TECHNICAL SUPPORT NOTE
Understanding Network Address Translation (NAT)

Introduction

NAT is most often performed by a router and/or firewall device. In its most fundamental form a NAT device connects an **inside,** internal, private or trusted network to an **outside**, external, public, or untrusted network. The terms trusted and untrusted are typically used in firewall NAT applications. The addressing on the inside network is referred to as **local** and is often from a private or obsolete range. The addressing on the outside network is typically a **global** address scheme from the public range such as the Internet. See Figure 1. NAT may also be used when connecting two private ranges such as when companies merge and need to combine two networks into one larger network but the networks contain overlapping addresses.

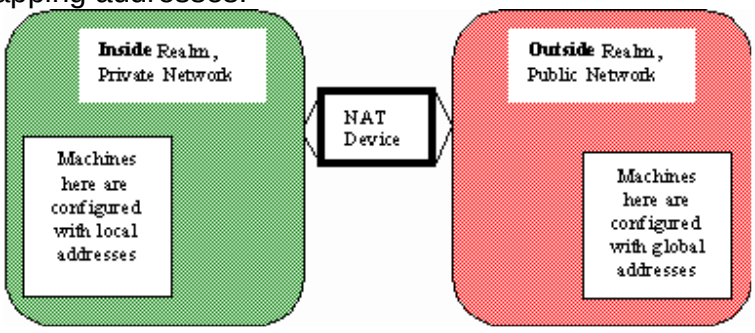

Figure 1 - NAT Connects Different Address Realms

Private address ranges are defined in RFC 1918 [2]. These addresses were set aside from the IPV4 address space to allow enterprises to run autonomous networks using TCP/IP. These ranges are not routed on the Internet. The ranges are defined as:

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

When an enterprise using this address space decides to connect to the Internet, NAT provides connectivity without requiring an overhaul of the existing IP address scheme on the enterprise network. Though this could be done using non-private addresses in the enterprise, use of private addresses eliminates the possibility of a conflict with any real public address (though NAT solutions exist for this scenario also).

How does NAT do it?

Referring to Figure 2, the IP portion of a packet resides at layer 3, corresponding to the OSI model's network layer. IP packets typically carry TCP or UDP at layer 4, corresponding to the OSI model's transport layer. The IP header contains the source and destination IP addresses of the packet. The TCP or UDP header contains the source and destination port. The source/destination port identifies the process on the source/destination machine with which this packet is associated.

The machine initiating a session will typically specify a well known destination port on the target machine, such as http or telnet. The source port is dynamically set to a unique value by the initiating machine. The combination of ip addresses and port values allows an individual session to be uniquely identified, therefore allowing multiple 'sessions' to be multiplexed between the same two machines.

Non-TCP/UDP protocols such as ICMP, IPsec, and others do not utilize ports. For these protocols, there are other values used to identify a particular session. For this reason, in some documents, the term 'transport ID' is used instead of 'port' to generically refer to a layer 4 identifier.

NAT changes the source and/or destination address in the IP header of a packet from one value to another as it crosses the NAT device. The IP header checksum is recalculated and set. Since the UDP and TCP checksum includes values from the IP header in its algorithm, those checksums must also be recalculated and set. In many applications, the IP address is also conveyed in the upper level protocol payload which often times also has to be translated. It becomes obvious that even the simplest NAT operation requires many more CPU cycles than simply routing a packet.

In certain NAT applications, NAT also changes the transport ID (TCP/UDP port, ICMP ID, etc.) This will be discussed in more detail below.

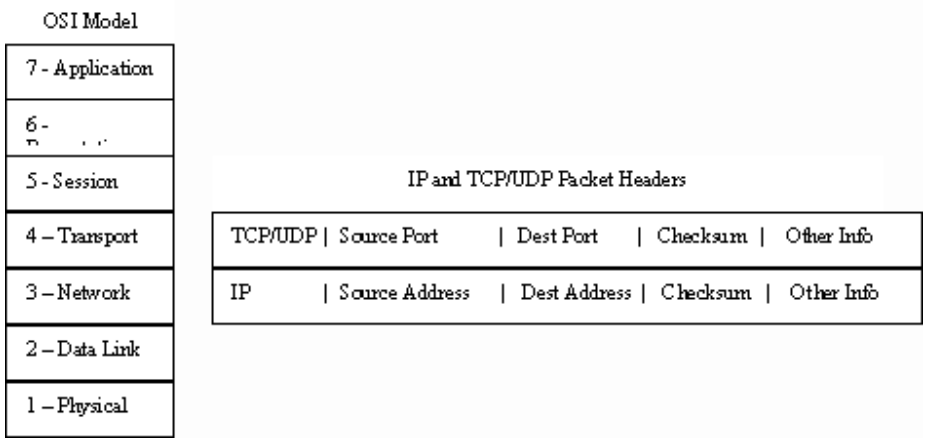

Figure 2 - The OSI Model and Corresponding TCP/UDP/IP Packet Header Fields

Session Flow vs. Packet Flow

Many underlying dynamics of NAT are session oriented, meaning they are specific to an individual session between two processes on two computers. Any two computers may have numerous sessions active at any given time. Sessions are directional though the session packet flow is bi-directional. Session direction is from the session initiator to the session target. For example, when you use a browser to access www.adtran.com, your PC is the initiator of that session while www.adtran.com is the target.

As mentioned above, a session can be uniquely identified by its combination of IP addresses and TCP/UDP ports.

Selecting Packets to be Translated

NAT is usually implemented in two steps. Step 1 is to select the traffic to be translated. Step 2 is to apply the desired translation. Selecting the traffic can be as simple as choosing ALL outbound traffic for a single translation action or as specific as selecting only packets to/from a specific IP address destined for a particular port (such as http or telnet).

If you experience any problems using your ADTRAN product, please contact ADTRAN Technical Support.