



Search Site

Search Rules

Account

email

password

LOGIN

[NOT REGISTERED?](#)[USER PREFERENCES](#)

CONSTRUCTION AND USE OF A PASSIVE ETHERNET TAP

by Michael Peters

This Tech Tip provides straightforward instructions on how to construct and use a passive Ethernet tap. The end product may be used with any hub or switch and any operating system. A passive Ethernet tap is useful when installing an intrusion detection system (IDS) sensor or when snooping Ethernet traffic.

Hardware Requirements

- A single 4-port Ethernet housing such as the Versatap AT44 Surface Jack Housing from [Allen Tel Products](#)
- 4 Category 5e modular snap-in jacks such as the AT55 Category 5e Modular Snap-In Jacks from [Allen Tel Products](#)
- A small section, about 6 inches, of Category 5e cable

Construction

Figure 1 represents the AT55 Category 5e jack. The wire termination pin positions and associated wire color codes are also shown.



Figure 1: AT55 Category 5e Jack

This diagram is usually included with new Category 5e jacks from any other vendor.

Disassemble the section of Category 5e wire that you have into eight separate wires. These wires should have the same color codes as in Figure 1.

The next step should be to partially assemble the Ethernet housing with the four jacks. These should snap into position easily. Once mounted, begin wiring the first jack position using the solid orange wire. Use the next diagram as a guide. The wires can be inserted with a small screwdriver or some other small flat tool.

Once you have terminated all eight wires, trim off any excess wire that remains. Snap the housing closed, and you should now have a completed passive Ethernet tap (see Figure 2).

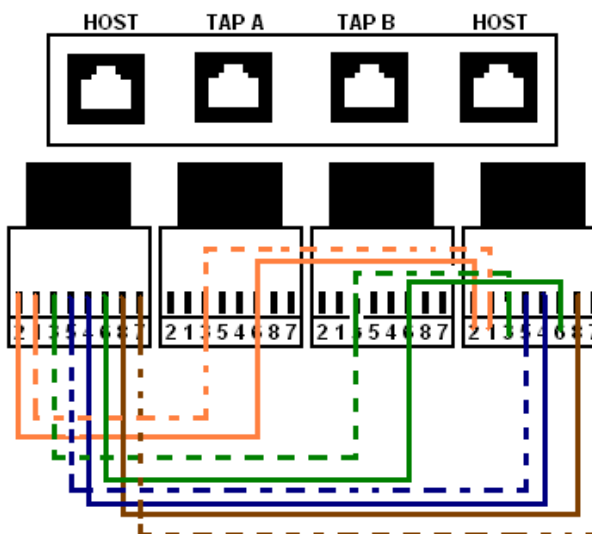


Figure 2: Passive Ethernet Tap

Instructions for Use

Place the passive Ethernet tap inline between a host machine and the Ethernet switch using the two outside positions labeled "HOST". Verify that the link status indicators on your host Ethernet interface and the Ethernet switch are connected again. You may now connect the Ethernet port of your sniffer or IDS sensor into the Tap A and/or Tap B connectors of the passive Ethernet tap.

Note: Keep in mind that when you have a full-duplex Ethernet connection, Tap A will show half-duplex traffic and Tap B will show the remaining traffic. You will need to use two Ethernet interfaces to examine both halves of the full-duplex signal. If you use Sun Trunking software, the traffic can be reassembled. See sun.com for information on [Sun Trunking software](#).

[site feedback](#) | [Terms of Use](#) | [Privacy Policy](#) | [forum archives](#) ©2007 Snort and Sourcefire are registered trademarks of Sourcefire, Inc. All rights reserved.