

Cyber security deals with the danger in cyberspace. Information security deals with the protection of data from any form of threat.

An information security expert may develop the means of data access by authorized individuals or establish security measures to keep information safe. Cyber security, on the other hand, focuses on protecting information from cyber attacks such as ransomware and spyware.

Information Security is comparatively a much broader field than Cyber Security, as it allows one to protect not just digitally stored data but the overall confidential and important data that requires security and protection.

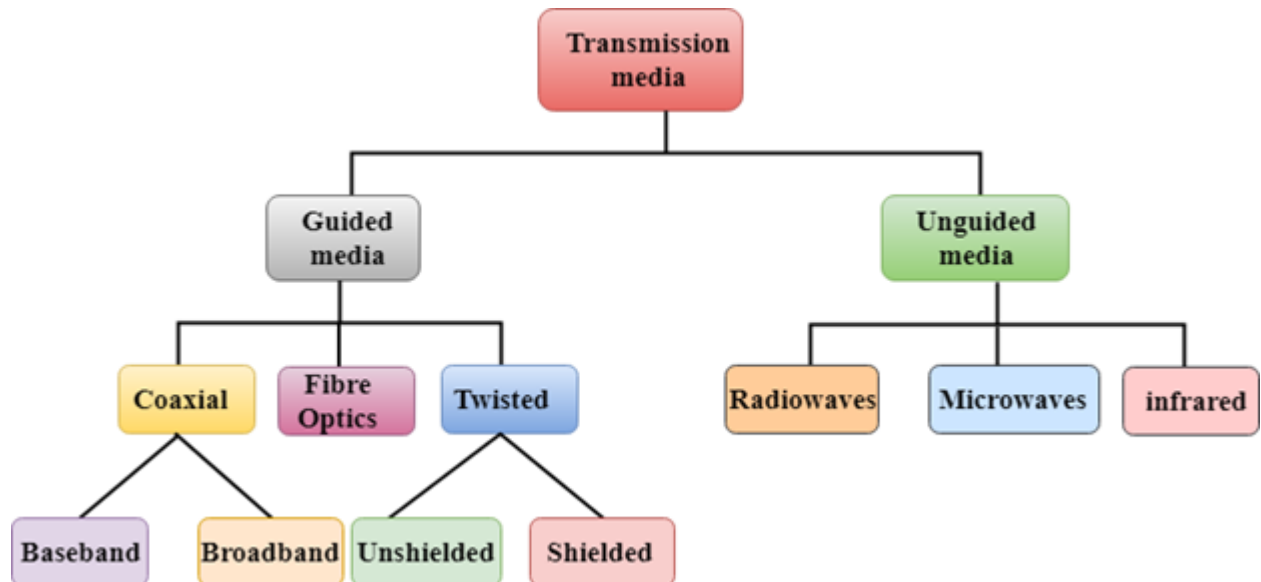
Information Security	Cyber Security
It protects all forms of data from unauthorized access, modification, deletion, etc., to provide CIA.	It mainly protects digital data from external threats like trojans, viruses, hackers, and other malicious activities that can take place on the internet.
It secures data from all types of attacks.	It mainly protects data available in cyberspace from various cyber threats.
It protects the various types of data.	It solely protects the data stored online.
It is the foundation of the security of data and professionals in this domain prioritize data sources before dealing with the threats.	Cyber Security professionals, on the other hand, deal with advanced and comp

Types of Cyber Security

There are various types of Cyber Security that professionals deal with on a regular basis. Some of them are listed below:

- **Network Security:** This type of security deals with securing networks from any misuse, interruption, unauthorized access, and service interruption.
- **Cloud Security:** It is a blend of several procedures, controls, technologies, and policies that are designed to work together to keep cloud-based systems and infrastructure secure.
- **Application Security:** This process helps to detect, fix, and enhance application security, enabling companies to prevent hackers from stealing their code and data that are in the applications.
- **Critical Infrastructure:** It involves a combination of tools that offer a range of security services, including anti-malware software, virus scanners, and more.

Classification Of Transmission Media:



The TCP handshake

TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps—SYN, SYN-ACK, and ACK—as shown in Figure below:

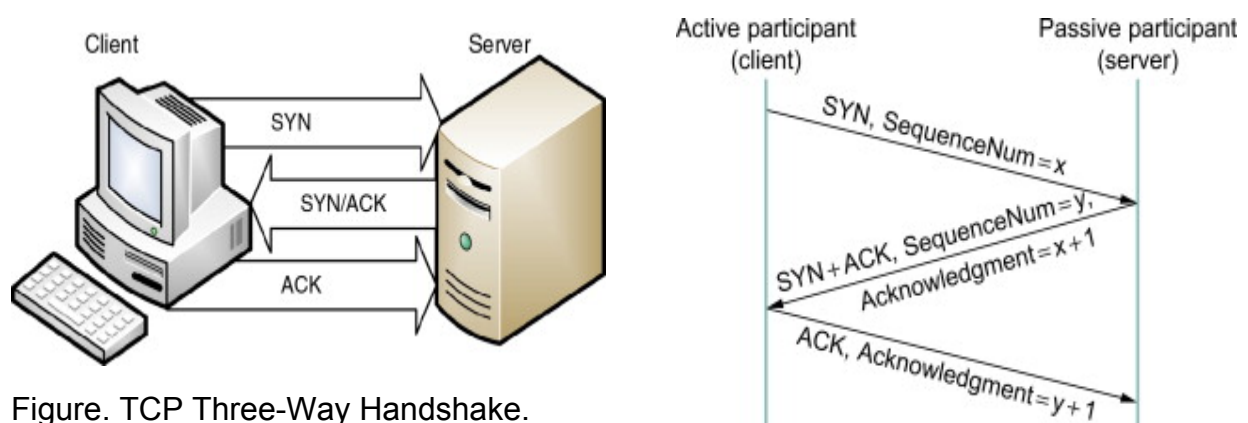


Figure. TCP Three-Way Handshake.

The client chooses an initial sequence number, the server also chooses its own initial sequence number, set in the SYN/ACK packet shown in Figure. Each side acknowledges each other's sequence number by incrementing it; this is the acknowledgement number. The use of sequence and acknowledgement numbers allows both sides to detect missing or out-of-order segments.

Once a connection is established, ACKs typically follow for each segment. The connection will eventually end with a RST (reset or tear down the connection) or FIN (gracefully end the connection).

Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

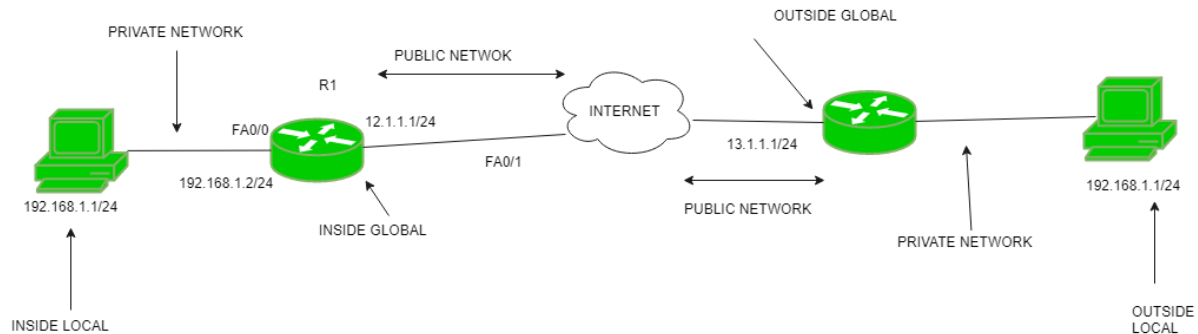
If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Why mask port numbers ?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies to the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are the same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address** – An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside global address** – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address** – This is the actual IP address of the destination host in the local network after translation.
- **Outside global address** – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

1. **Static NAT** – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.
Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.
2. **Dynamic NAT** – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be

dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT)** – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.