MuLOGIC

RSA-4222

Remote Site Access Router with ADSL/VDSL2 and Ethernet WAN ports.

Introduction

The MuLogic RSA-4222 is a router for providing access to unmanned remote locations such as power substations, traffic management systems and various other remote site automation equipment.

The unit is equipped with an ADSL/VDSL2 port and 4 Ethernet ports with VLAN support.

Two USB2.0 ports are available for connecting an external wireless WAN modem and USB devices like memory and interface devices for extra Ethernet and serial ports.

The RSA-4222 incorporates 2 serial port gateways that can be used for remote access to devices with a serial interface. One serial gateway connects to an RS232 port, the other to an RS485 port.

The unit is designed for industrial applications and is powered from low voltage DC or AC power sources.

The RSA-4222 operates over a temperature range from -40°C to +70°C.

Features

- Access router with Ethernet and ADSL/VDSL2 WAN ports.
- DSL interface supports standards for VDSL2, ADSL, ADSL2 and ADSL2+
- One hardware version for ADSL Annex A (PSTN overlay) and Annex B/J (ISDN overlay).
- ADSL Downstream rates up to 24 Mbit/s, upstream rates up to 1.4 Mbit/s (Annex A/B). Upstream rates up to 3 Mbit/s in Annex A/M and Annex B/J modes.
- VDSL2 Downstream rates up to 110 Mbit/s, upstream rates up to 50 Mbit/s.
- RFC4638 support for allowing PPPoE MTU size up to 1500.

- Ethernet ports: 10/100baseT, Auto-MDI/MDIX. All can be used as LAN or WAN port.
- Automatic Failover operation between xDSL, Ethernet or Wireless WAN ports.
- IEEE 802.1Q VLAN support for PTM, and Ethernet LAN interfaces.
- Automatic Failover operation between xDSL and Wireless WAN port.
- Ethernet port supports SCADA protocols like Modbus/TCP, DNP3/IP and IEC60870-5-104.
- Two serial port gateways for remote serial data (TCP/IP or UDP/IP) to serial ports (one RS232, one RS485). Data rates from 300 to 115200 bit/s.
- Serial ports support SCADA protocols like Modbus RTU/ASCII, DNP3 and IEC60870-5-101.
- IPsec and OpenVPN tunnels for secure communication with Ethernet and serial ports.
- GRE tunnels for linking multicast protocols like RIPv2 and OSPF over IPsec tunnels.
- Secure Layer-2 Ethernet bridging over OpenVPN tunnels.
- Secure access to Serial port gateways. (VPN tunnel or access restrictions in firewall).
- Up to 4 separate LAN networks with individual DHCP servers.
- Static routing and dynamic routing (BGP, OSPF, RIPv1 and RIPv2).
- Dynamic NAT (IP masquerading) for outgoing connections.
- Static NAT (Port forwarding) for incoming connections.
- Stateful firewall for access control, data forwarding and rate limiting (DoS protection).
- Device Management services: HTTP/HTTPS, CWMP(TR-069), IXplatform, SNMP and CLI.
- Firmware updates via local Ethernet port, remotely via HTTP/HTTPS (upload or download), invoked by CWMP(TR-069), SNMP, web interface or CLI command.
- Role-based access control for administrative access.
- RADIUS support for user authentication. Access roles determined by RADIUS attributes.
- IEEE 802.1X Port-based Network Access Control.
- Certificate management and enrolment: Manual or SCEP.
- System alerting by means of: Email, SNMP traps and SMS.
- Independent watchdog/reset controller for monitoring vital system functions.
- Dry contact sensor (input) with status reporting and alerting via SNMP, Email or SMS.
- Dry contact (output) for automatic alarm/status indication or remote control.
- Temperature sensors (system and WWAN) with status reporting via SNMP and HTTP and alerting via SNMP trap, Email or SMS.
- Isolated supply voltage input for industrial applications (suitable for AC and DC).

- Supply voltage ranges: 11-36Vdc/11-28Vac, 18-60Vdc/18-30Vac or 18-72Vdc.
- Extended operating temperature range: -40°C to +70°C
- Din-Rail or panel mounting.

Application Areas

Remote site access

The RSA-4222 is designed for access to unmanned remote sites like electric power substations, roadside cabinets for traffic control, remote surveillance etc. The unit provides connectivity for Remote Terminal Units, PLCs and other equipment and supports both Ethernet and serial ports. Various options for secure VPN tunnels like IPsec and OpenVPN are available. In combination with GRE tunnels or secure Layer2 tunnels, all possible layer2 and layer3 network protocols can be transported.

Remote Machine access

Machine builders often offer remote access support and diagnostics for their installed machines. However, network security policies of a factory or plant may make direct remote access very cumbersome or even impossible. To overcome these situations, the RSA routers and connected machines can be made accessible via a secure 3rd party cloud service.
The RSA router in the factory can make connection to the cloud platform via the factory network without the need for changing or adding firewall rules. Alternatively, the routers can have their own connection to the outside world via an ADSL or VDSL2 line thus totally bypassing the factory network.
The cloud platform offers access to the remote machines via smart phones, tablets or PCs connected to the internet and without the need to create your own VPN network. Via the platform, web based services are available for accessing the router's user interface and web servers or VNC servers of attached machines.

Failover operation of WAN ports and interfaces

All WAN interfaces can be used as primary WAN or back-up WAN interface.
Alternative paths are selected automatically according to priority and availability.

Serial port gateways

The integrated Serial Port gateways offer remote access to the unit's serial ports.
One gateway connects to the RS485/RS422 port, the other to the RS232 port.
Combined operation of RS232 and RS485 to a single gateway is also possible.

The network connection to the serial port gateways allows for the use of various tools like "virtual com port drivers", direct IP socket connection or dedicated application software. Also other "serial to Ethernet converters" or another MuLogic router can be used. In addition, the serial ports can also be accessed by means of a telnet or SSH connection.

Information and Access Security: IPsec, OpenVPN and Firewall

As the unit in most cases will be connected to the public internet, extra security features such as IPsec and OpenVPN are supported. IPsec and OpenVPN protect against unwanted access and eavesdropping of the data. With IPsec and OpenVPN encrypted virtual tunnel connections can be created. Only devices at the end-points of the tunnel can communicate and the data is protected from eavesdropping.

A single RSA-4222 can support multiple IPsec or OpenVPN tunnels.
The OpenVPN tunnels can operate in routing mode (layer-3) but can also be used to transparently bridge Ethernet frames (Layer-2).

The unit's firewall features are used for static or dynamic NAT routing (port forwarding and IP masquerading) and blocking or granting access to the devices attached to the unit and the unit's configuration and management interface.
This makes it possible to block all access from unknown IP addresses. In addition, several options are available to limit the rate of incoming or outgoing data as protection against DoS attacks.

Configuration and remote management

The RSA-4222 can be configured and managed in multiple ways:

- Web browser (http and https).
- TR-069 CWMP.
- HTTP Post for scripted configuration and control.
- IXplatform.
- Command line interface via telnet, SSH, or serial port.
- SNMP manager.

Device power supply

The RSA-4222 is equipped with a galvanically isolated power input.
Three voltage ranges are available:

- 11-36Vdc/11-28Vac.
- 18-60Vdc/18-30Vac.
- 18-72Vdc.

For mains power operation (100..240Vac) an external power adapter or power supply is used.

Extended temperature range

The RSA-4222 is designed for operating under extreme temperature conditions.
It is suitable for operating at ambient temperatures ranging from -40°C to +70°C.

Technical Specifications

xDSL modes

- ANSI T1.413 Issue 2 (ADSL)
- ITU-T G.992.1 (G.dmt)
- ITU-T G.992.2 (G.lite)
- ITU-T G.992.3/4 (ADSL2)
- ITU-T G.992.3 Annex L (RE-ADSL)
- ITU-T G.992.5 (ADSL2+)
- ITU-T G.992.5 Annex M (ADSL2+M)
- ITU-T G.993.2 VDSL2 (profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a)
- ITU-T G.993.5 and G.993.2 Annex Y VDSL2 Vectoring
- ITU-T G.998.4 (G.INP) Impulse Noise Protection
- SRA (Seamless Rate Adaption)
- Hardware is suitable for both ADSL Annex A/M and Annex B/J

xDSL encapsulation protocols

- PPP Over ATM (PPPoA, RFC2364)
- PPP Over Ethernet (PPPoE, RFC2516)
- Ethernet Over ATM (MER/IPoE, RFC2684)
- IP Over ATM (IPoA - CLIP, RFC2225)
- MAC Encapsulation Routing (MER, RFC2684)
- Ethernet bridging (RFC2684 Bridge mode)
- PTM with tagged or untagged VLAN
- PPPoE MTU up to 1500 (RFC4638)

IP routing

- Static routing
- Dynamic routing: OSPFv2, OSPFv3, RIPv1/v2 and BGP-4.

Firewall

- Stateful firewall for data forwarding and access control, Rate limiting, NAT routing and port forwarding.

Tunnel protocols

- IPsec (IKEv1/v2), OpenVPN and GRE (Layer 2 and Layer 3).

IPsec

- Mode of operation: Tunnel mode.
- Key exchange method: Automatic (IKE, IKEv2).
- Authentication method: Pre-shared key or X.509 Certificate.
- PFS support (Perfect Forward Secrecy): RFC 2412.
- Phase 1 mode: Main or Aggressive.
- Phase 1 and 2 Encryption Algorithms: 3DES, AES-128, AES-192 or AES-256.
- Phase 1 and 2 Integrity Algorithms: MD5, SHA-1, SHA-256, SHA-384, SHA-512 or SHA-256-96.

- Diffie-Hellman groups for key exchange: DH Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 15 (3072 bit), Group 16 (4096 bit). NIST ECG25 (192 bit), ECG26 (224 bit), ECG19 (256 bit), ECG 20 (384 bit) and ECG21 (521 bit).
  Brainpool ECG27 (224 bit), ECG28 (256bit), ECG29 (384 bit) and ECG30 (512 bit).
- Key Lifetime: 1-28800 seconds.
- DPD (dead peer detection).
- NAT-traversal and NAT KeepAlive.
- Layer-2 bridging over IPsec tunnels using GRE Layer 2 or OpenVPN Layer 2 bridging.
- Multicast over IPsec using GRE.
- Multiple tunnel configuration profiles.

OpenVPN

- P2P, client and Server mode
- UDP, TCP server, TCP client
- Modes: L2 Bridged, L3 Routed
- Authentication methods: Pre-shared secret, X.509 Client, X.509 Server.
- Encryption Algorithms: 3DES, AES-128, AES-192, AES-256 or Blowfish.
- TLS authentication.
- LZO Compression.
- Multiple tunnel configuration profiles.

GRE

- Layer 3 and layer 2 tunnelling.
- Multiple tunnel configuration profiles.

Ethernet ports

- 10/100baseT
- Half and Full duplex
- Auto-MDI/MDIX
- 802.1Q VLAN support

Serial ports

- Port 1: RS232 DB9 Male connector (DTE pinout).
- Port 2: RS485/RS422 at 4-pin screw terminal connector.
- Port rates: 300, 600, 1200, 2400, 4800, 9600, 19k2, 38k4, 57k6 or 115k2 bit/s.
- Data formats: 8N, 8E, 8O, 7E, 7O. One or two stop bits.
- Buffer size: 10, 20, 50, 100, 200, 300, 400, 500, 1000 or 1500 bytes.
- Forwarding timeout: 1, 2, 5, 10, 15, 20, 50, 100 or 200 msec.

Serial gateways

- Operating modes: TCP server, TCP client, Telnet server, UDP client/server
- Maximum number of concurrent connections: 256.
- TCP Alive check and Data Activity check.
- Statistics per connection.

I/O ports

- Input: contact sensor for dry contact. Closed contact current: max. 6 mA.
- Output: Isolated dry contact. On resistance: 8Ω, max. load current: 150 mA.

Power supply voltage ranges

- RSA-4222/Vr1: 11-36Vdc/11-28Vac (7W)
- RSA-4222/Vr2: 18-60Vdc/18-30Vac (6W)
- RSA-4222/Vr3: 18-72Vdc (6W)

Dimensions and weight

- Dimensions RSA-4222: 143x38x95mm(HxWxD), Weight: 530 gr.

Environment

- Operating temperature range: -40°C to +70°C, Humidity:5..95%
- Storage temperature range: -50°C to +80°C, Humidity:5..95%

Compliances

- CE directives: 2014/30/EU (EMC) and 2006/35/EU (LVD).
- EMC: EN 55022, EN55024: Emission limits and immunity for residential environments.
- EMC: EN 61000-6-2: Immunity for industrial environments.
- Safety: EN 60950-1:2006/A11:2009+A1:2010+A12:2011+A2:2013
- Mechanical Stability: IEC 60068-2-27 shock, IEC 60068-2-6 vibration.
- RoHS: 2002/95/EC (RoHS 1), 2011/65/EC (RoHS 2)

Order codes

- RSA-4222/Vr1 (11-36Vdc/11-28Vac)
- RSA-4222/Vr2 (18-60Vdc/18-30Vac)
- RSA-4222/Vr3 (18-72Vdc/no AC)