

## RE: Exploit code for IP Smart Spoofing

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-11/0221.html>

---

**From:** Stephen Gill ([gillsr@yahoo.com](mailto:gillsr@yahoo.com))

**Date:** 11/14/02

From: "Stephen Gill" <[gillsr@yahoo.com](mailto:gillsr@yahoo.com)>  
To: "'Laurent Licour'" <[llicour@althes.fr](mailto:llicour@althes.fr)>, <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>  
Date: Thu, 14 Nov 2002 09:09:31 -0600

Laurent,

Thanks for your note. In reality IP Smartspoofing is no different than ARP cache poisoning so I'm not entirely sure why a new name was "invented". In this particular case one is able to prevent the following:

- key ports and corresponding MAC entries are hardcoded and secured (ie gateways). If there is a MAC violation, this is logged and the port is shut down. 9 times out of 10 if someone is performing ARP spoofing they will go for a device that is best connected so consider this a fly trap.
- host ports are protected by only allowing one MAC address on a port at any given time with a lag of 5 minutes for timeout. Yes a station can change its hardcoded MAC. This will allow them to see at most the traffic of one other host on the switch. Not perfect, but the odds are greatly reduced.

A couple of ways that come to mind for having complete protection are:

- have a method of detecting duplicate MAC addresses on a switch
- enable "sticky" ARP. This will keep end stations from being able to change their MAC address, but at a potentially high administrative burden. I'll make a note of this option in the doc.

Cheers,

-- steve

-----Original Message-----

From: Laurent Licour [<mailto:llicour@althes.fr>]

Sent: Thursday, November 14, 2002 3:56 AM

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Cc: 'Stephen Gill'

Subject: RE: Exploit code for IP Smart Spoofing

Your document is quite usefull, but there is no way to protect against IP smartspoofing with a switch.

Smartspoofing use ARP cache poisoning of hosts.

Using a switch, you can only protect ag