

Welcome to TechNet Blogs [Sign in](#) | [Join](#) | [Help](#)

IPv6 Blog

News and comments on IPv6 from Sean Siler, IPv6 Program Manager

Teredo in Windows Vista: Designed with security in mind

I am pleased to present Christian Huitema as a "guest blogger" today. Thanks for contributing, Christian!

-Sean

Hi, I am Christian Huitema, Distinguished Engineer in Windows, and the author of the Teredo protocol specification [RFC 4380](#). For those who don't know what Teredo is, Teredo provides IPv6 access in environments otherwise limited to IPv4 and NAT. It enables application developers to deal with NAT traversal by simply using IPv6, instead of relying on a variety of proxying and tunneling techniques. Recently I have seen and heard some commentary on the security implications of using Teredo and I would like to address some concerns being discussed. In Windows Vista, we implemented Teredo responsibly, using the principle of "least exposure". Teredo connectivity is not turned on before an application has been specifically authorized to use it. When it is turned on, its connectivity services are limited to these authorized applications, and not usable by other applications that may be resident on the same PC. If Windows Vista detects that it is connected to an enterprise network, Teredo will not be turned on by default, even if some applications are authorized. With these precautions, I believe that Windows Vista is adopting the right security posture. In Windows Vista, Teredo provides controlled connectivity in unmanaged networks, without creating risks for enterprises networks.

First, some high-level background. More and more broadband users are deploying home networks and home routers. These routers incorporate a "network address translation" (NAT) function that allows a single IPv4 address to be shared by several computers in the home network. This works very well for some everyday tasks, like accessing web pages or mail servers. But the design of NAT does not naturally allow the incoming connections required for direct home to home transmissions, video or voice calls for example. To satisfy the users' requests to use this technology, application developers had to come up with a way to "traverse the NAT." They developed all kinds of solutions based on tunnels, proxies and other echo servers. All these solutions are different, costly to develop, and hard to maintain. They may also expose the enterprise networks to outside attacks, while being very difficult to control by firewalls. We designed Teredo with the IETF as a standard solution to this problem.

So, what actually happens? When two machines want to communicate using IPv6, they use the help of a Teredo server on the Internet to set up a direct UDP path between them. The UDP packets can be forwarded through the home routers, and inside these UDP packets, the hosts can exchange IP traffic. With Teredo, computers don't have to remain isolated behind these routers. They obtain global IPv6 addresses and join the global IPv6 Internet. They can communicate with other computers that use Teredo, and also with other computers that obtain IPv6 connectivity through any other means. They can participate in peer-to-peer applications, or even act as servers.

In Windows Vista, the user is safe by default because Teredo is subject to special rules in the Windows Firewall. An application will need special permission to use Teredo, different from just "listening on the local network" or even "listening on the regular Internet connections". By default, no application is authorized, and Teredo does not start. Teredo will only start when the users "opt in" and decide to authorize specific applications. For example, users may authorize applications like Windows Live Messenger if they want to enable direct video conferences between homes. Further, on Windows Vista, enabling Teredo does not expose all applications to the Internet. For example, the file and print sharing services are not authorized to use Teredo – they are meant to be used in the home network, not over the Internet. If no authorized application is currently active, the Teredo service will be placed in a "dormant" state, and the computer will not be visible from the IPv6 Internet.

I don't expect many people to use Teredo in corporate networks. There are other ways to deploy IPv6 in these networks, for example by using [ISATAP](#). Placing the users in control of connectivity in their own homes is the right decision, but in corporate networks IT managers would rather not delegate security decisions to their users. In fact, Microsoft implemented two important precautions to minimize risk for corporate networks. First, the Teredo implementation in Windows Vista detects whether the network is "managed", meaning Active Directory Domain Controllers are present, and to stay off if that is the case. Teredo can still be turned on, but only by users with administrative privileges. The second precaution is even more encompassing. To function, Teredo clients need to communicate with a Teredo server over UDP, using port 3544. IT managers can effectively prevent Teredo usage on their network by blocking UDP destination port 3544 at the network's edge.

Managed laptops pose a special case. They roam between the office and the home, not to mention airports and hotels. They don't need to use Teredo when connected to the corporate network, but they can certainly benefit from better connectivity when outside of work. For example, laptop users may want to use the "Windows Meeting" with remote collaborators when they are traveling. But these laptops are corporate properties, carrying valuable data, and the IT manager should decide how to arbitrate between security and connectivity. The implementation of Teredo in Windows Vista enables that. IT managers have a range of options to allow or disallow use of Teredo. For example, they can use Group Policy to control which applications get to use Teredo and which don't when the laptop roams outside of the corporate network.

Recently, we heard another concern about the packet format in Teredo, which supposedly is not easily handled by corporate firewalls. To put it mildly, I found that surprising. To start with, this is really a "corporate firewall" scenario, and, as I explained above, Microsoft recommends other ways than Teredo to deploy IPv6 in corporate networks. But even for the edge cases where organizations would use Teredo, the traffic is not hard to inspect. The packet format is well documented as a public standard, and Teredo traffic can be easily recognized by checking for the presence of constant 32-bit prefixes at fixed location in the header. That is much simpler than a lot of the "deep packet inspection" algorithms implemented in various products. That is also a lot simpler than the alternative to Teredo, which is to have a varied set of NAT traversal protocols developed by various application providers, without relying on any documented standard.

I expect Teredo to provide great benefits to application developers and thus to users of the Internet. For application developers, Teredo provides a very simple solution to the NAT traversal problem, using IPv6. For users, Teredo allows deployment of these applications in a controlled manner. Teredo provides IPv6 connectivity without requiring changes to the

home routers, home networks, or ISP services. The IPv6 connectivity is properly managed by the Windows Firewall, allowing users and IT managers to control the tradeoff between connectivity and security. This will enable IPv6 applications to be reliably deployed. These IPv6 applications, in turn, will motivate ISPs to offer native IPv6 service, moving to the next phase of the transition to IPv6. Over time, as IPv6 connectivity becomes widely available, Teredo will become unnecessary and might be turned off. But for now, it is a valuable tool for IPv6 transition and provides a lot of value for the home user.

Published Friday, December 14, 2007 4:16 PM by [SeanSiler](#)

Comments

Saturday, December 15, 2007 2:36 PM by [Windows Vista Teredo Protocol » D' Technology Weblog: Technology, Blogging, Tips, Tricks, Computer, Hardware, Software, Tutorials, Internet, Web, Gadgets, Fashion, LifeStyle, Entertainment, News and more.](#)

Windows Vista Teredo Protocol & D' Technology Weblog: Technology, Blogging, Tips, Tricks, Computer, Hardware, Software, Tutorials, Internet, Web, Gadgets, Fashion, LifeStyle, Entertainment, News and more.

PingBack from <http://www.ditii.com/2007/12/15/windows-vista-teredo-protocol/>

Thursday, November 27, 2008 1:22 PM by [Living with IPv6](#)

IPv6 is not a security issue

Every now and then, I read an article claiming that IPv6 poses some sort of grave security threat by its mere existence. I had such an encounter today, which prompted this entry. IPv6 is not a serious security concern at...

Anonymous comments are disabled
