What are channels? Would one be better than another?

Step 1:

A channel is a unique pathway where signals can travel in telecommunications generally.

A channel is one of several transmission pathways contained within a single link between network locations in the public switched telephone network (PSTN). For instance, the T-carrier system line service, which is widely used in North America, offers 24 64 Kbps channels for digital data transfer.

Step 2:

Because they don't overlap, certain channels perform WiFi better than others. The 2.4 GHz spectrum does really contain some channels that don't cross over with the others.

Why is WEP considered cryptographically weak?

Step 1:

The IEEE Wireless Fidelity (Wi-Fi) standard 802.11b contains the Wired Equivalent Privacy (WEP) security protocol. With the help of that standard, wireless local area networks (WLANs) will be able to maintain the same level of security and privacy as a traditional LAN.

Step 2:

Due to the low value of IVs, Wired Equivalent Privacy (WEP) suffers from vulnerability. All keys are recycled within a brief amount of time. Due to the fact that all encryption levels use the 24 bit IV, Wired Equivalent Privacy (WEP) suffers from the same flaw for all encryption levels.

With the amount of computer power that people carry around with them, a key this length is not very secure. Although WEP is not a good encryption standard, it is still more secure than nothing. It used a static key to encrypt all traffic to and from the access point, which was a flaw in the system.

What is the difference between WPA and WPA2?

Step 1:

A security standard for computing devices with wireless internet connections is called Wi-Fi Protected Access (WPA). The Wi-Fi Alliance created WPA to improve on the original Wi-Fi security standard, Wired Equivalent Privacy (WEP), in terms of data encryption and user authentication.

The Wi-Fi Protected Access security standard, or WPA2, is now in its second iteration and is therefore more secure than WPA. Most likely, both WPA and WPA2 security protocol options are available on your Wi-Fi router. WPA2 is the most secure Wi-Fi encryption to use when enabling it on your router.

Step 2:

Two security standards that safeguard wireless networks are WPA (Wi-Fi Protected Access) and WPA2 (Wi-Fi Protected Access 2). The Wi-Fi Protected Access security standard, or WPA2, is now in its second iteration and is therefore more secure than WPA.

Most likely, both WPA and WPA2 security protocol options are available on your Wi-Fi router. WPA2 is the most secure Wi-Fi encryption to use when enabling it on your router.

WPA2 is an improved version of WPA that builds a secure network using AES encryption and lengthy passwords. WPA2 is perfect for home users and organisations because it provides both personal and enterprise choices. However, if you have an outdated gadget, it can be slow or not work at all as it requires a substantial amount of computing power.

WPA2 is the better option for router owners since it is more secure than WPA, despite WPA being more secure than WEP. In order to increase the security of Wi-Fi connections, WPA2 mandates the use of more advanced wireless encryption than WPA does.

 Why do some networks run at 11 Mbps and others at 54 Mbps?

Step 1:

When utilised with other 802.11g devices, the 802.11g protocol supports data speeds of up to 54 Mbps. Up to four devices can be connected through wired RJ-45 connections at 100 Mbps, and the router is completely backwards compatible with the outdated 802.11b standard, which operates at 11 Mbps.

Stepv 2:

For ordinary broadband, an average good internet or broadband speed is 11 Mbps. Between 11Mbps and 50Mbps would be a quicker broadband speed. 100Mbps or more would be considered a very fast broadband speed.

A good internet speed would be between 10 and 11 Mbps for 1-2 persons. This is a typical, unrestricted broadband connection for usage with the internet in general. It is appropriate for occasional group video streaming, internet banking, and tasks like social media usage on various devices.

Why would someone want to use a Tor network?

Step 1:

The Onion Router, or Tor, is a piece of open-source, free software that makes it possible to communicate anonymously.

Step 2:

The purpose of Tor is to safeguard its users' right to personal privacy as well as their freedom and capacity for secure communication by employing Tor exit nodes to mask their IP addresses. Windows, IOS, Linux, BSD, and other Unix-like operating systems.

Many individuals use the Tor browser to access websites that aren't available on the surface web, view geo-restricted content, and avoid censorship. A area where unrestricted websites, pirated media, and illegal substances can be discovered is known as "the black web."

What do relay servers do in a Tor network? How do Tor networks provide anonymity?

Step 1:

Relays used by Tor are sometimes known as "routers" or "nodes." They take in traffic from the Tor network and forward it. For a more thorough breakdown of Tor's operation, visit its website. Middle relays, exit relays, and bridges are the three types of relays you can run to support the Tor network.

Step 2:

Onion sites, also called "hidden services," are found within the Tor network. By allowing traffic to enter or exit the network through nodes that only know the nodes that are immediately before and behind them in a relay, Tor makes it easier to browse anonymously. Encryption hides a message's origin and final destination.

Why is it still important to use an HTTPS connection if you are using a Tor network?

Step 1:

An application-layer protocol called Hypertext Transfer Protocol (HTTP) is used to send hypermedia documents like HTML. Although it was created for web browser and web server communication, there are other uses for it as well.

Even though Tor provides some privacy, it is insufficient to protect you from harm on the black web. Although there are many benefits to using Tor, it is also a haven for viruses and crooks. Your device and personal data are at risk even if you unintentionally click on the wrong link.

Step 2:

It's crucial because the connection between you and the server you're connecting to still has to be protected. It's not the end of the world if you're simply reading an article, but you must use HTTPS if you're logging into anything since else your login information could be stolen.

Tor isn't a magic solution for privacy and anonymity, though, as any data transferred via HTTP will be accessible to anyone eavesdropping if you aren't using HTTPS alongside Tor and your data is sent in plaintext once it leaves the Tor network.