Tor relays are also referred to as "routers" or "nodes." They receive traffic on the Tor network and pass it along. Check out the Tor website for a more [detailed explanation](https://www.torproject.org/about/overview.html.en#overview) of how Tor works.

There are three kinds of relays that you can run in order to help the Tor network: **middle relays, exit relays, and bridges**.

For greater security, all Tor traffic passes through at least three relays before it reaches its destination. The first two relays are **middle relays** which receive traffic and pass it along to another relay. Middle relays add to the speed and robustness of the Tor network without making the owner of the relay look like the source of the traffic. Middle relays advertise their presence to the rest of the Tor network, so that any Tor user can connect to them. Even if a malicious user employs the Tor network to do something illegal, the IP address of a middle relay will not show up as the source of the traffic. That means a middle relay is generally safe to run in your home, in conjunction with other services, or on a computer with your personal files. See our [legal FAQ on Tor](https://www.eff.org/torchallenge/legal-faq/) for more info.

An **exit relay** is the final relay that Tor traffic passes through before it reaches its destination. Exit relays advertise their presence to the entire Tor network, so they can be used by any Tor users. Because Tor traffic exits through these relays, the IP address of the exit relay is interpreted as the source of the traffic. If a malicious user employs the Tor network to do something that might be objectionable or illegal, the exit relay may take the blame. People who run exit relays should be prepared to deal with complaints, copyright takedown notices, and the possibility that their servers may attract the attention of law enforcement agencies. If you aren't prepared to deal with potential issues like this, you might want to run a middle relay instead. We recommend that an exit relay should be operated on a dedicated machine in a hosting facility that is aware that the server is running an exit node. The Tor Project blog has these excellent [tips](https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment) for running an exit relay. See our [legal FAQ on Tor](https://www.eff.org/torchallenge/legal-faq/) for more info.

**Bridges** are Tor relays which are not publicly listed as part of the Tor network. Bridges are essential censorship-circumvention tools in countries that regularly block the IP addresses of all publicly listed Tor relays, such as China. A bridge is generally safe to run in your home, in conjunction with other services, or on a computer with your personal files.

For a more detailed analysis, check out EFF's [legal FAQ on Tor](https://www.eff.org/torchallenge/legal-faq/).