Network Fundamentals

Whilst teaching networking in detail is not in the scope of BTL1, we will cover some basics to assist our students that don't have much experience with this topic of computing. This lesson will cover what TCP, UDP, and ICMP are, and cover what IP and Mac addresses are to help build a fundamental knowledge of networking.

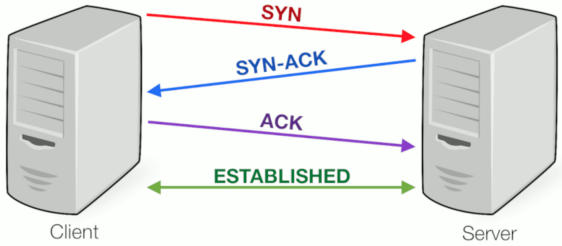
TCP

Transmission Control Protocol (TCP) is a connection-oriented protocol that allows two systems to establish a connection that allows two-way transmission of data. Any data loss is detected and automatically corrected, which is why TCP is known as a reliable protocol. TCP works at the transport layer in the OSI model. The term TCIP/IP protocol stack is also commonly used to refer to the Internet protocol suite since the TCP protocol is almost always based on the Internet protocol (IP) and this connection is the foundation for the majority of public and local networks and network services.

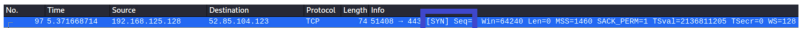
But how exactly do systems communicate with each other using TCP? A process referred to as the "three-way handshake" is conducted. To start, both systems must have unique IP addresses and have assigned and enabled the port for the data transfer. The IP address works as a primary identifier, while the specified port allows the operating system to assign connections to the specific client and server programs.

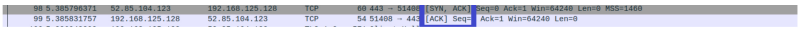
1. The requesting client sends the server an SYN (synchronize) packet with a random number, which ensures that data is sent in the right order and nothing is missed.
2. The server receives the packet and accepts the connection by sending an SYN-ACK (synchronize acknowledgment) packet back to the client, including the client's sequence number plus 1. It also transmits its own sequence number to the requesting client.
3. Finally, the **client** acknowledges the receipt of the SYN-ACK segment by sending its own **ACK packet**, which in this case contains the server's sequence number plus 1. At the same time, the client can already begin transferring data to the server.

You can see how this is conducted in the below graphic.



Using Wireshark, we can see the three-way handshake happening when we try to connect to a website from our host system. We have highlighted the handshake that shows the SYN, SYN-ACK, ACK sequence of our host system establishing a connection with a web server.





You can find more information about TCP by reading the original version RFC 793 or the most recent version RFC 7323.

UDP

User Datagram Protocol (UDP) is a protocol that allows datagrams to be sent without connection in IP-based networks. To achieve the desired services on the target hosts, it uses ports that are listed as one of the core components in the UDP header. Like many other network protocols, UDP belongs to the internet protocol family, where it is classified as a mediator between the network layer and the application layer at the transport level.

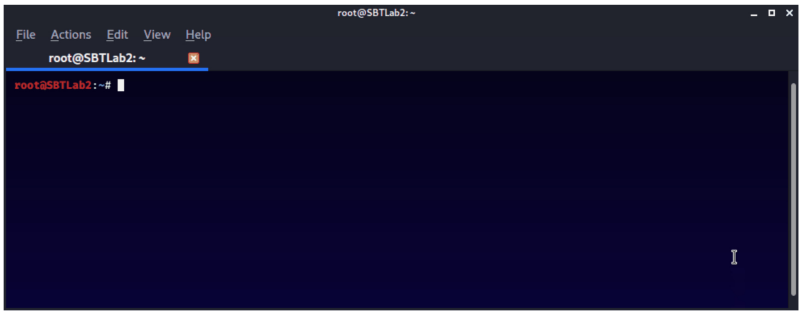
1. **UDP is connectionless**: Data transport via UDP is characterized by the fact that it takes place without an existing connection between addressee and recipient. The respective packets are then sent to the preferred IP address, **specifying the target port**, without the computer behind them having to respond. However, if packets are also to be returned to the recipient, the UDP header can optionally also contain the source port.
2. **UDP uses ports**: Like TCP, UDP uses ports so that the packets are transferred to the correct subsequent protocols or the desired applications on the target system. The ports are defined by numbers according to the proven pattern, with numbers between 0 and 1023 assigned to fixed services.
3. **UDP enables fast, delay-free communication**: The transport protocol is suitable for fast data transmission due to the lack of connection setup. This also results from the fact that the loss of individual packets only affects the quality of the transmission. With TCP connections, on the other hand, lost packets are automatically re-requested, causing the entire transmission process to come to a standstill.
4. **UDP does not guarantee the security and integrity of the data**: The absence of mutual authentication between addressee and recipient ensures the excellent transmission speed of UDP – however, the protocol can neither guarantee the completeness nor the security of the data packets. The correct sequence of the sent packets is also not guaranteed. For this reason, the services that use UDP must provide their own measures for correction or protection.

You can find more information about UDP by reading RFC 768.

ICMP

Have you ever pinged an IP address or domain to see if you can reach it? This process uses ICMP. The **Internet Control Message Protocol** is an internet layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers.

Let's demonstrate by pinging Google.com from our system.



IP ADDRESSES

An **Internet Protocol** (IP) address provides an identity to a networked device on the internet. Similar to a home or business address that supplies a specific physical location with an identifiable address, devices on a network are differentiated from one another through IP addresses.

If you send a package to a friend in another country, you have to know the exact destination. This same general process is used to send data over the internet. However, instead of using a physical mailing address, the computer uses DNS servers to look up a hostname to find its IP address.

For example, when you enter a website URL such as www.lifewire.com into a browser, your request to load that page is sent to DNS servers that look up the hostname of lifewire.com to find its corresponding IP address. Without the IP address, the computer has no clue what it is that you're after.

Private IP Addresses

These are used inside a network, for example, a home network that is used by tablets, Wi-Fi cameras, wireless printers, and desktop PCs. These types of IP addresses provide a way for devices to communicate with a router and the other devices on the private home network. Private IP addresses can be set manually or assigned automatically by the router. The private IP ranges are:

- **192.168.0.0 – 192.168.255.255** (65,536 IP addresses)
- **172.16.0.0 – 172.31.255.255** (1,048,576 IP addresses)
- **10.0.0.0 – 10.255.255.255** (16,777,216 IP addresses)

Public IP Addresses

These are used on the outside of a network and are assigned by an ISP. It's the main address that a home or business network uses to communicate with the rest of the networked devices around the world (for example, the internet). It provides a way for the devices in a home, for example, to reach an ISP, and therefore the outside world, allowing the devices to access websites and communicate directly with other computers and servers around the world.

Static and Dynamic IPs

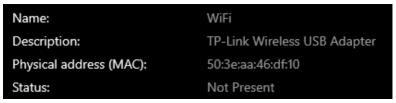
Both private IP addresses and public IP addresses are either dynamic or static, which means that, respectively, they either change or they don't.

An IP address that is assigned by a DHCP server is a dynamic IP address. If a device doesn't have DHCP enabled or doesn't support DHCP, then the IP address must be assigned manually, in which case it's called a static IP address.

MAC ADDRESSES

A **Media Access Control** (MAC) address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed (but it can be spoofed by attackers!). MAC addresses are made up of six two-digit hexadecimal numbers, separated by colons. For example, an Ethernet card may have a MAC address of 00:0d:83:b1:c0:8e.

We can view the MAC of our interface card in Windows by searching for "Network Status" in the Windows search bar, then clicking on "View your network properties". The screenshot on the left shows the MAC address for my wired ethernet connection, and the right image shows the MAC address for my wireless USB network adapter that allows me to connect to WiFi.



FURTHER READING MATERIAL

We have compiled a list of additional resources that we suggest students read if they do not feel overly confident with networking fundamentals and concepts.

- Professor Messer YouTube Videos
- Cisco Networking Fundamentals PDFs
- Computer Network Quizzes and Trivia
- Computer Networking Quiz For Beginners

Previous Topic
Back to Lesson
Next Topic