IP Network Emulation

Developing and Testing IP Products Under Configurable and Repeatable Network Conditions

www.PacketStorm.com

Contents

Purpose

The purpose of this document is to develop an understanding of the various impairments that network traffic can encounter across an IP Network and demonstrate how these conditions are reproduced in a laboratory environment for product development, testing and quality assurance.

Introduction

With the explosive growth of the Internet over the past several years, consumers have come to realize that the Internet will continue to affect the way they live and interact with others in their neighborhoods and around the world. Applications that are in the early stages of development today will soon become the reality of tomorrow. Buzzwords such as "Streaming Video" or "Voice Over IP (VoIP)" will become the next technologies that consumers welcome into their homes and offices just as they accepted other IP applications such as E-mail and web surfing only a short while ago.

Today's customers have high expectations from their vendors. They demand products that are reliable, complete and fully tested. But in this world of shorter development cycles and limited testing time, engineers have discovered that meeting customer expectations can be difficult as they find their time to market windows shrinking with each new product development cycle. So how can IP Technology Developers and Vendors provide high quality, thoroughly tested products in shorter amounts of time? By using advanced test tools that can provide extensive testing capabilities in an easy to use package.

This paper outlines some of the impairments that network traffic can encounter on an IP Network and discuss how those impairments affect the performance of IP products. In addition, the paper points out some of the key advantages to using an IP Network Emulator:

• Reducing engineering development and testing times thus limiting time-to-market delays.

• Enhancing the end user's experience by offering a product that has been thoroughly tested against multiple network scenarios.

• Limiting the need for after-sale customer support.

Target Audience

- **IP Technology Developers** - to test their designs against various IP network configurations and impairments.
- **IT Managers** - to confirm the capabilities of IP products or services they're considering for purchase.
- **Service Providers -** to test their applications and evaluate vendor products in a laboratory environment.
- **Website developers** – to verify and measure web site performance during typical network conditions.

Terminology

Familiarization with the following terms is helpful in understanding network configurations, IP Network Emulation, IP packet formatting and conditions traffic may encounter on an IP Network.

Source: Any device or computer that generates traffic for transmission over a network.

Destination: Any device or computer that receives traffic sent over a network.

Endpoint: Any device that is capable of generating and receiving traffic over a network.

IP Cloud: Conditions encountered on an IP Network that are beyond the control of the user or developer. Conditions include, but are not limited to, slow connections, time delays, packet reordering, packet loss and data collisions.

Link: The physical connection that connects devices on an IP Network. Links can have characteristics that affect the flow of traffic.

Router: Hardware that connects two or more links and determines which path is the most efficient for routing traffic.

Impairments:

Delay: provides latency to packets traveling though the network

Jitter: creates random time variation in the arrival of packets

Drop: random elimination of one or more packets from the stream of packets flowing in a network.

Decimate: elimination of a single packet from a stream of packets at a fixed interval. (i.e. The removal of every n^{th} packet from a stream of packets.)

Duplicate: reproduces a specific packet and inserts the copy into the stream of packets.

Re-Order: rearranges the order of packets flowing across a network.

Throttle: limits the traffic flow rate on a network link to a specified value.

Fragment: breaks up a single packet into multiple smaller packets according to Maximum Transmission Unit (MTU) size.

Burst Drop: drops multiple consecutive packets from a stream of packets.

Sink: drops all packets that flow down a specific connection on a network.

Source Address: The IP address of the network device that is the origination point of a packet.

Destination Address: The IP address of the network device that is the destination of a packet.

ToS: Type Of Service. Each IP packet is assigned a priority level between 1 and 5. Packets are routed through a network based upon their assigned priority level.

DiffServ: Differentiated Services. A relative importance level is assigned to an IP packet. Packets are routed through an IP network based upon their assigned importance level. A packet's importance level is described by its DSCP field.

DSCP: Differentiated Services Code Point. Each IP packet is assigned a priority level between 0 and 63. Packets are routed through a network based upon their assigned priority level.

Traffic Conditioning – network edge devices monitor and limit the end user's traffic rate. The traffic rate is determined by the Service Level Agreement between the end user and the service provider.

TTL: Time To Live. IP header field that indicates how many hops a packet may make as it travels across the network. Each time traffic passes through a router, the TTL value is reduced by one. If this value reaches 0, the packet is discarded.

Checksum: A computed value which depends on the contents of a packet of data and which travels with the packet in order to detect the corruption of data.

SLA: Service Level Agreement. Agreement between the end user and the service provider specifying the maximum amount of traffic.

How Network Conditions Affect Traffic Flow

Today the Internet allows an individual to access thousands of web sites in a seamless and user friendly manner. When surfing the Internet, users usually don't give much thought to how information packets flow through the network; until of course, they cannot access a desired web site or lose network connectivity altogether.

The Internet is comprised of many network nodes interconnected by many network links. At each node and each link there exists the possibility to drop, delay or corrupt the information stream transmitted between a web surfer and a web server. Network impairments negatively impact the "user experience" by increasing the time to access (download) information or by rendering an application unusable, like home banking.

Until recently, the Internet was a "best effort" network. Applications like web surfing, home banking and email delivery can tolerate large variations in packet dropping, packet delay and packet corruption. However, the activation of new "real-time" applications like Voice Over Internet Protocol (VOIP) and streaming video demand a stable and predictable network connection. These real time applications are spurring the development of a new Internet infrastructure, where Quality of Service (QoS) for real-time Internet applications can be guaranteed.

Using an IP network emulator to recreate Internet traffic impairments is one way manufacturers, service providers, and applications developers can verify the robustness of their Internet product. An IP network emulator can provide "what-if" testing in a laboratory environment and the ability to create reliable, repeatable and standard test configurations in a manufacturing environment.

The following impairments are intended to emulate the various network conditions of the Internet. Included with the each impairment definition is a brief description of a real world condition the network impairment recreates:

Limited Bandwidth – there are two main causes that limit bandwidth in the Internet: access systems and remote WAN links. Most access systems provide a bandwidth below 10Mbps. On the other hand, most Local Area Networks have a bandwidth of 100Mbps. Therefore access systems limit the bandwidth between the LAN and the Internet. Besides access systems, there are WAN links that connect to the Internet backbone that limit bandwidth. For instance, the destination server may be in a remote location that has a low bandwidth to the Internet.

Latency – there are two main sources of delay in the Internet. The first delay is the actual transmit time to go from the source to the destination. The second delay occurs at a router whose input rate is greater than its output rate. This rate difference causes packets to wait in memory while the router processes previous packets.

Loss – Equipment failure, overflowed buffers, and over capacity routers cause packet loss. Failure with a transmission link or router causes bursts of packets to be dropped. Queuing algorithms such as Random Early Detection (RED) drop packets on purpose to avoid its router's buffers from reaching capacity. If a router is over capacity then it will drop bursts of incoming packets.

Out-of-Order – Traffic engineering techniques such as MPLS change packet paths to avoid router congestion. If the path is changed and successful, then some of the packets may arrive at the destination prior to earlier packets. Therefore the receiving device must be able to rearrange packets in the proper order.

Errors – Faulty hardware devices, cross talk noise, and transmission mediums create errors in packets. A hardware device such as a router could have a bit stuck in one position and thus change the value of the packet. Cross talk noise from another cable could change bits and cause errors in a packet stream. Satellite links use a transmission medium that is susceptible to electromagnetic interference from thunderstorms and electronic equipment.

Fragmentation – Network devices specify a Maximum Transmission Unit (MTU) to limit packet length. Typical MTU is 1500 bytes (an Ethernet specification). If a packet is fragmented, then the receiving device must be able re-assemble the original packet.

Duplication – During heavy congested network conditions, some equipment will send duplicate packets to increase the odds that at least one packet arrives at the destination within a specified time limit. Therefore the receiving device must be able to handle duplicate packets.

Quality of Service

Real time applications such as voice and video streaming are greatly affected by latency and packet loss. As real time applications merge with traditional data services on the IP network, it becomes more critical for networks to provide minimum latency and packet loss. Differentiated Services (Diff Serv) was created to address these QoS concerns. Diff Serv specifies sixty four service levels and therefore provides the capability to give higher priority to certain packets and applications.

Along with Diff Serv, network traffic conditioning techniques are utilized to address QoS issues. Essentially traffic conditioning is performed at the edges of a network by measuring the end user's traffic flow rate. If the traffic flow rate is greater than the specified rate in the Service Level Agreement (SLA) then the packets are dropped, re-marked for a lower service level, or delayed. Again, multiple service levels are provided to give higher priority to the real time applications such as VoIP.

As discussed above, QoS will become an increasing important issue for service providers and network equipment manufacturers. Equipment must be able to perform packet prioritization and be compatible with Diff Serv and traffic conditioning implementations.

WAN Application

In the past, companies used their wide area network (WAN) to transfer data among their offices. To leverage this infrastructure, companies are implementing Voice over Internet Protocol (VoIP) as their inter-office communication system. Below in Figure 1, a corporate office and three branch offices are connected via an IP network. Before deploying VoIP, the company needs to test the application during typical and worst case network conditions. An IP network emulator can address these needs by emulating the following functions: network impairments, network bandwidth, Quality of Service (QoS) mechanisms, and Service Level Agreements (SLA).

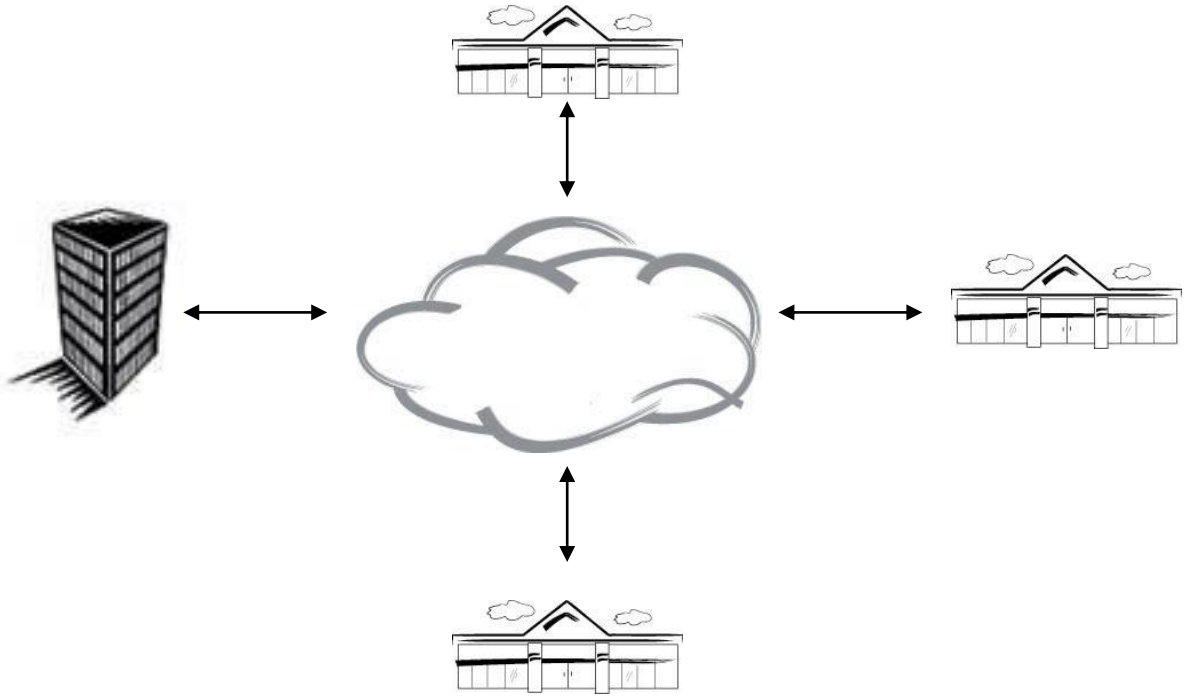

Figure 1 – Corporate Wide Area Network

For instance, the corporate WAN could have the following conditions:

	Latency	Loss	Bandwidth
Corporate - Branch #1	200ms	2%	1.5Mbps
Corporate - Branch #2	120ms	1%	10Mbps
Corporate - Branch #3	300ms	1.5%	56kbps
Branch #1 - Branch #2	160ms	1.8%	1.5Mbps
Branch #1 - Branch #3	210ms	2.2%	56kbps
Branch #2 - Branch #3	245ms	2.6%	56kbps

Table 1 WAN Parameters

Figure 2 shows the emulator's user interface to create the above WAN conditions:

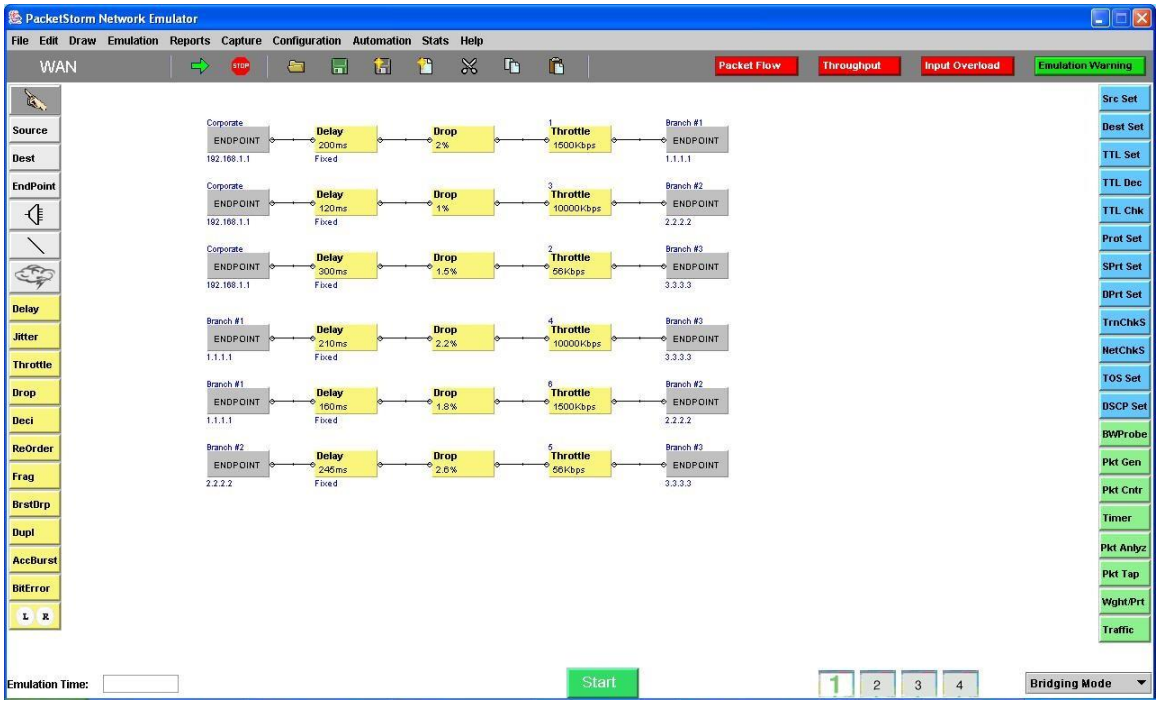

Figure 2. – User Interface

The above example is quite basic and doesn't address each location's bandwidth being shared from the other locations. However by adding Diff Serv and traffic conditioning, WAN applications can be fully tested before being deployed. Please see our WAN Bandwidth Emulation white paper to see the details of properly emulating a wide area network.

Quality of Service Application

Quality of Service becomes extremely important as voice and video traffic merge onto the IP network. Multimedia traffic doesn't have the luxury of retransmissions to recover lost or bad packets. Voice and video traffic are real time applications and therefore can't rely on "best effort" service. To meet the requirements of different applications in the future, the IETF created the Differentiated Services (Diff Serv) standard. Diff Serv provides sixty four service levels to allow carriers to offer multiple network performance levels to address the various application requirements. Therefore, the carrier can provide low latency service for VoIP, low packet loss service for video applications, and low cost service for applications such as e-mail. The Table 2 illustrates parameters for six Diff Serv service levels. By using the Diff Serv Code Point (DSCP), the end user specifies the priority of service for each application.

Application	DSCP	Latency	Pkt Loss	Bandwidth	Max MTU
Video Conf.	5	150 ms	1.0 %	100 Mbps	1500
VoIP	13	100 ms	3.0 %	10 Mbps	256
White Board	19	240 ms	0.2 %	24 Mbps	1500
IP Storage	31	420 ms	2.0 %	200 Mbps	1500
E-mail	41	600 ms	4.0 %	5 Mbps	1500
http	58	750 ms	5.0 %	4 Mbps	500

Table 2 - Differentiated Service Levels

In addition to Diff Serv, traffic conditioning affects QoS. Traffic conditioning is the method utilized by the carrier to ensure the end user stays within the traffic limitations of its Service Level Agreement (SLA). The SLA is a contract between the end user and carrier that specifies the service prices, network performance, and traffic load. The carrier may use one of the following network queues in Table 3 to enforce the SLA. The traffic conditioner performs marking, policing, and shaping operations on all incoming packets. Thus out-of-profile packets can be re-marked for another level, policed (dropped), or shaped (queued until they are in profile).

Weighted Fair Queuing	First In First Out (FIFO)
Stochastic Fair Queuing	Prioritized FIFO
Weighted Round Robin	Leaky Bucket
Random Early Detection (RED)	Token Bucket
Balanced RED	

Table 3 - Network Queues

In summary, QoS is implemented at the edge of the network by utilizing Differentiated Services and traffic conditioners. Diff Serv provides a mechanism to prioritize traffic among different applications or users. While traffic conditioners limit user's traffic bandwidth that ensures the carrier's network meets the performance metrics for all of its customers.

Carrier Network Application

There are various types of infrastructure equipment (edge routers, core routers, switches, etc.) in a carrier's network. These infrastructure devices utilize many types of network interfaces (10/100, Gigabit Ethernet, T1, E1, DS3, E3, OC-3, OC-12, etc.) and protocols (PPP, HDLC, Frame Relay, ATM, POS, etc.). To properly test network capabilities, the carrier must measure application performance in a controlled environment. By utilizing different combinations of infrastructure equipment with multiple network conditions, the carrier ensures the application will satisfy their customer's requirements.

For example, the carrier plans to offer Virtual Private Networking (VPN) to its customers. The most likely first step is to evaluate the vendor VPN equipment under normal and worst-case network conditions. The VPN equipment may have multiple network interfaces and therefore must be tested under every possible scenario. After selecting the preferred VPN equipment, the next step is to evaluate the equipment's performance under all possible network conditions. The last step is to evaluate the VPN performance with various enterprise VPN equipment under normal and worst-case network conditions. See Figure 3.

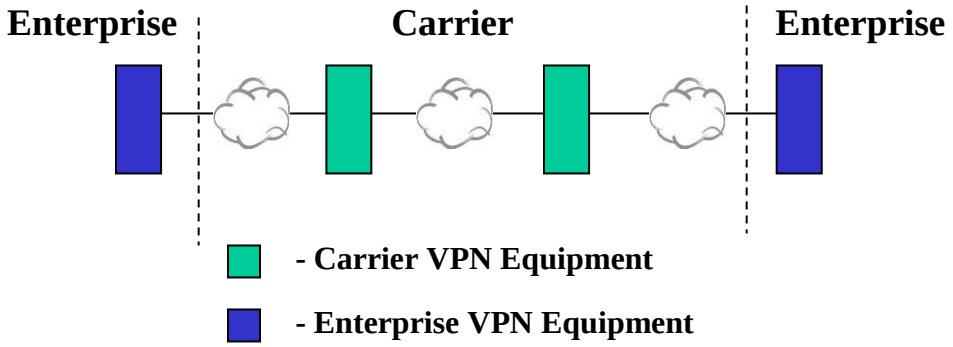

Figure 3 - VPN Network Configuration

In conclusion, network emulation with multiple interface types allows testing of all scenarios under every possible network condition. Thorough repeatable testing ensures proper vendor equipment evaluation and application performance validation.

Dynamic Emulation

The goal of using test equipment is to ensure the device under test works in the real world. To truly emulate the real world conditions, test systems need to reproduce all network conditions. The following example is an apartment building that has long Internet access delays after breakfast, school, and dinner. Chart 1 below illustrates one possible scenario of changing delay values versus time.

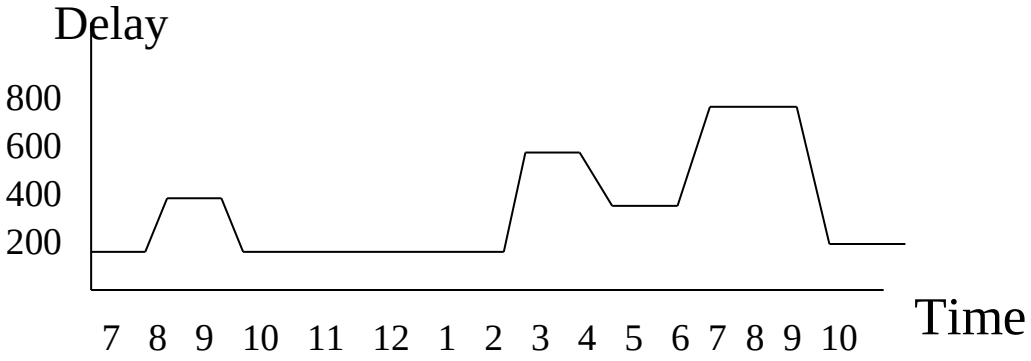

Chart 1 – Apartment Building Time Varying Internet Access Delay

Testing an application with a fixed amount of delay is a good starting point to evaluate performance. Using delays with mathematical distributions (ex: Gaussian, Exponential, Uniform) is even better to evaluate performance since mathematical distributions emulate changing delay values that are closer to real world conditions. However, the ideal method to evaluate performance is to emulate concise and repeatable time varying networks conditions to truly ensure the equipment under test will work in the real world.

PacketStorm Technology and Products

PacketStorm offers four different IP Network Emulators to choose from – The 1800E, 2600E, Hurricane and Hurricane II. All models use the same Graphical User Interface. There are two modes of user interface: Standard shown in Figure 2 and Basic shown in Figure 4. The models offer the same features but differ by packet processing capabilities.

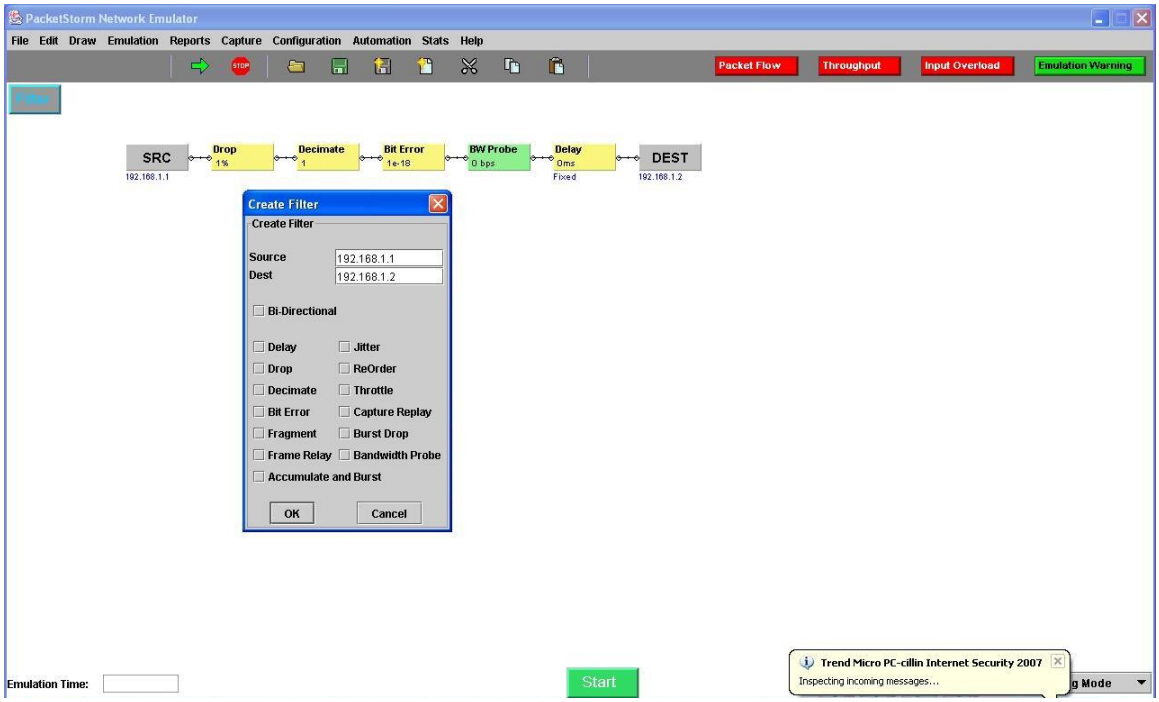

Figure 4 – Graphical User Interface. By keeping the User Interface simple to navigate, users will find it easy to create and modify simple and complex network configurations.

The PacketStorm1800E is targeted at network edge applications and the other models are targeted at high bandwidth applications.

The emulators provide up to five network interface slots, Ethernet bridging, routing mode, interface mapping, and dynamic emulation. Ethernet bridging provides an easy way to connect to other Ethernet devices. Routing mode provides a method to route IP traffic between different types of interfaces (ex. T1 and Ethernet). Interface mapping allows the emulator to be truly transparent to other network devices. Dynamic emulation provides capability to re-create traffic conditions with time varying impairment values.

By using a PacketStorm IP Network Emulator, developers emulate various network conditions to test their products and applications. Unlike testing a product live on the Internet, a PacketStorm Emulator allows tests to be repeated or modified.

By testing products against various network impairments and conditions, developers will have the opportunity to discover and correct problems in their labs before product deployment.

About PacketStorm Communications

PacketStorm Communications, Inc. develops IP Network Emulators that allow users to emulate various IP Network conditions. By developing proprietary hardware and software, PacketStorm has created emulators that can be used to extensively test networking applications that are available today as well as future technologies that have yet to be deployed

PacketStorm is a privately held company founded in 1998 by a team of engineers and managers from the prestigious Bell Laboratories. With extensive backgrounds and experience in both network development and testing, PacketStorm continues to focus on the needs of IP developers and network managers. PacketStorm's world headquarters in New Jersey handles product engineering, marketing, and customer support.

Headquarters
PacketStorm Communications, Inc.
1105 Industrial Parkway
Brick, New Jersey 08724
Phone: (732) 840-3871

Website
www.PacketStorm.com