System Watchdogs Whitepaper

DOCUMENT VERSION	DATE
- Initial document release	January 2013

Table 1 - Document Revision History

Introduction

The NetComm Wireless M2M range includes multiple layers of watchdogs to ensure that you always have a way to access your devices remotely in the case that the unit is not physically accessible.

There are multiple layers of hardware and software watchdogs which all work in conjunction to provide a reliable and stable service. The user configurable watchdog features on the unit are System Monitor and SMS diagnostics.

Internal watchdogs

Hardware watchdog

The CPU has an independent process with a counter which starts at 15 seconds and counts down to 0. If the counter ever reaches zero it will perform a reboot of the device.

When the system powers up, the boot loader executes code before the Linux kernel starts, sending a signal to reset the counter to 15. This avoids the possibility of the system becoming stuck in boot loader mode. The Linux kernel then boots and sets the counter to 2 seconds and sends a signal to reset the counter every second. This means if the kernel ever crashes (panics) it will be detected in 2 seconds and the system will reboot. After the kernel has loaded the user space loads and sends the signal to the kernel to reset the timer. If the kernel does not receive the signal it will perform the reboot.

If the system ever reboots the kernel messages will show whether it was caused by the watchdog, reset via hardware button or a power cycle.

Software watchdog

Phone module

The device's phone module produces a heartbeat (signal) which is received by the kernel from the CNS port connected to the module and writes a variable into the RDB manager. If this variable is not written, the kernel will detect if the module is not responding and perform a power cycle on the module.

Connection manager

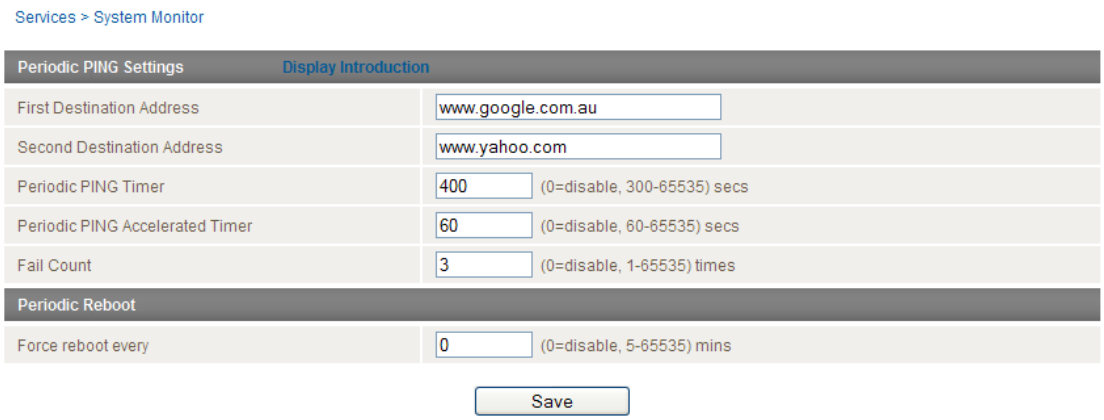
There is a connection manager which monitors the WAN connection. It detects if there is an active PDP session and reconnects if the device is rebooted.

User-configurable watchdogs

System monitor

The system monitor is a "keep alive" feature on top of the internal watchdogs. This detects cases where the device has a PDP session but no traffic can be passed through the connection. This situation may occur on the network from time to time. If the ping fails based on the prescribed conditions, the unit will reboot which will allow it to re-establish a valid data connection.

Below is an example configuration of the ping watchdog.



Note that the above settings are only valid if the device has a connection to the internet. If there is no internet connection, specify IP addresses on the WAN side of the router.

In the above configuration the unit will ping the destination address 3 times every 400 seconds, if they fail it pings the second address 3 times every 400 seconds. If this ping fails the unit will use the Periodic PING Accelerated Timer and ping every 60 seconds. If the Periodic PING Accelerated Timer ping fails it will be recorded as a failure. After 3 failures the unit performs a software reboot.

SMS diagnostics

SMS feature allows diagnostics and control over the unit by sending an SMS to the SIM card. This allows 3 types of functions.

GET – Retrieve system information e.g. DHCP settings, APN, signal strength, Cell ID
SET – Setting system values e.g. DHCP settings, APN, IP address
EXECUTE – Execute scripts or commands e.g. rebooting the device, enable/disable data connection

In the scenario where the device is unreachable over the packet switched network (3G), it is still possible to reboot the unit via an SMS or perform diagnostic commands. In most scenarios, the device will always be registered to the SGSN. Having this feature enabled allows additional options to access the device.