comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

RELIANCE RL1000GW

Small Form Factor Substation-Rated Secure Ethernet Layer 3 Router/Gateway with Optional 2G/3G/4G LTE Cellular Radio Link, and 100/1000 Mbps SFP Uplink Port

ComNet product series RL1000GW are substation-rated and industrially hardened layer 3 router/gateways, with a unique and highly robust packet processing SCADA-aware security firewall for the most mission-critical and demanding cyber-security applications. The RL1000GW is intended for deployment in environments where high levels of electromagnetic noise and interference (EMI) and severe voltage transients and surges are routinely encountered, such as electrical utility substations and switchyards, heavy manufacturing facilities, track-side electronic equipment, and other difficult out-of-plant installations. Layer 3 routing functionality allows for the participation and foundation of a core network infrastructure. The compact-sized DIN-rail mountable RL1000GW is ideally suited to those installations and applications where space may be limited. These features make the RL1000GW an effective platform for deploying a secure communications and networking gateway for remote electrical utility sites, and other critical infrastructure applications.

The RL1000GW is an ideal platform for deploying a secure communications and networking gateway for remote electrical utility sites, and other critical infrastructure applications.

Contents

About This Guide

This user guide includes relevant information for utilizing the Reliance RL1000GW line of switches.

The information in this document is subject to change without notice and describes only the product defined in the introduction of this document.

This document is intended for the use of customers of ComNet only for the purposes of the agreement under which the document is submitted, and no part of it may be reproduced or transmitted in any form or means without the prior written permission of ComNet.

The document is intended for use by professional and properly trained personnel, and the customer assumes full responsibility when using it.

If the Release Notes that are shipped with the device contain information that conflicts with the information in this document or supplements it, the customer should follow the Release Notes.

The information or statements given in this document concerning the suitability, capacity, or performance of the relevant hardware or software products are for general informational purposes only and are not considered binding. Only those statements and/or representations defined in the agreement executed between ComNet and the customer shall bind and obligate ComNet.

ComNet however has made all reasonable efforts to ensure that the instructions contained in this document are adequate and free of material errors. ComNet will, if necessary, explain issues which may not be covered by the document.

ComNet sole and exclusive liability for any errors in the document is limited to the documentary correction of errors. **ComNet is not and shall not be responsible in any event for errors in this document or for any damages or loss of whatsoever kind, whether direct, incidental, or consequential (including monetary losses),** that might arise from the use of this document or the information in it.

This document and the product it describes are the property of ComNet, which is the owner of all intellectual property rights therein, and are protected by copyright according to the applicable laws.

Other product and company names mentioned in this document reserve their copyrights, trademarks, and registrations; they are mentioned for identification purposes only.

Intended Audience

This user guide is intended for network administrators responsible for installing and configuring network equipment. Users must be familiar with the concepts and terminology of Ethernet and local area networking (LAN) to use this User Guide.

Related Documentation

The following documentation is also available:

» RL1000GW Data sheet

» RL1000GW Quick Start Guide

» RL1000GW_ES Enhanced Security Software Options Manual

» SFP Modules Data sheet

About ComNet

ComNet develops and markets the next generation of video solutions for the CCTV, defense, and homeland security markets. At the core of ComNet's solutions are a variety of high-end video servers and the ComNet IVS software, which provide the industry with a standard platform for analytics and security management systems enabling leading performance, compact and cost effective solutions.

ComNet products are available in commercial and rugged form.

Website

For information on ComNet's entire product line, please visit the ComNet website at **http://www.comnet.net**

Support

For any questions or technical assistance, please contact your sales person (**sales@comnet.net**) or the customer service support center (**techsupport@comnet.net**)

Safety

» Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.

» The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Overview

Introduction

The ComNet Service-aware Industrial Ethernet routers combine a ruggedized Ethernet platform with a unique application-aware processing engine.

As an Industrial Ethernet router the ComNet RL1000GW provide a strong Ethernet and IP feature-set with a special emphasis on the fit to the mission-critical industrial environment such as fit to the harsh environment, high reliability and network resiliency.

In addition the ComNet routers have unique service-aware capabilities that enable an integrated handling of application-level requirements such as implementation of security measures.

Such an integrated solution results in simple network architecture with an optimized fit to the application requirements.

Figure 1 - Illustration of ComNet RL1000GW

Key Features

The ComNet RL1000GW devices offer the following features:

» Compact systems
» Advanced Router feature-set
» Integrated Defense-in-Depth tool-set
» Ethernet and Serial interfaces
» Fit to harsh industrial environment

Seamless & Reliable Connection to Any Network

The RL1000GW provides connectivity to any copper, fiber optic, or cellular radio-based Ethernet network. Fiber optic networks are supported by the use of the optional 100/1000FX SFP uplink port. The optional highly resilient 2G/3G/4G LTE cellular radio uplink with 2 SIM card slots for network redundancy, is ideal where fiber optic infrastructure is not available, and may be used as a back-up link for those applications where interruption of service is not tolerable.

Extremely Effective Network Security, For the Most Mission-Critical Applications

Service Gateway

The RL1000GW service gateway includes a highly robust application layer, and provides legacy support, a Deep Packet Inspection (DPI) application-aware SCADA firewall, serial tunnelling, protocol gateway, and extremely effective encryption technologies. The service gateway offers a uniquely capable feature set which may serve as the hardware foundation to a secure industrial controls network, and includes Protocol Gateway, VPN, and IPsec features.

Protocol Gateway

Gateway functionality between a DNP3 TCP client (master) and a DNP3 Serial RTU, IED, PLC, or other compatible device is supported. This same functionality is supported across MODBUS TCP to MODBUS RTU, and IEC 61850 101/104 TCP to IEC 61850 101/104 RTU. This level of protocol conversion allows legacy protocols to be secured by enterprise and industry best practice level encryption across a TCP IP-based network.

VPN

VPN tunnels are included for secure inter-site connectivity with IPsec, DM-VPN, and VPN GRE tunnels with key management certificates. The supported VPN modes allow both layer-2 and layer-3 services, to best suit the user's application-specific cyber-protection needs.

IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet of a communication session. IPsec-VPN as well as IPsec encryption are supported over other VPN technologies. By implementing this level of industry-accepted encryption, data may traverse the network in a guaranteed delivery method, as well as providing a cohesive and secure methodology for network communication across legacy and modern networks.

Identity Management and Authentication Proxy Access (APA)

NERC-CIP-5 defines the important requirement for network security protection of remote and unattended facilities. The capability of identifying the user and creating specific network privileges per identified and authenticated user prior to granting the user access to the network therefore becomes critical

The Authentication Proxy Access (APA) is a highly sophisticated security feature, which allows the network operator to manage the substation or any other facility maintenance process. This feature

gives full control of the maintenance process to the operator by granting the capability to create dynamic policies to specific tasks within an explicitly defined time window. Following this time window, operators receive reporting on activities performed during the task. This audit trail comes in the form of an overview log, and a full packet capture (PCAP) of the session.

Before a user is allowed access to the network, they must log in to ComNet's internal authentication process with their unique user name and password. Upon validation of the user profile, specific access is granted to predefined devices and functions, and each operation is logged. Multi-factor authentication is available when combined with the Cyber-Physical Integration feature.

X.509 Certificate Exchange for VPN Connections

VPN tunnels for secure inter-site connectivity with IPsec VPN, GRE Tunnels, and DMVPN technologies are fully supported. In addition to IPsec encryption, X.509 key management certificates are provided. This certificate support allows for a secure signed key exchange between a Certificate Authority, and two secure nodes. Having a third-party authority as a signing participant offers end-to-end security that may be managed and reissued from a trusted central source within the user's network.

Cyber-Physical Integration

Integrated within the enhanced-security RL1000GW, is a physical identity server system, allowing the use of external authentication hardware, such as magnetic card readers, biometric identification sensors, facial recognition cameras, etc., to create a two-factor authentication to the APA feature. This provides an additional level of validation of the user and his/her credentials, prior to granting the user network access. Once the authentication is validated and approved, a set of defined policies allow the authenticated technician to perform their task.

Enhanced SCADA-Aware Firewall

A whitelist-based firewall is provided for every Ethernet and serial data port, so full firewall protection is available at all remote sites within the network. Every SCADA protocol packet (IEC 61850, DNP3 RTU/TCP, ModBus RTU/TCP, and IEC 101/104) is scanned and validated by the firewall engine for its source and destination, as well as its protocol and packet content.

The structure of the distributed firewall allows the creation of a unique firewall at each access point to the network. This is critical for securing against insider cyber-attacks, compromised field devices, man-in-the-middle attacks, and a myriad of alternate attack vectors, by providing a secure baseline.

Two firewall states are included: Monitoring, and enforcing. The monitoring state provides an alarm at the control center for any network violation, without blocking the network traffic. The enforcing state is extremely effective for blocking suspicious traffic, while also triggering a violation alarm at the control center.

DPI (Deep Packet Inspection) SCADA Protocols Firewall

ComNet's distributed DPI firewall ensures that the operator will have full control over the network, even when faced with a sophisticated attempt at breaching the network. Monitoring SCADA commands, this highly robust whitelist-based firewall analyses SCADA network traffic, and is

provided for every Ethernet and serial data port, so full firewall protection is available at all remote sites within the network, as well as all IEDs, RTUs, PLCs, or any other device connected to the network. Every SCADA protocol packet (IEC 61850, DNP3 RTU/TCP, ModBus RTU/TCP, and IEC 101/104) is scanned and validated by the firewall engine for its source and destination, as well as its protocol and its specific packet

Any detected abnormal traffic behavioral patterns are blocked, any affected subnets are isolated, and alerts are automatically generated.

Ease of Installation and Network Integration

High levels of cyber-security experience are not required to successfully deploy the RL1000GW. It is fully supported by ComNet's Reliance Product Configuration Utility and CLI, allowing the secure switch/router to be easily configured, and to diagnose network and security functions.

Configuration of the secure firewall is also simple. Once connected to the user's network, the RL1000GW immediately begins to collect and analyse information across the network, including from other connected devices, traffic behavior, etc. Recommended firewall rules are then suggested to the user; the implementation of these rules is optional, and they can be easily edited using the Configuration Utility.

OAM (IEEE 802.3-2005 & IEEE 802.1ag) and QoS are also supported. Strict priority, Weighted Round Robin (WRR), ingress policing, and egress traffic shaping are included for traffic management.

Serial Data Interface

The 2-port serial interface is available for applications including terminal server with protocol gateway and serial tunnelling functionality, and provides direct connectivity to legacy RS-232 or 4-wire RS-485 serial data IEDs, RTUs, PLCs, and other devices.

Hardware and Interfaces

Depending on the RL1000GW hardware variant ordered your router will hold physical Ethernet and Serial ports.

» Serial, RJ 45 ports are RS-232. Max 2 ports
» Serial, RJ 45 ports are RS-485. Max 1 ports
» Ethernet RJ45 copper ports are 10/100 FE. One port
» Ethernet SFP based ports are 100/1000 GE. One port.

Ordering options of Hardware

RL1000GW Standard Models

Part Number	Description
RL1000GW/12/E/S22	RL1000GW with 2 x RS-232 and 1 x 10/100 Tx, 12/24V DC
RL1000GW/12/E/S24	RL1000GW with 1 x RS-232, 1 x RS-485 and 1 x 10/100 Tx, 12/24 VDC
RL1000GW/12/ESFP/S22	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 1 x 100/1000 Fx SFP, 12/24 VDC
RL1000GW/12/ESFP/S24	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 1 x 100/1000 Fx SFP, 12/24 VDC
RL1000GW/12/E/S22/CH+	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 2G/3G/HSPA+ Cellular Modem, 12/24 VDC
RL1000GW/12/E/S24/CH+	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 2G/3G/HSPA+ Cellular Modem, 12/24 VDC
RL1000GW/12/ESFP/S22/CH+	RL1000GW with 2 x RS-232, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 2G/3G/HSPA+ Cellular Modem, 12/24 VDC
RL1000GW/12/ESFP/S24/CH+	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 2G/3G/HSPA+ Cellular Modem, 12/24 VDC
RL1000GW/12/E/S22/CNA	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 4G LTE Cellular Modem (NA Bands), 12/24 VDC
RL1000GW/12/E/S24/CNA	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 4G LTE Cellular Modem (NA Bands), 12/24 VDC
RL1000GW/12/ESFP/S22/CNA	RL1000GW with 2 x RS-232, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (NA Bands), 12/24 VDC
RL1000GW/12/ESFP/S24/CNA	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (NA Bands), 12/24 VDC
RL1000GW/12/E/S22/CEU	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 4G LTE Cellular Modem (EU Bands), 12/24 VDC
RL1000GW/12/E/S24/CEU	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 4G LTE Cellular Modem (EU Bands), 12/24 VDC
RL1000GW/12/ESFP/S22/CEU	RL1000GW with 2 x RS-232, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (EU Bands), 12/24 VDC
RL1000GW/12/ESFP/S24/CEU	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (EU Bands), 12/24 VDC
RL1000GW/48/E/S22	RL1000GW with 2 x RS-232 and 1 x 10/100 Tx, 24/48V DC
RL1000GW/48/E/S24	RL1000GW with 1 x RS-232, 1 x RS-485 and 1 x 10/100 Tx, 24/48 VDC
RL1000GW/48/ESFP/S22	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 1 x 100/1000 Fx SFP, 24/48 VDC
RL1000GW/48/ESFP/S24	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 1 x 100/1000 Fx SFP, 24/48 VDC
RL1000GW/48/E/S22/CH+	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 2G/3G/HSPA+ Cellular Modem, 24/48 VDC

Part Number	Description
RL1000GW/48/E/S24/CH+	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 2G/3G/HSPA+ Cellular Modem, 24/48 VDC
RL1000GW/48/ESFP/S22/CH+	RL1000GW with 2 x RS-232, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 2G/3G/HSPA+ Cellular Modem, 24/48 VDC
RL1000GW/48/ESFP/S24/CH+	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 2G/3G/HSPA+ Cellular Modem, 24/48 VDC
RL1000GW/48/E/S22/CNA	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 4G LTE Cellular Modem (NA Bands), 24/48 VDC
RL1000GW/48/E/S24/CNA	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 4G LTE Cellular Modem (NA Bands), 24/48 VDC
RL1000GW/48/ESFP/S22/CNA	RL1000GW with 2 x RS-232, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (NA Bands), 24/48 VDC
RL1000GW/48/ESFP/S24/CNA	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (NA Bands), 24/48 VDC
RL1000GW/48/E/S22/CEU	RL1000GW with 2 x RS-232, 1 x 10/100 Tx and 4G LTE Cellular Modem (EU Bands), 24/48 VDC
RL1000GW/48/E/S24/CEU	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx and 4G LTE Cellular Modem (EU Bands), 24/48 VDC
RL1000GW/48/ESFP/S22/CEU	RL1000GW with 2 x RS-232, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (EU Bands), 24/48 VDC
RL1000GW/48/ESFP/S24/CEU	RL1000GW with 1 x RS-232, 1 x RS-485, 1 x 10/100 Tx, 1 x 100/1000 Fx SFP and 4G LTE Cellular Modem (EU Bands), 24/48 VDC

Options

Optional Part No	Description
ANT3G-2M	2G/3G External Grade Cellular Antenna with 2M cable (1 required per switch)
ANT3G-5M	2G/3G External Grade Cellular Antenna with 5M cable (1 required per switch)
ANT4G-2M	4G LTE External Grade Cellular Antenna with 2M cable (2 required per switch)
ANT4G-5M	4G LTE External Grade Cellular Antenna with 5M cable (2 required per switch)
Power Supply	12 V, 24 V or 48 V DC DIN Rail power supply
Conformal Coat	Add suffix '/C' for Conformally Coated Circuit Boards to extend to condensation conditions
SFP Modules[1]	User selection of ComNet SFP (See SFP Modules data sheet for product numbers and compatibility)
DINBKT3	19-inch rack mount panel adapter

Graphic View of Hardware

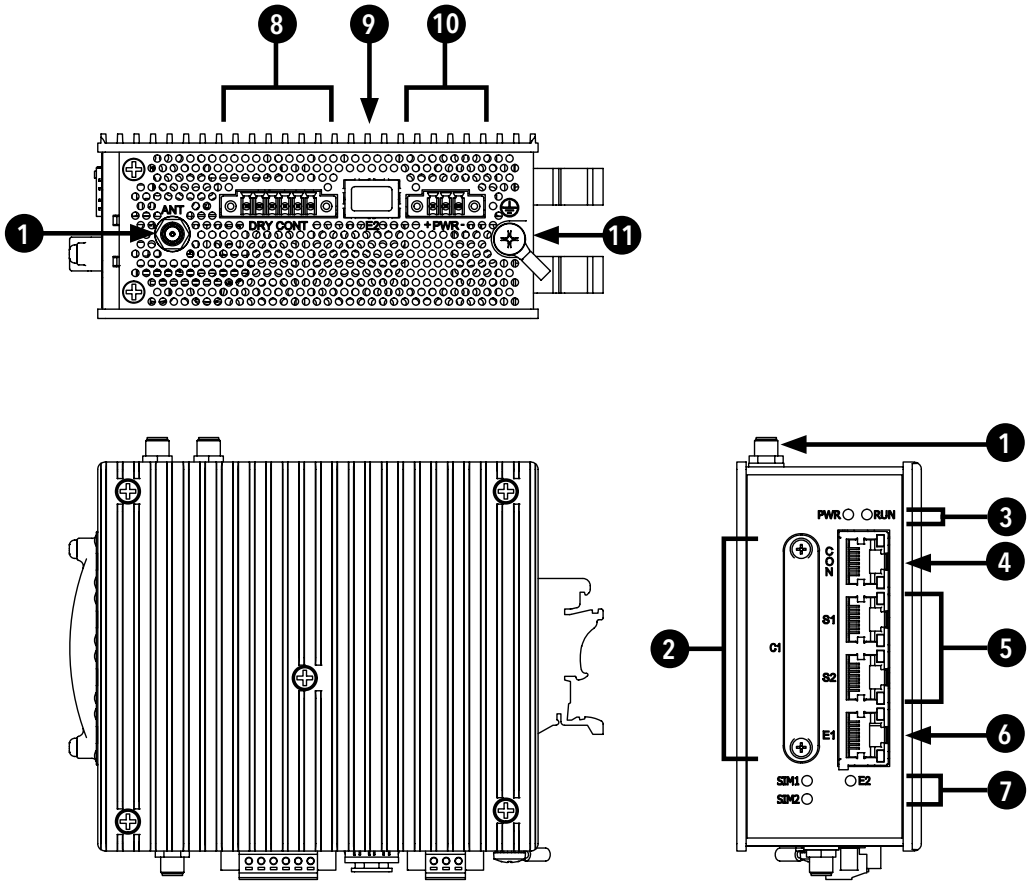


Figure 2 – RL1000GW Product

Table 1 – RL1000GW Physical Feature Descriptions

Call-out	Description	Manual Reference
1	Antenna Female Connection	–
2	SIM Card Ports 1 - 2	
3	Power and Run LED Indicators	
4	Console Interface, Link/Activity (L/A) and Speed LED Indicators	
5	RS-232 Ports 1 - 2, Link/Activity (L/A) and Speed LED Indicators	
6	10/100 TX Port, Link/Activity (L/A) and Speed LED Indicators	
7	SIM1, SIM2, Fast Ethernet Port LED Indicators	
8	Dry Contact DI/DO Interface	
9	USB Interface	
10	Power Interface	
11	Chassis GND Lug	

Distance kept for natural air flow

Proper installation depends on natural air flow for cooling. You must maintain a 10cm distance above and below the ComNet switch for proper air flow.

Logical Structure

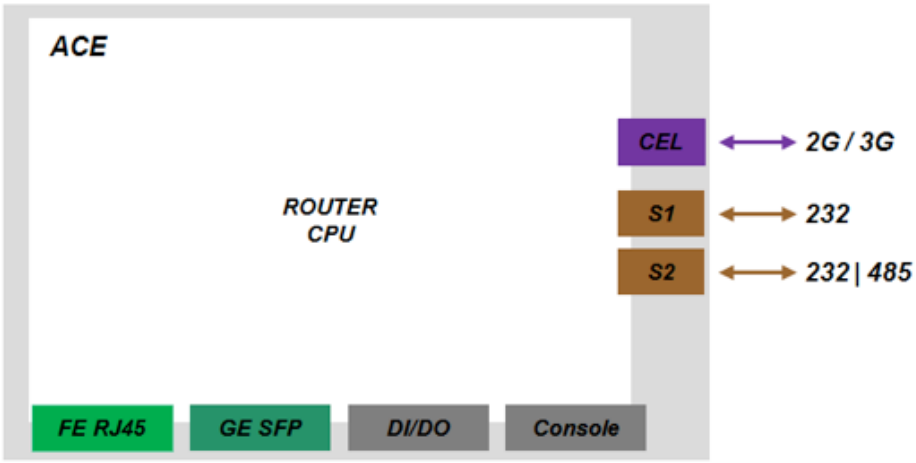


Figure 4 - Logical system view, illustration

Grounding

To install the grounding wire:

» Prepare a minimum 10 American Wire Gauge (AWG) grounding wire terminated by a crimped two-hole lug with hole diameter and spacing as shown in the below figure. Use a suitable crimping tool to fasten the lug securely to the wire. Adhere to your company's policy as to the wire gauge and the number of crimps on the lug.

» Apply some anti-oxidant onto the metal surface.

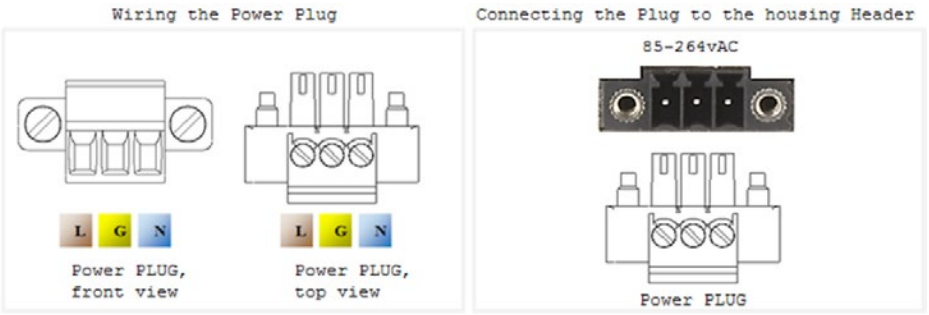
» Mount the lug on the grounding posts, replace the spring-washers and fasten the bolts. Avoid using excessive torque.

CAUTION – Do not remove the earth connection unless all power supply connections are disconnected.

DANGER – Before connecting power to the platform, make sure that the grounding posts are firmly connected to a reliable ground, as described below.

Connecting to a Power Source

Wiring AC Input voltage connector



For an AC product variant there is a single input connector.

Use a Brown wire for the Line (Phase) conductor, a Green/Yellow for the grounding and a Blue wire for the Neutral conductor. use 18AWG (1mm2) wire, with insulated ferrules.

Power Budget

The following table details power consumption of the Hardware variants with cellular and serial interfaces.

Unit Power feed	Max Power [Watt] Version without POE ports	Max Power [Watt] Version with POE ports
12vDC	18.5	80
24vDC	18.5	100
48vDC	18.5	140 (or 260*)
110vDC	18.5	120
220vDC	18.5	120
110vAC	20.35	149
220vAC	20.35	149 (or 275*)

** Refers to specific ordering option supporting 240w PoE.*

Configuration Environment

A CLI based configuration environment is available for the user.

Command Line Interface

The CLI (Command Line Interface) is used to configure the RL1000GW from a console attached to the serial port of the router or from a remote terminal using SSH. The following table lists the CLI environments and modes.

Table 3-1: Command Line Interface

Command Mode	Access Method	Prompt	Exit Method
Global Configuration Environment (GCE)	Following user log in this mode is available to the user.	RL1000GW#	To exit this mode would mean the user to log out from the system. Use the command 'exit'
Global Hierarchy Configuration	From the Global Configuration mode command you may drill down to specific feature sub tree. Example is shown here for router configuration sub tree.	[router/]	To exit one level back, the '..' (Two dots) is used.
Application Configuration Environment (ACE)	The ACE is an alternative configuration environment for supported features	ACE#	This mode is not supported at current version To exit back to the GCE mode use the 'exit' command.
ACE Config	Use the command 'configure' to access the ACE Configuration mode	ACE(config)#	To exit back to the ACE mode use the 'exit' command.
Application Hierarchy Configuration	Access the target feature. For example : 'interface vlan 1'	ACE(config-if-eth1.1)#	To return one level up use 'exit'. To return to the ACE use 'end'.

Supported Functionalities

The RL1000GW is a feature rich industrial router supporting:

» L3 dynamic and static Routing.
» SCADA services.
» Firewall.
» Secure networking.

The below table gives a high level view of the supported features.

Feature Set			
TFTP	Ethernet ports	Serial ports	Cellular modem
OSPF	Vlan tagging	IPSec	VPN
Management	Authentication	SCADA Gateway	SCADA Firewall
L3-L4 Firewall	QOS	Serial services	Terminal services
NAT	Syslog	OSPF	RIP*
DHCP Client			

The below table details the RL1000GW planned features.

Group	Feature	
Interfaces	Cellular modem with 2 SIM cards	X
	FE RJ45 Ports	X
	Fiber Optic port	X
	Gigabit port	X
	RS 232 ports	X
	RS 485 4wire ports	X
	SFP Port	X
	Auto Crossing	X
	Auto Negotiation IEEE 802.3ab	X
	VLAN segregation Tagging IEEE 802.1q	X
	Backup / Restore running config	X
	Conditioned/ scheduled system reboot	X
	Console serial port	X
	TFTP client	X
	Inband Management	X
	Outband Management	X
	Remote Upgrade	X
	Safe Mode	X
	SFTP Client	X
	Syslog	X
	Telnet Client	X
	Telnet server	X
	TFTP Client	X
Networking	QOS	X
Protection	Conditioned/ scheduled system reboot	X
	Protection between Cellular ISP (SIM cards backup)	X
Routing	DHCP Client	X
	IPv4	X
	OSPF v2	X
	RIPv2	X
	Static Routing	X
Security	ACLs , L3-L4	X
	Application aware IPS Firewall for SCADA protocols	X
	IPSec	X
	Local Authentication	X
	Port shutdown	X
Time	Local Time settings	X

Group	Feature	
Diagnostics	Counters & statistics per Port	X
	Led diagnostics	X
	Ping	X
	RMON	X
Serial Gateway	IEC 101/104 gateway	X
	IEC 104 Firewall	X
	Serial Transparent Tunneling	X
	Terminal Server	X
VPN	L3 mGRE DM-VPN	X

System Default state

The following table details the default state of features and interfaces.

Feature	Default state
Ethernet Ports	All ports are enabled
Serial interfaces	Disabled
Cellular modem	Disabled
Layer 3 interface	No default IP
Authentication	local
DHCP Client	disabled
SSH server	Enabled
SSH client	Enabled
Telnet client	Enabled
Telnet server	Blocked
TACACS	disabled
Syslog	Enabled
ACLs	No ACLs
Firewall	Disabled
VPN	No VPN settings

Main Commands

The Global Configuration Environment list of main CLI commands is shown below.

+ root

    + Router {interface | route |static |ospf |ip |rip}

    + cellular {connection | continuous-echo| disable |enable| modem| network| refresh| settings| show| wan}

    + commit

    + capture {delete |export |help |show |start |stop}

    + date

    + discrete {service| show}

+ dns {host| resolver}

    + exit

    + firewall {log| profile| tcp| serial}

    + idle-timeout

    + iec101-gw {cnt| operation| config iec-101| config iec-104| config gw| show}

    + ipsec {enable| disable| isakmp update| policy| preshared| log-show| show| show-sa proto}

    + ipsec-vpn tunnel {show | create | remove}

    + vpn {gre| ipsec| l2}

    + ping

    + reload {cancel| schedule| show}

    + schedule {add |show |remove}

    + serial {card |port| local-end-point| remote-end-point}

    + ssh

    + syslog show

    + telnet

    + terminal-server {admin-status| counters| settings| connections| serial-tunnel| telnet-service}

    + trace

    + version

System Version and Data Base

Configuration Database

User Configuration is taking effect immediately upon entering. No specific COMMIT command is required. In order to have configuration changes available after system reboot a COMMIT must take place.

The user can as well export his running configuration as a file with a chosen name for backup and import the file back to boot the system with when needed.

User configuration is saved using the following command

```
RL1000GW# commit
Building configuration...
[OK]
```

Removing all user configuration and setting the router to its factory defaults is done by erasing the RL1000GW.conf with the following command

```
RL1000GW# delete startup-cfg
RL1000GW# reload
```

Exporting the database is available using tftp to a tftp server.

```
RL1000GW# db export filename my-file-name remote-host aa.bb.cc.dd
```

NOTE: Importing of db file requires system reboot for its activation

OS VERSION

Updating of system version is available by TFTP/SFTP server od safe mode.

Available OS files on the router can be seen with command showed below.

Running OS file is marked with “active”.

```
RL1000GW#os-image show-list
Versions list:
RF _ RL1000GW _ 4.0.02.67.tar (active)
```

NOTE: The RL1000GW can hold at its disk maximum two OS image files. Before downloading a new OS file to the router make sure the RL1000GW has on it only one (the active) file. If needed, delete the unused file before attempting to download new.

Commands Hierarchy

+ Root

    - commit

    + delete

        - diagnostics

        - logs

        - startup-cfg

- os-image show-list

- os-image activate version-name <file_name

- os-image delete version-name <file_name>

- os-image download download-sw sftp://user:password@aa.bb.cc.dd/file_name

- os-image download download-sw tftp://aa.bb.cc.dd/file_name

- os-image download-status

-Reload

-db import {remote-host <IP, A.B.C.D>} [filename <>]

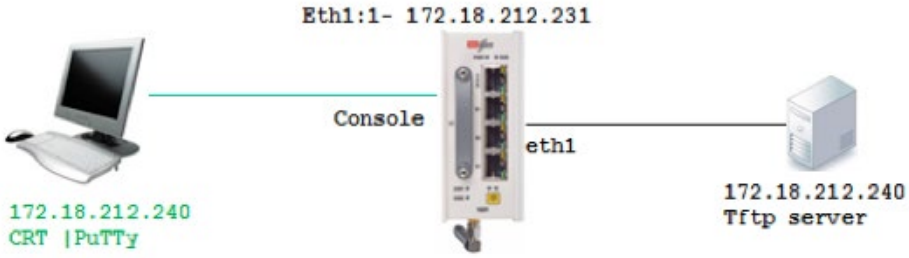
-db export {remote-host <IP, A.B.C.D>} [filename <>]

- show disk info

NOTE: System must be rebooted following activation of a new OS image file

Example

The following flow will show how to upgrade the OS image file and export the data base.



1. Connect your PC via serial console cable to the RL1000GW console port

2. Create an IP interface over eth1

```
RL1000GW#router interface create address-prefix 172.18.212.231/24 physical-interface eth1
purpose application-host
```

3. Check connectivity to the tftp server from which the software will be downloaded

```
PING 172.18.212.240 (172.18.212.240): 56 data bytes
64 bytes from 172.18.212.240: seq=0 ttl=64 time=1.026 ms
64 bytes from 172.18.212.240: seq=1 ttl=64 time=0.642 ms
64 bytes from 172.18.212.240: seq=2 ttl=64 time=0.647 ms
```

4. Display available OS files

```
RL1000GW# os-image show-list
Versions list:
RF _ RL1000GW _ 4.0.02.57.tar (active)
RF _ RL1000GW _ 4.0.02.56.tar
```

5. Deleting unneeded OS files

```
RL1000GW# os-image delete version-name RF _ RL1000GW _ 4.0.02.56.tar
RL1000GW# os-image show-list
Versions list:
RF _ RL1000GW _ 4.0.02.57.tar (active)
RL1000GW#
```

6. downloading OS file from TFTP server

```
Command syntax:
RL1000GW# os-image download download tftp://aa.bb.cc.dd/file _ name
Example:
os-image download download-sw tftp://172.18.212.240/RF _ RL1000GW _ 4.0.02.67.tar
```

7. following download progress

```
RL1000GW#os-image download-status

In progress 3 MB
RL1000GW#os-image download-status

In progress 10 MB
RL1000GW#os-image download-status

In progress 16 MB
RL1000GW#os-image download-status

Finished Download
```

8. Activating desired OS file (will automatically reboot the device)

```
RL1000GW# os-image activate version-name RF _ RL1000GW _ 4.0.02.67.tar
..
RL1000GW# os-image show-list
Versions list:
RF _ RL1000GW _ 4.0.02.57.tar
RF _ RL1000GW _ 4.0.02.67.tar (active)
```

9. Exporting configuration data base to TFTP server

```
Command syntax:
RL1000GW# db export filename my-file-name remote-host aa.bb.cc.dd
Example:
RL1000GW# db export filename db-May-14 remote-host 172.18.212.240
```

10. Importing configuration data base to TFTP server

```
Command syntax:
RL1000GW# db import filename my-file-name remote-host aa.bb.cc.dd
Example:
RL1000GW# db import filename db-May-14 remote-host 172.18.212.240
```

```
Completed OK, reboot to activate
RL1000GW# reload schedule in 0
```

Safe Mode

The system has two safe mode menus available.

To access safe mode, connect to the router via console cable, reboot the unit and interrupt the boot process at the safe mode prompt.

The first Safe mode is used for approved technician only and should not be used unless specified by ComNet. This safe mode state is available at the prompt

"For first safe mode Press 's'..."

The second safe mode is accessible at the following prompt:

##########################

For safe mode Press 's'...

##########################

Below screenshot details the 2 safe mode menus and their options for:

1. system reset
2. Load the factory-default configuration for the device
3. Write to EEPROM (should be used only after consulting with ComNet)
4. Recover the device's images from a package file
5. Export / Import DB (running configuration)

Safe mode view

```
For first safe mode Press 's'...
PHY: fixed-0:02 - Link is Up - 100/Full
s
-------------------------------------------------------------------------------
|safe mode menu:
|
|      reset               | 1 :  Reset the device
|
|      format              | 2 :  Format flash
|
|      activate            | 3 :  Activate sw version on flash
|
|      install             | 4 :  Install first sw version from TFTP
|
|      continue            | c :  Continue with start up process
|
|      help                | H :  Display help about this utility
|


c
Extracting software
\s
OK
01/01/70 00:01:09 Running applications

##########################
For safe mode Press 's'...
##########################


-------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device's images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      help                | H :  Display help about this utility
```

SW Image Installation

Following steps guides to software first installation.

1. Connect your PC via serial console cable to the RL1000GW console port

2. Rebott the unit and Enter safe mode. Select option 4

```
-------------------------------------------------------------------------------
|safe mode menu:
|
|      reset               | 1 :  Reset the device
|
|      format              | 2 :  Format flash
|
|      activate            | 3 :  Activate sw version on flash
|
|      install             | 4 :  Install first sw version from TFTP
|
|      continue            | c :  Continue with start up process
|
|      help                | H :  Display help about this utility
|


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!! This choice will delete data from flash !!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!               Continue [y/n]                !!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
y
```

3. Assign ip address and subnet to the RL1000GW

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Connect an ethernet cable to the ETH port and Enter the following parameters (xxx.xxx.
xxx.xxx) !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


DEVICE IP ADDRESS [10.10.10.5]: [enter here an ip for the RL1000GW]
DEVICE IP ADDRESS NETMASK [255.255.255.0]: [enter here subnet ip for the RL1000GW]
```

4. Choose the interface at which the telnet server is connected at

```
Select Interface (press 1 or 2)[1]:
1) ETH1 10/100 MB
2) ETH2
1
```

5. Set the ip address of the tftp server holding the OS-Image file

```
TFTP SERVER IP ADDRESS [10.10.10.10]: 10.10.10.6
```

6. Connect the RL1000GW at port ETH1 (RJ45) to your tftp server machine.

```
Verify ping availability between the two.
```

7. Enter the OS-image file name.

```
Enter version number on TFTP Server.
For main menu press X
RF _ RL1000GW _ 4.0.02.52.tar
```

8. OS-Image file will be downloaded and activated

```
01/01/70 00:03:18 downloading RF _ RL1000GW _ 4.0.02.52.tar from server 10.10.10.6 to /opt/
ComNet,try #1
==========25%==========50%==========75%=75%==========100%Version Download Complete
OEM Ver RF _ RL1000GW
OEM NEW _ VERSION RF _ RL1000GW _ 4.0.02.52.tar
Detected OEM 3
Veryfing sw version RF _ RL1000GW _ 4.0.0252.tar
=appl.tar.gz: OK
==vmlinux.UBoot: OK
SW version was verified successfully
vmlinux.tar
=vmlinux.UBoot: OK
Updating bank1 with vmlinux.UBoot file, please wait ...===OK
Version was installed and activated successfully
Reboot in 0=
```

Ethernet Port Interfaces

Depending on the variant ordered, your RL1000GW hardware may include the following Ethernet interfaces

Fastethernet, 10/100, copper RJ45. Included at all variants.

» Referred to in CLI as eth1.

Gigabitethernet, SFP SGMII. Optional ordering.

» SFP modules are not included.

» Copper and fiber SFP of 100/1000 types are supported.

» Referred to in CLI as eth2.

Commands Hierarchy

+ root

+ port

- set port { eth1| eth2} [admin-status {disabled |enabled}] [autoneg {on| off}] [duplex {half| full} [speed {10| 100| 1000}]

+ show

- interface-table port-type port {eth1| eth2}

- rmon-etherstat-table port {eth1| eth2}

- status

+ sf-port

- ddm

- detailed

- extended

Show example

```
RL1000GW# port show interface-table port eth1

                   Interface ETH1
+-----------------------+--------+------------------------+-------+
|       Counter Name       | Value  |       Counter Name        | Value |
+=======================+========+========================+=======+
| In non-unicast packets |  2670  | Out non-unicast packets |   5   |
+-----------------------+--------+------------------------+-------+
|   In unicast packets   |  233   |   Out unicast packets   |   4   |
+-----------------------+--------+------------------------+-------+
|   In errors packets    |   0    |   Out errors packets    |   0   |
+-----------------------+--------+------------------------+-------+
|        In octets         | 311651 |        Out octets         |  690  |
+-----------------------+--------+------------------------+-------+
|    Unknown packets     |   0    |                          |       |
+-----------------------+--------+------------------------+-------+

RL1000GW# port show status
+-----+------+------+-------------+-----------------+-------+--------+
| idx | slot | port | admin Status | auto Negotiation | speed | duplex |
+=====+======+======+=============+=================+=======+========+
|  1  |  1   | eth1 |   enabled    |         on         | 100M  |  full  |
+-----+------+------+-------------+-----------------+-------+--------+
|  2  |  1   | eth2 |   enabled    |         on         | 100M  |  full  |
+-----+------+------+-------------+-----------------+-------+--------+

RL1000GW# port show rmon-etherstat-table port eth1

                   Interface ETH1
+--------------+--------+---------------+-------+
| Counter Name  | Value  |  Counter Name  | Value |
+==============+========+===============+=======+
| total packets |  2789  |   undersize    |   0   |
+--------------+--------+---------------+-------+
| total octets  | 300591 |    oversize    |   0   |
+--------------+--------+---------------+-------+
|   broadcast   |  1832  |    Size 64     | 1055  |
+--------------+--------+---------------+-------+
```

```
|   multicast   |  725   |  Size 65-127   | 1239  |
+---------------+--------+----------------+-------+
|  align error  |   0    |  Size 128-255  |  435  |
+---------------+--------+----------------+-------+
| dropped event |   0    |  Size 256-511  |  35   |
+---------------+--------+----------------+-------+
|  fragmented   |   0    | Size 512-1023  |   4   |
+---------------+--------+----------------+-------+
|    jabbers    |   0    | Size 1024-1518 |  21   |
+---------------+--------+----------------+-------+
```

Login and Management

Configuring the Login Authentication Method sets the authentication method for user logins.

Default user of the system:

» Name : su
» Password : 1234
» Privileges : all
» Available by: Console and Telnet.

Serial Console Port

Management over the serial console port is enabled by default.

NOTE: A console cable is supplied in the box. The cable is uniquely colored white.

Connecting to the Console Port

The console port is an EIA232 VT-100 compatible port to enable the definition of the device's basic operational parameters.

Connecting the device to a PC using the Console Port:

Connect the RJ-45 connector of the console cable to the device's Console Port (CON).

Connect the other side of the cable to the PC.

Configure the PC port to 9600-N-8-1 (9600 bps, no parity,8 data bits, 1 stop bit, no flow control)

Below table details the console cable pin-out.

RJ45 Male	DB9 Female
1	-
2	3
3	2
4	5
5	5
6	-
7	-
8	-

CLI Terminal Commands

Following are commands related to the CLI terminal.

+ root

    - idle-timeout

Management

The router can be managed via following methods:

» IP based.

» Serial console port.

Default state

Feature	Default state
Layer 3 interface	No default IP
SSH	No available
Telnet	Enabled
Console	Enabled
User	User name : su
Password : 1234	
Privilege : all	
DHCP Client	disabled

Commands Hierarchy

+ root

+ reload

    - schedule date-and-time YYYY-MM-DD,HH:MM:SS

    - schedule every <180 – 604800 seconds >

    - schedule time HH:MM:SS

    - schedule in <0 – 604800 seconds >

    - cancel

    - show

+ users

    - modify username su password <password>

    - show

- commit

- delete diagnostics

- delete logs

- delete startup-cfg

- show disk info

- router interface show

- ping <destination>

- ssh {<user>@<remote IP>}

- telnet [user]@{remote IP}

Commands Description

Command	Description
reload schedule date-and-time	Set specific date and time for router reload. Time format: YYYY-MM-DD,HH:MM:SS configuration which was not committed will not be available after reload!
reload schedule every	Set time interval for cyclic automatic system reload. Permissible range in seconds is 180 – 604800. Configuration which was not committed will not be available after reload!
reload schedule time	Set specific time for router reload. Time format: HH:MM:SS configuration which was not committed will not be available after reload!
reload schedule in	Set specific timer for next router reload. Permissible range in seconds is 180 – 604800. Configuration which was not committed will not be available after reload!
reload cancel	Cancels all scheduled automatic reloads
reload show	Shows user set scheduled reloads
Users	password: alpha-numeric string. Mandatory to consist of minimum one Capital letter, one small letter, one special symbol, one number. Changing password is permitted to the default user 'su' only. Once changed from the default password 1234, returning to password 1234 is only possible by clearing the router to its manufacturing defaults from safe mode.

IP Interfaces

The RL1000GW supports multiple layer 3 interfaces to be set for the purposes of:

» Routing.
» Management.
» Serial services.

IP Interfaces

The following services require assignment of an IP interface.

» DHCP client
» Management
» Ping
» Trace route
» OSPF
» RIPv2
» Tftp client
» Serial tunneling
» Terminal server
» Protocol gateway
» L2-VPN
» L3-DMVPN
» IPSec

Interface Assignment Rules

» An IP interface may optionally be set with a VLAN tag to result on vlan tagging at the interface egress.
» The VLAN tag set to an interface must be unique.
» If a vlan tag is not set, packets will carry no vlan tag when egress the interface.
» An interface ID is automatically assigned to each IP interface.
» Each interface must be associated with a “purpose”.
  › One (and only one) of the interfaces must be set to purpose ‘application-host’
  › All other interfaces must be set to purpose ‘general’
  › If a “purpose” is not configured by the user, the interface will receive the ‘general’ status.

» Each interface must be in a unique subnet.

» Each interface must be associated to a physical interface. Either eth1 or eth2. An interface cannot be associated with both.

» Physical interfaces (eth1, eth2) may be associated with more than one IP interface. Tagged packets accessing the port will be routable to a relevant vlan IP interface. Untagged packets accessing the port will be routable with IP interface set to be in the same subnet as the packets origin (if such is available at the RL1000GW).

» IP interfaces associated to vlans are given an automatic name indicating the vlan tag they are created with. The name format is:
eth<1|2>.<vlan id>

» IP interfaces not associated to a vlan, are given an automatic name indicating the id they are created with. The name format is:
eth<1|2>:<id>

» Below is an example of interfaces configured with either vlan tag or id tag.

```
[/]router interface show
+----+------+---------+------------------+------+-----------------+-------------+----------
---+
| Id | VLAN |  Name   |      IP/Subnet      | Mtu  |      Purpose       | Admin status |
Description |
+====+======+=========+==================+======+=================+==============+====
=========+
| 1  | N/A  | eth1:1  | 172.17.203.100/24 | 1500 | application host |    enable    |
|
+----+------+---------+------------------+------+-----------------+-------------+----------
---+
| 2  |  20  | eth2.20 | 172.18.212.200/24 | 1500 |     general       |    enable    |
|
+----+------+---------+------------------+------+-----------------+-------------+----------
---+
[/]
```

IP interface id

When an IP interface is created without explicitly assigned vlan tag, it will not support vlan tagging. Packet coming inward to the physical interface (eth1 or eth2 as assigned) which are holding a vlan tag will not be received by the IP interface.

Packets originated from the IP interface (egress) will be without vlan tag.

NOTE: Use id assignment to an IP interface when the network does not support vlan tagging and ingress packets to the physical interface are untagged.

IP interface VLAN id

When an IP interface is assigned with a VLAN id it supports vlan tagging. Packet coming inward to the physical interface (eth1 or eth2 as assigned) will be received by the IP interface only if holding the required VLAN tag.

Packets originated from the IP interface will be without vlan tag.

NOTE: Use VLAN assignment to an IP interface when the network supports vlan tagging and a service segregation is required.

IP Interface Commands Hierarchy

+ root

    + router

        - interface {create | remove} address-prefix <IP address>/<netmask> [vlan <vlan id>] purpose {application-host |general} physical-interface [eth1 |eth2] [description <>] [mtu <1500,(128-1544)>]

    + static

        - enable

        - dissable

        - show running-cofig

        - exit

        + configure terminal

            - [no] ip route static <dest network> /<subnet> <Gateway>

            - write memory

- exit

+ dhcp {enable | dissable |show}

- enable physical-interface {eth1| eth2}

- disable physical-interface {eth1| eth2}

- show physical-interface {eth1| eth2}

- interface show

- route show

IP Interface Commands Description

Command Description

Router Enter the router configuration mode

interface
create | remove Add or Remove an IP interface. The configuration should include:
Address-prefix : IP address in the format aa.bb.cc.dd/xx
VLAN: vlan ID for egress packets from the interface
Purpose: application-host or general.
physical-interface: association to the relevant Ethernet port [eth1 |eth2]
mtu: set size in bytes. Default is 1500
description: descriptive text

Static Access the router static mode.
Enable: enable configuration
Disable: disable configuration
Exit: exit to upper level
show running-cofig: static route config

configure terminal

[no] ip route static dest network: a.b.c.d
subnet: 0-32
gateway: a.b.c.d

Show Show application engine IP interfaces

Example

1. Create an IP interface with vlan 1 and static route (default gateway).

```
RL1000GW#
router interface create address-prefix 10.10.10.100/24 vlan 5 purpose application-host
physical-interface eth1
commit
commit ok
router interface show
+----+------+--------+------------------+------+-----------------+-------------+-----------
--+
| Id | VLAN |  Name  |      IP/Subnet      | Mtu  |      Purpose       | Admin status |
Description |
+====+======+========+==================+======+=================+=============+=====
========+
| 1  |  5   | eth1.5 | 10.10.10.100/24   | 1500 | application host |     enable     |
|
+----+------+--------+------------------+------+-----------------+-------------+-----------
--+
[router/] static
router/static> enable
router/static# configure terminal
router/static(config)# ip route 0.0.0.0/0 172.17.212.100
router/static(config)# write
router/static(config)# exit
router/static# exit
commit

router route show
Kernel IP routing table
Destination     Gateway         Genmask          Flags Metric Ref    Use Iface
172.17.212.0    0.0.0.0         255.255.255.0    U     0       0          0 eth1.100
0.0.0.0         172.17.212.100  0.0.0.0          UG    0       0          0 eth1.100
Completed OK
```

2. Create an IP interface without vlan id

```
RL1000GW#

RL1000GW#router interface create address-prefix 172.17.203.100/24 physical-interface eth2
purpose application-host

commit

commit ok

RL1000GW#router interface show
+----+------+--------+------------------+------+-----------------+-------------+-----------
--+
| Id | VLAN |  Name  |      IP/Subnet      | Mtu  |      Purpose       | Admin status |
Description |
+====+======+========+==================+======+=================+==============+=====
========+
| 1  | N/A  | eth2:1 | 172.17.203.100/24 | 1500 | application host |     enable     |
|
+----+------+--------+------------------+------+-----------------+-------------+-----------
--+
```

Example

1. Enable dhcp on interface eth1 to retrieve an IP from a dhcp server

```
RL1000GW#
[/]router dhcp enable physical-interface eth1

[/]router interface show
+------+------+-----+-----------+---------+-------------+
| VLAN | Name | Id  | IP/Subnet | Purpose | Description |
+======+======+=====+===========+=========+=============+
| N/A  | eth1 | N/A |    N/A    |   N/A   |    DHCP     |
+------+------+-----+-----------+---------+-------------+
[/]

[/]router interface show
+------+------+-----+------------------+---------+-------------+
| VLAN | Name | Id  |     IP/Subnet    | Purpose | Description |
+======+======+=====+==================+=========+=============+
| N/A  | eth1 | N/A | 172.18.212.242/28 |   N/A   |    DHCP     |
+------+------+-----+------------------+---------+-------------+
```

Diagnostic

System logs export

The system logs can be exported to the flash drive as a time conditioned task.

Commands Hierarchy

+ Root

  + schedule

    - add task-name copy-logs [day |hour |minute |month |year]

    - remove task-name copy-logs

    - show

Commands Description

Command	Description
Schedule	manage scheduled task to copy system logs to the usb drive. To mound a usb drive insert it to the router usb port and reboot the router.
add task-name copy-logs	Add a scheduled task to copy system logs to the usb drive. Day : <1-31> Month : <1-12> year : <2013 -3000> hour : <1-24> minute : <1-60>
remove task-name copy-logs	Remove a scheduled task to copy system logs to the usb drive.
Show	Display tasks

Capture Ethernet service traffic

The system supports sniffing and capturing of Ethernet traffic for selected service IP interfaces. This capability is important in order to diagnose network traffic of a service for debugging.

The capturing is available for IP interfaces set at the ACE.

Captures can be displayed at the terminal or exported to a user tftp server.

Commands Hierarchy

+ root

  + capture

    - start –i {eth1.<vlan id> | eth1:<id>} [-C] [-s] [-y] [expression <>]

    - stop

    - delete

    - export remote-address <destination address,A.B.C.D>

    - show {captured-packets –c <number>| status}

    - help

Commands Description

Command	Description
Capture	Start: initiate Ethernet traffic capture on a selected ACE IP interface. -i: mandatory prefix to be followed with the IP interface name eth1.<vlan id> where “vlan id” is the vlan of the ip interface. Stop : stop Ethernet traffic capture Delete : delete capture files Export remote-address: export file to a tftp server. Show captured-packets –C<1-200>: display the captured content up to a chosen length (1-200) lines. Show status : display capture configuration Help: display help on settings options.

Example

1. Set an ip interface in the ACE for the vlan

```
router interface create address-prefix 172.18.212.232/24 vlan 1 purpose application-host
physical-interface eth2
commit
commit ok
```

```
router interface show
+------+--------+-----+----------------+-----------------+-------------+
| VLAN |  Name  | Id  |    IP/Subnet   |     Purpose     | Description |
+======+========+=====+================+=================+=============+
|  1   | eth2.1 | N/A | 172.18.212.232/24 | application host |             |
+------+--------+-----+----------------+-----------------+-------------+
```

2. Start capture

```
Capture start –i eth2.1
Capture show
[capture/] show status
capture is running
```

3. Stop the capture and display the output

```
Capture stop
capture show captured-packets -c 10
16:55:07.370814 IP 172.18.212.240.netbios-ns > 172.18.212.232.netbios-ns: NBT UDP PACKET(137):
QUERY; POSITIVE; RESPONSE; UNICAST
16:55:07.616319 IP 172.18.212.240.17500 > 255.255.255.255.17500: UDP, length 112
16:55:07.616628 IP 172.18.212.240.17500 > 172.18.212.255.17500: UDP, length 112
16:55:07.926503 arp who-has 172.18.212.232 tell 172.18.212.64
16:55:08.122046 IP 172.18.212.240.netbios-ns > 172.18.212.232.netbios-ns: NBT UDP PACKET(137):
QUERY; POSITIVE; RESPONSE; UNICAST
16:55:08.258801 arp who-has 172.18.212.232 tell 172.18.212.40
16:55:08.602306 IP 172.18.212.40.17500 > 255.255.255.255.17500: UDP, length 112
16:55:08.604927 IP 172.18.212.40.17500 > 255.255.255.255.17500: UDP, length 112
16:55:08.605016 IP 172.18.212.40.17500 > 172.18.212.255.17500: UDP, length 112
16:55:08.680664 CDPv2, ttl: 180s, Device-ID 'Router'[|cdp]
```

Syslog

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present.

This simplicity has greatly aided the acceptance and deployment of syslog.

User enables syslog server and configures the syslog related parameters. The logging process controls the distribution of logging messages to the various destinations, such as the local buffer or syslog server.

Severity of logging can be set with its name tag.

The syslog works in UDP mode, default port 514.

The default state of the syslog is enabled, destination ‘local’.

The Priority indicator

The Priority indicator is calculated as:

Priority = 8x facility_coefficient + severity_level.

facility coefficient	facility	Priority
0	kernel messages	0x8 + level
1	user-level messages	1x8 + level
2	mail system	2x8 + level
3	system daemons	3x8 + level
4	security/authorization messages	4x8 + level
5	messages generated internally by syslog	5x8 + level
6	line printer subsystem	6x8 + level
7	network news subsystem	7x8 + level
8	UUCP subsystem	8x8 + level
9	clock daemon	9x8 + level
10	security/authorization messages	10x8 + level
11	FTP daemon	11x8 + level
12	NTP subsystem	12x8 + level
13	log audit	13x8 + level
14	log alert	14x8 + level
15	clock daemon (note 2	15x8 + level
16	Local0	16x8 + level
17	Local1	17x8 + level
18	Local2	18x8 + level
19	Local3	19x8 + level
20	Local4	20x8 + level
21	Local5	21x8 + level
22	Local6	22x8 + level
23	Local7	23x8 + level

Example, Syslog message priority tag with facility local0

Level purpose	Numeric level	Priority (w. local0)
emergencies	0	16x8+0=128
alerts	1	129
critical	2	130
errors	3	131
warnings	4	132
notification	5	133
informational	6	134
debugging	7	135

Message Format

The following will describe the structure of syslog messages.

Message severity

Severity	S indicaror	Description
0	S=E	Emergency: system is unusable
1	S=A	Alert: action must be taken immediately
2	S=C	Critical: critical conditions
3	S=E	Error: error conditions
4	S=W	Warning: warning conditions
5	S=N	Notice: normal but significant condition
6	S=I	Informational: informational messages
7	S=D	Debug: debug-level messages

Firewall TCP SCADA Protocols

The following will describe the ComNet structure of syslog messages generated for firewall of IEC 104, DNP3 TCP, MODBUS TCP.

Console message format

The message format when sent to the CLI console is as follow,

```
{[APP-NAME] [PROCID][Severity] [MSGID] [Time Stamp]} {[MSG]} {STRUCTURED-DATA}
```

The message structured data includes following information fields,

```
|S=SEVERITY|SG=VLAN _ ID|SRC=SRC _ IP _ ADDR:SRC _ IP _ PORT|DST=DEST _ IP _ ADDR:DEST _ IP _
PORT|LEN=DATA _ MSG _ LEN|TTL=TTL|PROTO=PRTOCOL _ NAME|MSG=VIOLATION _ DESCR|
```

Examples of messages received at the CLI

(Use the command “firewall log show” at the ACE to retrieve following log entries.)

1. Example for violation type “no rule configured”

```
- RF _ Syslog : module 3 (firewall) severity 3 message : firewall
- |ID=74|T=2014-05-12,11:52:43
|S=E|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x100]
[45,0]:FW RULE - no rule configured| (164 bytes)
```

2. Example for violation type “protocol type mismatch”

```
- RF _ Syslog : module 3 (firewall) severity 1 message : firewall
- |ID=80|T=2014-05-12,11:52:59
|S=A|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x101]
[45,0]:FW PROTOCOL protcol type missmatch| (170 bytes)
```

Server message format

The message format when sent to a SYSLOG server is,

```
{<PRI> [Host IP] [Time Stamp] [APP-NAME]} {MSG} {STRUCTURED-DATA}
```

The message structured data includes following information fields,

```
|S=SEVERITY|SG=VLAN _ ID|SRC=SRC _ IP _ ADDR:SRC _ IP _ PORT|DST=DEST _ IP _ ADDR:DEST _ IP _
PORT|LEN=DATA _ MSG _ LEN|TTL=TTL|PROTO=PRTOCOL _ NAME|MSG=VIOLATION _ DESCR|
```

Examples of messages received at a server

1. Example for violation type “no rule configured”

```
- Local0.Error  172.18.212.183  May 12 11:52:54 SW RLGE2FE16R firewall
- |ID=79|T=2014-05-12,11:52:54
|S=E|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=62|TTL=128|PROTO=iec104|MSG=[0x100]
[45,0]:FW RULE - no rule configured|
```

2. Example for violation type “protocol type mismatch”

```
- 05-12-2014  16:53:40  Local0.Alert  172.18.212.183  May 12 11:52:59 SW RLGE2FE16R firewall
- |ID=80|T=2014-05-12,11:52:59
|S=A|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x101]
[45,0]:FW PROTOCOL protcol type missmatch| (170 bytes)
```

Firewall Serial SCADA Protocols

The following will describe the ComNet structure of syslog mssages generated for firewall of IEC 101, DNP3 RTU, MODBUS RTU.

```
IP=IP _ ADDR|SLOT=SLOT _ NUMBER|PORT=PORT _ NUMBER|DIR=DATA _ MSG _ DIR|LEN=DATA _ MSG _
LEN|PROTO=PROTOCOL _ NAME|MSG=VIOLATION _ DESCR|
```

Message fields description

The following will further describe the syslog message fields

Command	Description
VLAN_ID	The VLAN number
SRC_IP_ADDR	The pointed string source IP address.
SRC_IP_PORT	The source IP port number
DEST_IP_ADDR	The pointed string destination IP address.
DEST_IP_PORT	The destination IP port number
DATA_MSG_LEN	The total data message length
TTL|	The ttl value of the IP header
PRTOCOL_NAME	The protocol name field. The following values are available: "any" "icmp" "tcp" "udp" "ipencap" "gre" "modbus_tcp" "modbus_rtu" "iec104" "iec101" "dnp3"
VIOLATION_DESCR	The FW violation description string. The following format is used: [Major Protocol Id,Minor Protocol Id]:Violation description string Major Protocol Id: Major protocol id value, for ModBus – Function Code for IEC101/104 - Type Id for DNP3 - Function Code Minor Protocol Id: Minor protocol id value, for ModBus – Sub-Function Code for IEC101/104 - non used for DNP3 - non used Violation description string: The following values are available for general violations: "Flow is not allowed" "FW PROTOCOL no violation" "FW internal error (no drop)" "FW PROTOCOL SW problem" "FW PROTOCOL no free memory" "FW PROTOCOL illegal message length" "FW PROTOCOL illegal data length" "FW PROTOCOL illegal value", "FW PROTOCOL Timeout problem" "FW PROTOCOL message flow inconsistancy" "FW PROTOCOL invalid creation" "FW PROTOCOL general flow error" "FW PROTOCOL illeagl message" "FW PROTOCOL general session problem" "FW PROTOCOL illegal identifier" "FW PROTOCOL illegal address" "FW PROTOCOL protcol type missmatch" "FW RULE - illegal flow" "FW RULE - illegal message" "FW RULE - illegal identifier" "FW RULE - illegal address" "FW RULE - no rule configured"

Command	Description
VIOLATION_DESCR	The following values are available for MODBUS protocol violations: "Modbus validity: illegal function" "Modbus validity: illegal sub-function" "Modbus validity: illegal encapsulated interface" "Modbus validity: unknown device ID" "Modbus validity: illegal quantity " "Modbus validity: illegal FIFO byte counter" "Modbus validity: illegal FIFO counter" "Modbus validity: illegal record number" "Modbus validity: illegal reference type" "Modbus validity: illegal byte counter" "Modbus validity: illegal length of File sub-record" "Modbus validity: illegal write quantity", "Modbus validity: illegal read quantity" "Modbus validity: illegal File sub-record length" "Rule violation: not allowed function" "Rule violation: not allowed sub function" "Rule violation: out of allowed address range" "Rule violation: not allowed quantity" "Rule violation: out of allowed value range" "Rule violation: not allowed sub function" "Rule violation: not allowed file number" "Rule violation: not allowed record number" "Rule violation: out of allowed READ address range" "Rule violation: out of allowed WRITE address range" "Rule violation: not allowed READ quantity" "Rule violation: not allowed WRITE quantity" "Rule violation: out of the allowed address range" "Rule violation: out of the allowed FIFO addresse range" "Rule violation: out of the allowed encapsulated interface range" "Rule violation: out of the allowed devise identifiers range" "Rule violation: out of the allowed object identifiers range" "Rule violation: address and quantity are out of the allowed range" "Rule violation: illegal operation" "Rule violation: inconsistent TCP Unit Identifier" The following values are available for IEC104/IEC101 protocol violations: "Iec104 validity: Illegal TypeId field" "Iec104 validity: Illegal Cause field" "Iec104 validity: Illegal APCI header" "Iec104 validity: Illegal Control field 1 in APCI header" "Iec104 validity: Illegal Control field 2 in APCI header" "Iec104 validity: Illegal Control field 3 in APCI header" "Iec104 validity: Illegal Control field 4 in APCI header" "Iec104 rule validity: Illegal type id, no rule" The following values are available for DNP3 protocol violations: "DNP3 validity: Illegal Function Code field" "DNP3 validity: Illegal Group Id field" "DNP3 validity: Invalid Object" "DNP3 validity: Parsing Error" "DNP3 validity: unused" "DNP3 validity: unused" "DNP3 validity: unused" "DNP3 validity: unused" "DNP3 validity: MAX"
SLOT_NUMBER	Serial Slot number on ComNet equipment
PORT_NUMBER	Serial port number on ComNet equipment
DATA_MSG_DIR	The field defines data message direction. The following values are available: "access", "network", "N/A"

DM-VPN logs

The following will describe the DM-VPN logs.

Message fields description

The following will further describe the syslog message fields

Ssylg message	Description
"NHRP Event:<NHS-UP|NHS-DOWN>,i/f=<MGRE IF NAME>,NHS=<address>"	Appears when NHS status changed in spoke, happen when registered to NHS (NHS-UP) or NHS became unreachable (NHS-DOWN).
"<MGRE IF NAME>,<ip/mask>,<NBMA NAME>: state change <UP|DOWN> -> <UP|DOWN>"	Appears when status of mgre interface changed.
"Handle interface UP, walk over upper layer device via <ppp0>,Operator:<Mobile Operator>"	Appears when cellular interface connected to mobile network
"Handle interface DOWN, walk over upper layer devices via %s"	Appears when cellular interface disconnected from mobile network
"WTR expired for <ip/mask>,<MGRE IF NAME>"	Wait to restore timer expired. Relevant when protection group is configured between dm vpn interfaces
"WTR started for <MGRE IF NAME> <ip/mask>,<NBMA address> "	Relevant when protection group is configured between dm vpn interfaces
"WTR stopped for <MGRE IF NAME> <ip/mask>,<NBMA address> "	Relevant when protection group is configured between dm vpn interfaces
"Failed to create dm-vpn mGRE interface <MGRE IF NAME>"	Unexpected error while creating mGRE interface.
"Failed to reload config with <Mobile operator>"	Unexpected error trying to change configuration.
"Failed to create ipsec tunnel <IPSEC tunnel name>"	Failed to create ipsec tunnel
Failed to remove dm-vpn mGRE interface <MGRE IF NAME>"	Failed to remove dm-vpn mGRE interface
"Failed to remove ipsec-vpn tunnel <IPSEC tunnel name>"	Failed to remove ipsec-vpn tunnel

Cellular logs

The following will describe the Cellular logs.

Message fields description

The following will further describe the syslog message fields

Syslog message	Description
"admin status <UP|DOWN>"	Cellular enabled/disabled
"Modem is busy or no ready SIM, retrying..."	Modem is not responsive or SIM cards are not present
"Cellular Admin UP cannot be applied, SIMs are disabled. Stop operation"	SIMs are not configured.
"No ready SIMs"	A SIM is enabled, but not in READY state
"Only SIM in slot <1|2> is ready"	Only SIM in slot <1|2> is ready
"slot <1|2> is preferred"	slot <1|2> is selected as preferred
"<1|2> slot has better(or equal) RSSI (<RSSI>>=<RSSI>). Threshold is <Threshold>"	

Syslog message	Description
"Both slots are below required threshold <RSSI>,<RSSI> (threshold=<Threshold>)"	Both slots are below required threshold
"<1|2> slot is above threshold as required <RSSI>>=<RSSI>. Other slot <RSSI>"	"<1|2> slot is above threshold as required
"disconnected... attempt moving to alternative provider will be performed"	Announced disconnection while other provider is configured
"disconnected... attempt to recover will be performed"	Announced disconnection while other provider is not configured
"failed to connect... attempt to recover will be performed"	Announced failure while trying to connect
"T2 expired - remove caveat on slot <1|2>"	Announce of T2 timer expiration
"T1 expired on slot <1|2>"	Announce of T1 timer expiration
"Wait to restore expired. Attempt to move to primary..."	Wait to restore expired. Attempt to move to primary SIM
"Wait to restore expired, but primary SIM is not present or disabled"	Wait to restore expired, but primary SIM is not present or disabled
"RSSI is <RSSI> - below required threshold (<Threshold>)"	RSSI is <RSSI> - below required threshold
"RSSI is <RSSI> - below required threshold (<Threshold>), but primary SIM is not present or disabled"	RSSI is <RSSI> - below required threshold (<Threshold>), but primary SIM is not present or disabled
"Continiuty check failed, attempt moving to alternative provider will be performed "	Announce cont. check failure when alternative provider is configured
"Continiuty check failed, attempt to recover will be performed"	Announce cont. check failure when no alternative provider is configured
"unexpected failure, keep trying.... Retry within <SEC> sec"	Announce unexpected failure
"Clear caveat on slot <1|2>"	Announce clear caveat of specified slot
"Retry threshold exceeded <RETRIES>, reloading switch!"	Announce threshold exceeded of cellular failures while trying to connect
"<ppp0> connected to <Operator>,IP <address>, BAND=<WCDMA|GSM>, Channel=<channel>"	Cellular connection information
"Periodic echo check failed <NAME> LOSS=<%LOSS>(threshold=<%THRESHOLD>), RTT=<Round Trip>(threshold=<THRESHOLD>)"	Echo test failure
"change SIM slot to <1|2>"	SIM change
"SIM[<1|2>] state chg: <UNKNOWN|DISABLED|NOT_PRESENT|PIN_LOCK|PUK_LOCK|READY|CONNECTING|FAILED|CONNECTED|CONNECTED-AS-ALTERNATIVE|CONNECTED-AS-SECONDARY> ->	
<UNKNOWN|DISABLED|NOT_PRESENT|PIN_LOCK|PUK_LOCK|READY|CONNECTING|FAILED|CONNECTED|CONNECTED-AS-ALTERNATIVE|CONNECTED-AS-SECONDARY>"	SIM state change
"Cellular experienced <NUM1> backpressure events in last <NUM2> seconds.Total since connected <NUM3>: <NUM4>"	This log is to help to fine tune the rate limit for cellular interface (Relevant when QOS is enabled)

Serial Services logs

The following will describe the serial services logs.

<STRING from the module>
"connection with remote IP(<address>) for serial service id <SVC> is now resumed!!"
"no connection with remote IP(<address>) for serial service id <SVC>"
"no more missing data on Serial service id # <SVC>"
"Missing data on Serial service id # <SVC>"
"Serial Card on slot (<Slot>) is Active"
"Serial Card on slot (<Slot>) failure! Last seen <SEC>"
"Serial Station[<SLOT>,<PORT>]: Traffic is now resumed. Time=<TIME>, service-id <SVC>"
"Serial Point[<SLOT>,<PORT>,<SVC>]: No traffic since <TIME> (latest Rx=<NUM>)"

Scheduled Reload logs

The following will describe the scheduled reload logs.

Ssylog message
"Reload will happen every <SEC> seconds"
"Scheduled reload at <TIME> (within <SEC> seconds),daily=<TIME>"
"Next reload in <SEC> seconds"
"Scheduled reloading happens now!"

Commands Hierarchy

+ root

  + syslog

    - level severity { emergencies | alerts | critical | errors | warnings | notification | informational |debugging}

    - remote {remote-address <a.b.c.d>} [remote-port (514,<514-9999>)]

    - local

    - show

    -..

Output example

A typical output of syslog at console interface

```
May 18 19:27:48 SmartSwitch user.warn kernel:  Speed 100 Duplex 1 pause 0
May 18 19:27:48 SmartSwitch user.warn kernel: adjust _ link Addr 1 link 0 speed 100 o 100
dup 1 o 1
May 18 19:27:48 SmartSwitch user.info kernel: PHY: mdio@ff724000:01 - Link is Down
May 18 19:27:50 SmartSwitch user.warn kernel: adjust _ link Addr 1 link 1 speed 100 o 0 dup
1 o -1
May 18 19:27:50 SmartSwitch user.info kernel: PHY: mdio@ff724000:01 - Link is Up - 100/Full
```

Discrete IO Channels

Discrete signals are very common in industrial applications to monitor alarms and indications from the field side.

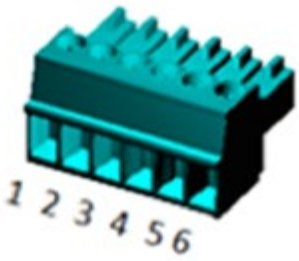
Monitoring the state of discrete input channels is supported by the RL1000GW.

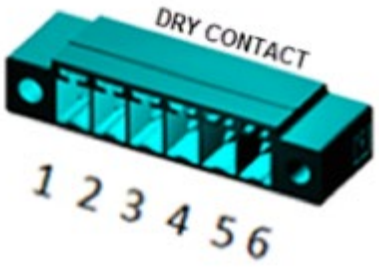
NOTE: Software support for the DI channels will be available from R5.0

Interfaces

Connection terminal are as shown in below figure.

1. Digital output 1
2. Digital output 2
3. Digital output ground
4. Digital Input ground
5. Digital Input 2
6. Digital Input 1





Diagnostics and logic states

1. Within the CLI diagnostics of the discrete channels can be viewed using the show command

```
RL1000GW # discrete show
```

2. Status of digital input is either high or low.
    a. Default: low.
3. Status of digital output is either open or closed.
    a. Default – open.

Technical data

At digital Inputs please connect a DC source in the range 12vDC at terminals 6,4 for channel 1 or 5,4 for channel 2.

Digital outputs are dry mechanical relay contacts. Maximum power to be implemented at the contacts :

AC: Max 250v, 37.5vA.

DC: Max 220v,30 watt.

Above mentioned power limitations should not be exceeded.

Maximum current allowed at the contacts is 1A.

Discrete IO Channels Commands Hierarchy

+ root

    + discrete

        - show

Discrete IO Channels Commands

Command	Description
Discrete	Enter the configuration mode for a specific physical serial ports
Show	

Clock and Time

Local time set and update is available.

Local Clock

Commands Hierarchy

+ config terminal

    + date {[YYYY.]MM.DD-hh:mm[:ss] | hh:mm[:ss]}

    - date

Commands Description

Command	Description
Config terminal	
date {[YYYY.]MM.DD-hh:mm[:ss] | hh:mm[:ss]}	Sets the current time and date.
date	Show the system time

1. Example for time configuration

```
RL1000GW#date 2014.02.02-10:01:30
Sun Feb 2 10:01:30 UTC 2014
Current RTC date/time is 2-2-2014, 10:01:30.
RL1000GW# date
Sun Feb 2 10:01:34 UTC 2014
```

TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

TACACS is used for several reasons:

» Facilitates centralized user administration.

» Uses TCP for transport to ensure reliable delivery.

» Supports inbound authentication, outbound authentication and change password request for the Authentication service.

» Provides some level of protection against an active attacker.

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or Network Access Server. TACACS+ allows a client to accept a username and password and sends a query to a TACACS+ authentication server, sometimes called TACACS+ daemon or simply TACACS+D.

The TACACS+ server is generally a program running on a host. The host determines whether to accept or deny the request and sends a response back.

Default Configurations

Feature	Default Setting
TCP port	49
retries	1
Timeout	5 msec
login authentication	Local
Operation state	disabled

TACACS Command Hierarchy

+root

- login authentication {local, local| tacacs-only| tacacs-local}

- login authentication show

+ tacacs-server

    - add {host <a.b.c.d.>} {retries (1,<1-10>} [timeout <5,(1-255)>] {port <49,(1-65535)>}

    - remove {host <a.b.c.d.>}

    - tacacs-server default host {host <a.b.c.d.>}

TACACS Commands Descriptions

Command	Description
login authentication	Select the authentication type. Local: tacacs is not used. authentication is based on local database only. Tacacs-only: tacacs server is used for authentication. If the server is unreachable, no fallback to local database. Tacacs-local: tacacs server is used AS default for authentication. If the server is unreachable, fallback to local database is supported.
tacacs-server add	This command configures the TACACS server with the parameters (host, retries, key) and specifies the IP address of one or more servers. Host <ipv4-address>: Configures the IPv4 address of the server (host). Port <tcp port (1- 65535)>: Configures the TCP port number in which the multiple sessions are established. The value ranges between 1 and 65535. default- 49. Retries <(1-10)>: Number of retries to connect to the host. default- 1. Key <secret key>: Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64. should be 1-64 charaters length. - May include small letters. - May include capitol letter. - must include numbers - May include special symbol. - allowed synbols: @#$%^&*()-+./<\`
tacacs-server remove	Host <ipv4-address>: Configures the IPv4 address of the server (host).
tacacs-server default host	This command sets the default server to be used. The server must be predefined.

Configuration Example

1. Set the authentication mode to tacacs

```
RL1000GW# login authentication tacacs-local
```

2. configure server list

```
RL1000GW# tacacs-server add host 192.168.1.250 key Ab11#59 retries 5 timeout 50 port 49
RL1000GW# tacacs-server add host 172.18.212.230 key Ab11#RF
```

3. configure default server

```
RL1000GW# tacacs-server default host 192.168.1.250
RL1000GW# commit
```

```
RL1000GW# tacacs-server show
+----------------+------+---------+---------+---------+
|      server      | port | retries | timeout | default |
+================+======+=========+=========+=========+
| 172.18.212.230 |   49   |     1     |     5     |           |
+----------------+------+---------+---------+---------+
| 192.168.1.250   |   49   |     5     |    50     |     *     |
+----------------+------+---------+---------+---------+
RL1000GW# login authentication show
login authentication tacacs-local
RL1000GW#
```

ACLs

ACLs (Access Control Lists) filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. ACLs are used to block IP packets from being forwarded by a router. The router examines each packet to determine whether to forward or drop the packet, based on the criteria specified within the access lists. Access list criteria can be the source address of the traffic, the destination address of the traffic or the upper-layer protocol.

There are many reasons to configure access lists - access lists can be used to restrict contents of routing updates or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for the network. Access lists must be used to provide a basic level of security for accessing the network. If access lists has not been configured on the router, all packets passing through the router can be allowed onto all parts of the network. For example, access lists can allow one host to access a part of the network and prevent another host from accessing the same area.

Flow of ACL Inspection

ACL Rules

- An ACL has a unique identifier, acl number <1001-65535>.
- ACL may consist of a single, or multiple rules.
- Each rule represents a specific condition to inspect the packet with and for which an action of permit/deny is set.
- A rule is assigned explicitly to a specific, single ACL.
- Each ACL rule must be set with a priority, integer of value 1-255.
  ACL rule with priority value 1 will be inspected before rule with priority value 255. Generally speaking, rule x will be inspected before y, if x<y.
  For a given ACL which has multiple rules assigned to it, each rule must have a unique priority value.
- A packet which is set to be inspected by the ACL will be inspected by its rules, according to their priority, until first match is found. The packet will then be permitted/ denied as per the action set for the rule. The packet will not be further inspected by following rules.
- An ACL may optionally be set with an action of 'redirect'. This action will redirect packets, which meet one of the ACL rules, to the IPS SCADA firewall process.
  A packet must meet one of the ACL rule with the action of 'permit'.
- When creating an ACL, by the default the system will add a last rule which permits all traffic which was not explicitly addressed by the user configured rules.

ACG

» For an ACL to take effect on incoming packets, it must be asserted on an interface. The assignment of the ACL to an interface is referred to as Port Access Group (ACG).

» An ACG assigns a specific ACL to an interface.

» Multiple ACGs, assigning the same ACL to the same interface are not allowed.

» Each ACG is assigned with a priority, integer of value 1-255.
An ACG with priority value 1 will be inspected before ACG with priority value 255. Generally speaking, priority x will be inspected before y, if x<y.

» A packet which is assigned multiple ACGs, will be inspected according to the ACG priorities until first match is found. The packet will then be permitted/ denied, with the ACL option of 'redirect'. The packet will not be further inspected by lower priority ACGs.

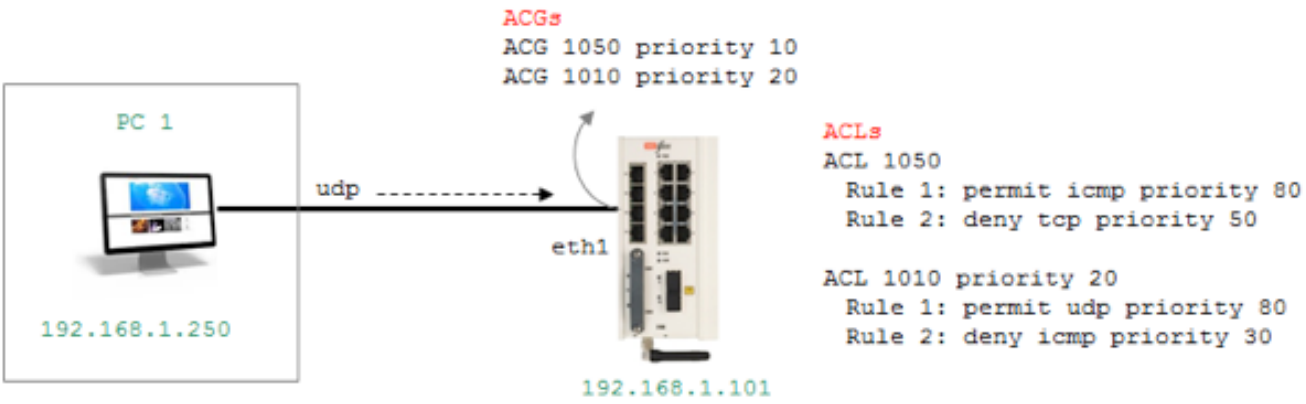
» If a packet does not meet any of the port assigned ACG conditions, it will be permitted.

Comments

1. An ACL rule which denies ICMP, does not block TCP or UDP traffic, only ICMP
2. An ACL rule which denies TCP, does not block ICMP or UDP traffic, only TCP
3. An ACL rule which denies UDP, does not block ICMP or TCP traffic, only UDP
4. Deleting an ACL will automatically remove corresponding ACGs on the interfaces, if such exists.
5. For an ACL which is already set to a port with an ACG, if a rule is added to the ACL (on the fly) it takes effect immediately on the ACG without need to reassign it to the interface.
6. To delete a rule, it is needed to delete the entire ACL it is assigned to.

Example

Following example will explain the ACL inspection flow.



The PC is sending udp packets. At the interface eth1, ACGs are intercepting the packets and examine them.

ACG with priority 10 will take effect first, examine the packet with ACL 1050 rules. Rule 2, which has priority 50, will be the first to be examined. As the rule addresses TCP packets, the condition is not met. The packet will then be examined with rule 1 which addresses ICMP and thus as well the rule is not met. The packet will now be examined with ACL 1010 rule 2 (priority 30). As the rule condition of ICMP is not met, the packet is examined by the next rule (priority 80). The condition of UDP is met and the packet is permitted.

ACL Commands Hierarchy

+ root

  + ip access-list extended

    - create {acl-num <1001-65535>} [acl-name <>] [redirect <off| on>]

    - delete {acl-num <1001-65535>}

    - permit tcp {acl-num <1001-65535>} [rule-name <>] [priority <1-256>] {src-ip [any| <a.b.c.d>]| <a.b.c.d/e>} {dst-ip [any| <a.b.c.d>]| <a.b.c.d/e>} [src-port <1-65535>] [dst-port <1-65535>] [src-port-range <(1-65535):(1-65535)>] [dst-port-range <(1-65535):(1-65535)>]

    - deny tcp {acl-num <1001-65535>} [rule-name <>] [priority <1-256>] {src-ip [any| <a.b.c.d>]| <a.b.c.d/e>} {dst-ip [any| <a.b.c.d>]| <a.b.c.d/e>} [src-port <1-65535>] [dst-port <1-65535>] [src-port-range <(1-65535):(1-65535)>] [dst-port-range <(1-65535):(1-65535)>]

    - permit udp {acl-num <1001-65535>} [rule-name <>] [priority <1-256>] {src-ip [any| <a.b.c.d>]| <a.b.c.d/e>} {dst-ip [any| <a.b.c.d>]| <a.b.c.d/e>} [src-port <1-65535>] [dst-port <1-65535>] [src-port-range <(1-65535):(1-65535)>] [dst-port-range <(1-65535):(1-65535)>]

- deny udp {acl-num <1001-65535>} [rule-name <>] [priority <1-256>] {src-ip [any| <a.b.c.d>]| <a.b.c.d/e>} {dst-ip [any| <a.b.c.d>]| <a.b.c.d/e>} [src-port <1-65535>] [dst-port <1-65535>] [src-port-range <(1-65535):(1-65535)>] [dst-port-range <(1-65535):(1-65535)>]
- permit icmp {acl-num <1001-65535>} [rule-name <>] [priority <1-256>] {src-ip [any| <a.b.c.d>]| <a.b.c.d/e>} {dst-ip [any| <a.b.c.d>]| <a.b.c.d/e>}
- deny icmp {acl-num <1001-65535>} [rule-name <>] [priority <1-256>] {src-ip [any| <a.b.c.d>]| <a.b.c.d/e>} {dst-ip [any| <a.b.c.d>]| <a.b.c.d/e>}

+ ip access-group

- apply {acl-num <1001-65535>} direction in {interface [eth1| eth2| cellular]} {priority <1-256>}
- remove {acl-num <1001-65535>} {interface [eth1| eth2| cellular]}
- show
- flush interface [all| eth1| eth2| cellular]

ACL Commands Descriptions

Command	Description
ip access-list extended	This command enters the IP Access-list configuration mode.
Create | delete	acl-num <1001-65535>} : the acl main identifier. acl-name: optional name to describe the acl. Redirect: redirect traffic to the SCADA firewall. <off| on>
Permit |deny tcp| udp	acl-num <1001-65535>} : the acl main identifier. rule-name: optional name to describe the rule. Src-ip: Any | <src-ip>| <src-ip/mask>. Source IP address can be: 'any' or the dotted decimal address or the IP address of the host that the packet is from and the network mask to use with the source IP address. dst-ip: any|host <dst-ip>|<dest-ip/mask>. Destination IP address can be: 'any' or the dotted decimal address or the IP address of the host that the packet is destined for and the network mask to use with the destination IP address. Src-port: source port number. dst-port: destination port number. Src-port-range: source port number range min:max. dst-port-range: destination port number range min:max. Priority: this field will determine the rules execution order. Higher value of filter priority implies it will be executed first. This value ranges between 1 and 256.
Permit |deny icmp	acl-num <1001-65535>} : the acl main identifier. rule-name: optional name to describe the rule. Src-ip: Any | <src-ip>| <src-ip/mask>. Source IP address can be: 'any' or the dotted decimal address or the IP address of the host that the packet is from and the network mask to use with the source IP address. Dst-ip: any|host <dst-ip>|<dest-ip/mask>. Destination IP address can be: 'any' or the dotted decimal address or the IP address of the host that the packet is destined for and the network mask to use with the destination IP address. Priority: this field will determine the rules execution order. Higher value of filter priority implies it will be executed first. This value ranges between 1 and 256.
ip access-group	
Apply| remove	acl-num <1001-65535>} : the acl main identifier. direction: supported direction is 'in'. interface: choose the target interface. Priority: this field will determine the ACL execution order. Higher value of al priority implies it will be executed first. This value ranges between 1 and 256.
Show	List the acl assignment to the interface.
Flush interfaces	Flush the acl assignment from a specific or all interfaces.

Configuration Example

Example 1

```
RL1000GW# ip access-list extended create acl-num 1010
RL1000GW# ip access-list extended permit icmp acl-num 1010 priority 10 src-ip any dst-ip any
RL1000GW# ip access-group apply acl-num 1010 interface eth1 direction in priority 10
```

Example 2

```
RL1000GW# ip access-list extended create acl-num 1010
RL1000GW# ip access-list extended permit icmp acl-num 1010 priority 10 src-ip 192.168.1.250
dst-ip 192.168.1.101
RL1000GW# ip access-list extended deny icmp acl-num 1010 priority 20 src-ip 192.168.1.250
dst-ip 192.168.2.101
RL1000GW# ip access-list extended permit tcp acl-num 1010 priority 40 src-ip any dst-ip
192.168.2.101
RL1000GW# ip access-list extended deny tcp acl-num 1010 priority 30 src-ip any dst-ip
192.168.1.101


RL1000GW# ip access-group apply acl-num 1010 interface eth1 direction in priority 1
```

Example 3

```
RL1000GW# ip access-list extended create acl-num 1010
RL1000GW# ip access-list extended permit icmp acl-num 1010 priority 10 src-ip 192.168.1.250
dst-ip 192.168.1.101
RL1000GW# ip access-list extended deny icmp acl-num 1010 priority 255 src-ip any dst-ip
192.168.1.101


RL1000GW# ip access-list extended create acl-num 1020
RL1000GW# ip access-list extended deny icmp acl-num 1020 priority 10 src-ip any  dst-ip
any


RL1000GW# ip access-group apply acl-num 1010 interface eth1 direction in priority 10
RL1000GW# ip access-group apply acl-num 1020 interface eth1 direction in priority 20
```

QOS

SCADA services are still commonly using serial legacy hardware. For such applications, the RL1000GW supports services as protocol gateway, serial tunneling and terminal server. These low bandwidth application may be of high importance to the utility process and require high network availability.

The QOS allows setting priority for serial services.

QOS Commands Hierarchy

+ qos

- mark-rule create {[src-ip <A.B.C.D/E>]| [dest-ip <A.B.C.D/E>]} [{protocol {tcp| udp}} [src-port <1-65535>] [dest-port <1-65535>]] {dscp <0-63>}
- mark-rule remove {src-ip <A.B.C.D/E>} [dest-ip <A.B.C.D/E>}
- mark-rule show
- show

QOS Commands Descriptions

Command	Description
qos	This command enters the quality of service configuration mode.
mark-rule	Create| update| show src-ip: IPv4 source IP of the packet. Should be one of the RL1000GW IP interfaces. A.B.C.D/E dest-ip: IPv4 destination IP of the packet. Protocol: tcp|udp protocol used at the packet. src-port: protocol source port used at the packet. dest-port: protocol source port used at the packet.

NAT

The RL1000GW routing package supports Static and Dynamic settings of Network Address Translation.

Dynamic NAT settings allow LAN members to initiate sessions with targets located at the WAN. The NAT router (RL1000GW) will use its WAN IP interface as the new source ip of the session request, hiding the original private IP of the initiating LAN device. The NAT router can use a single WAN ip interface to traverse multiple private IP addresses of its lan, thus limiting the required public ip addresses to a single one.

Static NAT settings, direct incoming WAN traffic to a particular target LAN client. As the WAN stations usually will not have a route to the private LAN, but only to the WAN ip address of the router, the static Nat settings are mandatory to allow them to initiate sessions towards LAN targets.

The NAT router serves both a routing function and security layer, allowing provisioning of WAN traffic access to the LAN.

Networking

Following picture will suggest NAT networking results per configuration option of dynamic/ static NAT set at the RL1000GW.

Figure 2 NAT networking 1

Looking at picture 'NAT networking 1', PC communication towards the server is dependent on the NAT configuration set at the RL1000GW NAT router.

» Static NAT only

The PC will not be able to initiate sessions towards the Server. Sessions initiated by the Server towards the PC will be received by the PC and replies of the PC will be received at the Server.

» Dynamic NAT only

The PC will be able to initiate sessions towards the Server and replies of the Server will be received at the PC. Sessions initiated by the Server towards the PC will not be received by the PC.

» Dynamic and Static NAT together

Both the Server and the PC can initiate sessions and receive replies.

NAT Commands Hierarchy

+ router

  + nat

    + Dynamic

      - Create {interface-name {eth1.<vlan-id>| eth2.<vlan id>| eth1:<id>| eth2:<id>| ppp0| eth0}} [description <text>]

      - remove {interface-name {eth1.<vlan-id>| eth2.<vlan id>| eth1:<id>| eth2:<id>| ppp0| eth0}}}

      - show

    + static

      - create {original-ip <A.B.C.D>} {modified-ip <>} [original-port <1-65535>] [modified-port <1-65535>] [protocol <tcp |udp| all>] [description <text>]

      - remove {[rule-id <>] | [{original-ip < A.B.C.D >} {modified-ip < A.B.C.D >} {protocol <tcp |udp| all>}]}

      - show

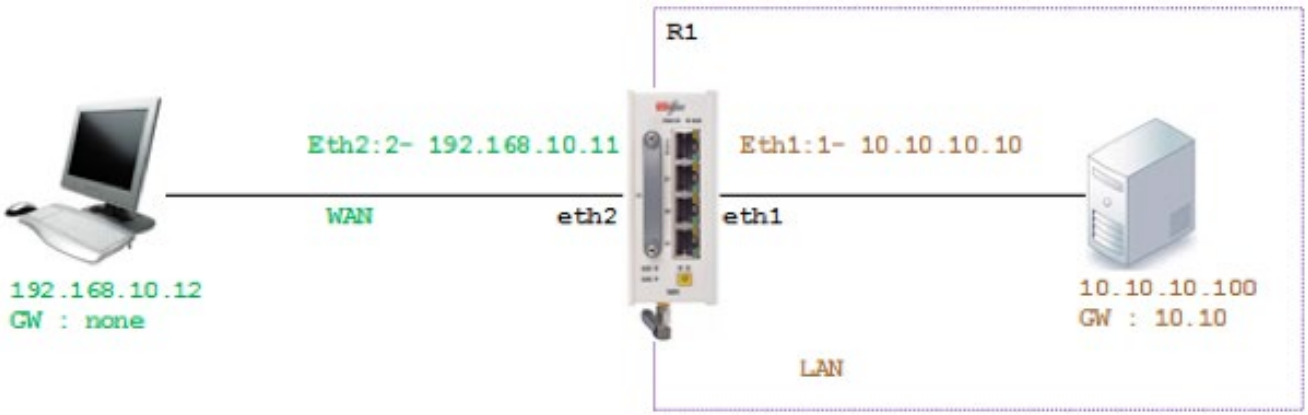
NAT Commands Description

Command	Description
nat	Access the nat configuration mode
Dynamic	Create| remove| show interface for dynamic nat. Interface name: the IP interface on which to enable the dynamic nat. Lan packets egressing the route rover this interface will have their 'source ip' replaced with the interface ip. The interface may be one which is associated with a physical port or the cellular ppp0 (GPRS/UMTS modem) or eth0 (LTE modem) interface. Description: text describing the interface. Optional.
static	Create| remove| show static nat entries. Original-ip: the original 'destination ip' at the incoming packet ip header. Modified-ip: the ip to which the nat should traverse the original-ip to. Original-port: the original protocol 'destination port' at the incoming packet ip header. Modified-port: the protocol port to which the nat should traverse the original-port to. Protocol: define the protocol, which the incoming packet uses, for which the nat should traverse. Packets which do not meet this condition will not traverse. Rule-id: an identifier given automatically by the system for each static nat entry. The rule-id is a sufficient parameter to remove an entry.

Example

Following setup example will explain how to use NAT to allow the PC, residing outside the LAN and with no routing to the LAN, connectivity to the LAN.

The PC is set to achieve management to the switch using the switch private interface and as well telnet to a server located at the LAN.



1. Set Interface for the LAN side

```
router interface create address-prefix 10.10.10.10/24 physical-interface eth1 description
LAN purpose application-host
```

2. Set ACE Interface for the WAN side

```
router interface create address-prefix 192.168.10.11/24 physical-interface eth2 description
WAN purpose general
```

3. Set Dynamic NAT settings using the WAN ACE interface

```
router nat dynamic create interface-name eth2:2 description wan
```

4. Set Static NAT settings, directing WAN traffic targeted to 192.168.10.11 with port Telnet (23) towards 10.10.10.10. This will allow the PC to achieve management to the RL1000GW.

```
router nat static create original-ip 192.168.10.11 modified-ip 10.10.10.10 original-port 23
modified-port 23 protocol tcp
```

5. Set Static NAT settings, directing WAN traffic targeted to 192.168.10.11 towards 10.10.10.100 with port 20000 (DNP3). This will allow the PC to establish DNP3 session with the server.

```
router nat static create original-ip 192.168.10.11 modified-ip 10.10.10.100 original-port
20000 modified-port 20000 protocol tcp
```

6. Commit

```
Commit
```

7. Show output example

```
RL1000GW#router interface show
+----+------+--------+------------------+------+---------+--------------+-------------+
| Id | VLAN |  Name  |     IP/Subnet      | Mtu  | Purpose | Admin status | Description |
+====+======+========+==================+======+=========+==============+=============+
| 1  | N/A  | eth1:1 |  10.10.10.10/24  | 1500 | general |    enable    |     LAN     |
+----+------+--------+------------------+------+---------+--------------+-------------+
| 2  | N/A  | eth2:2 | 192.168.10.11/24 | 1500 | general |    enable    |     WAN     |
+----+------+--------+------------------+------+---------+--------------+-------------+
[router/]nat dynamic show
+---------+---------+-------------+
| Rule-Id | If-Name | Description |
+=========+=========+=============+
|    1    | eth2:2  |     wan     |
+---------+---------+-------------+
RL1000GW#router nat static show
+---------+----------------+-----------------+----------+----------------+---------------
```

```
---+
| Rule-Id | Original-Dst-IP | Original-Dst-Port | Protocol | Modified-Dst-IP | Modified-
Dst-Port |
+=========+=================+===================+==========+=================+==========
=========+
|     1     |   192.168.10.11   |          23           |    tcp     |    10.10.10.10    |          23
|
+---------+-----------------+-------------------+----------+-----------------+----------------
---+
|     2     |   192.168.10.11   |        20000        |    tcp     |   10.10.10.100    |
20000         |
+---------+-----------------+-------------------+----------+-----------------+----------------
---+
```

OSPF

OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller more frequent update everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.

OSPF Commands Hierarchy

+ root

    + router ospf

        - enable

        - exit

        + configure terminal

            + router ospf

                - [no] area { A.B.C.D | < metric id ,(0-4294967295)> }

                - [no] router-id < A.B.C.D >

                - [no] network { A.B.C.D/M | <interface name ,eth1.(id)> }

                - [no] passive-interface <interface name,eth1.(id)>

                - [no] redistribute {connected | static}

                - [no] neighbor A.B.C.D

                - write

                - exit

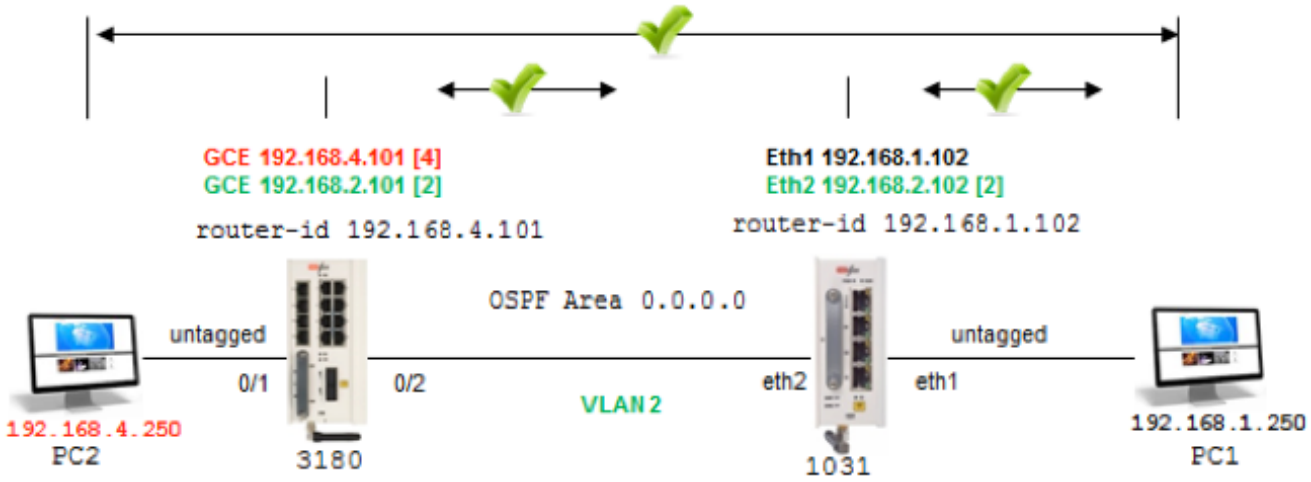
- exit

OSPF Commands Descriptions

Command	Description
Router ospf	enable
Configure terminal	Enter configuration mode
Router ospf	area – OSPF area parameters given in A.B.C.D format or as a metric id (0-4294967295). router-id – router-id for the OSPF process given in A.B.C.D format. network – Enable routing on an IP network . Network can be given as A.B.C.D/M or as a name of a preconfigured interface eth1.<vlan id>. passive-interface – Suppress routing updates on an interface. given as a name of a preconfigured interface eth1.<vlan id>. redistribute – Redistribute information from another routing protocol. neighbor – Specify a neighbor router. given as A.B.C.D/M . write – commit and preserve configuration

OSPF setup example

Below setup and configuration will example OSPF based routing between RL1000GW and RLGE2FE16R routers.



R1 configuration (RLGE2FE16R)

1. remove network ports from default vlan 1

```
config
vlan 1
no ports fa 0/1-2 untagged fa 0/1-2
exit
```

2. assign vlans and corresponding IP interfaces

```
vlan 101
config
vlan 2
ports fastethernet 0/2
exit

vlan 4
ports fastethernet 0/1 untagged all
exit
interface fast 0/1
switchport pvid 4
exit

interface vlan 2
ip address 192.168.2.101 255.255.255.0
no shutdown
exit
interface vlan 4
ip address 192.168.4.101 255.255.255.0
no shutdown
exit

end
```

3. configure OSPF

```
router ospf
router ospf
router-id 192.168.4.101
network 192.168.4.101 255.255.255.0 area 0.0.0.0
network 192.168.2.101 255.255.255.0 area 0.0.0.0
passive-interface vlan 4
end
write startup-cfg


R2 configuration (RL1000GW)
```

1. assign IP interfaces

```
RL1000GW# router interface create address-prefix 192.168.1.102/24 purpose application-host
physical-interface eth1


RL1000GW# router interface create address-prefix 192.168.2.102/24 vlan 2 purpose general
physical-interface eth2
```

2. configure OSPF

```
router ospf
enable
configure terminal
router ospf
router-id 192.168.1.102

network 192.168.1.102/24    area 0.0.0.0
network 192.168.2.102/24    area 0.0.0.0
passive-interface eth1:1
exit
write memory
exit
commit
```

```
RL1000GW# router interface show
+----+------+--------+------------------+------+-----------------+-------------+------------
-+
| Id | VLAN |  Name  |     IP/Subnet      | Mtu  |      Purpose       | Admin status |
Description |
+====+======+========+==================+======+=================+=============+======
=======+
| 1  | N/A  | eth1:1 | 192.168.1.102/24 | 1500 | application host |     enable     |
|
+----+------+--------+------------------+------+-----------------+-------------+------------
-+
| 2  |  2   | eth2.2 | 192.168.2.102/24 | 1500 |      general       |     enable     |
|
+----+------+--------+------------------+------+-----------------+-------------+------------
-+
router/ospf# show ip ospf neighbor


    Neighbor ID Pri State            Dead Time Address          Interface
RXmtL RqstL DBsmL
```

```
192.168.4.101      1 Full/Backup        33.167s 192.168.2.101    eth2.2:192.168.2.102      0
0      0
router/ospf# show ip ospf route
============ OSPF network routing table ============
N     192.168.1.0/24          [10] area: 0.0.0.0
                                 directly attached to eth1
N     192.168.2.0/24          [10] area: 0.0.0.0
                                 directly attached to eth2.2
N     192.168.4.0/24          [11] area: 0.0.0.0
                                 via 192.168.2.101, eth2.2

============ OSPF router routing table =============

============ OSPF external routing table ===========

router/ospf# exit
Connection closed by foreign host

RL1000GW# router  route show
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref     Use Iface
192.168.1.0      0.0.0.0          255.255.255.0    U      0       0          0 eth1
192.168.2.0      0.0.0.0          255.255.255.0    U      0       0          0 eth2.2
192.168.4.0      192.168.2.101    255.255.255.0    UG     11      0          0 eth2.2
Completed OK

RL1000GW# ping 192.168.4.101
PING 192.168.4.101 (192.168.4.101): 56 data bytes
64 bytes from 192.168.4.101: seq=0 ttl=64 time=1.509 ms
64 bytes from 192.168.4.101: seq=1 ttl=64 time=1.227 ms
64 bytes from 192.168.4.101: seq=2 ttl=64 time=1.231 ms
```

Serial Ports and Services

The serial interfaces connect legacy serial-based industrial devices to an Ethernet network. Each of the serial ports can be configured to work in one of these modes of operation:

1. Transparent tunneling
2. Terminal Server
3. Protocol Gateway.

Serial interfaces

Two serial interfaces are available at the RL1000GW.

Services configuration structure

Below table group the relevant configuration areas which should be included per application type

Hierarchy Level	Transparent Tunneling	Terminal Server	101/104 Gateway
Router IP Interface	X	X	X
Serial Port	X	X	X
Serial Local end point	X	X	X
Serial Remote end point	required if service is remote		
iec101-gw			X
termserver		X	

Below table details the state required for main configuration parameters depending on the used application.

Hierarchy level	Configurable Parameter	Transparent Tunneling	Terminal Server	101/104 Gateway
Serial Port	mode-of-operation	transparent	transparent	transparent
Serial Local end point	application	Serial-tunnel	Terminal-server	iec101-gw

Below table group relevant configuration options to the different application modes.

Parameter	Transparent Tunneling	Terminal Server	101/104 Gateway
baudrate	X	X	X
databits	X	X	X

Parameter	Transparent Tunneling	Terminal Server	101/104 Gateway
stopbits	X	X	X
allowed-latency	X	X	X
bus-idle-time	X	X	X
parity	X	X	X
dtr-dsr	X		
rts-cts	X		
local-dsr-delay	X		
local-cts-delay	X		

Serial Commands Hierarchy

+ serial

- Service show
- serial local-end-point filter show

+ card

- auto-recover {enable |disable |show}
- show

+ port

- clear counters
- create [slot <1>] {port <1-2>} [baudrate <9600,(50-368400)>] [parity <no,(no| odd| even)>] [stopbits <1,1|2>][bus-idle-time <bits (30-1000>] [mode-of-operation <Serial-tunnel,(serial-tunnel |terminal-server |iec101-gw |modbus-gw)>] admin-status [up| down] [allowed-latency <20msec,(2-255)> [tx-delay <msec,(0-255)>] [bus <RS232| RS485>]
- remove [slot <1>] {port <1-2>}
- update [slot <1>] {port <1-2>} [baudrate <>] [parity <no,(no| odd| even)>] [stopbits <>][bus-idle-time <bits (30-1000>] [mode-of-operation <Serial-tunnel,(serial-tunnel |terminal-server |iec101-gw |modbus-gw)>] admin-status [up| down] [allowed-latency <20msec,(2-255)> [tx-delay <msec,(0-255)>] [bus <RS232| RS485>]
- show

+ local-end-point

  - create [slot <1>] {port <1-2>} {service-id <1-100>} {position <master| slave>} [protocol <any>] [application {serial-tunnel |terminal-server |iec101-gw |modbus-gw}] [buffer-mode {byte| frame}]
    [iec101-link-address <0-65535>] [iec101-link-address-len (2,<1|2>]
    [iec101-originator-address {none| present}] [unit-id-len (2,<1|2>] [unit-id <0-65535>]

  - remove [slot <1>] {port <1-2>} {service-id <1-100>}

  - show

+ tunnel settings

  - update low-border-ip-port (9849, <1025- 65434>)

  - show

  + remote-end-point

    - create {remote-address <A.B.C.D>} {service-id <1-100>} {position <master| slave>} [buffer-mode {byte| frame}] [connection-mode [<udp| tcp>]

    - remove {remote-address < A.B.C.D>} {service-id <1-100>}

    - show

Serial Commands Description

Command	Description
Serial	Access serial configuration hierarchy. Configuration for ports, local-end-point, and remote-end-point are available here.
Service show	Provides configuration state of a serial service
local-end-point filter show	Provides detailed configuration state of an iec101 serial tunneling service
card	Auto-recover: allows automatic recovery when identifying continuous loss of serial infrastructure keep alive (between the serial processor and the Ethernet processor). Enable: auto recovery will reboot the process. Disable: no action taken. Show : show state Show : display the version and the provision state of the serial processor
port slot 1 port <>	Create/update the serial port
Clear counters	Clear counters

Command	Description
Create | update	Slot : 1 (constant) Port : port number .1-2 Baud rate : 50,75,100,110,134,150,200,300,600,1200,2400,4800,9600,19200,38400,57600,115200,230400,460800,921600 Parity : no, odd, even Stopbits : 1,2 admin-status: up| done. Default= up. Mode of operation: transparent bus-idle-time : number of total serial bits received over the local serial link to be considered as a single message allowed-latency: given in msec this value describe the network allowed latency. This value affects the time to be allowed to delay before transmitting UDP|TCP packets. The higher the value is the more serial frames can accumulate into a single UDP|TCP packets. Default value is 10msec which corresponds to max 3 bytes of serial data to be packed at a single UDP|TCP packet (with 9.6kbps rate)
Remove	Slot : 1 (constant) Port : port number .1-2
Show	
Local-end-point	
Create	Slot : 1 (constant) Port : port number .1-2 Service id: numeric value of serial service. Position: Master – point to multipoint Slave – point to multipoint Application : Serial-tunnel (default) Terminal-server iec101-gw modbus-gw buffer mode: byte (default) frame protocol : any (default) modbus_rtu iec101 iec101-link-address: set the IEC 101 link address. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <0-65535> iec101-link-address-len: set the IEC 101 link address length. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <1|2> bytes. Default is 2. iec101-originator-address: set if the 'originator' i=field is included in the IEC 101 message. This will reflect on the Cause Of Transmission being 1 byte or 2 byte size. If 'present', COT=2. If 'none', COT=1. unit-id: set the IEC 101 unit ASDU address. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <0-65535> unit-id-len: set the IEC 101 ASDU length. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <1|2> bytes. Default is 2.

Command	Description
Remove	Slot : 1 (constant) Port : port number .1-2 Service id: numeric value of serial service. Position: Master – point to multipoint Slave – point to multipoint Application : Serial-tunnel (default) Terminal-server iec101-gw modbus-gw show
tunnel settings	update low-border-ip-port: define here the range of port number used for tcp/udp connection. The set number will define the low border range value 'x' and result in a permissible range of x to x+100. The actual port number which will be used is dependent on the 'service-id' value as such: ['service-id'+ 'low-border-ip-port']. Default value is 9849 which results in port number 9850 for service-id=1. Changing the default 9849 is permitted to a value higher than 1024.
Remote-end-point	Defines the remote end points in a transparent serial tunneling service.
Create	remote-address : IPv4 address A.B.C.D Service id: numeric value of serial service. <1-100. Position: Master Slave connection mode: udp – default tcp Buffer mode: byte – default frame
Remove	address : IPv4 address A.B.C.D Service id: numeric value of serial service. show

Declaration of ports

Example of serial port declaration:

```
+ root
            serial
                  Port create  port 1
                  Port create   port 2
            ..
Commit
```

Default State

The default state of the serial ports is non-configured.

```
[/] serial port show
+-----+------+------+-----+------+------+------+--------+------+---------+-------+-------+-------+-------+-----+
| idx | slot | port | bus | mode | baud | data | parity | stop | latency |  tx   | start | stop  | admin | svc |
|     |      |      |     |      | rate | bits |        | bits |         | delay | delim | delim |       | id  |
+=====+======+======+=====+======+======+======+========+======+=========+=======+=======+=======+=======+=====+
+-----+------+------+-----+------+------+------+--------+------+---------+-------+-------+-------+-------+-----+

[/] serial local-end-point show
+-------+---------+------+------+-------------+----------+----------+----------+
| index | service | slot | port | application | position | firewall | firewall |
|       |   id    |      |      |             |          |   mode   | protocol |
+=======+=========+======+======+=============+==========+==========+==========+
+-------+---------+------+------+-------------+----------+----------+----------+
```

RS- 232 Port Pin Assignment

Below is the pin assignment of the serial ports.

ComNet RJ45 Female Port	
line	**pin**
DCD	2
TX	6
RX	5
DSR	1
GND	4
DTR	3
CTS	7
RTS	8

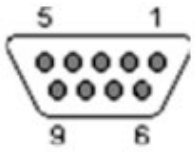
NOTE: The serial control lines are not supported at current version

RS-232 Serial cable

The RS-232 ports are of RJ-45 type, a cable is available as ordering option having one end of male RJ-45 and second end of female DB-9.

The cable should be used when no control lines are needed.

Serial port at the router



DB-9 female connector for end device

Pinout for crossed cable ("CBL-RJ45/DB9/NULL"):

RJ45 Male		**DB9 Female**
Female DB-9 (DCE)	Male RJ-45	Female RJ-45
2	6	6 Tx
3	5	5 Tx
5	4	4 GND

CAUTION: Take notice not to use the console cable for the user serial ports. The console cable is uniquely colored white. "CBL-TJ45-DB9/S-RPT"

RS-485 Port Pin Assignment

The RS-485 ports are of RJ-45 type.

The RS-485 supported mode is 4 wires.

RJ45 Female Router port		Direction
1	B (+)	Rx
4	GND	
5	A (-)	Rx
6	B (+)	Tx
8	A (-)	Tx

LED States

Each serial port has a led to indicate its state.

Port created	port admin state	Traffic passing	LED
No (default)	N/A	N/A	OFF
yes	down	N/A	OFF
yes	Up (default)	No	Green
yes	Up (default)	yes	Green blinking

Transparent Serial Tunneling

In transparent tunneling mode the router encapsulates the serial frames into UDP|TCP packets. The UDP|TCP packet is sourced with a local IP interface. Topologies supported are P2P, P2MP and MP2MP over a single unit or IP network.

The condition for transparent serial tunneling is having a ComNet router/ router at both ends of the network, connecting the devices.

The transparent tunneling implementation is based on encapsulation of standard serial frames is supported. The serial frames are structured with start, stop, data, and parity bits.

Following chapter will explain key serial properties and modes of operation.

Concept of Operation

The benefit of transparent serial tunneling is its simplicity.

Serial traffic received from the customer serial device at the router serial port, is encapsulated as UDP or TCP Ethernet packets by the router.

An IP interface is configured to route the packets over the Ethernet network. The Ethernet cloud may be layer 2 based, or layer 3 routing based and may involve any type of networking including cellular connectivity and VPN between the routers.

The serial devices must all be connected to ComNet routers.

The router serial port is configurable with a full set of serial properties.

Each serial port is assigned to a service-id. The service-id groups serial devices in the network to a logic communication segment at which members can communicate with each other.

At each service-id group there must be at least one device which is set a master and at least one device set as a slave.

The communication rules, which are maintained between service-id group members, are as follows:

1. Traffic sent from a master will be received at all slaves.

2. Traffic sent from a slave will be received at all masters.

3. Traffic between masters is blocked

4. Traffic between slaves is blocked.

Supported Network topologies

Transparent serial tunneling supports following topologies:

» Point to point
» Point to multipoint point
» Multi Point to multipoint point

Point to Point

Below picture illustrates Point-to-point service at which the master and slave are connected locally at the same router.

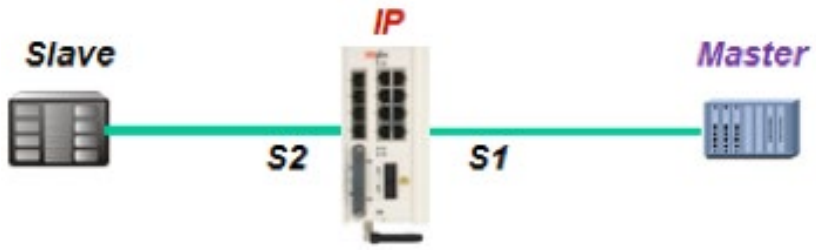


Figure 3: P2P, local service

Below picture illustrates Point to point service at which the master and slave are behind different routers.

Figure 4: P2P, remote service

Point to multipoint point

Below picture illustrates Point-to-multipoint service at which the master and slaves are connected locally at the same router.

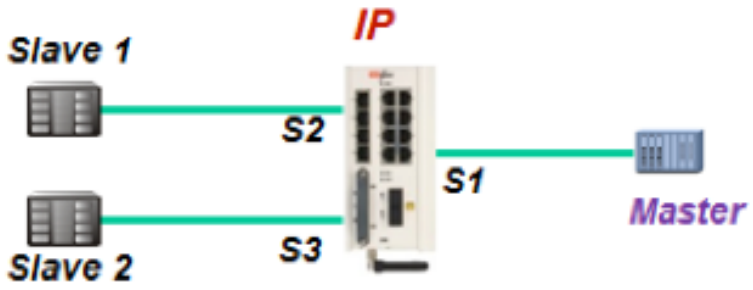


Figure 5: P2MP, local service

Below picture illustrates Point-to-multipoint service at which the service members are spread.

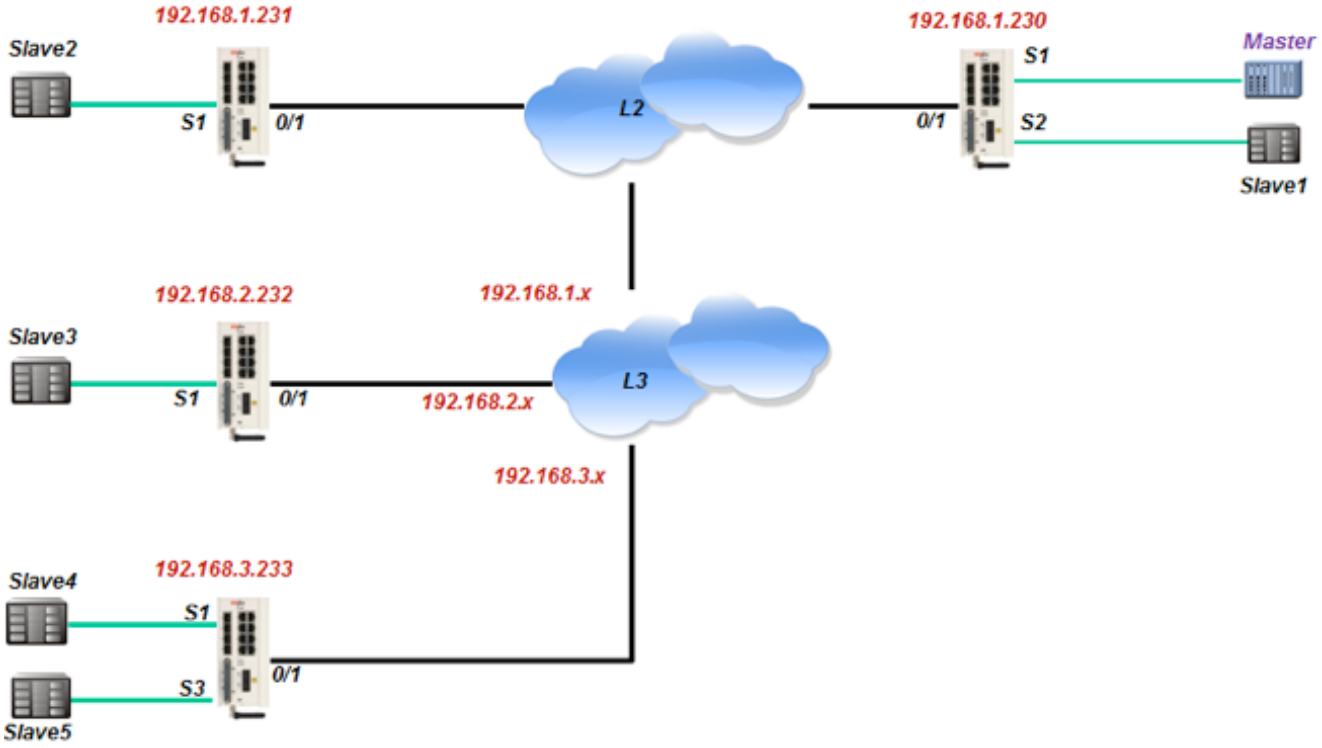


Figure 6: P2MP, remote service

Multi Point to multipoint point

Below picture illustrates a typical multipoint-to-multipoint service.

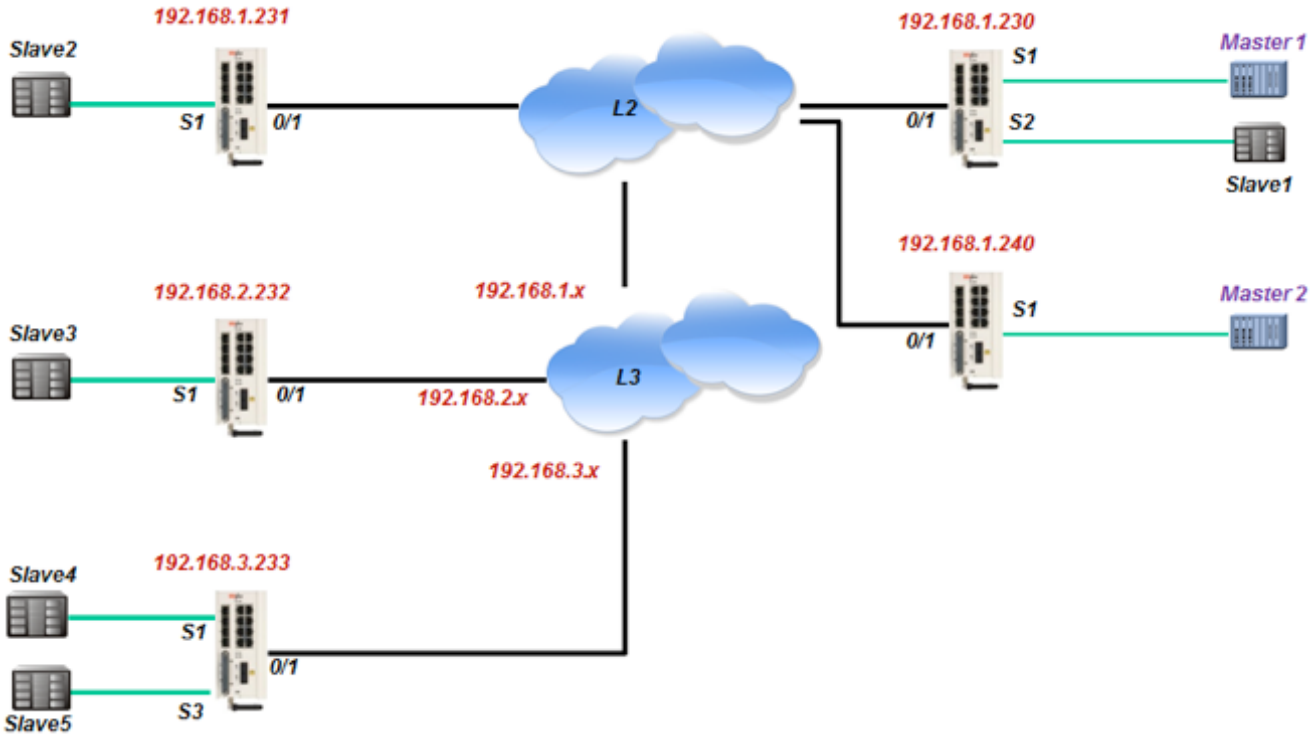


Figure 7: MP2MP, mixed service

Modes of Operation

Port Mode Of Operation

The port mode-of-operation is set at the serial port configuration level and defines how serial data is collected.

Transparent Tunneling

Transparent-tunneling is a mode at which serial data is sent with a distinct start bit, stop bit and a known length of data bits.

At this mode, the serial processor will collect data received until one of the following conditions is met:

» Bus idle time has expired.

» Allowed latency has expired.

At such time, the serial data collected will be encapsulated to a UDP|TCP packet and transmitted.

Service Buffer Mode

The service buffer-mode is set at local-end-point configuration level and defines the buffer operational mode for the service-id.

The default state is 'byte' mode. If the user keeps this field with its default state but configures the service 'connection-mode' to 'tcp', the buffer mode will be changed to 'frame' automatically. If the user explicitly set the buffer mode to either 'byte' or 'frame', the configuration will take effect for any connection-mode setting (tcp|udp).

Byte mode

A byte is structured as [start-bit, data-bits, parity-bit, stop-bits] whereas the number of data-bits may be 5 to 8.

At this mode, the serial-processor collects bytes and encapsulates the data at a UDP|TCP Ethernet frame.

The number of bytes collected to a single Ethernet packet is determined by the following factors:

» Allowed latency.

» Bus idle time.

Frame mode

A frame is a group of bytes sent by the customer equipment (CE) as complete message.

When using frame mode, the serial-processor will use the bus-idle-time to distinguish between frames. Each frame will be encapsulated as an individual UDP|TCP packet.

Service Connection Mode

The service connection-mode is set at remote-end-point configuration level and defines the protocol option to be used for the service-id.

UDP

Serial data will be encapsulated as UDP/IP frames.

This is the default option for a serial service.

UDP connection mode will use by default, byte mode for the service 'buffer-mode'. That is unless 'buffer-mode' was explicitly set to 'frame' by the user.

TCP

Serial data will be encapsulated as TCP/IP frames.

This mode allows higher availability for the end to end connection and traffic validation.

TCP connection mode will use by default, frame mode for the service 'buffer-mode'. That is unless 'buffer-mode' was explicitly set to 'byte' by the user.

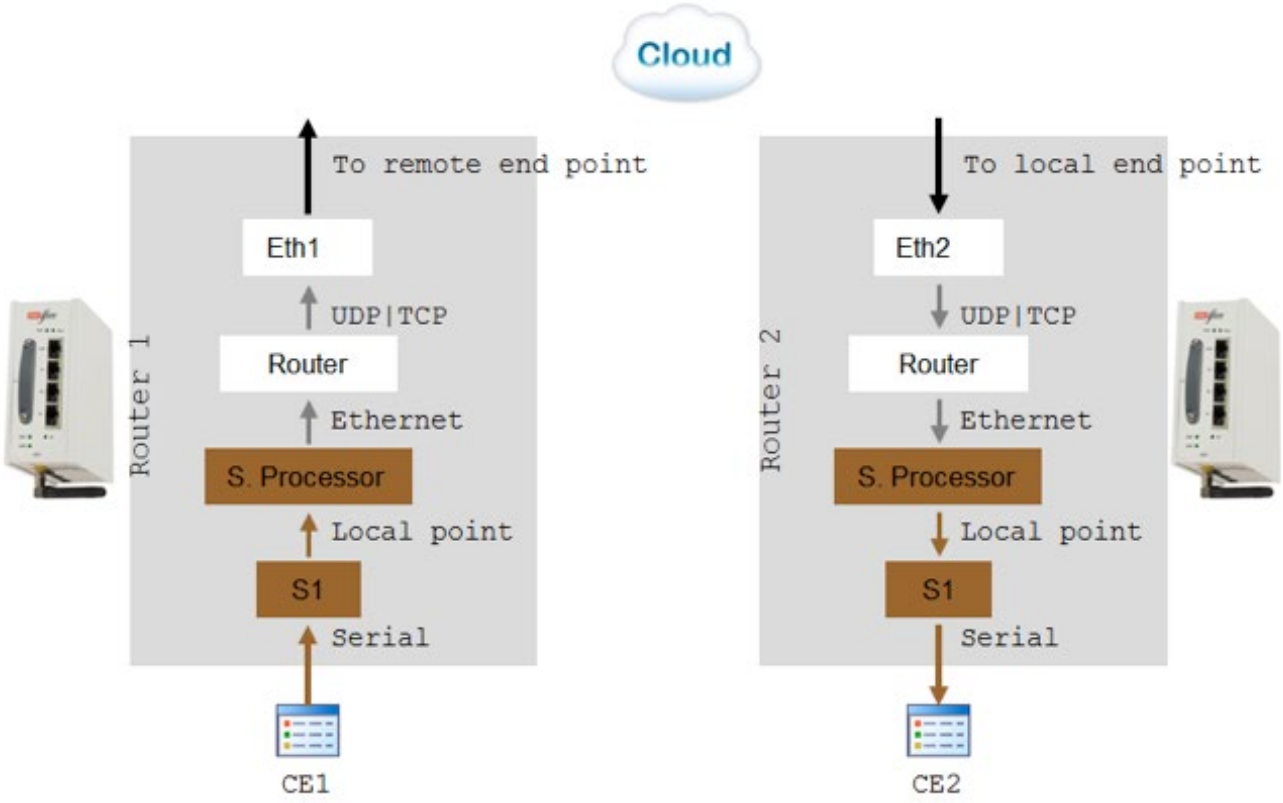
Service Port number

the TCP/UDP port number used at a serial tunneling connection is defined by the values of 'service-id' and the 'low-border-ip-port' set at the 'serial' 'settings'.

Reference drawing

For ease of explanation of following terms and serial properties at this chapter, below diagram will be used as a reference to follow on the serial traffic flow.

The diagram demonstrates two RL1000GW routers connected over an Ethernet network and sharing a transparent serial tunneling service.



The customer equipment #1 (CE1) is a serial master sending data to a serial slave CE2. For simplicity purposes, the diagram and explanations refer to unidirectional traffic from CE1 to CE2.

Serial Traffic Direction

Transmit direction represents the serial-processor traffic towards the CE, over the serial port.

Receive direction represents the traffic received at the serial-processor from the CE, over the serial port.

Serial ports counters

The Tx and Rx counters of the serial ports are controlled by the serial-processor.

Rx counters

» Switch1 – counters will increase when CE1 transmits. Data is received at the serial-processor via S1 and updates the counters.

» Switch2 – counters are not updated.

Tx counters

» Switch1 – counters are not updated.

» Switch2 –CE1 Data is received over the Ethernet network to router 2 and to the serial-processor. The serial processor transmits the data to CE2 over S1 and increases the Tx counters.

Allowed latency

Allowed latency is the maximum time allowed for the serial-processor to collect serial data from CE1 transmission, before closing an Ethernet packet and send it over the cloud.

This parameter refers to round-trip in milliseconds units. It reflects only the time for the serial processor to collect data, it does not consider the network self-latency.

Allowed latency is applicable in byte mode only.

» Switch1 – as CE1 transmits data to serial processor over S1, the allowed-latency properties are applicable. For a configured value x at allowed-latency, the serial processor will collect serial data for up to x/2 milliseconds time and then close the collected data as an Ethernet packet.

» Switch2- as CE2 is only receiving, the allowed-latency is not of influence.

Tx Delay

Tx-delay is set in bits. It determines a delay to take place by the serial processor before transmitting serial data to the port.

Depending on the baudrate chosen, and the number of bits, a time is calculated for Tx-delay.

» Switch1 – as the serial processor only receives serial data, the tx-delay is of no affect.

» Switch2- the Ethernet encapsulated data is received at router 2 and to its serial-processor. It is then transmitted to CE2 via S1 following a time elapse of the tx-delay.

The serial-processor will delay transmitting the first serial byte to CE2. Following data bytes are sent without delay.

Bus Idle Time

This parameter determines a silence on the serial line to identify frame end.

The configurable value for it is given in number of bits. Depending on the baudrate chosen, and the number of bits, a time is calculated for bus-idle-time.

Byte mode

When using byte mode, end of byte is determined by stop bits. Bus-idle-time is not applicable at this mode.

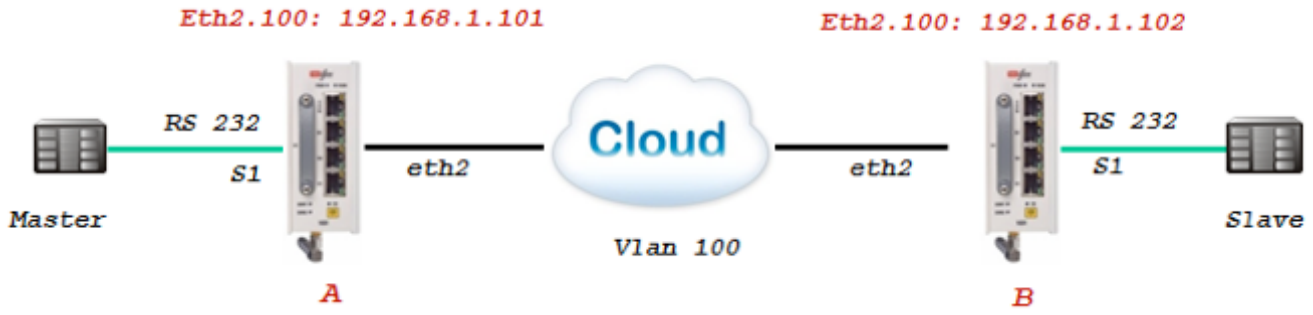
Frame mode

» Switch1- the serial-processor will collect serial data transmitted from CE1 until a silence is identified on the line for a time period equal or above the bus-idle-time.

» Switch2- the serial-processor transmits the serial frames to CE2 while maintaining a gap between frames. The gap is the bus-idle-time.

Example 1

Below network demonstrates a P2P topology of transparent serial tunneling between two RL1000GW routers.



Configuration router B (SLAVE)

1. Configure the IP interface

```
router interface create address-prefix 192.168.1.102/24 vlan 100 purpose application-host
physical-interface eth2
```

2. Configure the serial port and local end point

```
serial port create port 1 baudrate 9600 parity no mode-of-operation transparent
serial local-end-point create port 1 service-id 1 application serial-tunnel position slave
```

3. Configure the remote end point of the service

```
serial remote-end-point create remote-address 192.168.1.101 service-id 1 position master
commit
```

Configuration router A (MASTER)

1. Configure the IP interface

```
router interface create address-prefix 192.168.1.101/24 vlan 100 purpose application-host
physical-interface eth2
```

2. Configure the serial port and local end point

```
serial port create port 1 baudrate 9600 parity no mode-of-operation transparent
serial local-end-point create port 1 service-id 1 application serial-tunnel position
master
```

3. Configure the remote end point of the service

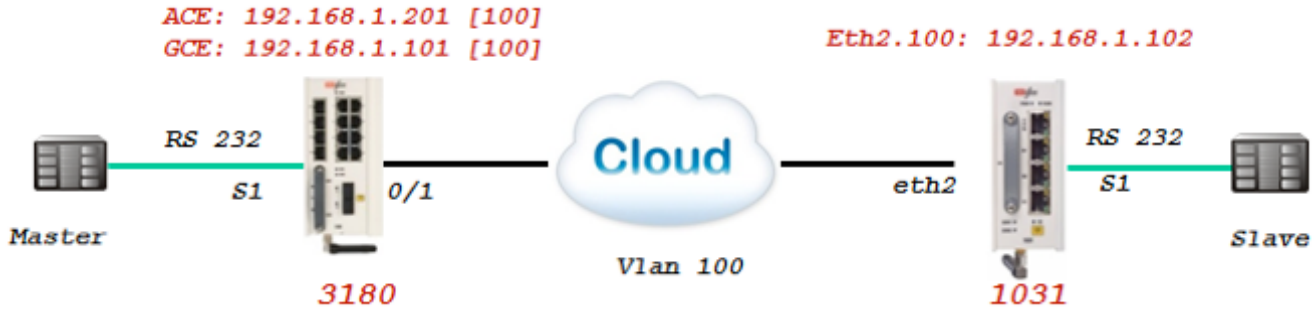
```
serial remote-end-point create remote-address 192.168.1.102 service-id 1 position slave
commit
```

```
router interface show
+------+----------+------------------+-----------------+-------------+
| VLAN |    Name    |      IP/Subnet      |      Purpose       | Description |
+======+==========+==================+=================+=============+
| 100   | eth2.100 | 192.168.1.101/24   | application host |               |
+------+----------+------------------+-----------------+-------------+
serial port show
```

```
+-----+------+------+-------+-------------+------+------+--------++
| idx | slot | port |  bus  |     mode      | baud | data | parity |
|     |      |      |       |               | rate | bits |        |
+=====+======+======+=======+=============+======+======+========+
|  1  |  1   |  1   | RS232 | Transparent | 9600 |  8   |  None  |
+-----+------+------+-------+-------------+------+------+--------+
RL1000GW# serial local-end-point show
+---------+------+------+--------------+----------+----------+--------+----------+----------+
| service | slot | port |  application  | protocol | position | buffer | firewall | firewall |
|   id    |      |      |               |          |          | mode   |   mode   | protocol |
+=========+======+======+==============+==========+==========+========+==========+==========+
|    1    |  1   |  1   | serial-tunnel |   any    |  Master  | Bytes  | disable  |   any    |
+---------+------+------+--------------+----------+----------+--------+----------+----------+
```

Example 2

Below network demonstrates a P2P topology of transparent serial tunneling between RLGE2FE16R and RL1000GW routers.



Configuration RL1000GW (SLAVE)

1. Configure the IP interface

```
router interface create address-prefix 192.168.1.102/24 vlan 100 purpose application-host
physical-interface eth2
```

2. Configure the serial port and local end point

```
serial port create port 1 baudrate 9600 parity no mode-of-operation transparent
serial local-end-point create port 1 service-id 1 application serial-tunnel position slave
```

3. Configure the remote end point of the service

```
serial remote-end-point create remote-address 192.168.1.201 service-id 1 position master
commit
```

Configuration RLGE2FE16R (MASTER)

1. Configure the network vlan and management IP interface

```
Config
vlan 100
ports gigabitethernet 0/1
ports add gigabitethernet 0/3
exit
interface vlan 100
ip address 192.168.1.101 255.255.255.0
no shutdown
end
write startup-cfg
```

2. Configure the ACE IP interface

```
application connect
router interface create address-prefix 192.168.1.201/24 vlan 100 purpose application-host
```

3. Configure the serial port and local end point

```
serial port create slot 1 port 1 baudrate 9600 parity no mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 1 application serial-tunnel
position master
```

4. Configure the remote end point of the service

```
serial remote-end-point create remote-address 192.168.1.102 service-id 1 position slave
exit
write startup-cfg
```

Protocol Gateway IEC 101 to IEC 104

The ComNet router, using its application module implements the gateway for IEC101 serial devices to the IEC104 IP protocol. The IEC101 and IEC104 protocols are fully integrated in the application module thus allowing the IEC101 slave devices to be represented as a IEC104 server in the IP network and to be addressed as such by IEC104 clients located anywhere in the network.

The gateway implementation consists of 3 functions:

» IEC104 Server – The application module will act as a IEC104 server to any IEC104 clients that connect to it over the Ethernet network. This function includes the full implementation of the state-machine of the IEC104 server, response to keep-alive test frames and listening of TCP port 2404 for any client requests.

» IEC60870 message router – The application module will act as a application router translating the requests received by the IEC104 server to commands issued by the IEC101 master with the proper IEC101 address and sending the responses vice versa.

» IEC101 Master – The application module will act as a IEC101 master to the IEC101 server devices connected to the assigned serial interfaces in the router. This function includes the full implementation of the state-machine of the IEC101 master, initialization and arbitration of the IEC101 bus and issuing commands to the appropriate IEC101 slave to provide the response to the requests which arrive from the message router.

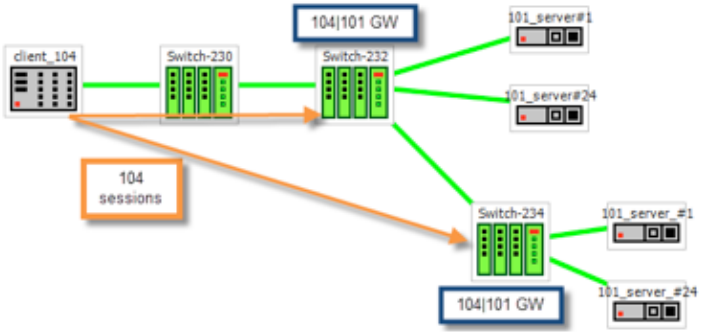
The IEC101 devices will be configured with their serial link properties, device address and ASDU address to be uniquely identified behind the gateway.

Overall the IEC101 devices will be addressed from the IEC104 remote client using the following hierarchical addressing scheme: IP address of the application module in which the IEC101/104 gateway is implemented, IEC101 device address, ASDU address and IOA (Information Object Address - for example ,the actual address of the discrete inputs mapped at the IEC101 RTU).

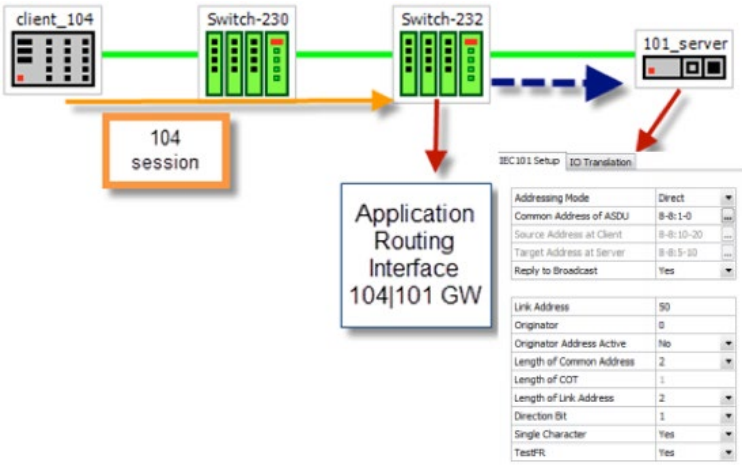
Modes of Operation

The gateway supports 2 topologies for the IEC101 devices as defined by the standard:

» Balanced Mode – Up to 24 unique IEC-101 servers behind each single gateway



» Unbalanced Mode – Up to 32 ASDU addresses behind each IEC101 server device



IEC101/104 Gateway properties IEC 101

- » System role : Controlling station definition (Master)
- » Network configuration :
  - › Point-to-point
  - › Multiple point-to-point
  - › Multipoint-party line (planned)
- » Physical layer
  - › Transmission speed in monitor & control direction: 300 – 38400bps
- » Link layer
  - › Link transmission procedure
    - ·Balanced transmission
    - ·Unbalanced transmission
  - › Address field of the link
    - ·Not present (balanced transmission only)
    - ·One octet
    - ·Two octets
    - ·Structured values translation
    - ·Unstructured
- » Application layer
  - › Common address of ASDU
    - ·One octet
    - ·Two octets
  - › Information object address
    - ·Two octets
    - ·Three octets
    - ·Structured
    - ·Unstructured
  - › Cause of transmission
    - ·One octet
    - ·Two octets (with originator address)

IEC101/104 Gateway Configuration

The IEC101/104 gateway can be configured through the systems CLI or as part of a IEC104 network-wide service-group in the iSIM service management tool.

In any case the configuration should include the following parameters:

» Application IP address – The application module must be configured with an IP address and should be associated with a VLAN for the uplink traffic. This application IP interface acts as the IEC104 server in the Ethernet network and represents all the IEC101 devices connected locally to the router towards the IEC104 clients.

» Optional remote IP addresses - When configuring the IEC104 service-group you should also provide the IP addresses of the IEC104 clients so the proper service-aware firewall rules can be defined.

» IEC101 device parameters - For the serial interfaces the physical link properties should be configured (baud-rate ,parity , stop bits). Furthermore the IEC101 addressing information should be provided and and the devices should be assigned to the IEC104/101 gateway.

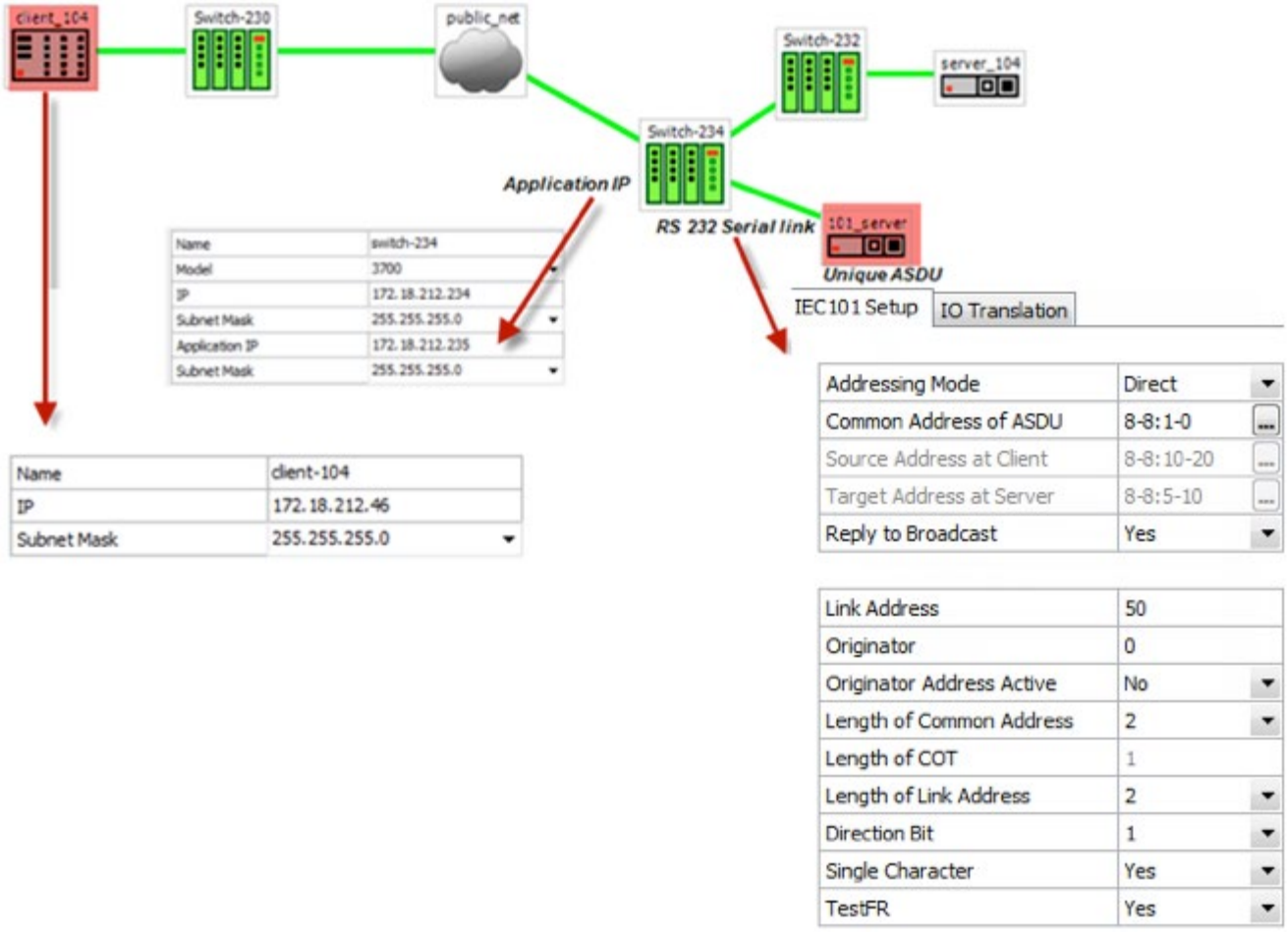


Figure 8 : Gateway service configuration in iSIM

Gateway 101/104 Configuration Flow

When attending a setup configuration, follow these below steps.

1. Ethernet connectivity towards the IEC 104 Client (SCADA)
    a. Set service vlan and assign relevant ports.
    b. Set ACE IP interface with the service vlan
    c. Set static or dynamic routing if needed to reach the IEC 104 Client.
    d. Verify by following methods
        i. Successful ping between the IEC 104 Client (SCADA) and the RL1000GW designated IP interface.
        ii. IEC 104 connection established. Use the command “iec101-gw show all” to verify connection at the switch.
2. Serial connection towards the locally connected IEC101 server (RTU)
    a. Configure a serial port
        i. Serial properties as baudrate, parity and such, must be consistent with those of the RTU.
        ii. The serial port must be configured with ‘mode-of-operation set to ‘transparent’.
    b. Configure a local service (serial local-end-point)
        i. Create a local-end-point and assign the serial port.
        ii. The local-end-point field ‘application’ must be set to ‘iec101-gw’
    c. Enable the gateway
        i. Assign the gateway to use the predefined ACE interface.
        ii. Set the desired mode ‘balanced’ or ‘unbalanced’.
    d. Configure the gateway with the RTU IEC101 properties. Key values are advised here
        i. Common Address of ASDU value (CLI field ‘asdu_addr’). As set at the RTU.
        ii. Common Address of ASDU length in bytes (CLI field ‘common_address_field_length’). As set at the RTU.
        iii. Link Address (CLI field ‘link_addr’). As set at the RTU.
        iv. Link Address length in bytes (CLI field ‘link_address_field_length’). As set at the RTU.
        v. Cause of Transmission length in bytes, determined by the usage of the originator address field in the protocol. (CLI field ‘orig_addr_participate’)
        vi. Connect the IEC101 server (RTU) to the serial port with a proper serial cable. Pin-out of the RS232 RJ45 port of the switch is given in this manual. Control lines are not supported

for the gateway application. Usage of Tx,Rx and GND lines are allowed.

e. Verify by following methods

i. Use the command “iec101-gw show all” to verify the operational status (‘OP ST’) is UP.

ii. Follow serial port and gateway counters to check if serial traffic is received and transmitted at the serial port.
Show commands “serial port show slot 1 port <x>” and “iec101-gw cnt show” are available.

3. Trouble shooting

a. Most trouble shooting is usually at the IEC101 connection to the locally connected RTU. The IEC 104 connection between the gateway and the client (SCADA) is based on straightforward Ethernet connectivity which is easy to establish and diagnose.

b. If the IEC101 (‘OP ST’) is in any other state other than ‘UP’, try the following

i. Verify your serial physical connection.

ii. Verify the RTU is on and properly configured.

iii. Follow the serial port counters to verify traffic is received and transmitted at the serial port. If only Rx counters are progressing, check again the serial properties of both the gateway and the RTU (baudrate, parity and such).

iv. Verify the IEC properties are consistent between the gateway and the RTU (CA, LA, CA length, LA length, COT)

Gateway 101/104 Commands Hierarchy

+ root

  + serial

    + port

      - clear counters

      - create {slot <1>} {port <1-2>} {mode-of-operation < transparent >} [baudrate <9600,(50-368400)>] [parity {no,no| odd| even}]
        [stopbits <1|2>] databits {8,<5-8>}
        admin-status [up| down]

      - update {slot <1>} {port <1-2>} {mode-of-operation < transparent >} [baudrate <9600,(50-368400)>] [parity {no,no| odd| even}]
        [stopbits <1|2>] databits {8,<5-8>}
        admin-status [up| down]

      - show

  + local-end-point

      - create create {slot <1>} {port <1-2>} {application <iec101-gw>}{service-id <1-100>}
        [position <slave>]

      - remove {slot <1>} {port <1-2>} {service-id <1-100>}

      - show

  + iec101-gw

    - operation {start | stop}

    - cnt show

    - show {all| iec101 {log| state} {slot <1>} {port <1-2>} }

  + config

    - gw update mode {balanced,(balanced| unbalanced)} ip_addr <A.B.C.D>

    - iec101 {create | update}
      {slot <1>} {port <1-2>} {asdu_addr {(1-255)| (1-65534)}}
      {link_addr {(1-255)| (1-65534)}}
      [common_address_field_length <2,(1|2)>]
      [translated_cmn_addr {(1-255)| (1-65534)}]
      [link_address_field_length <2,(1|2)>]
      [ioa_length <3,(1|2|3)>] [orig_address <1-255>]
      [orig_addr_participate <y,(y|n)>]

[dir_bit<AUTO,(AUTO|0|1)>] [single_char <y,(n|y)>]
[test_proc <y,(n|y)>] [gen_inter <n,(n|y)>] [time_tag <n,(n|y)>]

- iec101 remove [slot <1>] {port <1-2>}

- iec101 [add_asdu | remove_asdu] port <1-2>
  {asdu_addr {(1-255)| (1-65534)}} {link address {(1-255)| (1-65534)}}

- iec101 [add_ioa_trans>| remove_ioa_trans] port <1-2>
  src_ioa {a1-a2-a3| a1-a2| a} trans_ioa {a1-a2-a3| a1-a2| a}

- iec104 {update | remove} {ip_addr <>} [clock_sync <n|y>] [orig_addr <>] [t0 <30sec,[1-255]>]
  [t1 <15sec,[1-255]>] [t2 <10sec,[1-255]>] [t3 <20sec,[1-255]>]

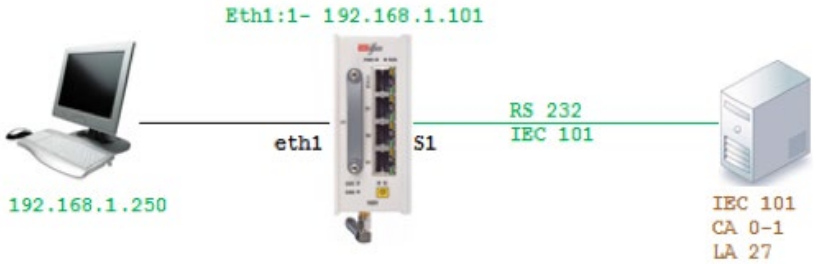
Gateway 101/104 Commands

Command	Description
iec101-gw	Configuration mode of 101/104 gateway
Operation	Start : activate the gateway Stop : stop the gateway *takes effect on all IEC 101 nodes connected to the switch
Config	
gw update mode	Unbalanced – for 101 servers unbalanced topology. Balanced (default)– for 101 servers balanced topology. ip_addr– IP address of a chosen application IP interface. The IP interface must be configured prior to it be used by the gateway !changing this field requires reloading the unit
iec101 create | update | remove	Slot ,Port: physical interface where the 101 slave is connected at. asdu_addr : Common Address of ASDU. Usually Should be configured as the ASDU address of the IEC101 Server unless a translation service is required. In the latter case, should be configured as the address which is set at the 104 Client for the server. A decimal value of 1-255 or 1-65534 is allowed depending if 'common_address_field_length' is set to one byte or two. common_address_field_length: length in bytes of the Common Address of ASDU. Permissible values are one or two bytes. Should be identical to the configuration at the IEC 101 server. translated_cmn_addr – used when a translation service required for the common address of asdu. The value should be identical to the actual common address of the IEC101 Server. A decimal value of 1-255 or 1-65534 is allowed depending if 'common_address_field_ length' is set to one byte or two. link_addr: Should be configured as the Link address of the 101 slave. A decimal value of 1-255 or 1-65534 is allowed depending if 'link_address_field_length' I set to one byte or two. link_address_field_length: length in bytes of the Link Address. Permissible values are one or two bytes. Should be identical to the configuration at the 101 slave. orig_addr: Should be configured as the Originator address set at the 101 slave. orig_addr_participate: y|n to indicate if the 101 slave uses the originator address field. Should be identical to the configuration at the 101 slave. the Cause Of Transmission (COT) will be influenced by this configuration. 'y' – COT will be 2 byte in size. 'n' - COT will be 1 byte in size. dir_bit: y|n are Permissible values. Should be oposite to the configuration at the 101 slave. relevant in Balanced mode only. single_char: y|n are Permissible values.Should be configured identical to the 101 slave configuration. relevant in Balanced mode only. ioa_len – IO object length. Permissible values are 1|2|3 bytes. Should be identical to the configuration at the 101 slave.

Command	Description
[add_ioa_trans>| remove_ioa_ trans]	Slot, Port: physical interface where the 101 slave is connected at. src_ioa: value of the 101 server Object address as set at the 104 client. May be 1/2/3 bytes long depending on the settings of 'ioa_length'. A value is expected as 'byte1'-'byte2'-'byte3' or 'byte1'-'byte2' or 'byte-1'. Permissible value for each byte is 1-255. example for 3 bytes size IOA: 5-212-151. trans_ioa: value of the 101 server Object address. May be 1/2/3 bytes long depending on the settings of 'ioa_length'. A value is expected as 'byte1'-'byte2'-'byte3' or 'byte1'-'byte2' or 'byte-1'. Permissible value for each byte is 1-255. example for 3 bytes size IOA: 5-212-151.
iec104 {update | remove}	ip_addr: IP address of the SCADA orig_addr: originator address of the SCADA. to: Time-out of connection establishment t1: Time-out of send or test APDUs t2 : Time-out for acknowledges in case of no data messages t2 < t1 t3: Time-out for sending test frames in case of a long idle state

Example Gateway 101/104

Below network demonstrates an IEC 101/104 setup using the RL1000GW as a gateway.



Configuration

1. Configure an IP interface for the gateway

```
RL1000GW#router interface create address-prefix 192.168.1.101/24 physical-interface eth1
description Network purpose application-host
```

2. Configure the serial port properties. Field 'mode-of-operation must be set to 'transparent'. The port properties must be in-line with the IEC 101 server device connected (same baudrate, parity, stop bits, data bits and such)

```
serial port create port 1 mode-of-operation transparent baudrate 9600 parity even
```

3. Create the local serial service for the port. the field 'application' must be set to 'iec101-gw'

```
serial local-end-point create port 1 service-id 1 application iec101-gw
```

4. Configure the gateway mode of operation and choose the ACE interface to be used. The IP interface must be available in advance.

```
iec101-gw config gw update mode balanced ip _ addr 192.168.1.101
```

5. Configure the gateway properties to be in line with the IEC101 server settings.

```
iec101-gw config iec101 create port 1 asdu _ addr 1 orig _ addr 0 link _ addr 27 link _
address _ field _ length 2 common _ address _ field _ length 2 orig _ addr _ participate y


commit
```

6. Follow show status

```
RL1000GW# router interface show
+----+------+--------+-----------------+------+-----------------+-------------+-----------
-+
| Id | VLAN |  Name  |    IP/Subnet     | Mtu  |     Purpose     | Admin status |
Description |
+====+======+========+=================+======+=================+=============+======
=======+
| 1  | N/A  | eth1:1 | 192.168.1.101/24 | 1500 | application host |    enable    |     WAN
|
+----+------+--------+-----------------+------+-----------------+-------------+-----------
-+


RL1000GW# iec101-gw show all
101-104 ROUTER
BALANCED MODE
IEC 104:
+--------------+-----------+-----------+----------+----+----+----+----+
|      IP      | ORIG. ADDR | CLOCK SYNC | TIME TAG | T0 | T1 | T2 | T3 |
+==============+===========+===========+==========+====+====+====+====+
```

```
| 192.168.1.101 |      0       |      n       |     n      | 30 | 15 | 10 | 20 |
| 192.168.1.250 |      0       |      n       |     n      | 30 | 15 | 10 | 20 |
+---------------+------------+------------+----------+----+----+----+----+

IEC 101:

+------+------+-------+----------+---------+-------------+----------+---------+---------+----
-----+---------+----------+

| SLOT | PORT | OP ST | LINK ADR | CMN ADR | CONV CMN ADR | LINK LEN | CMN LEN | COT
LEN | IOA LEN | SRC IOA | CONV IOA |

+======+======+=======+==========+=========+==============+==========+=========+=========
+=========+=========+==========+

|  1   |  1   |  UP   |    27    |    1    |      0       |    2     |    2    |
2    |    3    |          |           |

+------+------+-------+----------+---------+-------------+----------+---------+---------+----
-----+---------+----------+

+------+------+-----------+------+---------+---------+---------+----------+---------+---------
+----------+-----------+

| SLOT | PORT | ORIG. ADR | S CH | DIR BIT | TEST FR | GEN INT | TIME TAG | COT LEN |
IOA LEN | CMN (UB) | LINK (UB) |

+======+======+===========+======+=========+=========+=========+==========+=========+====
=====+==========+===========+

|  1   |  1   |     0     |  y   |  AUTO   |    y    |    n    |    n     |    2
|    3    |    1     |    27     |

+------+------+-----------+------+---------+---------+---------+----------+---------+---------
+----------+-----------+

RL1000GW#
```

Terminal Server

Terminal Server service

ComNet routers allows a special service for transposing of a TCP session to serial session.

Networking:

A router acting as the terminal server can be connected to the Ethernet telnet client (management station) via:

» local connection at its ports or

» Via IP network.

» In both cases the connection is TCP based.

A router acting as the terminal server can be connected to the serial end device (managed station) via:

» local connection at its RS-232 ports

» or Over UDP connection to a remote ComNet router to which the serial device is connected directly to.

» In this case there will be a “transparent serial tunneling service” over the IP network (encapsulation of serial data in UDP|TCP packets)

A usage example, console ports of remote devices to be reached via terminal server service using telnet from any PC with Ethernet link.

In below drawing the management station (PC) is a Telnet client which requires being able to manage the remote RTUs with a text based shell method.

The PC is an Ethernet device connected locally to the router A.

Router A acts as a telnet server towards it. A telnet session is hence established between the PC and the router.

Up to 100 such sessions can simultaneously be supported uniquely identified by their TCP Port numbers.

It is possible to support P2MP in 2 modes:

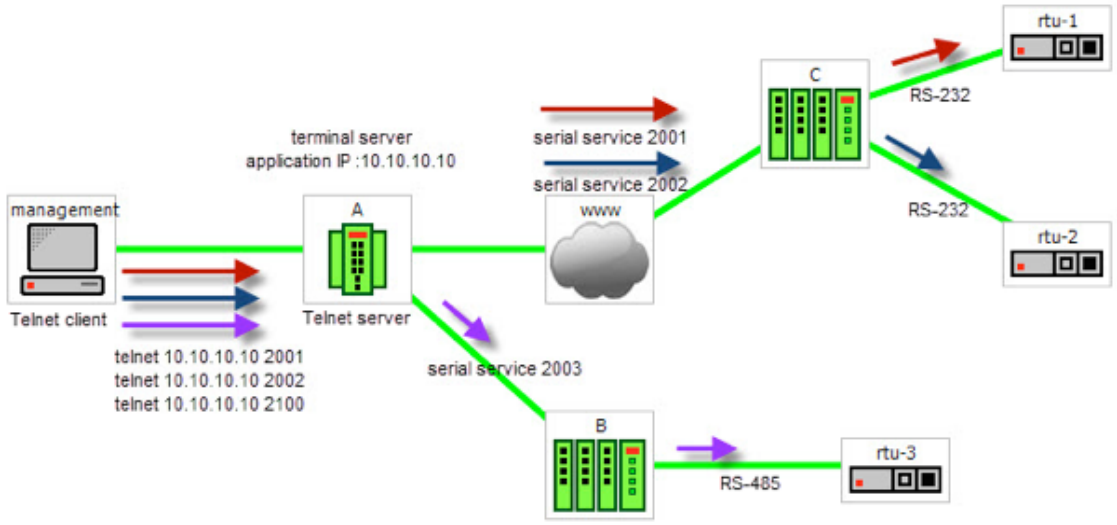
» Over the same service using the same TCP port number.

» Over different services using multiple TCP sessions each with a different TCP port.

The user will configure services ,to determine which RTU is to be addressed via which telnet session.

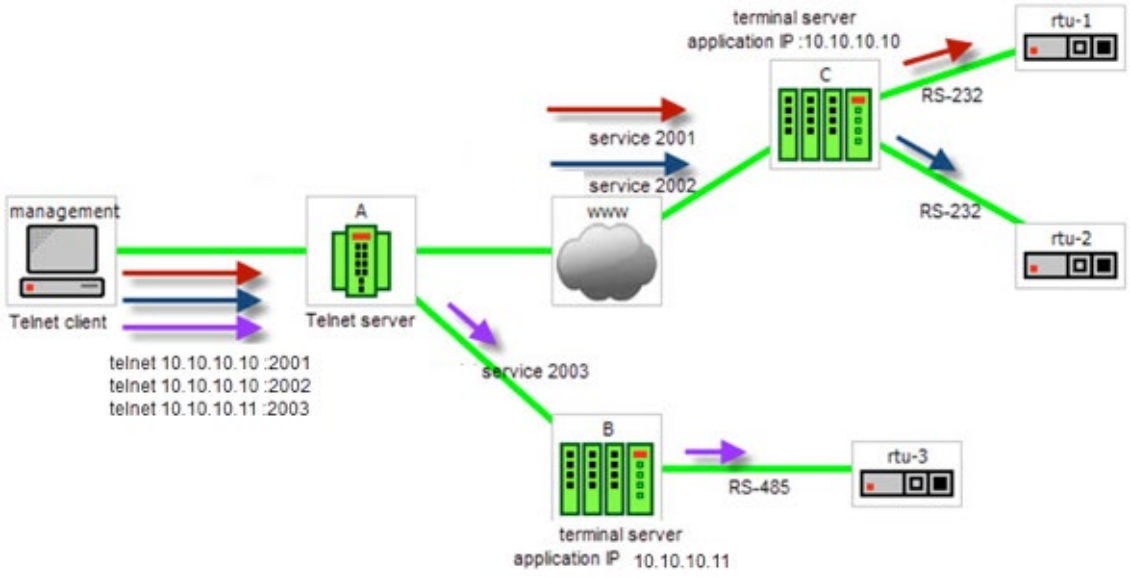
In below example Serial transparent tunneling (UDP|TCP traffic) will take place between the ComNet routers thus establishing the paths from the serial RTUs to router A . using the mapping

between the telnet sessions and the serial services the application will direct the traffic from the management station to the RTUs allowing each its own path for management.



Below is a second option at which the terminal servers are set at the remote router where the serial devices are connected locally.

The benefit in this scenario is having a TCP session over the IP network.



Service Buffer Mode

The service buffer-mode is set at the terminal server settings and defines the buffer operational mode for all the services.

Byte mode

A byte is structured as [start-bit, data-bits, parity-bit, stop-bits] whereas the number of data-bits may be 5 to 8.

At this mode, the serial-processor collects bytes and encapsulates the data at a UDP/TCP Ethernet frame.

The number of bytes collected to a single Ethernet packet is determined by the following factors:

» Allowed latency.

» Bus idle time.

Frame mode

A frame is a group of bytes sent by the customer equipment (CE) as complete message.

When using frame mode, the serial-processor will use the bus-idle-time to distinguish between frames. Each frame will be encapsulated as an individual UDP/TCP packet.

Service Connection Mode

The service connection-mode is set at the terminal server settings and defines the protocol option to be used for all services.

UDP

Serial data will be encapsulated as UDP/IP frames.

Since UDP is connectionless it is required by the user to configure the IP address of the UDP client as the destination. This is done at the 'terminal-serer' 'udp-service' cli hierarchy.

NOTE: UDP mode is not supported at current software version.

TCP

Serial data will be encapsulated as TCP/IP frames.

This mode allows higher availability for the end to end connection and traffic validation.

TCP connection will be established between the RLGE2FE16R router acting as a terminal server and the tcp client. The tcp client must initiate the connection so at this case there is no need to configure in advance the ip address of the client (unlike at UDP).

Service Port number

The TCP/UDP port number used at a terminal server service is defined explicitly at the user

configuration per 'service-id'. The port selected must be a member of the port range defined at the 'terminal-server' 'settings'.

Service Port number

The TCP port number used at a terminal server service is defined explicitly at the user configuration per 'service-id'. The port selected must be a member of the port range defined at the 'terminal-server' 'settings'.

Terminal Server Commands Hierarchy

+ root

    + serial

        + port

            - clear counters

            - create slot <1> port <1-2> [baudrate <9600,(50-368400)>] databits {8,<5-8>} [parity {no,no| odd| even}] [stopbits <1,1|2>] [bus-idle-time <bits (30-1000>] [bus <RS232| RS485>] [mode-of-operation <transparent>]admin-status [up| down]

            - remove slot <1> port <1-2>

            - show [slot <1> port <1-2>]

        + local-end-point

            - create slot <1> port <1-2> service-id <1-100> position <slave> application <terminal-server>

            - remove slot <1> port <1-2> service-id <1-100>

            - show

        + terminal-server

            - admin-status [enable | disable | show]

            - services show [service-id <>]

            + connections

                - dissconnect service-id <>

                - show service-id <>

            + counters [clear | show]

            + settings

- restore

- update [low-border-telnet-tcp-port (2001,<2001-65434>]
  [low-border-telnet-udp-port (2001,<2001-65434>]
  [low-border-serial-tunnel-port (9850,<1025- 65434>]
  [dead-peer-timeout <min,10 (0-1440)>]
  [buffer-mode (frame,<frame |byte>)]

- show

+ tcp-service

- create {remote-address <A.B.C.D>} {service-id <1-100>} {telnet-port <port num>}
  [null-cr-mode (off,<off|on>)]
  [max-tcp-clients (1,<1-8>)]

- remove service-id <1-100>

- show

+ udp-service

- create {remote-address <A.B.C.D>} {service-id <1-100>}
  {udp-server-port <port number>}
  {udp-client-address <A.B.C.D>} [null-cr-mode (off,<off|on>)]

- remove service-id <1-100>

- show

+ serial-tunnel

- create remote-address <A.B.C.D> service-id <1-100>

- remove service-id <1-100>

- show

Terminal Server Commands

Command	Description
Application connect	Enter the industrial application menu
Serial port	Create/update the serial port
Clear counters	Clear counters
Create	Slot : 1 (constant) Port : port number .1-2 Baud rate : 50,75,100,110,134,150,200,300,600,1200,2400,4800,9600,19200,38400,57600,115200,230400,460800,921600. Parity : no, odd, even Stopbits : 1,2 Mode of operation : transparent
Remove	Slot : 1 (constant) Port : port number .1-2
Show	
Local-end-point	
Create	Slot : 1 (constant) Port : port number .1-2 Service id: numeric value of serial service. Application : Terminal-server
Remove	Slot : 1 (constant) Port : port number .1-2 Service id: numeric value of serial service.
show	
terminal-server	Enter terminal server configuration
Admin-status	Enable / disable terminal server
Connections [disconnect | show]	Manage the tcp connections to the terminal server service-id : serial service-id number assigned to the terminal server
counters	Display counters

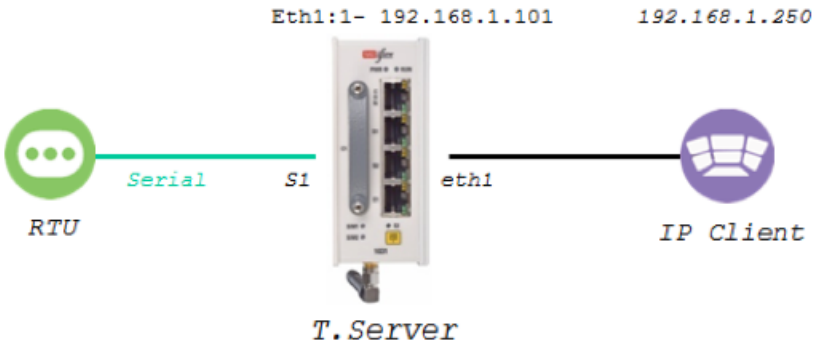
Command	Description
settings	Manage the range of TCP ports used for the terminal server to respond to. By default the allowed range is 2001-2100. Restore: restore to the default range. Update low-border-telnet-tcp-port <>: a numeric value for the tcp port range low border. The value must be >=2001. The allowed range will be the entered value (x) to x+100. The serial encapsulation will be in TCP packets. Update low-border-telnet-udp-port <>: a numeric value for the udp port range low border. The value must be >=2001. The allowed range will be the entered value (x) to x+100. The serial encapsulation will be in UDP packets. low-border-serial-tunnel-port <>: this option is used when the serial device is not connected locally to serial ports of the terminal server router, but rather to a remote router via serial tunneling. A numeric value for the udp/tcp port range low border. The allowed range will be the entered value (x) to x+100. default is 9849. changing the default can be to a range starting from 1025. The serial encapsulation will be in UDP or TCP packets depending on the serial-tunneling 'remote-end-point' configuration. Update dead-peer-timeout <0-1440>: this parameter will release the open TCP socket after the configurable time so a new connection could be established. Set in units of minutes, default value is 10. Setting the value 0 will disable the timeout and keep the session open until administratively release or ended by the client. Updating the counter requires removing the services configured in advance. Update buffer-mode: default –frame. frame – the terminal server will hold from egress the tcp packet until receiving validation from the serial local end that a message is completed. This mode avoids fragmentation of serial messages to different tcp packets. byte – serial originated packets will be egressed without additional buffering at the terminal server. Show : display the current tcp port range
Serial-tunnel	Configuration options to be used at the switch where the serial port is connected at. These fields will determine the remote side to where to draw the serial service to (the remote side is the switch at which the terminal server is established). If the terminal server is configured on a local switch which as well accommodates the serial port then this configuration of "serial-tunnel" should not be used!. Remote-address: the IP address of the terminal server .this would be the address of the application interface at the remote switch acting as the terminal server. Service-id: the local serial service-id to be mapped to the terminal server. show: display the configuration.
tcp-service	Configuration options to be used at the router where the terminal server is set. This option relates to a TCP service settings. Remote-address: the router own ACE 'application-host' interface IP address. Service-id: the serial service-id to which the terminal server serice relates to. the 'service-id' is created at the 'serial' 'local-end-point' and must be set to 'application'= 'terminal-server'. telnet-port: the tcp port to be used for the connection. Incoming tcp traffic with this port will be directed to the terminal server. Serial traffic will encapsulated to udp and send to the udp client with this port. mmax-tcp-clients: define how many tcp clients can open a connection at the specified service. null-cr-mode: this field settings (on|off) allows flexability in working with different types of terminals (as PuTTY, hyper terminal, CRT..)as each handles the CR bit differently. When set to On the switch will drop <NULL> character only if it arrives immediately after the <CR> (^M, 0x0d). For all other modes of operation, NULL_CR is ignored. default - off show : display the configuration.

Command	Description
udp-service	Configuration options to be used at the router where the terminal server is set. This option relates to a UDP service settings. Remote-address: the router own ACE 'application-host' interface IP address. Service-id: the serial service-id to which the terminal server serice relates to. the 'service-id' is created at the 'serial' 'local-end-point' and must be set to 'application'= 'terminal-server'. Udp-server-port: the udp port to be used for the connection. Incoming udp traffic with this port will be directed to the terminal server. Serial traffic will encapsulated to udp and send to the udp client with this port. Udp-client-address: an IPv4 address of the target UDP client to which the terminal server will reply to. null-cr-mode: this field settings (on|off) allows flexability in working with different types of terminals (as PuTTY, hyper terminal, CRT..)as each handles the CR bit differently. When set to On the switch will drop <NULL> character only if it arrives immediately after the <CR> (^M, 0x0d). For all other modes of operation, NULL_CR is ignored. default - off show : display the configuration.
remove	Address: IP address in the form of aa.bb.cc.dd. The IP is of the Application interface at the switch at which the serial port is connected at. Telnet-port: tcp port number in the range of 2000-2100. Service-id: serial service id number which the designated serial port is configured as a member in ("local end point). Slot : 1 (constant) Port : port number .1-4
show	Show port mapping

Example local Service

Below example demonstrates a setup of a local service at which both the telnet client and the serial slave are connected locally to the router.

The router is acting as a terminal-server.



1. Assign an IP interface

```
router interface create address-prefix 192.168.1.101/24 physical-interface eth1 purpose
application-host
```

2. Configure the serial port to be consistent with the properties of the serial slave.

```
The mode of operation of the serial port must be “transparent”
The local end point application type must be “terminal server”.
serial port create port 1 baudrate 9600 parity no databits 8 mode-of-operation
transparent
serial local-end-point create port 1 service-id  1 application terminal-server
```

3. Configure the terminal server to listen on port 20000

```
terminal-server admin-status enable
terminal-server settings update low-border-telnet-tcp-port 19999 buffer-mode byte
terminal-server tcp-service create service-id 1 remote-address 192.168.1.101 telnet-port
20000
commit
```

NOTE: Make sure to use proper serial connection between the RL1000GW serial port and the customer equipment.
The pin-out of the RL1000GW serial port is given in this documentation.

Testing the setup

4. Review your configuration using the following show commands

```
RL1000GW#router interface show
+------+---------+----+---------------+-----------------+-------------+
| VLAN |   Name    | Id |    IP/Subnet     |      Purpose       | Description |
+======+=========+====+===============+=================+=============+
| N/A   | eth1:1   | 1   |192.168.1.101/24|application host |               |
+------+---------+----+---------------+-----------------+-------------+
RL1000GW#serial port show
+-----+------+------+-------+-------------+------+------+--------++
| idx | slot | port |   bus   |     mode      | baud | data | parity |
|      |       |       |        |               | rate | bits |         |
+=====+======+======+=======+=============+======+======+========+
|   1   |   1    |   1    | RS232 | Transparent | 9600 |   8    |   None   |
+-----+------+------+-------+-------------+------+------+--------+
RL1000GW#serial local-end-point show
+-------+---------+------+------+----------------+----------+----------+----------+
| index | service | slot | port |    application    | position | firewall | firewall |
|        |    id     |       |       |                   |           |    mode    | protocol |
+=======+=========+======+======+================+==========+==========+==========+
|    1    |     1     |  1    |  1    | terminal-server |   Slave    | disable   |    any     |
```

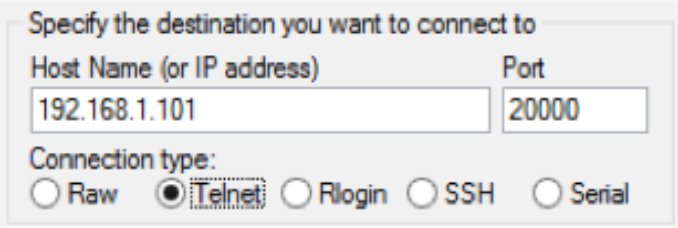
```
+-------+---------+------+------+----------------+---------+---------+----------+

RL1000GW# terminal-server settings show
+-------+------------+-----------+--------------+----------+--------+
| index | telnet-tcp  | telnet-udp | serial-tunnel | dead peer | buffer |
|       | port-range  | port-range |  port-range   |  timeout  |  mode  |
+=======+============+===========+==============+==========+========+
|   1   | 20000:20099 | 2001:2100  |   9850:9949   |    10     |  byte  |
+-------+------------+-----------+--------------+----------+--------+
RL1000GW#

RL1000GW# terminal-server tcp-service show
+-------+-----------+------------+---------------+-------------+----------------+
| index | service id | telnet port | dest ip        | null cr mode | max ip clients |
+=======+===========+============+===============+=============+================+
|   1   |     1      |    20000    | 192.168.1.101  |     off      |       1        |
+-------+-----------+------------+---------------+-------------+----------------+
```

5. Ping between the PC (192.168.1.250) and the RL1000GW (192.168.1.101) to validate IP connectivity.

6. Open a telnet session from the PC to the router "telnet 192.168.1.101 20000".



The connection will be indicated in the following show output

```
terminal-server connections show
+-------+---------+--------+---------------+---------------+--------+----------+---------
--
| index | service | telnet |     client     |     client     | service |  client   |
client
|       |   id    |  port  |   source IP    |    dest IP     |   id    | dest slot |
dest port
```

7. Connect your serial device to port S1 with proper serial connections.

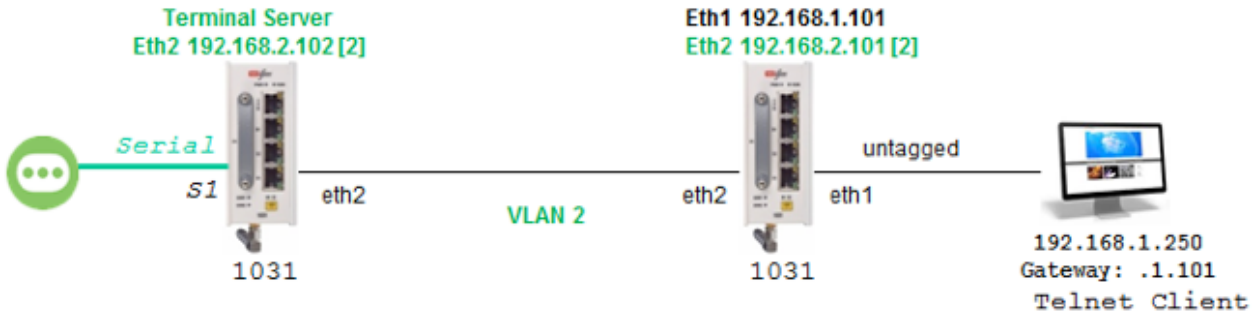
Your serial device shell will be reachable to telnet client (PC).

The serial connection can be validated by following the port counters.

```
RL1000GW#serial port show briefly slot 1 port 1
+-----+------+------+-----+-------------+------+------+--------+------+
| idx | slot | port | svc |     mode      | baud | data | parity | stop |
|     |      |      | id  |               | rate | bits |        | bits |
+=====+======+======+=====+=============+======+======+========+======+
|  1  |  1   |  1   |  1  | Transparent | 9600 |  8   |  None  |  1   |
+-----+------+------+-----+-------------+------+------+--------+------+

OctetsIn      : 20
OctetsOut     : 25
TxError       : 0
RxError       : 0
OctetsTotal   : 45
```

Example Networking



Left Router (Terminal Server)

1. Assign an IP interface

```
router interface create address-prefix 192.168.2.102/24 vlan 2 physical-interface eth2
purpose application-host
```

2. Assign routing towards the remote router lan subnet 192.168.1.x

```
router static
enable
configure terminal
```

```
ip route 192.168.1.0/24 192.168.2.101
write memory
exit
exit
```

3. Configure the serial port to be consistent with the properties of the serial slave.

```
The mode of operation of the serial port must be “transparent”
The local end point application type must be “terminal server”.
serial port create port 1 baudrate 9600 parity no databits 8 mode-of-operation
transparent
serial local-end-point create port 1 service-id  1 application terminal-server
```

4. Configure the terminal server to listen on port 20000

```
terminal-server admin-status enable
terminal-server settings update low-border-telnet-tcp-port 19999 buffer-mode byte
terminal-server tcp-service create service-id 1 remote-address 192.168.2.102 telnet-port
20000
commit
```

Right Router

1. Assign an IP interface for the lan connection

```
router interface create address-prefix 192.168.1.101/24 physical-interface eth1 purpose
general
```

2. Assign an IP interface for the wan connection

```
router interface create address-prefix 192.168.2.101/24 vlan 2 physical-interface eth2
purpose application-host
commit
```

Setup is ready.

you can now :

Ping between the PC to the terminal server 192.168.2.102 interface.

Open a telnet session from the PC to the router “telnet 192.168.2.102 20000”.

Your serial device shell will be available.

Modbus Gateway

The ComNet capability of gateway Modbus RTU to Modbus TCP is of yet another benefit to industrial area applications.

The router allows connecting an RS232 Modbus RTU and gateway it to a remote Modbus TCP client (SCADA) over the Ethernet.

The Modbus RTU slave is connected at the router local serial port, over an RS232 link. The Modbus TCP Client (SCADA) may be connected directly to the router Ethernet port or via an IP cloud. The router gateway will encapsulate the Modbus RTU to a TCP packet with port 502.

The router Modbus gateway is assigned with the stations ID of the Modbus RTU devices connected to it.

The gateway is set to use a ACE IP interface as its TCP traffic source.

Packet sent from Modbus TCP Client will carry the gateway IP interface and the Modbus RTU station ID as its target. The gateway will listen to incoming packets and forward the message in a serial uniform to relevant Modbus RTU using the station id as identifier.

Up to 5 instances of a gateway can co-exist. Each must use a different ACE IP interface and have a unique gateway-id.

A serial port, connecting a Modbus RTU device, can be associated with a single gateway instance.

A Modbus RTU device must have at least one Modbus ID. Each Modbus ID must be unique behind the gateway.

Implementation

The Modbus gateway is supported between a Modbus TCP and a Modbus RTU.

Modbus TCP gateway to Modbus ASCII is not implemented.

The gateway translates Modbus frames of same structure, meaning is it a prerequisite to have the Modbus TCP device use the same frame structure as the Modbus RTU device.

Modbus Gateway Commands Hierarchy

+ root

  + serial

    + port

      - create {slot <1>} {port <1-4>} {mode-of-operation < transparent >} [baudrate <>] [parity <>] [stopbits <>] admin-status [up| down]
        [bus <RS232| RS485>]

      - show

    + local-end-point

      - create create {slot <1>} {port <1-4>} {application < modbus-gw >}{service-id <>}
        [position <>] [protocol <>]

      - show

    + modbus-gw

      - show-gw-list

      - connection [clear | show]

      - counters

      - clear-id {gw-id <1-5>} {unit-id <1-255>}

      - clear-port {slot 1 port <1-4>}

      - show-by-id gw-id <1-5>} {unit-id <1-255>}

      - show-by-port {slot 1 port <1-4>}

    + debug

      - map-units-on-bus-show slot 1 port <1-4>

      - map-units-on-bus-start slot 1 port <1-4>

      - show-serial-points slot 1 port <1-4>

      - show-server-points slot 1 port <1-4>

      - show-tcp-points

    + history

      - clear {gw-id <1-5>}

      - show {gw-id <1-5>}

+ mapping

  - add-gw {address-prefix <a.b.c.d/e>} {admin-status (enable| diable} {gw-id <1-5>} [timeout-period <500-100,000>]

  - add-id {slot 1 port <1-4>} {gw-id <1-5>} {unit-id <1-255>}

  - remove-gw {gw-id <1-5>}

  - show-ids [gw-id <1-5>]

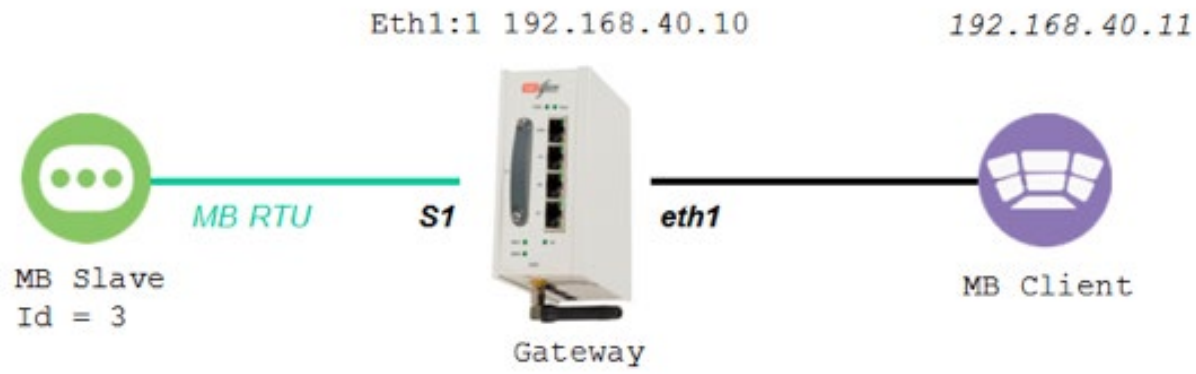
+ update [admin-status (enable| diable} | timeout {gw-id <1-5> timeout-period <500-100,000>}]

Modbus Gateway Commands Description

Command	Description
modbus-gw	
show-gw-list	Display the list of available gateway
Connection	Clear| show live and history TCP connections
counters	Clear| show counters per gateway id and unit id
debug	map-units-on-bus-start : initiate mapping of connected station ids behind a serial port. map-units-on-bus-show : show to station ids identified behind the serial port.
History	Show: Show latest reply from each unit and the time in seconds from that connection. Per gateway instance. Clear: Clear history table. Per gateway instance.
Mapping	Map a new gateway instance address-prefix: an IP address of an available ACE interface. A.b.c.d/e admin-status: (enable| diable) gw-id: unique gateway instance identifier. <1-5> timeout-period: set the maximum time allowed between incoming packets over the TCP session before dropping it <500-100,000> msec.
add-gw	add a gateway instance.
add-id	add a Modbus RTU station id to a serial port and a gateway instance.
Remove-gw	remove a gateway instance.
show-ids	show Modbus RTU station ids behind a gateway instance.
update	Update a gateway instance properties. admin-status (enable| diable. timeout-period <500-100,000>

Example

Following setup demonstrates Modbus gateway configuration.



1. assign IP interface for the gateway

```
router interface create address-prefix 192.168.40.10/24 physical-interface eth1 description
client admin-status enable purpose application-host
```

2. assign a serial port to be used for connecting the Modbus rtu slave

```
serial port create slot 1 port 1
serial local-end-point create slot 1 port 1 service-id 1 protocol modbus _ rtu application
modbus-gw
```

3. assign the gateway settings

```
modbus-gw mapping add-gw address-prefix 192.168.40.10/24 gw-id 4 admin-status enable
modbus-gw mapping add-id slot 1 port 1 gw-id 4 unit-id 3
```

output example

```
[/] modbus-gw connection show
+-------+-------+------------------+---------------+----------+
| Index | GW id |    GW IP/Subnet     |     ip addr      | src port |
+=======+=======+==================+===============+==========+
|    1    |    4    | 192.168.40.11/24   | 192.168.40.11 |   55132    |
+-------+-------+------------------+---------------+----------+
Completed OK

[modbus-gw/] debug map-units-on-bus-start port 1 slot 1
Port mapping started
```

```
Operation in process

[modbus-gw/] counters show-by-port
+------+------+----------+----------+----------+----------+
| Slot | Port | Rx valid | Rx error | Tx valid | Tx error |
+======+======+==========+==========+==========+==========+
|  1   |  1   |   477    |    0     |   582    |    0     |
+------+------+----------+----------+----------+----------+

[modbus-gw/] counters show-by-id gw-id 4
 gwid:4 unit id:65535
+----+---------+----------+----------+----------+----------+
| Gw | Unit Id | Rx valid | Rx error | Tx valid | Tx error |
+====+=========+==========+==========+==========+==========+
| 4  |    3    |   477    |    0     |   599    |    0     |
+----+---------+----------+----------+----------+----------+

+------+------+----------+----------+----------+----------+
| Slot | Port | Rx valid | Rx error | Tx valid | Tx error |
+======+======+==========+==========+==========+==========+
|  1   |  1   |   477    |    0     |   616    |    0     |
+------+------+----------+----------+----------+----------+

[modbus-gw/] debug map-units-on-bus-show
Operation in process

[modbus-gw/] history show gw-id 4
Units connected to Gw 4:
+----+-----------------+
| id | seconds elapsed |
+====+=================+
| 3  |       153       |
+----+-----------------+
[modbus-gw/] mapping show-ids
+----------+-----------------+---------+------+------+-------+
| GW index |   GW IP/Subnet  | Unit Id | slot | port |  bus  |
+==========+=================+=========+======+======+=======+
|    4     | 192.168.40.10/24 |    3    |  1   |  1   | RS232 |
+----------+-----------------+---------+------+------+-------+

[modbus-gw/] debug show-serial-points
```

```
Serial points:
slot:1, port:1, pointer:0x1007c408

[modbus-gw/] debug show-server-points
Server points:
IP addr:192.168.40.10, GwId:4, Subnet mask:255.255.255.0, pointer:0x10081580,

[modbus-gw/] debug map-units-on-bus-show
List of units for slot[1] port[1]:
Port mapping ended
```

DNP3 Gateway

DNP3 (Distributed Network Protocol) is an important protocol set used at SCADA applications.

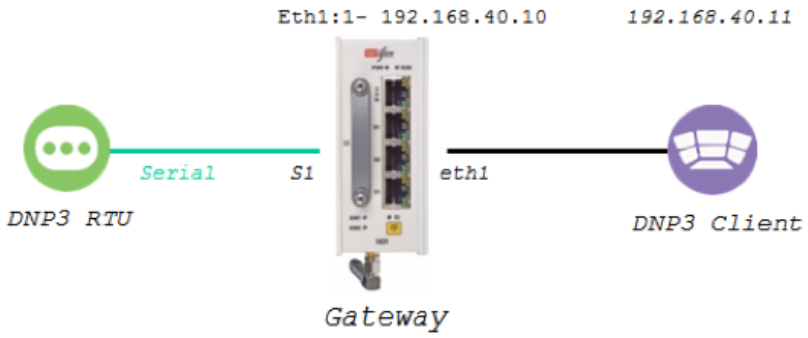
The ComNet switch supports gateway functionality between a DNP3 TCP client (master) and a DNP3 Serial RTU.

Configuration of a DNP3 gateway is made using the terminal server feature with the protocol well known tcp port 20000.

Please refer to the terminal server chapter for configuration structure.

Example

Following setup demonstrates DNP3 gateway configuration.



1. assign IP interface for the gateway

```
router interface create address-prefix 192.168.40.10/24 physical-interface eth1 purpose application-host
```

2. assign a serial port to be used for connecting the DNP3 RTU slave

```
serial port create port 1 mode-of-operation transparent
serial local-end-point create  port 1 service-id 1 protocol application terminal-server
```

3. assign the gateway using terminal server settings

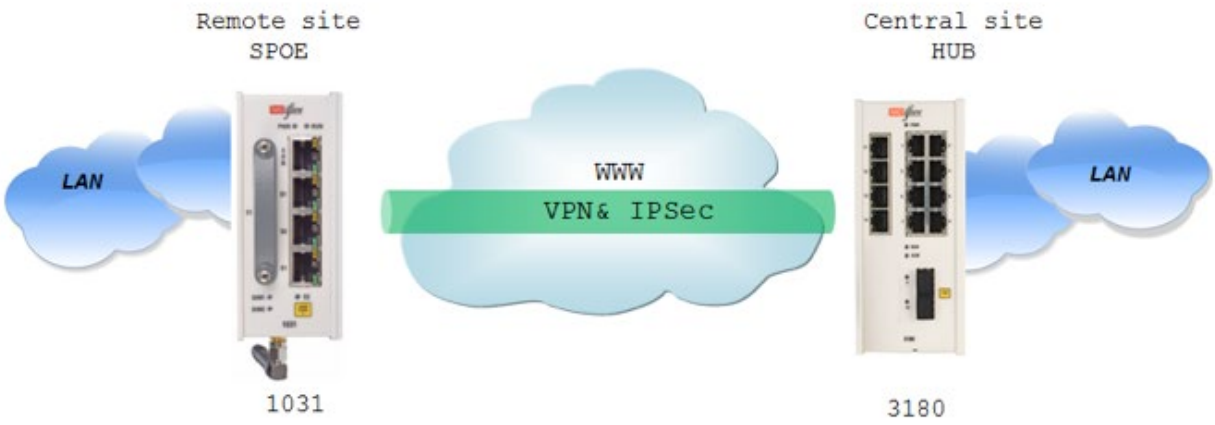
```
terminal-server admin-status enable
terminal-server settings update low-border-telnet-tcp-port 19999 buffer-mode frame
terminal-server tcp-service create service-id 1 remote-address 192.168.40.10 telnet-port 20000

commit
```

VPN

Background

When a distributed operational network uses public transport links for the inter-site connectivity, the traffic must be encrypted to ensure its confidentiality and its integrity. The RADiFlow switches support such a VPN (Virtual Private Network) connection using GRE tunnels (RFC2 2784) over an IPSec encrypted link. The IPSec tunnel can be set to use 3DES or AES encryption per the user configuration.



Modes supported

Folowing VPN modes are supported

1. IPSec VPN, route based
2. mGRE DM-VPN, route based

NOTE: Multiple VPN types cannot co-exist simultaneously

NOTE: The RL1000GW is recommended to be use as a spoke and less as a hub aggregation point.

Layer 3 DM-VPN

The DM-VPN mGRE mode is routing based and supports more complex networking and protection, providing higher scalability.

Topologies supported and guidelines

1. Multiple Hubs vs Multiple Spokes
2. Multiple Clouds
3. Multiple tunnels allowed at the hub.
4. Multiple tunnels allowed at each spoke towards different Hubs or towards the same hub via different clouds.
5. Supports static routing and OSPF
6. Layer 3 protection
7. The hub is recommended to be connected to the network using one of its Ethernet ports. A cellular uplink at the hub is not recommended as an aggregation interface to multiple VPNs.
8. A Spoke may have DM-VPN set over its cellular interface (at supported hardware) or Ethernet ports.
9. The hub listens for incoming NHRP requests from the spokes to initiate VPN. As such, it must hold a static IP address which is routable over the network.

Main advantages

1. Robust and supports large scale networks
2. Encryption of traffic as a protective measure against man in the middle attacks.
3. Addition of Spokes may not require further configuration at the Hub.

Layer 3 IPSec-VPN

IPSec VPN is designated for simple P2P networking where encryption is required.

The mode supported is 'transport' which is route based. A Tunnel logical interface is created at the routing table. User traffic which is designated to be encrypted is routed over the tunnel interface.

Topologies supported and guidelines

1. Point to Point, Hub vs Spoke.
2. Single tunnel allowed at the hub.
3. Single tunnel is allowed at the spoke.
4. The hub must be connected to the network using one of its Ethernet ports.
5. The spoke is recommended to be connected to the network using one of its Ethernet ports. The spoke may use a cellular connection only if the SIM is allocated by the ISP with a public, static IP address, without NAT.
6. Layer 3 protection to a second uplink is supported.
7. The hub must hold a static IP address which is routable over the network.
8. The spoke must hold a static IP address which is routable over the network.

Main advantages

1. Easy to configure an maintain.
2. Encryption of traffic as a protective measure against man in the middle attacks.
3. Interoperability with other vendors.

DM-VPN Commands Hierarchy

+ root

  + vpn gre

    + tunnel

      - create {name <>} {address-prefix <A.B.C.D/M>}
        {lower-layer-dev <ppp0| eth0| eth1.(vlan-id) | eth2.(vlan-id)>}
        {key <0.0.0.0,<a.b.c.d>} [ttl <64,0-255>]
        [holding-time<7200,1-65535>] [mtu (1418,<128-9600>)]
        [tos (inherint,<hex(0-255)>)][cisco-authentication <>]
        [tunnel-destination <>][tunnel-source <>]

      - remove {name<>}

      - show [name<>]

    + nhrp

      + map

        - {create | update} {multipoint-gre-name<>}
          {nbma-address<A.B.C.D>} {protocol-address-prefix< A.B.C.D/M>} [initial-register<no|yes>] [is-cisco<no|yes>]
          [protection-group<>] [position<master |slave>]

        - remove {multipoint-gre-name<>}

        - show

        - show-status

      - cache-flush

      - cache-purge

      - cache-show

      - {enable | disable}

      - log-show

      - route-show

      - show

    + protection-group

      - {create |udate |remove} {name<>} [default-route(yes,<no|yes>)] [wait-to-restore<0-1440>]

      - show

IPSec-VPN Commands Hierarchy

+ root

  + vpn ipsec

    + tunnel

      - crate {name <>} {address-prefix <A.B.C.D/M>}
        {lower-layer-dev <ppp0| eth0| eth1.(vlan-id) | eth2.(vlan-id)>}
        {remote-address<A.B.C.D>} [mtu<1400,128-1500>]
        [tos (inherint,<hex(0-255)>)] [ttl <64,0-255>]

      - remove {name<>}

      - show [name<>]

IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet of a communication session.

The IPSec protocol suite includes the modules described in this chapter.

Applications

IPSec should be configured when a VPN is used:

1. DM-VPN: IPSec is mandatory.
2. IPSec-VPN: IPSec is mandatory.
3. L2-VPN: IPSec Mandatory when the VPN is established over the public network and /or when security is required.

Authentication Header (AH)

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams.

» Supported mode per IKE phase 2. (transport ,tunnel)
» No specific configuration is available for AH. Authentication and encryption are implemented for ESP

Encapsulating Security Payload (ESP)

ESP provides origin authenticity, integrity and confidentiality protection of IP packets.

» Supported exchange mode per IKE phase 1. (main ,aggressive)
» Supported mode per IKE phase 2. (transport ,tunnel)
» Origin Authentication supported by IKE phase 1 and phase 2 HASH Cryptographic.
» Encryption supported by IKE phase 1 and phase 2 algorithms.

Security Associations

A Security Association (SA) is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. These entities are the VPN Hubs and Spokes.

This relationship is represented by a set of information that can be considered a contract between the entities. The information must be agreed upon and shared between all the entities.

ISAKMP provides the protocol exchanges to establish a security association between negotiating entities followed by the establishment of a security association by these negotiating entities in behalf of ESP/AH.

ISAKMP

ISAKMP provides a framework for a agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs.

First, an initial protocol exchange allows a basic set of security attributes to be agreed upon. This basic set provides protection for subsequent ISAKMP exchanges. It also indicates the authentication method and key exchange that will be performed as part of the ISAKMP protocol. After the basic set of security attributes has been agreed upon, initial identity authenticated, and required keys generated, the established SA can be used for the protection of the VPN tunnels.

ISAKMP implementations guards against denial of service, replay / reflection and man-in-the-middle. This is important because these are the types of attacks that are targeted against protocols.

As mentioned, A security association (SA) is a set of policy and key(s) used to protect information. The ISAKMP SA is the shared policy and key used by the negotiating peers in this protocol to protect their communication.

ISAKMP uses the Internet Key Exchange (IKEv1)for the authentication and encryption establishment.

Sources : RFC 4109 ,2408 ,2631 ,2412 ,racoon5.

IKE

Internet Key Exchange (IKE) negotiates the IPSec security associations (SAs). This process requires that the IPSec systems first authenticate themselves to each other and establish ISAKMP (IKE) shared keys.

Phase 2 is where Security Associations are negotiated on behalf of The VPN GRE services.

ISAKMP Phase 1

Phase 1 is where the two ISAKMP VPN peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA)or IKE Security Association.

The authentication is supported with Pre-Shared Keys or Digital Signatures (X.509)

Diffie and Hellman

Diffie and Hellman describe a means for two parties to agree upon a shared secret. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms.

Diffie-Hellman key agreement requires that both the sender and recipient of a message have key pairs.

The private key of each member is never sent over the insecure channel.

The public key is generated from the private key by each member and is the one sent over the insecure channel.

By combining one's private key and the other party's public key, both parties can compute the same shared secret number.

This number can then be converted into cryptographic keying material. That keying material is typically used as a key-encryption key (KEK) to encrypt the VPN GRE traffic. This key is kept secret and never exchanged over the insecure channel.

The D-H groups are identified by the length of the keys in bits. The larger the key (higher group id)the higher is the security but as well the resources required are higher and the user should consider performance degradation.

The D-H exchange can be authenticated with RSA signatures or pre-shared keys.

The exchange modes are "Main Mode" and "Aggressive Mode" and are accomplished at the phase 1.

Authentication

Pre-shared Key (PSK)

A PSK is an option for the IKE phase 1 authentication.

The encryption, hash, and authentication algorithm for use with a pre-shared key are a part of the state information distributed with the key itself.

Each VPN end point (Hubs, Spokes) must have a unique ID and a common shared key known to the remote VPN partner. Together these form the station PSK.

When a pre-shared key is used to generate an authentication payload, the certification authority is "None", the Authentication Type is "Preshared", and the payload contains the ID, encoded as two 64-bit quantities, and the result of applying the pseudorandom hash function to the message body with the KEY forming the key for the function

The PSK can be set as one of two forms:

1. IP address form A.B.C.D.
    a. Allowed in bot Main and Aggressive IKE modes
    b. The PSK of all members should be taken as their VPN network IP address.
2. Fully qualified domain name (FQDN).
    a. Allowed only when Aggressive IKE mode is used.

Below is an example of PSK configuration

1. Detail the preshared IDs of the VPN members and specify the id of local unit

```
RL1000GW#
ipsec isakmp update authentication-method pre _ shared _ key
ipsec isakmp update my-id SA.radiflow.com
ipsec preshared create id SA.radiflow.com key secretkey
ipsec preshared create id SB.radiflow.com key secretkey
ipsec policy create protocol gre
ipsec enable
commit
```

The above configuration example will result in following show output

```
[/] ipsec show global-defs
IPSec general defs
+--------------------------------+-----------------+
|           Parameter            |      Value      |
+================================+=================+
| Admin Status                   |     enabled     |
+--------------------------------+-----------------+
| My ID                          | SA.radiflow.com |
+--------------------------------+-----------------+
| Authentication method          |       PSK       |
+--------------------------------+-----------------+
| RSA Name                       |       N/A       |
+--------------------------------+-----------------+
| Log Level                      |      info       |
+--------------------------------+-----------------+
| DPD delay                      |        5        |
+--------------------------------+-----------------+
| DPD retry                      |        5        |
+--------------------------------+-----------------+
| DPD max fail                   |        5        |
+--------------------------------+-----------------+
| phase1 IKE mode                |   aggressive    |
+--------------------------------+-----------------+
| phase1 encryption algo         |     aes 128     |
+--------------------------------+-----------------+
| phase1 hash algo               |      sha1       |
+--------------------------------+-----------------+
| phase1 lifetime                |      86400      |
+--------------------------------+-----------------+
| Diffie Hellman group           |    modp1024     |
+--------------------------------+-----------------+
| phase2 encryption algo         |      3des       |
+--------------------------------+-----------------+
| phase2 auth algo               |       md5       |
+--------------------------------+-----------------+
| phase2 lifetime                |      86400      |
+--------------------------------+-----------------+
| PFS group                      |    modp1024     |
+--------------------------------+-----------------+

[ipsec/] show preshared
IPSec preshared keys
+-----------------+-----------------+
|   identifier    |       key       |
+=================+=================+
| SA.radiflow.com | *************** |
+-----------------+-----------------+
| SB.radiflow.com | *************** |
+-----------------+-----------------+
Total: 2

[ipsec/] policy show
IPSec policy database
+----------------+----------------+-------+-------+
|      from      |       to       | proto | notes |
+================+================+=======+=======+
| 0.0.0.0/0[any] | 0.0.0.0/0[any] |  gre  |       |
+----------------+----------------+-------+-------+
```

RSA Signatures (X.509)

Uses a digital certificate authenticated by an RSA signature.

The user is required to generate certificates from a trusted source and to import these to the VPN parties (Hubs, Spokes).

Two files are required, one is the certificate itself and the other is the key.

The files should have extensions of .crt and .key.

Below is a screenshot of such 2 files placed on a PC with tftp client and CLI example of importing them.

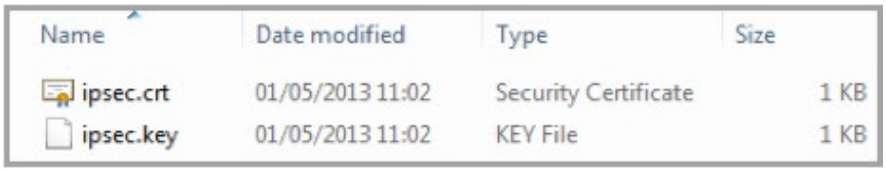


Figure 9 The certificate files

1. Import the key file

```
RL1000GW# rsA-signature import tftp://172.17.203.31/ipsec.key
 RSA signature file (ipsec.key) imported successfully
```

2. Import the certificate file

```
RL1000GW# rsA-signature import tftp://172.17.203.31/ipsec.crt
 RSA signature file (ipsec.crt) imported successfully
```

3. Validate successful import

```
RL1000GW# show rsA-signature list
ipsec.crt
ipsec.key
```

4. Activate the certificate

```
ipsec rsa-signature activate crt-file ipsec.crt key-file ipsec.key rsa-sig-name test _ 1
```

5. Update the ipsec isakmp to use the certificate instead of the PSK

```
ipsec isakmp update authentication-method rsasig
```

NOTE: The ipsec isakmp property "my id" is not of importance when using certificates as the authentication method

The above configuration example will result in following show output

```
[/] ipsec show global-defs
IPSec general defs
+--------------------------------+------------+
|           Parameter            |   Value    |
+================================+============+
| Admin Status                   |  enabled   |
+--------------------------------+------------+
| My ID                          |    N/A     |
+--------------------------------+------------+
| Authentication method          |  RSA-SIG   |
+--------------------------------+------------+
| RSA Name                       |   test1    |
+--------------------------------+------------+
| Log Level                      |    info    |
+--------------------------------+------------+
| DPD delay                      |     5      |
+--------------------------------+------------+
| DPD retry                      |     5      |
+--------------------------------+------------+
| DPD max fail                   |     5      |
+--------------------------------+------------+
| phase1 IKE mode                | aggressive |
+--------------------------------+------------+
| phase1 encryption algo         |  aes 128   |
+--------------------------------+------------+
| phase1 hash algo               |    sha1    |
+--------------------------------+------------+
| phase1 lifetime                |   86400    |
+--------------------------------+------------+
| Diffie Hellman group           |  modp1024  |
+--------------------------------+------------+
| phase2 encryption algo         |    3des    |
+--------------------------------+------------+
| phase2 auth algo               |    md5     |
+--------------------------------+------------+
| phase2 lifetime                |   86400    |
+--------------------------------+------------+
| PFS group                      |  modp1024  |
+--------------------------------+------------+
```

Exchange Modes

Main

Main mode is the more secure option for phase1 as it involves the identity protection.

Session flow:

- Session begins with the initiator sending a proposal to the responder describing what encryption and authentication protocols are supported, the life time of the keys, and if phase 2 perfect forward secrecy should be implemented. The proposal may contain several offerings. The responder chooses from the offerings and replies to the initiator.
- The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the IKE SA.
- The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPSec negotiation (Quick Mode) begins.

In applications at which the IP addresses used for the VPN network are not static (for example a cellular spoke retrieving dynamic IP from the ISP over its PPP interface) the Main mode of IKE is not applicable.

Pre-shared key

When used in main mode the PSK must be in the form of IP address and use the VPN network addresses of the parties.

NOTE: In Applications where the VPN is used over a cellular link, the IKE mode to be used is Aggressive. Main mode is not applicable.

Aggressive

In this mode the negotiation is quicker as the session is completed in only 3 messages. The disadvantage is in that the identity of the peers is not protected.

The first two messages negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities. In addition the second message authenticates the responder. The third message authenticates the initiator and provides a proof of participation in the exchange.

- The initiator send a request with all required SA information.
- The responder replies with authentication and its ID.
- The initiator authenticates the session in the follow-up message.

Pre-shared key

When used in Aggressive mode the PSK may be either in the form of IP address or fqdn. The PSK doesn't have to be the actual IP addresses of the VPN network interfaces as it considers the enter value as text (in the format of IP) and not as a valid IP address.

NOTE: In Applications where the VPN is used over a cellular link, the IKE mode to be used is Aggressive. The PSK may be of IP format or fqdn

Settings structure

- » Authentication method (PSK ,X.509)
- » Diffie–Hellman key exchange group (a.k.a OAKLY groups)
- » IKE exchange mode
  - › Main
  - › Aggressive
- » Encryption algorithm
  - › Advanced Encryption Standard (AES)
    - ·128 and 256 key size options
    - ·symmetric algorithm
  - › Triple Data Encryption Algorithm (3DES)
    - ·comprises of three DES keys, K1, K2 and K3, each of 56 bits
- » Authentication s HASH algorithms
    - ·Secure Hash Algorithm SHA-1 (160 bit)
    - ·Secure Hash Algorithm SHA-2 (256 |512 bit)
    - ·Message Digest (MD5) (128 bit)
- » Life time and Dead Peer Discovery settings

ISAKMP Phase 2

At this phase the negotiation of SA to secure the VPN GRE data using IPSec is made.

Modes

The common mode to use between end stations supporting IPSec (the VPN parties) is called Transport mode. This is the mode supported by ComNet.

Perfect forward secrecy (PFS)

The PFS is a part of the key agreement session and has a purpose to ensure that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future. The VPN (GRE, IPSEC) sessions can negotiate new keys for every communication and if a key is compromised only the specific session it protected will be revealed.

The PFS uses as well the D-H groups but independently from phase 1.

Settings structure

- » Supported mode
  - › Transport (yes)
  - › Tunnel (no)
- » Authentication s HASH algorithms
  - › Secure Hash Algorithm SHA-1 (160 bit)
  - › Secure Hash Algorithm SHA-2 (256 |512 bit)
  - › Message Digest (MD5) (128 bit)
- » Perfect Forward Secrecy type (PFS)
- » Encryption algorithm
  - › Advanced Encryption Standard (AES)
    - ·128 and 256 key size options
    - ·symmetric algorithm
  - › Triple Data Encryption Algorithm (3DES)
    - ·comprises of three DES keys, K1, K2 and K3, each of 56 bits
- » Life time
  - › Soft – hard coded. At this threshold value the IKE starts a new phase 2 exchange.
  - › Hard- SA which has exceeded this threshold value will be discarded.

IPSec Command Association

In below are detailed the configuration fields of the IPSec in their respective association to the ISAKMP structure.

Highlighted in blue are the CLI names of the configurable fields.

Enable IPSec

{enable |disable}

Settings

Log level (log-level)

Dead Peer Discovery

delay (dpd-delay)

max failure (dpd-maxfail)

max retires (dpd-retry)

flush Security Association (flush-sa proto)

id-type (id-type)

soft timer (soft-lifetime)

Phase 1

Authentication method {pre_shared_key | rsasig}

Diffie–Hellman key exchange Group (dh-group)

Internet Key Exchange mode (ike-phase1-mode)

Encryption Algorithm (phase1-encryption-algo)

Hash Algorithm (phase1-hash-algo)

Life Time (phase1-lifetime)

Phase 2

Perfect Forward Secrecy (pfs-group)

Encryption Algorithm (phase2-encryption-algo)

Authentication Algorithm (phase2-auth-algo)

- Life Time (phase2-lifetime)

IPSec Policy

- Name (notes)
- Source address (src-address-prefix)
- Destination address (dst-address-prefix)
- Source protocol port (src-port)
- Destination protocol port (src-port)
- Protocol (protocol)

Preshared Keys

- Key : (key)
- Own PSK id : (id)
- Partner PSK id : (id)
- Partner PSK id : (id)

Certificates X.509

Import crt file (flush-sa proto)

Import key file (rsA-signature import)

Activate certificate file (rsa-signature activate)

Certificate name (rsa-sig-name)

IPSec Commands Hierarchy

+ root

- rsA-signature import {flash:<file name> | sftp://<user:password@<ip>/<file_name> | tftp://<ip>/<file_name> }

- show rsA-signature list

    + ipsec {enable | disable}

        - flush-sa proto {ah | esp | ipsec | isakmp}

        - rsa-signature activate {crt-file <file name> | key-file <file name> |rsa-sig-name <name>}

        + isakmp update

            - authentication-method {pre_shared_key | rsasig}

            - dh-group <none | modp768 | modp1024 | modp1536 | modp2048 | modp3072 |modp4096 | modp6144>

            - pfs-group < none | modp768 | modp1024 | modp1536 | modp2048 | modp3072 |modp4096 | modp6144 |modp8192>

            - dpd-delay <5,0-120> dpd-maxfail <5,2-20> dpd-retry <5,1-20>

            - log-level <error |warning |notify |info |debug |debug2>

            - my-id <>

            - soft-lifetime <1-99>

            - id-type {none| fqdn}

            - ike-phase1-mode <aggressive |main> phase1-encryption-algo <3des | aes-128 | aes-256> phase1-hash-algo <md5 |sha1 |sha256 |sha512>

            - phase2-auth-algo < hmac_md5 | hmac_sha1 | hmac_sha256 | hmac_sha512> phase2-encryption-algo <3des |aes-128 |aes-256>

            - phase1-lifetime <86400,(180-946080000)> phase2-lifetime <86400,(180-946080000)>

            - rsa-sig-name <name>

+ policy {create | remove | show}

            src-address-prefix <A.B.C.D/E> dst-address-prefix < A.B.C.D/E > src-port <> dst-port <> protocol [gre |tcp |udp] notes [text]

+ preshared {create | remove} key <> id <>

+ show
    - log {grep| num-of-lines }
    - global-defs
    - policy
    - preshared
    - rsa-signature-file
    - sa [proto {ah | esp | ipsec | isakmp}]

IPsec Commands

Command	Description
rsA-signature import	Import the X.509 certificate file and key file to the application from a connected USB drive or tftp /sftp servers. These files are mandatory for IPSec to encrypt using X.509 certificates. These files are not required if IPSec is used with preshared keys. show rsA-signature list Show the files available
IPsec	Enter the IPsec configuration mode
Enable | disable	Default is disable
rsa-signature activate	Activation of the available certificate and key files. Crt-file ; name of the certificate file. Key-file : name of the key file. rsa-sig-name : user configurable name for the signature.
isakmp update	
authentication-method	pre_shared_key : preshared keys will be used. (default) Rsasig : X.509 certificates will be used.
dh-group	Diffie–Hellman key exchange Group. Relates to phase 1. determines the strength of the key used in the key exchange process. The higher the group number, the stronger the key and security increases. Options : none modp768 (DH group 1) modp1024 (default) (DH group 2) modp1536 (DH group 3 and 5) modp2048 (DH group 14) modp3072 (DH group 15) modp4096 (DH group 16) modp6144 (DH group 17) modp8192 (DH group 18)
pfs-group	Perfect Forward Secrecy type. Relates to phase 2. determines the strength of the key used in the key exchange process. The higher the group number, the stronger the key and security increases. Options: none modp768 modp1024 (default) modp1536 modp2048 modp3072 modp4096 modp6144 modp8192
dpd-delay	Dead Peer Discovery delay .defines the interval between following keep alive messages. Permissible range : 0-120 (default is 5)
dpd-maxfail	Dead Peer Discovery max attempts to determine failure. Permissible range :2-20 (default is 5)
dpd-retry	Dead Peer Discovery max retry attempts. A retry is initiated after a failure at “dpd-maxfail”. Permissible range : 1-20 (default is 5)

Command	Description
log-level	Syslog warnings levels to be logged. error warning notify info (default) debug debug2
my-id	Own preshared id. Dependent on "id-type" set ,my-id can be in either domain name format or ipv4 format. If "id-type" is set to "none": No need to set value in "my-id" as it will automatically use a valid IP address. If "id-type" is set to "fqdn": "my-id" should be set with a domain name format. for example : * Spoke.radiflow.com
Id-type	Set the type of form used for the IPSec local id. None : the units own preshared id will be the default ip interface. Address : this option is not supported in current version. fqdn : the units own preshared id will be in a domain name format. For example spoke. radiflow.com default : none
ike-phase1-mode	Internet Key Exchange mode type use for Phase 1. Aggressive (default) main
phase1-encryption-algo	Encryption Algorithm used for phase 1. 3des aes-128 (default) aes-256 phase1-hash-algo Hash Algorithm used for phase 1. md5 sha1 (default) sha256 sha512
phase1-lifetime	The lifetime of the key generated between the stations. 180-946080000 sec. Default is 86400
phase2-auth-algo	Authentication Algorithm for phase 2. hmac_md5 (default) hmac_sha1 hmac_sha256 hmac_sha512
phase2-encryption-algo	Encryption Algorithm for phase 2. 3des (default) aes-128 aes-256
Phase2-lifetime	The lifetime of the key generated between the stations. 180-946080000 sec. Default is 86400

Command	Description
soft-lifetime	When a dynamic IPSec SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPSec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. Permissible values are 1-99 and represents percentage. soft lifetime = <1-99>*hard lifetime /100
rsa-sig-name	The name set by the user for the signature
Policy create	Configure the policy to determine the type of traffic to encrypt: src-ip : A.B.C.D form Ip address of the packet source. dst-ip : A.B.C.D form Ip address of the packet destination. src-port : port number of the packet source. dst-port : port number of the packet destination. protocol : the type of protocol ,for example TCP ,UDP,GRE. Preshared {create | remove} Configuration of pre shared identifiers for local node and all remote IPsec nodes. ID: unique identifier for the IPSec participant node Can be in either domain name format or ipv4 format.) Key: preshared key which should be common for all nodes participating. text, numerical or combination string. notes : name of the policy
Show	Show IPsec

IPSec defaults

```
[/] ipsec show global-defs
IPSec general defs
+--------------------------------+-----------------+
|           Parameter            |      Value      |
+================================+=================+
| Admin Status                   |    disabled     |
+--------------------------------+-----------------+
| ID Type                        |       none      |
+--------------------------------+-----------------+
| My ID                          |       N/A       |
+--------------------------------+-----------------+
| Authentication method          | pre_shared_key  |
+--------------------------------+-----------------+
| RSA Name                       |       N/A       |
+--------------------------------+-----------------+
| Log Level                      |       info      |
+--------------------------------+-----------------+
| DPD delay                      |        5        |
+--------------------------------+-----------------+
| DPD retry                      |        5        |
+--------------------------------+-----------------+
| DPD max fail                   |        5        |
+--------------------------------+-----------------+
| phase1 IKE mode                |   aggressive    |
+--------------------------------+-----------------+
| phase1 encryption algo         |     aes128      |
+--------------------------------+-----------------+
| phase1 hash algo               |       sha1      |
+--------------------------------+-----------------+
| phase1 lifetime                |     86400       |
+--------------------------------+-----------------+
| Diffie Hellman group           |    modp1024     |
+--------------------------------+-----------------+
| phase2 encryption algo         |       3des      |
+--------------------------------+-----------------+
| phase2 auth algo               |    hmac_md5     |
+--------------------------------+-----------------+
| phase2 lifetime                |     86400       |
+--------------------------------+-----------------+
| PFS group                      |    modp1024     |
+--------------------------------+-----------------+
```

Cellular Modem

Cellular coverage is widely spread nowadays and has become quite a reliable medium. Hence an integrated cellular modem interface is of great benefit especially in utility applications where small sites require a backup traffic path on top of the physical line.

As well it might be the case that the customer installation is at a remote site or not permanent at a fixed location. Such cases will be classical use cases where the cellular solution will be of advantage over laying a physical connection to site.

The RL1000GW supports options for GPRS/UMTS modem or LTE.

A modem provides a key solution for connectivity to remote sites.

The modem support dual SIM card for redundancy and backup between Internet Service Providers.

LTE Modem

Two ordering options are available for the LTE modem, one for European bands and a second for North America.

At both cases the modem supports LTE (in corresponding bands) and as well GSM/GPRS/EDGE.

Following table describes the bands supported per ordering option.

Topic	Type	Frequency	Band	N.America	Europe
AIR INTERFACE	LTE			Y	Y
AIR INTERFACE	HSPA+			Y	Y
AIR INTERFACE	GSM			Y	Y
AIR INTERFACE	GPRS			Y	Y
AIR INTERFACE	EDGE			Y	N
FREQUENCY BANDS	LTE	2100	1	N	Y
FREQUENCY BANDS	LTE	1900	2	Y	N
FREQUENCY BANDS	LTE	1800	3	N	Y
FREQUENCY BANDS	LTE	AWS	4	Y	N
FREQUENCY BANDS	LTE	850	5	Y	N

FREQUENCY BANDS	LTE	2600	7	N	Y
FREQUENCY BANDS	LTE	900	8	N	Y
FREQUENCY BANDS	LTE	700	13	Y	N
FREQUENCY BANDS	LTE	700	17	Y	N
FREQUENCY BANDS	LTE	800	20	N	Y
FREQUENCY BANDS	LTE	1900	25	Y	N
FREQUENCY BANDS	LTE	2600	38	N	N
FREQUENCY BANDS	LTE	2300	40	N	N
FREQUENCY BANDS	LTE	700	-	N	N

GPRS/UMTS Modem

Following modes and spectrums are supported:

- » 3G UMTS– HSDPA. cat 5/6
  - › Triple band : 2100/1900/900 MHz
  - › Triple band : 2100/1900/850 MHz
- » 2G GSM- EDGE / GPRS. class 12
  - › Quad band :850/900/1800/1900 MHz

The maximum data throughput is determined according to the cellular service and might be different for down-stream and up-stream.

Topologies supported:

Point to Point – single spoke to a single Hub.

Multi Point to Point – multiple spokes to a single Hub.

NAT support using the IPsec encryption enables the spoke the important availability also when retrieving private IP from the ISP.

Interface Name

At various applications the addressing of configuration to the cellular interface will be done using its name.

A cellular interface established with an LTE modem is referenced with the name eth0.

A cellular interface established with the GPRS/UMTS modem is referenced with the name ppp0.

Examples of addressing the cellular modem via its name

DM-VPN

```
vpn gre tunnel create address-prefix 10.10.10.20/24 lower-layer-dev ppp0 name mgre1 key
10.0.0.0 admin-status enable


vpn gre tunnel create address-prefix 10.10.10.20/24 lower-layer-dev eth0 name mgre1 key
10.0.0.0 admin-status enable
```

NAT

```
router nat dynamic create interface-name eth0 description LTE
router nat dynamic create interface-name ppp0 description GPRS
```

Method of operation

At the RL1000GW spoke side, a simple configuration of the cellular modem is enough to have the spoke approach the ISP to retrieve an IP address using known link protocol PPP. Authentication versus the ISP will be made using the SIM cards and PAP protocol. Dependent on the ISP service this IP might be private behind NAT or public.

The Cellular connection is typically used with following services:

1. DM-VPN

2. NAT

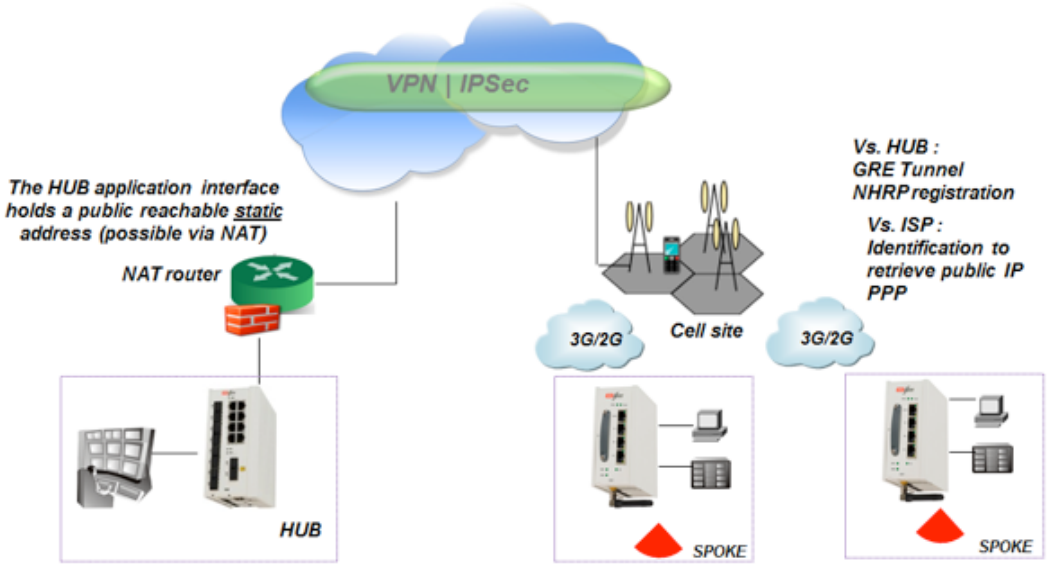
VPN Application

Once Holding an IP address retrieved from the ISP at its PPP interface, and with a VPN configured, the Spoke will initiate NHRP request for registration towards the Hub.

The Hub must be a well know participant in the network by holding a static address. The IP assigned to the hub must be routable with the IPs the cellular ISP will allocate to the cellular Spokes. If the network cloud is a public one (as www) then the Hub must have a PUBLIC, STATIC IP assigned to it.

The Hub will listen on its interface to NHRP requests from the spoke and will allow the VPN establishment dependent on the authentication.

A Hub must have a fixed connection to the network, it may not be connected with the cellular modem as a spoke.



SIM card state

The modem can occupy 2 different SIMs. The SIMs may be of the same ISP or not.

At a given moment a connection can be available via a single SIM.

Redundancy can be achieved using RSSI measurements and echo tests to determine which SIM is preferred to be used.

The user can decide if to select a certain SIM as preferred for default connection.

The Modem can be set to work in a specific technology 2G/3G/4G or to be set for AUTO select mode at which it will aim to connect to the best network available.

Each SIM can be individually configured and enabled /disabled.

Dependent on configuration and availability, the status of a SIM may be one of the following at the modem:

- Unknown – SIM is either:
  - Not available at the slot
  - Cellular modem is not enabled
  - Cellular modem in under refresh state
  - Modem malfunction
- Disabled – The modem is enabled but the SIM was not configured.
- Ready – SIM is available and configured.
- Connecting – Modem is trying to retrieve IP from the ISP using the SIM
- Connected – the modem retrieved an IP address from the ISP with the selected SIM.
- Failed – failure to connect with the selected SIM.
- Connected as Secondary – Modem is connected with the alternative SIM, meaning not to the SIM originally chosen by the user as preferred.
- Connected as Alternative – modem is connected with the alternative SIM, due to a recognized failure in connecting to the preferred SIM.

SIM state example

1.Below is an example of SIMs admin state. SIM in slot 1 had been enabled while SIM in slot 2 is disabled.

The show command used is cellular wan show.

```
[/] cellular wan show
+----------+-----------+----------+-----------+-----------+----------------+-----+-------------+---------+
| sim slot | sim admin | operator | apn name  | user name |    password    | pin |   radio     | flow    |
|          |   status  |   name   |           |           |                |     |   access    | control |
|          |           |          |           |           |                |     | technology  |         |
+==========+===========+==========+===========+===========+================+=====+=============+=========+
|    1     |  enabled  | cellcom  | internetg |   guest   | ************** | N/A |    auto     |   YES   |
+----------+-----------+----------+-----------+-----------+----------------+-----+-------------+---------+
|    2     | disabled  |   N/A    |    N/A    |    N/A    | ************** | N/A |    auto     |   YES   |
+----------+-----------+----------+-----------+-----------+----------------+-----+-------------+---------+
```

2. SIM 1 is connected following the modem enable and the SIM properties configured.SIM 2 is configured an in READY state.

```
cellular enable
cellular wan update admin-status enable apn-name internetg sim-slot 1 operator-name
cellcom user-name guest password guest


cellular wan update admin-status enable apn-name internet.pelephone.net.il sim-slot 2
operator-name pelephone user-name pcl@3g password pcl
```

```
[/] cellular show
cellular enabled
[/] cellular wan show
+----------+-----------+----------+-------------------------+-----------+----------------+-----+-------------+---------+
| sim slot | sim admin | operator |        apn name         | user name |    password    | pin |   radio     | flow    |
|          |   status  |   name   |                         |           |                |     |   access    | control |
|          |           |          |                         |           |                |     | technology  |         |
+==========+===========+==========+=========================+===========+================+=====+=============+=========+
|    1     |  enabled  | cellcom  |        internetg        |   guest   | ************** | N/A |    auto     |   YES   |
+----------+-----------+----------+-------------------------+-----------+----------------+-----+-------------+---------+
|    2     |  enabled  | pelephone| internet.pelephone.net.il | pcl@3g  | ************** | N/A |    auto     |   YES   |
+----------+-----------+----------+-------------------------+-----------+----------------+-----+-------------+---------+

[/] cellular network show
+------+-------------+-------------+---------+----------+-----------+--------+------+-------------+
| slot |    oper     |    Last     | Changes | Failures |   Last    | Caveat | RSSI | Last RSSI   |
|      |   status    | update(sec) |         |          |  Failure  |        | [dBm]| check(sec)  |
+======+=============+=============+=========+==========+===========+========+======+=============+
|  1   | CONNECTED!  |     96      |   10    |    0     |    N/A    |   No   | -67  |     132     |
+------+-------------+-------------+---------+----------+-----------+--------+------+-------------+
|  2   |   READY     |     117     |    5    |    0     |    N/A    |   No   | -79  |     113     |
+------+-------------+-------------+---------+----------+-----------+--------+------+-------------+
```

3. The modem retrieved an IP from the ISP

```
[/] cellular connection show
+-----------+---------------+--------+-------+----------+-------+
| interface |    local ip   |   tx   |   tx  |    rx    |   rx  |
|           |               | packet | error | packets  | error |
+===========+===============+========+=======+==========+=======+
|   ppp0    | 46.210.197.173|    6   |   0   |    5     |   0   |
+-----------+---------------+--------+-------+----------+-------+
```

3. The modem retrieved an IP from the ISP

```
[/] cellular connection show
+-----------+-----------------+---------+--------+----------+--------+
| interface |    local ip     |   tx    |   tx   |    rx    |   rx   |
|           |                 | packet  | error  | packets  | error  |
+===========+=================+=========+========+==========+========+
|   ppp0    | 46.210.197.173  |    6    |   0    |    5     |   0    |
+-----------+-----------------+---------+--------+----------+--------+
```

Backup and redundancy

Backup between Interfaces (between GSM or Physical interface)

A cellular link is by nature a high cost path and with a significant lower bandwidth then a physical channel.

When the cellular link is to be used for backup to a physical link then resilient routing protocols can determine the primary and backup paths.

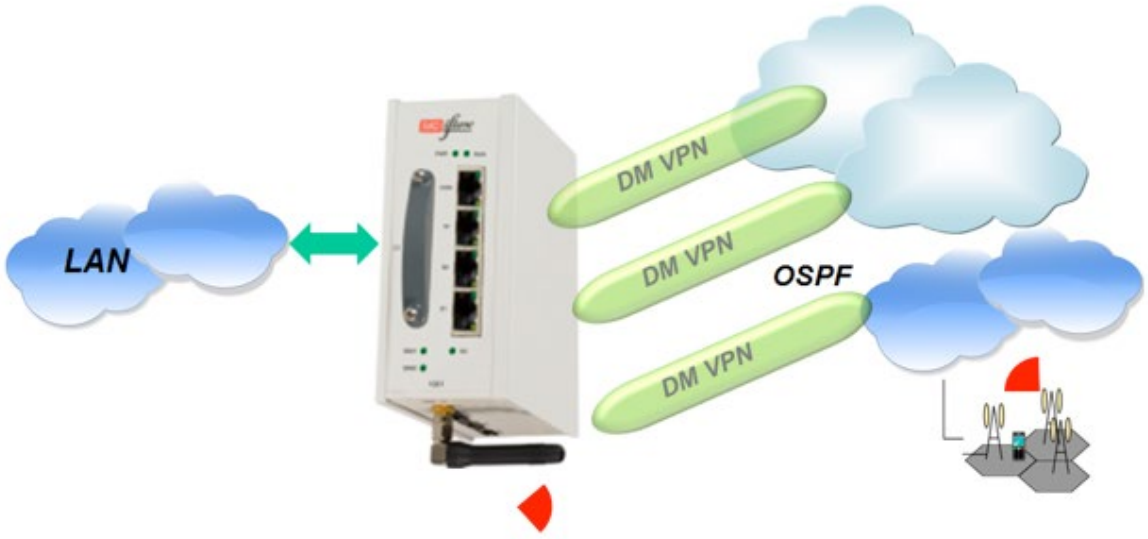


Figure 10 : L3 protection

Modem conditional reload

In case the modem is continuously unsuccessful in establishing a connection and retrieving an IP from the ISP, a reload can be trigger to the router.

A configuration parameter "retry-threshold-reload" is available to be set between 0 (disabled) and 30, whereas values 1-30 represents the number of consecutives failures.

A typical flow is as follow:

- Once a SIM is in "CONNECTING…" and instead of reaching "CONNECTED" has reached "FAILED". Such attempt is approximately 2 minutes long (non configurable).
- The counter progresses with every such above condition and summarize for both Sims together.
- The following states will reset the counter: "CONNECTED", "CONNECTED AS ALTERNATIVE","CONNECTED AS SECONDARY".

NOTE: The quality echo tests are applicable when the status of the SIM is "CONNECTED". At "connected" state, the "retry-threshold-reload" counter is cleared. This means the quality tests have no direct influence on this counter.

NOTE: In case of a single SIM card is used, the 'continuous-echo' test will result in action of 'cellular modem refresh' in case the test fails. If the modem is in 'conencted' state but the echo test fails to meet the configured criterias (ping loss/ rtt..) the router will refresh the modem as attempt to recover.

Cellular Commands Hierarchy

+ root

  + Cellular

    + continuous-echo

      - {create | update} {name <>} {dest-ip-address <ip address>} [loss-threshold <50,10-99>] [num-of-requests <3,1-100>] [rtt-threshold < 5000msec(1,000-20,000)>] [interval (60sec<1-1440>)] [request-size (100bytes<64-1500>]

      - remove {dest-ip-address <ip address>} {name <> }

      - show-config

      - show-status

    + modem

      - power_down

      - power-up

      - send command at+cgsn]

      - get {iccid| imei| model| version}

    + settings

      - update [quality check <0,time interval>] [backoff1 < 60sec,10-600>] [backoff2<300sec,10-600>] [default-route {yes|no}] [lcp-echo-interval<10sec,0-600>] [lcp-failure<4,1-64>] [preferred-sim {1|2|none}] [rssi-threshold-dbm<-100dbm ,-144 to -61>] [wait-to-restore <14400sec,120-86400>]

      - update retry-threshold-reload <0-30>

      - show

    + wan

      - update {sim-slot <slot(1-2>} {admin-status <enable | disable>} {apn-name <name>} [operator-name <name>] [pin <pin>] [user-name <name>] [password <password>] [radio-access-technology {auto |2G |3G |2Gthen3G |3Gthen2G| 4G| 4Gthen3Gthen2G| 4Gthen3G}] [flow-control {enable | disable}]

- show
- refresh

- network {show}
- Connection {show}
- enable
- disable
- show

Cellular Commands Description

Command	Description
Cellular	Enter the configuration mode for the Cellular application Enable: enable application Disable: disable application
continuous-echo	Configure icmp traffic test to validate network connectivity to a remote host. The test sets optionally 2 triggers to be used by the application watch dog : round trip delay and percentage of lost icmp messages sent. A test is determined by a configurable number of icmp request following which the average of rrt is calculated. A sufficient trigger to a watchdog is one of these 2 conditions to be met.
Create | update	name : name of the test (text) dest-ip-address : ip address of a reachable (routable) host. Format aa.bb.cc.dd rtt-threshold : round trip threshold in msec. <1,000-20,000> loss-threshold : calculated percentage of icmp requests which were not responded. <10-99> interval : time interval in seconds between icmp messages sent. <1-1440>. num-of-requests : number of icmp messages to send before calculating results of losses and rrd. <1-100>. request-size : icmp message packet size
remove	name : name of the test (text)
Show-config	Show configuration
Show-status	Show result of loss % and calculated round trip delay
Modem	Power-up : power the modem Power-down : shut the modem Send command at+cgsn : retrieve the IMEI identifier of the modem The modem must be enabled for these commands to take effect. get : retrieve the identifiers of the modem. iccid| imei| model| version

Command	Description
Settings update	quality check: define time interval in seconds for internal RSSI check of active SIM.<0-604800>. 0 –disable RSSI check. backoff1 : minimum time to stay on a SIM after any fail over. < sec,10-600> backoff2 : minimum time to stay on a SIM if “caveat” flag is set. This flag is set in case if there was already fail over in last 2 hours. < sec,10-600> wait-to-restore : maximum time allowed to stay on non-preferred SIM. default-route: setting the cellular interface to be the default gateway for the application IP interfaces. {yes | no} lcp-echo-interval : lcp protocol test of connectivity towards the connected ISP. 1 to 600 seconds interval between tests.0 –disable. lcp-failure : number of failed lcp echo tests. <1-64> update retry-threshold-reload <0-30> : sets a router reload after a configurable number of failed attempts to establish “Connected” status of the cellular modem. Configuration which was not committed will not be saved after the reload.
Settings show	Show: show configured interval time.
Wan update	Sim-slot: location of SIM to be configured, 1 or 2. Admin-status: enable/disable SIM card. Apn-name: as given by the network provider. operator-name : operator name (text) Pin: as given by the network provider. User-name: as given by the network provider. password: as given by the network provider. Flow-control : enable | disable. radio-access-technology : preferred network to connect to. Auto – if 3G available it will be chosen over 2G. 3G – only 3G will be optional to connect to. 2G - only 2G will be optional to connect to. 2Gthen3G – 2G is preferred over 3G. 3Gthen2G - 3G is preferred over 2G. 4G – only 4G will be optional to connect to 4Gthen3Gthen2G –4G will be the preferred optional to connect. Fallback to 3G/2G is allowed. 4Gthen3 –4G will be the preferred optional to connect. Fallback to 3G is allowed.
Wan Show	Show configuration and status of SIM cards
Network show	Show connection time and RSSI per SIM card
Connection show	Show cellular connection status

Default State

The default state of the cellular modem is “disabled”. The settings default state is as shown in below table.

```
[cellular/] settings show
+------------+-----------+---------+----------+----------+----------+----------+---------+-----------+-----------+
|  quality   |    dBm    | default | LCP echo | LCP echo | Backoff1 | Backoff2 | Wait to | Preferred |   Retry   |
| check(sec) | threshold |  route  | interval | failure  |  timer   |  timer   | restore |    SIM    | threshold |
|            |           |         |          |          |          |          |         |           |  reload   |
+============+===========+=========+==========+==========+==========+==========+=========+===========+===========+
|     0      |   -100    |   Yes   |    10    |    4     |    60    |   300    |  14400  |   none    |     0     |
+------------+-----------+---------+----------+----------+----------+----------+---------+-----------+-----------+
```

LED States

The modem has a led indicator for each SIM slot to represent the SIM cad state.

Modem admin state	SIM admin state	SIM Operation state	LED
disable	N/A	N/A	OFF
enable			
	disable	N/A	OFF
	enable	Ready	ON
	enable	not present	Blink 1 Hz
	enable	Failed	Blink 1 Hz
	enable	PIN lock	Blink 1 Hz
	enable	PUK lock	Blink 1 Hz
	enable	connecting	ON
	enable	connected	ON
	enable	connected - secondary	ON
	enable	connected - alternative	ON
	enable	Connected and traffic	ON

Example for retrieving the IMEI

Below is an example of retrieving the IMEI identifier of the modem.

```
RL1000GW#
cellular disable
cellular modem power-up
Completed OK
cellular modem send command at+cgsn
send : at+cgsn
reply : +cgsn
357524040483438
OK
```

Example for Sim Status

Below is a configuration example of 2 SIM cards and their permissible state status.

```
cellular wan update admin-status enable apn-name internetg sim-slot 1 operator-name
cellcom user-name guest password guest


cellular wan update admin-status enable apn-name internet.pelephone.net.il sim-slot 2
operator-name pelephone user-name pcl@3g password pcl


cellular enable

commit

cellular refresh
```

```
[/] cellular network show
+------+---------+-------------+---------+----------+---------+--------+-------------+-------------+
| slot | oper    | Last        | Changes | Failures | Last    | Caveat | RSSI        | Last RSSI   |
|      | status  | update(sec) |         |          | Failure |        | [dBm]       | check(sec)  |
+======+=========+=============+=========+==========+=========+========+=============+=============+
| 1    | UNKNOWN |      16     |    7    |    0     |   N/A   |   No   |     -67     |     23      |
+------+---------+-------------+---------+----------+---------+--------+-------------+-------------+
| 2    | UNKNOWN |      16     |    4    |    0     |   N/A   |   No   | not measured |     N/A     |
+------+---------+-------------+---------+----------+---------+--------+-------------+-------------+

[/] cellular network show
+------+---------+-------------+---------+----------+---------+--------+-------------+-------------+
| slot | oper    | Last        | Changes | Failures | Last    | Caveat | RSSI        | Last RSSI   |
|      | status  | update(sec) |         |          | Failure |        | [dBm]       | check(sec)  |
+======+=========+=============+=========+==========+=========+========+=============+=============+
| 1    | READY   |      9      |    8    |    0     |   N/A   |   No   |     -67     |      1      |
+------+---------+-------------+---------+----------+---------+--------+-------------+-------------+
| 2    | UNKNOWN |      21     |    4    |    0     |   N/A   |   No   | not measured |     N/A     |
+------+---------+-------------+---------+----------+---------+--------+-------------+-------------+

[/] cellular network show
+------+---------+-------------+---------+----------+---------+--------+------+-------------+
| slot | oper    | Last        | Changes | Failures | Last    | Caveat | RSSI | Last RSSI   |
|      | status  | update(sec) |         |          | Failure |        | [dBm]| check(sec)  |
+======+=========+=============+=========+==========+=========+========+======+=============+
| 1    | READY   |      38     |    8    |    0     |   N/A   |   No   | -67  |      30     |
+------+---------+-------------+---------+----------+---------+--------+------+-------------+
| 2    | READY   |      15     |    5    |    0     |   N/A   |   No   | -79  |      10     |
+------+---------+-------------+---------+----------+---------+--------+------+-------------+

[/] cellular network show
+------+--------------+-------------+---------+----------+---------+--------+------+-------------+
| slot | oper         | Last        | Changes | Failures | Last    | Caveat | RSSI | Last RSSI   |
|      | status       | update(sec) |         |          | Failure |        | [dBm]| check(sec)  |
+======+==============+=============+=========+==========+=========+========+======+=============+
| 1    | CONNECTING...|      1      |    9    |    0     |   N/A   |   No   | -67  |      31     |
+------+--------------+-------------+---------+----------+---------+--------+------+-------------+
| 2    | READY        |      16     |    5    |    0     |   N/A   |   No   | -79  |      12     |
+------+--------------+-------------+---------+----------+---------+--------+------+-------------+

[/] cellular network show
+------+------------+-------------+---------+----------+---------+--------+------+-------------+
| slot | oper       | Last        | Changes | Failures | Last    | Caveat | RSSI | Last RSSI   |
|      | status     | update(sec) |         |          | Failure |        | [dBm]| check(sec)  |
+======+============+=============+=========+==========+=========+========+======+=============+
| 1    | CONNECTED! |      96     |    10   |    0     |   N/A   |   No   | -67  |     132     |
+------+------------+-------------+---------+----------+---------+--------+------+-------------+
| 2    | READY      |     117     |    5    |    0     |   N/A   |   No   | -79  |     113     |
+------+------------+-------------+---------+----------+---------+--------+------+-------------+

[/] cellular connection show
+-----------+----------------+---------+---------+---------+---------+
| interface | local ip       | tx      | tx      | rx      | rx      |
|           |                | packet  | error   | packets | error   |
+===========+================+=========+=========+=========+=========+
| ppp0      | 46.210.197.173 |    6    |    0    |    5    |    0    |
+-----------+----------------+---------+---------+---------+---------+
```

Discrete IO Channels

Discrete channel interface

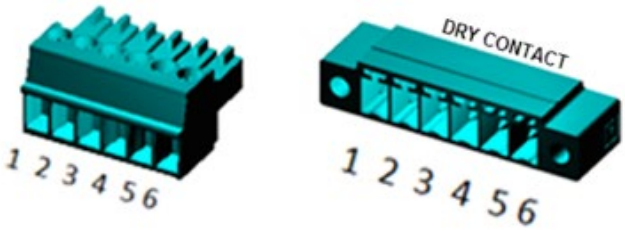
Discrete signals are very common in industrial application to monitor alarms and indications from the field side.

The status of the digital input can be read so the operator can decide if any action is required.

Digital output channels are not supported at current version.

Connection terminal are as shown in below figure.

1. Digital output 1
2. Digital output 2
3. Digital output ground
4. Digital Input ground
5. Digital Input 2 (6-12vDC)
6. Digital Input 1 (6-12vDC)



Technical data

At digital Inputs please connect a DC source in the range 6-12v at terminals 6,4 for channel 1 or 5,4 for channel 2.

Digital outputs are dry mechanical relay contacts. Maximum power to be implemented at the contacts:

AC: Max 250v, 37.5vA.

DC: Max 220v, 30 watt.

Above mentioned power limitations should not be exceeded.

Maximum current allowed at the contacts is 1A.

Discrete IO Channels Commands Hierarchy

+ root

    + discrete in

        - no-shutdown

        - shutdown

        - set name <>

        - clear

        - show

Discrete IO Channels Commands

Command	Description
Discrete in	Shutdown: disable the input channels no-shutdown: enable the input channels
Set name	Set a name to describe each channel
clear	Clear the name configuration back to defaults names 'Discrete-in1', 'Discrete-in2'.
Show	Display the channels state. 'HIGH', 'LOW'. Default: HIGH.

VPN Setup Examples

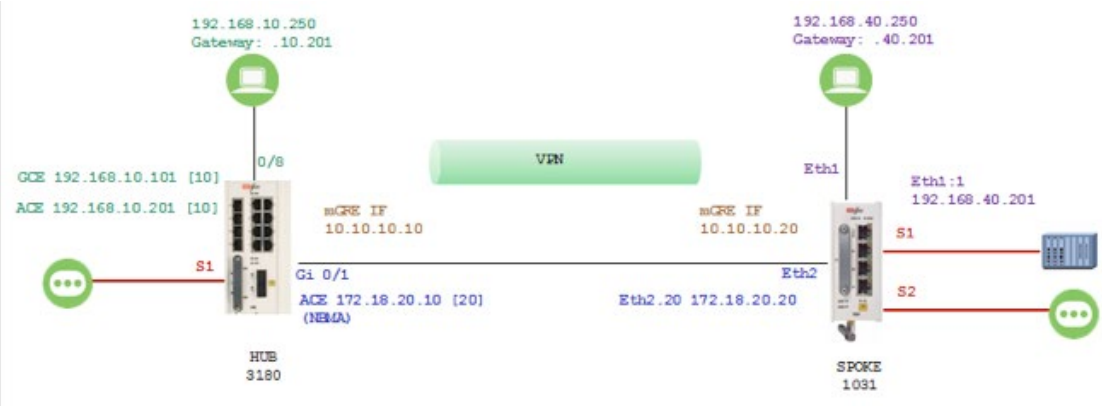
DM-VPN Setup

Below network demonstrates a Spoke – Hub networking over a fixed connection topology.

Implementation concepts:

1. The spoke and Hub will establish connection over the shared link. At below examples see vlan 20, subnet 172.18.20.x.
2. Both will be set with a common mGRE tunnel each holding an mGRE interfaces. See 10.10.10.x interfaces
3. The Spoke will set with NHRP configuration, pointing towards the Hub.
4. IPSec configuration will be set for both to encrypt all traffic.
5. Local IP interfaces will be set at both, to route the user equipment (private subnets) over the mGRE.

Network drawing



HUB (RLGE2FE16R)

1. Set router host name (not mandatory)

```
set host-name hub
```

2. Disable spanning tree and remove the ports to be used in the VPN from default vlan 1

```
config terminal
no spanning-tree

vlan 1
no ports fastethernet 0/1,0/8 gigabitethernet 0/3 untagged fastethernet 0/1,0/8
exit
```

3. Assign the user and network vlans and set PVID for the untagged ports

```
vlan 10
 ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
 exit

 vlan 20
 ports fastethernet 0/8  gigabitethernet 0/3 untagged fastethernet 0/8
 exit

 interface fastethernet 0/1
 alias UNI
 switchport pvid 10
 exit
```

```
interface fastethernet 0/8
alias NNI
switchport pvid 20
exit
```

4. Assign GCE IP interface for management (not mandatory)

```
interface vlan 10
shut
ip address 192.168.10.101 255.255.255.0
no shut
exit
```

5. Assign static route so router management will be routable over the VPN

```
ip route 0.0.0.0 0.0.0.0 192.168.10.201 1
end
commit
```

6. Assign ACE IP interface which will route user traffic

```
application connect

router interface create address-prefix 192.168.10.201/24  vlan 10 purpose general
```

7. Assign ACE IP interface for networking towards the WAN router

```
router interface create address-prefix 172.18.20.10/24 vlan 20 purpose application-host
```

8. Assign the GRE tunnel

```
vpn gre tunnel create address-prefix 10.10.10.10/24 lower-layer-dev eth1.20 name mgre1 key
10.0.0.0
vpn gre nhrp disable
vpn gre nhrp enable
```

9. Assign routes for the remote user network

```
router static
Enable
configure terminal
```

```
ip route 192.168.40.0/24 10.10.10.20
write
exit
exit
```

10. Configure IPSec

```
ipsec isakmp update my-id HUB.radiflow.com
ipsec preshared create id HUB.radiflow.com key secretkey
ipsec preshared create id RTU1.radiflow.com key secretkey
ipsec isakmp update  id-type fqdn
ipsec policy create protocol gre
ipsec disable
ipsec enable
exit
write startup-cfg
```

SPOKE (RL1000GW)

1. Assign IP interface to route user traffic

```
router interface create address-prefix 192.168.40.201/24 physical-interface eth1 description
UNI purpose general admin-status enable
```

2. Assign IP interface towards the WAN router

```
router interface create address-prefix 172.18.20.20/24 vlan 20 physical-interface eth2
description NNI purpose application-host admin-status enable
```

3. Assign the local GRE tunnel and the NHRP addressing towards the Hub

```
vpn gre tunnel create address-prefix 10.10.10.20/24 lower-layer-dev eth2.20 name mgre1 key
10.0.0.0 admin-status enable


vpn gre nhrp map create multipoint-gre-name mgre1 protocol-address-prefix 10.10.10.10/24
nbma-address 172.18.20.10


vpn gre nhrp disable
vpn gre nhrp enable
```

4. Assign routes for the remote user network

```
router static
Enable
configure terminal
ip route 192.168.10.0/24 10.10.10.10
write
exit
exit
```

5. Configure IPSec

```
ipsec isakmp update my-id RTU1.radiflow.com
ipsec preshared create id HUB.radiflow.com key secretkey
ipsec preshared create id RTU1.radiflow.com key secretkey
ipsec isakmp update  id-type fqdn
ipsec policy create protocol gre
ipsec disable
ipsec enable
commit
```

Test

Ping is now possible between :

» The application IPs : 172.18.20.10 and 172.18.30.20
» The router interfaces : 192.168.10.201 and 192.168.40.201
» The PCs : 192.168.10.250 and 192.168.40.250

DM-VPN over Cellular Setup

Below network demonstrates a Spoke – Hub topology.

Implementation concepts:

1. The spoke will retrieve via PPP an IP from the cellular ISP.
   In below example the valid IP 46.210.228.96 was issued to the Spoke from the ISP "Cellcom".
2. At the Hub side, a static, public address should be assigned to the router interface.
   In below example the hub is located behind a NAT router. The NAT, holding a public address 80.74.102.38 should route all traffic designated to it to the ACE interface of the hub 172.18.212.230.
3. At the Hub, ip interface 192.168.10.10 is created and is called ETH1.10. This interface will route the user IP and serial user traffic towards the network.
   IP interface 192.168.212.230 (ETH1.20) is as well created, as the interface to the cloud via the NAT router.
4. As the hub is located behind a NAT router, a default gateway should be assigned at the ACE interface (172.18.212.100).
5. As this is layer 3 service, the users behind the spoke and hub are in different vlans and different subnets.
6. At the Spoke, ip interface 192.168.40.10 is created and is called ETH1:1. This interface will route the IP and serial user traffic towards the network.
7. At both the spokes and the hub, private ip interfaces for the tunnel end point will be created.
   See interfaces of 10.10.10.x in below example
8. IPSec must be configured to ensure secure traffic and proper NAT traversal.
9. Ip connectivity is established between the user stations (SCADA & PC) 192.168.10.11 and 192.168.40.11.
10. At the second part of the example a terminal server service is configured between 192.168.10.11 and the serial device connected at RS-232 port 1 of the spoke.
11. At the third part of the example a transparent serial tunneling service is configured between the SCADA (connected via its com port to the router RS-232 port 1 at the hub) and the serial device connected at the spoke (RS-232 port 2).

Network drawing

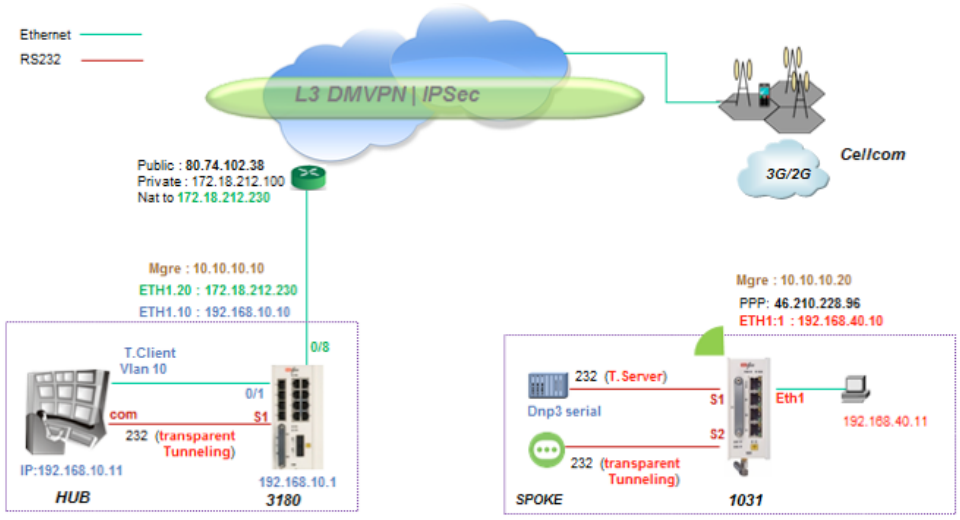


Figure 12 : L3 VPN, cellular spoke - RL1000GW hub

Configuration

Spoke (RL1000GW)

1. Create an interface to route the lan traffic coming at port eth1

```
RL1000GW# router interface create address-prefix 192.168.40.10/24 physical-interface eth1
description UNI purpose application-host admin-status enable
```

2. Setting the cellular modem

```
cellular settings update default-route yes
```

3. Wan update menu ,SIM card configuration –slot 1

```
cellular wan update sim-slot 1 admin-status enable operator-name cellcom apn-name
internetg user-name guest password guest
cellular enable
commit
```

4. Create an mgre private interface for tunnel end. This interface will use the PPP of the cellular as its lower layer.

```
vpn gre tunnel create address-prefix 10.10.10.20/24 lower-layer-dev ppp0 name mgre1 key
10.0.0.0 admin-status enable
```

5. Describe the tunnel remote end private interface behind the hub public address.

```
vpn gre nhrp map create multipoint-gre-name mgre1 protocol-address-prefix 10.10.10.10/24
nbma-address 80.74.102.38
```

6. Describe the tunnel remote end private interface behind the hub public address.

```
vpn gre nhrp disable
vpn gre nhrp enable
commit
```

7. assign static route to the remote user subnet behind the hub via the tunnel remote end

```
router static
enable
configure terminal
ip route 192.168.10.0/24 10.10.10.10
write memory
exit
exit
commit
```

8. IPSec configuration

```
RL1000GW#
ipsec isakmp update my-id RTU1.radiflow.com
ipsec preshared create id HUB.radiflow.com key secretkey
ipsec preshared create id RTU1.radiflow.com key secretkey
ipsec isakmp update id-type fqdn
ipsec policy create protocol gre
ipsec enable
commit
```

Hub (RLGE2FE16R)

1. Create vlan UNI 10 to direct traffic from the PC to the application.

```
port  gigabitethernet 0/3  must be a tagged member at this vlan.
Interface 192.168.10.1 will allow management to the router over this vlan via the tunnel.
vlan 20 will be towards the router.
Set hostname hub
config
```

```
vlan 10
 ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
 exit

 vlan 20
 ports fastethernet 0/8  gigabitethernet 0/3 untagged fastethernet 0/8
 exit

 interface fastethernet 0/1
 alias UNI
 routerport pvid 10
 exit

 interface fastethernet 0/8
 alias NNI
 routerport pvid 20
 exit

 interface vlan 10
ip address 192.168.10.1 255.255.255.0
 no shut

 exit
  ip route 0.0.0.0 0.0.0.0 192.168.10.10 1
   end
```

2. Create an IP interface ETH.20 in the subnet of the router

```
router interface create address-prefix 172.18.212.230/24 vlan 20 purpose application-host
```

3. Create an ip interface ETH.10 to route user subnet 192.168.10.x/24

```
router interface create address-prefix 192.168.10.10/24 vlan 10 purpose general
```

4. Create an mgre private interface for tunnel end. This interface will use the interface ETH.20 of towards the router as its lower layer.

```
dm-vpn multipoint-gre create address-prefix 10.10.10.10/24 lower-layer-dev eth1.20 name
mgre1 key 10.0.0.0 holding-time 120
```

5. Enable nhrp

```
dm-vpn nhrp enable
```

6. assign static route to the remote user subnet 192.168.40.x behind the spoke via the tunnel remote end 10.10.10.20

```
router static
enable
configure terminal
ip route 192.168.40.0/24 10.10.10.20
ip route 0.0.0.0/0  172.18.212.100
write
exit
exit
```

7. IPSec configuration

```
RL1000GW#application connect
ipsec isakmp update my-id HUB.radiflow.com
ipsec preshared create id HUB.radiflow.com key secretkey
ipsec preshared create id RTU1.radiflow.com key secretkey
ipsec isakmp update id-type fqdn
ipsec policy create protocol gre
ipsec enable

commit
exit
write startup-cfg
```

Testing the setup

1. Use show commands to check configuration

a. Spoke

```
RL1000GW#
 router interface show
 cellular show
 cellular wan show
 cellular Connection show
 ipsec show
```

b. Hub

```
RLGE2FE16R(hub)#Show vlan
[]router interface show
```

2. Make sure both the IP of the hub and the one of the spoke are each accessible from the internet.
   using a PC connected to the internet send ping commands.
   ping 'public ip of the spoke'.
   ping 80.74.102.38.

3. Send traffic between the 2 PCs.

4.

5. Show example at the spoke

6.

```
RL1000GW#router interface show
+----+------+--------+-----------------+------+-----------------+-------------+------------
-+
| Id | VLAN |  Name  |     IP/Subnet      | Mtu  |      Purpose       | Admin status |
Description |
+====+======+========+=================+======+=================+=============+======
=======+
| 1  | N/A  | eth1:1 | 192.168.40.10/24 | 1500 | application host |     enable     |      UNI
|
+----+------+--------+-----------------+------+-----------------+-------------+------------
-+



RL1000GW#router route show
```

```
Kernel IP routing table
Destination     Gateway         Genmask          Flags Metric Ref    Use Iface
0.0.0.0         0.0.0.0         0.0.0.0          U     0      0        0 ppp0
10.10.10.0      0.0.0.0         255.255.255.0    U     0      0        0 mgre1
192.168.10.0    10.10.10.10     255.255.255.0    UG    0      0        0 mgre1
192.168.40.0    0.0.0.0         255.255.255.0    U     0      0        0 eth1
Completed OK


 RL1000GW#cellular connection show
+-----------+---------------+---------+--------+----------+--------+
| interface |   local ip    |   tx    |   tx   |    rx    |   rx   |
|           |               |  packet |  error |  packets |  error |
+===========+===============+=========+========+==========+========+
|   ppp0    | 46.210.228.96 |   563   |   0    |   413    |   0    |
+-----------+---------------+---------+--------+----------+--------+

RL1000GW#vpn gre nhrp map show-status
+--------+---------------+---------+--------+-----------+
| Tunnel |    Protocol   | Changes |  Oper  |   Last    |
|  Name  | address/prefix |         | Status |  change   |
|        |                |         |        | (sec.ago) |
+========+===============+=========+========+===========+
| mgre1  | 10.10.10.10/24 |    1    |   up   |   1151    |
+--------+---------------+---------+--------+-----------+


RL1000GW#ipsec show sa
46.210.228.96[4500] 80.74.102.38[4500]
        esp-udp mode=transport spi=65028829(0x03e042dd) reqid=0(0x00000000)
        E: 3des-cbc  212f6143 2987525a 927faec1 f962d02c 8b88d194 8112df9d
        A: hmac-md5  b9aaf05a 660ba29b b40a97d4 7f90d6c2
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May 18 13:09:36 2014   current: May 18 13:29:15 2014
        diff: 1179(s)   hard: 86400(s)  soft: 69120(s)
        last: May 18 13:09:41 2014      hard: 0(s)      soft: 0(s)
        current: 5992(bytes)    hard: 0(bytes)  soft: 0(bytes)
        allocated: 102  hard: 0 soft: 0
        sadb _ seq=1 pid=5265 refcnt=0
80.74.102.38[4500] 46.210.228.96[4500]
```

```
        esp-udp mode=transport spi=27166054(0x019e8566) reqid=0(0x00000000)
        E: 3des-cbc  7b9bb5bb e8e16e18 d48af2f6 cd22aab5 d357dc07 cdf0c300
        A: hmac-md5  16bc188c 6f7b7f9f 54025146 8963f9c8
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May 18 13:09:36 2014   current: May 18 13:29:15 2014
        diff: 1179(s)   hard: 86400(s)  soft: 69120(s)
        last: May 18 13:09:47 2014      hard: 0(s)      soft: 0(s)
        current: 1852(bytes)    hard: 0(bytes)  soft: 0(bytes)
        allocated: 27   hard: 0 soft: 0
        sadb _ seq=2 pid=5265 refcnt=0
46.210.228.96[4500] 80.74.102.38[4500]
        esp-udp mode=transport spi=107710234(0x066b871a) reqid=0(0x00000000)
        E: 3des-cbc  e106edb4 40103b21 95609c4a 2dcedbe5 4ac0a5d2 b6762651
        A: hmac-md5  5719c1c7 a42a25b5 b9a3bb2a d391f8da
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May 18 13:09:36 2014   current: May 18 13:29:15 2014
        diff: 1179(s)   hard: 86400(s)  soft: 69120(s)
        last: May 18 13:09:36 2014      hard: 0(s)      soft: 0(s)
        current: 100(bytes)     hard: 0(bytes)  soft: 0(bytes)
        allocated: 1    hard: 0 soft: 0
        sadb _ seq=3 pid=5265 refcnt=0
80.74.102.38[4500] 46.210.228.96[4500]
        esp-udp mode=transport spi=198284673(0x0bd19581) reqid=0(0x00000000)
        E: 3des-cbc  ac3c6e35 d9491440 3927ca04 3f7b0a57 85c67056 7b32139f
        A: hmac-md5  73e6d7f3 7876038a 0a3cad0a 08549e61
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May 18 13:09:36 2014   current: May 18 13:29:15 2014
        diff: 1179(s)   hard: 86400(s)  soft: 69120(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)       hard: 0(bytes)  soft: 0(bytes)
        allocated: 0    hard: 0 soft: 0
        sadb _ seq=0 pid=5265 refcnt=0
RL1000GW#
```

Adding a terminal server service

Spoke :

1. Create the serial port

```
serial port create port 1 baudrate 9600 parity no databits 8 mode-of-operation
transparent


serial local-end-point create port 1 service-id  1 application terminal-server


commit
```

2. Create the terminal server service

```
terminal-server admin-status enable


terminal-server tcp-service create service-id 1 remote-address 192.168.40.10 telnet-port
2050


commit
```

Testing the setup:

1. From the hub station 192.168.10.11 ping to the remote application interface 192.168.40.10.

2. Open a telnet session towards address 192.168.40.10 with port 2050.

3. The serial port will respond

Adding a transparent serial tunneling service

Hub :

1. Create the serial port and transparent serial tunneling service

```
application connect
serial port create slot 1 port 1 mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 2 application serial-tunnel
position master
serial remote-end-point create remote-address 192.168.40.10 service-id 2 position slave
exit
write startup-cfg
```

Spoke :

1. Create the serial port and transparent serial tunneling service

```
serial port create port 2 mode-of-operation transparent
serial local-end-point create port 2 service-id 2 application serial-tunnel position slave
serial remote-end-point create remote-address 192.168.10.10 service-id 2 position master
commit
```

Testing the setup:

1. From the SCADA send serial traffic over its COM port.

2. The remote serial device at the spoke will respond

Application Aware Firewall

The integrated SCADA protocol firewall provides a network-based distributed security.

The firewall implemented is “application-aware”, meaning that it inspects the contents of the data packets of selected SCADA protocols according to the rules set by the user.

Using the firewall, the router becomes distributed Intrusion Prevention System (IPS) realizing detailed service-aware inspection.

» Supported protocols: Modbus TCP, IEC 104, DNP3

The service-aware firewall checks each packet in details including:

» Protocol validity – Check that the packet structure and all its control fields comply with the standard and that the session flow follows the expected logic (i.e. session initiated by master, response matches request, session setup sequence, etc.).

» Application logic – Per each pair of source and destination devices verify that only the allowed communication is performed by checking the function code and the command parameters according to the operator defined values.

Firewall Service flow

In order for a protocol flow to be inspected by the firewall the following is achieved by the ComNet NMS- iSIM.

» A designated service vlan is created and the ports are tagged.

» ACLs are placed on the relevant access port and network ports to redirect the traffic flow to service vlan and to the firewall process. The ACLs will allow traffic between service members only. ACLs will permit traffic only of the TCP/UDP type correlating to the service protocol determined by the user. Other ports are blocked by default.

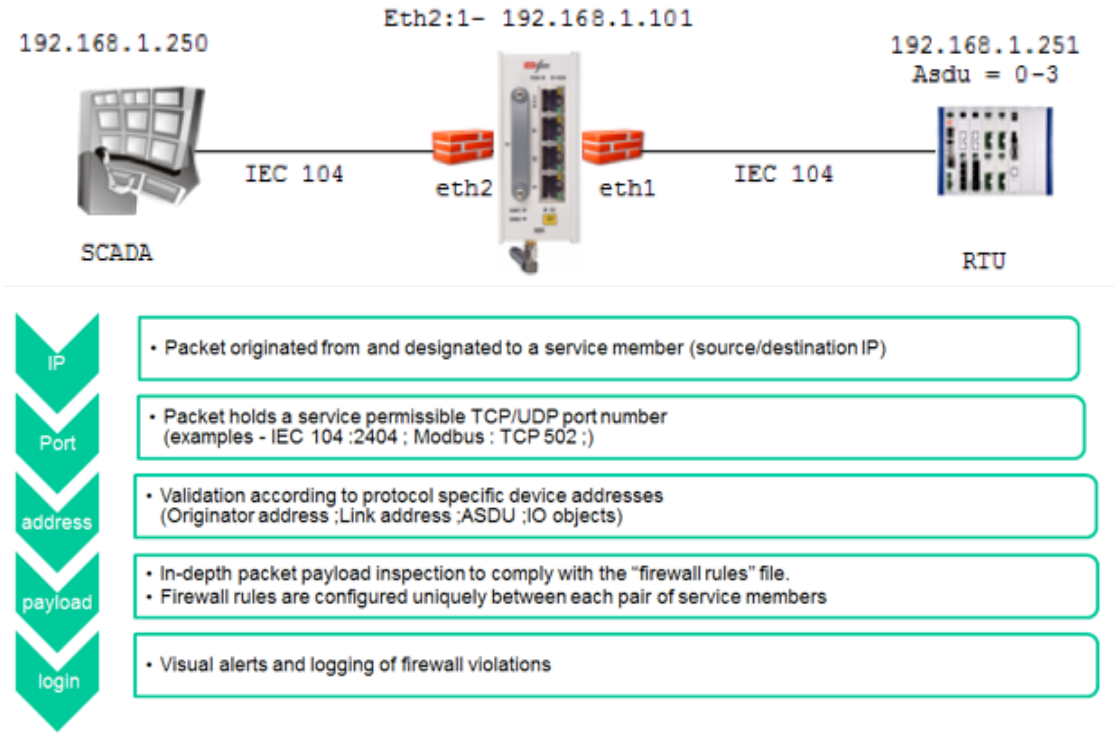
» The ACLs as well validate the packet direction and block messages in violation of proper session.

» A file holding a list of allowed messages is created upon user configuration and is downloaded to the router. The file holds specific addressing properties of the target device under the relevant SCADA protocol (for example Common Address of ASDU in IEC104) and so the packet inspection is done not only at the IP header but as well in the payload itself.

» Service packets will be inspected towards this file.

» A packet originated and designated to a service member will be directed to the firewall process for in depth inspection of the payload before allowed to pass to the network.

Firewall Flow Illustration



Supported Hardware

All RL1000GW variants support the firewall as an option

Configuration

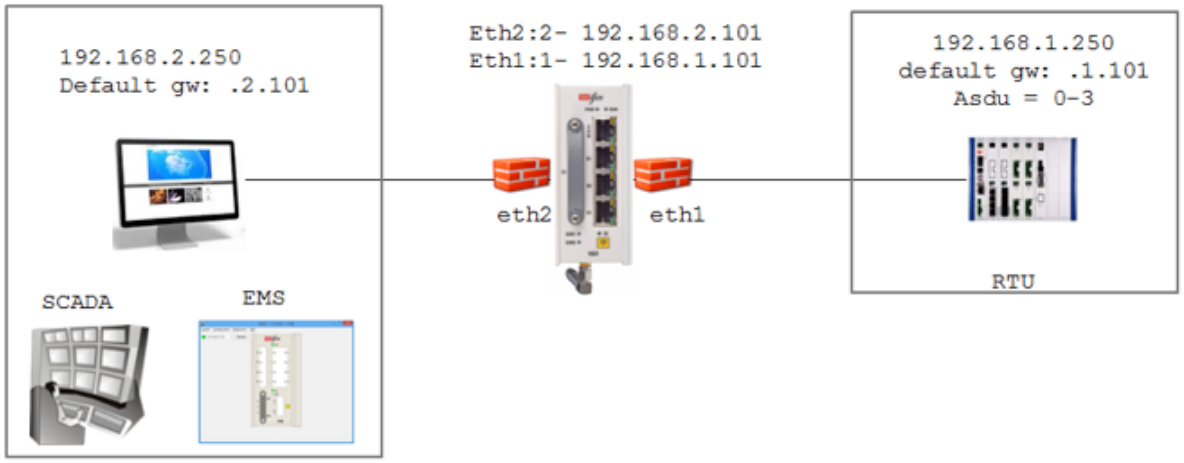
The firewall configuration consists of two parts

1. Access lists at the ports, filtering L3-L4 traffic and directing the designated SCADA service to the firewall DPI process.
   This step can be achieved both in CLI and via the iEMS.

2. Firewall DPI rules.
   This step can be achieved only via the iEMS.

Example

Below is an example of an IEC 104 firewall setup.



1. Create IP interfaces for routing and management

```
RL1000GW# router interface create address-prefix 192.168.1.101/24 physical-interface eth1
Completed OK
RL1000GW# router interface create address-prefix 192.168.2.101/24 physical-interface eth2
Completed OK
RL1000GW#
```

2. Set ACL designated for port eth2 to direct SCADA IEC 104 traffic to the firewall

```
RL1000GW# ip access-list extended
RL1000GW# ip/access-list/extended/create acl-num 1101 acl-name SCADA redirect fw
RL1000GW# ip/access-list/extended/permit tcp  acl-num 1101 rule-name fw1 priority 11 src-ip
192.168.2.250/32 dst-ip 192.168.1.250/32
completed ok (rule #1)
```

3. Set ACL designated for port eth2 to direct SCADA IEC 104 traffic to the firewall

```
RL1000GW# ip/access-list/extended/create acl-num 1102 acl-name RTU redirect fw
RL1000GW# ip/access-list/extended/permit tcp  acl-num 1102 rule-name RTU priority 12 src-ip
192.168.1.250/32 dst-ip 192.168.2.250/32
completed ok (rule #2)
RL1000GW#ip/access-list/extended/..
RL1000GW#ip/access-list/..
RL1000GW#ip/..
RL1000GW#
```

4. Assign the ACLs to the corresponding ports

```
RL1000GW#ip access-group apply acl-num 1101 interface eth2 direction in priority 10
completed ok
RL1000GW#ip access-group apply acl-num 1102 interface eth1 direction in priority 10
completed ok
```

5. Create the firewall.rules file

```
Done only with EMS
```

6. Download and activate the firewall.rules file

```
firewall profile import tftp remote-host 192.168.2.250 filename firewall.rules
firewall tcp activate mode enabled
commit
```

Firewall Commands Hierarchy

+ root
    + firewall
        + profile
            - show
            - import tftp {[filename <>] | [remote-host <ip>]}
        - log {show [lines-to-show(1000,<>)] |clear}
        + tcp
            - show
            - counters {show| clear}
            - activate mode {disabled | enabled | simulate}

Firewall Commands

Command	Description
firewall	Enter the configuration mode for the Cellular application Enable: enable application Disable: disable application
Profile show	Display the content of the firewall.rules file Log show show : Display the firewall log clear : clears the log
Tcp	Show : status of the firewall is displayed
Tcp activate mode	Disabled : firewall is disabled. Packets are not inspected. Enabled : packets are inspected and blocked in case of violation. Violations are logged. Simulate : packets are inspected but are not blocked in case of violations. Violations are logged.
Create | update	name : name of the test (text) dest-ip-address : ip address of a reachable (routable) host. Format aa.bb.cc.dd rtt-threshold : round trip threshold in msec. <1,000-20,000> loss-threshold : calculated percentage of icmp requests which were not responded. <10-99> interval : time interval in seconds between icmp messages sent. <1-1440>. num-of-requests : number of icmp messages to send before calculating results of losses and rrd. <1-100>. request-size : icmp message packet size

ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.
Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET