

# Network Problems

## GPRS/UMTS Detection and Recovery



## Network Problems – GPRS/UMTS Detection and Recovery

### Contents

<b>1.0</b>	<b>Introduction .....</b>	<b>3</b>
1.1	Outline .....	3
1.2	Stateful Route Inspection Overview .....	3
<b>2.0</b>	<b>Configuration.....</b>	<b>4</b>
2.1	Enabling Stateful Route Inspection .....	4
3.2	GPRS Error Detection and Recovery Techniques .....	5

### Technical Support

If you require assistance with any of the instructions in this application note you can contact Westermo as follows:

Web:	<a href="http://www.westermo.co.uk">www.westermo.co.uk</a>
Technical e-mail:	<a href="mailto:technical@westermo.co.uk">technical@westermo.co.uk</a>
Telephone:	+44 (0)1489 580585
Fax:	+44 (0)1489 580586

## 1.0 INTRODUCTION

### 1.1 Outline

GPRS/UMTS technology has proven to be extremely reliable. However the consequences of losing contact with a remote unit miles from anywhere are so severe in terms of recovery costs (site visits etc.) that it warrants extra precautions.

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

There are a number of features built into the MR-200/250's latest firmware that are designed to recover - without user intervention - from any GPRS/UMTS module or network problems that may occur.

Some of these options are **passive**

- They work simply by monitoring traffic on the GPRS/UMTS network and spotting problems.

Some of them are **active**

- They work by actually generating traffic to the network. The active options have the advantage of working even when the hosts on the MR-200/250's Ethernet network are not sending packets to the network. The disadvantage is that data charges will be incurred if your network provider charges for the quantity of data sent.

NB 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.

### 1.2 Stateful Route Inspection Overview

SRI or Stateful Route Inspection is a passive error detection technique. All MR series Routers units now contain a powerful stateful firewall facility. In addition to blocking un-authorized traffic the firewall can be used to monitor traffic on a particular interface and flag routes as OOS (out of service) or even deactivate PPP links. In the context of GPRS/UMTS problem detection this facility can be used to deactivate the PPP link to the network (PPP instance 1) and cause it to re-negotiate thus potentially fixing the problem identified.

It could also be used to cause the MR-200/250 to send the data through a backup interface but this will not be detailed in this application note.

## 2.0 CONFIGURATION

### 2.1 Enabling Stateful Route Inspection

To enable SRI for GPRS take the following steps.

On the MR-200's web server navigate to the **Configure** → **PPP Instance** → **Standard** web page and set the "Firewall" parameter to "ON". Click OK at the bottom of the page.

On the MR-200's web server navigate to the **Configure** → **Firewall** web page. This page allows multiple entries to be made in the router's's firewall by first clicking the "Insert" button, filling out the text box and then clicking the "OK" button. Most simple SRI firewalls can be achieved in just two lines.

Three examples follow. The syntax of the firewall commands will not be explained in detail, for detailed explanation of the syntax please see the latest Westermo MR/DR router reference manual. Adjust one of these examples to match your requirements and enter it into three lines of the firewall.

#### TCP:

Line 1: pass out break end on ppp 1 proto tcp from any to 192.168.20.1 flags S!A inspect-state oos 1 t=5 c=5 d=5

Line 2: pass

The above firewall will cause PPP 1 (the WAN PPP interface) to be deactivated if several TCP connection attempts to the IP address 192.168.20.1 fail.

#### UDP:

Line 1: pass out break end on ppp 1 proto udp from any to 192.168.0.0/16 port=1001 inspect-state oos ppp 1 1 t=10 c=5 d=5

Line 2: pass

The above firewall will cause PPP 1 (the WAN interface) to be deactivated if five ( $c = 5$  &  $d = 5$ ) UDP packets are sent to IP subnet 192.168.0.0/16 on port number 1001 and no UDP packet is received back from the 192.168.0.0/16 subnet. NB 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.

#### ICMP PING:

Line 1: pass out break end on ppp 1 proto icmp from any to 192.168.99.99 icmp-type echo inspect-state oos 1 t=10 c = 2 d = 2

Line 2: pass

The above example will cause PPP 1 (the WAN interface) to be deactivated if two ( $c = 2$  &  $d = 2$ ) ICMP PING (echo request) packets are sent to the 192.168.99.99 IP address and no ICMP PING (echo response) is received back within 20 seconds ( $d=2 \times t=10 = 20$  seconds).

Click the “Save (fw → fw.txt)” button to save your firewall

On the MR-200/250's web server menu click on the “Save” entry and then click the “OK” button to save the running configuration to the current power up profile. (e.g. config.da0 file)

Finally to activate the configuration changes navigate to **Status → PPP → PPP 1** and click on “Drop Link”. The PPP 1 link will automatically re-activate (subject to the unit containing a default configuration) and the new SRI feature activated.

You should test the new feature by deliberately generating traffic to trigger the firewall and checking that PPP 1 deactivates itself and re-activates itself as expected. This can be easily seen in the router's event log. **Status → Event Log**

## 2.2 GPRS/UMTS Error Detection and Recovery Techniques

### Automatic PING failure detection

This is an active error detection technique. The Router can be configured to automatically generate pings at a specified interval and send them to a destination IP address. If the Router receives no reply to these pings in a specified amount of time then the unit will deactivate PPP 1 (the GPRS PPP interface).

NB On some GPRS networks PING packets are blocked so this technique cannot be used on such a network. SRI should be used instead.

To enable automatic PING failure detection follow the steps below:

On the router's web server navigate to the **Configure → PPP Instance → Advanced** web page and set the “**PING hostname**” parameter to either, an IP address or a website that the MR-200/250 should be able to PING over the GPRS/UMTS network.

Next enter the interval in seconds at which the Router is to send a ping into the “**PING request interval (s)**” parameter (e.g. 60 seconds).

Now enter the time in seconds that the Router will wait for a reply to one of the pings into the “**No PING response reset delay (s)**” parameter. (e.g. 65 seconds which means wait 60 seconds after sending the first ping and an extra 5 seconds in case we receive a reply to the second ping within five seconds.) With this configuration, if the Router does not receive a reply to 2 pings in row then the PPP 1 link will be deactivated.

On the router's web server menu click on the “Save” entry and then click the “OK” button to save the running configuration to the current power up profile. (e.g. config.da0 file)

Finally to activate the configuration changes navigate to **Status → PPP → PPP 1** and click on “Drop Link”. The PPP 1 link will automatically re-activate (subject to the unit containing a default configuration) and the PPP ping failure detection feature activated.

You should test the new feature by deliberately ensuring that the IP address the router 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 router's event log. **Status → Event Log**. You should see an entry similar to the following; “PPP 1 PING failure.”

## GPRS Module Power Cycle

This is a passive error detection technique designed to be used by itself or in conjunction with any of the other methods mentioned in this application note.

When this parameter is set after a number of unsuccessful attempts at raising PPP 1 (i.e. obtaining an IP address from the GPRS network) the Router will power cycle the GPRS module.

This feature can be enabled by Navigating to **Configure** → **GPRS Module** and setting the “Link retries:” parameter to a value such as 15. This means that after 15 unsuccessful attempts at activating PPP the GPRS module will be power cycled. This feature can be checked by deliberately “sabotaging” the Router’s attempts to connect to the GPRS network by for example programming in a wrong APN. Next deactivate PPP instance 1 and then inspect the Router’s event log. Check for an entry like the “GPRS Link Failed → power cycle” entry below which will occur after 15 failed attempts at connecting.

```
15:30:30, 24 Jun 2003,LAPB 5 up
15:30:30, 24 Jun 2003,LAPB 4 up
15:30:30, 24 Jun 2003,LAPB 3 up
15:30:18, 24 Jun 2003,LAPB 5 down,Lower deactivated
15:30:18, 24 Jun 2003,LAPB 4 down,Lower deactivated
15:30:18, 24 Jun 2003,LAPB 3 down,Lower deactivated
15:30:17, 24 Jun 2003,PPP 1 down,LL disconnect
15:30:17, 24 Jun 2003,GPRS link failed -> power cycle
15:29:11, 24 Jun 2003,PPP 1 down,LL disconnect
15:28:06, 24 Jun 2003,PPP 1 down,LL disconnect
15:27:00, 24 Jun 2003,PPP 1 down,LL disconnect
15:25:55, 24 Jun 2003,PPP 1 down,LL disconnect
15:24:49, 24 Jun 2003,PPP 1 down,LL disconnect
```

## MR-200/250 unit reboot

This is a passive error detection technique designed to be used in conjunction with the GPRS Module Power Cycle technique above.

Under some very rare circumstances it may be necessary to reboot the entire unit to recover from a serious GPRS error. Note that we are not aware of any such situations currently but the functionality is included just in case. To enable this functionality;

On the router’s web server navigate to the **Configure** → **PPP Instance** → **Advanced** web page and set the “Reboot after this many consecutive failed connections” parameter to a suitable value such as 25. Click the “OK” button at the bottom of the page.

Next enter the interval in seconds at which the Router is to send a ping into the “PING request interval (s)” parameter (e.g. 60 seconds).

On the router’s web server menu click on the “Save” entry and then click the “OK” button to save the running configuration to the current power up profile. (e.g. config.da0 file)

Finally to activate the configuration changes navigate to **Status** → **PPP** → **PPP 1** and click on “Drop Link”. The PPP 1 link will automatically attempt to re-activate (subject to the unit containing a default configuration).

NB The “Reboot after this many consecutive failed connections” MUST ALWAYS be set to a value significantly larger than the GPRS Module Power Cycle “Link Retries” parameter or the GPRS module will NEVER be power cycled. (Rebooting the Router will not power cycle the GPRS module and power cycling the GPRS module is of much greater importance when trying to fix a GPRS problem then rebooting the Router itself.

The correct functioning of this facility can be tested by entering an incorrect APN into the Router, saving this change and inspecting the event log. The event log below shows the Router power cycling the GPRS module after 15 attempts to connect and then rebooting the entire Router after a further 10 attempts:

```

15:41:46, 24 Jun 2003, PPP 1 down, LL disconnect
15:40:40, 24 Jun 2003, PPP 1 down, LL disconnect
15:40:24, 24 Jun 2003, LAPB 5 up
15:40:24, 24 Jun 2003, LAPB 4 up
15:40:24, 24 Jun 2003, LAPB 3 up
15:40:15, 24 Jun 2003, PPP 1 down, LL disconnect
15:39:56, 24 Jun 2003, PPP 1 down, LL disconnect
15:39:41, 24 Jun 2003, ETH 0 up
15:39:40, 24 Jun 2003, ETH 1 up
15:39:38, 24 Jun 2003, Power-up
15:39:38, 24 Jun 2003, Eventlog Counters Reset
15:39:30, 24 Jun 2003, Reboot
15:39:30, 24 Jun 2003, PPP 1 failed -> reboot
15:39:30, 24 Jun 2003, PPP 1 down, LL disconnect
15:38:24, 24 Jun 2003, PPP 1 down, LL disconnect
15:37:19, 24 Jun 2003, PPP 1 down, LL disconnect
15:36:13, 24 Jun 2003, PPP 1 down, LL disconnect
15:35:08, 24 Jun 2003, PPP 1 down, LL disconnect
15:34:02, 24 Jun 2003, PPP 1 down, LL disconnect
15:32:57, 24 Jun 2003, PPP 1 down, LL disconnect
15:31:51, 24 Jun 2003, PPP 1 down, LL disconnect
15:30:46, 24 Jun 2003, PPP 1 down, LL disconnect
15:30:30, 24 Jun 2003, LAPB 5 up
15:30:30, 24 Jun 2003, LAPB 4 up
15:30:30, 24 Jun 2003, LAPB 3 up
15:30:18, 24 Jun 2003, LAPB 5 down, Lower deactivated
15:30:18, 24 Jun 2003, LAPB 4 down, Lower deactivated
15:30:18, 24 Jun 2003, LAPB 3 down, Lower deactivated
15:30:17, 24 Jun 2003, PPP 1 down, LL disconnect
15:30:17, 24 Jun 2003, GPRS link failed -> power cycle
15:29:11, 24 Jun 2003, PPP 1 down, LL disconnect
15:28:06, 24 Jun 2003, PPP 1 down, LL disconnect
15:27:00, 24 Jun 2003, PPP 1 down, LL disconnect
15:25:55, 24 Jun 2003, PPP 1 down, LL disconnect
15:24:49, 24 Jun 2003, PPP 1 down, LL disconnect
15:23:44, 24 Jun 2003, PPP 1 down, LL disconnect
15:22:38, 24 Jun 2003, PPP 1 down, LL disconnect
15:21:33, 24 Jun 2003, PPP 1 down, LL disconnect
15:20:27, 24 Jun 2003, PPP 1 down, LL disconnect
15:19:22, 24 Jun 2003, PPP 1 down, LL disconnect
15:18:16, 24 Jun 2003, PPP 1 down, LL disconnect
15:17:11, 24 Jun 2003, PPP 1 down, LL disconnect
15:16:05, 24 Jun 2003, PPP 1 down, LL disconnect
15:15:00, 24 Jun 2003, PPP 1 down, LL disconnect
15:13:54, 24 Jun 2003, PPP 1 down, LL disconnect
15:13:38, 24 Jun 2003, LAPB 5 up

```

```
15:13:38, 24 Jun 2003,LAPB 4 up
15:13:38, 24 Jun 2003,LAPB 3 up
15:13:29, 24 Jun 2003,WEB Login OK by username lvl 0
15:13:25, 24 Jun 2003,ETH 0 up
15:13:24, 24 Jun 2003,ETH 1 up
15:13:22, 24 Jun 2003,Power-up
```

## GPRS Module Status Retries

This is a passive error detection technique. In the event that a serious error causes the Router to loose contact with its GPRS module, if no data is being routed it could be some time before the Router is made aware of the problem (e.g. via SRI) and is thus able to fix it. The Router regularly polls the GPRS module for signal strength and other status readings. Should the Router be unable to obtain these readings from the GPRS module it can be configured to power cycle the GPRS module hopefully fixing the problem.

Such an occurrence should be extremely rare but if you wish to enable this protection navigate to **Configure → GPRS Module** and set the “Status retries” parameter to a large value such as 30. This means that after 30 unsuccessful attempts at reading the status from the GPRS module, the Router will power cycle the GPRS module.