MuLogic

RSA-SERIES

INDUSTRIAL REMOTE ACCESS ROUTER

RSA-series web configuration guide
Issue 1.10
July 2018

MuLogic BV
Plesmanstraat 58D
3905KZ, Veenendaal, The Netherlands

RSA-Series Industrial Remote Access Routers

About this user guide

Although this user guide was written with greatest possible care, omissions and errors cannot be precluded.
MuLogic BV accepts no liability for any inaccuracies that may be found.
However, if you have comments or suggestions about this guide, then please don't hesitate to contact us in order to help us improving our documentation.

Use of open source software

The firmware of the RSA-series partly contains open source software that was written under GNU General Public Licence (GPL) and other public licences.
We can make the source code of this open source software available on request. Contact MuLogic for more information.

Tel: +31 850 160600
Fax: +31 850 160601
E-mail: doc@mulogic.com
Website: www.mulogic.com

Issue No 1.10 (July 2018)

Contents

1 Introduction

This user guide describes the web based configuration of the RSA-series of DSL and WWAN routers.

Hardware details are found in the “hardware and start-up guides” of the individual units.

RSA-Series product feature table

	Eth Ports	ADSL2+	VDSL2	RS232 port	RS485 port	USB ports	2G WWAN	3G WWAN	4G WWAN
RSA-1120D	1	✓	-	✓	✓	-	-	-	-
RSA-1220D	1	✓	✓	✓	✓	-	-	-	-
RSA-1020DW3	1	-	-	✓	✓	-	✓	✓	-
RSA-1020DW4	1	-	-	✓	✓	-	✓	✓	✓
RSA-1120M	1	✓	-	✓	✓	-	-	-	-
RSA-1120W3	1	✓	-	✓	✓	-	✓	✓	-
RSA-1120W4	1	✓	-	✓	✓	-	✓	✓	✓
RSA-1220M	1	✓	✓	✓	✓	-	-	-	-
RSA-1220W3	1	✓	✓	✓	✓	-	✓	✓	-
RSA-1220W4	1	✓	✓	✓	✓	-	✓	✓	✓
RSA-4122	4	✓	-	✓	✓	2	-	-	-
RSA-4122W3	4	✓	-	✓	✓	2	✓	✓	-
RSA-4122W4	4	✓	-	✓	✓	2	✓	✓	✓
RSA-4222	4	✓	✓	✓	✓	2	-	-	-
RSA-4222W3	4	✓	✓	✓	✓	2	✓	✓	-
RSA-4222W4	4	✓	✓	✓	✓	2	✓	✓	✓

2 Login

Introduction

Configuration and management

The RSA series of routers can be configured, managed and monitored by means of:

- Web browser interface (HTTP or HTTPS).
- Command line interface (SSH, telnet or RS-232 port).
- Proprietary configuration (provisioning) system.
- TR-069 CWMP.
- SNMP (v1/2 and v3)

For details on the command line interface, provisioning, TR-069 CWMP and SNMP, contact MuLogic or your local sales representative.

Default settings

The unit is shipped with the following default settings:

- LAN IP address: **192.168.1.1**
- Admin password: **rsa-admin**

When in doubt on whether or not these settings are still active and when no LAN connection can be made with address 192.168.1.1, use the reset button to restore the factory default settings.

To restart the unit with its original factory default settings, power on the unit and wait 5 seconds. Then keep the reset button pressed for at least 10 seconds until the PWR LED blinks off. The factory default settings can also be restored using the Web-browser or command line interface.

First time Login

The web interface allows you to set up, modify, and view configuration variables and operational data.

Note: *To access the web interface in factory default settings, make sure that the PC's LAN port is operating on LAN network 192.168.1.0/24 (i.e. the PC should have an IP address between 192.168.1.2 and 192.168.1.254).*

- Connect to **http://192.168.1.1**
- Log in with user name **admin** and password **rsa-admin.**
- After you have successfully logged in, you should see the Device Info Summary page.

Inactivity timeout

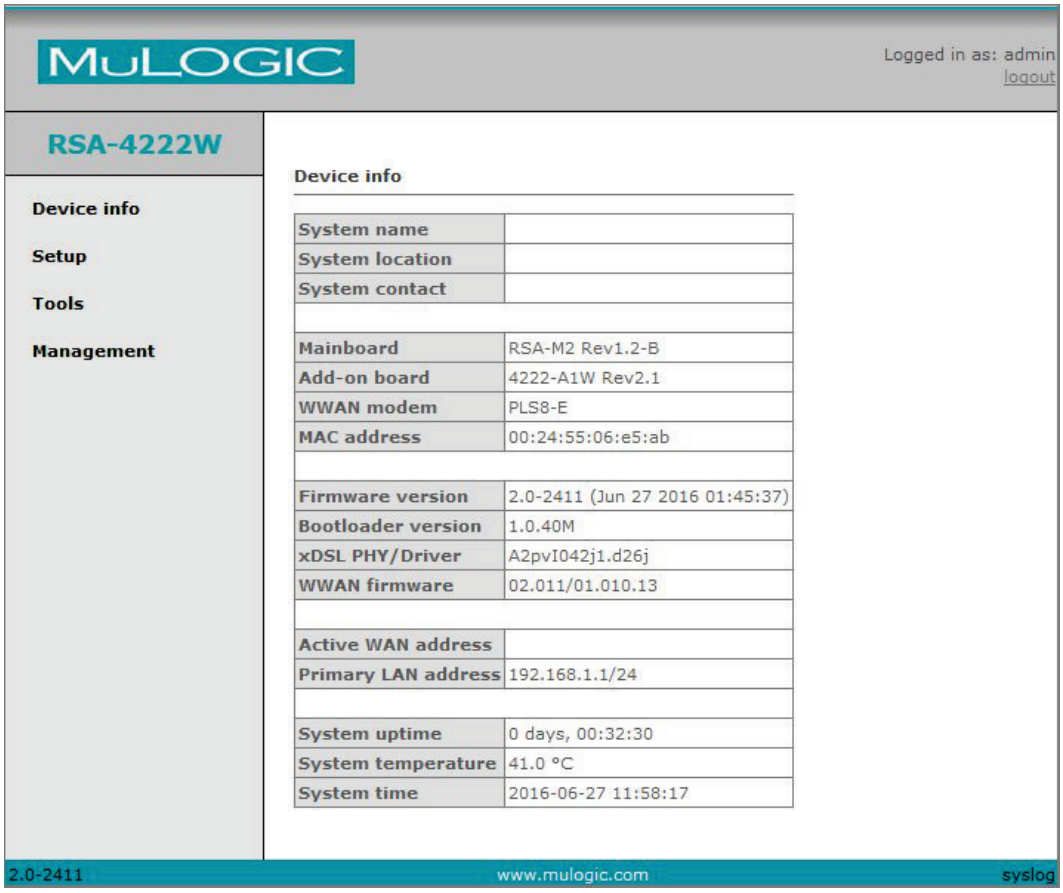
After a certain amount time of no activity via the web interface, you will be logged off automatically. The inactivity timeout can be set at **Management>Access control>Services**.

Logout

To log out of the web interface, click the logout link in the top right corner of the page.

Device Info page

The Info summary page will show the general information and status of the unit.



System name: System name as set at **Management>System ID**.
System location: Location as set at **Management>System ID**.
System contact: Contact name as set at **Management>System ID**.

Mainboard: Type, hardware revision and Annex A or B setting.
Add-on board: Type and hardware revision of add-on board.
WWAN modem: Type of WWAN modem (W-versions only)
MAC address: Base MAC address of the unit.

Firmware version: Firmware version and firmware build date.
Bootloader version: Boot loader software version.
xDSL PHY/Driver: Version of the xDSL PHY and driver currently used.
WWAN firmware: (if present) Firmware version of WWAN modem.

Active WAN address: Address of the currently active WAN interface.
Primary LAN address: Address of the primary LAN interface.

System uptime: Elapsed time since last start or restart.
System temperature: Current internal temperature of the system.
System time: Actual time as used by the system.

3 Setup

The Setup menu tree contains the items for the configuration of modem and router functions and the configuration and control of the physical ports.

Eth ports

The Eth ports setup menu is used for defining the function of the Ethernet ports. Ethernet ports can be used for either LAN side or WAN side connections. LAN side ports have features like DHCP servers to support connected LAN devices. WAN side ports have features like PPPoE, DHCP client and other features to allow automatic IP assignment from the ISP or Network Provider.

For LAN use 4 different LAN bridges are available. Each LAN-bridge has a dedicated DHCP server and can be configured with up to 2 IP addresses.
A LAN-bridge with assigned Ethernet ports behaves like a virtual Ethernet switch. All ports connected to the same LAN-bridge can communicate with each other and are part of the same LAN network.

LAN/WAN convention

Although there is no strict distinction between LAN and WAN operation, on the RSA-series there is a presumed difference in the role of LAN and WAN interfaces:

- LAN interfaces are meant for local (inside) access. Multiple Ethernet ports can be assigned to a virtual network switch called a "LAN-bridge". There are 4 LAN bridges in total and each LAN-bridge can operate its own DHCP server to assign IP addresses to attached devices.
- WAN interfaces are meant for connection to (outside) public operator services (xDSL, WWAN, fiber-optic) or private WANs. WAN interfaces use a dedicated physical port (for example an Ethernet or DSL port) and can have a DHCP client running in order to receive an IP address and other network information from the operator or DHCP server in the private WAN.

LAN connections

On units with more than one Ethernet port you can assign all Ethernet ports to a single LAN-bridge. All ports will then be connected together like on an Ethernet switch. Alternatively you can assign one or more Ethernet ports and VLANs to other LAN bridges at **Setup>Eth ports** .
To add VLAN ports, first configure one or more VLAN ports at **Setup>VLAN** and then assign the configured VLAN ports to one of the LAN bridges at **Setup>Eth ports**.
Ethernet interfaces and VLANs can also be configured as "not assigned". This can be used to exclude untagged Ethernet traffic on a specific port or to completely disable specific Ethernet ports or VLANs.

WAN connections

Individual Ethernet ports can also be designated as WAN port.
VLAN ID settings for WAN ports are made in the Setup>EthWAN menu.

LAN setup

Note: The LAN settings will become active immediately upon clicking "Apply/Save". When connected to the LAN port, make sure to connect your web browser to the new address.

Initially, all Ethernet ports are assigned to internal LAN-bridge "LAN1".
Multiple LANs or VLANs can be configured and created by means of the **Setup>Eth ports** and **Setup>VLAN** pages.
Only LAN bridges that are enabled in the Setup>Eth ports menu are shown as Setup>LAN sub menus.

Ethernet port physical setup

The physical parameters of the Ethernet ports, such as 10/100baseT and half/full duplex, are set at **Setup>Physical ports>Ethernet**.

LAN: LAN1-LAN4

Address: Enter the IP address/prefix length (CIDR notation).
/24 corresponds to a netmask of 255.255.255.0
Click "Apply/Save" to activate and store the setting.

Ifname: This is the name of the IP interface as used by the operating system. Internally this interface is a *bridge interface* to which multiple Ethernet ports, VLANs or xDSL bridge interfaces can be assigned. Ethernet ports and VLANs are assigned to LAN-bridges in the **Setup>Eth** ports menu.

Ports: This entry shows which Ethernet ports and VLANs are assigned to this IP interface.

Secondary IP address

A secondary IP address can be assigned to each LAN-bridge. Click "Enable" and enter the IP address/prefix length. Click "Apply/Save" to activate and store the setting.

DHCP server

Each LAN has a dedicated DHCP server. Click "Enable DHCP server" and enter the IP address range, lease time and (optional) domain name. Click "Apply/Save" to activate and store the setting.

Check for DHCP server conflict

When enabled, the system will check the presence of another DHCP server in the network to avoid network problems caused by DHCP server conflicts. When another DHCP server is found, the internal DHCP server will be disabled.

Static DHCP Leases

Apart from automatically assigned DHCP leases, also static DHCP leased can be set. Click "Add Lease" and enter the IP address and the MAC address of the device. Click "Apply/Save" to activate and store the setting.

VLAN setup

Multiple VLANs can be created. Each VLAN is assigned to a physical Ethernet port and has a VLAN-ID. On units with one Ethernet port, only port Eth0 is available but multiple VLANs can be created on Eth0. To configure or add a VLAN entry, click the “Add VLAN” button.

Name

Optionally a name can be given to each VLAN entry. VLAN names can be used for reference but are not relevant for the configuration.

Iface

The Iface (interface) entry is created automatically. This is the name of the interface as used by the system.

VLAN ID

Enter the VLAN ID. The value must in the in the range of 0 to 4095.

Port

Select the physical Ethernet port to assign the VLAN to. On units with one Ethernet port only port Eth0 is available.

DSL interface setup

The routers that are suited for xDSL (ADSL2+ or VDSL2) have one physical DSL port that can carry up to 8 Layer3 or Layer 2 virtual DSL interfaces. Multiple virtual interfaces must all be of the same type: either ADSL or VDSL2.

In general, ADSL (ADSL, ADSL2 and ADSL2+) connections use ATM as an intermediate layer on top of the DSL layer. The ATM channel is indicated by means of a VPI/VCI combination.
VDSL2 connections mainly use PTM as intermediate layer. The PTM channel is indicated by means of a VLAN ID.

Each DSL interface is given a unique ATM connection known as a Permanent Virtual Circuit or PVC. A PVC is indicated by a Virtual Path Identifier (VPI) and a Virtual Channel identifier (VCI).
The PVC (VPI/VCI) to use is determined by the operator that offers the DSL service.

DSL Physical setup

The setup of the parameters of the physical DSL (modem) connection such as ADSL mode and POTS/ISDN overlay is done at **Setup>Physical ports>DSL**.

*Note: Make sure that the correct PHY version (Annex A or B) is selected. See the **Device info>summary** page to check which xDSL PHY is in use.*

DSL interface

Click the “Add DSL interface” to add a new DSL interface entry.

Name

Optionally a name can be given to each DSL interface entry. DSL names can be used for reference but are not relevant for the configuration. The default name is “DSL interface”.

Enable

Click the checkbox to enable the DSL interface. An already configured DSL interface can be disabled in this way without losing the configuration.

Status

This field is generated automatically and shows the actual status and the assigned IP address of the DSL link.

Mode

Select ATM for ADSL connections and PTM for VDSL2 connections.

VPI (ADSL/ATM mode)

Enter the ATM Virtual Path Identifier as indicated by the DSL provider or ISP.

VCI (ADSL/ATM mode)

Enter the ATM Virtual Channel Identifier as indicated by the DSL provider or ISP.

VLAN

Enable VLAN and enter the VLAN ID in case a VLAN ID is indicated by the DSL provider or ISP. (Usually for PPPoE over VLAN).

Link type

Multiple link types can be selected. The appropriate link type will be indicated by the DSL provider or ISP.

Encapsulation method (ADSL/ATM mode)

The appropriate encapsulation method will be set automatically after selecting the link type. Manual selection should not be necessary.

PPP authentication (PPPoE and PPPoA link types)

For PPPoE and PPPoA link types the authentication method can be selected. In general this entry can be left at “Auto”.

PPP username (PPPoE and PPPoA link types)

If required, enter the username as issued by the ISP.
When no username/password is required then the default user name and password can remain untouched.

PPP password (PPPoE and PPPoA link types)

If required, enter the password as issued by the ISP.
When no username/password is required then the default user name and password can remain untouched.

PPPoE service name (PPPoE link type)

The use of a PPPoE service name allows the use of multiple PPPoE connections over the same link. If not provided by the ISP, this field can remain empty.

IP assignment (PPPoE, PPPoA and IPoE link types)

In general, when the ISP provides an IPoE link type, the setting will be “DHCP” which will allow automatic IP address, gateway, and DNS assignment by the ISP. Optionally a static IP address with gateway and DNS can be entered.

Custom MAC address (IPoE link type with DHCP)

When enabled, the entered MAC address will be used for the EthWAN interface. This can be useful when an Internet connection or WAN IP address is associated with a particular MAC address.

IP address (PPPoE, PPPoA, IPoA and static IPoE)

Enter the WAN IP address. This will only have effect when the ISP does not automatically issue an IP address.

Gateway (IPoA and static IPoE)

Enter the gateway address. This will only have effect when the ISP does not automatically issue an IP address.

Primary/secondary name server

Enter the DNS addresses here. This will only have effect when the ISP does not automatically issue an IP address.

LAN bridge (Bridge and PPPoA-to-PPPoE link types)

If encapsulation method “Bridge” is selected, this field connects the DSL interface in layer2 mode with one of the 4 LAN bridges. DSL bridge mode allows for direct layer 2 connection between the Ethernet ports (or VLAN) and the DSL port. It can be used for end to end layer2 communication or for PPPoE or IPoE operation with an external router. In this mode, the external router will be assigned with the WAN IP address.

Service category

This field selects the ATM service category. For regular applications this setting can remain unchanged at UBR.

PPP debugging

This option can be used to send more detailed information to the system log during PPPoE or PPPoA connection establishment. It serves a way to troubleshoot PPPoE or PPPoA connection failures.

PPPoA to PPPoE

The PPPoA to PPPoE link type is a special mode for connecting external routers in a similar way as in “Bridge” link type mode when the ISP offers a PPPoA connection. PPPoA cannot be transported over Ethernet as PPPoE can. In order to facilitate external PPPoE routers, the PPPoA frames are converted in PPPoE frames and the authentication is handled in the same way as for a PPPoE connection over a “Bridge” link.

DSL Physical setup

The setup of the parameters of the physical DSL (modem) connection such as ADSL mode and POTS/ISDN overlay is done at **Setup>Physical ports>DSL**.

Wireless WAN interface setup

Those units that support wireless WAN operation (WWAN) are equipped with an internal Wireless WAN modem that uses the mobile cellular network for WAN connection. The units that are equipped with USB ports can be used with external cellular modems connected to one of these USB ports.

WWAN Physical setup

The setup of the parameters of the physical connection parameters of the internal WWAN modem, such as wireless network type (2G/3G/4G) and frequency band selection is made at **Setup>Physical ports>WWAN**.
This may only apply to units with an internal WWAN modem (the W-versions).

Wireless WAN interface

Name

Optionally a name can be given to the WWAN interface entry. WWAN names can be used for reference but are not relevant for the configuration.
The default name is “WWAN interface”.

Enable

Click the checkbox to enable the WWAN interface. An already configured interface can be disabled in this way without losing the configuration.

Dial on demand

When dial on demand is enabled, the WWAN connection will only be activated when the WWAN port is the only or the highest priority WAN interface (see **Setup>WAN Failover**). This will avoid unwanted costs for mobile data usage. Note that In dial on demand mode it may take more time before the WWAN connection becomes active.

PPP debugging

This option can be used to send more detailed information to the system log during PPP connection establishment. It serves a way to troubleshoot PPP connection failures.

MTU

If needed, the MTU of the WWAN PPP interface can be set to a lower value. The default value is 1400.

Status

This field is generated automatically and shows the actual status of the WWAN link and the assigned IP address when the status is “Connected”.

SIM status

This field is automatically generated and shows the status of the SIM card. When “OK”, the SIM card is detected and the PIN code is correct.

PIN

Enter the correct PIN of the SIM card. If the PIN is incorrect, a warning will appear at the SIM status.

Note: *Make sure to enter a correct SIM PIN. When a wrong PIN is detected, no further action is taken is taken until the next restart of the .*
After 3 restarts with the wrong PIN, the PUK code must be entered in order to unlock the SIM card.

Access point name

Enter the Access Point Name (APN) as provided by the mobile network operator.

Note: *Make sure to enter the correct APN. Using an invalid APN may result in high costs for data usage.*

PPP authentication

The type of authentication (PAP, CHAP, automatic PAP/CHAP or None) can be selected. In most cases this selection can remain at “Auto”.

PPP username

Enter the user name for authentication here. If the network operator does not require a specific user name, you can leave the entry at “default”.

PPP password

Enter the password for authentication here. If the network operator does not require a specific password, you can leave the password entry as it is.

Entering PUK code

When the SIM card is blocked after 3 consecutive activations with wrong a PIN code, a field will appear where you can enter the PUK code to unblock the card.

WWAN Physical setup

The setup of the parameters of the physical connection parameters of the internal WWAN modem such as wireless network type (2G/3G/4G) and frequency band selection is made at **Setup>Physical ports>WWAN**.
This only applies to units with an internal WWAN modem (the W-versions).

Ethernet WAN interface setup

The RSA routers can have one or more Ethernet ports assigned as WAN port. WAN ports can be connected to a private WAN network, another DSL modem operating in “Bridge” mode or a fiber optic internet connection. Both untagged and tagged (VLAN) Ethernet frames are supported.

Ethernet port physical setup

The setup of the parameters of the physical Ethernet ports such as 10/100baseT, half/full duplex and hub/switch mode is made at **Setup>Physical ports>Ethernet**.

Ethernet WAN functional setup.

Make sure that one or more Ethernet ports are assigned as EthWAN in the **Setup>Eth ports** menu. Click “Add Eth WAN interface” to add a new entry and select the Ethernet port. Even on routers with one Ethernet port, this single Ethernet port can be used as WAN port. This will serve applications where only the serial interface is used as local interface and no local Ethernet LAN connection is needed.

Name

Optionally a name can be given to the interface entry. Eth WAN names can be used for reference but are not relevant for the configuration. The default name is “Eth interface”.

Enable

Click the checkbox to enable the Ethernet WAN interface. An already configured interface can be disabled in this way without losing the configuration.

Status

This field is generated automatically and shows the actual status and assigned IP address of the WAN link.

Link type

Select IP for DHCP assigned or static IP address. Select PPPoE If the WAN connection is made over a PPPoE link.

VLAN

Select this option when the ISP or network operator specifies a VLAN ID for data (internet) operation.

VLAN ID

When the option VLAN is enabled enter the VLAN ID as specified by the ISP or network operator.

IP assignment

This option selects automatic IP address assignment (DHCP) or manual (static) configuration of the IP address, gateway and name servers. In most cases the ISP will assign the IP address by means of DHCP in which case static configuration may not be allowed or possible.

IP address (IP assignment: static)

If the option “static” in IP assignment is selected, enter the unit’s WAN IP address here.

Gateway (IP assignment: static)

If the option “static” in IP mode is selected, enter the gateway address here.

Primary/Secondary name server (IP assignment: static)

If the option “static” in IP mode is selected, enter the IP address of the primary and secondary name (DNS) servers here.

PPP authentication

If PPPoE is selected, the type of authentication (PAP, CHAP, automatic PAP/CHAP or None) can be selected. In most cases this selection can remain at “Auto”.

PPP username

If PPPoE is selected, enter the user name for authentication here. If the ISP does not require a specific user name, you can leave the entry at “default”.

PPP password

If PPPoE is selected, enter the password for authentication here. If the ISP does not require a specific password you can leave the password entry as it is.

PPPoE service name

If PPPoE encapsulation is selected, enter the PPPoE service name if provided by the ISP. In most cases this field can be left blank.

PPP debugging

When this option is selected, additional information of the PPPoE handshake and PPP connection status is written in the System log.

Custom MAC address

When enabled, the entered MAC address will be used for the EthWAN interface. This can be useful when an Internet connection or WAN IP address is associated with a particular MAC address.

WAN failover setup

The WAN failover page manages the failover operation between WAN interfaces when multiple WAN interfaces are configured.
Each configured WAN interface is given a priority number where '1' stands for the highest priority.
Connection is continuously checked by sending ICMP ping requests to the entered Ping Addresses. The interval and number of retries determine how frequently the WAN connection is checked and how many retries are attempted. When the number of Retries is reached, the active WAN connection will failover to the interface with the next lower priority

Each WAN interface is listed. The priority is set in order of configuration of a WAN interface but can be changed manually. The default IP addresses are 8.8.8.8 and 8.8.4.4. The default ping interval is 5 seconds and the default amount of failed retries before selecting a lower priority WAN interface is 2. These parameters can be edited by clicking the “Edit” button of the specific entry.

Enable

Use the checkmark to include/exclude a WAN interface in the failover list.

Note: *Take care to not accidentally disable the active WAN interface while being connected from a remote location via this interface.*

Prio

Set the priority of the WAN interface. The lowest number has the highest priority.

Edit

Click “Edit” to edit parameters such as ping interval, retries and the ping addresses.

Type

This field is generated automatically and shows the type of WAN interface.

Name

This field is generated automatically and shows the name given to the WAN interface.

Linkname

This field is generated automatically and shows the name of WAN interface as used by the failover mechanism.

Interval

The value here (in seconds) determines how often the two “ping addresses” are checked.

Retries

After a timeout on both “ping addresses”, this value determines how often a retry is done before the link is declared unavailable and failover to the next priority WAN interface is initiated.

Note: *Make sure that the IP addresses to be pinged can be reached over the WAN port. If the entered address cannot be reached, the WAN connection will not be established.*

Connect on demand (WWAN port only)

When the ‘Dial on demand’ option is enabled in the WWAN setup menu, a WWAN data connection will only be made when the WWAN port becomes the active (highest available priority) WAN interface. This will avoid unwanted costs for mobile data usage. Note that in this mode it may take more time before the WWAN connection becomes active.

Firewall setup

The firewall options are used for enabling or disabling access to the unit from individual IP addresses or groups of IP addresses. In addition the rate of certain types of incoming packets can be limited in order to protect against DoS or DDoS attacks.

Custom firewall rules

Although many firewall and NAT features are supported by the system, it may be necessary to add custom firewall (iptables) rules in special situations. Such rules can be added by means of running a script that is executed by the system upon start-up and after changes invoked by the system. This feature requires knowledge of writing scripts and iptables rules. Contact MuLogic or your local sales representative for details.

IP Filtering

Enable IP filtering

When unchecked, all incoming filtering rules are disabled. This can be used for testing purposes but should not be used for regular operation. When IP filtering is disabled the shortcuts below do not apply. The shortcuts will become active after clicking ‘Apply/Save’ at the bottom of the page.

Shortcuts

In order to allow for rapid testing without setting firewall rules first, some “shortcuts” can be made.

Warning: *for reasons of security it is advised to* ***not*** *use these shortcuts in the final setup and create individual filter rules for all types of access instead.*

The following shortcuts, when enabled, override the filtering 'Accept' rules but not the ‘Drop’ rules.

Bypass filter for traffic via VPNs

When checked, all access via IPsec or OpenVPN tunnels is allowed, except for those addresses for which ‘drop’ rules are made.

Bypass filter for LAN-side traffic

When enabled, all access via LAN interfaces is allowed, except for those addresses for which ‘drop’ rules are made.

Bypass filter for HTTP/HTTPS access

When enabled, access to the unit’s web server ports 80 and 443 is allowed from any address in either LAN or WAN, except for those addresses for which ‘drop’ rules are made.

Allow ICMP ping from any address

When enabled, the unit accepts and replies to ICMP ping requests coming from any address, except for those addresses for which ‘drop’ rules are made.

Allow routing between LANs

When enabled, IP traffic is routed between different LAN bridges. Keep this option disabled if you want isolation between different LAN-bridges, for example when Individual LAN bridges (Ethernet ports or VLANs) are used for individual VPN tunnels and access from one tunnel/network to the other is not allowed.

Filter rules

Filter rules can be made to either accept or to deny (drop) incoming packets. The drop rules have priority over the shortcuts but will not be active when IP filtering is disabled. Click “Add Rule” to add an incoming filtering rule.

Name

Optionally a name can be given to each filter rule. Rule names can be used for reference but are not relevant for the configuration.

Enable

Click the checkbox to enable the filtering rule. An already configured rule can be disabled in this way without losing the configuration.

Action

When “Accept” is selected, incoming traffic that matches the parameters below is allowed for access.
When “Drop” is selected, incoming traffic that matches the parameters below is denied access. This can be used for blocking access from specific IP addresses.

Protocol

Select the IP protocol type for this rule: TCP, UDP, ICMP, IGMP, OSPF or GRE, or ANY for any protocol.

Src addr

Enter a specific address or network as IP address/prefix size to filter incoming traffic.

Src port

This entry can usually be left at “0” unless you want to allow or deny access from specific port numbers.
Enter a specific source port number to filter incoming traffic or use “0” to allow all incoming source ports.

Dst addr

The destination address can usually be left at 0.0.0.0/0 which will allow access via all configured WAN interfaces. When multiple WAN interfaces are used, this option allows control of access to a specific WAN interface address.

Dst port

Enter the destination port of the system service you want to have accessed. The default port numbers for system services are:

SSH:	22
Telnet:	23
HTTP:	80
HTTPs:	443
Serial server 1:	6363
Serial server 2:	6364
IPsec (IKE):	500
IPsec (IKE and ESP):	4500
OpenVPN:	1194

Example

A typical rule for limiting access to one of the system services looks like:

Name: Telnet access host 1
Enable: ✓
Action: Accept
Protocol: TCP
Src addr: 212.124.53.16/32
Src port: 0
Dst addr: 0.0.0.0/0
Dst port: 23

This allows telnet access from the host with address 212.124.53.16 only.

Rate limiting

Rate limiting is used to control the rate of traffic received via the WAN ports and serves as protection against DoS and DDoS attacks.

Rate limiting speed

This is a global setting for all rate limiting options. The value sets the maximum rate in packets/sec. The default value is 5 packets per second.

TCP SYN rate limiting

Limit the rate of incoming TCP SYN packets to the rate as set at “Rate limiting speed”.

UDP rate limiting

Limit the rate of incoming packets for UDP ports 161 (SNMP) and 500 (IPsec) to the rate as set at “Rate limiting speed”.

ICMP rate limiting

Limit the rate of incoming ICMP packets to the rate as set at “Rate limiting speed”.

NAT Setup

NAT (network address translation) is a feature of the firewall which allows for translation or remapping of network addresses into other addresses based on specific addresses, ports or protocols.

Static NAT

A form of a static NAT method, known as Port Forwarding, is used for redirecting incoming IP traffic from the WAN side (identified by protocol, address and port) to a destination address and destination port of a device on the LAN side.
In order to communicate via the WAN port, the devices to which the port forwards are made must set the local LAN address of this router as default gateway address. In case the gateway address cannot be changed the 'Rewrite source address' feature can be used. See below.

Click the Add Forward button to add a new Static NAT entry.
To remove entries select these entries by clicking one or more Remove boxes and then click the Remove button.

Name

Each static NAT entry can optionally be given a name. The name can be used for reference but is not relevant for the configuration.

Protocol

Select the protocol of the packets to forward: TCP, UDP or TCP and UDP.

Source address (for access)

Enter the address of the remote device or network to be given access.
For example 123.45.67.98/32 only applies to the host with address 123.45.67.98 while 123.45.67.0/24 enables access from all 256 hosts on the 123.45.67.0 network. A Source address of 0.0.0.0/0 allows access from all addresses.

External Port

Enter the port to contact for the remote device. This must be a port that is not used by any of the internal system services. For example, to use port 80 while the internal (http) webserver is enabled, move the port of the internal webserver to another number.

Destination Address

Enter the address of the LAN side host to connect to. The address of this host must be within the LAN network range that it is connected to. The router's LAN address must be used as gateway address on the host to connect to, unless the 'Rewrite source address' feature is used.

Destination Port

Enter the port number of the service of the LAN side host to connect to.

Rewrite source address

This feature enables hosts or devices that are connected to a LAN port to be reachable by means of port forwarding without the need for setting their default gateway address to the LAN address of the router.
The source address of the incoming traffic is rewritten into the local address of the router so that the incoming connection appears to be coming from the router rather than the remote host. This applies only to hosts or devices that have a layer 2 connection (like a physical Ethernet connection) to the router's LAN port.

Source address (rewrite)

When 'Rewrite source address' is enabled, enter the actual local LAN address of the router here.

Example

Static NAT rule for giving external host 123.45.67.89 access to port 80 of a web server connected to an internal LAN network by connecting to port 8080 of the router's WAN address. The router's LAN address in this example is 192.168.1.1

Name: https access Host 1
Protocol: TCP
Source address: 123.45.67.89/32
External port: 8080
Destination address: 192.168.1.24
Destination port: 80

Make sure that the host connected to the internal LAN is using this unit's LAN address as gateway address, unless the 'Rewrite source address' feature is used:

Rewrite source address: Enabled
Source address: 192.168.1.1

Note: *When assigning external port numbers that equal to those that are used for the RSA unit's device management, the ports of the device management will have to be relocated to other port numbers. The default port numbers are: SSH: 22, Telnet: 23, HTTP: 80, HTTP: 443, SNMP: 161*

Dynamic NAT

Dynamic NAT (IP masquerading or Port Address Translation) allows hosts that are connected to the LAN ports to all have internet access using this unit's WAN address as public address. The Dynamic NAT mechanism keeps track of the outgoing packets and modifies the incoming responses with the LAN address of the internal device.

Dynamic NAT can be disabled for preventing devices that are connected to a LAN port from having direct internet access.

Enable

Each configured LAN is shown in a table. Select the Enable box and click Apply/Save to enable/disable Dynamic NAT for the selected LAN.

Routing Setup

Default Gateway

Current Gateway

"Current gateway" shows the address of the currently active or configured gateway.

Mode

When the Mode is set to 'Automatic', the default route is automatically assigned to the gateway of the active WAN interface. When 'Manual' is selected, the entered Default Gateway address is used regardless if the chosen connection is active or not

Static route

Click "Add Route" for adding entries to the routing table. Stored routes can be enabled/disabled by means of the "Enable" checkmarks.

Description

Each routing entry can optionally be given a description which can be used for reference but is not relevant for the configuration.

Destination

Enter the destination address or network of the static route.

Gateway

Enter the address of the gateway via which to reach the destination network.

Rip Global

Enable

Click "Enable" to start the RIP service.

Version

Select RIP v1 or RIP v2.

Status

This field is generated automatically and shows the status and error messages of the RIP service.

Redistribution

Redistribution is used for advertising routes that are learned by another routing protocol, static routes etc.

Kernel: redistribute routing info from kernel route entries into the RIP tables.
OSPF: redistribute routing info from OSPF route entries into the RIP tables.

RIP Keys

RIP keys are used for authentication between RIP routers.
Click “Add Key” to add a Key and a Key ID.

RIP interfaces

Click “Add interface” to select an interface from the list.

Name

Select an interface from the list. An entry must be made for:
1. interfaces that are used for sending the route advertisements to a neighbour RIP router (active)
2. interfaces of which the routes are to be advertised.

Enable

Click the checkbox and “Apply/Save” to enable advertisement of the interface.

Mode

Select “Active” for interfaces that are used for advertising routes, such as the WAN interface of tunnel towards the other RIP router. Select “Passive” for interfaces that only need to be included in the RIP advertisements.

Split horizon

The Split horizon mechanism is used for preventing routing loops in a network. Click the checkbox and “Apply/Save” to disable this feature.

Authentication

Click the “Authentication” checkbox to enable RIP authentication and select the authentication method.

OSPF Global

Enable

Click “Enable” to start the OSPF service.

Status

This field is generated automatically and shows the status and error messages of the OSPF service.

Specify router ID

Click the checkbox and enter the Router ID to uniquely identify the OSPF router. The ID should be formatted like an IP address and must be unique within the entire OSPF domain. If no ID is specified then the system will generate an ID automatically.

Redistribution

Redistribution is used for advertising routes that are learned by another routing protocol, static routes etc.

Kernel: redistribute routing info from kernel route entries into the RIP tables.

RIP: redistribute routing info from RIP route entries into the OSPF tables.

OSPF Keys

OSPF keys are used for authentication between OSPF routers.
Click “Add Key” to add a Key and a Key ID.

OSPF interfaces

Click “Add interface” to select an interface from the list.

Name

Select an interface from the list. An entry must be made for:
1. interfaces that are used for sending the route advertisements to a neighbour RIP router (active)
2. interfaces of which the routes are to be advertised.

Enable

Click the checkbox and “Apply/Save” to enable advertisement of the interface.

Mode

Select “Active” for interfaces that are used for advertising routes, such as the WAN interface of tunnel towards the other router. Select “Passive” for interfaces that only need to be included in the OSPF advertisements.

Area

Enter the OSPF area number here. The default is 0 (0.0.0.0)

Link cost

Enter the OSPF link cost here. The default is 10

Hello interval

Enter the hello interval here. The default is 10 seconds

Dead interval

Enter the OSPF dead interval here. This value must be the same for all routers attached to a common network. The default value is 40 seconds.

Authentication

Click the “Authentication” checkbox to enable RIP authentication and select the authentication method.

BGP Global

Enable

Click “Enable” to enable the BGP service.

Status

This field is generated automatically and shows the status and error messages of the BGP service.

Router ID

Enter the Router ID to uniquely identify the BGP router. The ID should be formatted like an IP address and must be unique within the entire BGP domain. If no ID is specified then the system will generate an ID automatically.

Local-AS

Set the local-AS.

Keep-alive timer

Set the keep-alive time. The default value is 60 seconds.

Hold timer

Set the hold time. The default value is 180 seconds.

Networks

Click “Add Network” to add a network to be advertised via BGP.

Description

Enter a description of the advertised network. This description can be used for reference but is not relevant for the configuration.

Address

Enter the address of the advertised network.

Neighbors

Click “Add Neighbor” to add a neighbour network for BPG.

Description

Enter a description of the neighbour network. This description can be used for reference but is not relevant for the configuration.

IP address

Enter the IP address of the neighbour.

Authentication

To use authentication, click checkmark and en the Password.

Soft reconfiguration inbound

Click the checkmark to enable the *Soft reconfiguration inbound* feature.

Next hop self

Click the checkmark to enable the *next-hop-self* feature.

Local preference

When needed, click the checkmark and enter the Local-preference direction.

Prepend

Click the checkmark and set the Prepend direction. Click the *prepend last-as* checkmark when needed.

DNS Setup

DNS Server

Mode

When the Mode is set to Automatic, the DNS servers of the active WAN connection are used. In most cases (except for when the WAN addresses are configured manually) the addresses of these DNS servers are automatically assigned during connection with the ISP or network operator.

When Manual is selected, the entered DNS server addresses are configured regardless if the chosen connection is active or not.

VPN Tunnels

The RSA-units support 3 types of VPN tunnels: IPsec, OpenVPN and GRE.

IPsec can be used between two RSA-units and between an RSA-unit and central site security appliances. It is the de-facto standard for encrypted VPN tunnels and is supported by many devices. For IPsec, both key exchange protocols -IKEv1 and IKEv2- are supported.

OpenVPN can be used between two RSA-units and between an RSA-unit and a host computer (very often a Linux-based system) supporting OpenVPN. OpenVPN is a full-featured SSL VPN implementation but is not often seen on the regular central site security appliances that usually run a proprietary form of SSL VPN. OpenVPN offers the feature to also transport Layer2 data like Ethernet frames and can be used in a network with Layer2 (Ethernet) switches. OpenVPN can also run over IPsec tunnels to transport Layer2 (Ethernet) data transparently.

GRE tunnels are not encrypted and are very often used in combination with IPsec tunnels for security. GRE tunnels are especially useful for transporting multicast packets like OSPF, RIP, and EIGRP. Also streaming audio and video applications and VoIP may use multicast.

IPsec

Click Add profile to add a new IPsec tunnel connection profile.
In the profile overview page, tunnels can be enabled or disabled.
Click the “Clone” button to make a copy of an existing profile. This can be used for making similar profiles in an easy way.

Name

Optionally a name can be given to each tunnel profile. Tunnel names can be used for reference but are not relevant for the configuration.

Tunnel ID

This field is generated automatically and shows the ID of the tunnel profile as used by the system.

Status

This field is generated automatically and shows the actual status of the IPsec tunnel.

Enable

Click the checkbox to enable the VPN tunnel. An already configured tunnel profile can be disabled in this way without losing the configuration.

IPsec debugging

When enabled, while setting up the tunnel connection, extra information is written into the system log.

Phase1 /IKE-SA setup

Connection mode

Three connection modes can be selected: Active, Passive or Anonymous.
In Active mode, this unit will actively try to connect to the Remote peer address.

In passive mode, this unit will wait for incoming connections from the unit with the Remote peer address. Note that firewall input filter rules (UDP ports 500 and 4500) must be configured in order to accept the incoming connections.

In Anonymous mode, this unit will accept incoming connections (with matching Phase 1 and Phase 2 parameters) from any address. Note that a firewall input filter rules must be configured in order to accept the incoming connections.

Remote peer address (Active and Passive connection mode)

Enter the address to connect to or to accept incoming tunnel connections from.

Key exchange method

Three key exchange methods can be selected: IKEv1, IKEv2 and manual.
IKEv1 is widely used as key exchange method but is gradually being replaced with IKEv2.
IKEv2 has several advantages over IKEv1 such as less bandwidth consuming, less interoperability issues and offers multiple sets of networks in a single exchange.
When Manual key exchange is selected, the encryption keys must be entered manually and keys are not automatically re-negotiated. This feature is usually only necessary to connect to a device which does not support IKE and the method should be considered deprecated.

Authentication method

IKE knows two authentication methods: Pre Shared Key (PSK) and the use of Certificates according to the ITU-T X.509 standard.

When PSK is selected, the entered PSK is the keyword from which the session keys used by the IPsec process are generated. The keyword can be any (secret) name and does not have to be a complex keyword to ensure secure operation; however, to prevent “brute force entry”, the normal rules for password strength apply. The keyword must be equal at both local and remote IPsec router. Optionally, local and/or remote identifiers can be used.

When Certificate is selected one of the configured certificates can be selected. Optionally, a remote identifier or remote certificate can be used.

PSK (Authentication method PSK)

Enter the pre shared key.

Local Identifier

When required by the remote peer, select “Specify identifier” and enter the local identifier.

Remote Identifier (Authentication method PSK)

When a specific remote identifier is required, select “Specify identifier” and enter the remote identifier.

Local x.509 certificate (Authentication method Certificate)

Certificates are configured in the **Management>Certs and keys** menu.
The local certificate is used by the remote peer to verify this unit’s identity against the list of CA certificates at the remote peer.
This unit, in turn, verifies the local certificate of the remote peer by checking if this certificate was signed by one of the CA certificates stored on this unit.

Remote identifier (Authentication method Certificate)

Apart from matching the certificate of the remote peer with one of the stored CA certificates, an additional remote identifier or certificate can be required for granting access.
When a specific remote identifier is required, select “Specify identifier” and enter the remote id, or select “Remote certificate” and select one of the configured remote certificates.

Remote cert (Authentication method Certificate)

Select one of the certificates stored at **Management>Certs and keys>Remote certs.**

Exchange mode (IKEv1 Only)

The default exchange mode for IKEv1 is the “Main mode”. The use of the “Aggressive mode” is deprecated and should only be used when the remote peer does not support IKEv1 Main mode or when there are compatibility issues.

Phase1 Key Life Time

Enter the life time of the IKE Phase 1 (authentication) security association.
The default life time is 10800 seconds (3 hours). 540 seconds before expiry of the life time, a new key exchange is negotiated. The key life time does not have to be equal on both peers. Usually the shortest key time of the two peers is selected automatically.

Phase1 Encryption Algorithm

Select one of the Phase 1 Encryption Algorithms. The following encryption algorithms are available: 3DES, AES128, AES192 and AES256.
The encryption algorithm must be equal on both peers.

Phase 1 Integrity Algorithm

Select one of the Phase 1 integrity algorithms. The following integrity algorithms are available: MD5, SHA1, AES-XCBC, AES256, AES384, AES512 and AES 256-96. The integrity algorithm must be equal on both peers.

Phase1 Diffie-Hellman Group

Select one of the Phase 1 Diffie-Hellman Group. The following DH groups are available: DH Groups 1, 2, 5, 14, 15, 16, NIST ECG Groups 25, 26, 19, 20, 21, Brainpool ECG Groups 27, 28, 29 and 30.
Note that DH groups 15 and 16 are quite compute-intensive and can slow down the establishment of IPsec tunnels considerably. For rapid connection with higher security, the NIST or Brainpool Elliptic Curve Groups are preferred.
The DH group must be equal on both peers.

NAT-traversal (NAT-T)

As IPsec (ESP) data packets are fully encrypted techniques like Dynamic NAT cannot be used because there are no readable ports to refer to. To overcome this problem, the ESP packets are encapsulated in UDP packets with port number 4500. The need for NAT-T can be automatically detected between peers but in some occasions (like the use of Mobile WWAN networks) it may be necessary to force NAT-T mode. When in NAT-T mode, keep alive messages are sent at regular intervals in order to prevent the state information of the NAT router from expiring.

NAT KeepAlive interval

The value of the NAT keep alive interval determines how often NAT keep alive packets are sent. The default value is 10 seconds. For use on mobile networks the interval can be increased in order to reduce network traffic costs.

Dead Peer Detection

Dead Peer Detection (DPD) is needed to detect if connection with a remote peer is lost. Normally in IKEv1 mode, no packets are exchanged when no data passes the tunnel. To detect if connection with the remote peer is still available, messages are sent between peers.

DPD interval

The value of the DPD interval determines how often the messages for dead peer detection are sent. The default value is 10 seconds. The value can be increased to reduce network traffic when rapid discovery of disconnected peers is not required.

DPD timeout (IKEv1 only)

The DPD timeout value defines the time after which the connection to the remote peer is deleted in case of no reply to DPD messages.

MOBIKE (IKEv2 only)

When enabled, the MOBIKE (IKEv2 Mobility and Multihoming Protocol) can be negotiated with the peer. The use of MOBIKE offers a greater flexibility for connections with changing IP addresses due to change of WAN interface or ISP-forced IP address changes.

Phase 2 / Child-SA Setup

Local Network

Enter the address or network for the device(s) at the local end of the tunnel. This can be a single address like 192.168.10.22/32 or a network like 192.168.10.0/24. In IKEv2 mode, multiple addresses/networks can be entered. Multiple addresses are entered as comma separated.

Remote Network

Enter the address or network for the device(s) at the remote end of the tunnel. This can be a single address like 192.168.10.22/32 or a network like 192.168.10.0/24. In IKEv2 mode, multiple addresses/networks can be entered. Multiple addresses are entered as comma separated.

Create local loopback address

When enabled, a local loopback interface with the address as entered at “Local Network” will be created. This feature is used for tunnel end-points that reside on the unit itself like for device management, the use of the Serial Gateways, GRE tunnels and other local services that need to be accessed via an IPsec tunnel.

Phase2 Key Life Time

Enter the life time of the IKE Phase 2 (IPsec) security association.
The default life time is 3600 seconds (1 hour). 540 seconds before expiry of the life time, a new key exchange is negotiated. The key life time does not have to be equal on both peers.

Phase2 Encryption Algorithm

Select one of the Phase 2 Encryption Algorithms. The following encryption algorithms are available: 3DES, AES128, AES192 and AES256.
The encryption algorithm must be equal on both peers.

Phase2 Integrity Algorithm

Select one of the Phase 1 integrity algorithms. The following integrity algorithms are available: MD5, SHA1, AES-XCBC, AES256, AES384, AES512 and AES 256-96. The integrity algorithm must be equal on both peers.

Perfect Forward Secrecy (PFS)

This option defines whether or not the Perfect Forward Secrecy (PFS) option is used.

Phase2 Diffie-Hellman Group (PFS enabled)

When PFS is enabled, select one of the Phase 2 Diffie-Hellman groups
Note that DH groups 15 and 16 are quite compute-intensive and can slow down the establishment or rekeying of IPsec tunnels considerably. For rapid connection with higher security, the NIST or Brainpool Elliptic Curve Groups are preferred. The DH group must be equal on both peers.

Priority

The priority option can be used for IPsec failover operation by means of two active tunnel profiles. The remote peers must be individual IPsec devices. The lowest number stands for the highest priority. Leave at 0 if not used.

OpenVPN

Click “Add profile” to add a new OpenVPN tunnel connection profile.
In the profile overview page tunnels can be enabled or disabled.

Name

Optionally a name can be given to each tunnel profile. Tunnel names can be used for reference but are not relevant for the configuration.

Status

This field is generated automatically and shows the actual status of the OpenVPN tunnel.

Enable

Click the checkbox to enable the VPN tunnel. An already configured tunnel profile can be disabled in this way without losing the configuration.

Tunnel mode

Select point-to-point (P2P) or Client. Client mode can be selected for connection with an OpenVPN server. In this case the server pushes all routing information. P2P mode can be used for connections between two RSA routers or for connections with other hosts or devices that are configured for P2P operation.

Protocol

When P2P mode is selected the available protocols are UDP, TCP client and TCP server. In tunnel mode “client” the options are TCP (client) or UDP.

Remote peer address

Enter the address to connect to or to accept incoming tunnel connections from. Both IP addresses and names can be given (provided that the unit has access to a DNS server).

Port

Enter the (UDP or TCP) port for the OpenVPN tunnel. The default OpenVPN port is 1194 but also other port numbers can be selected. The port numbers must be the same on both peers.

Interconnection mode

Two modes can be selected: L2 bridged or L3 routed.
Bridging has the advantage that all Layer 2 traffic is passed through the tunnel transparently. This has benefits when local Ethernet devices need to be in the same broadcast domain as the devices at the remote end of the tunnel, like for example, for receiving configuration from a central site DHCP server.
Routing has the advantage of less overhead in the tunnel as no broadcast or multicast traffic is routed and transports only Layer 3 packets.

LAN Bridge (L2 bridged mode only)

In L2 bridged mode, one of the 4 LAN bridges can be selected. This enables the traffic to be passed over (a) dedicated Ethernet port(s) or VLAN without additional configuration.
In addition, no LAN (none) can be selected for preventing the “tap” interface from being added to one of the LAN bridges.

Authentication mode

The following authentication modes can be selected: None, Pre-shared secret (static key), X.509 TLS client and X.509 TLS server.
- Authentication mode “None” can be used when no authentication/encryption is needed, for example when a (bridging) OpenVPN tunnel is set up over an IPsec tunnel in order to transport Layer2 packets.
- In static key mode, a pre-shared key is generated and shared between both OpenVPN peers before the tunnel is started.
- In TLS client or TLS server mode the authentication is based on X.509 certificates. One peer must be configured as TSL client, the other as TLS server. The designation of client or server is only for the purpose of negotiating the TLS control channel.

Local interface address

Enter the address of the local tunnel endpoint. This address should be set as Remote interface address at the remote peer. The local and remote interface addresses are used for internal tunnel interfaces over which the VPN connection is routed.

Remote interface address

Enter the address of the remote tunnel endpoint. This address should be set as Local interface address at the remote peer. The local and remote interface addresses are used for internal tunnel interfaces over which the VPN connection is routed.

Remote network

Enter the address or network for the device(s) at the remote end of the tunnel. This can be a single address like 192.168.10.22/32 or a network like 192.168.10.0/24. In IKEv2 mode, multiple addresses/networks can be entered. Multiple addresses are entered as comma separated.

Local certificate

The local certificate is used by the remote peer to verify this unit’s identity against the list of CA certificates at the remote peer.
This unit, in turn, verifies the local certificate of the remote peer by checking if this certificate was signed by one of the CA certificates stored on this unit.

CA certificate

Select one of the CA certificates stored on this unit. The selected CA certificate will be used to check if the certificate used by the remote unit is signed by this certificate. Certificates are configured in the Management>Certificates menu.

TLS Authentication

TLS authentication adds an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks. This mode is recommended when OpenVPN is running in a mode where it is listening for packets from any IP address.
Both passphrases and static keys can be selected.

TLS auth passphrase

When “Passphrase” is selected for TLS authentication, enter a passphrase here. The passphrase must be equal on both peers and is converted into the HMAC key by taking a secure hash.

TLS auth key

When “Static key” is selected for TLS authentication, select one of the keys stored in this unit at **Setup>Certs and keys>OpenVPN keys**. In this mode also a Key direction can be selected where one side must be configured as client and the other as server.

Key direction

When “Static key” is selected for TLS authentication a key direction can be selected.
When direction “None” is selected 2 keys are used bi-directionally, one for HMAC and the other for encryption/decryption.
When “Client” or “Server” is selected 4 distinct keys are used (HMAC-send, cipher-encrypt, HMAC-receive, cipher-decrypt), so that each data flow direction has a different set of HMAC and cipher keys. One peer must be “client” (key-direction 1), the other “Server” (key-direction 2).

GRE tunnels

GRE tunnels are not encrypted and are very often used in combination with IPsec tunnels for security. GRE tunnels are especially useful for transporting multicast packets like OSPF, RIP, and EIGRP. Also streaming audio and video applications and VoIP may use multicast.
Click the “Add Tunnel” button to add a new GRE tunnel connection profile.
In the GRE tunnels overview page, tunnels can be enabled or disabled.

Name

Optionally a name can be given to each GRE tunnel profile. Tunnel names can be used for reference but are not relevant for the configuration.

Ifname

This field is generated automatically and shows the interface name us used by the system.

Enable

Click the checkbox to enable the GRE tunnel. An already configured tunnel profile can be disabled in this way without losing the configuration.

Local peer address

This field can usually be set to 0.0.0.0 and defines from which WAN interface the GRE tunnel will be set up. Usually this will be the active WAN interface. When 0.0.0.0 is entered the active WAN interface is used automatically.

Remote peer address

Enter the IP address (public WAN address) of the remote GRE peer.

Local interface address

Enter the address of the local tunnel endpoint. This address should be in the same network as the local interface address in the GRE configuration of the remote peer. For example: 11.0.0.1/30 for the local and 11.0.0.2/30 for the remote peer.

Remote network

When enabled, entries for static routes to remote network are added to the routing table when the GRE tunnel is activated.
Enter the address or network for the device(s) at the remote end of the tunnel. Multiple, comma-separated addresses can be entered.
When no routes are needed, for example when RIP or OSPF routing is enabled, this option can remain unchecked.

MTU

Enter the MTU of the GRE packets. The default value is 1400..

GRE over IPsec

For GRE over IPsec, create an IPsec tunnel with tunnel end-points as a single address. This address can be one of the local interface addresses or a local loopback address (created in the IPsec setup menu, see page 35).
Configure the Local network address of the IPsec tunnel as Local peer address, and the remote network address of the IPsec tunnel as Remote peer address.

Serial Gateways setup

The serial RS-232 and RS-485 ports can be used as “serial port gateway” connected via the LAN, WAN or VPN tunnel.

The remote device can be another RSA unit, a computer system, or another serial server that supports one of the protocols used by this unit. The two possible IP protocols for network access to the serial port are **TCP** or **UDP**.

In the TCP modes a TCP/IP connection is made between the two end-points. The data packets that are sent are checked for errors and, when necessary, retransmitted. For TCP mode, one end must be configured as “Server” and the other as “Client”. The Server will wait for incoming connections. The Client will continuously make an attempt to connect to the remote server.

In the UDP modes no real connection is made, but for each character, or group of characters sent into the serial port, a UDP/IP packet is sent to the remote address and port. Equally, all characters in the UDP packet received at the defined port number are sent to the serial port. The advantage of UPD over TCP mode is the flexibility and efficiency. The disadvantage is the lack of error correction and complete packets may be lost.

Telnet server mode can be used to access the serial port directly via a telnet session.

Serial ports Physical setup

The setup of the parameters (like bitrate and format) of the physical RS232 and RS485 ports is made at **Setup>Physical ports>Serial**.

RS-232/RS485 port

Mode

The following modes are available: TCP server, TCP client, UDP server, UDP client and Telnet server. When Disabled, no serial gateway function is active. When the serial RS232 port is used for console or serial CLI (command line interface), the serial gateway function will be disabled.

Note: *To allow access in server mode (TCP, UCP or telnet) you must add incoming IP filter rules in the* ***Setup>Firewall*** *page.*

Maximum concurrent connections (server modes)

In TCP, UDP or telnet server mode, multiple concurrent connections can be made to the same serial gateway. The entered value determines how many connections are allowed at the same time.

New connection drops oldest (server modes)

When enabled, a new connection made to the Server will automatically drop (disconnect) the previous connection. When “Maximum concurrent connections” is set to a number higher than 1, the first made connection will be dropped when the maximum amount of connections is exceeded.

Port

Selects the IP port used for transferring the serial port data.
In Server mode, the unit listens at this port for incoming connections.
In Client mode, the unit will make connection to this port of the IP address defined in “Remote address”**.**

DTR connection control (RS232 TCP client mode only)

When enabled, connection will be made when the DRT input of the RS232 ports becomes active. The connection will be dropped when DTR goes down.

Remote Address (Client modes only)

Defines the address (or name) of the remote port server. When using a name rather than an IP address, make sure that the DNS settings are correct.

TCP keep-alive (TCP modes only)

When TCP Alive check is enabled, the Client or Server will check if the remote connection is still alive by sending “TCP Keepalive packets” on a regular basis. When no ‘TCP Alive replies’ are received for the time set in “TCP keep-alive timeout”, the TCP port will be closed automatically.

Keep-alive timeout (TCP modes only)

Defines the timeout for dropping the TCP connection when no ‘TCP Alive replies’ are received.

DCD lag (UDP only)

The value entered here determines how long the DCD LED (when enabled) and the DCD interface signal (RS232 only) will remain On after the UDP packet is received.

Buffer size

Selects the amount of characters stored in the data buffer before they are transmitted over the network. It enables data packets that are sent to the serial port as one block, to be sent as one block over the network and thus sent as one block to the remote application. This is important when using protocols like Modbus RTU or other protocols that are sensitive to inter-character delay.

The default value is 300 characters (bytes), which allows for the use of the most common SCADA protocols.
Note that a block of data is considered to have an inter-character time that is less than the “Forwarding timeout”.

Forwarding timeout

Selects the time that the unit waits before sending a character or block of characters over the network.
The default value is 5ms, which is appropriate for all data rates above 2400 bit/s. For higher data rates shorter timeout values can be selected.

Serial ports Physical setup

The setup of the parameters (like bitrate and format) of the physical RS232 and RS485 ports is made under **Setup>Physical ports>Serial**.

Physical ports

The parameters of the unit's physical ports are configured here.

DSL Phy Setup

Status

This field is generated automatically and shows the current link status of DSL connection.

DSL mode: This field is generated automatically and shows the mode of the DSL link: ADSL, ADSL2, ADSL2+ or VDSL2 (VDSL2 on RSA-x2xx units only).

Transport mode: This field is generated automatically and shows the transport mode for the DSL connection. Normally this is ATM for ADSL and PTM for VDSL2.

Line status: This field is generated automatically and shows the line status when the connection status is "Connected". Usually the message "No defect" will be shown here.

ADSL overlay mode

This setting determines the overlay mode (Annex A or Annex B) for ADSL connections. Annex A is mainly used as POTS(PSTN) overlay while Annex B is intended as overlay for ISDN services. Note that in some countries the overlay mode is always Annex B regardless if POTS, PSTN or no telephony services are used.

Current overlay mode: This field is generated automatically and shows the mode in which the unit is configured.

Overlay mode: The overlay mode is selected here. A for Annex A, B for Annex B. In mode 'Auto' the default setting of the overlay mode depends on a hardware or jumper pre-setting on the main board. The pre-set overlay mode can be seen at **Device info>summary** at 'Mainboard" (-A or –B)

Note: *When changing the overlay mode the unit will reset and start again in the selected mode.*

DSL mode

In the default settings all xDSL modes are enabled. The unit will automatically select the mode that allows for the highest possible data rate as offered by the DSL provider.
Annex M (Annex A overlay mode) and Annex J (Annex B overlay mode) allow for a higher upstream data rate. This feature has to be supported by the DSL provider in order to be effective.

Warning: *Disabling certain modes may disable DSL operation completely. Leave all modes enabled if not sure.*

Rate adaptation

Two rate adaptation options are supported: Bitswap and Seamless Rate Adaptation (SRA). Both features are enabled in the default settings.

DSL SNR margin Settings

The DSL SNR margin settings can be used for changing the target SNR margin (noise margin) of the downstream channel. The default value is 6dB. Increasing the target SNR margin will result in a link with lower downstream data rate but higher reliability. Decreasing the target SNR margin will result in a link with higher downstream data rate but lower reliability.

Ethernet Phy Setup

On this page a list of available Ethernet ports is shown. These can be the internal port(s) and USB-Ethernet adapters connected to the USB ports. When a USB Ethernet port is inserted, a new entry will be made automatically. This entry will remain after the USB-Ethernet adapter is removed. To remove the entry, click the Remove checkmark and the Remove button.

Edit ports

Ifname

This field is generated automatically and shows the Ethernet port assignment as used by the system.

Enable

The Ethernet port can be disabled here. This can serve as a security feature to prevent unused Ethernet ports from being used.

Media type

The Ethernet ports are normally set to ‘Auto-negotiation mode’. In cases of conflicts with legacy Ethernet devices that do not support auto-negotiation The internal ports can be set to one of these modes: 10baseT Half Duplex 10baseT Full Duplex, 100baseTx Half Duplex and 100baseTx Full Duplex.

Status

This field is generated automatically and shows the link state and the negotiated or selected media type.

Hwaddr

This field is generated automatically and shows the hardware address of this Ethernet port.

External

This field is generated automatically and shows a ✔ checkmark when the Ethernet port is an external USB-Ethernet adapter.

Serial Ports Setup

The serial RS232 and RS485 ports can be configured individually. Click edit to change the settings.

Name

A name can be given to each serial port. These names are used for reference only and are not relevant for the configuration.

Baudrate

Select the data rate of the serial port. Speeds from 50 bit/s up to 115.200 bit/s can be selected.

Parity

Select Even, Odd or No parity.

Data bits

Select the number of data bits.

Note:
For 10-bit asynchronous data, the best option to use is "8-bit, No parity".
In this way, the serial channel is transparent for all 10-bit formats like 7E, 7O and 8N.
For 11 bit data, the number of Data bits must be set to 8 and the Parity must be set to Odd or Even. In 11-bit mode, the parity bit is generated by the unit.

Stop bits

Select the number of Stop bits in the Asynchronous character frame. When set to "2" one extra stop bit is added in the data path from the RSA-4122's serial port towards the connected device. In the majority of cases this option can remain at "1".

Flow Control (RS-232 port only)

Selects the use of RTS/CTS flow control for the RS-232 port.

Control LEDs

When enabled, the serial port LEDs (TxD, RxD, DTR and DCD) are used as indicator for this port. When the LEDs are enabled on both RS232 and RS485 ports, the states of the two ports will be an "and" function.

4 wire only (RS485 port only)

When enabled the RS485 (RS422) receive input is only on the outer pins of the RS485 connector (4-wire interface). When disabled, the receive input is on both inner and outer pins (2-wire or 4-wire interface).

USB Power Setup

The USB ports page controls the power of the 2 external USB ports.
It can be used to enable or disable devices that are powered via the USB ports of the unit.

Note: *only the power of the USB ports is controlled. The USB data ports will remain active. When an attached USB device is not powered by the RSA unit, the USB device will remain logically connected, regardless of the state of the USB power.*

Power

This field controls whether or not power is applied to the USB port.
Click Apply/Save after checking/unchecking the checkmark.

Status

This field is generated automatically and shows the actual status of the USB power.

Device

This field is generated automatically and shows what kind of device is connected with this USB port.

WWAN

The internal WWAN module has options for setting operating modes like radio band. For external (USB) WWAN modems these options may be limited depending on the type of USB WWAN modem.

If a USB-WWAN module is detected or an internal WWAN module is present, click ‘Edit’ to change the WWAN port settings.

Status

This field shows whether or not the WWAN port is registered on the mobile network. When registered, data connections can be made and SMS text messages can be sent.

USB port

This field shows the internal logical device number to which the USB WWAN modem or module is assigned (enumerated).

Bands

This field shows and make all the available bands selectable for the internal WWAN modules.

Limits

The data limits and threshold for warning of the WWAN data can be entered here. The ’Max’ field defines the maximum amount of data expected per month. The ‘Perc’ field defines the threshold as which system alerts will be sent.

IO

All RSA units are equipped with a (dry) contact input and a dry contact output.

Contact in

This field shows the status of the contact input sensor. The status is either ‘open’ or ‘closed’.

Contact out

This field allows for the manipulation of the contact output. When the contact output is used for system alerts, the status entered here will override the status as set by the system alerts. Equally, a change will in system alerts will override the setting made here.

Electrical characteristics

Consult the hardware manual of the device for details and electrical characteristics of the I/O ports.

4
Tools

Network

Ping

The ping tool can be used to check connection and transit delay of local or remote IP addresses. Both active (Default gateway) and standby WAN interfaces can be selected. Leave the selector at ‘Default gateway’ to ping addresses on the LAN side or connected via VPN tunnels.

Traceroute

The traceroute tool can be used to display the route and transit delays to local or remote IP addresses. Both active (Default gateway) and standby WAN interfaces can be selected. Leave the selector at ‘Default gateway’ to trace the route for addresses connected via the LAN side or via VPN tunnels.

DSL

DSL Test options

The xDSL test modes are used for diagnostics purposes. They serve no purpose to normal operation. The selections made will not be stored and will return to the default values after a restart of the unit.

DSL BER test

The DSL BER test can be used to check the bit error rate of the raw xDSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

To start the test, click “Start BER test”. To change the duration of the test, enter the required duration (seconds).
The test will run for the selected time duration. Upon completion, the number of transferred bits, the number of error bits, and the bit error rate will be shown.

Serial CLI

When enabled, the serial RS232 port is used for command line access to the system. The serial gateway is disabled. The default user name is ‘admin’ the default password is ‘rsa-admin’.

For details on the command line interface, contact MuLogic or your local sales representative.

Terminal

The “Terminal” feature offers a simple web based command line interface to the system. It can be used for entering Linux commands for system information, editing scripts or making configuration changes. This feature is available only to users with the role of Administrator.

Note that this web based command line interface will not offer all features as are common with telnet or SSH clients or terminal emulators.

For details on the command line interface, contact MuLogic or your local sales representative.

5 Management

The Management menu tree contains the items for configuration of the device-management settings such as system ID, authentication of users, access services, certs and keys, system logs and alerts, and the update of settings files and firmware.

System ID

System identification

Name

The name entered here will be used as the SNMP MIB-2 “sysName”, for email and SMS system alerts, in the CLI command line prompt, and will show up in the top frame of the web interface and the Device info Summary page.

Location

The name entered here will be used as the SNMP MIB-2 “sysLocation”, for email and SMS system alerts, and will show up in the top frame of the web interface and the Device info Summary page.

Contact

The name entered here will be used as the SNMP MIB-2 “sysContact”.

User accounts

Roles

Access control of the RSA-series is role based (RBAC). Users are assigned with a specifically defined “role” which offers a collection of permissions.
A user inherits those permissions when acting under that role.

RBAC applies to access via HTTP(S). For access via SSH or telnet, only users with the role of Administrator are permitted.

The system distinguishes 5 roles. Each role has specific permissions:

- **Administrator**: All permissions for Web interface and command-line interfaces.
- **Web administrator**: All permissions for Web interface. No command-line interfaces.
- **Operator**: Enable/disable interfaces and ports. View device info, configuration and system log.
- **Auditor**: View device info summary, system log, account log and WWAN data usage.
- **Updater**: View device info summary, update firmware.

Add User

Click ‘Add User’ to add a new user to the list.

Role: Select the role of the new user.
Login: Enter the user name.
Password: Enter a password. The password can later be changed by the user at **Management>User accounts>Password**.

RADIUS

Apart from storing the login information locally on the system, users for HTTP(S) and SSH access can also be authenticated via a RADIUS service. The roles are determined

Note: For telnet access, only locally stored users with the role of Administrator are permitted.

Enable RADIUS for login authentication: click the check mark to enable RADIUS authentication.

Deny local authentication when RADIUS server is accessible: Click the check mark to enable this feature. When enabled, locally stored users will not be authenticated as long as one or more RADIUS servers can be accessed.

Primary Server address: enter the IP address of the primary RADIUS server.

Primary Server secret: enter the password for access to the primary RADIUS server

Secondary Server address: enter the IP address of the secondary RADIUS server.

Secondary Server secret: enter the password for access to the secondary RADIUS server.

Server UDP port: enter the port number of the servers. The default is 1812.

Retries: Enter the number of retries for the unit to re-authenticate with the RADIUS server.

RADIUS Attributes

The roles of users that are authenticated via RADIUS are defined by RADIUS attributes.

The roles of Administrator and Operator can be defined through RFC 2865 attribute 6(Service-type); with value 6 (Administrative-User) for the role of Administrator and value 7 (NAS-Prompt-User) for the role of Operator.

All available roles can be defined through the vendor specific attribute, named MuLogic-Login-Role (type "string"). Valid strings are *admin, webadmin, operator, audit and updater*.

Password

In this menu, the password of the user that is logged in can be changed. Users with the role of Admin can change the password of any user on the ‘Manage users’ web page.

Certs and keys

Certificates are used for authentication between peers for IPsec and OpenVPN tunnels, and for secure webserver operation (HTTPs).
Apart from certificates, SSH and OpenVPN keys can be added here.

Local certs

Local certificates are used by a remote peer to verify the identity of this unit by checking if such certificate was signed by a Certificate Authority or private CA.

These certificates are used for IPsec, OpenVPN and HTTPs.
A certificate for testing is present in the default configuration.

***Warning:** do **not** use the test certificate in the final setup. Add your own certificate instead.*

In principle, the private key part of the local certificate key pairs should be kept on the device and should not be exported to other devices. However, the option of importing and exporting private keys is provided.

Local certificates (cert and private key) can be added manually by clicking "Import certificate" and uploading the Cert and Key files (in PEM format) from a local PC.

Another (and more appropriate) way is to generate a Certificate Signing Request and have this request signed by a Certificate Authority or private CA. This process can be automated by means of using a SCEP service.

Import Certificate

Click "Import certificate" to manually add a local certificate and key. This method can be used when both certificate (public key) and private key are stored on an external computer.

Name

A name can be given to each certificate/key combination. Certificate names can be used for reference but are not relevant for the configuration.

Status

This field is generated automatically after a valid certificate and key combination are loaded. When the cert and key match, this field shows: "Certificate and key ok". If there is a mismatch between the certificate and key, this field shows: "Certificate and key do not match".

Valid

When the certificate is valid, this field will show a ✔checkmark.

Cert

Click the Upload button to load a certificate file in PEM format. PEM files can have the .pem file extension but also other file extensions may be encountered. A PEM-formatted file can be recognised by the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines at the beginning and end of the file.
After a file is uploaded, a View and Download button will appear. These buttons can be used to view the file for "copy-paste" purposes or for saving the file.

Click Apply/Save for storing the certificate or continue to loading the key.

Key

Click the Upload button to load a key file in PEM format. PEM files can have the .pem file extension but also other file extensions such may be encountered.
A PEM-formatted file can be recognised by the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines at the beginning and end of the file.
After a file is uploaded, a View and Download button will appear. These buttons can be used to view the file for “copy-paste” purposes or for saving the file.
Click Apply/Save for storing the key and validating the cert/key combination.

Info

This field is generated automatically after successful upload of a certificate/key combination.

Generate CSR

Click “Generate CSR” to create a Certificate Signing Request. A new page will open where the Certificate information can be entered.

Name

The “Name” field is for internal reference only and is no part of the signing request.

Certificate information

Fill out the information for the Certificate Signing Request. This information will be present in the certificate generated and signed by the CA.

Key

Select the Key size from the drop-down menu.

Enrollment method

File based
When “Mode” is set to “File based”, upon clicking “Generate CSR” a private key will be generated and a signing request will be made. This process will take several seconds depending on the key size. Upon completion a new page will open where the CSR can be viewed or downloaded. This CSR must be sent to the CA for signing. The signed certificate can be added by clicking the “Upload” button at “Cert”.

SCEP
When “Mode” is set to “SCEP”, enter the URL of the CA Server and the Challenge Password. Then click “Generate CSR”. The CA server will return a signed certificate which will be added automatically.

Remote certs

Remote certificates are used by this unit for additional verification of a remote peer. Apart from checking the certificate's signature of the remote peer towards a CA certificate, the certificate of the remote peer must match the certificate stored here. Click Add certificate to add a remote certificate.

Name

A name can be given to each certificate. Certificate names are used for reference only and are not relevant for the configuration.

Status

This field is generated automatically after a proper certificate is loaded. When the certificate is valid, this field shows: "Certificate ok".

Cert

Click the Upload button to load a certificate file in PEM format. PEM files can have the .pem file extension but also other file extensions may be encountered. A PEM-formatted file can be recognised by the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines at the beginning and end of the file.
After a file is uploaded and saved, a View and Download button will appear. These buttons can be used to view the file for "copy-paste" purposes or for saving the file. Click Apply/Save for storing the certificate.

Info

This field is generated automatically after successful upload of a certificate.

CA certs

CA certificates are used by IPsec, OpenVPN and HTTPS transactions for verifying the digital certificates sent from the remote peer. Click Add certificate to add a CA certificate.

Name

A name can be given to each certificate. Certificate names are used for reference but are not relevant for the configuration.

Status

This field is generated automatically after a proper certificate is loaded. When the certificate is valid, this field shows: "Certificate ok".

Cert

Click the Upload button to load a certificate file in PEM format. PEM files can have the .pem file extension but also other file extensions may be encountered. A PEM-formatted file can be recognised by the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines at the beginning and end of the file.
After a file is uploaded and saved, a View and Download button will appear. These buttons can be used to view the file for "copy-paste" purposes or for saving the file. Click Apply/Save for storing the certificate.

Info

This field is generated automatically after successful upload of a CA certificate.

SSH keys

SSH (public) keys can be used as an alternative of a username/password combination for SSH access of this unit. Click ‘Add public key’ to add a key.

Name

A name can be given to each SSH key. Key names are used for reference but are not relevant for the configuration.

Enable

Click the checkbox to enable the key. An already configured tunnel profile can be disabled in this way without losing it.

Key

Click the ‘Upload’ button to browse for and load the key file. Click Apply/Save to store the file.

OpenVPN keys

OpenVPN keys are used for OpenVPN ‘Pre-shared secret’ operation and TLS authentication. Click ‘Add static key’ to add a key.

Name

A name can be given to each key. Key names are used for reference and are not relevant for the configuration.

Key

Click the ‘Upload’ button to browse for and load the key file. Click Apply/Save to store the file.

Access services

This chapter describes the various services that can be used for system management.

Note: *To enable access to the system services, rules may need to be set for the firewall input filter.*
Warning: *Access from the LAN interfaces (LAN Ethernet ports) is enabled by default. It can be disabled by unchecking the "Bypass filter for LAN-side traffic" shortcut checkmark at* ***Setup>Firewall>IP filtering****.*
Warning: *HTTP and HTTPS access via the WAN ports is enabled by default. It can be disabled by unchecking the "Bypass filter for HTTP/HTTPS access" shortcut checkmark at* ***Setup>Firewall>IP filtering****.*

HTTP server

The HTTP server is used for web access of this device. Both HTTP and HTTPS protocols are supported and can be enabled /disabled individually.
The default HTTP port is 80. The port can be changed in the 'HTTP port' field.
The default HTTPs port is 443. The port can be changed in the 'HTTPs port' field. For HTTPS an X.509 certificate must be added (local certificate) and selected. The default HTTP session timeout is 30 minutes.

SNMP

SNMP global

SNMP access can be set to read-only or to read-write.
In read-only mode no SNMP "sets" are accepted, only SNMP "gets".
Check the "Enable SNMP-invoked firmware update" to allow firmware updates from a remote server to be initiated via SNMP.
Check the "Enable SNMP-invoked settings update" to allow updates of the settings file from a remote server to be initiated via SNMP.

SNMP Version 1/2c

The SNMPv1/v2c mode is enabled by means of the checkmark and clicking 'Apply/Save'. When enabled, the SNMP v1/v2c community names can be entered and stored.

SNMP v3

The SNMPv3 mode is enabled by means of the checkmark and clicking Apply/Save. Enter the user name, authentication password and cypher, and privacy password. Select DES or AES as privacy cypher.

Shell Access

SSH server

The SSH server is enabled by means of the checkmark and clicking 'Apply/Save'. The default port is 22. The port can be changed in the 'Port' field.
The SSH server accepts both logins with username/password and by means of an SSH public key. Generate an SSH public/private rsa key pair and load the public key on this unit (**Certificates>SSH keys**). Consult the documentation of your SSH client for information on how to log in by means of an SSH key.

Telnet server

The telnet server is enabled by means of the checkmark and clicking ‘Apply/Save’. The default port is 23. The port can be changed in the ‘Port’ field

CLI session timeout

Command line access via serial CLI, SSH and telnet is time restricted. The default inactivity timeout is 30 minutes.

IXagent

The internal IXagent (optional) offers access to the IXON IXplatform for cloud access to the router and/or to attached Ethernet devices equipped with an HTTP, VNC or WS server.
Contact MuLogic for additional information on the use of the IXplatform.

Enable

Use the Enable checkmark to enable/disable the IXagent.

Company ID

Enter the company ID as issued via the IXplatform.

Turn on VPN LED when connected

This option makes the VPN LED to be turned on when the IXagent is connected with the IXplatform.

Status

This field is generated automatically and shows the current status or most resent status change of the connection with the IXplatform.

TR-069

The internal TR-069 client offers a means for the router to be managed via the CPE WAN Management Protocol (CWMP).
The TR-069 client will contact an Auto Configuration Server (ACS) at regular intervals by sending “inform” messages. The ACS then in turn can retrieve status information, change parameters or send commands to update the firmware or configuration file. By means of a “Connection request”, the ACS can provoke the router to send an inform message at any time.
Contact MuLogic for additional information on using TR-069.

Enable TR-069

Use the Enable checkmark to enable/disable TR-069 CWMP operation.

Status

This field is generated automatically and shows the current status or most resent status change of the connection with the TR-069 ACS.

ACS URL

Enter the URL (http or https) and port number of the ACS. Host name and port number are separated with a : colon sign.

ACS username

Enter the user name for access to the ACS

ACS password

Enter the password for access to the ACS

Local x.509 certificate

If needed by the ACS for authentication, select a local certificate from the drop-down list or add the appropriate certificate to the list of local certificates first.

Strict verification of remote certificate

When the ACS is contacted in HTTPS mode, this option is used for verification of the certificate of the ACS. The CA certificate of the ACS must be added to the list of CA certificates.

Periodic inform

When enabled, the router will send TR-069 inform messaged at the interval as configured at “Inform interval”

Inform interval

Enter the inform interval here.

Connection request port

Enter the port number at which the Connection requests from the ACS are to be received. The TR-069 client will send this information, along with its URL and authentication credentials, to the ACS in every inform.

Note: *Make sure to add an accept rule to the table of Setup>Firewall>IP filtering for the port number (TCP) entered here.*

System time

Date and time

Time zone

Select the time zone of the location of the unit.

Current time

This field is generated automatically and shows the actual data and time of the system.

Run NTP time server

This option enables the system's time server to allow other devices to synchronise their system time with this unit.

Method

When NTP is selected, the system will synchronise its clock with one of the configured NTP servers.
When Manual is selected, the date and time can be entered manually in the format: yyyy-dd-mm hh:mm:ss.
Alternatively, the system time of the web browser can be used by clicking "Sync with browser". Click 'Apply/save' after making the changes.

Alert messaging

Various system events can be configured to generate a system alert. System alerts can be indicated by sending email or SMS messages, SNMP traps, written to the system log or indicated by setting or resetting the I/O contact, and, if present, the ALM LED.

Alert rules

Select the events and alert method by clicking the checkboxes and 'Apply/Save'. Passed events are indicated by means of a red dot. These indications can be cleared by clicking the "Clear alerts' button.

Recipients

Write alerts to syslog

When enabled, the alert messages are written in the system log file.

Email

When enabled, email messages are sent to the address(es) configured in the "To address" field(s). When SMTPS mode is enabled, enter a username and password for access to the SMTPS server.
The 'From address' can be any valid email address. This address will show up as the sender's email address. The 'From name' can be any string. This name will show up as the email sender's name. The name as defined on the 'Management>System ID' page is used in the subject line and the body of the email. The location as defined on the 'Management>System ID' page is used in the body of the email.

SNMP Trap

When enabled, SNMP traps are sent to all of the configured addresses. For information on the type of traps, refer to the RSA-series SNMP MIB file.

SMS (Versions with internal or external WWAN interface only)

When enabled, SMS text messages are sent to all of the configured numbers. The name and location as defined on the 'Management>System ID' page are shown in the SMS message.

Test alerts

For testing if messages will be delivered to the configured recipients, test alerts can be generated. To generate an email, SMS or SNMP test alert click the checkbox and click "Generate test alert". The checkmarks will be cleared automatically. Note that when testing the ALM LED and contact, the status will not be cleared. After testing LED on or Contact On, one should use LED off or contact off to turn off the ALM LED or open the contact again.

System log

System log

The system log page shows the messages of the unit's syslog. The most recent message is written on top.
The list will be updated automatically. The update of the syslog screen is interrupted when the page is scrolled down. Printing will resume when the browser's scroll bar is completely at the top of the page.

Settings

Display level

The Display level determines the severity level of the messages printed on the system log screen.
Levels can vary from "Emerg" to "Debug". At the emergency level, only the most important system messages will be printed. At debug level all messages including those for debugging will be printed.

Remote syslog

When enabled, syslog messages are sent to a remote syslog server at the configured address. The default port for remote syslog is 514 but other port numbers can be configured in the "Port" field.
Levels can vary from "Emerg" to "Debug". At the emergency level, only the most important system messages will be sent. At debug level all messages including those for debugging will be sent.

USB syslog

When enabled, syslog messages will be written to a USB flash drive inserted in one of the USB ports.
Levels can vary from "Emerg" to "Debug". At the emergency level, only the most important system messages will be written. At debug level all messages including those for debugging will be written.
The 'Rotate size' field determines the maximum file size. When the maximum size is reached, a new file will be created.
The 'Rotate files' determines how many files are created before the oldest file is deleted.

Raw file

The raw file option displays the syslog file in text format. The most recent message is written on the bottom of the list as opposed to the normal view. The list is not updated automatically. Click the "Raw file" menu link for updating the list with the most resent messages.

Account Log

When enabled, the account log page shows all login attempts and configuration changes. The most recent message is written on top and the list will be updated automatically. The update of the syslog screen is interrupted when the page is scrolled down. Printing will resume when the browser's scroll bar is completely at the top of the page.

Settings

Use the "Enable" check mark to enable account logging. When enabled, the account log will be stored on the system.

Account log download

Use the "Download" button to download the account log file for storage on your computer. The size of the internal file is limited and the oldest entries will be overwritten when the maximum file size is reached.

Raw file

The raw file option displays the account log file in text format. The most recent message is written on the bottom of the list, as opposed to the normal view. The list is not updated automatically on the screen. Click the "Raw file" menu link for updating the list with the most resent messages.

WWAN data usage

WWAN Data Volume Counter

For purposes of costs control, the amount of data sent and received over the Cellular WWAN network is logged and stored on the system.

Note: *The shown data volumes serve as an indication only and may differ from the mobile data operator's accounting.*

When the data volume reaches a certain value, a System Alert can be sent. See **Management >System Alerts**.

Both actual volume and the data volume of the previous month are shown.

Monthly Data Volume limit

Enter the maximum amount of data (in MB) that is allowed per month.

Percentage of data volume limit before alerting

The value entered here represents the maximum percentage of the monthly data volume before a system alert is activated. It should be set to a save value below 100% in order to cater for differences in accounting by the network operator. Click 'Save/Apply' to store the settings. Click 'Clear counters to reset both actual and previous month counters.

Watchdog

Each unit of the RSA-series is equipped with a watchdog microcontroller that runs independently from the main CPU. It controls the system power and monitors the general operation of the unit. Should a system error occur, the watchdog circuit powers down and restarts the unit.
In addition, checks on the internal processes and services can be selected

Another function of the watchdog/reset controller is making sure that the unit properly starts up at extremely low temperatures. The reset controller circuit can operate at temperatures as low as -55°C /-67,00°F and, if needed, will cycle the power of the main unit until it is heated up sufficiently and operates correctly.

Network connection

When enabled, up to two remote IP addresses or host names are monitored by means of checking the response to ICMP Ping packets. If both addresses fail to respond after the time as set in 'Timeout', the reset controller will restart the unit.

Internal SNMP server

If SNMP access to this unit is of high importance, an automated check can be made on the internal SNMP server. Should the SNMP server fail to respond within the time as set in the 'Timeout' field, the reset controller will restart the unit.

DSL connection

When enabled, the physical DSL connection is monitored. Should DSL connection fail (after having been up) for the time as set in the "Timeout" field, the reset controller will restart the unit. Note that only the DSL "modem" connection is monitored, not the actual network access. In general it will be more reliable to monitor the network connection.

Internal HTTP server

If HTTP/HTTPS access to this unit is of high importance, an automated check can be made on the internal HTTP server. Should the HTTP server fail to respond within the time as set in the 'Timeout' field, the reset controller will restart the unit.

Task scheduler

The task scheduler offers a means for scheduling events like a reboot or the restart of an interface. Tasks can be executed at a pre-determined time for once a day, once a week or a single time.
Use the "Add event" button, select a task from the drop-down list, the time at which the task must be executed and the occurrence of the execution of the selected task.

The "Restart interfaces" tasks can be used for dictating the time at which the ISP or mobile operator renews the issued IP address by staying ahead of the renewal period which expires 24 hours after link-up.

Settings management

The unit is shipped with factory default settings that allow for easy access to carry out web based configuration of the system.
Also a user defined (custom) default file can be stored on the system.
The custom default file can be used for configuring other default settings than the MuLogic factory defaults but is also used as “pre-provisioning file” for configuring the unit with all parameters required to access a provisioning server (like a TR-069 CWMP ACS).

View/download configuration with private info

Click the ‘View’ button to print the settings file in a new browser window.
Click the ‘Download’ button to download the settings file to your system.

Warning: *This file will contain* ***all*** *stored usernames, passwords, private keys and certificates. It is meant to serve as a backup for the settings of the very unit from which it was retrieved and should not be distributed to other units.*

View/download configuration without private info

Click the ‘View’ button to print the settings file in a new browser window.
Click the ‘Download’ button to download the settings file to your system.

Note: *the file viewed or downloaded will not contain privacy sensitive information such as user names, passwords and private keys.*
For HTTPS the default test certificate from the MuLogic factory defaults will be used and the default login user name and password will apply.

Load configuration from file

Click the ‘Upload’ button and browse for a configuration file. Then click ‘Upload file’. This action will load the configuration and will restart the unit with the new settings.

Load custom defaults config from file

Click the ‘Upload’ button and browse for a configuration file. Then click ‘Upload file’. This action will

Copy configuration to custom defaults

Click the ‘Apply’ button to copy the current configuration to the custom default configuration file. This file is also used as pre-provisioning file for TR-069 CWMP operation.

Note**:** *A “FactoryReset” RPC from a TR-069 CWMP ACS will reset the unit to the settings of the custom default file. If no custom default file is present then a reset to the factory defaults will be made.*

Restore custom default configuration

Click the 'Apply' button to restart the unit with the custom default settings. You will be asked for confirmation first.

Restore factory default configuration

Click the 'Apply' button to restart the unit with the factory default settings. You will be asked for confirmation first.

Warning*: *This action will delete all configuration, user-made scripts and log files stored on the system.

Settings update invoked by SNMP and CWMP

Apart from uploading a settings file from a PC, the unit can also download a firmware image file from a remote server. The download can be initiated via CWMP and SNMP. SNMP initiated downloads can be enabled/disabled under **Management>Access services>SNMP**.

Changing individual parameters

The individual configuration parameters of the unit can be changed by means of direct access to the configuration database. The changes will take effect immediately and, with few exceptions, no system restart is needed.

Changing parameters via CLI commands

For changing parameters in the configuration database the 'dbctl' shell command is used. Entering 'dbctl' without options will show the list of subcommands.
For details on the command line interface contact MuLogic or your local sales representative.

Note*: *Only parameters changed via the dbctl command will be stored. Changing parameters in the various –Linux- configuration files will not take immediate effect and none of the changes made will be stored on the system.

Changing parameters via HTTP(S) post

CLI commands via HTTP(S) post allow for scripted execution of dbctl commands.

Usually tools like Wget and cURL are used for this. A typical curl command would look like:

```
curl -u <user>:<password> http://<hostname>/mud/exec -d '<shell command>'
```

For details on this feature contact MuLogic or your local sales representative.

Firmware update

Update system firmware

The update process consists of uploading a firmware image file and writing the image to flash memory.
The unit will restart after the flash process is completed.

Current firmware version:

This field is generated automatically and shows the current version of firmware running on this unit.

Update from local file

Browse for a firmware image file on your PC and click "Update Firmware".
First the file will be loaded on the system and checked. After the file has been verified, the flash process will start and the unit will restart.

Note: *Do not close your browser window while the file is being transferred.*

Update from remote server

Apart from uploading the firmware image file from a PC, the unit can also download a firmware image file from a remote server.

Enable “Update from remote server” and enter the URL of the image file.
Click "Update Now" to immediately start the download and update process, or click “Save” to store the URL.

After the download, the file will be verified and the flash process will start. After the flash process the unit will restart.

If a HTTPS server is used, make sure that a valid root CA certificate is added to the list of CA certificates.

Firmware updates from a remote server can also be initiated via SNMP and TR-069 CWMP. SNMP initiated updates can be enabled/disabled under **Management>Access services>SNMP**.

Reboot

To reboot the unit, click the ‘Apply’ button. You will be asked for confirmation first.
All system processes and connections will be shut down and closed properly before the unit is restarted.

6
Device info

Summary

The summary shows an overview of system information and status.

System name: System name as set at **Management>System ID**.
System location: Location as set at **Management>System ID**.
System contact: Contact name as set at **Management>System ID**.

Mainboard: Type, hardware revision and Annex A or B setting.
Add-on board: Type and hardware revision of add-on board.
WWAN modem: Type of WWAN modem (W-versions only)
MAC address: Base MAC address of the unit.

Firmware version: Firmware version and firmware build date.
Bootloader version: Boot loader software version.
xDSL PHY/Driver: Version of the xDSL PHY and driver currently used.
WWAN firmware: (if present) Firmware version of WWAN modem.

Active WAN address: Address of the currently active WAN interface.
Primary LAN address: Address of the primary LAN interface.

System uptime: Elapsed time since last start or restart.
System temperature: Current internal temperature of the system.
System time: Actual time as used by the system.

WAN interfaces

The WAN interfaces page shows all configured WAN interface.
The table shows limited information of each interface.
For details click the “Details” button.

Details

Prio: This field shows the priority as set in the Setup>WAN Failover page.
Linkname: The name as configured in the interface setup page.
Type: Type of WAN connection
Up: Shows if the interface is connected (auto assigned IP address only).
Active: Shows if this interface is the currently active (gateway) interface.
Ifname: name of the interface as used by the system.
Address: Assigned or configured IP address.
Gateway: Gateway for this interface (not necessarily the active gateway).
DNS1: First DNS server for this interface.
DNS2: second DNS server for this interface.

IPsec tunnels

The IPsec connection state table shows all enabled IPsec tunnels.
The table shows limited information of each tunnel.
For details click the “Details” button.

Details

The details show information on the IKE-SA (authentication or Phase 1)

Connection: (profile name)

State: the state of the IKE-SA.
Hosts: the addresses of local and remote peer.
SPI: the current local and remote Security Parameter index.
Version: IKE version (IKEv1 or IKEv2)
Reauthentication time: time in sec. before re-authentication will take place.
Established time: time in seconds since last re-authentication.
Integrity algorithm: the currently used integrity algorithm.
Encryption algorithm: the currently used IKE encryption algorithm.
PRF algorithm: the currently used PseudoRandom Function.
DH group: the currently used DH (MODP) group.
Local ID: Details of the local certificate used.
Remote ID: Details of the local certificate of the remote peer.

Child SA: (profile number)

Note that multiple child SAs can exist under a single IKE-SA.

State: the state of the IPsec-SA.
Mode: Tunnel or Transport (only tunnel mode is supported).
Local network: the address of the local network or device.
Remote network: the address of the remote network or device.
Protocol: IPsec protocol: ESP or AH (only ESP is supported).
SPI in: Security Parameter index of the incoming channel.
SPI out: Security Parameter index of the outgoing channel.
Integrity algorithm: the currently used encryption algorithm.
Encryption algorithm: the currently used IPsec encryption algorithm.
DH group: the currently used DH (MODP) group.
Bytes in: Bytes received from remote end since last re-authentication.
Bytes out: Bytes sent to remote end since last re-authentication.
Packets in: Packets received from remote end since last re-authentication.
Packets out: Packets sent to remote end since last re-authentication.
Rekey time: time in seconds before rekeying will take place.
Install time: time in seconds since last rekey or installation of the tunnel.
Life time: Maximum life time (in seconds) of this SA (tunnel).
Rekeying is attempted 540 seconds beforehand.

OpenVPN tunnels

The OpenVPN connection state table shows all enabled IPsec tunnels.
The table shows limited information on configuration and status of each tunnel.
For details click the “Details” button.

Details

Connection: (profile name)

Status: shows connection status and local interface address when connected.
Remote Address: Address or DNS name of the remote peer.
Control channel: shows the cipher information of the control channel.
Encrypt channel: shows the encryption cipher information of the data channel.
Decrypt channel: shows the decryption cipher information of the data channel.
TCP/UDP bytes: Amount of bytes transferred between the peers.
TUN/TAP write bytes: Amount of bytes transferred through the tunnel.

Connection warnings

Warnings will be shown when different protocols are used by the peers.
If there are no warnings, this field will not be shown.

DSL

Statistics

The DSL statistics page shows both status and statistics information of the xDSL link. Some of the fields shown differ depending om whether the link is in an ADSL mode or in VDSL2 mode.

Mode: The current xDSL mode
Link uptime: Elapsed time since last (re)connect.
Traffic type: ATM for ADSL, PTM for VDSL2
Status: Status of the connection (“Showtime” when established)
Link power state: the xDSL Power Management state (L0, L2 or L3)
Line coding (Trellis): Trellis coding ON or OFF for upstream/downstream.
Vendor ID: Vendor ID code of the technology used in the remote DSLAM.

Actual rate (kbit/s): Actual data rate for downstream and upstream direction.
Attainable rate (kbit/s): the theoretically attainable rate for down and upstream
SNR margin (dB): margin between the actual and the minimum required SNR.
Attenuation (dB): The attenuation of the line at downstream and upstream.
Output power (dBm): the transmit level of the xDSL line driver.

Interleaver depth: Interleaver depth. (when value is 1, no interleaver is used)
Delay (msec): when in interleaved mode, shows the delay in the interleaver.

Super frames: Amount of Superframes since last (re)connect.
Super frame errors: Amount of Superframes errors since last (re)connect.
RS words: when in interleaved mode, shows the amount of RS Words.
RS correctable errors: in interleaved mode, shows the RS correctable errors.
RS uncorrectable errors: the amount of RS uncorrectable errors.

Total ES: the total amount of Errored Seconds since last (re)connect.
Total SES: the total amount of Severely Errored Seconds since last (re)connect
Total UAS: amount of secs that the link was unavailable since last re)connect.

Graph

The line graphs show the condition of the connection and line between this unit and the remote DSL unit (DSLAM). The x-axis of the graph represents the sub-carriers of the xDSL link. Details can be seen by using the mouse to select a smaller portion of the graph. Depending on the remote DSL unit, more or less information on the upstream direction is shown.
The sub-carrier number can be converted into frequency by multiplying the number by 4.312 KHz.

Bit allocation

This graph shows the amount of bits coded in each sub-carrier. The better the signal to noise ratio (SNR) of a sub-carrier, the more bits can be coded.

Signal to noise ratio (SNR)

This graph shows the absolute SNR of each sub-carrier. The higher the signal to noise ratio of a sub-carrier, the more bits can be coded.

Quiet line noise (QLN)

This graph shows the line noise at each sub-carrier frequency in absence of xDSL signals. The lower the noise level the better the SNR and the higher the amount of bits that can be coded in each sub-carrier.

Channel response

This graph shows the line attenuation at each sub-carrier frequency. The lower the attenuation the better is the chance for a good SNR.

ATM/PTM

This table shows the statistics of the ATM (in ADSL mode) layer, or the PTM (in VDSL2 mode) layer.

WWAN

Status

The WWAN status page shows the status and details of the WWAN connection.

Modem: the type of modem module used.
Interface status: shows whether or not the WWAN interface is enabled.
Modem status: shows when the port is registered to the operator's network.
Firmware version: shows the firmware version of the WWAN module
IMEI: the International Mobile Equipment Identity number of the module.
IMSI: the primary identifier of the subscriber (stored on the SIM card).
ICCID: the identifier of the inserted SIM card (chip).
Temperature: the current temperature of the modem module

Link type: shows the type of network: GPRS, EDGE, UMTS, HSPA and LTE.
Signal level: shows the received signal level in RSSI and dBm format.
Channel: shows the used channel number.
Frequency (down/up): receiver's (down) and the transmitter's (up) frequency.
Band: the current frequency band used
Designation: the designation of the current frequency band.

Network: name of the mobile network in use. Shows (home) when on home net
APN: the configured name of the Access Point.
PPP status: status of the data connection.
Link uptime: the elapsed time since last (re)connect.

Cell information

Depending on the type of network used, information is shown on the serving cell (the actual used cell). In 2G and 3G modes also the neighbour cells are shown.

Signal graph

The signal level screen shows a bar graph of the current signal level (Time 0) and the levels of the past 90 seconds.
Note that the levels measured and shown are lagging the actual level at the antenna. When using the signal level information for optimising antenna location or direction, please allow for several seconds to pass to make sure that the actual level is shown.

Ethernet

The Ethernet statistic page shows the status of the physical interface port(s), the amount of data passed and the amount of errors and drops detected.

Interface: shows the system name of the physical Ethernet port.
Status: the status of the port. up/down, negotiated mode, auto negotiation/fixed.
Rx bytes: the amount of bytes received since last start-up or reset.
Rx packets: the amount of frames received since last start-up or reset.
Rx errors: the amount of errors encountered since last start-up or reset.
Rx drops: amount of receive frame drops since last start-up or reset.
Tx bytes: the amount of bytes transmitted since last start-up or reset.
Tx packets: the amount of frames received since last start-up or reset.
Tx errors: amount of transmit frame errors since last start-up or reset.
Tx drops: amount of transmit frame drops since last start-up or reset.

Click the “Clear” button to reset the counters.

Serial gateways

When one or both of the serial gateways are enabled, this page will show the status and statistics of the serial gateway and the individual information on the connected peers.

Totals

Bytes_rx: the amount of bytes received via the serial port.
Bytes_tx: the amount of bytes transmitted via the serial port.
Num_clients: the amount of connected clients.
Control_signals (RS232 only): Upper case when active, lower case when not.

Peer n

Uptime: Elapsed time since last established connection.
Address: Address of the connected peer.
Port: Src port of the connected peer.
Bytes_rx: the amount of bytes received from this peer.
Bytes_tx: the amount of bytes transmitted to this peer.

Routing table

This page shows the current routing and interfaces table as used by the system.

Destination: the destination network (‘default’ for 0.0.0.0/0)
Via: the gateway via which the destination is reached.
Device/interface: the IP interface name as used by the system.
Scope: the scope of this interface.
Source: the source address of this interface.
Proto: the routing protocol ID. Shows which process added the route.

ARP table

This page shows the current ARP table as used by the system.

IP address: the IP address of the ARP entry.
MAC address: the hardware (MAC) address of the ARP entry.
Device: the IP interface where the device is found.
State: the state of the entry: Reachable or Stale.

DHCP leases

This page shows the current DHCP table as used by the system.

Interface: the LAN-bridge from which the address is assigned.
Type: the type of assignment, dynamic or static.
MAC address: the MAC address of the configured host.
IP address: the IP address assigned to the configured host.
Host name: the network name of the configured host.
Expires in: shows when this lease will expire.

Note: the list will show the entries of the devices that have done a DHCP request since the last reboot of this unit. Devices that already received a valid address before the last reboot will not do a request again and will not be shown in this list.

Logged-in users

This page shows the users that are currently logged-in. Each entry contains the user name, the used access service, the time of login and the IP address, if applicable, from which the connection is made.

RSA-series web configuration guide
Issue 1.10
July 2018

MuLogic B.V.
Plesmanstraat 58D
3905KZ, Veenendaal, The Netherlands