CSCI-UA.9480 Introduction to Computer Security

Session 2.1

Networking Basics, TCP, IP and DNS

Prof. Nadim Kobeissi

Welcome to Part 2 of the course!

Part 2 discusses how computer networks work and security threats their face.

- Networking basics.
- IP, TCP and DNS.
- Denial of Service.
- Designing Secure Network Systems.
- New Secure Protocols: WireGuard.
- *With special guest Jason A. Donenfeld.*
- Practical Assignment 1 and mid-term.

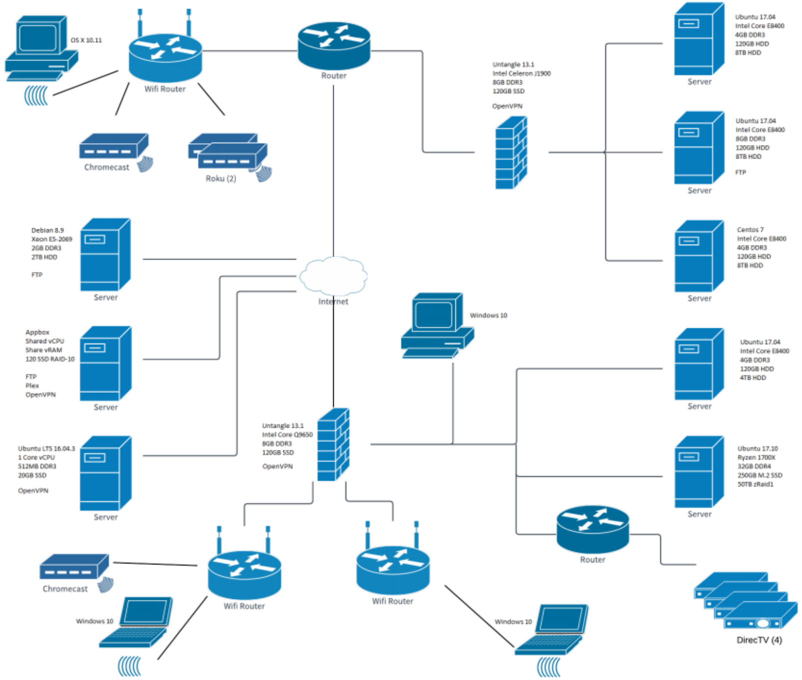
What's in a Network?

2.1a

A typical small office network.

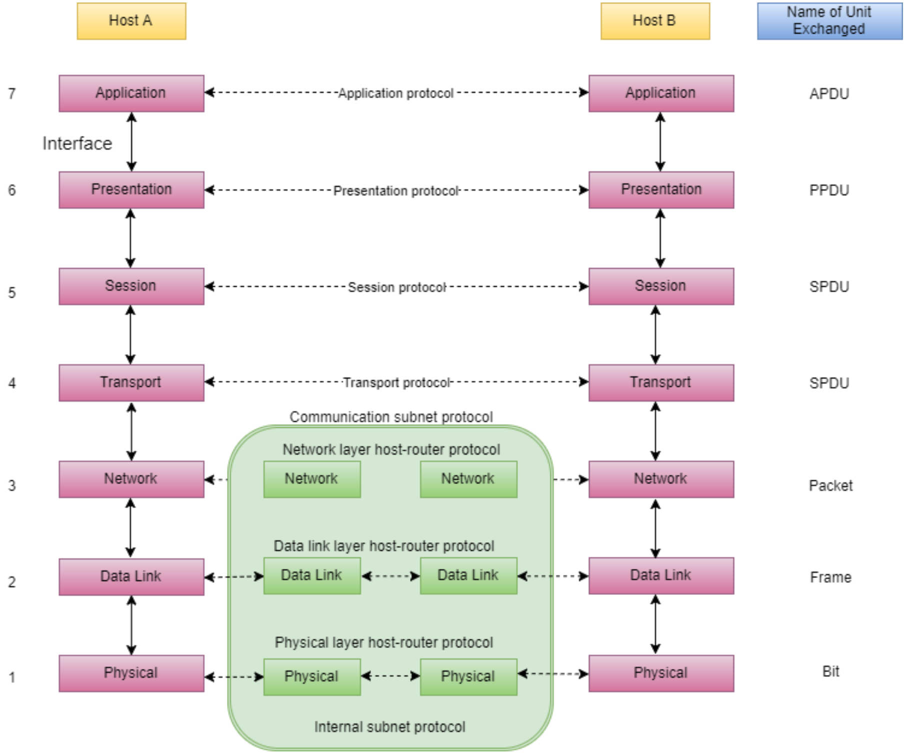
Networks contain different physical devices with different roles, entry points and attack surfaces.

- NATs and firewalls may protect intranet devices but leave routers vulnerable.
- Different device types merit different security models.



The OSI layer-based model.

1. *Physical Layer*: Wire radio…
2. *Datalink Layer*: Ethernet, WiFi, GSM…
3. *Network Layer*: IP…
4. *Transport Layer*: TCP/UDP…
5. *Session Layer*
6. *Presentation Layer*: XML/UTF-8…
7. *Application Layer*: FTP, SSH…



Test your knowledge!

At which layer would the Signal protocol operate within WhatsApp?

□ **A:** Transport layer.

□ **B:** Network layer.

□ **C:** Application layer.

Test your knowledge!

At which layer would the Signal protocol operate within WhatsApp?

□ **A:** Transport layer.

□ **B:** Network layer.

☑ **C:** Application layer.

Security Questions for Network Protocols

2.1b

"Alice and Bob?"

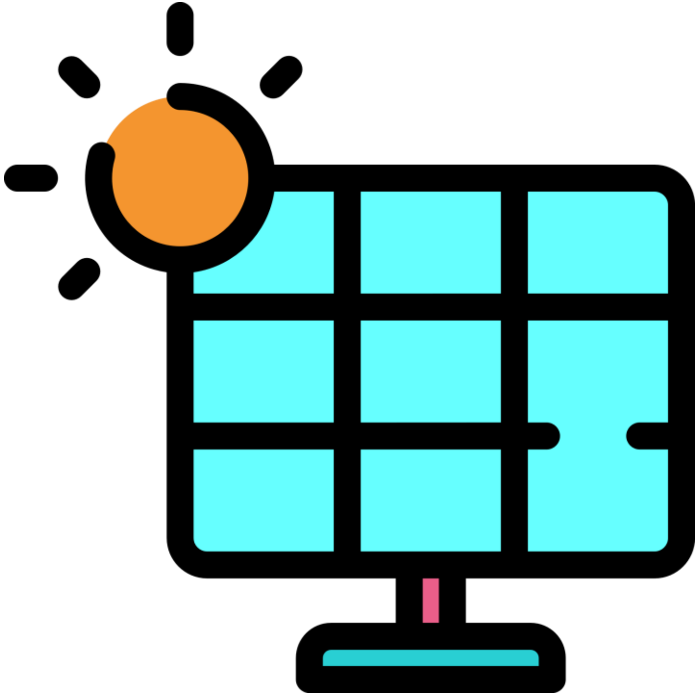
In *protocols*, we reason about:

- Principals: Alice, Bob.
- Security goals: confidentiality, authenticity, forward secrecy...
- Use cases and constraints.
- Attacker model.
- Threat model.

“Application Security.”

In *applications* and many *user-facing systems*, we reason about:

- User compromise: device compromise, impersonation, phishing…
- Server compromise: leaks, database hacks…
- Usability and security.



Additional concerns for networks.

In networks, we also focus on:

- *Availability*: can the network be prevented from operating?
- *Access control*: who is allowed to access, affect or manage data flows?

Test your knowledge!

Which security property would *denial of service* affect?

□ **A**: Availability.

□ **B**: Access control.

□ **C**: Confidentiality.

Test your knowledge!

Which security property would *denial of service* affect?

☑ **A:** `Availability.`

□ **B:** `Access control.`

□ **C:** `Confidentiality.`

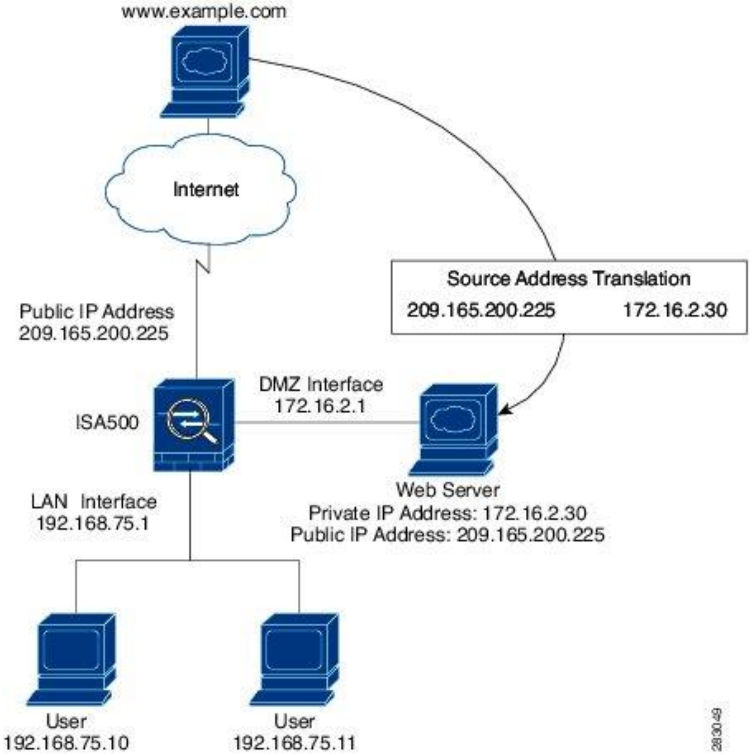
A Closer Look at Network Components

2.1c

IP: Internet Protocol.

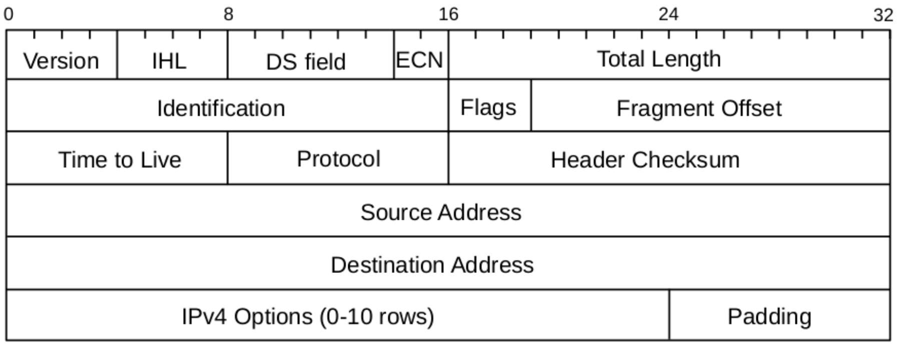
IPv4: 172.26.85.153

- *IPv6*: fe80::7d44:8c17:e19b:6e73
- Public address spaces versus private address spaces.
- IP has *no source authentication*: we're trusting the client to embed the correct source IP.
- Anyone can send any packet with any source IP. Response will be sent back to this source IP.



IPv4: Internet Protocol version 4.

- Introduced in September 1981.
- Does not guarantee delivery or proper sequencing of messages.
- Addresses are a sequence of four bytes.



Version	IHL	DS field	ECN	Total Length
Identification			Flags	Fragment Offset
Time to Live		Protocol		Header Checksum
Source Address				
Destination Address				
IPv4 Options (0-10 rows)				Padding

Test your knowledge!

How many potential IPv4 addresses could exist on the Internet?

□ **A:** 32!

□ **B:** 256^4

□ **C:** 2^{32}

Test your knowledge!

How many potential IPv4 addresses could exist on the Internet?

□ **A:** 32!

☑ **B:** 256^4

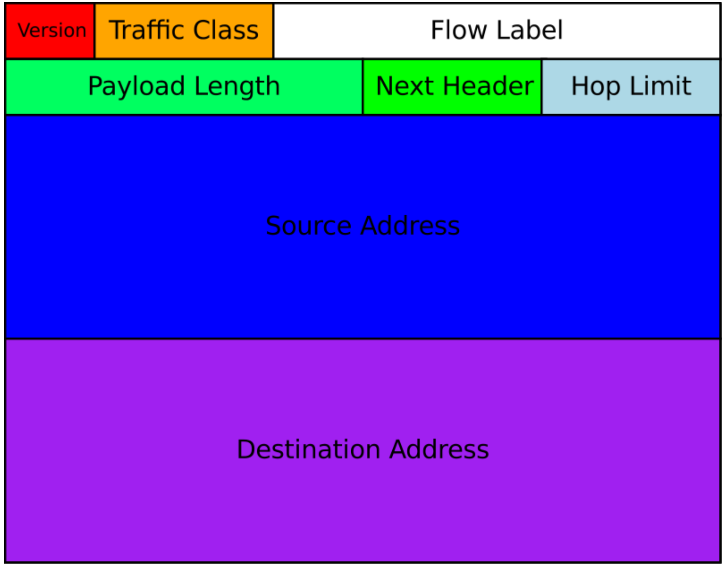
☑ **C:** 2^{32}

IPv6: Internet Protocol version 6.

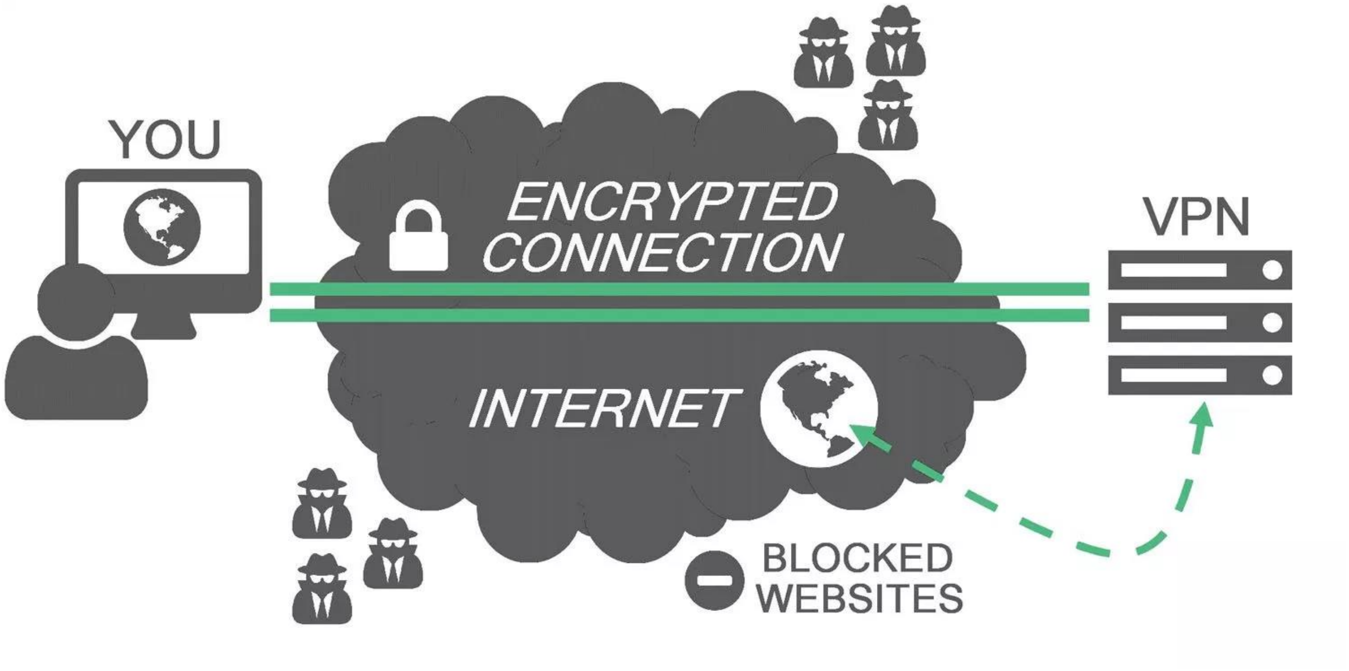
Introduced in 1998, standardized in 2017.

Today, 20% of Internet traffic.

- Address space of 2^{128} compared to 2^{32} for IPv4.
- No need for Network Address Translation (NAT).
- Flow Labeling allows for more efficient packet handling.



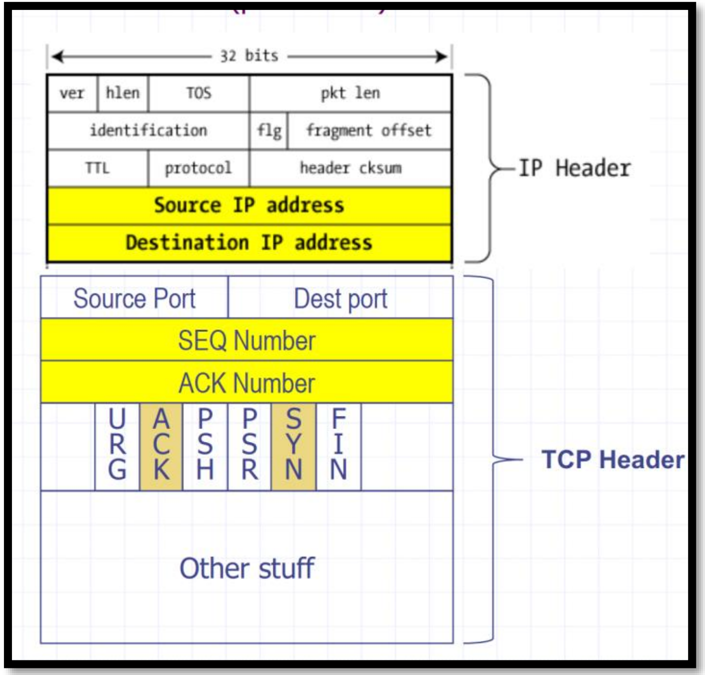
IP: Virtual Private Networks (VPNs.)



TCP: Transmission Control Protocol.

Delivers packets in-order (unlike UDP.)

- Sends a packet stream to a particular socket/port on a client.
- Contains error recovery logic (unlike UDP.)

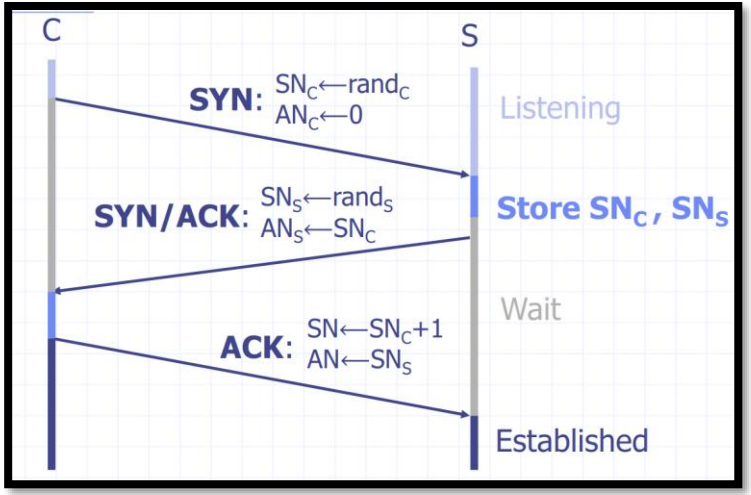


Source: Prof. Dan Boneh.

TCP: Transmission Control Protocol.

Basic security problems:

- Network packets pass by untrusted hosts.
- TCP state easily obtained via eavesdropping.
- Denial of Service vulnerabilities.

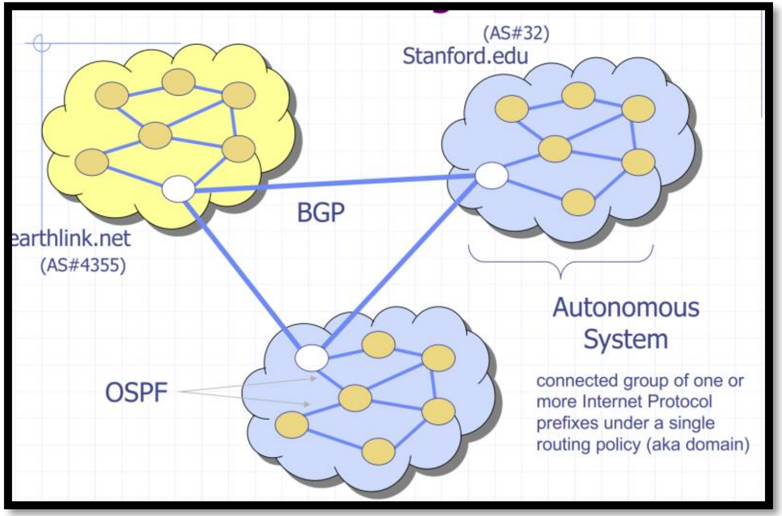

C
S
SYN: $SN_C \leftarrow rand_C$ $AN_C \leftarrow 0$
Listening
SYN/ACK: $SN_S \leftarrow rand_S$ $AN_S \leftarrow SN_C$
Store SN_C, SN_S
Wait
ACK: $SN \leftarrow SN_C+1$ $AN \leftarrow SN_S$
Established

Source: Prof. Dan Boneh.

BGP: Routing between autonomous systems.

BGP routes between “autonomous systems”, for example your city’s ISP and an ISP in another continent.

- Route updates are unauthenticated.
- *“After receiving a censorship order from the telecommunications ministry directing that YouTube.com be blocked, Pakistan Telecom went even further. By accident or design, the company broadcast instructions worldwide claiming to be the legitimate destination for anyone trying to reach YouTube's range of Internet addresses.” – CNet News*

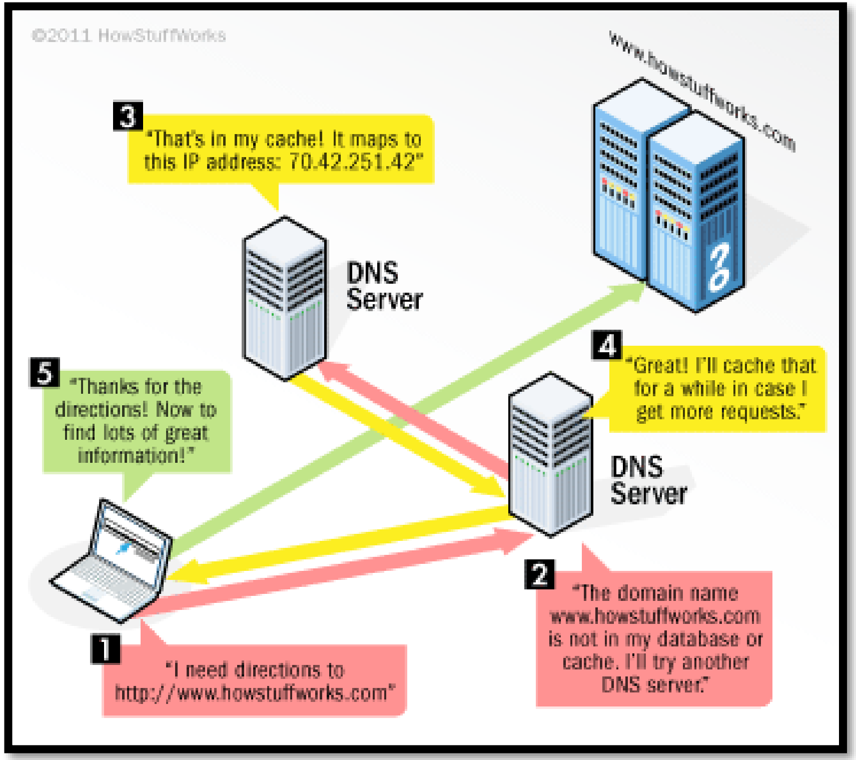

(AS#32)
Stanford.edu
earthlink.net
(AS#4355)
BGP
OSPF
Autonomous System
connected group of one or more Internet Protocol prefixes under a single routing policy (aka domain)

Source: Prof. Dan Boneh.

DNS: Domain Name System.

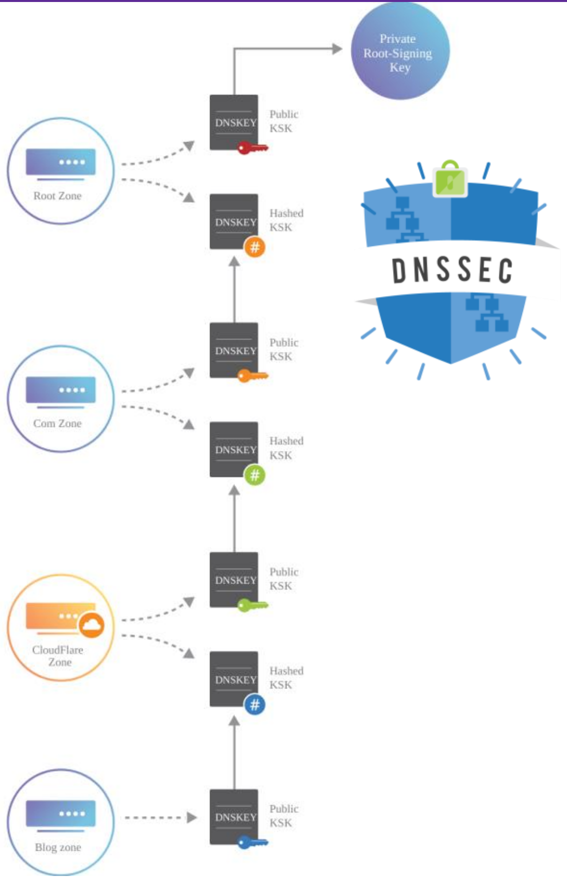
DNS servers contain maps translating IP addresses to domain names.

- Name servers advertise to each other which IP addresses domains want to map each other to.
- A record: IP address.
- CNAME record: other domain.
- MX record: mail addresses.
- TXT record: arbitrary text value.
- Etc.


©2011 HowStuffWorks
www.howstuffworks.com
3
"That's in my cache! It maps to this IP address: 70.42.251.42"
DNS Server
4
"Great! I'll cache that for a while in case I get more requests."
5
"Thanks for the directions! Now to find lots of great information!"
DNS Server
2
"The domain name www.howstuffworks.com is not in my database or cache. I'll try another DNS server."
1
"I need directions to http://www.howstuffworks.com"

DNSSEC.

- Attempts to force DNS requests to include credentials certifying that they are correct.
- DNS records are cryptographically signed through new DNS record types: `RRSIG, DNSKEY, DS,` NSEC, etc.
- Chain of signatures goes from the root zone to the website being protected (here, Cloudflare is an optional CDN.)



Interesting Experiments to Try.

- Trace route: see the IP routing path to an address.
- Nmap: Port scanning a server.
- Dig: show DNS records.

Test your knowledge!

Which security property does DNSSEC attempt to provide?

- □ **A**: Confidentiality.
- □ **B**: Authenticity.
- □ **C**: Access Control.

Test your knowledge!

Which security property does DNSSEC attempt to provide?

□ **A:** Confidentiality.

☑ **B:** Authenticity.

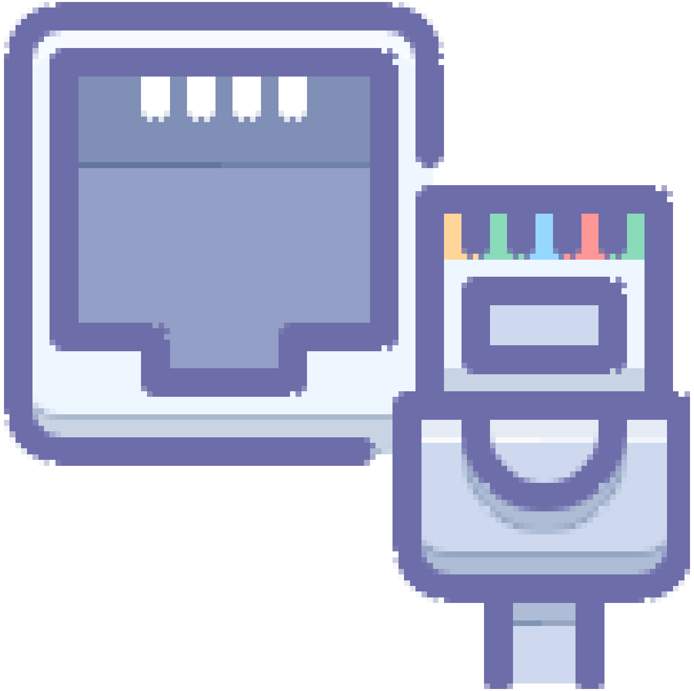
□ **C:** Access Control.

Some Examples

2.1d

Ethernet.

- *Confidentiality*: None. Even the wire itself may be a side-channel (TEMPEST).
- *Integrity*: None.
- *Availability*: Physical attacks, jamming, denial of service on endpoints…
- *Access control*: MAC filtering (easily bypassed.)



WiFi.

- *Confidentiality, integrity*:
  - Open: none.
  - WEP: broken.
  - WPA2: KRACK. WPA3 incoming.
  - SSID spoofing?
- *Availability*: Physical attacks, jamming, denial of service on endpoints…
- *Access control*: MAC filtering (easily bypassed), RADIUS, WPA-PSK…

GSM.

- *Confidentiality, integrity*:
    - A5/1 (US/EU): Broken.
    - A5/2: Broken in real-time (Goldberg et al)
    - A5/3 (KASUMI):
        - 2003: Downgrade attack to A5/2.
        - 2010: Shown to be broken unlike original design (MISTY1.)
- *Availability*: Physical attacks, jamming, denial of service on endpoints…
- *Access control*: SIM.

Next time:
Denial of Service

2.2