

## Re: IP changes to 255.255.255.255??

**Source:** <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-04/0483.html>

---

**From:** Joe Mama (*Joe.Mama\_at\_SomeWhere.net*)

**Date:** 04/23/04

Date: Fri, 23 Apr 2004 09:41:06 -0500

"Joe Mama" <Joe.Mama@SomeWhere.net> wrote in message  
news:c616ak\$6p2si\$1@ID-102870.news.uni-berlin.de...

> "Aaron B. Lingwood" <ten.EGNUM.edonretni@reraos where munge='on'> wrote in  
> message news:513880ht3n8et2ls6gc9310f7s951cnojv@4ax.com...

>> On Mon, 19 Apr 2004 10:37:58 -0500, "Joe Mama"

>> <Joe.Mama@SomeWhere.net> wrote:

>>

>>> I have several print servers that the IP address changes to  
> 255.255.255.255

>>> I do not know what causes this. When I change them back to the required  
> IP

>>> they work for several days without problem. Then *\_bam!* they all get  
> changed

>>> back to 255.255.255.255 at the same time.

>>>

>>> These print servers have worked flawlessly for over a year and *\_no\_*  
there

> is

>>> no firmware updates available. They are DLink DP101p+ devices.

>>>

>>> The PC's on the network are all clean of viruses and trojans as far as  
I

> can

>>> tell.

>>> Has anyone had experience with the likes of this? Any ideas?

>>>

>>> Thanks in advance

>>

>>> Have you added a new XP machine or router (incl wireless router, adsl

>> modem/router) to the network? May be a problem with DHCP and/or an IP

>> Lease time.

>

>

> There is no DHCP being used anywhere. Also as far as the conflicting IP

> theory goes, that does not fly because it happens to all the print servers

> at the same instance and they all have different static IP's. This

instance

alt.computer.security: Re: IP changes to 255.255.255.255??

- > *is unfortunately in the wee hours of the morning while I am sound asleep.*
- > *Figures.*
- >
- > > *Could also be that another device on the network is attempting to use*
- > > *the same IP thus disabling the interface. This is often a staff member*
- > > *using their personal laptop.*
- >
- > *This is what I am leaning to because, well, it must be. I guess I'll*
- > *install SNORT on a machine and try to catch some (bastardized) machine*
- > *spewing the crap that causes the problem.*
- >
- > *I am amazed that every search I have preformed comes up empty for this*
- type
- > *of problem. I would have thought that someone, somewhere, sometime would*
- > *have had a (very) similar problem and effect that I could draw from.*
- >
- > *Thanks for the response Aaron.*

Update:

I have read the other posts and while all good info and suggestions, does not apply here or already covered. Thank you for the input.

Here is all I have had time to do concerning this problem to date:

The passwords have been changed.

SNORT is on that segment of the LAN (hoping to get a exploit signature match with source IP)<--- Me thinks this is going to be the answer to what the source is --->

DLink has been "zero" help and seems not to give a hoot beings it's on my network. (even though it affects their product and no others) go figure.

There are no firmware updates available for the product. I was hoping to flash them with an update to rid them of the symptom but that's not to be. They all have same firmware (v.2.00) and I tried one that has (v.2.10) but the same result last time the "hit" rolled by. There are 19 of these print servers affected. There is a total of 23 print servers on the network but the four that are not affected are other brands.(primarily HP)

I have ordered 3 different print servers form 3 different manufactures to put online and see what ones don't get "hit" next time this rolls around. They should be here today or Monday. Two of the replacement ones claim to be fully compatible with HP's JetDirect admin program and that leads me to believe they have the internal chip set that is not vulnerable to whatever it is I've got. :-)

At any rate if one of them works I will buy the required number to replace the el-cheap-o DLinks. I will report back results.

I have fired up the trusty ol'sniffer and am monitoring several of print servers ip addresses. This is to pin point the exact time of the hit and what they receive. Not looking forward to poring thru the capture. :-( But that should be helpful I think.

alt.computer.security: Re: IP changes to 255.255.255.255??

FWIW, this is a very low traffic network i.e. these are simply serving print jobs from an AS/400 to some barcode printer in manufacturing lines and probably only print 2 jobs an hour each printer. Yes they all have UPS's inline to the printers and PC workstations, transceivers and hubs.  
(lots-o-fiber)

Anyway the problem still exists. 19 Dlink DP101P+ print server's static IP changes to 255.255.255.255 once or twice a week. It has happened 5 times over the last 3 weeks and never had any problem in the past year and half they have been online. No other print servers are affected.

I will keep this thread posted as to any pertinent outcome/changes/solutions.

tia