**Main Idea of Routing**

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of routing:

**1. Static routing –**   
Static routing is a process in which we have to manually add routes in routing table. 

**Advantages –** 

* No routing overhead for router CPU which means a cheaper router can be used to do routing.
* It adds security because only administrator can allow routing to particular networks only.
* No bandwidth usage between routers.

**Disadvantage –** 

* For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
* The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

1. **Default Routing –**

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn’t matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks. 

1. **Dynamic Routing –**

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. [RIP](https://www.geeksforgeeks.org/computer-network-routing-vs-routed-protocols/)(Routing Information Protocol) and [OSPF](https://www.geeksforgeeks.org/computer-network-open-shortest-path-first-ospf-protocol-fundamentals/)(Open Shortest Path First) are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol have following features: 

* The routers should have the same dynamic protocol running in order to exchange routes.
* When a router finds a change in the topology then router advertises it to all other routers.

**Advantages –** 

* Easy to configure.
* More effective at selecting the best route to a destination remote network and also for discovering remote network.

**Disadvantage –** 

* Consumes more bandwidth for communicating with other neighbors.
* Less secure than static routing.

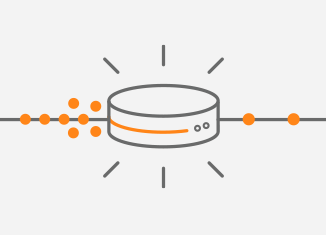
**What is TCP/IP?**

The Internet Protocol (IP) is the address system of the Internet and has the core function of delivering packets of information from a source device to a target device. IP is the primary way in which network connections are made, and it establishes the basis of the Internet. IP does not handle packet ordering or error checking. Such functionality requires another protocol, typically TCP.

The TCP/IP relationship is similar to sending someone a message written on a puzzle through the mail. The message is written down and the puzzle is broken into pieces. Each piece then can travel through a different postal route, some of which take longer than others. When the puzzle pieces arrive after traversing their different paths, the pieces may be out of order. The Internet Protocol makes sure the pieces arrive at their destination address. The TCP protocol can be thought of as the puzzle assembler on the other side who puts the pieces together in the right order, asks for missing pieces to be resent, and lets the sender know the puzzle has been received. TCP maintains the connection with the sender from before the first puzzle piece is sent to after the final piece is sent.

IP is a connectionless protocol, which means that each unit of data is individually addressed and routed from the source device to the target device, and the target does not send an acknowledgement back to the source. That’s where protocols such as the Transmission Control Protocol (TCP) come in. TCP is used in conjunction with IP in order to maintain a connection between the sender and the target and to ensure packet order.

**Network Congestion and Retransmission in TCP/IP**



Network congestion may occur when a sender overflows the network with too many packets. At the time of congestion, the network cannot handle this traffic properly, which results in a degraded quality of service (QoS). The typical symptoms of a congestion are: excessive packet delay, packet loss and retransmission.

Insufficient link bandwidth, legacy network devices, greedy network applications or poorly designed or configured network infrastructure are among the common [causes of congestion](https://www.noction.com/blog/network-congestion-technical-implications). For instance, a large number of hosts in a LAN can cause a broadcast storm, which in its turn saturates the network and increases the CPU load of hosts. On the Internet, traffic may be routed via the shortest but not the optimal AS\_PATH, with the bandwidth of links not being taken into account. Legacy or outdated network device may represent a bottleneck for packets, increasing the time that the packets spend waiting in buffer. Greedy network applications or services, such as file sharing, video streaming using UDP, etc., lacking TCP flow or congestion control mechanisms can significantly contribute to congestion as well.

The function of TCP (Transmission Control Protocol) is to control the transfer of data so that it is reliable. The main TCP features are connection management, reliability, flow control and congestion control.  Connection management includes connection initialization (a 3-way handshake) and its termination. The source and destination TCP ports are used for creating multiple virtual connections. A reliable P2P transfer between hosts is achieved with the sequence numbers (used for segments reordering) and retransmission. A retransmission of the TCP segments occurs after a timeout, when the acknowledgement (ACK) is not received by the sender or when there are three duplicate ACKs received (it is called fast retransmission when a sender is not waiting until the timeout expires). Flow control ensures that a sender does not overflow a receiving host. The receiver informs a sender on how much data it can send without receiving ACK from the receiver inside of the receiver’s ACK message. This option is called the sliding window and it’s amount is defined in Bytes. Thanks to the sliding window, a receiving host dynamically adjusts the amount of data which can be received from the sender. The last TCP feature – congestion control ensures that the sender does not overflow the network. Comparing to the flow control technique where the flow control mechanism ensures that the source host does not overflow the destination host, congestion control is more global. It ensures that the capability of the routers along the path does not become overflowed.

## **What is a Domain Name and How Does DNS work?**

The Domain Name System (DNS) is the Internet's system for mapping alphabetic names to numeric Internet Protocol (IP) addresses like a phone book maps a person's name to a phone number. For example, when a Web address (URL) is typed into a browser, a DNS query is made to learn an IP address of a Web server associated with that name.

Using the www.example.com URL, example.com is the domain name, and www is the hostname. DNS resolution maps www.example.com into an IP address (such as 192.0.2.1). When a user needs to load a webpage, a conversion must occur between what a user types into their web browser (www.example.com) into an IP address required to locate the www.example.com site.

The DNS system is an open worldwide network of database name servers that include 13 authoritative name servers that serve the DNS root zone level, known as "root servers". A root server (also called a DNS root nameserver) receives a DNS query that includes a domain name (e.g. www.thousandeyes.com), and responds by directing that request to a top-level domain (TLD) nameserver, based on the TLD of that domain such as .com, .net, and .org. It directly responds to requests for [DNS records](https://blog.thousandeyes.com/guide-to-dns-record-types/" \o "A Guide to DNS Record Types" \t "https://www.thousandeyes.com/learning/techtorials/_blank) in the root zone by returning an appropriate list of the authoritative TLD name servers for the appropriate TLD that can resolve the initial DNS lookup request for an IP address of that domain name.