PRODUCT DATA SHEET

Rugged deviation emulator (Rude)

Sure, you can test your network in your lab. But isn't it a bit too optimal for realistic and thorough testing?

Rugged deviation emulator

Datasheet

NETWORK
ELEMENT
RUDE
TARGET
SERVICE

Test quality, security and robustness

New ubiquitous internet and IP based services are launched every day, attracting a growing number of customers. Increasing cyber attack vectors along with the increasing number of connected end user equipment set tremendous pressure on network and service quality, continuity and security. A service that works well in an optimal laboratory network will almost inevitably fail in a live network unless tested properly in advance.

With Rude, it is possible to save time and money by simulating live network conditions before network deployment. Rude provides unique flexibility by allowing you to accurately target the data you want to deviate. You can select any type of data within the packet header or payload and target the modification even to a single bit when necessary.

Key benefits:

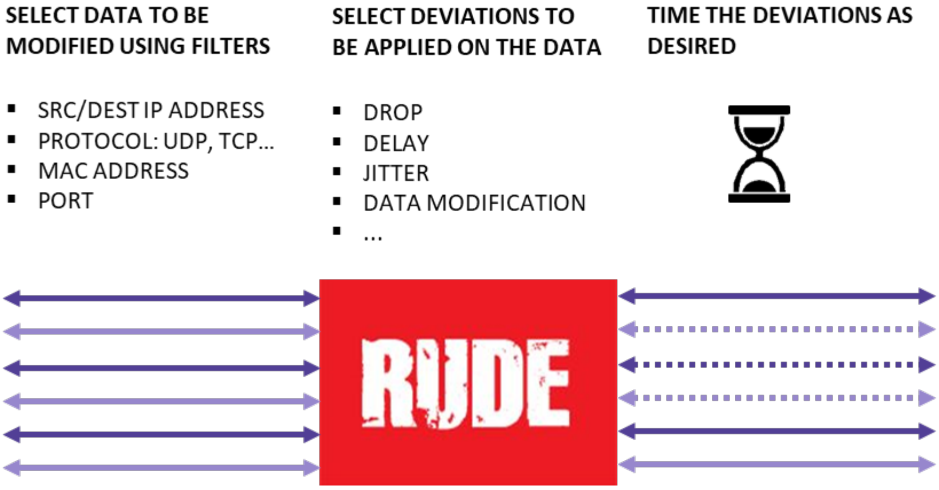
- Unique high-speed deviations for massive amounts of data flows
- Suitable for security and robustness use cases
- Flexibility to build the test scenarios you need

Rude is suited for

- Ethernet / IP performance testing
- Recovery testing from network challenges
- Security robustness testing
- QoS class simulation and QoE verification
- Network KPI validity testing
- Protocol and codec development phase testing
- Emulation of deployment target network
- Provocative testing with e.g. line breaks

Emulating live network conditions

Rude simulates live network conditions by deviating the data passing through it. It is possible to modify any type of traffic within the packet header or payload . Rude offers extremely accurate and flexible packet handling as it does not use any third-party operating system that would cause uncontrolled interruptions. All of the deviations can be applied to a traffic stream on the fly. Rude's operation is based on filtering, deviations and timed rules, as shown in the figure below.



SELECT DATA TO BE MODIFIED USING FILTERS

- SRC/DEST IP ADDRESS
- PROTOCOL: UDP, TCP…
- MAC ADDRESS
- PORT

SELECT DEVIATIONS TO BE APPLIED ON THE DATA

- DROP
- DELAY
- JITTER
- DATA MODIFICATION
- …

TIME THE DEVIATIONS AS DESIRED

Figure 1. Rude workflow

Traffic profiles

Rude also includes ready made traffic profiles for various network conditions. The profiles create a realistic network environment in a few simple steps avoiding the detail set-up process.

Networks	Variables
3G network **LTE network**	Stationary and moving user, low or medium traffic flow and normal, rush hour and congested conditions
ITU_T_G1050	Regional and international well-managed, partially managed and unmanaged networks.

Deviation functions

Rude offers a combination of deviation functions that can be used to modify traffic to simulate a live network. It is possible to target deviations even to the lowest protocol stack layers. Rude can perform hardware and protocol-specific checksum recalculations to ensure modified packets are not discarded. Rude deviation functions are as listed in the table below. Deviations are executed according to the rules defined by the user.

Deviation	Basic function	Additional info
Data hammering	Fragments IPv4 and IPv6 packets according to user-specified fragment sizes.	Fragmented packets can be re-ordered, dropped or multiplied.
Data content modification	Adds, removes, changes or overwrites data in data headers or payload.	Target data by defining either protocol header or with user-defined offset from beginning of packet.
Bandwidth limitation	Limits bandwidth according to user-defined limit. Packets exceeding the limit are dropped.	Limit set as bits per second. User-defined token bucket size.
Packet delay	Incoming packet is delayed by a user-defined time period.	User-defined delay range from 1µs to 60s.
Jitter	Additional feature to delay function. Adds variation to packet delay.	Normal (Gaussian) and uniform distribution supported.
Packet drop	Drops packets according to user-defined settings.	Random, bursts (Gilbert-Elliot model) and constant interval and predefined pattern for drop supported.
Line Break	Physical line break.	Global operation within a port pair.
Packet duplication	Packet is duplicated.	Constant and random modes supported.
Packet reordering	Holds a packet in Rude memory temporarily and resends it after a user-defined offset.	Constant and random modes supported.
Packet corruption	Data replacement with user-defined, random or inverted data or data targeted on the basis of offset from beginning of frame.	Random or constant intervals supported
Bursty data	Incoming traffic is rearranged as traffic bursts.	Bandwidth limit and burst duration specified the user.

Rude rules with timing feature

A rule is a set of parameters that can be applied to a certain traffic stream. The user can select deviations, and target them to the specific data flow and type at the required time. It is possible to set an individual rule for each data flow, subnet or protocol, while running them all at the same time, and edit the rules on the go.

Filters are used to target the deviations to a specific traffic type or traffic flow. Possible filters include

- src/dst MAC address
- VLAN tags
- MPLS labels
- IP src/dst address
- IP protocol (UDP, TCP, SCTP, ICMP)
- TCP/UDP/SCTP src/dst ports

- GTP tunnel endpoint identifier (TEID)
- VLAN PCP
- IP net mask
- IP DSCP
- TCP/UDP/SCTP port range
- IP address range
- Negation-based filtering
- Port with possibility to filter even or odd ports
- etc.

Filters can be combined with the operations ‘and’, ‘or’ or ‘not’. Also, Rude supports the possibility to filter any content on the basis of the offset from the beginning of the packet.

Rules can be timed as needed, either to simulate a gradually degrading network connection or to employ provocative testing by creating a series of line breaks with varying durations and intervals. Examples of modified data are presented in Figure 2. Filtering and timed profiles can be combined to create real life scenarios in the lab.

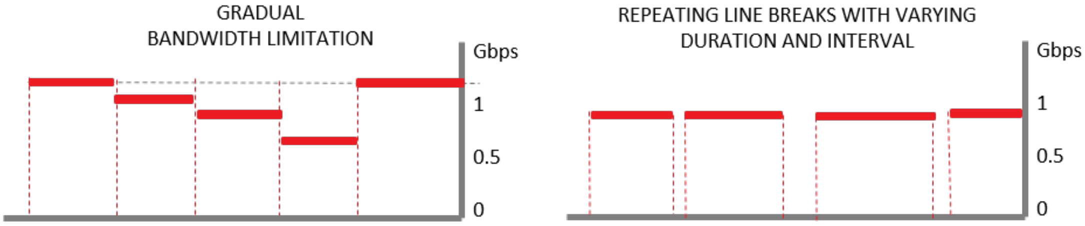


Figure 2. Examples of Rude output data

Statistics

Both the input data and the modified output data can be analysed using rule-specific statistics for the following counters for incoming data:

- Flow count (the number of incoming flows matching the rule filter)
- Flow rate [flow/s]
- RX & TX packet count
- RX & TX rate [packet/s]
- RX & TX byte count
- RX & TX rate [bits/s]
- RX average packet size
- Drop count
- Drop rate [packets/s]
- RX & TX fragment count
- Count of multiplied fragments

Statistics can be saved to a file as comma-separated values (CSV) for further analysis and processing.

Rude test environment

When using Rude in the basic setup, Rude is set in the System Under Test as the Man-in-the-Middle and data modifications are controlled through GUI, with a PC connected to the control port.

Multiple user capability

You can build additional test line capability with Rude’s multi-user feature. Each user can control one or more port pairs. The deviations can be set separately for each port pair and they do not interfere with each other. Rude supports up to two parallel GUI users on the same device.

Test automation

Rude can be integrated into the customer’s automated test system using the Command Line Interface (CLI). The CLI interface supports generating multiple CLI instances for multiple users within one port pair. A user can reserve a number of rules into his use, and see statistics for those reserved rules. The rules can be added and removed during the runtime.

The CLI interface can be controlled either manually from the command prompt of the operating system or automatically from the test automation platform scripts. Shell scripts can also be used. Any scripting language supporting exe interface can be used.

Technical specifications

Rude is available in 2 platforms: Blizzard and Breeze.

Both platforms offer the same data generation features.

Physical interfaces			
Interface	*Capacity*	*Connector type*	*Usage*
*40 GbE optical ports***	*40 Gb*	*QSFP+*	*Connection to traffic source and System Under Test (IN/OUT)*
25 GbE optical ports 2 port pairs	*50 Gbps total 2 x 25 Gbps*	*SFP+*	*Connection to traffic source and System Under Test (IN/OUT)*
25 GbE optical ports 1 port pair	*25 Gb*	*SFP+*	*Connection to traffic source and System Under Test (IN/OUT)*
10 GbE optical ports 2 port pairs	*20 Gbps total 2 x10 Gb*	*SFP+*	*Connection to traffic source and System Under Test (IN/OUT)*
10 GbE optical ports 1 port pairs	*10 Gb*	*SFP+*	*Connection to traffic source and System Under Test (IN/OUT)*
*1 GbE electrical ports **	*1 Gb*	*RJ45*	*Connection to traffic source and System Under Test (IN/OUT)*
Control port	*1 Gb*	*RJ45*	*Connection to host PC with GUI or CLI*

* Breeze platform ** Expected Q2/2021

	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

Device pass-through latency	
3,6 µs / Blizzard	in precision measurement environment
9 µs / Breeze	in precision measurement environment

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

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

Supported operating systems

Rude client software is supported in Windows and Linux.

V4.3 Jan 2021

Rugged Tooling
Oulu, Finland
sales@ruggedtooling.com
www.ruggedtooling.com