What is UDP?

A transport layer communication protocol, UDP is a very common protocol for voice and video traffic.

Learning Objectives

After reading this article you will be able to:

- Define UDP/IP
- Describe some use cases for UDP

RELATED CONTENT

HTTP

TCP/IP

Web Application Firewall (WAF)

Ping (ICMP) flood attack

UDP flood attack

Copy article link

What is the User Datagram Protocol (UDP/IP)?

The User Datagram Protocol, or UDP, is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred. This allows data to be transferred very quickly, but it can also cause packets to become lost in transit — and create opportunities for exploitation in the form of DDoS attacks.

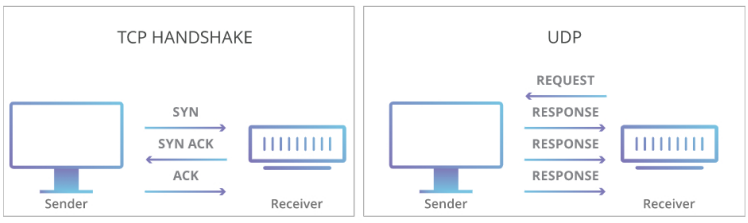
How does UDP work?

Like all networking protocols, UDP is a standardized method for transferring data between two computers in a network. Compared to other protocols, UDP accomplishes this process in a simple fashion: it sends packets (units of data transmission) directly to a target computer, without establishing a connection first, indicating the order of said packets, or checking whether they arrived as intended. (UDP packets are referred to as 'datagrams'.)

UDP is faster but less reliable than TCP, another common transport protocol. In a TCP communication, the two computers begin by establishing a connection via an automated process called a 'handshake.' Only once this handshake has been completed will one computer actually transfer data packets to the other.

UDP communications do not go through this process. Instead, one computer can simply begin sending data to the other:

TCP vs UDP Communication



In addition, TCP communications indicate the order in which data packets should be received and confirm that packets arrive as intended. If a packet does not arrive — e.g. due to congestion in intermediary networks — TCP requires that it be re-sent. UDP communications do not include any of this functionality.

These differences create some advantages. Because UDP does not require a 'handshake' or check whether data arrives properly, it is able to transfer data much faster than TCP.

However, this speed creates tradeoffs. If a UDP datagram is lost in transit, it will not be re-sent. As a result, applications that use UDP must be able to tolerate errors, loss, and duplication.

(Technically, such packet loss is less a flaw in UDP than a consequence of how the Internet is built. Most network routers do not perform packet ordering and arrival confirmation by design, because doing so would require an unfeasible amount of additional memory. TCP is a way of filling this gap when an application requires it.)

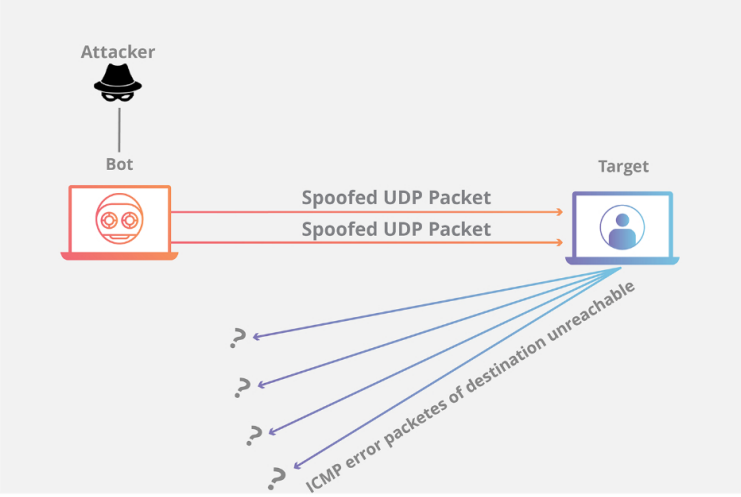
What kinds of services rely on UDP?

UDP is commonly used in time-sensitive communications where occasionally dropping packets is better than waiting. Voice and video traffic are often sent using this protocol because they are both time-sensitive and designed to handle some level of loss. For example, VoIP (voice over IP), which is used by many Internet-based telephone services, typically operates over UDP. This is because a static-y phone conversation is preferable to one that is crystal clear but heavily delayed.

This also makes UDP the ideal protocol for online gaming. Similarly, because DNS servers both need to be fast and efficient, they operate through UDP as well.

How is UDP used in DDoS attacks?

UDP 'risks' like packet loss are not a serious problem in most use cases. However, UDP can be exploited for malicious purposes. Since UDP does not require a handshake, attackers can 'flood' a targeted server with UDP traffic without first getting that server's permission to begin communication.



A typical UDP flood attack sends a large number of UDP datagrams to random ports on its target computer. This forces the target to respond with an equally large number of ICMP packets, which indicate those ports were unreachable. The computing resources required to respond to each fraudulent datagram can exhaust the target, resulting in a denial-of-service to legitimate traffic. (To learn more, read our article on UDP flood attacks.)

Organizations can defend against UDP flood attacks with a variety of methods. One is to limit the response rate of ICMP packets, though this approach can also filter out legitimate packets. Another method is to receive and respond to UDP traffic through an intermediary network of many distributed data centers, preventing a single origin server from being overwhelmed with fraudulent requests. Learn more about how Cloudflare uses this strategy to help organizations mitigate DDoS attacks.

Sales

Enterprise Sales

Become a Partner

Contact Sales:
+65 3158 3954

About DDoS attacks

What is a DDoS attack?

What is a DDoS botnet?

Famous DDoS attacks

DDoS mitigation

DDoS attacks

Memcached DDoS attack

NTP amplification attack

DNS amplification attack

SSDP attack

Low and slow attack

Application layer attack

Layer 3 attacks

Cryptocurrency attacks

Ransom DDoS attack

Smurf attack (historic)

Ping of death (historic)

ACK flood attack

DNS flood

HTTP flood

Ping (ICMP) flood attack

QUIC flood attack

SYN flood attack

UDP flood attack

DDoS attack tools

How to DDoS

Low Orbit Ion Cannon

High Orbit Ion Cannon

R U Dead Yet? (R.U.D.Y.)

Slowloris attack

DDoS booter/IP stresser

IP spoofing

Malware

Mirai botnet

DDoS glossary

Denial of service

Blackhole routing

OSI Model

TCP/IP

ICMP

HTTP

Web Application Firewall (WAF)

User Datagram Protocol (UDP)

Layer 7

Internet of Things (IoT)

Learning Center navigation

Learning Center Home

DNS Learning Center

CDN Learning Center

Serverless Learning Center

Security Learning Center

Performance Learning Center

SSL Learning Center

Bots Learning Center

Cloud Learning Center

Access Management Learning Center

Network Layer Learning Center

Privacy Learning Center

Video Streaming Learning Center

Email Security Learning Center