Application Note

Watchdog Concept

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0072-EN, revision from 15th November, 2024.

© 2024 Advantech Czech s.r.o. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and it does not represent a commitment on the part of Advantech.

Advantech Czech s.r.o. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that can arise in specific situations.

Information – Useful tips or information of special interest.

Contents

1. Watchdog Concept Introduction **1**

2. Hardware Watchdog **2**

2.1 Brief Description . . . 2
2.2 Detailed Description . . . 2
2.3 v2 Routers Timing . . . 2
2.4 v3 Routers Timing . . . 2

3. Software Watchdogs **3**

3.1 Key Daemons Supervised . . . 3
3.2 Mobile Network Registration Supervised . . . 3
3.3 Uptime, Standard Ways to Reboot and System Log . . . 4

4. Continuous Connectivity Features **6**

4.1 Check Connection to Mobile Network . . . 6
4.2 Backup SIM Card or APN . . . 6
4.3 Backup Routes System . . . 7
4.4 Daily Reboot . . . 8
4.5 VRRP Check Connection . . . 8
4.6 OpenVPN Check Connection . . . 8
4.7 Expansion Ports and USB Interface Keepalive . . . 9

5. Related Documents **11**

List of Figures

1 Uptime information in the *Status*, *General* . . . 4
2 Standard reboot feature in the *Administration* section . . . 4
3 Automatic Update configuration . . . 4
4 System Log messages . . . 5
5 Check mobile connection configuration . . . 6
6 Backup SIM card configuration . . . 7
7 Backup Routes configuration . . . 7
8 Daily Reboot router app configuration . . . 8
9 Example of VRRP topology . . . 8
10 TCP Keepalive configuration . . . 9

List of Tables

1 Items of check mobile connection configuration . . . 6
2 VRRP *Check connection* parameters . . . 9
3 VRRP *Check connection* parameters . . . 9
4 TCP Keepalive parameters at Expansion Ports and USB interfaces . . . 9

5 CD/DTR signals and the indication/control of a TCP connection 10

1. Watchdog Concept Introduction

This document explains the operation of watchdogs in Advantech 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 what are the possibilities of connection checks and monitoring in the Advantech cellular routers.

2. Hardware Watchdog

2.1 Brief Description

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

2.2 Detailed Description

The watchdog in Advantech routers is an extra component on the PCB, not integrated in the router's processor. Watchdog has it's own independent internal timer, it doesn't share the clock with the processor or other peripherals. There's a refreshing signal route from the processor to the watchdog circuit WDI input (Watch Dog-In) and the watchdog responds to level change of this signal (edges). Router's processor sends the refreshing signal very early after initialization – it is one of Linux kernel drivers waiting on the prompt from one of the initialized program – so when the refreshing signal is sent, it is the information 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 off and on the router). Not only processor is reset, but the global reset is done (including all the peripherals like memories, etc.).

2.3 v2 Routers Timing

In v2 routers platform, the watchdog circuit waits 60 seconds after turning on the power supply of the router. The processor does the initialization and sends the first refreshing pulse to watchdog before 60 seconds interval expire. The first refreshing pulse turns the watchdog into next operating mode – now the watchdog is waiting on the refreshing pulse every 1 second. (So the reboot is done up to 1 second when processor stuck).

2.4 v3 Routers Timing

In v3 routers platform the watchdog operates in one mode only – it waits 60 seconds always – at the initialization and after the first refreshing pulse delivered. (So the reboot is done up to 60 seconds when processor stuck).

3. Software Watchdogs

3.1 Key Daemons Supervised

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. *Watchdogd* daemon is refreshing the hardware watchdog. If there is a problem in *pppsd* or *bard* (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 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* doesn't have a daemon, they can get out of problems by themselves.

3.2 Mobile Network Registration Supervised

The *pppsd* daemon supervises the registration to 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 on back again. If this happens 5 times in a row, then reboot of the router will be done. The examples of the cellular module reboot reasons (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`
etc.

3.3 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.

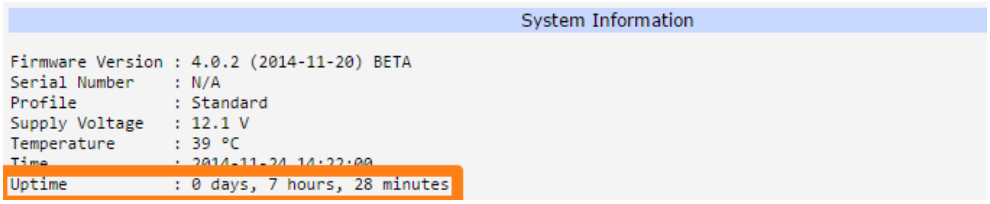

Figure 1: Uptime information in the *Status*, *General*

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.

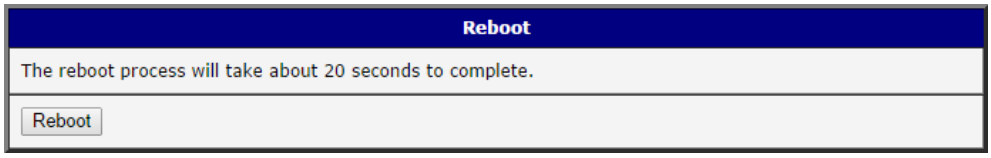

Figure 2: Standard reboot feature in the *Administration* section

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).

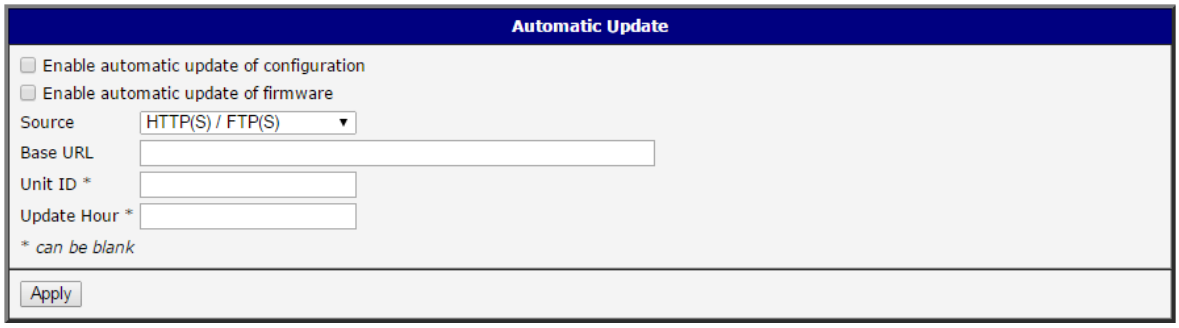

Figure 3: Automatic Update configuration

If the *Enable automatic update of configuration* or *Enable automatic update of firmware* option enabled, the router will check the configured source (Server or USB flash disc 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* comes and the router finds out the configuration file or the firmware file is different from the running one, it will download the new one and reboot. In case of the new configuration the reboot takes up to 20 seconds. Update of the firmware takes up to 3 minutes and the reboot is done when finished. During the firmware update some services of the router can be temporarily unavailable.

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, too. *Restore Configuration* offers choosing

of 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* performed manually, it will reboot when finished, of course.

When clicking the *Apply* button anywhere else in the router's web interface to change the configuration, reboot is not done, only the proper script is called.

System Log

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

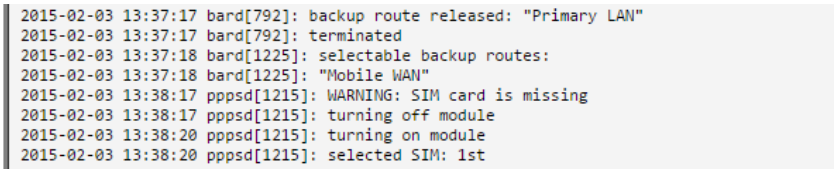

Figure 4: System Log messages

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 via Telnet, FTP or SSH.

4. Continuous Connectivity Features

4.1 Check Connection to Mobile Network

The important feature for continuous connection to the mobile network is done using the ICMP ping requests. Pings are sent to defined IP address in defined time interval. If there are three failures in a row (did not get 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 necessary to enable this feature for uninterrupted and lasting connection to the mobile network.

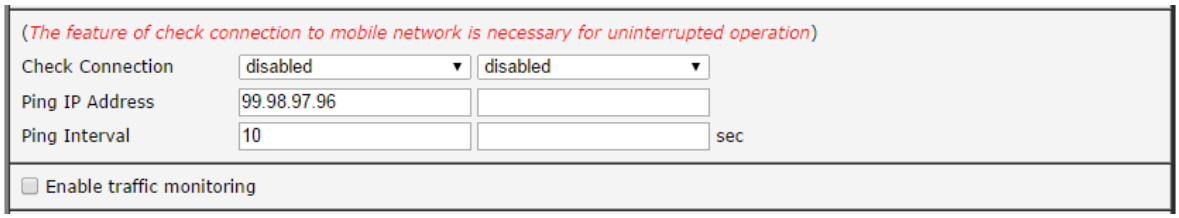

Figure 5: Check mobile connection configuration

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.
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.

Table 1: Items of check mobile connection configuration

4.2 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*, too. If the parameter *Backup SIM card* is set to none, then parameters bellow (beginning *Switch ...*) are not applicable. When parameter *Switch to other SIM card when connection fails* enabled, then 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 connection loss indicated by *Check Connection* feature (can't reestablish the connection when didn't received the ping Echo Reply)

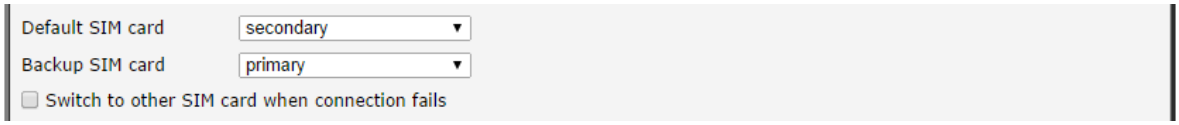

Figure 6: Backup SIM card configuration

4.3 Backup Routes System

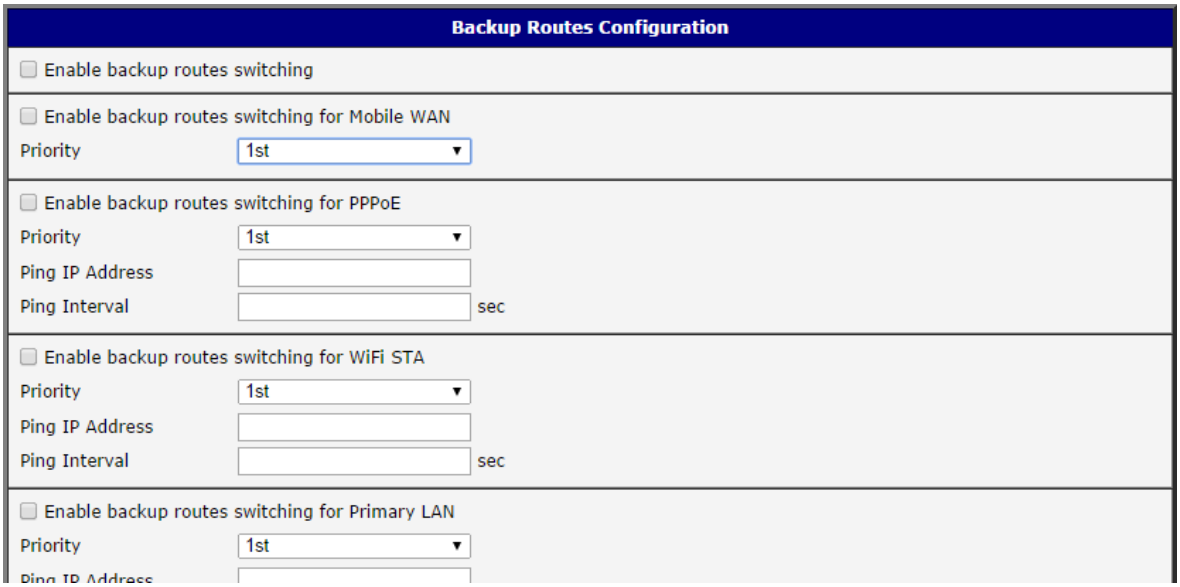

Figure 7: Backup Routes configuration

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. See the configuration form on the fig. 7. The backup routes system can be enabled, particular connections can be added to the backup routes system and the priority can be 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 priorities. There are implicit priorities even if backup routes system disabled (network interfaces in brackets):

— Mobile WAN (pppX, usbX)
— WiFi STA (wlan0)
— Secondary LAN (eth1)
— Tertiary LAN (eth2), on v3 routers only
— Primary LAN (eth0)

4.4 Daily Reboot

The daily reboot feature – for preventive 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 router app *Daily Reboot*. This router app can be downloaded from icr.advantech.com web pages and uploaded to the router in the *Router Apps* 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 – see fig. 8.

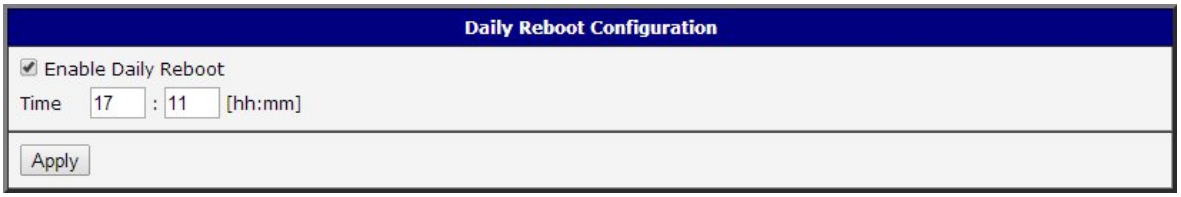

Figure 8: Daily Reboot router app configuration

4.5 VRRP Check Connection

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

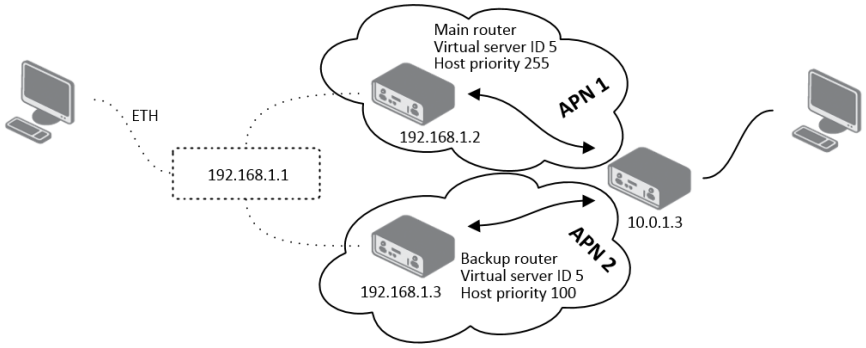

Figure 9: Example of VRRP topology

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 *Check connection* checkbox. See the table below for parameters explained:

4.6 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.

Item	Description
Ping IP Address	Destinations IP address of ping queries. Address can not be specified as a domain name.
Ping Interval	Time intervals between the outgoing pings.
Ping Timeout	Time to wait for the answer.
Ping Probes	Number of failed ping requests the route is took as disconnected after.
Enable traffic monitoring	Pings are not being sent. If there is no traffic for *Ping Timeout* time, the pings are being sent to see if the route is disconnected or not.

Table 2: VRRP *Check connection* parameters

Item	Description
Ping Interval	time interval of checking the existence of the tunnel's opposite side.
Ping Timeout	time interval to wait for the answer from the opposite side. For proper verification of OpenVPN tunnel, *Ping Timeout* must be longer than *Ping Interval*.

Table 3: VRRP *Check connection* parameters

4.7 Expansion Ports and USB Interface Keepalive

It is possible to activate the TCP Keepalive check connection feature at the *Expansion Port 1*, *Expansion Port 2* and *USB Port* items of the router's web interface (*Configuration* section). These items in the configuration correspond to the physical router's interfaces (serial line connectors of expansion ports and USB connector). If access via TCP/IP to the Expansion Port (or USB serial converter) used (in the upper part of the form), the *Check TCP Connection* can be activated. Explanation of the parameters in the table below:

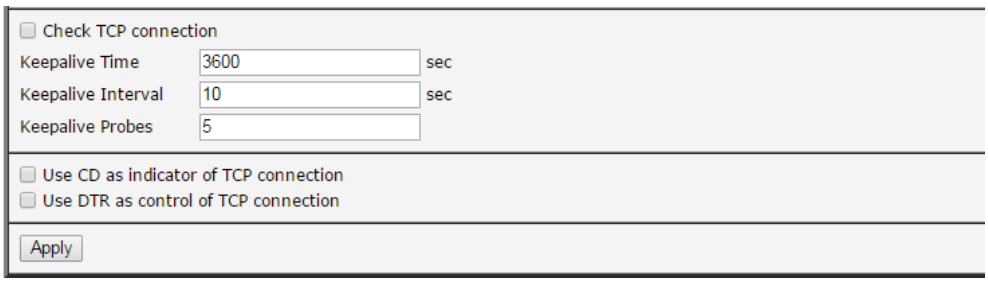

Figure 10: TCP Keepalive configuration

Item	Description
Keepalive Time	Time interval between the check transmissions.
Keepalive Interval	Time of waiting for the answer when the check transmission sent.
Keepalive Probes	Number of check retransmissions. These are sent if there is no answer in *Keepalive Interval*.

Table 4: TCP Keepalive parameters at Expansion Ports and USB interfaces

The TCP Keepalive mechanism is good for checking dead peers and preventing disconnection due to

network inactivity. Check transmissions are the empty data packets with the ACK (Acknowledge) flag turned on. The answer is the empty data packet with ACK flag on, too – according to the TCP/IP specifications.

It is possible to use the serial line signals as the indicator or control of the TCP connection, too. The table bellow explains these options:

Item	Description
Use CD as indicator of TCP connection	Active CD signal (Carrier Detect) indicates the TCP connection is on in the serial device to router direction. Active DTR signal (Data Terminal Ready) indicates the same in the router to serial device direction.
Use DTR as control of TCP connection	Enables control of the TCP connection dependent on the interface's TCP configuration (Server/Client): — **Router is the TCP Server** – Active CD/DTR signal means the establishment of a TCP connection is allowed — **Router is TCP Client** – Active CD/DTR signal means the router starts the TCP connection.

Table 5: CD/DTR signals and the indication/control of a TCP connection

5. Related Documents

You can obtain product-related documents on the **Engineering Portal** at *icr.advantech.com*.

To access your router's documents or firmware, go to the *Router Models* page, locate the required model, and select the appropriate tab below.

Documents that are common to all models and describe specific functionality areas are available on the *Application Notes* page.

The **Router Apps** installation packages and manuals are available on the *Router Apps* page.

If you are interested in further options for extending router functionality, either through scripts or custom Router Apps, please see the information available on the *Development* page.