Ch.3: Building Blocks of UDP

Ciro S. Costa

Jul 07, 2015

UDP stands for *User Datagram Protocol* (and colloquially referred as a *null protocol*), being important by features that it chooses to omit.

Datagram is a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination nodes without reliance on earlier exchanges between nodes and the transporting network.

A big use of UDP is as the transport protocol that is used by DNS (Domain Name System). DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server. DNS is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various informations with domain names assigned to each of the participating entities. Most prominently it translates domain names to IP addresses. Another one is WebRTC (Web Real-Time communication).

Null Protocol Services

UDP sits in a layer between IP and TCP protocols. IP's task is delivering datagrams from source to destinations based on their addresses. UDP encapsulates user messages into its own package structure, adding 4 fields (2 optional). At its core it simply provides "application multiplexing" on top of IP by embedding the source and the target application ports of the communicating hosts. It offers:

- no guarantee of message delivery
- no guarantee of order of delivery
- no connection state tracking
- no congestion control

UDP datagrams have definitive boundaries: each datagram is carried in a single IP packet and each application read yields the full message (can't be fragmented).

NAT

Nat stands for a methodology of remapping one IP address space into another by modifying network address information in IP datagram packet headers while theya are in transit across a traffic routing device.

Address Space defines a range of discrete addresses, each of which may correspond to a network host, memory cell or other logical or physical entity.

Private Network is a network that uses private IP address space. Adresses in this space are not allocated to any specific organization and anyone may use these addresses without approval. However, IP datagrams addressed from them cannot be transmitted through the public Internet, it must do so via a NAT gateway or a proxy server.

The trouble that a protocol implementor has is that NAT translation depends on connection state, which UDP doesn't have. Since the translator doesn't even know about a connection drop, it has to rely on timers. To solve this the de factor best practice for long-running sessions over UDP is to introduce bidirectional keepalive packets to periodically reset the timers.

The real problem comes when handling inbound traffic. For outbound (acting as a client) the NAT can deal well with the traffic as it knows how to perform the traversal properly at that direction. When it comes to acting as a server, then we have the problem of transmitting with UDP over a network with NAT layers. The work around for this comes in various traversal techniques (TURN, STUN and ICE).

STUN, TURN and ICE

Session Traversal Utilities for NAT (STUN) is a protocol that allows the host application to discover the presence of a NAT on the network and when present to obtain the allocated public IP and port tuple for the current connection.

Whenever two peers want to talk to each other uver UDP, they firt send binding request to their respective STUN servers, and following a successful response on both sides, they can then use the established public IP and port tuples to exchange data.

- With STUN the application discovers its public IP and port tuple and is then able to use this information as part of its application data when communicating with its peers.

- The outbound binding request to the STUN server establishes NAT routing entries along the path such that the inbound packets arriving at the public IP and port tuple can now find their way back to the host application on the interna network.
- Defines a simple mechanism for keepalive pings to keep the NAT routing entries from timing out.

It's fine for simple networks but in practice it might fail with some NAT topologies (might get blocked by firewall or other network appliance).

Traversal Using Relay around NAT (TURN) another protocol which can run over UDP and switch to TCP if all else fails.

Both clients begin their connections by sending an allocate request to the same TURN server, followed by permission negotiation. Once the negotiation is complete, both peers communicate by sending their data to the TURN server, which then relays it to the other peer (not really peer to peer anymore).

Interactive Connectivity Establishment (ICE) is a protocol and a set of methods that seeks to establish the most efficient tunnel between the participants: direct connection through STUN negotiation where needed and finally falling back to TURN if all the rest fails.