

Make a Passive Network Tap

by **joe** on September 8, 2008

Table of Contents

intro: Make a Passive Network Tap	2
step 1: Parts	2
step 2: Tools	3
step 3: Strip wire	3
step 4: wire the first jack	4
step 5: Wire the second jack	4
step 6: Third jack	5
step 7: close it up	6
Related Instructables	6
Advertisements	7
Customized Instructable T-shirts	7
Comments	7

intro: Make a Passive Network Tap

This instructable will show you how to make an inexpensive network tap to monitor your network.

Companies like Network Optics make incredible taps, for all sorts of media, but if you have 10/100 home network then for \$18 in parts from home depot you can make a tap and send the output to YAF/snort/tcpdump/wireshark and see if any data is leaking that should not be.

I have been doing Flow Analysis lately instead of using other tools. I like [YAF](#) . Then again I work on it...

If you want to see step by step instructions on setting up a flow collection infrastructure look at [this wiki page](#).



step 1: Parts

You will need:

- 3x Leviton Multi Use Cat 5e Jacks (5G108-W)
- I used 2 white and 1 blue, to let me know which one is the tap.
- Leviton 3 port wall plate (#41080-3W)
- Handy Box
- 5 inches of cat 5 cable





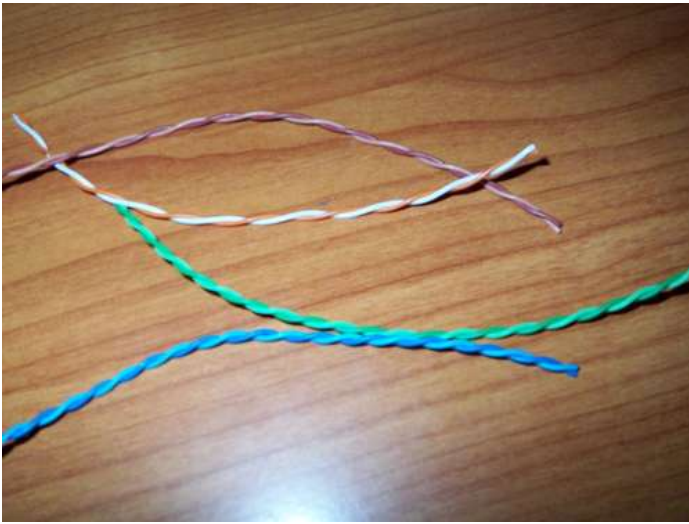
step 2: Tools

You will need a wire stripper and a screw driver.



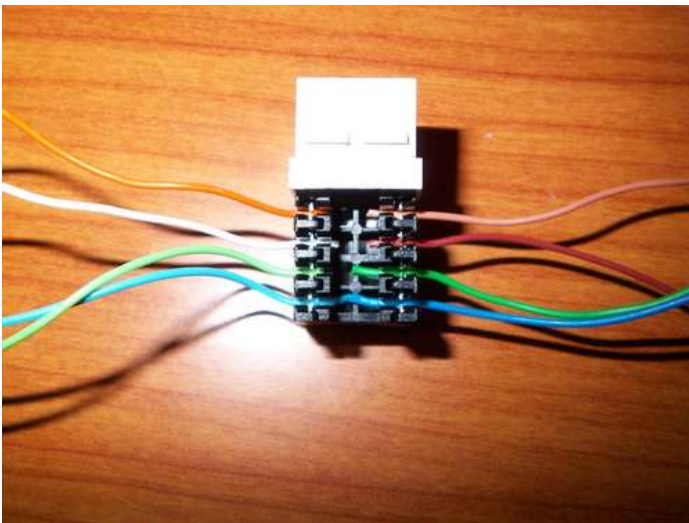
step 3: Strip wire

Cut 5 inches of cat 5 cable, and pull out the 8 strands of wire.



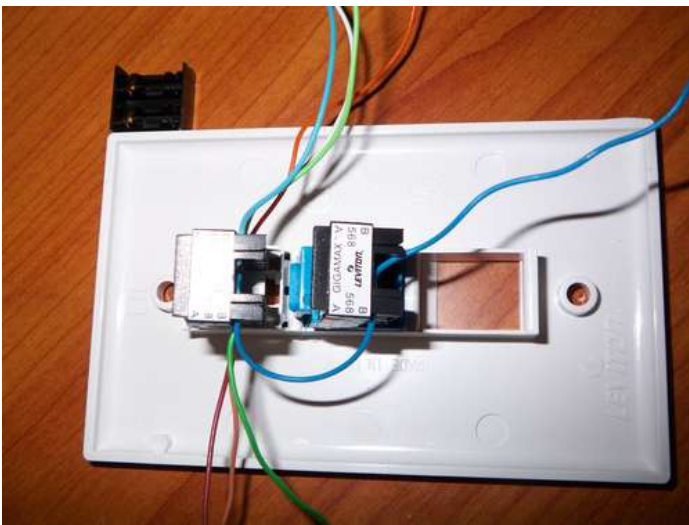
step 4: wire the first jack

Separate the strands of wire and wire up the leviton jack. It comes with a little punchdown tool to make this job easy. I followed the color code on the side of the jack, it does not really matter though, as long as you are consistent the whole way through.



step 5: Wire the second jack

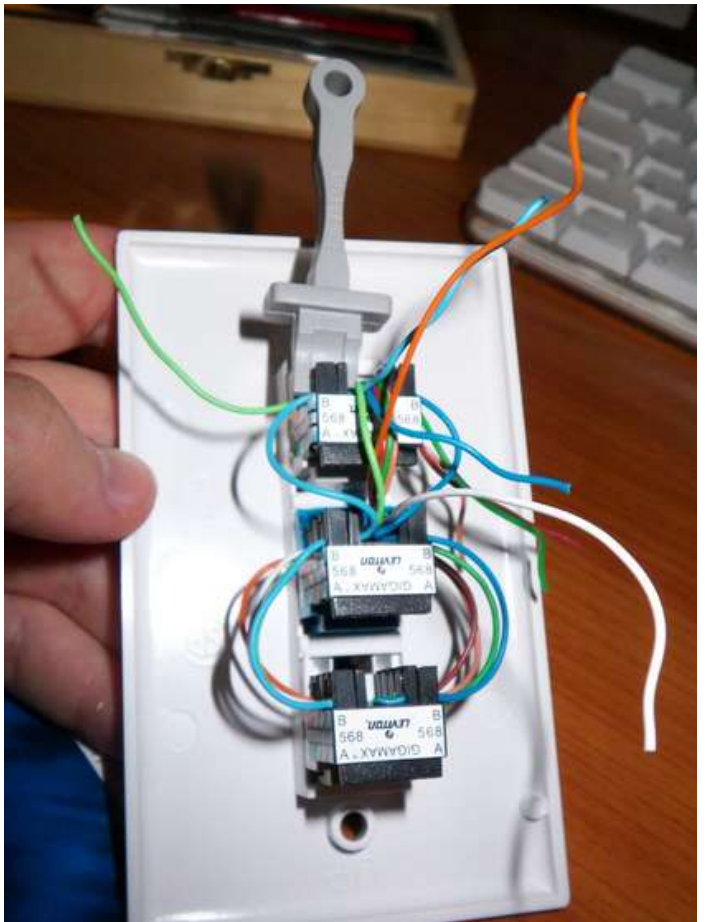
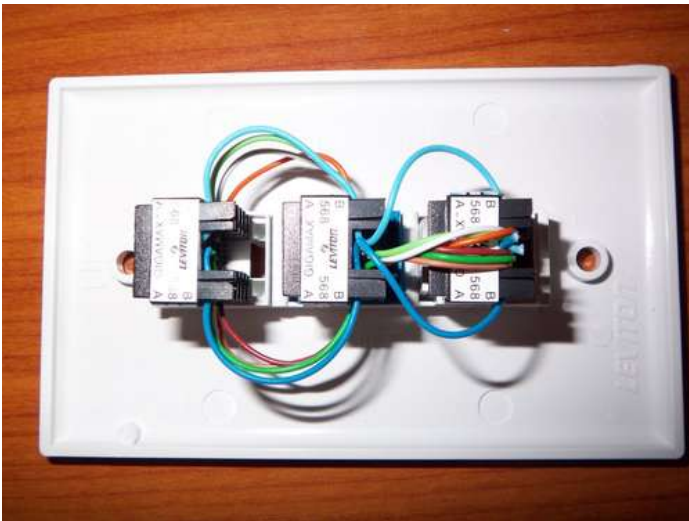
To wire the second jack, you should put both the jacks in the wall plate. Use the punchdown tool to put the wires in the jack using the color codes or same pattern as you did on the first jack. Make sure to leave enough wire left over to reach the third jack.



step 6: Third jack

To wire the third jack, drop the third jack in the panel then wire it up just like the 1st and 2nd.

Trim any excess wire.

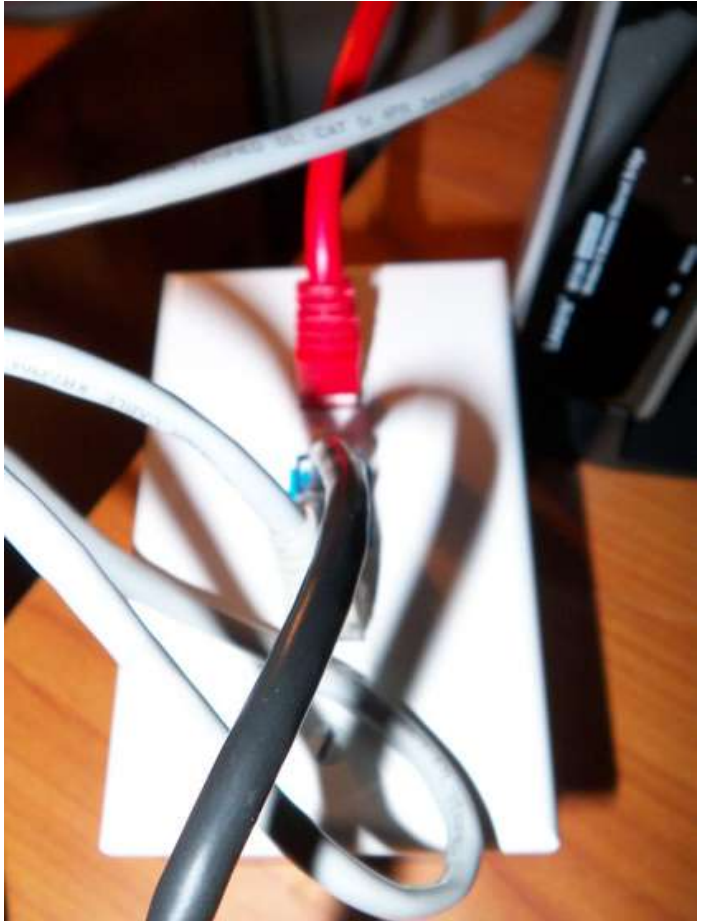
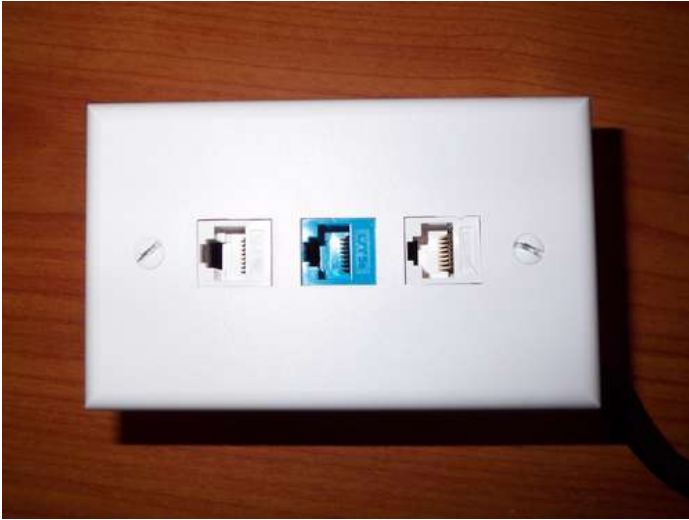


step 7: close it up

At this point you can close up the box and you are done.

Test it by hooking up the input in the top jack, snooping interface in the middle, and the destination on the bottom.

You can start up your snooping program and watch the traffic spin by. Make sure to have the snooping interface set to promiscuous mode and not assigned an ip.



Related Instructables



Maxwell House Wireless Antenna by burningsuntech



How to network a wireless printer by coolz



Urban Survival 101: Mobile Computing on the Fringe by johnnyallenshaw



Networking Drives by wrestler 103



Soft Reset Your Palm PDA Without Using the Reset Hole In the Back (DOES NOT APPLY TO FREEZES) by Aeshir



XP Security by stranoster



HP Scanjet5 upgrade by chrwei





Network Cards Notebook by arkangel





Comments


28 comments [Add Comment](#)


 **primekhan** says: Sep 17, 2008. 10:46 PM [REPLY](#)
Without twisting the pairs, what's to guard against NEXT (Near end cross talk)? It seems not have been a problem in your case, but if the desire is to monitor *all* traffic, perhaps it would be worth the time to make certain that the hardware wasn't causing any packet loss. Just a thought. I love your idea though!


 **nubie** says: Sep 17, 2008. 9:45 AM [REPLY](#)
Nice, I am very interested in the software tools that you use, it is much cheaper to buy a commercial connector for a \$1 if you don't have network stuff laying around:
http://www.monoprice.com/products/product.asp?c_id=105&cp_id=10513&cs_id=1051304&p_id=1112&seq=1&format=2
The 2 I bought are wired as your custom jack here, I opened mine and moved the pins around for use as normal t-splitters to put 2 100Mb LAN links through a single run of Cat5.
If you purchase these they should be wired identically to your box :)

 **dings** says: Sep 12, 2008. 1:31 AM [REPLY](#)
Bridge Couldn't you just put a box in between with two network cards, set up an ethernet bridge and listen to the traffic on the bridge?
I really like the idea by the way. What would be really nice was just two outlets and a "short circuit switch," so that traffic either could go through something connected to both or directly across.


 **benjamander** says: Sep 9, 2008. 3:26 PM [REPLY](#)
How is this better than just plugging the sniffer into your router/network switch? Wouldn't that allow the same thing?


 **baconfish** says: Sep 10, 2008. 4:44 PM [REPLY](#)
Routers and switches don't work that way. They keep track of which IP is connected to which jack and only forwards the packet on the appropriate connection.
Hubs, on the other hand, don't bother and will send everywhere.


 **Hoagie** says: Sep 11, 2008. 12:56 PM [REPLY](#)
There's a technique called ARP cache poisoning that makes switches send you the data but it's easier to use a hub if you can get one these days.


 **baconfish** says: Sep 11, 2008. 1:53 PM [REPLY](#)
True, I just kind of figured that defeated the whole "passive" thing.


 **Hoagie** says: Sep 12, 2008. 12:14 AM [REPLY](#)
Definitely. Some switches detect it as a security breach too.

 **joe** says: Sep 10, 2008. 4:43 PM [REPLY](#)
Its not better at all, if your router has the ability to do a span port, or if you a sniffer/tap you don't need this.
This would be more aimed at the home user who wanted to see , for example if non routeable traffic was making it past your linksys firewall.
Thanks for looking.
-Joe


 **wethecom** says: Sep 11, 2008. 9:22 PM [REPLY](#)
this is over my head but...dont laugh to hard for this suggestion...
couldn't you use windows xp or something like that and give everyone service
threw your machine and use wireshark to monitor the data
.....im more than sure i missed a few fine points in this discussion but wouldn't it be the same or at least similar results

 **redshirt3** says: Sep 11, 2008. 7:15 PM [REPLY](#)
Be careful with hooking in a hub, a switch is full duplex at the speed on each direction. A hub is not. you can lose critical packets. A hub will allow you to
insert packets into the stream. This solution is still better if stealth is required.

 **puffyfluff** says: Sep 11, 2008. 4:38 PM [REPLY](#)
Neat Idea, I never would have thought of this.

 **Zak** says: Sep 9, 2008. 1:17 PM [REPLY](#)
This may work a bit but is is not 'correct'. The snooping PC will have its input connected to one direction of communication, while the other direction is not
monitored, but even hampered as it is connected to the output of the 'snooping PC'.


TO do this right needs 2 network cards in the snooper, of which one RX pair listens to what goes from A to B, while the other listens to what goes in the
other direction (over a different wire pair).

 **Hoagie** says: Sep 11, 2008. 1:06 PM [REPLY](#)
That's true - especially the bit about the TX pair hindering the link.

Sometimes, just one direction is all you want. In those cases just connecting one pair in the sniffer socket and using one NIC would be fine. Can't
remember which pair is which off the top of my head though.

 **mackjr** says: Sep 10, 2008. 6:17 PM [REPLY](#)
your exactly right


 **mackjr** says: Sep 10, 2008. 6:17 PM [REPLY](#)
your exactly right Zak

 **joe** says: Sep 10, 2008. 4:45 PM [REPLY](#)
Hey Zak - You are correct, you can make the tap your are talking about and use two nics.


I have had success using this tap with fedora setting the nic to promiscuous and disabling arp and am able to see all traffic.


I'll put together another instructable showing the tap you are talking about.


Thanks for bringing this up.
-Joe


 **Spokehedz** says: Sep 11, 2008. 12:34 PM [REPLY](#)
The much easier solution (and indeed, a much more robust solution) is to find a cheap 10/100 HUB (not a switch) and put it in the middle of whatever you
want to monitor. yeah. The ones that are \$1 at fleamarkets.

Oldest trick in the book.

 **Marche** says: Sep 9, 2008. 12:00 PM [REPLY](#)
Awesome work dude!
Ill post pics when I finish building one inside a altoids tin for mobile tapping :3

 **joe** says: Sep 10, 2008. 5:26 PM [REPLY](#)
Thanks! I knew I should have jammed it in a altoids tin :)
-Joe

 **rancidbry** says: Sep 9, 2008. 12:25 PM [REPLY](#)
Sorry... stupid question. What exactly can you use this for? I can monitor my network using the network monitor application...

 **joe** says: Sep 10, 2008. 4:50 PM [REPLY](#)
Hey rancidbry- This would used for looking at all the traffic on your network not just what is being sent to your nic.

A way to use it would be say if you had a cheap firewall that did not have logging. Clearly you are dropping packets at the firewall for incoming smb
requests, but you do not have a way to see where they are coming from. You could place this between the firewall and cable modem, fire up wireshark
and see what was coming in.

-Joe



mrmath says:

Sep 8, 2008. 7:18 AM [REPLY](#)

Alright, stupid question time. I know that the pairs are twisted to deal with magnetic stuff. I used to know exactly why, but that was in a geekier lifetime.

Wouldn't you be better off leaving the wires as twisted as possible? Doesn't untwisting deteriorate the signal some? Or is the distance you're covering here so small that it won't make a difference? (That last one, by the way, doesn't seem possible, as the wires are pretty tightly wrapped.



tehmilller says:

Sep 8, 2008. 7:54 AM [REPLY](#)

The distance between the jacks here is too insignificant to cause much signal deterioration. For something like this, it doesn't really matter, at least in my experience. But watch someone come along and completely blow my theory out of the water :P



AllanButton says:

Sep 9, 2008. 9:49 PM [REPLY](#)

I have validated a 10ft run of Cat 5e that was completely untwisted, for 1gb speed.



frollard says:

Sep 8, 2008. 11:22 PM [REPLY](#)

In my network wiring classes, we were instructed when punching keep the wires twisted as long as humanly possible - but reality is that the tolerances are built into the hardware these days that a a millimeter or even an inch untwisted wont hurt you in noise/attenuation...much.



crapflinger says:

Sep 8, 2008. 10:00 AM [REPLY](#)

at this distance it shouldn't make a difference at all..you could just strip a small portion of the ethernet sheathing on the ends and just double punch the lines (i.e. two of the same color in each punch) but that could get a little funky



brs928 says:

Sep 9, 2008. 12:16 PM [REPLY](#)

I don't think it matters what jack you plug into for the incoming, monitoring, and outgoing cables. They're all just wired in parallel, so it makes no difference.