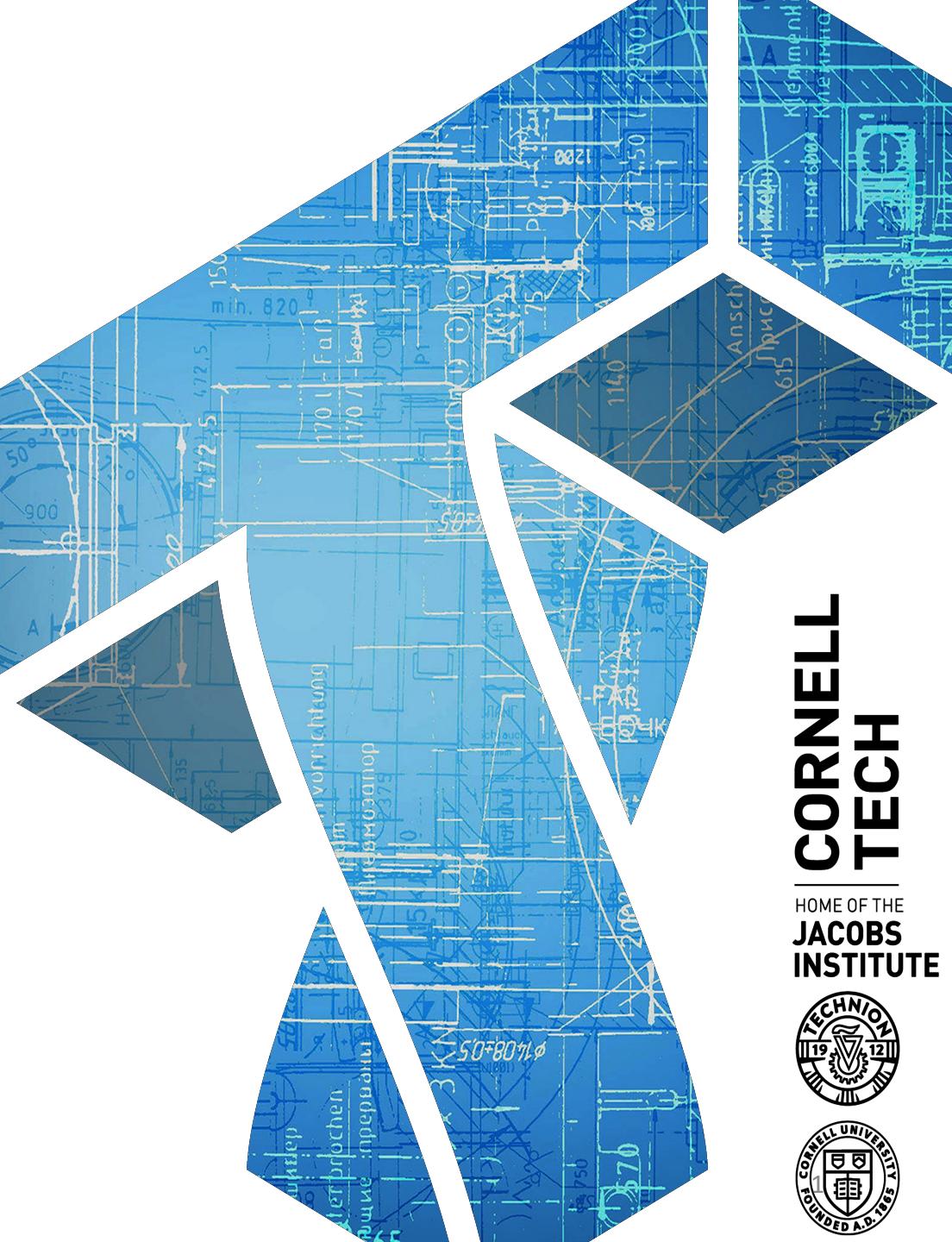


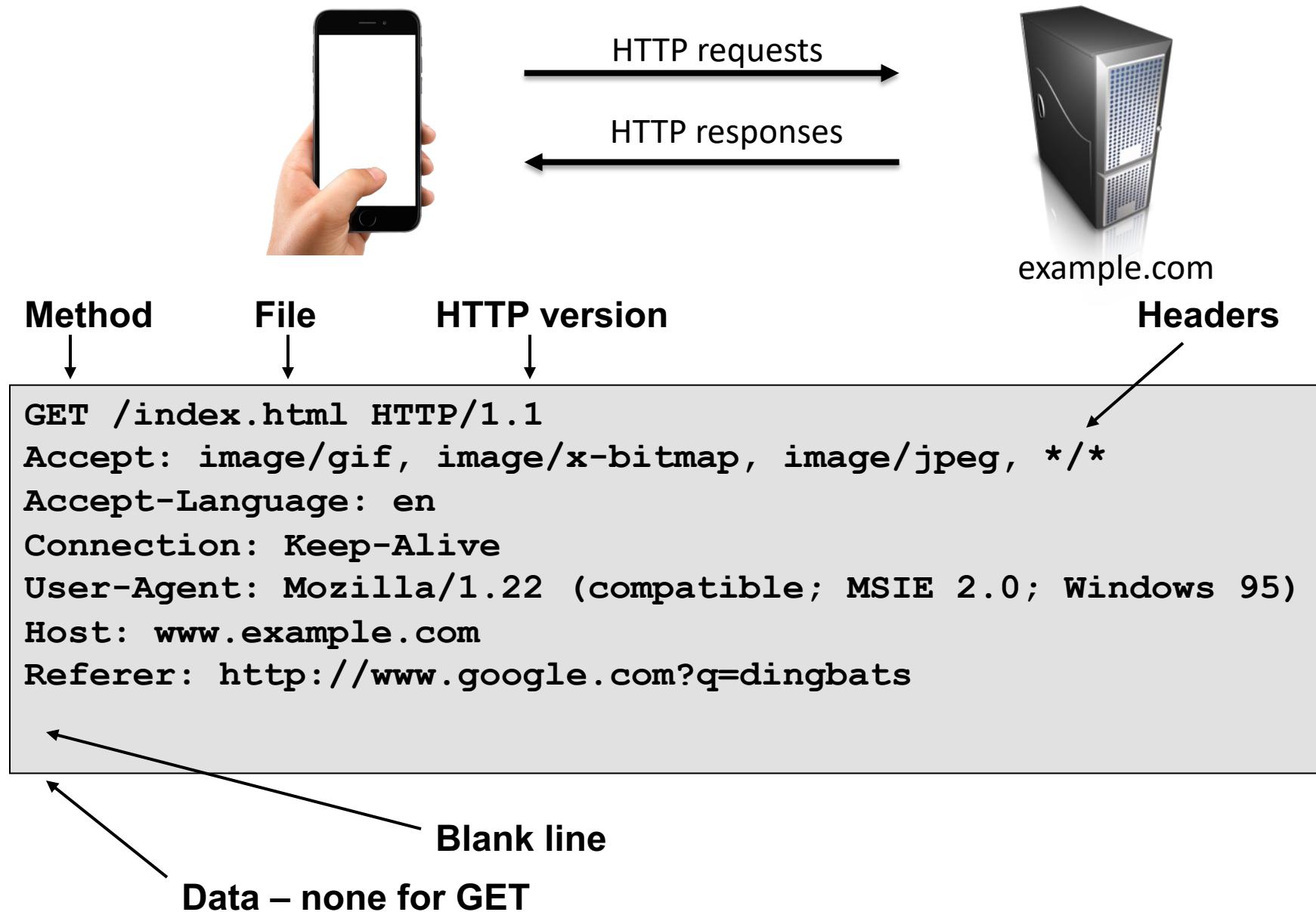
# CS 5435: Network security

Instructor: Tom Ristenpart

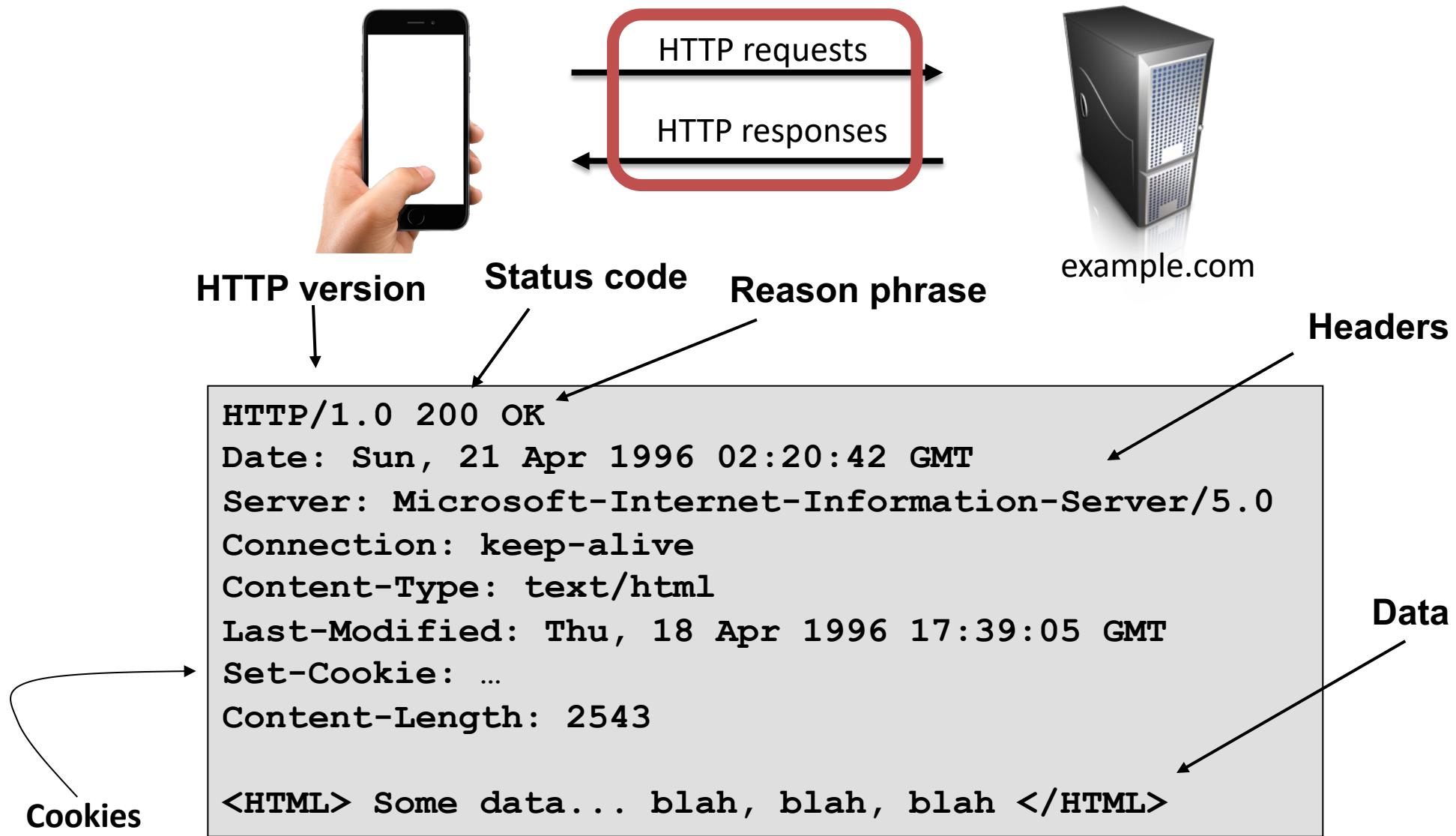
<https://github.com/tomrist/cs5435-fall2024>



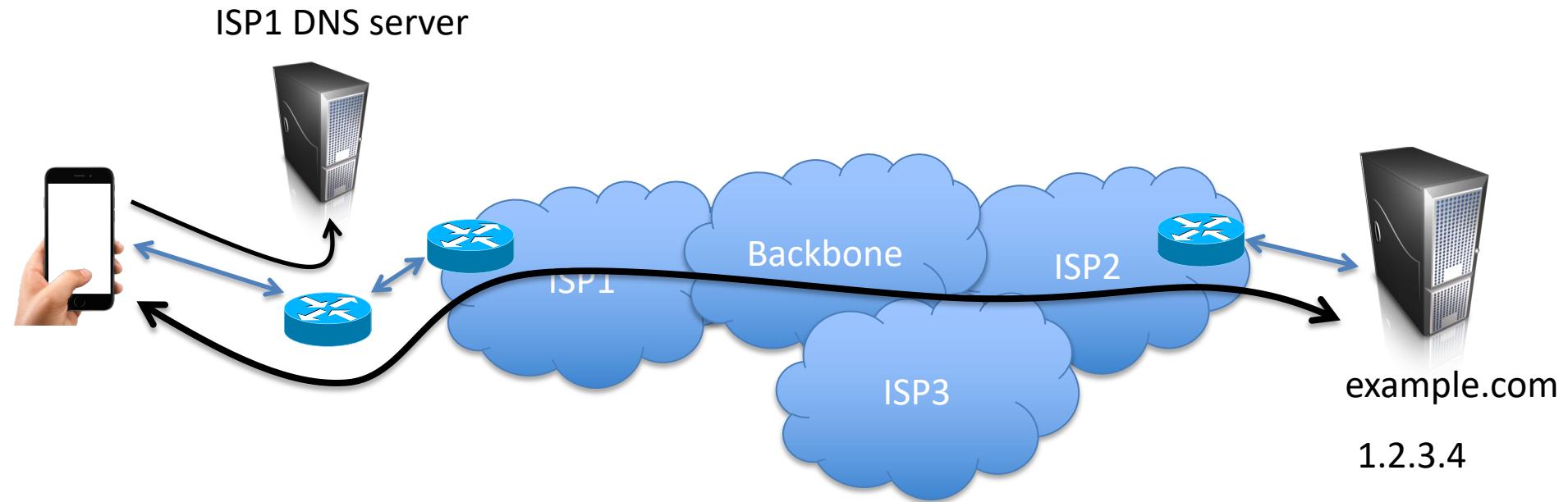
# The web runs on HTTP



# The web runs on HTTP

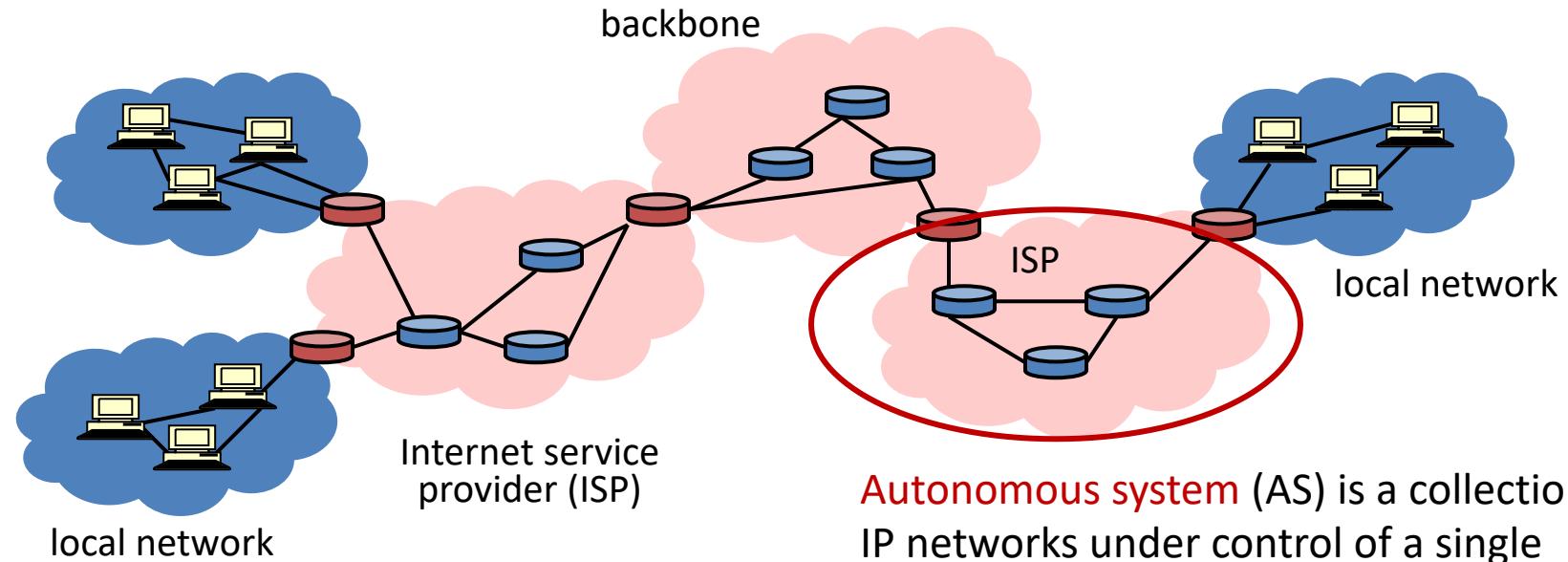


# Steps to send an HTTP request (pre HTTP/3)



1. DNS lookup on example.com to get IP address (1.2.3.4)
2. TCP connection setup via 4-way handshake of IP packets to and from 1.2.3.4
3. Send HTTP request over TCP connection

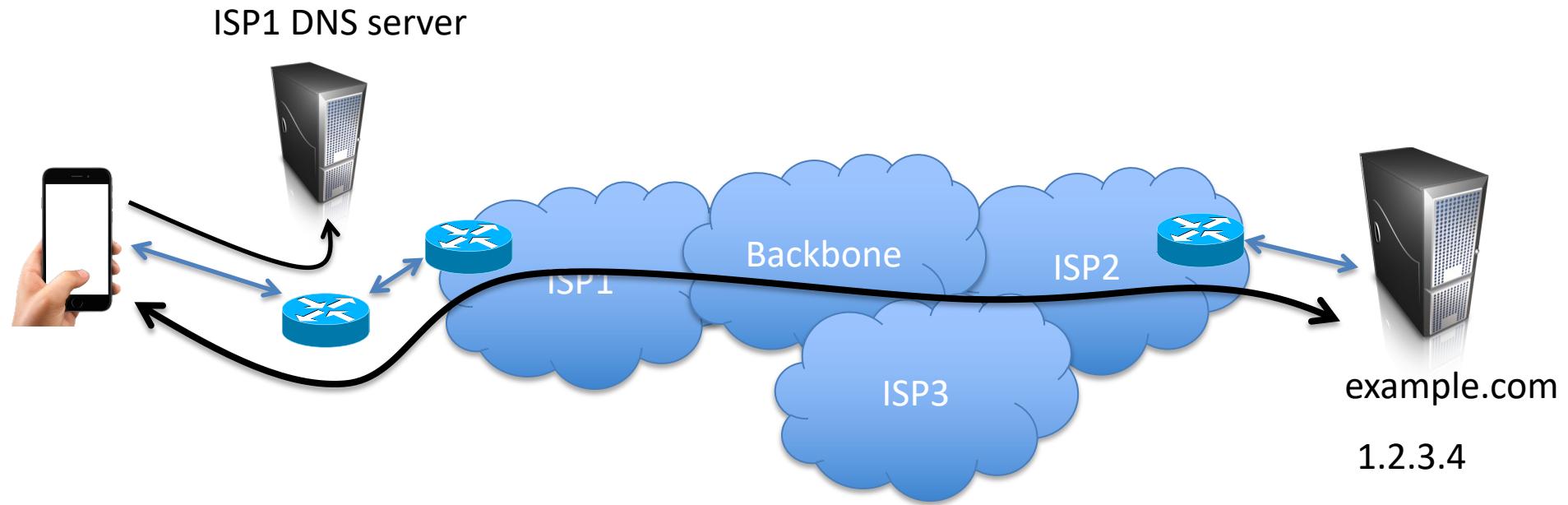
# Internet Is a Network of Networks



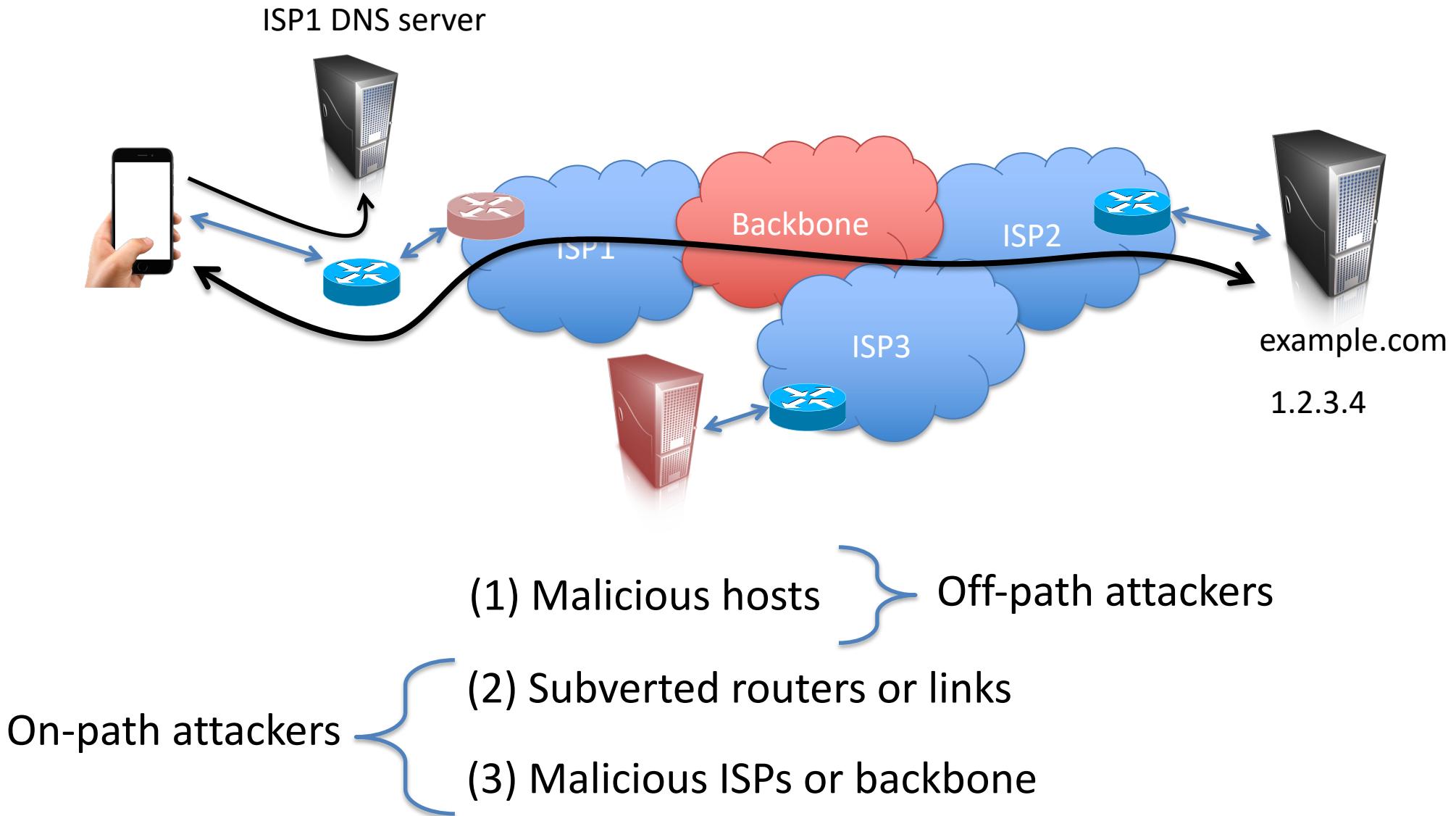
**Autonomous system (AS)** is a collection of IP networks under control of a single administrator (e.g., ISP)

- **TCP/IP** for packet routing and connections
- **Border Gateway Protocol (BGP)** for route discovery
- **Domain Name System (DNS)** for IP address discovery

# Network threat models



# Network threat models

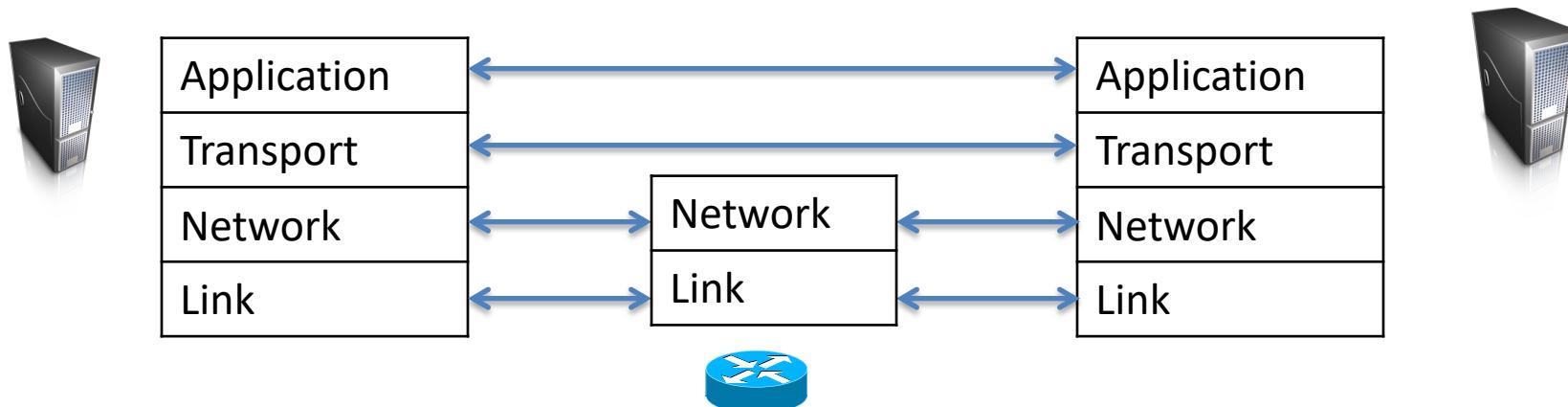


# Some attacks we'll cover

- BGP IP hijacking
- DNS cache poisoning
- IP spoofing
  - Simple untraceable DoS attacks
- Off-path TCP injection
  - Allows injecting traffic into other connections

# Internet protocol stack

Application	HTTP, DNS, FTP, SMTP, SSH, etc.
Transport	TCP, UDP
Network	IP, ICMP, ...
Link	802x (802.11, Ethernet)



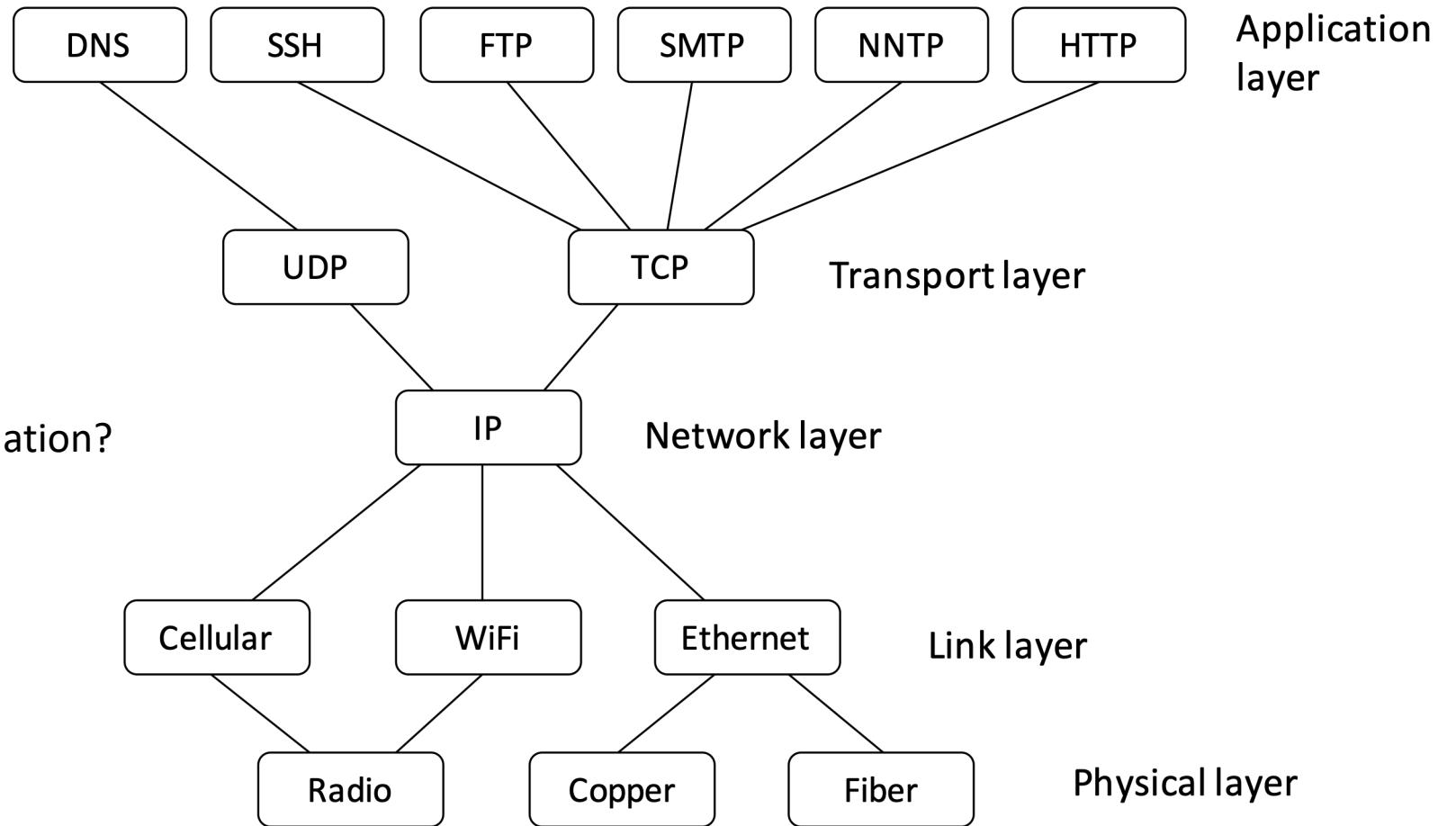
# IP: “The Narrow Waist”

How does application structure data?

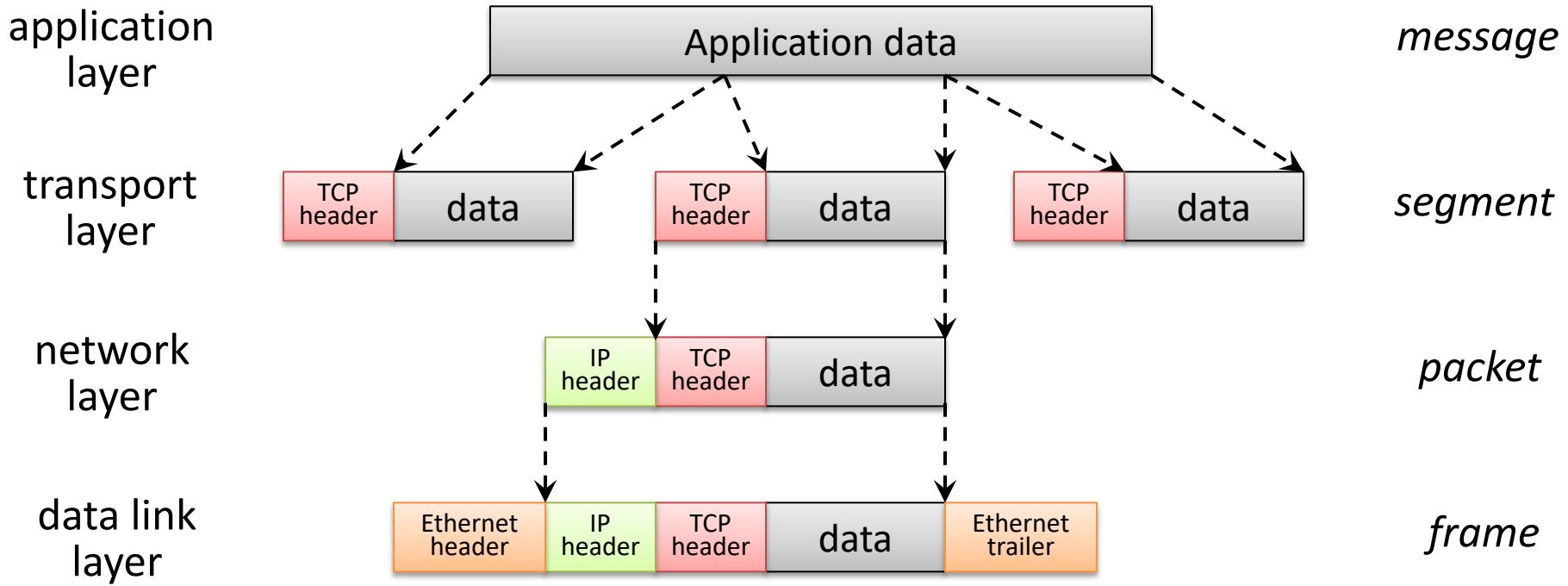
How to set up a communication stream or channel?

How does a packet reach final destination?

How does information get to next hop?



# Data Formats



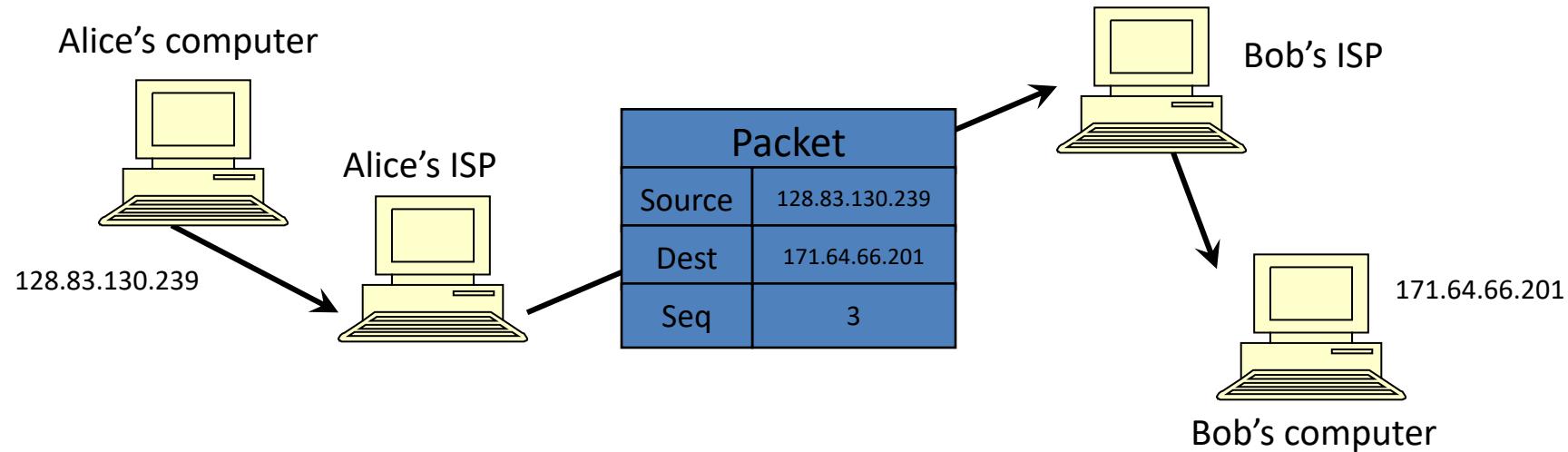
# IP (Internet Protocol)

## Connectionless

- Unreliable, “best-effort” protocol: no ordering, no retransmission, no error checking, no acknowledgement

Uses **numeric addresses** for routing

- Typically, several hops in the route



# IP Is Not Enough for Packet Delivery

Given an IP packet, how does the router  
know where to send it next?

*BGP*

On a local network, what MAC address  
corresponds to a given IP address?

*ARP*

# Global IPv4 Addresses

Globally unique

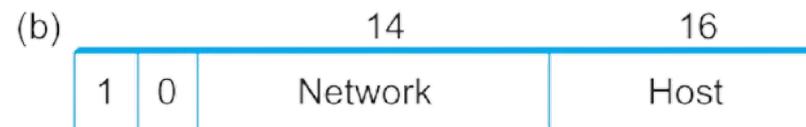
Hierarchical: network + host

Dot notation

- 10.3.2.4
- 128.96.33.81
- 192.12.69.77



Prefix of IP address identifies  
the network it belongs to



Class A network: owns all addresses with a given top byte

Class B network: ... top 2 bytes

Class C network: ... top 3 bytes

# Classless inter-domain routing (CIDR)

128.168.0.0/16

a.b.c.d / x

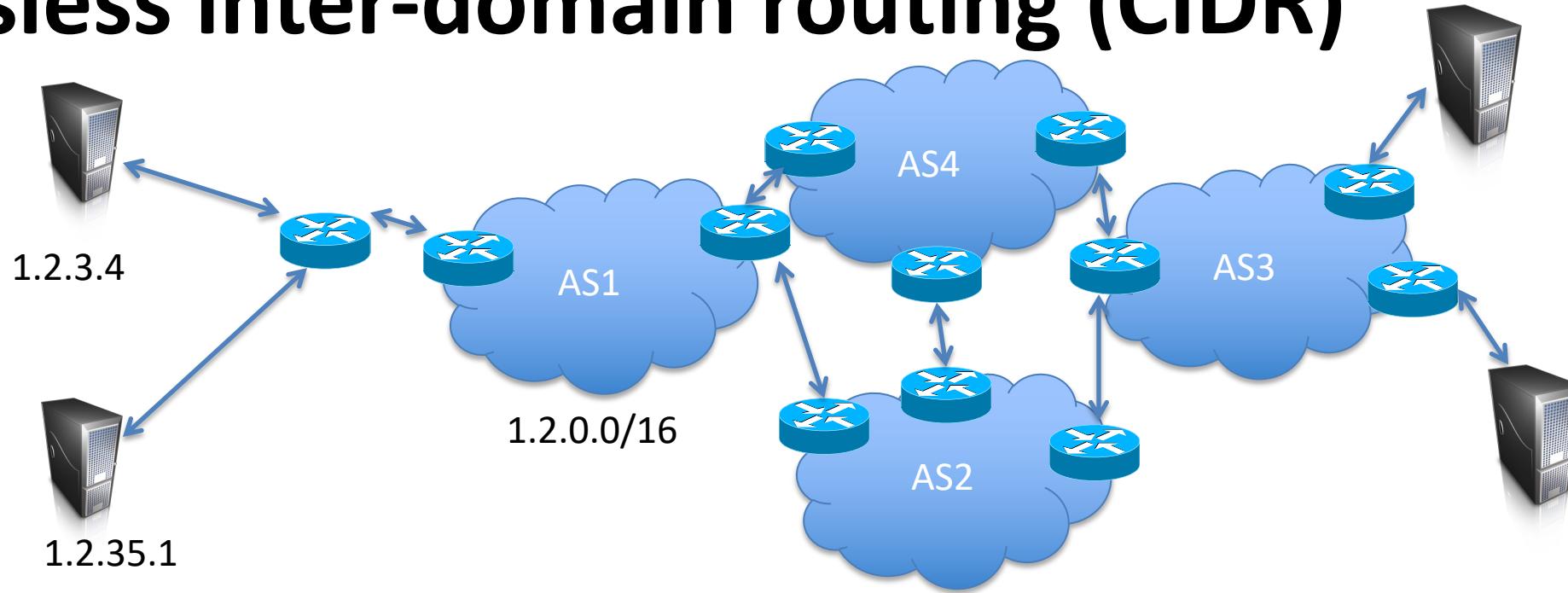
x indicates number of bits used for a routing prefix

IP addresses with same /x prefix share some portion of route

CIDR balances two objectives:

- (1) minimize the number of routes that a router needs to know
- (2) hand out addresses efficiently

# Classless inter-domain routing (CIDR)



Prefixes used to setup hierarchical routing

Autonomous systems (AS) assigned  $a.b.c.d/x$  manages addresses prefixed by  $a.b.c.d/x$

**Border gateway protocol (BGP)** used to *announce routes* between AS's

- Routers prefer more specific prefixes, shorter paths (+ AS-specific policies)
- AS gets update, recomputes routes, announces new paths to neighbors, etc.

~900,000+ routes on the internet in 2022 <https://blog.apnic.net/2023/01/06/bgp-in-2022-the-routing-table/>

# Overview of BGP

BGP is a **path-vector** protocol between ASes

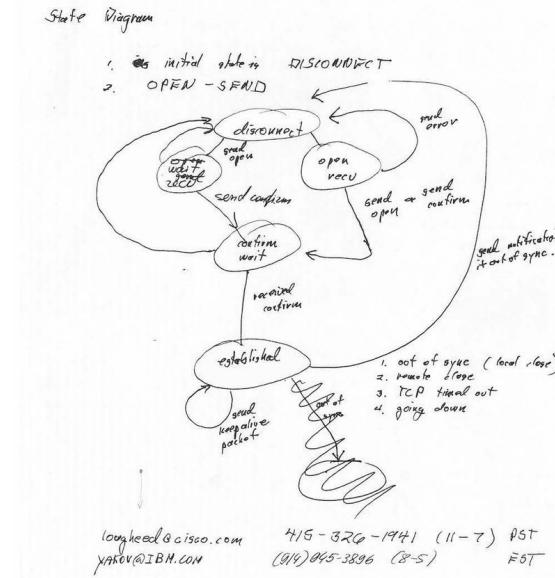
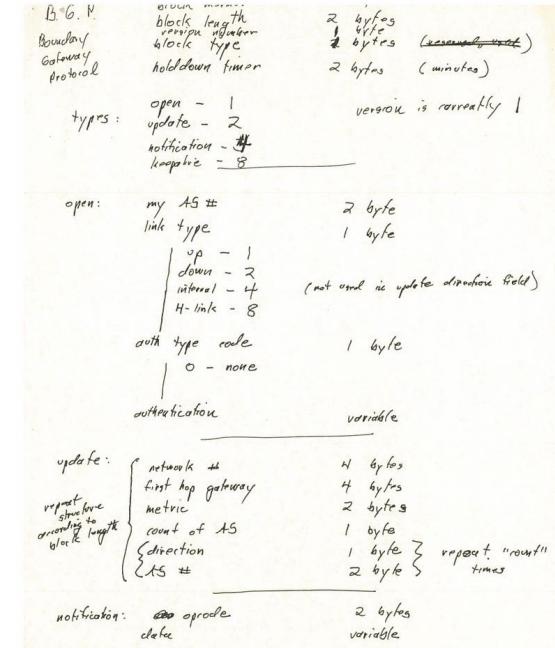
- Routing updates contain path to destination node
- Path: list of traversed ASes & set of network prefixes belonging to the first AS on the list

Each BGP router receives update messages from neighbors, selects one “best” path for each prefix, and advertises this path to its neighbors

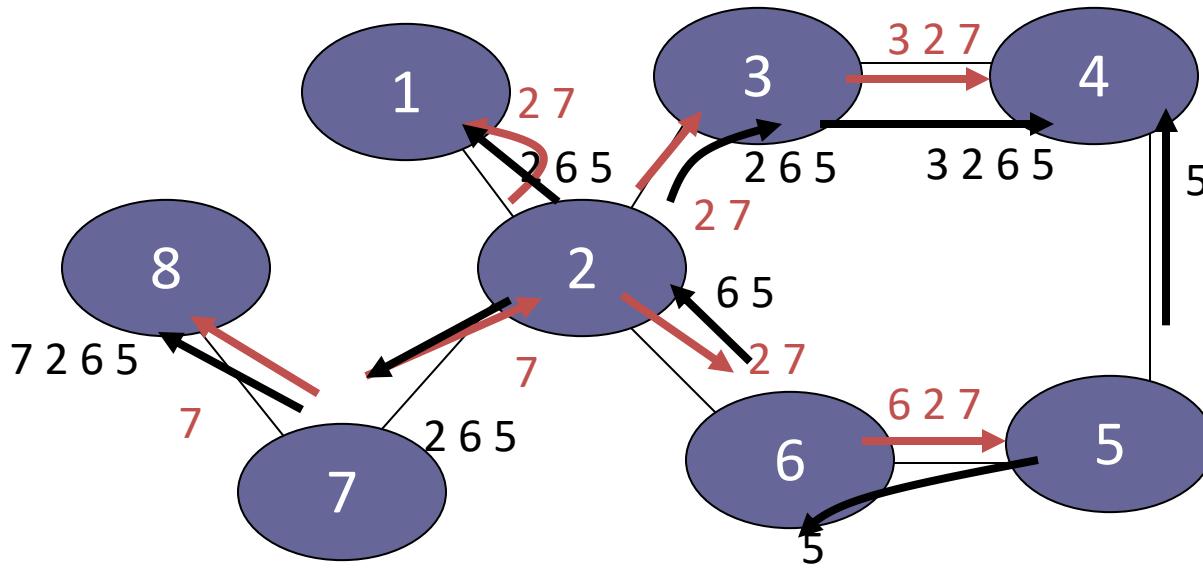
- Can be the shortest path, but doesn’t have to be
- Always route to the **most specific prefix** for a destination

Invented in 1989 at lunch by Kirk Lougheed, Yakov Rekhter

- “Two napkin protocol”



# BGP Example



AS 2 provides **transit** for AS 7

- Traffic to and from AS 7 travels through AS 2

# BGP had no security model

- BGP unauthenticated
  - Anyone can advertise any routes
  - False routes may be propagated to other AS's
- This allows ***IP hijacking***
  - AS announces it originates a prefix it shouldn't
  - AS announces it has shorter path to a prefix
  - AS announces more specific prefix

In-class 5-min exercise:

What attacks/problems can result from BGP insecurity?  
How would you prevent IP hijacking?

# BGP Incident:

**Summary:** Routing Leak briefly takes down Google

**Start:** 2015-03-12 08:58:00

**End:** Unknown

**Details:** This morning, users of Google around the world were unable to access many of the company's services due to a routing leak in India. Beginning at 08:58 UTC Indian broadband provider Hathway (AS17488) incorrectly announced over 300 Google prefixes to its Indian transit provider Bharti Airtel (AS9498). Bharti in turn announced these routes to the rest of the world, and a number of ISPs accepted these routes including US carriers Cogent (AS174), Level 3 (AS3549) as well as overseas incumbent carriers Orange (France Telecom, AS5511), Singapore Telecom (Singtel, AS7473) and Pakistan Telecom (PTCL, AS17557). Like many

# More incidents

- 1997: AS 7007 incident
  - Announced specific routes for most of IPv4 address space, took down much of Internet
  - “Okay, so panic ensued, and we unplugged \*everything\* at 12:15PM almost to the second.” [sic]
  - <http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html>
- 2008 Pakistan attempts to block Youtube
  - youtube is 208.65.152.0/22 , youtube.com = 208.65.153.238
  - Pakistan ISP advertises 208.65.153.0/24 (more specific, prefix hijacking)
  - Internet thinks youtube.com is in Pakistan ... outage resolved in 2 hours...
- 2018: BGP leak/hijack of AWS Route53 DNS servers
  - Used to serve up IP addresses for (only) myetherwallet.com
  - The served IP addresses went to Russian AS

# Facebook Outage in 2021

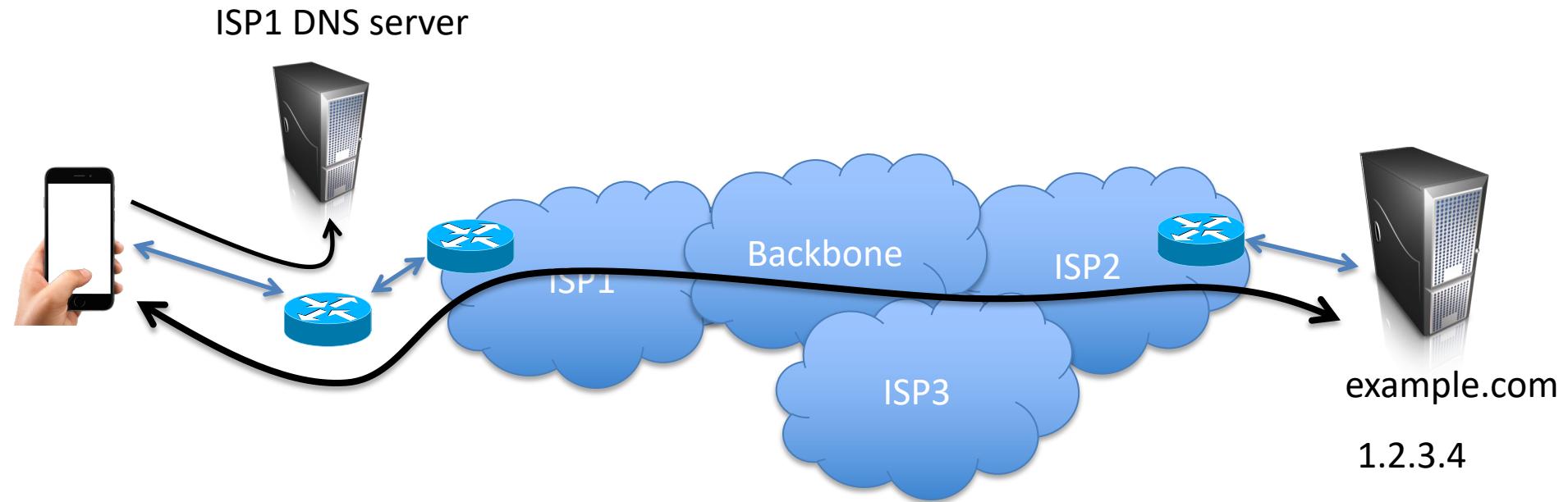


<https://krebsonsecurity.com/2021/10/what-happened-to-facebook-instagram-whatsapp/>

# BGP security efforts

- Advertisement filtering
  - Rules that AS's use to filter out bad requests
  - E.g.: only accept an advertisement for IP address owned by advertising AS
- Cryptographic efforts:
  - Resource Public Key Infrastructure (RPKI)
    - Digitally sign advertisements to bind it to valid AS
    - <https://blog.cloudflare.com/rpki/>
  - BGPsec (cryptographic validation of AS paths)
  - Both still only partially deployed

# Steps to send an HTTP request (pre HTTP/3)



1. DNS lookup on example.com to get IP address (1.2.3.4)
2. TCP connection setup via 4-way handshake of IP packets to and from 1.2.3.4
3. Send HTTP request over TCP connection

# Domain Name System (DNS)

We don't want to have to remember IP addresses

DNS solves this:  
What is IP address for myetherwallet.com?

IP address in answer section

Information on ***name servers*** that are authoritative for domain

```
Tue Oct 01 21:53:37:website$ dig myetherwallet.com

; <>> DiG 9.10.6 <>> myetherwallet.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59696
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5

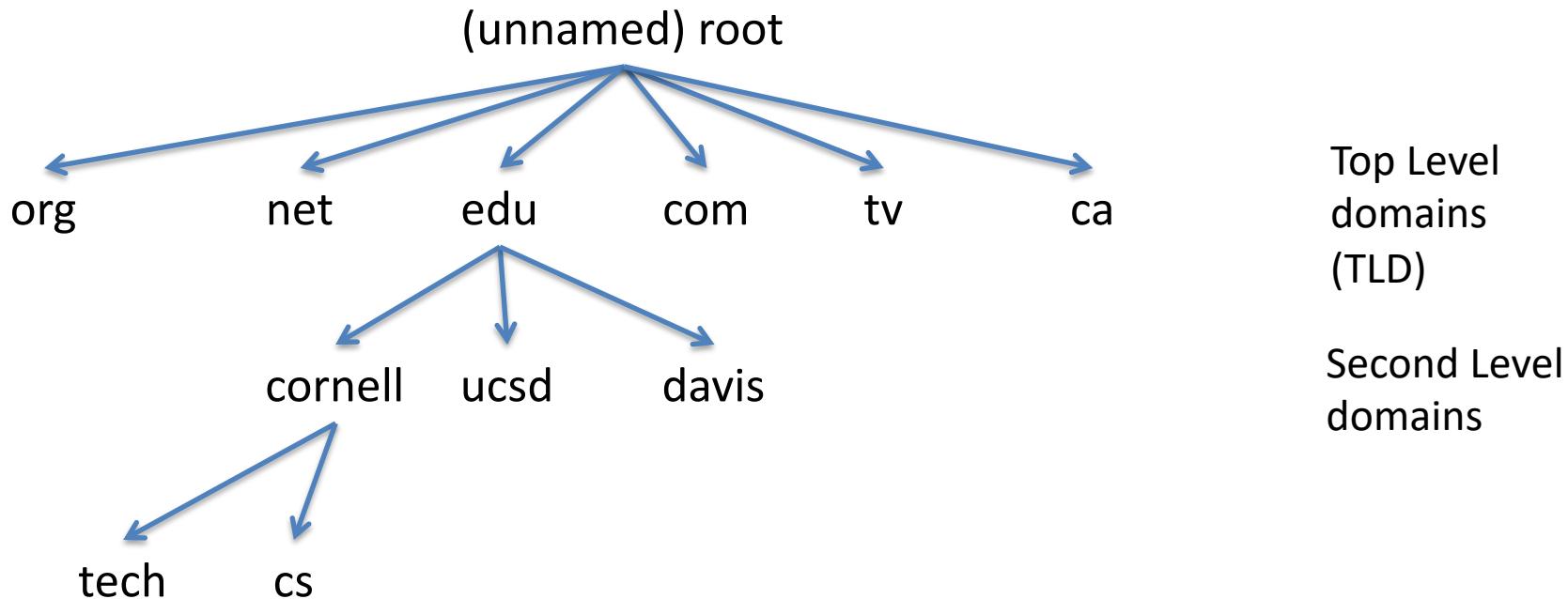
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;myetherwallet.com.           IN      A

;; ANSWER SECTION:
myetherwallet.com.    300    IN      A      104.18.201.107
myetherwallet.com.    300    IN      A      104.18.202.107

;; AUTHORITY SECTION:
myetherwallet.com.    141990  IN      NS      ali.ns.cloudflare.com.
myetherwallet.com.    141990  IN      NS      ivan.ns.cloudflare.com.

;; ADDITIONAL SECTION:
ali.ns.cloudflare.com. 42241   IN      A      173.245.58.59
ivan.ns.cloudflare.com. 52319   IN      A      173.245.59.120
ali.ns.cloudflare.com. 42241   IN      AAAA   2400:cb00:2049:1::adf5:3a3b
ivan.ns.cloudflare.com. 102167  IN      AAAA   2400:cb00:2049:1::adf5:3b78
```

# Heirarchical domain name space



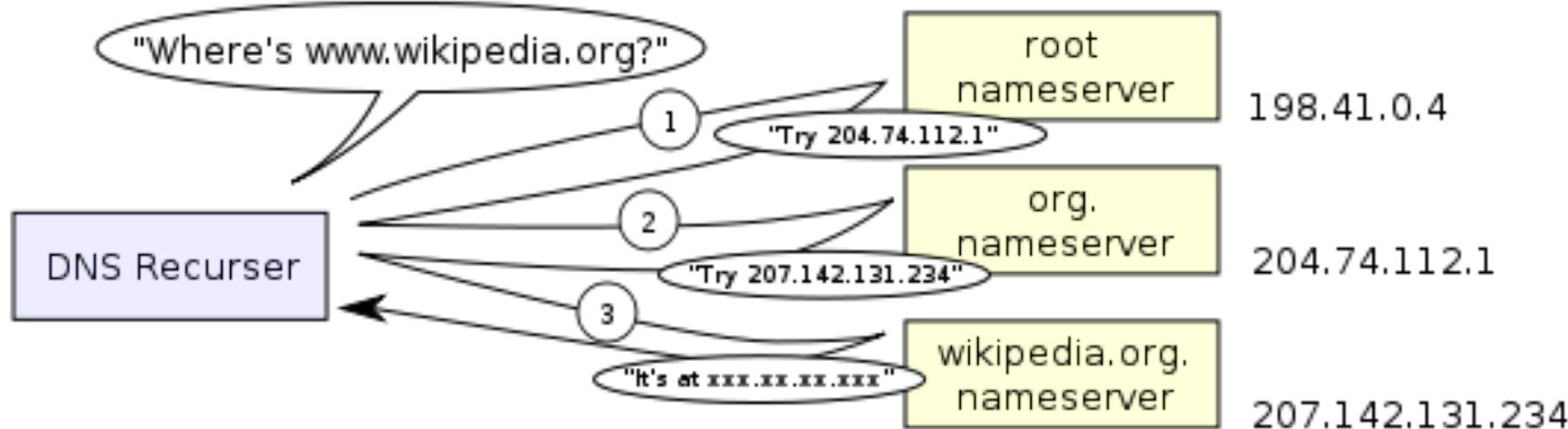
max 63  
characters

ICANN (Internet Corporation for Assigned Names and Numbers)

root nameservers and authoritative nameservers

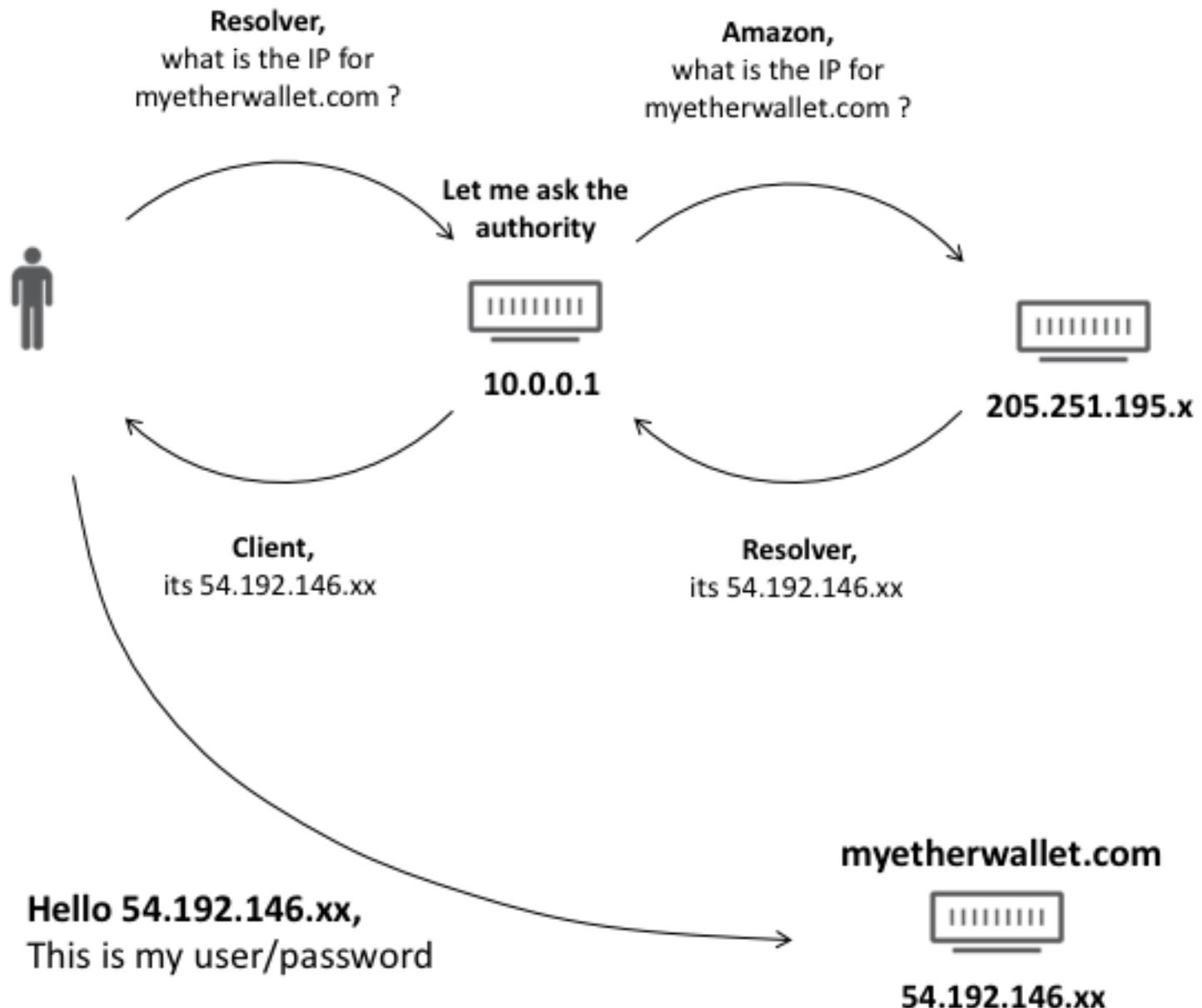
Zone: subtree

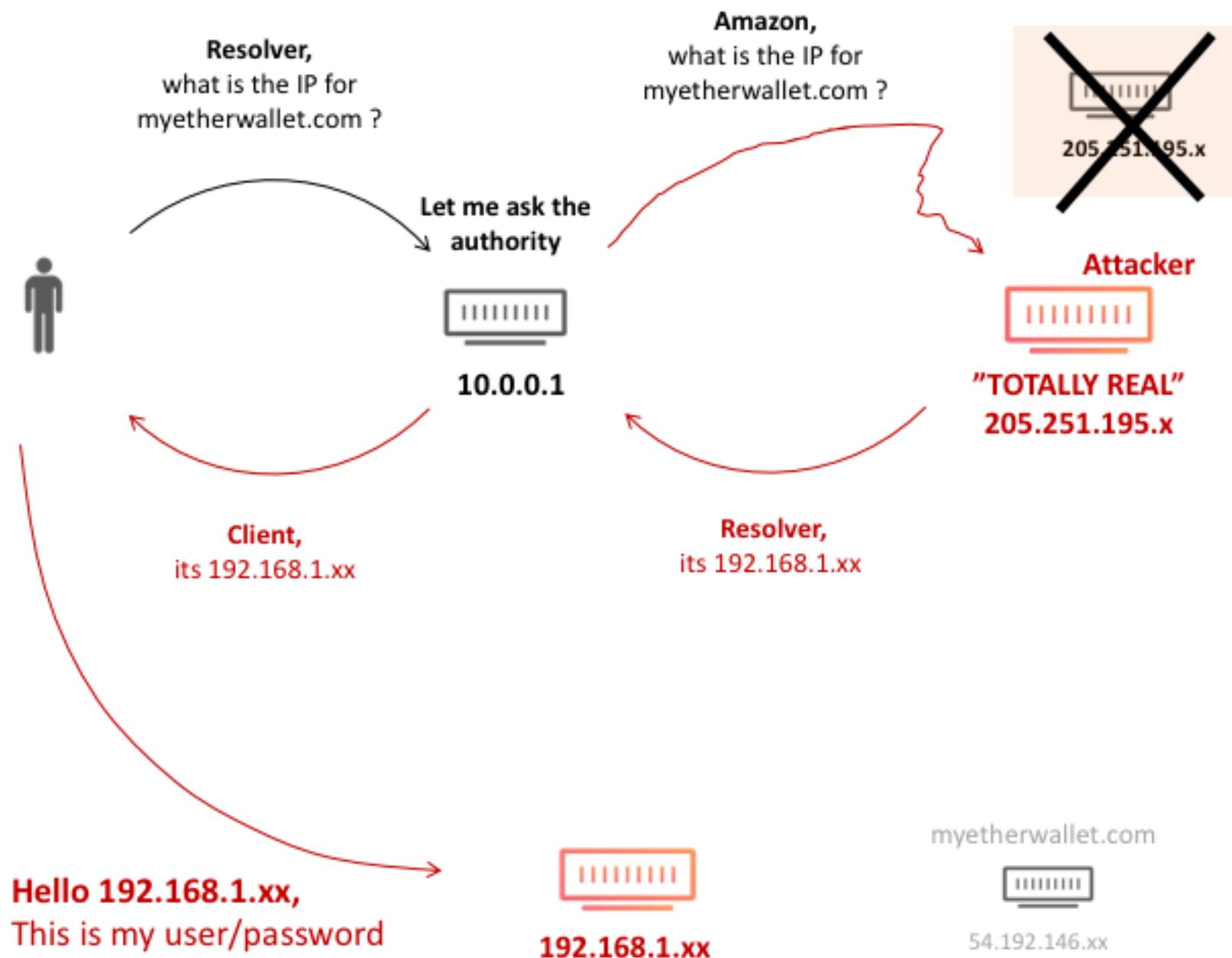
# Resolving names



From

[http://en.wikipedia.org/wiki/File:An\\_example\\_of\\_theoretical\\_DNS\\_recursion.svg](http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg)

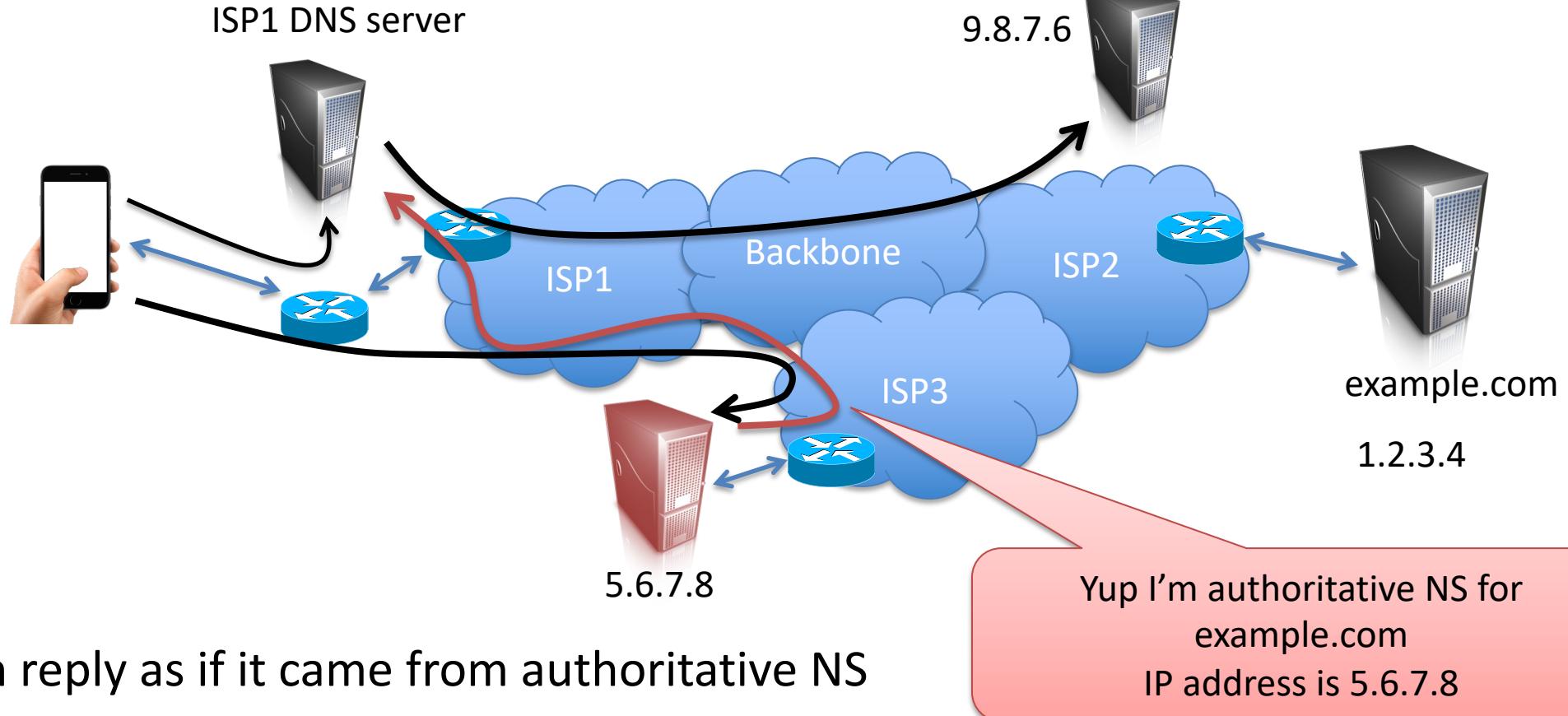




# Other attacks against DNS

- DNS is plaintext protocol without authentication
  - What can on-path adversaries do?
- DNS cache poisoning by off-path adversaries
  - Flaw in DNS protocol that allows inserting records
- DNS typo-squatting
- Compromise DNS admin accounts, edit records

# DNS poisoning



# DNS protocol

DNS uses User Datagram Protocol (UDP)

- Connectionless transport protocol
- Port is used to distinguish different network end points on same system
- Port 53 is standard dst. port for DNS

Normally:

Request = one UDP datagram

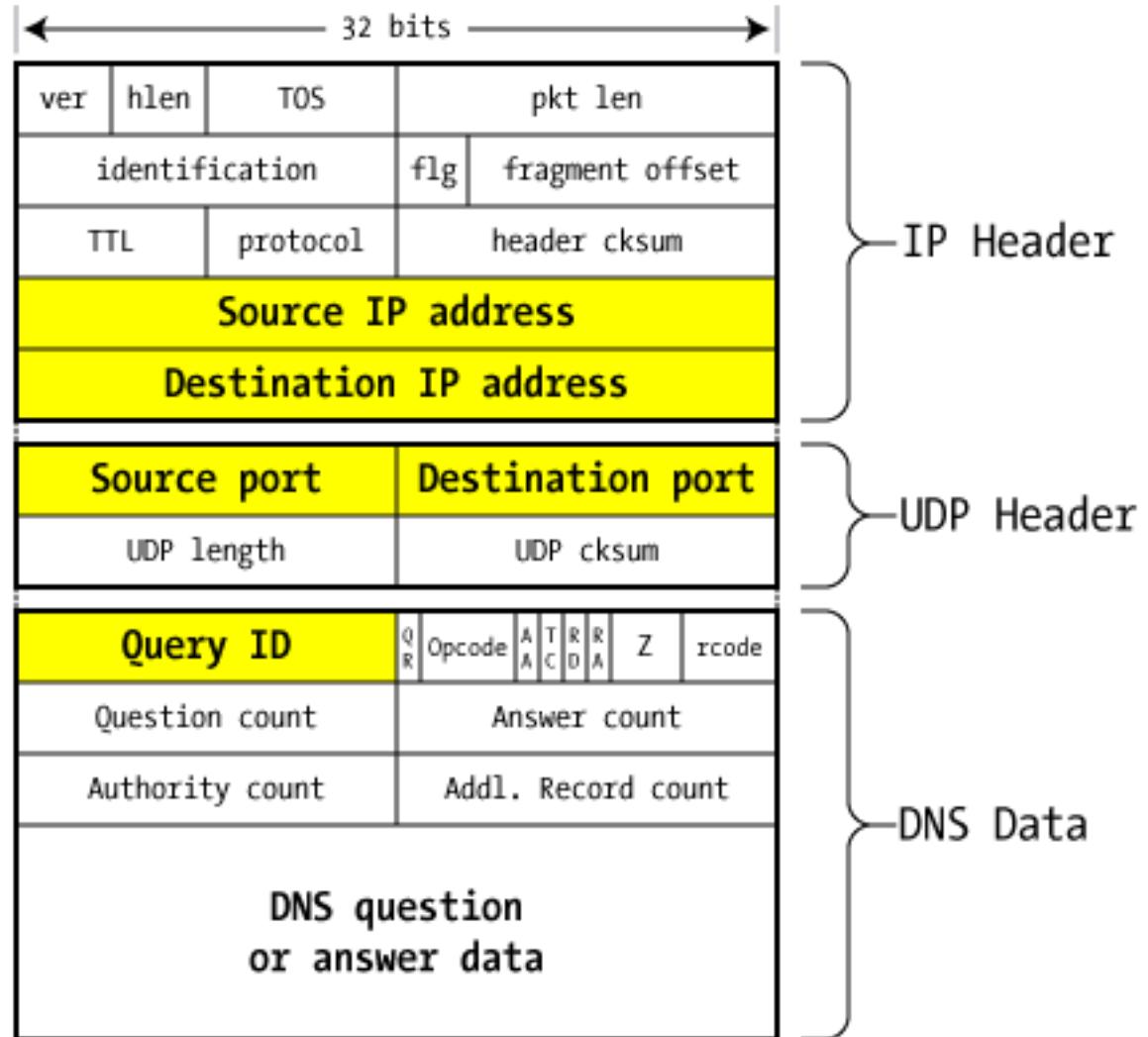
Response = one UDP datagram

DNS:

Query ID is 16-bit number

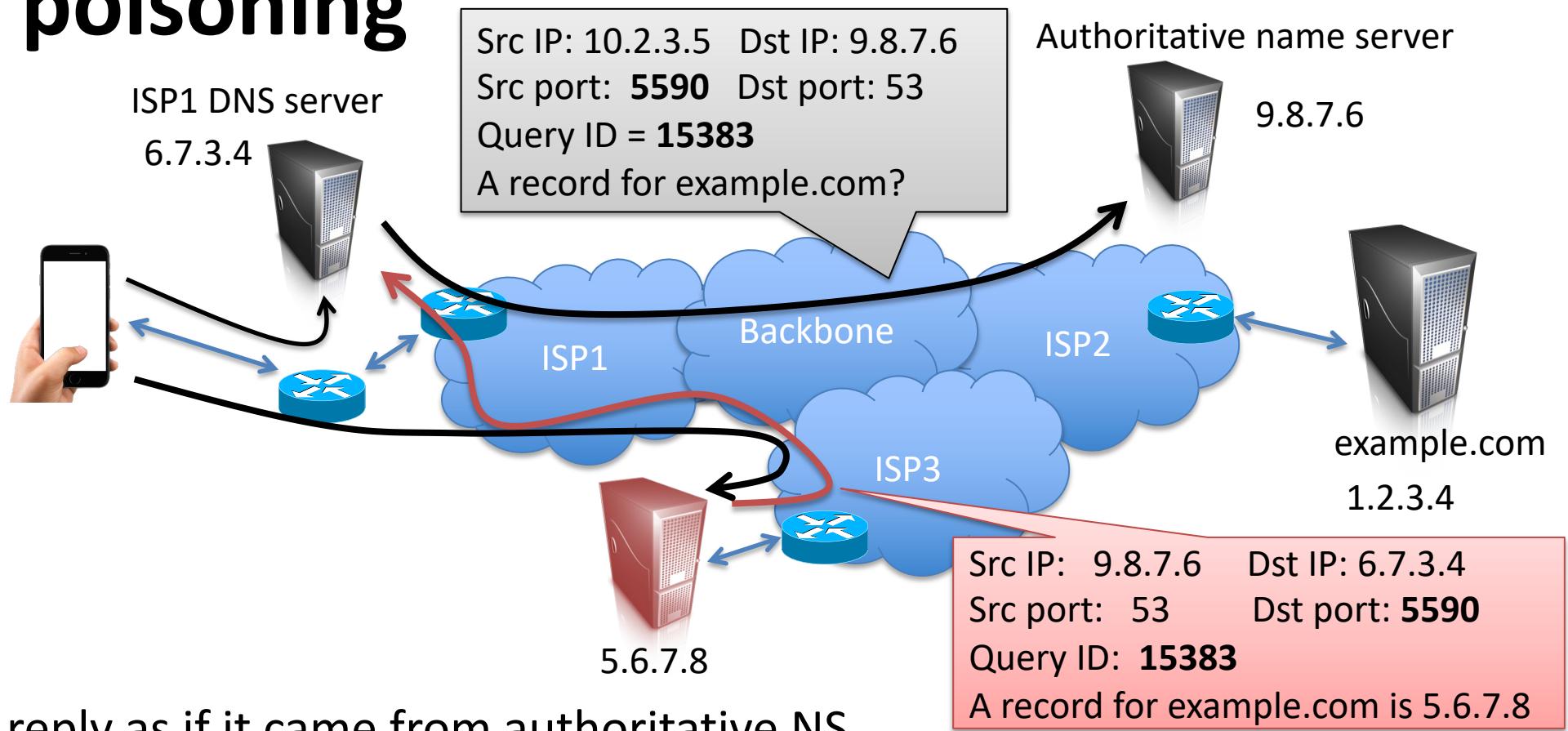
Response must include same query ID

Response must be to src port of request



<http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

# DNS poisoning



## Goal:

Sneak in reply as if it came from authoritative NS

## Requires:

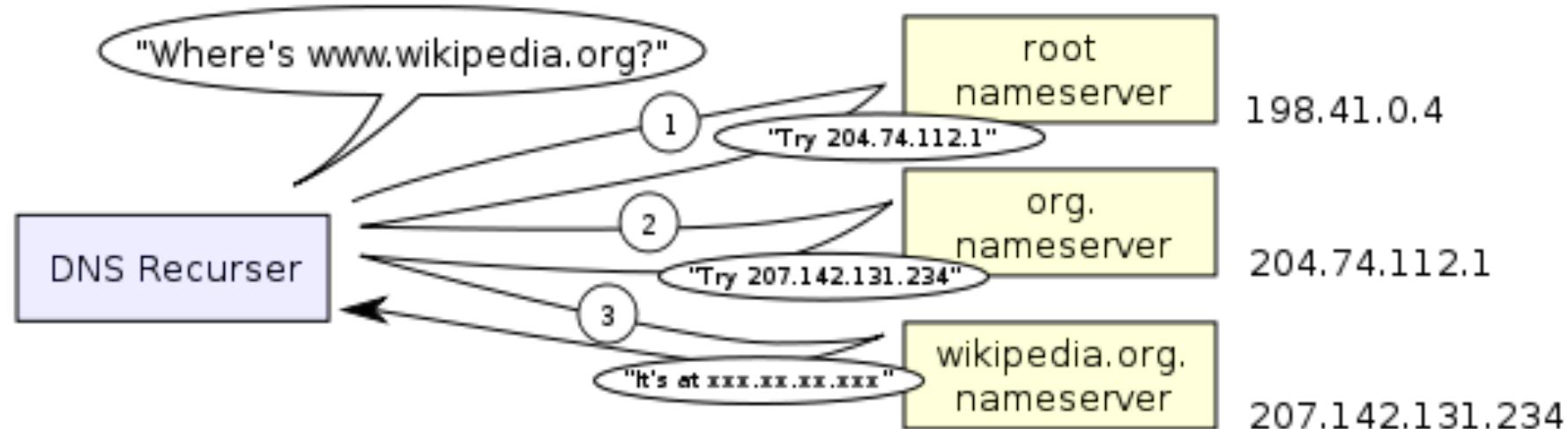
- Spoofing the src IP address of name server
- Guessing query ID, knowing source port of request
- Getting timing right

If deterministic (e.g., counters)  
can be predicted

Just random query IDs can be  
defeated ( $2^{16}$  space too small)

# More advanced DNS cache poisoning

- Target NS response to trick ISP1 resolver into thinking malicious server is authoritative NS
- Can do many attempts by forcing DNS requests to ISP1 that trigger fresh requests for step 3 below



# DNS cache poisoning defenses

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
  - Doubles the space
- Randomize UDP ports
- DNSsec
  - Cryptographically sign DNS responses, verify via chain of trust from roots on down
- DNS-over-HTTPS
  - Send DNS requests over encrypted, authenticated channel to NS's

A MORE SECURE WEB —

# Why big ISPs aren't happy about Google's plans for encrypted DNS

DNS over HTTPS will make it harder for ISPs to monitor or modify DNS queries.

TIMOTHY B. LEE - 9/30/2019, 6:57 PM

<https://arstechnica.com/tech-policy/2019/09/isps-worry-a-new-chrome-feature-will-stop-them-from-spying-on-you/>

# Some attacks we'll cover

- BGP IP hijacking
- DNS cache poisoning
- IP spoofing
  - Simple untraceable DoS attacks
- Off-path TCP injection
  - Allows injecting traffic into other connections