Version 7.0

Impairment Emulator Software
for IP Networks (IPv4 & IPv6)

Contents

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 you to disturb flows over an IP network helping to study 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.
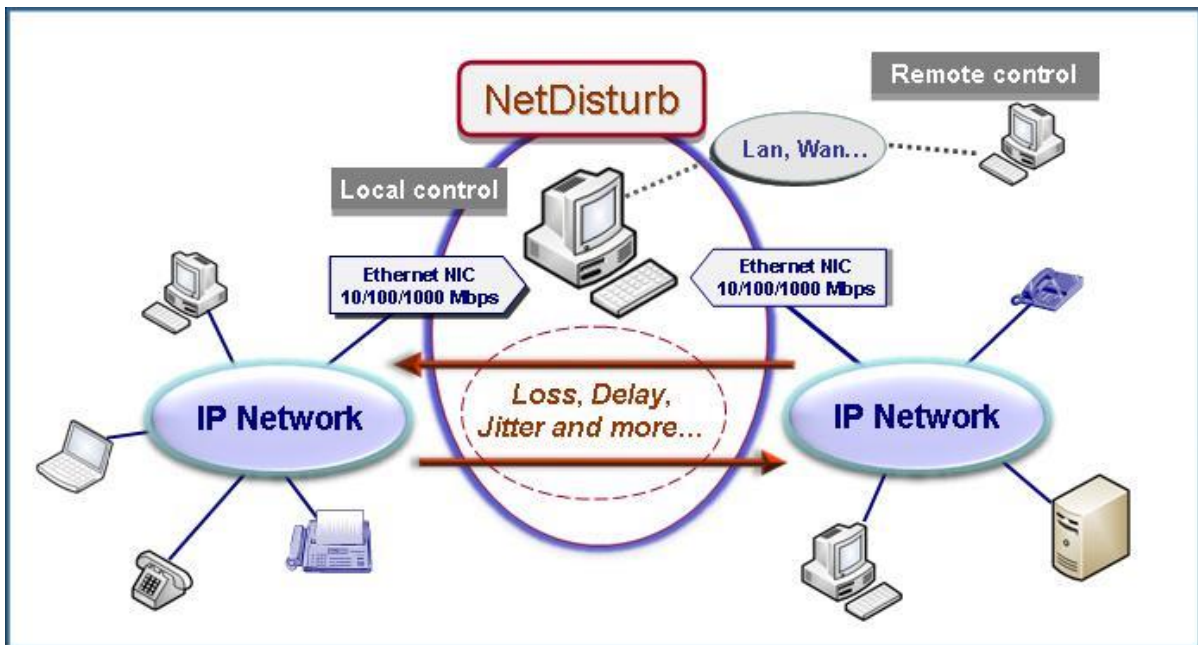
1.1   Product Requirements

*   Platform: 64-bit version of Windows Seven, 8, 10 or Server 2008R2 and upper with at least 3 GB Ram. 75 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) / 100% and Font size = Normal.

1.2   Typical Applications

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

- *Development assistance and debug of automatons for IP equipments:* particularly on Set-Top Boxes operating in cable or telecom environments.
- *Performance & Acceptance Tests:* Qualify and evaluate the behavior of IP equipments (phone, fax, gateway, set-top box, IMS core, call server, application server, residential gateway, ADSL wireless router, and more…) 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 the 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, and so re-create real world problems in the lab.
- *Applications test:* NetDisturb allows you to test applications such as Voice over IP, Fax over IP, streaming audio and video, IPTV, VoD, real time applications and services, and 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.

See some worldwide references of satisfied customers:

ABB Group, Agilent, Alcatel-Lucent, Alstom, ANZ Bank, AT&T, Bell Canada, Booz Allen Hamilton, Bose Corp., British Telecom, Broadcom, Catena Corp., Cisco, Commtech Wireless, Department of Defence, Detasad, DivX, Echelon, Equant, FAA, Fastweb, France Telecom, French Space Agency, Fuji Xerox, Gensight, Global Crossing, GlobeCast, Harris, Honeywell, ITT Corp., Iwatsu, Juniper Networks, KDDI, L-3 Communications, Leadtek, LG Electronics, Lockheed Martin, Microsoft, Motorola, NASA, NATO, NEC, NMS Communications, NSS, NTT, Orange, Panasonic, Philips, PIKA Technologies, Polycom, Psytechnics, Qualcomm, Raytheon, Rhode & Schwarz, Ricoh, Rothschild & Cie, Sagem, Samsung, Schlumberger, Scopus, Spawar, Sprint, Swisscom, T-Mobile, TdF, Tekelec, TeliaSonera, Telenor, TF1, Thales, Thomson Video Networks, Toshiba, UTStarcom, Vodaphone, WL Gore, Xerox, and more… as well as many universities and telecom institutes.

1.4   Key Features

With NetDisturb 7.0, two software editions are available: **Standard** and **Enhanced.** What are the major features of NetDisturb v7.0?

Common Key features for Standard and Enhanced Editions

- 64-bit Windows operating systems – Seven, 8, 10 Server 2008R2 and upper.
- Simultaneous support of **IPv4** and **IPv6**
- Client-Server Architecture based on the SOAP mechanism which uses the HTTP protocol and the XML format for the exchanges between the client and the server.
- NetDisturb is an **Ethernet Bridge** to avoid any network configuration.
- NetDisturb is an IP Router for WiFi NICs
- Use of standard Ethernet Network Interface Cards up to **1 Gbps or** WiFi card to make impairment.
- **Automatic start mode for new users with a set of predefined contexts (PING, TCP, UDP, HTTP, Video, etc.)**
- **Automatic discovery and configuration the NICs to use with NetDisturb.**
- Symmetric or Asymmetric **Bandwidth limitation** with Throughput Limitation laws.
- Very easy to use and intuitive 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
- Ethernet-type filter
- Enhanced RTP detection for Audio and Video SDP flows
- PTPv1 and PTPv2 (IEEE 1588) impairment at UDP and MAC layers
- **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
- Change of law parameters **on the fly** for a given flow (Percentage laws, Uniform Law parameters, etc.).
- Ability to **impair the remaining network traffic** that could be either only 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
- 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)
  - PTPv1 and PTPv2 (PTP Message Type)
  - 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.
- MOS impairment laws
- 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 table below summarizes the main differences between NetDisturb Standard edition and NetDisturb Enhanced edition.
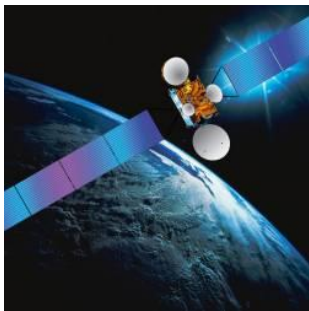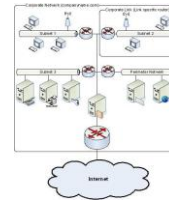
Features	NetDisturb Standard	NetDisturb Enhanced
Impairment of IPv4 and IPv6 packets, ARP and Ethernet frames	**Yes**	**Yes**
Automatic NIC configuration and Automatic Sample start mode	**Yes**	**Yes**
Filter parameters to define a flow: • Activity rules: - Start/Stop after a time limit or a packet counter or a pattern trigger - Loop to reapply the rule with delay between each iteration • Packet filters: Ethernet-type, Ethernet length, source address, destination address, source port, destination port, protocol, DSCP DiffServ (ToS), MPLS, VLAN, MAC address… • User-defined pattern filter based on Ethernet packet content	**Yes**	**Yes**
16 user-defined flows to impair using filters and 'Unfiltered Flows, Frames, Packets, etc.' to impair without using filters	**Yes**	**Yes**
Dynamically modify impairments on-the-fly per flow in each direction when running	**Yes**	**Yes**
Aggregates of flows (set of flows sharing the same delay and/or jitter laws)	**Yes**	**Yes**
View Per-Flow statistics and NICs statistics	**Yes**	**Yes**
Accuracy = 1 millisecond	**Yes**	**Yes**
Standard impairments: drop/loss, duplicate, delay (latency), jitter, bandwidth limiting, congestion, packet error, bit error, reorder, burst errors Delay from 1 millisecond up to 100 seconds in each direction Emulate bandwidth up to 1Gbps	**Yes**	**Yes**
Impairments by using the IP protocol field	**Yes**	**Yes**
Definition of flows to disturb based on protocol primitives:		
• ARP (ARP Operation Code)	No	**Yes**
• PTPv1 and PTPv2 (PTP Message Type)	No	**Yes**
• DHCP (DHCP Message Type)	No	**Yes**
• DNS (DNS Message Type, DNS Message Operation)	No	**Yes**
• FTP (FTP Command, FTP Returned Status)	No	**Yes**
• FTP-DATA	No	**Yes**
• HTTP (HTTP Method, HTTP Returned Status,)	No	**Yes**
• NTP	No	**Yes**
• RTP (Audio Payload Type, Video Payload Type, DTMF)	No	**Yes**
• SIP (SIP Method, SIP From, SIP To, SIP Returned Status)	No	**Yes**
• MOS impairment	No	**Yes**
Detailed events log per flow	No	**Yes**

1.6 Examples of Use

The following examples illustrate a subset of use cases implemented in various 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. Before 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.
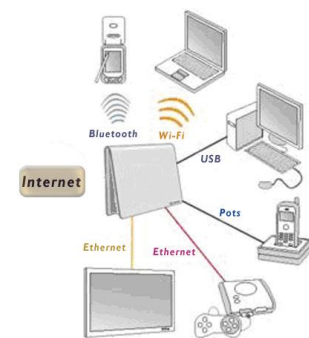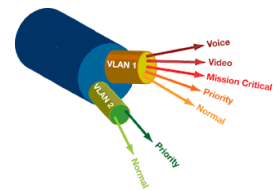
Tests of robustness for application protocols used in Triple Play Set-Top Box over DSL with NetDisturb Enhanced Edition

VoIP use case: for example, 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: for example, 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… .
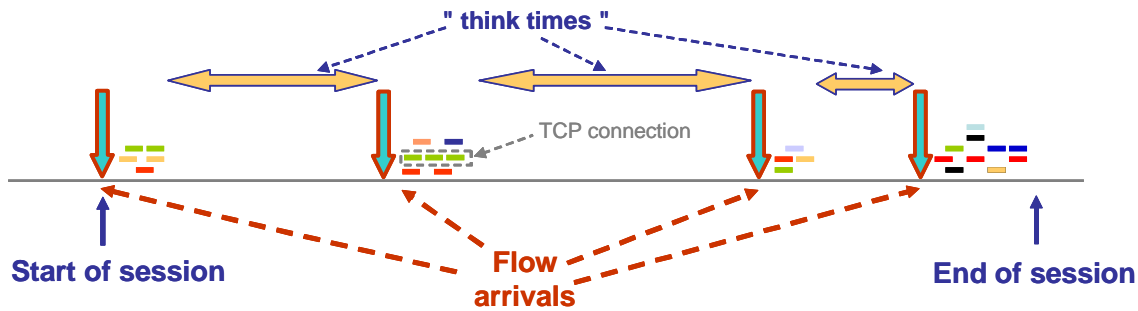
---

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 for 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
- Ethernet Packet type
- 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, PTP, 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 applying of the impairments.

With NetDisturb you can define up to 16 filters, i.e. 16 flows. An additional item named "Unfiltered Flows, Frames, Packets, etc." is in charge to handle all flows (IP or not) that have not been user defined. For this item no filter can be defined, but 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.
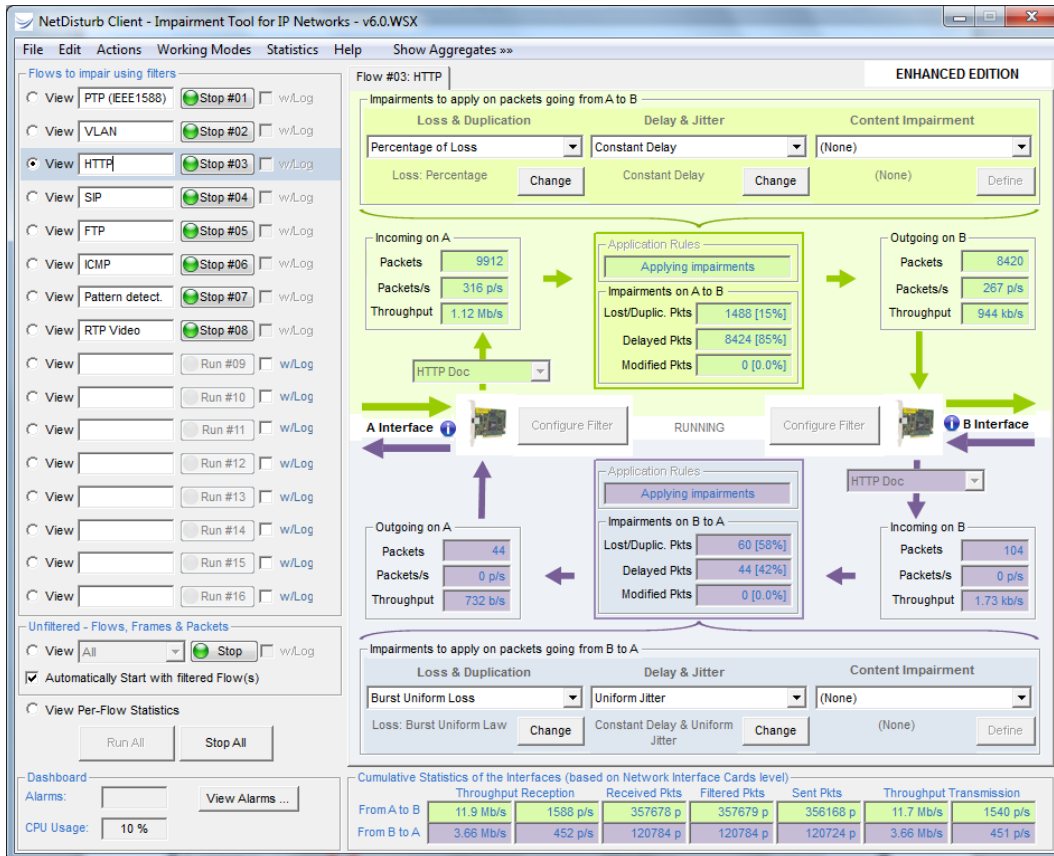
The graphical user interface represents the two NIC cards used by NetDisturb as "A Interface" and "B Interface" as illustrated below.
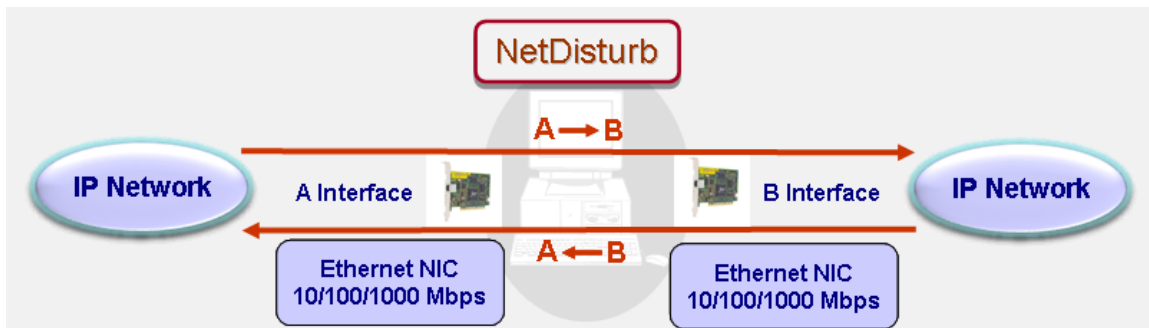
For each direction **A → B** or **B → A**, 16 flows can be defined by the user. And for each flow, loss or duplication, delay and jitter, and content impairment laws can be applied as shown in the figure below.
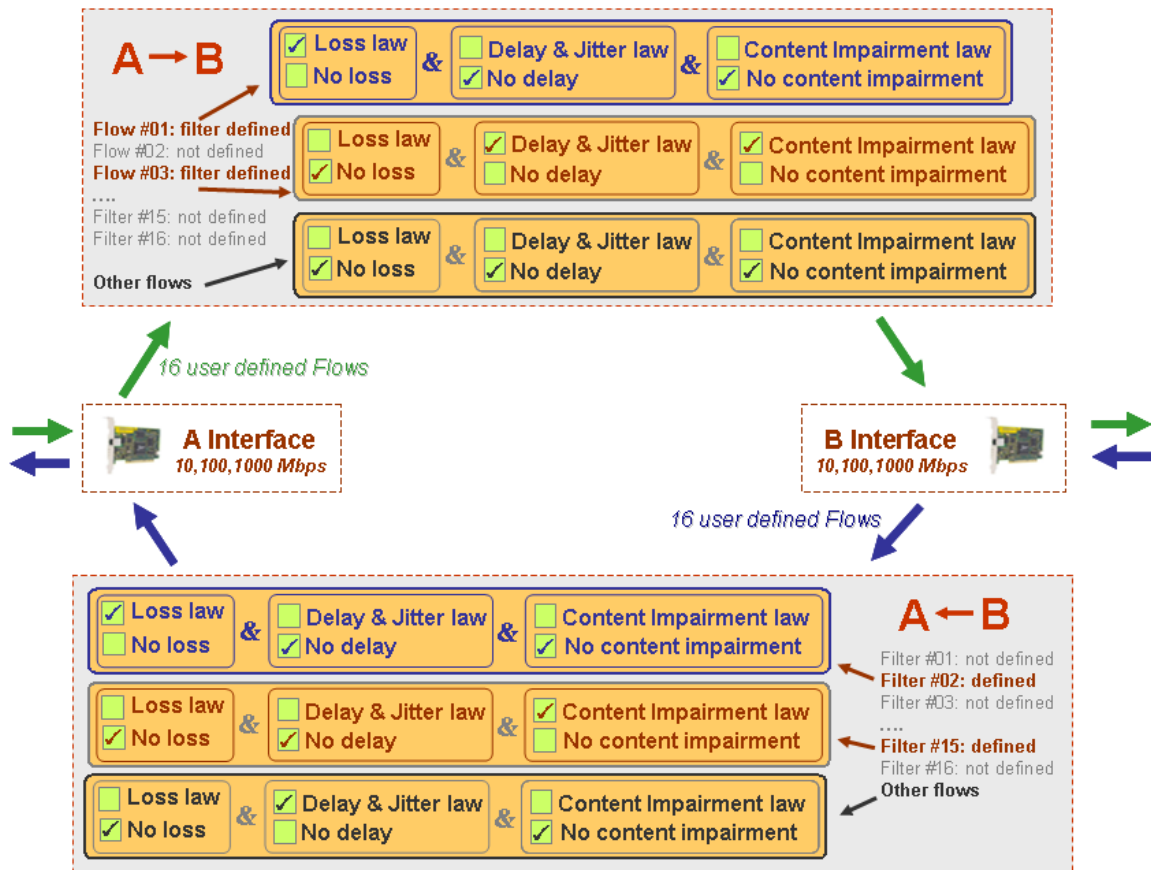
In the above example, NetDisturb has been configured with the following parameters:

Direction A → 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 'Unfiltered Flows, Frames, Packets, etc.', 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 'Unfiltered Flows, Frames, Packets, etc.', 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 B interface.
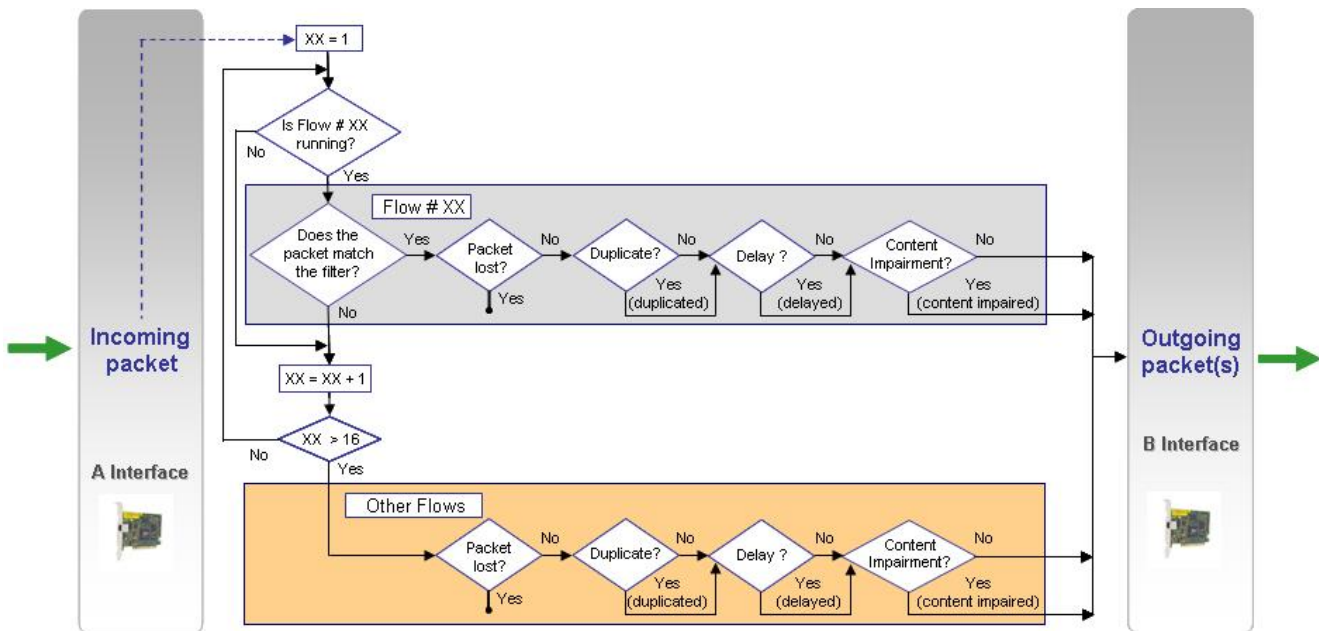
Depending on the active user-defined flows, NetDisturb checks the incoming packet against the filter of the flow before applying loss, delay or content impairment treatments.

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 treatments for the 'Unfiltered Flows, Frames, Packets, etc.' and based on the laws defined i.e. lost/duplicated, delayed and content impairment.

For each packet received on an interface, NetDisturb analyzes in order the filters from 1 to 16 before considering this packet belongs to the 'Unfiltered Flows, Frames, Packets, etc.'

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 'Unfiltered Flows, Frames, Packets, etc.' should 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
  - Ethernet type and length
  - VLAN
  - MPLS
  - IP (TCP/UDP)
  - Protocol primitives (only for Enhanced version): ARP, PTP, 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 several 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 because a delay is defined before applying the impairments. This state changes to the state "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 because 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 don't apply anymore. 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 facilitates defining filters including protocol primitives whose list is detailed below. So you can define precisely the exact primitive of the protocol to disturb if needed.

ARP
- ARP request
- ARP reply
- RARP request
- RARP reply
- DRARP request
- DRARP reply
- DRARP error
- InARP request
- InARP reply

DHCP
- DHCPDISCOVER   (BOOTP request)
- DHCPOFFER   (BOOTP reply)
- DHCPREQUEST   (BOOTP request)
- DHCPACK   (BOOTP reply)
- DHCPNACK   (BOOTP reply)
- DHCPDECLINE   (BOOTP request)
- DHCPRELEASE   (BOOTP request)
- DHCPINFORM   (BOOTP request)

DNS
DNS Message Type
- Query
- Response
DNS Message Operation
- QUERY
- IQUERY
- NOTIFY
- STATUS
- UPDATE

FTP
FTP Returned STATUS
- OK (200)
- Not Found (404)
- 1xx Series
- 2xx Series
- 3xx Series
- 4xx Series
- 5xx Series
FTP Command
- ABOR
- ACCT
- ALLO
- APPE
- CDUP
- CWD
- DELE
- EPRT
- EPSV
- FEAT
- HELP
- LIST
- MKD
- MODE
- NLST
- NOOP
- OPTS

FTP Command (cont.)
- PASS
- PASV
- PORT
- PWD
- QUIT
- REIN
- REST
- RETR
- RMD
- RNFR
- RNTO
- SITE
- SMNT
- STAT
- STOR
- STOU
- STRU
- SYST
- TYPE
- USER

FTP DATA

HTTP
HTTP Returned STATUS
- OK (200)
- Not Found (404)
- Moved (301)
- 1xx Codes
- 2xx Codes
- 3xx Codes
- 4xx Codes
- 5xx Codes
HTTP Method
- OPTIONS
- GET
- HEAD
- POST
- PUT
- DELETE
- TRACE
- CONNECT

NTP

PTP
- SYNC
- DELAY_REQ
- PDELAY_REQ
- PDELAY_RESP
- ANNOUNCE
- FOLLOW_UP
- DELAY_RESP
- PDELAY_RESP_FOLLOW_UP
- MANAGEMENT
- SIGNALLING

RTP
Audio Payload Type
- 0 PCMU
- 3 GSM
- 4 G723
- 5 DVI4
- 6 DVI4
- 7 LPC
- 8 PCMA
- 9 G722
- 10 L16
- 11 L16
- 12 QCELP
- 13 CN
- 14 MPA
- 15 G728
- 16 DVI4 (11,025 Hz)
- 17 DVI4 (22,050 Hz)
- 18 G729
Video Payload Type
- 25 CelB
- 26 JPEG
- 28 nv
- 31 H261
- 32 MPV
- 33 MP2T
- 34 H263
User-defined audio or Video
DTMF
RTP (SIP From)
RTP (SIP To)

SIP
SIP From
SIP To
SIP Returned STATUS
- OK (200)
- Trying (100)
- Ringing (180)
- Moved (301)
- 1xx Codes
- 2xx Codes
- 3xx Codes
- 4xx Codes
- 5xx Codes
- 6xx Codes
SIP Request
- INVITE
- ACK
- BYE
- CANCEL
- OPTIONS
- REGISTER
- PRACK
- SUBSCRIBE
- NOTIFY
- PUBLISH
- INFO
- REFER
- MESSAGE
- UPDATE

The following screenshot illustrates for example the parameters of a user-defined filter ("My New SIP Filter") for a SIP message ("REGISTER") that we want to disturb. This filter can be used for example to study the retransmission mechanism when a SIP REGISTER is lost by using NetDisturb with a Set-Top Box.
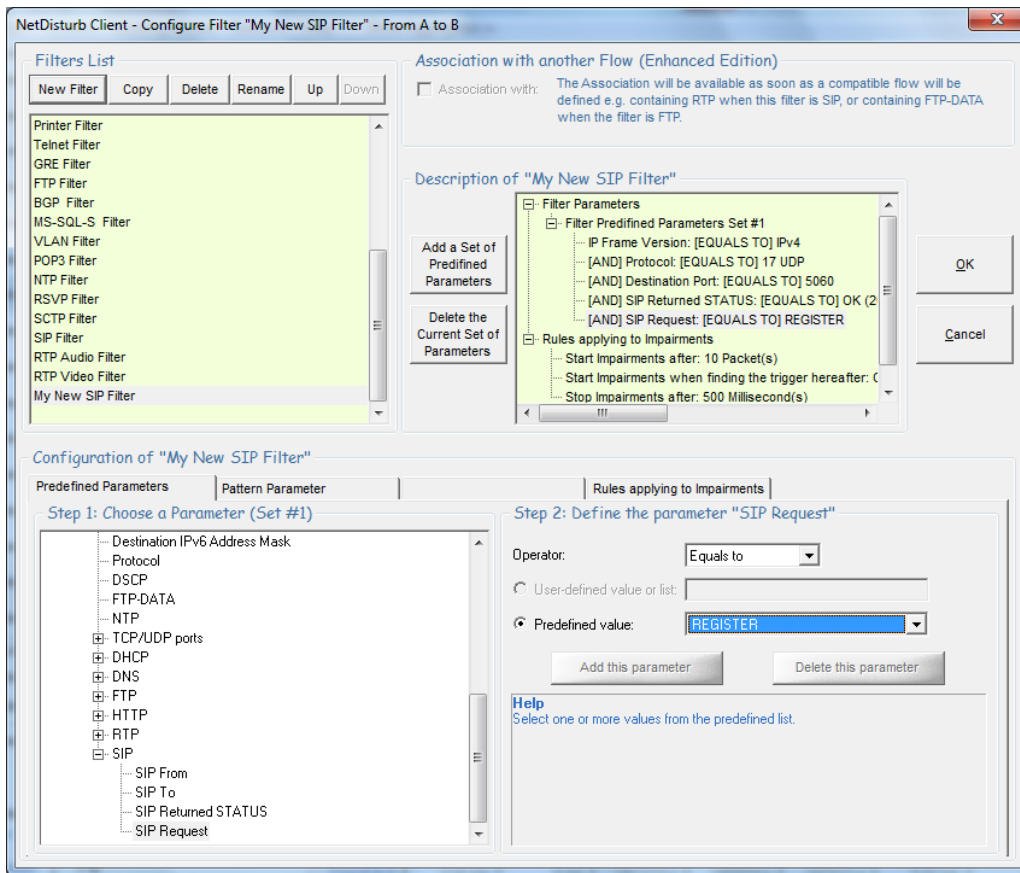
2.5   List of impairments

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

- Loss: based on MOS (VoIP)
  Parameters: MOS to reach

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

- Throughput Limit & Constant Delay
  Parameters: IP throughput, max memory, constant delay

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

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

- Uniform Jitter & Duration
  Parameter: Max Jitter, duration

- Throughput & Jitter & Duration
  Parameter: user file

Pre-defined Content impairment laws:

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

- Percentage
  Parameter: percentage, minimum burst, maximum burst

- 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 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 hasn't got this constraint regarding the packet order: some packets can use one route while others use another one, with the consequence the receiver may get packets unordered.
NetDisturb can 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 can dispatch IP packets into the TCP or UDP connection they belong to. This mode makes possible to apply the same impairment values to each packet of each connection.
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 previous 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 belongs to.

- *Impairment laws to be applied to each TCP/UDP connection of the IP flow*
When this option is selected, NetDisturb analyses each received packet in order to associate this packet to a TCP or UDP connection already existing by using these parameters: protocol, IP addresses and port numbers. If the connection doesn't exist, a new one is created. With the previous example of 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 the 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. While the top flow packets get the highest priority, the other flow packets are queuing 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)
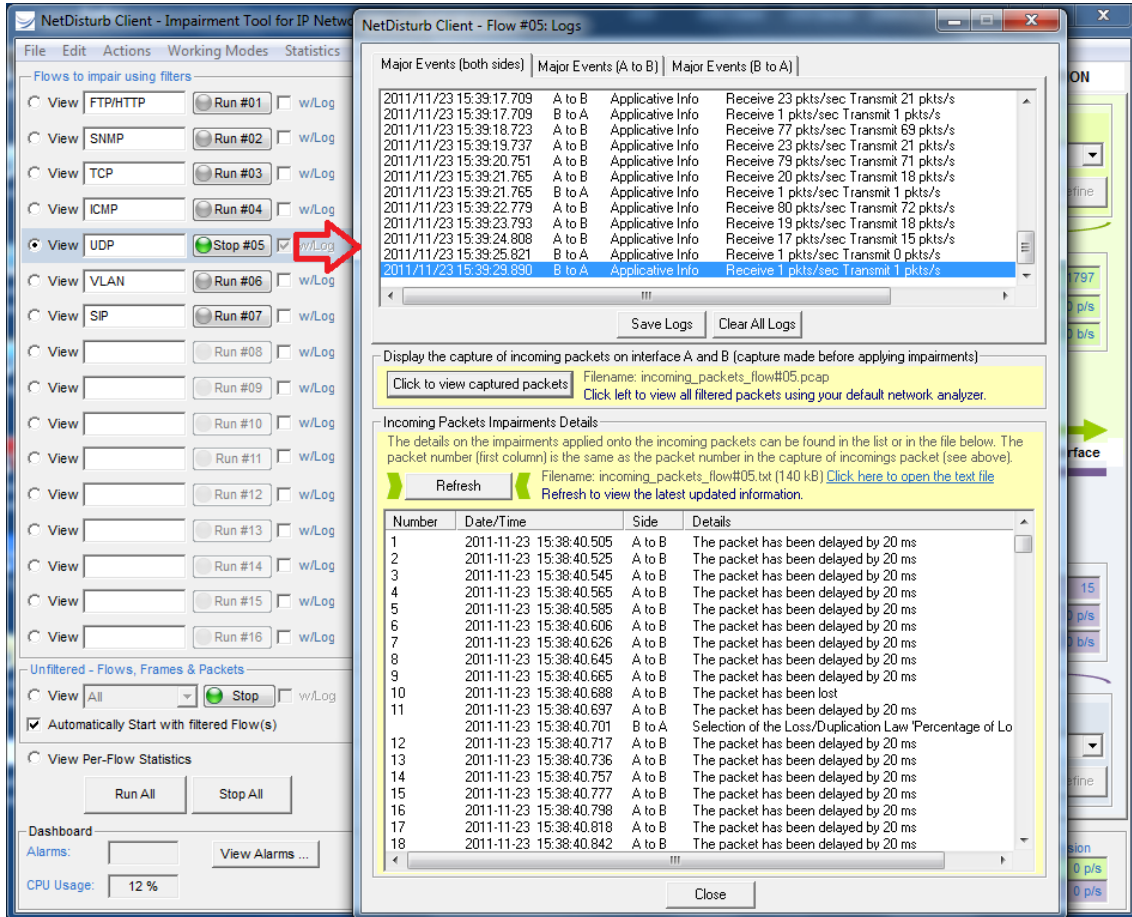- The dark blue colored aggregate collects the flows #05, #06 and #07.

2.7 Traces and logs (Enhanced Edition only)

Once a filter is defined for a flow, it's 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 when the option ☐ **w/Log** 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.
By using the opened log window when the flow is started by pressing the corresponding Run #xx button, you can:
- Display the major events for both directions (**A → B** and **B → A**).
- View the captured packets of the flow (for both directions) before applying impairments by using your default network analyzer launched automatically (for example: 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 w/Log 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).
- incoming_packets_flow#xx.txt for the flow No. xx (this text file contains the description of the impairment applied for each incoming packet for the two interfaces that is numbered and time-stamped by NetDisturb).

You can then examine very precisely by using these two files what 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 a later use.

Detailed statistics for each Flow

For each direction (A → B or B → A) NetDisturb displays:
- ① For the incoming interface: the number of received packets matching the filter, the number of received packets per second and the throughput
- ② For the impairments:
    - The number and percentage of lost or duplicated packets
    - The number and percentage of delayed packets
    - The number and percentage of modified packets
- ③ For the outgoing interface: the number of sent packets, the number of sent packets per second and the throughput
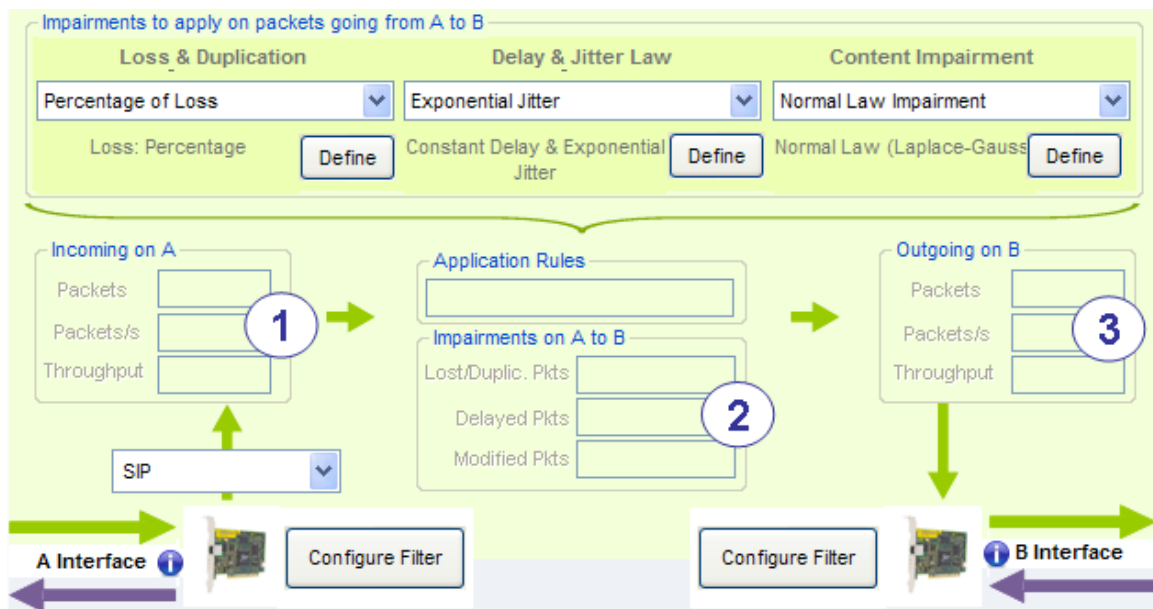
Summary table of Per-Flow statistics

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

View Per-Flow Statistics

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

Cumulative Statistics of the Interfaces (based on Network Interface Cards level)						
	Throughput Reception	Received Pkts	Filtered Pkts	Sent Pkts	Throughput Transmission	
From A to B	3.95 Mb/s	365 p/s	18295 p	18295 p	17187 p	3.56 Mb/s	332 p/s
From B to A	8.96 Mb/s	5945 p/s	316668 p	316667 p	285742 p	7.79 Mb/s	5072 p/s

Alarms

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

Incoming direction	Outgoing direction
• Number of lost packets • Number of lost bytes • Number of errors returned by the driver of the Network Interface Card • Number of missing buffers to let NetDisturb to get the incoming packets • Number of lost TCP/UDP connections due to the upper limit of connections handled by NetDisturb	• Number of lost packets • Number of packets lost due to the unplugged Network Interface Card • Number of lost bytes • Number of errors returned by the driver of the Network Interface Card

2.9   Configurations

Based on Client-Server architecture, NetDisturb software is made of two parts: NetDisturb Server and NetDisturb Client. NetDisturb Server handles the impairment characteristics and the Client manages the Server using a simple graphical interface.

There are two possible 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 dialogs with the Server by using 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.

Configuration No 1	Configuration No 2
PC Windows Seven, 8, 10, Server 2008R2 and upper *NetDisturb Client* **Client application and GUI** *NetDisturb Server* **Server application and GUI** **NetDisturb Driver 64-bit** **Ethernet NDIS driver** **Ethernet NIC (A)** **Ethernet NIC (B)** **LAN (A)** **LAN (B)** **Ethernet 10/100/1000 Mbps** **Ethernet 10/100/1000 Mbps**	**PC Windows Seven, 8, 10, Server 2008R2 and upper** *NetDisturb Client* **Client application and GUI** ⇕ *WAN / LAN* **PC Windows XP, Vista, Seven, Server 2003 or Server 2008** *NetDisturb Server* **Server application & GUI** **NetDisturb Driver 64-bit** **Ethernet NDIS driver** **Ethernet NIC (A)** **Ethernet NIC (B)** **LAN (A)** **LAN (B)** **Ethernet 10/100/1000 Mbps** **Ethernet 10/100/1000 Mbps**
Client and Server on the same PC	*Client and Server on two different PCs*

The NetDisturb driver is 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 Seven).

Example 1: use of 2 Fast Ethernet NICs
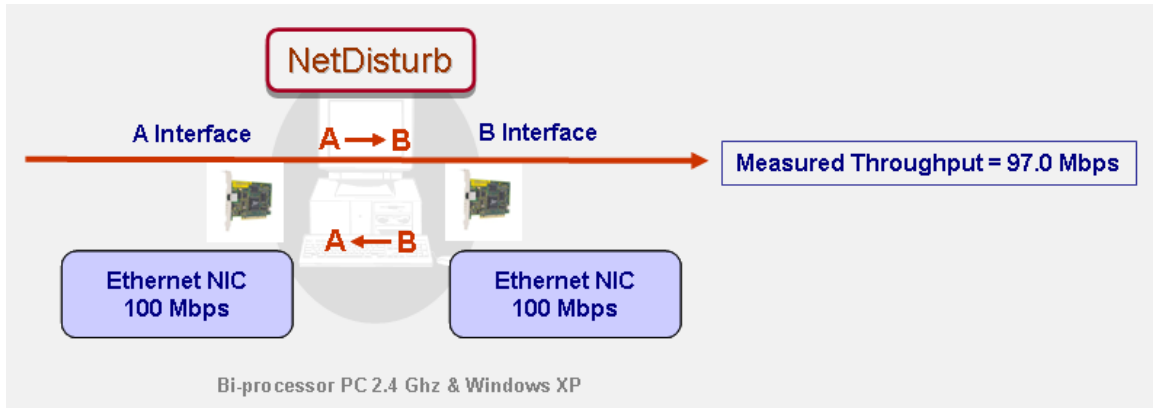
NetDisturb is configured with 16 flows (no loss and no delay for each flow).
With Fast Ethernet NICs, the throughput measured is 97 Mbps in one direction.

Example 2: use of 2 Gigabit Ethernet NICs
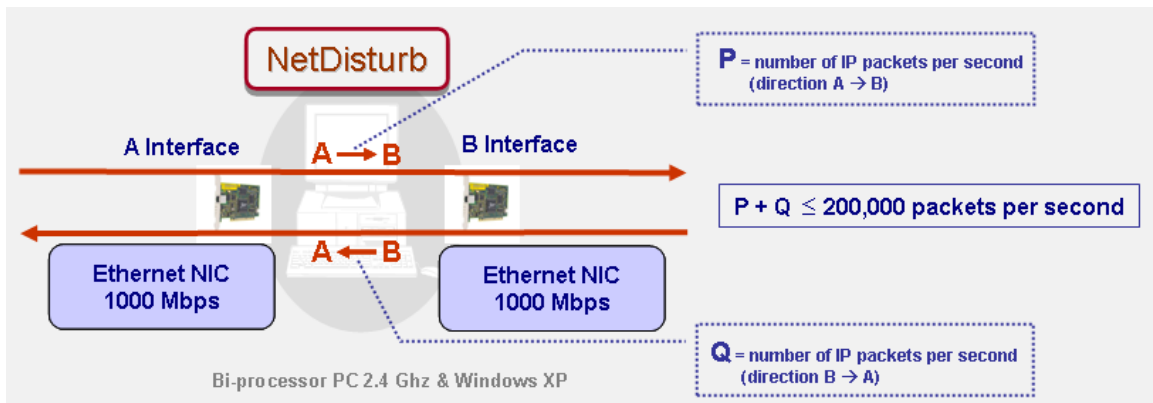
Measured incoming and outgoing throughput up to 980 Mbps
By using 2 Gigabit NICs, NetDisturb Standard Edition can handle up to 200,000 packets per second with 16 flows defined (for both directions).
Please refer for more detailed information to the "NetDisturb Performance Characteristics on Gigabits Networks" document.

These two examples show some performances of NetDisturb. This will avoid heavy investments in expensive hardware solutions.

2.11 Some publications and thesis mentioning 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".*

::: Raake, A*., ITU-T Delayed Contribution D.221 (2004). "E-Model: Additivity of Burst Packet Loss Impairment with other Impairment Types." Germany (Author: A. Raake). ITU-T SG 12 Meeting, CH-Geneva, 24-31 March 2004,* Institute of Communication Acoustics, University of Bochum, Germany, 2004

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

::: University of Western Ontario, London ON Canada, Canada, 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

::: Chen L., *An Adaptive Consistency Maintenance Approach for Replicated Continuous Applications*, 11th International Conference on Parallel and Distributed Systems (ICPADS'05), College of Computer Science, Zhejiang University, Hangzhou 310027, P.R. China, 2005.
Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on
Volume 1, 20-22 July 2005 Page(s):795 - 801

::: Chen L., *Effects of Network Characteristics on Task Performance in a Desktop CVE System,* 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers), College of Computer Science, Zhejiang University, Hangzhou 310027, P.R. China, 2005, Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on
Volume 1, 28-30 March 2005 Page(s):821 – 826 vol.1

::: *Effects of Latency on Telesurgery: An Experimental Study*
Authors: Reiza Rayman[1], Serguei Primak[2], Rajni Patel[2], Merhdad Moallem2, Roya Morady1,
Mahdi Tavakoli2, Vanja Subotic2, Natalie Galbraith2, Aimee van Wynsberghe1 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
Book: Medical Image Computing and Computer-Assisted Intervention – MICCAI 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

::: Broderick T.J., *NASA Extreme Environments Mission Operations – Evaluation of Robotic and Sensor Technologies for Surgery in Extreme Environments*, University of Cincinnati, Ohio, USA, 2006
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).

::: Staroniewicz P., Majewski W., *Methodology of Speaker Recognition Tests in Semi-real VoIP Conditions*, Institute of Telecommunications, Teleinformatics and Acoustics, Wroclaw University of Technology, Poland, 2006

::: Westermark, C., *Mobile Multiplayer Gaming*, Master of Science Thesis, Stockholm, Sweden 2007 Quality of gaming experience by using NetDisturb to emulate different controlled network parameters.

::: Network Technology Seminar 2007 "**To IP and beyond**", EBU (European Broadcasting Union) International Training, Switzerland, Geneva, 2007.

::: Weckert P., *Experimentelle Untersuchung der Ableitbarkeit von Dienstgütezuständen aus Messgrößen der optischen Netze,* Institut für Informatik, München, Germany, 2008.

::: 3GPP Technical Specification Group Services and System Aspects TSG-S4
- Test Plan for the Adaptative 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 that is simulated for these tests.
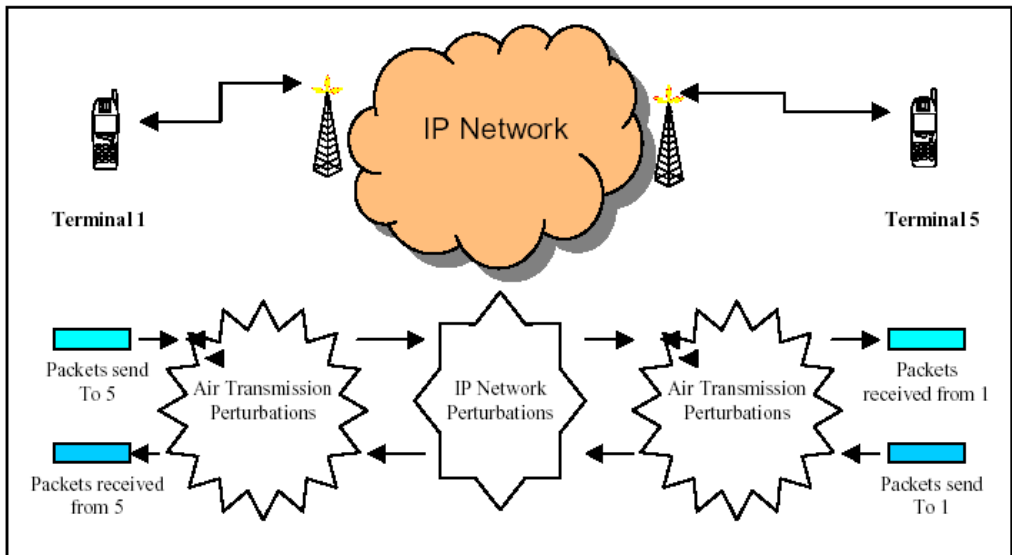
Packet switch audio communication simulator

This is simulated by using 5 PCs as shown below, with PC# 3 using NetDisturb as network simulator.
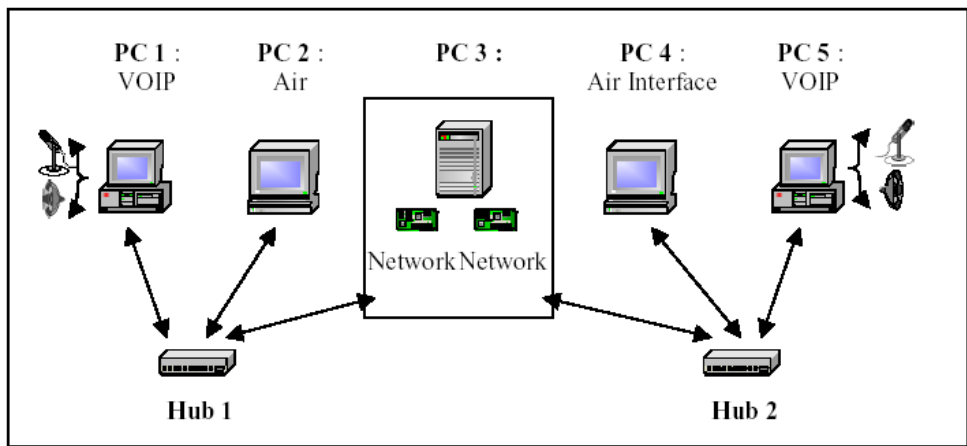
Simulation platform

3   Conditions of use

NetDisturb software (Standard or Enhanced edition) is composed of two parts: **Server** and **Client**. NetDisturb **Server** is licensed on a per workstation basis, and you can install NetDisturb **Client** on the same PC or on several PCs (only one instance of NetDisturb **Client** can be used with NetDisturb **Server** at a given time).
*Note: in most cases, **Server** and **Client** are installed on the same PC (default installation of software).*
You can install NetDisturb **Server** on several PCs, but you need a valid license for each PC where you want to use it.

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 ZTI Communications sales:

    Mob   +33 6 6218 4343
    Email sales@zti-communications.com

or email the technical support for a prompt answer: support@zti-communications.com

To download the trial version of NetDisturb**,** please visit us at www.zti-communications.com

ANNEX: GLOSSARY OF TERMS

Bandwidth Throttling
Bandwidth throttling 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-directional 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.
Jitter particularly affects the performance of real time network applications such as streaming video and audio. In these types of applications, data needs to arrive at a specific time frame or it becomes useless. As a result, many streaming audio and video application can be severely impacted by high jitter.

Latency (End-to-End Delay)
Latency is defined as the period of time it takes 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 which boils down to 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. This typically 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: is caused by errors in the physical layer, which 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 ordering.

Packet Loss

Packet loss is a normal phenomenon on packet networks: when data transmitted from an originating device don't arrive at the 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 of the transmission time of data to the reception time at the other end).

Quality of Service (QoS)

A list of measurable attributes that 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.