The IP Differentiated Services Code Point (DSCP)

The IP Differentiated Services Code Point (DSCP)

The Differentiated Services framework is defined in RFC 2474 and RFC 2475. This defines a set of network policies and rules for a network domain. A router reads the DSCP value in each received packet to classify the packet. Once the class has been determined, it is mapped to one of 64 possible forwarding behaviors known as Per Hop Behavior group (PHB group). Multiple DSCPs can be mapped to the same PHB group, but each PHB group has a queue in which the packets are stored prior to forwarding.

Each PHB provides a particular service level (capacity, queuing, and dropping decisions) in accordance with a network policy. The AF group allows packets to be preferentially discarded when a particular AF class is overloaded.

- At the edges of a Differentiated Services domain, packets can be conditioned. That is they can be policed (dropped according to a policy), remarked (assigned to a different DSCP) or shaped (delayed with respect to other traffic). This happens at the network edge to enforce the required treatment across the domain. For example, a packet with an EF DSCP can be admission-controlled to protect the network from overload by excessive EF traffic. The DSCP value CS6 and CS7 could also be blocked at the edge, when an operator uses these classes for network control traffic.
- Measurements in 2017 suggest it is safe to enable DSCP in enedpoints by setting a suitable value in the IP header. This is based on observations that packets are seldom dropped solely because a non-default DSCP was set. Applications though need to be aware that the DSCP they choose may (or may not) have an assigned PHB - that is the network could decide to ignore the DSCP value, or even to rest the field to another value.

- The 6bit DSCP is appended to the header of an IPv4 or IPv6 packet in order to ensure the packet receives a particular forwarding treatment as it traverses a DiffServ enabled IP network. Different DSCP values will be used to apply different forwarding treatment and as such, a packet must be classified before ingress to the network to make sure that packets are given the appropriate forwarding treatment.

TCP/IP Model

TCP/IP Model

- Prerequisite – Layers of OSI Model The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:
- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer
- What are the main 5 layers in TCP IP model?
- **Each host that is involved in a communication transaction runs a unique implementation of the protocol stack.**
- Physical Network Layer. The physical network layer specifies the characteristics of the hardware to be used for the network. ...
- Data-Link Layer. ...
- Internet Layer. ...
- Transport Layer. ...
- Application Layer.

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

- 1. Network Access Layer –

- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data. We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

- The Network Access Layer is a layer in the OSI model that is responsible for establishing a connection between a device and the physical network. It is responsible for transmitting and receiving data over the physical medium of the network, such as a wire or wireless connection.

- One common use case of the Network Access Layer is in networking devices, such as routers and switches. These devices use the Network Access Layer to establish connections with other devices on the network and transmit and receive data. For example, a router may use the Network Access Layer to establish a connection with a device on the network and then forward data packets to and from that device.

- Another use case of the Network Access Layer is in communication devices, such as phones and laptops. These devices use the Network Access Layer to establish a connection with a wireless or wired network and transmit and receive data over that connection. For example, a phone may use the Network Access Layer to connect to a wireless network and send and receive phone calls and text messages.

- **2. Internet Layer –**
- This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :
- **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
- **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.
- The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.
- Here is an example of a use case for the Internet Layer:
- Imagine that you are using a computer to send an email to a friend. When you click “send,” the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend’s computer can reassemble them into the original email message.
- In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend’s computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

- **3. Host-to-Host Layer –**
- This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :
- **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
- **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.
  - **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
  - **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
  - **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.
- The host-to-host layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing communication between hosts (computers or other devices) on a network. It is also known as the transport layer.

User Datagram Protocol (UDP)

User Datagram Protocol (UDP)

- **User Datagram Protocol (UDP)** is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.The UDP enables process to process communication.
- Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of the Internet services; provides assured delivery, reliability, and much more but all these services cost us additional overhead and latency. Here, UDP comes into the picture. For real-time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth. User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

- **UDP Header -**
- UDP header is an **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contains all necessary header information and the remaining part consist of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.
- **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
- **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
- **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

- **Notes -** Unlike TCP, the Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting. Also UDP provides port numbers so that is can differentiate between users requests.

- **Applications of UDP:**
- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
- The application layer can do some of the tasks through UDP-
  - Trace Route
  - Record Route
  - Timestamp
- UDP takes a datagram from Network Layer, attaches its header, and sends it to the user. So, it works fast.
- Actually, UDP is a null protocol if you remove the checksum field.
  - Reduce the requirement of computer resources.
  - When using the Multicast or Broadcast to transfer.
  - The transmission of Real-time packets, mainly in multimedia applications.