Impairment Emulator Software for IP Networks (IPv4 & IPv6)

Contents

1 Product Overview ........................................................................................................... 2
1.1 Product Requirements .................................................................................................. 2
1.2 Typical Applications ..................................................................................................... 3
1.3 Customer references .................................................................................................. 3
1.4 Key Features ................................................................................................................ 4
1.5 Comparison between Standard and Enhanced Editions .............................................. 5
1.6 Examples of Use ......................................................................................................... 6
2 Product Description ........................................................................................................ 7
2.1 NetDisturb handles and impairs flows ......................................................................... 7
2.2 How does it work? ....................................................................................................... 10
2.3 Filter characteristics and user-defined impairment rules for the flow ......................... 11
2.4 Apply Impairments to Applicative Protocols with NetDisturb Enhanced Edition ........ 12
2.5 List of impairments .................................................................................................... 13
2.6 Working modes and flow aggregation ......................................................................... 15
2.6.1 Two Working Modes ............................................................................................ 15
2.6.2 Flow Aggregation .................................................................................................. 16
2.7 Traces and logs (Enhanced Edition only) .................................................................. 17
2.8 Statistics & Alarms .................................................................................................... 18
2.9 Configurations .......................................................................................................... 21
2.10 Performances ............................................................................................................ 22
2.11 Some publications and thesis mentioning the use of NetDisturb .............................. 23
3 Conditions of use .......................................................................................................... 25
4 Delivery ......................................................................................................................... 25
5 For more information .................................................................................................... 25
1 Product Overview

NetDisturb is an IP network emulator software that can generate impairments over IP networks (IPv4 and IPv6) such as: latency, delay, jitter, bandwidth limitation, loss, duplication and modification of the packets.

NetDisturb allows disturbing flows over an IP network aiding the study of the behavior of applications, devices or services in a disturbed network environment.

NetDisturb is inserted between two Ethernet segments acting as a bridge and operates bi-directional packet transfer on Ethernet, Fast Ethernet and Gigabit network interface cards.

1.1 Product Requirements

* Platform: Pentium PC running 32-bit or 64-bit version of Windows XP, Vista, Seven, Server 2003 or Server 2008 with Microsoft TCP/IP installed and at least 1 GB Ram. 20 MB free hard disk space.
* Hyper-threading, multi core and PC multiprocessors are also supported.
* Two Identical Network Interfaces Cards (NIC) are recommended: Ethernet, Fast Ethernet, or Gigabit Ethernet.
* Display resolution: at least 1024 x 768 (more readable: 1152 x 768 and sup.), DPI setting = Normal size (96 DPI) and Font size = Normal.
1.2 Typical Applications

No need to buy expensive hardware, use NetDisturb software as hundreds customers around the world!

- **Development assistance and debug of automatons for IP equipment**: particularly Set-Top Boxes operating in cable or telecom environments.
- **Performance & Acceptance Tests**: Qualify and evaluate the behavior of IP equipment (phone, fax, gateway, set-top box, IMS core, call server, etc...) and applications (audio and video streaming) on IP networks.
- **Configuration and control of IP Equipments for product verification and test**: Define different QoS levels in an Intranet or Internet environment to configure terminals, gateways and routers.
- **Test Laboratories**: NetDisturb provides repeatable QoS on different flows using configuration mode and values (loss, duplicate, delay, packet content impairment) defined by the user, thus re-creating real world problems in the lab.
- **Applications test**: NetDisturb allows testing applications such as Voice over IP, Fax over IP, streaming audio and video, IPTV, VoD, real time applications and services, plus other distributed applications.
- **Emulation of symmetric or asymmetric network conditions found on the Internet and enterprise networks (LAN, MAN, WAN)**: latency, jitter, packet loss, bandwidth limitations, and more... to test IP applications (VoIP, streaming audio & video, etc.), services and products sensitive to various real conditions.

1.3 Customer references

Present on the market since 1998, NetDisturb is used in more than 45 countries.

Satisfied customers worldwide include:

1.4 Key Features

What are the Key Features of **NetDisturb** V4.8?

Two editions of **NetDisturb** V4.8 are available: **Standard** and **Enhanced**

**Common Key features for Standard and Enhanced Editions**

- Latest 32-bit and 64-bit Windows operating systems – Vista, Seven, Server 2003 and Server 2008
- Simultaneous support of **IPv4** and **IPv6**
- Client-Server Architecture based on the SOAP mechanism which uses the HTTP protocol and XML format for the exchanges between the client and the server
- NetDisturb is an **Ethernet Bridge** to avoid any network configuration
- Use of standard Ethernet Network Interface Cards up to **1 Gbps**
- Symmetric or Asymmetric **Bandwidth limitation** with router simulation
- Intuitive, very easy to use **Graphical User Interface**
- 16 configurable flows per direction
- **Aggregates** of flows can be defined (set of flows sharing the same Delay & Jitter Law)
- User-defined rules for disturbances: pattern trigger; starting time after delay or number of packets received; stop impairments after number of received packets or elapsed time; loops; and more…
- Predefined filter parameters based on the main protocol header fields (MAC, MPLS, VLAN, IP, TCP and UDP headers) and user-defined pattern filter
- **Unidirectional** or **bi-directional** packet impairments
- Impairments: Latency; Loss; Duplication; bandwidth limitation; Delay and Jitter; Content Impairment (mathematical laws and user-defined files)
- Change the impairment law **on-the-fly** for a flow
- Ability to **impair the remaining network traffic** which can be solely the IP packets or all the Ethernet frames
- **Connections per flow**: impairments are applied to the flow or to each connection of the flow
- Ethernet / Internet modes (Out-of-Sequence packets)
- Command Line Interface (CLI) to use NetDisturb in test beds
- Ability to handle Ethernet Jumbo frames (payload up to 17976 bytes)
- Statistics display and export detailed statistics into a file
- **Accuracy = 1 millisecond resolution**

**Specific Key features for the Enhanced Edition**

- Impairments based on protocol primitives:
  - **ARP** (ARP Operation Code)
  - **DHCP** (DHCP Message Type)
  - **DNS** (DNS Message Type, DNS message Operation)
  - **FTP** (FTP Command, FTP Returned Status)
  - **FTP-DATA**
  - **HTTP** (HTTP Method, HTTP Returned Status)
  - **NTP**
  - **RTP** (Audio Payload Type, Video Payload Type, DTMF)
  - **SIP** (SIP Method, SIP From, SIP To, SIP Returned status)
- **RTP** and **FTP** data flow automatic discovery.
- Detailed event log window per flow viewing the events and application of the impairments according to the user-defined rules.
1.5 Comparison between Standard and Enhanced Editions

The following table summarizes the main differences between NetDisturb Standard and Enhanced editions:

<table>
<thead>
<tr>
<th>Features</th>
<th>NetDisturb Standard</th>
<th>NetDisturb Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impairment of IPv4 and IPv6 packets, ARP and Ethernet frames</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Filter parameters to define a flow:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Activity rules:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Start/Stop after a time limit or a packet counter or a pattern</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>trigger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Loop to reapply the rule with delay between each iteration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Packet filters: source address, destination address, source port,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>destination port, protocol, DSCP DiffServ (ToS), MPLS, VLAN, MAC</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>address…</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• User-defined pattern filter based on Ethernet packet content</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>16 user-defined flows to impair using filters and other flows to impair</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>without using filters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamically modify impairments on-the-fly per flow in each direction</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>when running</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregates of flows (set of flows sharing the same delay and/or</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>jitter laws</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Per-Flow statistics and NICs statistics</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Accuracy = 1 millisecond</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Standard impairments: drop/loss, duplicate, delay (latency), jitter,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bandwidth limiting, congestion, packet error, bit error, reorder, burst</td>
<td></td>
<td></td>
</tr>
<tr>
<td>errors</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delay from 1 millisecond up to 10 sec in each direction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emulate bandwidth up to 1Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impairments by using the IP protocol field</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Definition of flows to disturb based on protocol primitives:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ARP (ARP Operation Code)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• DHCP (DHCP Message Type)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• DNS (DNS Message Type, DNS Message Operation)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• FTP (FTP Command, FTP Returned Status)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• FTP-DATA</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• HTTP (HTTP Method, HTTP Returned Status,)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• NTP</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• RTP (Audio Payload Type, Video Payload Type, DTMF)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>• SIP (SIP Method, SIP From, SIP To, SIP Returned Status)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Detailed events log per flow</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
1.6 Examples of Use

The following examples illustrate a variety of NetDisturb implementations in recent client projects;

Simulation of packet loss rate for a corporate network

The modeling of packet loss rate of a banking network has generated a loss rate file with 1.3 million values. Prior to the deployment of new applications on the network, NetDisturb Standard Edition simulates the network to test these applications by using this external file containing loss rates to recreate the actual conditions of exploitation.

Simulation of a satellite link (with a 2 Mbps downlink and a 512 Kbps uplink throughput) for workstations of a branch office that generate TCP and UDP flows.

NetDisturb Standard Edition simulates the satellite link with limited uplink and downlink bandwidth. An aggregate is defined to submit all TCP and UDP flows to a function of delay - to reflect the delay of several hundreds of milliseconds introduced with the satellite link.

Application of disturbances on VLANs encapsulated over MPLS frames.

NetDisturb Standard Edition generates losses and delays of packets for specific VLANs implemented in a very large MPLS core network.

Tests for robustness of application protocols used in Triple Play Set-Top Box over DSL with NetDisturb Enhanced Edition

VoIP use case: verify that the SIP REGISTER or the SIP INVITE message is retransmitted in case of no answer and then apply a loss and delay for RTP packets of the SIP session.

DHCP use case: check that the OFFER message is lost following a transmitted DISCOVER message to validate automatic DHCP retransmission.

Test Video over IP using RTP with NetDisturb Enhanced Edition

NetDisturb generates impairments (loss, delay, duplication, modification of packets…) for the testing of codecs integrated in gateways, servers, STB and more…
2 Product Description

2.1 NetDisturb handles and impairs flows

NetDisturb is based on the notion of flows. A flow is a set of packets with a set of common packet properties, and can be unidirectional or bi-directional. Flows are part of sessions (successions of flows and "think times") related to some homogeneous user activity (e-commerce, mail, MP3 file, web, etc.).

An IP flow is described by using an n-tuple. In the typical case, the following 5-tuple is used: IP addresses (source and destination), protocol and port numbers (source and destination). An IP flow is composed of connections (such as TCP connections to make FTP transfer by example).

To define the n-tuple for a flow, NetDisturb uses the notion of filter. A filter is the combination of the following optional parameters:

- Ethernet header
  - Destination MAC address
  - Source MAC address
  - Ethernet Packet Length
  - IP Version (IPv4 or IPv6)
  - Other protocols (ARP)

List of VLAN-ID (Ethernet frames 802.1Q)

List of MPLS-ID

IP Header
- Destination IP address (IPv4 or IPv6)
- Destination IP Mask (bit mask for IPv6)
- Source IP address (IPv4 or IPv6)
- Source IP Mask (bit mask for IPv6)
- Protocol (ICMP, TCP, UDP…)
- Differentiated Services Code Point (DSCP) / ToS Byte

List of Ports (for TCP or UDP packets)
- Destination port list
- Source port list

Protocol primitives (only for Enhanced version): ARP, DHCP, DNS, FTP, FTP-DATA, HTTP, NTP, RTP and SIP.
User-defined Pattern Parameter (search for a defined pattern with an offset in the Ethernet frame content)

User-defined rules can be added to the predefined filter conditions for the application of the impairments.

With NetDisturb you can define up to 16 filters, i.e. 16 flows. An additional item named "Other Flows" is designated with handling all flows (IP or not) that have not been user defined. For this item no filter can be defined however, impairments can be applied.

NetDisturb manages up to 10,000 connections – all flows included.

The client window below illustrates the management of flows by NetDisturb.
The graphical user interface represents the two NIC cards used by NetDisturb as "A Interface" and "B Interface" as illustrated below.

For each direction $A \rightarrow B$ or $B \rightarrow A$, 16 flows can be defined by the user. For each flow, loss or duplication, delay and jitter, and content impairment laws can be applied as shown below.

In the above example, NetDisturb has been configured with the following parameters:

**Direction $A \rightarrow B$**
- The Filter #01 defines the "Flow #01", and a loss law is applied to the packets of this flow,
- The Filter #03 defines the "Flow #03", a Jitter law and a content impairment law are applied to the packets of this flow,
- As no loss, no delay and no content impairment laws are applied to the 'Other flows', all non-matching packets with the Filters #01 and #03 are relayed directly from A to B.
Direction B → A
- The Filter #02 defines the "Flow #02", and a loss law is applied to the packets of this flow,
- The Filter #15 defines the "Flow #15", a content impairment law is applied to the packets of this flow,
- As a delay law is applied to the 'Other flows', all non-matching packets with the filters #02 and #15 are delayed from B to A.

2.2 How does it work?

We illustrate how NetDisturb handles incoming packets with the following figure from the A to the B interface.

Dependant upon the active user-defined flows, NetDisturb checks the incoming packet against the filter of the flow before applying loss, delay or content impairment treatments. When this packet matches the filter of a flow (Flow #xx for example), then NetDisturb identifies whether this packet must be lost/duplicated and/or delayed, and/or its content must be impaired. If this packet does not match any filter, NetDisturb applies the parameters for 'Other Flows' and based on the laws defined i.e. lost/duplicated, delayed and content impairment.

For each packet received on an interface, NetDisturb analyzes the filters in order from 1 to 16 before considering that the packet belongs to the "Other Flows".

So, NetDisturb can apply impairments on the flows defined by the user either unidirectional (A → B or B → A) or bi-directional (the same or different impairments are being applied for both directions: A → B and B → A).

To go through NetDisturb (interface A → B or B → A), a packet should belong to flow 1 to 16 or to 'Other Flows' which ought to have been started.

When no filter is running, no packet goes through NetDisturb.
2.3 Filter characteristics and user-defined impairment rules for the flow

Two types of parameters can be used to define the filter for a flow:

- Predefined Parameters with the following options:
  - ARP
  - VLAN
  - MPLS
  - IP (TCP/UDP)
  - Protocol primitives (only for Enhanced version): ARP, DHCP, DNS, FTP, FTP-DATA, HTTP, NTP, RTP and SIP.
- And/Or User-defined Pattern Parameter (search for a defined pattern with an offset in the Ethernet frame content)

One of the features of NetDisturb is the definition of optional rules to link the launch of the impairments for a flow with an event or not.

Definition of the optional rules to apply impairments for the flow:
- Start when finding a pattern (with an optional offset) in the packet [Trigger]
- Delay before applying impairments (number of packets or elapsed time)
- Stop impairments after a number of received packets or elapsed time
- Reapply the previous conditions n times (n=0 means infinite), with a delay (elapsed time or number of received packets) between each cycle

Thus, the flow can be impaired continuously or impaired following user-defined rules with activity cycles.

If selected, notice that the Trigger is an intermediate step after the frame has been classified in a flow and before the frame is impaired.

The delay between 2 cycles acts as when the flow is not running.

For example, when NetDisturb is running a flow with user-defined rules including a trigger, several states are possible:

- **Waiting for the Trigger**: the impairments do not apply. This state is the initial state of the Trigger.
- **Delay before applying impairments**: the impairments still do not apply as a delay is defined before applying the impairments. The state changes to "Applying impairments" when the activation condition is reached. All packets or frames are relayed without treatment.
- **Applying impairments**: the impairments are applying.
- **Delay before next cycle running**: the impairments still do not apply as a delay is defined before reapplying the impairments. All packets or frames are relayed without treatment. This is available only when cycles are defined.
- **No more impairment**: the impairments no longer apply. All packets or frames are relayed without treatment.

A Trigger can remain active permanently when no duration limit is defined.
2.4 Apply Impairments to Applicative Protocols with NetDisturb Enhanced Edition

Two editions of NetDisturb software are available: Standard Edition and Enhanced Edition. The Enhanced Edition allows defining filters including protocol primitives as listed in detail below. If required, you are able to precisely define the exact primitive of the protocol to disturb.

<table>
<thead>
<tr>
<th>ARP</th>
<th>FTP Command (cont.)</th>
<th>Audio Payload Type (cont.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ARP request</td>
<td>• PASS</td>
<td>• 12 QCELP</td>
</tr>
<tr>
<td>• ARP reply</td>
<td>• PAV</td>
<td>• 13 CN</td>
</tr>
<tr>
<td>• RARP request</td>
<td>• PORT</td>
<td>• 14 MPA</td>
</tr>
<tr>
<td>• RARP reply</td>
<td>• PWD</td>
<td>• 15 G728</td>
</tr>
<tr>
<td>• DRARP request</td>
<td>• QUIT</td>
<td>• 16 DV4 (11,025 Hz)</td>
</tr>
<tr>
<td>• DRARP reply</td>
<td>• REIN</td>
<td>• 17 DV4 (22,050 Hz)</td>
</tr>
<tr>
<td>• DRARP error</td>
<td>• REST</td>
<td>• 18 G729</td>
</tr>
<tr>
<td>• InARP request</td>
<td>• RETR</td>
<td>Video Payload Type</td>
</tr>
<tr>
<td>• InARP reply</td>
<td>• RMD</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DHCP</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• DHCPDISCOVER</td>
<td>(BOOTP request)</td>
<td>26 JPEG</td>
</tr>
<tr>
<td>• DHCPOFFER</td>
<td>(BOOTP reply)</td>
<td>28 nv</td>
</tr>
<tr>
<td>• DHCPREQUEST</td>
<td>(BOOTP request)</td>
<td>31 H261</td>
</tr>
<tr>
<td>• DHCPACK</td>
<td>(BOOTP reply)</td>
<td>32 MPV</td>
</tr>
<tr>
<td>• DHCPNACK</td>
<td>(BOOTP reply)</td>
<td>33 MP2T</td>
</tr>
<tr>
<td>• DHCDECLINE</td>
<td>(BOOTP request)</td>
<td>34 H263</td>
</tr>
<tr>
<td>• DHCPRELEASE</td>
<td>(BOOTP request)</td>
<td>DTMF</td>
</tr>
<tr>
<td>• DHCPINFORM</td>
<td>(BOOTP request)</td>
<td>RTP (SIP From)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Message Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Message Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• QUERY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IQUERY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NOTIFY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• STATUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UPDATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FTP</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Returned STATUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• OK (200)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Not Found (404)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1xx Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 2xx Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3xx Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4xx Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 5xx Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP Command</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ABO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ACCT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ALLO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• APPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• CDUP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• CWD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DELE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• EPRT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• EPSV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FEAT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HELP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MKD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MODE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NLST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NOOP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• OPTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP DATA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTP</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Returned STATUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• OK (200)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Not Found (404)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Moved (301)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1xx Codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 2xx Codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3xx Codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4xx Codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 5xx Codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• OPTIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• GET</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HEAD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• POST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• PUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• TRACE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• CONNECT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| NTP | | |

<table>
<thead>
<tr>
<th>RTP</th>
<th>Audio Payload Type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Payload Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 0 PCMU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 3 GSM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4 G723</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 5 DVIPv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 6 DVIPv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 7 LPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 8 PCMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 9 G722</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 10 L16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 11 L16</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following screenshot illustrates an example of the parameters of a user-defined filter ("My New SIP Filter") for a SIP message ("REGISTER") that we wish to disturb. This example filter can be used for studying the retransmission mechanism when a SIP REGISTER is lost by using NetDisturb with a Set-Top Box.

2.5 List of impairments

Pre-defined Loss and Duplication laws:

- Loss: Constant Law
  Parameter: number of packets

- Loss: Uniform Law
  Parameters: alpha, beta, threshold

- Loss: Burst Uniform Law
  Parameters: alpha, beta, threshold(n), threshold(n + x), depth

- Loss: File (Loss Values)
  Parameters: file name, threshold

- Loss: Percentage
  Parameter: percentage

- Loss: 1 Packet out of N
  Parameter: range (N)

- Loss: Percentage & Duration (time-limited losses percentage)
  Parameter: percentage, duration
- Loss: File (Percentage & Duration)
  Parameter: file name

- Duplication: Percentage (send n times the received packet)
  Parameters: percentage, Min ≤ n ≤ Max

- Duplication: 1 Packet out of M (duplicate 1 packet n times every M received packets).
  Parameters: range (M), Min ≤ n ≤ Max

- Duplication: Uniform Law
  Parameters: alpha, beta, threshold, Min ≤ n ≤ Max

- Loss (1 out of N) then Duplication (1 out of M): the loss law (1 Packet out of N) is used first before the duplication law (1 Packet out of M)
  Parameters: Loss range (N), Duplication range (M), Min ≤ n ≤ Max

**Pre-defined Delay & Jitter laws:**

- Constant Delay
  Parameter = constant delay

- Constant Delay & Exponential Jitter
  Parameters: constant delay, λ

- Constant Delay & Uniform Jitter
  Parameters: constant delay, alpha, beta

- Constant Delay & File (Jitter)
  Parameters: constant delay, user file

- File (Packet Sending Minimum Cadences)
  Parameter: user file

- Router Simulation & Constant Delay
  Parameters: IP throughput, max memory, constant delay

- Router Simulation & File (Packet Sending Minimum Cadences)
  Parameters: IP throughput, max memory, user file

- Constant Delay & File (Throughput & Duration)
  Parameters: constant delay, user file

**Pre-defined Content impairment laws:**

- 1 Packet out of N
  Parameter: range (N)

- Percentage
  Parameter: percentage

- Normal Law (Laplace-Gauss)
  Parameters: average, standard deviation, threshold

- Uniform Law
  Parameters: alpha, beta, threshold
2.6 Working modes and flow aggregation

Two important features of NetDisturb allow you to define how disturbances will apply to the flow of packets:
- the working mode
- the aggregation of flows

2.6.1 Two Working Modes

NetDisturb offers two working modes by applying impairments:
- Enable/Disable Out-of-Sequence packets in a flow,
- Impairment laws apply to the IP flow or to each TCP/UDP connection of the IP flow.

These modes are used together.

For example, when NetDisturb is set with the following modes, it simulates the Internet network with disturbed flows:
- Enable Out-of-Sequence packets in a flow
- Impairment laws apply to the IP flow

Another example: to disturb VoIP communications in the same way on an Ethernet network, use NetDisturb with the following modes:
- Disable Out-of-Sequence packets in a IP flow
- Impairment laws apply to each TCP/UDP connection of the IP flow

Enable/Disable Out-of-Sequence Packets

Impairment may introduce changes in the packet sequence – for example by introducing different delays for the packets of a flow. One of the Ethernet characteristics is to keep packets received in order. Internet does not have this constraint regarding the packet order: some packets use one route whilst others use another one, the consequence being that the receiver may get disordered packets. NetDisturb is able to simulate the Internet network (enable out-of-sequence packets) or to react as Ethernet does (disable out-of-sequence packets).

Impairment laws apply to the IP flow or to each TCP/UDP connection of the IP flow

NetDisturb is able to dispatch IP packets into whichever TCP or UDP connection they belong to. This mode makes it possible to apply the same impairment values to each packet of each connection.

For example, assuming the impairment has been defined with a loss law "lose the third packet for 10 packets received", the results depends on the way this law handles the packets:

- Impairment laws to be applied to the IP flow
  When this option is selected, every received packet matching the filter for this flow is considered to belong to the same flow. Processing is carried out in "continue". With the aforementioned example of loss law (lose the 3rd packet on 10 received), NetDisturb will lose the 3rd packet for ten received packets whatever the TCP/UDP connection it belongs to.

- Impairment laws to be applied to each TCP/UDP connection of the IP flow
  When this option is selected, NetDisturb will analyse each received packet in order to associate this packet to an existing TCP or UDP connection by using these parameters: protocol, IP addresses and port numbers. If the connection is non-existent, a new one is created. With the example loss law (lose the 3rd packet on 10 received), NetDisturb will lose the 3rd packet for ten received packets of each TCP or UDP connection. Up to 10,000 connections can be handled simultaneously by NetDisturb.

The option “Impairment laws to be applied to each TCP/UDP connection of the IP flow” is not available for flows using a filter based on applicative protocol primitives.
2.6.2 Flow Aggregation

An aggregate is a consecutive set of flows sharing the same Delay & Jitter Laws. All flows of an aggregate share only one aggregate's Delay & Jitter law (with one law per direction).

This feature is particularly useful for the following cases: satellite simulation, VPN, routing, bandwidth limitation...

Up to 8 aggregates for all 16 flows can be defined.

The flow order in the aggregate defines the priority of packets to delay. Whilst the top flow packets get the highest priority, the other flow packets queue until there are no higher priority packets.

In the example illustrated below, two aggregates have been defined:
- The light blue colored aggregate collects two flows (#01 and #02)
- The dark blue colored aggregate collects the flows #04, #05 and #06.
2.7 Traces and logs (Enhanced Edition only)

Once a filter is defined for a flow, it becomes possible to trace the events and packets to impair with NetDisturb Enhanced Edition.

The following screenshot shows the log window displayed after running the flow where the option \( \Box \) has been checked for the flow.

For each flow with the checked log option, all incoming packets for the two interfaces \( A \) and \( B \) are saved into a capture file.

Using the opened log window when the flow is started by pressing the corresponding Run \#xx button, you are able to:

- Display the major events for both directions \( (A \rightarrow B \text{ and } B \rightarrow A) \).
- View the captured packets of the flow (for both directions) prior to applying impairments by using your default network analyzer launched automatically (e.g.: Wireshark/Ethereal).
- View the impairment applied for each packet of the flow (for both directions): (no impairment) or (lost) or (delayed) or (modified)…

NetDisturb generates two files per flow when the \( \Box \) option is checked:

- incoming_packets_flow#xx.pcap for the flow No. xx (this capture file contains all incoming packets for the two interfaces and can be viewed with a network analyzer such as Wireshark).
By using these two files, you are then able to examine very precisely which incoming packet is concerned and the nature of the applied impairment.

2.8 Statistics & Alarms

Different statistics are calculated and displayed by NetDisturb:
- Detailed Statistics for each Flow (and for both directions)
- Summary table of Per-flow statistics
- Interfaces Statistics (based on Network Interface Card level) and Alarms

These statistics can be saved into a file for later use.

Detailed statistics for each Flow

For each direction (A → B or B → A) NetDisturb displays:

- Incoming interface: the number of received packets matching the filter, the number of received packets per second and the throughput
- Impairments:
  - The number and percentage of lost or duplicated packets
  - The number and percentage of delayed packets
  - The number and percentage of modified packets
- Outgoing interface: the number of sent packets, the number of sent packets per second and the throughput
Summary table of Per-Flow statistics

The View Per-Flow statistics displays for each flow and for each direction:
- The incoming throughput and number of received packets per second
- The number of packets matching the filter
- The number of lost/duplicated packets
- The number of delayed packets
- The number of modified packets
- The outgoing throughput and the number of sent packets per second

Interfaces Statistics

At the bottom of the Client window, the Interface Statistics displays the following parameters for both NICs (A → B or B → A):
- Throughput and number of received packets per second
- Number of received packets
- Number of filtered packets
- Number of sent packets
- Throughput and number of sent packets per second

<table>
<thead>
<tr>
<th>Interfaces Statistics (based on Network Interface Cards level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>From A to B</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>From B to A</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Alarms

The alarms encountered by the NetDisturb driver can be displayed and are classified per direction for both interfaces:

<table>
<thead>
<tr>
<th>Incoming direction</th>
<th>Outgoing direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Number of lost packets</td>
<td>• Number of lost packets</td>
</tr>
<tr>
<td>• Number of lost bytes</td>
<td>• Number of packets lost due to the unplugged Network Interface Card</td>
</tr>
<tr>
<td>• Number of errors returned by the driver of the Network Interface Card</td>
<td>• Number of lost bytes</td>
</tr>
<tr>
<td>• Number of missing buffers to let NetDisturb get the incoming packets</td>
<td>• Number of errors returned by the driver of the Network Interface Card</td>
</tr>
<tr>
<td>• Number of lost TCP/UDP connections due to the upper limit of connections handled by NetDisturb</td>
<td></td>
</tr>
</tbody>
</table>
2.9 Configurations

Based on Client-Server architecture, NetDisturb software has two parts: NetDisturb Server and NetDisturb Client. NetDisturb Server handles the impairment characteristics and NetDisturb Client manages the Server using a simple graphics interface. This allows two configurations where the Server and the Client parts may be installed on the same PC (local control), or the Server is located on one PC and the Client is located on a second PC (remote control). In this second configuration, the Client communicates with the Server by using either a Wan (for example: PSTN or ISDN) or a LAN link.

**Note:** It is recommended for better performances to use two identical Ethernet Cards for NetDisturb Server.

<table>
<thead>
<tr>
<th>Configuration No 1</th>
<th>Configuration No 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Windows XP, Vista, Seven, Server 2003 or 2008</td>
<td>PC Windows 2000, XP, Vista Seven, Server 2003 or Server 2008</td>
</tr>
<tr>
<td>NetDisturb Client</td>
<td><strong>NetDisturb Client</strong></td>
</tr>
<tr>
<td>Client application and GUI</td>
<td>Client application and GUI</td>
</tr>
<tr>
<td>NetDisturb Server</td>
<td><strong>NetDisturb Server</strong></td>
</tr>
<tr>
<td>Server application and GUI</td>
<td>Server application &amp; GUI</td>
</tr>
<tr>
<td>Driver &quot;Disturb.sys&quot;</td>
<td>Driver &quot;Disturb.sys&quot;</td>
</tr>
<tr>
<td>Ethernet NDIS driver</td>
<td>Ethernet NDIS driver</td>
</tr>
<tr>
<td>Ethernet NIC (A)</td>
<td>Ethernet NIC (A)</td>
</tr>
<tr>
<td>Ethernet NIC (B)</td>
<td>Ethernet NIC (B)</td>
</tr>
<tr>
<td>LAN (A)</td>
<td>LAN (B)</td>
</tr>
<tr>
<td>Ethernet 10/100/1000 Mbps</td>
<td>Ethernet 10/100/1000 Mbps</td>
</tr>
<tr>
<td><strong>Client and Server on the same PC</strong></td>
<td><strong>Client and Server on two different PCs</strong></td>
</tr>
</tbody>
</table>

The Disturb.sys driver is located in the kernel of the operating system and is installed above the NIC drivers. This driver is used by NetDisturb to handle the exchanges with the NICs.
2.10 Performances

To illustrate the key performances of NetDisturb, 2 examples are presented hereafter (by using an Intel Xeon 5140 2.33 GHz with windows XP SP2).

Example 1: use of 2 Fast Ethernet NICs

NetDisturb is configured with 16 flows (no loss and no delay for each flow).
With Fast Ethernet NICs, the throughput measured is 97 Mbps in one direction.

Example 2: use of 2 Gigabit Ethernet NICs

NetDisturb Standard Edition is able to handle up to 200,000 packets per second with 16 flows defined (for both directions).
For more detailed information, please refer to the "NetDisturb Performance Characteristics on Gigabits Networks" document.

The two examples above show some of the performances of which NetDisturb is capable, thus demonstrating the avoidance of costly investment in expensive hardware solutions.
2.11 Publications and Theses that mention the use of NetDisturb

::: Gros L., Chateau N., *The impact of listening and conversational situations on speech quality for time-varying impairments*, France Telecom R&D, France, 2002
Degradation of the speech signal by using NetDisturb which introduced impairments in real time according to quality profiles.

::: The Communications and Information network Association of Japan (CIAJ) which represents manufacturers supplying network devices and terminals has published a report on 2002: *Report on speech quality investigation of VoIP Terminals (gateways and IP phones)*: “We adopted NetDisturb as a network simulator because of its ease of installation and operation in Windows”.


::: Koziniec, T., *Asymmetric Networks: Managing Reverse Path Congestion to Optimize TCP Forward Throughput*, Murdoch University, Western Australia, 2004


::: Raake, A., *Predicting Speech Quality under Random Packet Loss: Individual Impairment and Additivity with other Network Impairments*, Institute of Communication Acoustics, University of Bochum, Germany, 2004


::: *Effects of Latency on Telesurgery: An Experimental Study* Authors: Reiza Rayman1, Serguei Primak2, Rajni Patel2, Merhdad Moallem2, Roya Morady1, Mahdi Tavakoli2, Vanja Subotic2, Natalie Galbraith2, Aimee van Wysberghe1 and Kris Croome1
(1) Canadian Surgical Technologies & Advanced Robotics (CSTAR), 339 Windermere Road, London, Ontario, N6A 5A5, Canada
(2) CSTAR & Department of Electrical and Computer Engineering, The University of Western Ontario, London, Ontario, N6A 5B9, Canada
Publisher: Springer Berlin / Heidelberg
Volume 3750/2005
Springerlink date: Tuesday, September 27, 2005
The delay in the network was controlled by NetDisturb software.

::: *Speech Quality of VoIP*. Published November 24, 2006
Appendix B: Simulation of Quality Elements
Author: Alexander Raake, Deutsche Telekom Laboratories, Germany
Copyright © 2006 John Wiley & Sons, Ltd

Prepared for: U.S. Army Medical Research and Materiel Command, Fort Detrick, Maryland, USA
NetDisturb is used to invoke time delays during selected activities (the lunar delay of a couple seconds is incurred during all uplinks and downlinks. This includes audio, video, data transfer, and commands).


::: 3GPP Technical Specification Group Services and System Aspects TSG-S4 - Test Plan for the Adaptive Multi-Rate Wide-Band (AMR-WB) and Narrow-Band (AMR-NB) in packet switched networks.
- Test Plan for 3G packet switched conversation tests (comparison of quality offered by different speech coders over packet switched networks)
NetDisturb is used as the simulated network.

The following illustrations describe the system which has been simulated for these tests.

![](image1.png)

*Packet switch audio communication simulator*

Simulation utilising 5 PCs as shown below - PC# 3 is the designated Network Simulator using NetDisturb.

![](image2.png)

*Simulation platform*
3 Conditions of use

NetDisturb is licensed on a per workstation basis. Separate licenses will need to be purchased for each machine on which you wish to run the programme. Each licensed copy of the software is supplied with one corresponding USB Software Protection Key. This key should be plugged into the target PC prior to executing NetDisturb.

4 Delivery

The delivery includes one CD-ROM with printed installation guide and one USB Software Protection Key (dongle) per license.

*Recommended option:* the Technical support and software maintenance (including major and minor software upgrades) for a period of twelve months can be purchased with the license.

5 For more information

Please contact Packet Data Systems sales:
  Tel  +44 (0) 1491 684013
  Fax  +44 (0) 1491 684180
  Email info@pds-test.co.uk

To download the trial version of NetDisturb, please visit us at:
http://www.pds-test.co.uk/trial.php
ANNEX: GLOSSARY OF TERMS

Bandwidth Strangulation
Bandwidth strangulation is used for two main purposes:
- Quantify network resources - by evaluating the application's bandwidth requirements, network managers can determine in advance the amount of bandwidth to purchase.
- Evaluate QoS mechanisms - prior to a decision on which QoS mechanism is appropriate for the enterprise, network managers can emulate different Service Level Agreements and evaluate the ROI of different services such as Frame Relay, Diffserv etc.

Delay jitter
Delay variation of the packet transfer caused by the queuing and access delays in the source node, all transit node delays, and the receive buffer delay in the destination node.

IP Flow
A flow is a set of packets with a set of common packet properties. The IP flow can be Uni or Bi-directional and is defined by n-tuple (typical case: 5-tuple – IP source address, IP destination address, Source port number, destination port number, and transport type).

Jitter or Inter-Packet Delay Variation (IPDV)
In data networks, jitter refers to packet jitter, NOT bit jitter and represents the variation in a stream's delay (expressed in seconds). Jitter is the standard deviation of delay and is one of the IP performance metrics. The jitter is the absolute value of the difference between the delay measurements of two packets belonging to the same stream. The jitter between two consecutive packets in a stream is reported as the "instantaneous jitter". Instantaneous jitter can be expressed as |D(i+1) – D(i)| where D equals the delay and i is the test sequence number. Packets lost are not counted in the jitter measurement.

Latency (End-to-End Delay)
Latency is defined as the period of time taken for the information element (voice, e-mail, web, etc.) to traverse the network from its origin to its destination. For basic data where a small delay can be tolerated, latency is usually not an issue. However, for communications services used for videoconferencing or VoIP for example, latency can interfere with the audio and/or visual communications. In shared bandwidth transmission environments, it is possible to encounter latency that varies dynamically, caused by perhaps a single user accessing or originating multi-megabyte-sized files or accessing high bandwidth streaming signals.

When discussing network latencies relative to the operation of H.323, there are 3 general categories to consider:
- End-to-End latency in a given direction. This category addresses the total transit time for data of a given data stream to arrive at the remote endpoint.
- Intra-stream latency. This category addresses latencies within a given data stream i.e. inter-packet latencies that deviate outside of the normal transmit time by more than a predefined value.
- Inter-stream latency. This category addresses the relative latencies that can be encountered between the audio and video data streams.
Network Errors
Generally, packet losses or corruptions are the source of the network errors:

- Main cases of packet loss:
  - Network load - which can cause a packet queue in a network hop to overflow. This will cause new packets to be dropped due to lack of memory space. Typically this results in a burst loss where several packets from one endpoint are lost at once.
  - Limited bandwidth - QoS parameters such as Frame Relay CIR (Committed Information Rate) or Diffserv bandwidth polices can define a data rate limit which, when exceeded, can result in dropped packets.
  - Congestion avoidance mechanisms, such as RED (Random Early Detection) implemented in network gateways and routers can selectively decode and drop packets in order to avoid what seems to be an upcoming congestion trend.
  - IP header corruption is an error that creates a malformed IP header. A malformed IP header will cause the next router receiving the corrupted packet to drop it.
  - Hardware faults such as link disconnections and device shutdown.

- Packet corruption: This is caused by errors in the physical layer and, in turn causes data bits to toggle.

Network Impairment
Network impairment is the process of interfering with network traffic for the purpose of testing and evaluating the overall performance of TCP/IP networks. Due to TCP/IP's dynamic routing algorithms, packets may be delayed, reordered, duplicated, fragmented or even lost.

Out Of Sequence Packets (OOS)
Out of sequence packets typically occur when the packet stream is transmitted over multiple paths of unequal delay to a particular endpoint. Packets may arrive at the destination with incorrect sequencing.

Packet Loss
Packet loss is a normal phenomenon on packet networks where data transmitted from an originating device does not arrive at it's intended destination. Loss can be caused by many different reasons: overloaded links, excessive collisions on a LAN, and physical media errors, to name a few. Transport layers such as TCP account for loss and allow packet recovery under reasonable loss conditions.

Propagation Delay
The propagation delay is the time required for a packet to travel over the network (difference between the transmission of data and it's receipt at the other end).

Quality of Service (QoS)
A list of measurable attributes which should be met for a specific communications service on a network: bandwidth, latency, packet loss rate, out-of-sequence packet and latency variation (jitter) for real-time applications such as VoIP, and service availability.