User Guide – OWL Self-Monitoring Concepts

Contents

Introduction

This document explains the operation of watchdogs in OWL cellular routers. The hardware watchdog and software watchdogs are described to make it clear why the router reboots.

Continuous connectivity features are described subsequently to understand the possibilities of connection checks and monitoring in OWL cellular routers.

Hardware Watchdog

Brief Description

The routers have an internal hardware watchdog circuit. This extra component oversees the operation of the router's processor. The processor sends a keep alive signal to the watchdog regularly, so the watchdog knows the processor is still running. If the watchdog circuit doesn't get any keep alive signal (processor stuck), it will reboot the router.

Detailed Description

The watchdog in the routers is an extra component on the PCB, not integrated in the router's processor. The watchdog component has its own independent internal timer and it doesn't share the clock with the processor or other peripherals. There is a keep alive signal route from the processor to the watchdog circuit WDI input (Watch Dog-In) and the watchdog responds to level changes of this signal (edges). The router's processor sends the keep alive signal very early after initialization - it is one of Linux kernel drivers waiting on the prompt from one of the initialized applications - so when the keep alive signal is sent, it is the awaited information that the system was initialized successfully. The frequency of the refreshing signal from the processor is higher than 1 Hz. If the watchdog circuit doesn't get the refreshing pulse in the expected time, it will reboot the whole router (equal to turning the router off and on). Not only the processor is reset, but a global reset is done (including all the peripherals like memories, etc.).

Router Timing

In OWL routers the watchdog operates in one mode only - it always waits 60 seconds - at the initialization and after the first refreshing pulse is delivered. (So the reboot is done up to 60 seconds when the processor gets stuck).

Software Watchdogs

Supervised Applications

There is a daemon `watchdogd` *supervising the operation of the key daemons* `pppsd` *and* `bard`*. These key daemons handle the connection to WAN (establishing connections and backup routes) and refresh the* `watchdogd` *daemon. The* `watchdogd` *daemon is refreshing the hardware watchdog. If there is a problem in* `pppsd` *or* `bard` *(e.g. stuck, looped or terminated unexpectedly), it will stop to refresh the* `watchdogd` *daemon, which will stop to refresh the hardware watchdog component. This will cause the reboot of the router.*

There is an internal reboot log, messages from the reboot log will appear in the System Log. These are possible System Log messages leading to reboot:

```
Multiple instances of daemon detected - rebooting (reboot called
directly by pppsd) Unable to create thread "main_loop" - rebooting

Unable to create thread <level of the thread>

service <name of service> timed out (<time in sec.> sec) (looped or
terminated unexpectedly)
```

There are also less important services supervised by daemons such as `l2tp` *or* `pppoe`*. Services like* `eth` *or* `wlan` *do not have a daemon, they can get out of problems by themselves.*

Mobile Network Registration Supervised

The `pppsd` *daemon supervises the registration to the mobile network also and it can cause the reboot of the cellular module (only if needed). By default it checks the registration every 2 minutes. If the cellular module is not registered, it is switched off and back on again. If this happens 5 times in a row, then a reboot of the router will be performed. These are examples of the cellular module reboot (messages in the System Log):*

```
module not responding

unable to kill process (when terminating the connection) WARNING: module
not detected

unable to prepare module for mobile communications
```

Uptime, Standard Ways to Reboot and System Log

Uptime

The information about the Uptime of the router (time of operation without reboot) is on the main page (General item in the Status section) of the router's web interface at the bottom in the ***System Information*** *block.*

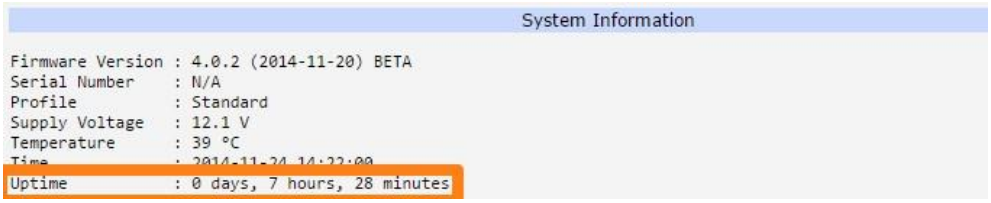

Figure 1: Uptime information in the Status section

Standard Reboots

The standard way to reboot the router mechanically is to disconnect the power supply cable from the router and connect it back again. This can be done remotely from router's web interface using the **Reboot** *item in the* **Administration** *section.*

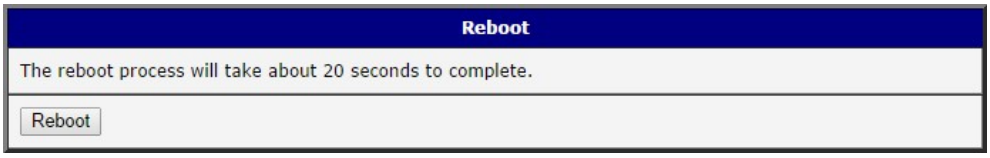

Figure 2: Reboot through the webinterface

Standard reboot of the router without user's intervention can be caused by the **Automatic Update** *feature (Configuration section of the router's web interface) as well.*

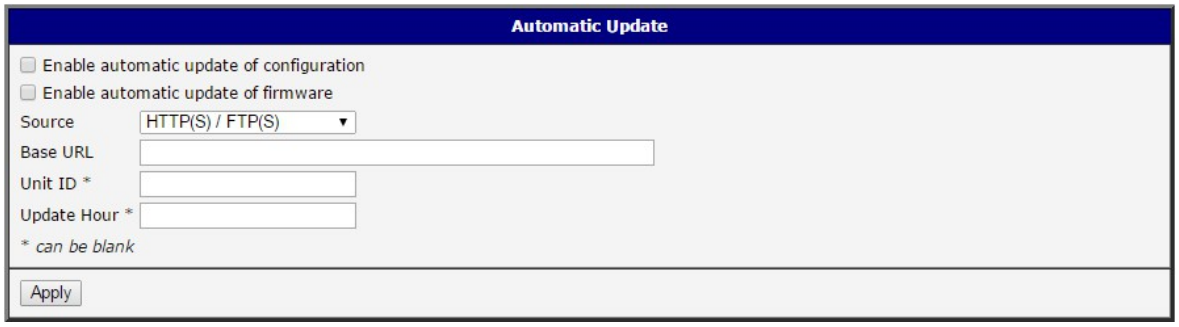

Figure 3: Automatic Update configuration

If the `Enable automatic update of configuration` *or* `Enable automatic update of firmware` *options are enabled, then the router will check the configured source (Server or USB flash or both) at the configured time* `Update Hour` *every day (or 5 minutes after start and then every 24 hours if not specified). When the* `Update Hour` *arrives and the router finds out the configuration file or the firmware file is different from the currently running one, it will download the new one and reboot.*

- *A new configuration reboot takes up to 20 seconds*
- *Update of the firmware takes up to 3 minutes and the reboot is done when it finished. During the firmware update some services of the router can be temporarily unavailable.*

A standard reboot of the router can be performed by user in the `Restore Configuration` *and* `Update Firmware` *items in the Administration section of the router's web interface as well.*

`Restore Configuration` *offers choosing the configuration file from the computer and uploading it to the router. If the configuration file is different, the user is offered to reboot the router to take effect of the new configuration.*

When `Update Firmware` *is performed manually, it will reboot once it is completed.*

When clicking the `Apply` *button anywhere else in the router's web interface to change the configuration, no reboot is performed. Only the proper scripts are called.*

System Log

```
2015-02-03 13:37:17 bard[792]: backup route released: "Primary LAN"
2015-02-03 13:37:17 bard[792]: terminated
2015-02-03 13:37:18 bard[1225]: selectable backup routes:
2015-02-03 13:37:18 bard[1225]: "Mobile WAN"
2015-02-03 13:38:17 pppsd[1215]: WARNING: SIM card is missing
2015-02-03 13:38:17 pppsd[1215]: turning off module
2015-02-03 13:38:20 pppsd[1215]: turning on module
2015-02-03 13:38:20 pppsd[1215]: selected SIM: 1st
```

Figure 4: System log messages

The information about starting and stopping services, applications or the wireless modules are accessible in the `System Log` *item in the Status section of the router's web interface.*

The messages of the System Log are stored and available in the `/var/log/messages` *file of the router's file system. You can access this file for example via Telnet, FTP or SSH.*

Continuous Connectivity Features

Check Connection to Mobile Network

Ensuring a continuous connection to the mobile network is done using ICMP ping requests. Pings are sent to a defined IP address in defined time interval. If there are three failures in a row (ICMP Echo Reply), the router terminates the current connection and tries to establish a new one. `Check connection` *can be set separately for two SIM cards or two APNs. It can be configured in the* `Mobile WAN` *item in the* `Configuration` *section of the router's web interface. See the table below explaining the configuration items.*

It is highly recommended to enable this feature for an uninterrupted and lasting connection to the mobile network.

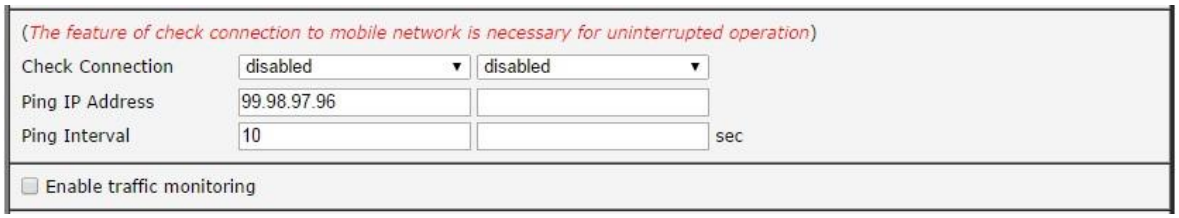

Figure 5: Mobile connection check

Table 1: Mobile connection check settings

Item	Description
Check Connection	• `Disabled` - *Check of connection is not performed.* • `enabled` - *Check of connection activated, the router will automatically send ping requests to the Ping IP Address in regular Ping Interval. Ping requests are sent according to the route table through any network interface.* • `enabled+bind` - *Ping requests are sent only via the same interface the connection was created by. Necessary for use within the Backup Routes system.*

Item	Description
Ping IP Address	*Destinations IP address or domain name of ping queries (e.g. DNS server of the operator).*
Ping Interval	*Time interval between the outgoing pings.*
Enable traffic monitoring	*The router will stop sending ping requests and will watch the mobile traffic. If there is no traffic for interval longer than Ping Interval, the router will start to send ping requests.*

Backup SIM Card or APN

It is possible to set up the `Backup SIM` *card or APN (Access Point Name, if using one SIM card) and the behavior of switching between SIM cards (APNs). This can be configured in the* `Mobile WAN` *menu. If the parameter* `Backup SIM` *card is set to* `none`*, then the following parameters are not applicable. When parameter* `Switch to other SIM card when connection fails` *is enabled, then then the Backup SIM card is used (or APN set at that SIM card if using one SIM card).*

Failure of the primary SIM card connection to mobile network can occur:

- *When there are three failures to establish the connection after turning on the router.*
- *When there is a connection loss indicated by the* `Check Connection` *feature (e.g. it cannot reestablish the connection or it did not receive the ICMP Echo Reply)*

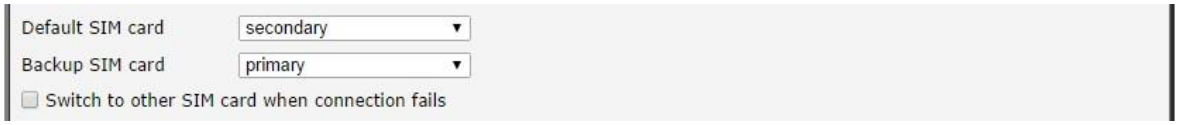

Figure 6: Backup SIM card configuration

Backup Routes System

It is possible to setup priorities of the multiple connections to WAN in the `Backup Routes` *item in the* `Configuration` *section of the router's web interface. The backup routes system can be enabled, particular connections can be added to the backup routes system and the priority can be*

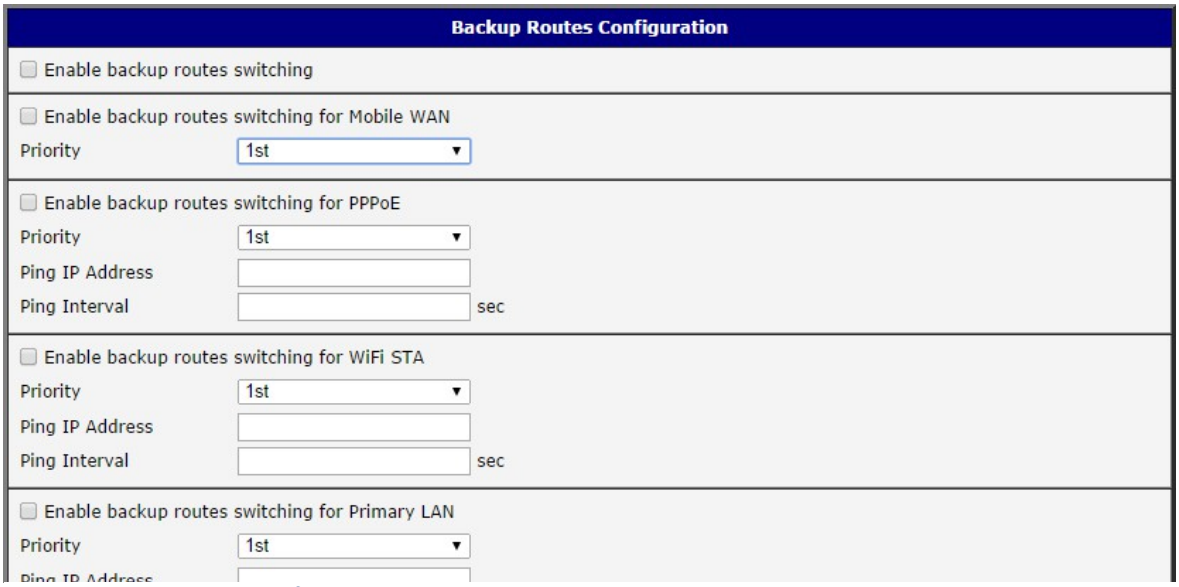

Figure 7: Backup routes configuration

defined at each connection. Ping IP Address and Ping Interval for every connection can be set. If the target is unreachable, the system uses another connection according to the priorities.

There are implicit priorities even if the backup routes system is disabled (network interfaces in brackets):

1. *Mobile WAN (pppX, usbX)*
2. *WiFi STA (wlan0)*
3. *Secondary LAN (eth1)*
4. *Primary LAN (eth0)*

Daily Reboot

The daily reboot feature - for a preemtive reboot of the router at the same time every day - is not a standard part of the router's firmware. It can be added as a user module `Daily Reboot`*. This user module is available on request from https://hirschmann-support.belden.com web pages and can be uploaded to the router in the* `User Modules` *item in the* `Customization` *section of the router's web interface. It is possible to enable or disable the daily reboot and set the time of the reboot.*

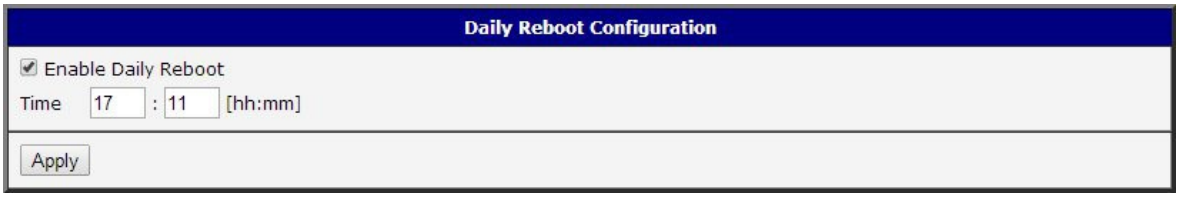

Figure 8: Daily reboot configuration

VRRP Check Connection

The router supports the VRRP (Virtual Router Redundancy Protocol) so it is possible to configure this redundancy backup using two routers.

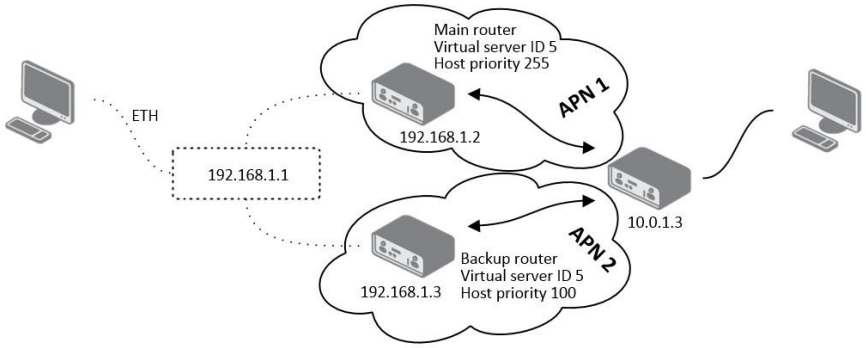

Figure 9: Example VRRP topology

The VRRP configuration is accessible via the `VRRP` *item in the* `Configuration` *section of the router's web interface. It is possible to setup VRRP standard parameters (Virtual Server IP Address, Virtual Server ID, Host Priority) and also the* `Check connection` *feature ticking the checkbox.*

Table 2: VRRP Check connection parameters

Item	Description
Ping IP Address	Destinations IP address of ping queries. Only IP addresses, no domain names (DNS) allowed.
Ping Interval	Time intervals between the outgoing pings.

Item	Description
Ping Timeout	Time to wait for the answer.
Ping Probes	Number of failed ping requests after which the route is considered disconnected.
Enable traffic monitoring	Pings are only sent when no other traffic is present. If there is no traffic for `Ping Timeout` time, the pings are being sent to see if the route is disconnected or not.

OpenVPN Check Connection

There is a check connection feature at the OpenVPN tunnel configuration (OpenVPN item in the Configuration section of the router's web interface). In the middle of the configuration form, there are these optional parameters:

When the Check connection feature finds the opposite side of the tunnels is unreachable by ping, it will terminate the tunnel connection and will try to create it again.