

Re: Wireless Network in Public Places Options

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2005-02/0755.html>

From: Floyd L. Davidson (*floyd_at_barrow.com*)

Date: 02/13/05

Date: Sun, 13 Feb 2005 13:29:01 -0900

(This is a repost, because the original hasn't shown up in over an hour...)

Jeff Liebermann <jeffl@comix.santa-cruz.ca.us> wrote:

>On Sun, 13 Feb 2005 01:58:05 -0900, floyd@barrow.com (Floyd L.

>Davidson) wrote:

>We may be arguing semantics here.

You are. Please stop.

>To the best of my knowledge, a

>wireless router (such as the WRT54G) is a wireless bridge (also known

>as an access point) with an ethernet router hung on one of the

>switched ports. (A switch is a multi-port bridge). Therefore, if I

The earth is flat? ... despite all evidence to the contrary!

>replacement firmware. I will NOT concede that tweaking the router,

>that's not even in the data path, will do anything useful to affect

>the bridging between wireless clients.

I'll concede you were correct when you said you didn't know what you were talking about (a WRT54G).

> Had I known it this discussion would grow to acrimonious levels

I'm trying to get you to actually listen instead of just talk about the things you imagine to be true.

>However, I'm weird and prefer technical debates to product searches.

I prefer facts to your imagination, which is no different than marketing hype.

>>>I'm not sure how the WRT54G works.

>>So I noticed.

>

>Well, I have a WRT54G v1.1 sitting in the office that I could test.

Then test it and stop imagining what the test would show if it was built differently than it is. (I tested a version 2.0 unit.)

>I'm not thrilled with the time it takes to replace the firmware, but

A really severe constraint... all 53 seconds of wasted time.
(Well, okay... you need to add 30 seconds for a reset before and after. Call it 90 seconds.)

>I'm willing if I can find the time. There are also a few hot spots
>running in the area:

> <http://www.thirdbreak.org/hotspots.html>

>which are running mostly WRT54G hardware with alternative firmware. I

>guess this would be easier than modifying my own. I'll let you know

>what I find. It's gonna be weird walking in with two laptops, but

>I've done stranger things in the past. I'll also ask on their mailing

>list.

To what purpose? You might as well test more bridges to see if they route! It makes no difference how many hot spots are *not* configured to do that. The only reasonable test is to configure your own WRT54G and test it.

(Of course, if you luck onto even so much as one hot spot that does have it configured that way, that is a definitive test.
But who knows how many you'll need to test...)

>>>Well, a simple traceroute will usually detect the extra hop.

>>Traceroute won't even show that the WRT54G is there, never mind

>>an intruder.

>

>Oops, you're half right.

Actually, you are simply wrong again. Let me repeat that for you:

The WRT54G `_won't_ _even_ _show_ _up_ _with_ _traceroute_`, and there is no expectation that an intruder would be stupid enough to configure a node that would.

Again, you imagine what it might do, if it works as you assume.

But alas, I just described *precisely* what happens. No guessing involved. (Do you need the version number of my traceroute program? The serial number of my WRT54G??)

>With a man in the middle attack, the extra

>(laptop) router in the path will show up only if set to respond to

>ICMP or UDP pings. I guess that can be disabled. However, it would

>still show up as a "hop" in traceroute, although no info would be

>returned.

What traceroute returns depends on how the TTL field is handled.
It has nothing to do with either ICMP or UDP pings.

>>*Sigh. The WRT54G is an AP that routes. Probably others do to.*

>

>*I don't suppose it would help if I repeat myself once more.*

Don't be a boor, stop arguing silly semantics. It's an AP.

>>*Think wrong equipment, get wrong results. Don't install a*

>>*bridge, install a router. (Get one with an AP built in... :-)*

>

>*My contention is that*

Your contention is that semantics is more interesting than
equipment. I deleted it because I don't care...

>*If I'm wrong, I'll gladly admit it. I trip to the local hot spot*

>*should be sufficient. I'll do it today and see.*

You are in fact wrong, and that has been demonstrated already.

The logic of going to a local hot spot is the same as testing
bridges to see if they will route. It makes no difference how
many you find that do what you say, it only matters that the
WRT54G **does** route, regardless of what you say.

>*I wasn't aware that*

>*there was a point of contention when I first replied and therefore*

>*didn't verify my statements with prior testing.*

Imagination is always going to be a point of contention.

>*I agree that it's a*

>*good idea to test before one posts, but that's also impractical and*

>*time consuming.*

That is true if we are discussing proving the Theory Of
Relativity. But it took only minutes to test a WRT54G to see
that it does not work the way you describe.

>*However, I wanna do my own testing first.*

Then test before you make claims based on imaginary equipment.

Not that speculation is bad! But you've posted it as **fact**,
and when someone points to real examples that contradict your
speculation you obfuscate with illogical arguments, semantic
games, and irrelevant examples... and say it isn't true.

>>>Sorry. I missed the example. How do you control broadcasts by
>>>routing? Without a destination address, there's no way to direct
>>>broadcasts anywhere. That's why it had to be done on Layer 2 with
>>>VLAN 802.1q.

>>

>>So tell us what happens when the broadcast packet hits a router?

>>Is that done in Layer 2, according to VLAN 802.1q???

>

>With a VLAN, there's a few extra bytes tacked onto each packet that
>labels the virtual LAN in which the packet belongs. It's all layer 2.

>The tags are also attached to broadcasts, so that the switch knows
>which VLAN the packets need to stay inside. It's really kinda cool

>with wireless as it cuts down on excessive broadcast traffic. Here's
>a wireless VLAN implementation.

><http://www.cpx.com/whitepapers/Compex%20Psuedo%20VLAN.pdf>

You missed the point: It affects a lot more than Layer 2 when it
hits a router. Does it get routed, or not? If it does, it
certainly is not happening at Layer 2! (And of course if it
doesn't, none of the above is relevant then either!)

>>You responded to the OP's summary dismissal of your technically

>>_useless_ detail with a rebuke, which you claimed would "sting".

>>Yet you don't seem willing to read the *pertinent* technical

>>details provided to demonstrate where your analysis was

>>incomplete.

>

>Guilty as charged. How would you feel if I had replied to your long

>posting detailing your offered WRT54G solution to the hotel hot spot

>problem with a one line summary judgment? That, combined with some

>current personal problems tend to ruin what little diplomacy I have

>left.

The non-techie OP can logically respond with a one line summary
judgment to what you posted. Your response to my detail was
illogical, and far less appropriate than what the OP had to say.

You don't seem interested in learning about the equipment and
how to use it.

>I was hoping a for a bit more detail. In:

> 87u0okjj7z.fld@barrow.com

>you describe the use of two VLAN's, one for the ethernet, and one for

>the wireless as in the edited ifconfig output below (lo and WDS

>deleted):

>

> br0 Link encap:Ethernet HWaddr 00:12:17:27:FE:B8

> inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0

>

> eth0 Link encap:Ethernet HWaddr 00:12:17:27:FE:B8

>

> eth1 Link encap:Ethernet HWaddr 00:12:17:27:FE:BA
>
> vlan0 Link encap:Ethernet HWaddr 00:12:17:27:FE:B8
>
> vlan1 Link encap:Ethernet HWaddr 00:12:17:27:FE:B9
> inet addr:192.168.0.3 Bcast:192.168.255.255 Mask:255.255.0.0
>
>I agree that you can use the VLAN feature to isolate the two ethernet
>VLAN's from each other and possibly from the br0 (wireless) port.
>What I'm asking is if the same mechanism can be used to isolate
>individual users on br0 from each other. Methinks not or there would
>be multiple VLAN's showing on the wireless side.

That is not required to separate wireless clients.

>With all due respect, I just re-read **ALL** your previous postings in
>this thread and cannot find any comments where you've stated that two
>wireless clients cannot ping (or "see") each other. I may have missed
>something.

"Here's a route table copied from a WRT54G which
will not allow packets to be routed between
anything on the 192.168.1.0 subnet, ..."

Perhaps terse, and I realize that you have to apply some simple
logic to that statement to realize that it answers your
question. But I was assuming that you understood that ping uses
routed packets, and if there is no route... then two wireless
clients cannot ping each other.

You might even have drawn the conclusion (giant leap of faith
that it is) that the only reasonable way I would know it does
not route packets between wireless clients would be because I
tried to ping one wireless client from another (or in this case,
a couple of them) and found that it failed, while at the same
time it was possible to ping hosts on the Internet via the
gateway. Why else would I say that it works the way I
described?

Do you need to know the version of ping?

@(#) Copyright (c) 1989 The Regents of the University of California.
All rights reserved.
\$Id: ping.c,v 1.39 2000/07/23 04:16:21 dholland Exp \$\br/>\$NetKit: netkit-base-0.17 \$

The OS, the specifications on the ethernet cables, or any other
of insignificant or obvious details?

>You've stated that you've tested your WRT54G, but I can't
>find how or what application was used for testing. I'm not looking

*>for a detailed procedure. Just a simple question: Can two wireless
>clients ping each other? Extra credit for using arping to ping by MAC
>address. If so, I'm correct. If not, I'm wrong.*

You aren't right about this either.

Whatever, if you aren't looking for a detailed procedure don't claim it can't be correct short of having a detailed procedure listed. The procedures and tests are trivial and obvious.

I see that this response does not contain an ounce of useful technical information. For me, that pretty much signifies there is no point in continuing the discussion. I'll certainly read whatever you have to say in a followup; but unless this gets back onto a technical track, absent the imagination and the semantic debates, I'm not likely to discuss it further.

--

Floyd L. Davidson

Ukpeagvik (Barrow, Alaska)

http://web.newsguy.com/floyd_davidson

floyd@barrow.com