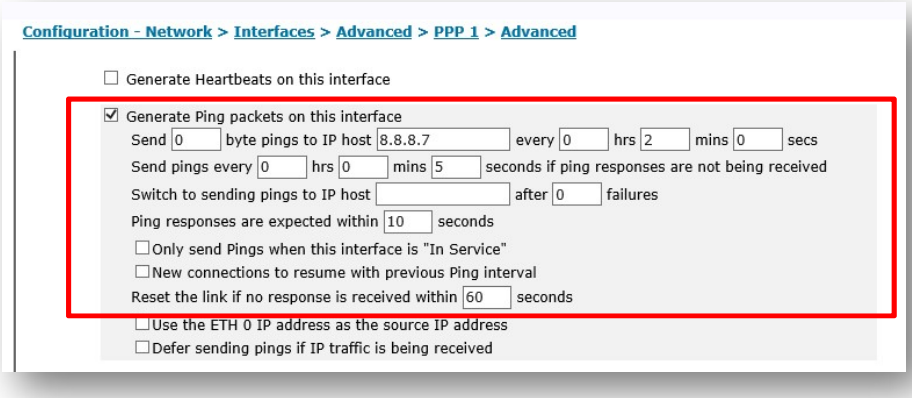
Enter the parameters as desired and click “Finish” to complete the wizard.

In the above example, the router will send test pings normally at 120 second intervals and wait 10 seconds for a reply. When a reply is not received within 10 seconds, the next ping will be sent after 5 seconds (not 120). If 60 seconds pass without receiving replies to any ping request, the link is detected as dead.

Optionally, a secondary monitored host can be configured. That means that, after a certain number of failures on the primary one, the link is not marked as dead but other tries are made with the ping requests being sent to the secondary address.

In order to check what changes have been made by the wizard, navigate to the PPP 1 advanced settings page and check the following parameter:

CONFIGURATION - NETWORK > INTERFACES > ADVANCED > PPP 1 > ADVANCED



You can also see the changes and the PPP reactivation events in the eventlog section:

MANAGEMENT – EVENTLOG

```
12:30:51, 24 Feb 2017,Default Route 0 Available,Activation
12:30:51, 24 Feb 2017,PPP 1 Available,Activation
12:30:51, 24 Feb 2017,PPP 1 up
12:30:51, 24 Feb 2017,PPP 1 Start
12:30:51, 24 Feb 2017,Modem connected on asy 4
12:30:48, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
12:30:41, 24 Feb 2017,Modem disconnected on asy 4,NO CARRIER
12:30:40, 24 Feb 2017,Default Route 0 Out Of Service,Activation
12:30:40, 24 Feb 2017,PPP 1 Out Of Service,Activation
12:30:40, 24 Feb 2017,PPP 1 down,CLI request
12:30:37, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingdeact to 60
12:30:37, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingint2 to 5
12:30:37, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingresp to 10
12:30:37, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingip to 8.8.8.7
12:30:37, 24 Feb 2017,Par change by PYTHON 22, ppp 1 ip2count to 0
12:30:37, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingint to 120
```

Testing:

An easy way to test this feature is deliberately ensuring that the IP address the Digi TransPort is pinging cannot reply and then checking that PPP 1 deactivates itself and re-activates itself as expected. This can be easily seen in the Digi TransPort's event log:

```
12:34:02, 24 Feb 2017,Default Route 0 Available,Activation
12:34:02, 24 Feb 2017,PPP 1 Available,Activation
12:34:02, 24 Feb 2017,PPP 1 up
12:34:02, 24 Feb 2017,Event delay,Logger busy
12:34:01, 24 Feb 2017,PPP 1 Start
12:34:01, 24 Feb 2017,Modem connected on asy 4
12:33:59, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
12:33:51, 24 Feb 2017,Modem disconnected on asy 4,NO CARRIER
12:33:51, 24 Feb 2017,Default Route 0 Out Of Service,Activation
12:33:51, 24 Feb 2017,PPP 1 Out Of Service,Activation
12:33:51, 24 Feb 2017,PPP 1 down,PPP PING Failure
```

There will be entries showing that the PPP 1 (and then the related default route) has been deactivated due to "PPP

PING Failure" After that, as configured as default to automatically reconnect, the PPP comes UP again.

3.2.2 Generate & monitor traffic with the firewall

The TransPort can be configured to generate UDP or PING traffic and monitor them with the firewall in order to detect problems on the cellular link.

Compared with the method described in the previous section, where the firewall is not used, this technique is more powerful, as it not just resets the link when a failure is detected. In fact, with the firewall, the route associated with the PPP interface will be kept as OOS until a certain amount of time expires or until a recovery is detected.

Moreover, hourly statistic will be collected on this traffic (both PING and UDP) and optionally Digi Remote Manager can produce reports based on this data.

With the wizard a basic configuration of this functionality can be achieved, but other options regarding the yse of [insoect-state] with the Out of Service option are available, and explained in TransPort User Guide (pag.672):

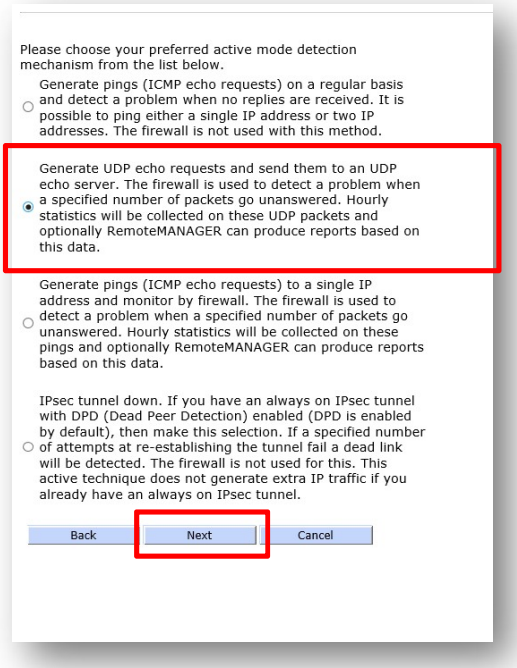
http://ftp1.digi.com/support/documentation/90001019.pdf.

Of course, adding the firewall, will also add complexity to the system, in particular, for example, if the firewall is not used for something else and/or is not needed to use it with RM, it may be an easier solution to decide that PPP method is enough, instead of adding a not strictly needed complexity basing on the environment.

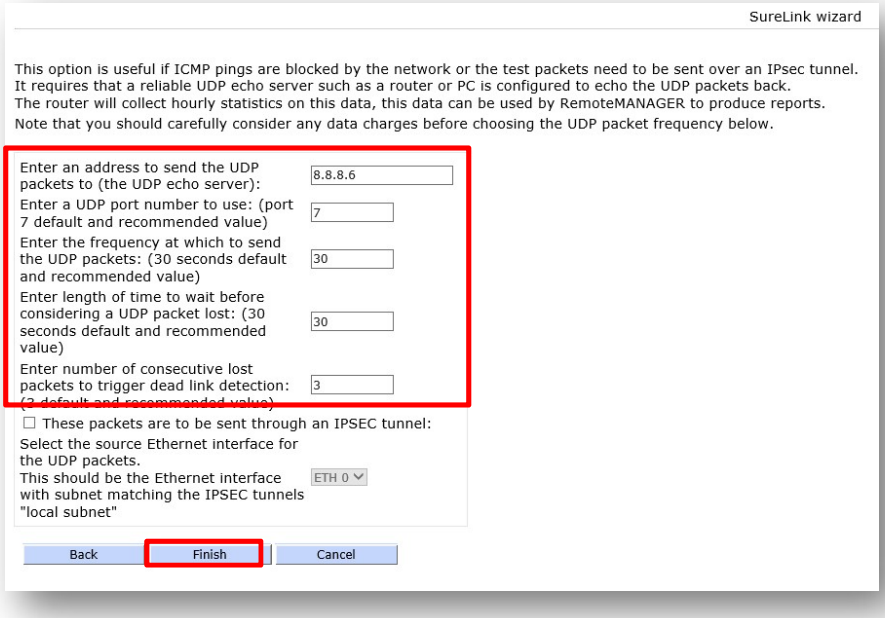
Next subsections will provide example of using the Sure Link wizard to configure the TransPort to generate and monitor UDP and ICMP traffic.

3.2.2.1 Generate & monitor UDP traffic

Configuration: From the active techniques main screen, chose the second one and clock on “Next”:



This screen will be shown:



Fill in the parameters field as desired and click on “Finish” to complete the wizard.

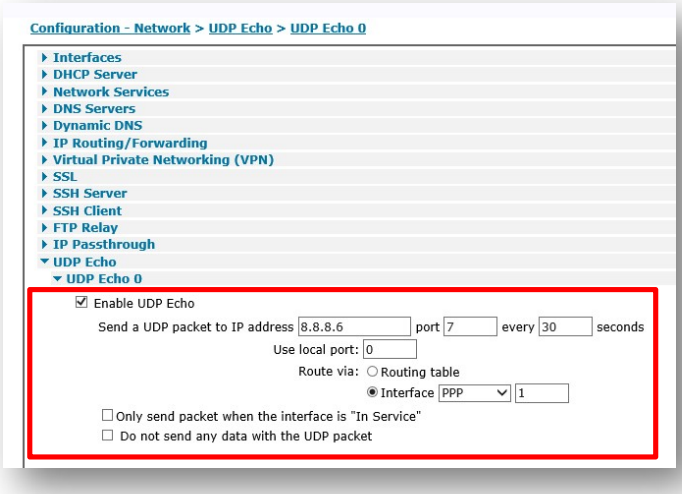
In the example above, the router will send UDP packets in port 7 to the address 8.8.8.6 every 30 seconds.

If no reply has been received in 30 seconds, the packet is considered lost. After 3 lost packet the link is detected s dead.

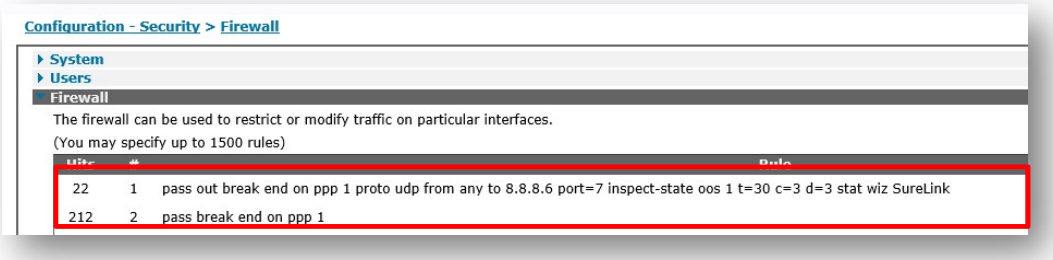
Optionally, the UDP packets can be sent through an IPsec tunnel with as source the ETH interface with a subnet matching the IPsec tunnel local subnet.

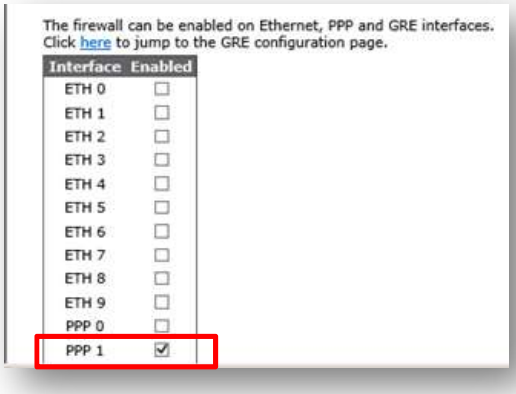
In order to check the configuration changes made by the wizard, navigate to the UDP Echo settings and in the firewall page:

CONFIGURATION – NETWORK > UDP ECHO > UDP ECHO 0:



CONFIGURATION – SECURITY > FIREWALL:





You will see that two Firewall rules are added in order to monitor the UDP traffic configured, and the Firewall is now enabled on the PPP 1 Interface.

The changes are also shown in the eventlog:

MANAGEMENT – EVENTLOG

```
12:50:18, 24 Feb 2017,Par change by PYTHON 22, ppp 1 firewall to ON
12:50:18, 24 Feb 2017,Par change by PYTHON 22, udpecho 0 dstport to 7
12:50:18, 24 Feb 2017,Par change by PYTHON 22, udpecho 0 ifent to PPP
12:50:17, 24 Feb 2017,Par change by PYTHON 22, udpecho 0 ifadd to 1
12:50:17, 24 Feb 2017,Par change by PYTHON 22, udpecho 0 interval to 30
12:50:17, 24 Feb 2017,Par change by PYTHON 22, udpecho 0 dstip to 8.8.8.6
```

Testing:

In order to test this feature, it is enough to set in the wizard a no responding address (so a not reachable one as in the example above) and check the eventlog:

MANAGEMENT – EVENTLOG

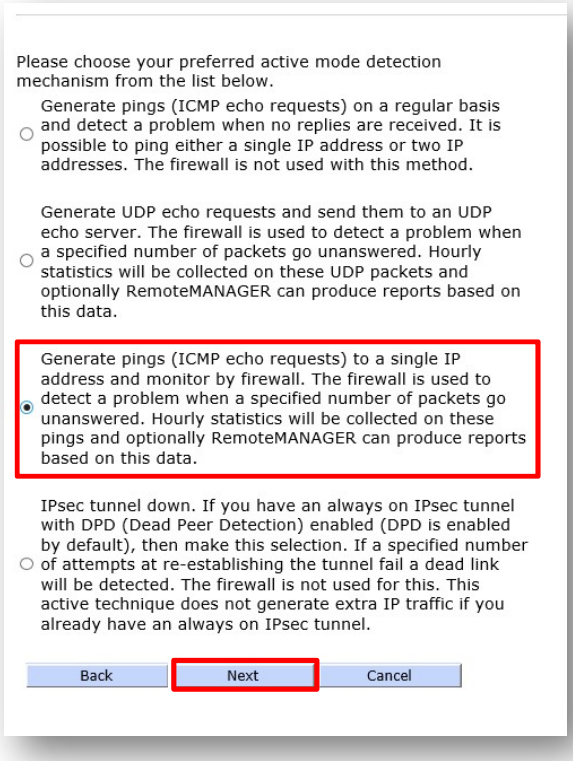
```
12:54:29, 24 Feb 2017,PPP 1 Available,Activation
12:54:29, 24 Feb 2017,PPP 1 up
12:54:29, 24 Feb 2017,PPP 1 Start
12:54:29, 24 Feb 2017,Modem connected on asy 4
```

```
12:54:26, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
12:54:19, 24 Feb 2017,Modem disconnected on asy 4,NO CARRIER
12:54:18, 24 Feb 2017,PPP 1 down,Firewall Request
12:54:18, 24 Feb 2017,Default Route 0 Out Of Service,Firewall
12:54:18, 24 Feb 2017,PPP 1 Out Of Service,Firewall
```

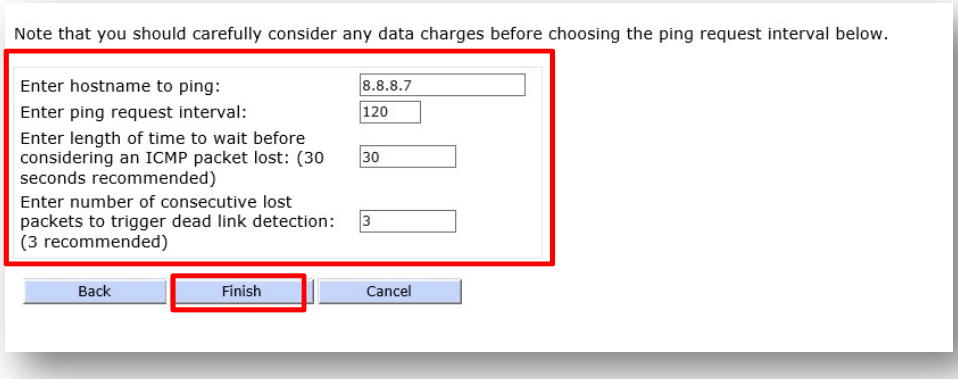
There will be entries showing that the PPP 1 (and then the related default route) has been deactivated due to Firewall request. After that, as configured as default to automatically reconnect, the PPP comes UP again.

3.2.2.2 Generate & monitor ICMP traffic

Configuration: From the active techniques main screen, chose the third one and clock on “Next”:



This screen will be shown:



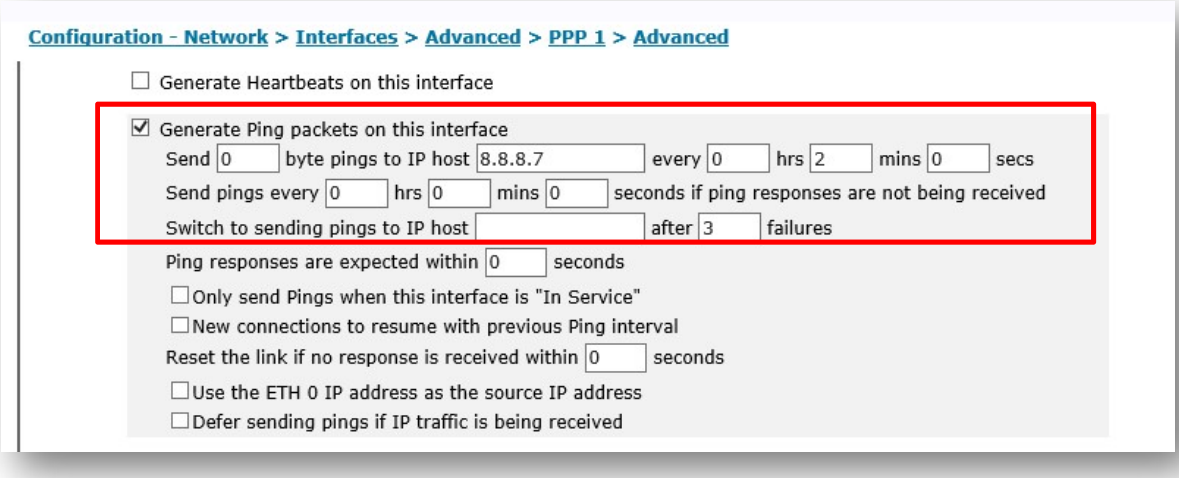
Fill in the parameters field as desired and click on “Finish” to complete the wizard.

In the example above, the router will send ping to the address 8.8.8.7 every 120 seconds.

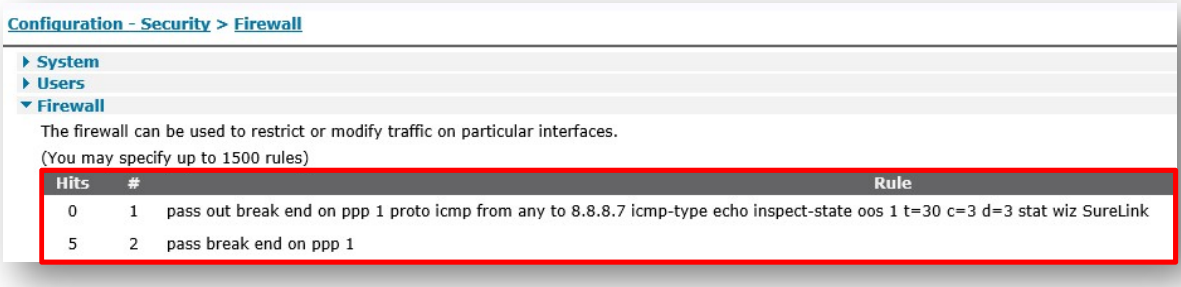
If no reply has been received in 30 seconds, the packet is considered lost. After 3 lost packet the link is detected as dead.

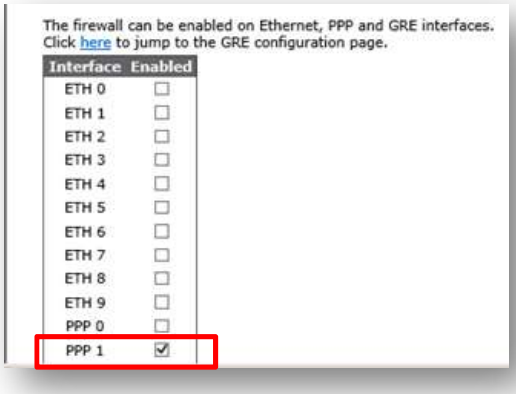
In order to check the configuration changes made by the wizard, navigate to the PPP advanced settings and the Firewall page.

CONFIGURATION – NETWORK > INTERFACES > ADVANCED > PPP 1> ADVANCED



CONFIGURATION – SECURITY > FIREWALL:





You will see that two Firewall rules are added in order to monitor the ICMP traffic configured, and the Firewall is now enabled on the PPP 1 Interface.

The changes are also shown in the eventlog:

MANAGEMENT – EVENTLOG

```
14:01:15, 24 Feb 2017,Default Route 0 Available,Activation
14:01:15, 24 Feb 2017,PPP 1 Available,Activation
14:01:15, 24 Feb 2017,PPP 1 up
14:01:15, 24 Feb 2017,PPP 1 Start
14:01:15, 24 Feb 2017,Modem connected on asy 4
14:01:12, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
14:01:05, 24 Feb 2017,Modem disconnected on asy 4,NO CARRIER
14:01:04, 24 Feb 2017,Default Route 0 Out Of Service,Activation
14:01:04, 24 Feb 2017,PPP 1 Out Of Service,Activation
14:01:04, 24 Feb 2017,PPP 1 down,CLI request
14:01:02, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingip to 8.8.8.7
14:01:02, 24 Feb 2017,Par change by PYTHON 22, ppp 1 firewall to ON
14:01:02, 24 Feb 2017,Par change by PYTHON 22, ppp 1 pingint to 120
```

Testing:

In order to test this feature, it is enough to set in the wizard a no responding address (so a not reachable one as in the example above) and check the eventlog:

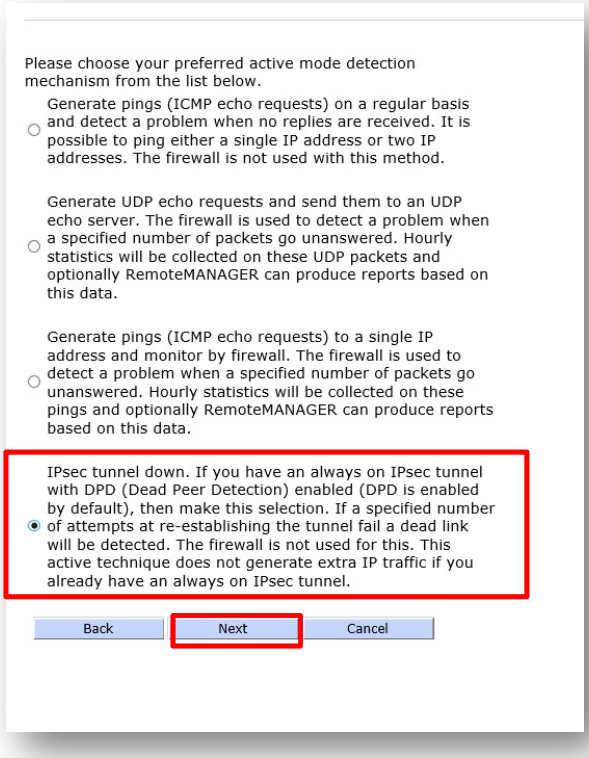
MANAGEMENT – EVENTLOG

```
14:07:55, 24 Feb 2017,Default Route 0 Available,Activation
14:07:55, 24 Feb 2017,PPP 1 Available,Activation
14:07:55, 24 Feb 2017,PPP 1 up
14:07:55, 24 Feb 2017,PPP 1 Start
14:07:55, 24 Feb 2017,Modem connected on asy 4
14:07:52, 24 Feb 2017,Modem dialing on asy 4 #:*98*1#
14:07:45, 24 Feb 2017,Modem disconnected on asy 4,1
14:07:44, 24 Feb 2017,PPP 1 down,Firewall Request
14:07:44, 24 Feb 2017,Default Route 0 Out Of Service,Firewall
14:07:44, 24 Feb 2017,PPP 1 Out Of Service,Firewall
```

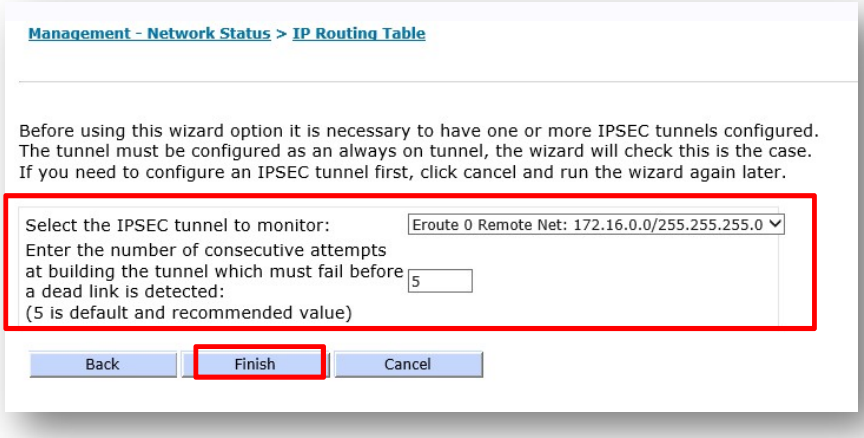
There will be entries showing that the PPP 1 (and then the related default route) has been deactivated due to Firewall request. After that, as configured as default to automatically reconnect, the PPP comes UP again.

3.2.3 Dead link detected using IPsec tunnel DPD

Configuration: From the active techniques main screen, chose the last one and clock on “Next”:



The following screen will be shown:

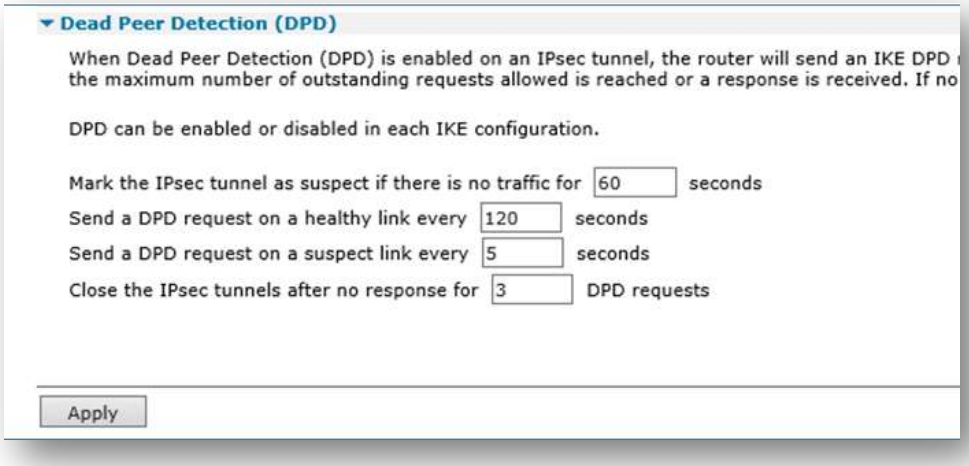


Select the IPsec tunnel to monitor and the number of consecutive failing attempts of establish the tunnel to wait until marl the link as dead.

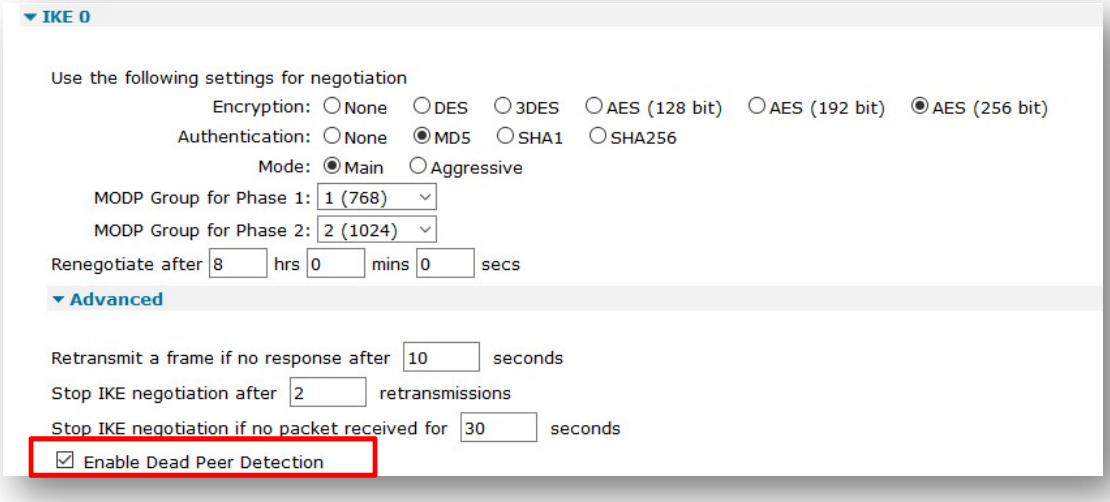
As explained in that screen, in order to use this method, an “always ON” IPsec tunnel needs to be configured and should be as an “Always On” one. Also, DPD configured (it is by default).

DPD sand “Always On” settings can be checked as follows:

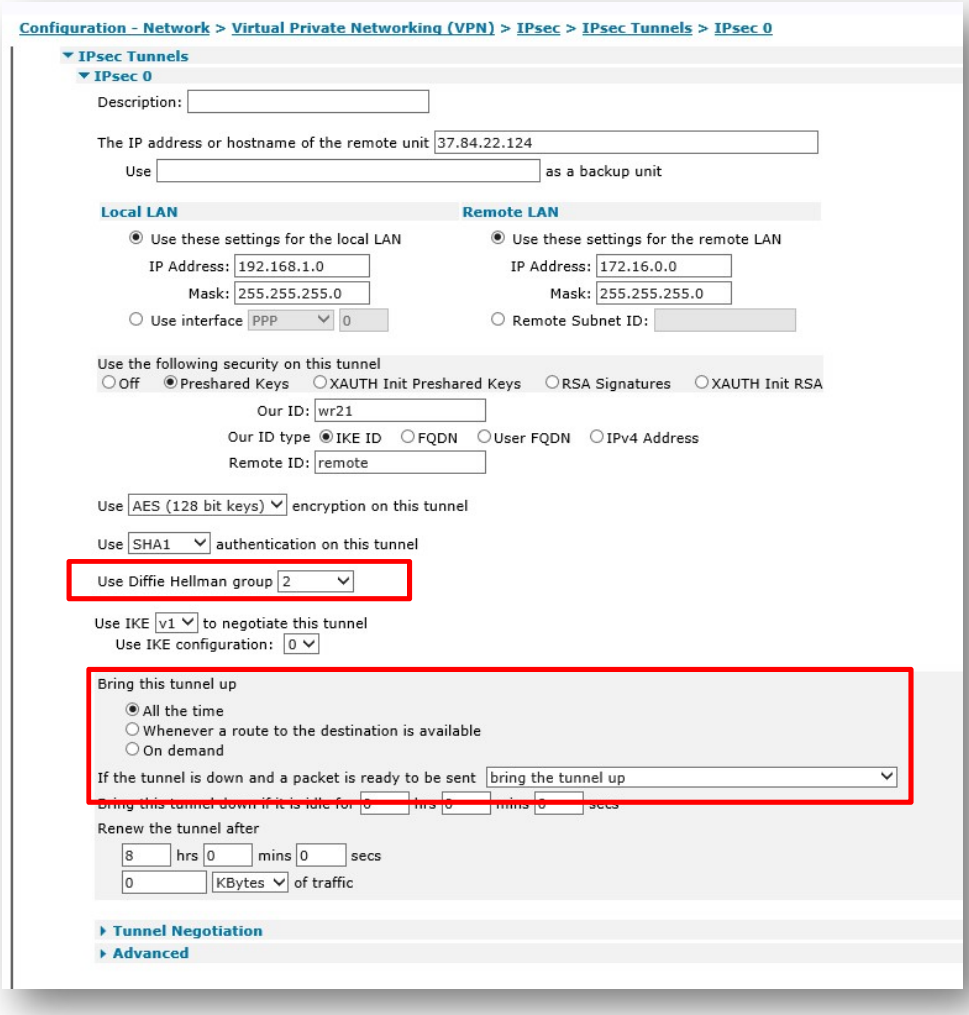
CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > DEAD PEER DETECTION (DPD)



CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE > IKE 0



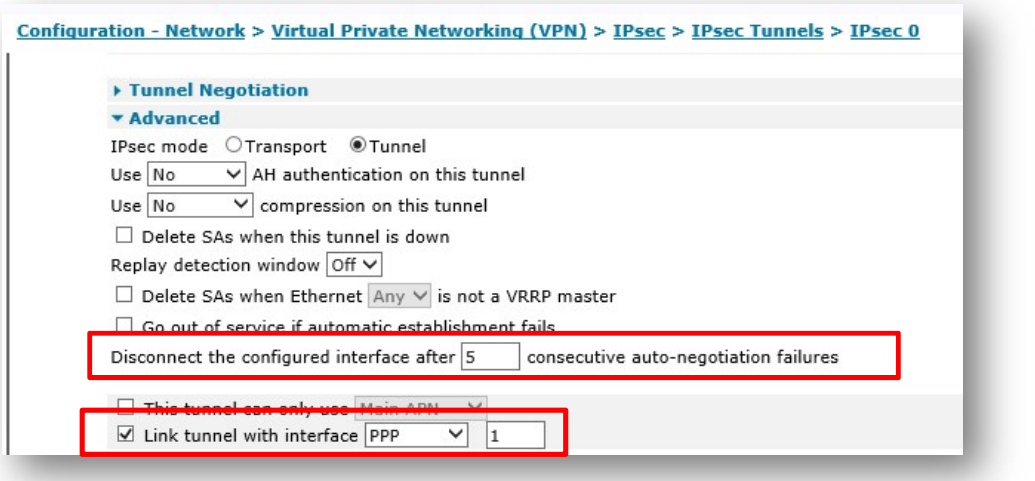
CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0



For more details about configuring IPsec VPN over Cellular see the App Note here: AN10 - IPSec over Cellular using Digi TransPort Routers with Pre-Shared key authentication

In order to check the configuration changes made by the wizard, navigate to the IPsec tunnel page:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0 > Advanced



The changes are also shown in the eventlog:

MANAGEMENT – EVENTLOG

```
15:21:14, 22 Mar 2017,Par change by PYTHON 22, eroute 0 ifadd to 1
15:21:14, 22 Mar 2017,Par change by PYTHON 22, eroute 0 ifent to PPP
15:21:14, 22 Mar 2017,Par change by PYTHON 22, eroute 0 nosadeactcnt to 5
```

Testing: To test this feature, an easy way is to simulate a fault over the link causing the IPsec tunnel does not renegotiate (for example a failure on the remote peer)

```
11:15:33, 28 Feb 2017,Modem disconnected on asy 4,1
11:15:32, 28 Feb 2017,Default Route 0 Out Of Service,Activation
11:15:32, 28 Feb 2017,PPP 1 Out Of Service,Activation
11:15:32, 28 Feb 2017,PPP 1 down
11:15:27, 28 Feb 2017,(20) IKE SA Removed. Peer: ,Link Deactivated
11:15:17, 28 Feb 2017,(20) New Phase 1 IKE Session 37.84.22.124,Initiator
11:15:17, 28 Feb 2017,IKE Request Received From Eroute 0
11:15:17, 28 Feb 2017,(19) IKE SA Removed. Peer: ,Negotiation Failure
11:15:17, 28 Feb 2017,(19) IKE Negotiation Failed. Peer: ,Retries Exceeded
11:15:07, 28 Feb 2017,IKE Request Received From Eroute 0
11:14:57, 28 Feb 2017,IKE Request Received From Eroute 0
11:14:51, 28 Feb 2017,Network technology changed to HSDPA/HSUPA
11:14:47, 28 Feb 2017,(19) New Phase 1 IKE Session 37.84.22.124,Initiator
11:14:47, 28 Feb 2017,IKE Request Received From Eroute 0
11:14:47, 28 Feb 2017,(5) IKE SA Removed. Peer: remote,Dead Peer Detected
11:14:47, 28 Feb 2017,Eroute 0 VPN down peer: remote
11:14:47, 28 Feb 2017,IPSec SA Deleted ID remote,Dead Peer Detected
11:13:25, 28 Feb 2017,Clear Event Log
```

There will be entries showing the VPN going down due to DPD and then, after the failing attempts to establish it, the PPP 1 goes down due to the “Link deactivated” when the IKE SA is removed. After that, as configured as default to automatically reconnect, the PPP comes UP again.