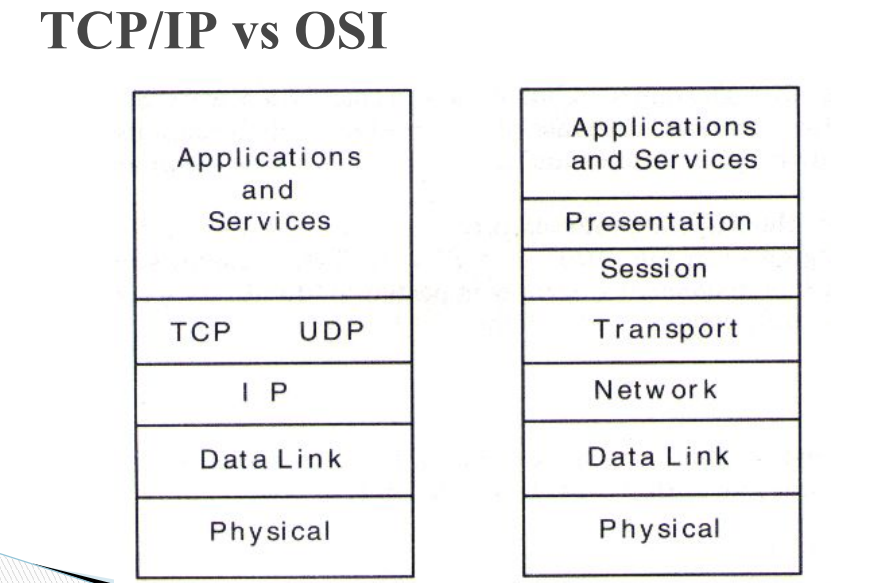
The TCPIIP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.



We will assume that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the application layer.

**Physical and Data Link Layers :** At the physical and data link layers, TCPIIP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

**Network Layer :** At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

**Transport Layer :** Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

**Application Layer :** The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model Many protocols are defined at this layer.

**TCP Vs UDP :**

|  |  |
| --- | --- |
| **TCP (Transmission Control Protocol)** | **UDP (User Datagram Protocol)** |
| 1. It is a communications protocol, using which the data is transmitted between systems over the network. In this, the data is transmitted into the form of packets. It includes error-checking, guarantees the delivery and preserves the order of the data packets. | 1. It is same as the TCP protocol except this doesn’t guarantee the error-checking and data recovery. If you use this protocol, the data will be sent continuously, irrespective of the issues in the receiving end. |
| 2. TCP is a connection oriented protocol. | 2. UDP is a connection less protocol. |
| 3. As TCP provides error checking support and also guarantees delivery of data to the destination router this make it more reliable as compared to UDP. | 3. While on other hand UDP does provided only basic error checking support using checksum so the delivery of data to the destination cannot be guaranteed in UDP as compared to that in case of TCP. |
| 4. In TCP the data is transmitted in a particular sequence which means that packets arrive in-order at the receiver. | 4. On other hand there is no sequencing of data in UDP in order to implement ordering it has to be managed by the application layer. |
| 5. TCP is slower and less efficient in performance as compared to UDP. Also TCP is heavy-weight as compared to UDP. | 4. On other hand UDP is faster and more efficient than TCP. |
| 6. Retransmission of data packets is possible in TCP in case packet get lost or need to resend. | 5. On other hand retransmission of packets is not possible in UDP. |

**DHCP**

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters. Request for comments (RFC) 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF)- defined standard based on the BOOTP protocol.

**DHCP simplifies IP address management**

The primary reason DHCP is needed is to simplify the management of IP addresses on networks.  No two hosts can have the same IP address, and configuring them manually will likely lead to errors. Even on small networks manually assigning IP addresses can be confusing, particularly with mobile devices that require IP addresses on a non-permanent basis. Also, most users aren’t technically proficient enough to locate the IP address information on a computer and assign it. Automating this process makes life easier for users and the network administrator.

## Components of DHCP

When working with DHCP, it’s important to understand all of the components.  Below is a list of them and what they do:

* DHCP server: A networked device running the DCHP service that holds IP addresses and related configuration information. This is most typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
* DHCP client: The endpoint that receives configuration information from a DHCP server. This can be a computer, mobile device, IoT endpoint or anything else that requires connectivity to the network.  Most are configured to receive DHCP information by default.
* IP address pool: The range of addresses that are available to DHCP clients. Addresses are typically handed out sequentially from lowest to highest.
* Subnet: IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
* Lease: The length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it.
* DHCP relay: A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. This can be used to centralize DHCP servers instead of having a server on each subnet.

## Benefits of DHCP servers

In addition to simplified management, the use of a DHCP server provides other benefits.  These include:

* Accurate IP configuration: The IP address configuration parameters must be exact and when dealing with inputs such as “192.168.159.3”, it’s easy to make a mistake. Typographical errors are typically very difficult to troubleshoot and the use of a DHCP server minimizes that risk.
* Reduced IP address conflicts: Each connected device must have an IP address. However, each address can only be used once and a duplicate address will result in a conflict where one or both of the devices cannot be connected. This can happen when addresses are assigned manually, particularly when there are a large number of endpoints that only connect periodically, such as mobile devices.  The use of DHCP ensures that each address is only used once.
* Automation of IP address administration: Without DHCP, network administrators would need to assign and revoke addresses manually.  Keeping track of which device has what address can be an exercise in futility as it’s nearly impossible to understand when devices require access to the network and when they leave.  DHCP allows this to be automated and centralized so network professionals can manage all locations from a single location.
* Efficient change management: The use of DHCP makes it very simple to change addresses, scopes or endpoints. For example, an organization may want to change its IP addressing scheme from one range to another. The DHCP server is configured with the new information and the information will be propagated to the new endpoints. Similarly, if a network device is upgraded and replaced, no network configuration is required.

## DHCP poses security risks

The DHCP protocol requires no authentication so any client can join a network quickly. Because of this, it opens up a number of security risks, including unauthorized servers handing out bad information to clients, unauthorized clients being given IP addresses and IP address depletion from unauthorized or malicious clients.

Since the client has no way of validating the authenticity of a DHCP server, rouge ones can be used to provide incorrect network information. This can cause denial-of-service attacks or man-in-the-middle attacks where a fake server intercepts data that can be used for malicious purposes. Conversely, because the DHCP server has no way of authenticating a client, it will hand out IP address information to any device that makes a request.  A threat actor could configure a client to continually change its credentials and quickly exhaust all available IP addresses in the scope, preventing company endpoints from accessing the network.

The DHCP specification does addresses some of these issues. There is a Relay Agent Information Option that enables engineers to tag DHCP messages as they arrive on the network. This tag can be used to control access to the network. There is also a provision to authenticate DHCP messages, but key management can be complicated and has held back adoption. The use of 802.1x authentication, otherwise known as network access control (NAC), can be used to secure DHCP.  Most of the leading network vendors support NAC, and it has become significantly simpler to deploy.