

## **How to sniff network traffic on a home network.**

The proliferation of home networks sharing cable or DSL connections to the Internet has brought about new challenges to the home guru. No longer is Mom or Dad just the person with the credit card able to buy new games, they are now faced with being a "Network Administrator".

Believe it or not, there are some sharp folks that have advanced beyond a few pings and trace routes and want to sniff their network.

Please note that this document is intended for a reader that is not a full time, trained network technician. Enterprise networks found in corporate environments have gear that is capable of avoiding some of the makeshift environment described later.

### **Definitions:**

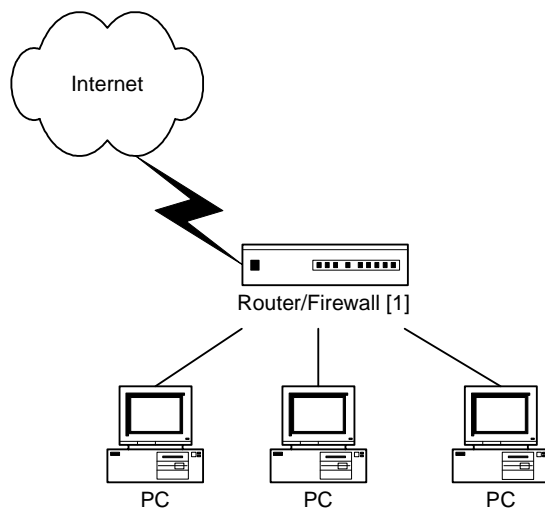
*Host*- anything on the network that can send and receive data, including a computer, router, firewall, etc.

*Hub*- a device that can have several computers connected. When network traffic from a computer is sent to it, the traffic is sent to all of the ports. The computer that is supposed to receive the traffic eventually filters out traffic bound for other computers and gets its information.

*Sniffer*- software that can gather data off of the network. Once gathered it can be analyzed for various reasons including troubleshooting, maintenance, or even eavesdropping on data that is not encrypted (AIM traffic comes to mind <grin>). I recommend Ethereal. It is available for Linux as well as Windows operating systems, plus the price is right (free). More information about Ethereal can be found at <http://www.ethereal.com>

*Switch*- looks like a hub but has much better performance because each port has a dedicated connection to all of the other ports. When a port receives traffic from a computer it knows which port the receiving host is on and sends it to that port. This eliminates collisions and all of the packets conglomerating in the hub's shared traffic medium.

The home networking gear is usually setup as follows:



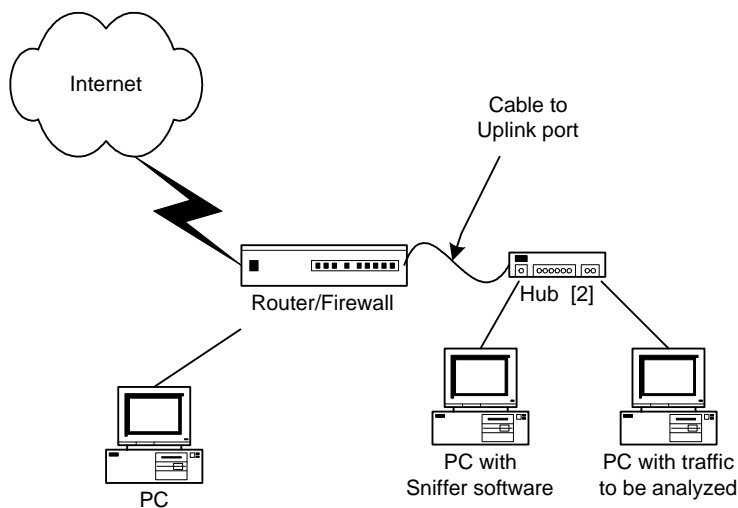
[1] This device is usually a switch with one port to connect to the Internet.

To be able to gather data (sniff) the first thing that must be done is to put the computer with the sniffer software and the computer to gather data from onto a hub. Doing so removes the isolation that occurs in a switch.

Most switches or hubs have a port labeled "Uplink". Plug a cable from a port on a hub to a port on the switch. NOTE: only one end must be plugged into an uplink port. There should be active link lights on the two ports used.

Plug the Sniffer computer and the computer to be monitored into the hub. You are now ready to start the sniffer program of your choice and begin capturing the packets.

Below is a diagram of the described setup.



[2] As many computers as there are available ports on the hub can be plugged in and analyzed. Beware, the data can become overwhelming!