The **User Datagram Protocol (UDP)** is a **lightweight data transport protocol** that works on top of IP.

UDP provides a mechanism to **detect corrupt data** in packets, but it does ***not*** attempt to **solve** other problems that arise with packets, such as **lost or out of order packets**. That's why UDP is sometimes known as the ***Unreliable* Data Protocol**.

UDP is simple but fast, at least in comparison to other protocols that work over IP. It's often used for time-sensitive applications (such as real-time video streaming) where speed is more important than accuracy.

**Packet format**

When sending packets using UDP over IP, the data portion of each IP packet is formatted as a **UDP segment**.

Graphical user interface, application

Description automatically generated

Each UDP segment contains an 8-byte header and variable length data.

### **Port numbers**

The first four bytes of the UDP header store the port numbers for the source and destination.

### **Segment Length**

The next two bytes of the UDP header store the length (in bytes) of the segment (including the header).

### **Checksum**

The final two bytes of the UDP header is the checksum, a field that's used by the sender and receiver to check for data corruption.

Before sending off the segment, the sender:

1. Computes the checksum based on the data in the segment.
2. Stores the computed checksum in the field.

Upon receiving the segment, the recipient:

1. Computes the checksum based on the received segment.
2. Compares the checksums to each other. If the checksums aren't equal, it knows the data was corrupted.

Unfortunately, the recipient **can not** use the computed checksum to reconstruct the original data, so it will likely just discard the packet entirely.