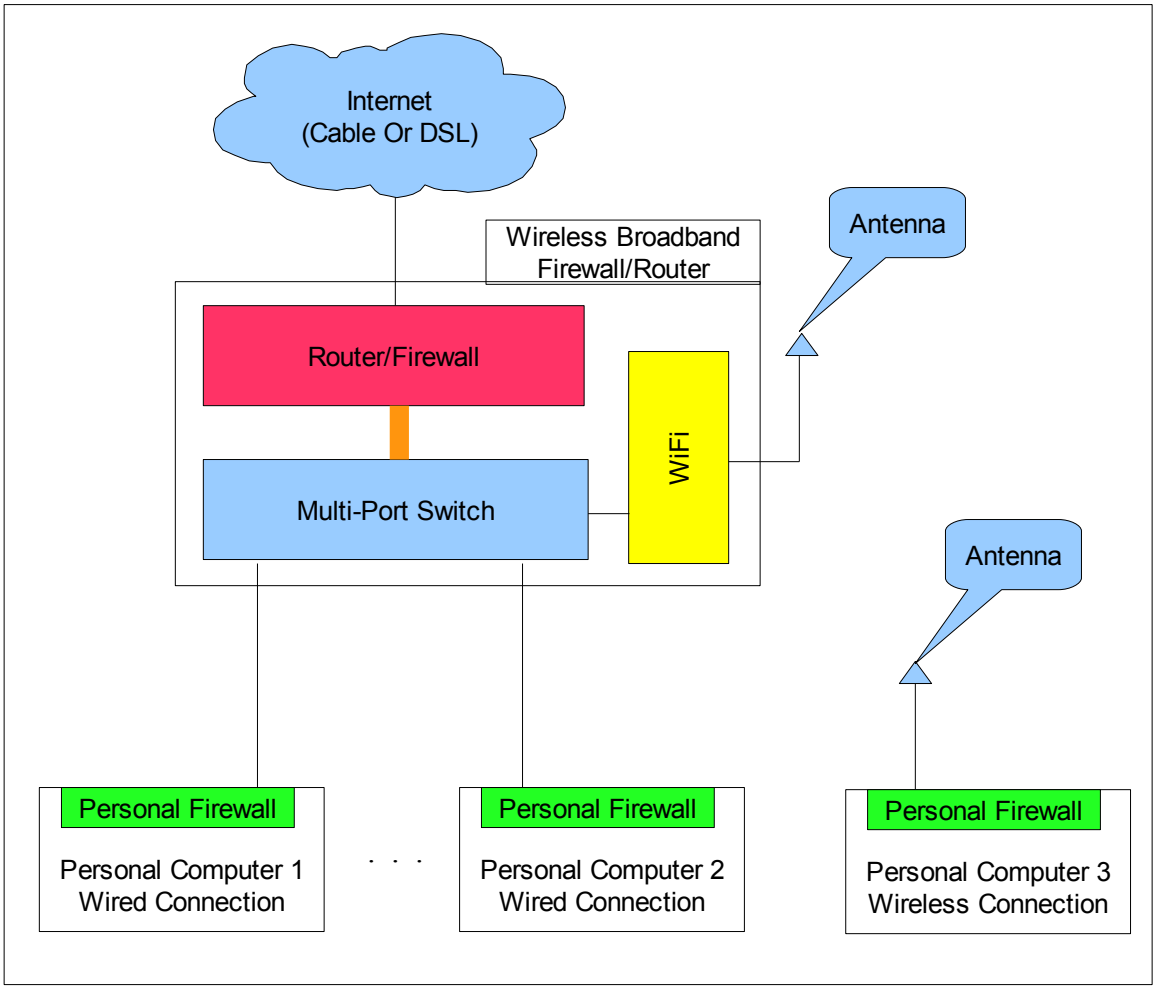
How Firewalls Work



The above diagram shows three personal computers connected to the Internet via a wireless broadband firewall router. The first two personal computers are directly wired to the built-in multi-port switch, while the third personal computer uses a wireless path.

The multi-port switch's job is to handle communication between all the computers connected to the wireless broadband firewall/router. The WiFi controller handles all the wireless connections and connects them to the multi-port switch.

The multi-port switch is connected to the router/firewall. That connection is shown as the thick orange line between the multi-port switch and the router/firewall. Notice that all connected computers must pass through this path to get to the Internet, but can communicate with each other without going through the router/firewall.

The purpose of the router/firewall (shown with the red background) is to ensure that no communications with the Internet are allowed unless initiated by one of the attached computers. This is a powerful defense from probe attempts initiated from the Internet.

It is possible for a computer connected to your wireless broadband firewall router to become infected via a transaction it initiated. This happens all the time when folks surf to sites that serve up malware. Notice that the router/firewall is not in a position to protect the other attached computers from the one(s) that become infected. That is the job of the personal firewall, shown with the green backround.