



NetDisturb

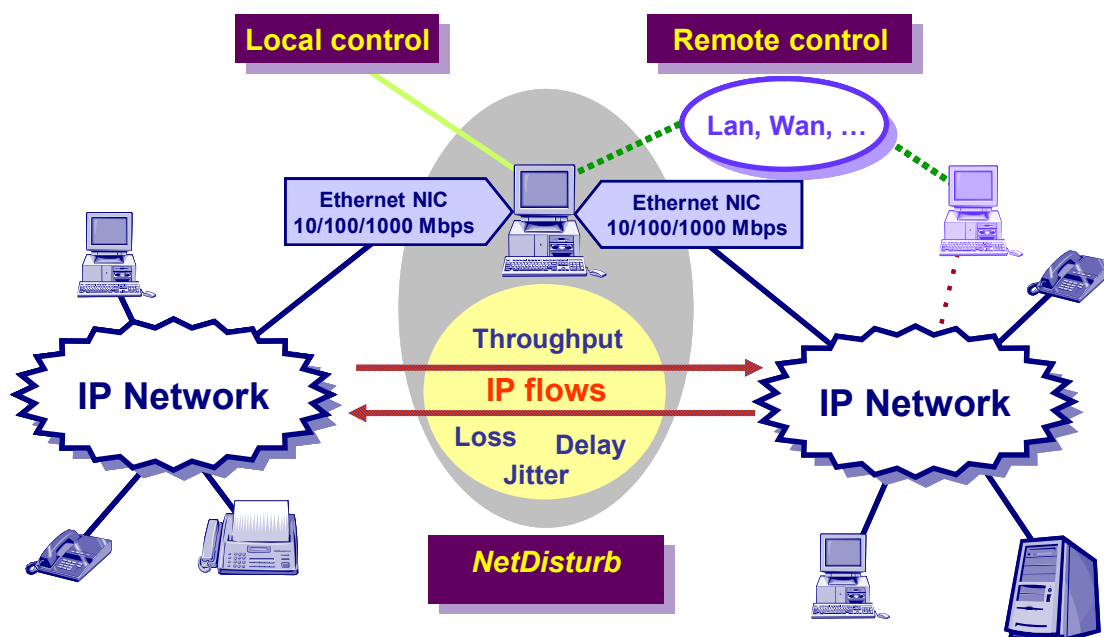
Version 4.2

Impairment emulator software for IP Networks

Overview

NetDisturb is an IP network emulator software that can generate impairments (latency, delay, jitter, limited bandwidth, lost and duplicate packets) over IP networks. NetDisturb allows the user to disturb flows on an IP network and so to study the behavior of applications, devices or services in a disturbed network environment.

NetDisturb is inserted between two Ethernet segments (on the same IP network or two different IP networks) and operates bi-directional packet transfer on Ethernet, Fast Ethernet and Gigabit network interface cards.



Product Requirements

- * Platform: PC running Windows NT4 (SP6), 2000 or XP with Microsoft TCP/IP installed and at least 256 MB Ram.
- * PC multiprocessors and hyper-threading supported.
- * Display: 1024 x 768 min. resolution.
- * Two Identical Network Interfaces Cards (NIC): Ethernet, Fast Ethernet, or Gigabit Ethernet network interface card.

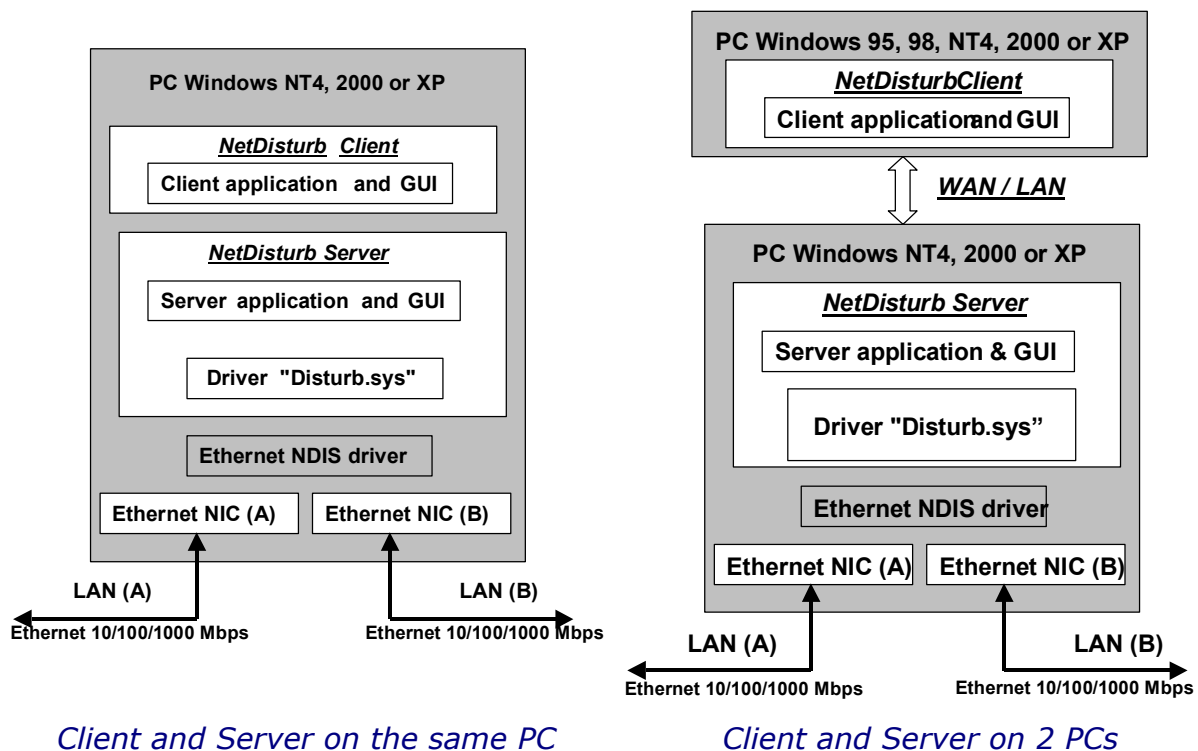


Configurations

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

This allows two configurations where the Server and Client parts may be installed on the same PC host (local control) or the Server part resides on one PC and the Client part resides 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 LAN link.

Both configurations require two identical Ethernet Cards for the Server.



The "Disturb.sys" NetDisturb driver sets 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.

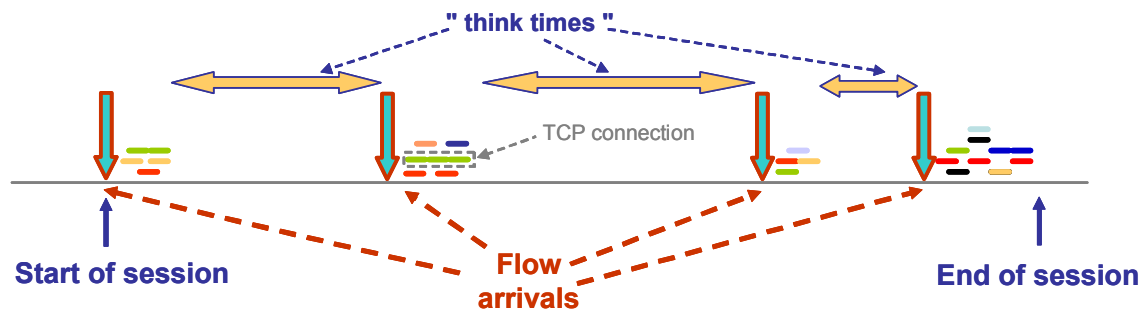
Products features

What are the major features of NetDisturb V4?

NetDisturb V4 is based on the notion of IP flows.

A flow is a set of packets with a set of common packet properties, and can be unidirectional or bidirectional.

Flows are part of sessions (successions of flows and "think times") relating to some homogeneous user activity (e-commerce, mail, MP3 file, web, ...)



An IP flow is described by using a n-tuple. In the typical case, the following 5-tuple is used: IP addresses, protocol and port numbers.

An IP flow is composed of connections (such as TCP connections to realize a FTP transfer by example).

To define the n-tuple for an IP flow, NetDisturb introduces the notion of mask.

A mask is the combination of the following optional parameters:

Ethernet header

- MAC destination address
- MAC source address

List of VLAN-ID (Ethernet frames 802.1Q)

IP Header

- Type of Service (TOS)
- Protocol (ICMP, TCP, UDP, SIP, ...)
- Destination IP address
- Source IP address

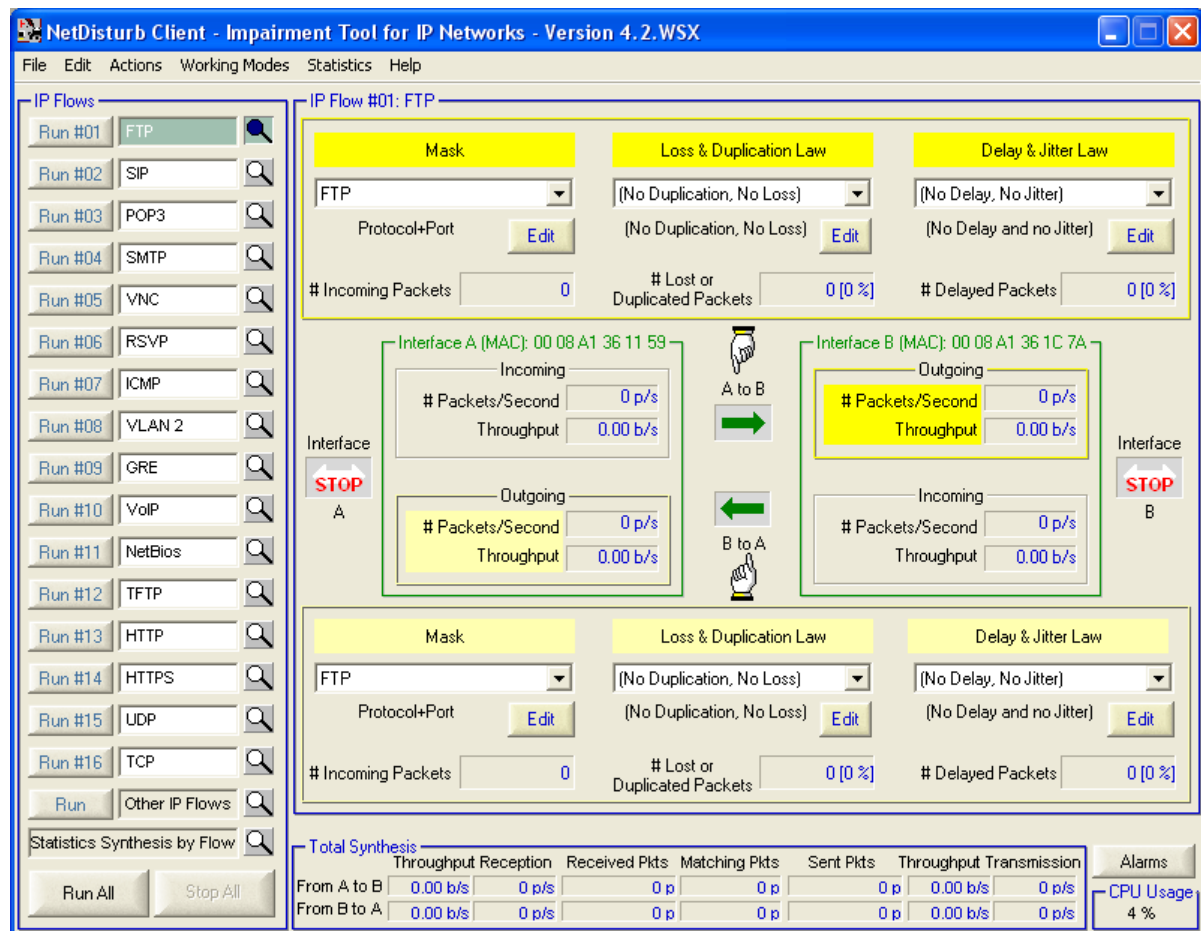
List of Ports (for TCP or UDP packets)

- Destination port list
- Source port list

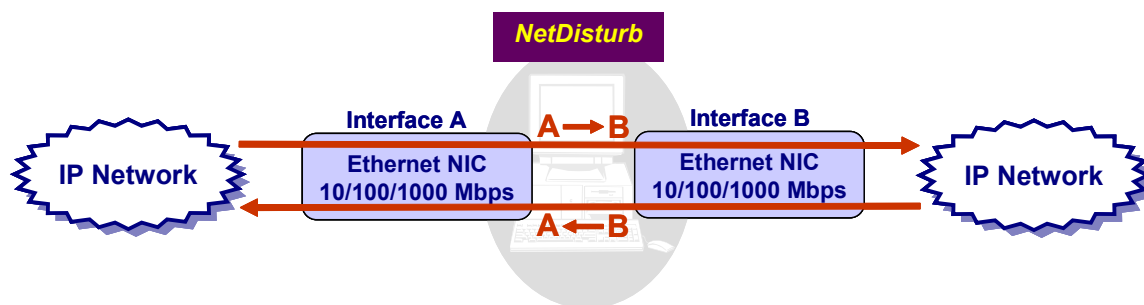
With NetDisturb, the user defines up to 16 masks, i.e. 16 IP flows. An additional item named "Other IP Flows" is in charge to handle all IP flows that have not been user defined. For this item, no mask can be defined, but impairments can be applied.

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

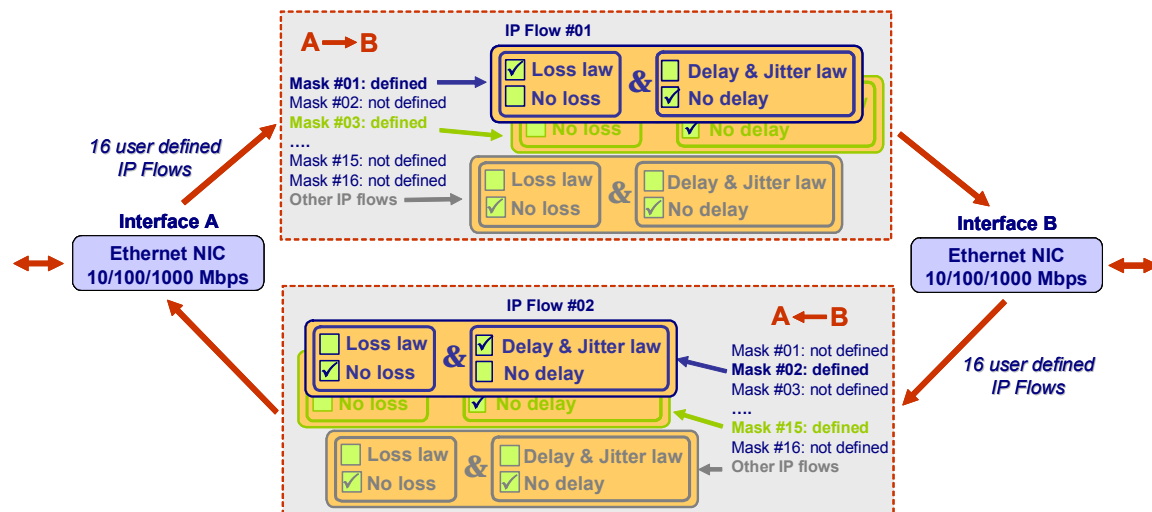
The client window below illustrates the management of IP flows by NetDisturb.



The graphical user interface represents the NIC cards as "Interface A" and "Interface B" as illustrated below.



For each direction $A \rightarrow B$ or $B \rightarrow A$, 16 flows can be defined by the user. And for each IP flow, loss and / or delay 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

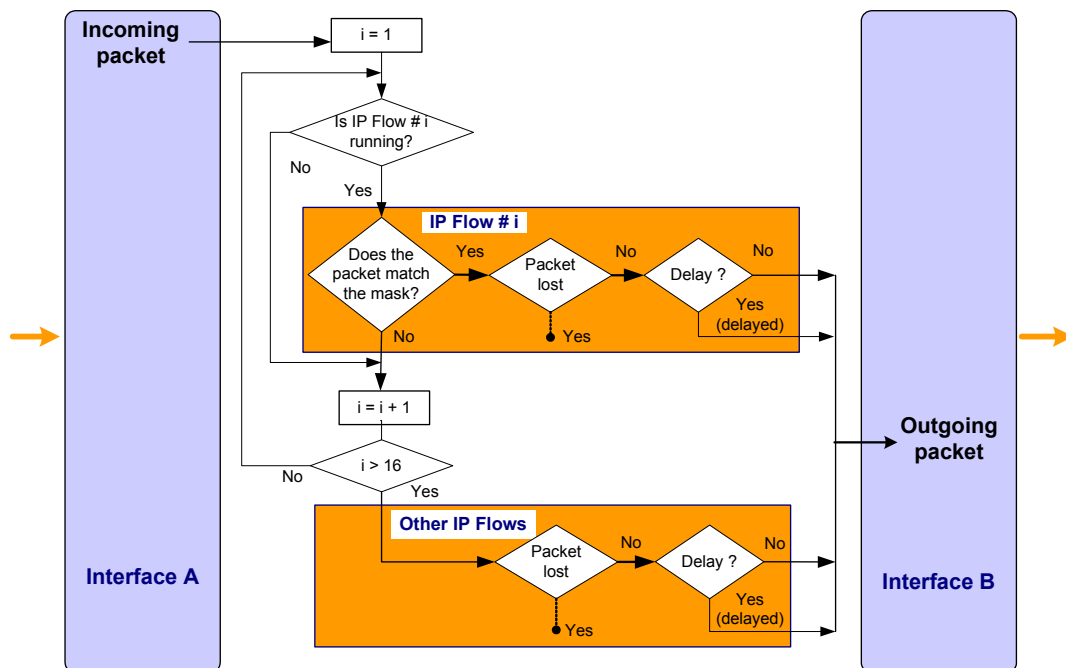
- the Mask #01 defines the "IP Flow #01", and a loss law is applied to the packets of this flow,
- the Mask #03 defines the "IP Flow #03", and a loss law is applied to the packets of this flow,
- As no loss and delay law is applied to the 'Other IP flows', all packets that don't match the masks #01 and #03 are relayed directly from the interface A to B.

Direction B → A

- the Mask #02 defines the "IP Flow #02", and a delay law is applied to the packets of this flow,
- the Mask #15 defines the "IP Flow #15", and a loss law is applied to the packets of this flow,
- As no loss and delay law is applied to the 'Other IP flows', all packets that don't match the masks #02 and #15 are relayed directly from the interface B to A.

How does it work?

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



Depending of the active user-defined IP flows, NetDisturb identifies if the incoming packet belongs to an IP flow before applying loss or delay treatments. If this packet matches with the mask of an IP Flow (IP Flow #i for example), then NetDisturb identifies if this packet must be lost or delayed.

If this packet does not match any mask (a mask defines an IP flow), then NetDisturb applies the treatments for the 'Other IP Flows' and identifies if this packet must be lost or delayed.

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

So, NetDisturb can apply impairments on the IP flows defined by the user either unidirectional ($A \rightarrow B$ or $B \rightarrow A$) or bidirectional (the same impairments apply for the two directions: $A \rightarrow B$ and $B \rightarrow A$).

Key features

- Client-Server Architecture
- 16 configurable IP flows per direction
- Unidirectional or bidirectional packet impairments with pre-defined mathematical laws or user defined files
- Connections per IP flow: impairments are applied to the IP flow or to each connection of the IP flow
- Ethernet / Internet modes (desequencing of the packets)
- Easy to use and intuitive Graphical User Interface
- Statistics display
- Multiprocessor support

Packet impairments

Pre-defined loss and duplication laws:

- Constant loss law
Parameter: number of packets
- Uniform Loss law: $f(x) = dx/(\beta - \alpha)$
Parameters: alpha, beta, threshold
- Burst Uniform Loss law: $f(x) = dx/(\beta - \alpha)$
Parameters: α , β , threshold(n), threshold(n + x), depth
- User-defined Loss File
Parameters: file name, threshold
- Percentage Loss law
Parameter: percentage
- 1/N Loss law: 1 packet is lost every N Packets received
Parameter: range(N)
- Percentage duplication law: send n times the received packet
Parameters: percentage, $\text{Min} \leq n \leq \text{Max}$
- 1/M duplication law: duplicate 1 packet n times every M packet received. Parameters: range(M), $\text{Min} \leq n \leq \text{Max}$
- Uniform Duplication law: $f(x) = dx/(\beta - \alpha)$
Parameters: alpha, beta, threshold
- 1/N Loss then 1/M duplication law: duplicate 1 packet n times every M packet received and not lost.
Parameters: range(N), range(M), $\text{Min} \leq n \leq \text{Max}$

Pre-defined Delay & Jitter laws:

- Constant Delay & No Jitter
Parameter = constant delay
- Constant Delay & Exponential Jitter law: $f(x) = \lambda e^{-\lambda x} dx$
Parameters: constant delay, λ
- Constant Delay & Uniform Jitter law: $f(x) = dx/(\beta - \alpha)$
Parameters: constant delay, alpha, beta
- Constant Delay & User File with Jitter values
Parameters: constant delay, user file
- User File with Delay & Jitter values
Parameter: user file

- Router Simulation & Constant Delay
Parameters: IP throughput, constant delay, max memory
- Router Simulation & User File with Delay and Jitter values
Parameters: user file, IP throughput, max memory

Working modes

Two working modes are offered by NetDisturb to apply impairments:

- Enable/Disable desequencing of the packets in a flow
- Impairment laws apply to the flow or for each connection of the flow

These modes are used jointly.

For example, NetDisturb is set with the following modes:

- Enable desequencing of the packets in a flow
- Impairment laws apply to the flow

to simulate the Internet network with disturbed flows.

Another example is to use the following modes:

- Disable desequencing of the packets in a flow
- Impairment laws apply to each connection of the flow

to disturb VoIP communications in the same way on an Ethernet network.

Enable/Disable Desequencing Packets

Impairment may introduce changes in the packet sequence – by introducing different delays for the packets of a flow for example.

One of the Ethernet characteristics is to keep packets received in order. Internet hasn't this constraint regarding the packet ordering: some packets can use one route while others another one, with the consequence the receiver may get packets unordered.

NetDisturb can simulate the Internet network (enable desequencing packets) or can react as Ethernet does (disable desequencing packets).

Impairment laws apply to the flow or to each connection of the flow

NetDisturb can analyze IP packets to split them 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.

Let us suppose that this impairment has been defined with a loss law: lose the third packet for 10 packets received.

- *Impairment laws apply to the flow*

When this option is selected, every received packet matching the mask 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 it belongs to.

- *Impairment laws apply to each connection of the 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 10000 connections can be handled simultaneously by NetDisturb.

A flow disappears automatically when the TCP connection is closed and after a configurable inactivity time for the UDP connection.

Statistics & Alarms

Different statistics are computed and displayed by NetDisturb:

- for each IP Flow (and for both directions)
- Statistics synthesis by Flow
- Total synthesis & Alarms

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

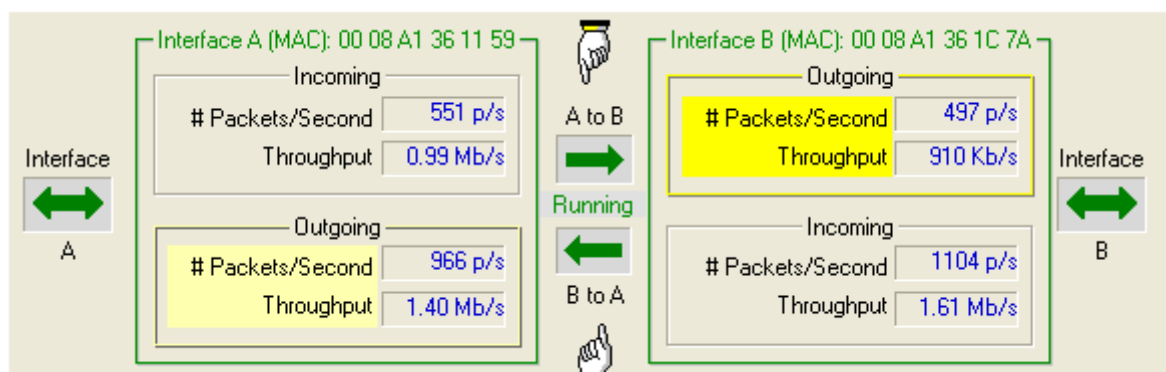
Statistics for each IP Flow

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

- number of packets matching the mask
- number and percentage of lost packets
- number and percentage of delayed packets

Mask	Loss & Duplication Law	Delay & Jitter Law
TCP	Duplicated if not Lost	Exponential Jitter
Protocol	Loss then Duplicate 1/10 & 1/20	Delay & Exponential Jitter From 20ms to 72ms
# Incoming Packets	# Lost or Duplicated Packets	# Delayed Packets
17191	1719 [10 %]	15472 [90 %]

and a complete view of traffic statistics (number of packets and throughput) over the A and B interfaces as shown below:



Statistics synthesis by Flow

The complete synthesis for all IP flows displays for each flow and for each direction:

- the incoming throughput and number of received packets per second
- the number of packets matching the mask
- the number of lost packets
- the number of delayed packets
- the outgoing throughput and number of sent packets per second

NetDisturb Client - Impairment Tool for IP Networks - Version 4.2.WSX

File Edit Actions Working Modes Statistics Help

IP Flows

IP Flows	%	Incoming Throughput	Incoming Pkts	Lost Pkts	Delayed Pkts	Outgoing Pkts	Outgoing Throughput
#01 A to B	4	263 Kb/s	36 p/s	1051	0 [0 %]	1016	246 Kb/s
#01 B to A	1	282 Kb/s	44 p/s	1194	0 [0 %]	1194	282 Kb/s
#02 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#02 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#03 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#03 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#04 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#04 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#05 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#05 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#06 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#06 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#07 A to B	0	592 b/s	1 p/s	52	0 [0 %]	52	592 b/s
#07 B to A	0	592 b/s	1 p/s	126	0 [0 %]	126	592 b/s
#08 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#08 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#09 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#09 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#10 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#10 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#11 A to B	0	0.00 b/s	0 p/s	1	0 [0 %]	1	0.00 b/s
#11 B to A	0	0.00 b/s	0 p/s	1	0 [0 %]	1	0.00 b/s
#12 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#12 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#13 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#13 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#14 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#14 B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#15 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#15 B to A	0	0.00 b/s	0 p/s	14	0 [0 %]	14	0.00 b/s
#16 A to B	96	925 Kb/s	455 p/s	27571	0 [0 %]	27312	903 Kb/s
#16 B to A	98	3.88 Mb/s	699 p/s	80169	0 [0 %]	80169	3.88 Mb/s
..... A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
..... B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s

Total Synthesis

	Throughput Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput Transmission	Alarms
From A to B	1.16 Mb/s	491 p/s	28675 p	28381 p	1.12 Mb/s	487 p/s
From B to A	4.16 Mb/s	745 p/s	81630 p	81504 p	4.16 Mb/s	745 p/s

CPU Usage: 18 %

Statistics synthesis by Flow - example

Total synthesis

At the bottom of the Client window, the total synthesis displays the following parameters for both directions (A → B or B → A):

- Throughput and number of packets per second received
- Number of packets received
- Number of matching packets
- Number of packets sent
- Throughput and number of packets per second transmitted

Total Synthesis							Alarms
	Throughput Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput Transmission		
From A to B	1.16 Mb/s	491 p/s	28675 p	28381 p	1.12 Mb/s	487 p/s	CPU Usage 18 %
From B to A	4.16 Mb/s	745 p/s	81630 p	81504 p	4.16 Mb/s	745 p/s	

Alarms

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

<i>Incoming direction</i>	<i>Outgoing direction</i>
<ul style="list-style-type: none"> • Number of lost packets • Number of lost bytes • Number of errors returned by the Driver at the Interface • Number of missing buffers to keep packets • Number of ignored flows (when the multi-flows option is active). 	<ul style="list-style-type: none"> • Number of lost packets • Number of lost bytes • Number of errors returned by the Driver at the interface

NetDisturb Client - Alarms Summary

Alarms Linked to the Direction from Interface A to Interface B

Incoming on A	A to B	Outgoing to B
# Packets Lost: 0	 Details	# Packets Lost: 0
# Bytes Lost: 0		# Bytes Lost: 0
# Driver Errors: 0		# Driver Errors: 0
# Buffer Missing Errors: 0		
# Flows Exceeded: 0		

Alarms Linked to the Direction from Interface B to Interface A

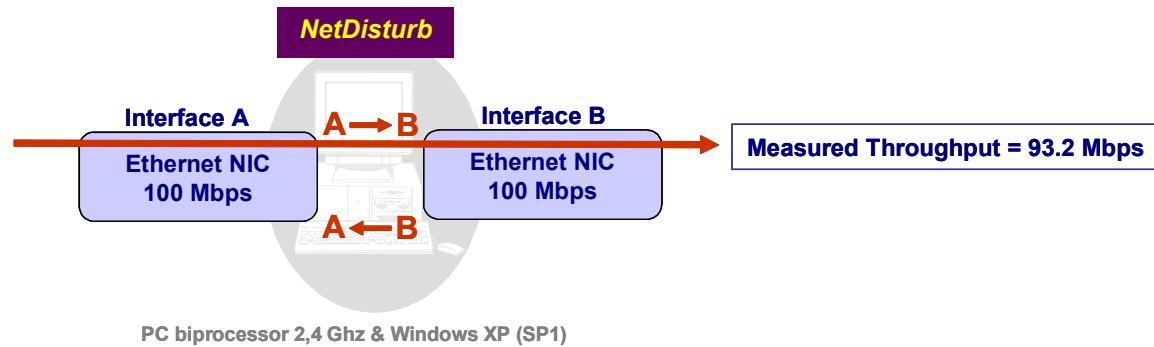
Outgoing to A	B to A	Incoming on B
# Packets Lost: 2	 Details	# Packets Lost: 0
# Bytes Lost: 596		# Bytes Lost: 0
# Driver Errors: 2		# Driver Errors: 100
		# Buffer Missing Errors: 0
		# Flows Exceeded: 0

[OK](#)
[Clear Alarms](#)
[Update Alarms Summary](#)

Performances

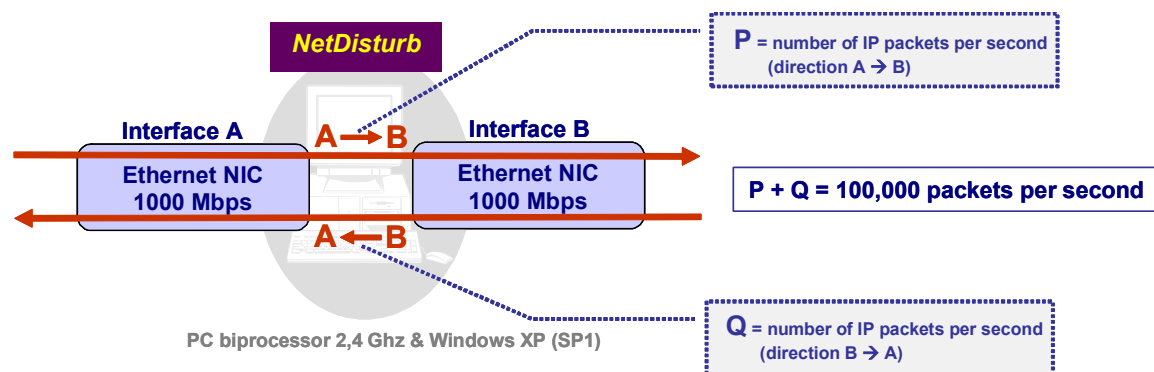
To illustrate the key performances of the NetDisturb software, 2 examples are presented hereafter (by using a PC biprocessor 2,4 Ghz with windows XP SP1).

Example 1: use of 2 Fast Ethernet NICs



NetDisturb is configured with 16 IP flows (no loss and no delay for each flow). With Fast Ethernet NICs, the throughput measured is 93.2 Mbps in one direction.

Example 2: use of 2 Gigabit Ethernet NICs



By using 2 Gigabit NICs, NetDisturb handles up to 100,000 packets per second with 16 IP flows defined (for both directions).

These two examples show an extract of the NetDisturb performances, thus avoiding investing in expensive hardware solutions.

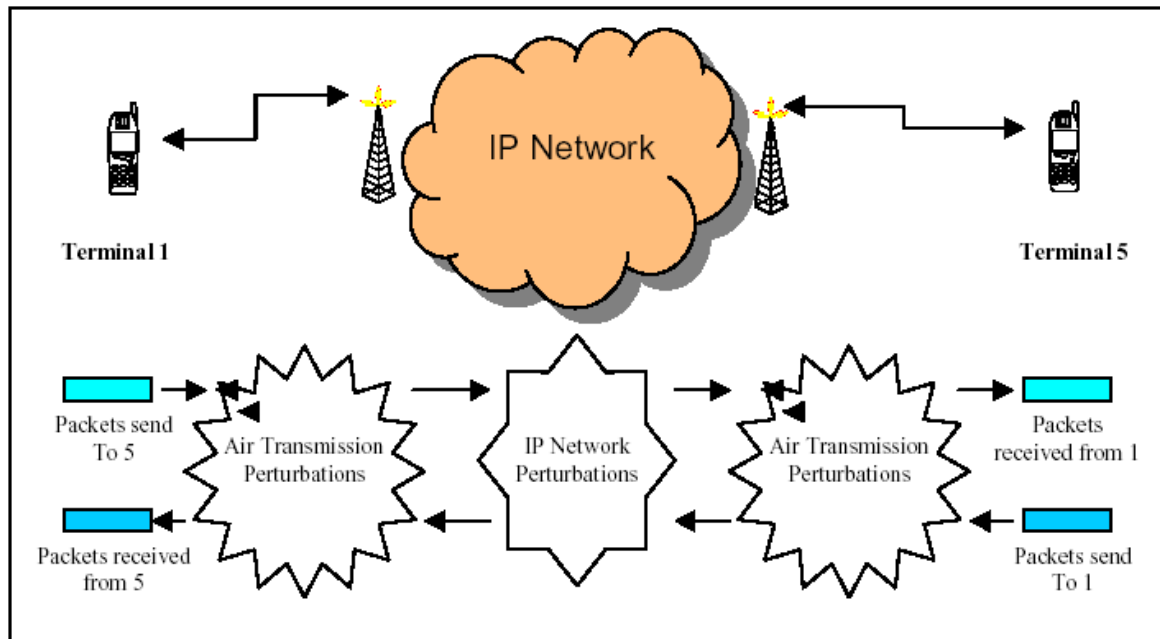
Applications

- **Performance & Acceptance Tests:** Qualify and evaluate the behavior of IP equipments (phone, fax, gateway, ...) 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, delay) defined by the user, and so re-create real world problems in the lab.
- **Applications test:** NetDisturb allows testing applications such as Voice over IP, streaming audio and video, and other distributed applications.
- **Emulation of symmetric or asymmetric network conditions (Lan, Man, Wan):** latency, jitter, packet loss, bandwidth limitations, ... to test IP applications (VoIP, streaming audio & video, ...), services and products sensitive to various real conditions.

Some publications mentioning the use of NetDisturb

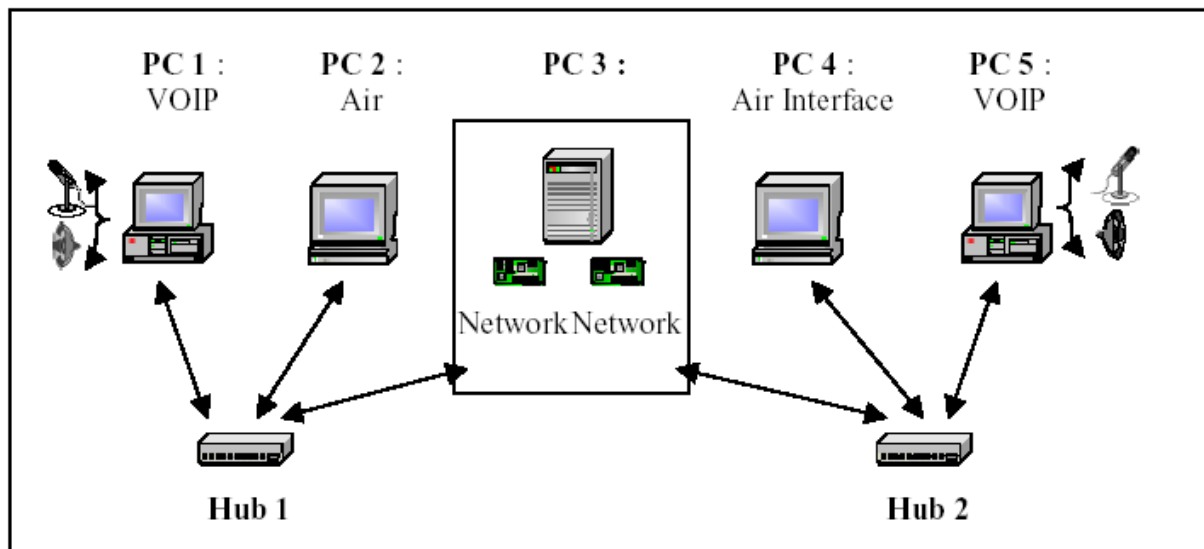
- The Communications and Information network Association of Japan (CIAJ) which represents manufacturers supplying network devices and terminals has published a report on 2002: Report on speech quality investigation of VoIP Terminals (gateways and IP phones):
http://www.ciaj.or.jp/tusin/pressrelease/voip_1e.html
"We adopted NetDisturb, ... as a network simulator because of its ease of installation and operation in Windows".
- 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 figure describes 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 the NetDisturb software as network simulator.



Simulation platform

Customer references

Present on the market since 1998, the NetDisturb software is used by many PTTs (Bell Canada, Equant, France Telecom, Global Crossing, NTT, Telenor, ...) and manufacturers (Alcatel, Nortel Networks, Philips, Tekelec, UTStarcom, ...) as well as many companies and universities.

Conditions of use

The NetDisturb software is licensed on a per workstation basis. You will need to purchase a separate license for each machine that you install it on.

Each licensed copy of the software installed on a workstation has a unique Site Code that requires the corresponding unique Site Key to be entered before the tool is operational.

Delivery

Includes CD with documentation, printed installation guide, technical support and maintenance (including major and minor software upgrades) for a period of twelve months from the date of purchase.

<p>To download an evaluation of NetDisturb please visit us at: http://www.zti-telecom.com/pages/main-ip.htm</p>

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

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 measurement 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 which 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 between the transmission of data to its receipt 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, packet desequencing and latency variation (jitter) for real-time applications such as VoIP, and service availability.