* **Difference between router and switch devices?**
* **Router:**
* A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to their intended [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and allowing multiple devices to use the same Internet connection.
* Layer 3
* **Switch:**
* Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
* **What is the routing table?**
* A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.
* **What is the difference between public and private IP?**
* **Public Ip:**
* These are public (global) addresses that are used on the Internet. A public IP address is an IP address that is used to access the Internet. Public IP addresses can be routed on the Internet, unlike private addresses.
* The presence of a public IP address on your router or computer will allow you to organize your own server (VPN, FTP, WEB, etc.), remote access to your computer, video surveillance cameras, and get access to them from anywhere on the global network.
* **Private Ip:**
* Private (internal) addresses are not routed on the Internet, and no traffic can be sent to them from the Internet; they are only supposed to work within the local network.
* **Difference between public and private subnets?**
* **Public subnet:**
* The servers within this sub network will have access to the internet (external Ip’s).
* **Private subnet:**
* The servers within this sub network will not have access to the internet (external Ip’s). For them to access the internet, they must go through NAT gateway.
* **Threat-mitigation methods?**

### Implement firewalls and antivirus software

### Establish network access controls

### Continuously monitor network traffic

* Conduct a risk assessment to determine vulnerabilities