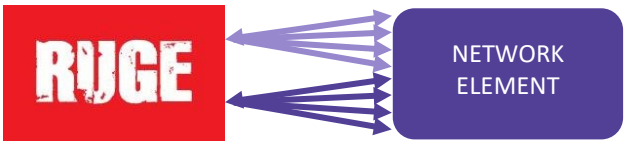
PRODUCT DATA SHEET

Rugged IP load generator (Ruge)

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

Rugged IP load generator

Datasheet



Test the boundaries of your network

The need for cyber security continues to increase as cyber attacks become more commonplace due to the ease with which attacks can be created and the devastating effects they can bring upon any business. At the same time, ubiquitous IP based services such as IoT services are launched every day, setting tremendous pressure on network load handling. Rugged IP load generator (Ruge) is a versatile test tool for creating cyber attack drills and for ensuring that your product or service meets the targeted limits – before it goes live and it's too late.

Ruge combines high data volumes with anomalous behaviour, which makes it suitable for e.g

- Simulation of cyber-attacks (DDoS) and recovery from attacks
- Load testing of IP based network equipment or network services
- Network optimisation
- Negative testing with data generation beyond spec boundaries

Key benefits:

- *Simultaneous generation of various data types*
- *Extremely fast ramp-up of load generation*
- *Flexible protocol stack control*

Features

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.

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

Unique flexibility and accuracy

Ruge engine SW has no third-party operating system. Thus, product performance is not affected by a third-party operating system overhead.

This also means that all protocol stacks 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.

Ruge supports high load stress testing with extremely accurate time stamping in which the theoretical line rate can be reached with any data type and their combinations. The accuracy of repeatability is up to microsecond level and exact repeatability in data content.

Ruge overview

Ruge is the traffic source in the test setup. Traffic is generated on the basis of scripts that can be built in Ruge GUI by the user. A library of readymade scripts is also available for creating typical scenarios.

Ruge can be used for testing recovery from cyber attacks or for testing the load capacity of the system. Ruge can generate multiple datatypes simultaneously, which means that practically any real life situation can be duplicated with Ruge.

- Capacity testing with realistic traffic generated from captured PCAP files
- Negative testing, with out-of-spec traffic
- DDoS attack emulation, generated with ready-ade or custom scripts

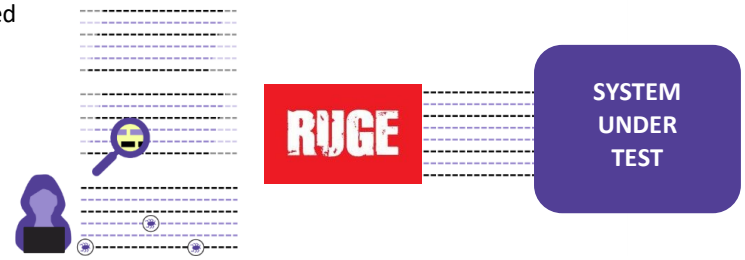


Figure 1. Ruge use scenarios

Ruge use scenarios

Cyber security: Distributed Denial of Service (DDoS) testing

Ruge can create realistic DDoS attack scenarios either by user-defined values or by involving readymade script libraries in the emulation of the most typical DDoS attacks. Figure 1 shows the basic setting for using Ruge in an attack simulation. Ruge represents a large number of attackers, and delivers a high load of predefined traffic to the system under test.

Top-20 DDoS attacks

This DDoS script library covers the majority of the most common Distributed Denial of Service attacks. The attacks use various protocols, such as Ethernet, IPv4/IPv6, TCP, UDP, ICMPv4/ICMPv6 and ARP. Several different methods, such as flooding, spoofing, malformed packets and fragmentation, are used in the attacks.

VoIP DDoS attacks

This script library includes seven different attack scenarios which use a dedicated SIP session establishment. The attacks use RTP, ICMP, IP and SIP protocols.

DDoS attacks for base station testing

This script package includes 30 different attack scenarios that can be used to find the security vulnerabilities of a base station. The attacks target the following protocols: Ethernet, IPv4/IPv6, TCP, UDP, ICMPv4/ICMPv6, ARP, SCTP, GTP-U and VLAN.

Flooding, spoofing, port scanning, malformed packets and fragmentation methods are used in the attack scenarios. The scripts are capable of scanning TCP ports, reporting open ports and targeting attacks to open ports.

Latency measurements

Ruge can measure latency with nanosecond level accuracy, allowing testing for 5G and mission critical IoT applications. This is due to ability to save timestamps of both sent and received traffic and measure the time difference between sent the received packets.

Load testing

Ruge can generate massive peaks of IP load to test the system's load capacity. It can also be used for testing SLA commitments with predefined settings, and for latency measurements, pass through check and data verification. Ruge is capable of generating provocative out-of-spec data to test the robustness of the system.

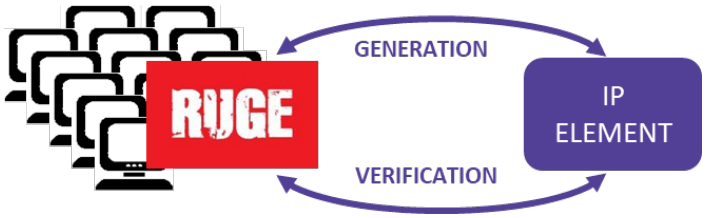


Figure 2. Ruge in load testing

IoT load testing

Ruge supports IoT load testing by simulating the data stream transmitted by a large number of IoT sensors.

Rich Communication Service (RCS) load testing

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

VoIP load testing

Ruge supports VoIP testing with a high performance basic SIP / RTP call.

Product configuration

Protocol stack support

Stateless protocols

The supported protocols are listed below. 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

Stateful protocols

Stateful operation is supported for the following protocols:

- SIP
- IKE
- CoAP
- MSRP
- MQTT
- TLS
- HTTP
- incl. JSON
- TCP

Supported encryption mechanisms

Protocol	Algorithm	Notes
TLS v1.1	AES CBS 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	
NAS	AES CTR 128 bit** SNOW3G 128 bit	** Supported as stateless, i.e. encryption is done

Statistics

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

- 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
- Expected and unexpected received message counters for stateful protocols.

Ruge in test environments

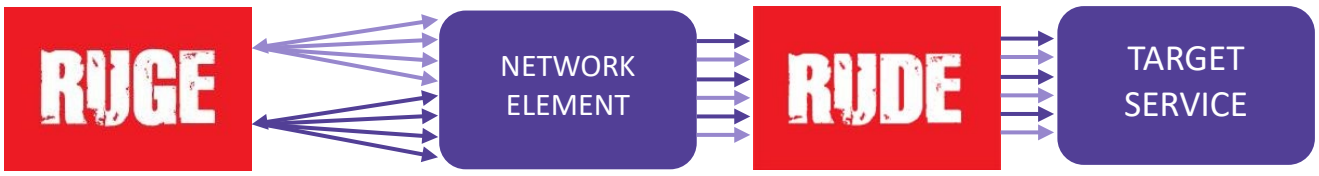
Test automation

Ruge can be integrated into the customer's automated test system using the Command Line Interface (CLI). In practice, control is accomplished by feeding command line arguments to a Ruge executable. This can be done manually from the command prompt of the operating system or automatically from scripts. Any scripting language supporting exe interface can be used.

Ruge combined with Rugged deviation emulator (Rude)

Ruge can be combined with Rugged deviation emulator (Rude), which enables integrating realistic IP network characteristics into 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.



Technical specifications

Ruge is available in 2 platforms: Blizzard and Breeze. Both platforms offer the same data generation features.

Physical interfaces			
Capacity	*Interfaces*	*Connector type*	*Usage*
100 Gbps	*Alternatively:* *4 x 25 Gbps* *16 x 10 Gbps* *2 x 25 Gbps and 8 x 10 Gbps*	*SFP+*	
80 Gbps	*8 x 10 Gbps*	*SFP+*	
50 Gbps	*2 x 25 Gbps*	*SFP+*	
25 Gbps	*1 x 25 Gbs*	*SFP+*	*Connection to System Under Test*
10 Gbps	*1 x 10 Gb*	*SFP+*	*Connection to System Under Test*
*1 GbE electrical ports**	*1 Gb*	*RJ45*	*Connection to System Under Test*
Control	*Control port*	*RJ45*	*Connection to host PC with GUI or CLI*

*Breeze platform

	Blizzard**	**Breeze**
Mounting	1U rack mountable	Portable
Dimensions (W x H x D)	430 x 44 x 535 mm	230 x 44 x 140 mm
Weight	12.7 kg	1.1 kg
Max power consumption	550 W	40 W

Environment	**Blizzard****	**Breeze**
Operating temperature	0…40 °C / 32…104 F	0…40 °C / 32…104 F
Storage temperature	-40…85°C / -40…185 F	-20…70 °C / -4…158 F
Operating humidity	10% to 90% RH	5% to 85% RH
Storage humidity	5% to 95% RH	5% to 95% RH

** Blizzard expected release P1/2020

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

Supported operating systems

Ruge client software is supported in Windows and Linux.

V4.0 Jan 2021

Rugged Tooling

Oulu, Finland

sales@ruggedtooling.com

www.ruggedtooling.com