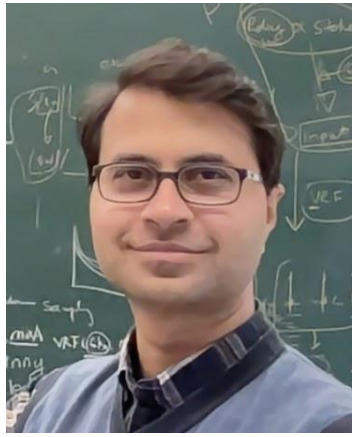
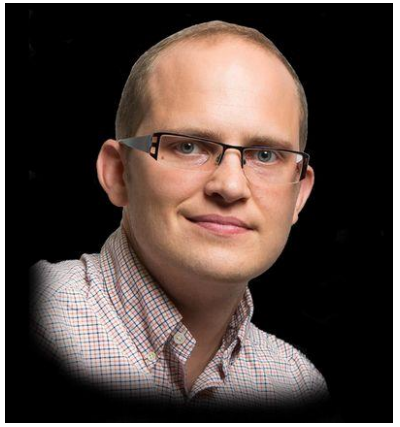
CSEC-10/11 Admin

Teaching team



Tariq Elahi
CO CSEC-10

Marc Juarez
CO CSEC-11



Markulf Kohlweiss

TAs: CSEC-10 (Mhghna Sengupta, Rachel Somerset), CSEC-11 (Lawrence Piao)

Assessment

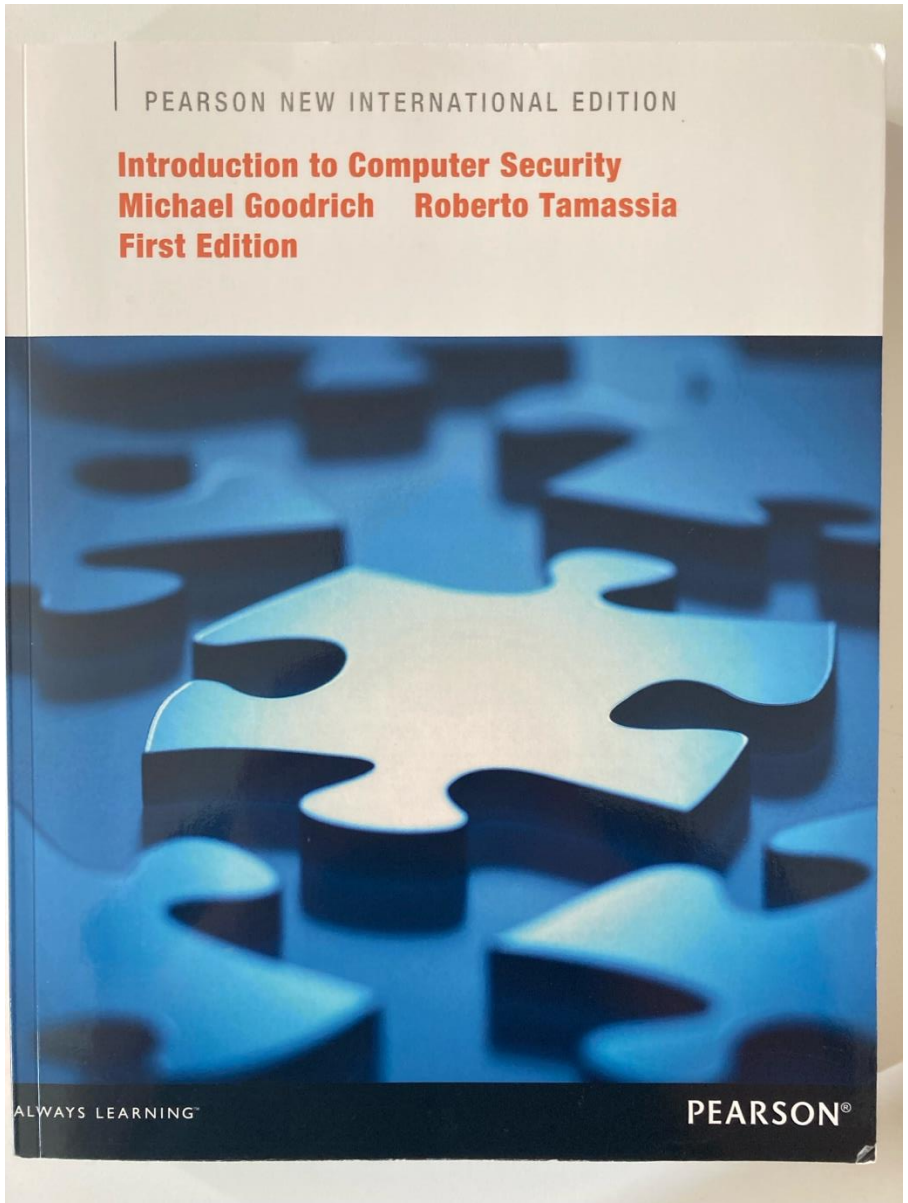
CSEC-10

- CW1 (formative)
- CW2 (25% of total)
- Final exam (75% of total)

CSEC-11

- CW1 (30% of total)
- Final exam (70% of total)

Textbook


PEARSON NEW INTERNATIONAL EDITION
Introduction to Computer Security
Michael Goodrich Roberto Tamassia
First Edition
ALWAYS LEARNING
PEARSON

Where to find information

- Course Learn page
  - Schedule
  - Lecture recordings
  - Coursework submission links
  - Piazza (student discussions, CW Q&A)
    - Office hours
    - Post-recital Q&A

Course overview

- What are our goals in this course?
- What is trust?
- What is security?
- What is privacy?
- Who are the adversaries?
- Terminology
- Common defence methods

What are our goals in this course?

- To be able to identify security, privacy, and trust issues in various aspects of computing, such as:
  - Programs
  - Operating systems
  - Networks
  - Distributed systems
  - Internet applications
- The awareness of how security, privacy, and trust can be achieved in practice

The landscape

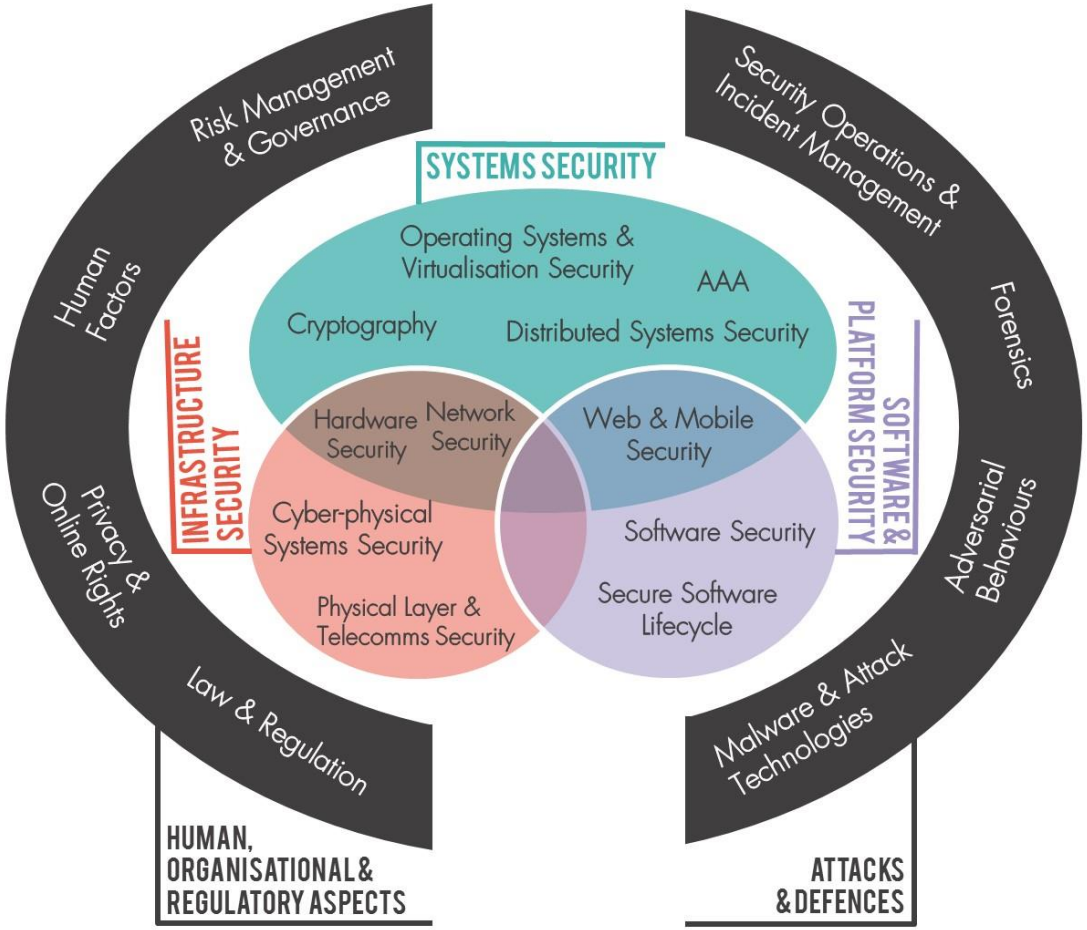


Image: CyBOK

What do we want?

What do the we mean when we say…?

- Authentic
- Safe
- Common language/sense → (more) Formal language/models
  - Based on definitions
  - Properties of the system, the data, usage, and abilities of the participants
  - Wide-spread agreement (in some areas; still evolving)

Who is we?

- Ordinary citizen
- Whistle blower
- Corporate worker
- Dissident activist
- Secret agent

What is security?

- The main general properties are:
  - Confidentiality
    - Information access to only authorized entities

Authenticity

  - Integrity
    - The data is untampered and uncorrupted
  - Availability
    - Both the data and the system that provides access to it are there when you need them
- Are these enough? What can still go wrong?

Failure of Security: Apple Security Cert Validation Bug

- The bug occurs in code that is used to check the validity of the server's signature on a key used in an SSL/TLS connection.
- An active attacker (a “malfactor-in-the-middle”) could potentially exploit this aw to get a user to accept a counterfeit key that was chosen by the attacker.

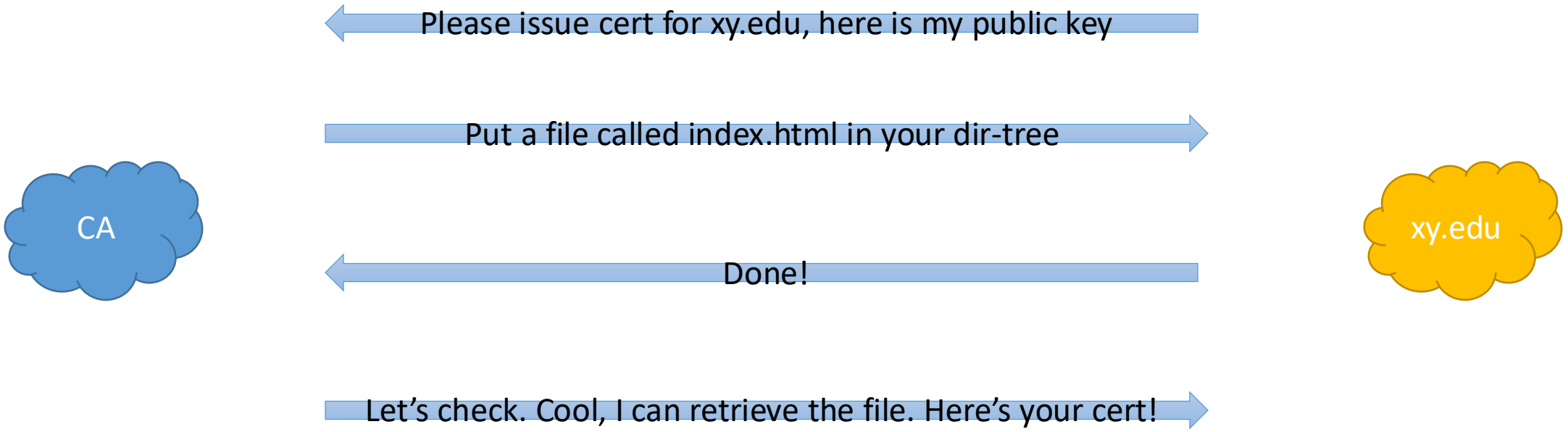
```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
        OSStatus        err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...

fail:
        SSLFreeBuffer(&signedHashes);
        SSLFreeBuffer(&hashCtx);
        return err;
}
```

What is trust?

- Generally, we trust when we have:
  - Assurance
    - The means to know that the system is secure
  - Reliability/Resilience
    - To operate intact in the face of natural disasters and human-launched attacks
  - Accountability
    - The means to verify that the system is operating as designed (i.e. securely)

NB: There is a difference between trustworthy and trusted

Failure of Trust:
CA Domain Control Validation



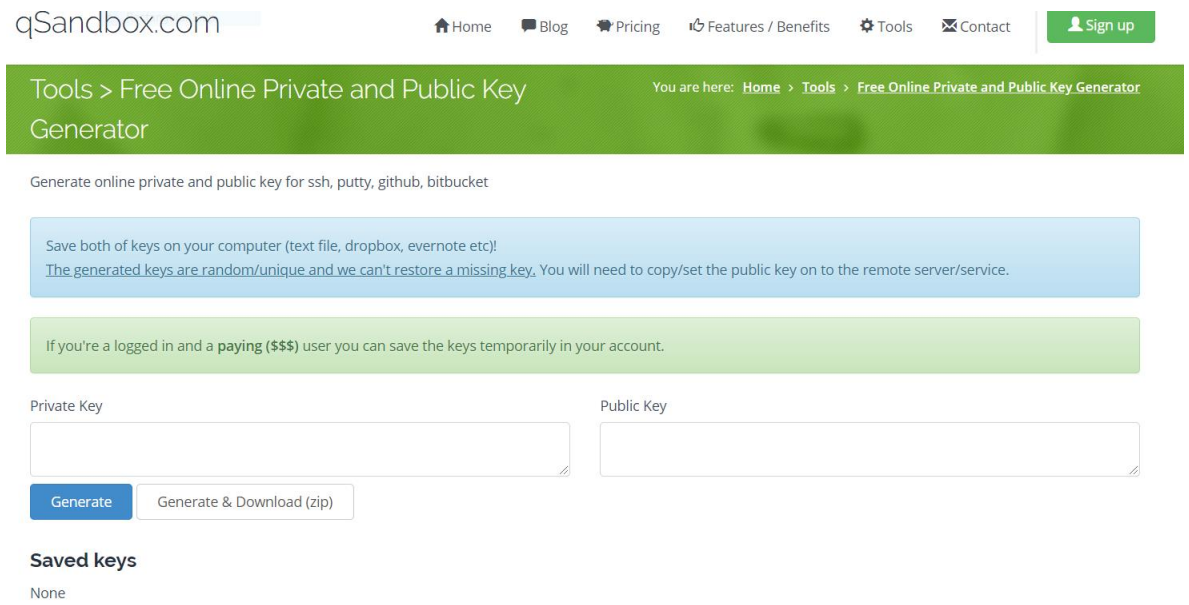
Failure of Trust:
Operational security of digital certs

- Symantec has a track record of fumbling certificate issuance, once even wrongly issuing one for google.com
- Google chrome, among other browsers removes Symantec as a root CA
- Trustico (Symantec reseller) emails 23,000 private keys for certs they issued, thus invalidating them (how did they get them?)
- All 23,000 certs are revoked within 24 hours

*Logo from Trustico website

Convenient insecurity

- Offer a service to generate public/private key pairs
- Do not delete the keys afterwards
- ???
- Profit



What is privacy?

- Concerns individuals and their expectations on how their data, behaviours, and interactions are recorded, utilized, and spread

- A useful definition: “Information self-determination”
  - A person gets to control information about themselves

  - Controls can include:
    - Who gets to see it
    - Who gets to use it
    - What they can use it for
    - Who they can give it to

Failure of Privacy: New York Taxi Database

- Database released for research
- Taxi numbers and licence numbers pseudonymized
  - MD5 hash
  - Same input = Same result
- Taxi/Lic. numbers have structure
  - Results in reduced number of possible values
  - Brute force is feasible on 24 million numbers

https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn

Failure of Privacy:
New York Taxi Database

Taxi #	Lic. #
3A3D444BB	01001EDFD
…	…
…	…
ADE034523	B0BB321AA

DATABASE

1. Enumerate all values with structures:
5X55, XX555, XXX555, 5XXXXXX, 5XXXXXXX

2. Hash all values above with MD5

3. Compare results with database on left

How could we have prevented this?

- Was the problem lack of education?
- Could some processes have helped?
- Were the problems obvious?
- Were the right stakeholders involved?

Who are the adversaries?

- All systems are vulnerable to all manner of threats

- Adversary types:
  - Nature
  - Script kiddies
  - Crackers/Hackers
  - Organised Crime
  - Governments
  - Terrorists

- Who should we worry about most? Can we ignore anyone?

Threat Modelling

- Who is the adversary (the system may protect against many types)?
- What are they allowed to do? Or, what can't we prevent them from doing?
  - The adversary need not be malicious, he could merely be curious
- What do we want to prevent the adversary from doing or learning?
  - What is the adversary's aim, or, when does he win?
- The set of threats we want to protect against given this (set of) adversaries
  - When do we win?
  - When does the adversary win?

Terminology

- Assets: Things we want to protect, like:
  - Hardware
  - Software
  - Information

- Vulnerabilities
  - Weaknesses in a system that may be exploited
    - Example: Public facing email server without spam protection

Terminology

- Threats
  - Loss or damage to the system, its users, or operators
    - E.g. Proprietary source code being stolen and sold
  - The six major categories of threats:
    - Interception
    - Interruption
    - Modification
    - Fabrication
    - Repudiation
    - Epistemic

Terminology

- Attack
  - An action that exploits a vulnerability to carry out a threat
    - E.g. Hacking the company public facing email server to read emails to steal company trade-secrets
- Controls
  - Mitigating or removing a vulnerability
  - The control mitigates a vulnerability to prevent an attack and that defends against a threat
  - No system is perfect: Control vulnerabilities when discovered

Security Principles (pp. 15-18)

- Economy of mechanism: easy to understand, verify, and maintain
- Fail-safe defaults: conservative permissions and functionality
- Complete mediation: every access should be checked (again)
- Open design: no security by obscurity
- Separation of privilege: cooperation required to act, no single point of failure
- Least privilege: programs and users on bare minimum of access
- Least common mechanism: minimize shared means of access to resources
- Psychological acceptability: well designed UI that are intuitive and clear
- Work factor: comparable effort for the value of the resource
- Compromise recording: record failures and breaches

Common defence methods

- There are 5 common defence patterns:
  - Prevent
  - Deter
  - Deflect
  - Detect
  - Recover

  NB: Not all attacks can be prevented!

- Best practice to employ some form of all to get “defence in depth”

Defence tools of the trade

- Protect assets that can be
  - Hardware, software, data (PII, social graph, confidential information, etc.)

- Many forms of control
  - Cryptography
  - Software controls
  - Hardware controls
  - Physical controls
  - Policies and procedures

Cryptography

- Protects the data, making it unreadable by anyone without keys
- Authenticating users with digital signatures
- Authenticating transactions with cryptographic protocols
- Ensures the integrity of data against unauthorized modification

Software controls

- Passwords
- Sandboxes
- Virus scanners
- Source code versioning systems
- Software Firewalls
- Privacy enhancing technologies (PETs)


KeePass

Hardware controls

- Fingerprint readers
- Smart tokens
- Firewalls
- Intrusion detection systems

Physical controls

- Protecting against unauthorized physical access to hardware
- Locks
- Guards
- Off-site backups
- Not placing critical systems in natural disaster zones

Policies and procedures

- Non-technical means to protect against some type of attacks
- Disallow personal hotspot within work place
- Password rules
- Security training against social engineering attacks

Recap

- What is our goal in this course?
  - Identify security and privacy issues
  - Design systems that are more protective of security and privacy
- What is Security?
  - Confidentiality, Integrity, Availability, Authenticity
- What is Trust?
  - Assurance, Reliability/Resilience, Accountability
- What is Privacy?
  - Informational self-determination

Recap

- Who are the adversaries?
  - Threat modelling
  - Learn to think like an attacker
- Trade-offs
  - Security, Privacy, Performance, Cost
- Assets, vulnerabilities, threats, attacks and controls
  - You control a vulnerability to prevent an attack and block a threat
- Methods of defence
  - Cryptography, software controls, hardware controls, physical controls, policies and procedures

Network security: Networking Principles

COMPUTER SECURITY

TARIQ ELAHI

Some slides adapted from those by Markulf Kohlweiss, Myrto Arapinis, Kami Vaniea, and Roberto Tamassia

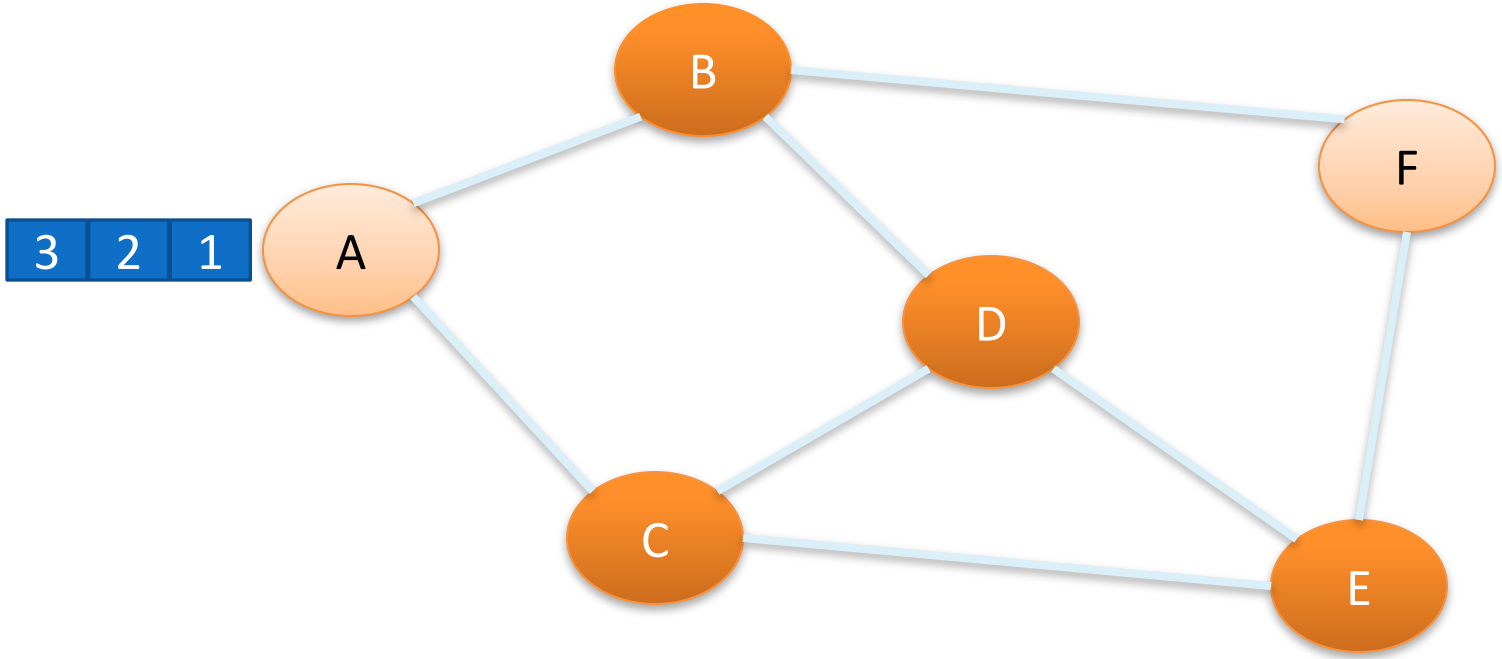
Network Communication

- Communication in modern networks is characterized by the following fundamental principles
  - Packet switching
  - Stack of layers
  - Encapsulation

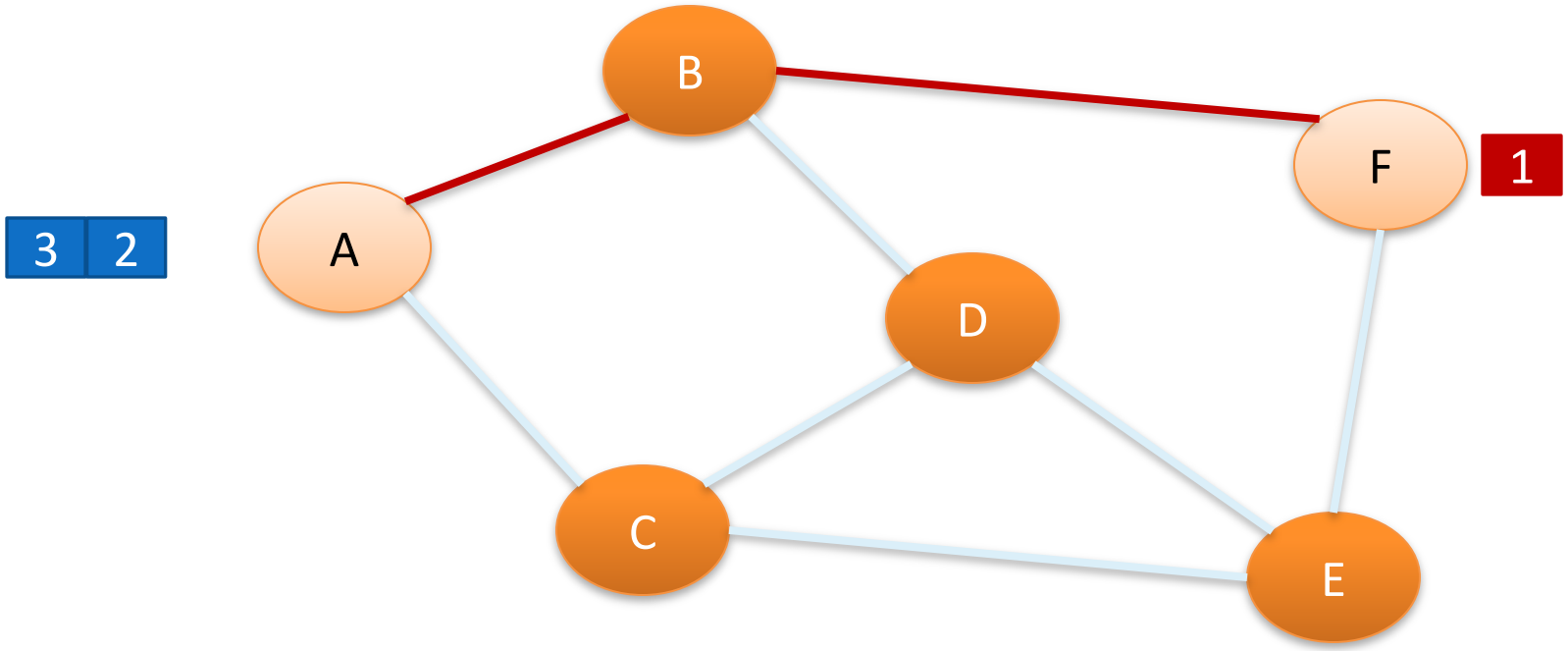
Packet Switching

- Data split into packets
- Each packet is
  - Transported independently through network
  - Handled on a best efforts basis by each device
- Packets may
  - Follow different routes between the same endpoints
  - Be dropped by an intermediate device and never delivered

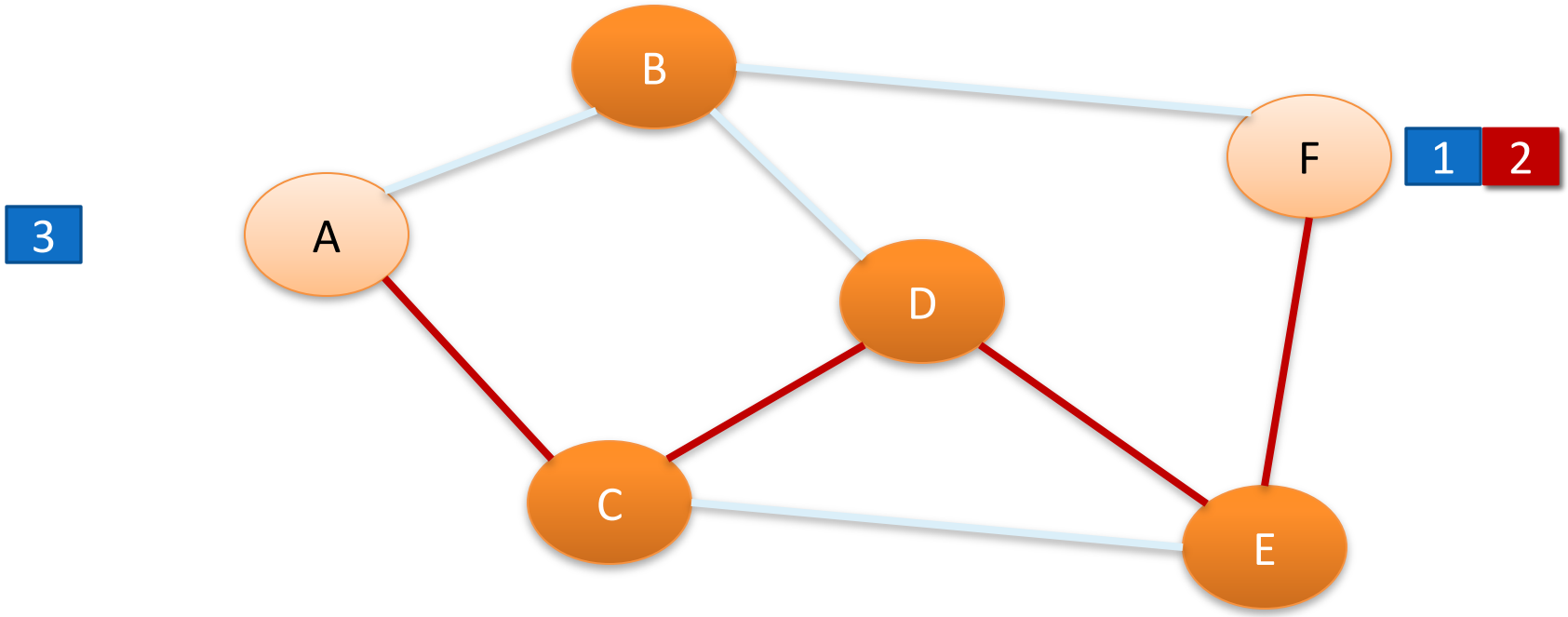
Packet Switching



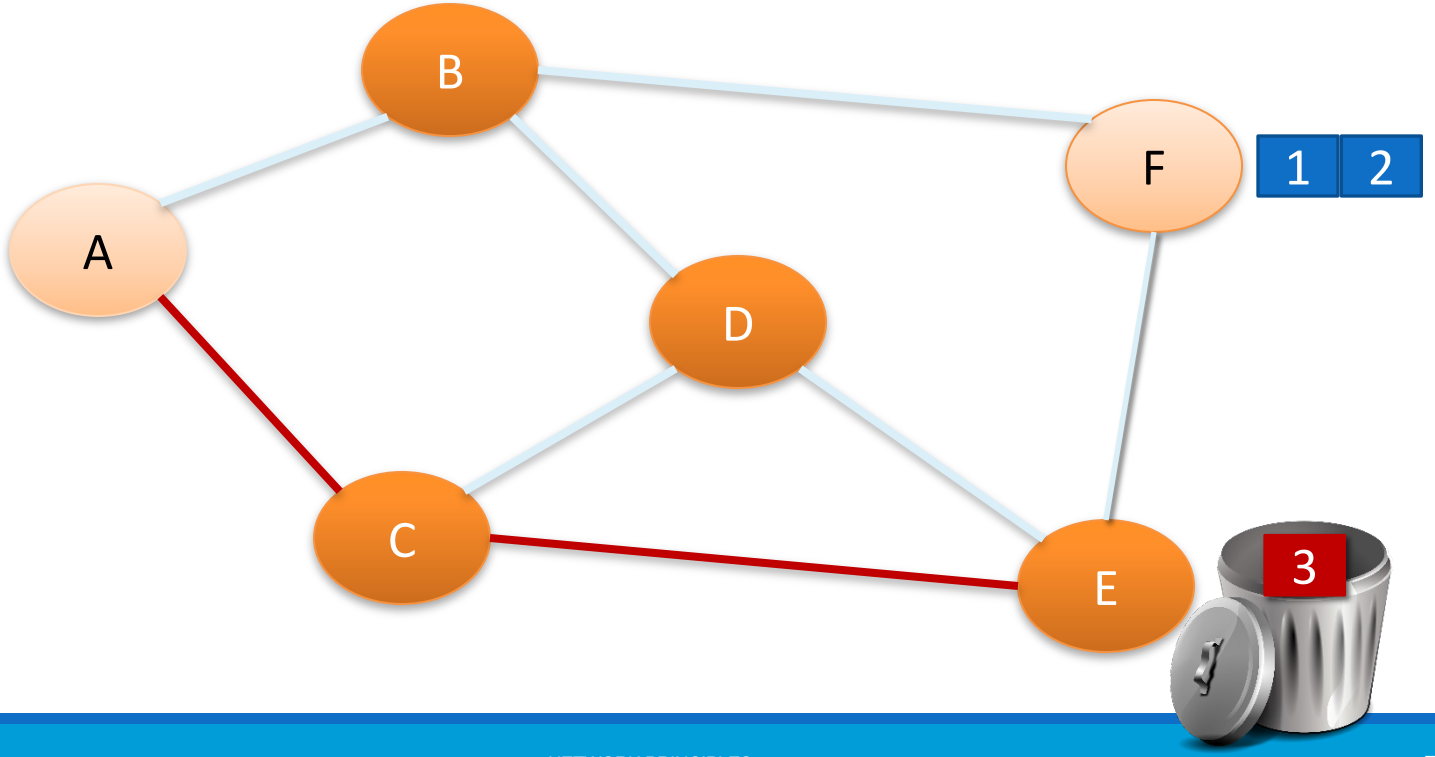
Packet Switching



Packet Switching



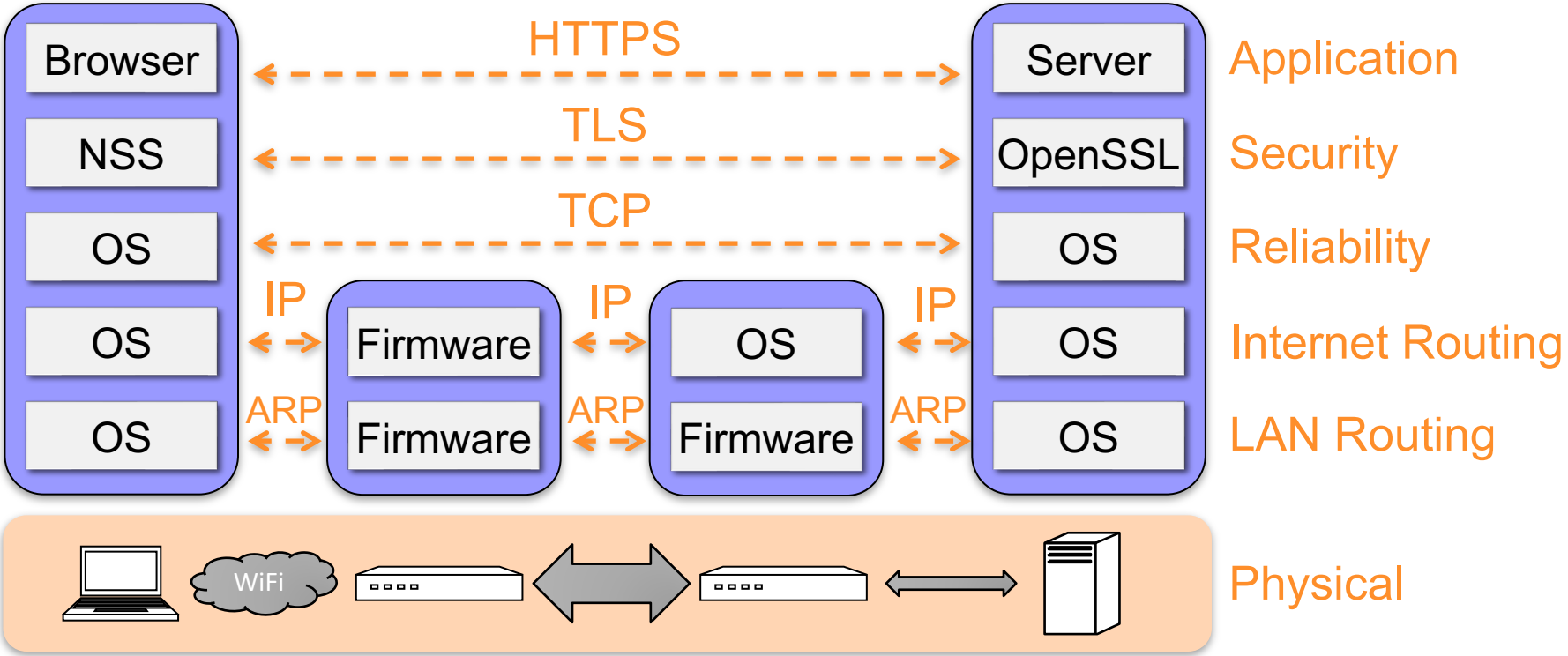
Packet Switching



Stack of Layers

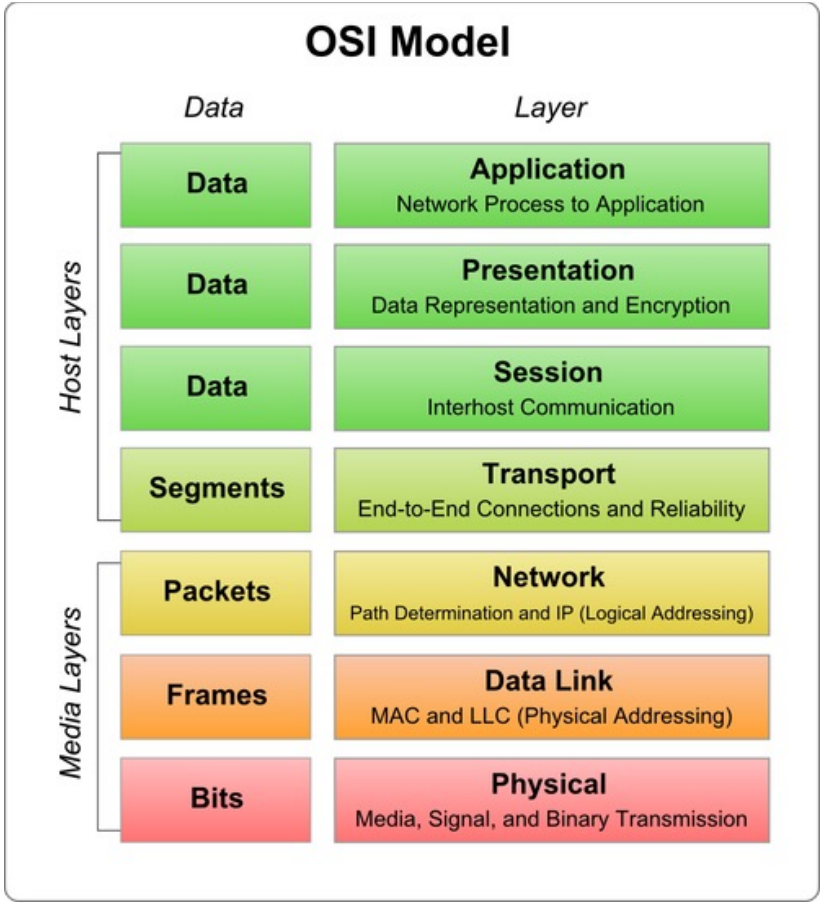
- Network communication models use a stack of layers
  - Higher layers use services of lower layers
  - Physical channel at the bottommost layer
- A network device implements several layers
- A communication channel between two devices is established for each layer
  - Actual channel at the bottom layer
  - Virtual channel at higher layers

Internet Stack (simplified)

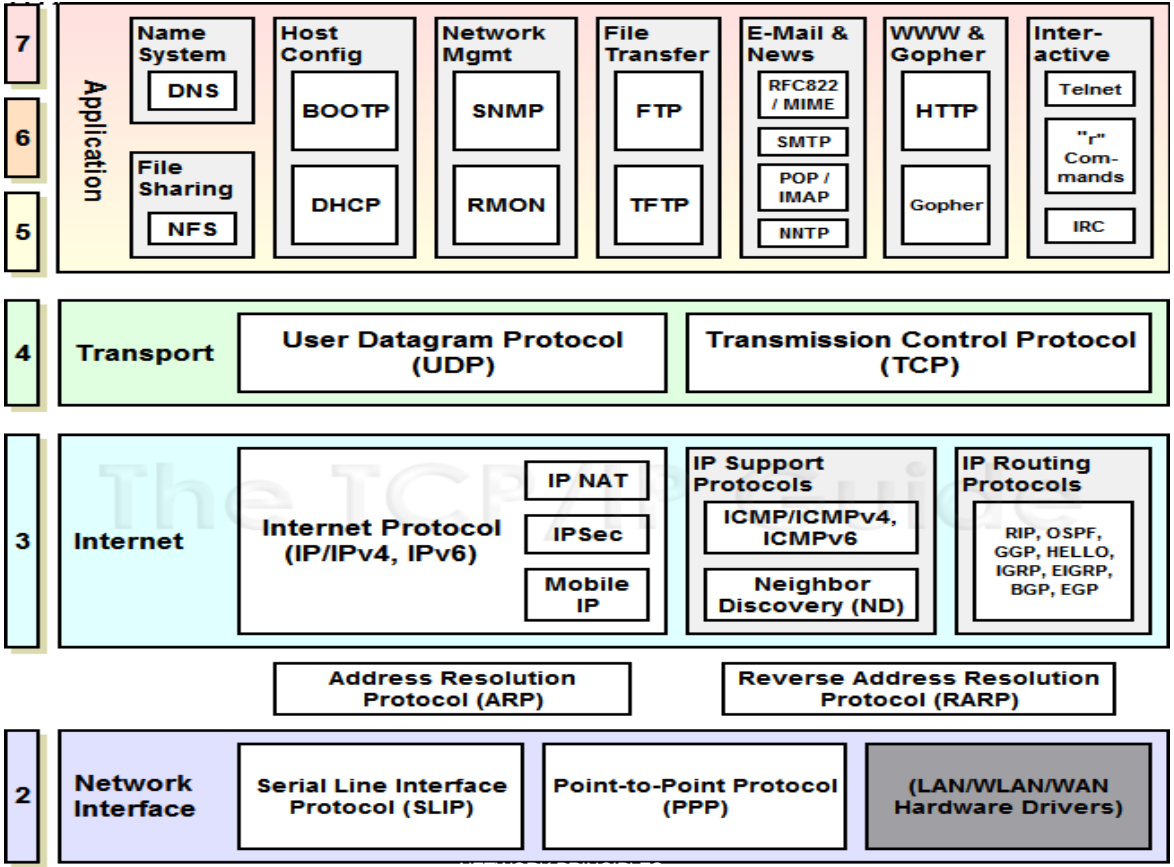


The OSI Model

- The OSI (Open System Interconnect) Reference Model is a network model consisting of seven layers
- Created in 1983, OSI is promoted by the International Standard Organization (ISO)

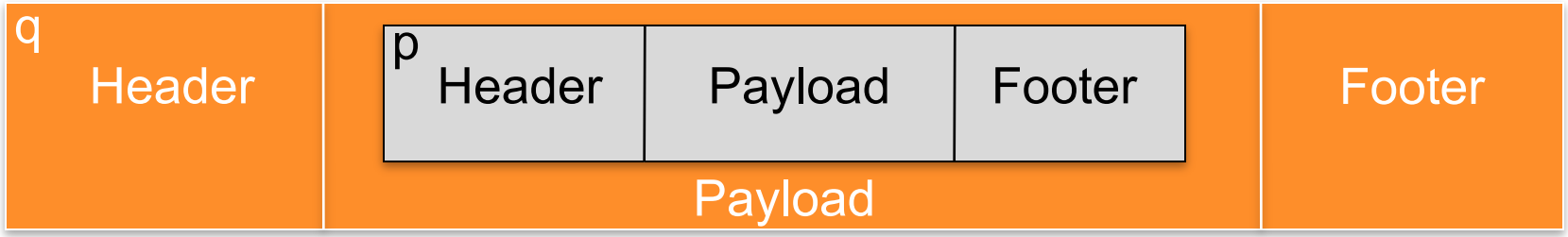


TCP/IP Model Mapped onto OSI

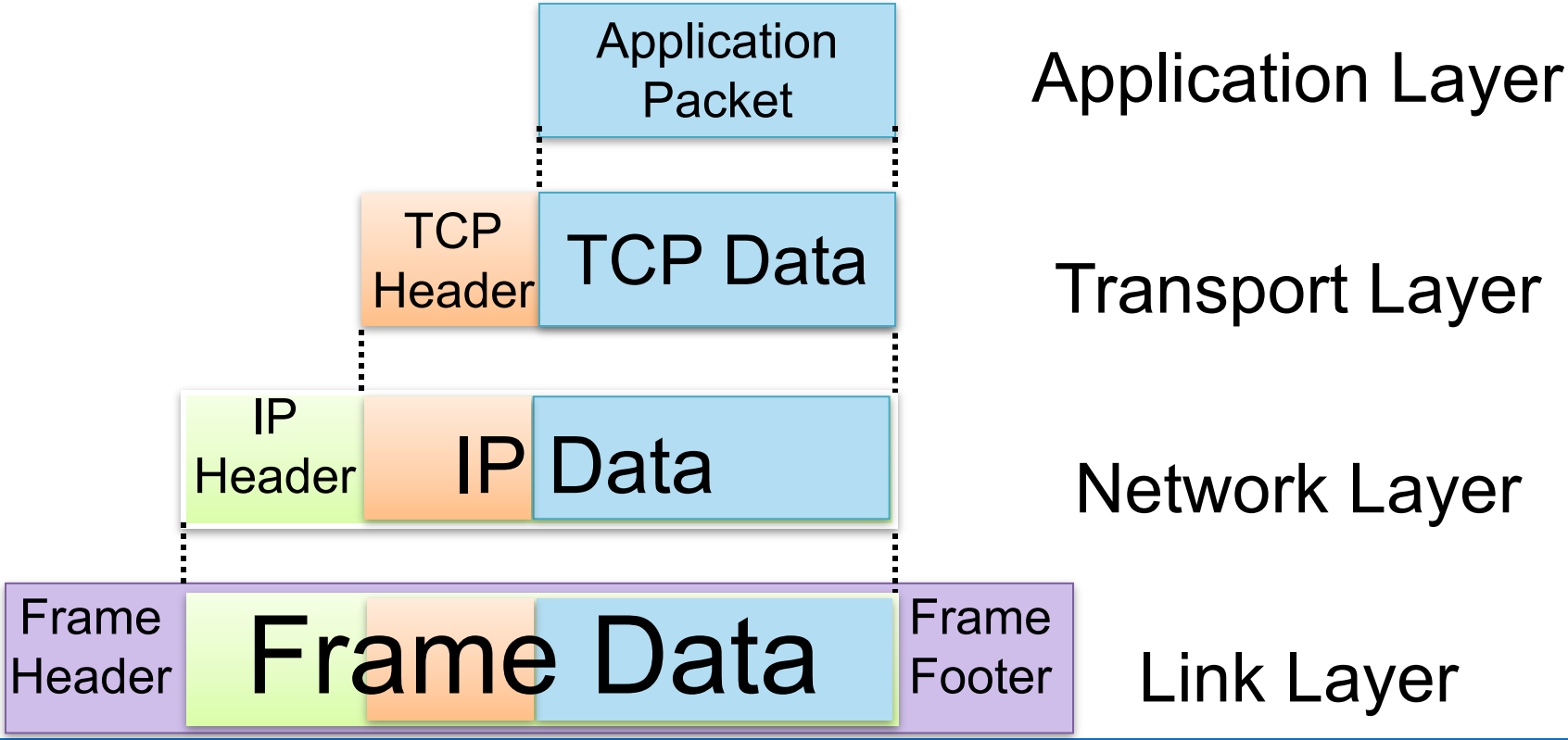


Encapsulation

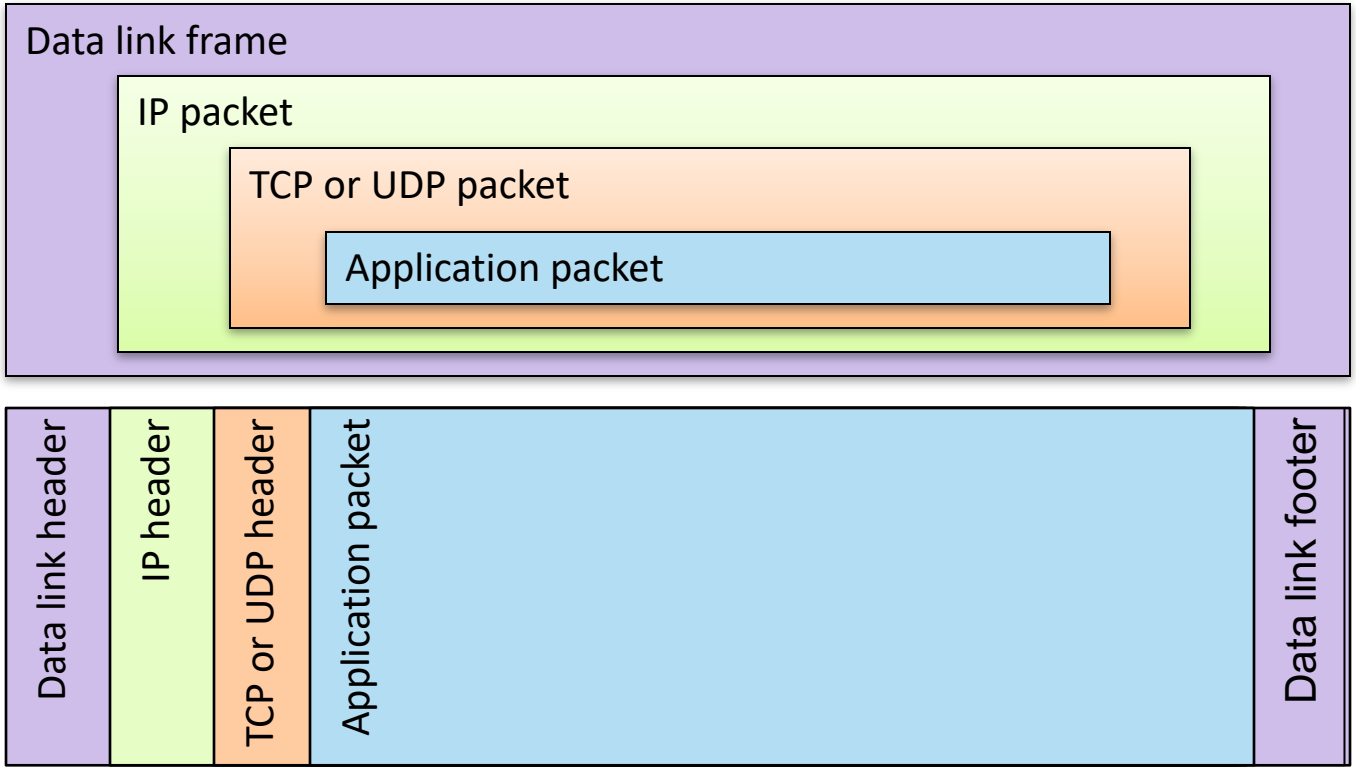
- A packet typically consists of
  - Control information: header and footer
  - Data: payload
- A protocol P uses the services of another protocol Q through encapsulation
  - A packet p of P is encapsulated into a packet q of Q
  - The payload of q is p
  - The control information of q is derived from that of p



Internet Packet Encapsulation



Internet Packet Encapsulation



Network Interfaces

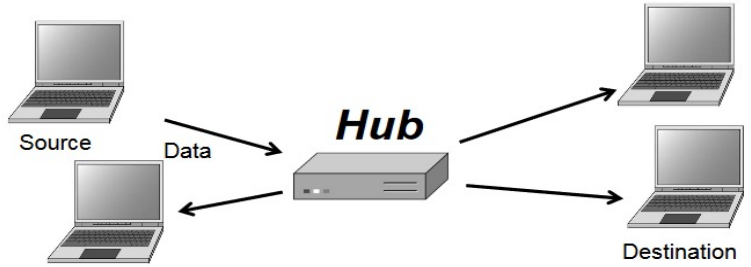
- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
  - DSL modem
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames

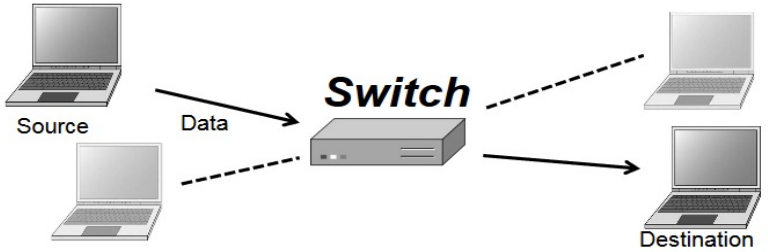
Media Access Control (MAC) Addresses

- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92, 00-0a-95 ??????
- The next three can be assigned by organizations as they please, with uniqueness being the only constraint

Switch

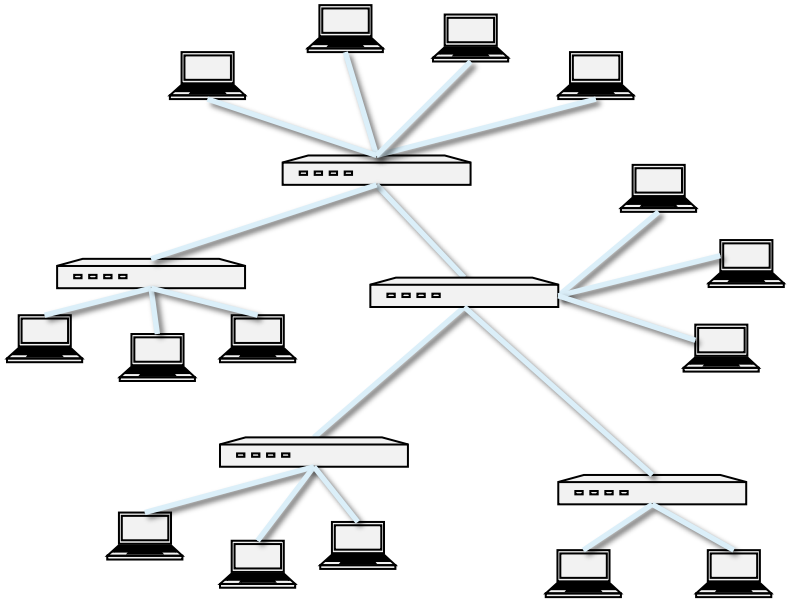
- A switch performs routing in a local area network
  - Operates at the link layer
  - Has multiple interfaces, each connected to a computer/segment
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer



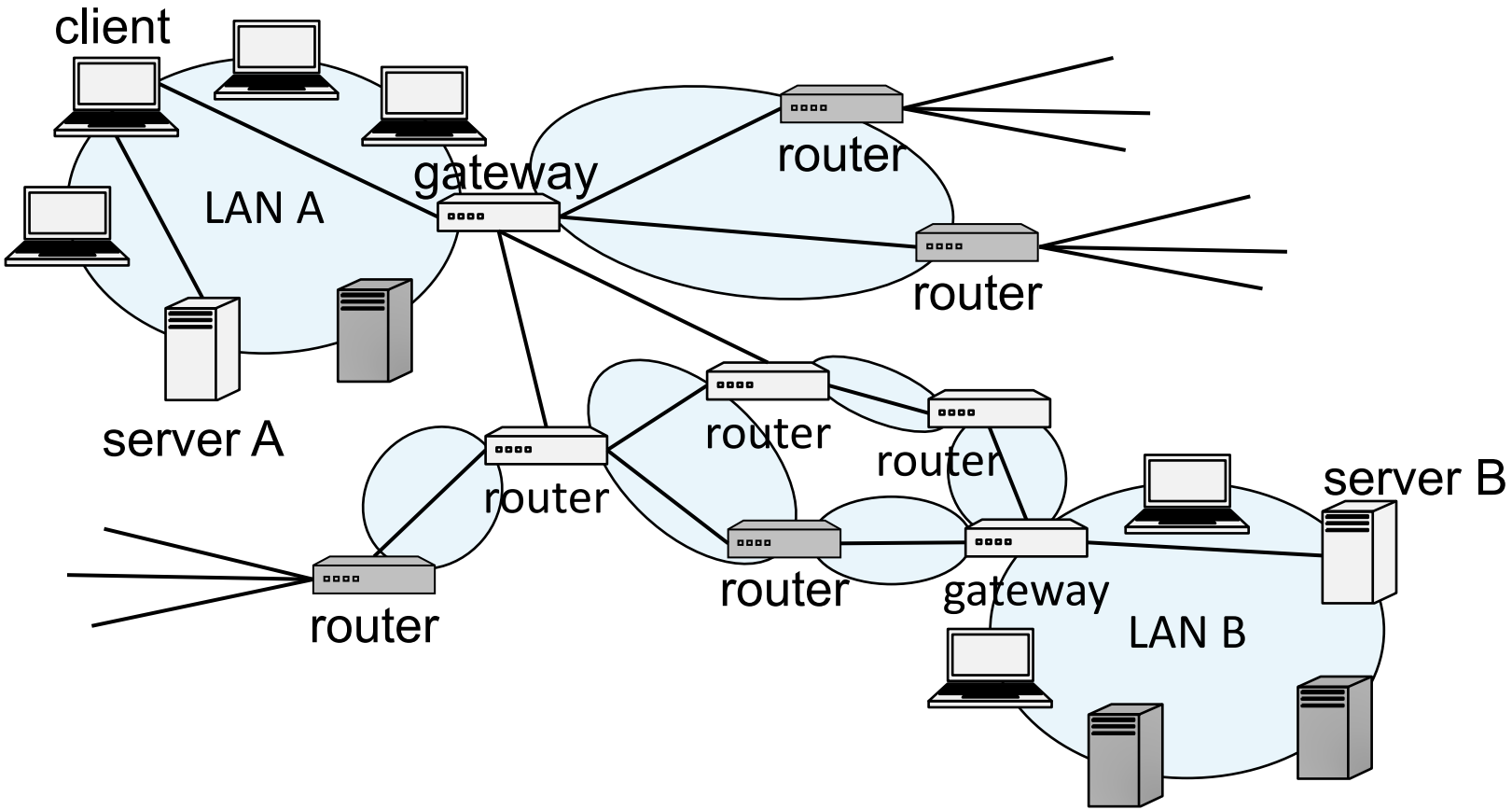


Combining Switches

- Switches can be arranged into a tree
- Each forwards frames for the MAC addresses of the machines in the segments (subtrees) connected to it
- Frames to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored

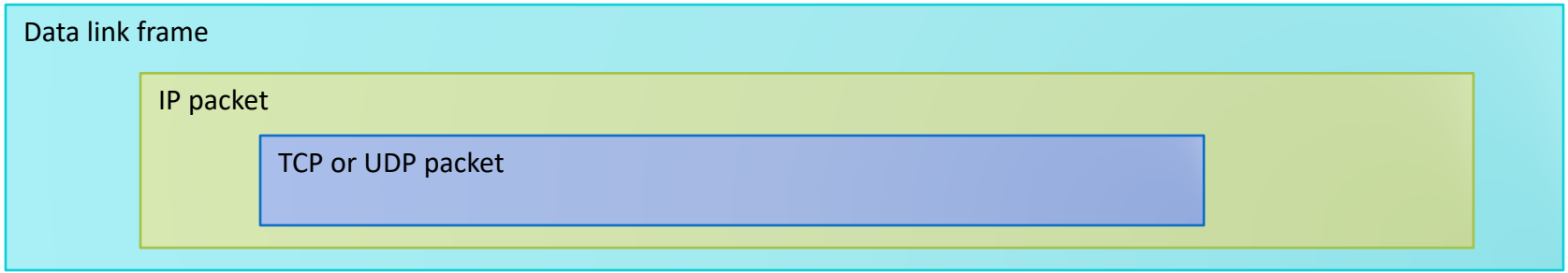


The Internet



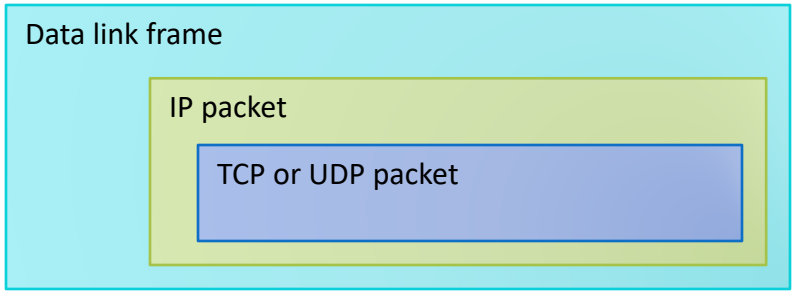
Internet Protocol (IP) Functions

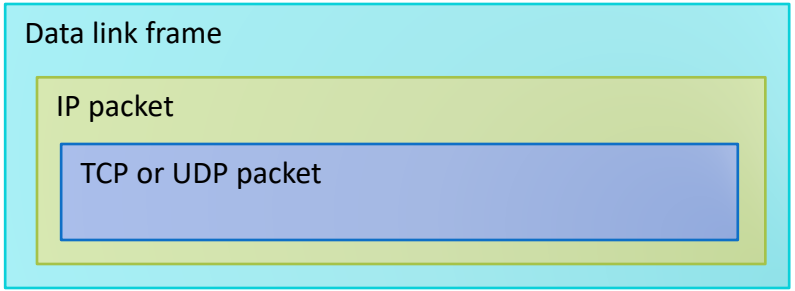
- Addressing: In order to deliver data, IP needs to be aware of where to deliver data to, and hence includes addressing systems
- Routing: IP might be required to communicate across networks, and communicate with networks not directly connected to the current network



Internet Protocol Functions

- Addressing: In order to deliver data, IP needs to be aware of where to deliver data to, and hence includes addressing systems
- Routing: IP might be required to communicate across networks, and communicate with networks not directly connected to the current network



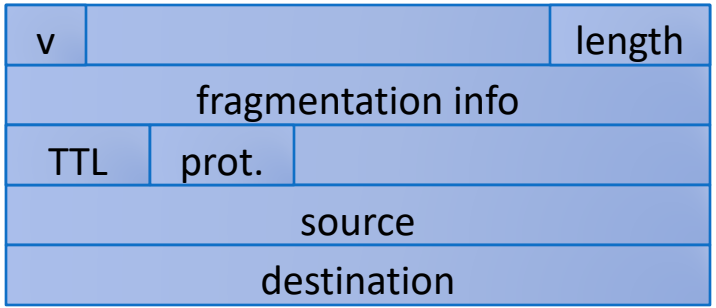


Fragmentation and Reassembly: IP packets are carried across networks which may have different maximum packet length.

IP Addresses and Packets

- IP addresses
  - IPv4: 32-bit addresses
  - IPv6: 128-bit addresses
- Address subdivided into network, subnet, and host
  - E.g., 128.148.32.110
- Broadcast addresses
  - E.g., 128.148.32.255
- Private networks
  - not routed outside of a LAN
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

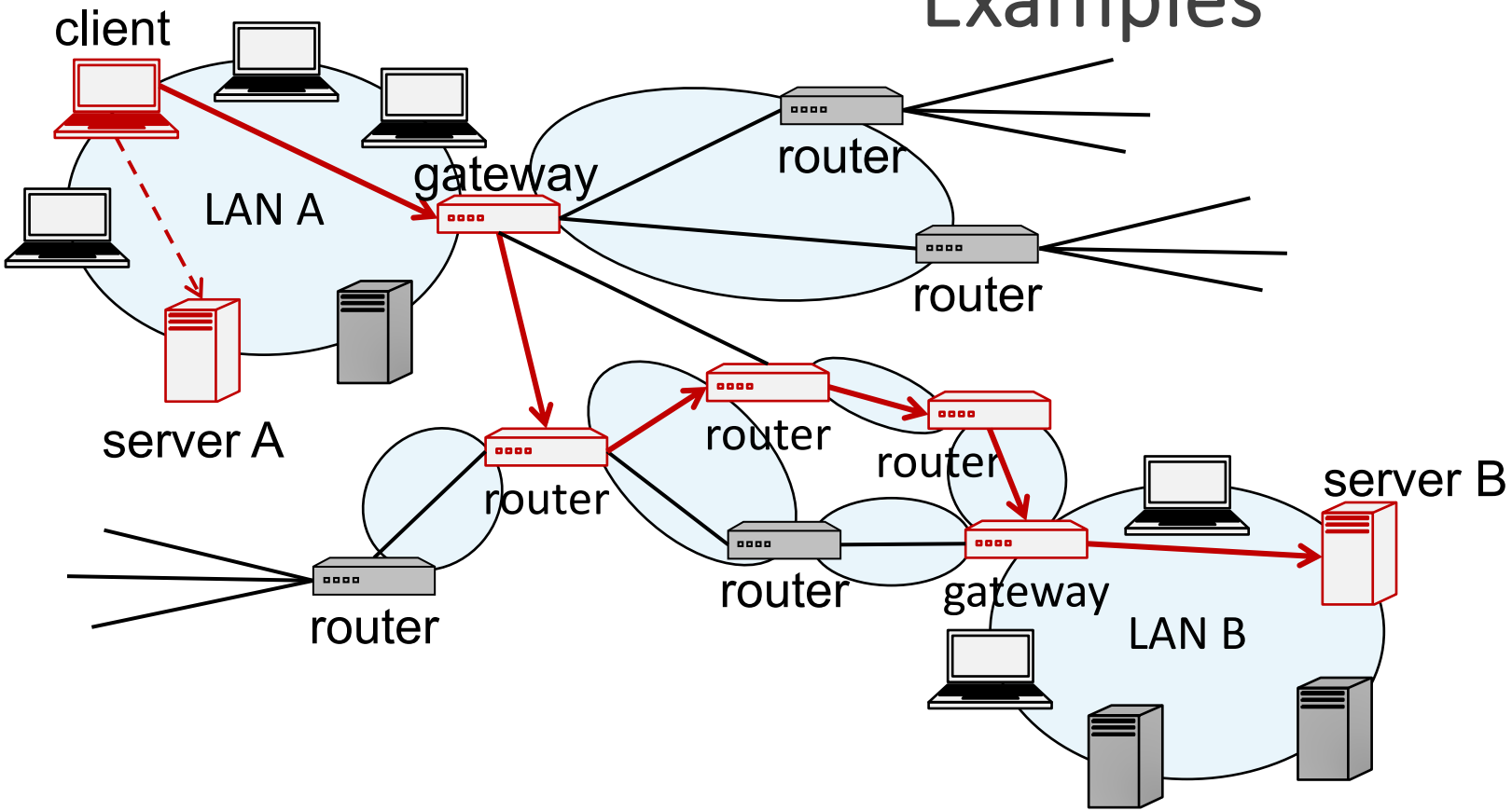
- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)



IP Routing

- A router bridges two or more networks
  - Operates at the network layer
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

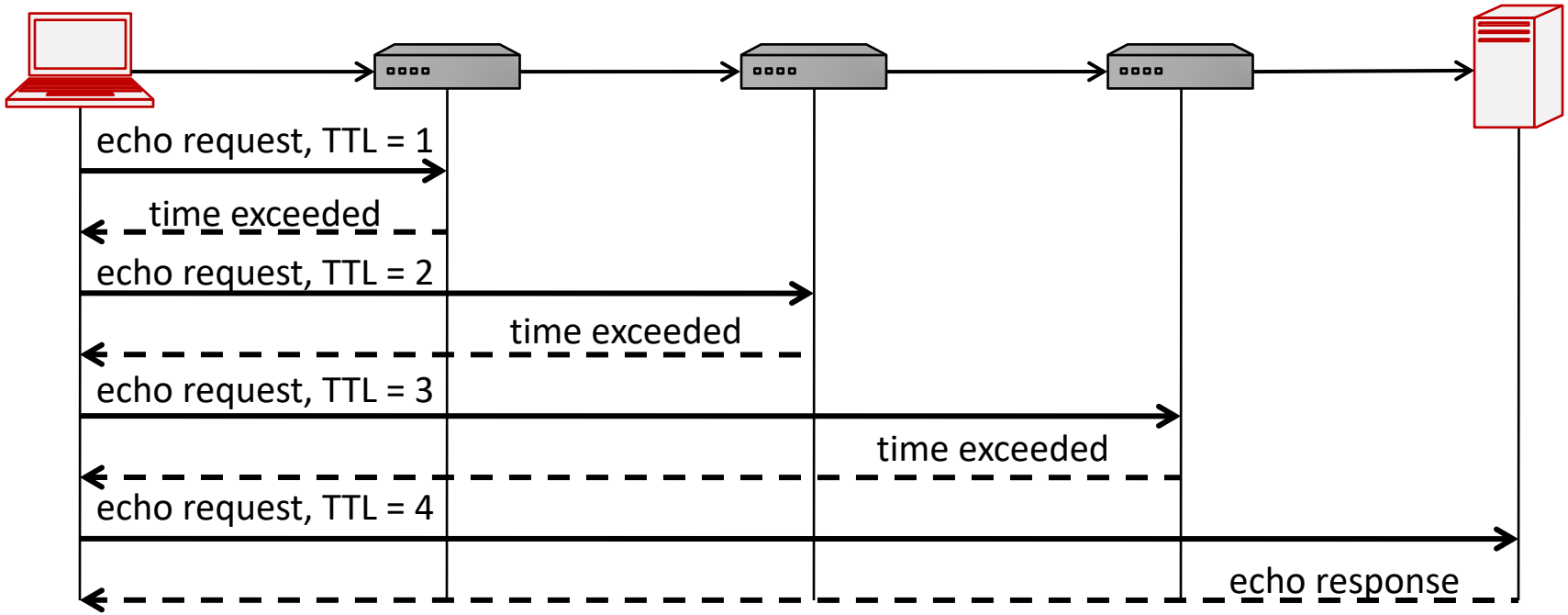
Routing Examples



Exploring Internet Routes

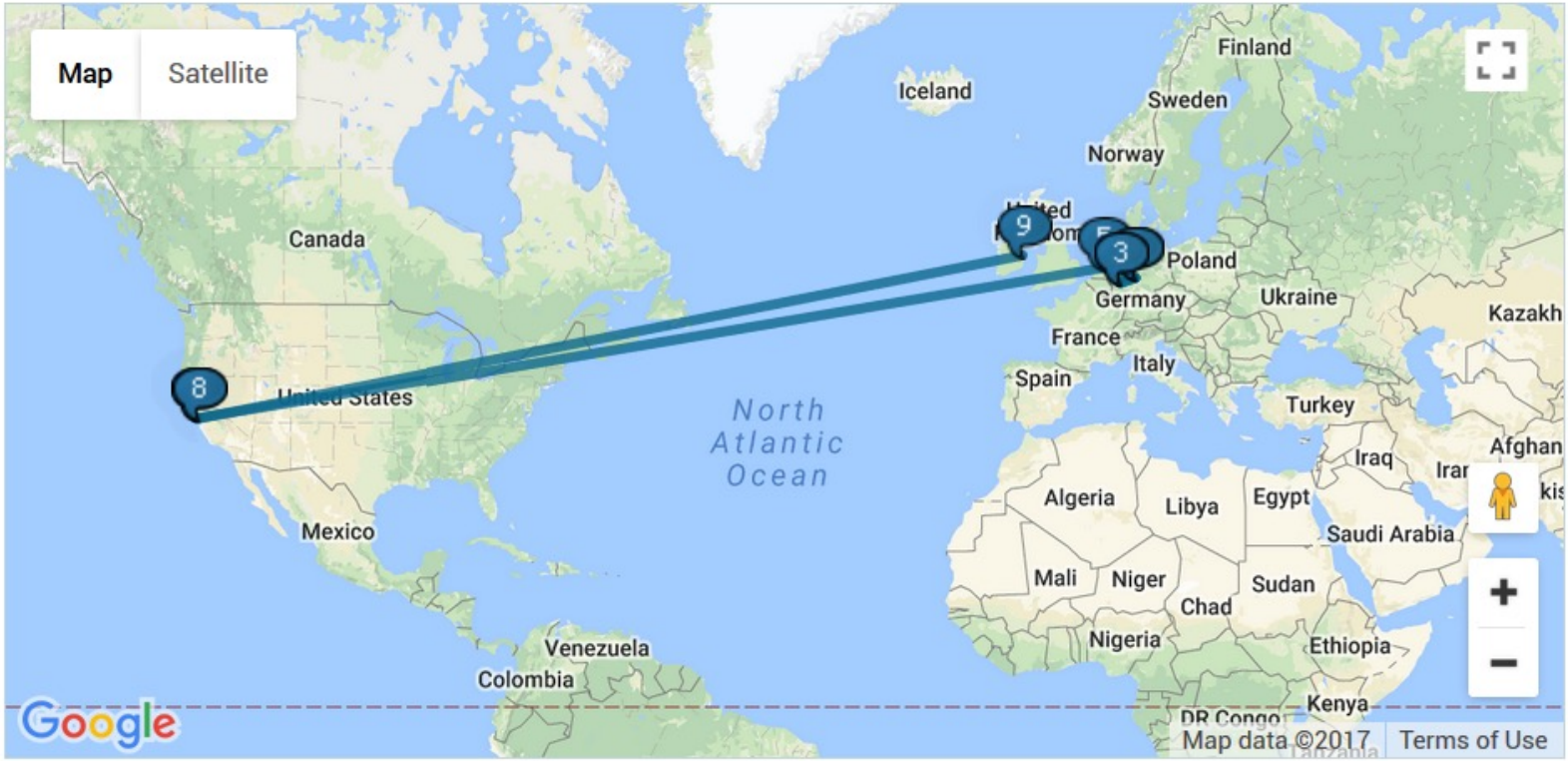
- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Simple messages encapsulated in single IP packets
  - Considered a network layer protocol
- Tools based on ICMP
  - Ping: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  - Traceroute: sends series ICMP packets with increasing TTL value to discover routes

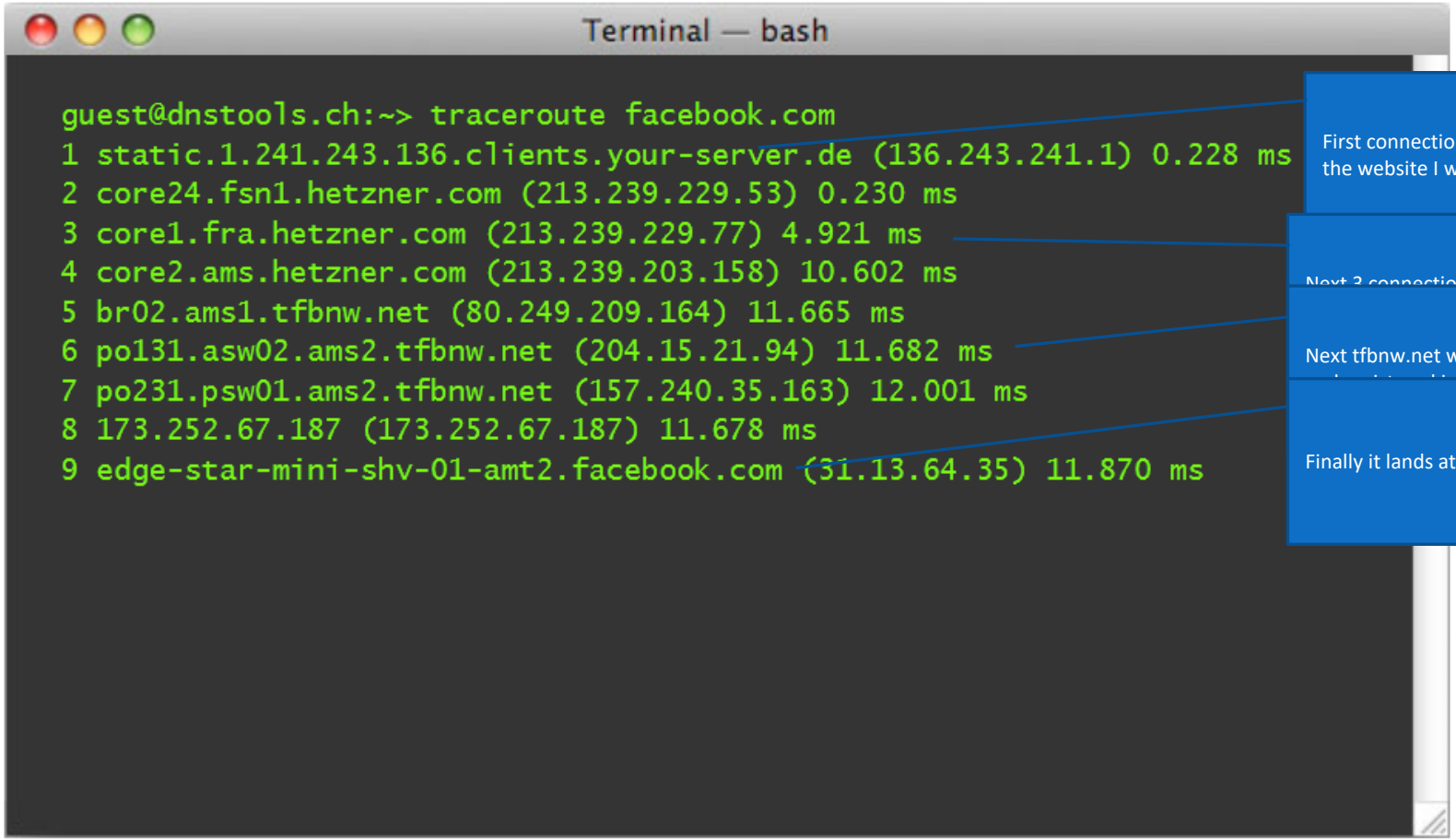
Traceroute


echo request, TTL = 1
time exceeded
echo request, TTL = 2
time exceeded
echo request, TTL = 3
time exceeded
echo request, TTL = 4
echo response

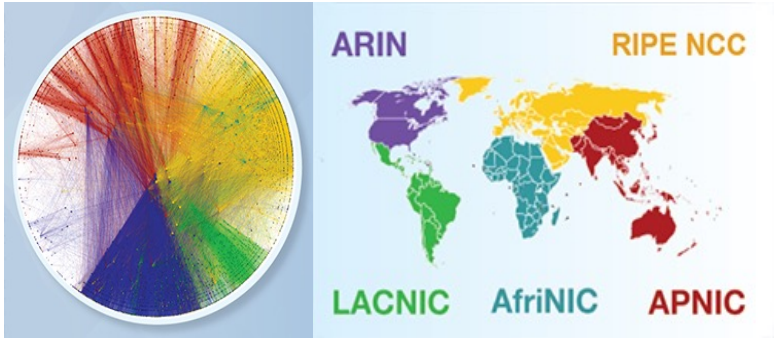
Host (Domain/IP) facebook.com **Trace**

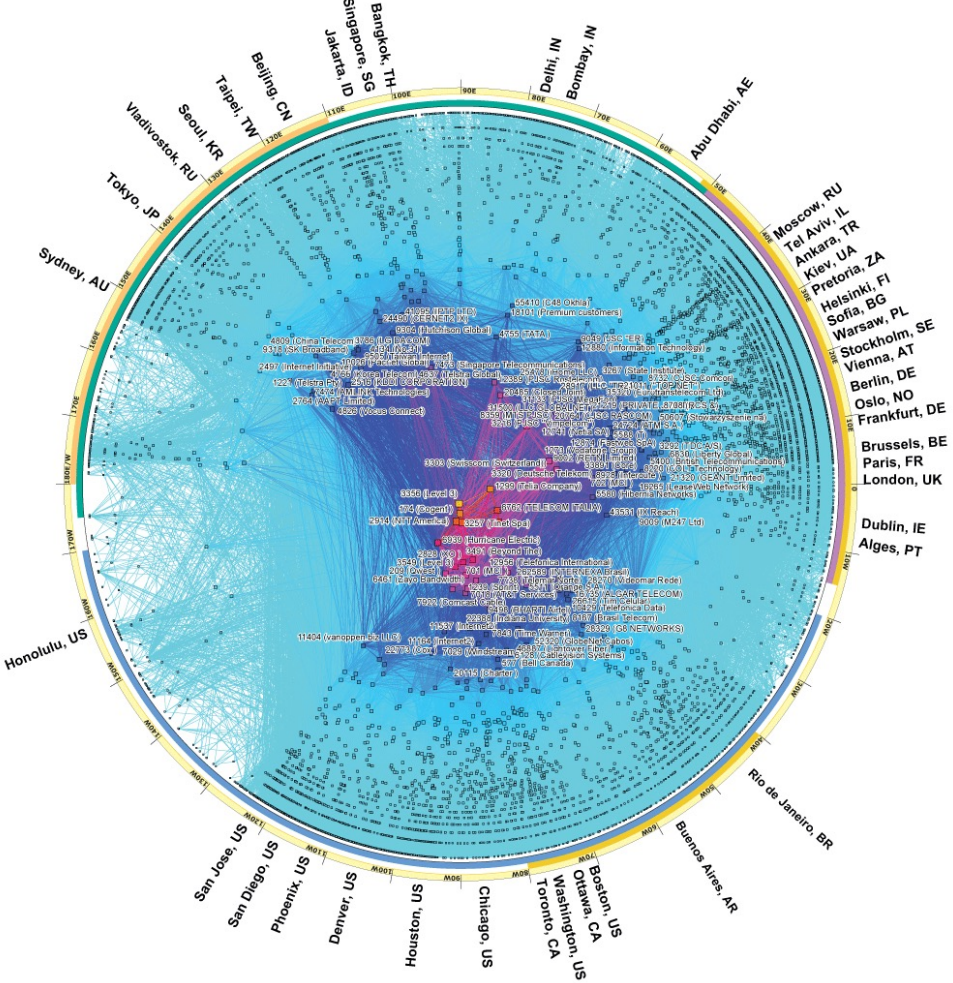
microsoft.com or bluewin.ch




Terminal — bash
guest@dnstools.ch:~> traceroute facebook.com
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.228 ms
2 core24.fsn1.hetzner.com (213.239.229.53) 0.230 ms
3 core1.fra.hetzner.com (213.239.229.77) 4.921 ms
4 core2.ams.hetzner.com (213.239.203.158) 10.602 ms
5 br02.ams1.tfbnw.net (80.249.209.164) 11.665 ms
6 po131.asw02.ams2.tfbnw.net (204.15.21.94) 11.682 ms
7 po231.psw01.ams2.tfbnw.net (157.240.35.163) 12.001 ms
8 173.252.67.187 (173.252.67.187) 11.678 ms
9 edge-star-mini-shv-01-amt2.facebook.com (31.13.64.35) 11.870 ms
First connection was in Germany (.de) where the website I was using is hosted.
Next 3 connections are to hetzner.com
Next tfbnw.net which is owned by Facebook
Finally it lands at Facebook

Caida's AS-level Internet Graph Jan 2017





https://www.caida.org/research/topology/as_core_network/pics/2017/ascore-2017-feb-ipv4-standalone-1000x1037.png

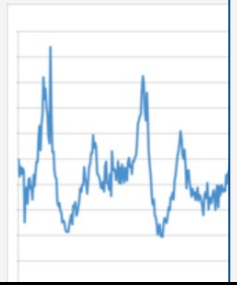
A real world example

How Syria Turned Off the Internet

29 Nov 2012 by Matthew Prince.

LinkedIn Like Tweet

Today, 29 November 2012, between 1026 and 1028 (UTC), all traffic from Syria to the rest of the Internet stopped. At CloudFlare, we witnessed the drop off. We've spent the morning studying the situation to understand what happened. The following graph shows the last several days of traffic coming to CloudFlare's network from Syria.



What Happened?

The Syrian Minister of Information is being reported as saying that the government did not disable the Internet, but instead the outage was caused by a cable being cut. Specifically: "It is not true that the state cut the Internet. The terrorists targeted the Internet lines, resulting in some regions being cut off." From our investigation, that appears unlikely to be the case.

To begin, all connectivity to Syria, not just some regions, has been cut. The exclusive provider

https://blog.cloudflare.com/how-syria-turned-off-the-internet/

THE VERGE TECH SCIENCE CULTURE CARS REVIEWS LONGFORM VIDEO MORE

US & WORLD

85

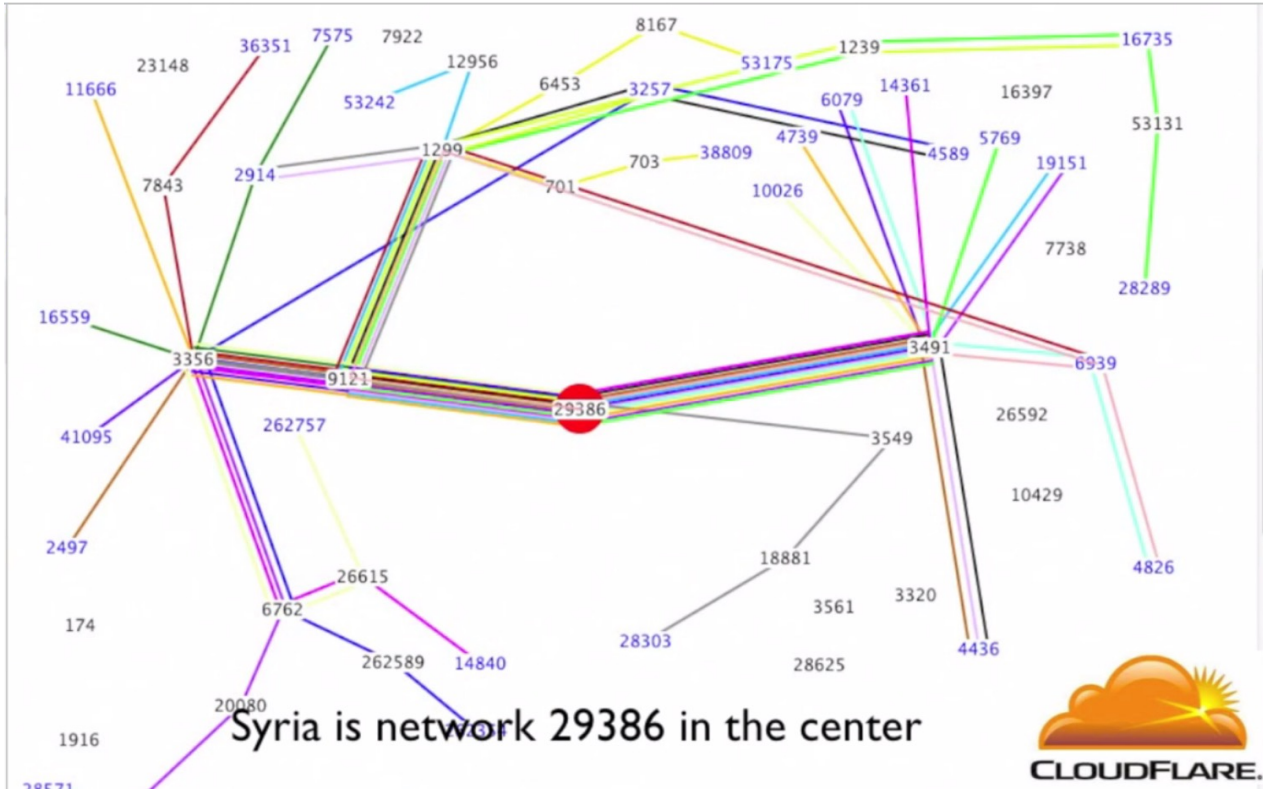
NSA was responsible for 2012 Syrian internet blackout, Snowden says

An elite hacking unit broke a router

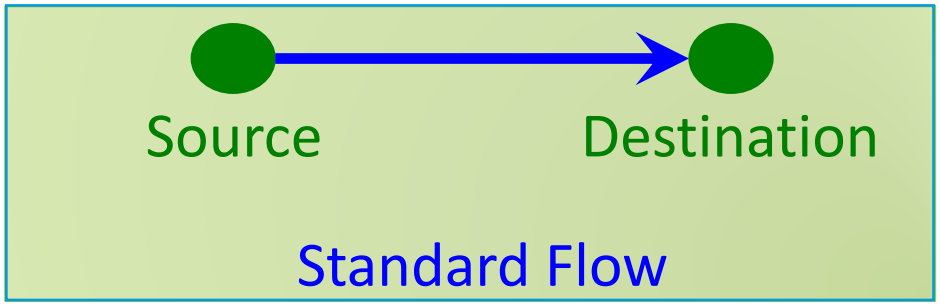
By Jacob Kastrenakes | @jake_k | Aug 13, 2014, 10:28am EDT

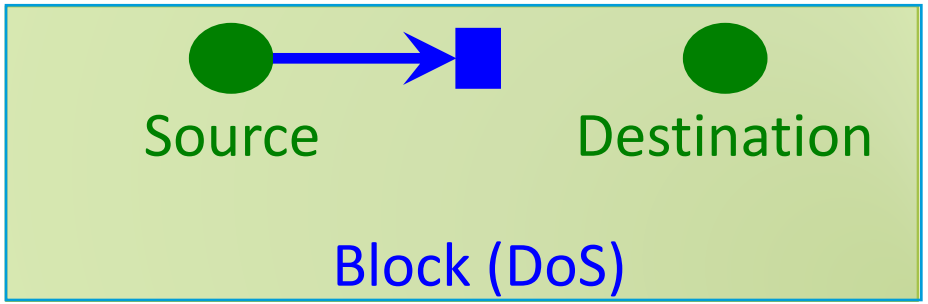
Syria going offline – November 2012

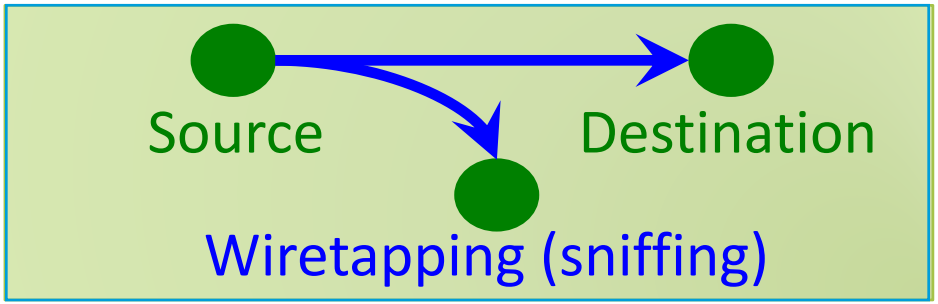
- Article: https://blog.cloudflare.com/how-syria-turned-off-the-internet/
- Going offline: https://www.youtube.com/watch?v=OZHKeYwnALc

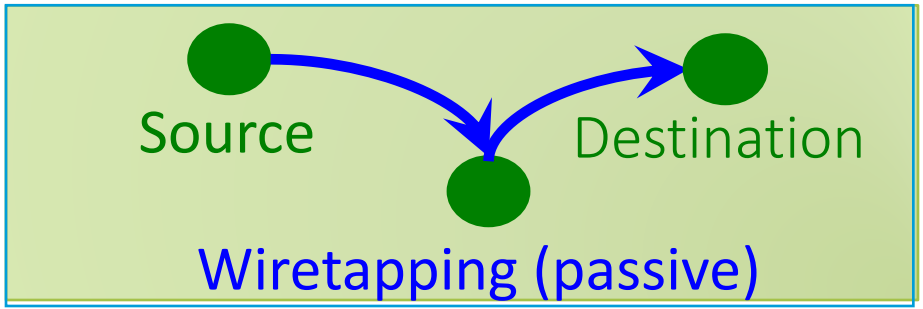


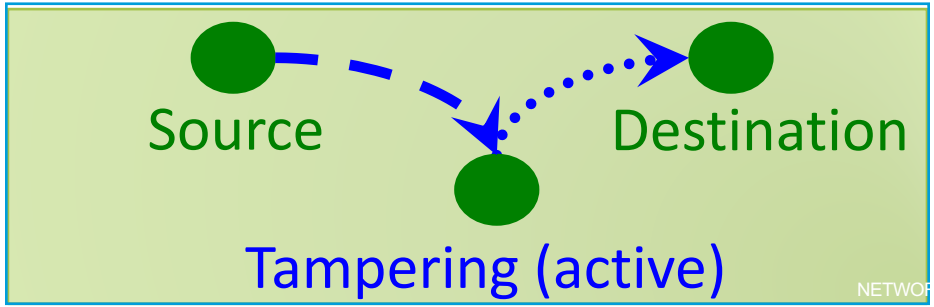
Network Attacks

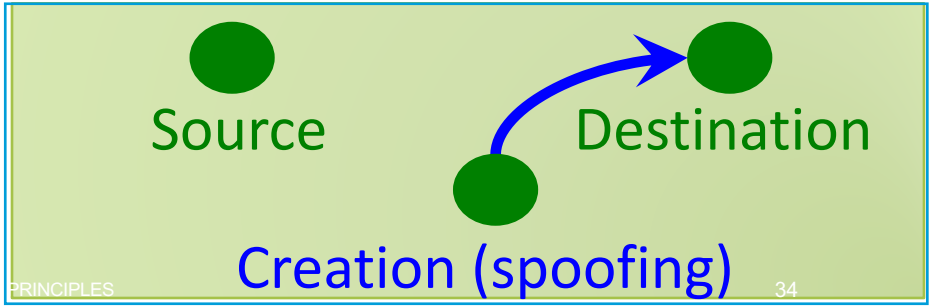






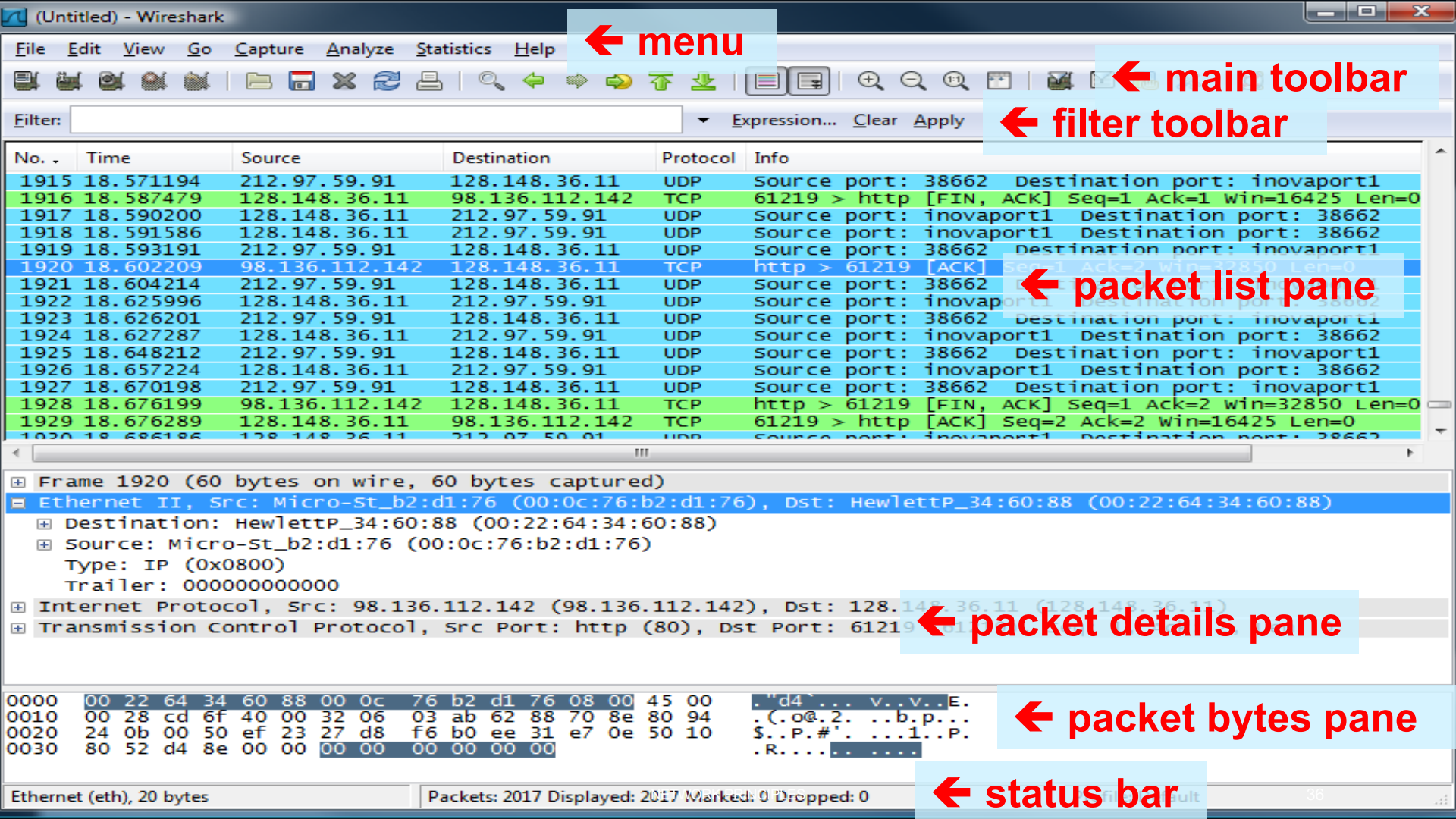






Wireshark

- Packet sniffer and protocol analyzer
- Captures and displays network packets for analysis
- Supports plugins
- Usually requires administrator privileges because of security risks associated with the program
- When run in promiscuous mode, captures traffic across the network
- Freely available on www.wireshark.org


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
menu
main toolbar
Filter:
Expression... Clear Apply
filter toolbar
No. Time Source Destination Protocol Info
1915 18.571194 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1916 18.587479 128.148.36.11 98.136.112.142 TCP 61219 > http [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
1917 18.590200 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1918 18.591586 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1919 18.593191 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1920 18.602209 98.136.112.142 128.148.36.11 TCP http > 61219 [ACK]
1921 18.604214 212.97.59.91 128.148.36.11 UDP Source port: 38662
1922 18.625996 128.148.36.11 212.97.59.91 UDP Source port: inovaport1
1923 18.626201 212.97.59.91 128.148.36.11 UDP Source port: 38662
1924 18.627287 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1925 18.648212 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1926 18.657224 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1927 18.670198 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1928 18.676199 98.136.112.142 128.148.36.11 TCP http > 61219 [FIN, ACK] Seq=1 Ack=2 Win=32850 Len=0
1929 18.676289 128.148.36.11 98.136.112.142 TCP 61219 > http [ACK] Seq=2 Ack=2 Win=16425 Len=0
packet list pane
Frame 1920 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76), Dst: HewlettP_34:60:88 (00:22:64:34:60:88)
Destination: HewlettP_34:60:88 (00:22:64:34:60:88)
Source: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76)
Type: IP (0x0800)
Trailer: 000000000000
Internet Protocol, Src: 98.136.112.142 (98.136.112.142), Dst: 128.
Transmission Control Protocol, Src Port: http (80), Dst Port: 6121
packet details pane
0000 00 22 64 34 60 88 00 0c 76 b2 d1 76 08 00 45 00 ."d4`... v..v..E.
0010 00 28 cd 6f 40 00 32 06 03 ab 62 88 70 8e 80 94 .(.o@.2. ..b.p...
0020 24 0b 00 50 ef 23 27 d8 f6 b0 ee 31 e7 0e 50 10 $..P.#'. ...1..P.
0030 80 52 d4 8e 00 00 00 00 00 00 00 00 .R...... ....
packet bytes pane
Ethernet (eth), 20 bytes
Packets: 2017 Displayed: 2017 Marked: 0 Dropped: 0
status bar

What We Have Learned

- Networking principles
  - Packet switching
  - Stack of layers
  - Encapsulation
- Network interfaces, MAC addresses, and Switches
- Internet Protocol (IP) Routing, autonomous systems
- Types of network attacks
- Traceroute and Wireshark tool

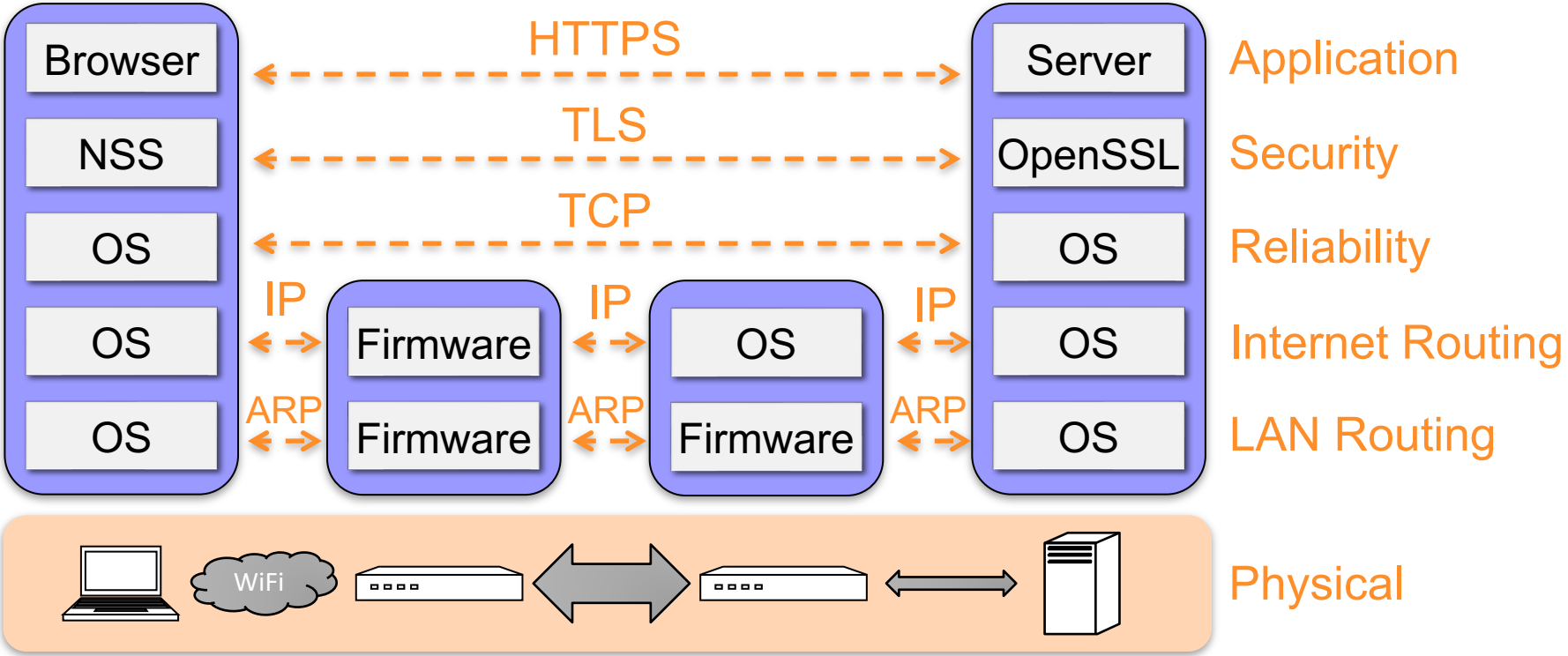
Network Security: ARP, IP, TCP, UDP

COMPUTER SECURITY

TARIQ ELAHI

Some slides adapted from those by Markulf Kohlweiss, Myrto Arapinis, Kami Vaniea, and Roberto Tamassia

Internet Stack (simplified)



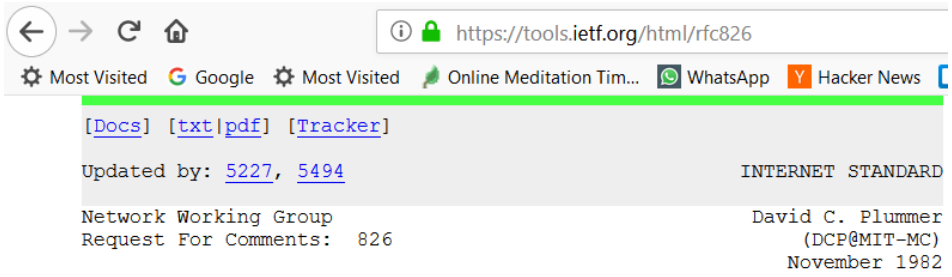
IP and MAC Addresses

- Devices on a local area network have
  - IP addresses (network layer)
  - MAC addresses (data link layer)
- IP addresses are used by high level protocols
- MAC addresses are used by low level protocols
- How to translate IP Addresses into MAC addresses?

The Problem:

The world is a jungle in general, and the networking game contributes many animals.

At nearly every layer of a network architecture there are several potential protocols that could be used.



For example, at a high level, there is TELNET and SUPDUP for remote login. Somewhere below that there is a reliable byte stream protocol, which might be CHAOS protocol, DOD TCP, Xerox BSP or DECnet. Even closer to the hardware is the logical transport layer, which might be CHAOS, DOD Internet, Xerox PUP, or DECnet.

Address Resolution Protocol (ARP)

- Connects the network layer to the data link layer
- Maps IP addresses to MAC addresses
- Based on broadcast messages and local caching
- Does not support confidentiality, integrity, or authentication
- Defined as a part of RFC 826 (IETF, Request For Comments)

ARP Messages

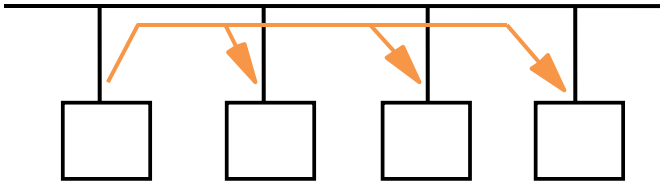
- ARP broadcasts requests of type

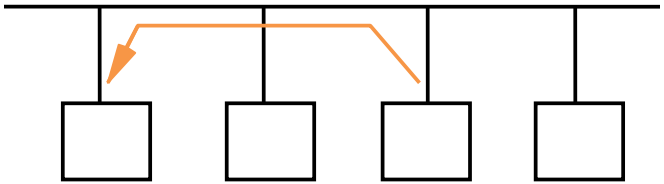
  who has <IP addressC >
  tell <IP addressA >

- Machine with <IP addressC> responds

  <IP addressC > is at <MAC address>

- Requesting machine caches response
- Network administrator configures IP address and subnet on each machine





ARP Cache

- The Linux, Windows and OSX command arp - a displays the ARP table

Internet Address	Physical Address	Type
128.148.31.1	00-00-0c-07-ac-00	dynamic
128.148.31.15	00-0c-76-b2-d7-1d	dynamic
128.148.31.71	00-0c-76-b2-d0-d2	dynamic
128.148.31.75	00-0c-76-b2-d7-1d	dynamic
128.148.31.102	00-22-0c-a3-e4-00	dynamic

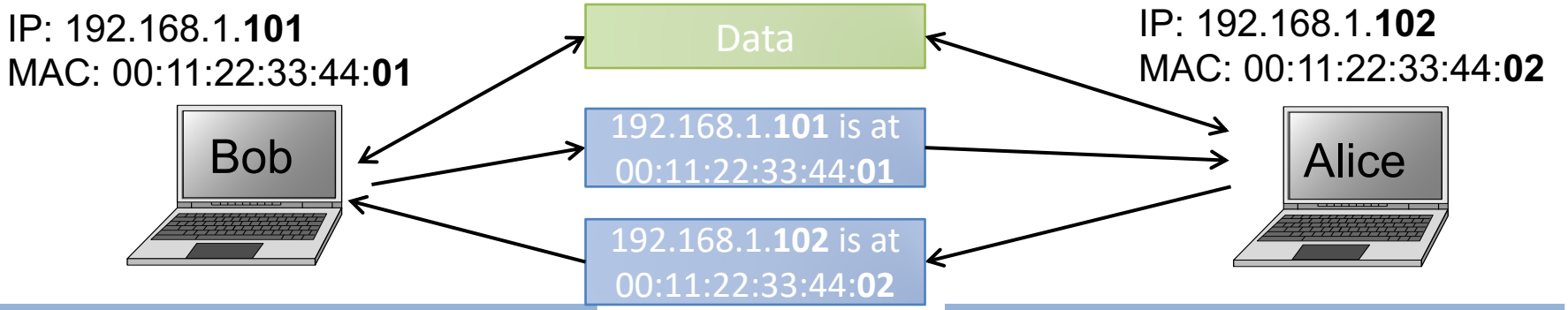
- Command arp –a –d flushes the ARP cache (Windows)
- ARP cache entries are stored for a configurable amount of time

ARP Cache Poisoning (aka ARP Spoofing)

- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

ARP Normal Operation

- Normal operation
  - Alice communicates with Bob

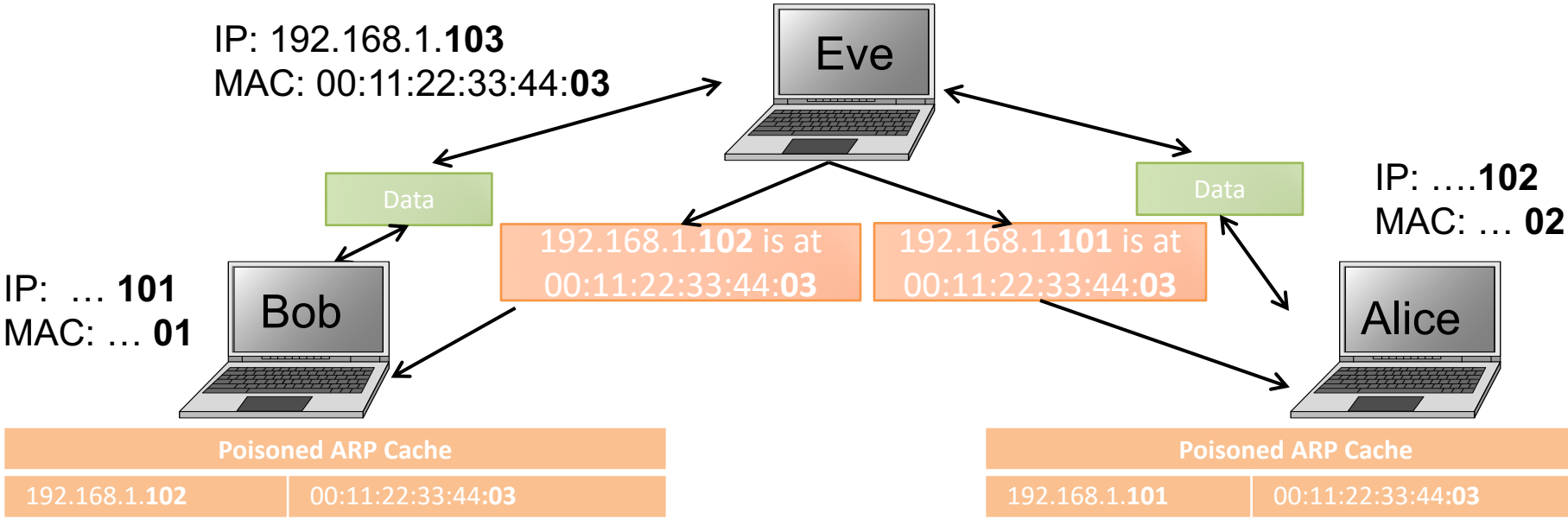


ARP Cache	
192.168.1.**102**	00:11:22:33:44:**02**

ARP Cache	
192.168.1.**101**	00:11:22:33:44:**01**

ARP Cache Poisoning Attack

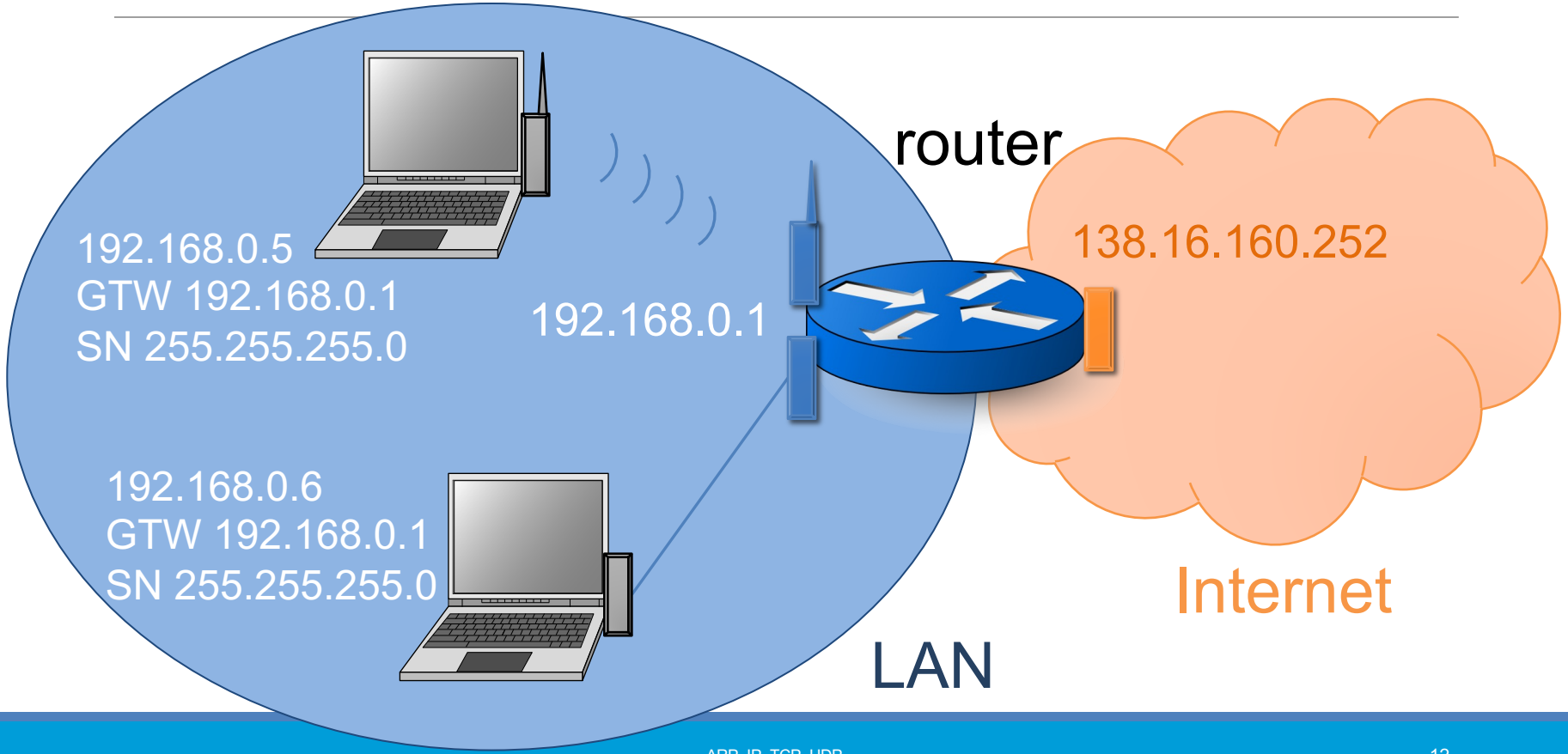
- Mal actor-in-the-middle attack (MITM)
  - ARP cache poisoning leads to eavesdropping



ARP Cache Poisoning (ARP Spoofing)

- Almost all ARP implementations are stateless
- An ARP cache updates every time that it receives an ARP reply
  - … even if it did not send any ARP request!
- Can “poison” ARP cache with gratuitous ARP replies
- Using static entries solves the problem but it is almost impossible to manage!

From the LAN to the Internet

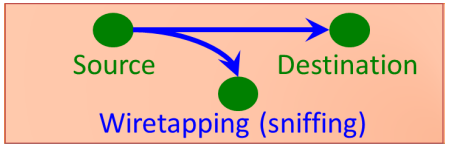


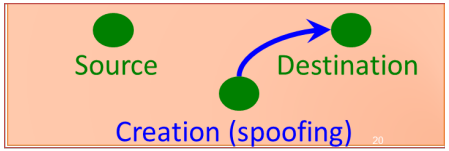
Edinburgh's IP Space

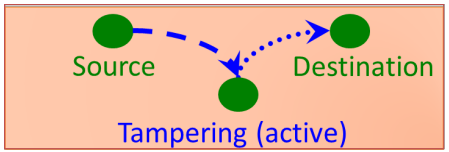
- Edinburgh is part of the autonomous system (AS786) of Jisc, for Joint Information Systems Committee, operate Janet
  - Class B network 129.215.0.0/16 (64K addresses)
- School of Informatics
  - 40 or so sub-networks, class C (/24) with 254 addresses or slightly larger
  - Server machines: 129.215.33.0/24
  - DICE desktop machines: 129.215.24.0/22
  - Laptops without a fixed IP address: 129.215.90.0/23

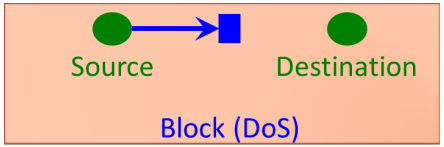
IP Vulnerabilities

- Unencrypted transmission
- No source authentication
  - Sender can spoof source address, making it difficult to trace packet back to attacker
- No integrity checking
  - Entire packet, header and payload, can be modified, enabling content forgeries, redirections, and mal actor-in-the-middle attacks
- No bandwidth constraints
  - Large number of packets can be injected into network to launch a denial-of-service attack
  - Broadcast addresses provide additional leverage









User Datagram Protocol

- UDP is a stateless, unreliable datagram protocol built on top of IP, i.e. it is at the transport layer
- UDP does not provide delivery guarantees or acknowledgments, which makes it efficient
- Can however distinguish data for multiple concurrent applications on a single host
- A lack of reliability implies applications using UDP must be ready to accept a fair amount of corrupted and lost data
  - Most applications built on UDP will suffer if they require reliability
  - VoIP, streaming video, and streaming audio all use UDP

Transmission Control Protocol

- Transport layer protocol for reliable data transfer, in-order delivery of messages and ability to distinguish multiple applications on same host
  - HTTP and SSH are built on top of TCP
- TCP is stateful: it keeps track of connection state in memory
- TCP packages a data stream into segments transported by IP
  - Order maintained by marking each packet with a sequence number
  - Every time TCP receives a packet, it sends out an acknowledgement (ACK) to indicate successful receipt of the packet
- TCP generally checks data transmitted by comparing a checksum of the data with a checksum encoded in the packet

Ports

- TCP (& UDP) supports concurrent applications on the same server
- Ports are 16 bit numbers identifying where data is directed
  - `>telnet 192.168.0.1:80` `https://example.co.uk:8080`
- The TCP header includes both a source and a destination port
- Ports 0 through 1023 are reserved for use by known protocols
  - E.g., HTTPS uses 443 and SSH uses 22
- Ports 1024 through 49151 are known as user ports, and are used for listening to connections

TCP Packet Format

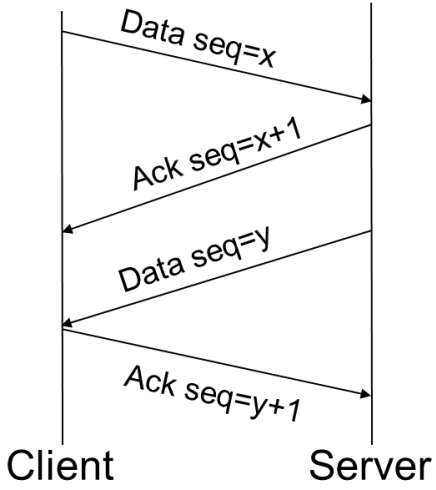
Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Source Port			Destination Port	
32	Sequence Number				
64	Acknowledgment Number				
96	Offset	Reserved	Flags	Window Size	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Payload				

TCP Data Transfer

- During connection initialization using the three way handshake, initial sequence numbers are exchanged
- The TCP header includes a 16 bit checksum of the data and parts of the header, including the source and destination
- ACKs (or lack thereof) and window size are used by

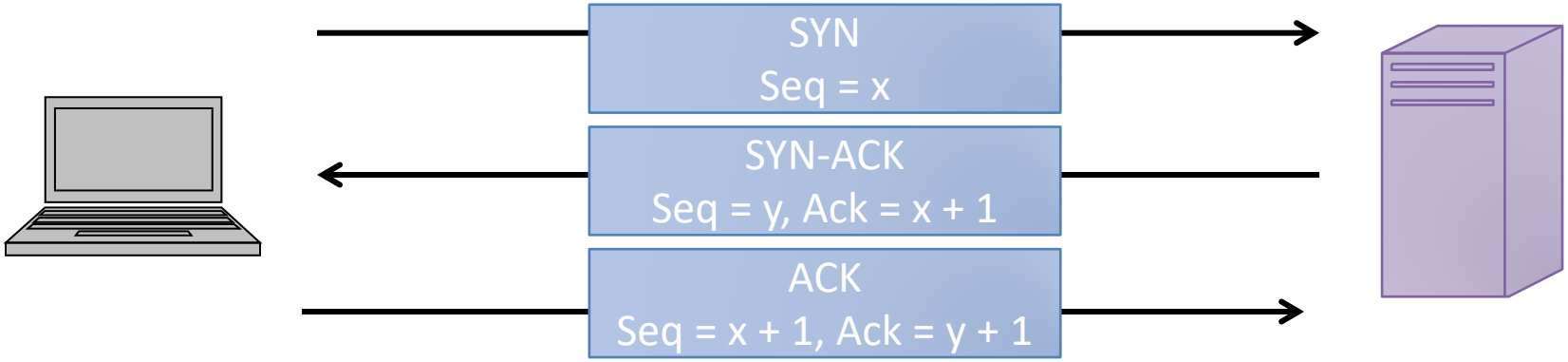
TCP to keep track of:

- packet loss
- network congestion
- flow control



Establishing TCP Connections

- TCP connections are established through a three-way handshake.
- The server generally is a passive listener, waiting for a connection request
- The client requests a connection by sending out a SYN packet
- The server responds by sending a SYN/ACK packet, acknowledging the connection
- The client responds by sending an ACK to the server, thus establishing connection

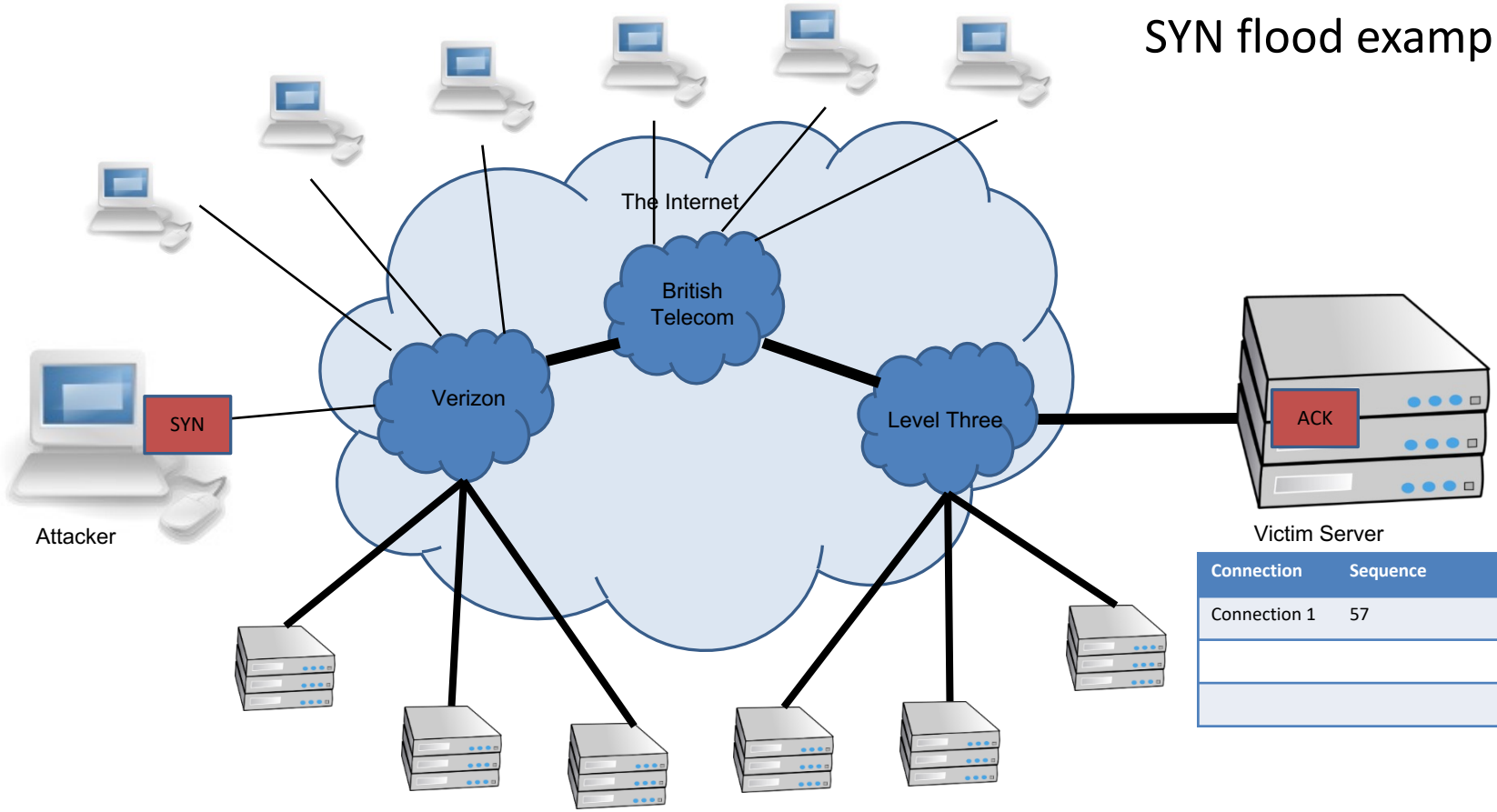


SYN Flooding

Send thousands of SYN requests to the victim

- Alice sends many SYN packets, without acknowledging any replies. Bob accumulates more SYN packets than he can handle (i.e. runs out of space in state table).

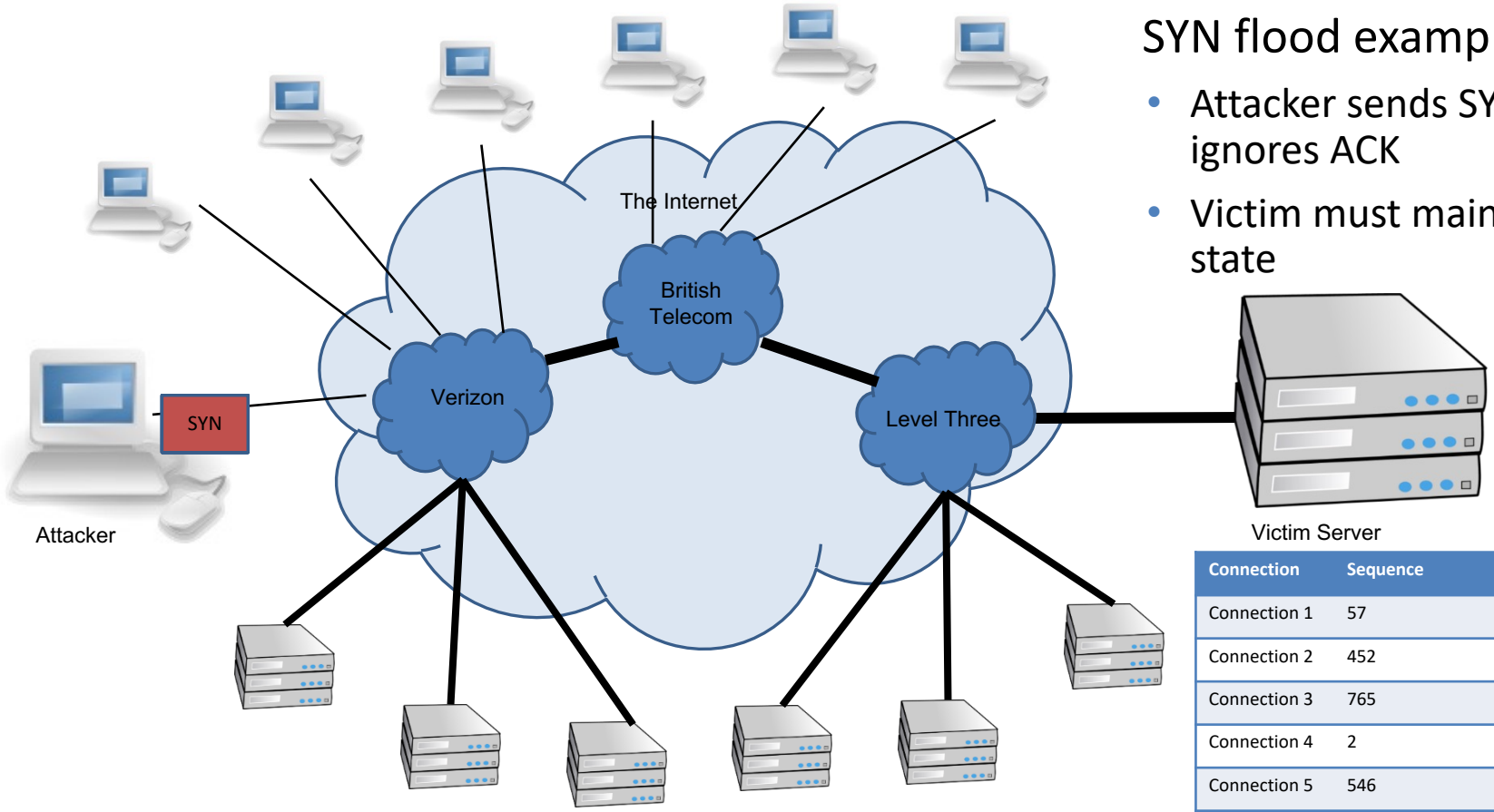
SYN flood example



Connection	Sequence	IP
Connection 1	57	1.1.1.1

SYN flood example

- Attacker sends SYN and ignores ACK
- Victim must maintain state



Connection	Sequence	IP
Connection 1	57	1.1.1.1
Connection 2	452	1.1.1.1
Connection 3	765	1.1.1.1
Connection 4	2	1.1.1.1
Connection 5	546	1.1.1.1
Connection 6	97	1.1.1.1
Connection 7	56	1.1.1.1
Connection 8	15	1.1.1.1

SYN Flooding

- Problems
  - Attribution – attacker uses their own IP which could be traced
  - Bandwidth – attacker uses their own bandwidth which is likely smaller than a server's
- Effective against a small target
  - Someone running a game server in their home
- Not effective against a large target
  - Company website

Spoofing: forged TCP packets

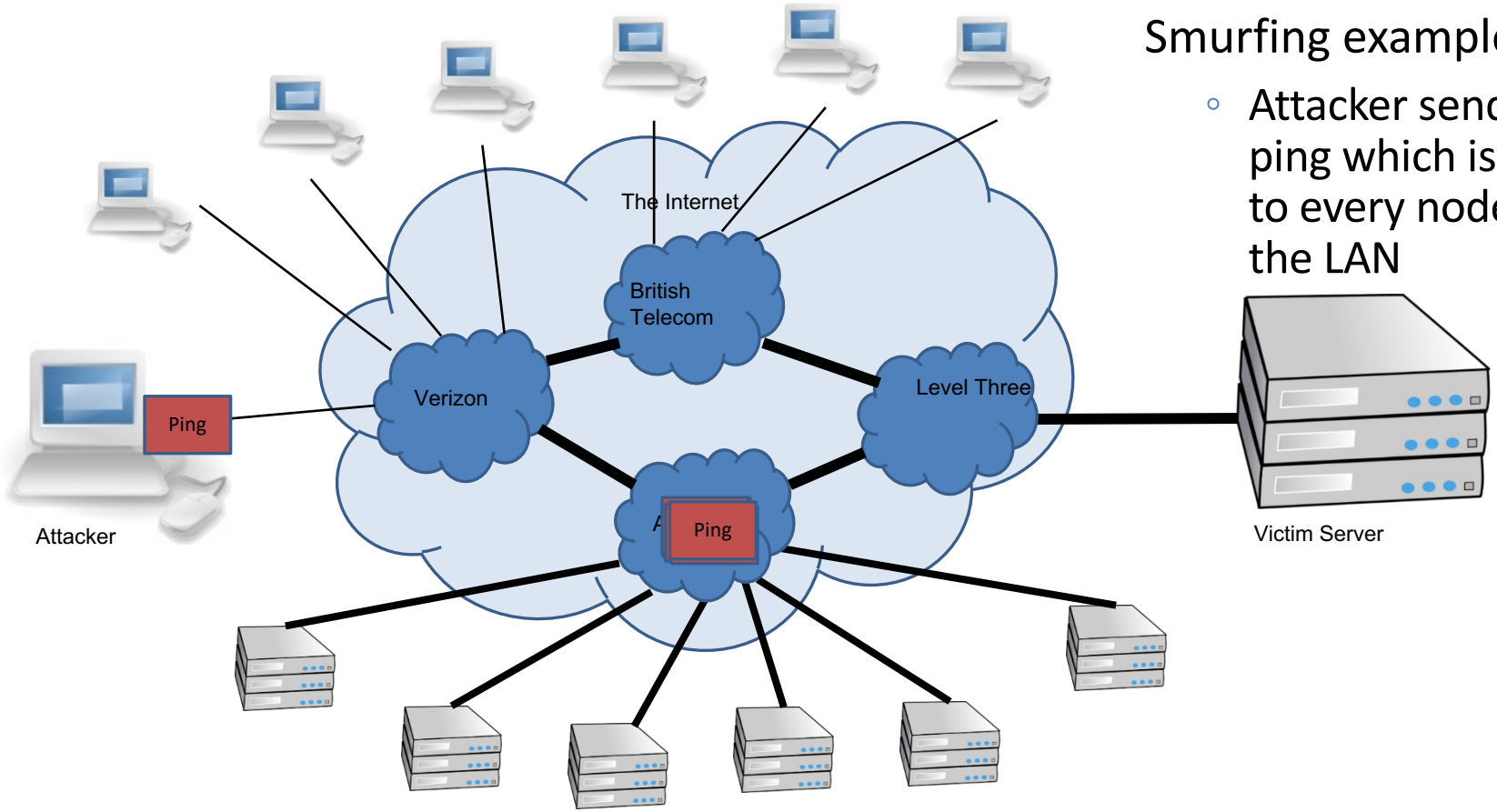
- Same as SYN flooding, but forge the source of the TCP packet
- Advantages:
  - Harder to trace
  - ACKs are sent to a second computer, less attacker bandwidth used
- Problems:
  - Ingress filtering is commonly used to drop packets with source addresses outside their origin network fragment.

Smurfing (directed broadcast)

- The smurfing attack exploits ICMP (Internet Control Message Protocol) ping requests whereby remote hosts respond to echo packets to say they are online
- Some networks respond to pings to broadcast addresses. We call these networks “Smurf amplifiers”.
- Idea: Ping a LAN on a broadcast address, then all hosts on the LAN reply to the sender of the ping
- Attack
  - Make a forged packet with the victim’s IP address as the source
  - Send it to a Smurf amplifier, which then causes a huge number of replies to the victim
- This is a form of reflection attack

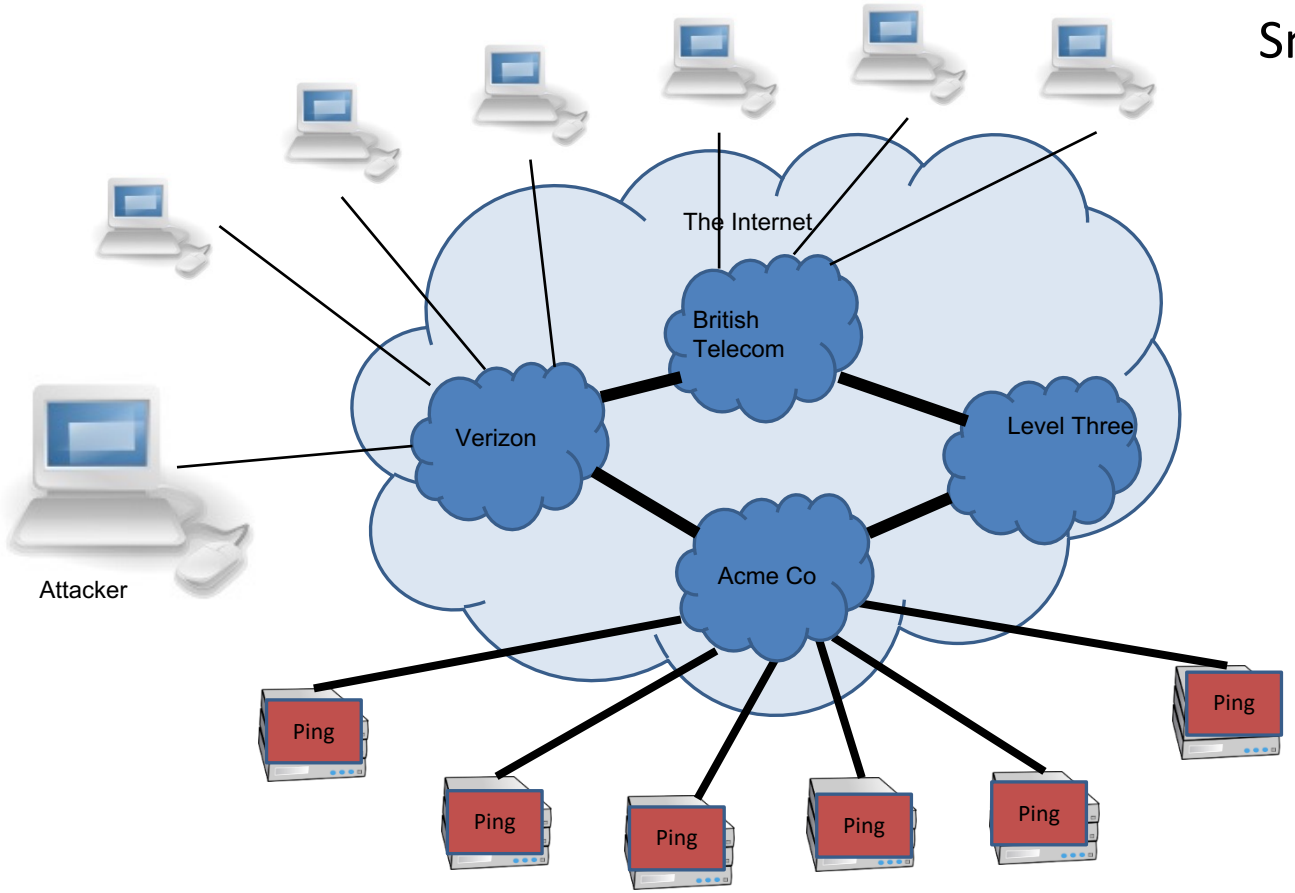
Smurfing example

- Attacker sends 1 ping which is sent to every node on the LAN



Smurfing example

- Each node responds to victim



Victim Server

LANs that allow Smurf attacks are badly configured. One approach is to blacklist these LANs.

powertech

Smurf Amplifier Registry (SAR)
http://www.powertech.no/smurf/

Current top ten smurf amplifiers (updated every 5 minutes)
(last update: 2016-01-17 23:31:02 CET)

Network	#Dups	#Incidents	Registered at	Home AS
212.1.130.0/24	38	0	1999-02-20 09:41	AS9105
204.158.83.0/24	27	0	1999-02-20 10:09	AS3354
209.241.162.0/24	27	0	1999-02-20 08:51	AS701
159.14.24.0/24	20	0	1999-02-20 09:39	AS2914
192.220.134.0/24	19	0	1999-02-20 09:38	AS685
204.193.121.0/24	19	0	1999-02-20 08:54	AS701
198.253.187.0/24	16	0	1999-02-20 09:34	AS22
164.106.163.0/24	14	0	1999-02-20 10:11	AS7066
12.17.161.0/24	13	0	2000-11-29 19:05	not-analyzed
199.98.24.0/24	13	0	1999-02-18 11:09	AS6199

2457713 networks have been probed with the SAR
56 of them are currently broken
193885 have been fixed after being listed here

What We Have Learned

- ARP protocol
- ARP poisoning attack
  - MitM attack on a LAN
- Network and transport layer protocols
  - ICMP
  - TCP for reliable transmission
  - UDP when packet loss/corruption is tolerated
  - DoS Attacks: SYN flooding, Smurf
- Lack of built-in security in network protocols
  - In future lectures we'll see how security must be incorporated at the application layer (e.g. TLS)

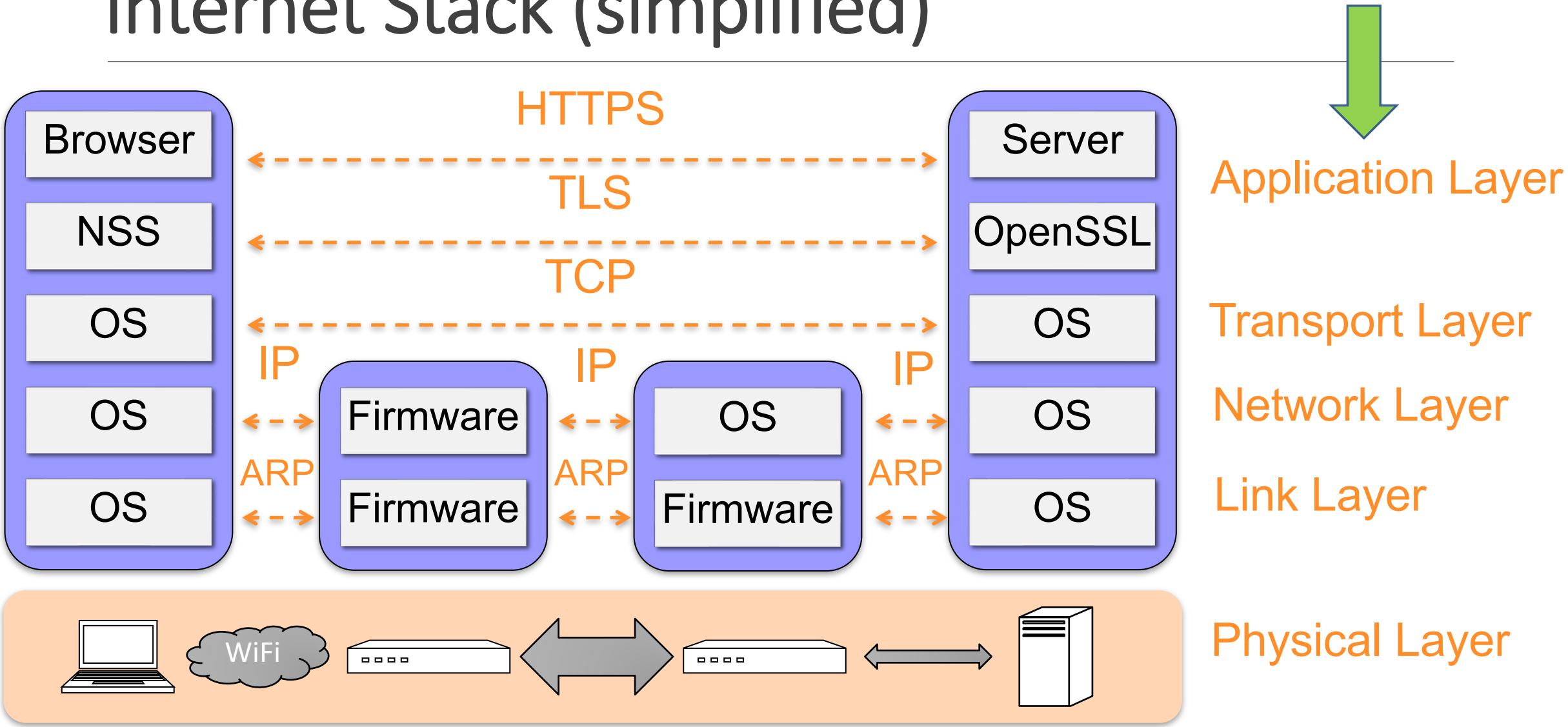
Network Security: Application-Layer and Domain Name System

COMPUTER SECURITY

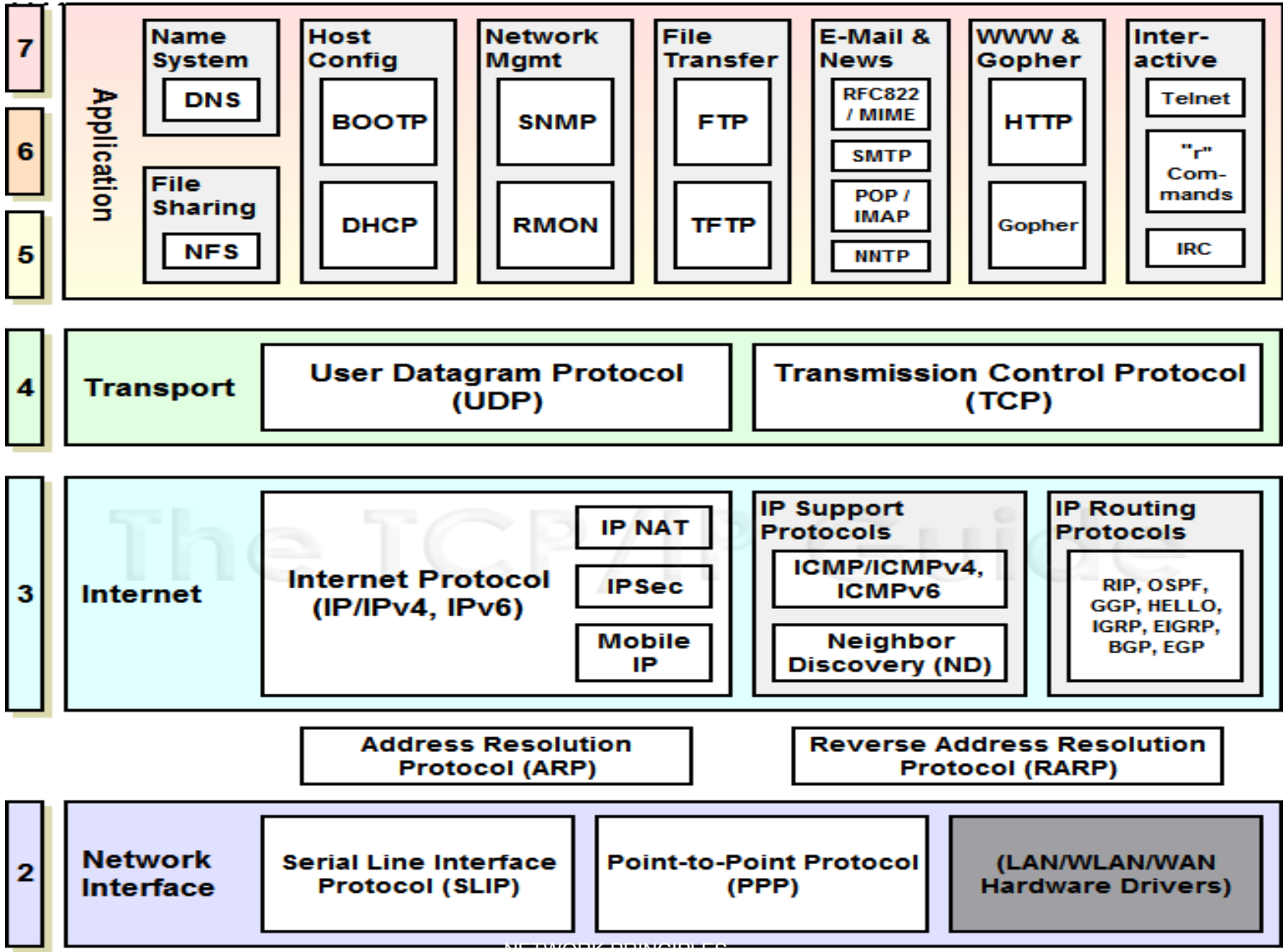
TARIQ ELAHI

Some slides adapted from those by Markulf Kohlweiss, Myrto Arapinis, Kami Vaniea, and Roberto Tamassia

Internet Stack (simplified)



TCP/IP Model Mapped onto OSI



Sample Application-Layer Protocols

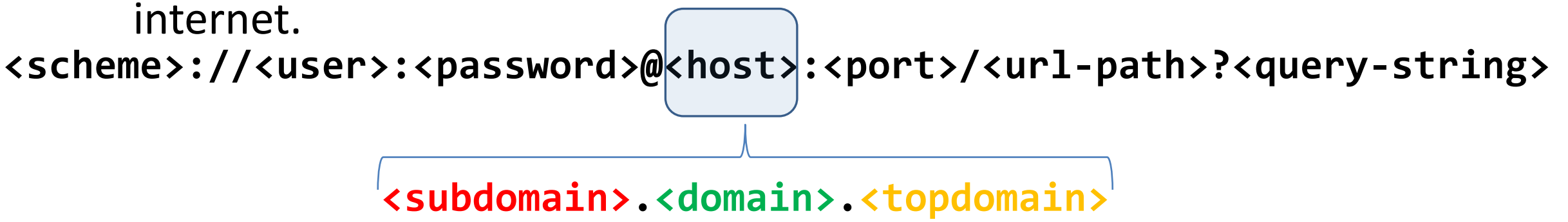
- Domain name system (DNS)
- Hypertext transfer protocol (HTTP)
- SSL/TLS. Protocol used for secure, encrypted browsing (HTTPS)
- IMAP/POP/SMTP. Internet email protocols
- File transfer protocol (FTP). An old but still used protocol for uploading and downloading files
- Telnet. Early remote access protocol
- SSH. More recent secure remote access protocol.

Other protocol examples [edit]

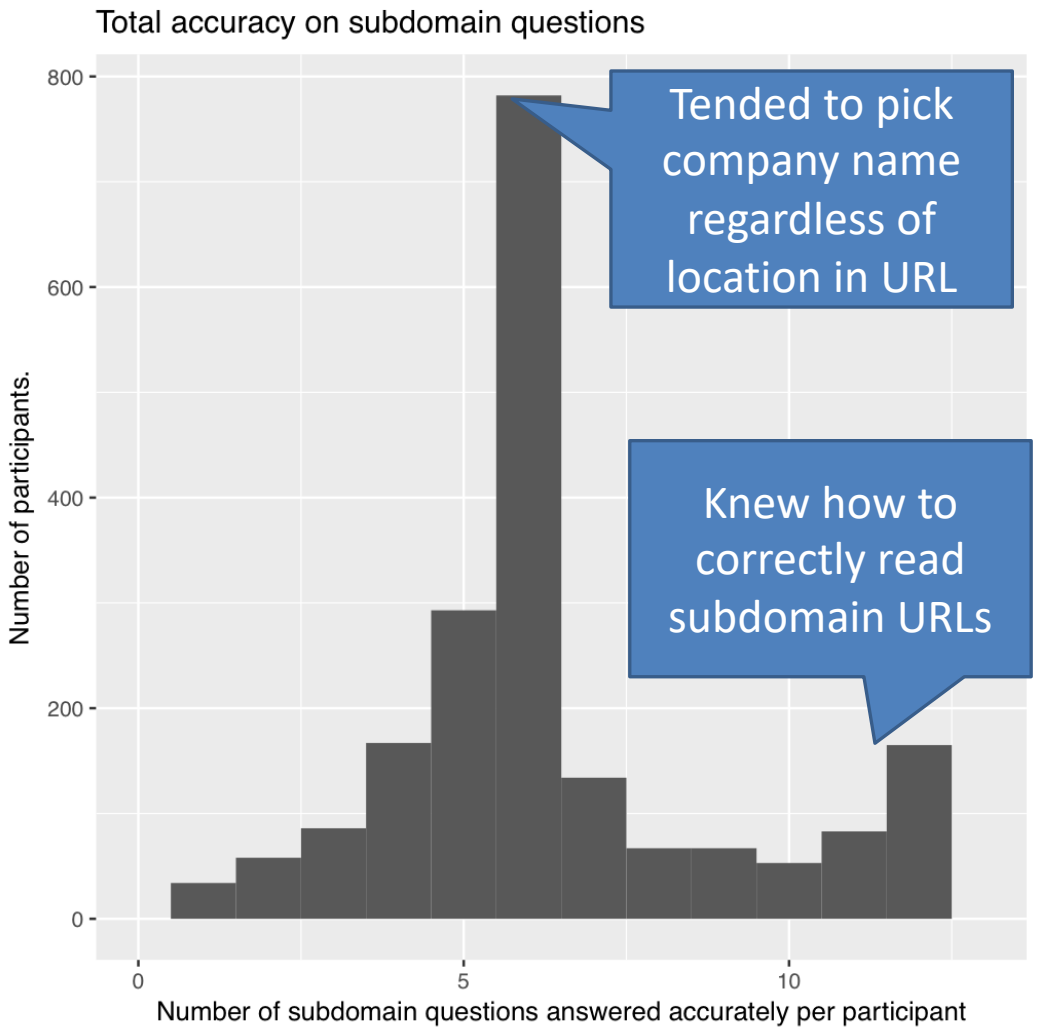
- 9P, Plan 9 from Bell Labs distributed file system protocol
- AFP, Apple Filing Protocol
- APPC, Advanced Program-to-Program Communication
- AMQP, Advanced Message Queuing Protocol
- Atom Publishing Protocol
- BEEP, Block Extensible Exchange Protocol
- Bitcoin
- BitTorrent
- CFDP, Coherent File Distribution Protocol
- CoAP, Constrained Application Protocol
- DDS, Data Distribution Service
- DeviceNet
- eDonkey
- ENRP, Endpoint Handlespace Redundancy Protocol
- FastTrack (KaZaa, Grokster, iMesh)
- Finger, User Information Protocol
- Freenet
- FTAM, File Transfer Access and Management
- Gopher, Gopher protocol
- HL7, Health Level Seven
- HTTP, HyperText Transfer Protocol
- H.323, Packet-Based Multimedia Communications System
- IMAP, Internet Message Access Protocol
- IRCP, Internet Relay Chat Protocol
- IPFS, InterPlanetary File System
- Kademlia
- LDAP, Lightweight Directory Access Protocol
- LPD, Line Printer Daemon Protocol
- MIME (S-MIME), Multipurpose Internet Mail Extensions and Secure MIME
- Modbus
- MQTT Protocol
- Netconf
- NFS, Network File System
- NIS, Network Information Service
- NNTP, Network News Transfer Protocol
- NTCIP, National Transportation Communications for Intelligent Transportation System Protocol
- NTP, Network Time Protocol
- OSCAR, AOL Instant Messenger Protocol
- POP, Post Office Protocol
- PNRP, Peer Name Resolution Protocol
- RDP, Remote Desktop Protocol
- RELP, Reliable Event Logging Protocol
- Rlogin, Remote Login in UNIX Systems
- RPC, Remote Procedure Call
- RTMP, Real Time Messaging Protocol
- RTP, Real-time Transport Protocol
- RTPS, Real Time Publish Subscribe
- RTSP, Real Time Streaming Protocol
- SAP, Session Announcement Protocol
- SDP, Session Description Protocol
- SIP, Session Initiation Protocol
- SLP, Service Location Protocol
- SMB, Server Message Block
- SMTP, Simple Mail Transfer Protocol
- SNTP, Simple Network Time Protocol
- SSH, Secure Shell
- SSMS, Secure SMS Messaging Protocol
- TCAP, Transaction Capabilities Application Part
- TDS, Tabular Data Stream
- Tor (anonymity network)
- Tox
- TSP, Time Stamp Protocol
- VTP, Virtual Terminal Protocol
- Whois (and RWhois), Remote Directory Access Protocol
- WebDAV
- X.400, Message Handling Service Protocol
- X.500, Directory Access Protocol (DAP)
- XMPP, Extensible Messaging and Presence Protocol

What is a URL?

- Uniform Resource Locators (URLs) are a standardized format for describing the location and access method of resources via the internet.



eg. https://profile.facebook.com

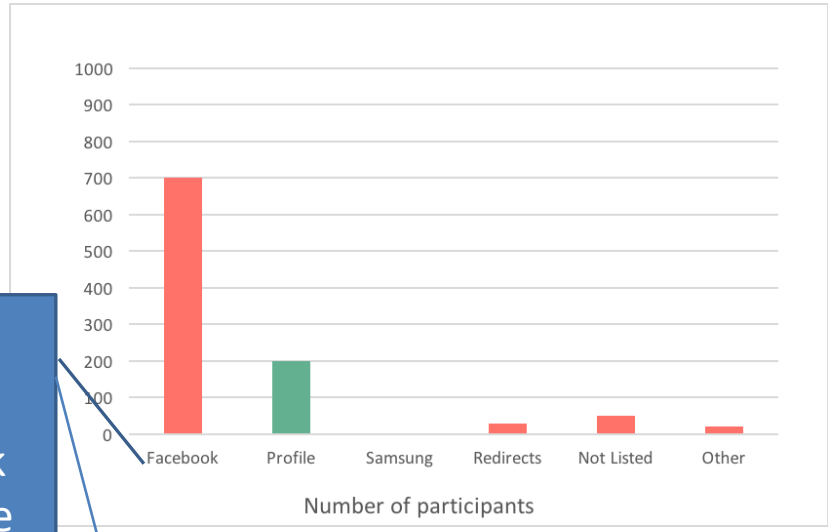


Tended to pick company name regardless of location in URL

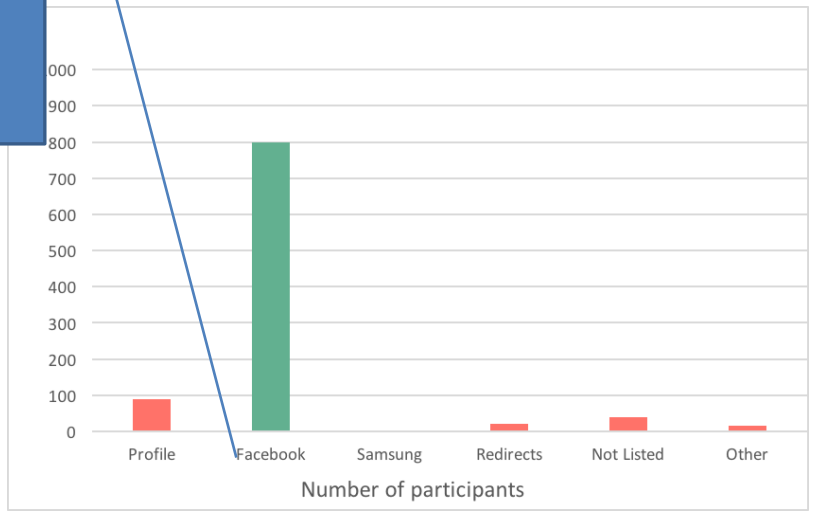
Knew how to correctly read subdomain URLs

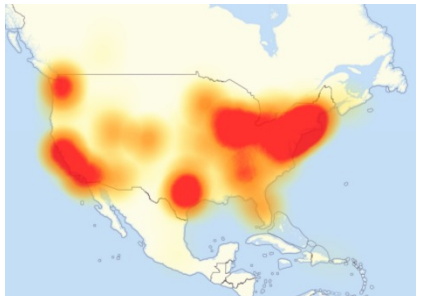
Tended to pick company name regardless of location in URL

https://facebook.profile.com



https://profile.facebook.com





DNS Servers are soft targets for attackers, take out the mapping and the website goes “offline”

DoS attack on major DNS provider brings Internet to morning crawl [Updated]

Dyn’s US East region hit hardest in attack that affected Twitter, Reddit.

SEAN GALLAGHER - OCT 21, 2016 1:59 PM UTC

118

Update (12:04p ET): A second wave of DDoS attacks against Dyn is underway, as of noon Eastern Time today. Dyn is continuing to work on the issue. Our original story follows below; further updates will be added as information becomes available.

A distributed denial of service attack against Dyn, the dynamic DNS service, affected the availability of dozens of major websites and Internet services this morning, including Twitter and Reddit. The attack, which began this morning at 7:10am Eastern Time (12:10pm UK), is apparently focused on Dyn’s US East Coast name servers.

“This morning, Dyn received a global DDoS attack on our Managed DNS infrastructure in the east coast of the United States,” Doug Madory, Director of Internet Analysis at Dyn, said in an e-mail sent to Ars this morning. “DNS traffic resolved from east coast name server locations are experiencing a service interruption during this time.” By 9:20am ET this morning, Dyn had mitigated the attack and services returned to normal.

[Update, 1:20 PM ET] Less than three hours later, the attack began again, and is still in progress.

CNN Home International Edition +

Syrian group cited as New York Times outage continues

By Heather Kelly, CNN

Updated 1330 GMT (2130 HKT) August 29, 2013

The hackers gained access to a Melbourne IT reseller account using a phishing email and proceeded to change the DNS records of multiple domains, including NYTimes.com, according to the company.

The N

Stor

New
probl

Syria
York

The group is loyal to Syrian President Bashar Al-Assad

Twitter also experienced problems on Tuesday due to a similar attack

multiple attacks on media websites in recent months and, on Twitter, took credit for a sophisticated hack that had hobbled the Times' news site for roughly 20 hours.

"The @nytimes attack was going to deliver an anti-war message but our server couldn't last for 3 minutes," the group posted on its Twitter feed at about 9:40 Wednesday morning.

Domain Name System

The domain name system (DNS) is an application-layer protocol

Basic function of DNS

- Map domain names to IP addresses
- The mapping is many to many

Examples:

- www.ed.ac.uk and edwc.is.ed.ac.uk map to 129.215.228.101
- google.com maps to 216.58.213.110, 198.7.237.249, and other addresses

More generally, DNS is a distributed database that stores resource records

- Address (A) record: IP address associated with a host name
- Mail exchange (MX) record: mail server of a domain
- Name server (NS) record: authoritative server for a domain

Domains

Domain name

- Two or more labels, separated by dots (e.g., inf.ed.ac.uk)

Top-level domain (TLD)

- Generic (gTLD), e.g., .com, .org, .net
- Country-code (ccTLD), e.g., .ca, .it
- New top level domains, e.g., .scot, .tirol

ICANN

- (non-profit) Internet Corporation for Assigned Names and Numbers
- Keeps database of registered gTLDs (InterNIC)
- Accredits registrars for gTLDs

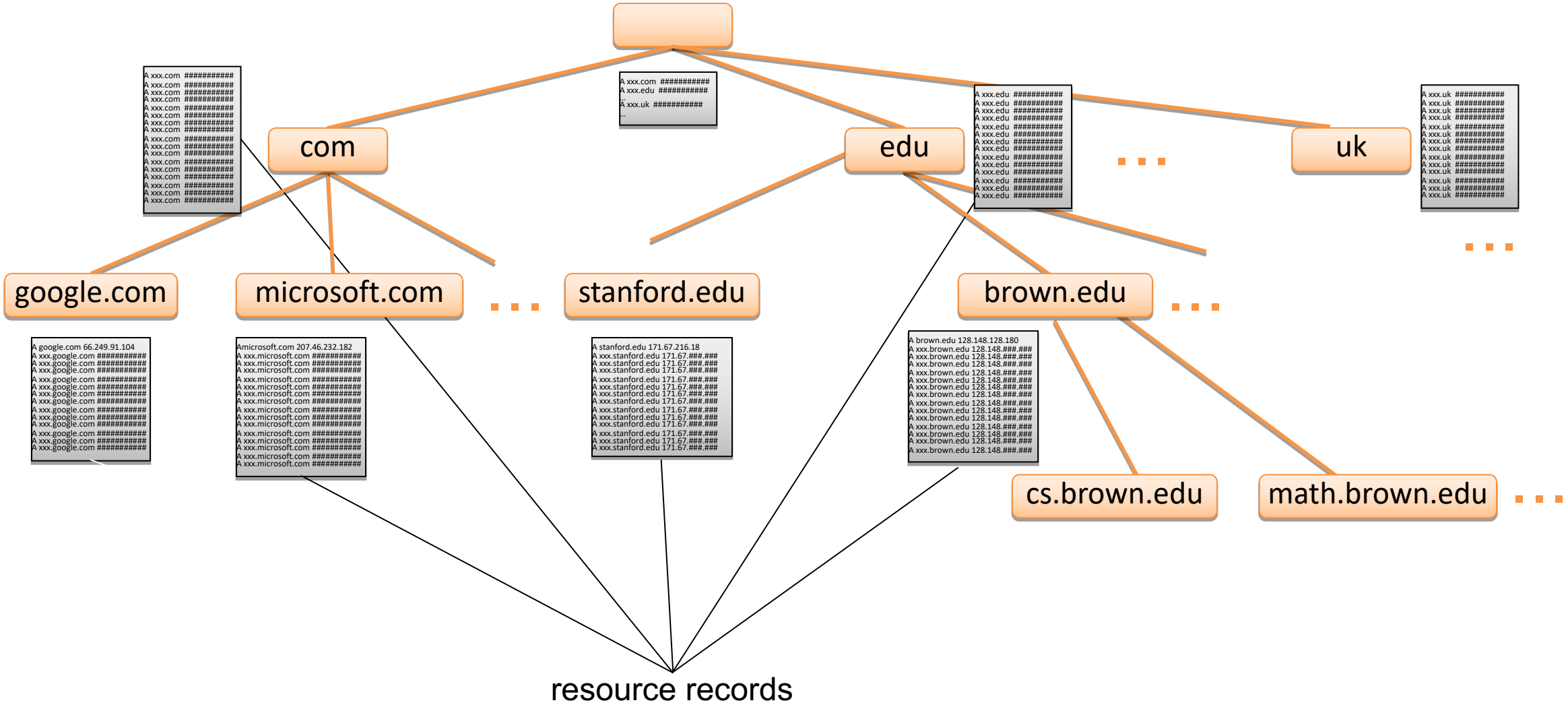
gTLDs

- Managed by ICANN

ccTLDs

- Managed by government organizations

DNS Tree


com
edu
uk
google.com
microsoft.com
stanford.edu
brown.edu
cs.brown.edu
math.brown.edu
resource records

Name Servers

- Name server
  - Keeps local database of DNS records
  - Answers DNS queries
  - Can ask other name servers if record not in local database
- Authoritative name server
  - Stores reference version of DNS records for a zone (partial tree)
- Examples
  - dns0.ed.ac.uk is authoritative for ed.ac.uk and dns0.inf.ed.ac.uk for inf.ed.ac.uk
- Root servers
  - Authoritative for the root zone (TLDs)
  - [a-m].root-servers.net
  - Supervised by ICANN

Name Resolution

- Resolver
  - Program that retrieves DNS records
  - Connects to a name server (default, root, or given)
  - E.g., dig in Linux and nslookup in Windows
  - Caches records received

Iterative resolution

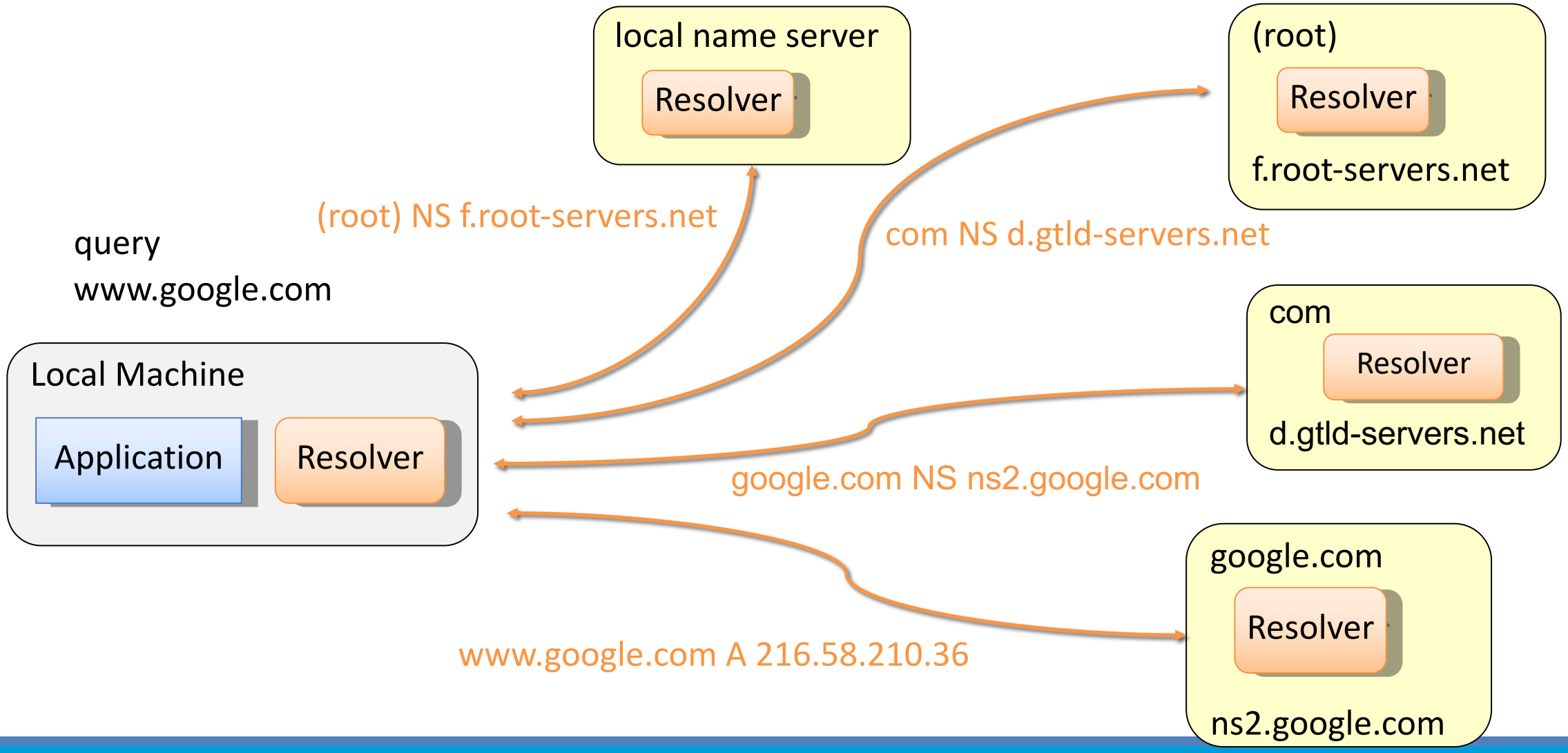
Name server refers client to authoritative server (e.g., a TLD server) via an NS record

Repeat

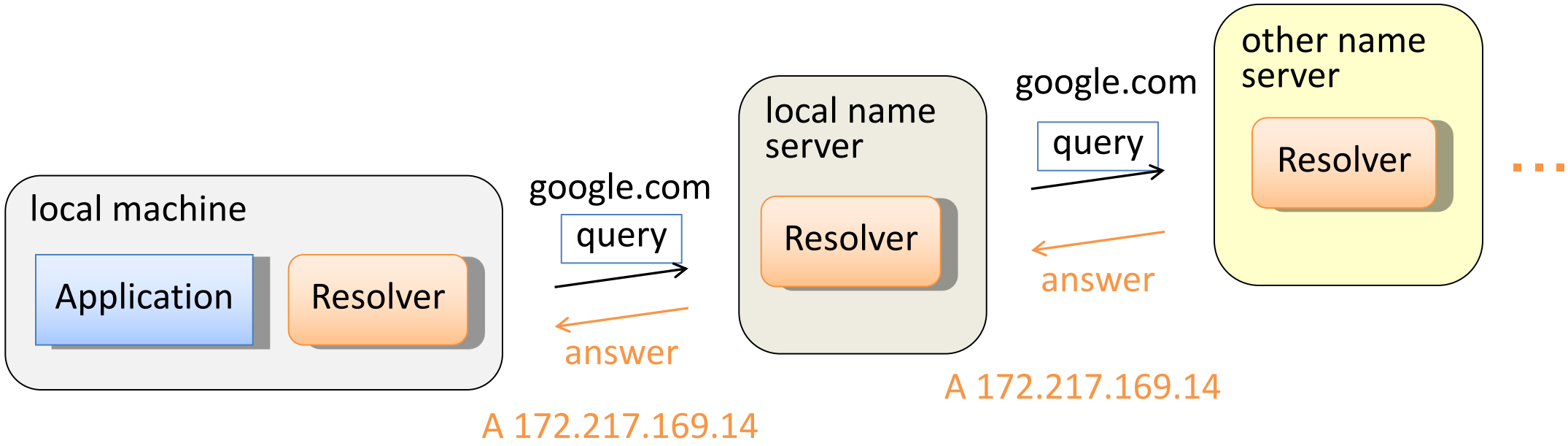
Recursive resolution

Name server queries another server and forwards the final answer (e.g., A record) to client

Iterative Name Resolution



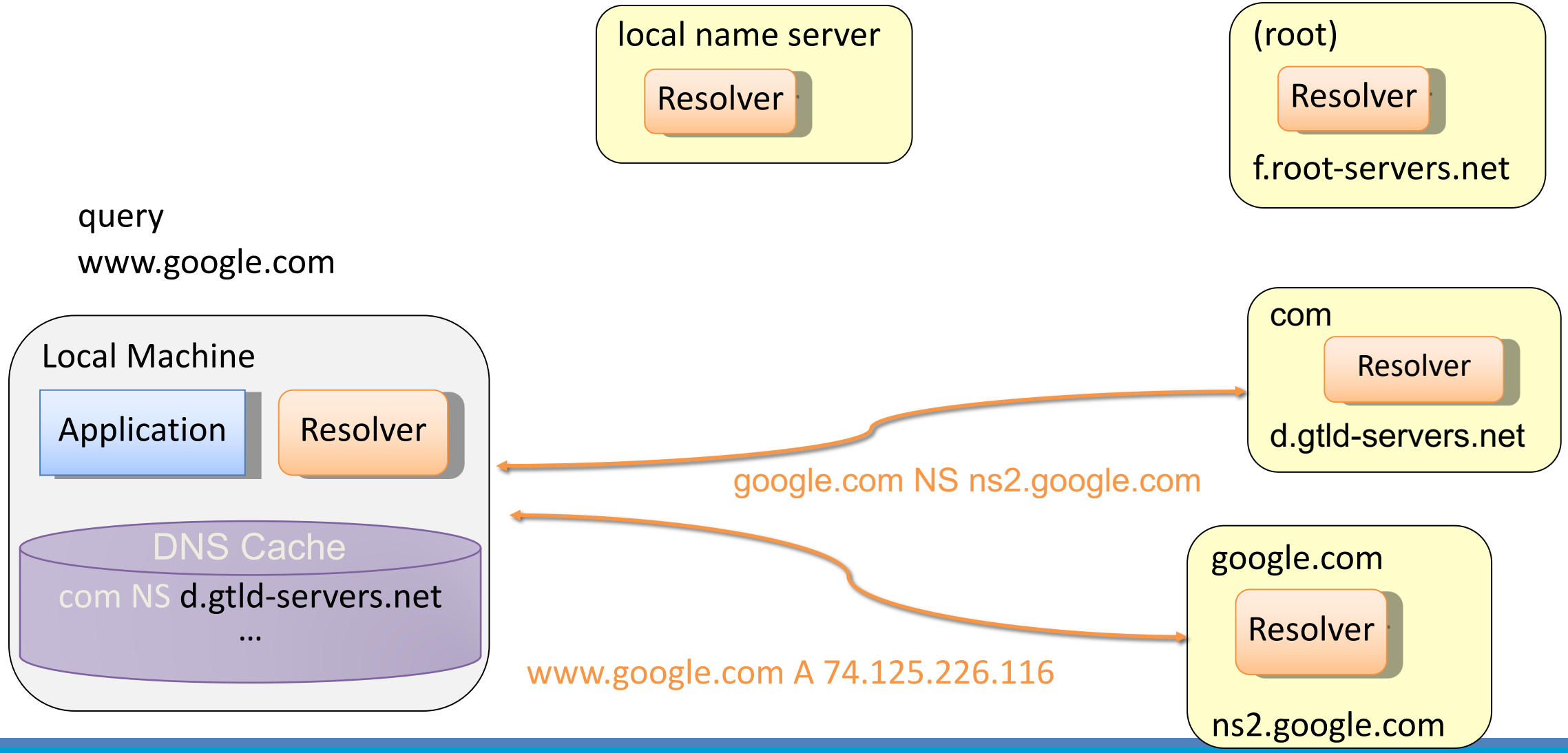
Recursive Name Resolution



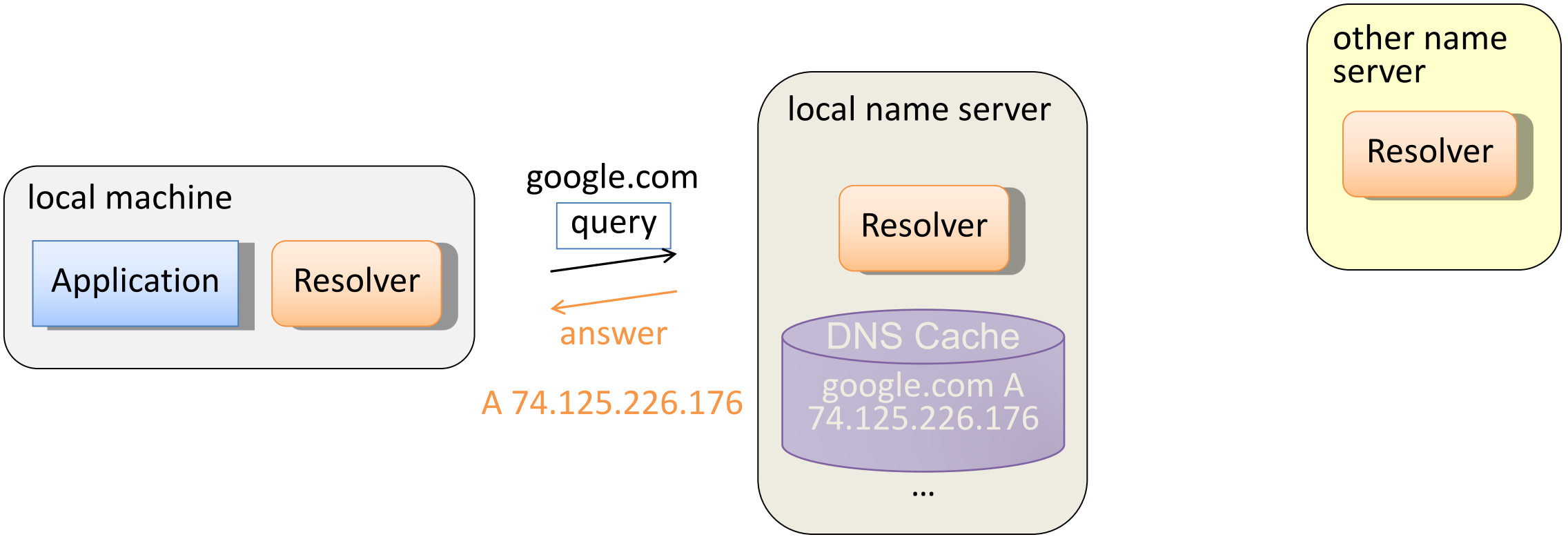
DNS Caching

- There would be too much network traffic if a path in the DNS tree would be traversed for each query
  - Root servers and TLD servers would be rapidly overloaded
- DNS servers cache records that are results of queries for a specified amount of time
  - Time-to-live field
- DNS queries with caching
  - First, resolver looks in cache for A record of query domain
  - Next , resolver looks in cache for NS record of longest suffix of query domain

Iterative Name Resolution with Caching



Recursive Name Resolution with Caching



Local DNS Cache

```
C:\Users\marku>ipconfig /displaydns

Windows IP Configuration

    arstechnica.com
    ----------------------------------------
    Record Name . . . . . : arstechnica.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 128
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 50.31.169.131
```

- Operating system maintains DNS cache
  - Shared among all running applications
  - Can be displayed to all users
  - View DNS cache in Windows with command ipconfig /displaydns
  - Clear DNS cache in Windows with command ipconfig /flushdns
- Privacy issues
  - Browsing by other users can be monitored
  - Note that private/incognito browsing does not clear DNS cache

DNS Cache Poisoning

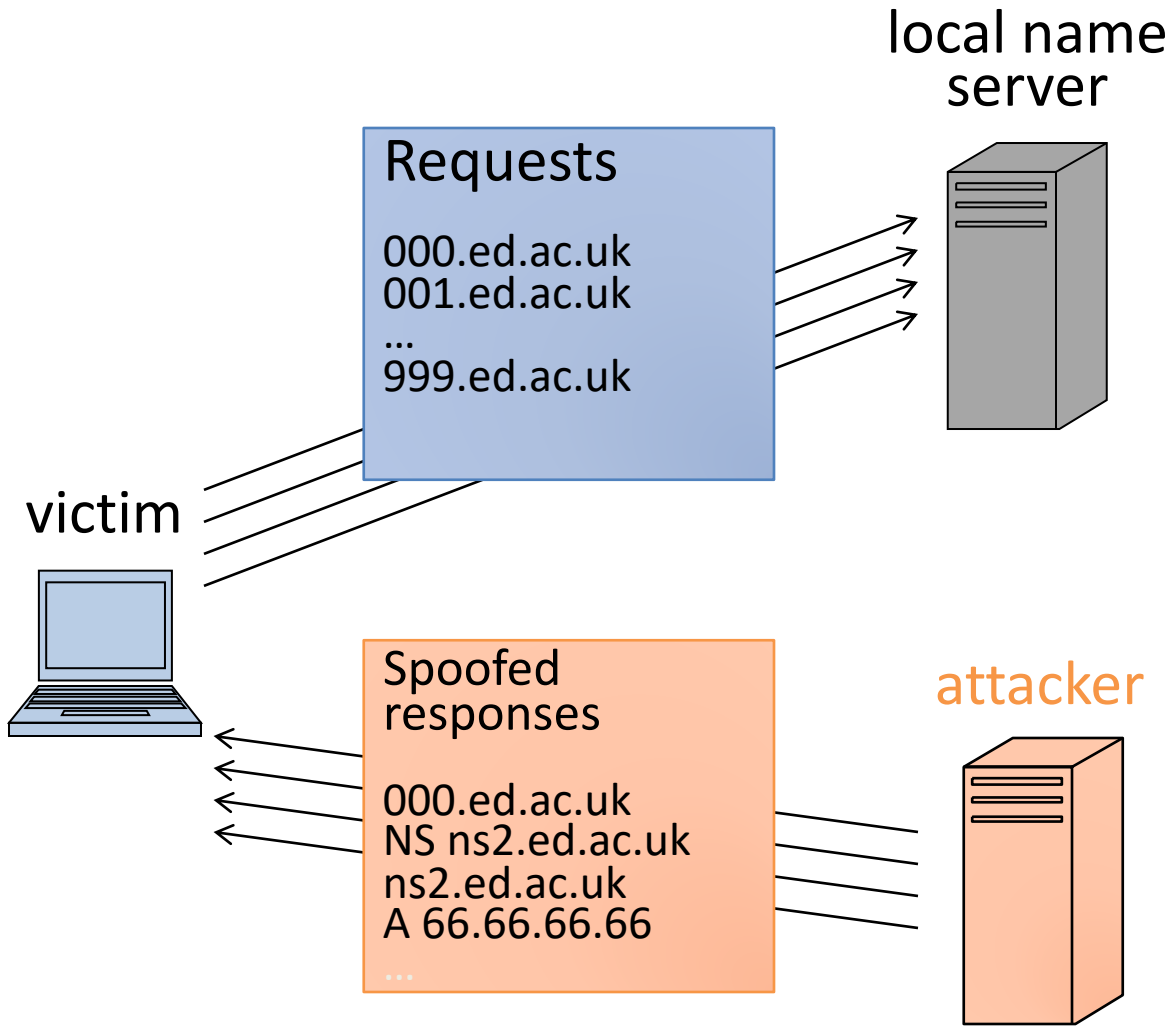
- Basic idea
  - Give a DNS server a false address record and get it cached
- DNS query mechanism
  - Queries issued over UDP on port 53
  - 16-bit request identifier in payload to match answers with queries
  - No authentication
- Cache may be poisoned when a resolver
  - Query has predictable identifiers and return ports
  - Attacker answers before authoritative name server
  - Ignore identifier, accepts unsolicited DNS records
- Early versions of BIND (popular DNS software) vulnerable to cache poisoning

DNS Cache Poisoning Defenses

- Query randomization
  - Random request identifier (16 bits)
  - Random return port (16 bits)
  - Probability of guessing request ID or return port
    - $1 / 2^{16} = 0.0015\%$
  - Probability of guessing request ID and return port is
    - $1 / 2^{32}$ (less than one in four billion)
    - Single guess low likelihood
    - But many guesses?

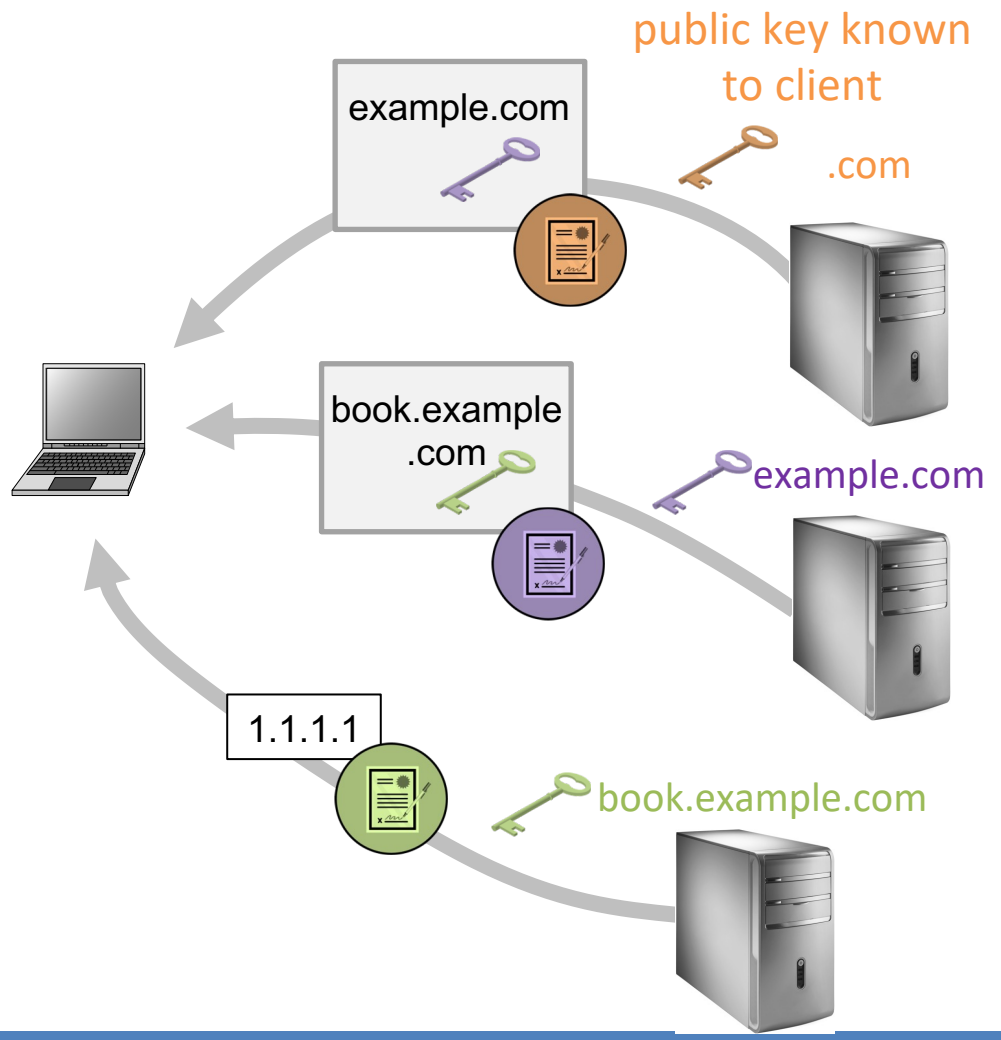
Subdomain DNS Cache Poisoning (Kaminsky)

- Attacker causes victim to send
  - Many DNS requests for nonexistent subdomains of target domain
- Attacker sends victim
  - Forged NS responses for the requests
- Format of forged response
  - Random ID
  - Correct NS record
  - Spoofed glue record pointing to the attacker's name server IP



DNSSEC

- Goals
  - Authenticity of DNS answer origin
  - Integrity of reply
  - Authenticity of denial of existence
- Implementation
  - Signed DNS replies at each step
  - Public-key cryptography
- Slow deployment
  - Root servers support since 2010



What We Have Learned

- How DNS operates
  - Distributed database
  - Resolvers and name servers
  - Iterative vs. recursive resolution
  - Caching
- DNS cache poisoning attacks and early defenses
- DNSSEC

Firewalls, NAT, and Intrusion Detection

COMPUTER SECURITY

TARIQ ELAHI

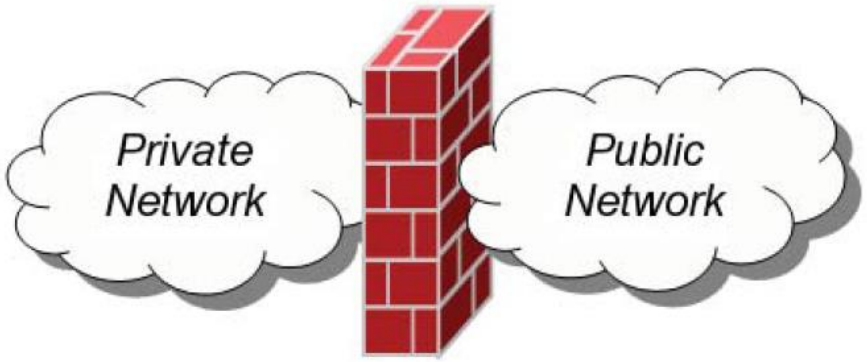
Some slides adapted from those by Markulf Kohlweiss
Kami Vaniea, Aggelos Kiayias, and Michael Goodrich

Today

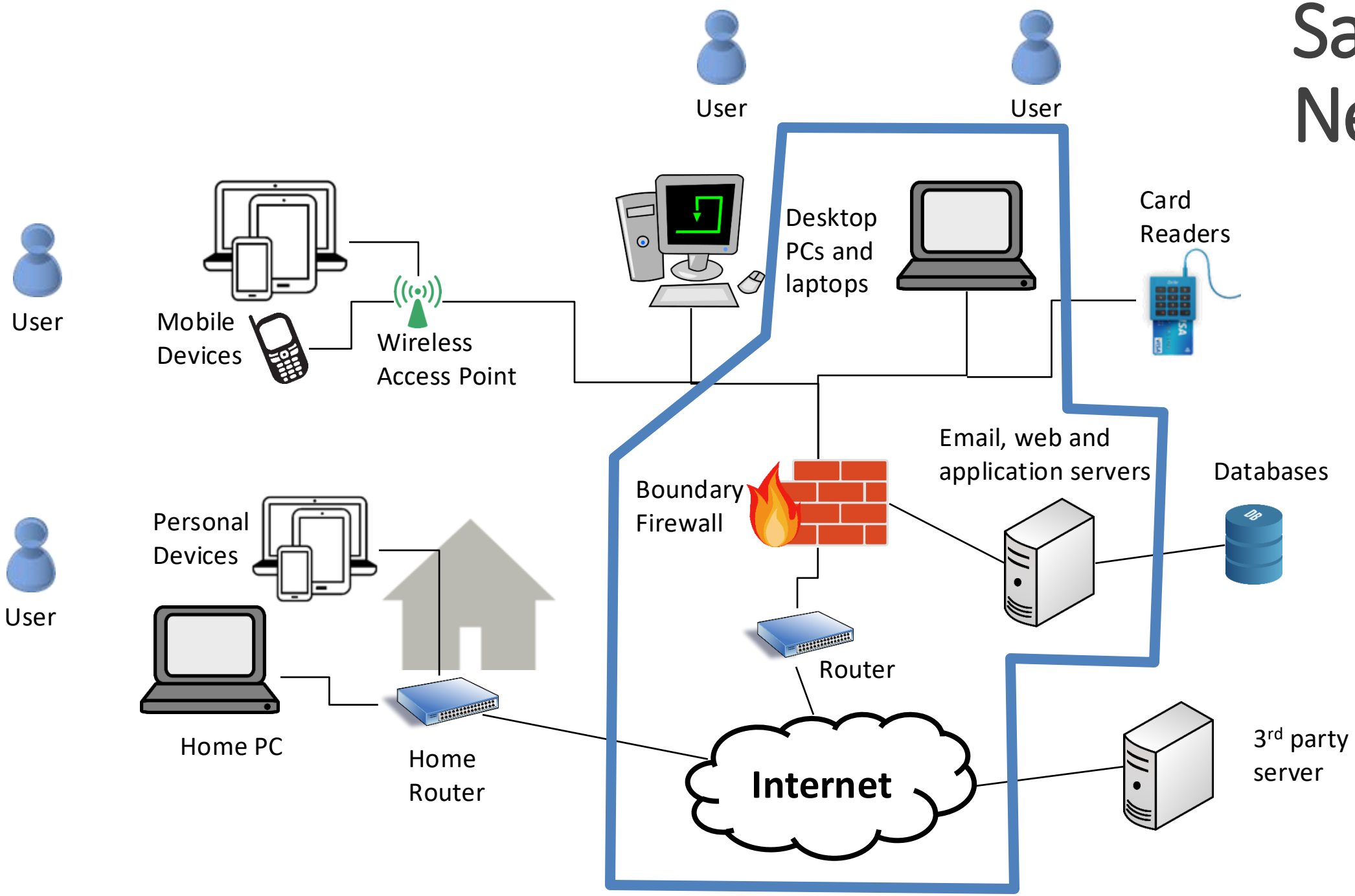
- Methods for observing, managing, and controlling network information flows
  - Firewalls
  - Network Address Translation (NAT)
  - Intrusion Detection Systems (IDS)

Firewalls

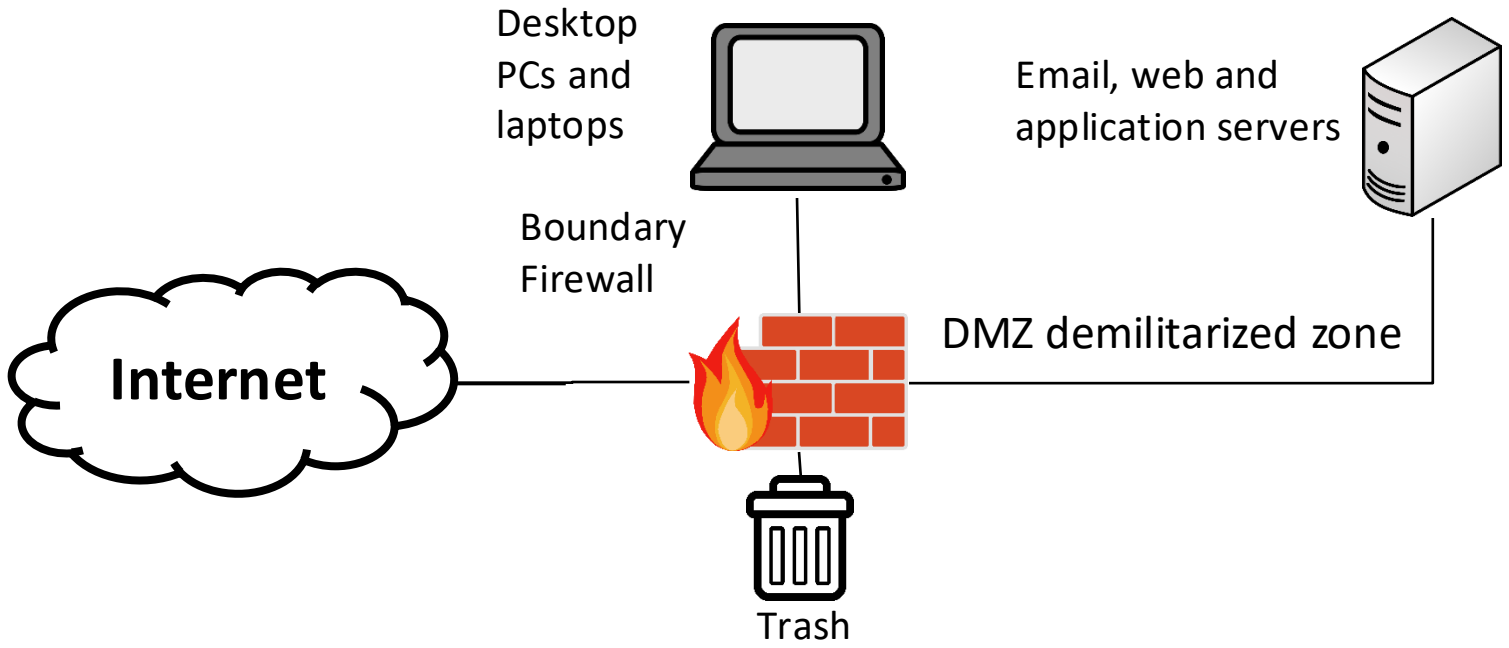
- A **firewall** is a security measure designed to prevent unauthorized electronic access to a networked computer system.
- Intuition: Similar to firewalls in building construction. Intent is to isolate one “network” or “compartment “ from another.



Sample Network



- Malicious actions from the **Internet** AND **local network**
- Firewall applies a set of rules called **firewall policies**
- Based on rules, it allows or denies the traffic
- Blocklist: Allow-by-default
- Allowlist: Deny-by-default



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	22	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	UDP	*	192.168.1.*	*	Deny

Custom Firewall ruleset from a home router

root@ars-router: ~

```
##### Service rules
# OpenVPN
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DE
FAULT --mask 255.255.255.255 --rsource
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seco
nds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

##### forwarding ruleset
```

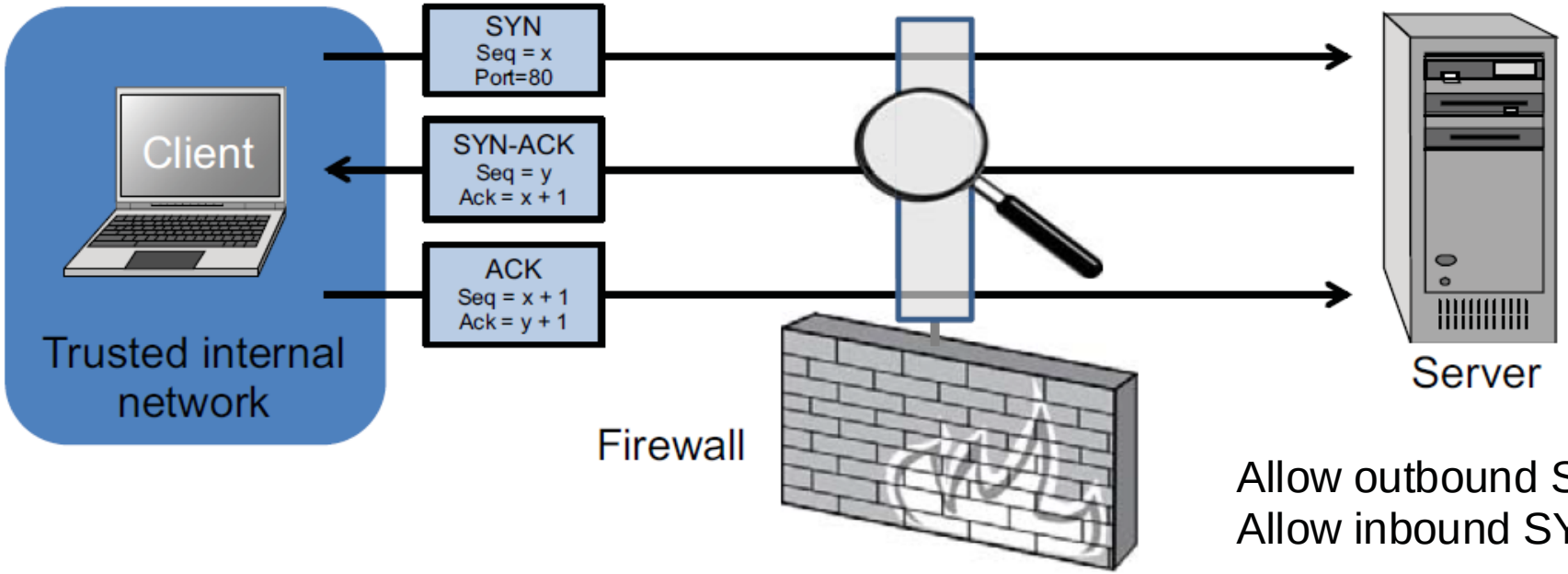
Image:
http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/
https://arstechnica.com/gadgets/2016/04/the-ars-guide-to-building-a-linux-router-from-scratch/

Firewall Types

- **packet filters (stateless)**
  - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **stateful filters**
  - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
  - It works like a **proxy** it can “understand” certain applications and protocols.
  - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Stateless Firewalls

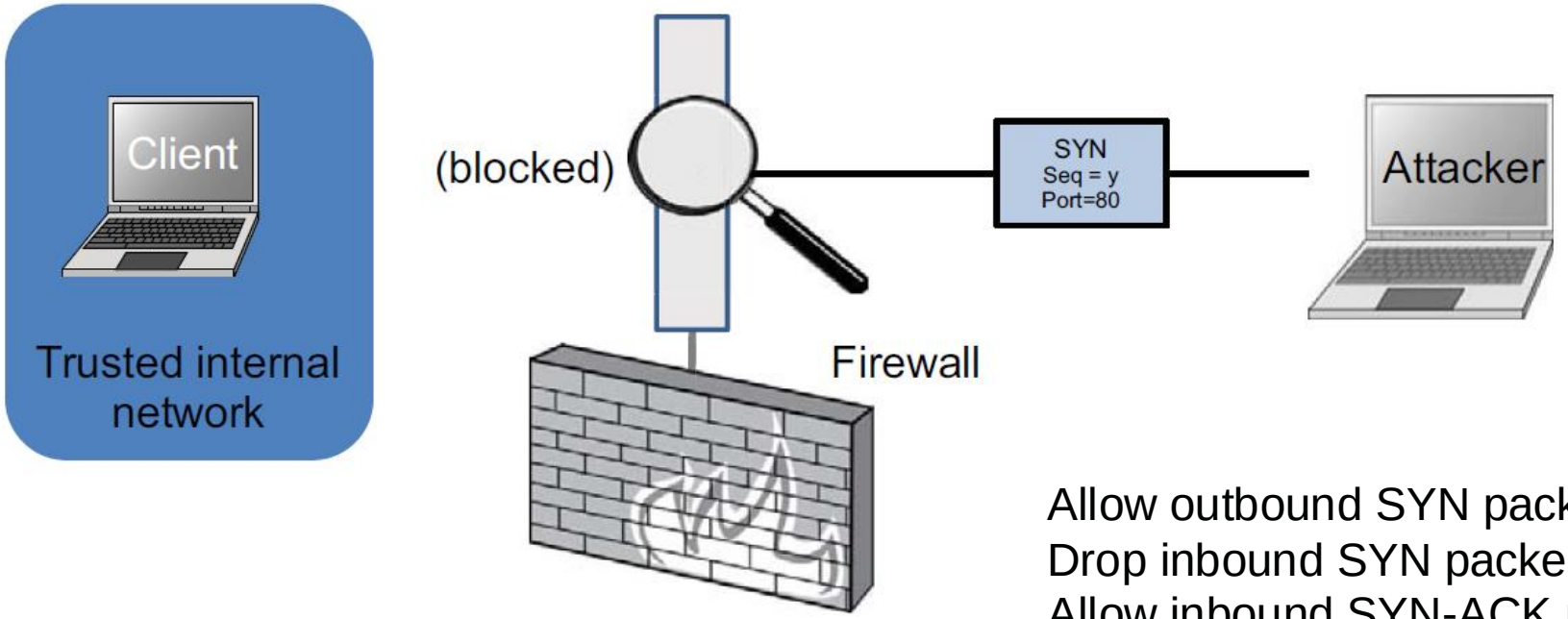
- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



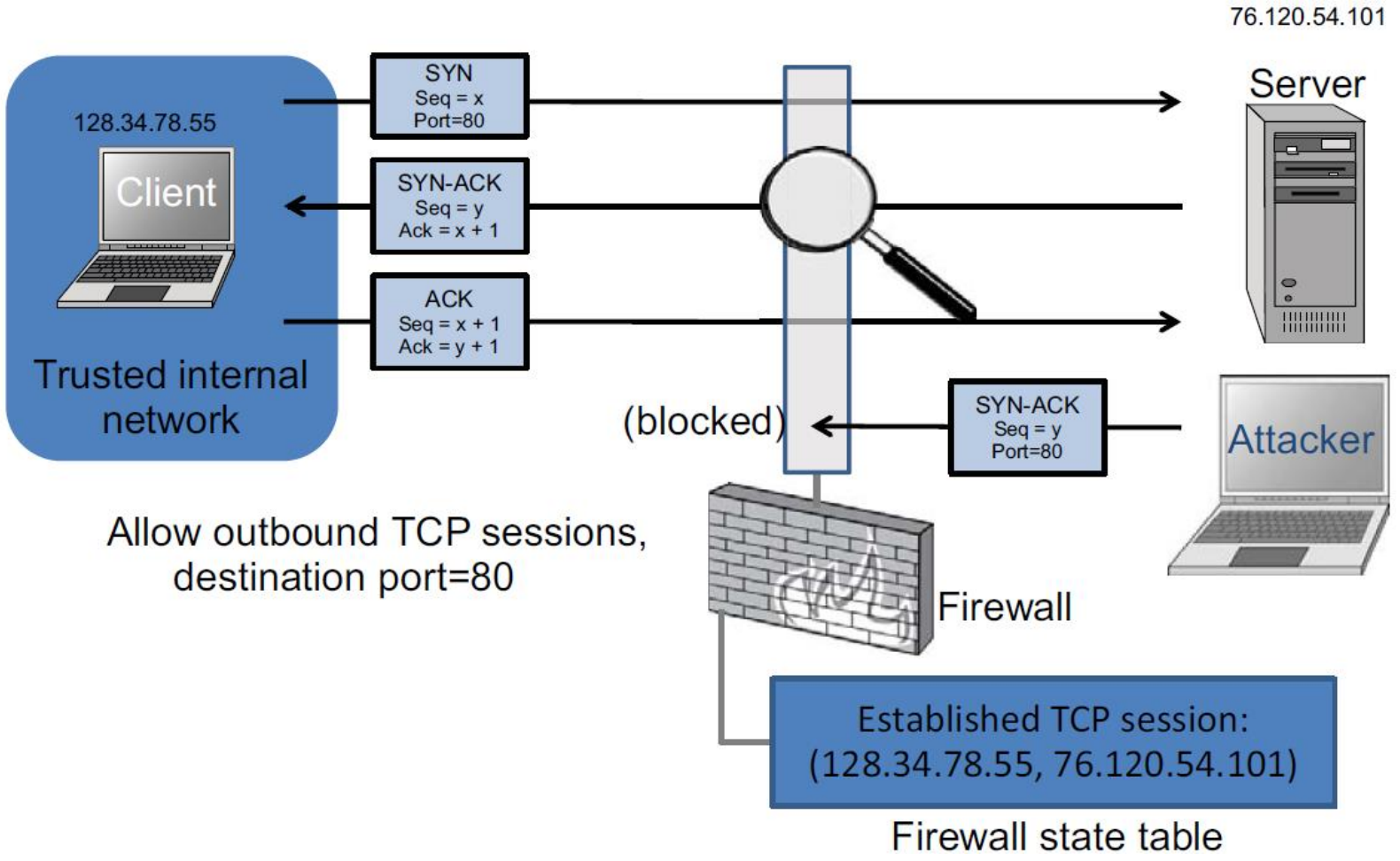
Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Stateful Firewalls

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

Stateful Firewall Example

- Allow only requested TCP connections:



Port scan

- An attacker is looking for applications listening on ports
- A single IP address (right) is contacting many ports (left) to see if any respond

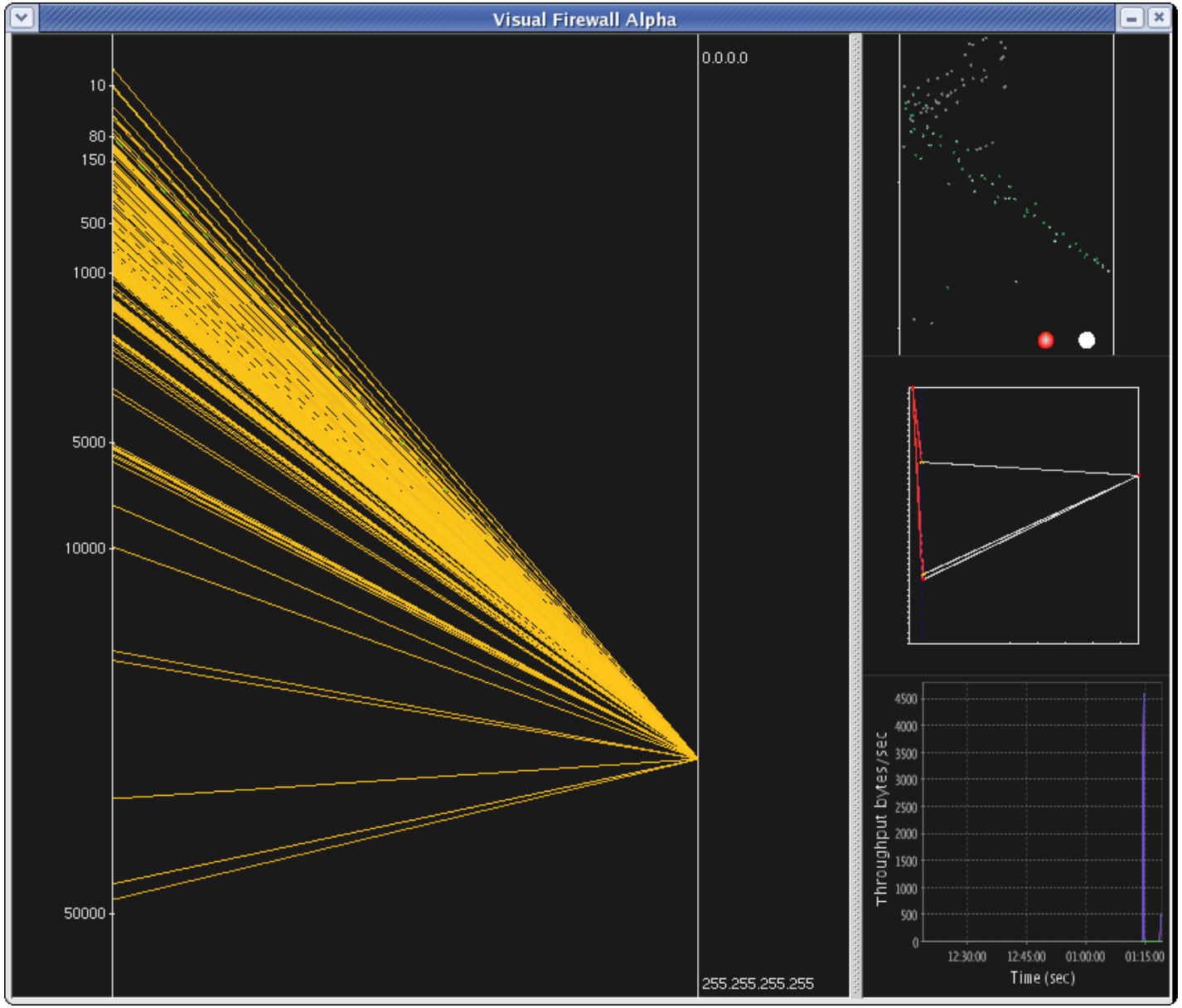
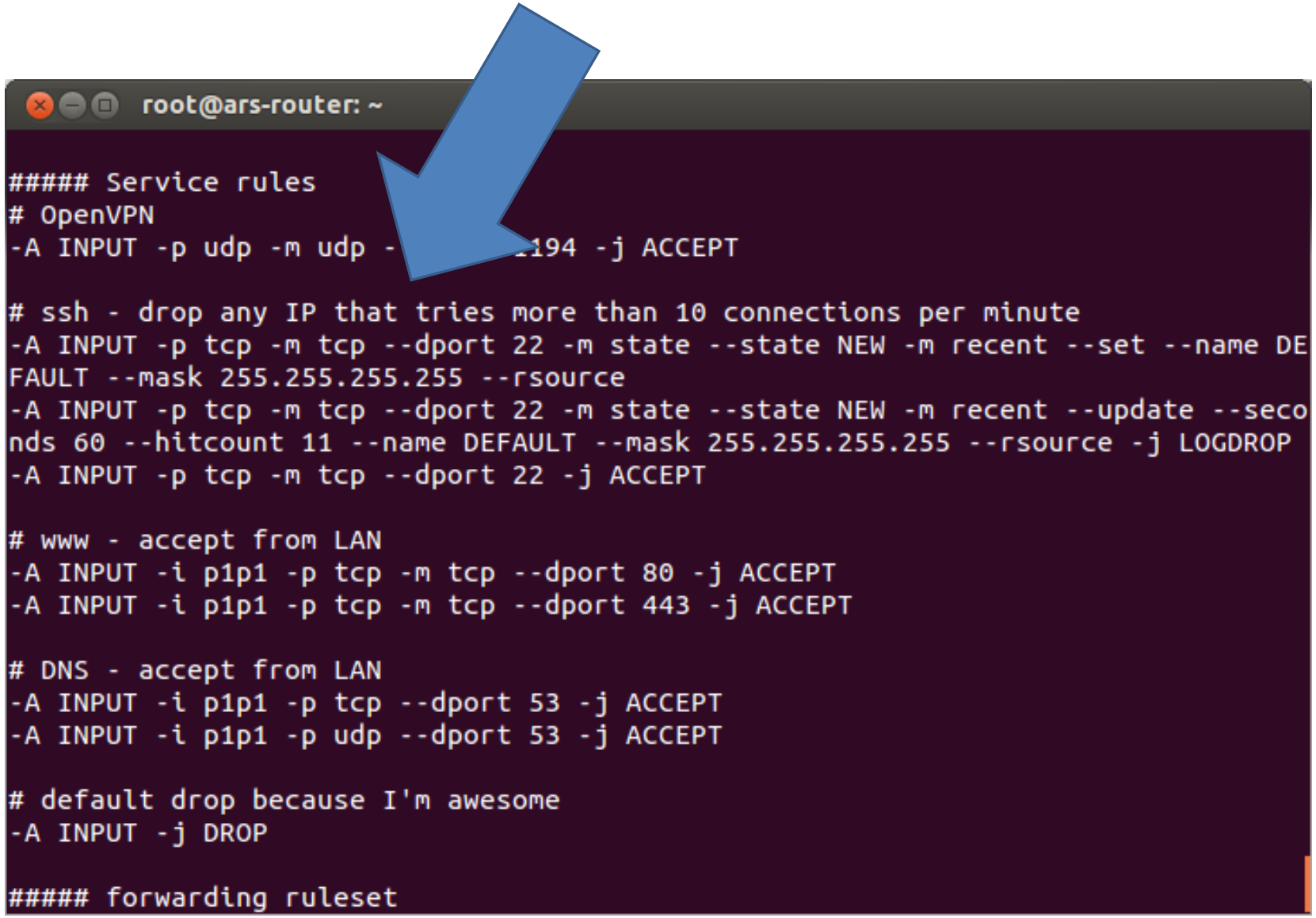


Image: http://chrislee.dhs.org/projects/visualfirewall.html

Custom Firewall ruleset from a home router



Application layer firewall/proxy

- Simulates the (proper) effects of an application
- Effectively a ***protective*** **interceptor** that screens information at an application layer
- Allows an administrator to block certain application requests.
- For example:
  - Block all web traffic containing certain words (aka censorship)
  - Remove all macros from Microsoft Word files in email
  - Prevent anything that looks like a credit card number from leaving a database

Personal firewalls

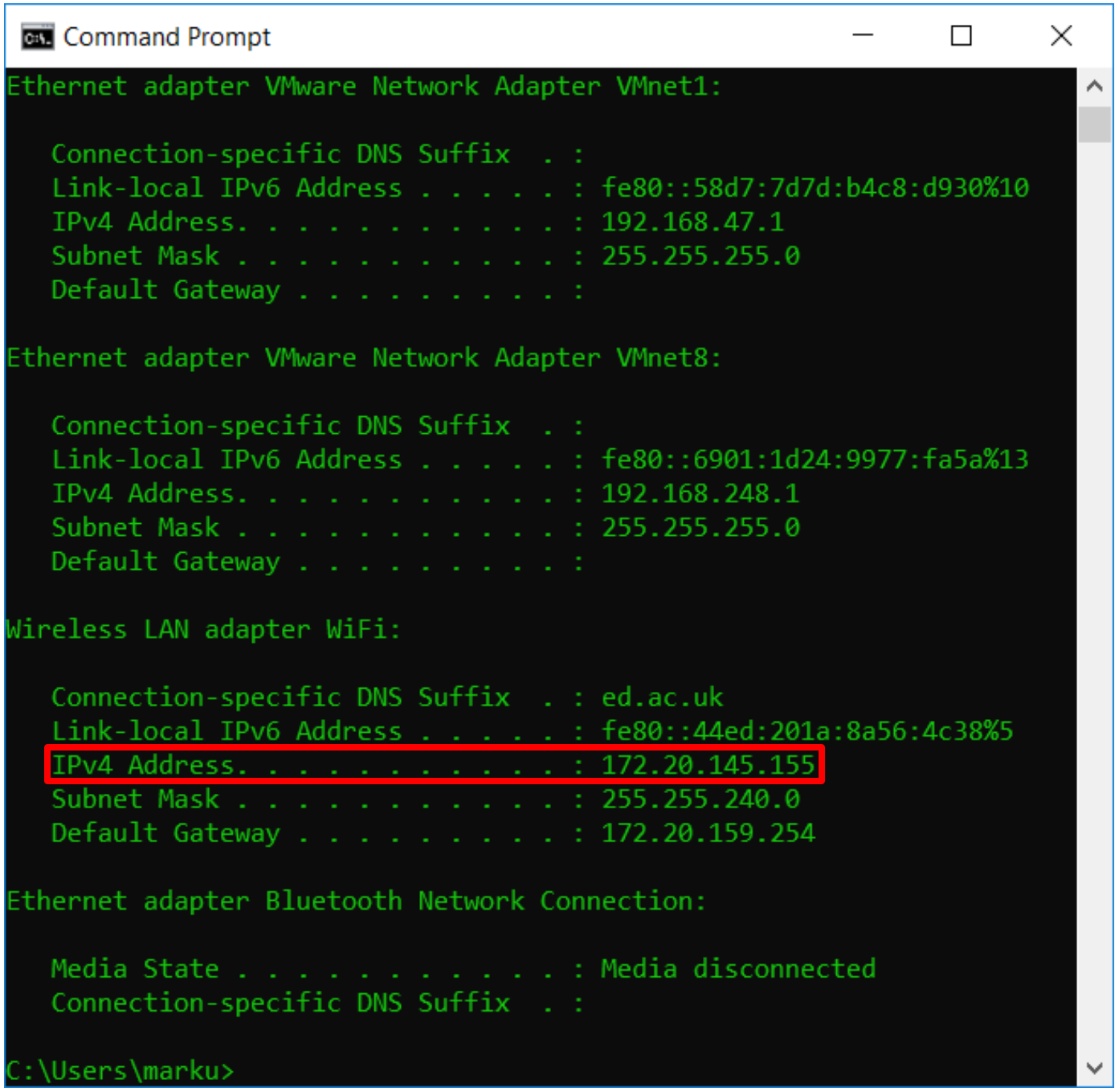
- Runs on the workstation that it protects (software)
- Provides basic protection, especially for home or mobile devices
- Any rootkit type software can disable the firewall

Firewalls Pros and Cons

- **They do** prevent straightforward attacks and information leakages.
- **They can be circumvented**, and may have unintended consequences
- Increasing their effectiveness increases their operational cost substantially (overhead/configuration).
- May give false sense of security.
- **Bottom-line**: you have to have one but do not count on it for much.

Network Address Translation (NAT)

Looking at the IP address of my laptop which is connected to the University WIFI.



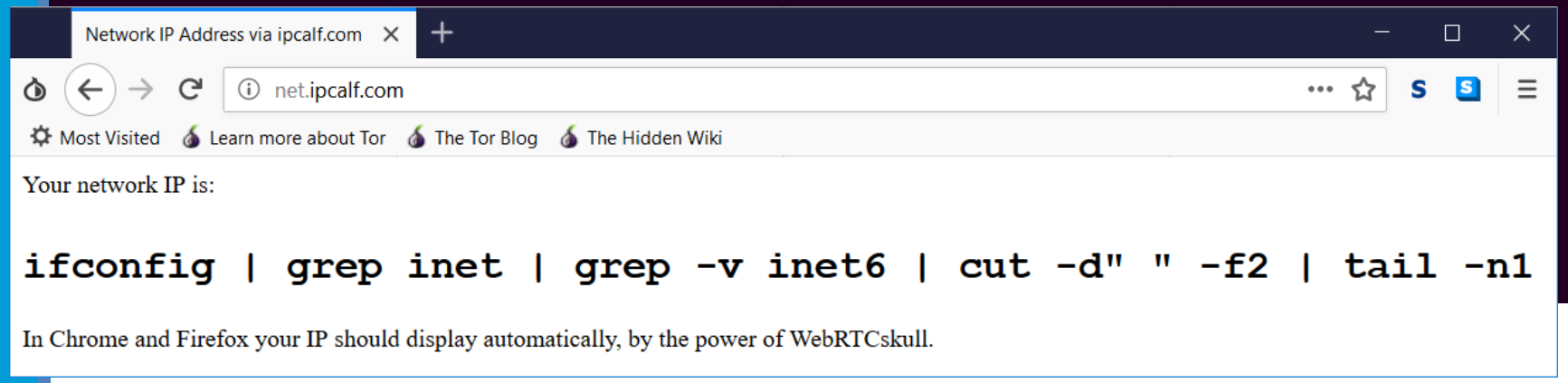
My computer as seen from a remote server

http://www.hashemian.com/whoami/

My IP previously showed as: 172.20.106.96

What happened?

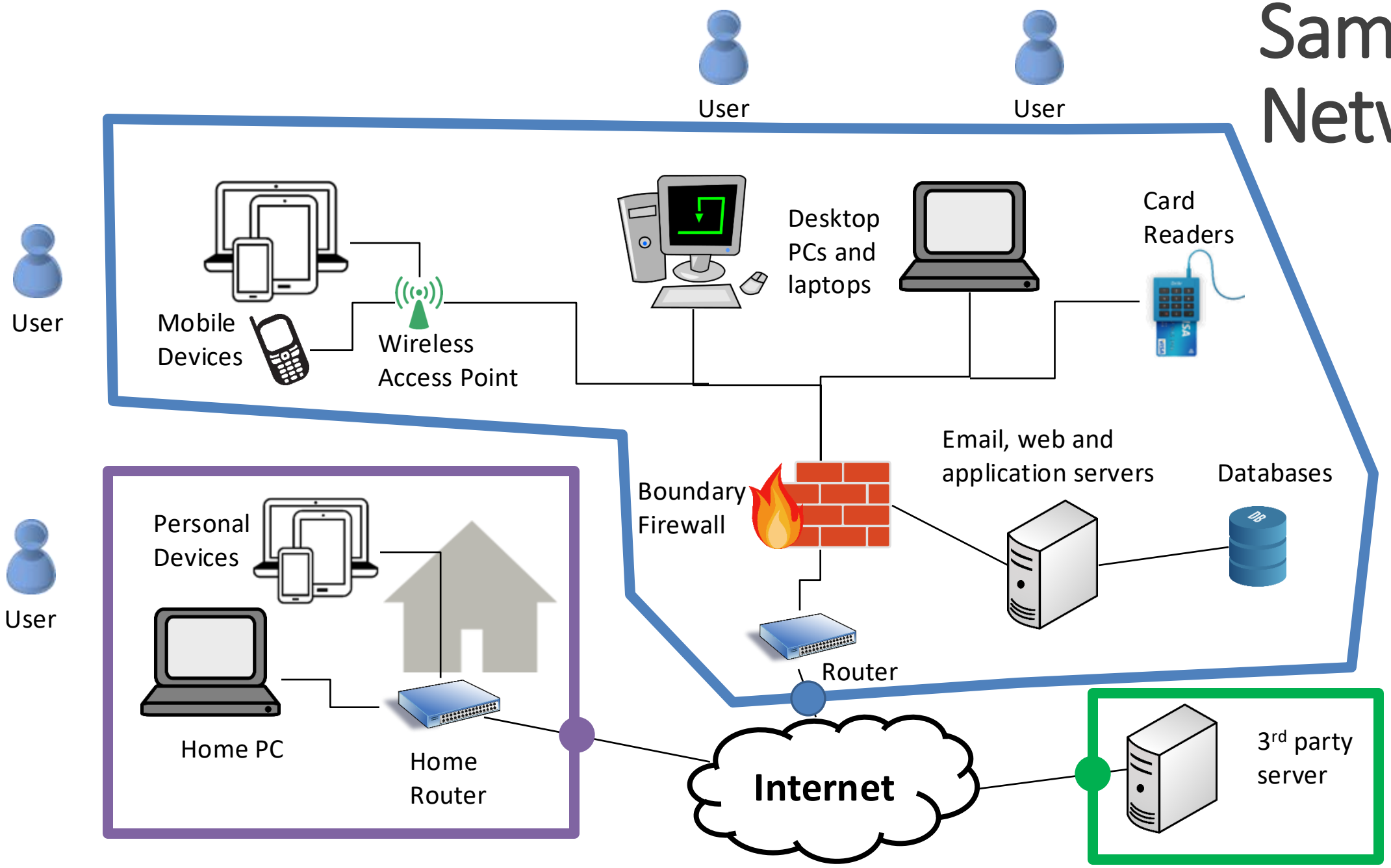
```
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.5
HTTP_CONNECTION: keep-alive
HTTP_COOKIE: __utma=145846189.271110778.1474893692.1474893692.1474893692.1; __utmc=
.1474893692.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provide
4893691768; PRUM_EPISODES=s=1474893750106&r=http%3A//www.hashemian.com/whoami/
HTTP_HOST: www.hashemian.com
HTTP_REFERER: https://www.google.co.uk/
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefo
REMOTE_ADDR: 192.41.131.255
REMOTE_PORT: 7535
REQUEST_METHOD: GET
REQUEST_TIME: 1474906336
REQUEST_URI: /whoami/
```

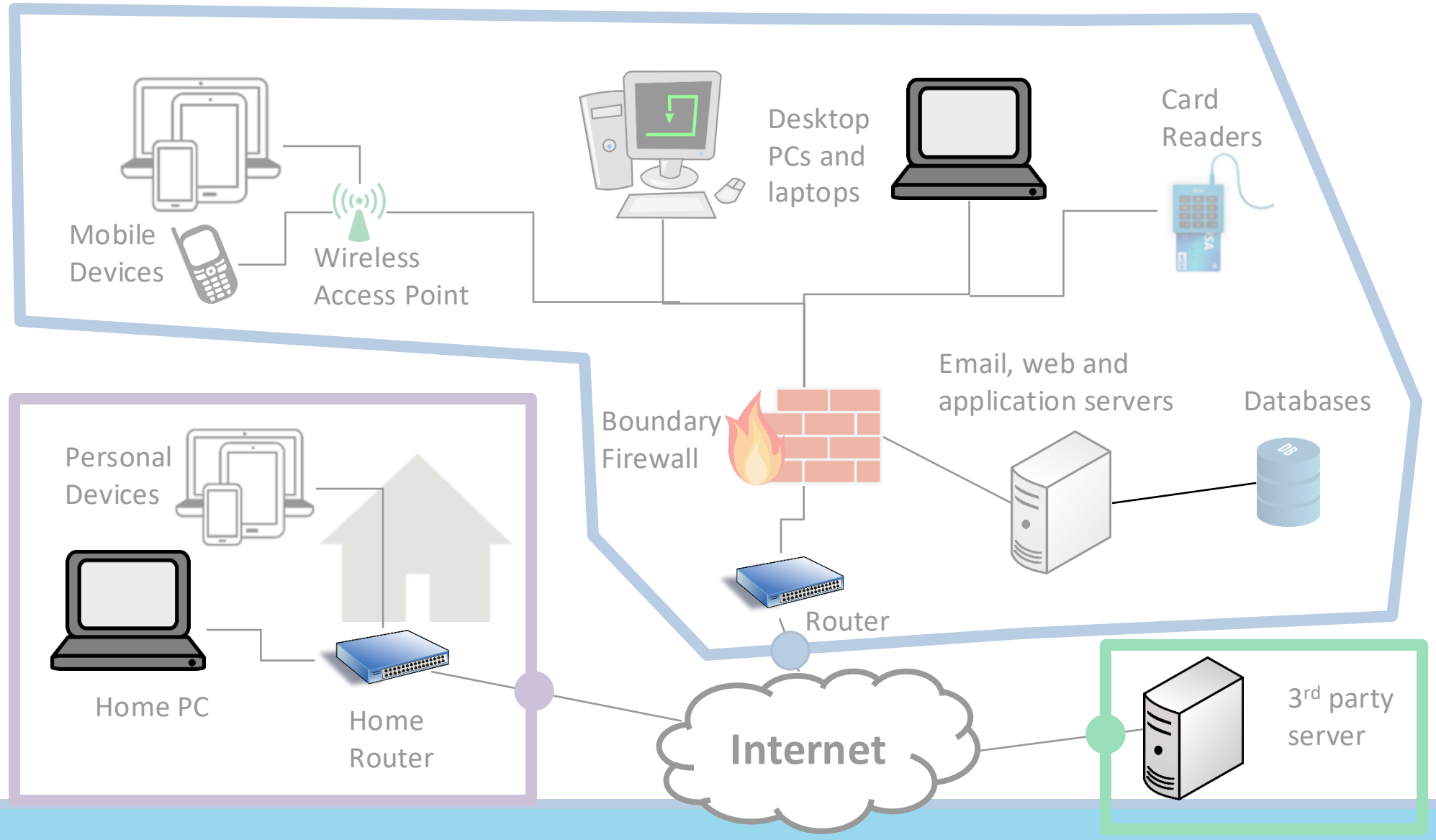


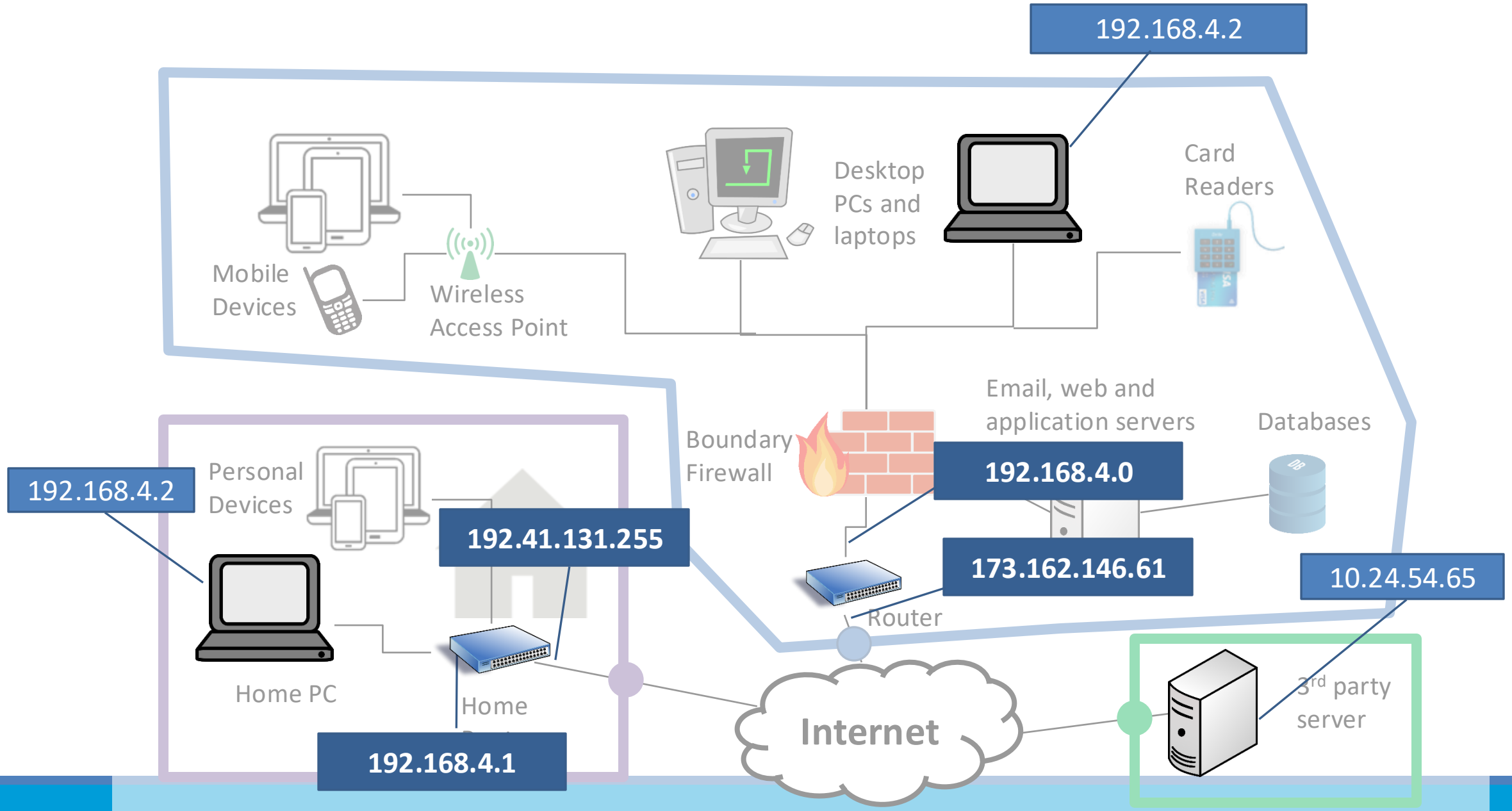
IPv4 and address space exhaustion

- Version 4 of the Internet Protocol
  - 192.168.2.6
- There are less than 4.3 billion IPv4 addresses available
- We do not have enough addresses for every device on the planet
- Answer: Network Address Translation
  - Internal IP different than external IP
  - Border router maps between its own IP and the internal ones
- Alternative Answer: IPv6?

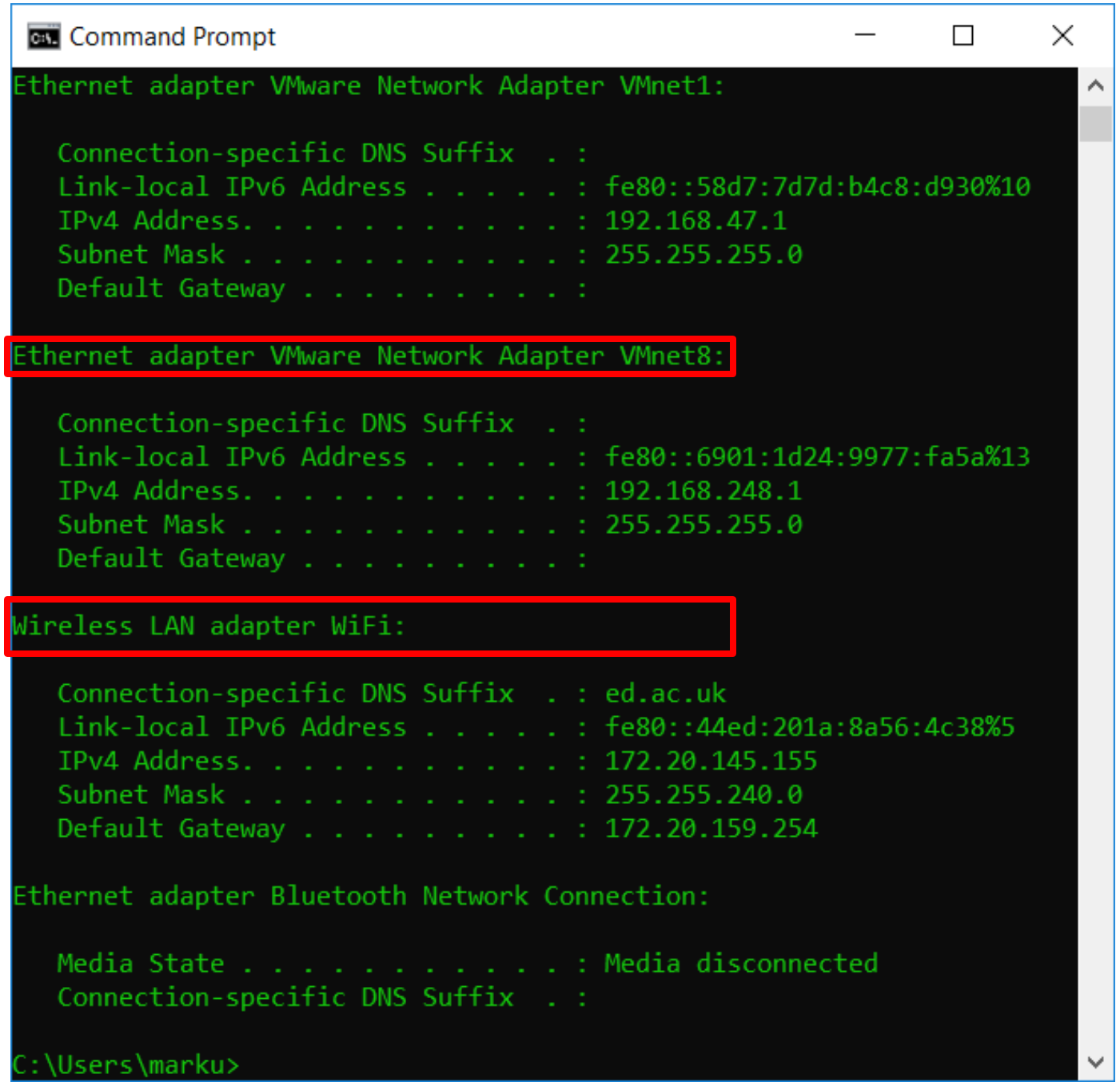
Sample Network

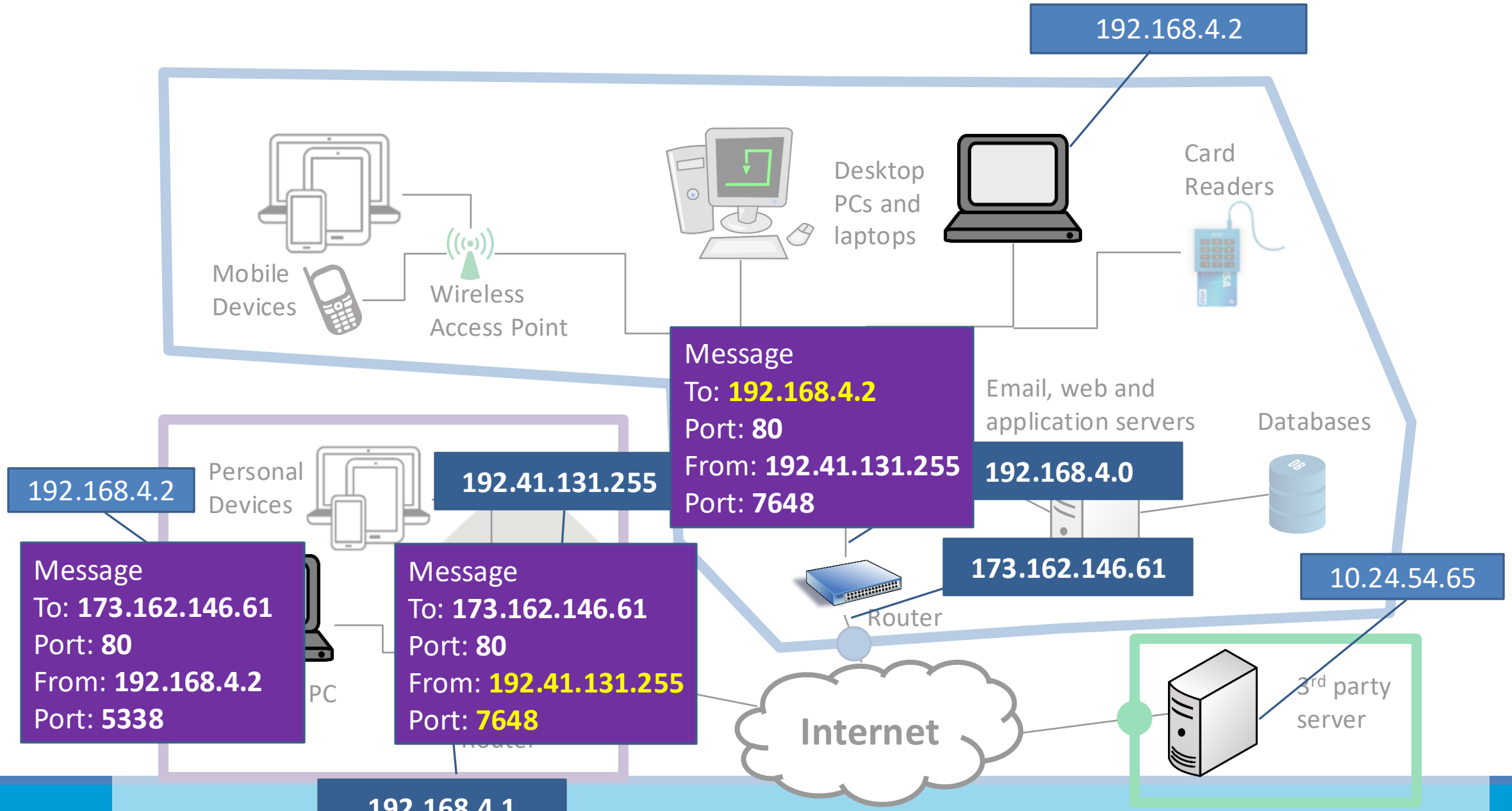



Mobile Devices
Wireless Access Point
Desktop PCs and laptops
Card Readers
Boundary Firewall
Email, web and application servers
Databases
Router
Personal Devices
Home PC
Home Router
Internet
3rd party server


192.168.4.2
Mobile Devices
Wireless Access Point
Desktop PCs and laptops
Card Readers
Email, web and application servers
Databases
Boundary Firewall
192.168.4.0
173.162.146.61
10.24.54.65
Router
192.168.4.2
Personal Devices
192.41.131.255
Home PC
Home
192.168.4.1
Internet
3rd party server

My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIFI.




192.168.4.2
Mobile Devices
Wireless Access Point
Desktop PCs and laptops
Card Readers
Message
To: 192.168.4.2
Port: 80
From: 192.41.131.255
Port: 7648
Email, web and application servers
Databases
192.168.4.0
192.168.4.2
Personal Devices
192.41.131.255
Message
To: 173.162.146.61
Port: 80
From: 192.168.4.2
Port: 5338
Message
To: 173.162.146.61
Port: 80
From: 192.41.131.255
Port: 7648
173.162.146.61
10.24.54.65
Router
PC
Internet
3rd party server
192.168.4.1

Convenience vs security/privacy

How-To Geek

How Secure Are Wi-Fi Security Cameras?

CHRIS HOFFMAN @chrisbhoffman
JUNE 17, 2018, 6:40AM EDT

Everyone's seen the horror stories. Someone placed an Internet connected camera in their home and left it open to attack, allowing strangers to eavesdrop on their most private moments. Here's how to pick a camera that guarantees your privacy.

Intrusion Detection Systems (IDS)

Firewalls are preventative, IDS detects a potential incident in progress

- At some point you have to let some traffic into and out of your network (otherwise users get upset)
- Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves
- These cannot be prevented or anticipated in advance
- The next step is to identify that something bad is happening quickly so you can address it


12:53:58
T22 COUNTDOWN

Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative)

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	True Positive	False Positive
No Alarm Sounded	False Negative	True Negative

Rule-Based Intrusion Detection

- Rules identify the types of actions that match certain known intrusion attack. Rule encode a **signature** for such an attack.
- Requires that admin anticipate attack patterns in advance
- Attacker may test attack on common signatures
- Impossible to detect a new type of attack
- High accuracy, low false positives

Statistical Intrusion Detection

- Dynamically build a statistical model of acceptable or “normal” behavior and flag anything that does not match
- Admin does not need to anticipate potential attacks
- System needs time to warm up to new behavior
- Can detect new types of attacks
- Higher false positives, lower accuracy

Base-Rate Fallacy

Suppose an IDS is 99% accurate, having a 1% chance of false positives or false negatives.

Suppose further…

- An intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Because of the success rate of the IDS, of the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative.**
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That is, roughly 99% of our alarms are false alarms.

Number of alarms is a big problem

- In the **2013 Target breach** the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a liability

Key take-aways

- Well configured Firewalls are helpful tools to defend against known attacks
- Network Address Translation allows traffic to flow from routable Internet addresses and private local area networks, but we have to be careful
- Intrusion detection systems may be able to detect malicious activity that the Firewall allows (due to usability reasons)
- A layered approach (Firewalls+IDS) is more resilient (but not perfect!)