An Industry Standard Benchmark Consortium

Networking Version 2.0

Benchmark Name: IP Network Address Translator (NAT)

Highlights

- **Based on NetBSD kernel code**
- **Stresses data cache efficiency and latency**

Application

Basic Network Address Translation (NAT) is a method by which an Internet router maps IP addresses from one group to another, transparent to end users. NAT is traditionally required when a network's internal IP addresses cannot be used outside the network, either because they are not globally unique, or for privacy reasons.

A NAT router, residing on the border between two networks, translates the addresses in the IP headers so that when the packet leaves one network and enters another, it can be correctly routed. For egress packets, the source address is mapped to a globally unique external network address, while, for ingress packets, the destination address is mapped from the external address to the relevant address in the private network. IP header checksums (and UDP and TCP checksums if applicable) are also updated to reflect the address translation.

Benchmark Description

The dataset for the NAT benchmark focuses on the handling of egress packets. When a packet "arrives," initial processing ascertains what action, if any, needs to be undertaken. The NetBSD NAT implementation uses a 128-entry hash table to hold information about current connections. By using the source address, destination address, protocol, and ports (if applicable) of the packet, the system computes an offset into the hash table. If this entry in the hash table relates to the current packet, the packet belongs to a "connection" that is already established and the packet processing is undertaken as dictated by the NAT table entry. If the packet doesn't belong to a current connection, the list of NAT rules are searched to ascertain if a rule exists for the packet handling. If a rule exists for this "connection" (rules are specified during an initialization phase before the benchmark is started), the system creates an entry in the hash table for this "connection" to accelerate future handling of packets for this connection.

If the packet is determined to correspond to a NAT entry, the source address of the packet is altered as stipulated by the pertinent rule. The IP header checksum is then fixed to reflect this modification. Additionally, if the packet is a TCP packet, the TCP checksum is also updated to reflect the modification in source address. The translated packet is then sent onward.

Analysis of Computing Resources

Aggressive pointer chasing tests cache latency. Hash table searching tests processors' ability to perform loads and compares and stresses processors' branch prediction logic and ability to recover gracefully from misprediction.

Special Notes

P. Srisuresh, “IP Network Address Translator (NAT) Terminology and Considerations,” RFC2663, August 1999.

P. Srisuresh et al, “Traditional IP Network Address Translator (Traditional NAT),” RFC3022, January 2001.