RUGGED TOOLING
A STREAM COME TRUE

PRODUCT DATA SHEET

Rugged deviation emulator (Rude)

RUDE

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

Introduction

Internet and IP based services are undoubtedly today's true boom industries. New services are launched every day attracting more and more users to find their favorite solutions. However, the fast growing number of potential customers sets tremendous pressure on network and service quality. A service working well in an optimal laboratory network will almost inevitably fail in a live network unless tested properly in advance.

Rugged deviation emulator (Rude) can be used to bring realistic live network conditions into the test laboratory. Rude can be used to simulate different types of network deviations, such as

- packet delay with or without jitter
- bandwidth limitation
- packet duplication and drop
- packet corruption
- packet reordering
- packet length change
- data fragmentation

All deviations can be targeted on the basis of precise filters.

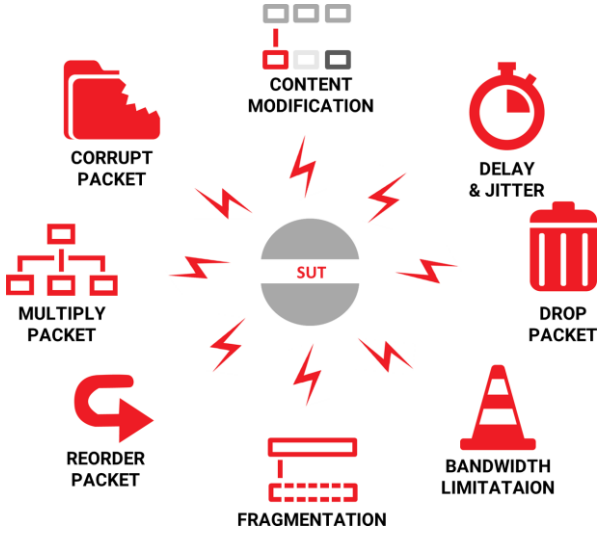
Great performance and high accuracy

Rude uses powerful network processing units (NPUs) and is optimised to handle internet protocol (IP) based packet traffic. Rude hardware engine has up to 32 GB of memory and deviation can be generated to IP traffic at line rate (1Gb/10Gb).

As there is no third-party operating system in the product and thus no uncontrolled interruptions, Rude offers extremely accurate packet handling. Delay and jitter resolution are within microsecond level.

Unique flexibility

Rude offers a possibility to modify any type of traffic on top of Ethernet frames. Traffic deviation can be targeted on the basis of several parameters, e.g. service type, user ID, IP address, flow, protocol or tunnel ID.



Suitability for various use cases

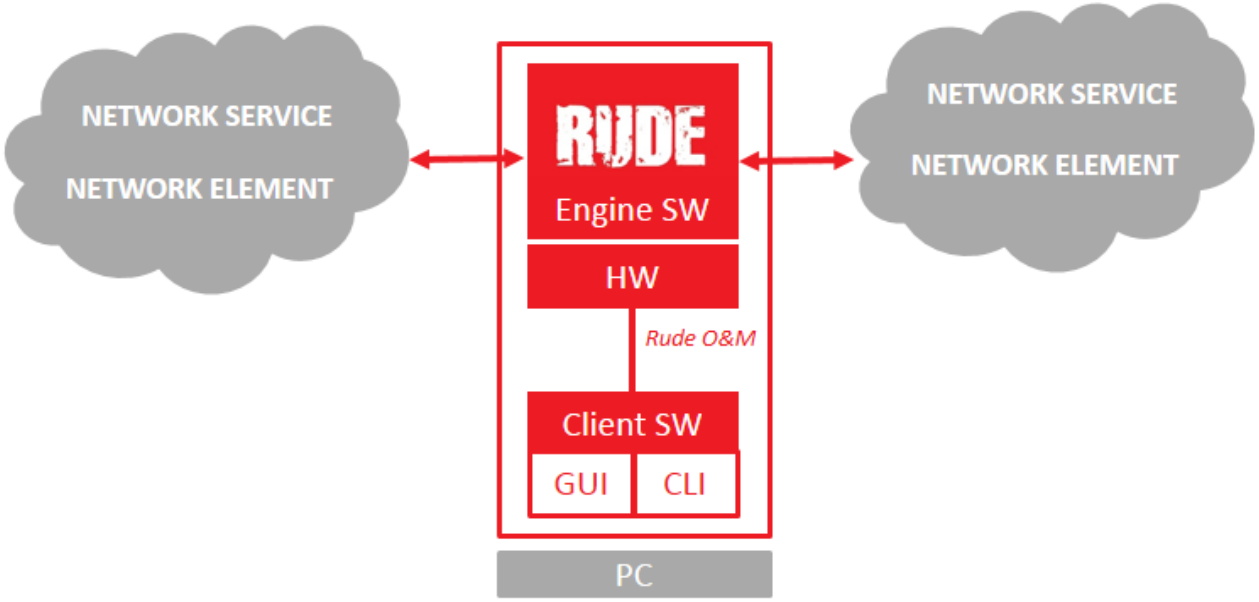
Rude is at its best when you use it from the early R&D phase. Rude can be used for different types of testing such as

- Ethernet / IP transmission performance testing with impairment by applying jitter, delay, packet drops, duplicates and re-ordering
- Data content modifications on the fly by adding or deleting packets
- Provocative testing by using Rude features such as electrical line breaks and timed profiles to create a test environment which is varying over time

Rude is suitable for various use cases including:

- Recovery testing from generated errors
- Users' Quality of Experience (QoE) verification
- Network Key Performance Indicator (KPI) testing
- Protocol and codec development phase testing
- Emulation of deployment target network

Product configuration



Rude hardware

Rude engine consists of Rude hardware and Rude engine software. Rude hardware uses network processing units (NPUs) which are optimised for IP packet processing. Co-processors perform all time critical actions, such as CRC calculation.

Rude is available for 1 Gbps (RJ-45 electrical) and 10 Gbps (optical) interfaces. Up to three 1 Gbps port pairs or one 10 Gbps port pair are supported in one unit.

Rude software

Rude engine software controls NPUs and is responsible for traffic deviation.

Rude client software runs on Windows 7 and Linux and is used to configure and control Rude engine. In addition to Rude Graphical User Interface, a Command Line Interface (CLI) is provided for testing automation.

Product features

Rude supports basic deviation functionalities such as delay, jitter, packet loss, duplication, corruption, reordering and bandwidth limitation according to ITU-T G.1050. Additionally, data content modification and IPv4/IPv6 data fragmentation are also supported.

Rude rules

A rule is a set of parameters that can be applied to a certain traffic stream.

Rude is configured by creating and editing rules (traffic profiles). It is possible to set a unique live network scenario for each desired data flow, subnet or protocol while running them all at the same time. Individual rules can be edited on the go, with no need to hold other ongoing simulations.

Up to 20 parallel rules are supported.

Flow types

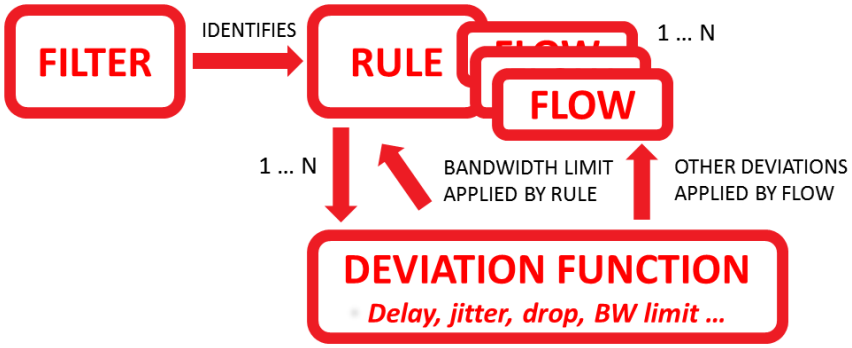
A flow is a unique combination of the following parameters:
- Source and destination MAC address
- VLAN tags
- MPLS labels
- IP source and destination address
- IP protocol (UDP, TCP, SCTP, ICMP)
- TCP/UDP/SCTP source and destination ports
- GTP tunnel endpoint identifier (TEID)

Example. When the user defines a rule that will drop 10 percent of the packets, the definition of traffic flow guarantees that the same drop amount will be applied to all sessions or calls.

Filter types

A filter is used to target the rule for the desired traffic flow.

Filtering can be done on the basis of any of the flow types described previously and additionally, on the basis of:



- VLAN PCP
- IP net mask
- IP DSCP (Differentiated Services Code Point)
- TCP/UDP/SCTP port range
- Port with possibility to filter even or odd ports
- Filters can be combined with ‘and’ or ‘or’ operations.

Example: Filtering can be applied to either IP_address_1 *or* IP_address_2.

Rude supports the possibility to filter any content on the basis of offset from the beginning of the packet.

Offset based filtering

With offset based filtering the user may filter in traffic based on any protocol field in the incoming packet. The offset from the beginning of the packet has to be known and constant.

Timed profile

The timed profile functionality (a.k.a dynamic impairment) is efficient when variation of good data and bad data is needed. Rude rules can be defined as timing based profiles and used to test recovery from error situations.

Symmetric and asymmetric deviation

Rude supports both symmetric and asymmetric deviation. This means that rules can be set independently to both directions.

Deviation functions

Deviations are executed according to the rules defined by the user and as specified in ITU-T G.1050.

Packet delaying

With the packet delay function the user can simulate packet delay in the network. An incoming packet that is to be delayed is held in Rude memory for a user-defined period of time before sending it on.

Adding jitter

The jitter function makes it possible to simulate changes in packet delay in the network. The jitter function can only be used together with the delay function. While delay represents the constant (or mean) part of the overall time the packet is held in Rude memory, jitter represents the deviation part.

Rude supports normal (Gaussian) and uniform jitter distribution with ordered and non-ordered packets.

Packet drop

This function enables the user to simulate packet loss in the network. Packet drop can be done randomly, at constant intervals or in bursts according to the Gilbert-Elliott model (ITU-T G.1050).

Packet duplication

Packet duplication can be set to occur to occur at random or at constant intervals.

Packet reordering

This function enables the user to simulate packet reordering in the network. A reordered packet is held temporarily in Rude memory and sent on only after a user-defined number of other packets within the flow have been received and sent.

The reorder interval can be constant or random.

Packet corruption

This function makes it possible for the user to simulate packet content corruption in the network.

The corruption functionality allows data replacement with user-defined, random or inverted data. Corruption can be done randomly or at constant intervals.

The deviation can be targeted on the basis of the user-specified offset from the beginning of the frame.

Bandwidth limitation

This function makes it possible for the user to simulate limited bandwidth in the network. The limit is set as bits per second. The packets exceeding the limit are dropped.

Data content modification

Rude offers the possibility to change the content of any data. The user can, for example, change packet length by adding or removing bytes.

Data content modification will be further enhanced so that the user can directly select the target of the content change, e.g. when an IP address needs to be changed to another one. In this case, there is no need to know the offset of the IP address byte from the beginning of the packet.

Data hammering

The smaller the IP packets are, the harder it is for the network element to handle them. With Rude data hammering, the user can create challenging traffic scenarios by first fragmenting IPv4 or IPv6 packets. Fragmented packets can be re-ordered and some amount of data can even be dropped. Data fragmentation can be executed by defining the Maximum Transmission Unit (MTU) with Rude.

The feature allows targeting fragmentation to certain traffic only, e.g. on the basis of the IP address, and ensuring that other parts of the network remain intact. There is no longer any need for manual configuration routines on the test network.

Automated electrical line break testing

It is crucial to test how network elements and services recover from common infrastructure-related problems such as electrical line breaks. Rude supports emulation of both software and hardware line breaks. In a SW line break 100 percent of L2 traffic packets are dropped, whereas in a HW line break all L1 traffic is dropped.

Statistics

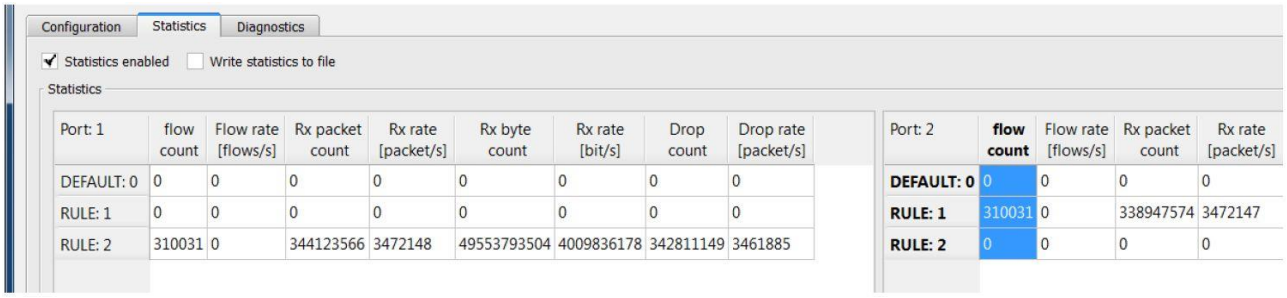
Rude offers rule specific statistics for the following counters for incoming data:

- Flow count (the number of incoming flows matching the rule filter)
- Flow rate [flow/s]
- RX packet count
- RX rate [packet/s]
- RX byte count
- RX rate [bits/s]
- Drop count
- Drop rate [packets/s]

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

Multiple user capability

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



Port: 1	flow count	Flow rate [flows/s]	Rx packet count	Rx rate [packet/s]	Rx byte count	Rx rate [bit/s]	Drop count	Drop rate [packet/s]
DEFAULT: 0	0	0	0	0	0	0	0	0
RULE: 1	0	0	0	0	0	0	0	0
RULE: 2	310031	0	344123566	3472148	49553793504	4009836178	342811149	3461885

Port: 2	flow count	Flow rate [flows/s]	Rx packet count	Rx rate [packet/s]
DEFAULT: 0	0	0	0	0
RULE: 1	310031	0	338947574	3472147
RULE: 2	0	0	0	0

Rude statistics tab.

Technical specifications

Rude hardware

Processor & memory		**Port capacity**	
Processor	Cavium Octeon II NPU	Port pair capacity 1 GbE	1 … 4
Number of cores	32	Port pair capacity 10 GbE	1
Internal memory	32 GB		

Physical interfaces			
Interface	Capacity	Connector type	Usage
10 GbE ports	10 Gb	SFP+	Connection to traffic source and System Under Test (IN/OUT)
1 GbE 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
Console port		RJ45	Additional control of Rude

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

Safety Certifications / Compliance

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

Supported operating systems

Rude client software is supported in Windows 7 and Linux.

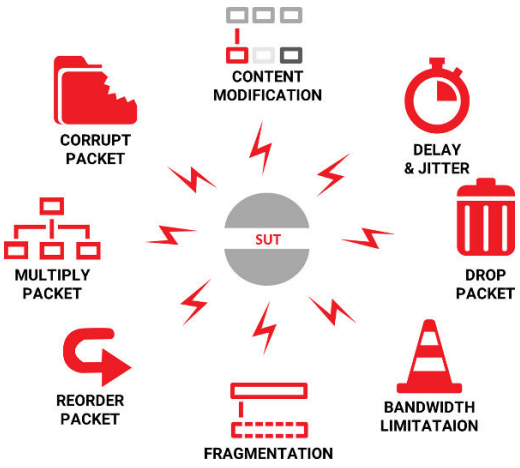
Prerequisites

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

World wide sales I sales@ruggedtooling.com

V2.9 9 April 2015

CONTROLLED NETWORK CHAOS



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.