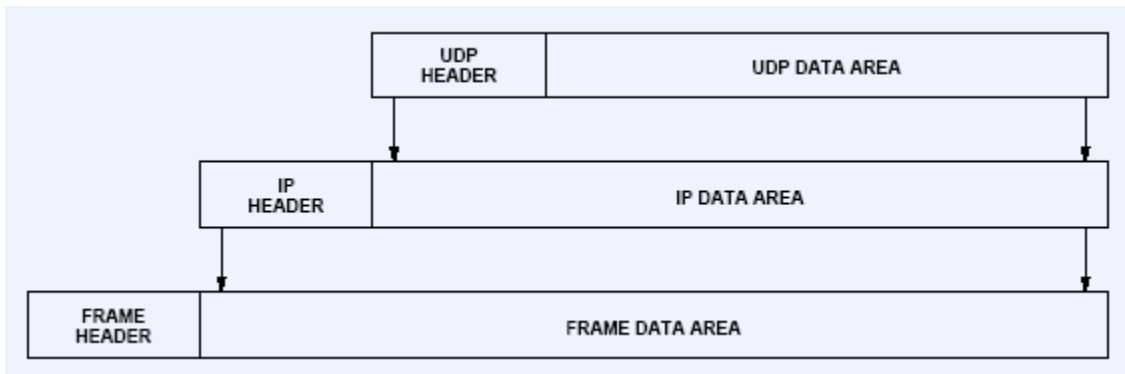


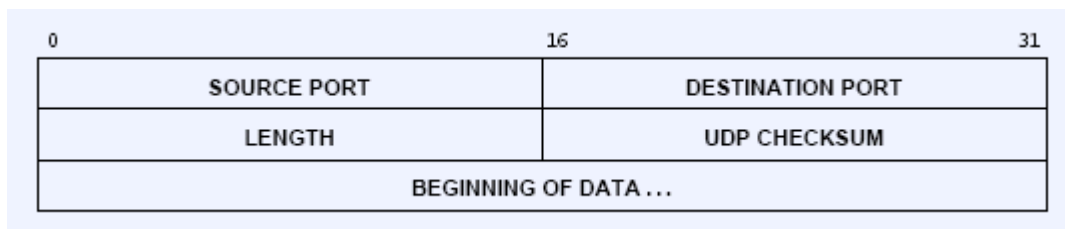
# UDP Protocols

## (1) UDP: User Datagram Protocol

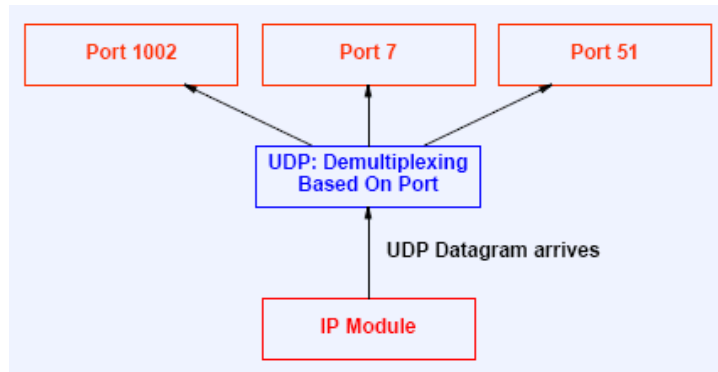
- ❖ Why need UDP (or TCP)
  - On a single host, there might be many application programs
  - IP only identifies host, not application programs running on host
  - We need another thing to distinguish one application from another, so when the TCP/IP software receives a packet, it knows which program to send to.
  - TCP/IP uses protocol port number to distinguish programs. Application programs bind themselves to port numbers.
  - Both TCP and UDP have port numbers. They are different.
- ❖ UDP
  - Transport-layer protocol
  - Connectionless service
  - Same best-effort semantics as IP
    - Messages can be delayed, lost, or duplicated
    - Messages can arrive out of order
  - Application accepts full responsibility for errors
  - UDP-based applications
    - DNS: Normal hosts query DNS servers using UDP in practice
    - Streaming video, Voice-over-IP
- ❖ Encapsulation



### ❖ UDP Message Format



## ❖ UDP Multiplexing, Demultiplexing, and Ports



## ❖ Reserved and Available UDP Port Numbers

- Small numbers are reserved for specific applications
  - Called well-known ports
  - Same interpretation throughout the Internet
  - Used by server software
- Large numbers are not reserved
  - Available to arbitrary application programs
  - Used by client software
- Examples:
  - 7 for Echo, 13 for daytime, 53 for DNS name server.

---

## (2) UDP Attacks

### ❖ Fraggle

- Broadcast UDP packet sent to the "echo" service.
- All computers reply (amplification).
- Source IP was spoofed, victim is overwhelmed
- Similar to the ICMP Smurf attack.

### ❖ UDP Ping-Pong:

- Some service or application issues a UDP reply no matter what is the input packet (e.g., error message).
- Set the source and destination ports of a UDP to be one of the following ports
  - daytime (port 13)
  - time (port 37)
- This causes a Ping-Pong effect between the source and the destination.

## ❖ DoS Attacks

- Key: Applications that reply with large packets to small requests, e.g., games
  - Battlefield 1942
  - Quake 1 (CAN-1999-1066)
  - Unreal Tournament
- Hosts can be attacked by using these applications as amplifiers, with forged source IP packets