MULOGIC

RSA-SERIES

INDUSTRIAL REMOTE ACCESS ROUTER

RSA-series web configuration guide
Issue 2.05
April 2025

MuLogic BV
Plesmanstraat 62
3905KZ, Veenendaal, The Netherlands

RSA-Series Industrial Remote Access Routers

About this user guide

This user guide applies to all models of the RSA-M1, RSA-M2 and RSA-M4 series. See page 9 for an overview of the various models.

The features and settings as described in this user guide reflect software version 2.2.16 and onwards for the RSA-M1 and RSA-M2 models and version 1.0.2 and onwards for the RSA-M4 models.
Some features may not be present in previous software versions.

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 upon 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 2.05 (April 2025)

Contents

About this user guide 1
Use of open source software 1
Contents 1

Introduction 9
Supported models in this user guide 9

Login 11
Introduction 11
Configuration and management 11
Default settings 11
First time Login 11
Inactivity timeout 12
Logout 12
Device Info page 12

Setup 13
Eth ports 13
Port mirror 13
Access control MAC authentication 13
RADIUS (for MAC authentication) 14
LAN/WAN convention 15
LAN connections 15
WAN connections 15
LAN setup 16
Ethernet port physical setup 17
VLAN setup 17
DSL interface setup 18
DSL Physical setup 18
DSL interface 18
PPPoA to PPPoE 20
DSL Physical setup 21
Wireless WAN interface setup 21
Wireless WAN interface 21
SIM1/2 settings 22
Dual SIM failover 24
SIM1/2 failover criteria 24
Physical port settings 24
Ethernet WAN interface setup 25
Ethernet port physical setup 25
Ethernet WAN functional setup. 25
WAN failover setup 27
Connect on demand (WWAN port only) 28
Firewall setup 29
Custom firewall rules 29
Incoming filter 29
Shortcuts 29
Incoming filter rules 30
Forwarding filter 32
IP Filtering (forwarding) 32
Forwarding filter rules 32
MAC filtering 33
New MAC address alerting 34
Rate limiting 34
NAT Setup 35
Static NAT 35

Example ... 36
Dynamic NAT ... 36
Routing Setup ... 37
Default Gateway ... 37
Static route ... 37
Rip - Global ... 38
RIP - Keys ... 38
RIP - interfaces ... 38
OSPF - Global ... 39
OSPF - Keys ... 39
OSPF - interfaces ... 39
BGP - Global ... 40
BGP - Networks ... 40
BGP - Neighbors ... 40
DNS Setup ... 41
DNS Server ... 41
DNS Relay ... 41
VPN Tunnels ... 42
IPsec ... 42
Global IPsec settings ... 43
IPsec tunnel connection profile ... 44
OpenVPN ... 51
GRE tunnels ... 54
GRE over IPsec ... 55
Serial Gateway setup ... 56
Serial ports Physical setup ... 56
RS-232/RS485 port ... 56
Serial ports Physical setup ... 57
Physical ports ... 58
DSL Phy Setup ... 58
SFP Setup ... 59
Ethernet PHY Setup ... 59
Serial Ports Setup ... 61
USB Power Setup ... 62
WWAN ... 62
IO ... 63
Advanced ... 64
Scripts ... 64
Script registers ... 64

Tools ... 65
Network ... 65
DSL ... 65
Serial CLI ... 66
Terminal ... 66

Management ... 67
System ID ... 67
System identification ... 67
User accounts (Local authentication) ... 68
Remote (external) Authentication ... 69
RADIUS ... 69
TACACS+ ... 70
Password ... 70
Certs and keys ... 71
Local certs ... 71
Import Certificate ... 71
Generate CSR ... 72
Remote certs ... 73
CA certs ... 73
SSH keys ... 74
OpenVPN keys ... 74

Access services 75
HTTP server 75
SNMP 75
Shell access 76
TR-069 77
SMS 79
System time 80
Date and time 80
Temperature 80
Alert messaging 81
Alert rules 81
Recipients 81
Test alerts 81
History 81
System log 82
System log 82
Settings 82
Raw file 82
Accounting 83
Settings 83
Raw file 83
Account log download 83
WWAN data usage 84
Watchdog 84
Network connection 84
Internal SNMP server 84
DSL connection 85
Internal HTTP server 85
Task scheduler 85
Tasks 85
Settings management 86
View/backup configuration incl. private info 86
View/backup configuration excl. private info 86
Load configuration file 86
Load custom defaults configuration file 86
Copy current configuration to custom defaults 86
Restore settings to custom defaults 87
Restore settings to factory defaults 87
Load custom settings from USB flash drive 87
Settings update invoked by SNMP and CWMP 87
Changing individual parameters 87
Firmware update 88
Update system firmware 88
Update from local file 88
Update from remote server 88
Reboot 88

Device info 89
Summary 89
WAN interfaces 89
Details 89
IPsec tunnels 90
Details 90
OpenVPN tunnels 91
Details 91
DSL 92
Statistics 92
Graph 93
ATM/PTM 93
WWAN 94
Status 94
Signal graph 94

Ethernet 95
SFP 95
USB 95
Serial gateways 95
Routing table 96
ARP table 96
DHCP leases 96
Logged-in users 96

1 Introduction

This user guide describes the Web Based Configuration of the RSA-series of DSL and WWAN routers. Hardware details can be found in the “RSA-series hardware and start-up guide”.

Supported models in this user guide

Series Models	Eth ports	SFP port	ADSL2+	VDSL2	RS232 port	RS485 port	USB ports	2G WWAN	3G WWAN	4G WWAN	Dual SIM
RSA-M1 (Obsolete)											
RSA-1120D	1	-	✓	-	✓	✓	-	-	-	-	-
RSA-1020D	1	-	-	-	✓	✓	-	✓	✓	–	-
RSA-1120M	1	-	✓	-	✓	✓	-	-	-	-	-
RSA-1120W4	1	-	✓	-	✓	✓	-	✓	✓	✓	-
RSA-4122	4	-	✓	-	✓	✓	2 x USB2.0	-	-	-	-
RSA-4122W(3)	4	-	✓	-	✓	✓	2 x USB2.0	✓	✓	–	-
RSA-4122W4	4	-	✓	-	✓	✓	2 x USB2.0	✓	✓	✓	-
RSA-M2											
RSA-1220D	1	-	✓	-	✓	✓	-	-	-	-	-
RSA-1020DW4	1	-	-	-	✓	✓	-	✓	✓	✓	-
RSA-1220M	1	-	✓	✓	✓	✓	-	-	-	-	-
RSA-1220W4	1	-	✓	✓	✓	✓	-	✓	✓	✓	-
RSA-4222	4	-	✓	✓	✓	✓	2 x USB2.0	-	-	-	-
RSA-4222W4	4	-	✓	✓	✓	✓	2 x USB2.0	✓	✓	✓	(✓)*
RSA-4222WU	4	-	✓	✓	✓	✓	2 x USB2.0	-	-	LTE450	(✓)*
RSA-M4											
RSA-4422	4	-	✓	✓	✓	✓	2 x USB3.0	-	-	-	-
RSA-4422W4	4	-	✓	✓	✓	✓	2 x USB3.0	✓	✓	✓	✓
RSA-4422WU	4	-	✓	✓	✓	✓	2 x USB3.0	-	-	LTE450	✓
RSA-5422	5	-	✓	✓	✓	✓	2 x USB3.0	-	-	-	-
RSA-5422W4	5	-	✓	✓	✓	✓	2 x USB3.0	✓	✓	✓	✓
RSA-5422WU	5	-	✓	✓	✓	✓	2 x USB3.0	-	-	LTE450	✓
RSA-6422	4	✓	✓	✓	✓	✓	2 x USB3.0	-	-	-	-
RSA-6422W4	4	✓	✓	✓	✓	✓	2 x USB3.0	✓	✓	✓	✓
RSA-6422WU	4	✓	✓	✓	✓	✓	2 x USB3.0	-	-	LTE450	✓

Note: All RSA-4222W4 and RSA-4222WU units supplied after July 2024 are dual SIM versions. The RSA-4222WD4 and RSA-4222WDU type indications have become obsolete.

2 Login

Introduction

Configuration and management

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

- Web browser and settings-database access (HTTP or HTTPS).
- Command line interface (SSH, Telnet or RS-232 port).
- TR-069 CWMP.
- SNMP (v1/2 and v3)
- SMS (WWAN versions only)

For details on device management, contact MuLogic or your local sales representative.

Default settings

The unit is shipped with the following factory default settings:

- LAN IP address: **192.168.1.1**
- User name: **admin**
- Password: **rsa-admin**

Factory default settings

To reset the unit to its original factory default settings, power on the unit and wait at least 60 seconds. Then press and hold the reset button for more than 5 seconds until the PWR, DSL, PPP and VPN LEDs start blinking. Then release the reset button. The unit will restart within 15 seconds.

Custom default settings

When custom default settings are present (see Settings Management on page 80 and onwards), the procedure as described above will force a reset to the custom default settings. To force factory default settings, wait at least 60 seconds after power on and then press and hold the reset button for more than 30 seconds. The unit will restart within 15 seconds.

First time Login

The web interface allows you to set up, modify and view settings 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*

- 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.

Note: *Change the password **immediately** upon first configuration in case the unit will be connected to the public internet.*

Inactivity timeout

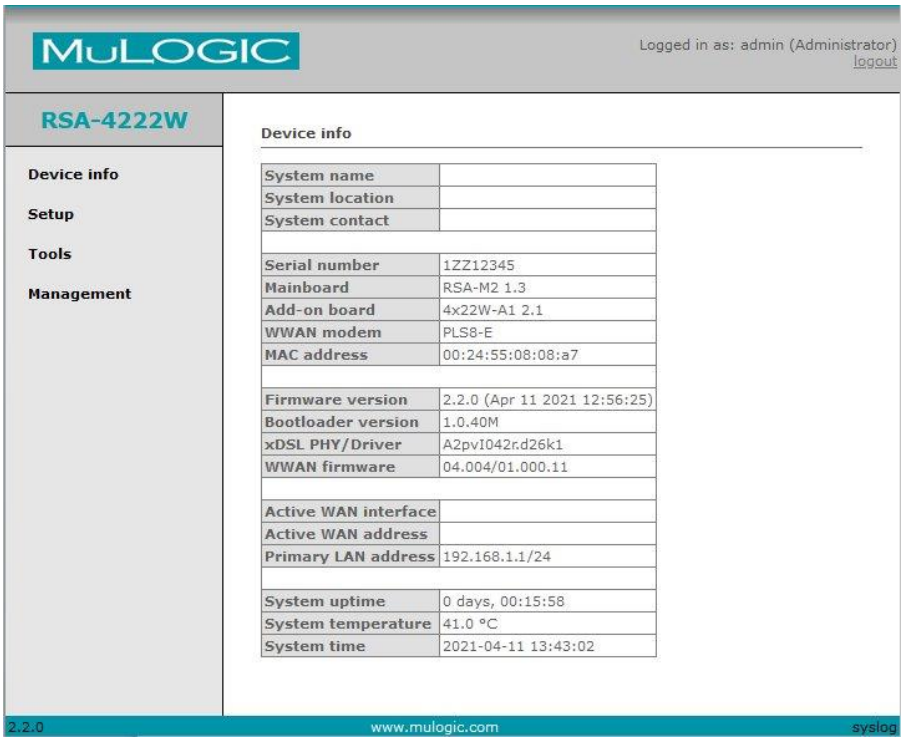
After a certain amount time of no activity via the web interface, you will be logged off automatically. The inactivity timeout can be set at **Management>Access control>Services**.

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**.
Serial number	The serial number of the unit.
Main board	Type and hardware revision of the main board.
Add-on board	Type and hardware revision of add-on board.
WWAN modem	Type of WWAN modem (if present)
MAC address	Base MAC address of the unit.
Firmware version	Firmware version and firmware build date.
Boot loader version[1]	Boot loader software version.
xDSL PHY/Driver	Version of the xDSL PHY and driver currently used.
WWAN firmware	Firmware version of WWAN modem (if present).
Active WAN address	IP address of the currently active WAN interface.
Primary LAN address	IP address of the primary LAN interface.
System uptime	Elapsed time since last start or restart.
Power usage[2]	Current power consumed by the system.
System temperature	Current internal temperature of the system.
System time	Actual time as used by the system.

Note 1. RSA-M1/M2 models only.
Note 2. RSA-M4 models only.

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 defines 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.

A total of 6 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 are part of the same LAN.

Port mirror

For testing purposes, the traffic over one or more Ethernet ports (mirrored ports) can be copied to another Ethernet port (mirror port). Select the Mirror port and one or more Mirrored ports. The ingress and egress can be selected separately.

Access control MAC authentication

The MAC Authentication feature uses 802.1X MAB (MAC Authentication Bypass) for Network Access Control. It facilitates devices without 802.1X support by using an external RADIUS server for authentication based on the device's MAC address.

Ports

All available Ethernet ports (including configured VLANs) are shown here.
MAC authentication can be enabled for each individual port by ticking the check mark and the 'Apply/Save' button.

Force authorized

The Force authorized option can be used for checking RADIUS acceptance of the network device without actually blocking access. This can be especially useful on models of the RSA-series with a single Ethernet port.
RADIUS acceptance can be verified in the System log or on the **Device info> Logged-in users** page. The shown state should be 'accept', which indicates that access will be granted also when Force authorized is disabled. When the state shows 'force_auth' or the System log indicates 'rejected' then this MAC address will be blocked when the Force authorized option is disabled.

MAC group size, separator and case.

By default the MAC address of the attached device will be sent to the RADUIS server as both username and password in a format like 00:24:55:aa:22:ff, that is: groups of 2, separated by a colon : and with lower case characters.
Other formatting (both username and password) can be selected by changing the group size, separator type and case. Note that for a group size of 12 the separator type is not relevant.

Password type

Selects either the MAC address or a specified string to be sent as password. By default, the MAC address of the device is sent as both username and password to the RADUIS server. In case the server does not allow username and password to be the same, or enforces a more complex password, a dedicated password can be specified.

Re-authentication period

The value (in seconds) entered here, specifies the time before a MAC address is re-authenticated. Very short times are not recommended, except for testing purposes. Upon expiry of the re-authentication period, a new RADIUS request is made for the device's MAC address.
A value of 0 disables re-authentication. Accepted addresses will remain having access until reboot or a disable/enable action of the MAC authentication feature.

RADIUS (for MAC authentication)

Primary Server address

Specifies the IP address of the primary RADIUS server.

Server UDP port

Specifies the port number of the server. The default is 1812.

Primary Server secret

Specifies the password for access to the primary RADIUS server

Secondary Server address

Specifies the IP address of the secondary RADIUS server.

Secondary Server secret

Specifies the password for access to the secondary RADIUS server.

Secondary Server UDP port

Specifies the port number of the server. The default is 1812.

Retries

Specifies the number of retry attempts for contacting RADIUS servers.

Note: *An alternative to 802.1X MAC authentication is the use of the MAC filtering feature. See Setup>Firewall>MAC filtering*

LAN/WAN convention

Although there is no strict distinction between LAN and WAN networks, on the RSA-series there is a presumed difference between 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 6 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, SFP or DSL port) and can receive an IP address and other network information from the operator by means of DHCP or PPPoE or PPPoA.

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 to the new LAN address.*

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

LAN: LAN1-LAN6

Address: Enter the IP address/prefix length (CIDR notation) like **192.168.1.1/24** where "/24" corresponds to a netmask of 255.255.255.0
Click "Apply/Save" to activate and store the setting.

Interface: 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/DHCP Relay Agent

Each LAN has a dedicated DHCP server or Relay Agent. In "DHCP Server" mode, enter the IP address range, lease time and (optional) domain name.

In "DHCP Relay Agent" mode, select the interface towards the remote DHCP server and the IP address(es) of the DHCP server(s) in case these servers are connected via a unicast network. The format of the Server address is <ip address>[:port number] (the port number is optional).
Enable the option "Source address = Gateway IP address" to use the LAN interface address (giaddr) as source address for the packets sent to the remote DHCP server(s). Click "Apply/Save" to activate and store the settings.

Check for DHCP server conflict (DHCP Server)

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 (DHCP Server)

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.

Ethernet port physical setup

The physical parameters of the Ethernet ports, such as Auto-MDIX, bit rate, and half/full duplex operation, are set at **Setup>Physical ports>Ethernet**.

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.

Interface

The 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 xDSL mode and POTS/ISDN overlay is done at **Setup>Physical ports>DSL**.

Note: *For ADSL operation make sure that the correct PHY version (Annex A or Annex B) is selected. For VDSL2 operation both PHY versions can be used. See* ***Device info>summary*** *page to check which xDSL PHY version is in use. The Annex A PHY versions will start with "A", the Annex B versions with "B".*

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". The name entered here is shown in the SNMP ifXtable 'ifAlias' object entry.

Port ID

This field is generated automatically and shows the ID of the port as used in the internal configuration database.

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 provided by the ISP.

VLAN

Enable VLAN and enter the VLAN ID in case a VLAN ID is provided by the ISP. (Usually for PPPoE over VLAN).

VLAN auto-detect

When enabled, both PPPoE over the configured VLAN ID and without VLAN will be tried. Note that this detection process may take up to several minutes. Once connection is established, the correct setting under VLAN will be stored. When a VLAN ID is set and VLAN auto-detect is enabled, the first connection attempt will be with VLAN. When VLAN is not checked, the first connection attempt will be without VLAN.

Link type

The link type (like PPPoE, PPPoA or other), as provided by the ISP is selected here.

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.

Negotiate MTU 1500

When enabled, RFC4638 MTU negotiation will be conducted over PPPoE links to increase the link MTU to from 1500 to 1508 and the PPPoE MTU from 1492 to 1500.

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

Wireless WAN operation (WWAN) is supported by units with an internal WWAN modem or an external (MuLogic) WWAN modem connected with one of the USB ports. The following setup parameters apply to both internal and external (MuLogic) WWAN modems.

Note: *The parameters of the physical connection of the WWAN modem, such as Radio Access Type (2G/3G/4G/5G) and frequency band selection, are set on the* ***Setup>Physical ports>WWAN*** *page.*

Wireless WAN interface

Name

Optionally a name can be given to the WWAN entry. WWAN names can be used for reference but are not relevant for the configuration. The name entered here is shown in the SNMP ifXtable 'ifAlias' object entry.

The default name for the internal WWAN modem is "WWAN 1". The default names of the external WWAN modems are "WWAN Ext 1" and "WWAN Ext 2".

Port ID

This field is generated automatically and shows the ID of the port as used in the internal configuration database.

Registration state

This field is generated automatically and shows the state of the Network registration. When the state is "Registered", SMS text messages can be sent and a data link can be established to create an IP interface.

Interface state

This field is generated automatically and shows the state of the data (IP) interface. When the state is "Connected" also the assigned IP address is shown here.

Enable

Click the checkbox to fully enable the WWAN port. When disabled, the WWAN modem will not be registered on the mobile network and cannot send SMS messages. It is advised to not keep the WWAN port enabled when no SIM card is inserted. When not used, leave the WWAN modem disabled.

Data mode

- When the modem is enabled and the Data mode is “Off”, it will register on the mobile network and SMS messages can be sent but no IP interface will be established.
- When the Data mode is “Always on” an IP interface will be created directly upon connection with the mobile network. Make sure to enter the correct APN.
- When Data mode is set to “On demand”, an IP data connection will only be activated when the WWAN port is serving the highest priority WAN interface. (see **Setup>WAN Failover**). This avoids unexpected mobile data usage.

Enable Dual SIM (dual SIM models only)

This option is present for Dual SIM models. When enabled, configuration parameters for both SIM1 and SIM2 are shown.

Default SIM (dual SIM models only)

When SIM failover is not enabled, the Default SIM setting is used for manually selecting the SIM card to be used. When SIM failover is enabled, this setting determines which of the two SIM cards is selected initially on power-up.

SIM1/2 settings

APN

Enter the Access Point Name (APN) as provided by the mobile network operator for the used SIM card.

Operator selection

When set to Automatic, the operator is selected according to the information on the SIM card. When set to Manual, a specific operator can be chosen by means of the (numerical) PLMN code. This feature can be used in combination with “Global SIM cards” that allow registration with multiple operators.

SIM 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 the correct SIM PIN. When a wrong PIN is issued, no further action is taken until the next restart of the WWAN interface.*
After 3 restarts with the wrong PIN, the SIM needs be unlocked by means of the PUK code.

Authentication

If needed, select the type of authentication (PAP, CHAP or None). In most cases this setting can remain at “PAP”.

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”.
Note: When PAP or CHAP authentication is selected, you must add an entry here, even when no authentication is required.

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.

Note: *When PAP or CHAP authentication is selected, you must add an entry here, even when no authentication is required.*

MTU

The default MTU value of the WWAN IP interface is 1500. The MTU can be manually reduced down to a value of 576.

MTU Negotiation

When enabled, the MTU automatically adjusts to the value provided by the WWAN operator.

Note: *If a manually configured MTU is set to a value lower than the one negotiated with the operator, the system will use the lower, manually specified value.*

Dual SIM failover

The Dual SIM models offer automatic failover from SIM1 to SIM2 and vice versa.

Enable

Click the ‘Enable’ checkmark to show and select the failover settings.

SIM1/2 failover criteria

Return to SIM1/2

This option sets the timeout for returning to the other SIM, regardless of the other criteria.

Data connection

When enabled, failover to the other SIM is started when the mobile data link is lost for longer than the time specified at “Timeout”.

Signal level (RSSI)

When enabled, failover to the other SIM is started when the signal level (RSSI) remains below the specified level for longer than the time specified at “Timeout”.

Ping response

When enabled, failover to the other SIM is started when no response is received to ICMP (ping) messages to the specified IP address for longer than the time specified at “Timeout”.

Data limit reached

When enabled, failover to the other SIM is started when the data limit as set in **Management>WWAN data usage** is reached.

Physical port settings

The setup of the parameters of the physical connection parameters of the internal WWAN modem such as wireless radio access type (2G/3G/4G/5G) and frequency band selection is made at **Setup>Physical ports>WWAN**.

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 media converter. 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 10/100BASE-T, 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”. The name entered here is shown in the SNMP ifXtable ‘ifAlias’ object entry.

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: *Be careful to not accidentally disable the active WAN interface while being connected from a remote location via this very interface.*

Priority

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.

Port ID

This field is generated automatically and shows the ID of the port as used in the internal configuration database.

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.

Ping address 1, Ping address 2

Enter the addresses to be used for checking the condition the WAN interface.

Note: *Make sure that the IP addresses to be pinged can be reached over the WAN port. If none of the entered address can be reached, or if no addresses are entered, no failover will take place.*

Connect on demand (WWAN port only)

When the Data mode ‘On demand’ is selected in the WWAN setup menu, a WWAN data connection will only be made when the WWAN port serves the active (highest available priority) WAN interface. Using the “On Demand” mode can avoid unwanted costs for mobile data usage. Note that, when this option is selected, it will take extra time before the WWAN data connection becomes active.

Firewall setup

The firewall options offered by the web interface are used for:

- Controlling access to the unit itself for management access, VPN tunnels and other system services like serial gateways. This is done by means of the “Incoming filter rules”.
- Controlling all traffic to be forwarded through the router. This is done by means of the “Forwarding filter rules”.

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 several firewall and NAT features are supported by the system, it may be necessary to add custom firewall (iptables) or traffic control (tc) rules in special situations. Such rules can be added by means of creating a shell script (named ‘firewall.post’) that is executed by the system upon start-up and each time the firewall is reconfigured. This feature requires knowledge of writing Linux shell scripts, and creating ‘tc’ and ‘iptables’ rules. The script can be written and edited under **Setup>Advanced>Scripts** in ‘Firewall post’. Contact MuLogic or your local sales representative for details or technical support for writing scripts.

Incoming filter

Enable incoming 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 (see below) and the incoming filter rules do not apply. The shortcuts will become active after clicking ‘Apply/Save’ at the bottom of the page.

Warning: *for reasons of security it is advised to* ***not*** *have incoming IP filtering disabled. This feature is intended only for testing purposes.*

Shortcuts

In order to allow for rapid testing without setting firewall rules first, some “shortcuts” are made and enabled by default.

Warning: *for reasons of security it is advised to* ***not*** *use these shortcuts in the final setup. 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, OpenVPN or GRE tunnels is allowed except for those addresses for which ‘drop’ rules are made. Note that this shortcut is based on interface and protocol types. It is advised to make more granular access restrictions based on IP address or network.

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.

Incoming filter rules

Incoming Filter rules can be made to either accept or to specifically deny (drop) incoming packets from certain addresses. The drop rules have priority over the Shortcuts and Accept rules 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 select ANY for any protocol.

Source address

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

Source 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.

Destination address

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 via a specific WAN interface.

Destination 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

Priority

For ease of configuration the order of the firewall (iptables) rules is determined automatically by the system. However, there may be cases where one specific rule needs priority over another rule. The rule with the higher priority number is executed before a rule with a lower priority number. If not used, the priority numbers can remain at 0.

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
Source address: 212.124.53.16/32
Source port: 0
Destination address: 0.0.0.0/0
Destination port: 23

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

Forwarding filter

Forwarding filtering rules can be added to control the IP traffic that passes through the router.

IP Filtering (forwarding)

Enable forwarding IP filtering

Forwarding filtering is disabled by default. When enabled without additional accept rules, no data will pass through the router regardless of passing via NAT routing, port forwarding, VPN tunnels or straight IP routing.

Forwarding filter rules

Forwarding filter rules can be made to either accept or to specifically deny (drop) packets from passing through the router. The drop rules have priority over the accept rules but will not be active when IP forwarding filtering is disabled.

Note: *a forwarding filter rule must be made for the direction from which the IP connection is set up. The firewall will be opened automatically for the (related) return traffic.*

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

Protocol

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

Source address

Enter the address or network as IP address/prefix size for the traffic source.

Source port

This entry can usually be left at “0” unless you want to control access for specific source port numbers.

Input interface

Select a specific input interface or all interfaces.

Destination address

Enter the address or network as IP address/prefix size for the traffic destination.

Destination port

This entry can usually be left at “0” unless you want to control access for specific destination port numbers.

Output interface

Select a specific output interface or all interfaces.

Priority

For ease of configuration the order of the firewall (iptables) rules is determined automatically by the system. However, there may be cases where one specific rule needs priority over another rule. The rule with the higher priority number is executed before a rule with a lower priority number. If not used, the priority numbers can remain at 0.

Examples

1. Access from a unit in the local LAN (192.168.1.12) to a remote host at port 22 (SSH) only:

   Name: SSH access host1
   Enable: ✓
   Action: Accept
   Protocol: TCP
   Source address: 192.168.1.12/32
   Source port: 0
   Destination address: 212.124.53.16/32
   Destination port: 22

2. Access from all units in the local LAN (192.168.1.0/24) to all ports of a single remote host and allowing all IP protocols:

   Name: Access to host1
   Enable: ✓
   Action: Accept
   Protocol: All
   Source address: 192.168.1.0/24
   Destination address: 212.124.53.16/32

MAC filtering

MAC address filtering adds an extra layer of protection for access from devices connected to the local LAN ports. MAC addresses are automatically stored and added to the MAC address table (ARP table) when a LAN device interacts with the router. Devices can also be manually added to the table. When MAC address filtering is enabled, newly added devices (either manually or automatically) must first be granted access before they can pass data to or via the router.

Enable MAC address filtering

This option globally enables or disables MAC address filtering. To enable the filter, add the checkmark and click “Apply/Save” to active and store the setting. Note that addresses remain to be stored and added to the table also when MAC address filtering is disabled. Entries can be edited by means of the “Edit” button. The ‘Name’ field of the table is automatically written when a device name is discovered from a DHCP request.

Allow checkmark

Set the “Allow” checkmark to grant access to a device.

Note: *When configuring the router via a local LAN port, make sure to first set your device’s MAC address to “allow” before to enable MAC address filtering.*

Remove checkmark

Devices can be removed from the table by setting the “Remove” checkmark and clicking the “Remove” button at the bottom of the table.

Add Device

Click this button the manually add a device. Enter the MAC address and IP address and the device name (optionally). Click the “Allow” checkmark to directly grant access from the device. Click “Apply/Save” to activate and store the setting.

New MAC address alerting

Apart from MAC address filtering, an alert can be sent when a new MAC address is seen on the Ethernet ports. See page 77 for setting the alerts.

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, All, or Other. When All is selected, all packets will be forwarded, no matter the protocol. When Other is selected the protocol number needs to be entered.

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 are equal to those used for the unit's access services, the ports of these access services will have to be relocated to other port numbers. The default port numbers for the access services are: SSH: 22, Telnet: 23, HTTP: 80, HTTP: 443, SNMP: 161*

Dynamic NAT

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

Dynamic NAT can be disabled to prevent local devices from having direct internet access, for example when connections are to be restricted via a VPN tunnel.

Note: *Dynamic NAT must be disabled in case devices at the LAN ports are to be connected via IP routing (static routes or via routing protocol).*

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.

Wan interfaces

To enable individual WAN interfaces for Dynamic NAT, click the edit button and enable/disable the WAN interfaces. By default, all WAN interfaces are enabled for Dynamic NAT.

Click Apply/Save to store the settings.

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 are 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 type

The gateway can be indicated by IP address or the interface (device) that acts as gateway. When the ‘Gateway type’ is ‘IP address’, enter the IP address of the gateway in the ‘Gateway address’ field below. When ‘Gateway type’ is ‘Interface (list)’, you can select one of the gateway interfaces in the field below. When ‘Gateway type’ is ‘Interface ’, you must enter the name of the interface in the ‘Network interface’ field below. The names of the various interfaces can be found on the **Device info>Routing table** page in the table of IP interfaces.

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 or tunnel towards the other RIP router.
Select “Passive” for interfaces of which the routes are to be advertised but do not need to send routing updates to a neighbour RIP router.

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.

Enable

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

Mode

Select “Active” for interfaces that are used for advertising routes to neighbour OSPF routers, such as the WAN interface or GRE tunnel towards the neighbour router.
Select “Passive” for interfaces of which the routes are to be advertised but do not need to establish adjacencies or send routing updates.

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.

BGP - 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.

BGP - Neighbors

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

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 enter 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, the addresses of these DNS servers are automatically assigned during connection establishment with the ISP.

When ‘Manual’ is selected, the entered DNS addresses are used.

DNS Relay

When DNS relay is enabled, the unit can serve as DNS server for local LAN devices. DNS requests from the LAN will automatically be forwarded to one of the DNS servers assigned during WAN setup or one of the servers entered for mode "Manual".

VPN Tunnels

Three types of VPN tunnels are supported: IPsec, OpenVPN and GRE.

IPsec can be used between two RSA-units and between an RSA-unit and central site security appliances. IPsec is the de-facto standard for encrypted VPN tunnels and is supported by many devices.

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 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. GRE can be used for the transfer of multicast or broadcast packets or for transporting Layer2 (Ethernet) data transparently. If a secure and encrypted tunnel is required, GRE can run over IPsec.

IPsec

For IPsec, two key exchange protocols are available: IKEv1 and IKEv2.

IKEv1 is still often used as key exchange method but should be considered deprecated. It is being replaced with IKEv2.

IKEv2 has several advantages over IKEv1 such as being less bandwidth consuming, less interoperability issues and offers the option of having multiple sets of networks in a single exchange (note that this feature may not be supported by IKEv2 peer devices from other manufacturers).

A single IKEv1 IPsec tunnel supports only one pair of local and remote networks at each end of the tunnel. To add multiple pairs of subnets between the same peers, use the “Clone” button in the profile overview to copy the same Phase1/IKE-SA settings in a new profile and then change the local and/or remote network (traffic selector). This method can also be used in IKEv2 mode, should the remote peer not support multiple subnets in one IPsec/Child SA.

With the introduction of software version 2.2, both **policy-based IPsec** and **route-based IPsec** are supported.

Policy-based IPsec is the standard operating mode as described in RFC 6071. The traffic to be processed for an IPsec tunnel is based on a “security policy”, rather than the routing table. The regular routing table is ignored.
The security policies describe what local and remote networks or addresses can communicate via the IPsec tunnel. Policies have priority over routes.

Route-based IPsec is made possible by adding a virtual “xfrm” interface to act as end-point of the tunnel. This end-point can be given an IP address over which traffic can be directed via the routing table or a routing daemon. An xfrm interface can be created at both ends of the tunnel, or at one end while the other side remains in policy based mode.

GRE over IPsec: Routable IPsec interfaces can also be created by means of a GRE tunnel over an IPsec tunnel. Note that GRE interfaces need to be configured for both end-points.

Global IPsec settings

The global settings apply to all tunnels that are created. In the majority of cases these settings do not need to be changed.

NAT KeepAlive Interval

The NAT KeepAlive Interval determines how often "keepalive" packets are sent when the IPsec tunnel is in NAT traversal (NAT-T) mode. The default value is 20 seconds.

Install routes for local unit

The "install routes for local unit" option is for making sure that the unit's local LAN addresses are used as source address for reaching the remote ends of IPsec tunnels. This option can be disabled in case it conflicts with other settings, for example when the remote traffic selector is 0.0.0.0/0.
This feature is not relevant when in route-based IPsec mode.

IKEv2 reauth make before break

IKEv2 reauth "make before break" can be enabled to prevent data loss during the re-authentication of the IKE SA in IKEv2 mode. When enabled, on IKE re-authentication new Child (IPsec) SAs are created before the old ones are terminated. Note that this option may not be supported by IPsec peers from other manufacturers.

Ignore routing tables (policy-based IPsec)

The "Ignore routing tables" field is used for preventing local address lookup conflicts when, apart from the main routing table, other routing tables are present on the system. Table numbers must be entered space-separated.
This feature is not relevant when in route-based IPsec mode.

Exclude networks (policy-based IPsec)

The "Exclude networks" option is used for excluding local networks from IPsec processing. For example, in case of 0.0.0.0/0 as remote traffic selector in policy-based IPsec mode, the local LAN should be entered here to prevent the unit's local LAN address from being unreachable from the LAN as soon as the tunnel is installed. Multiple networks can be entered by clicking the + button.
This feature is not relevant when in route-based IPsec mode.

IPsec tunnel connection profile

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 and for adding multiple subnets between the same peers in IKEv1 mode.

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

This part of the IPsec setup defines the authentication between the peers of an IPsec tunnel. In IKEv1 mode this phase is referred to as “Phase1”, in IKEv2 mode it is called “the IKE-SA”.

Connection mode

Three connection modes can be selected: Active, Passive or Anonymous.
In **Active** mode, this unit will act as initiator and actively try to connect to the Remote peer address. It will however also be able to act as responder.

In **Passive** mode, this unit will be responder only and will wait for incoming connections from the unit with the Remote peer address. Note that firewall incoming filter rules for UDP ports 500 and 4500 must be configured in order to accept the incoming connections from the remote initiator.

In **Anonymous** mode, this unit will be responder only but will accept incoming connections (with matching Phase 1 and Phase 2 parameters) from any address. In this mode the unit can be used as a concentrator for multiple VPN tunnels. Note that Anonymous mode can only be used with authentication by means of certificates. Also note that firewall incoming filter rules for UDP ports 500 and 4500 must be configured in order to accept the incoming connections from the remote initiator.

Remote peer address (Active and Passive connection mode)

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

In Active connection mode, multiple addresses for failover operation can be added by clicking at the + sign. Each address is tried for connection for a period of 30 seconds. If no connection is established, connection to the next address is attempted. The last established connection will remain until connection is lost.

Key exchange method

Three key exchange methods can be selected: **IKEv1**, **IKEv2** and **Manual**.

IKEv1 is still used as key exchange method but should be considered deprecated. It is 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 devices that do not support IKE and this 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 proper 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 in addition.

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

PSK (PSK authentication method)

Enter the pre shared key in the PSK field. It is advised to use strong passwords in order to minimise the risk of brute-force attacks.

Local Identifier

When required by the remote peer, select “Specify identifier” and enter the local identifier. Note that in IKEv2 PSK mode, only the local WAN address can be used as identifier.

Remote Identifier

When a specific remote identifier is required, select “Specify identifier” and enter the remote identifier. Note that in IKEv2 PSK mode, only the IP address of the remote WAN port can be used as identifier.

Local x.509 certificate (Certificate authentication method)

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 (Certificate authentication method)

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 (Certificate authentication method)

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

Exchange mode (IKEv1 Only)

The default exchange mode for IKEv1 is Main mode. The use of the Aggressive mode is deprecated and considered unsafe, 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.
Note that the 3DES algorithm is considered "broken" and should not be used.
The selected 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. Note that the MD5 and SHA1 algorithms are considered "broken" and should not be used. The integrity algorithm must be equal on both peers.

Phase1 Diffie-Hellman Group

Select one of the Phase 1 Diffie-Hellman Group.
Note that DH groups 1 and 2 are considered weak and should be avoided.
Also 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 selected DH group must be equal on both peers.

NAT-traversal (NAT-T)

As IPsec (ESP) data packets are fully encrypted, techniques like Dynamic NAT (IP masquerading) cannot be used because there are no readable ports to refer to. To solve this, 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 (for example on some mobile WWAN networks) it may be necessary to force NAT-T mode. When in NAT-T mode, keepalive messages are sent every 20 seconds (default setting) in order to prevent the state information of the NAT router from expiring. The NAT-T keepalive interval can be changed in the IPsec global settings.

Dead Peer Detection

Dead Peer Detection (DPD) is needed to detect if connection with a remote peer is lost. To detect if connection with the remote peer is still available, R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically 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)

In IKEv1 mode 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. The default value is 30 seconds. In IKEv2 mode the default retransmission timeout applies, as every exchange is used to detect dead peers.

MOBIKE (IKEv2 only)

When enabled, the MOBIKE (IKEv2 Mobility and Multi-homing 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. When MOBIKE is enabled at both ends then, after a WAN failover action, in general the IPsec tunnel will be re-established faster. However, complex WAN failover configurations may require MOBIKE to be disabled.
Note that the MOBIKE feature is not used when route-based IPsec is enabled.

Enable re-authentication (IKEv2 only)

In IKEv2, when disabled, the IKE SA will be re-keyed without uninstalling the Child SAs. When re-authentication is enabled, after expiry of the IKE lifetime a new IKE SA is created and all Child SAs will be recreated. This will cause short data interruptions every time the IKE lifetime expires.
The option “IKEv2 reauth make before break“ in the global settings can be enabled to create a new Child SA before the previous one is terminated. Note that this may not work towards peer devices from other manufacturers.

Phase 2 / Child-SA Setup

This part of the IPsec setup defines the actual IPsec tunnel(s) that are to be installed between the peers after successful authentication. In IKEv1 mode, this part is referred to as “Phase2”, in IKEv2 it is called “Child-SA”.

Two VPN types can be selected for the Phase2 (child-SA) setup:
- Policy-based IPsec (all tunnel end-points defined by IPsec policies)
- Route-based IPsec (one tunnel end-point created that can be used for routing)

Create local loopback interface (Policy-based VPN type)

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

Local Network / Traffic Selector (Policy-based VPN)

In **policy-based** IPsec mode, the traffic to be encrypted is determined entirely by the traffic selectors in the security policy data base. All packets with a matching source address will be encrypted regardless of entries in the IP routing table.
Enter the address or network for the (LAN) device(s) at the local end of the tunnel or a local address on the router itself. This can be a single address like 192.168.10.22/32 or a network like 192.168.10.0/24.

In IKEv2 mode, the greatest common network of the local and remote subnets will be negotiated. Note that in IKEv1 mode, when connected with IPsec peers from other manufacturers, this may not work and the subnets on both peers must be identical.

Entering 0.0.0.0/0 as local network must be done with caution, as it may cause routing issues when a remote (policy based) peer has 0.0.0.0/0 set as remote network. Use the “Exclude networks” option of the global IPsec settings in order to exclude the local LAN from the address range. See page 40.

In IKEv2 mode, multiple addresses/networks can be added by clicking at the + sign. In IKEv1 mode, adding multiple networks has no effect. Only the first entry will be used.

Local Interface address (Route-based VPN)

In **route-based** IPsec mode, the tunnel end-point (xfrm interface) can be given an IP address. This address is used as “gateway address” for routing traffic via the tunnel. Routes can also be set via the interface name (xfrm0, xfrm1, etc.).

In IKEv2 mode, multiple addresses/networks can be added by clicking at the + sign. In IKEv1 mode, adding multiple networks has no effect. Only the first entry will be used.

Remote Network / Traffic Selector (Policy-based VPN type)

In policy-based IPsec mode, the traffic to be decrypted is determined entirely by the traffic selectors in the security policy data base. All encrypted packets with a matching address will be delivered at the remote end of the tunnel.

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, the greatest common network of the local and remote subnets will be negotiated. Note that in IKEv1 mode this may not work in connection with IPsec peers from other manufacturers and the subnets on both peers must be identical.

Entering 0.0.0.0/0 as remote network must be avoided as it may cause connection issues should the remote peer have 0.0.0.0/0 set as local network. In case of the use of 0.0.0.0/0 as remote traffic selector (while the local traffic selector of a policy-based remote peer is also 0.0.0.0/0), the option “install routes for local unit” must be disabled in the global settings. In this case the local LAN must be entered at “Exclude networks” in the global IPsec settings or otherwise connection to the router from the local LAN will be lost as soon as the IPsec tunnel is installed.

For creating multiple networks between peers in IKEv1 mode, use the “clone” function to create additional profiles with the same IKE-SA settings and only different traffic selectors for the IPsec SAs.

In IKEv2 mode, multiple addresses/networks can be added by clicking at the + sign. In IKEv1 mode, adding multiple networks in this way has no effect and only the first entry will be used. Note that this feature may not be supported by remote IPsec peers from other manufacturers. In that case, use the “clone” function to create multiple IPsec SA pairs like in IKEv1 mode.

Remote Network (Route-based VPN)

In route-based IPsec mode, the routing table determines what traffic is routed via the tunnel. By entering the remote network here, a route-entry is created automatically. Routes can also be configured via **Setup>Routing>Static route**.

Local traffic selector (Route-based VPN)

In route-based IPsec mode, the default traffic selector can usually remain at 0.0.0.0/0 as only the traffic as determined by the routing table will pass through the tunnel. For a hub-spoke topology, this entry is used to give each spoke an individual address.

Remote traffic selector (Route-based VPN)

In route-based IPsec mode, the default traffic selector can usually remain at 0.0.0.0/0 as only the traffic as determined by the routing table will pass through the tunnel. For a hub-spoke topology, this entry is used to give each spoke an individual address.

XFRM interface ID (Route-based VPN)

For normal configurations the xfrm interface is assigned automatically and this field can be left empty. In route-based IPsec mode the tunnel end point is a local (IP) interface of the router. This interface (called 'xfrm interface') will act as the gateway for traffic destined for the tunnel. The xfrm interface ID field will be filled-in or updated automatically after clicking "Apply/Save". It can be changed manually if needed.

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.
When in IKEv2 mode with re-authentication enabled, new child SAs will be created when the IKE SA is rekeyed.

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. The use of PFS is strongly recommended.

Phase2 Diffie-Hellman Group (PFS enabled)

When PFS is enabled, select one of the Phase 2 Diffie-Hellman groups.
Note that DH groups 1, 2 and 3 are considered weak and should be avoided. Also 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 when two tunnels share the same or overlapping networks/traffic selectors. Traffic that matches multiple tunnels will pass through the (established/installed) tunnel with the highest priority (i.e. the lowest priority number). This option can be used for creating redundant IPsec tunnels. If the priority and networks/traffic selectors are the same, then traffic will pass through the last installed tunnel.
Leave at 0 when 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.

Custom config

When enabled, the tunnel configuration can be entered as text. This enables easy ´cut and paste´ from other (text based) OpenVPN configurations and the use of options that are not present in the graphical user interface.

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 or DNS name to connect to (in UDP and TCP client mode) or (in TCP server mode) to accept incoming tunnel connections from.
In TCP server mode, enter the address 0.0.0.0 or leave the field empty in order to accept incoming connections from all addresses. Access restriction in addition can be made by means of firewall Incoming Filter Rules.

In client modes, multiple addresses can be added for failover operation by clicking at the + sign. Each address is tried for connection for a period of 60 seconds. If no connection is established, connection to the next address is attempted. The last established connection will remain until connection is lost.

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 only Layer 3 packets are transported.

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 **Pre-shared secret** mode, a pre-shared key is shared between both OpenVPN peers before the tunnel is started.

- In **X.509 client** or **X.509 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,* only serves 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. Multiple addresses/networks can be added by clicking at the + sign.

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 often used in combination with IPsec tunnels to create a routable IP interface. GRE tunnels are especially useful for transporting multicast packets like OSPF and RIPv2.
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.

Interface

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.

Mode

Select “L2 bridged” or “L3 routed”. In L3 routed mode, an IP interface will be created as end-point of the tunnel. Traffic can be lead over the L3 tunnel by means of adding static routes (see “Remote network” below).
In L2 bridged mode, no IP interface will be made but a Layer 2 interface that can be assigned to one of the 6 internal LAN bridge interfaces (LAN1..LAN6).

Local interface address (Mode is L3 routed)

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.

LAN Bridge (Mode is L2 bridged)

Select one of the 4 LAN bridge interfaces to assign the L2 tunnel interface to.

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.

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. On a WAN link with an MTU of 1500, the maximum MTU in L3 mode is 1476. The maximum MTU in L2 mode is 1462. Note that the MTU size will have to be reduced when the GRE tunnel is created over another tunnel like IPsec. The recommended MTU for GRE over IPsec 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 “Create local loopback address “ on page 45).
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.

Note that the MTU size of the GRE tunnel will have to be reduced on order to fit the maximum MTU of the IPsec tunnel. The recommended MTU for GRE over IPsec is 1400.

Serial Gateway 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 is converted into UDP/IP packets and vice versa. 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.

When Modbus server mode is selected, the unit converts Modbus TCP packets at the network ports to Modbus RTU packets at the serial ports and vice versa.

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, Telnet server and Modbus 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 settings for the 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 for 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 of POTS, ISDN, or no telephony services.

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

Overlay mode: The overlay mode (Annex A or Annex B) is selected here.
On the RSA-M1/M2 models, the ‘Hardware preset’ option reflects the overlay mode as selected by the hardware or jumper setting on the main board.
See **Device info>summary** page to check which xDSL PHY version is in use.
The Annex A PHY versions will start with “A”, the Annex B versions with “B”.

Notes:
1. After changing the overlay mode the unit will reset and start again in the selected mode.
2. For VDSL2 operation, both Annex A and Annex B PHY versions can be used.

DSL mode

In the default settings all xDSL modes, except for ANSI-T1.413, 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 (except for ANSI-T1.413) 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.

SFP Setup

This page allows for manual setting of the type of SFP module in case it is not detected automatically.

SFP type

When not detected automatically, the SFP type can be selected manually.

SFP present LED

This setting selects the behaviour of the yellow “SFP present” LED.
The LED can be set to be On as soon as any SFP module is inserted, or blink when the module characteristics are not detected or when the module is not supported by the SFP port.

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.

Click the “Edit” button to enable/disable physical Ethernet ports, add or change the assigned name or change port settings.

Port

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

Name

Optionally a name can be given to a specific physical Ethernet port. These names are shown in the SNMP ifXtable ‘ifAlias’ object entry.

Enable

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

SPD LED 100BASE-T (RSA-M4 models only)

When enabled, the yellow “speed” LED will be On in case of a 100BASE-T or 1000BASE-T link.
When disabled, the LED will only be On in case of a 1000BASE-T link.

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: 10BASE-T Half Duplex 10BASE-T Full Duplex, 100BASE-Tx Half Duplex and 100BASE-Tx Full Duplex, and, for RSA-M4 models only, 1000BASE-Tx Half Duplex and 1000BASE-Tx Full Duplex .

Status

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

MAC address

This field is generated automatically and shows the hardware (MAC) 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.

Data rate

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. When an external WWAN modem is connected, the USB power can be used for resetting the WWAN modem.*

Power

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

Status

This field is generated automatically and shows the actual power status of the USB port: **on**, **off** or **overcurrent*** (*depending on model).

WWAN

The internal WWAN module has options for enabling/disabling the radio bands as supported by the internal WWAN modem.

Info

Shows information on the used WWAN modem and the connection status:

- Modem model.
- Firmware version.
- State: the current state of the WWAN connection.
- Current band: the general name of the frequency band in use.
- Receive frequency: the receive frequency of the WWAN modem.
- Transmit frequency: the frequency at which the modem transmits.

Management

The ‘Restart modem’ button can be used to re-initialise the WWAN modem. Upon clicking the button, the modem will be restarted. First a soft restart will be attempted. If that fails, a hardware reset will follow. It will take approx. 30 seconds for the modem to resume operation and start the connection setup.

Bands

Depending on the type of internal WWAN modem, various operating modes and frequency bands can be selected. Click ‘Apply/Save’ after selecting or deselecting bands.

This feature is mainly used for testing purposes. Under normal conditions it is advised to leave all bands and modes enabled.

Note that not all shown bands will be operational at the location where the unit is installed.

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’. The state can also be monitored via shell command

Contact out

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

Loss of power detection and signalling

The contact input sensor can be used for loss of power detection in combination with an external power buffer, UPS or backup battery. An external relay is needed to signal that the mains power is down. Signalling a loss of power can be on either the opening of the relay contact or the closure of the relay contact.

The contact should be triggered at least 15 seconds before the actual power runs out, to allow the system to do a proper shutdown and generate alert messages. This means that the power back-up must have the capacity to power the unit for at least 15 seconds.

The Shutdown delay should be set to at least 15 seconds before the back-up power runs out. Loss of power can be signalled by means of Email, SNMP trap or SMS (for those models equipped with a WWAN modem).

The restart delay can be used to prevent the system from restarting while the back-up power is running out in case the shutdown delay was set much shorter than the actual duration of the back-up power to be present.

Electrical characteristics

The contact input is designed for use with a dry contact (switch or relay contact) It may not work with “open collector” or “open drain “ contacts. Consult the hardware manual of the device for details and electrical characteristics of the I/O ports.

Advanced

Settings that are not supported by the regular web interface, can be made by means of system scripts. These scripts can be written via the web interface or via shell access. The scripts are automatically stored in the configuration file.

Scripts

boot.post

The *boot.post* script can be written, edited or pasted into the text field.
This script is executed once after system initialization and can be used for configurations or actions that are not dependent on changes in the firewall settings or changes during WAN fail-over events .
Click “Apply/Save” to store the script on the system and configuration file.
To immediately run or test the *boot.post* script, use the ‘Test Script’ button in the web interface.

firewall.post

The *firewall.post* script can be written, edited or pasted into the text field.
This script is executed each time the firewall is reconfigured, which happens on various events like WAN failover, changes in firewall settings, and establishment or teardown of VPN tunnels etc.
Click “Apply/Save” to store the script on the system and configuration file.
To immediately run or test the *firewall.post* script, use the ‘Test Script’ button in the web interface.

Action scripts

Action scripts are used for performing a single action and can be run from command line or invoked by the task scheduler and the network monitor.
The script can be written, edited or pasted into the text field.
Click “Apply/Save” to store the script on the system and configuration file.

SMS control

The SMS control script allows for all possible SMS commands to be created.
The script can be written, edited or pasted into the text field.
Click “Apply/Save” to store the script on the system and configuration file.

Script registers

Registers are available for use in the system scripts. These registers allow for storing states or passing data between scripts and the settings database.

Note: *details on writing scripts and using the registers are outside the scope of this user guide. Contact MuLogic or your local sales representative if you need additional information.*

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 route) 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 route) 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.

Monitor

Click "Add Monitor" to create or add monitoring entries.
The monitor tool can be used for automatic testing the connectivity of local or remote IP addresses by sending ICMP pings and showing the results in the web interface or via the SNMP rsaNwMonTable.
Both active (default route) and standby WAN interfaces can be selected. Leave the Gateway selector at '----' to ping addresses on the LAN side or connected via VPN tunnels.
In addition, Action scripts as created under Setup>Advanced> Scripts can be selected. One for a successful monitor test and one for a failed monitor test.

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 default user name is ‘admin’ the default password is ‘rsa-admin’. The data rate of the serial port is set at **Setup>Physical ports>Serial**.

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 for the SNMP MIB-2 “sysName” OID, for the MuLogic RSA features MIB “rsaSysName” OID, and in system alerts via email and SMS. This name 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 for the SNMP MIB-2 “sysLocation” OID, for the MuLogic RSA features MIB “rsaSysLocation” OID, and in system alerts via email and SMS. This name 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” OID.

Note:
The System name and location can also be written via an SNMP-set to the rsaSysName and rsaSysLocation OIDs of the MuLogic RSA features MIB. The MIB-2 sysName, sysLocation and sysContact OIDs cannot be written via an SNMP-set.

User accounts (Local authentication)

Users of the system can be authenticated via credentials (name and password) stored on the system itself. This is referred to as “local authentication”. Remote authentication can be done via the RADIUS or TACACS+ protocols.

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 permission for 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**.

Hash password: This option causes the password to be hashed before stored on the system, rather than being encoded (by default). Encoded passwords can be decoded in order to retrieve the actual password.
Hashed passwords, however, cannot be decoded, i.e. the actual password cannot be retrieved from the stored hash.

Remote (external) Authentication

For remote authentication, two methods are supported: RADIUS and TACACS+ This enables the use of a centralized access management system.

When external authentication is enabled, users for HTTP(S) and SSH access can be authenticated by a RADIUS or TACACs+ server.

Up to two RADIUS or TACACS+ server addresses can be configured.

When the option "Deny local authentication when RADIUS/TACACS+ server is accessible" is enabled, no local authentication will be performed when the authentication servers are accessible. When this option is disabled, then also the users defined in the local database are authenticated.

Notes:
1. For Telnet access no remote authentication is available. Only locally stored users with the role of Administrator are permitted.
2. For Telnet and SSH login the user must have the role of "Admin".
Upon login, the name in the command prompt will be "admin" regardless of the user name used for login.

External Authentication and Authorization

For RADIUS authentication select the option "RADIUS then local".
For TACACS+ authentication select the option "TACACS+ then local".
If the external authentication fails, the local user database will be checked.

RADIUS

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 a RADIUS server can be accessed.

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

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

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.

Secondary 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*.

TACACS+

Deny local authentication when TACACS+ server is accessible: Click the check mark to enable this feature. When enabled, locally stored users will not be authenticated as long as a TACACS+ server can be accessed.

TACACS+ service: enter the TACACS+ service name. The default name is ‘shell’.

TACACS+ authentication service: select the type of service from the pull-down menu. The default is “ppp”.

Primary server address: enter the IP address of the primary TACACS+ server.

Primary server port: enter the port number of the servers. The default is 49.

Primary server key: enter the key for access to the primary TACACS+ server

Secondary server address: enter the IP address of the secondary TACACS+ server.

Secondary server key: enter the password for access to the secondary TACACS+ server.

Secondary server port: enter the port number of the servers. The default is 49.

TACACS+ privilege levels

For TACACS+ the roles are mapped to "privilege levels" in the following manner: 15 = Web Administrator and SSH, 12 = Web Administrator (no shell), 5 = Updater, 3 = Auditor and 1 = Operator.

TACACS+ accounting

Apart from Authentication and Authorization, TACACS+ also offers Accounting. When enabled (in **Management>Accounting>Settings**) , events such as login, logout and changes in the configuration database are logged on the remote AAA server.

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 by editing the entry in the table.

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. This certificate should never be used for other purposes than testing!

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

***Warning.** Using X.509 certificates based on RSA keys of more than 2048 bits will create instability on the RSA-M1 models. On the RSA-M2 models, the use of such certificates is strongly discouraged.*

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 and Digest from the drop-down menus.
Note that key sizes below 1536 bits, and the MD5 and SHA-1 digest algorithms are considered broken with regard to security and should not be used.

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 allow access to system services, it may be necessary to configure rules 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 are 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.

Note . *The HTTP mode is no longer considered safe for access over the public internet without the use of an encrypted VPN.*

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.

Note: *Make sure that a valid X.509 certificate is selected before starting HTTPS Without a certificate the HTTPS server will not start.*

Warning. *Using X.509 certificates based on RSA keys of more than 2048 bits will create instability on the RSA-M1 models. On the RSA-M2 models the use of such certificates is strongly discouraged.*

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 "Enable SNMP-invoked firmware update" to allow firmware updates from a remote server to be initiated via SNMP.
Check "Enable SNMP-invoked settings update" to allow SNMP-initiated updates of the settings file or firmware file from a remote server.
Click 'Apply/Save' to store the changes.

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, the privacy password and the privacy cypher.

Additional SNMPv3 users

Click the “Configure additional SNMPv3 users” link to add users.

SNMP MIB file

The SNMP MIB file for the RSA-series is stored within the firmware and can be viewed or downloaded by clicking the ‘Download RSA series MIB’ link.

Shell access

Network access to the system shell for command line operation is given via the SSH and Telnet service.

Notes:
1. *For Telnet access no RADIUS authentication is available. Only locally stored users with the role of Administrator are permitted.*
2. *For Telnet and SSH login the user must have the role of “Administrator”. Upon login, the name in the command prompt will be “admin” regardless of the user name used for login.*

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.

Note 1. *Telnet mode is no longer considered safe for access over the public internet without using an encrypted VPN*.

CLI session timeout

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

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 messages at the interval as configured at “Inform interval”

Inform interval

Enter the inform interval here. The inform interval determines the frequency at which the unit contacts the ACS.

Allow connection requests

Connection requests are sent by the ACS in order to directly initiate a connection instead of waiting for the scheduled informs. The response to the connection requests can be enabled or disabled here. Note that an input filter rule in the firewall must be made in order to receive connection requests.

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 in* ***Setup>Firewall>Incoming filtering*** *for the port number (TCP) entered here.*

Provisioning code

This code is supplied via the ACS . It is displayed for reference purposes only.

SMS

Units equipped with an internal WWAN modem or with support for external WWAN modems can be controlled by means of SMS messages. Some basic commands are provided. Custom made commands can be added by means of the 'SMS control' script. See Setup>Advanced>Scripts.

Enable

Click the 'Enable' checkbox to enable the SMS control feature.

Secret

Enter the secret passphrase. This can be any alphanumeric string of up to 32 characters. The secret is the first string in the SMS message. Secret and command are separated by a space.

Whitelist

When enabled, only SMS messages from the specified telephone numbers are accepted. Up to 3 numbers can be entered. The numbers should be formatted according the ITU-T E.164 recommendation, hence start with "+" followed by the country code.

Reboot control

When enabled, the message **<secret> reboot** (where <secret> is the configured secret passphrase) will reboot the unit.

WWAN IP interface control

When enabled, the message **<secret> <wwan port ID> off** will disable the WWAN IP interface. The message **<secret> <wwan port ID> on** enables the WWAN IP interface. <wwan port ID> is the port ID as shown in the WWAN interface setup page. For example: **abcd1234 wwan-1 off**

DSL interface control

When enabled, the message **<secret> <dsl port ID> off** will disable the DSL interface. The message **<secret> <wwan port ID> on** will enable the WWAN data link. For example: **abcd1234 dsl-1 off**

Enable script execution

When enabled, the SMS control script will be executed.
(see: **Setup>Advanced>Scripts>SMS control**)

Note: *details on writing SMS control scripts are outside the scope of this user guide. Contact MuLogic or your local sales representative if you need additional information.*

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. Up to 4 addresses can be entered.

When 'Manual' is selected, the date and time can be entered manually in the format: yyyy-mm-dd 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.

NTP client status

This line shows the IP address of the connected NTP server.

Temperature

Current temperature

This field shows the actual system temperature in °C. If mounted vertically and with sufficient airflow on the top and bottom of the unit, the system temperature will be approx. 14 to 18 °C above the ambient temperature.

Enable temperature alerting

When enabled, an alert (see: **Management>Alert messaging>Alert rules**) will be sent when the system temperature exceeds the temperature threshold.

Temperature threshold

Sets the threshold at which the alert will be triggered.

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 cellular 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.

History

The history page shows the last boot or reboot reason, and the last 20 alerts as selected on the Alert rules page.

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. Updates 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 the debug level, all messages, including debugging messages, 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.

Accounting

Events such as login, logout and changes in the configuration database can be logged locally, or on a remote TACACS+ AAA server.

When local logging is enabled, the Account log page shows all login attempts and configuration changes.

Settings

Local log: Use the “Enable” check mark to enable account logging. When enabled, the account log will be stored on the system.

TACACS+ Accounting: Use the “Enable” check mark to remote account logging and configure the server settings:

Primary Server address: enter the IP address of the primary TACACS+ server.

Primary Server key: enter the key for access to the primary TACACS+ server

Secondary Server address: enter the IP address of the secondary TACACS+ server (optional).

Secondary Server key: enter the password for access to the secondary TACACS+ server (optional).

Server port: enter the port number of the servers. The default is 49.

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.

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.

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. The watchdog circuit controls the system power supply 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 and the ATM layer are monitored. Should the DSL or ATM 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 use the Network connection check.

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.

Tasks

Hibernate

The unit can be put in “hibernate mode” in order to reduce power consumption. During hibernation, all of the unit’s functions are disabled and the PWR LED will be off. While hibernating, the unit can only be woken up by disconnecting and reconnecting the power supply.
Select the “Hibernate time” for the duration of the power-down state.
The “Time of day” determines the start time of the hibernation period.

Reboot

Select the time of day at which the unit should reboot.
Execution can be “Once”, “Daily” or “Weekly”.

Restart Interfaces

The “Restart interfaces” tasks determine the time of day when the DSL, EthWAN or WWAN connections are restarted.

This can be used, amongst other, 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.

Run script

Select one of the Action scripts created under Setup>Advanced>Scripts and select the time of execution. Execution can be “Once”, “Daily” or “Weekly”.

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 for initial access to a provisioning server (like a TR-069 CWMP ACS).

View/backup configuration incl. 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/backup configuration excl. 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 file

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

Load custom defaults configuration file

Click the ‘Upload’ button and browse for a configuration file. Then click ‘Upload file’. This action will write the uploaded file as custom defaults file. The unit will not restart after uploading this file.

Copy current configuration to custom defaults

Click the ‘Apply’ button to copy the current configuration to the custom default configuration file. The custom default configuration allows you to program your own default settings which can be restored via the web interface, network or by means of pressing the reset button. The custom default configuration 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.*

Restore settings to custom defaults

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

Restore settings to factory defaults

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.

Load custom settings from USB flash drive

On units that are equipped with USB ports, the custom defaults file can be loaded by placing a USB flash drive in one of the USB slots. This option can be disabled by means of removing the checkmark and clicking ‘Apply/Save’. For details on this feature, contact MuLogic or your local sales representative.

Warning: For reasons of safety this option shall be turned off when not used.

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 settings 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 settings 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 and executing shell commands via HTTP(S) post
CLI commands via HTTP(S) post allow for scripted execution of dbctl and other shell 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**.

Serial number: The serial number of this unit.
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: Firmware version of WWAN modem(s).

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

Priority: This field shows the priority as set in the Setup>WAN Failover page.
Port ID: The reference as used in the internal configuration database.
Name: 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.
Interface: name of the interface as used by the system.
Address: IP address of the WAN interface.
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 Pseudo Random 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

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).
Interface: the IP interface of the IPsec tunnel (route-based VPN type only).
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 used DH (MODP) group for Perfect Forward Secrecy .
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).

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.

Port ID: Internal ID of this WWAN port.
Port status: the status of the WWAN port (enabled or disabled).
Modem status: shows the current status of the WWAN modem.

Modem type: the type of WWAN modem used.
Firmware version: the firmware version of the WWAN modem.
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.
Temperature: the temperature of the modem module.

Network: the name of the mobile network in use as received by the modem.
Registration state: shows if the modem is registered or in the process of registering to the mobile network, or the reason why registration is not possible: e.g. wrong PIN code, PUK code needed, port disabled, no SIM card present.
APN: the configured name of the Access Point.
IP interface status: the status of the IP interface and address when connected.
IP interface uptime: the time expired since the last (re)connect of the data link.

Radio access type: like 2G GPRS/EDGE, 3G UMTS/HSPA, 4G LTE or 5G NR.
Signal level*: the received signal level in RSSI and dBm format.
Channel number: shows the current radio *ARFCN*/UARFCN/EARFCN.
Frequency (Rx/Tx): the receiver and the transmitter frequency.
Band: the frequency band used

(Tracking) Area code: the area code of the currently connected access node.
Cell ID / eNB (4G): the Cell global ID and the eNodeB identifier of the LTE cell.
Cell ID (2G, 3G): the identifier of the GSM or WCDMA cell.
Physical Cell ID (4G): the (physical) identifier of the connected cell.
PSC (3G): Primary Scrambling Code (cell indicator).
UL bandwidth (4G): the current bandwidth of the upstream data channel.
DL bandwidth (4G): the current bandwidth of the downstream data channel.
RSRP (4G): the Reference Signals Received Power. (signal level).
RSRQ (4G): the Reference Signal Received Quality. (signal quality).
RSCP (3G): the Received Signal Code Power. (signal level).
Ec/Io (3G): the signal to interference ratio. (signal quality).

***Note*:** The Signal level (RSSI) as shown in the table is corrected when the radio access type is 3G, 4G or 5G. When in 3G, 4G or 5G mode, more commonly used signal level figures are available: the 3G RSCP and the 4G/5G RSRP. These figures are a measure of the reference signal level of the connected cell.*

Signal graph

The signal level screen shows the bar graphs of the RSSI, RSRP or RSCP levels and the Ec/Io or RSRQ values. Note that the levels shown may be lagging the actual levels at the antenna.

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.

SFP

This page will show the inventory and status information (if present) of the inserted SFP module.

USB

This page will show information of the inserted USB devices.

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 <peer number>

Uptime: Elapsed time since last established connection.
Address: Address of the connected peer.
Port: Source 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 and stored ARP entries.
All addresses resolved by means of the ARP protocol are stored on the system and can be used by the MAC filtering option in **Setup>Firewall>MAC filtering.** See page 31. Old entries can be removed from the MAC filtering table.

Name: the reference name as entered in **Setup>Firewall>MAC filtering** or as discovered from the DHCP request.
MAC address: the hardware (MAC) address of the ARP entry.
IP address: the IP address of the ARP entry.
Device: the IP interface where the device is found.
Active: shows a checkmark when recently seen.
Last seen: shows when the address has last been resolved.

New ARP entries can be reported as alerts. See page 77.

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 a restart of the router may not do a request again and then will not be shown in this list until a new DHCP request is made.

Logged-in users

This page shows the users that are currently logged-in and the devices that are authenticated by MAC authentication. Each entry contains the user name and role, the used access service, the time of login, authentication type, and the IP address (if applicable) from which the connection is made.