TetherNet Anti-NAT – Secure Internet Subnet Rental System

Joseph D. Touch, Lars Eggert, Yu-Shun Wang
USC/Information Sciences Institute
{touch, larse, yushunwa}@isi.edu

Abstract[1]

TetherNet is a system for dynamically relocating Internet subnets. It provides real Internet service consisting of real IP addresses, and forward and reverse DNS, even behind NAT boxes. TetherNet has been used to support demos at numerous DARPA PI meetings, and provides on-demand infrastructure for real network experiments.

1. Introduction

TetherNet is a NAT-like router box that provides leased Internet connectivity in environments with less-than-complete Internet access. At home, in remote labs, or at conference demonstration facilities, network connectivity can challenge Internet assumptions. When installed in such environments, TetherNet can restore complete Internet access, thus reversing the effects of a NAT – in effect, an "anti-NAT".

2. Pesky NATs and Other Issues

Networks often advertise Internet access even when they violate basic Internet principles. Complete Internet access assumes that client machines are granted unique, globally-routable Internet addresses. However, in many cases "the Internet" means a connection behind a NAT box. In those cases, all the hosts behind a NAT use a translator which modifies packets, and can break many Internet protocols [3].

For many network protocols, addresses are not enough; they require forward (name to number) and reverse (number to name) DNS entries as well. Consider *telnet*, commonly used for remote login during debugging. To confirm that the login is proceeding, *telnet* prints the name of the machine just before asking for the username and password, where that name is the reverse DNS of the IP address of the connection. If the DNS entry is missing, telnet waits (often up to 30 seconds) before proceeding anyway; such delays are at best annoying, and at worst debilitating during time-critical debugging. Similar lookups can stall web server access as well.

In some places, ISPs provide real IP addresses via DHCP, but use very short lease times and change the address frequently. This 'lease spinning' complicates demos, because the client IP address changes during the experiment.

There are a number of other components to Internet access, including dynamic address assignment (DHCP), DNS configuration, default mail forwarding, etc. Any of these components, when missing, can make the difference between a seamless network access experience and frustration.

3. TetherNet Solution

TetherNet solves this problem much as any competent network engineer would – by tunneling traffic back to a real Internet access point. TetherNet combines a thorough tunnel configuration together with remote automation, making setting up a remote network as easy as using a NAT box.

Figure 1 TetherNet box (11"x6"x1")

TetherNet relies on a set of remote lease sites, preconfigured and available to lend blocks of real

[1] Effort sponsored by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement number F30602-01-2-0529 entitled "DynaBone". The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Defense Advanced Research Projects Agency (DARPA), the Air Force Research Laboratory, or the U.S. Government.

0-7695-1897-4/03/$17.00 (C) 2003 IEEE

Internet addresses (possibly for a fee). The TetherNet client resembles a NAT box, the latter also known as a home router, though that is closer to what TetherNet does and NATs fail to do. TetherNet sits on the wire between the WAN (wall connection) and LAN (network in the room), as shown in Figure 2. TetherNet is configured the same as NAT boxes (e.g., Linksys, SMC, etc.), using a web browser on a client (e.g., PC) on the LAN.

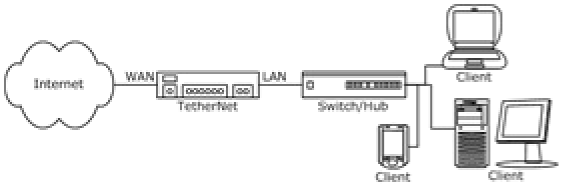


Figure 2 TetherNet location

Just as with NATs, TetherNet allows the user to attach the box using DHCP or static addresses to the WAN (e.g., DSL Ethernet, cable router Ethernet, etc.). Just as with NATs, TetherNet allows the user to configure the box's wireless (channel, SSID, WEP key), or set a variety of other local parameters.

When the TetherNet is initially installed, it is, in fact, a NAT box, translating addresses of a number of machines on the LAN side, just as any NAT would. What makes TetherNet different is its "lease" menu, and how it can reverse the effects of a NAT.

4. Demo Description

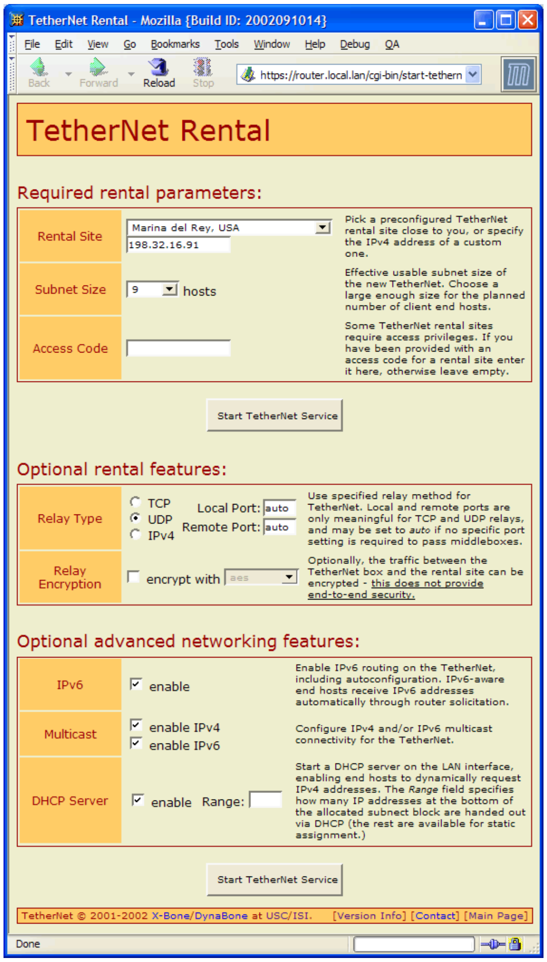
TetherNet rents blocks of IP addresses, then provides that rented set via DHCP to the LAN. It tunnels traffic between the LAN and the rental site, encrypting it if desired.

A sample rental request is shown in the browser snapshot in Figure 3. A rental site is selected, and a subnet size is requested. Access codes are required for certain subnets, e.g., one subnet might be internal to a corporate site.

The tunnel can utilize UDP, TCP, or IP (though the first two are required to traverse NATs), and port selection is automatic unless overridden. Tunneled packets can be encrypted with a variety of algorithms.

TetherNet provides complete IPv4 and IPv6 rental, including multicast and DHCP. Some of these features can be disabled or managed as well.

The tunnel configuration, requiring configuring components both at the TetherNet box and at the lease site, is completely automated. The tunneling mechanism is based on the X-Bone IP overlay architecture and allows recursion [2][4]; one TetherNet box can be attached to another, etc., providing additional address space as needed.


TetherNet Rental - Mozilla {Build ID: 2002091014}
File Edit View Go Bookmarks Tools Window Help Debug QA
Back Forward Reload Stop
https://router.local.lan/cgi-bin/start-tethern
Done

TetherNet Rental

Required rental parameters:

Rental Site	Marina del Rey, USA 198.32.16.91	Pick a preconfigured TetherNet rental site close to you, or specify the IPv4 address of a custom one.
Subnet Size	9 hosts	Effective usable subnet size of the new TetherNet. Choose a large enough size for the planned number of client end hosts.
Access Code		Some TetherNet rental sites require access privileges. If you have been provided with an access code for a rental site enter it here, otherwise leave empty.

Start TetherNet Service

Optional rental features:

Relay Type	○ TCP ● UDP ○ IPv4 Local Port: auto Remote Port: auto	Use specified relay method for TetherNet. Local and remote ports are only meaningful for TCP and UDP relays, and may be set to *auto* if no specific port setting is required to pass middleboxes.
Relay Encryption	□ encrypt with aes	Optionally, the traffic between the TetherNet box and the rental site can be encrypted - this does not provide end-to-end security.

Optional advanced networking features:

IPv6	☑ enable	Enable IPv6 routing on the TetherNet, including autoconfiguration. IPv6-aware end hosts receive IPv6 addresses automatically through router solicitation.
Multicast	☑ enable IPv4 ☑ enable IPv6	Configure IPv4 and/or IPv6 multicast connectivity for the TetherNet.
DHCP Server	☑ enable Range:	Start a DHCP server on the LAN interface, enabling end hosts to dynamically request IPv4 addresses. The *Range* field specifies how many IP addresses at the bottom of the allocated subnet block are handed out via DHCP (the rest are available for static assignment.)

Start TetherNet Service

TetherNet © 2001-2002 X-Bone/DynaBone at USC/ISI. [Version Info] [Contact] [Main Page]

Figure 3 Renting a subnet (browser snapshot)

5. Related Work

TetherNet is a version of a VPN, providing VPN-like remote access for a network. VPNs traditionally support remote access for a single client. TetherNet provides remote access for an entire network, renting a subnet from the remote site. TetherNet further serves that network via DHCP to the LAN. VPNs clients typically do not support subordinate clients.

There are notable advantages to the TetherNet system, compared with custom VPN solutions [1]. TetherNet supports all protocols that use IP, including experimental application protocols. It requires no support from the client hosts, so that PCs, PDAs, and other network appliances require no custom software. It can be used to coordinate secure remote access, such as for home access to corporate networks.

TetherNet establishes connections behind NAT boxes or where DHCP leases are short. It provides a complete Internet environment in both cases; this differs from NATs and the numerous ways in which they break Internet protocols [3].

6. Status

TetherNet has been used for several meetings and demos, including over a dozen DARPA PI meetings (each meeting concurrently supporting dozens of demos), numerous remote demonstrations at hotels, universities, and conferences, and secure home VPN access.

Each TetherNet rental box currently costs approximately $600 including wireless, and less than $400 for a wire-only system. It is a turnkey system, with current firmware comparable to commercially-available NAT boxes.

TetherNet is currently available for limited demonstrations from USC/ISI on a per-case basis. We are currently seeking a vendor to provide TetherNet access as a service.

For more information:

- http://www.isi.edu/tethernet

7. References

[1] Scott, C., Wolfe, P., Erwin, M., *Virtual Private Networks*, O'Reilly & Assoc., Sebastapol, CA, 1998.

[2] Touch, J., “Dynamic Internet Overlay Deployment and Management Using the X-Bone,” Computer Networks Jul. 2001, pp. 117-135. Previously in Proc. ICNP 2000, pp. 59-68.

[3] Touch. J., Those Pesky NATs. IEEE Internet Computing, July/August 2002, pp. 96.

[4] Touch, J., Wang, Y., Eggert, L., “Virtual Internets,” ISI Technical Report ISI-TR-2002-558, July 2002.