

## Re: Defending ARP Spoofing

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.ms-windows.nt.admin.security/2005-11/0005.html>

---

**From:** Karl Levinson, mvp ([levinson\\_k\\_at\\_despammed.com](mailto:levinson_k_at_despammed.com))

**Date:** 11/08/05

Date: Mon, 7 Nov 2005 19:45:25 -0500

"Chris" <[chrismc911@hotmail.com](mailto:chrismc911@hotmail.com)> wrote in message  
news:dklo1p\$01f\$1@news2.rz.uni-karlsruhe.de...

> *Hi all,*

>

> *I want to build up a resource containing all possibilities to defend ARP  
> spoofing. As I think ARP spoofing is one of the most powerful, easiest  
> and underestimated attacks I want to know all your tricks, patches,  
> anything that you know/apply to defend ARP spoofing.*

>

> *I know the standard things to do (like static ARP entries and so on),  
> what I want to know from you is something like:*

Here are some:

Use IPSec / VPN to verify client identities;

Use any solution that includes client certificates, such as SSL;

Use "port security" on switches to control which MAC addresses can access  
that switch port;

Use physical security and personnel security to ensure that people on your  
internal network are relatively trusted;

Train users to recognize and report the possible symptoms of ARP spoofing  
[this is rarely done in real life]; and/or,

Harden all your hosts as best you can against compromise using the usual  
methods;

Accept ARP spoofing as a theoretical risk.

I do not believe ARP spoofing happens all that frequently in real life.

Generally, someone doing ARP spoofing has physical or remote access to a  
host on your internal network. Someone that is in the position to do ARP  
spoofing is usually in the position to do whatever they want to you given  
enough time.

Before wasting a lot of time and money trying to defend against ARP  
spoofing, be sure you've done enough to get rid of the more commonly  
exploited vulnerabilities on your systems first. I don't know too many  
people that can say they are in that position.

comp.os.ms-windows.nt.admin.security: Re: Defending ARP Spoofing

- > *-OS x has a patch y which helps preventing ARP spoofing (like antidote)*
- > *or*
- > *-OS x in version y has a small built in ARP prevention (like SunOS)*
- > *or*
- > *-Firewall/IDS x is able to prevent/detect ARP spoofing*

None of these really exist as far as I know.