

CS 772/872: Advanced Computer and Network Security

Fall 2022

Course Link:

<https://shhaos.github.io/courses/CS872/netsec-fall2022.html>

Instructor: Shuai Hao

shao@odu.edu

www.cs.odu.edu/~haos



OLD DOMINION
UNIVERSITY

CS 772/872: Advanced Computer and Network Security

- Network Security
- Web Security
- Cloud Security
- System Security



Network Security

- TCP/IP
- (D)DoS Attacks
- DNS
- BGP
- CDN
- Applied Cryptography
- PKI
- SSL/TLS and HTTPS
- DNSSEC/RPKI



Network Security

- **Confidentiality:** only sender, intended receiver should “understand” message contents
 - sender encrypts message
 - receiver decrypts message
- **Integrity:** sender, receiver want to ensure message not altered (in transit, or afterwards)
- **Authentication:** sender, receiver want to confirm identity of each other

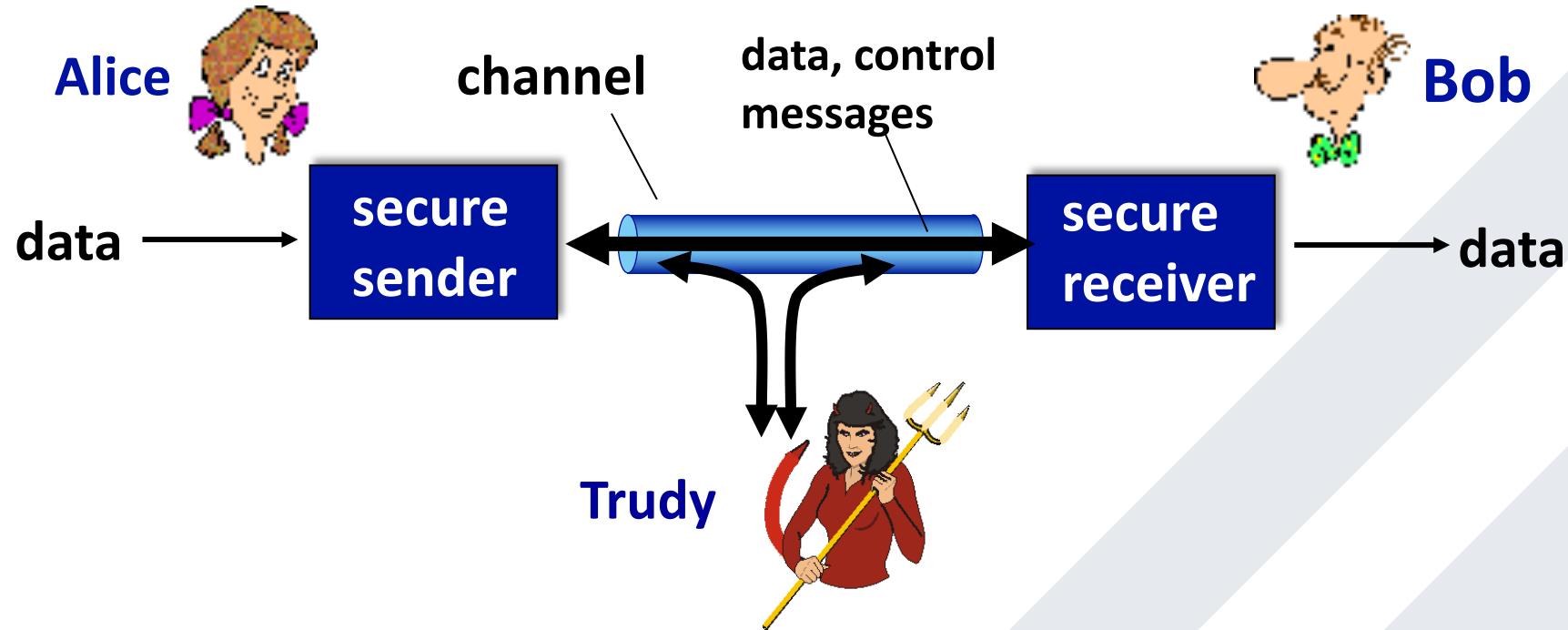


Network Security

- **Confidentiality:** only sender, intended receiver should “understand” message contents
 - sender encrypts message
 - receiver decrypts message
- **Integrity:** sender, receiver want to ensure message not altered (in transit, or afterwards)
- **Authentication:** sender, receiver want to confirm identity of each other
- **Accessibility and Availability:** services must be accessible and available to users

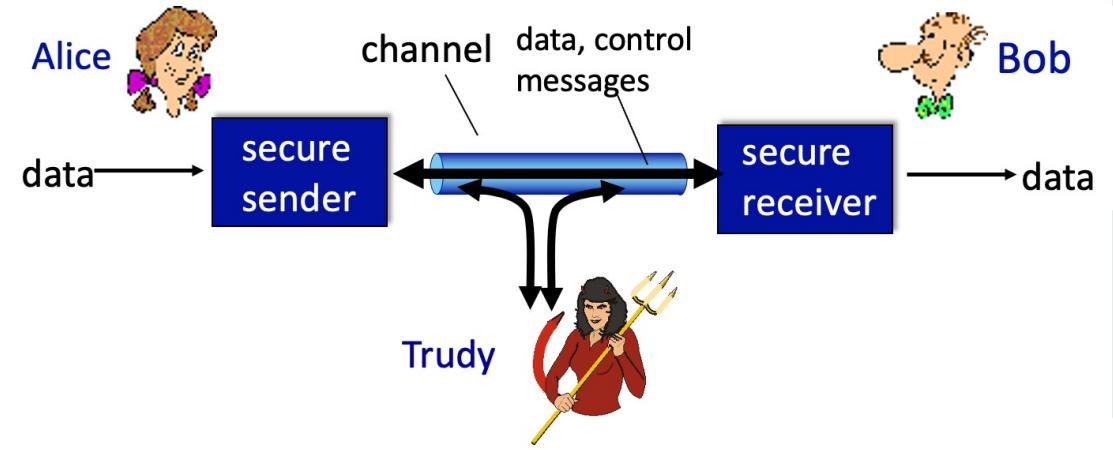


Network Security



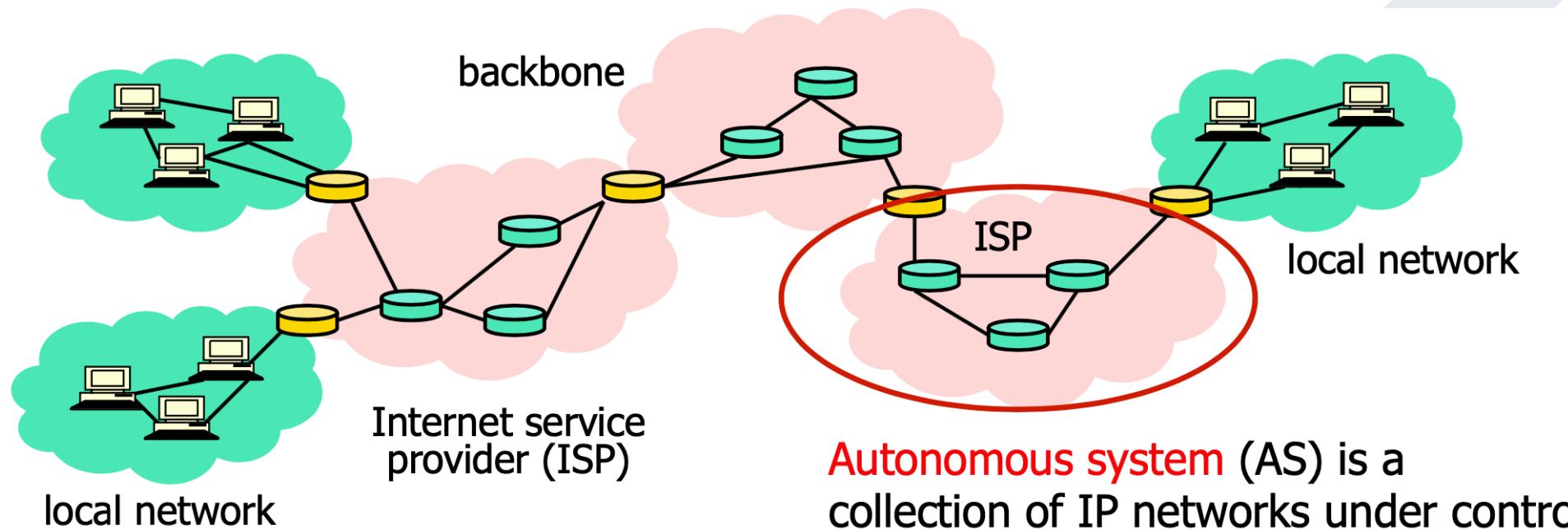
Network Security

- **Eavesdrop:** Intercept messages
- **Impersonation:** fake/spoof source address of packets
- **Hijacking:** “take over” ongoing connection by inserting himself in place
- **Denial of service:** prevent service from being used by others



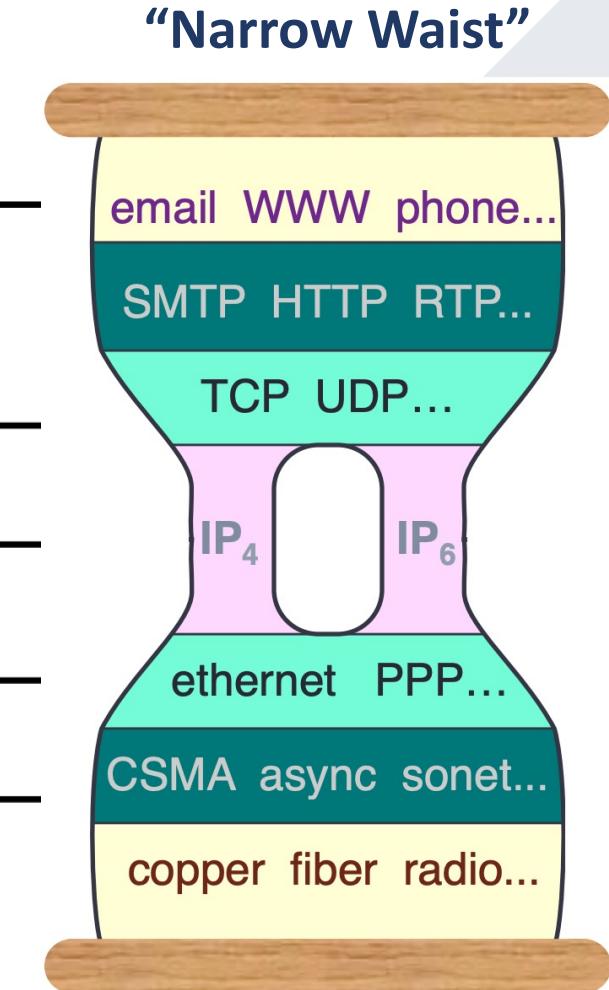
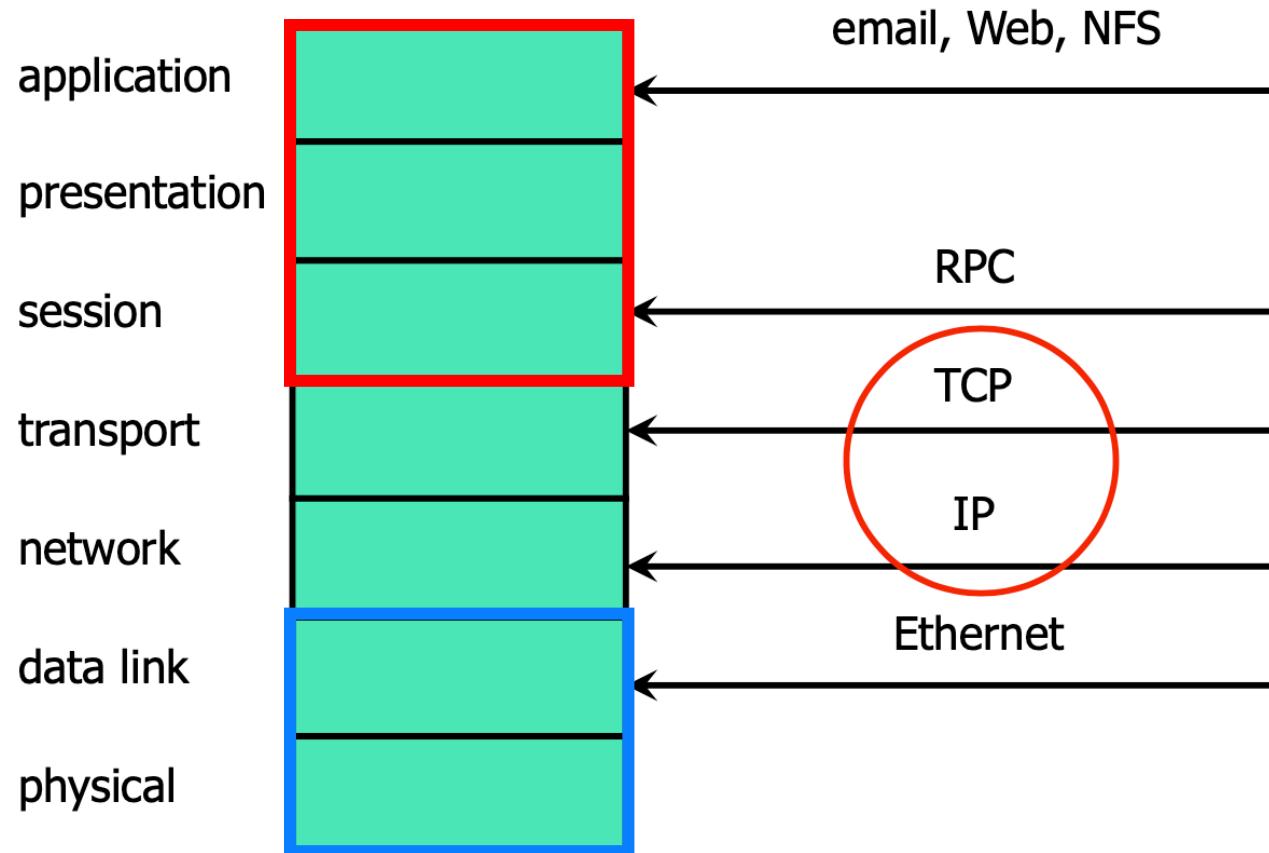
Network Security

- Internet: a Network of Network



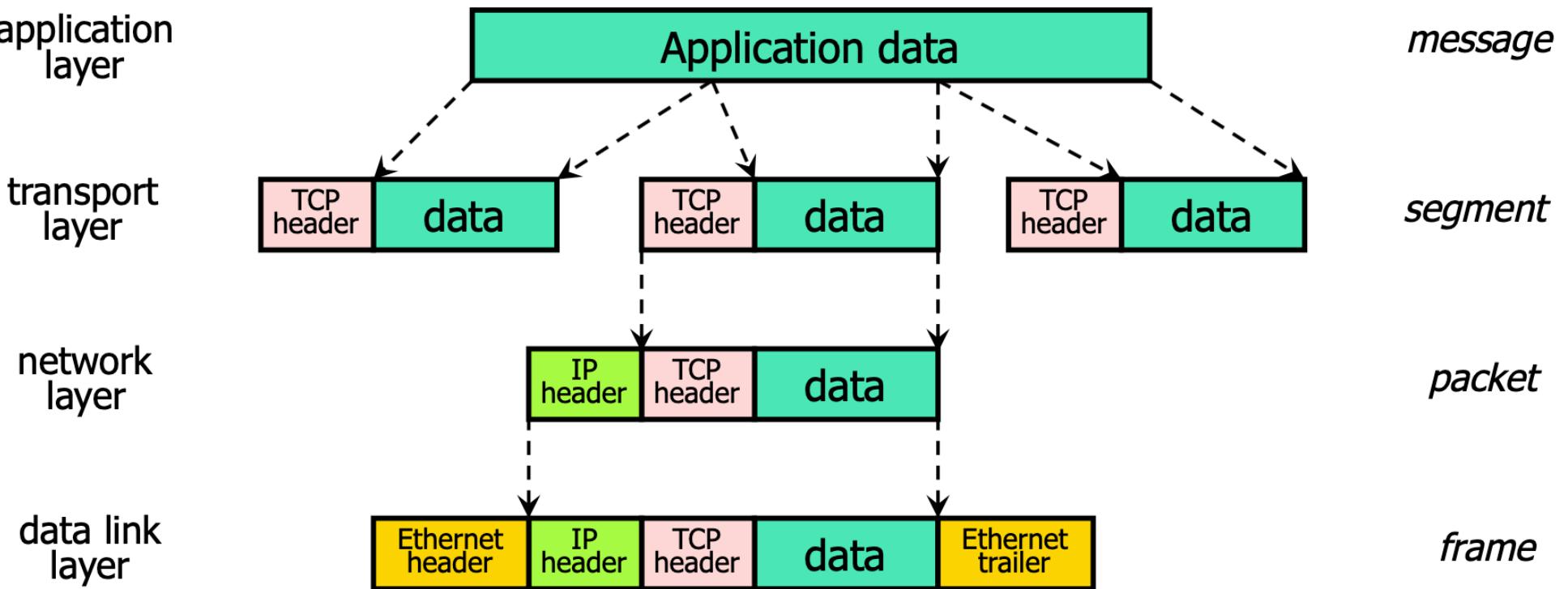
Network Security

- OSI Protocol Stack



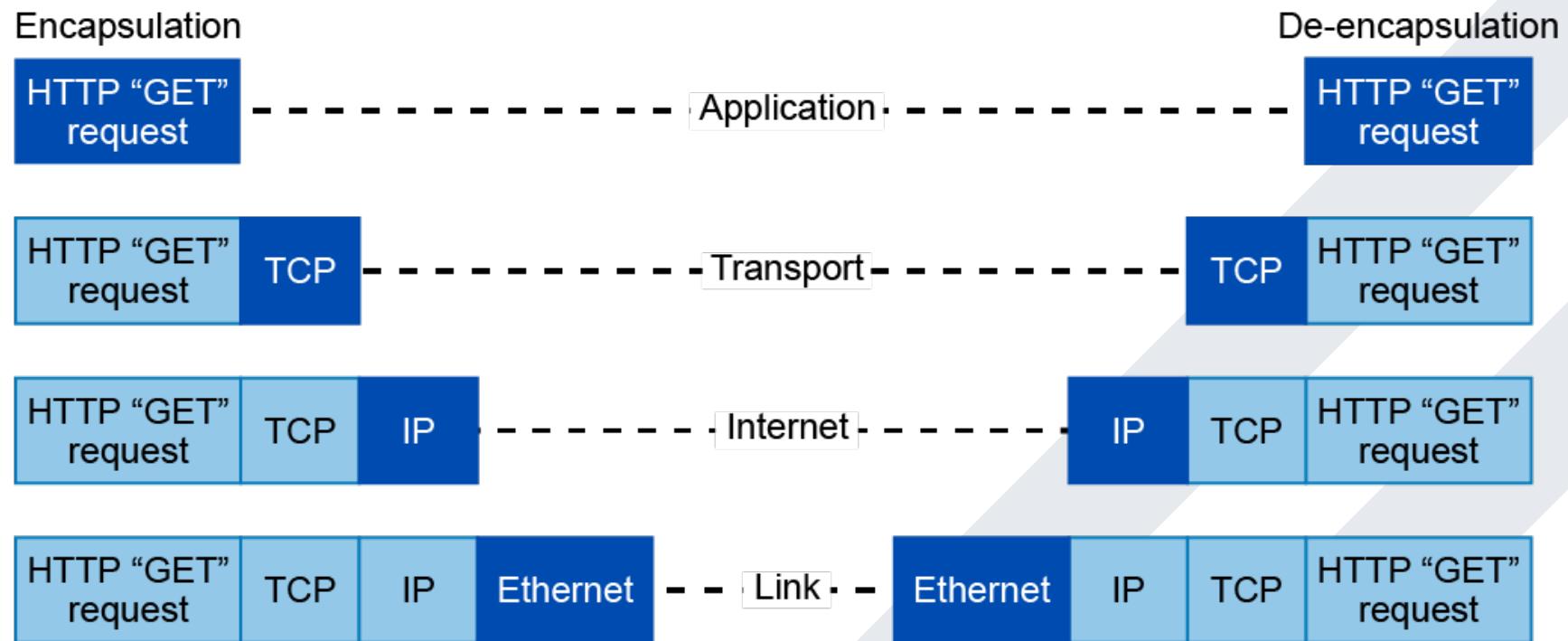
Network Security

- Encapsulation



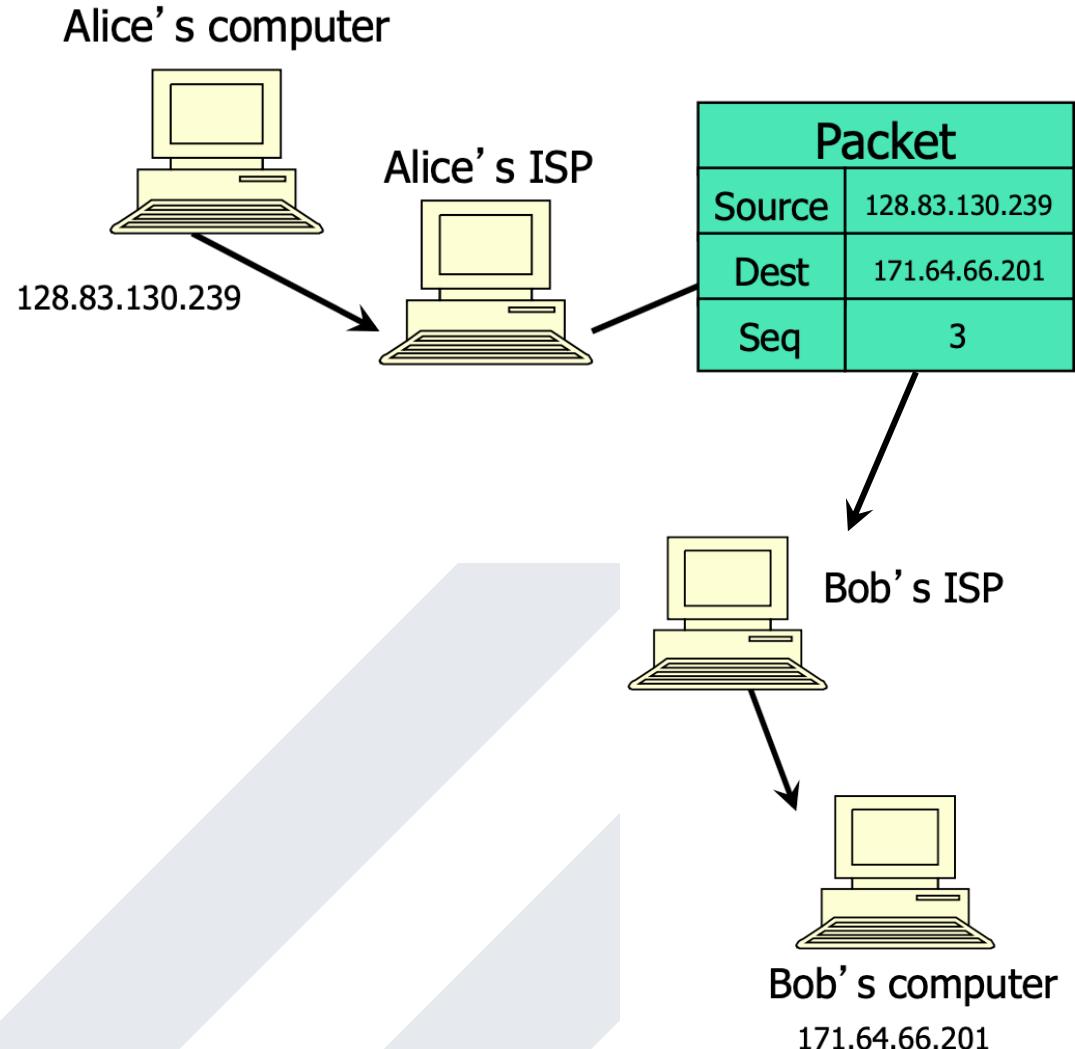
Network Security

- Encapsulation



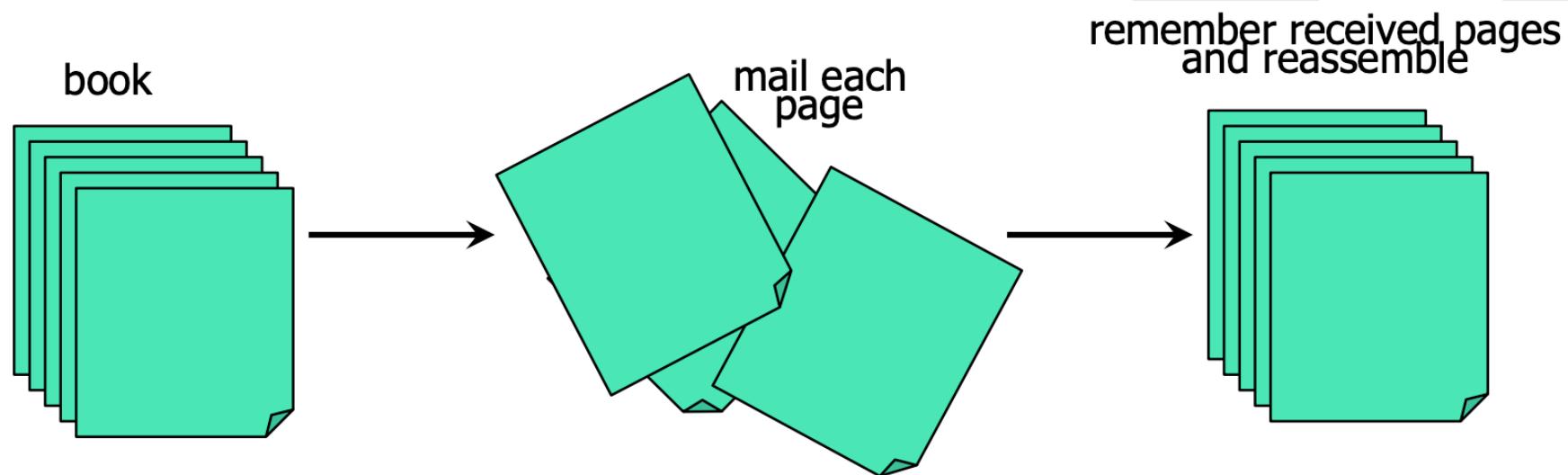
IP – Internet Protocol

- **Connectionless**
 - Unreliable, “best-effort” protocol
- **Destination-based Routing**



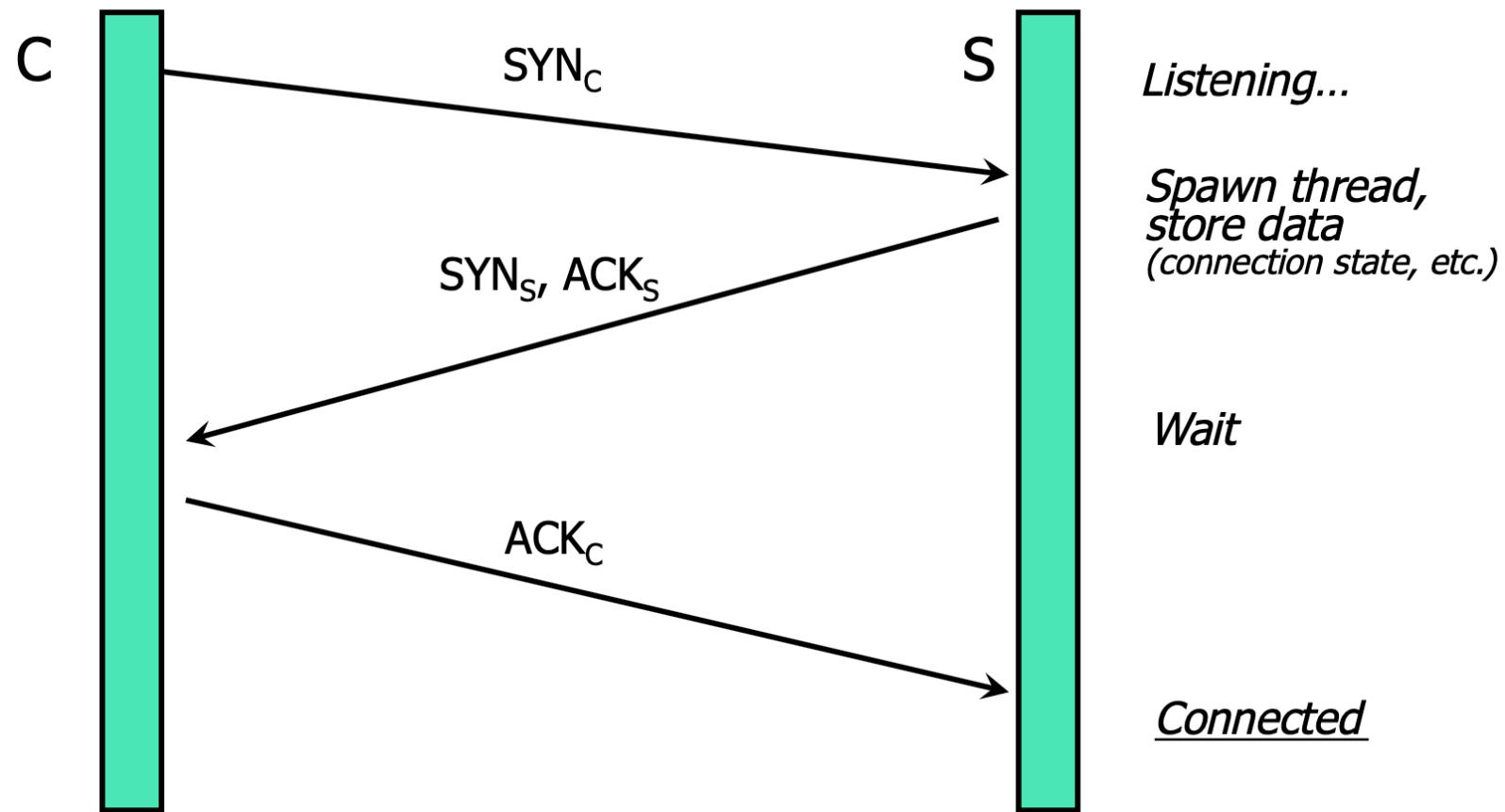
TCP – Transmission Control Protocol

- **Sender: break data into segments**
 - Sequence number is assigned to every segment
- **Receiver: reassemble segments in correct order**
 - Acknowledge receipt; lost segments will be re-sent
- **Connection state maintained on both sides**



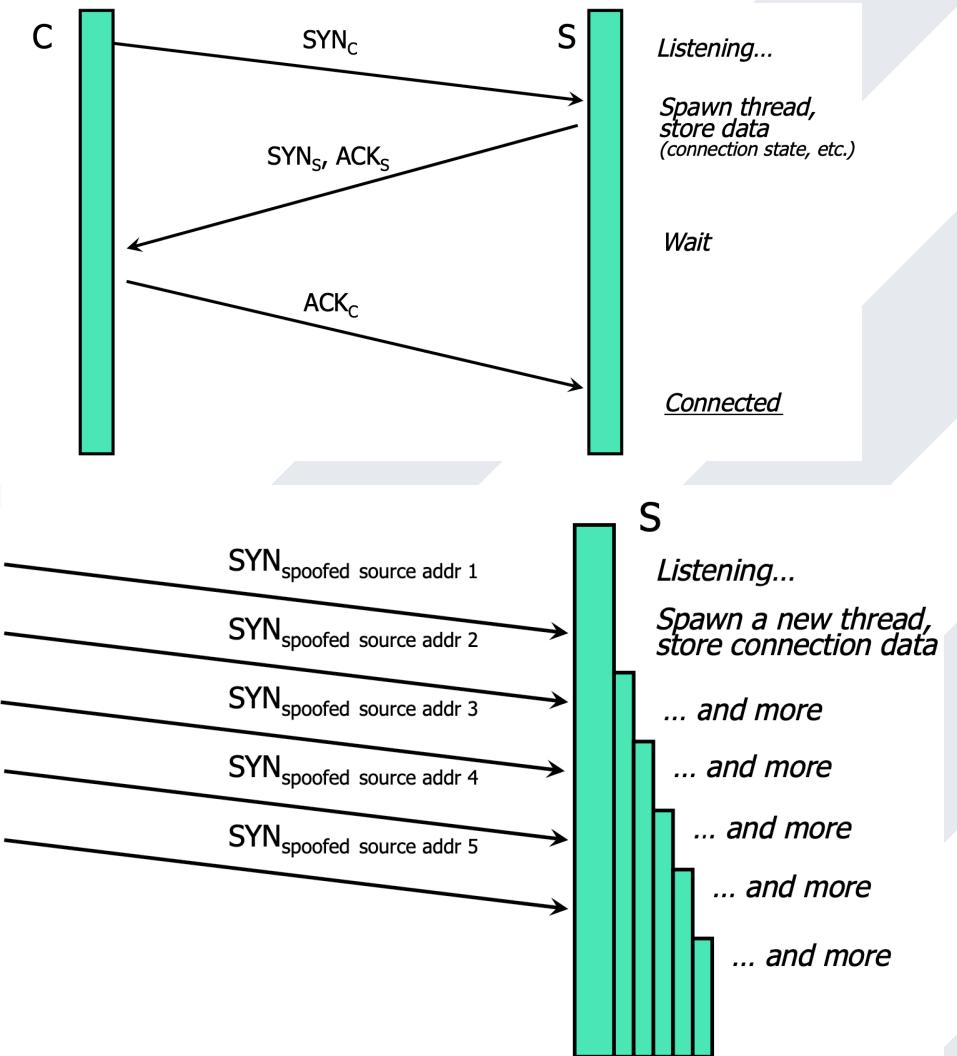
TCP – Transmission Control Protocol

- TCP Handshake



TCP – Transmission Control Protocol

- **SYN Flooding Attack**
 - Attacker sends many connection requests with spoofed source address
 - Victim allocates resources for each request
 - New thread
 - “half-open” connections
 - Once resources exhausted, legitimate requests are dropped
 - **Classic (Distributed-)Denial-of-Service (DDoS) pattern**



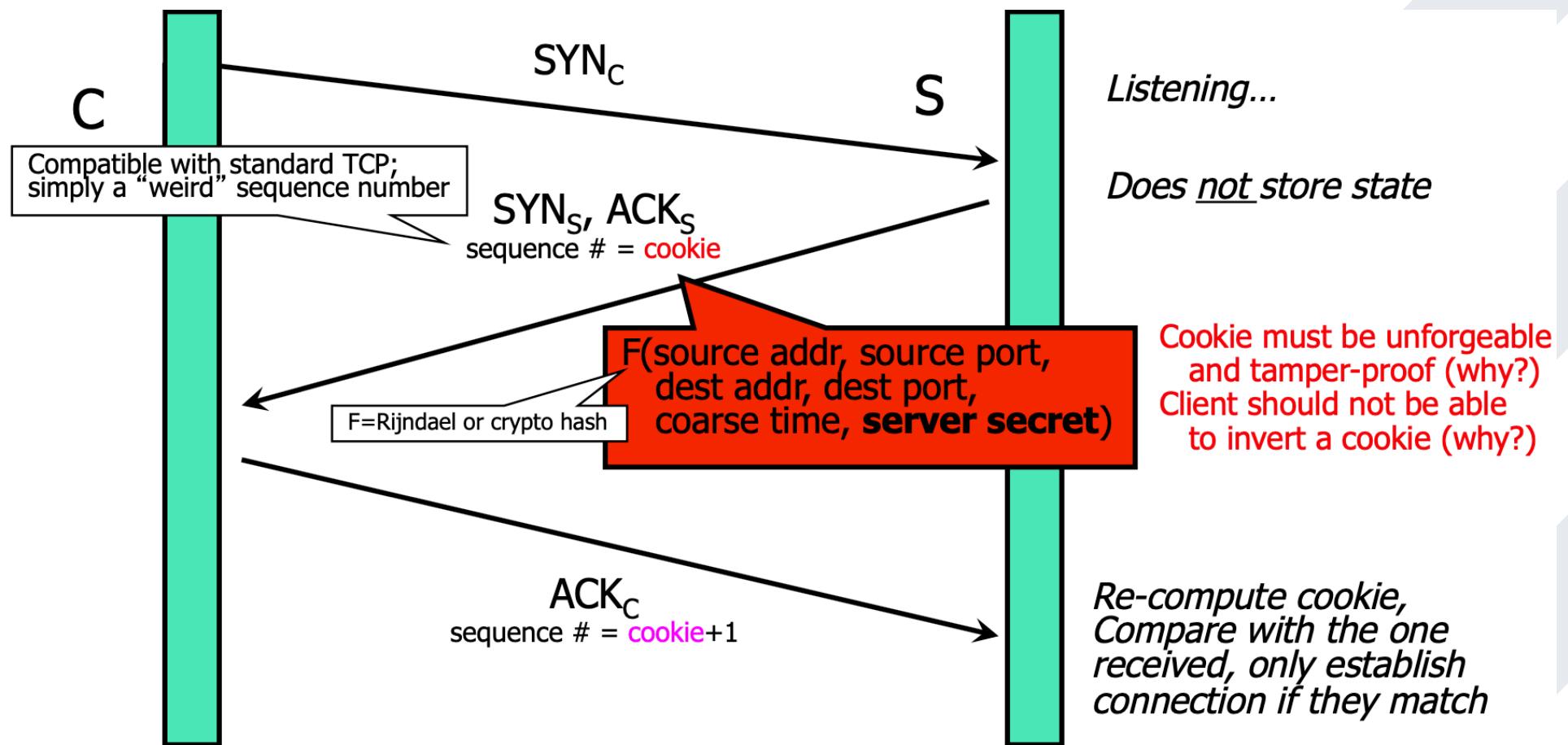
TCP – Transmission Control Protocol

- Preventing Denial of Service
 - DoS is caused by asymmetric state allocation
 - If a victim server opens new state for each connection attempt, attacker can initiate thousands of connections from bogus or forged IP addresses
 - **Cookies** ensure that the responder (victim) is stateless until initiator produced at least one acknowledgment
 - Responder's state (IP addresses and ports of the connection) is stored in a cookie and sent to initiator
 - After initiator responds, cookie is regenerated and compared with the cookie returned by the initiator



TCP – Transmission Control Protocol

- Preventing Denial of Service



TCP – Transmission Control Protocol

- Denial of Service by Connection Reset
 - If attacker can guess/predict/monitor the current sequence number for an existing connection, can send RESET packet to close it
 - Especially effective against long-lived connection
 - Widely used in Internet Censorship



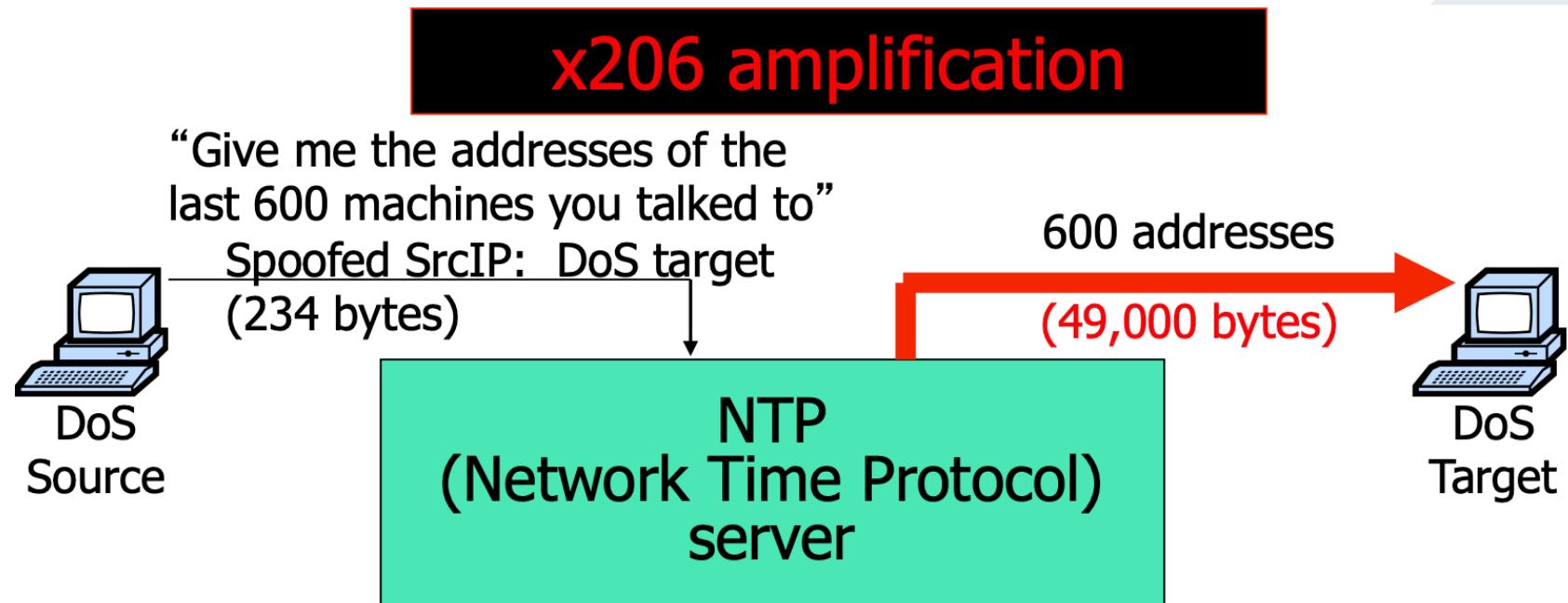
UDP – User Datagram Protocol

- **Connectionless protocol**
 - Simply send datagram to application process at the specified port of the IP address
 - Source port number provides return address
 - Applications: media streaming, broadcast
- **No acknowledgement, no flow control, no message continuation**



UDP – User Datagram Protocol

- NTP Amplification Attack
 - “Reflection-and-Amplification” attack



- Dec. 2013 – Feb. 2014: 400Gbps DDoS attacks involving 4,500+ NTP servers



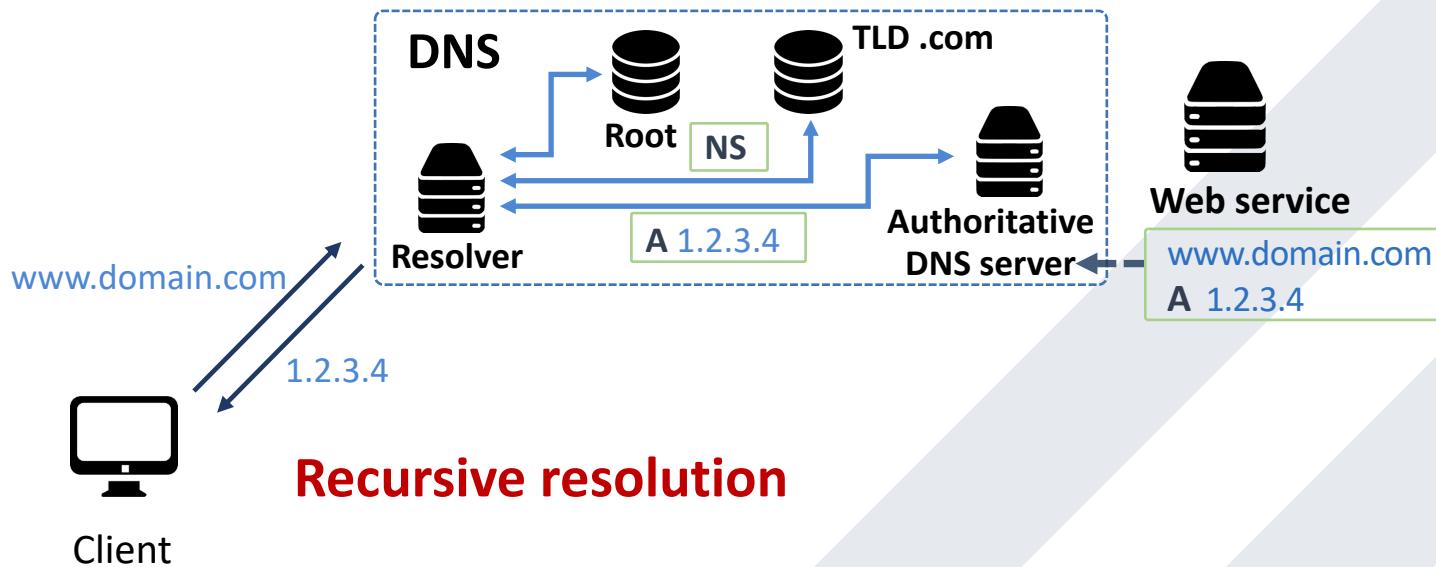
Network Defenses

- **Rate-limiting**
 - Straightforward but cannot differentiate legitimate traffic from malicious traffic
- **Egress Filtering against IP spoofing**
 - ISPs are lack of motivation to deploy
- **DDoS Protection Service offered by Content Delivery Networks (CDNs)**
 - Re-route the traffic to CDN's highly distributed network infrastructures
 - Must hide the origin IP address



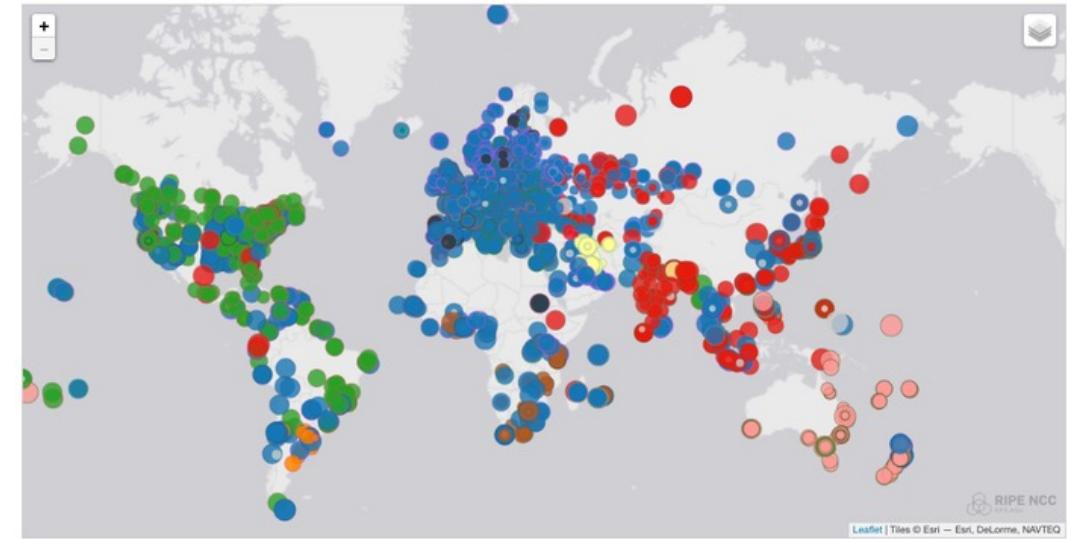
DNS – Domain Name System

- Internet Dictionary
 - Maps symbolic names to numeric IP addresses



DNS – Domain Name System

- **Hierarchical System Design**
 - Root nameservers for top-level domains (.com, .edu, .uk, etc)
 - 13 root server systems (A - M)
 - Top-level domain (TLD) nameservers indicate authoritative nameservers
 - Authoritative nameservers (ADNS) resolve subdomains
 - Local resolvers contact authoritative servers for requested domains



K-root servers



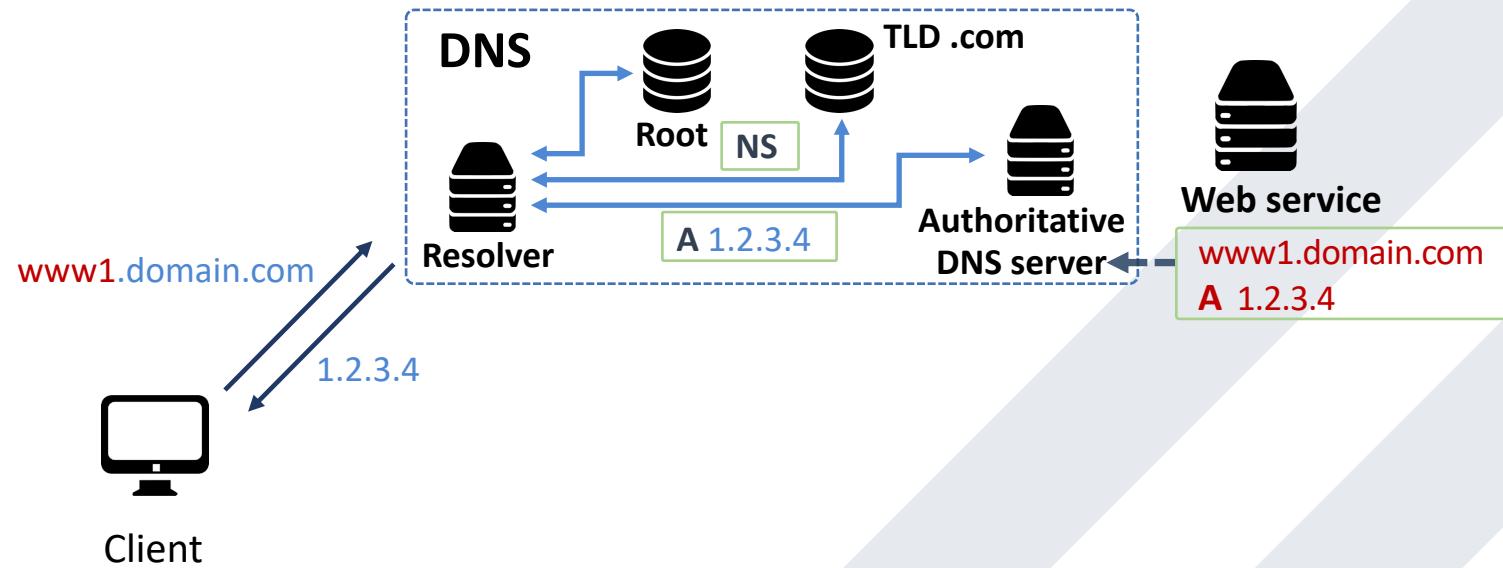
DNS – Domain Name System

- **DNS Caching**
 - DNS responses can be cached (on local resolvers)
 - Quick response for repeated translations
 - Other queries may reuse some parts of lookup
 - NS records identify name servers responsible for a domain
 - DNS negative queries can be cached
 - Don't have to repeat past mistakes (failed domains, misspellings, etc.)
 - Cached data will periodically time out
 - Lifetime (TTL) of data controlled by owner of data, passed with every record



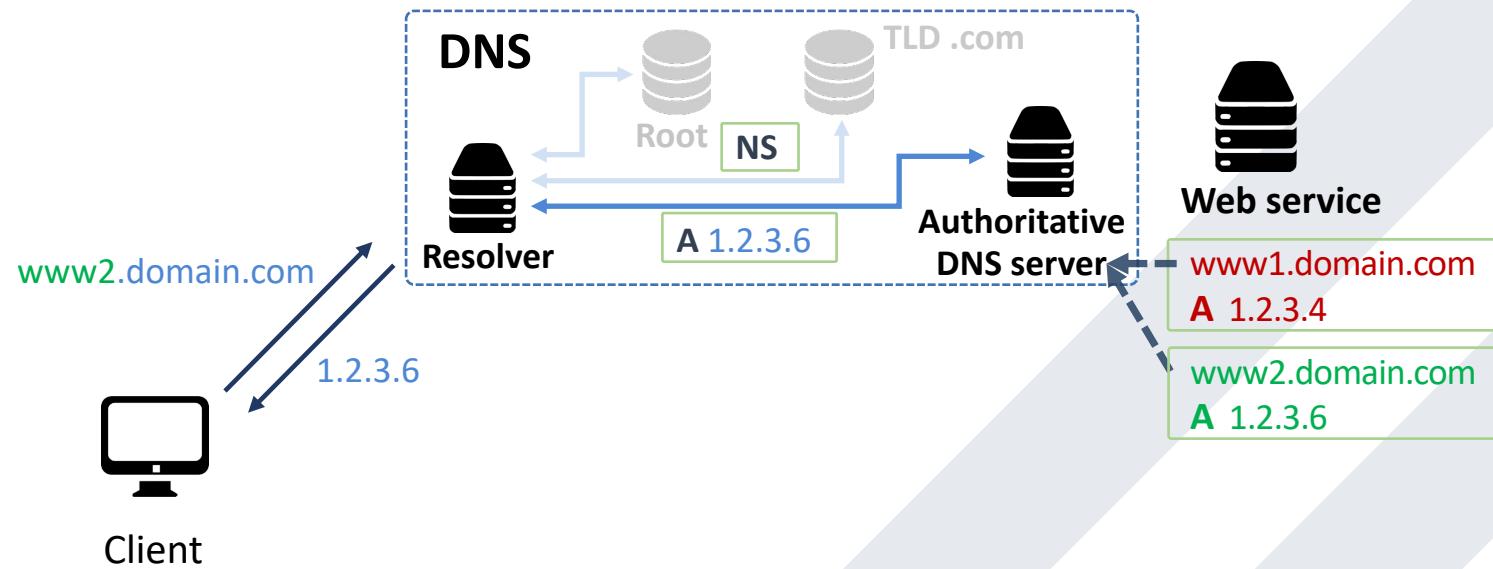
DNS – Domain Name System

- DNS Caching



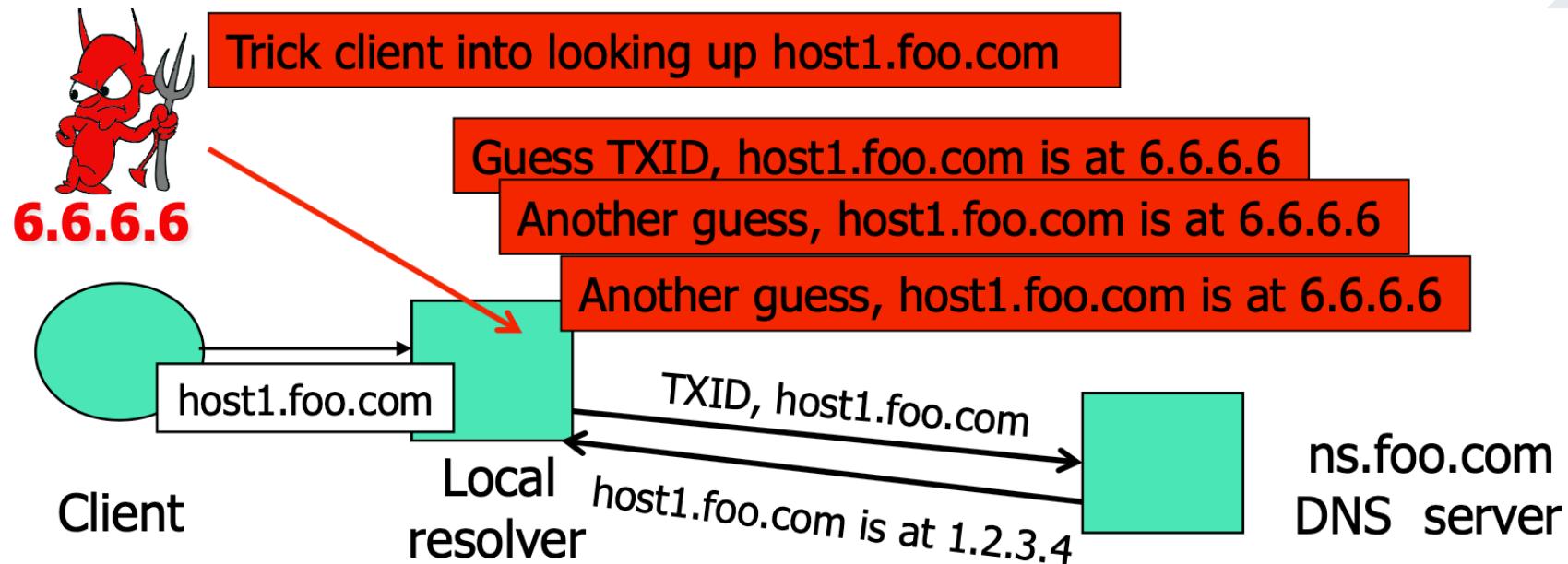
DNS – Domain Name System

- DNS Caching



DNS – Domain Name System

- DNS Spoofing (Cache Poisoning)

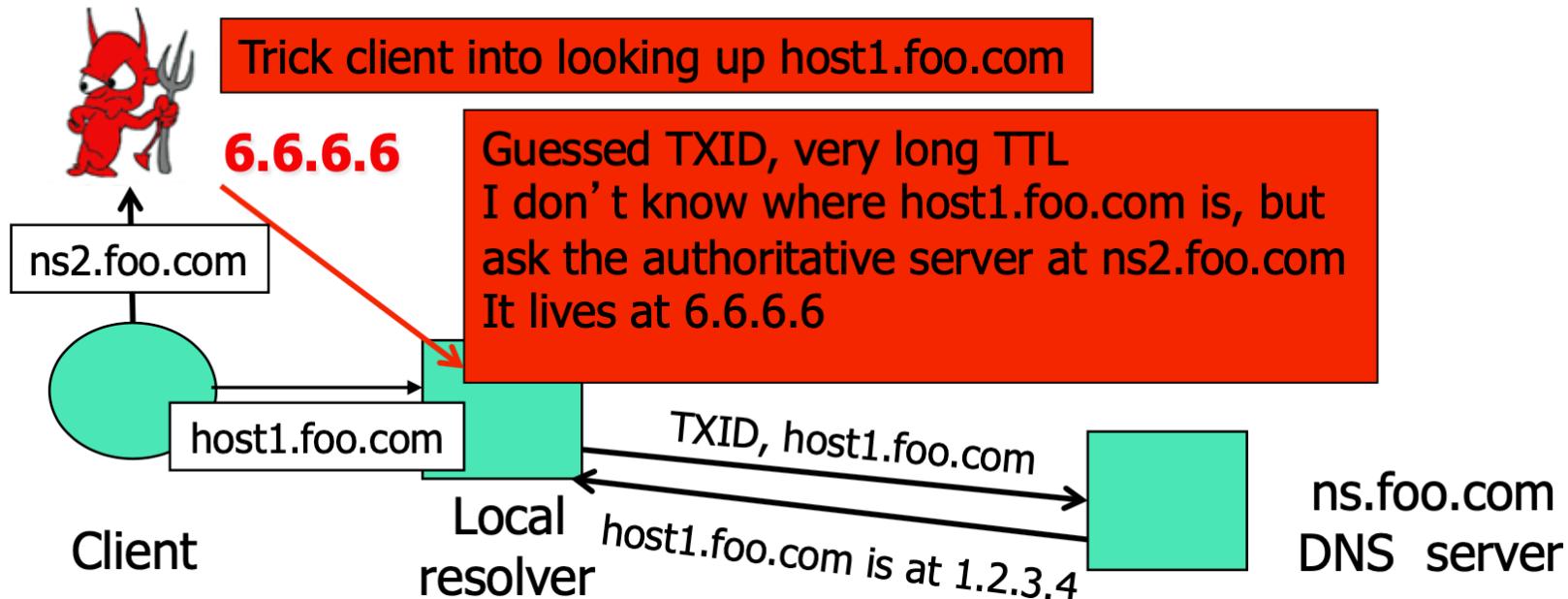


- Several opportunities to win the race.
- Here attacker attempts to pollute individual A records



DNS – Domain Name System

- DNS Spoofing (Cache Poisoning)



- If win the race, any request for <XXX>.foo.com will go to 6.6.6.6.
The NS record is poisoned for a very long time
- If lose, try again with <ANYTHING>.foo.com



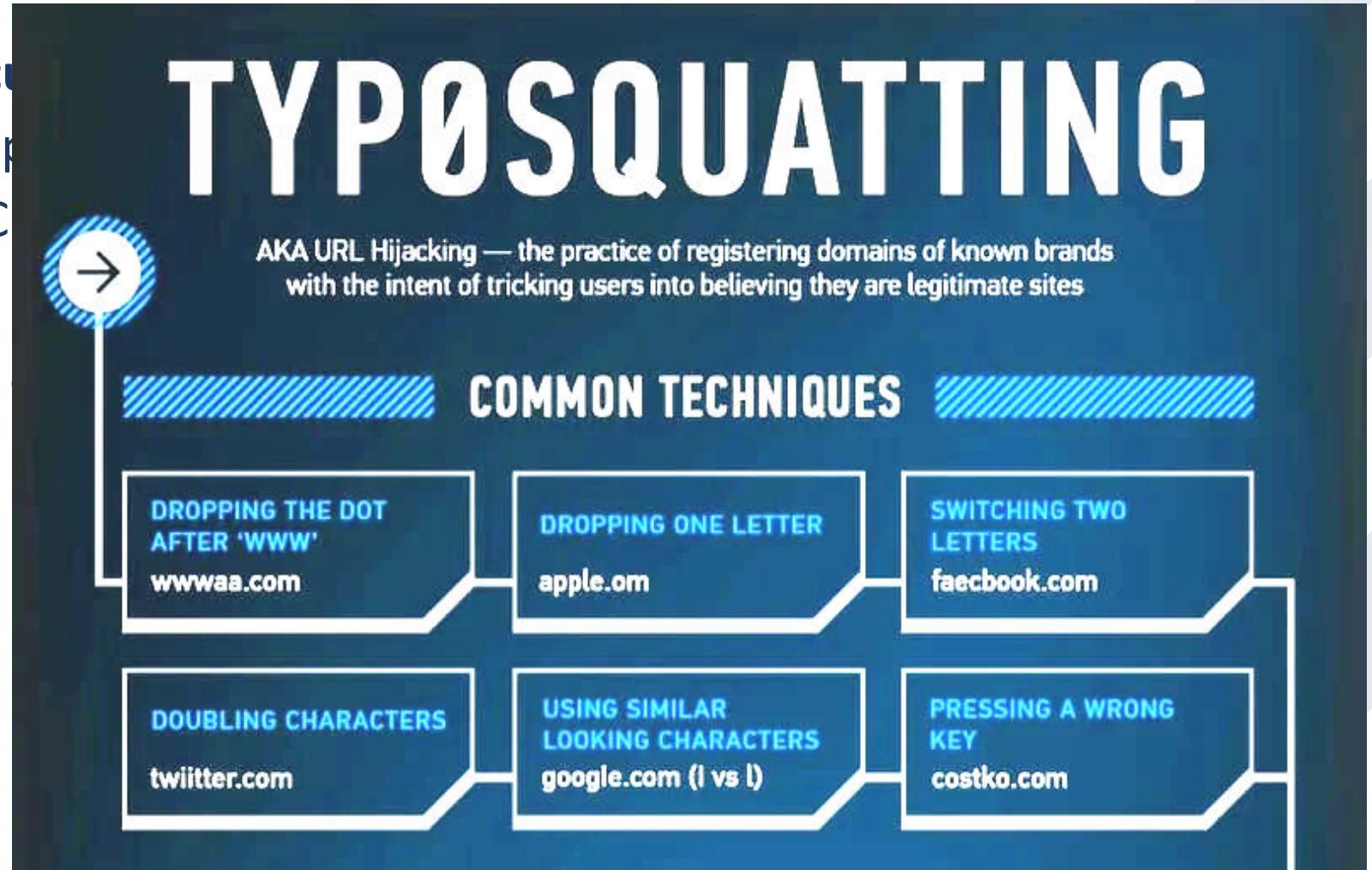
DNS – Domain Name System

- Solving the DNS Spoofing Problem
 - Long TTL for legitimate responses?
 - Does it really help?
 - Randomize port in addition to TXID
 - 32 bits of randomness, makes it harder for attacker to guess TXID+port
 - DNSSEC
 - Cryptographic authentication of host-address mappings



DNS – Domain Name System

- Other DNS-related Security Issues
 - Fast flux in DNS mapping
 - DNS-based C&C
 - DNS squatting
 - typo-squatting,



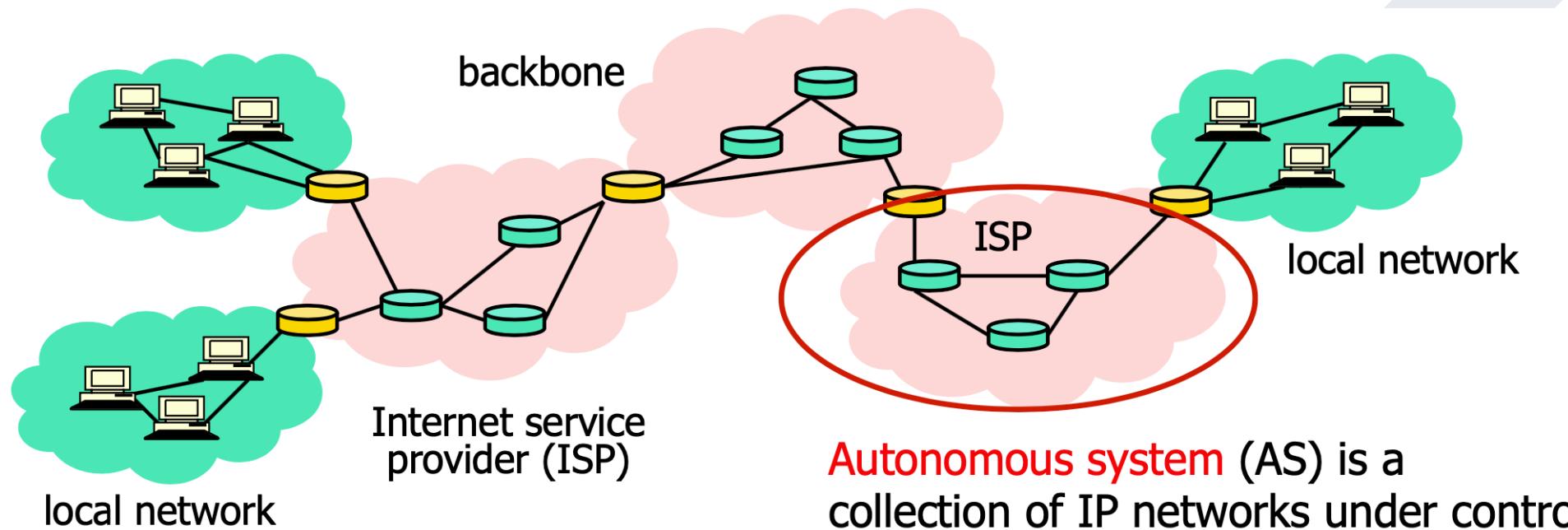
DNS – Domain Name System

- Other DNS-related Security Issues
 - Fast flux in DNS mappings
 - DNS-based C&C (Control-and-command) in botnets
 - DNS squatting
 - typo-squatting, combo-squatting
 - Domain/subdomain hijacking
 - Dangling DNS records, domain shadowing



IP Routing – BGP (Border Gateway Protocol)

- Internet: a Network of Network

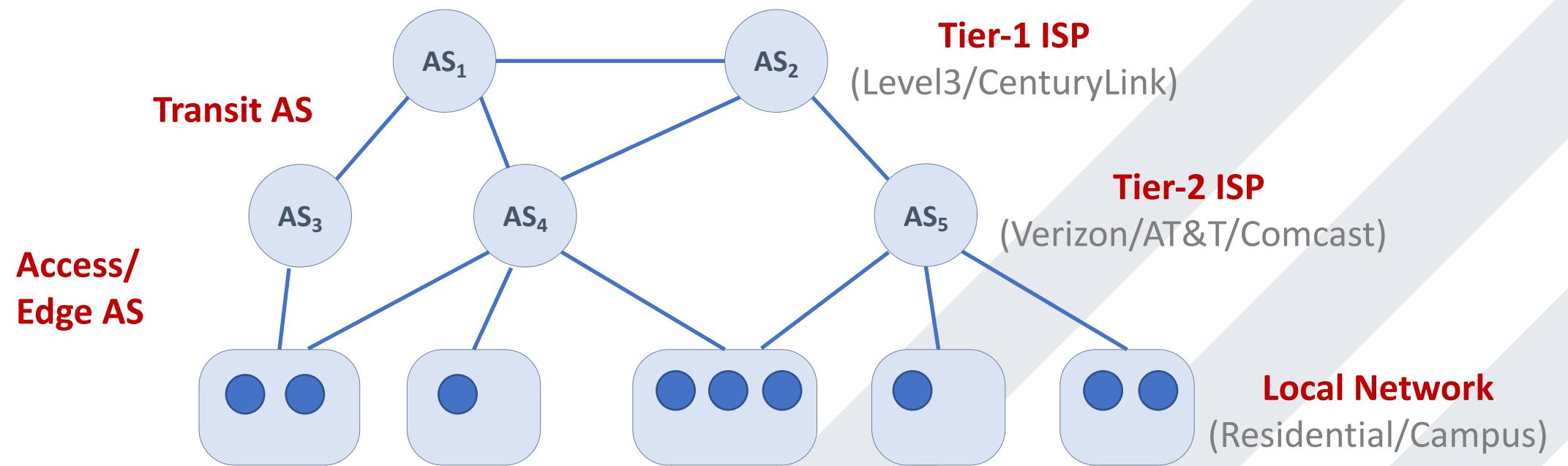


Autonomous system (AS) is a collection of IP networks under control of a single administrator (e.g., ISP)



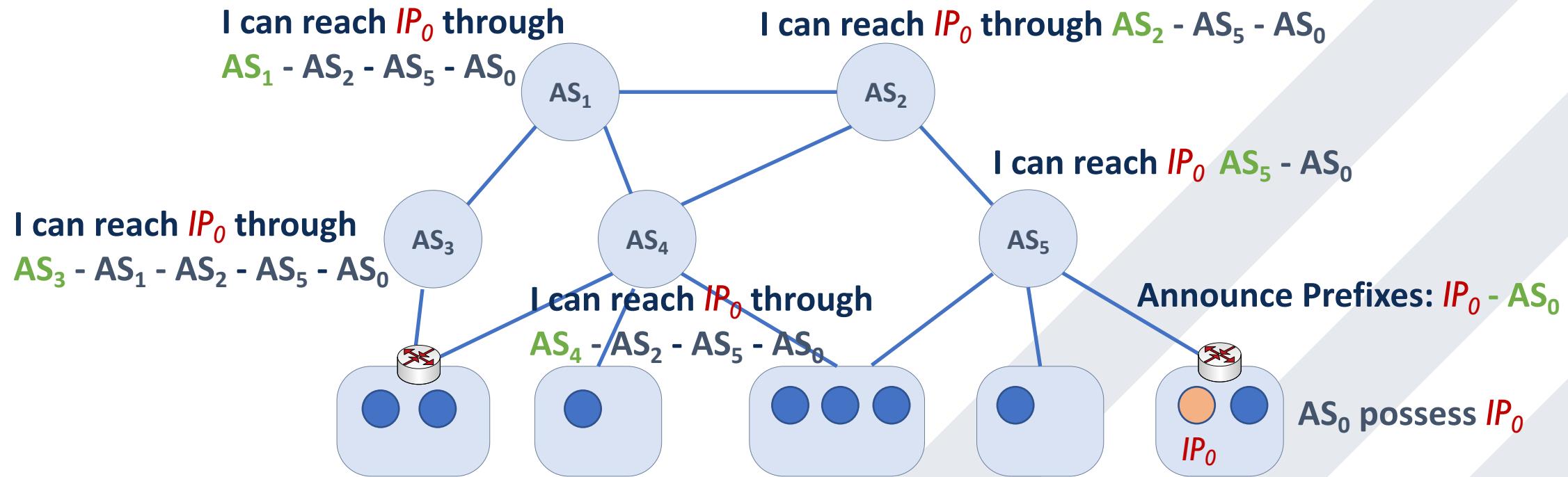
IP Routing – BGP (Border Gateway Protocol)

- Internet: a Network of Network



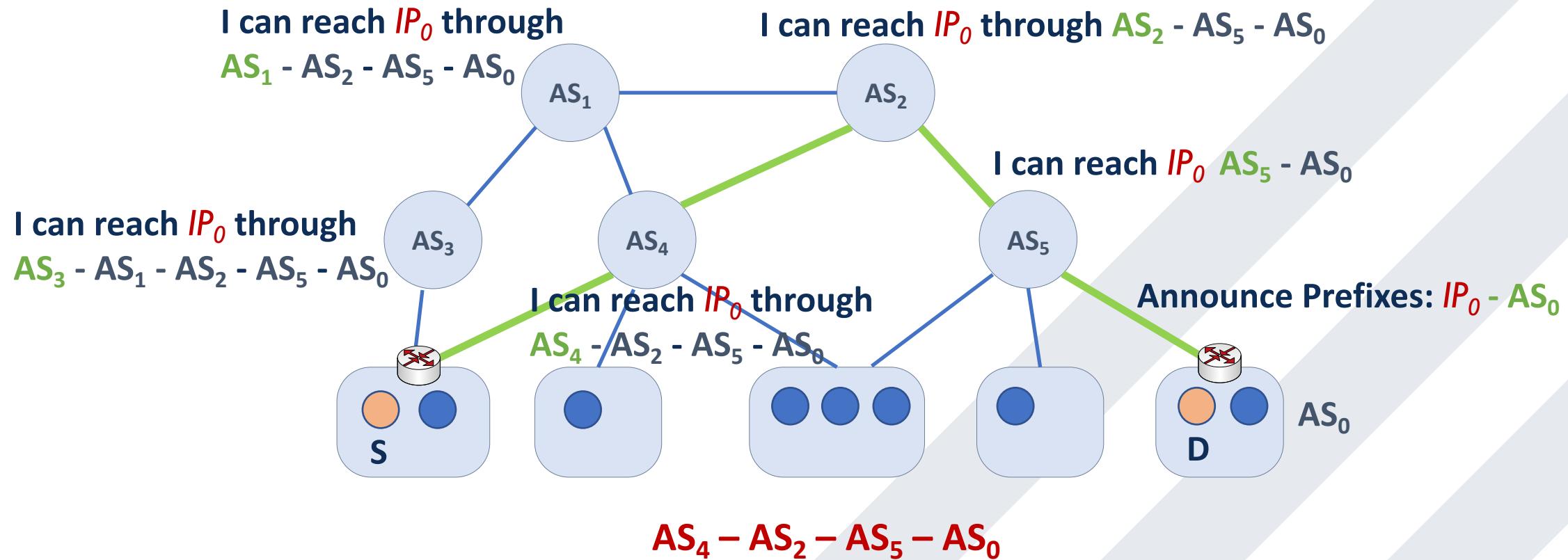
IP Routing – BGP (Border Gateway Protocol)

- Internet: a Network of Network



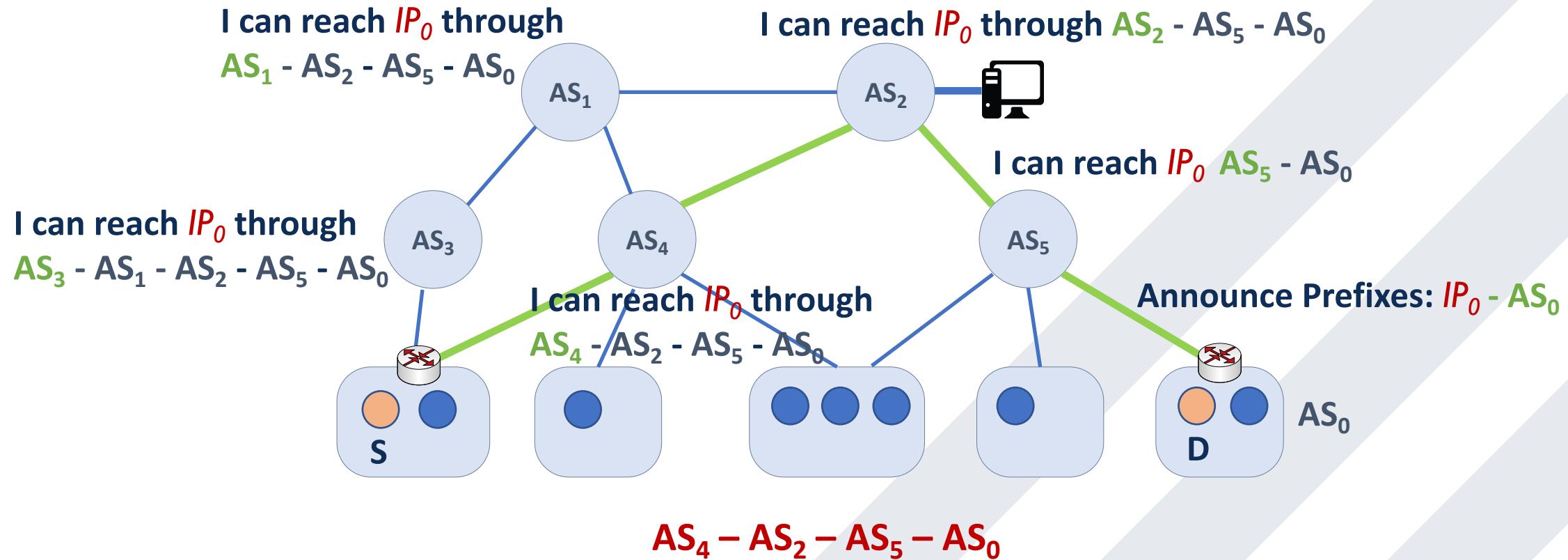
IP Routing – BGP (Border Gateway Protocol)

- Internet: a Network of Network



IP Routing – BGP (Border Gateway Protocol)

- Internet: a Network of Network



BGP (In)Security

- BGP update messages contain no authentication or integrity protection
- Attacker (malicious ASes or misconfiguration) may falsify the advertised routes (BGP Hijacking)
 - Modify the IP prefixes associated with a route
 - Can blackhole traffic to certain IP prefixes
 - Change the AS path
 - Either attract traffic to attacker's AS, or divert traffic away
 - Economic incentive: an ISP wants to dump its traffic on other ISPs without routing their traffic in exchange



BGP (In)Security

- **BGP Hijacking – (Sub-)prefix Hijacking**
 - Routers perform routing by the manner of the most specific prefix matching (i.e., longest-matching)
 - Adversaries may intentionally announce a prefix “smaller” than originally advertised one
 - A fraction of Internet traffic destined to the prefix to be captured by the adversary
 - Captured traffic is blackholed



BGP (In)Security

- BGP Hijacking – **Path Hijacking (Interception attack)**
 - ASes selectively/incidentally put themselves on the path
 - Adversaries may announce reachability of a prefix to attract traffic to be routed through the AS
 - The interception attack allows the malicious AS to become an intermediate AS in the path
 - Traffic can be routed back – keep the connection alive



BGP (In)Security

- **BGP Incident**

- Domain advertises good routes to access the Internet
 - Result: packets go into a network
 - April 25, 1997: “The day the Internet exploded”
 - AS7007 (Florida Internet Exchange) re-advertised all prefixes as if it were the Internet
 - In effect, AS7007 was advertising the Internet
 - Huge network instability as incorrect routing data propagated and routers crashed under traffic

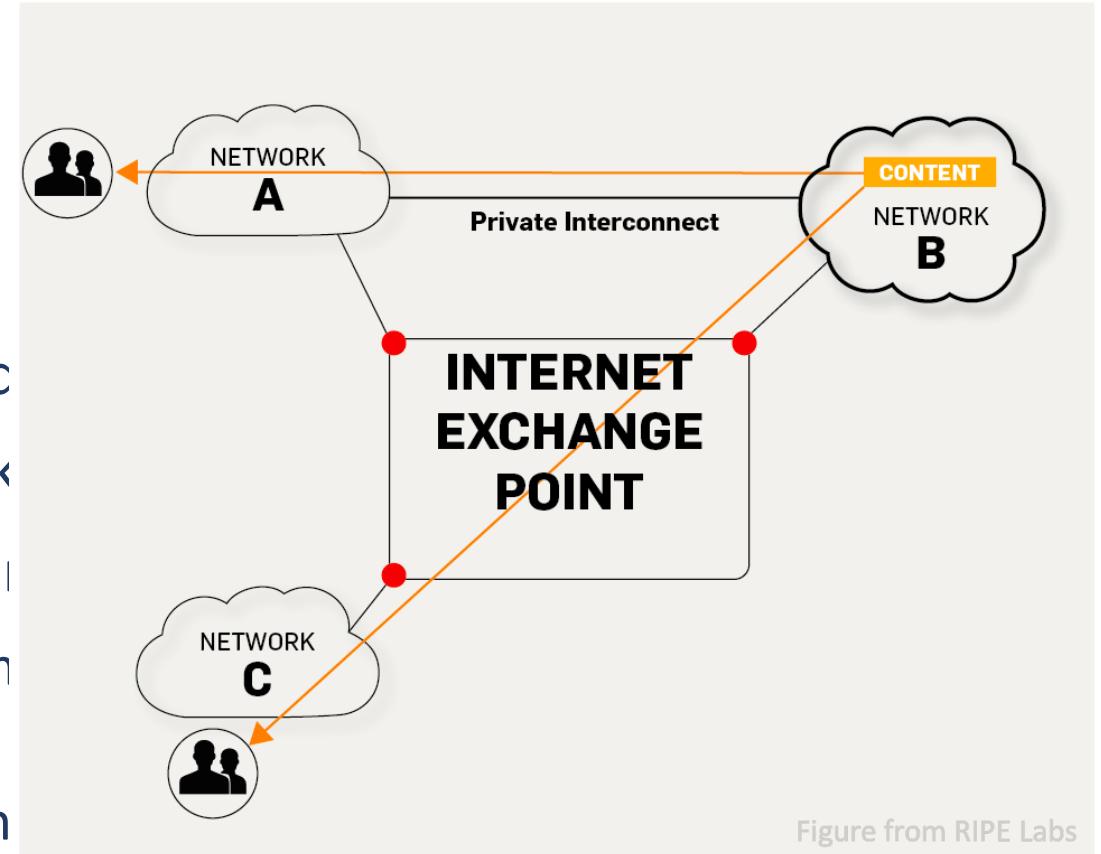


Figure from RIPE Labs



BGP (In)Security

- **BGP Incident**
 - Domain advertises good routes to addresses it does not know how to reach
 - Result: packets go into a network “blackhole”
 - April 25, 1997: “The day the Internet died”
 - AS7007 (Florida Internet Exchange) de-aggregated the BGP route table and re-advertised all prefixes as if it originated paths to them
 - In effect, AS7007 was advertising that it has the best route to every host on the Internet
 - Huge network instability as incorrect routing data propagated and routers crashed under traffic



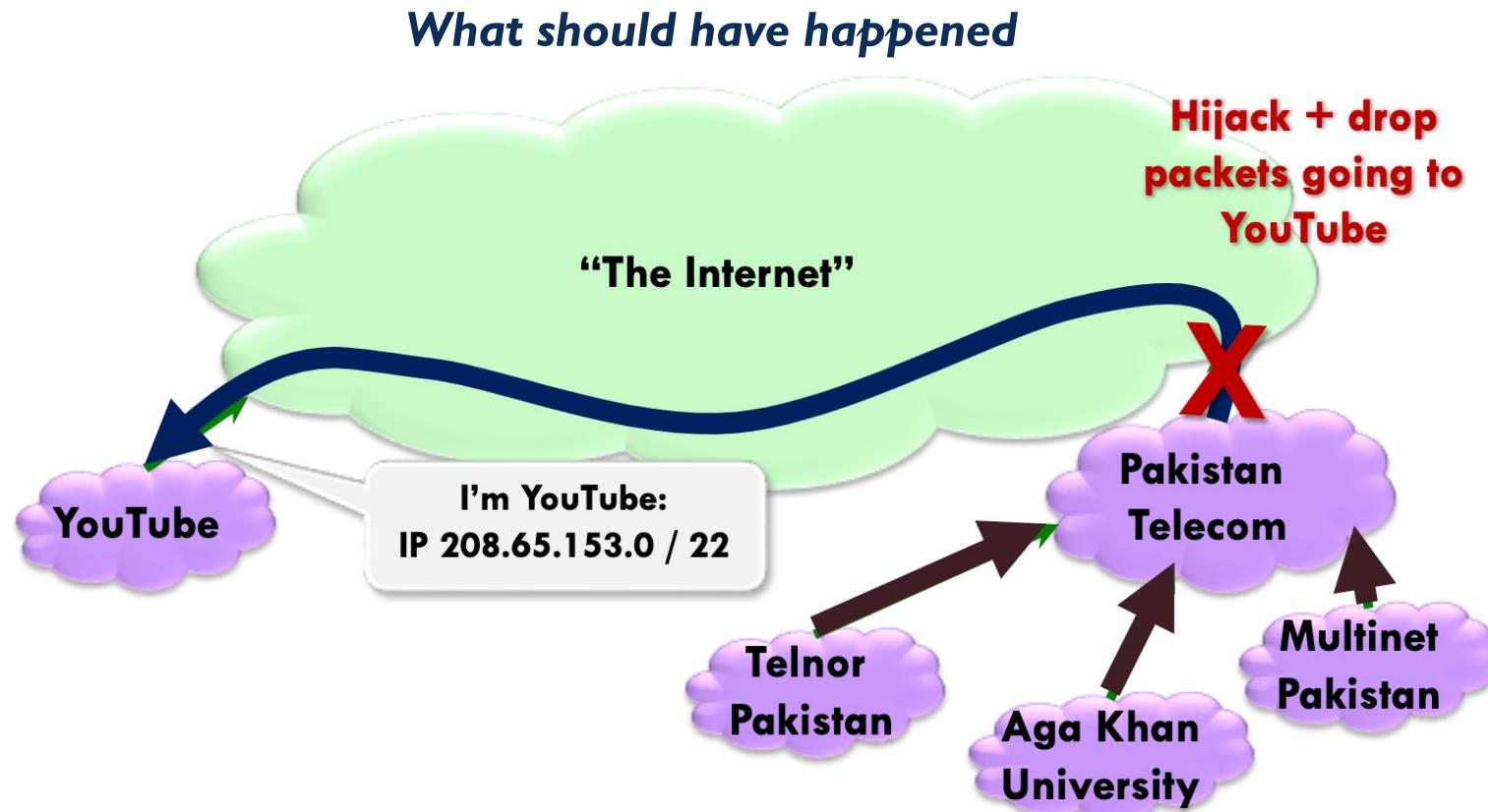
BGP (In)Security

- **BGP Incident:** Pakistan Telecom hijacks YouTube (February 2008)
 - Pakistan government wants to block YouTube
 - AS17557 (Pakistan Telecom) advertises 208.65.153.0/24
 - All YouTube traffic worldwide directed to AS17557



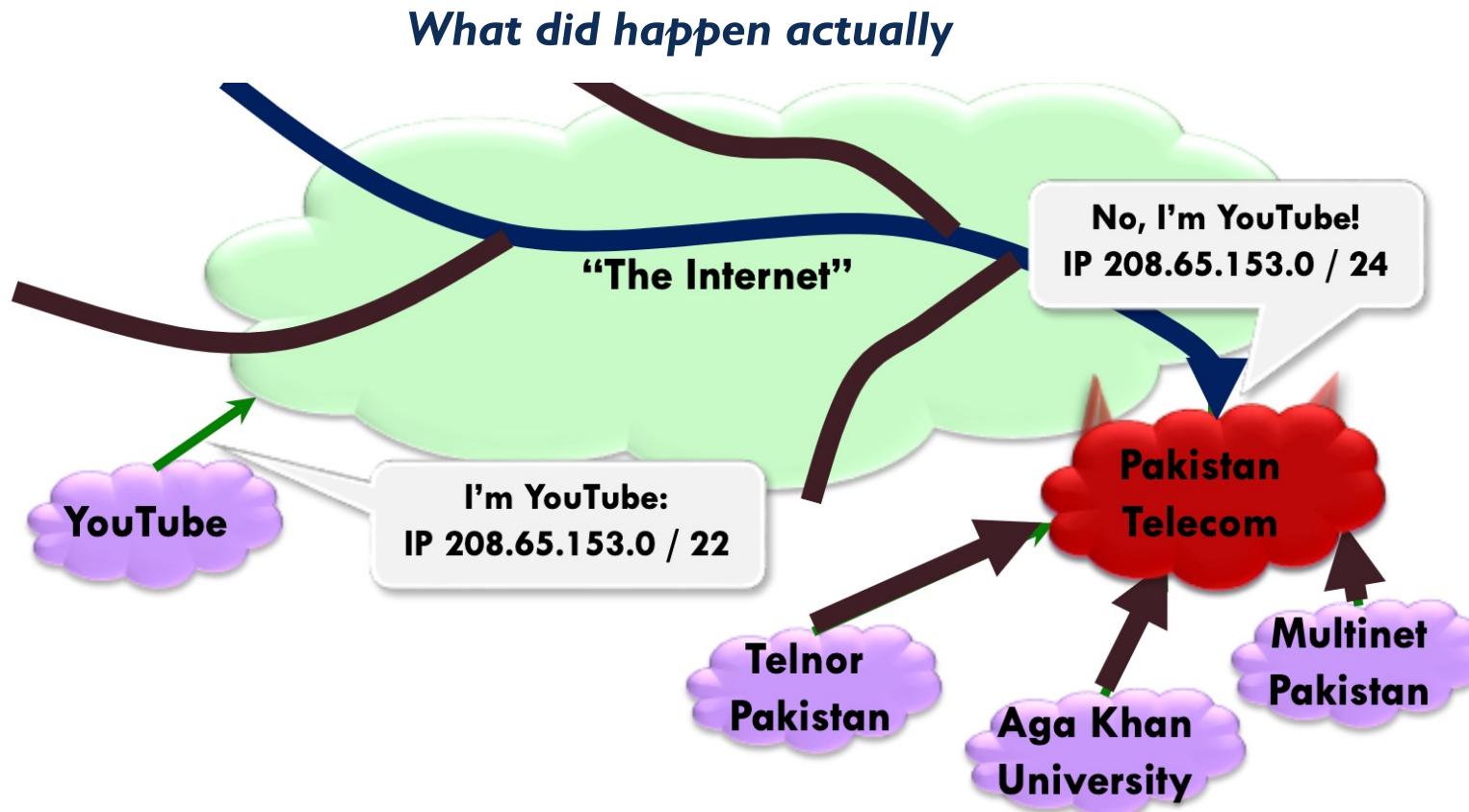
BGP (In)Security

- BGP Incident: Pakistan Telecom hijacks YouTube (February 2008)



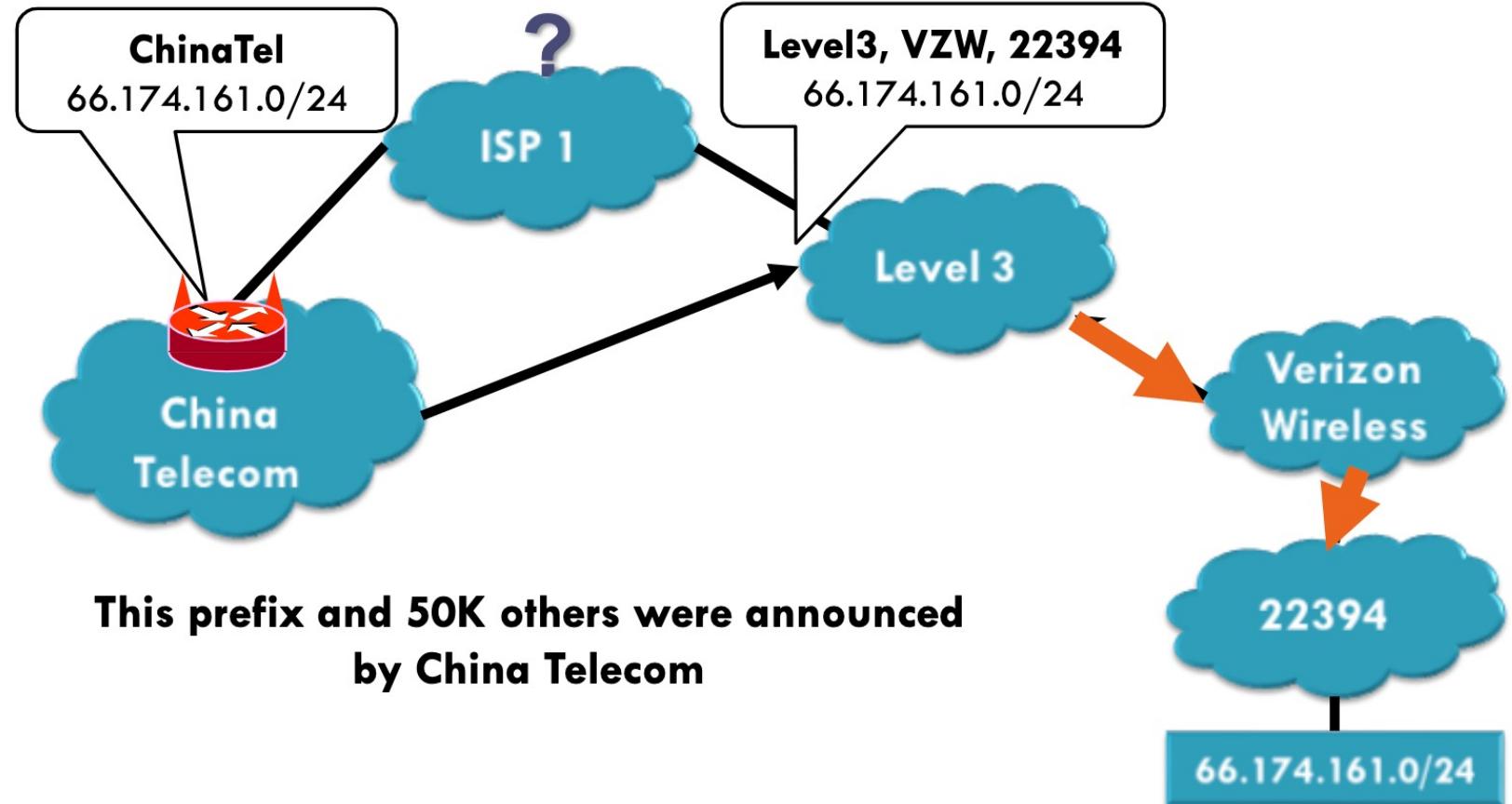
BGP (In)Security

- BGP Incident: Pakistan Telecom hijacks YouTube (February 2008)



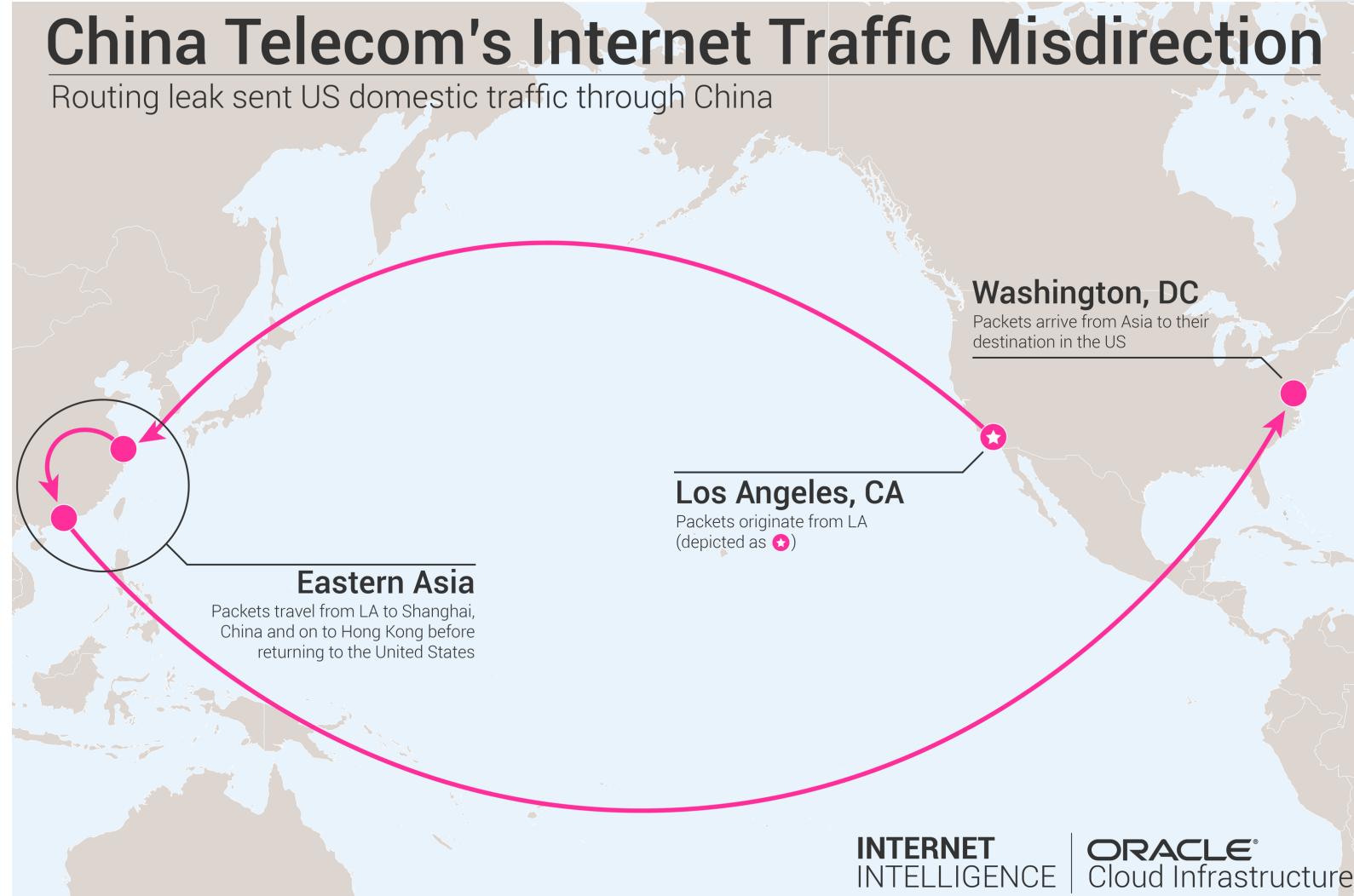
BGP (In)Security

- BGP Incident



BGP (In)Security

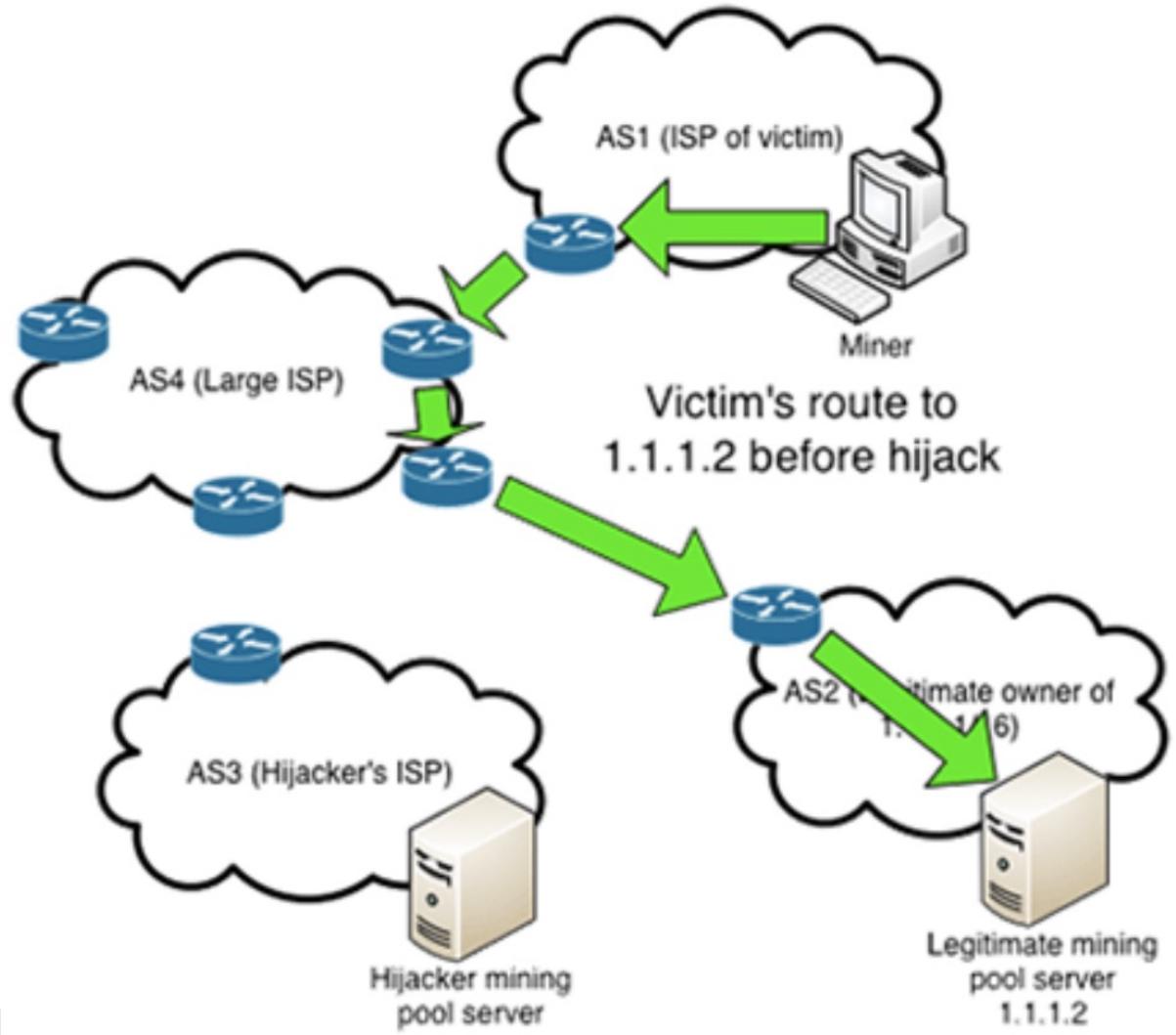
- BGP Incident



BGP (In)Security

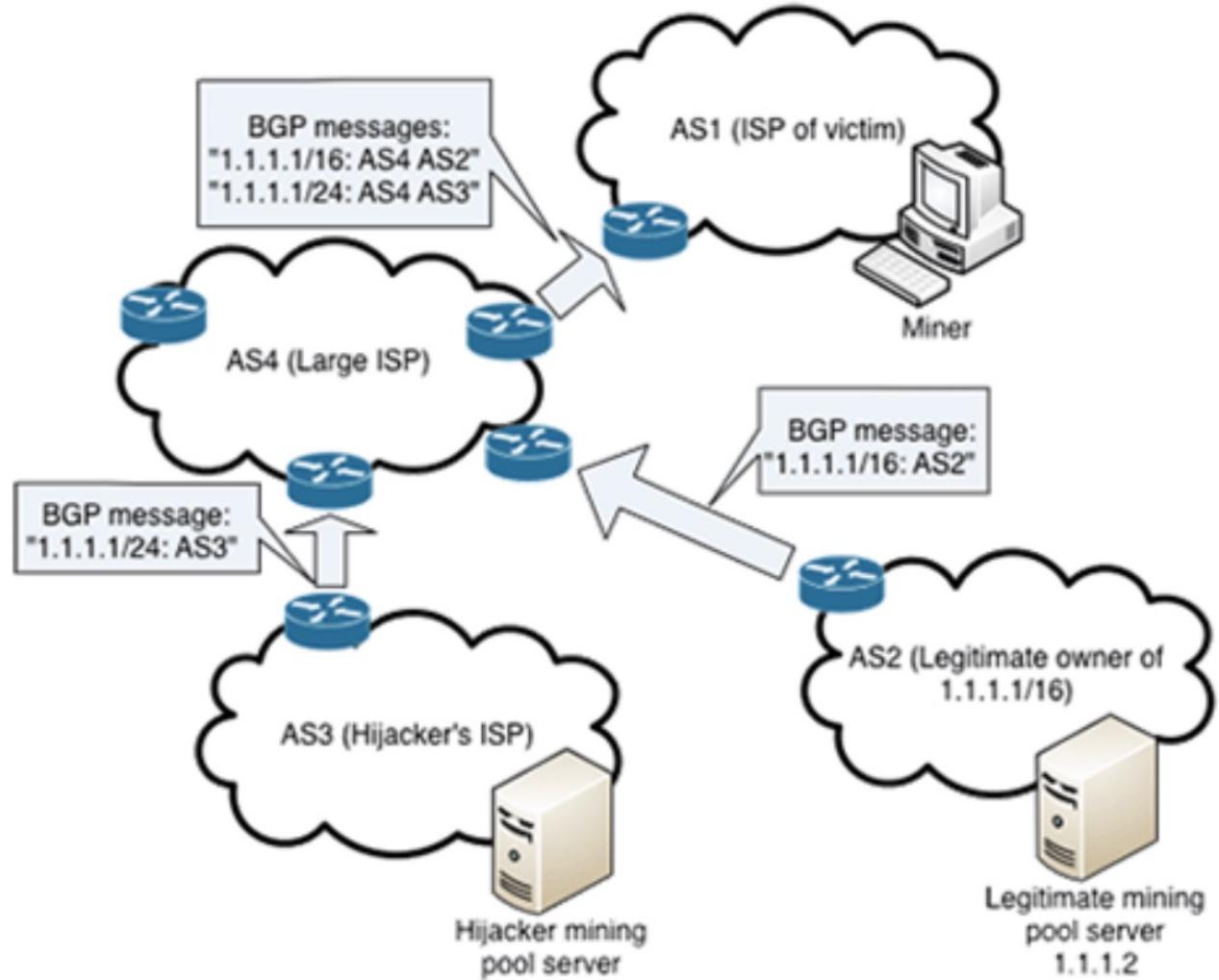
- **BGP Incident**

- Bitcoin Hijack (February 2014)
 - Hijacked users got directed to a mining server that was under the control of hijacker and redirects them to a malicious mining pool
 - Miners continues to receive mining tasks but don't get compensated



BGP (In)Security

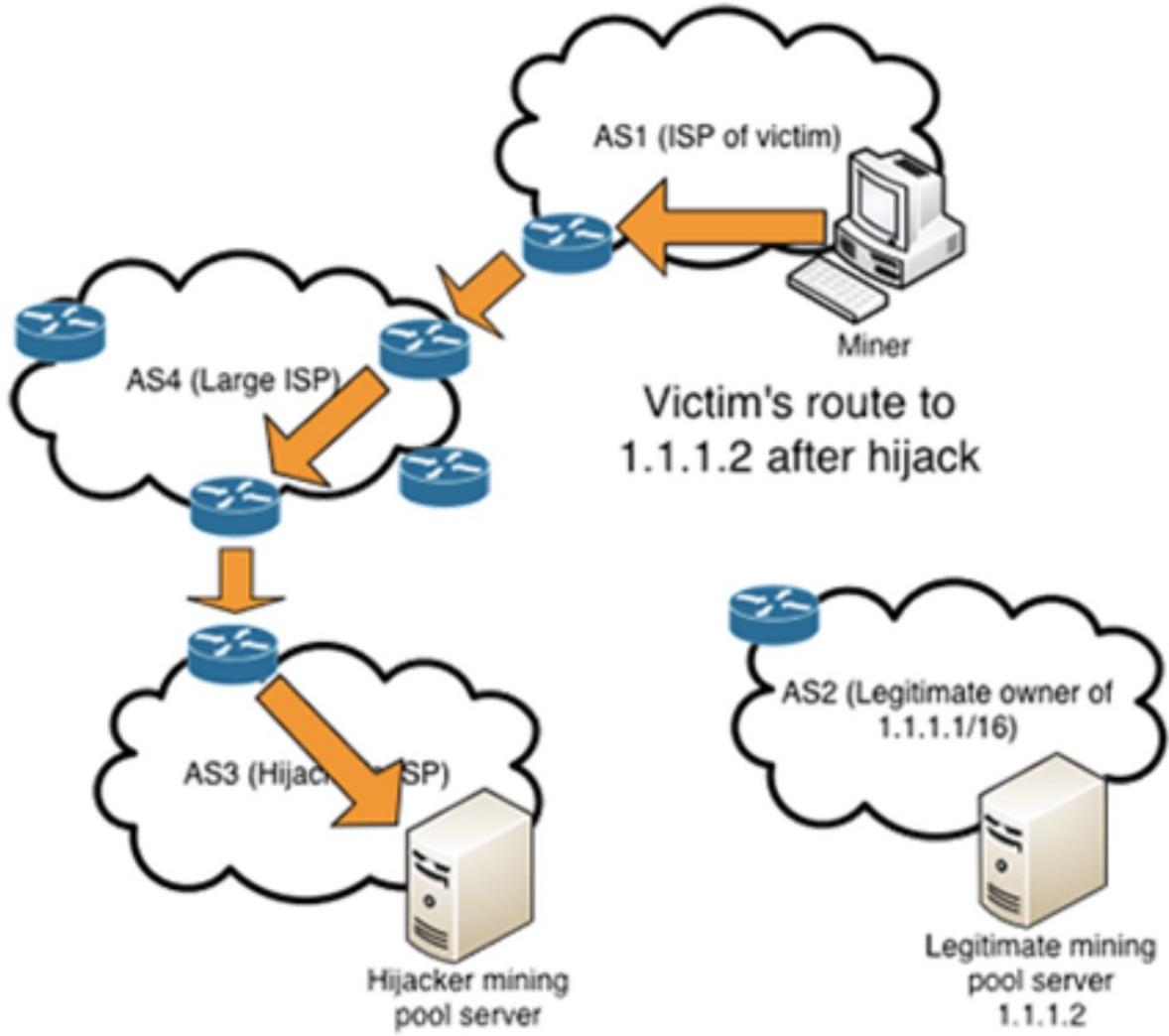
- BGP Incident
 - Bitcoin Hijack (February 2014)
 - Hijacked users got directed to a mining server that was under the control of hijacker and redirects them to a malicious mining pool
 - Miners continues to receive mining tasks but don't get compensated



BGP (In)Security

- **BGP Incident**

- Bitcoin Hijack (February 2014)
 - Hijacked users got directed to a mining server that was under the control of hijacker and redirects them to a malicious mining pool
 - Miners continues to receive mining tasks but don't get compensated



BGP (In)Security

- Secure BGP is extremely hard
 - The victim AS doesn't see the problem
 - Picks its own route
 - May not cause entire loss of connectivity
 - Partial damage
 - Performance degradation
 - Diagnosing prefix hijacking
 - Analyzing updates from many vantage points



BGP (In)Security

- **Secure BGP is extremely hard**
 - Complex System
 - Around 100K Autonomous Systems
 - Decentralized Control among ASes
 - Hard to reach agreement on the solution
 - Hard to deploy the solution even standardized
 - Low incentive: many solutions benefit others rather than the deployer itself, e.g., ingress filter to defend IP spoofing



BGP (In)Security

- **Secure BGP is extremely hard**
 - RPKI – Resource Public Key Infrastructure
 - Against prefix hijacking
 - Secure BGP/BGPsec
 - Against path hijacking



Content Delivery Network (CDN)

- Content Delivery Network
 - Deploy a large number of **edge servers** proximal to clients
 - Emerging in late 90s



Content Delivery Network (CDN)

- Content Delivery Network

- Deploy a large number of edge servers
 - Emerging in late 90s



HISTORY The First Victim of Sept. 11

He was likely the first person killed, but his influence was felt that entire terrible day—online.

By MOLLY KNIGHT RASKIN

SEPT 11, 2015 • 7:34 AM



The legacy of Danny Lewin, the first man to die on 9/11

By Todd Leopold, CNN
Updated 7:24 AM ET, Wed September 11, 2013



MORE FROM CNN BUSINESS

 Handshake aims to help students launch their career

 Dow plunges after Trump tweets about China

Recommended by Outbrain



Content Delivery Network (CDN)

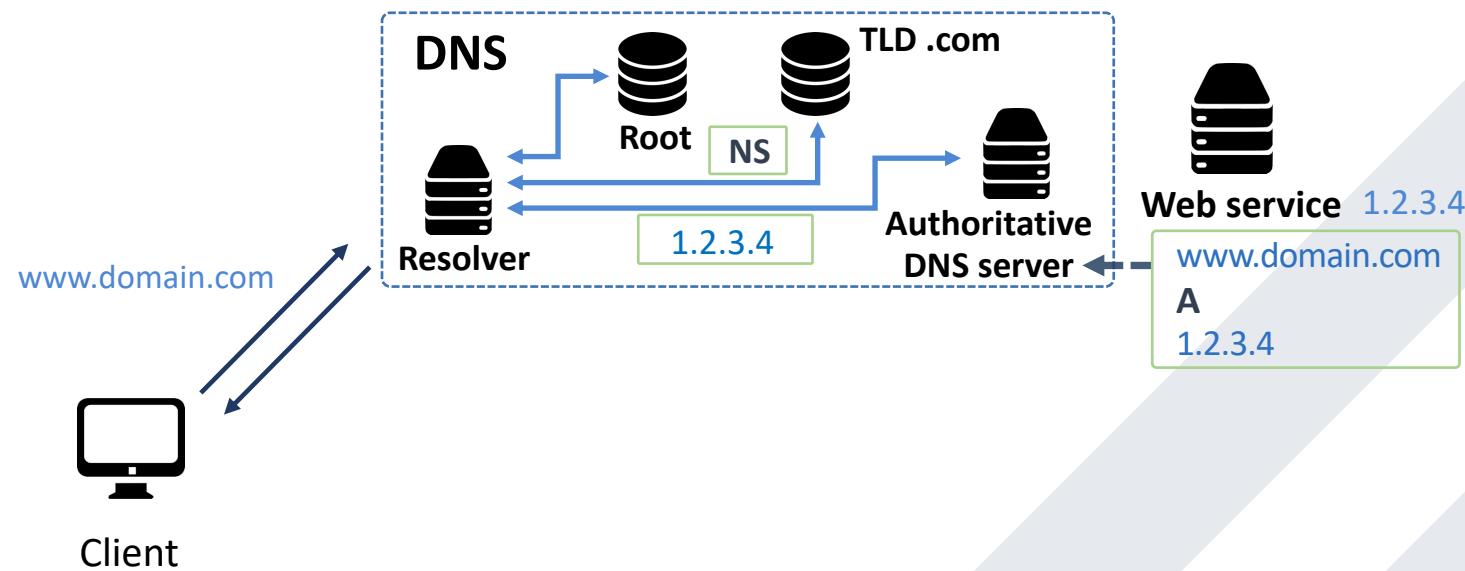
- Content Delivery Network

- Deploy a large number of **edge servers** proximal to clients
 - Emerging in late 90s
- Delivery significant port of Internet traffic
 - All top Internet services leverage CDNs
- DNS-based CDNs vs. Anycast-based CDNs



Content Delivery Network (CDN)

- Content Delivery Network

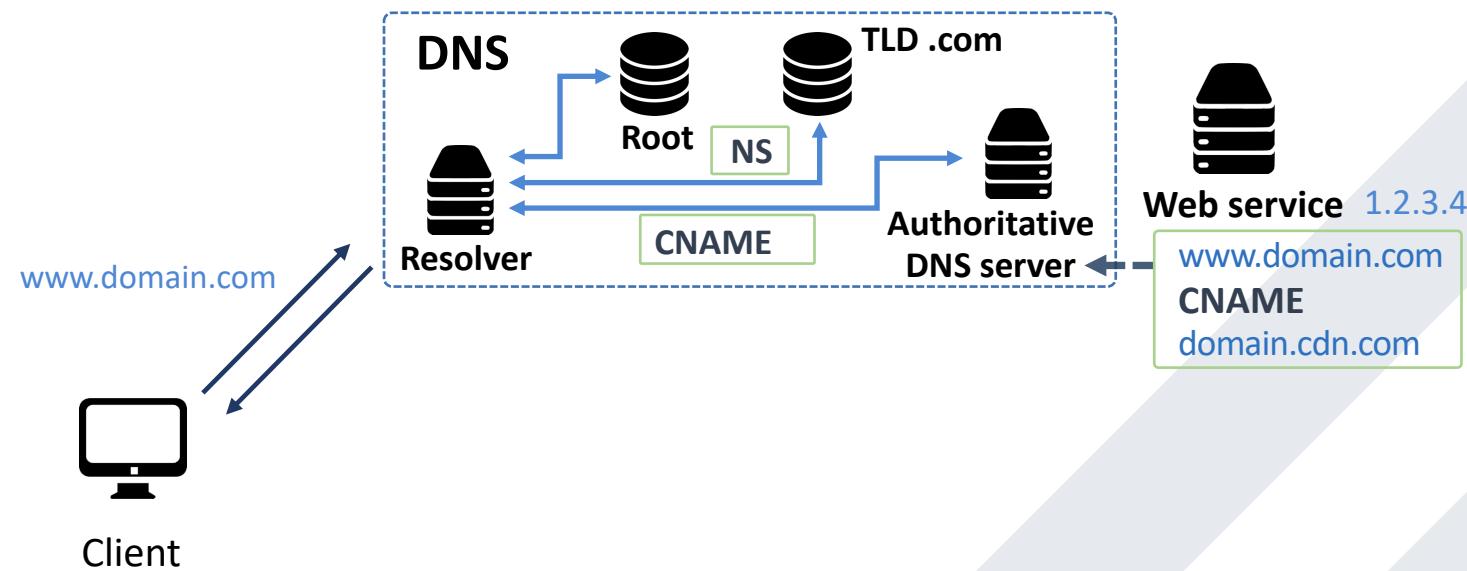


DNS-based CDNs



Content Delivery Network (CDN)

- Content Delivery Network

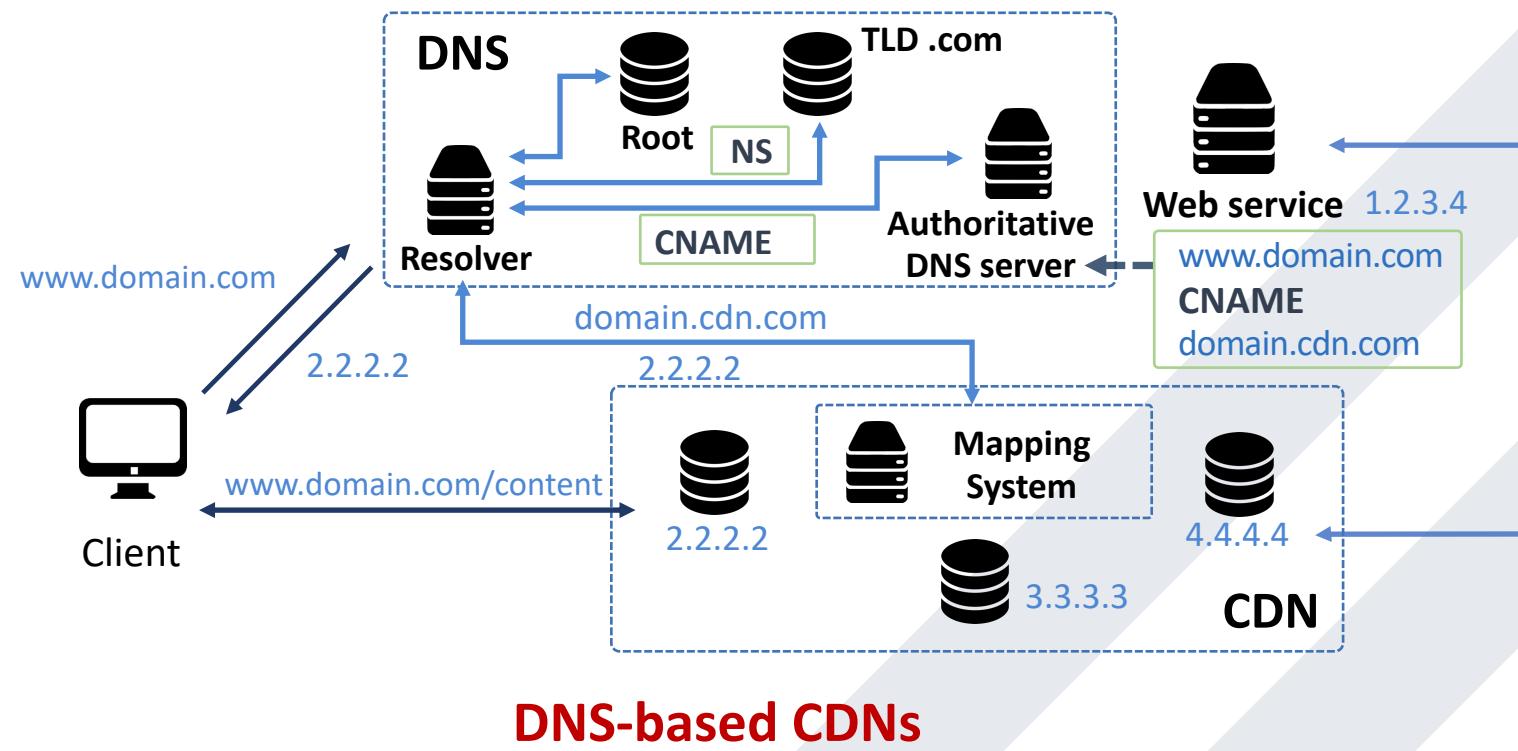


DNS-based CDNs



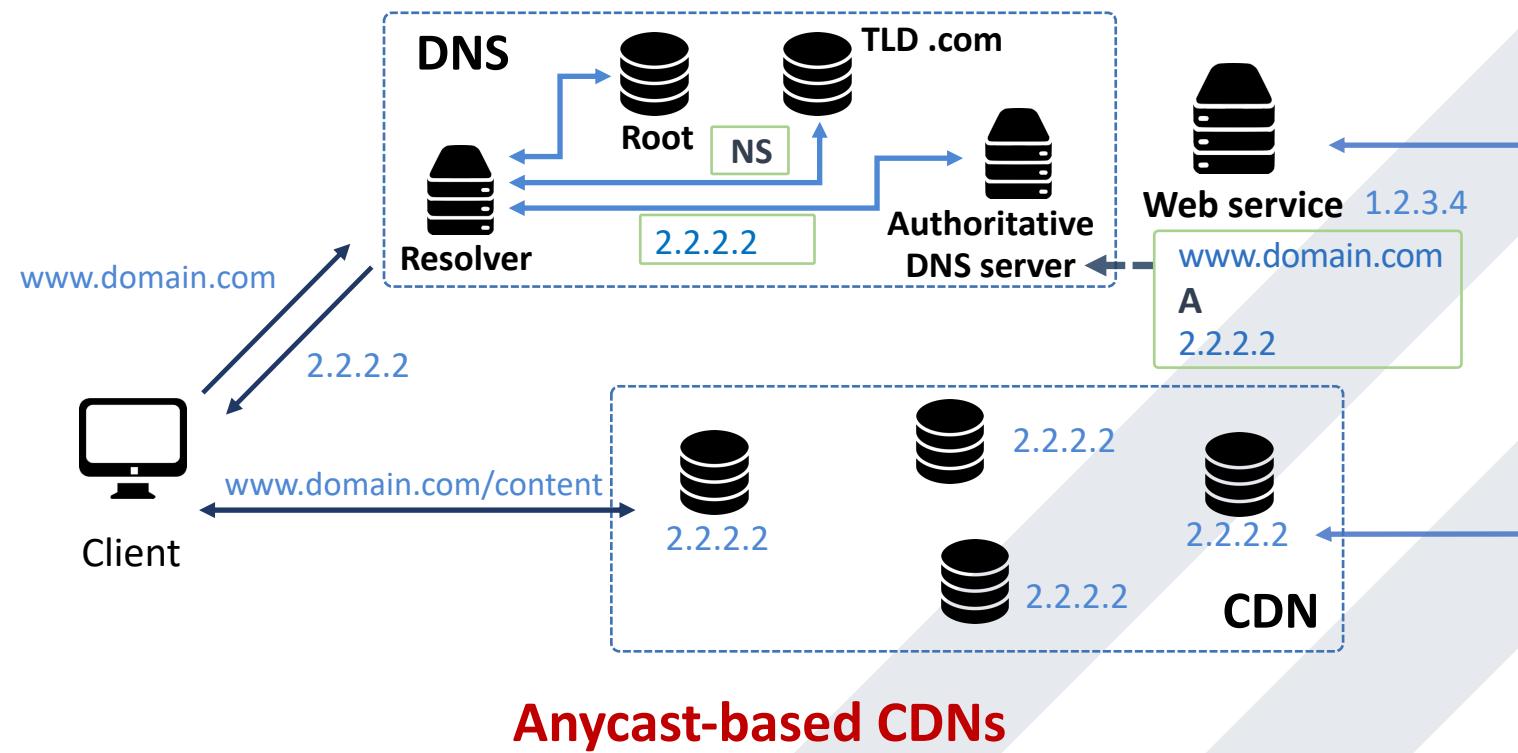
Content Delivery Network (CDN)

- Content Delivery Network



Content Delivery Network (CDN)

- Content Delivery Network



Content Delivery Network (CDN)

- **Instinct nature of security provided by CDNs**
 - Additional layer of proxy
 - Hide the actual origin source of web services
 - Highly distributed, scalable platforms
 - Absorb malicious traffic (blackholing/scrubbing traffic)
 - Redundancy of service instance
 - Provision of integrity/authentication (TLS/SSL)



Network Security

- TCP/IP
 - DoS Attacks
 - DNS
 - BGP
 - CDN
-
- Applied Cryptography
 - PKI
 - SSL/TLS and HTTPS
 - DNSSEC
 - RPKI





CS 772/872: Advanced Computer and Network Security

Fall 2022

Course Link:

<https://shhaos.github.io/courses/CS872/netsec-fall2022.html>

