A B&B ELECTRONICS Company

List of FW 4.0.0 changes

All routers

Added a password check when remote access is enabled

If a password to access the router is set to *root*, remote access is disabled. This means that remote access via http, HTTPS, FTP, SSH or Telnet can't be enabled via a web interface until the user changes the default password (root).

Added the option configure multicast for GRE tunnels

The User is allowed to choose whether multicast is enabled or disabled (applies only to GRE tunnels). In previous versions of the firmware, multicast strictly disabled.

This option was added per customer request.

Enhanced configuration of firewall

Security of the routers was enhanced though new firewall configurations. To configure via a web interface, a new form for rule definition regarding filtering of forwarded packets is included on the page for Firewall Configuration. The first item – *Enabled filtering of forwarded packets* – determines the forwarding policy (if it's not checked, packets are automatically accepted). Then, users are presented with a table for rule definition. It is possible to allow all traffic within the selected protocol (rule specified) or; the user can create stricter rules by specifying items for source and destination IP address.

There is also the option to drop a packet whenever a request for service arrives that is not in the router (checkbox named *Enable filtering of locally destinated packets*).

To protect against DoS attacks, the option named *Enable protection against DoS attacks* limits the number of connections per second to five.

Modified reading of temperature and supply voltage via SNMP protocol

Currently, if any router does not support reading of temperature or supply voltage, a *null* value is sent. Now, the reading of temperature and supply voltage via SNMP protocol is performed for all routers. This is an advantage when using the monitoring system R-SeeNet, because the request for reading temperature and supply voltage values can be sent to all routers.

Changed value of enterprise OID in SNMP traps

Each type of router has its own OID. This means that the monitoring system can identify the type of a router.

Disabled remote access via SNMP in default configuration

Remote access via SNMP is disabled as default (in previous versions this was enabled). If the user wishes to enable it, it is necessary to do it manually in the web interface of the router.

Prohibited processing DNS request incoming from WAN

Any DNS request coming from anywhere but the WAN is dropped. This change was performed to improve security

Added new algorithm for reliable identification of backup route parameter change

Under certain circumstances, identification of backup router may result in incorrect switching. This change solved it.

Removed router identification during login process

During the login process, it was not clear which router the user was logging into (the router is not identified). This change was made to improve security.

Fixed VRRP initialization

If the VRRP superstructure was activated by selecting the *Check connection* option; VRRP was terminated when the backup route was switched for the first time. Now, VRRP initialization works correctly.

DHCP timestamp

If the timezone was set to GMT+1, GMT was displayed on the DHCP Status page. This has been corrected.

All routers with the exception of the ER75i and the UR5

Fixed processing of IPsec packets when subnets are overlapping each other

Fixed a bug that occurred whenever a smaller subnet was a part of a larger subnet (ie. subnets of a tunnel overlaped). In this situation, the local packets were sent to the other side of a tunnel.

Upgraded OpenSSL to version 1.0.1g

OpenSSL has been upgraded to version 1.0.1g.

Upgraded OpenSSH to version 6.4p1

OpenSSH has been upgraded to version 6.4p1.

Upgraded OpenVPN to version 2.3.3

OpenVPN has been upgraded to version 2.3.3.

Upgraded OpenSWAN to version 2.6.41

OpenSWAN has been upgraded to version 2.6.41.

Upgraded dhcpcd to version 6.2.1

Dhcpcd has been upgraded to version 6.2.1.

Upgraded dnsmasq to version 2.68

Dnsmasq has been upgraded to version 2.68.

Upgraded ftpd to version 1.9.2

Ftpd has been upgraded to version 1.9.2.

Upgraded ppp to version 2.4.5

Ppp has been upgraded to version 2.4.5.

Upgraded pptp to version 1.8.0

Pptp has been upgraded to version 1.8.0.

Upgraded pptpd to version 1.4.0

Pptpd has been upgraded to version 1.4.0.

Upgraded tcpdump to version 4.5.1

Tcpdump has been upgraded to version 4.5.1.

All routers apart from ER75i, UR5 and XR5i

Added passing of interface name to scripts ip-up and ip-down in user modules

After establishing the connection, the name of interface is passed to ip-up and ip-down scripts in user modules. Therefore, scripts will know the name of current used interface, making it possible to use this name within the scripts.

All v2 routers

Added WiFi support

It is now possible to configure a WiFi connection in the web interface of v2 router. In previous versions, it was necessary to use a specific user module (WiFi STA or WiFi AP). Backup routes switching for the WiFi client is also available (see the *Backup Routes* page in the web interface).

Added an indicator of the XC-SD expansion board

The XC-SD expansion port is now correctly recognized and displayed as *XC-SD* in the web interface. Previously, this expansion port was displayed as *unknown*.

Upgraded kernel to version 3.5.0

Linux kernel has been upgraded to version 3.5.0.

All routers apart from the XR5i, XR5i v2 and SPECTRE RT

Fixed the online to offline mode change when the same SIM is used

When both the online and offline modes used the same SIM card, the change did not take place. This has been corrected.

All routers apart from the XR5i, XR5i v2, CR10 v2 and SPECTRE RT

Fixed a problem with switching back from offline mode to default one when the preferred operator is specified but not selected by GSM module. (even if available)

It is possible to switch to the default SIM card after timeout, even though roaming on the current SIM card is detected. To configure via the router web interface, select the checkbox named *Switch to default SIM card after timeout*, even though checkbox named *Switch to backup SIM card when roaming is detected and switch to default SIM card when home net-work is detected* has already been selected.

Enabled SMS reading from module when connection is not established or not in offline mode

The identified routers have the following rule: It is not possible to communicate with the module on the second channel (where SMS messages are read) when a ppp/dip connection is being established. Since FW 3.0.7, the space for reading SMS was slightly narrowed beyond this rule. However, this reduction in space made it difficult to read SMS when system rules allowed. The space for reading SMS messages was re-extended.

All routers apart from XR5i, XR5i v2, CR10 v2 and SPECTRE routers

Added default APN "com4" for PLMN 24209

APN database is now supplemented with further APN ("com4" for PLMN 24209).

Modified default APN for PLMN23205 to "fullspeed"

The APN for PLMN23205 in APN database has been modified (to "fullspeed").

ER75i and UR5

Added match extension "limit" to iptables

This limit is used by the new firewall in Conel routers, so it was necessary to update older models. It is used to limit the data flow, which is useful for defense against DoS attacks.

Fixed demaging of packets that go through GRE tunnel

Incorrect functioning of GRE tunnels (the demaging of packets that go through a GRE tunnel) was corrected.

UR5 v2 and UR5i v2

Fixed SMS message receipt from the PHS8 module

If a router was equipped with a PHS8 module, the receipt of SMS messages was problematic. This is now corrected.

SPECTRE 3G and SPECTRE LTE

Updated driver for Gobi 3000/4000modules to version S2.17N2.23

The driver (from Sierra Wireless company) for Gobi 3000/4000 modules was updated. The new driver increases download speed and fixes bugs.

CR10 v2 and UCR11 v2

Modified initialization of CDMA modules due to issues with newer firmware

An essential change was made to the default settings in Cellient modules which are used in CDMA routers.

UCR11 v2

Added blocking of traffic from module which is not used as default route

When two ppp/dip connections are established, one it typically the lead default route and the other is ready as a backup. However, a packet occasionally arrive through the backup connection. When this happens, the router generates a response to this packet and the response is routed to the default connection. If the default connection leads to a CDMA network and the packet has an unknown IP address, (for example, in the UMTS network from which original message came through); the operator disconnects the connection and it becomes necessary to re-establish it. The problem was solved as follows: All incoming traffic on the backup connection is blocked with the exception of the echo reply. This still makes it possible to check the backup route.

Fixed the default SIM card indicator

If the priority is changed using the configuration form on *Mobile WAN* page in the web interface, the indicator is now correctly updated in the information section on the *Mobile WAN* page.

SPECTRE LTE

Fixed initialization of Sierra Wireless MC7750 modules

SPECTRE LTE routers indicated an incorrect initialization for the Sierra Wireless MC7750 modules. This problem is now corrected.

ER75i

Fixed indication of selected SIM card

This change applies to the oldest versions of the ER75i router. There was a problem with pin, which performed SIM selection. This pin is now re-initialized.