Network Security II

CSE 565: Fall 2024
Computer Security

Xiangyu Guo (xiangyug@buffalo.edu)

University at Buffalo

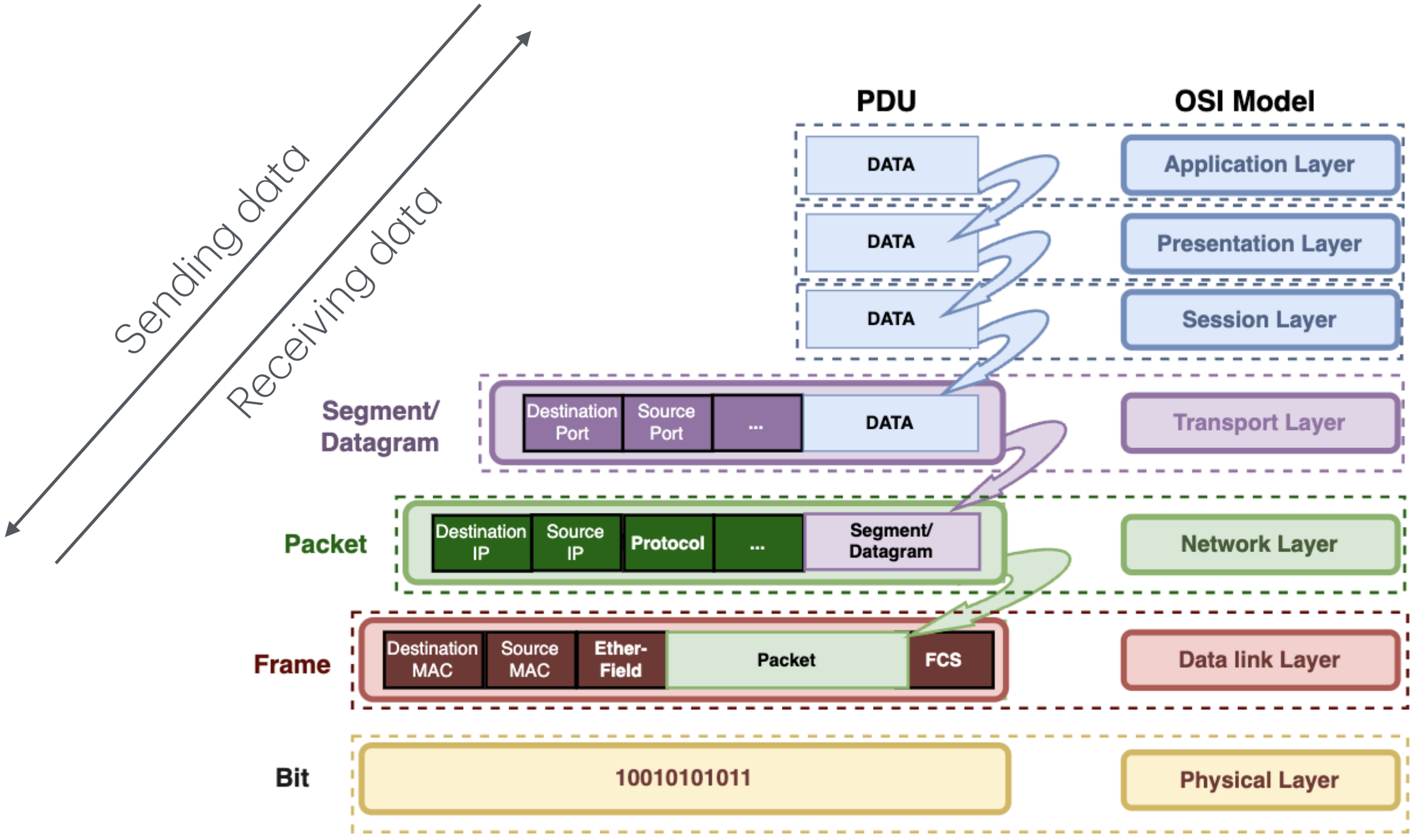
Acknowledgement

- We don’t claim any originality of the slides. The content is developed heavily based on
  - Slides from Prof. Dan Boneh and Prof. Zakir Durumeric’s lecture on Computer Security (https://cs155.stanford.edu/syllabus.html)
  - Slides from Prof Nick McKeown’s lecture on Computer Network (https://vixbob.github.io/cs144-web-page/)
  - Slides from Prof Ziming Zhao’s past offering of CSE565 (https://zzm7000.github.io/teaching/2023springcse410565/index.html)
  - Slides from Prof Hongxin Hu’s past offering of CSE565

Review of Last Lecture

- Network protocol layers
  - OSI 7-Layer model; TCP/IP 5-Layer model
- Link Layer protocol
  - Ethernet; MAC address
- Network Layer protocol
  - IP
- Routing 101

The Protocol Layering



Layer 2: Ethernet

- Provides connectivity between hosts on a single **Local Area Network** (physically connected devices)
- Data is split into ~1500 byte Frames, which are addressed to a device's 6-byte physical (MAC) address — assigned by manufacturer
- **Switches** forward frames based on learning where different *MACs* are located. No guarantees that frames are not sent to other hosts!
- No security (confidentiality, authentication, or integrity)

Layer 3: Internet Protocol (IP)

- Provides routing between hosts on the Internet. Unreliable. Best Effort.
  - Packets can be dropped, corrupted, repeated, reordered
- Routers simply route IP packets based on their destination address.
  - Must be simple in order to be fast — insane number packets FWD'ed

- No inherent security. Packets have a checksum, but it’s non-cryptographic. Attackers can change any packet.
- Source address is set by sender—can be faked by an attacker

ARP: Address Resolution Protocol

- ARP lets hosts to find each others' MAC addresses *on a local network*. For example, when you need to send packets to the upstream router to reach Internet hosts
  - Works only within a LAN.
- Client: Broadcast (all MACs): Which MAC address has IP `192.168.1.1`?
  Response: I have this IP address (sent from correct MAC)
- No built-in security. Attacker can impersonate a host by faking its identity and responding to ARP requests or sending gratuitous ARP announcements

BGP (Border Gateway Protocol)

- Internet Service Providers (ISPs) announce their presence on the Internet via BGP. Each router maintains list of routes to get to different announced prefixes

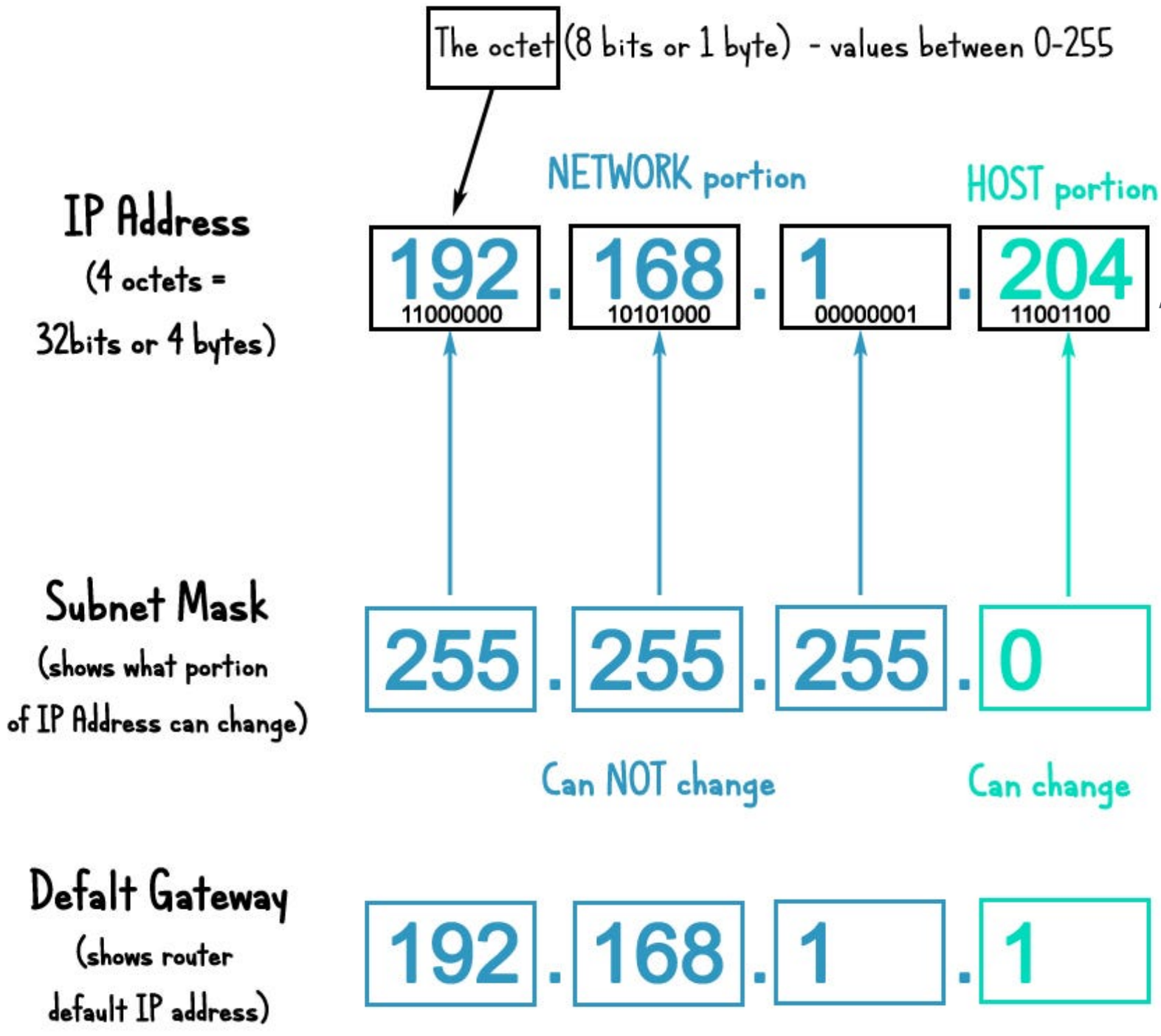
- No authentication—possible to announce someone else's network
  - Commonly occurs (often due to operator error but also due to attacks)

Today's Topic

- More on IP
- Transmission Control Protocol (TCP)
- Domain Name Services (DNS)

More on IP

IP Address



- Indicates the length of the network portion
- Essentially replace subnet mask

Subnet

- A subnet is a **logical** division of IP addresses within a network. It defines which devices belong to the same IP network.
- All hosts in the same subnet have the same network portion in their IP addresses.

Subnet v.s. LAN

Feature	LAN	Subnet
Definition	A physical network of interconnected devices	A logical division of IP addresses within a network
Scope	Physical (focuses on connectivity and infrastructure)	Logical (focuses on IP address organization)
Communication	Devices in the same LAN communicate via MAC addresses	Devices in the same subnet communicate via IP addresses
Purpose	Provides local connectivity and resource sharing	Optimizes traffic, improves security, and reduces broadcast traffic
Example	Office LAN with computers and printers connected via switches	Subnet 1: `192.168.1.0/24`, Subnet 2: `192.168.2.0/24`
Routing	Typically no routing required unless different LANs	Routing needed for communication between different subnets
IP Addressing	Not concerned with IP addressing (Layer 2)	Defines the IP address range for devices (Layer 3)

Private vs Public IP Address

- **Private IP addresses** are reserved for use within **Local Area Networks (LANs)** and are *not* routable on the internet. The following IP ranges are *reserved* for internal networks:
  - Class A: `10.0.0.0` to `10.255.255.255` (CIDR: `10.0.0.0/8`)
  - Class B: `172.16.0.0` to `172.31.255.255` (CIDR: `172.16.0.0/12`)
  - Class C: `192.168.0.0` to `192.168.255.255` (CIDR: `192.168.0.0/16`)
- **Public IP Addresses (External IPs)**:
  - Public IP addresses are used on the internet and are globally unique. Any IP address not in the above private ranges is considered public.

Private vs Public IP Address

- **Network Interface**
  - Network Interface Card (NIC): Hardware used to connect to network
  - Often referred to by the implemented Link Layer protocol, e.g. Ethernet card, Wi-Fi card.
- IP Addresses are assigned to NICs
  - Multiple NICs $\Longrightarrow$ multiple IP addr

How are IPs assigned?

- Where does a device get its IP?
  - **Inside a LAN**
    - A **router** or a **DHCP server** assigns a *private* IP to each device
      - If no router/DHCP server exists, most OS will *assign itself* an IP from Automatic Private IP Addressing (APIPA)
        - Avoid conflict by broadcasting ARP requests (see later)
- The external-facing device (usually the router) of a LAN gets its *public* IP from the ISP.

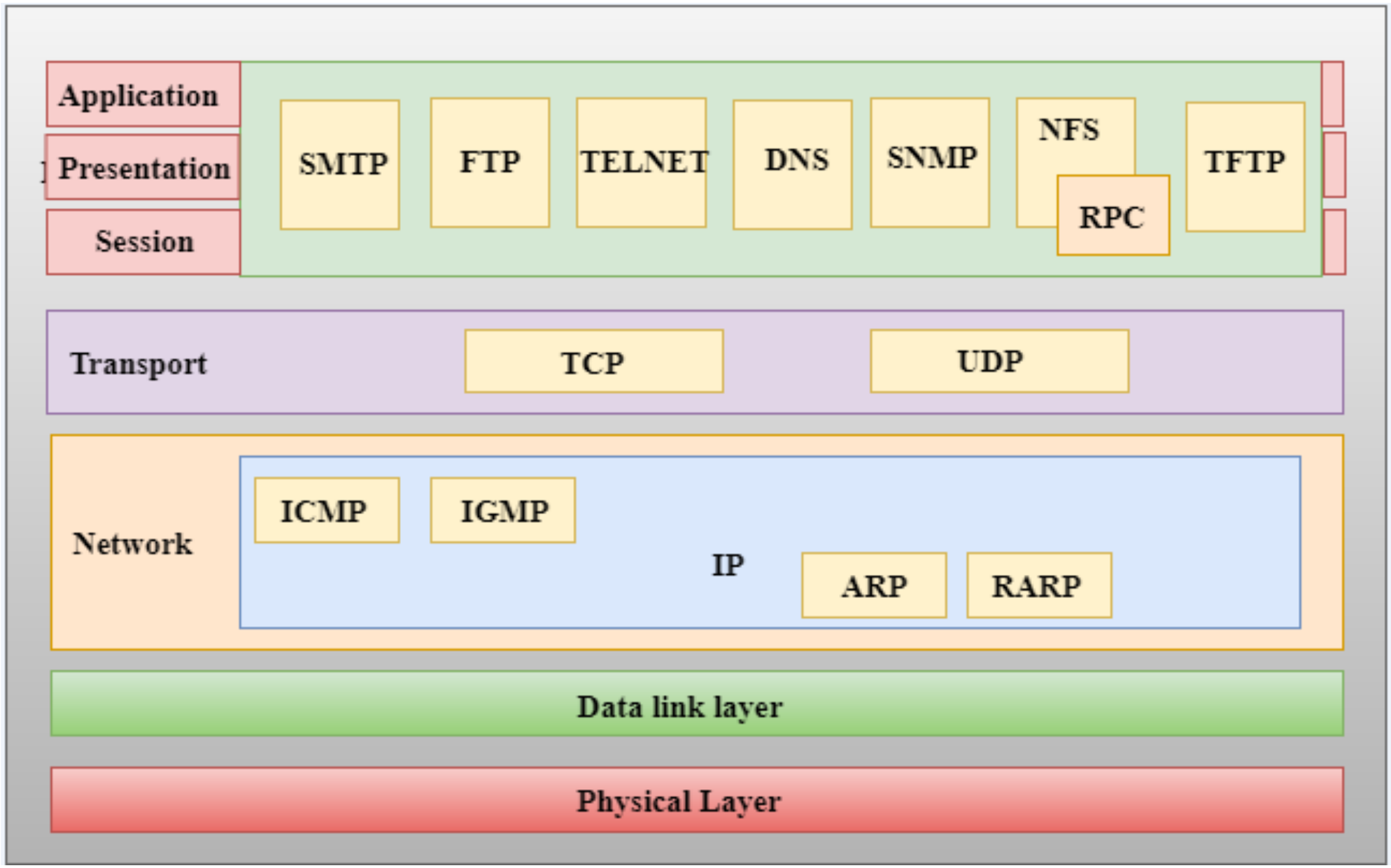
Relation with ARP

- The delivery of a packet to a host or a router requires two levels of addressing:
  - **logical** and **physical**.
- We need to be able to map a logical address to its corresponding physical address and vice versa. These can be done using either static or dynamic mapping.

Relation with ARP

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
  - But the IP datagram must be encapsulated in a frame to be able to pass through the *physical* network.
- This means that the sender needs the physical address of the receiver.
- ARP accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the Link layer.

Relation with ARP

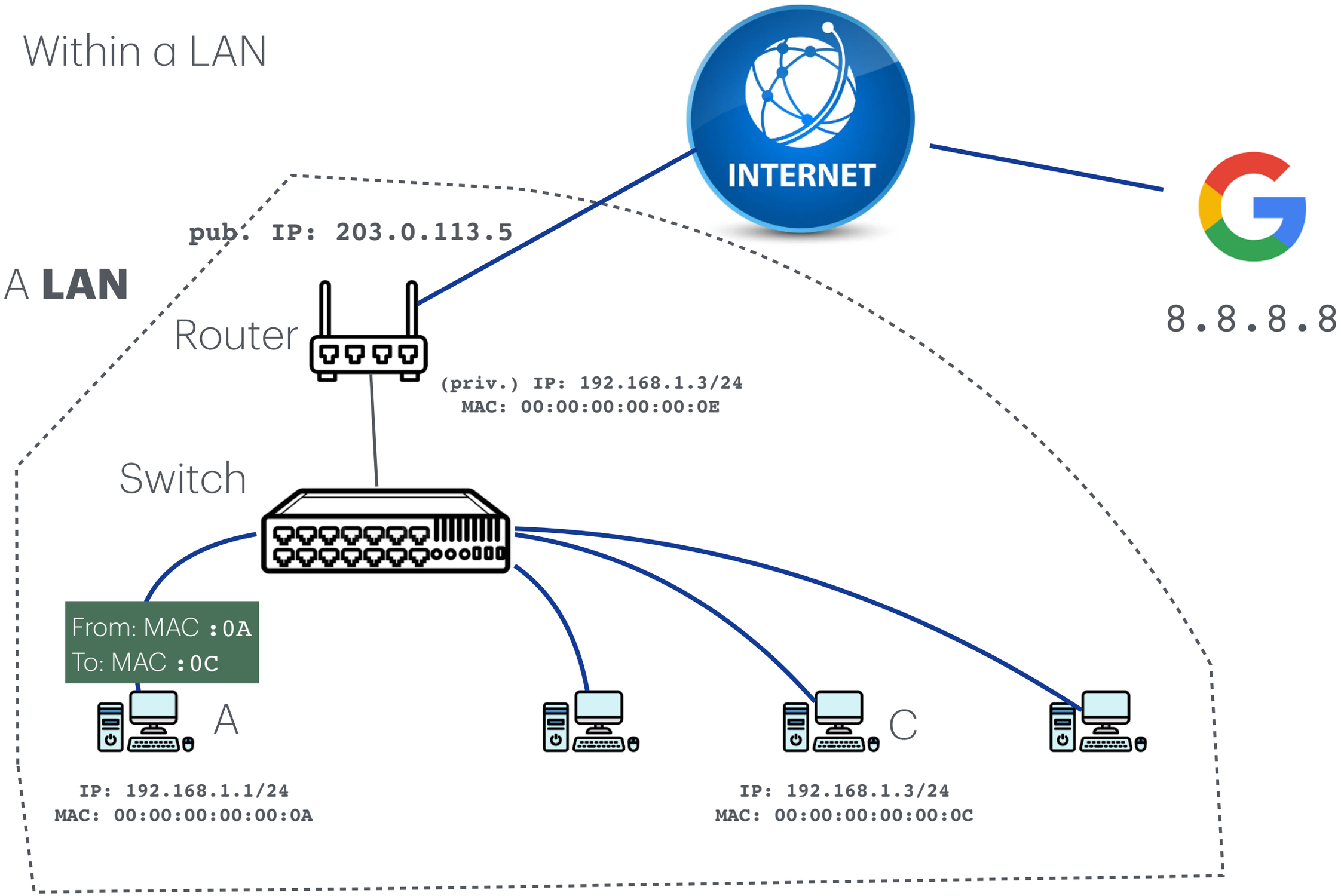


Communicating at the Link & Network Layer

- Summary
  - **Within a same LAN**
    - Only need Link Layer support: MAC address
    - Peer-to-peer or centralized (forwarded by a switch)
  - **Between different LANs**
    - Need Network Layer support: IP address
    - Go through routers

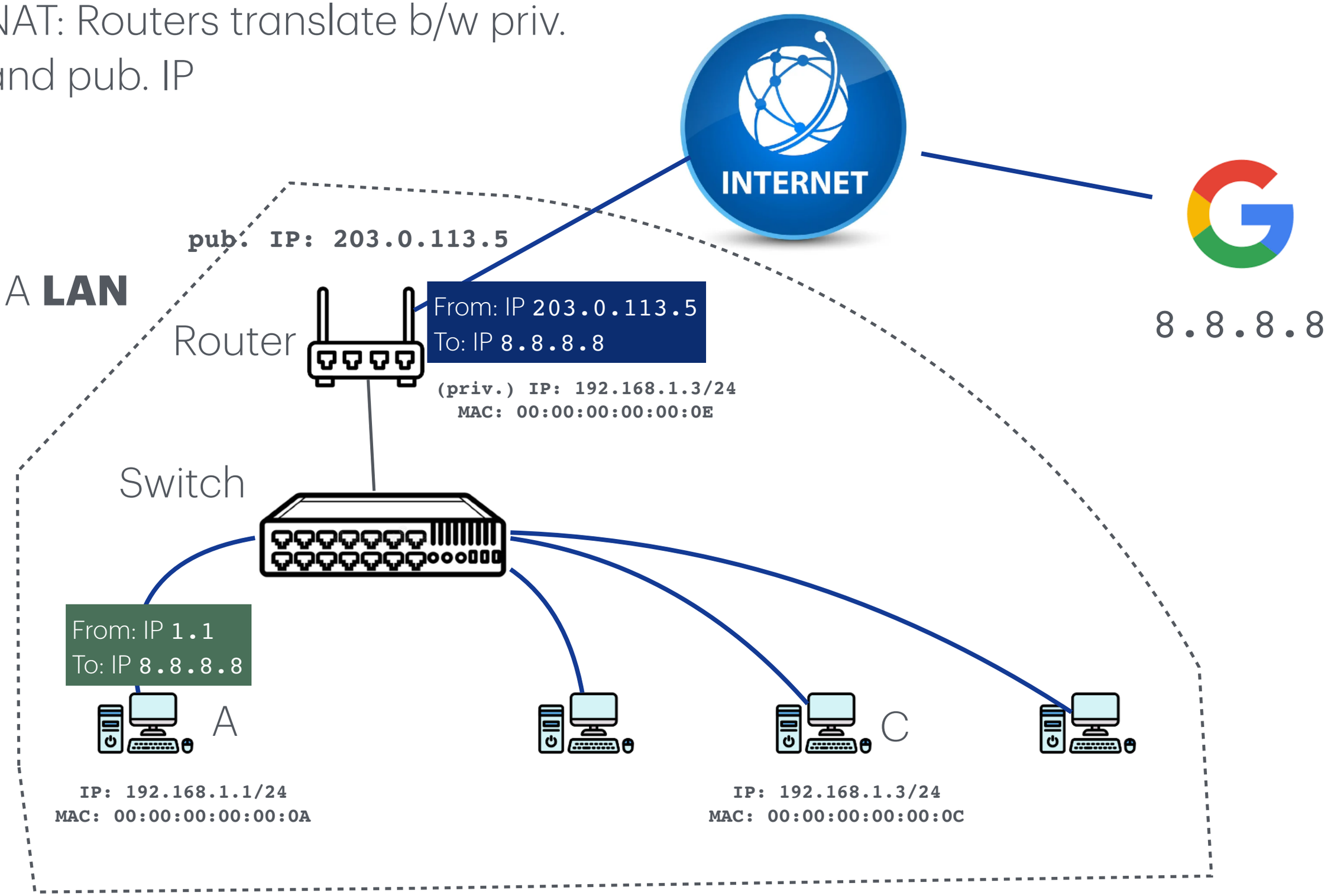
Communicating at the Link & Network Layer

Within a LAN



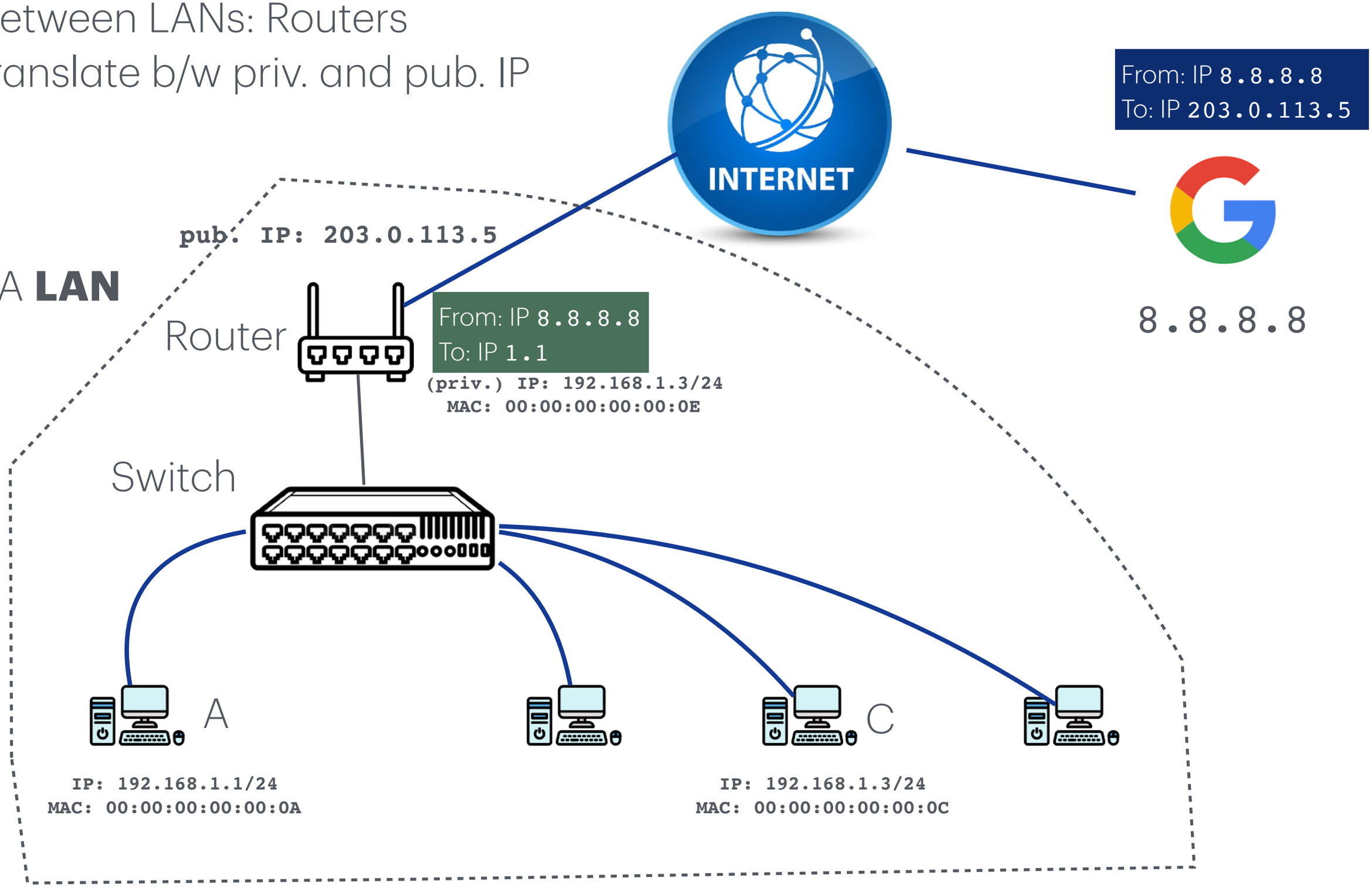
Communicating at the Link & Network Layer

NAT: Routers translate b/w priv. and pub. IP



Communicating at the Link & Network Layer

Between LANs: Routers
translate b/w priv. and pub. IP

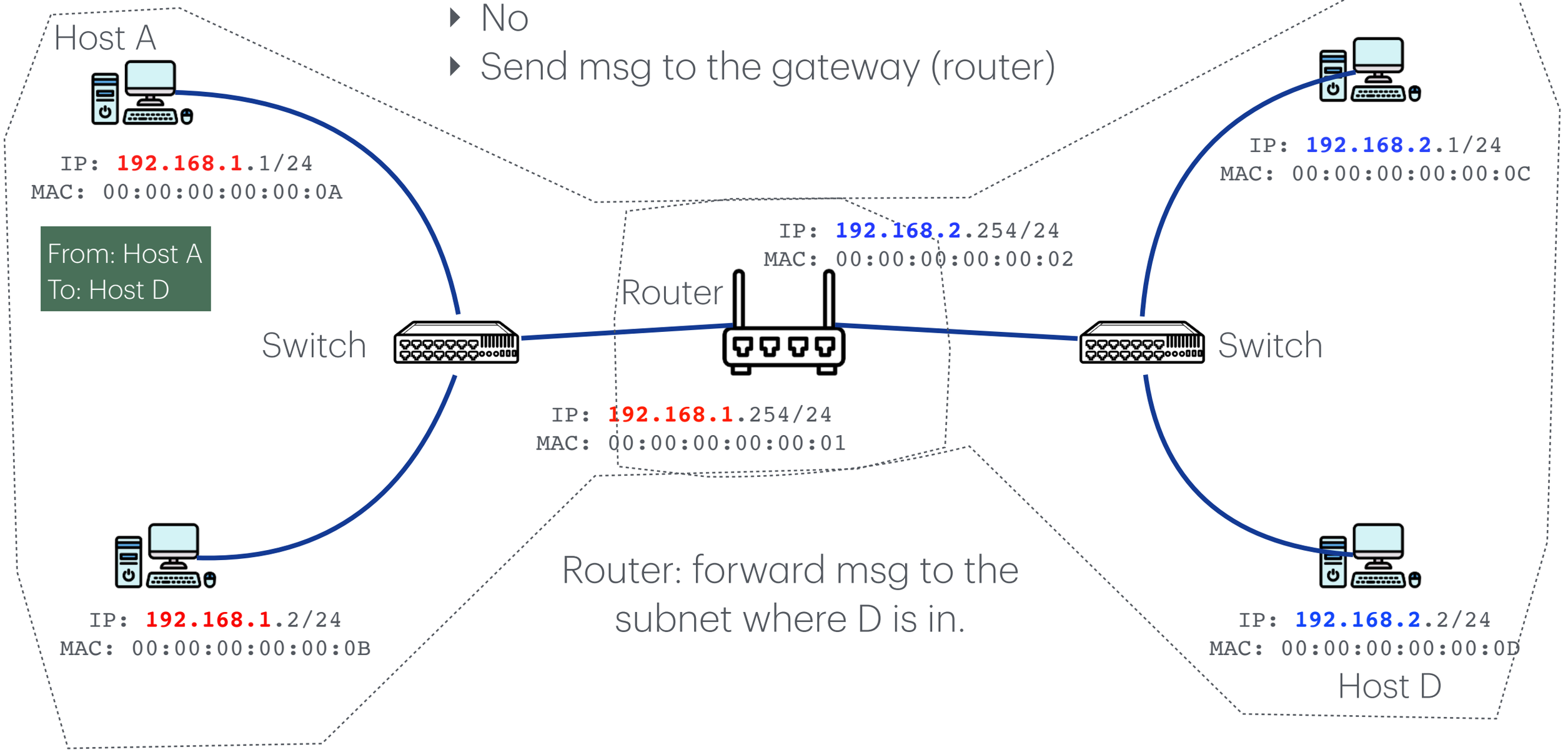


Communicate between subnets

But still within a same LAN

Host A: is D (**192.168.2.**2/24) on my subnet?

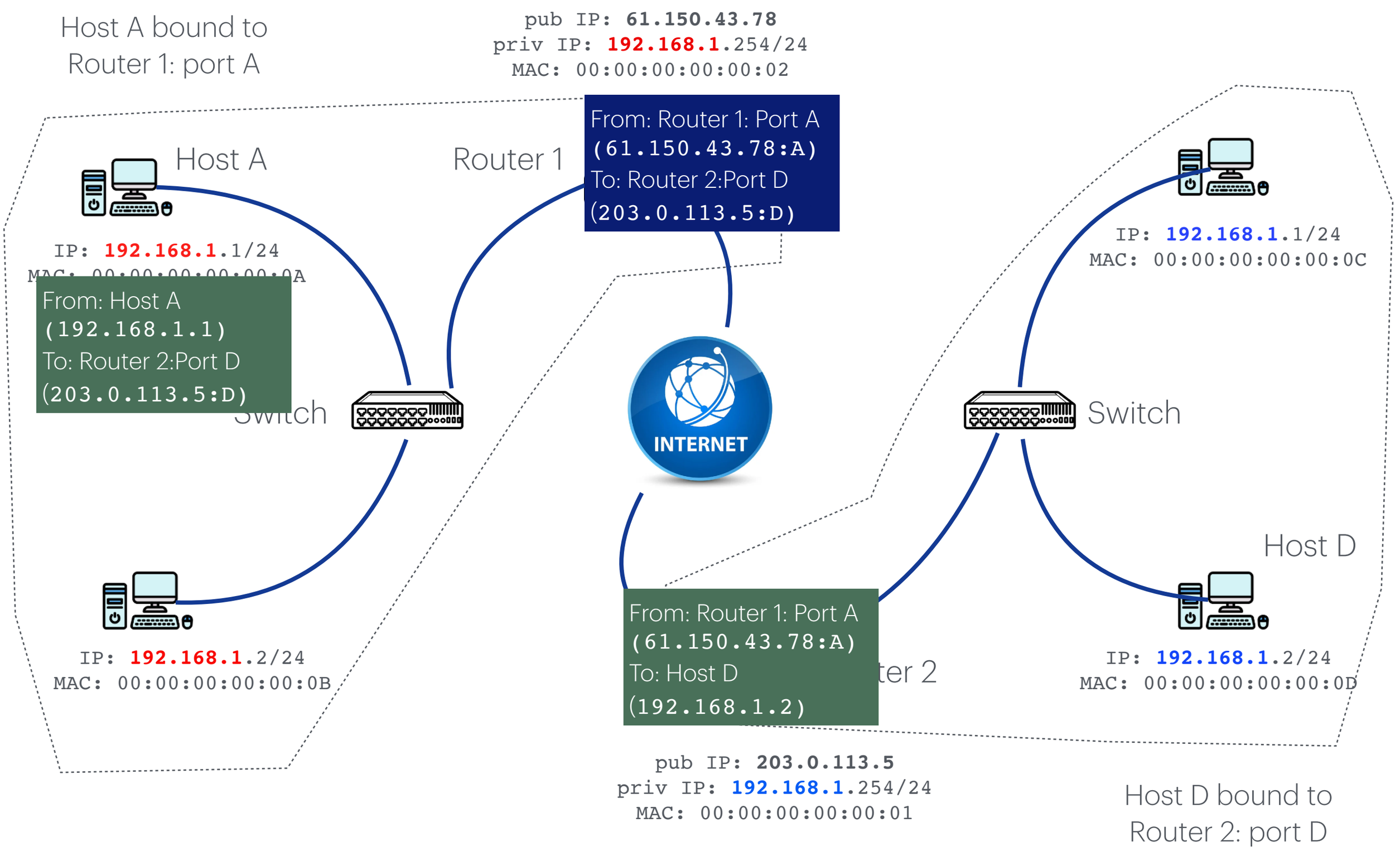
- No
- Send msg to the gateway (router)



Communicate between LANs

- Devices in a same LAN shares a *same* public IP via the router
  - Usually they are bound to different ports of the router
  - E.g., a web server may bind port 80 of the router
- Anyone outside the LAN can *only* send msg to the router's public IP addr
- The router will forward the msg based on the receiving port
  - Usually involves *translating* the destination from **`public_ip:port_A`** to some **`private_ip:port B`**
  - Known as Network Address Translation (NAT)

Communicate between LANs



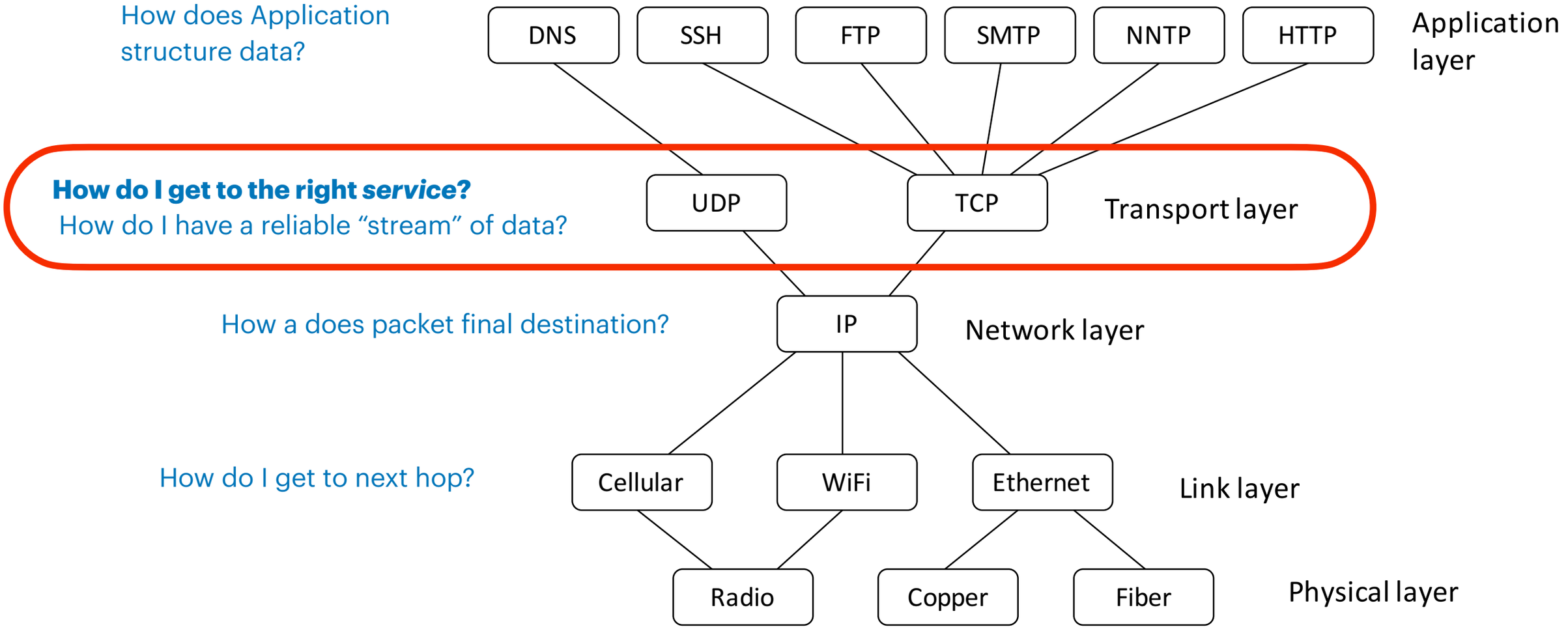
Takeaway

- IP Packet **crossed** the network boundary, but
- Data-Link **frames do not**

Transmission Control Protocol (TCP)

Transport Layer Protocols

How does Application structure data?



Ports

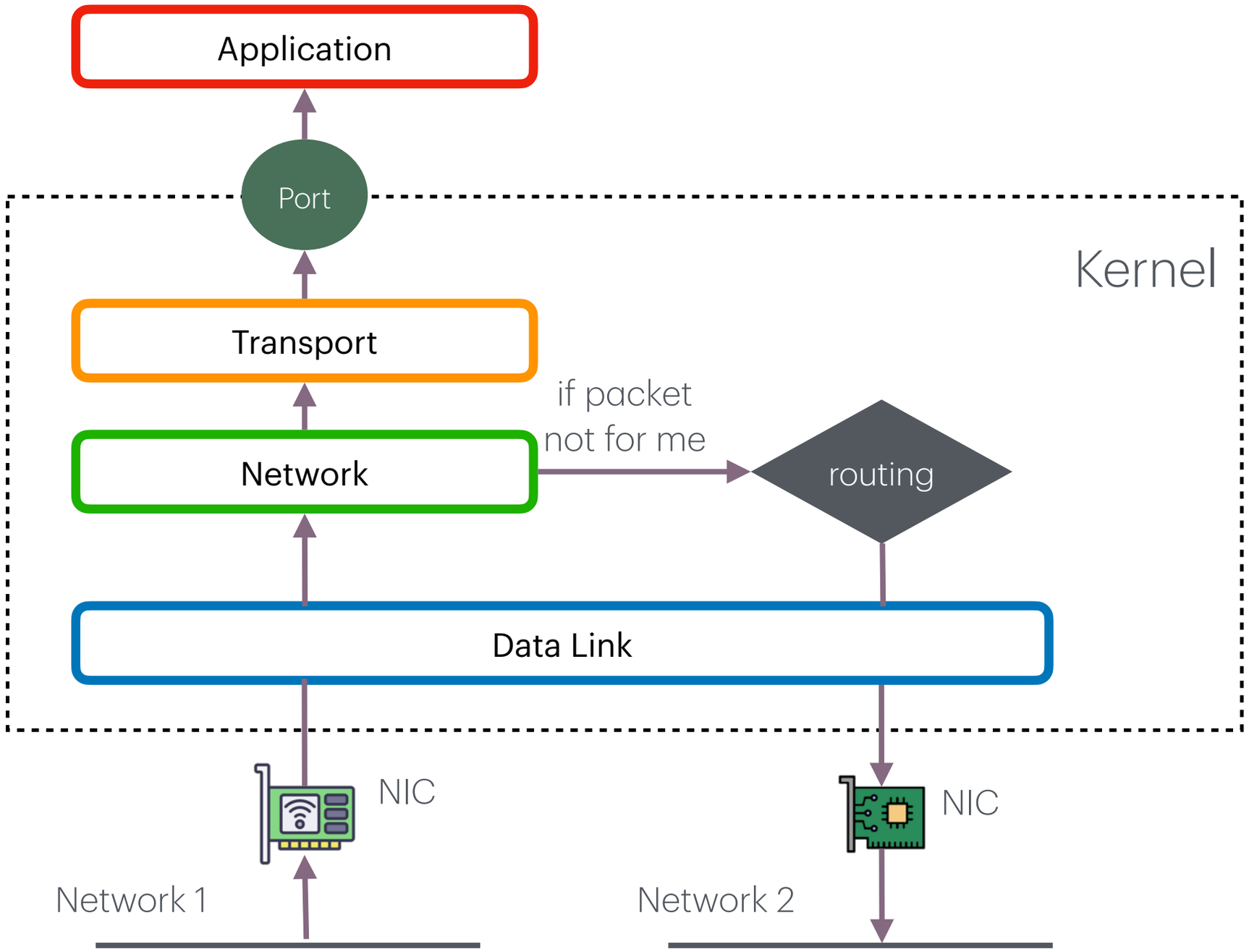
- Each **application/process** on a host is identified by a port number
  - Ports are numbered from 1 – 65535 (16 bits)
- TCP connection established between port `A` on host `X` to port `B` on host `Y`
- Extend network layer (IP)'s service from host-to-host delivery to process-to-process delivery.

Common Ports

Some destination port numbers used for specific applications by convention.

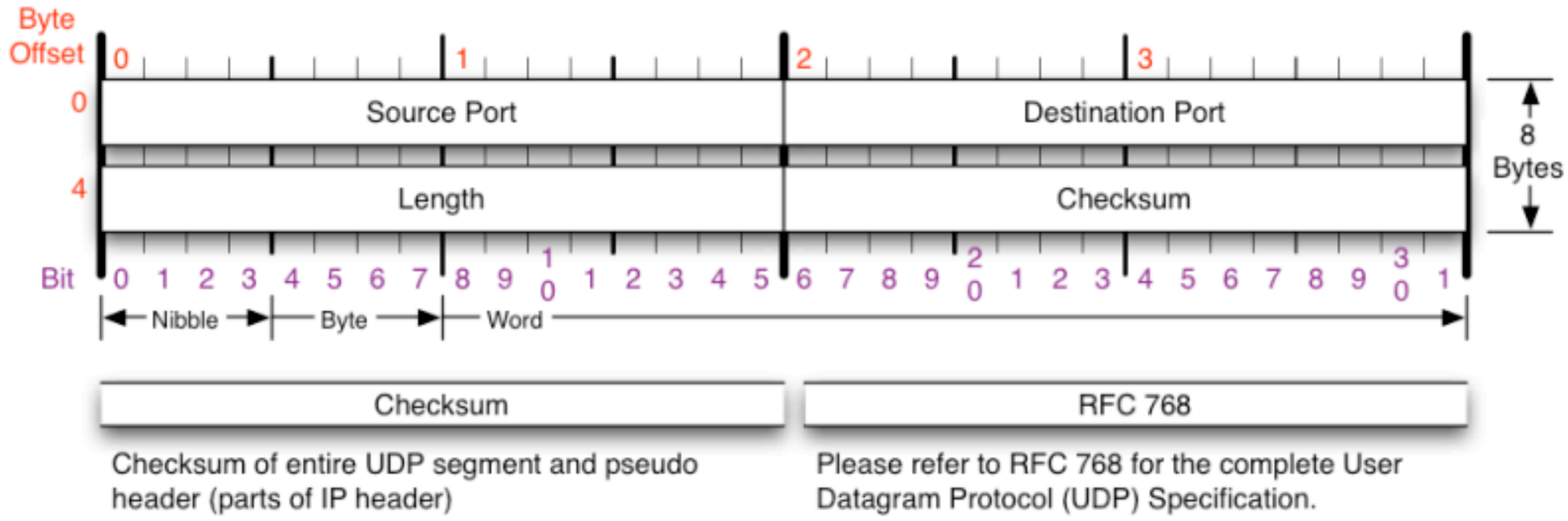
Port	Application
80	HTTP (Web)
443	HTTPS (Secure Web)
25	SMTP (mail delivery)
67	DHCP (host config)
22	SSH (secure shell)
23	Telnet

Packet receiving



UDP (User Datagram Protocol)

- **User Datagram Protocol (UDP)** is a transport layer protocol that is *essentially a IP packet with ports*
  - Adds ports to demultiplex traffic by application



UDP Header

UDP (User Datagram Protocol)

UDP is designed on top of IP.

- **Pros**: Lightweight.
    - Avoid overhead and delays of ordered, reliable delivery;
    - No delay for connection establishment; No connection state.
    - Small packet header overhead
- **Cons**: just like the cons of IP
    - Unreliable data transfer between sending and receiving processes
    - No ordering of messages, no tracking connections; No flow control or congestion control; No timing or throughput guarantee

Who uses UDP?

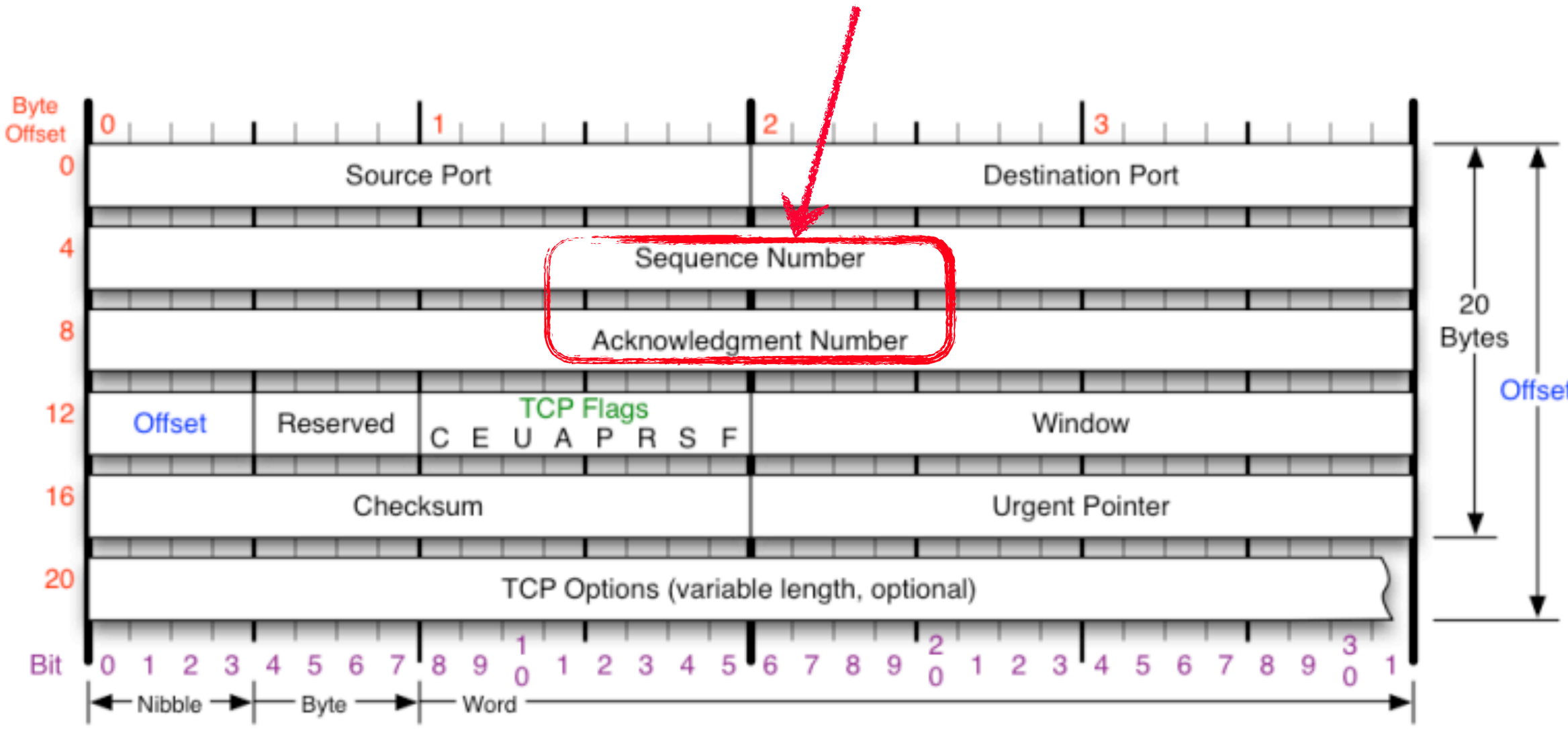
- Multimedia streaming
  - Retransmitting lost/corrupted packets is not worthwhile
    - By the time the packet is retransmitted, it's too late
    - E.g., telephone calls, video conferencing, gaming
- Simple query protocols like Domain Name System
  - Overhead of connection establishment is overkill
  - Easier to have application retransmit if needed

From Packets to Bytestreams

- Many applications want a stream of bytes delivered reliably and in-order between applications on different hosts
- **Transmission Control Protocol (TCP)** provides …
  - Connection-oriented protocol with explicit setup/teardown
  - Reliable in-order byte stream
  - Congestion control
- Despite IP packets being dropped, re-ordered, and duplicated

TCP Packet

Key fields that enable reliable transmission

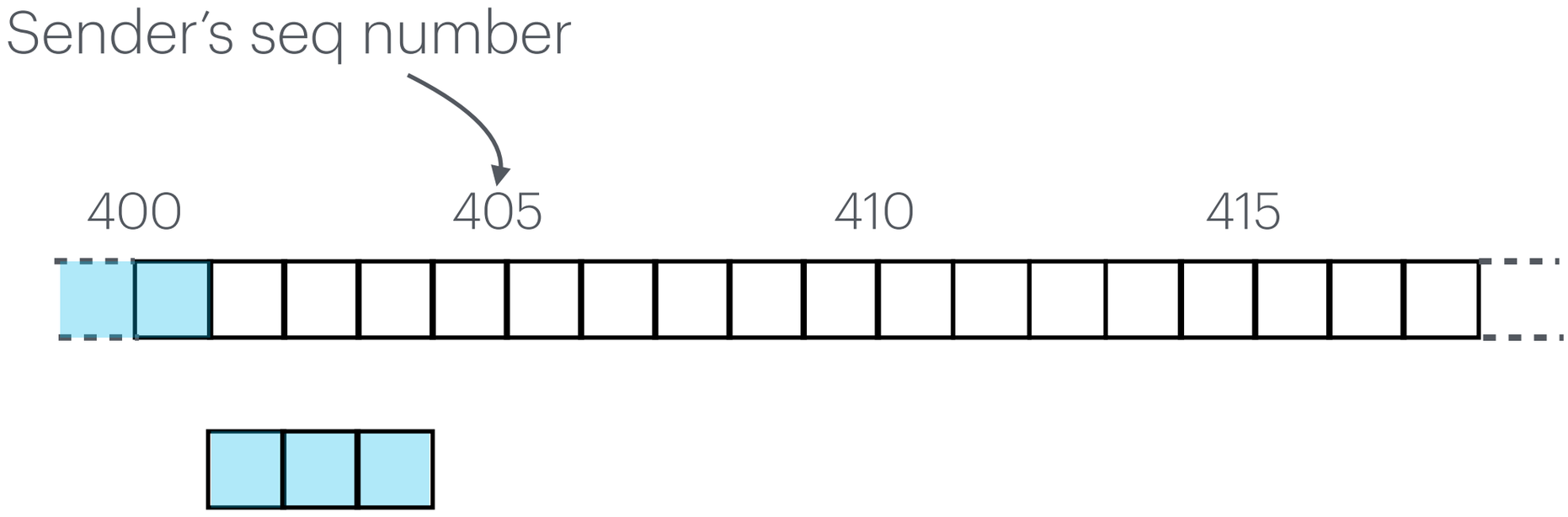


TCP Seq. No. and Ack. No.

- Two data streams in a TCP session, one in each direction
- **Sequence Number**: Bytes in each data stream are numbered with a 32-bit number.
  - The numbering starts with an random offset.
- **Acknowledge Number**: Receiver sends acknowledgement number that indicates data received
  - The value of the acknowledgment field in a segment defines the number of the next byte a party expects to receive.

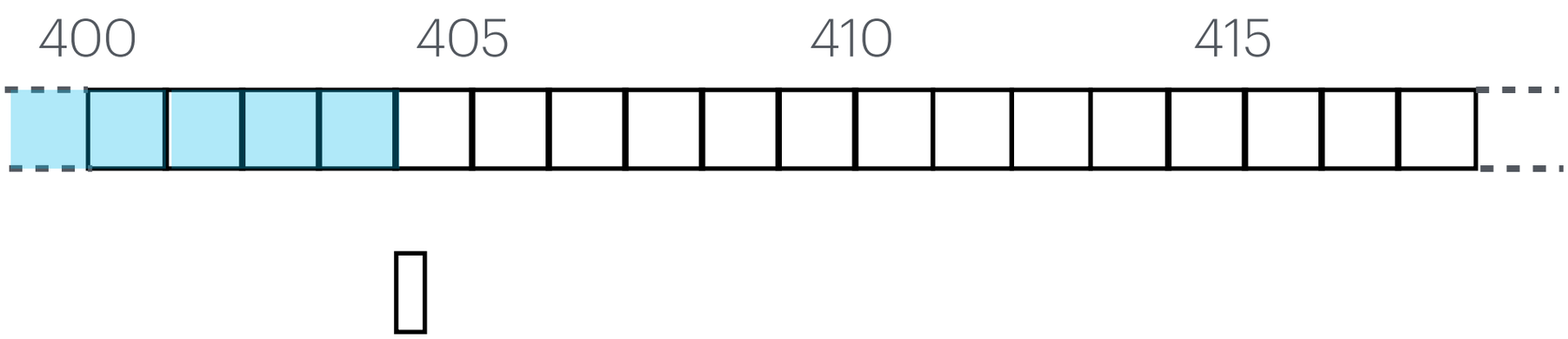
TCP: Sending data

- Sender sends 3-byte segment
- Sequence number indicates where data belongs in byte sequence (at byte 401)



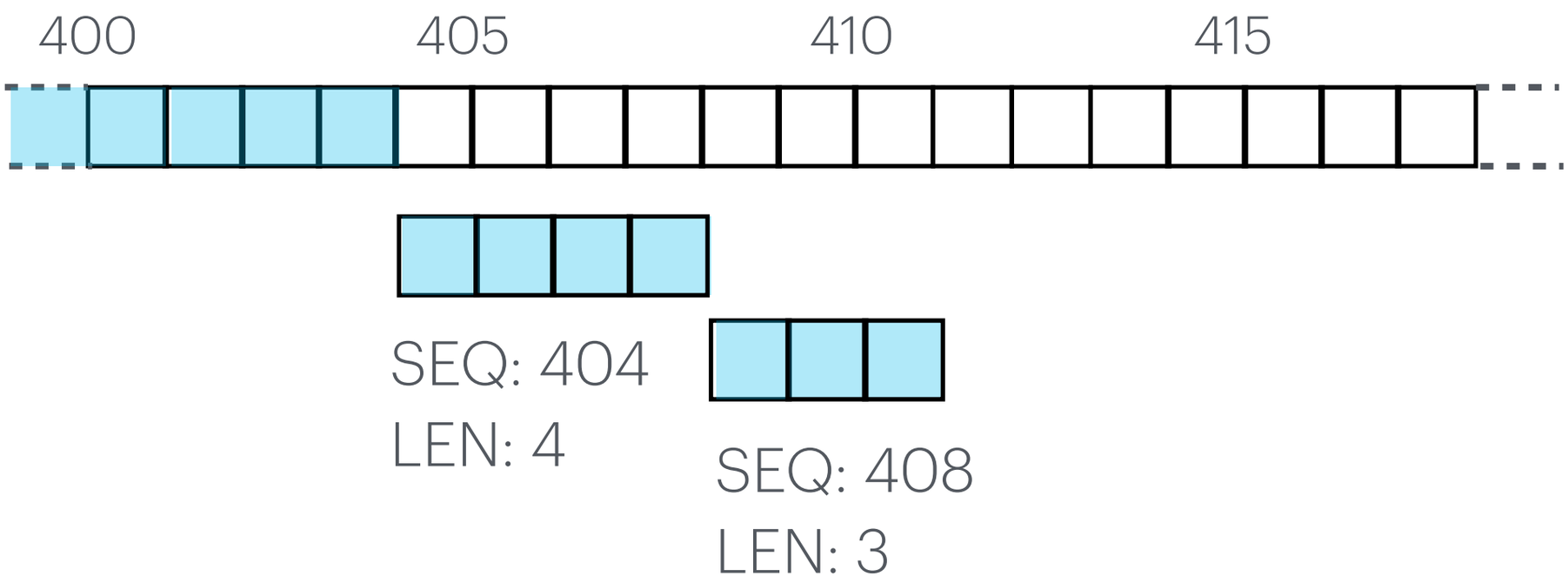
TCP: Acknowledging data

- Receiver acknowledges received data
  - Set ACK flag in TCP header
  - Set acknowledged number to indicate next expected byte in the stream.



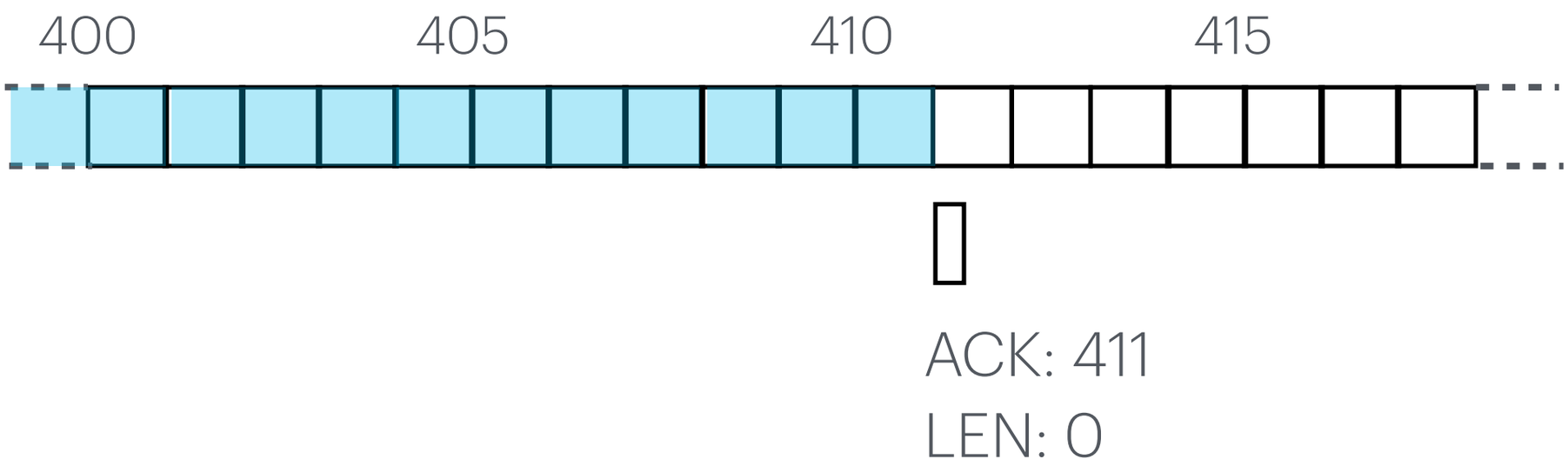
TCP: Ack multiple segments

- Sender may send several segments before receiving acknowledgement.



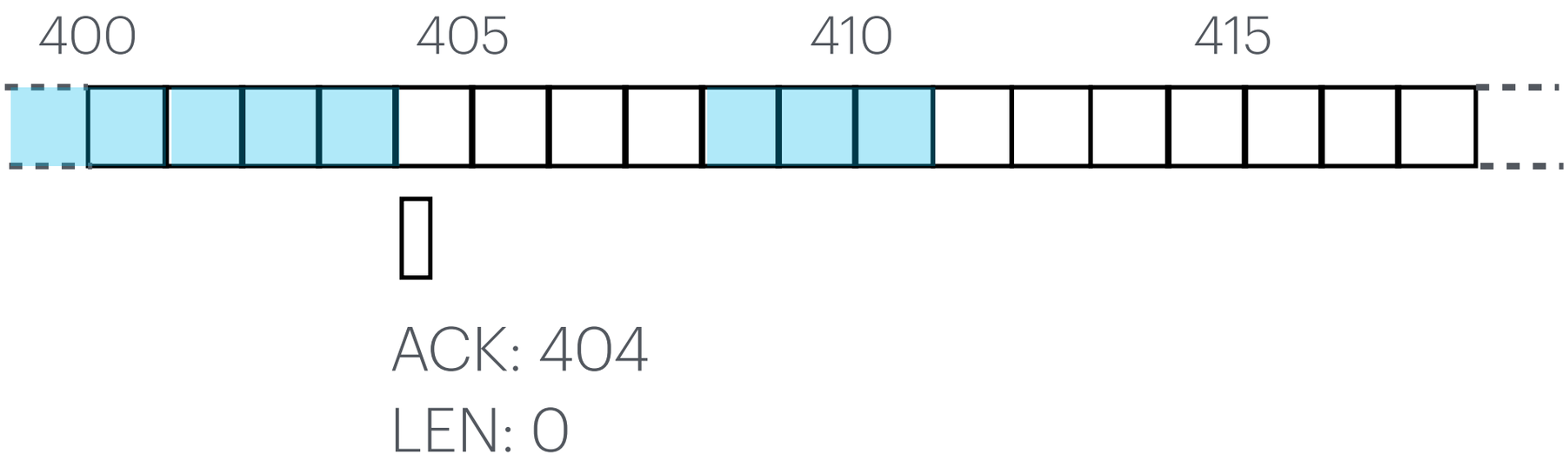
TCP: Ack multiple segments

- Sender may send several segments before receiving acknowledgement.
- Receiver always ack the seq number of *next expected byte*



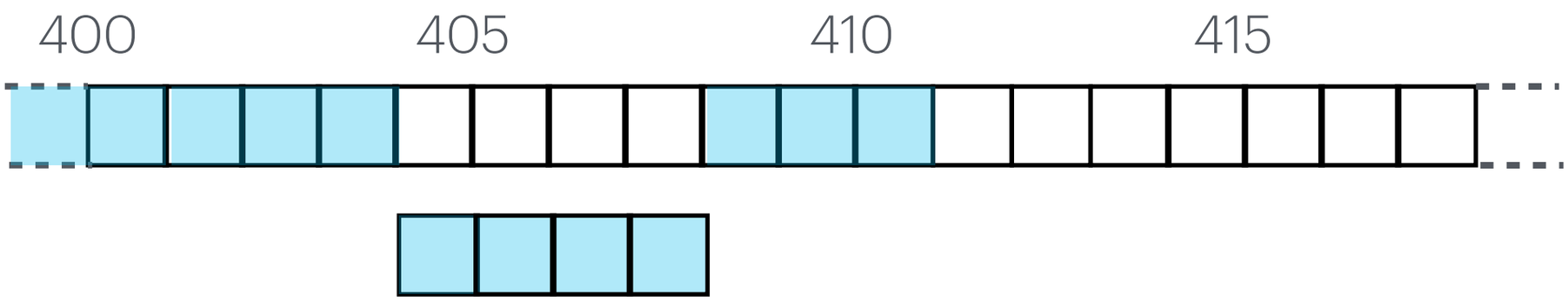
TCP: Packet re-transmission

- What if the first packet was dropped in network?
- Receiver always ack with the seq number of *next expected byte*



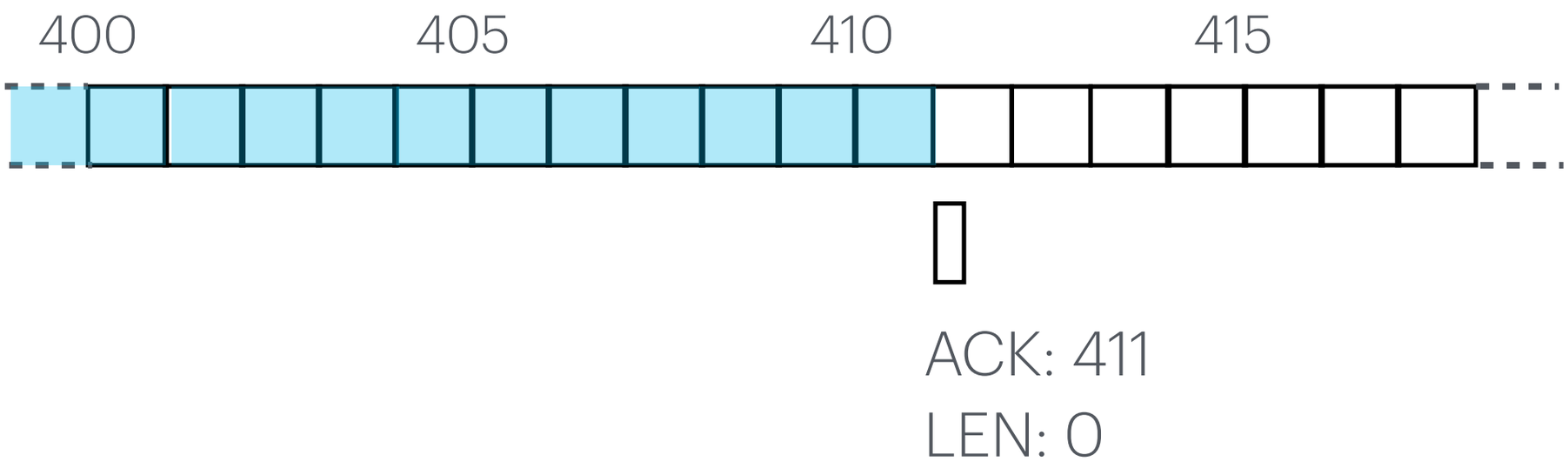
TCP: Packet re-transmission

- What if the first packet was dropped in network?
- Receiver always ack with the seq number of *next expected byte*.
- Sender retransmits the lost segment

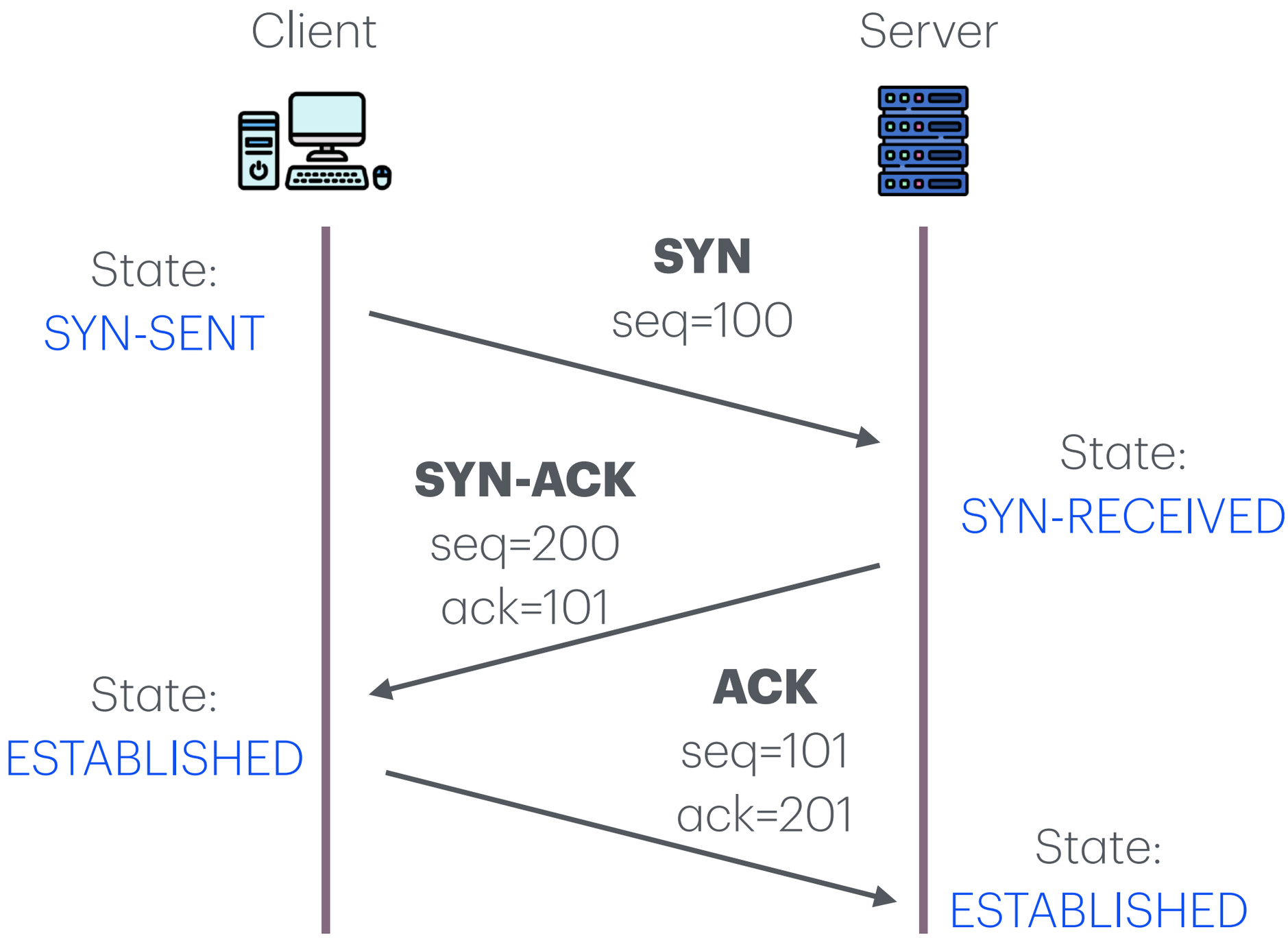


TCP: Packet re-transmission

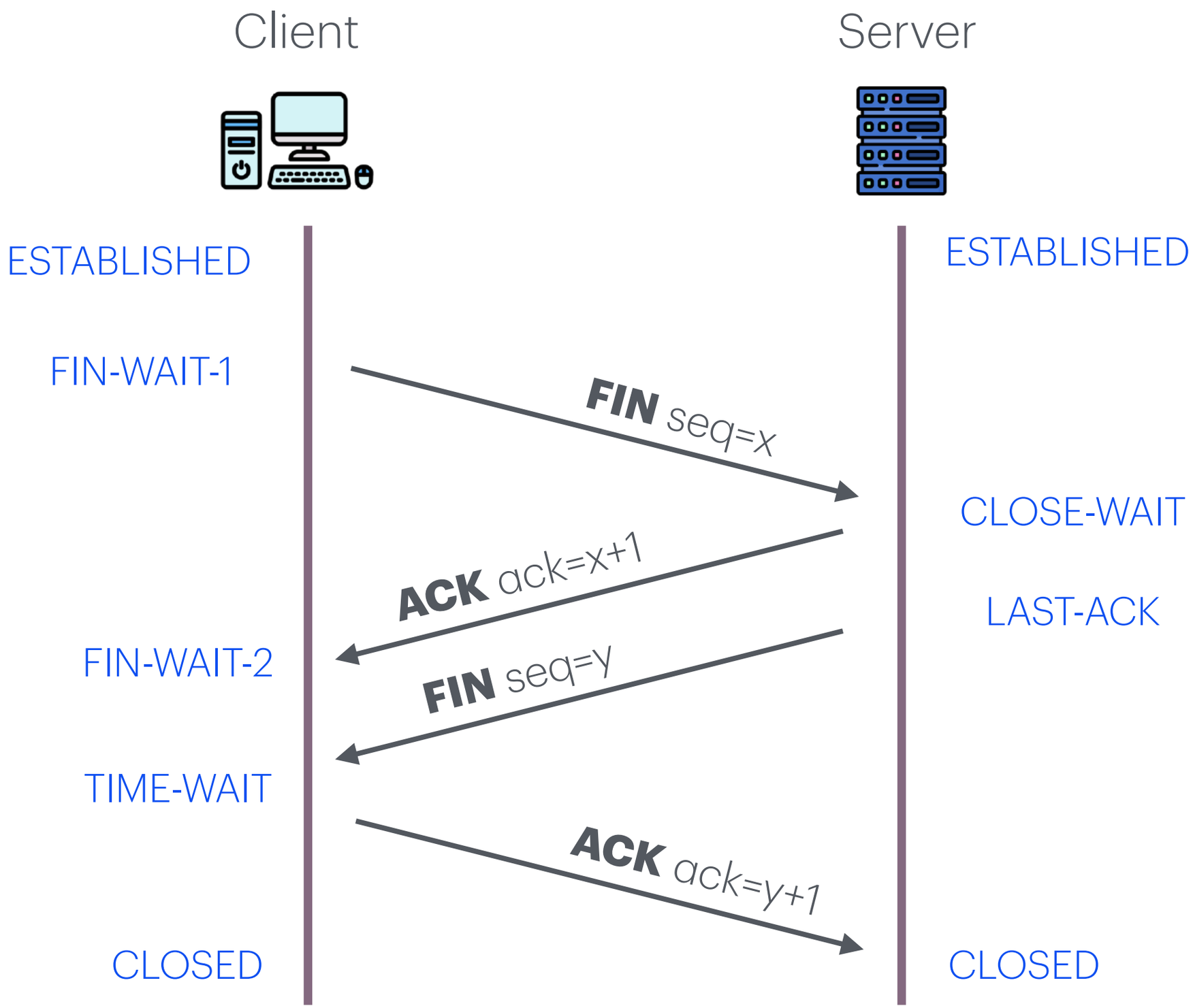
- What if the first packet was dropped in network?
- Sender retransmits the lost segment
- Receiver always ack the seq number of *next expected byte*



TCP Three-Way Handshake



Connection Ending Handshake

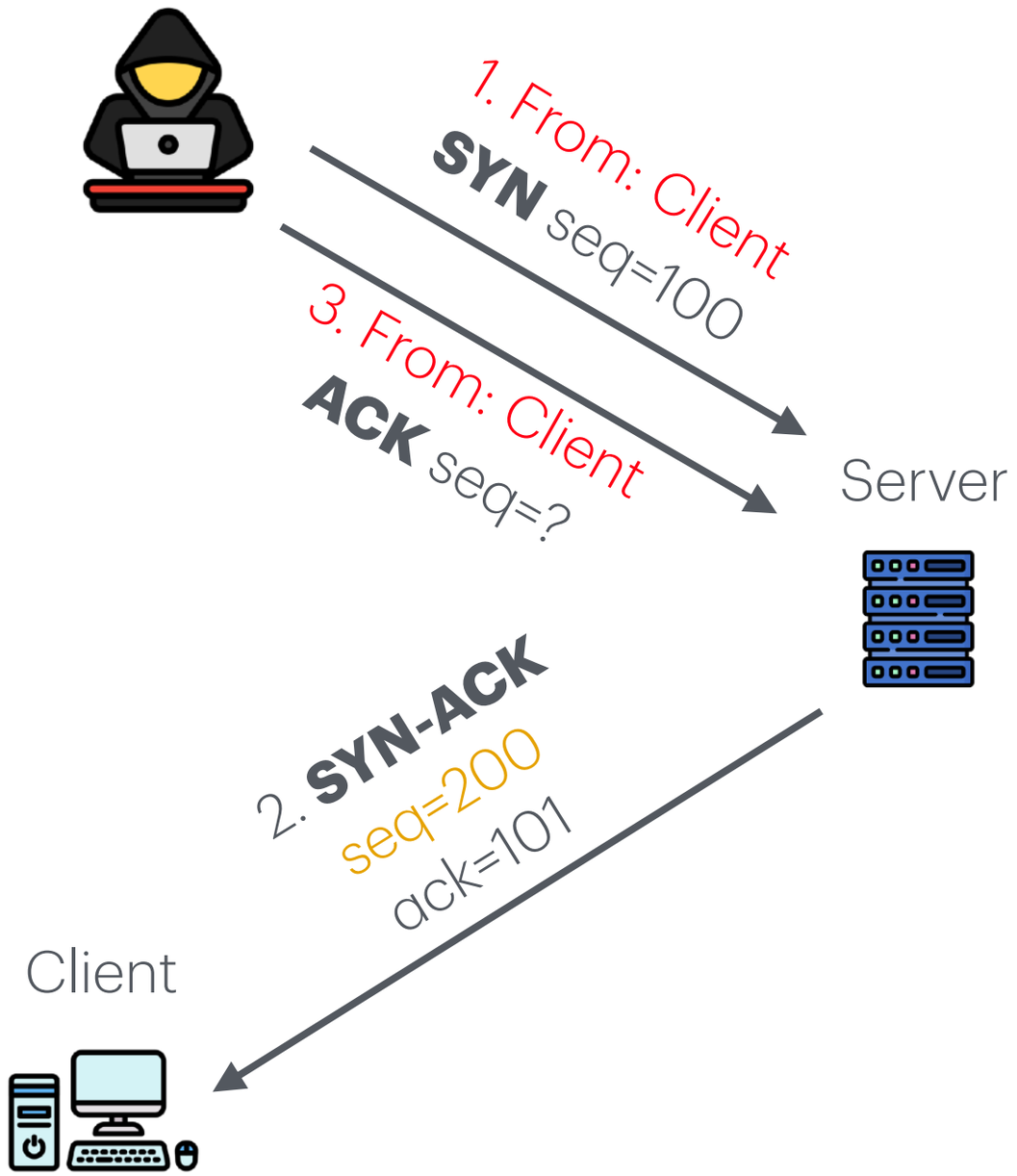


TCP Connection Reset

- TCP designed to handle possibility of spurious TCP packets (e.g. from previous connections)
- Packets that are invalid given current state of session generate a TCP reset
  - If a connection exists, it is torn down
  - Packet with **RST** flag sent in response
- If a host receives a TCP packet with RST flag, it tears down the connection

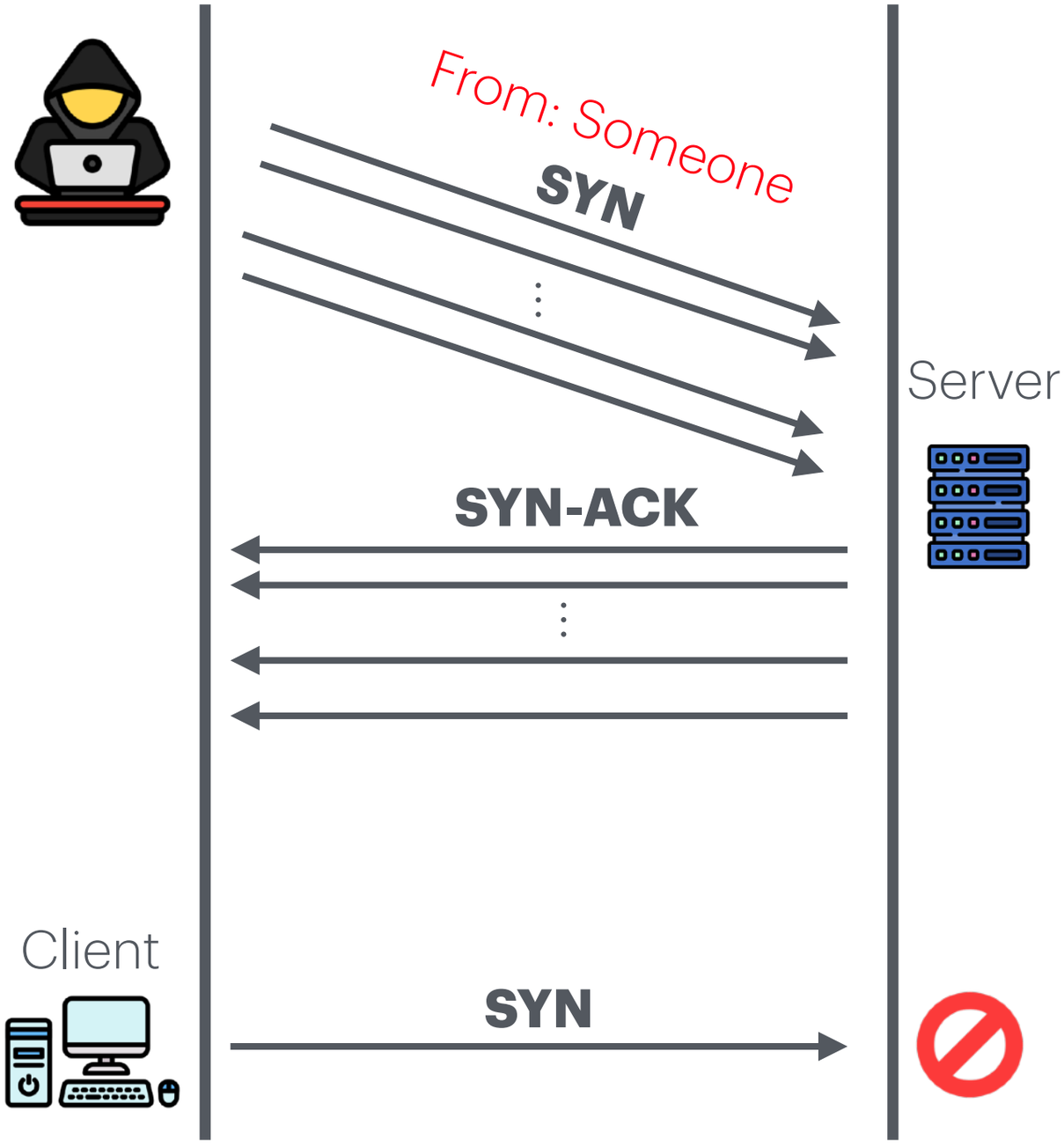
TCP Connection Spoofing

- Can we impersonate another host when *initiating* a connection?
- Off-path attacker can send *initial* SYN to server ..... *but cannot complete three-way handshake without seeing the server's sequence number*
- 1 in 2^{32} chance to guess right if initial sequence number chosen uniformly at random



TCP SYN Flooding

- Attacker sends many connection requests
  - May use spoofed source IP addresses
- Victim allocates resources for each request
  - Connection requests exist until timeout
- Resources exhausted ⇒ legitimate requests rejected
- No need to guess sequence number



TCP Session Hijacking

TCP Reset Attack

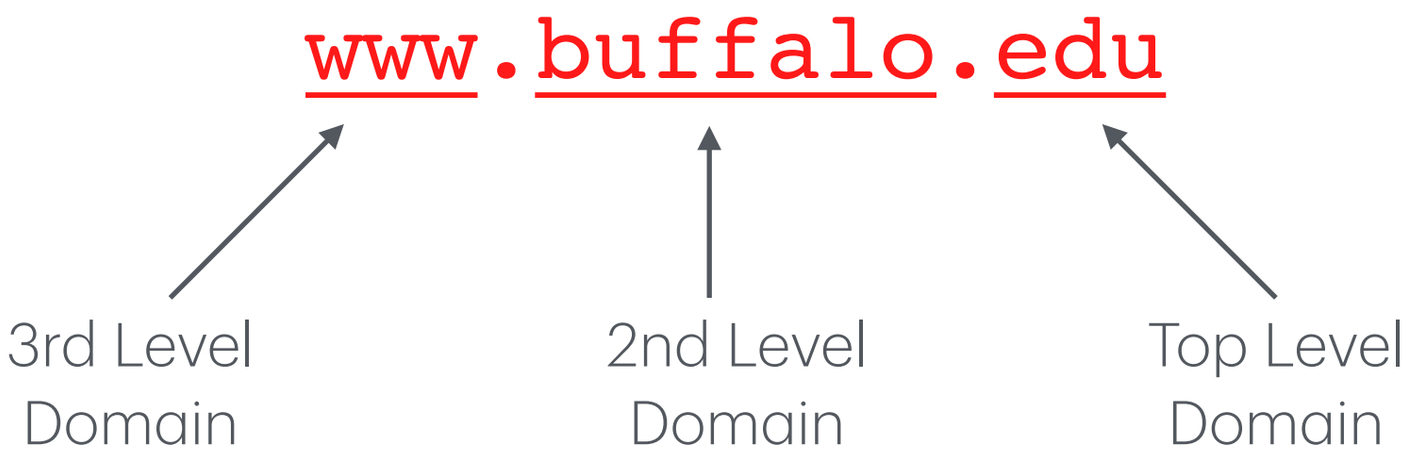
- Can we reset an *existing* TCP connection?
  - Need to know port numbers (16 bits)
    - Initiator's port number usually chosen random by OS
    - Responder's port number may be well-known port of service
  - There is leeway in sequence numbers B will accept
    - Must be within window size (32-64K on most modern OSes)
- 1 in $2^{16+32}/W$ (where W is window size) chance to guess right

Domain Name Services (DNS)

DNS (Domain Name Service)

- Application-layer protocols (and people) usually refer to Internet host by host name (e.g., **`google.com`**)

- DNS is a delegatable, hierarchical name space

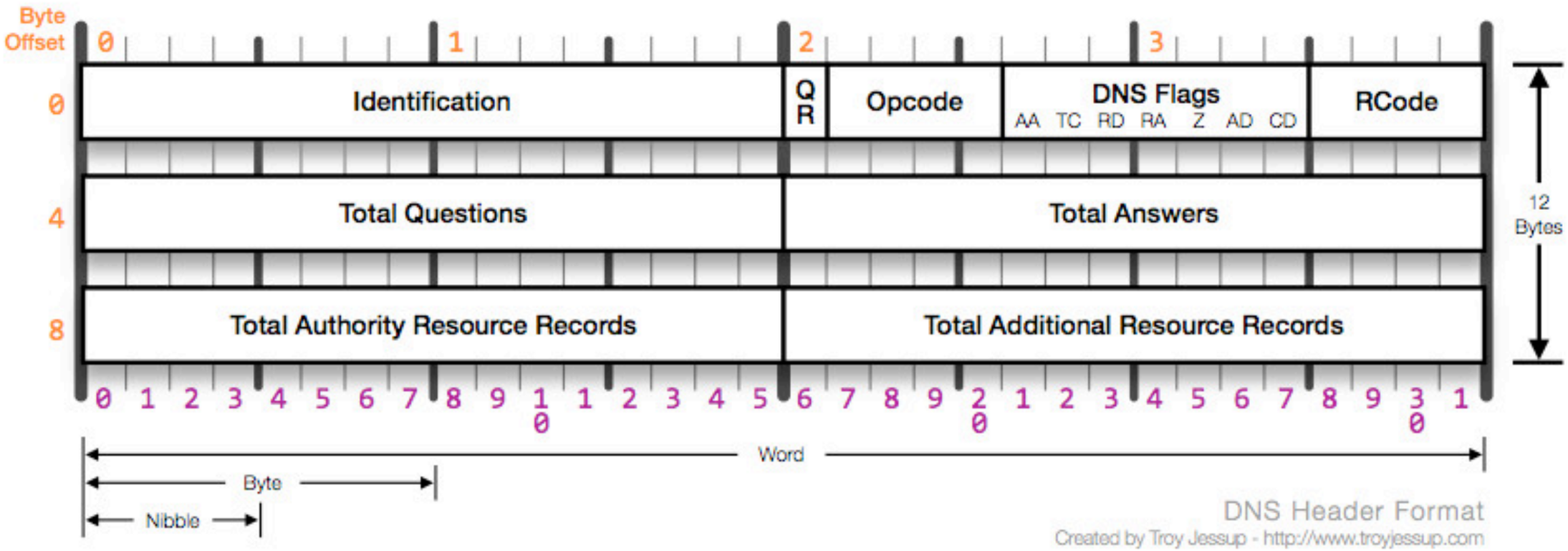


DNS Root Servers

In total, there are 13 main DNS root servers, each of which is named with the letters 'A' to 'M'.

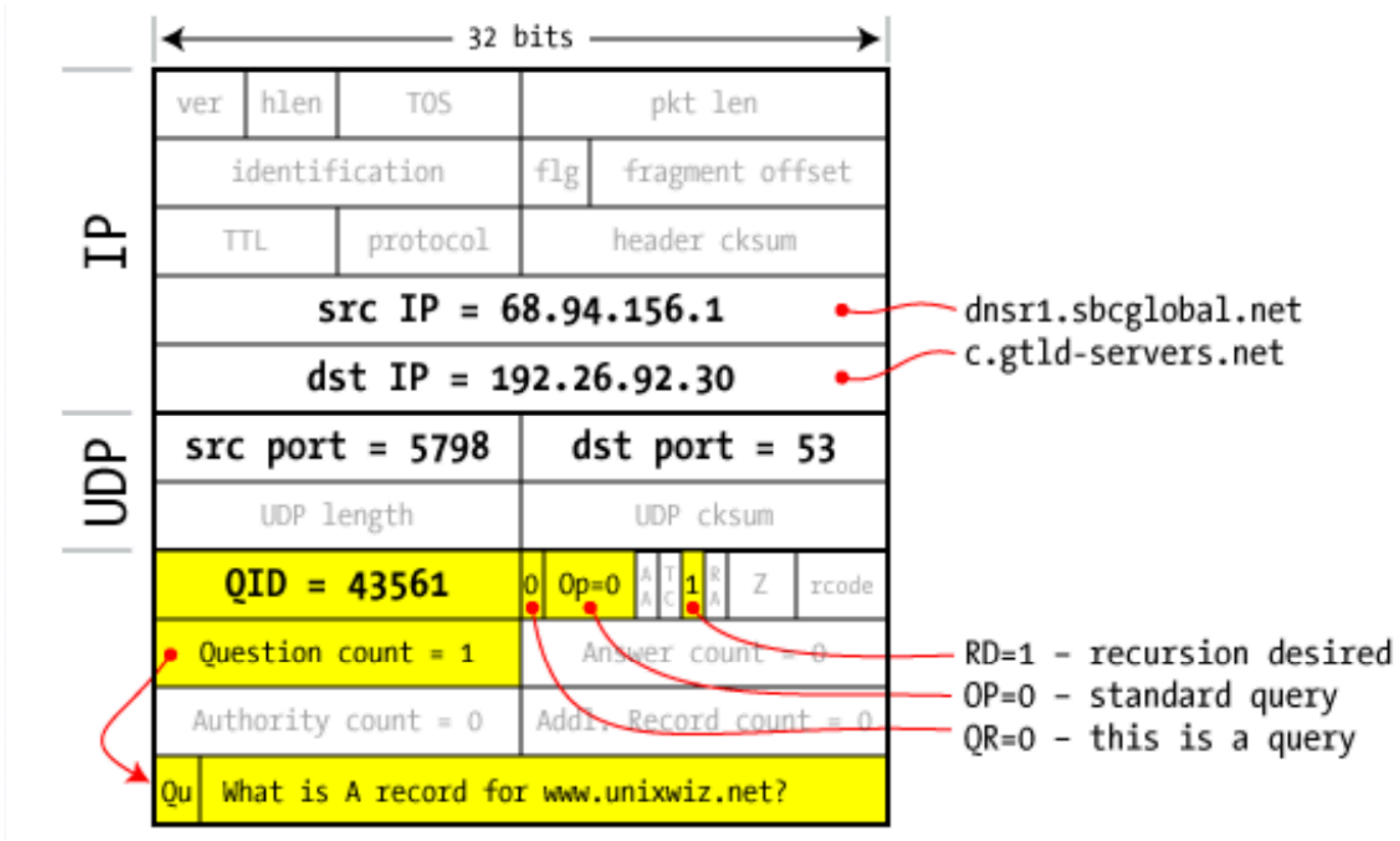
HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

DNS Packet

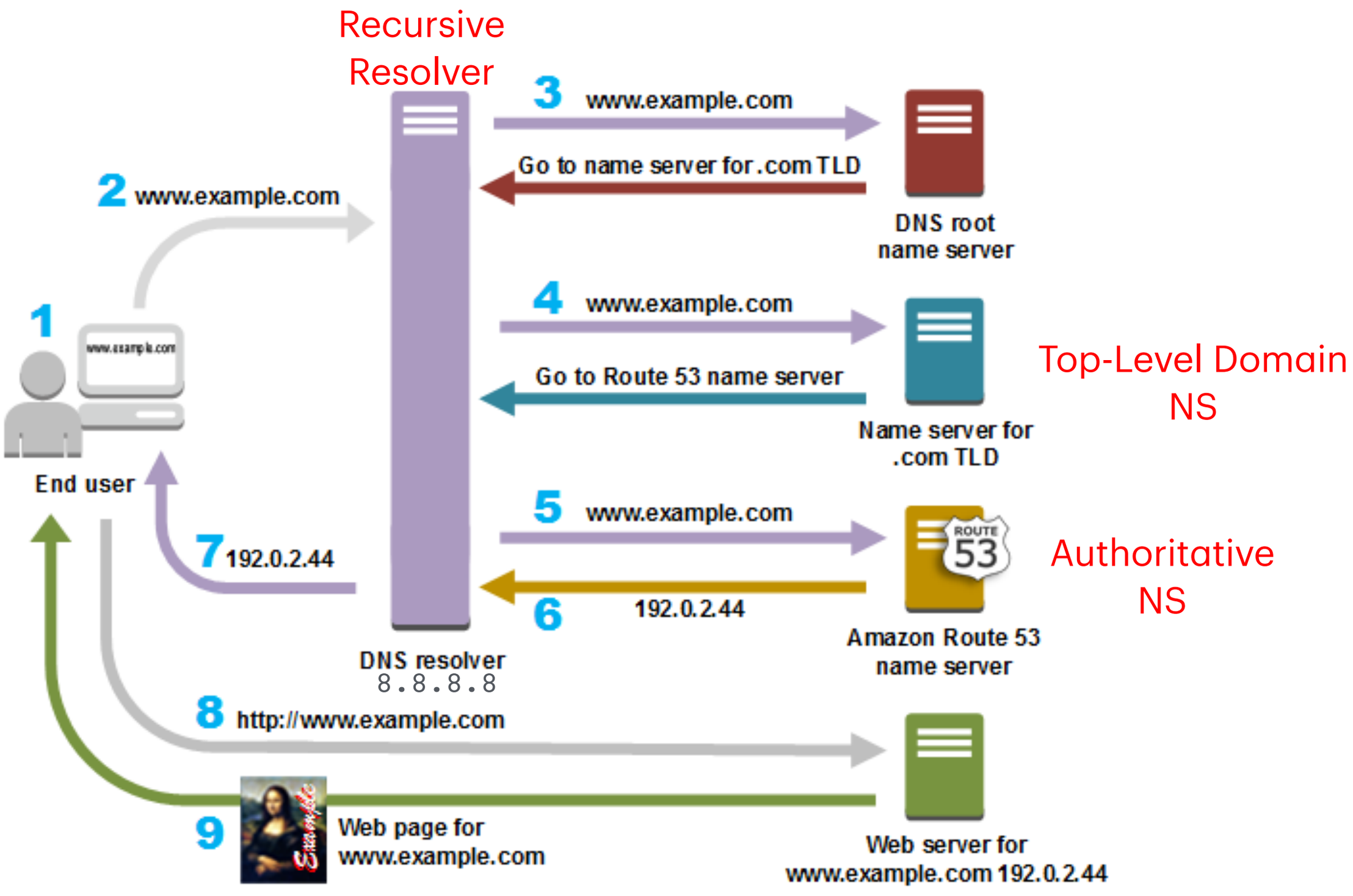


- DNS requests sent over UDP
- **Four sections**: questions, answers, authority, additional records
- **Query ID**: 16 bit random value links response to query

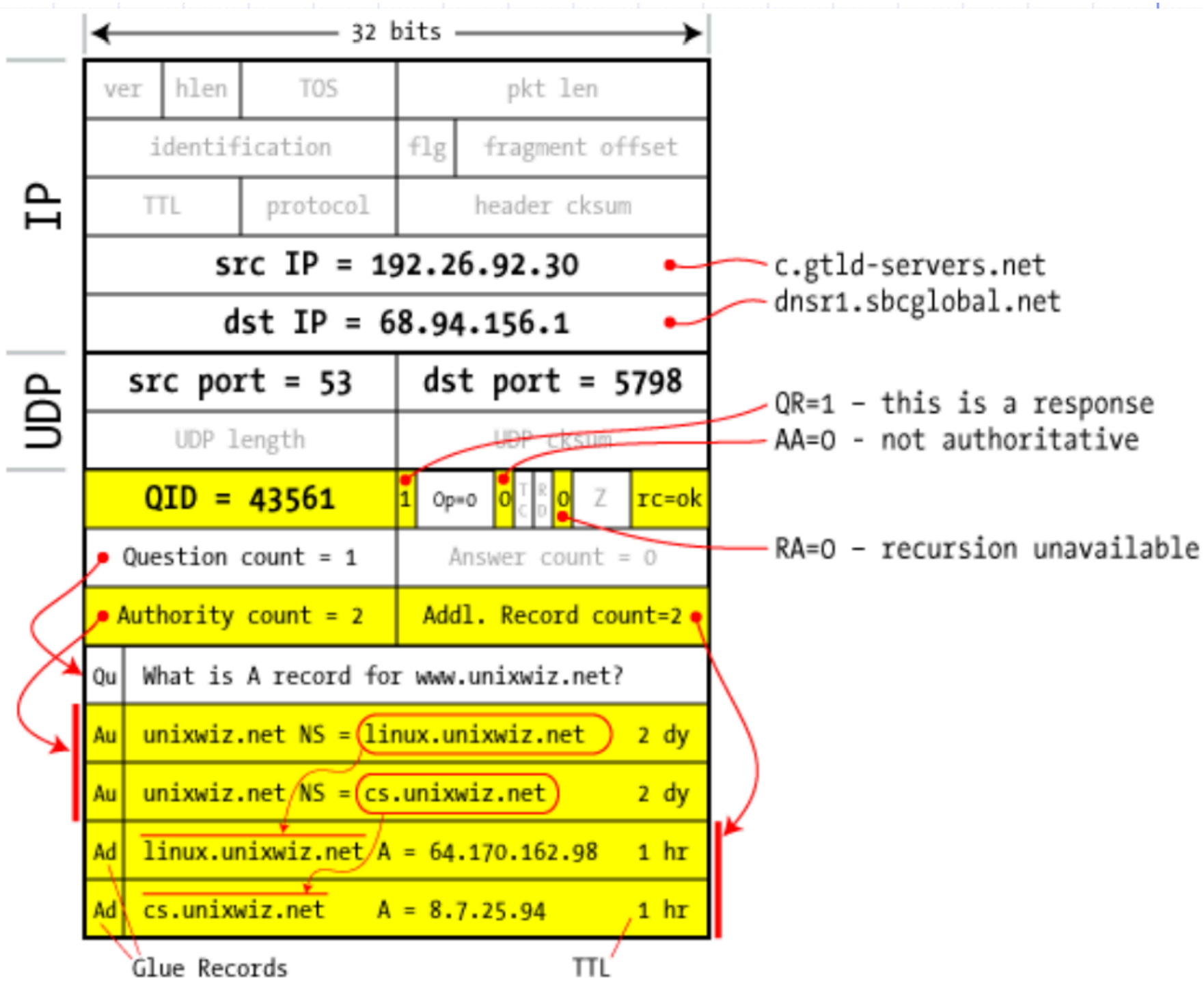
DNS Request


32 bits
IP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 68.94.156.1
dst IP = 192.26.92.30
dnsr1.sbcglobal.net
c.gtld-servers.net
UDP
src port = 5798
dst port = 53
UDP length
UDP cksum
QID = 43561
0
Op=0
A A
T C
1
R A
Z
rcode
Question count = 1
Answer count = 0
Authority count = 0
Addl. Record count = 0
Qu
What is A record for www.unixwiz.net?
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query

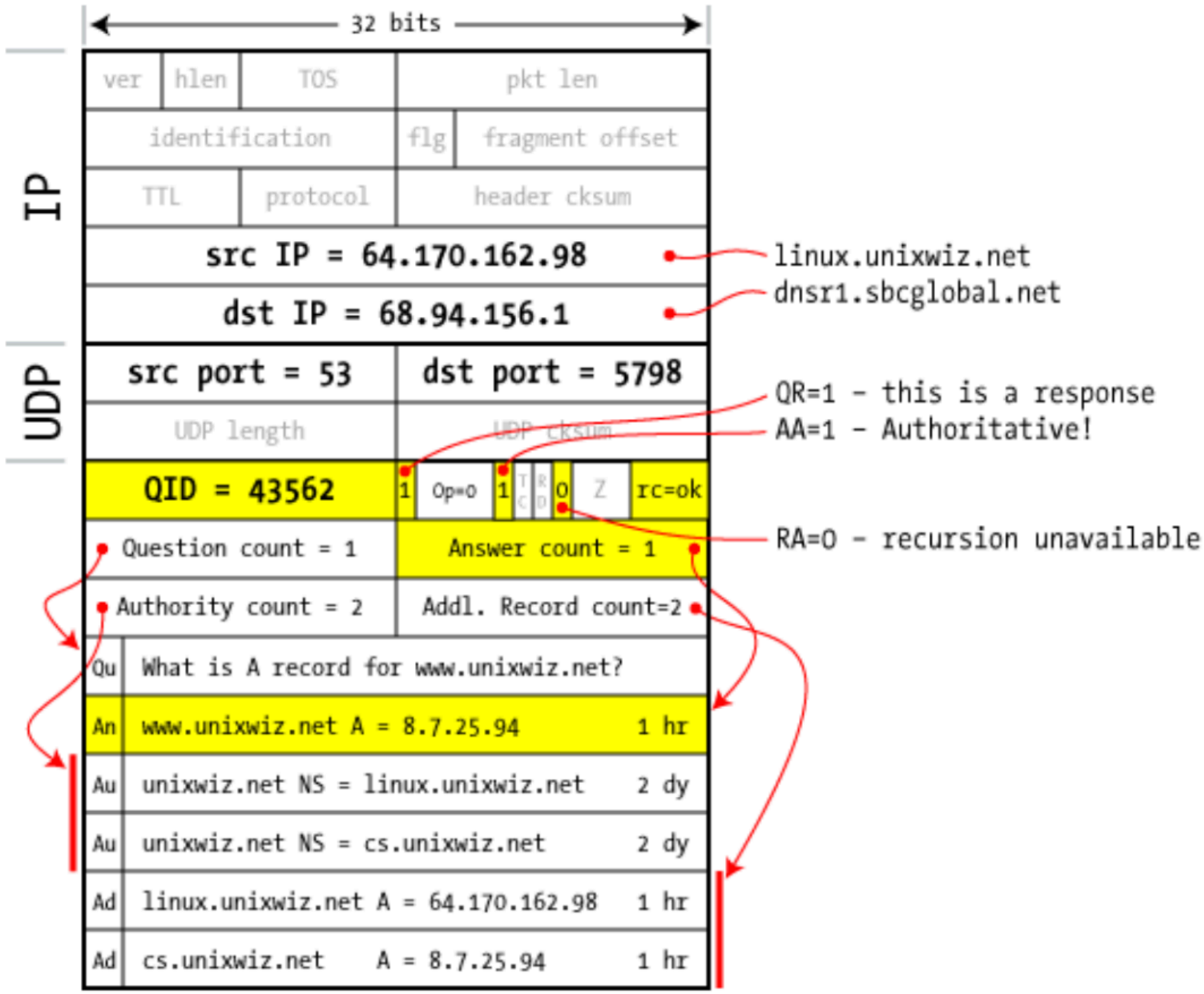
(Recursive) DNS resolution



DNS Response



Authoritative Response



DNS Query Example

```
$ dig www.example.com

; <<>> DiG 9.10.6 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5076
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.         3600    IN      A       93.184.215.14

;; Query time: 176 msec
;; SERVER: 162.252.172.57#53(162.252.172.57)
;; WHEN: Thu Oct 24 11:17:42 EDT 2024
;; MSG SIZE  rcvd: 60
```

The IP addr found for **example.com**

The DNS server that answers the query

DNS Security

- Users/hosts trust the host-address mapping provided by DNS
  - Used as basis for many security policies:
  - Browser same origin policy, URL address bar
- Interception of requests or compromise of DNS servers can result in incorrect or malicious responses

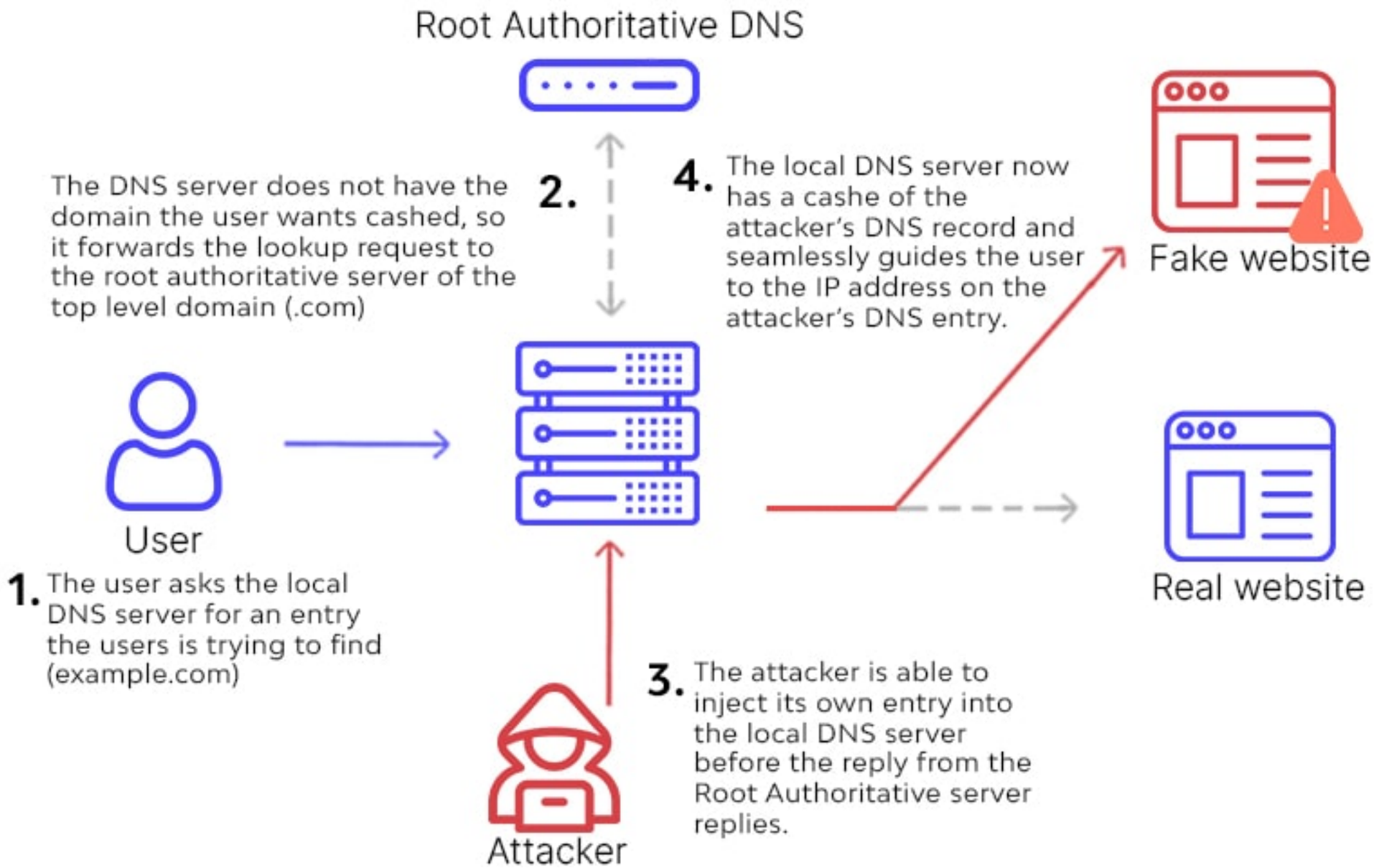
DNS Caching

- DNS responses are cached
  - Quick response for repeated translations
  - NS records for domains also cached
- DNS negative queries are cached
  - Save time for nonexistent sites, e.g. misspelling
- Cached data periodically times out
  - Lifetime (TTL) of data controlled by owner of data
  - TTL passed with every record

DNS Cache Poisoning

- A typical DNS query (e.g., for **`www.bank.com`**) is usually sent to a *recursive* DNS resolver.
  - If the resolver doesn't have the answer cached, it will query the necessary authoritative DNS servers.
- The attacker sends forged DNS responses to the recursive DNS resolver before it receives a legitimate response from the authoritative server.
- The goal of the attacker is to trick the resolver into caching a false IP address for a specific domain (e.g., pointing **`www.bank.com`** to a malicious server controlled by the attacker).

DNS Cache Poisoning

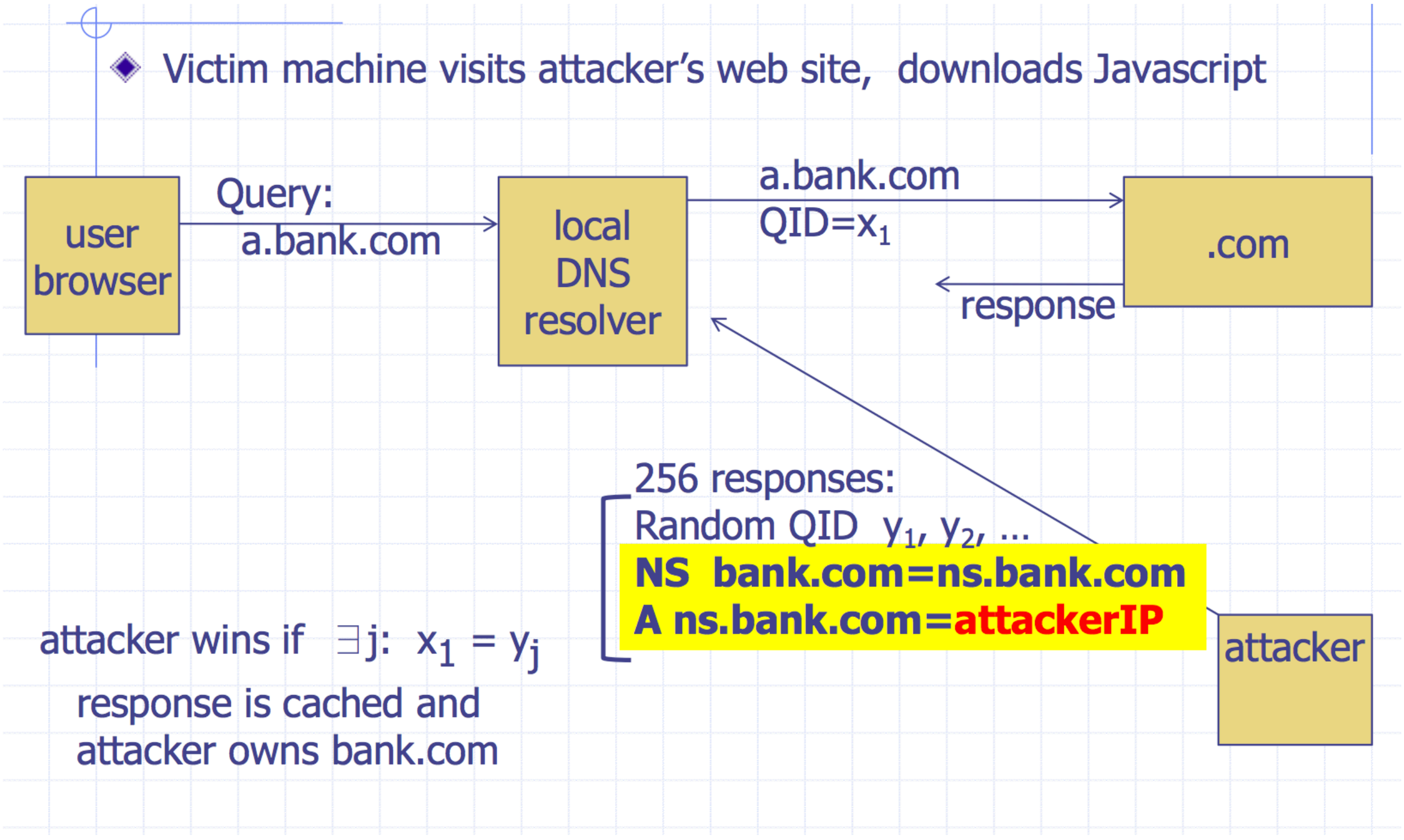


DNS Cache Poisoning

- The corrupted entry can be injected via spoofing
- How does client authenticate response?
  - UDP port numbers must match
  - Destination port usually port 53 by convention
  - **16-bit** query ID must match

Kaminsky Attack

- Victim machine visits attacker's web site, downloads Javascript



Questions