

The sys admin's daily grind: Miredo

EXPLORING THE TUNNEL

The move from IPv4 to IPv6 must be gradual rather than abrupt. After just two minutes of configuration work, Charly leans back and watches his first IPv6 packets pass through a Miredo tunnel.

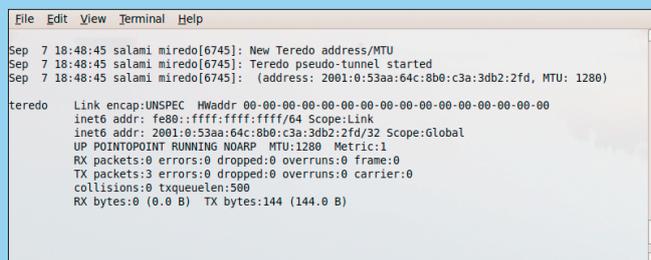
BY CHARLY KÜHNAST

Network component manufacturers are still spreading the dread tidings: IP addresses are becoming scarce. Stories spread of large access providers buying out smaller ones to get their hands on their IPv4 address pools. If you prefer not to be a victim of the digital famine, you need to switch quickly, says the industry that offers IPv6-capable switches and gateways.

But really, not many access providers can give you native IPv6. In fact, in the context of discussions on IPv6, the word “move” doesn’t seem to be all that appropriate. “Co-location” sounds more like it but does tend to remind one of grammar lessons at school. “Dual-tracking” is maybe the best option, because a peaceful coexistence of IPv4 and IPv6 is likely to become the rule, rather than the exception, in the near future.

If you are a customer with an IPv4 provider and would like to add IPv6 to

your home network, many tunneling solutions are around that you can try. Configuring them will typically require admin-level skills and is probably beyond the ability of less experienced users, who simply want to explore the field. Teredo solves this problem. The technology,



```
File Edit View Terminal Help
Sep 7 18:48:45 salami miredo[6745]: New Teredo address/MTU
Sep 7 18:48:45 salami miredo[6745]: Teredo pseudo-tunnel started
Sep 7 18:48:45 salami miredo[6745]: (address: 2001:0:53aa:64c:8b0:c3a:3db2:2fd, MTU: 1280)

teredo Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet6 addr: fe80::ffff:ffff:ffff/64 Scope:Link
inet6 addr: 2001:0:53aa:64c:8b0:c3a:3db2:2fd/32 Scope:Global
UP POINTOPOINT RUNNING NOARP MTU:1280 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 B) TX bytes:144 (144.0 B)
```

Figure 1: The tunnel gives you a sneak preview of the IPv6 future. This example uses the prefix 2001::/32.

which was developed by Microsoft, sets up an IPv6 tunnel behind a NAT router and automatically distributes the required addresses. Teredo encapsulates the IPv6 payload in v4 UDP datagrams. The Teredo RFC 4380 points out that this is simply an interim solution – other people have been known to refer to it as a “dirty hack.”

This Is Not What Problems Look Like

Whatever your opinion, however, Teredo isn’t a bad choice for some cautious, initial steps toward IPv6. Setting up Teredo requires virtually no configuration work, and clients are available for any recent operating system. For example, the Linux Miredo [1] client is included with practically any popular distribution. On

my Ubuntu lab machine, all I needed to do was type:

```
apt-get install miredo
```

to both install the client and start the service. In less than a minute, I had a working IPv6 connection with a prefix of 2001::/32, as defined by the RFC (Figure 1), even though my client resides behind no fewer than two NAT gateways.

Miredo doesn’t need a modified kernel; instead, it runs completely in user-space. Although you need to launch Miredo as root to define the required interface parameters, it de-escalates its privileges to *nobody* after launch. The `-u username` option lets you specify a user other than *nobody*. Some distros create a *miredo* account during the installation.

Finally, a word about security: Whereas NAT routers, which just about every DSL user in the IPv4 world has, put up some kind of protection against undesirable access, IPv6 tears down these barriers. If you are worried about delving into ip6tables, you should at least bind all services suitable for this purpose to localhost (:::1). ■

INFO

- [1] Miredo:
<http://www.remlab.net/miredo/>

THE AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, fresh water aquariums, and learning Japanese, respectively.



SYSADMIN

Security Lessons 56

Troubleshoot a network problem or watch server transactions with Wireshark.

OpenVAS 58

Find security problems in remote systems and applications with OpenVAS.