



PRODUCT DATA SHEET

## Rugged IP load generator (Ruge)

**RUGE**

**Ruge gives your network a serious beating. Just to make sure it does not fail when it is time to go live.**

## Introduction

Rugged IP load generator (Ruge) is a versatile test tool to run different stress tests and to ensure that your product or service meets the targeted limits – before it goes live and it's too late. Use Ruge for load testing, network optimisation and DDoS attack simulation by combining high data volumes with anomalous behaviour.

Ruge is based on an innovative software architecture and a powerful network processor hardware platform.

Ruge utilizes pre-recorded data streams, control messages and timestamps to reproduce realistic sessions. Furthermore, it is possible to build state machines to simulate interactive, stateful protocol behaviour against the system under test. For session multiplication, lower layer protocols (e.g. Ethernet, IP and UDP) can be redefined and populated with variables. It is also possible to add, for example, tunneling protocols for pre-recorded streams.

### Great performance and high accuracy

Ruge uses powerful network processing units (NPUs) and is optimised to handle IP packet traffic. Ruge hardware engine has up to 32 GB of memory.

Ruge is able to generate stateless load up to full line rate almost instantly. Millions of concurrent stateful sessions (e.g. SIP calls) up to full line rate (1/10 Gbps) can be started within a couple of seconds.

Ruge supports high load stress testing with extremely accurate time stamping where the theoretical line rate can be reached with any data type and their combinations.

Ruge offers repeatability accuracy up to microsecond level and exact repeatability in data content.

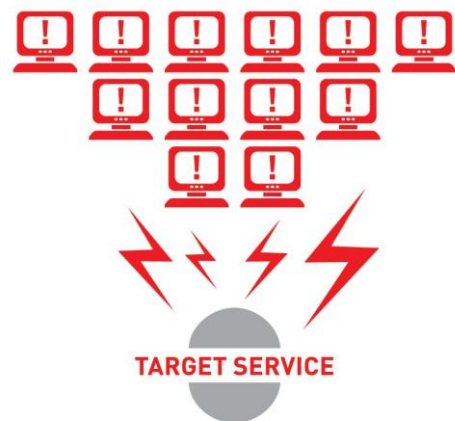
### Unique flexibility

Ruge engine SW controls network processors directly – there is no third-party operating system. Thus, product performance is not affected by a third-party operating system overhead.

This also means that no protocol stacks are dependent on any third-party implementation, but are fully controlled by Ruge. This offers a unique possibility to emulate non-standard behaviour even within lower layers such as Ethernet and internet protocol (IP).

Ruge supports any content type in stream generation since all data content is based on pre-recorded reference sessions. Anything that can be recorded, can be played back and multiplied. These reference sessions can be multiplied to represent a high number of different sources or users.

Example: When a new voice codec is supported by the equipment under test, it can be instantly supported by Ruge. Testing is based on a pre-recorded reference session and no voice codec implementation is needed in Ruge.



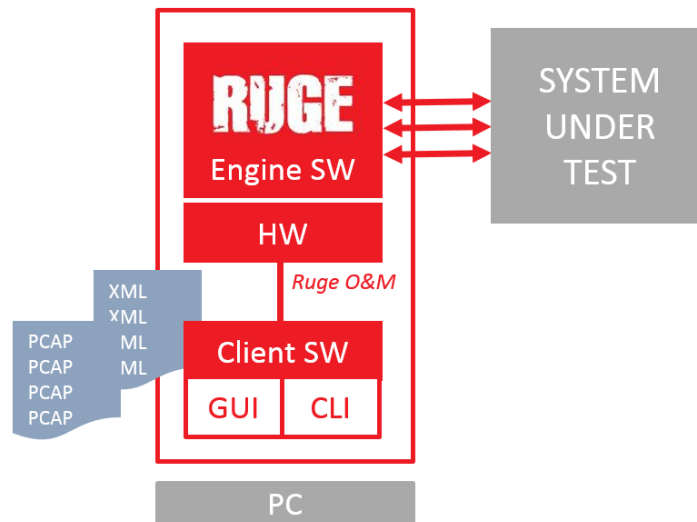
### Suitability for various use cases

Ruge is suitable for various use cases including

- Load testing of IP based network equipment or network services
- Simulation of cyber-attacks (DDoS)
- Security testing of gateways, firewalls and other network elements
- Negative testing with data generation beyond spec boundaries
- Simultaneous generation of various data types
- Multiplication of reference traces or self-created hex patterns

This product fact sheet is aligned with Ruge version 2.2.

## Product configuration



### Ruge hardware

Ruge engine SW runs on network processing units (NPU) which are optimised for IP packet processing. Co-processors perform all time critical actions, such as CRC calculation and ciphering.

The Ruge high-end platform supports 1 Gigabit Ethernet based interfaces with a RJ-45 copper connector.

### Ruge software

Ruge software consists of two parts: the engine SW running on the hardware platform and the client

software controlling the engine. The host application runs on Windows 7 and Linux. In addition to Ruge Graphical User Interface, Command Line Interface (CLI) is provided for testing automation.

### Ruge scripts

A script is a testing sequence which is built with Ruge GUI and saved to XML files. Testing consists of executing the scripts.

## Product features

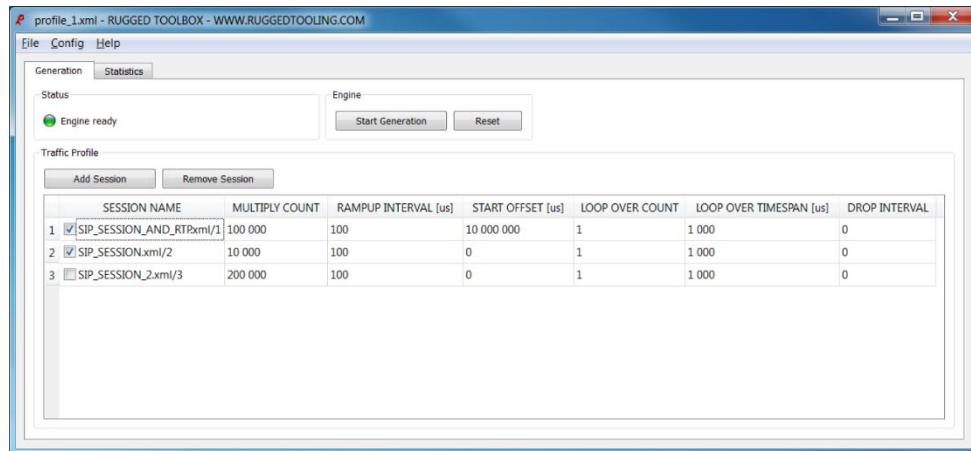


Figure 1. Main window of Ruge Graphical User Interface.

### Support for Rich Communication Service (RCS) load testing

Ruge supports load testing of RCS with the help of the following product features: stateful TCP, Transport Layer Security (TLS) and Message Session Relay Protocol (MSRP).

Ruge is capable of generating millions of concurrent RCS sessions by using pre-recorded data. Highly customizable traffic profiles are available, with combinations of various RCS related services.

The RCS load testing application supports testing of the following RCS features:

- Registration
- SIP options polling
- 1-to-1 chat sessions
- Group chat sessions (1-to-many chat)
- Image share
- Video share
- File transfer of any type and size of file
- VoIP calls

For more details, refer to the RCS load testing Application Note.

### Ruge scripts for general use

- SIP call generation

### Ruge scripts for Distributed Denial of Service (DDoS)

Ruge scripts cover the majority of the most common Distributed Denial of Service attacks including:

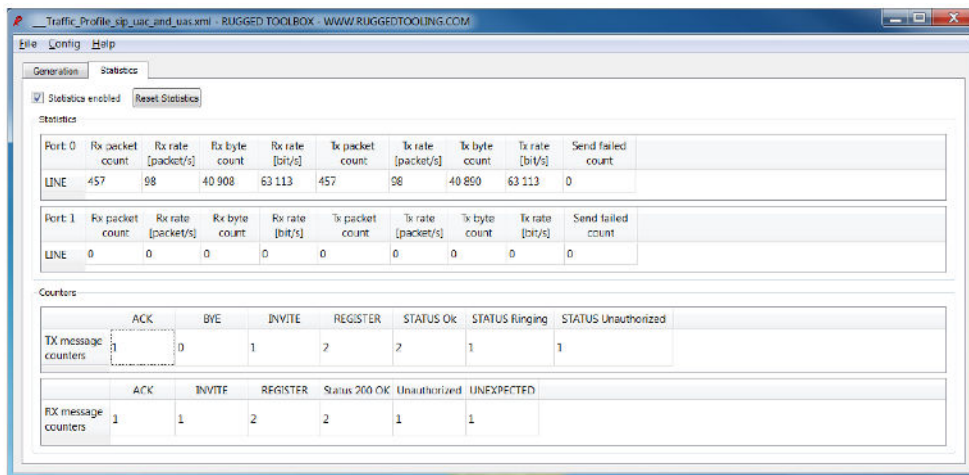
- IP Spoofing
- IP Malformed Packet
- Fragments Reassembly w/different offsets ("Tear Drop")
- Fragments Reassembly off by one IP header ("Nestea Attack")
- ICMP Oversized packet (> 65536) ("Ping of Death/SSPing Attack")
- ICMP Incomplete Fragment ("Jolt Attack")
- ICMP Flood
- ICMP spoofed unreachable flood ("Smack/Bloop/Puke Attack")
- TCP SYN Fragments - Reassembly with overlap ("Syndrop Attack")
- TCP Scan Attack – TCP Port
- SYN Attack w/IP Spoofing ("Land Attack")
- SYN Attack ("SYN Flood")
- UDP Short Header

## Product data sheet: Rugged IP load generator (Ruge)

- UDP Flood
- UDP spoofed broadcast echo ("Fraggle Attack")
- UDP attack on diag ports ("Pepsi Attack")
- RTP rogue packets (after-call)
- RTP flooding during call
- RTP flooding attack
- RTP spoofing
- ARP ARP Flood ("Poink Attack")
- RX/TX packet and byte counts
- RX/TX packet and bit rates
- Possible send failures caused by exceeding line capacity
- User given message counters for any generated message, 0-64 counters per message
- Receive message counters for stateful protocols (SIP and TCP).

## Statistics

Ruge displays various statistics of the test sessions in the graphical user interface. The statistics include:



Port 0	Rx packet count	Rx rate [packet/s]	Rx byte count	Rx rate [bit/s]	Tx packet count	Tx rate [packet/s]	Tx byte count	Tx rate [bit/s]	Send failed count
LINE	457	98	40 908	63 113	457	98	40 850	63 113	0

Port 1	Rx packet count	Rx rate [packet/s]	Rx byte count	Rx rate [bit/s]	Tx packet count	Tx rate [packet/s]	Tx byte count	Tx rate [bit/s]	Send failed count
LINE	0	0	0	0	0	0	0	0	0

Counters	ACK	BYE	INVITE	REGISTER	STATUS Ok	STATUS Ringing	STATUS Unauthorized
TX message counters	1	0	1	2	2	1	1

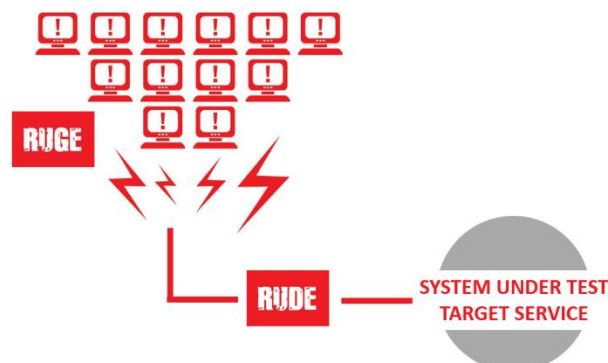
  

Counters	ACK	INVITE	REGISTER	Status 200 OK	Unauthorized	UNEXPECTED
RX message counters	1	1	2	2	1	1

Figure 2. Ruge statistics tab.

## Ruge combined with Rugged deviation emulator (Rude)

Ruge can be combined with Rugged deviation emulator (Rude), which enables integrating realistic IP network characteristics as a part of the test environment. Rude offers a possibility to modify heavy load packet streams by, for example, adding delay, jitter, packet reordering, packet corruptions and packet duplications, simulating the actual behaviour of real networks. With the combination of Ruge and Rude, real world scenarios can be simulated and tested even more reliably.



## Protocol stack support

### Stateless protocols

The supported protocols are presented in the following figures. Dynamically changeable fields, such as message length and CRC, are calculated automatically and dynamically for each protocol.

However, as explained earlier, any data content can be generated on the basis of a pre-recorded reference stream. It is also possible to include any protocol as user data or payload.

The supported stateless protocols are:

- Ethernet, VLAN

- IPv4, IPv6
- UDP, TCP, SCTP, GTPv1\_U, GRE, ICMP, ICMPv6
- RTP

USER DATA
ICMP / ICMPv6
IPv4 / IPv6
Ethernet_II / VLAN

Figure 3. Protocols supported in control messages.

USER DATA	USER DATA								
UDP	TCP					USER DATA	USER DATA		
Inner IPv4 / Inner IPv6						UDP	TCP		
GTPv1_U		USER DATA	USER DATA			Inner IPv4 / Inner IPv6			
UDP		TCP	SCTP			GRE			
IPv4 / IPv6									
Ethernet_II / VLAN									

Figure 4. Protocols supported in control messages.

PAYLOAD	PAYLOAD								
RTP	RTP					PAYLOAD	PAYLOAD		
UDP	TCP					RTP	RTP		
Inner IPv4 / Inner IPv6		PAYLOAD	PAYLOAD			UDP	TCP		
GTPv1_U		RTP	RTP			Inner IPv4 / Inner IPv6			
UDP		TCP				GRE			
IPv4 / IPv6									
ETHERNET / VLAN									

Figure 5. Protocols supported in streams.

### Stateful protocols

Stateful operation is supported for the following protocols:

- SIP over UDP
- TCP

SIP	
UDP	TCP
IPv4 / IPv6	
ETHERNET / VLAN	

Figure 6. Supported stateful protocols.

**Supported encryption mechanisms**

*TLS*

- AES CBC 128 bit
- Supported as stateful with both encryption and decryption. Negotiation of keys supported.

*IPsec*

- AES CTR 128/192/256 bit
- AES CBC 128/192/256 bit
- Supported as stateless, i.e. encryption is done

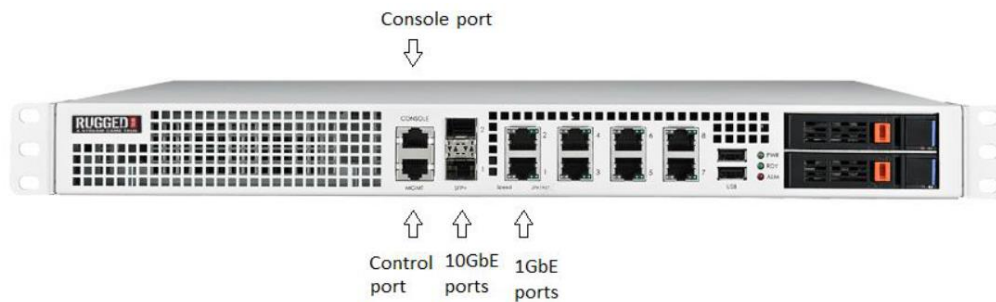
*NAS*

- AES CTR 128 bit
- Supported as stateless, i.e. encryption is done
- SNOW3G 128 bit

## Technical specifications



Processor & memory		Port capacity	
Processor	Cavium Octeon II NPU	Port capacity 1 GbE	1 ... 8
Number of Cores	32	Port capacity 10 GbE	1 ... 2
Internal Memory	32 GB		



Physical interfaces			
Interface	Capacity	Connector type	Usage
10 GbE ports	10 Gb	SFP+	Connection to System Under Test
1 GbE ports	1 Gb	RJ45	Connection to System Under Test
Control port	1 Gb	RJ45	Connection to host PC with GUI or CLI
Console port		RJ45	Additional control of the Ruge engine

Physical measures		Environment	
Mounting	1U rack mountable	Temperature range	0 ~ 40 °C / 32 ~ 104 F (operating) -20 ~ 70 °C / -4 ~ 158 F (storage)
Dimensions (W x H x D)	430 x 44 x 349 mm	Humidity	20% to 90% RH (operating) 5% to 95% RH (storage)
Weight	7.2 kg (unpacked) 11 kg (packed)		

Compliance	
EMC/Safety	CE/FCC/UL/CB/CCC

### Supported operating systems

Ruge host software is supported in the Windows 7 64-bit and Linux operating systems.

### Prerequisites

WinPCAP and Wireshark are required to operate the product.

A terminal program is required to change the engine IP address. Third-party applications such as PuTTY are recommended.

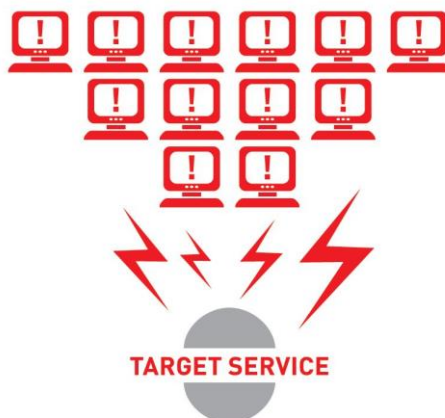


World wide sales | [sales@ruggedtooling.com](mailto:sales@ruggedtooling.com)

© Copyright 2010 - 2015 Rugged Tooling Oy. All rights reserved.

Version 1.6 15 January 2015

# CYBER ATTACKS ON DEMAND



## WHY RUGGED TOOLING?

We want you to catch bugs before live network deployment. Our deep SW expertise and the technological flexibility of our products can deliver unique features for your testing needs. Combine Rude with Ruge for best test results.