

Super Proxy

- **There seemed to be some consensus**
 - Desire to provide complete network connectivity
 - (but avoid tun/ta grunge if possible)
 - DNS looks more useful than ICMP
- **Your mission**
 - A TCP port forwarder using DNS as transport.
 - You can run an HTTP or SOCKS proxy on the other end.
 - You can run ppp over it if you'd like.

Super Proxy starting point

- **Several similar projects exist**
 - NSTX
 - OzymanDNS –
www.doxpara.com/slides/BH_EU_05-Kaminsky.pdf
- **You will improve upon them**
 - Portable
 - Better bit density (compression?)
 - Proper windowing
- **You should use you TCP code to packetize.**

Super Proxy basic architecture

- **Terms**

- “Laptop” runs client “tcp2dns” listening on port X
- “Desktop” runs “dns2tcp” listening on port 53
- dns2tcp forwards the client’s stream to machine:Y
- machine is often “localhost”

- **DNS is your “IP”**

- Encode TCP segments as DNS Requests.
- Upstream data is a “large” request.
- Downstream data is a “large” response to a small request.

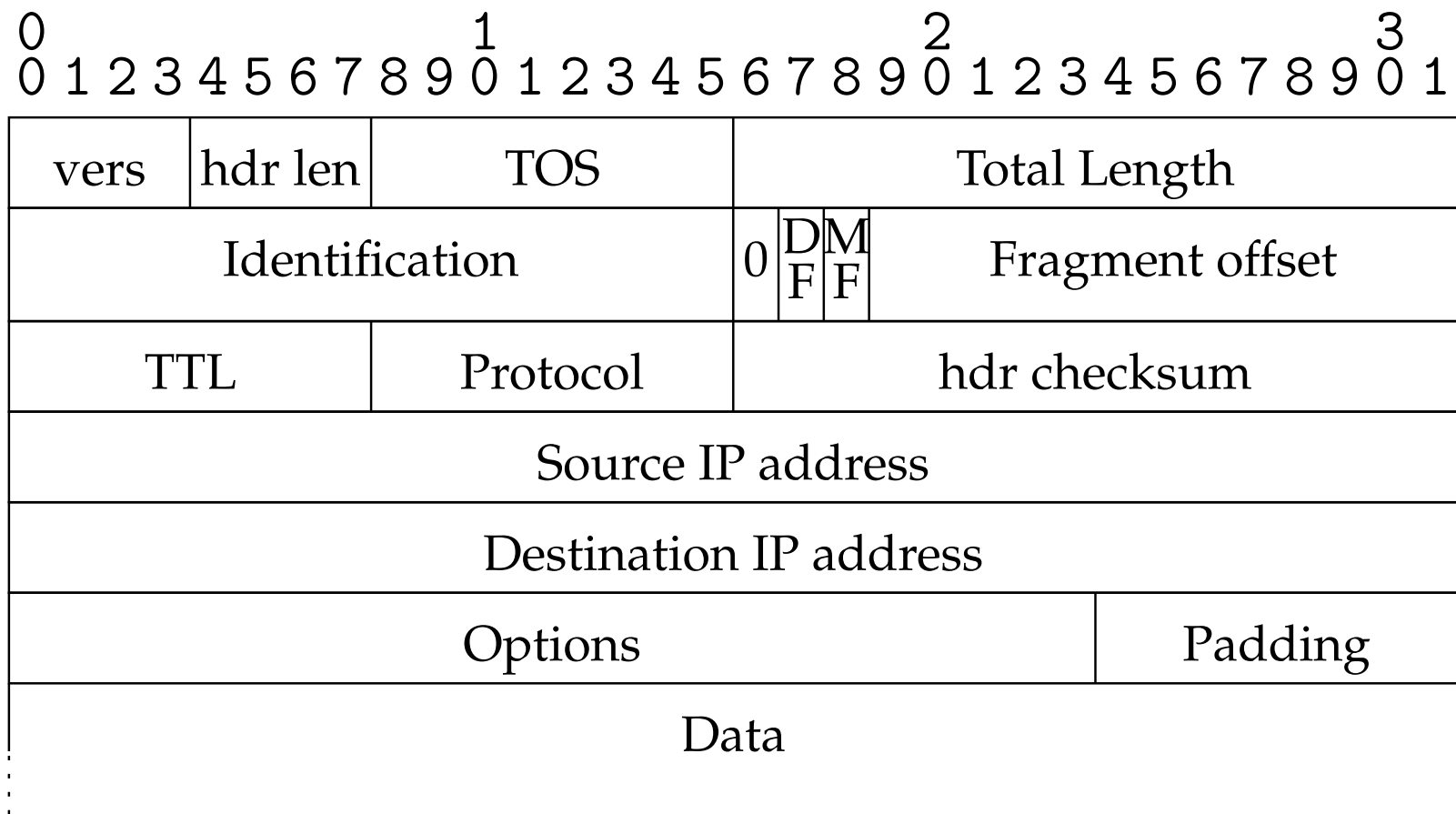
Upstream Data

- **Encoding limitations, see RFC for details, but consider**
 - 253 character limit, 63 characters per label
 - Allowable characters?
 - Any extra room?
- **Need to encode all of TCP segment fields?**

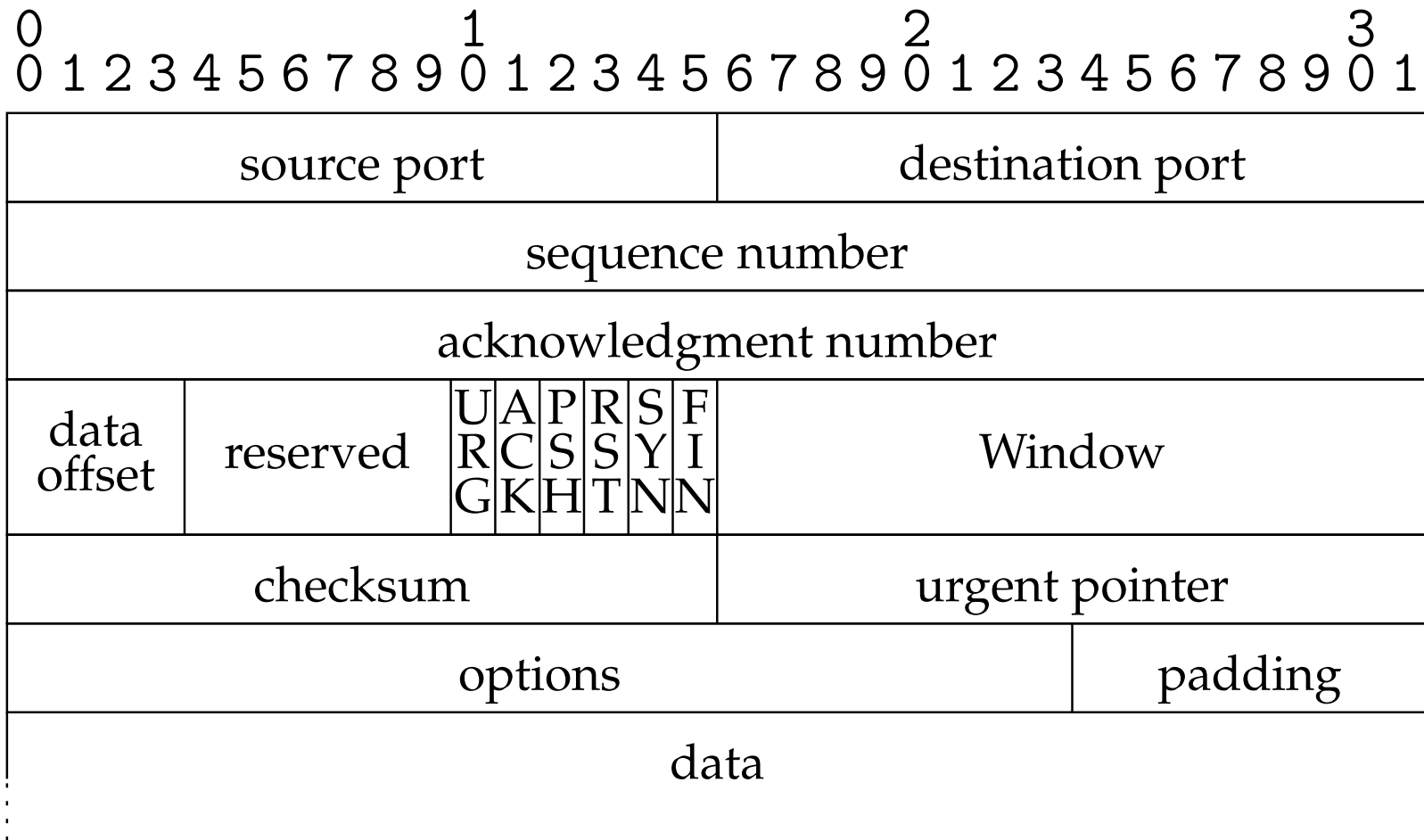
Downstream Data

- **TXT Records**
- **Encoding limitations, see RFC, but consider**
 - Packet must be less than 512 bytes
 - Allowable characters? (probe for 8 bit clean?)
- **How to send downstream data “spontaneously”?**
 - Needs to be a response to *something*.

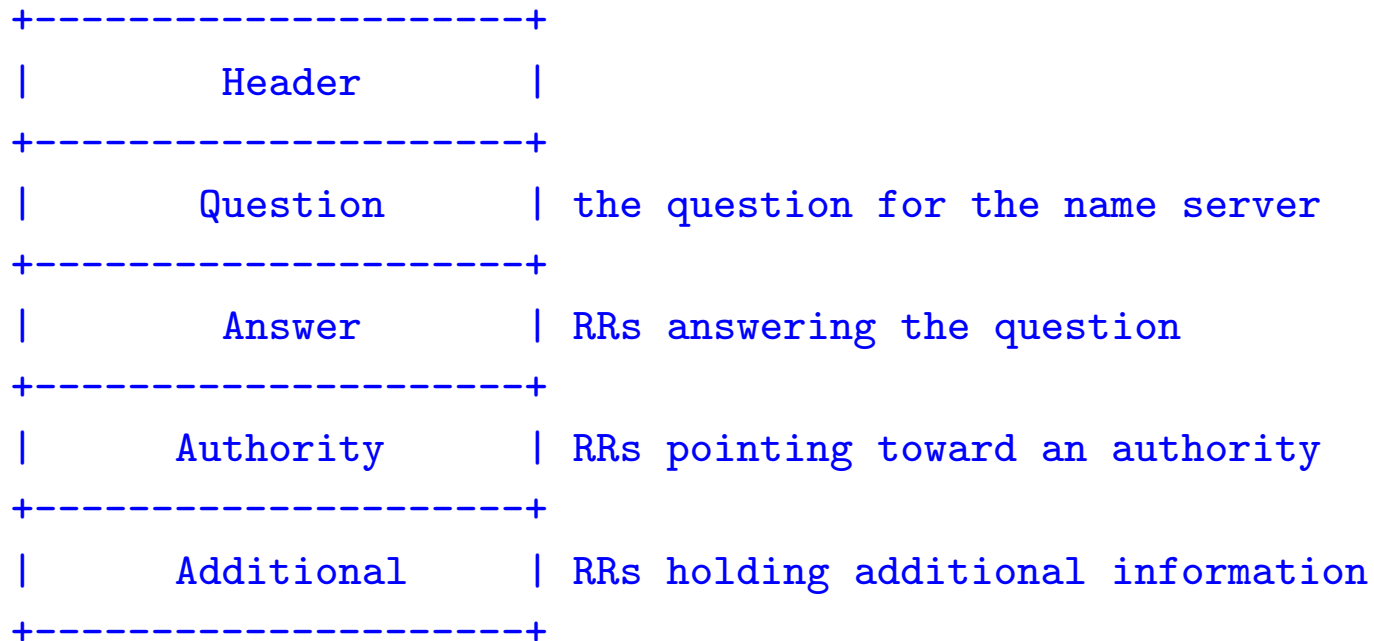
IP packet format



TCP segment

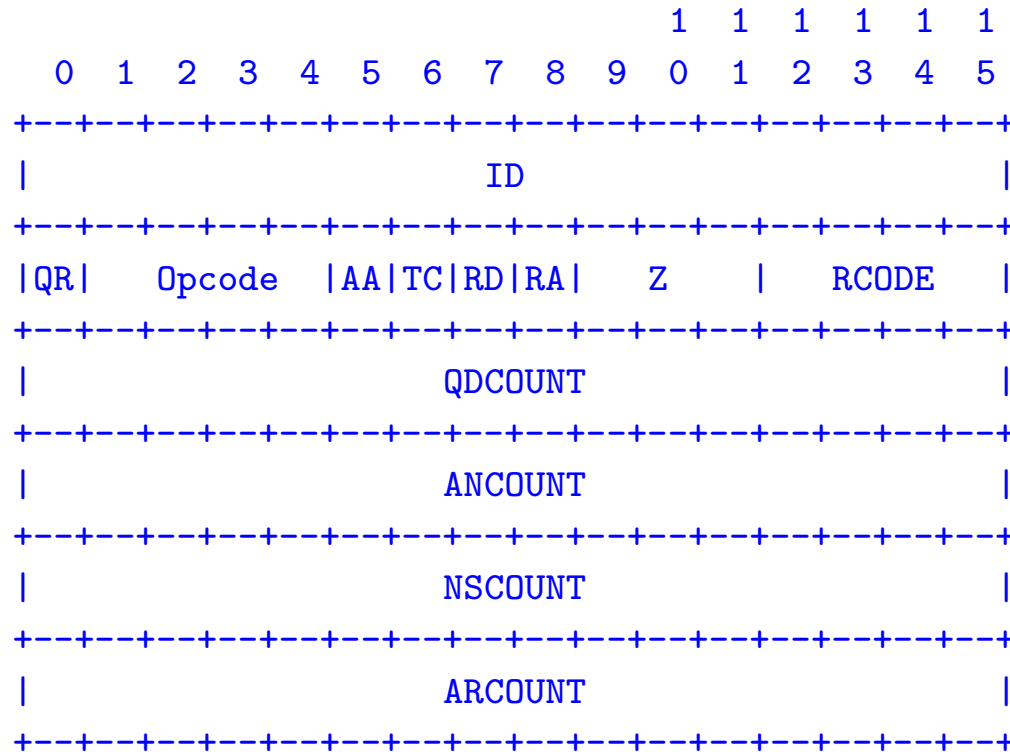


Structure of a DNS message



- **Same message format for queries and replies**
 - Query has zero RRs in Answer/Authority/Additional sections
 - Reply includes question, plus has RRs
- **Authority allows for delegation**
- **Additional for glue + other RRs client might need**

Header format



- **QR** – 0=query, 1=response
- **RCODE** – error code
- **AA**=authoritative answer, **TC**=truncated,
RD=recursion desired, **RA**=recursion available

Available resources

- You may assume you have root access on two Linux machines to run your server and test your clients.
- You will be sharing the server, but it will have several IP addresses, so you may each listen on port 53 on one, for example.
- How will you test difficult scenarios?

Next Steps

- **You (plural) will agree to a spec by Thursday, 29th.**
- **Homework 4 will be individual spec writeups, due Monday**
- **Checkpoint (incompatible reliability) by the 7th.**
- **Deadline and bake-off, 15th (Sunday, no finals)**

Coming up

- **CS 141 Needs UTAs for the Spring!**