

## Re: Why Ping does not Work

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network\\_web/2004-08/2575.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2004-08/2575.html)

---

**From:** Chuck (*none\_at\_example.net*)

**Date:** 08/18/04

Date: 18 Aug 2004 12:30:17 -0500

On Wed, 18 Aug 2004 09:32:55 -0700, "Chaplain Doug"  
<anonymous@discussions.microsoft.com> wrote:

*>I cannot ping our remote server (which is connected to the  
>Internet), nor can I ping my server here in Richmond from  
>my home computer. However, I can ping my home computer  
>from my server in Richmond, and I can ping my home  
>computer from my remote server. Is there something I need  
>to turn on on our remote and Richmond servers (Windows  
>2000 Server) to allow them to be pinged?*

Doug,

Your servers are probably behind firewalls or routers that either block, or do not forward, pings. The days of routinely responding to a ping are long gone – net paranoia prevents it.

If you are able to ping your home computer, it is probably improperly protected, and possibly wide open to the worm of the month. Please protect yourself, and the rest of the internet.

Protection requires a good layered defense. Each layer is necessary because no layer produces complete protection.

The first layer is a NAT router (hardware firewall). If you have broadband internet, or PPP-compatible dialup internet, you can and should use a hardware firewall.

The second layer is a software firewall, or a port monitor like Port Explorer (free) from <<http://www.diamondcs.com.au/portexplorer/index.php?page=home>>. See various discussions in comp.security.firewall for good advice on choosing a firewall.

The third layer is good software. This layer has multiple components.

AntiVirus protection. Realtime, plus a regularly scheduled virus scan. Regularly updated.

## microsoft.public.windowsxp.network\_web: Re: Why Ping does not Work

Adware / spyware protection. Realtime, plus a regularly run adware / spyware scan. Regularly updated.

Complete instructions, using Spybot S&D and HijackThis (both free) are here: <<http://forums.spywareinfo.com/index.php?showtopic=227>>.

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use.

<http://www.jasons-toolbox.com/BrowserSecurity/>

<http://bcheck.scanit.be/bcheck/>

[https://testzone.secunia.com/browser\\_checker/](https://testzone.secunia.com/browser_checker/)

Block Internet Explorer ActiveX scripting from hostile websites (Restricted Zone).

<<http://netfiles.uiuc.edu/ehowes/www/main.htm>> (IE-SpyAd)

Block known dangerous scripts from installing.

<<http://www.javacoolsoftware.com/spywareblaster.html>>

Block known spyware from installing.

<<http://www.javacoolsoftware.com/spywareguard.html>>

Make sure that the spyware detection / protection products that you use are reliable:

[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

Harden your operating system. Check at least monthly for security updates.

<http://windowsupdate.microsoft.com/>

Block possibly dangerous websites with a Hosts file. Three Hosts file sources I use:

[http://www.accs-net.com/hosts/get\\_hosts.html](http://www.accs-net.com/hosts/get_hosts.html)

<http://www.mvps.org/winhelp2002/hosts.htm>

(The third is included, and updated, with Spybot (see above)).

Maintain your Hosts file (merge / eliminate duplicate entries) with:

eDexter <[http://www.accs-net.com/hosts/get\\_hosts.html](http://www.accs-net.com/hosts/get_hosts.html)>

Hostess <<http://accs-net.com/hostess/>>

Secure your operating system, and applications. Don't use, or leave activated, any accounts with names or passwords with trivial (guessable) values. Don't use an account with administrative authority, except when you're intentionally doing administrative tasks.

The fourth layer is common sense. Yours. Don't install software based upon advice from unknown sources. Don't install free software, without researching it carefully. Don't open email unless you know who it's from, and how and why it was sent.

The fifth layer is education. Know what the risks are. Stay informed. Read Usenet, and various web pages that discuss security problems. Check the logs from the other layers regularly, look for things that don't belong, and take

microsoft.public.windowsxp.network\_web: Re: Why Ping does not Work

action when necessary.

Cheers,

Chuck

Paranoia comes from experience – and is not necessarily a bad thing.