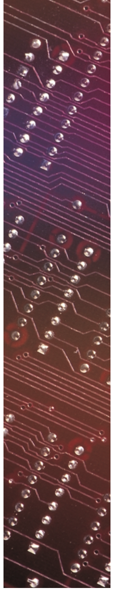

There's always more online...

Those Pesky NATs

Joseph D. Touch • *Postel Center for Experimental Networking, USC/ISI* • *touch@isi.edu*

Read the full story at
http://dsonline.computer.org/0207/departments/w4icon.htm

Whether buried deep inside ISPs, or camouflaged as DSL routers, Network Address Translators, or NATs, have become a ubiquitous tool in the Internet landscape. NATs enable telco and cable operators to prevent commercial use of consumer accounts. They also let home users run open community access wireless networks off a single purchased account. It is what NATs disable, however, that makes them nefarious.

How NATs Work

A NAT makes a group of networked computers appear to the rest of the Internet as if they were a single computer, using a single address. To the Internet, traffic coming from the computers behind a NAT appears as if coming directly from the NAT itself. To accomplish this, NATs assign local addresses to the systems they hide and translate packets between them and the Internet. NATs keep an internal table to track associations and guide this translation.

A NAT uses a simple set of rules to hide a set of machines. This can be useful where addresses are limited, because it a single Internet address provides access for a whole set of machines. It can also be harmful: NATs work only when the translation works (when addresses are used in ways the NAT is unaware of, they fail); NATs work only for connections or associations that originate on the hidden computers (not connections that terminate there); and NATs assume a persistent association – that's what keeps the address translation table entry active.

NATs are so ubiquitous because ISPs use them internally to support their business model. ISPs, like many businesses, would like to charge business customers more than consumers, particularly to subsidize infrastructure and provide competitive consumer prices. To charge different prices, there needs to be different levels of service. ISPs decided early that businesses need to run Web servers – and consumers probably didn't. NATs help enforce this model, where uplink connections from consumers are aggregated to reduce costs, and businesses pay hefty fees for the privilege of running servers.

Where's the Rub?

NATs eventually break something. New protocols with embedded addresses, protocols that need to connect to (not from) the hidden computer, or associations that change – all break when used behind NATs. Recently, L2TP, resource discovery, and peer applications, respectively, have caused such problems, and the future will surely bring more.

Because NATs can be hidden inside the ISP or local network infrastructure, it can be difficult to determine where a protocol fails and that a NAT is responsible. Also, there is very little an individual user can do to overcome problems created by NATs. Proposed solutions – intelligent NATs that can be reprogrammed for new protocols, middle-box interfaces to let hidden computers find NATs and control them, and alternative translations that decouple end addresses from connection addresses – all eventually revisit some level of this problem.

The best solution is to avoid NATs altogether and insist on real Internet addresses. Some ISPs can provide real IP addresses for a small additional charge. If yours does not, shop around. In the current version of IPv4, addresses might be in short supply if we all ask at once. This shortage might be the needed incentive for ISPs to support IPv6, which has more than enough address space.

Also, don't be fooled by so-called DSL/cable "routers"; they're just NATs in disguise. If you want a router, insist that it actually routes. You might not have a protocol that breaks under NATs now, but (to paraphrase Yoda), *you will.*

Joseph D. Touch is the director of the Postel Center for Experimental Networks at the University of Southern California's Information Sciences Institute where he also serves as a research associate professor.