

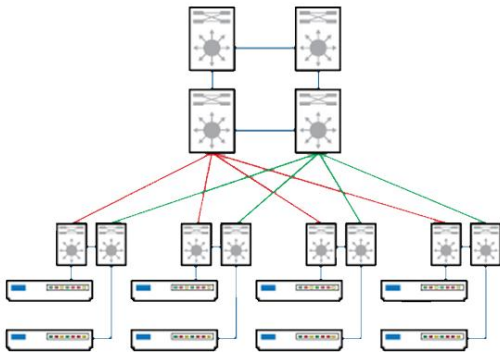
Network Simulation – Traffic, Paths and Impairment

Summary

Network simulation software and hardware appliances can emulate networks and network hardware. Wide Area Network (WAN) emulation, by simulating network paths, devices and impairments can test device configuration and application behavior. Stateful network traffic, injected into test devices and WAN connections help determine quality and throughput. Injecting network traffic provides a way to test device configurations, such as QoS, port blocking and VLAN configurations to name a few. Additionally, traffic generation can be used for burn-in testing before product delivery.

Device Testing

Complex modern networks with configurations for router paths, redundancy, VLAN's, QoS and firewalls with stateful packet inspection and port blocking, require that devices be tested before deployment.



By generating stateful network traffic the configuration, throughput, packet loss, jitter and latency of network devices can be tested and evaluated.

Stateful network traffic is the real thing – it is not just sending packets through devices, it knows when the packet was sent, when it was received and that it accomplished the handshakes required by a specific protocol.

For testing VoIP - multiple protocols such as SIP, H.323 and RTP need to be generated, and reports producing statistics such as MOS, R-Factor, jitter, lost packets and QoS are needed to evaluate calls.

Sometimes devices need to be tested for the number of connections they will support or how close to line rate ports on a device will reach. Traffic generation can help determine the performance limits of a firewalls or other devices. At various levels of traffic or utilization, the stability and latency caused by the device can be predicted.

Devices may also need to be tested when converting from IPv4 to IPv6. And traffic generators are often used by device manufacturers to perform burn-in testing before product shipment.

Connection Testing

Various carrier based connections link together an organizations' networks – point to point, MPLS, DSL, Cable, and Satellite. Other purchased solutions, such as wireless or microwave may also be deployed.



When connections are carrier based, organizations want to validate the throughput they are truly getting and compare it the throughput they contracted. Using a network traffic generator they can test the maximum rate by sending and receiving UDP packets across the connection and then determine an operational rate by sending and receiving TCP packets.

As a connectionless protocol, UDP does not incorporate any handshake such as establishment, teardown or maintenance logic. Whereas TCP is designed for accurate delivery rather than timely delivery, that is, it can incur relatively long delays while working through its logic, therefore, resulting in lower throughput.



Other connections such as wireless are affected by factors such as distance and signal interference. The connection may need to be tested to determine if the throughput will be adequate to carry the determined load.

For deploying certain technologies such as VoIP and streaming media connections typically need to be tested for throughput and more importantly quality. Quality is impacted if there is a high level of lost packets or are packets out of order. In essence :Is the connection clean enough to deploy this type of technology?

With streaming technologies connection quality can be protected by implementing Quality of Service (QoS), which refers to resource reservation control mechanisms rather than the achieved service quality or bandwidth. QoS allows, for example, VoIP packets to have a higher priority than other packets moving across a connection. To test connections with QoS the traffic generator must be able to generate a number of different types of traffic pairs with a unique Type of Service (ToS) byte specified.

Networks that carry applications that use multicast protocol for connections, such as video conferencing, may need to be tested with multicast traffic and traffic with Time To Live (TTL) settings. This can mean sending traffic over all of the possible connection paths or to multiple endpoints.

Network Traffic Generator Features

Features and Transmit Characteristics	Description
Connection Types	Layer 2 and 3 - Raw Ethernet, TCP/IP and UDP/IP, IPv4 and IPv6 Layer 4 - FTP, HTTP, HTTPS, SCP,FTP, TELNET, IMAP,IMAPS, POP3, POPS3, SMTP, SMTPS, PING, DNS,SNTP and NMAP VoIP - SIP,H.323, RTP and RTCP File Endpoints - NFS, iSCSI or SMB (SAMBA) Multicast Streaming audio and video with flexible plugin architecture Wireless - Emulates 802.11a/b/g/n virtual stations
Transfer Rate	Fixed, minimum and maximum and transmit rates in bits per second (bps). Random variation between the min and max creating a random stair-step pattern of data transmission over time.
Packet Size	Fixed, minimum and maximum and random in bytes.
Payload	The payload pattern for the data can be increasing, decreasing, zeros, ones, pseudo random, random and custom.
Port	Specify a particular port for IP traffic
ToS/QoS	For IP based protocols, you can specify the ToS (aka QoS) bits in the IP header.
TTL	This specifies the 'time-to-live' when configuring multicast endpoints.
Checksum	Performs a 32-bit CRC calculation on the payload.
VoIP	Specify SIP or H.323, CODEC, Ports, ToS, call setup, gateways, number of calls, ring time, inter-call gap and duration.
Connections	Simulate thousand and tens of thousands of connections.
Virtual Interfaces	Emulates unique machines with one physical interface. Emulates Ethernet, IP, 802.1Q VLAN's and wireless virtual stations.
Secondary IPs	Allows thousands of traffic test connections between thousands of IP addresses.

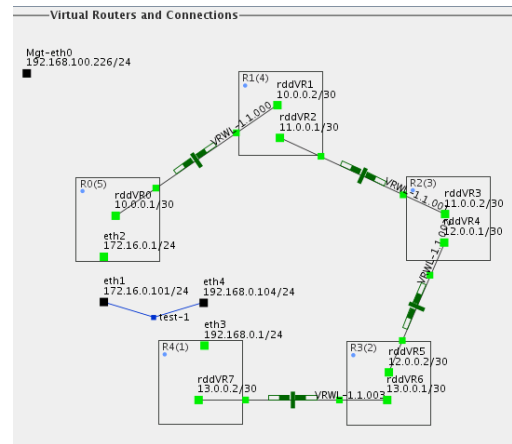
Network Device Simulation

It is very costly to duplicate hardware in a test lab for an actual network and difficult to replicate delay effects caused by hardware. But some sort of environment is needed to test device configurations and applications before deployment. A network simulator can significantly reduce hardware and development costs.

A virtual network builder can support virtual routers, emulated network links, bridges (switches), virtual and physical interfaces and more. Virtual routers, for example, can be configured to support static routing for IPv4 and IPv6, OSPF routing for IPv4 and IPv6 and IPv4 multicast routing protocols.

Some examples of what a network device simulator can do:

- ❖ Emulate a live routed network by using multiple virtual routers to form a working multi-hop network
- ❖ Emulate networks of arbitrary complexity using real-world routing protocols
- ❖ Emulate the behavior of multiple Layer-2 Switches connected together for traffic fail-over testing
- ❖ Add network impairments such as latency, dropped packets and jitter
- ❖ Add stateful network traffic



Network Impairment

The purpose of a network emulator is to emulate network connections such as T1, DSL, OC3, OC12, Satellite, Dial-Up and other limited speed network links with impairments. A network emulator allows organizations to test and verify that applications and equipment will perform when conditions degrade due to bandwidth, latency, packet loss, jitter and packet errors.

Before deploying applications to remote sites it is a good idea to test how they will perform when impairments are encountered. Conducting early application testing with impairments can address problems such as chatty applications, latency sensitive transactions, caching inefficiencies and other network performance conditions.

Impairment testing can be useful when hardware relocations are necessary, testing VoIP equipment and implementing WAN acceleration products.

Network Impairment Features

Features and Packet Impairments	Description
Bi-Directional	Simulates different connection types on each side of a WAN connection (symmetrical and asymmetrical), T1, DSL, Cable, Wireless or Satellite.
802.1Q VLAN	Able to bridge 802.1Q VLAN Interfaces.
Router	Simulates routers and connections.
Buffer	Emulates the smoothing buffer found on equipment used in Wide-Area-Networks. The buffers are implemented to smooth bursty traffic so that packets are not needlessly dropped.
Delay/Latency	The time it takes in milliseconds for a packet of data to get from one designated point to another.
Jitter	Simulates the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes.
Drop	Simulates the disappearance of a packet that was transmitted or ought to have been transmitted. Packets can also be dropped in a burst or specifically every xth packet.
Duplicate	Simulates duplication which occurs when one packet becomes two (or more) identical packets. Can also specify every xth packet.
Re-Order	Packets are moved out of order from their original sequence. This packet delay has an earlier packet being delayed greater than a subsequent packet. The subsequent packet will arrive before the earlier packet. Typical of load balanced links.
Bit Error	Inserts random or periodic errors in either the payload only or the complete packet. Supports packet corruptions, including bit-flips, bit-transposes and byte overwrites. Able to specify multiple corruptions.
Checksum	Recalculates the IP, UDP, and TCP checksum for a packet after applying the corruption. This will allow the corrupted packet to be accepted by the stacks on the receiving machine as if the data were actually valid.

Operative Software Products specializes in software and appliances that helps IT professionals test, troubleshoot, manage and monitor their applications and systems. We have solutions for small/medium business, corporate divisions and corporate enterprises.

