Network Working Group
Internet Draft
Expiration Date: February 1999

Yakov Rekhter
cisco Systems

Implications of NATs on the TCP/IP architecture

draft-ietf-nat-arch-implications-00.txt

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

2. Abstract

In light of the growing interest in, and deployment of network address translation (NAT - RFC 1631), this document will present some highlights of the architectural implications. A reader is assumed to be well familiar with the principles of NAT operations [RFC1631].

3. Implications on routing and addressing

Use of NATs allows to build a TCP/IP network as a collection of routing realms, rather than require the network to be a single routing realm. Routing realms are interconnected via NATs, where a NAT is assumed to be connected to two or more routing realms.

Regardless of whether a network is constructed as a single routing realm, or as an interconnection of multiple routing realms, an IP address carried in a packet acts as a "locator". The distinction between the former (single routing realm) and the latter (multiple routing realms) is that in the former case the same address acts as a locator across the whole network (network-wide locator), while in the latter case the same address acts as a locator only within a part of the network (within a single routing realm). Moreover in the former case to act as a locator, an address in the IP header has to be modified at the boundaries between routing realms. This, in turn, implies that addresses in the IP header may not be preserved end-to-end (in fact, they are guaranteed not to be preserved end-to-end for any communication than spans multiple routing realms).

With NATs temporal uniqueness of IP addresses is no longer assured. It may be quite short, possibly comparable to a transport connection time. In such cases an IP address is no longer a suitable long-term end point identifier. This has some impact on end-to-end security (see below). Note that DHCP, PPP, and renumbering are some of the other factors that make IP addresses unsuitable as long-term end-point identifiers.

Constructing a network out of multiple routing realms allows to build a network whose size is no longer bounded by the scaling limitations of the IP routing system. Using multiple routing realms, instead of a single one allows to reduce the load on the network layer routing system, as the routing system has to handle routing only within individual routing realms. As a result, the amount of routing information that the routing system has to handle is bounded by the size of the individual routing realms that form a network, rather than by the size of the whole network.

Use of multiple routing realms, instead of a single one, may permit relaxation of some of the constraints on IP address assignment within a network. Specifically, since the routing system operates within the confines of a single routing realm, any constraints on address assignment imposed by the routing system are confined to a single routing realm as well.

For example, addresses are required to be unique only within a single routing realm, but not across multiple routing realms. This simplifies IP address administration and management, as each routing realm could administer and manage its address space independent of all other routing realms, thus reducing the amount of required coordination among organizations involved in address administration and management, and ultimately reducing the cost associated with address administration and management.

Likewise, hierarchical address assignment required to support hierarchical routing is required only within individual routing realms (only within parts of the network), but not across multiple routing realms (not across the whole network). This reduces the need for renumbering when network topology changes (e.g., an enterprise changes its Internet Service Provider), which in turn lowers the overall cost of operations by reducing the cost of renumbering.

Complexity of interconnecting routing realms with NATs depends (among other factors) on the network topology at the level of routing realms. Current practice could be closely (although not precisely) approximated by a two level hierarchy, with the Internet being at the top level of the hierarchy. Further work is needed to understand how routing realms could be interconnected (via NATs) in an arbitrary (mesh) topology.

Since NATs maintain state associated with inter-realm connectivity, failure of a NAT may cause disruption of inter-realm connections handled by the NAT. Techniques such as "hot stand-by" NAT could be used to avoid the disruption. Such techniques require syncronization of state between the "primary" and the "hot stand-by".

4. Implications on DNS

A network formed by multiple routing realms relies on DNS for providing connectivity among these realms. This places certain requirements on DNS.

For a network formed by a set of interconnected routing realms, fully qualified domain names are required to be unique across the whole set (across the whole network), even if IP addresses are no longer unique across the set. Note that this requirement has to be satisfied regardless of whether the network is formed by a single or multiple routing realms.

A routing realm may contain one or more zones.

In general one should try to avoid (or at least minimize) spreading a single DNS zone across multiple routing realms. This is because spreading a DNS zone across multiple routing realms increases the amount of manual configuration on NATs interconnecting these realms.

Further work is required to identify implications on DNS in the presence of DNS Security and DNS Dynamic Updates.

5. Implications on transport layer

Since communication across multiple routing realms requires addresses in the IP header to be modified at the boundaries between the realms, transport header checksum has to be adjusted at the boundaries between the realms. Procedures for doing this are described in [RFC1631].

6. Implications on applications

If hosts in different routing realms communicate among themselves via an application that carries IP addresses in the application data stream (e.g., FTP), the NATs that interconnect the realms have to be augmented with the Application Layer Gateway (ALG) functionality for that application. This is because IP addresses are guaranteed to be unambiguous only within a single routing realm. Thus when they are carried in the application data stream the data stream has to be modified as it crosses routing realm's boundaries by the NATs placed at the boundaries. Modifying this application data stream requires to understand the semantics of the stream, which in turn requires the ALG functionality specific to the application.

Unconstrained proliferation of applications that carry IP addresses in the application data stream clearly complicates support of such applications across multiple routing realms. Whether this is a problem of practical significance, or how wide is going to be the proliferation of such applications is a matter of opinion.

Applications that do not carry IP addresses in the application data stream place no additional requirements, other than what is required by NAT (address translation and transport header checksum adjustment).

The discussion on whether applications should carry IP addresses in the application data stream is outside the scope of this document, but may well be within the scope of the overall TCP/IP architecture.

7. Implications on security

As long as a security mechanism doesn't depend on addresses in the IP header being preserved end-to-end, using such mechanism for communications that span multiple routing realms places no additional requirements on either the mechanism or NATs. For example, use of SSH for communications that span multiple routing realms poses no problem, as proven by operational experience.

On the other hand, the use of IPSec, or any other protocol which uses IP addresses as part of a security association, for communications that span multiple routing realms is problematic. Use of IPSec is likely to require boundaries between different IP Security domains to be aligned with routing realms boundaries. More work is needed to identify specific scenarios where IPSec could work, as well as the scenarios where IPSec is not going to work.

While NATs clearly limit the scope where IPSec could be applicable (or vice versa, IPSec could limit the scope where NATs could be applicable), one need to remember that IPSec is just one mechanism for providing security, but not the only one possible. Moreover, there are scenarios where IPSec could be used in conjunction with NATs.

The discussion on whether IPSec should depend on preserving addresses in the IP header end-to-end is outside the scope of this document, but may as well be within the scope of the overall TCP/IP architecture.

For applications that carry IP addresses in the application data stream, a combined NAT/ALG needs to "see" the application data stream in clear. If security is viewed as necessary for such applications, then satisfying this requires to align security domains with routing realms boundaries, at least for such applications.

8. Implications on performance

It is quite clear that performing IP forwarding on a packet requires less processing than performing NAT. Whether this difference has any practical impact is a matter of opinion.

The impact on performance is clearly going to be more significant for applications that carry IP addresses in the application data stream, and handling such applications require not just NAT, but ALG as well (which has longer path length than NAT).

9. "Many-to-one", "one-to-many"

NATs allow to model a collection of hosts as a single "virtual" host. Doing this requires no host modifications. One possible application of this mechanism is to provide load sharing across multiple servers.

NATs allow to present a host with a single IP address as if the host would have multiple IP addresses. Doing this requires no modifications to host software. One possible application of this mechanism is support connectivity between multi-homed sites and the Internet.

10. Preserving addresses end-to-end

In general any application that assumes that addresses in the IP header would be preserved end-to-end is going to be impacted by NATs, as NATs clearly violate this assumption. The degree of the impact may depend on a variety of factors, and is likely to be application specific.

The discussion on whether the TCP/IP architecture should evolve to explicitly recognize the possibility that addresses in the IP header may not be preserved end-to-end is outside the scope of this document, but may well be within the scope of the overall TCP/IP architecture.

11. Security Considerations

The impact of NATs on security is discussed in section "Implications on security" of this document.

12. References

[RFC 1631], Egevang, K., Francis, P., "The IP Network Address Translator", RFC 1631, May 1994

[RFC 2101], Carpenter et. al., "IPv4 Address Behavior Today", RFC 2101, February 1997

13. Acknowledgments

TBD

14. Author's Addresses

Yakov Rekhter
cisco Systems
170 West Tasman Drive
San Jose, CA 95134
Email: yakov@cisco.com
Phone: 1-914-215-2128