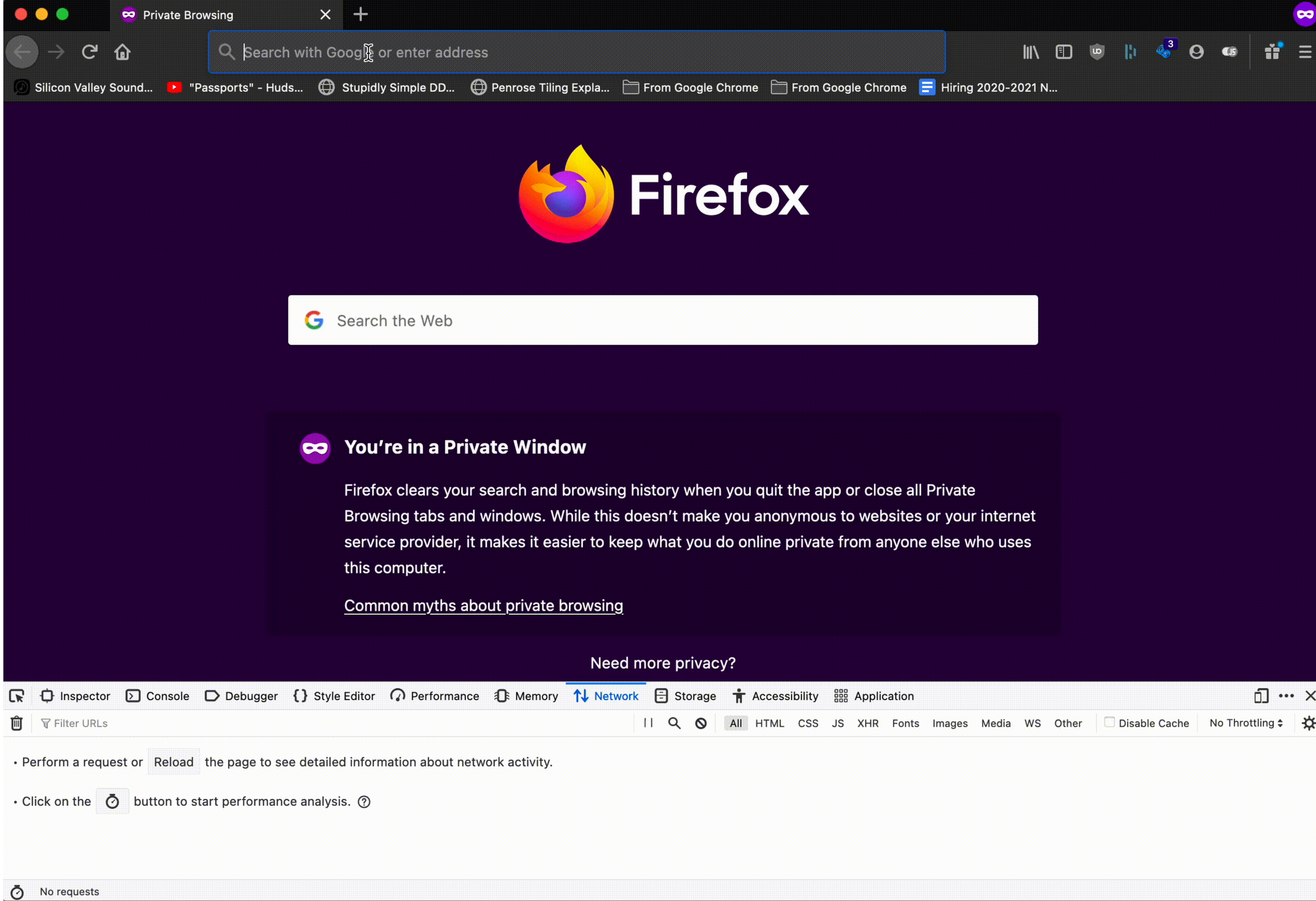
2550 Intro to cybersecurity

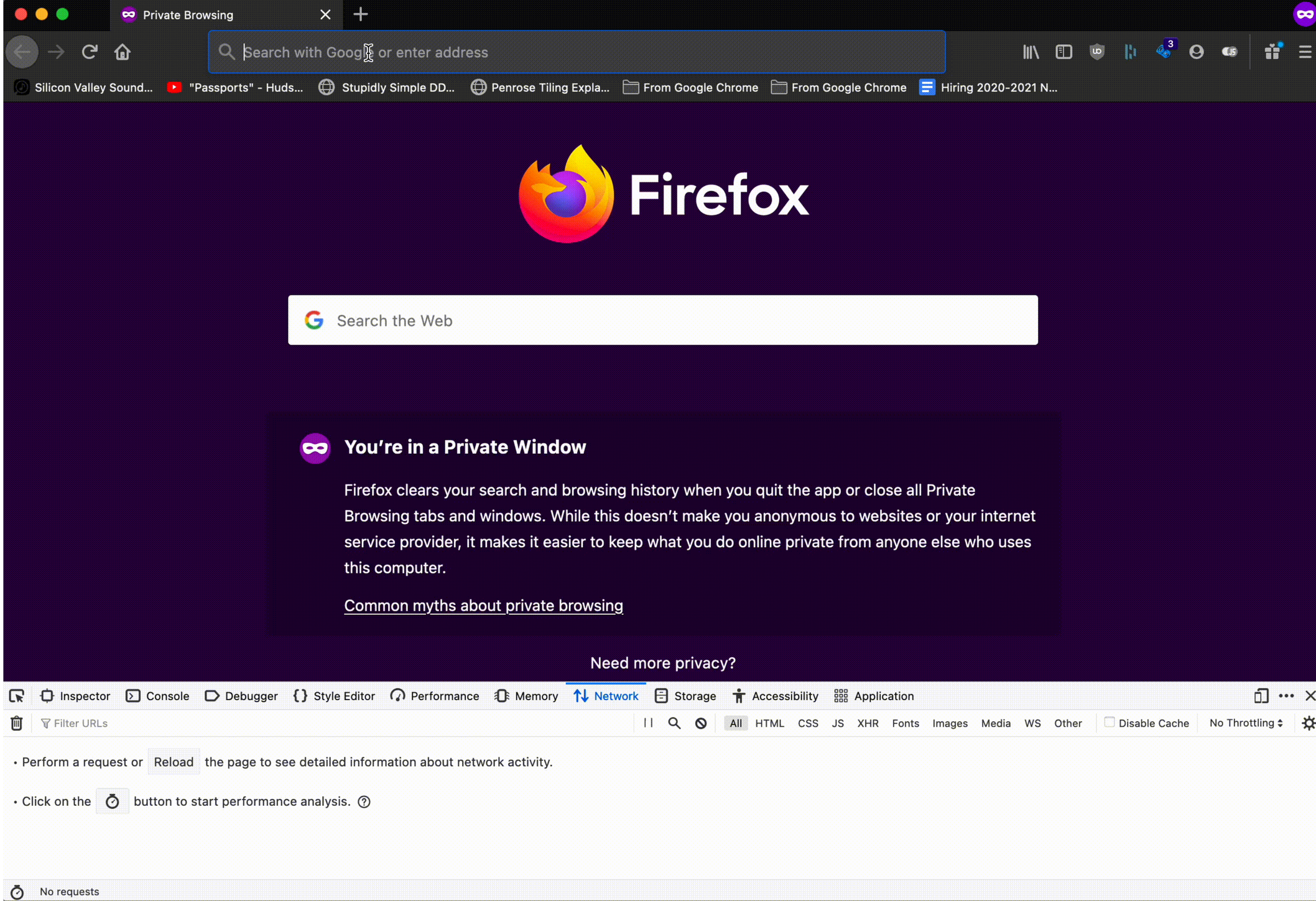
L25: Networking

abhi shelat

How does this work?

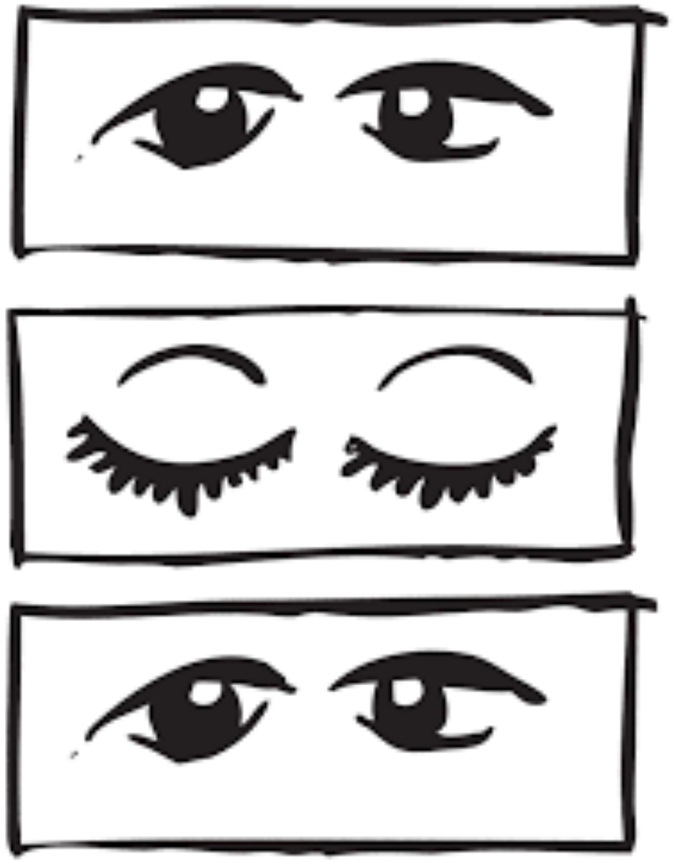


How does this work?



Networks

How long does it take to blink?



People also ask

How long is a blink of an eye?

The **duration** of a **blink** is on average 100–150 milliseconds according to UCL researcher and between 100–400 ms according to the Harvard Database of Useful Biological Numbers. Closures in excess of 1000 ms were defined as microsleeps.

en.wikipedia.org › wiki › Blinking

Blinking - Wikipedia

Search for: How long is a blink of an eye?

Network protocols

Wifi/Ethernet

Network protocols

HTTP

TLS

DNS

TCP

IP

Wifi/Ethernet

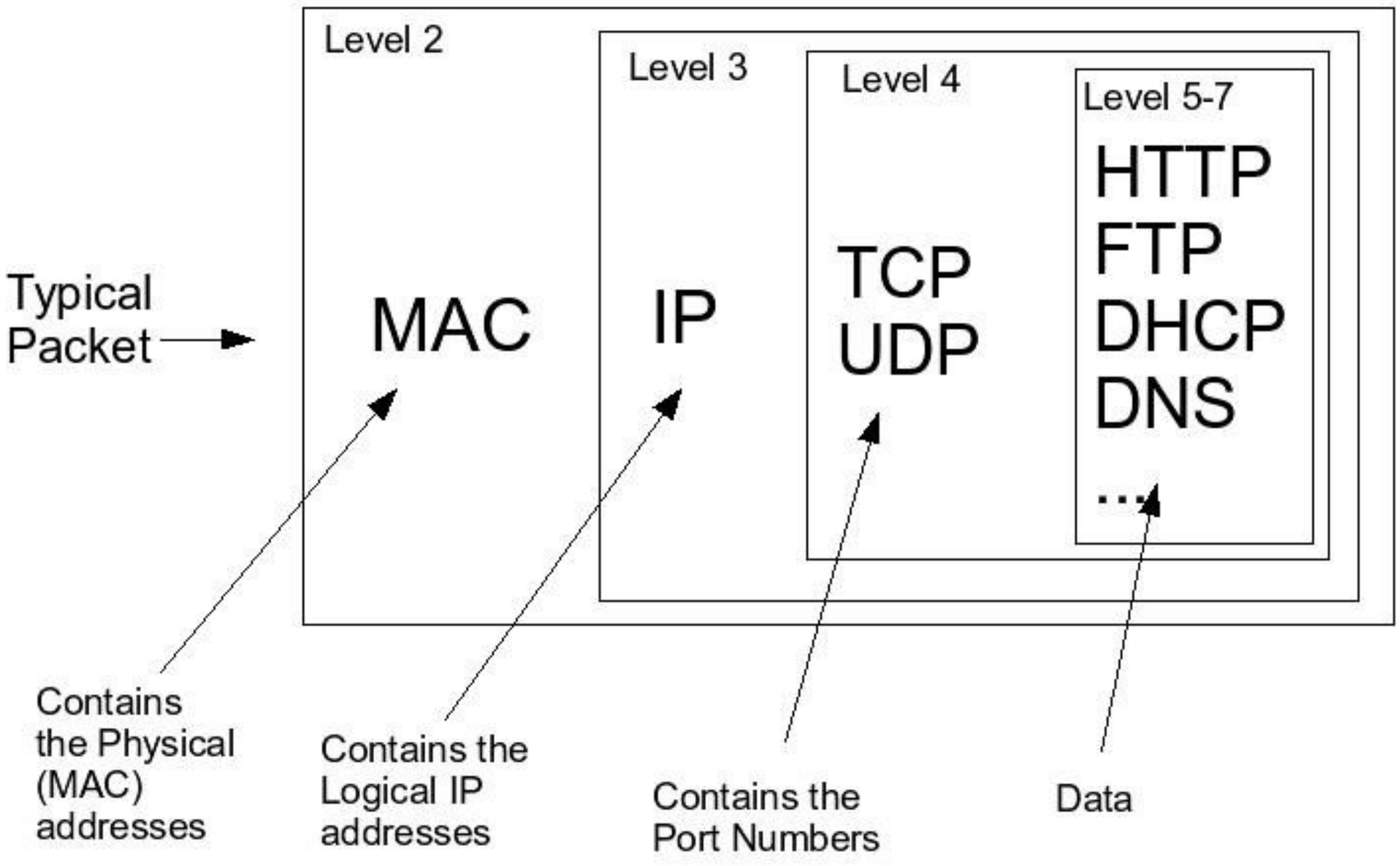
Packet-switched networks

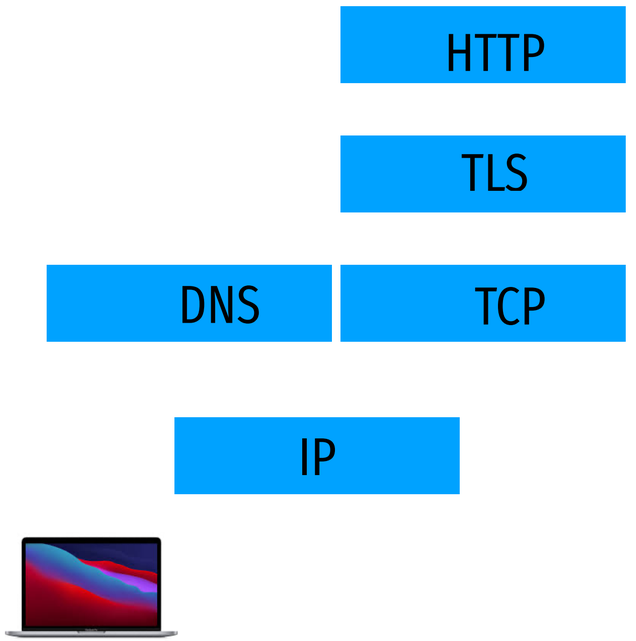
Machines communicate by breaking their messages into small packets. These small packets include information about how to get to their destination. Each protocol “on the stack” has its packet format.

Incredibly fast & efficient today

```
MacBook-Pro:demos abhi$ ping www.northeastern.edu
PING e12215.dscb.akamaiedge.net (23.38.112.43): 56 data bytes
64 bytes from 23.38.112.43: icmp_seq=0 ttl=59 time=15.304 ms
64 bytes from 23.38.112.43: icmp_seq=1 ttl=59 time=23.825 ms
64 bytes from 23.38.112.43: icmp_seq=2 ttl=59 time=19.247 ms
64 bytes from 23.38.112.43: icmp_seq=3 ttl=59 time=14.852 ms
64 bytes from 23.38.112.43: icmp_seq=4 ttl=59 time=20.334 ms
64 bytes from 23.38.112.43: icmp_seq=5 ttl=59 time=20.111 ms
64 bytes from 23.38.112.43: icmp_seq=6 ttl=59 time=14.169 ms
64 bytes from 23.38.112.43: icmp_seq=7 ttl=59 time=21.056 ms
^C
```

Anatomy of a Packet





Packet Encapsulation is like

Packet Encapsulation is like

How packets are formed

Remember this demo:

```
MacBook-Pro:demos abhi$ nc shelat.khoury.neu.edu 80
GET / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Server: nginx/1.12.2
Date: Tue, 13 Apr 2021 12:31:15 GMT
Content-Type: text/html
Content-Length: 185
Connection: close
Location: https://localhost/

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.12.2</center>
</body>
</html>
```

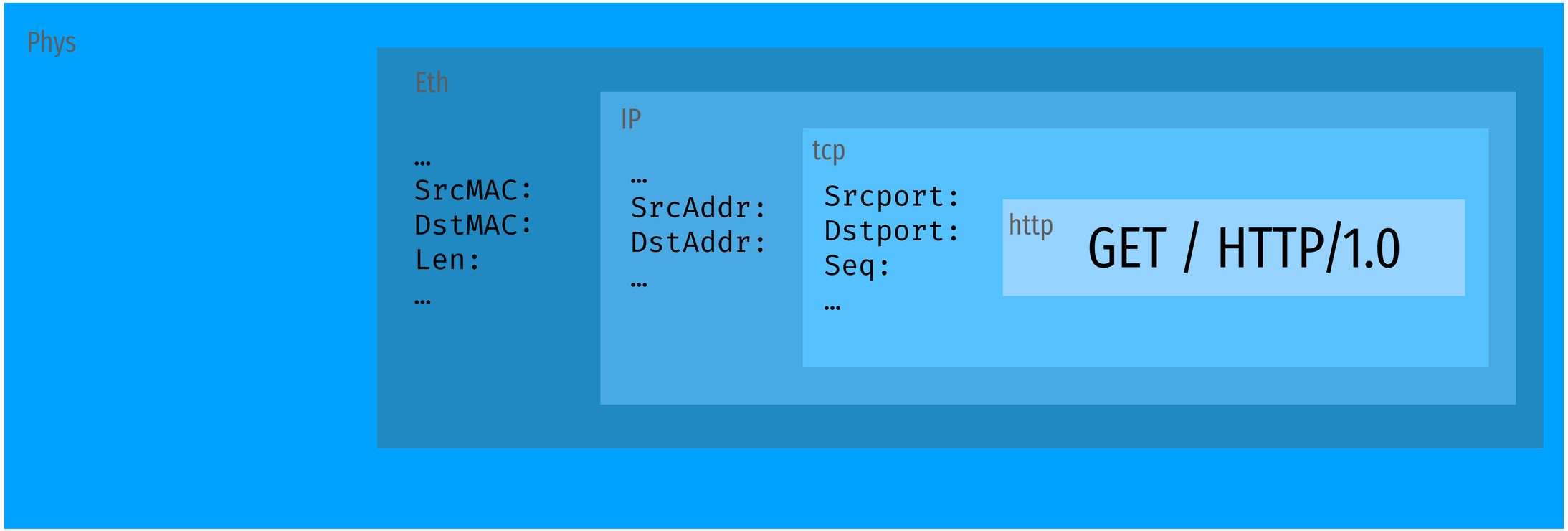
How data is encapsulated

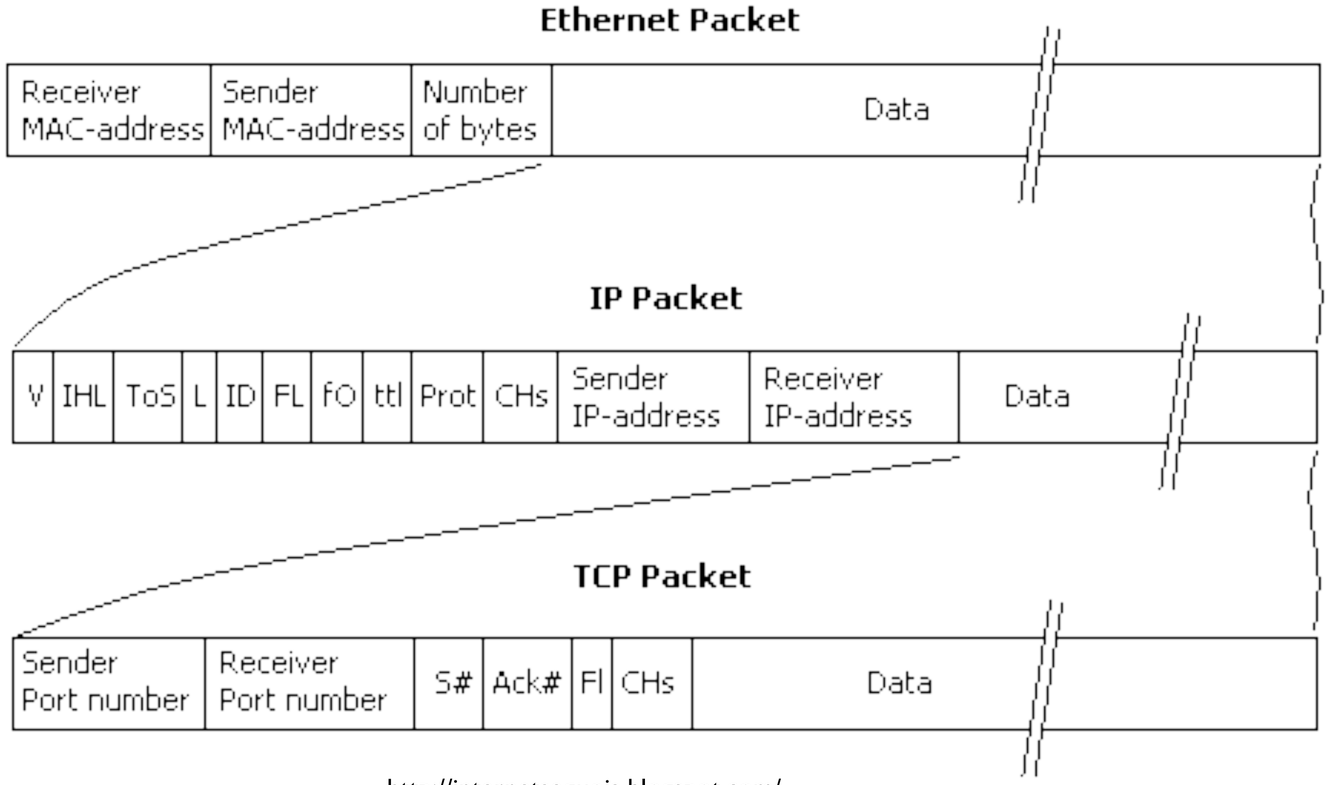
How data is encapsulated

How data is encapsulated

How data is encapsulated

How data is encapsulated



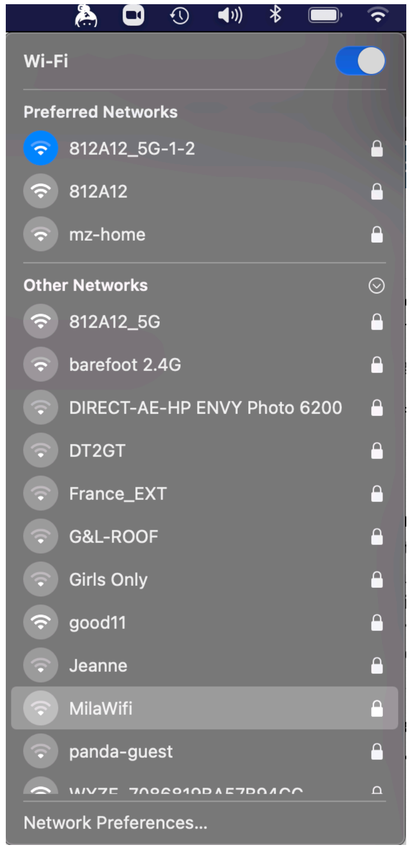


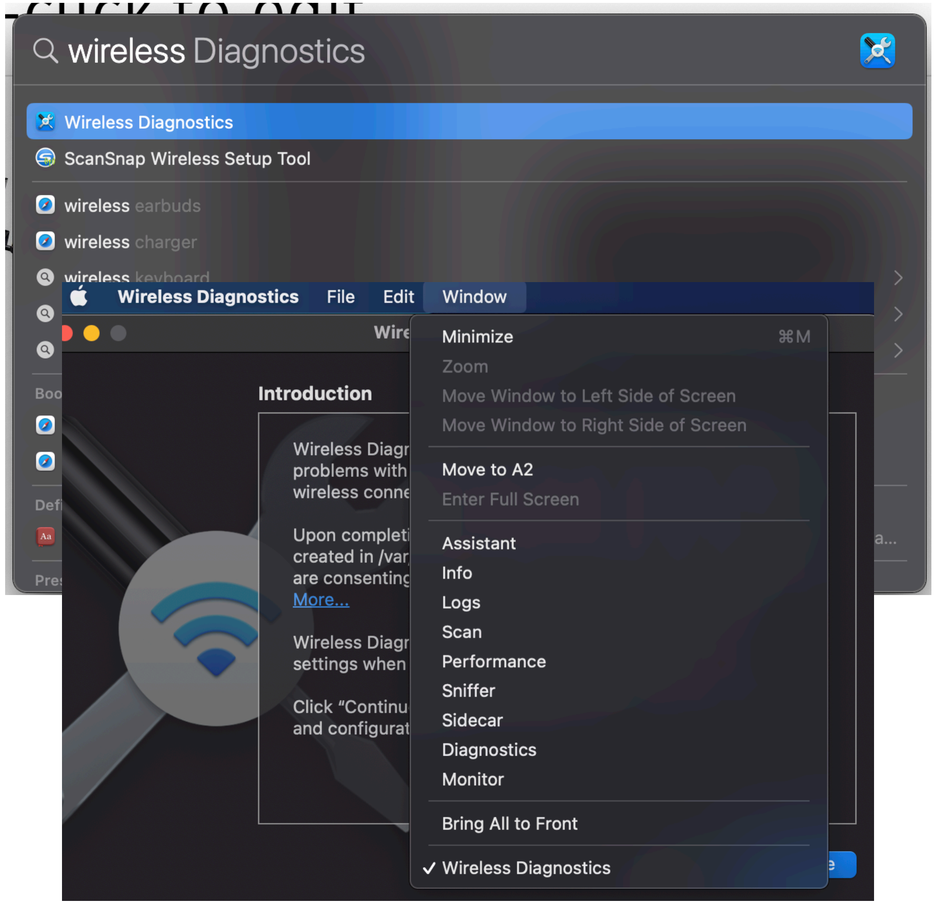
http://internetsequoia.blogspot.com/

http://learn-networking.com/tcp-ip/how-the-internet-layer-works

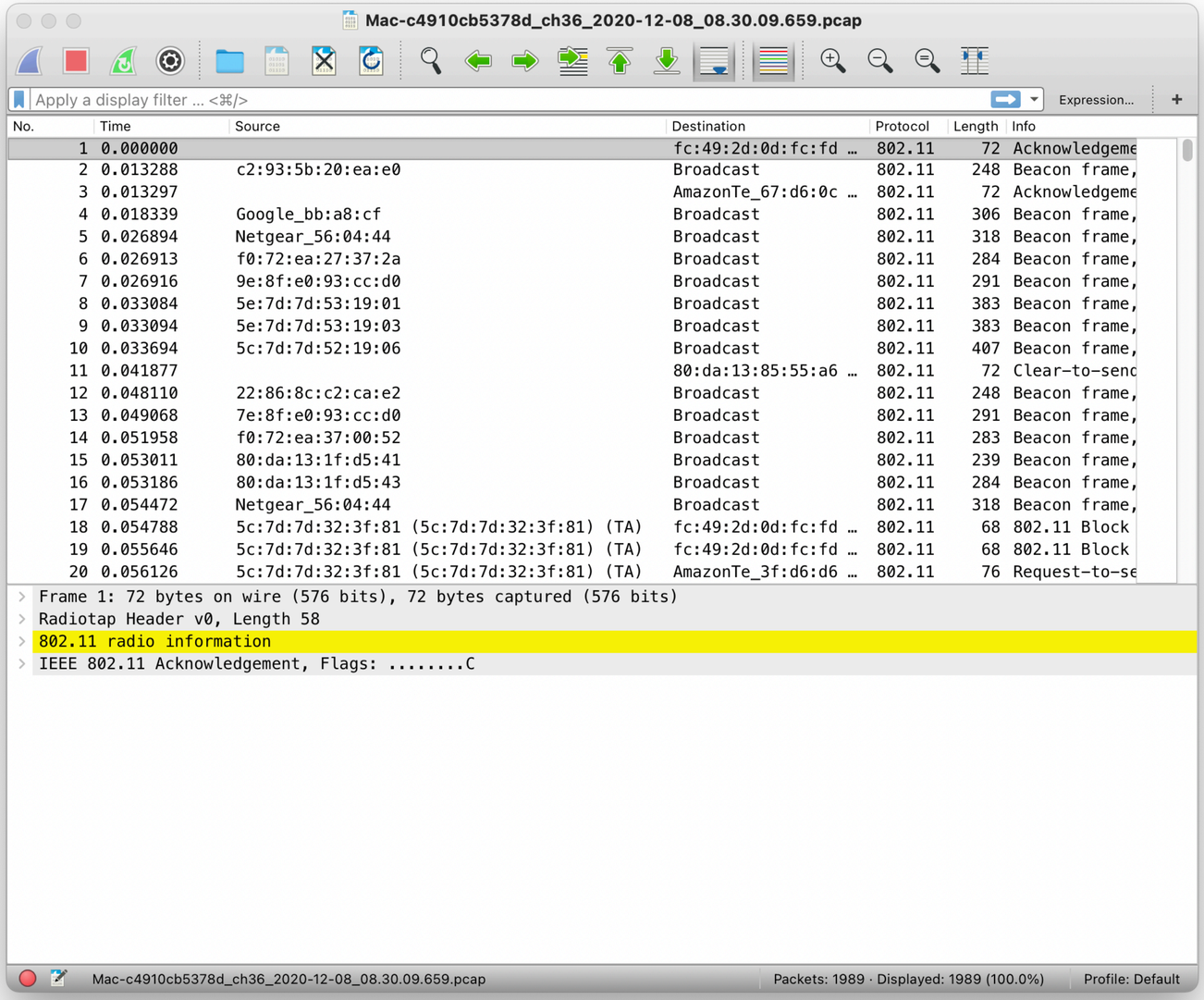
A more detailed picture of the previous cartoon

How to inspect packets





Wireshark

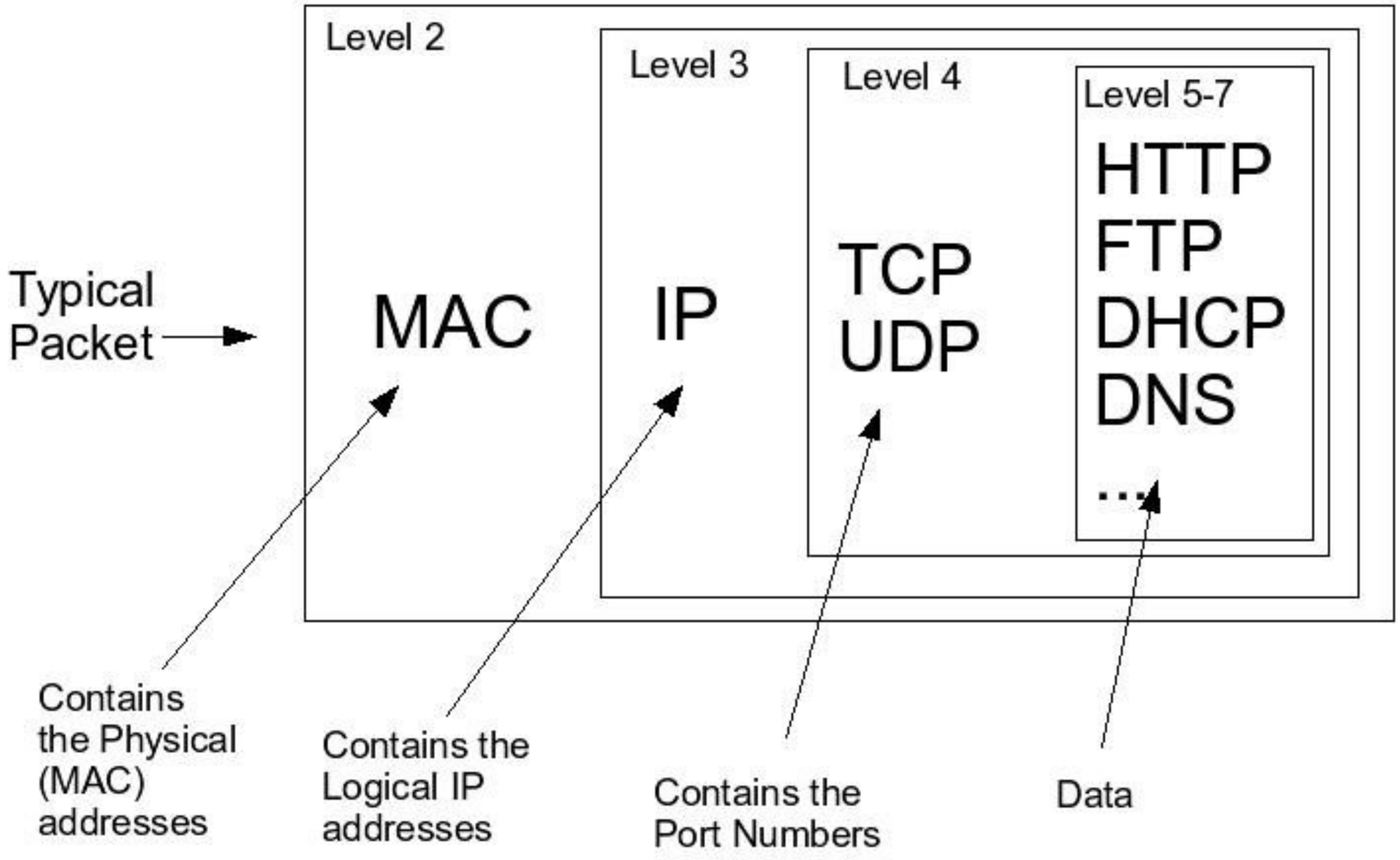


See course page for link to channel6.pcap file.

traceroute

```
MacBook-Pro:Desktop abhi$ traceroute -A www.northeastern.edu
traceroute: Warning: www.northeastern.edu has multiple addresses; using 23.38.112.43
traceroute to e12215.dscb.akamaiedge.net (23.38.112.43), 64 hops max, 52 byte packets
 1  [AS0] router.asus.com (192.168.1.1)  4.343 ms  3.298 ms  3.188 ms
 2  [AS7922] 96.120.67.185 (96.120.67.185)  10.345 ms  11.228 ms  10.395 ms
 3  [AS33657] 24.124.212.73 (24.124.212.73)  10.965 ms  10.040 ms  10.032 ms
 4  [AS7922] 162.151.150.6 (162.151.150.6)  9.843 ms  9.079 ms  9.787 ms
 5  [AS7922] be-334-ar01.needham.ma.boston.comcast.net (96.108.70.141)  12.047 ms  12.082 ms  12.034 ms
 6  [AS7922] 50-222-48-18-static.hfc.comcastbusiness.net (50.222.48.18)  17.514 ms  17.504 ms  19.669 ms
 7  [AS35994] a23-38-112-43.deploy.static.akamaitechnologies.com (23.38.112.43)  12.001 ms  14.432 ms  12.884 ms
MacBook-Pro:Desktop abhi$
```

Anatomy of a packet

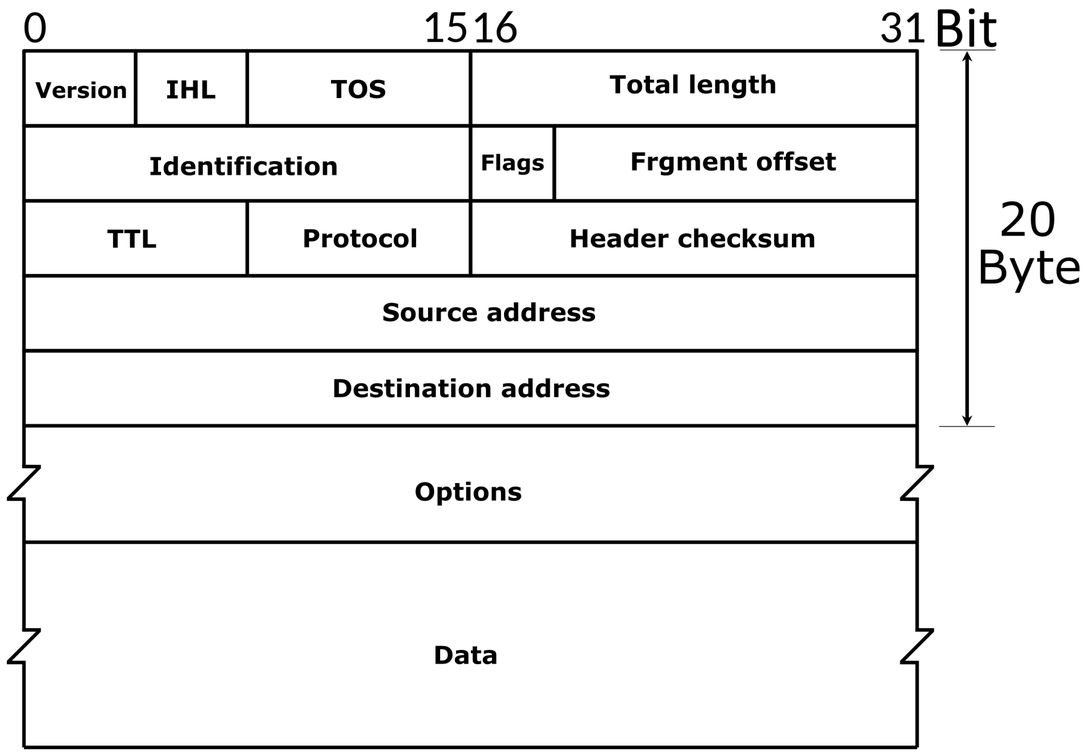


Example packet capture

```
2020-12-08 14:11:07.473254 42:01:0a:96:00:01 > 42:01:0a:96:00:03, IPv4, length 587: (tos 0×0, ttl 47, id 0, offset 0, flags [DF], proto TCP (6), length 573)
    24.147.105.137.53946 > 10.150.0.3.8000: tcp 521
      0×0000:  4201 0a96 0003 4201 0a96 0001 0800 4500  B.....B.......E.
      0×0010:  023d 0000 4000 2f06 bd06 1893 6989 0a96  •=..@./.....i...
      0×0020:  0003 d2ba 1f40 e734 de06 3b40 95fc 8018  .....@.4..;@....
      0×0030:  0800 1a3b 0000 0101 080a 064a fe59 9a5b  ...;.......J.Y.[
      0×0040:  8cc8 504f 5354 202f 6c6f 6769 6e20 4854  ..POST./login.HT
      0×0050:  5450 2f31 2e31 0d0a 486f 7374 3a20 6c32  TP/1.1..Host:.l2
      0×0060:  342e 6e65 7563 7279 7074 2e6f 7267 3a38  4.neucrypt.org:8
      0×0070:  3030 300d 0a4f 7269 6769 6e3a 2068 7474  000..Origin:.htt
      0×0080:  703a 2f2f 6c32 342e 6e65 7563 7279 7074  p://l24.neucrypt
      0×0090:  2e6f 7267 3a38 3030 300d 0a43 6f6e 7465  .org:8000..Conte
      0×00a0:  6e74 2d54 7970 653a 2061 7070 6c69 6361  nt-Type:.applica
      0×00b0:  7469 6f6e 2f78 2d77 7777 2d66 6f72 6d2d  tion/x-www-form-
      0×00c0:  7572 6c65 6e63 6f64 6564 0d0a 4163 6365  urlencoded..Acce
      0×00d0:  7074 2d45 6e63 6f64 696e 673a 2067 7a69  pt-Encoding:.gzi
      0×00e0:  702c 2064 6566 6c61 7465 0d0a 436f 6e6e  p,.deflate..Conn
      0×00f0:  6563 7469 6f6e 3a20 6b65 6570 2d61 6c69  ection:.keep-ali
      0×0100:  7665 0d0a 5570 6772 6164 652d 496e 7365  ve..Upgrade-Inse
      0×0110:  6375 7265 2d52 6571 7565 7374 733a 2031  cure-Requests:.1
      0×0120:  0d0a 4163 6365 7074 3a20 7465 7874 2f68  ..Accept:.text/h
      0×0130:  746d 6c2c 6170 706c 6963 6174 696f 6e2f  tml,application/
      0×0140:  7868 746d 6c2b 786d 6c2c 6170 706c 6963  xhtml+xml,applic
      0×0150:  6174 696f 6e2f 786d 6c3b 713d 302e 392c  ation/xml;q=0.9,
      0×0160:  2a2f 2a3b 713d 302e 380d 0a55 7365 722d  */*;q=0.8..User-
      0×0170:  4167 656e 743a 204d 6f7a 696c 6c61 2f35  Agent:.Mozilla/5
      0×0180:  2e30 2028 4d61 6369 6e74 6f73 683b 2049  .0.(Macintosh;.I
      0×0190:  6e74 656c 204d 6163 204f 5320 5820 3130  ntel.Mac.OS.X.10
      0×01a0:  5f31 355f 3629 2041 7070 6c65 5765 624b  _15_6).AppleWebK
      0×01b0:  6974 2f36 3035 2e31 2e31 3520 284b 4854  it/605.1.15.(KHT
      0×01c0:  4d4c 2c20 6c69 6b65 2047 6563 6b6f 2920  ML,.like.Gecko).
      0×01d0:  5665 7273 696f 6e2f 3134 2e30 2e31 2053  Version/14.0.1.S
      0×01e0:  6166 6172 692f 3630 352e 312e 3135 0d0a  afari/605.1.15..
      0×01f0:  5265 6665 7265 723a 2068 7474 703a 2f2f  Referer:.http://
      0×0200:  6c32 342e 6e65 7563 7279 7074 2e6f 7267  l24.neucrypt.org
      0×0210:  3a38 3030 302f 6c6f 6769 6e0d 0a43 6f6e  :8000/login..Con
      0×0220:  7465 6e74 2d4c 656e 6774 683a 2033 340d  tent-Length:.34.
      0×0230:  0a41 6363 6570 742d 4c61 6e67 7561 6765  .Accept-Language
      0×0240:  3a20 656e 2d75 730d 0a0d 0a              :.en-us....
```

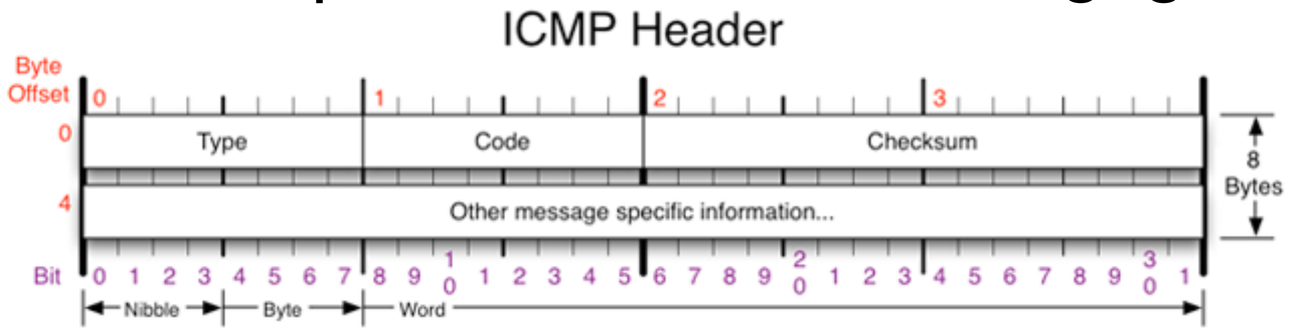
IPv4

Allows “internetworking” with a logical address system and routing mechanisms. Connectionless, best-effort, no guarantees.



ICMP

IP packet out-of-band messaging



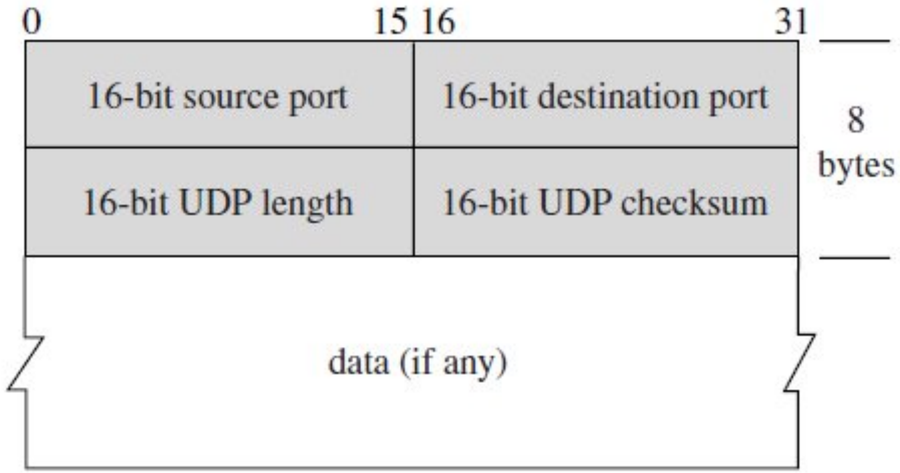
Destination unreachable

- Time exceeded
- Parameter problem
- Redirect to better gateway
- Reachability test (echo / echo reply)
- Message transit delay (timestamp request / reply)

http://www.insecure.in/images/ICMP-Header.png

UDP

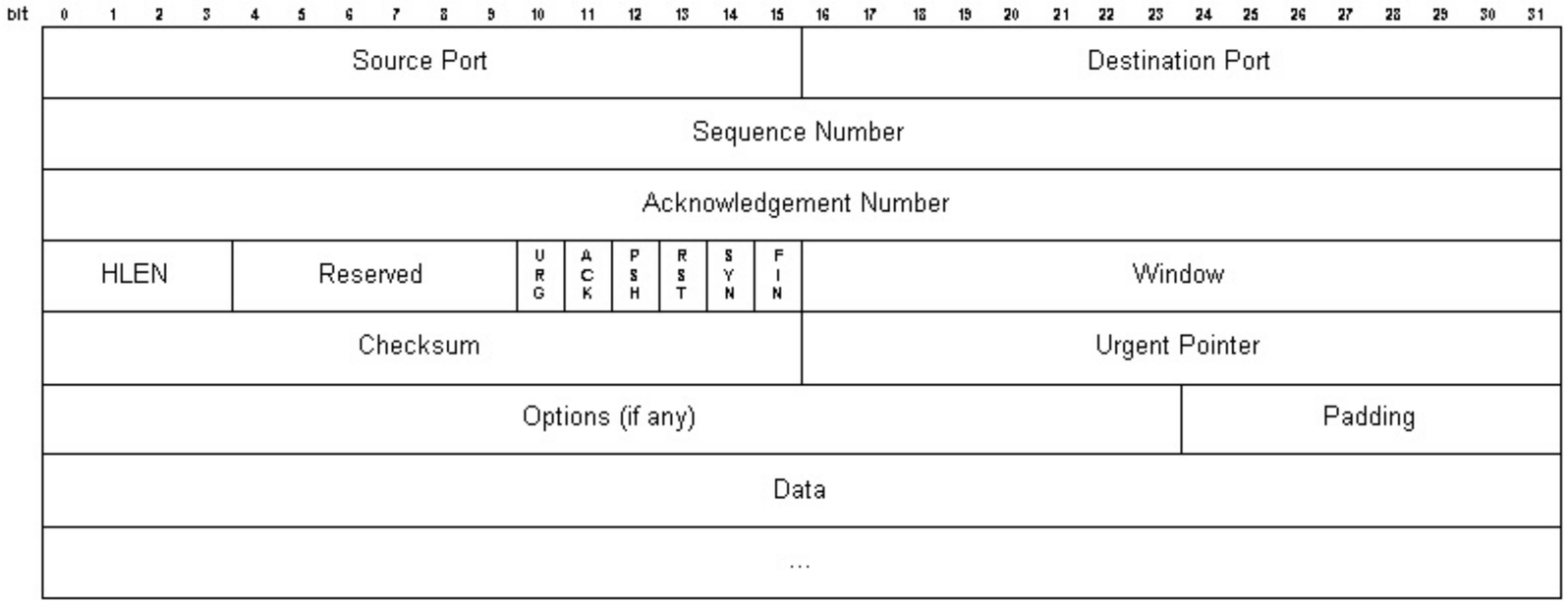
msg delivery guarantee: best effort



https://encrypted-tbn2.google.com/images?q=tbn:ANd9GcQ8XUDz5VbTPYA5ne8BbURey1StcoH5uU-u4i4EsLkDO-T_DZCg

TCP

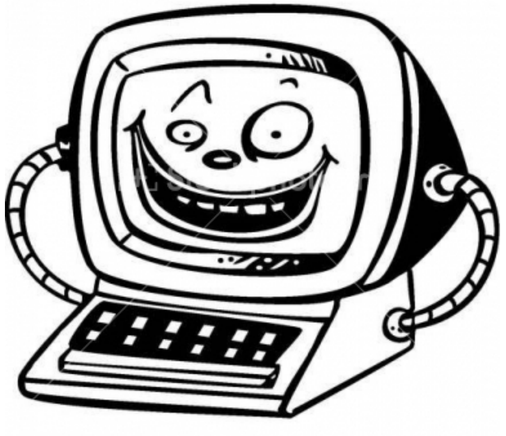
msg delivery guarantee: data arrives in order, receipt acknowledged



http://condor.depaul.edu/jkristof/technotes/tcp-segment-format.jpg

How a TCP begins

Alice



Bob

SYN_A

ACK_A SYN_B

ACK_B

Demos

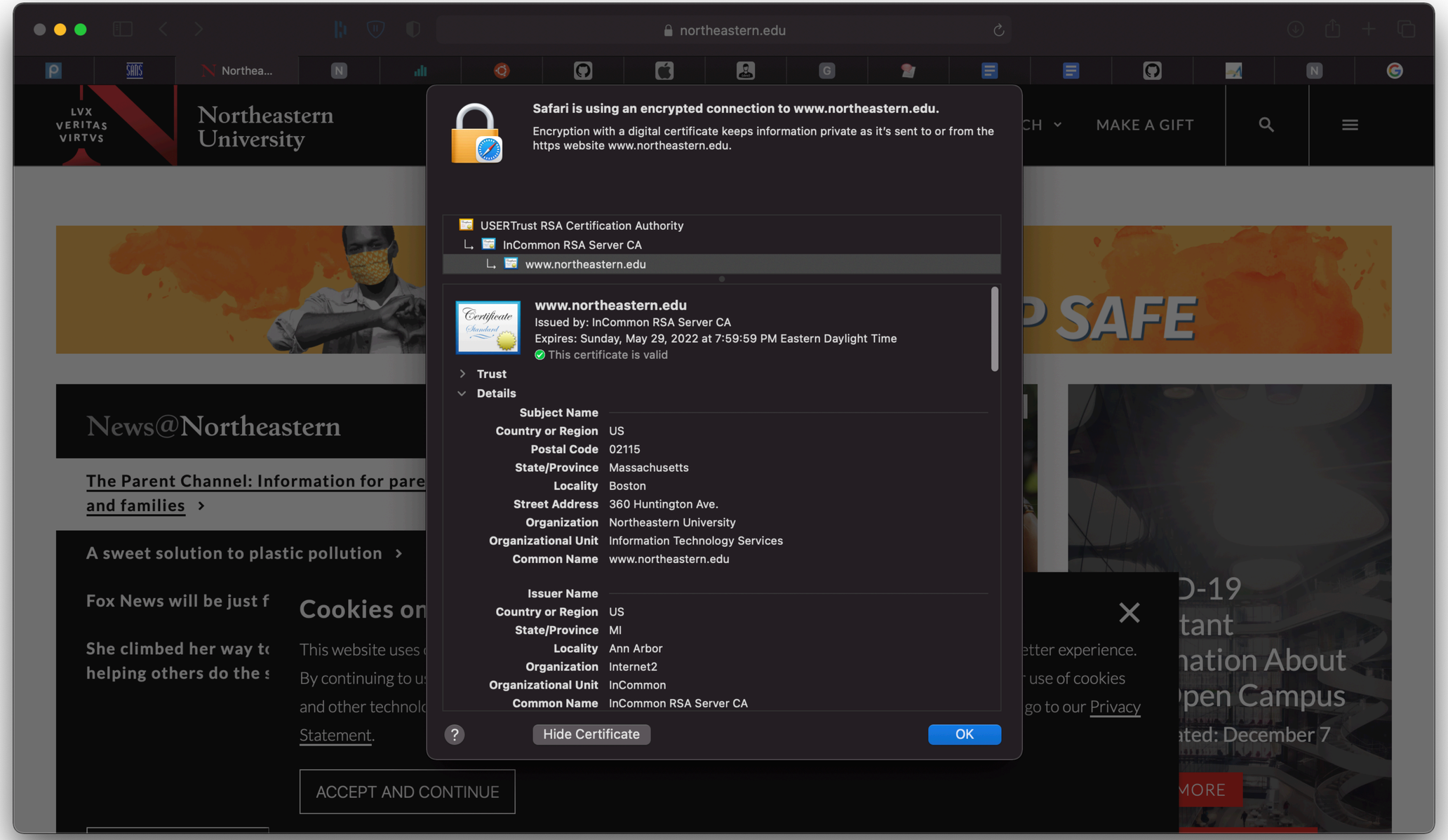
Download Wireshark

https://www.wireshark.org/download.html

Download ch6.pcap

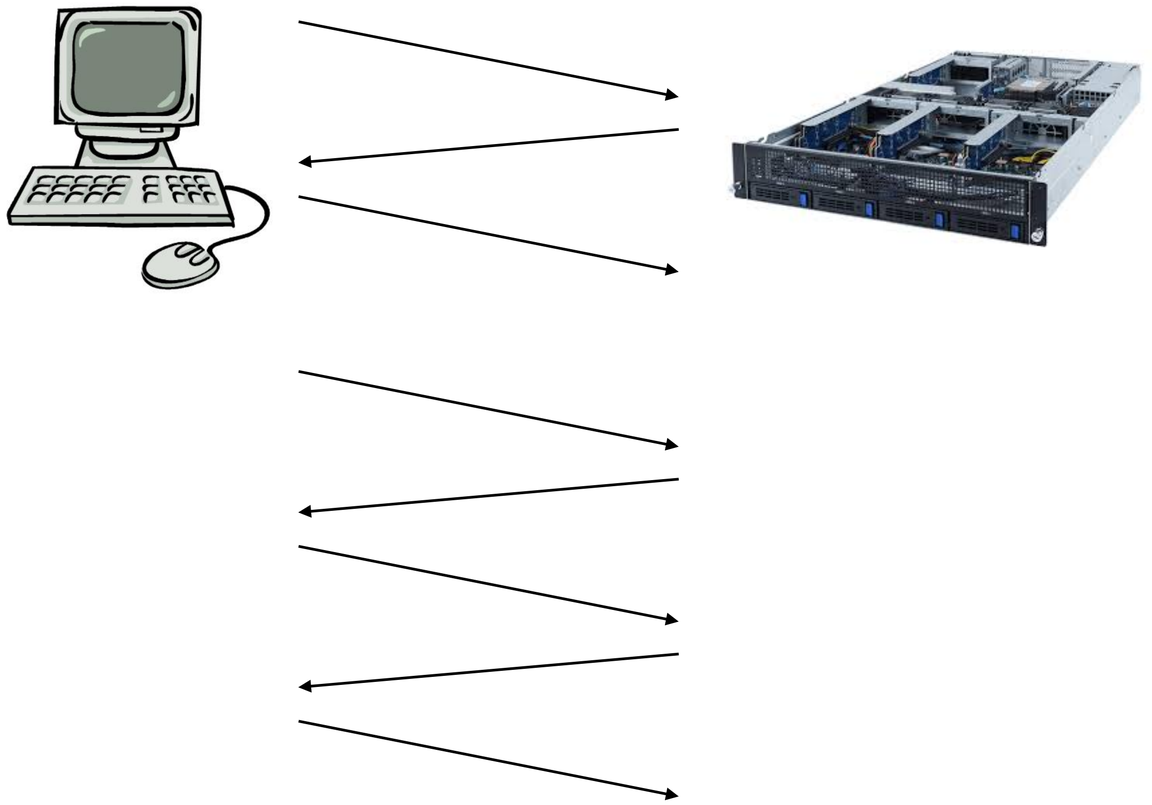
https://shelat.khoury.northeastern.edy/dl/2550-s21/channel6.pcap

https


northeastern.edu
Northeastern University
MAKE A GIFT
Safari is using an encrypted connection to www.northeastern.edu.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.northeastern.edu.
USERTrust RSA Certification Authority
InCommon RSA Server CA
www.northeastern.edu
www.northeastern.edu
Issued by: InCommon RSA Server CA
Expires: Sunday, May 29, 2022 at 7:59:59 PM Eastern Daylight Time
This certificate is valid
Trust
Details
Subject Name
Country or Region US
Postal Code 02115
State/Province Massachusetts
Locality Boston
Street Address 360 Huntington Ave.
Organization Northeastern University
Organizational Unit Information Technology Services
Common Name www.northeastern.edu
Issuer Name
Country or Region US
State/Province MI
Locality Ann Arbor
Organization Internet2
Organizational Unit InCommon
Common Name InCommon RSA Server CA
Hide Certificate
OK
News@Northeastern
The Parent Channel: Information for pare
and families
A sweet solution to plastic pollution
Fox News will be just f
She climbed her way t
helping others do the
Cookies on
This website uses
By continuing to u
and other technol
Statement.
ACCEPT AND CONTINUE
P SAFE
etter experience.
use of cookies
go to our Privacy
D-19
tant
nation About
pen Campus
ated: December 7
MORE

```
abhi@l21:~/l25$ openssl s_client -connect www.google.com:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
   i:C = US, O = Google Trust Services, CN = GTS CA 1O1
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRAOWJUBT/plbPAgAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
…
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBLgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = GTS CA 1O1
   i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgINAeO0mqGNiqmBJWlQuDANBgkqhkiG9w0BAQsFADBMMSAw
HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs
…
IRdAvKLWZu/axBVbzYmqmwkm5zLSDW5nIAJbELCQCZwMH56t2Dvqofxs6BBcCFIZ
USpxu6×6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==
-----END CERTIFICATE-----
---
Server certificate
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 1O1

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2640 bytes and written 386 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
```

```
abhi@l21:~/l25$ openssl s_client -connect www.google.com:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
   i:C = US, O = Google Trust Services, CN = GTS CA 1O1
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRAOWJUBT/plbPAgAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
…
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBLgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = GTS CA 1O1
   i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgINAeO0mqGNiqmBJWlQuDANBgkqhkiG9w0BAQsFADBMMSAw
HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs
…
IRdAvKLWZu/axBVbzYmqmwkm5zLSDW5nIAJbELCQCZwMH56t2Dvqofxs6BBcCFIZ
USpxu6×6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==
-----END CERTIFICATE-----
---
Server certificate
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 1O1

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2640 bytes and written 386 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
```



Network stack

HTTP

TLS

DNS TCP

IP

Wifi/Ethernet

How does neu.edu resolve to IP address?

Domain name service

```
MacBook-Pro:demos abhi$ dig www.northeastern.edu

; <<>> DiG 9.10.6 <<>> www.northeastern.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47992
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.northeastern.edu.INA

;; ANSWER SECTION:
www.northeastern.edu.          300   IN  CNAME  northeastern.edu.edgekey.net.
northeastern.edu.edgekey.net. 300   IN  CNAME  e12215.dscb.akamaiedge.net.
e12215.dscb.akamaiedge.net.   20    IN  A      23.38.112.43
e12215.dscb.akamaiedge.net.   20    IN  A      23.38.112.27

;; Query time: 31 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Apr 13 06:24:41 EDT 2021
;; MSG SIZE  rcvd: 160
```

DNS is a distributed database

Purpose: map a name to an IP address.

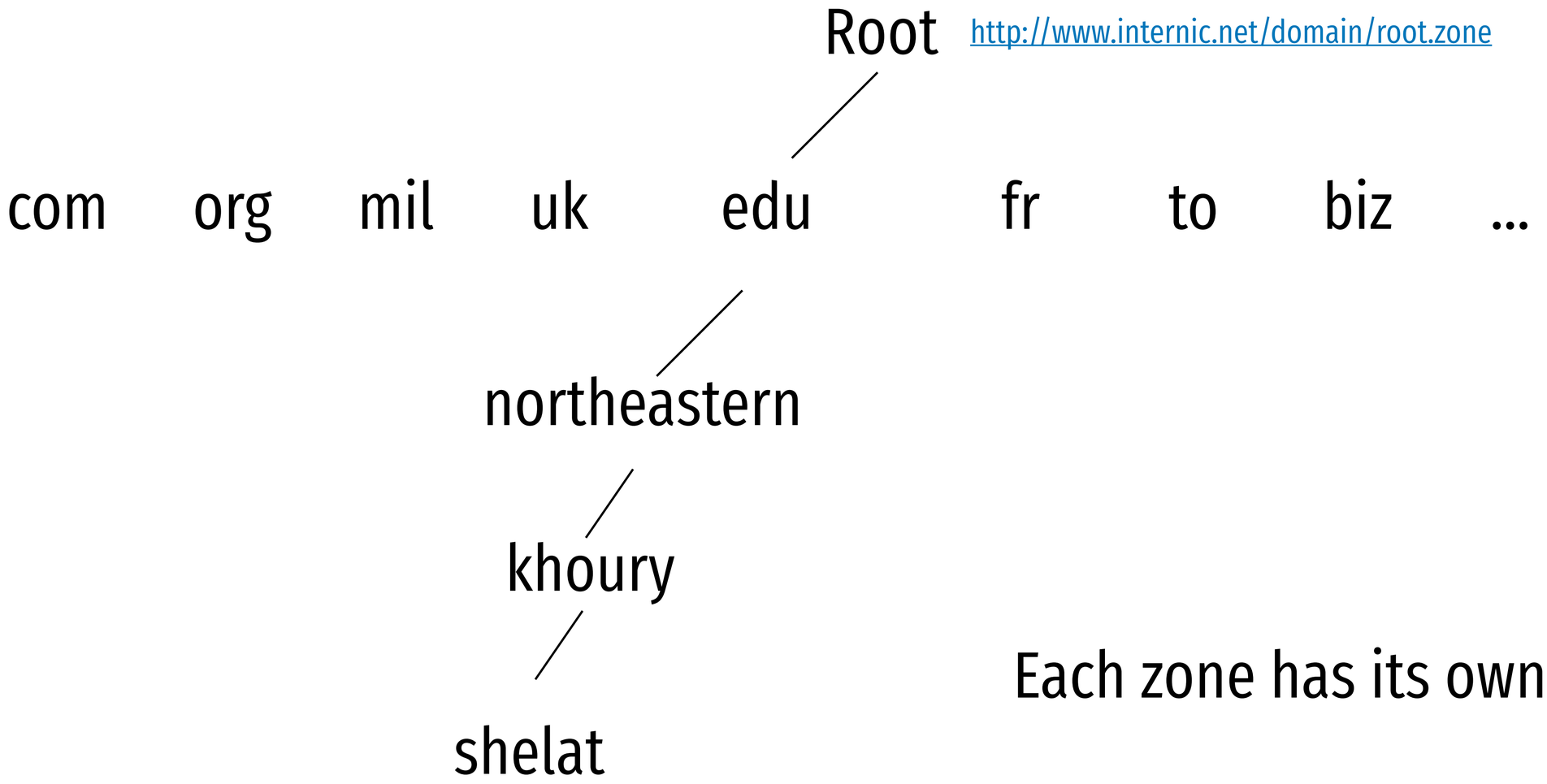
No single database contains all map entries. It is hierarchical.

Database is a “rooted tree”, internal nodes are delegated to domain owners.

Runs over UDP on port 53 (usually).

Queries are usually cached for performance.

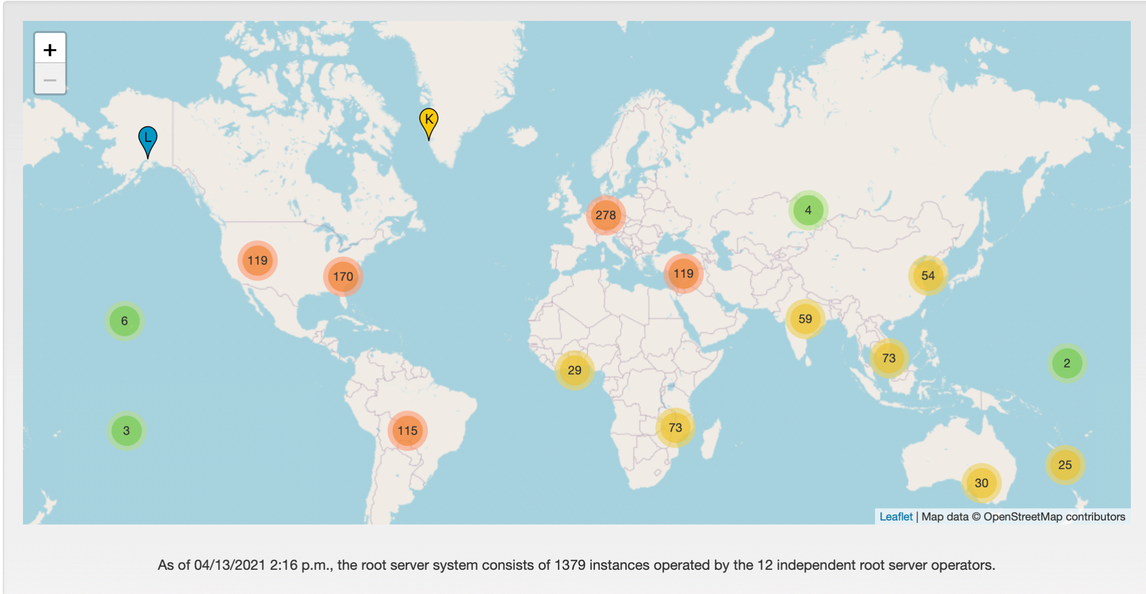
DNS hierarchy



Each zone has its own administrator.

Zone file

```
.       86400 IN  SOA a.root-servers.net. nstld.verisign-grs.com. 2021041300 1800 900 604800 86400
.       86400 IN  RRSIG SOA 8 0 86400 20210426050000 20210413040000 14631 .
TR1THuipZNwnIGYPDUrvwk627UUS0×2tzA34+K3KfC9sujDsgFpiipXEo5R8lLuhwlIG2/
jzxg7UNVlbVk8VytAyQKoPZ3RDM8SqlRRT7h3O7tEKRpQsu+1UwWlPcNMM740lAxRnao/qDEU2P2TvfYn6xTgeiXP/2g0EcPcUb/
fnIbijwbaef07m8OEQBRO/R3Ssr71c0fCJ31fjmw0HHdRpnGEV1fkE4PescB0Qr/
fBn0zL2l2JwY5LpSIsTK9YsxFkEPUAfLmefPGmFWVp2QR2CgMCVBiPZZs4cGuEjHkDdcpL0uIDr80OdmJcOzznAMZPUIv73DGJFcHz
ow==
.       518400  IN  NS  a.root-servers.net.
.       518400  IN  NS  b.root-servers.net.
.       518400  IN  NS  c.root-servers.net.
.       518400  IN  NS  d.root-servers.net.
.       518400  IN  NS  e.root-servers.net.
.       518400  IN  NS  f.root-servers.net.
.       518400  IN  NS  g.root-servers.net.
.       518400  IN  NS  h.root-servers.net.
.       518400  IN  NS  i.root-servers.net.
.       518400  IN  NS  j.root-servers.net.
.       518400  IN  NS  k.root-servers.net.
.       518400  IN  NS  l.root-servers.net.
.       518400  IN  NS  m.root-servers.net.
.       518400  IN  RRSIG NS 8 0 518400 20210426050000 20210413040000 14631 .
rL2H84ehh9QBxCsjSUaEuKoevwQNBT+lEdOX5KRAJvFxSqnjiHLl6c37d8ADrIA7H7/4oasFntGzOJc3vex7MhzvsZiZomJT0vvUCU
TWpyB0429ZEVRuzggI6wulEEc9bdWtERXiDGAFLGGgBorIkDuodIzTCNgzRrK8IFCxDj8B2hZr2djOpWllPms82TfWW3ci+k3Fb0+v
j5Aeo6jL0R5Qha8puyIQWnO31cqGH/2j+VVL0WA0RLgzo4FQkH35Dxs3X+vaYmIQNmDyByjqC39QgT
+Erh35a5IRiQ4cISrf1Q0HcG2Ybd/jmaogTdUyQBZSMKmjywE2Q==
.       86400 IN  NSEC  aaa.  NS SOA RRSIG NSEC DNSKEY
```



root-servers.org

Where is shelat.khoury.northeastern.edu?

Use root to find .edu DNS name server:

Network exploits

Network exploits

Previous insight: security vulnerabilities arise when external input is not verified.

Network insight: security vulnerabilities arise due to failures of design and abstraction.

Networks were designed for convenience.

Security was an afterthought.

Networks increase number of possible attackers.
(Attack surface is increased.)

Networks provide some anonymity to the attacker.

Issues with

Privacy of Information

Authentication of parties

Availability of services

Infrastructure attacks

actively listen and modify traffic as it flows across your nodes

denial-of-service

attack the routers that control traffic flow

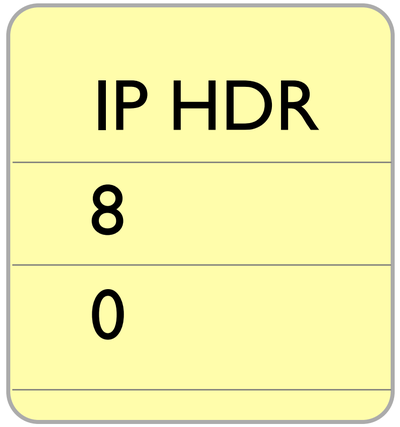
attack the domain naming system to redirect traffic

Availability attacks

ICMP

ECHO request

“Ping”



ECHO request

Code 0

Attacker

SRC: Victim

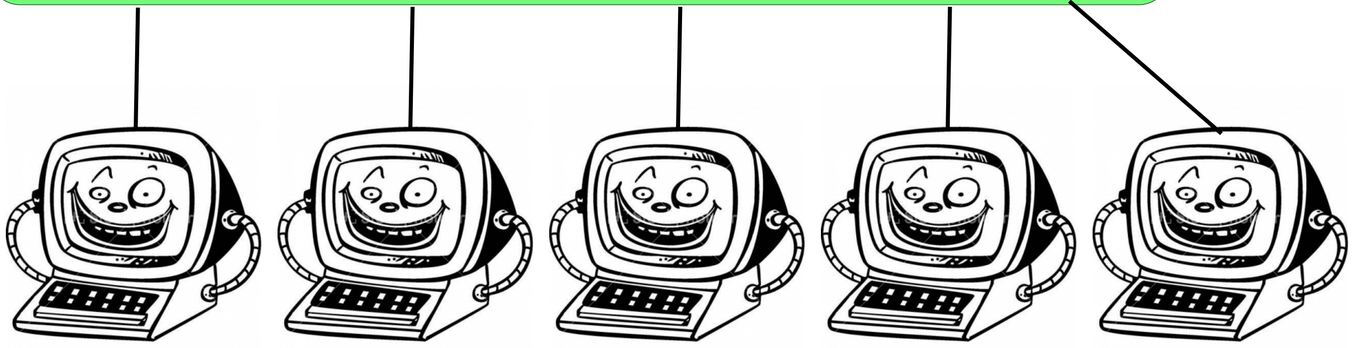
DES: Broadcast

8 ECHO

0

Victim

Network



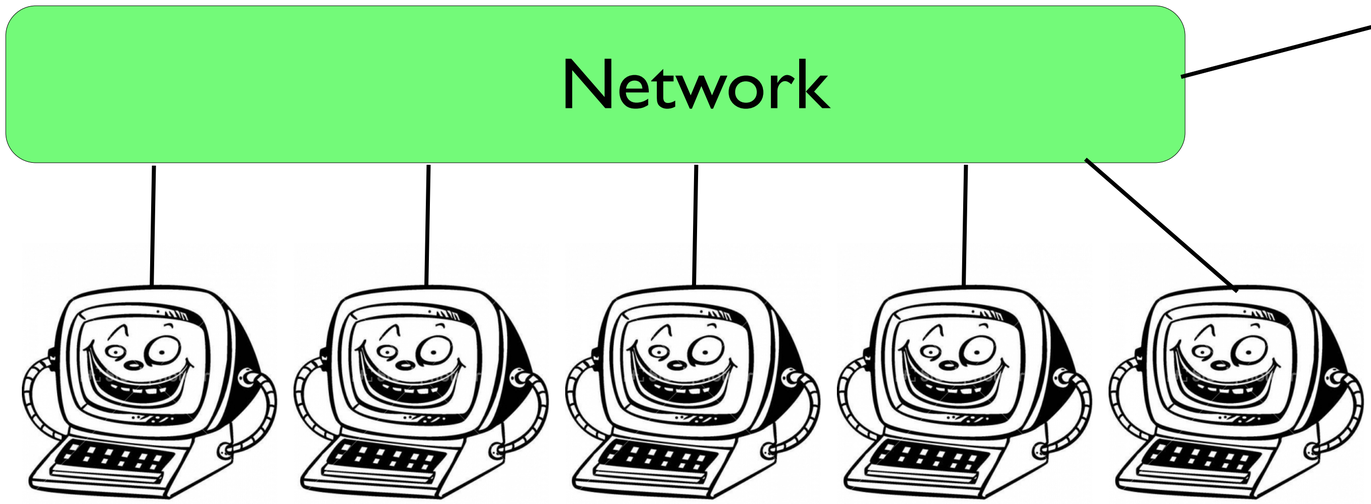
Patsies

http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA

Attacker

SRC: Victim
DES: Broadcast
8 ECHO
0



Network

Victim

This computer now receives thousands of packets.

Unaware accomplices

http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA

What missing security property enables the attack?

What missing security property enables the attack?

Authentication

of parties

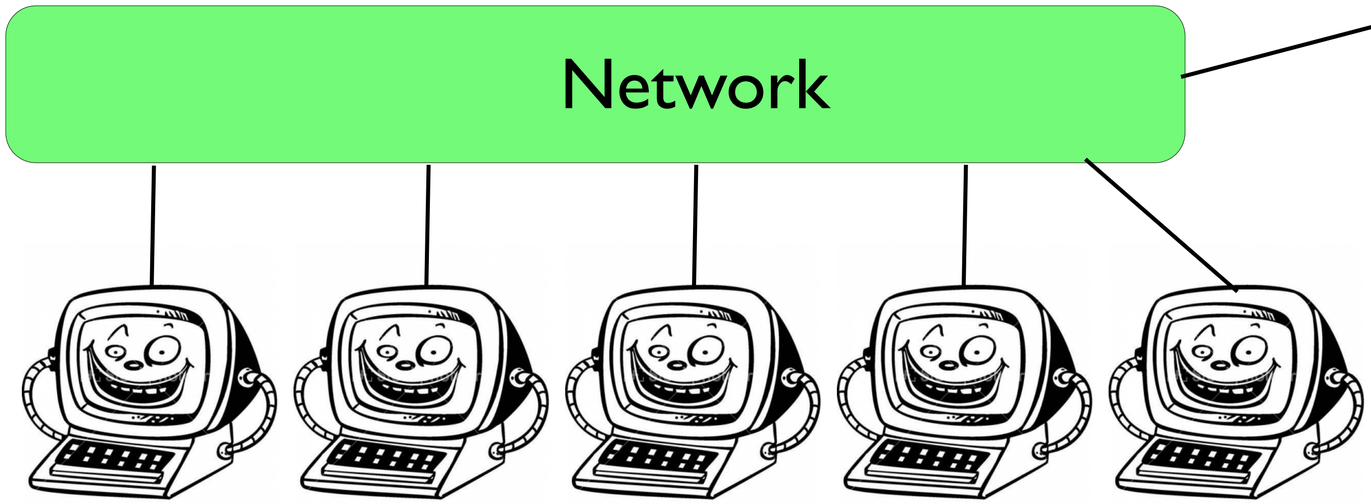
The SRC/DST fields of a packet are unauthenticated.
It is possible to mimic any node on the internet.

Proper network configuration can limit the attack.

What steps should a network router/gateway/accesspoint take?

Attacker

SRC: Victim
DES: Broadcast
8 ECHO
0



Network

Victim

This computer now receives thousands of packets.

Patsies

http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

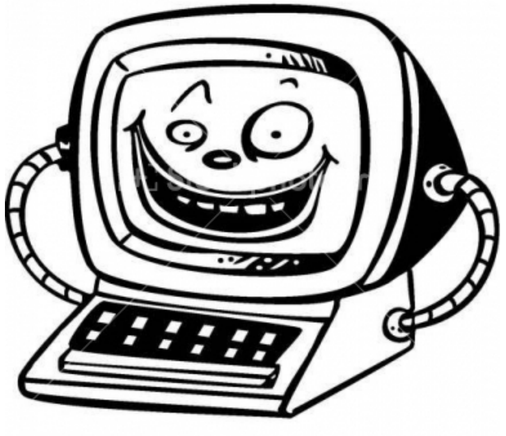
https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA

Attacker is able to LEVERAGE its resources.

1 attack packet becomes 1000s.

How a TCP begins

Alice



Bob

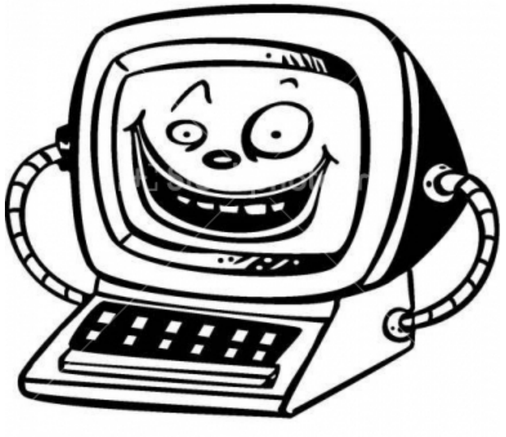
SYN_A

ACK_A SYN_B

ACK_B

How a TCP begins

Alice



Bob

SYN_A

store this

$ACK_A\ SYN_B$

wait for a response

ACK_B

How a TCP flood begins

SYN_A

SYN_{A2}

SYN_{A3}

SYN_{A4}

SYN_{A5}

victim stores each of these for timeout (1-2 min)

soon, entire memory is consumed

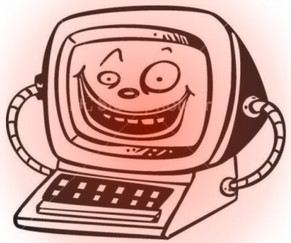
Amplification

SYN_A

SYN_{A2}

SYN_{A3}

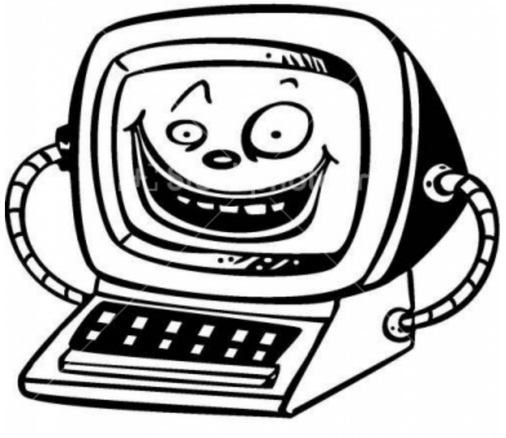
victim stores each of these for timeout (1-2 min)



1 32b packet causes **1024b** alloc.

SYN Cookies

Alice



Bob

SYN_A

ACK_A SYN_B

seq# = f(state)

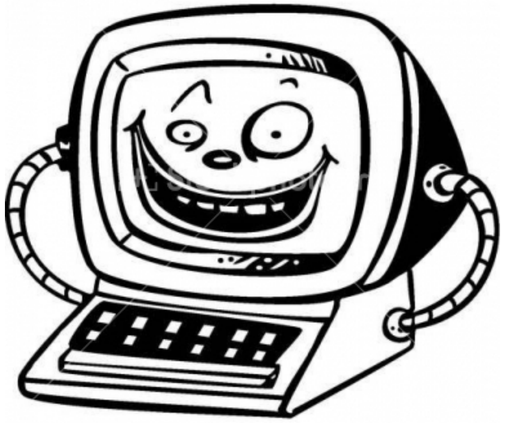
don't store this

ACK_B seq#

use f(state) to recompute state

SYN Cookies

Alice



Bob

SYN_A

ACK_A SYN_B

seq# = f(state)

ACK_B seq#

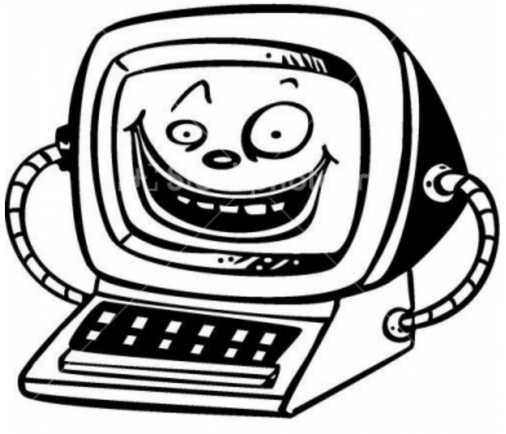
don't store this

use f(state) + IP addr to recompute/verify state

What cryptographic properties does the function f require?

Cuckoo TCP

Alice



Bob

SYN_A

$ACK_A\ SYN_B$

ACK_B

if state is full, then randomly evict a "WAITING" TCP Entry

Ping of DEATH

Normal PING requests require 32 bytes.

Attack: send a 65k PING request.

DNS traffic amplification

dig yahoo.com any

;; Query time: 6 msec
;; SERVER: 128.143.2.7#53(128.143.2.7)
;; WHEN: Thu Sep 13 13:44:04 2012
;; MSG SIZE rcvd: 506

~50byte UDP packet leads to a 506b response

10x

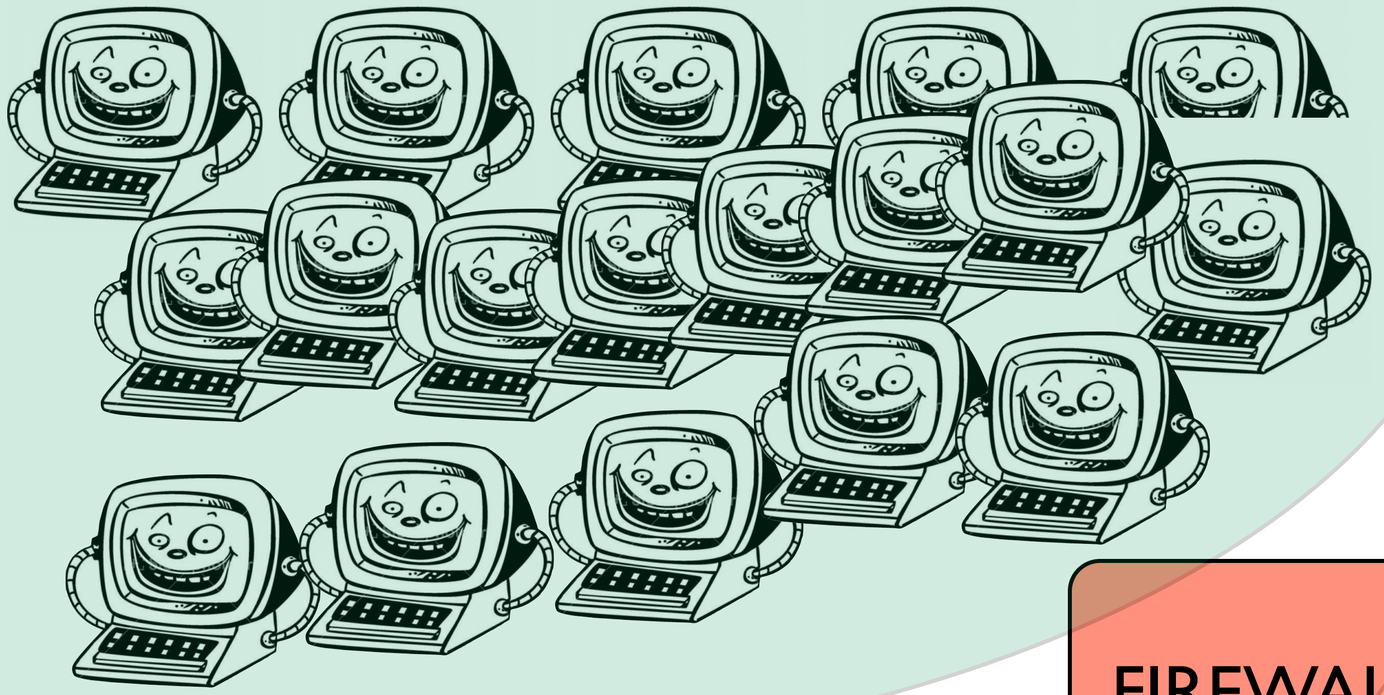
d-172-27-45-104: abhi$ dig +bufsize=4096 +dnssec any se @a.ns.se

```
; <<>> DiG 9.8.1-P1 <<>> +bufsize=4096 +dnssec any se @a.ns.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29242
;; flags: qr aa rd; QUERY: 1, ANSWER: 20, AUTHORITY: 0, ADDITIONAL: 26
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;se.                            IN      ANY

;; ANSWER SECTION:
se.                     172800  IN      SOA     catcher-in-the-rye.nic.se. registry-default.nic.se. 2012091304 1800 1800 864000 7200
se.                     172800  IN      RRSIG   SOA 5 1 172800 20120925190422 20120913081101 58656 se. DtVv7a9TE2PorcAHozltJ8x8lkkrSJYbUf9zsAUzkZHmadMMcRvm1u1N snzCnURQHILqB7+v0mXySrpl4bW15wVZn6UjcpEEQjq7uqeahK8nOlxJ
XqLvxdz5Ro7WR1+V3dAPm3RH5X7962mZrKdVXF/E01upf96+zxwimOTN lf4=
se.                     172800  IN      NS      e.ns.se.
se.                     172800  IN      NS      b.ns.se.
se.                     172800  IN      NS      c.ns.se.
se.                     172800  IN      NS      a.ns.se.
se.                     172800  IN      NS      i.ns.se.
se.                     172800  IN      NS      g.ns.se.
se.                     172800  IN      NS      d.ns.se.
se.                     172800  IN      NS      f.ns.se.
se.                     172800  IN      NS      j.ns.se.
se.                     172800  IN      RRSIG   NS 5 1 172800 20120924194433 20120911201101 58656 se. M3jZ0lhDkvBfizaxzFgsFWbAEJKN6aj4fn5ZPBlHIwgVTL7jhhsiTd2u HB9Kp0bDSwlBDxnwvGtr8g+Hem9RitYZXxHkbfP9SXhuKsZVtM7Y5WUB
CF7lwRywwnSikjb8su7Ewki7bO5aLTHCWu+1/jPDRNUofHfISqSIJxKm gvl=
se.                     172800  IN      TXT     "SE zone update: 2012-09-13 09:07:13 +0000 (EPOCH 1347527233) (auto)"
se.                     172800  IN      RRSIG   TXT 5 1 172800 20120927095501 20120913081101 58656 se. CKXLjyfqXBYQqYdkUTKPbAwhzQi24DebVrDqrhOo0vMLqCum4AwjrzaV snDHgv1KSMM9ifPYEz5jSrVUsOOyxNgmRKjmIXgjRiaylurvZjlpu2kE
Nd3ppJ5LkP7LuZnbrtVWYmFlYNzlkJDj62TZFdYrFRkGXf6JedU8IdIr zpg=
se.                     7200    IN      NSEC    0-0.se. NS SOA TXT RRSIG NSEC DNSKEY
se.                     7200    IN      RRSIG   NSEC 5 1 7200 20120924215357 20120910221101 58656 se. ZwvY5T0fW84iqsdrQkgIfFhJ6aXYWmLkm+HCiv9/wisTmTj8UJC1dSHm ysZnr0zZ1PS/D+ymVGc/cMiKb3d8Nq2w+/piAHpEqiOtkh38e1ngGX+C
MclBkYV5FiuEC1QSiM+D7H7GSSPrqUBx2M3heWz8MucQvO3MCL81ESsJ WaE=
se.                     3600    IN      DNSKEY  257 3 5 AwEAAZYYG1hpk8XKHNHpdO/EEg+r4YmIEC4Fn3x2DEsygxDuoT9d/QCi X1pz0omFGCaVfCWHvaScVvWd4xP4kNDnSDQxBzPwLEXE3l0cLseMJ2YM QeBPf3hGhLs6VSDnGFKAzNG4fhri9EBTLv9ubL8Kx8cWQKuu3A5HRVD3
li7lZB+0kmUKqGiIQdERKt/Ec36BkK93lyGags5RrR2VDdrXCj9Yay90 KCKITk52AbwVoMPm0OYlPbD4ViBPMk5nmh/dPeCoZoVJxgANZ/doVQxR 5vDkMBYxuhrXuQk3CvZBB011NsXxk9yHtHvp/5gjUVJjvhdRvjRB6/xY R03c9owi/aM=
se.                     3600    IN      DNSKEY  256 3 5 AwEAAbTmWA2HUXP60ITEiYuK2E08t4LECz3acvQbzRWScFNI9FWqwcDY mWjZgXYmHWsAqM/Nl3xWR+eQ7/VgLTXMbVlxWMLFlPLGHCe1vI69kNNN N4V/iYt0bjWwvkhys5cYYRocjfYhusGumpqJ2G9OUkjJdk5m6EH/+Llp PJmpIg
se.                     3600    IN      DNSKEY  256 3 5 AwEAAe7gh8/AVUjbsQq9PKtoBHOfl/WHTopJCOsEoB7tOaCBov6eN7yO VZT4TOl4idc0R1HGc9bFzQ0U+/4wWBPbVltV8bm1EQm+SNtlONtd6T2d 3wDXhouf1nHCdDKt1mYXuSCaQbgf55xYaPNLEvu5VDtwOIL9C2Gu+XdH aONnbY
se.                     3600    IN      RRSIG   DNSKEY 5 1 3600 20120924020128 20120910101101 59747 se. GEHtQQL8VOc8FiVCB7SfQ6/WYrzWhA1ftT8v2JElRXF0e6e1TurXepZW QZ1F1jky0lQ31Qt7pbsBA/sOvfWaB4GLMKkgYG2dZgQUwifMi5I5cXyF
EvZzH+jg63Hh1fsorCEcRLNlxRZ4sTkUx/cH7lGp1dpZYpGlRkbQl4Tp zALzkjBuIHfMM05hrt6Bh5d/3AfUhlwtN8iu5JX3qPRY+5BVufvTKVpB Dw8zR38sHeqBDL3nPLLje6PhlyyMoM0NuzZh0WfwqFmbJCs+WZiyq1QZ Nm2K3uBMQx7NLaLqFptHb3XB0IhXTWE3PLNij17qg+RHHBPgzwiJY+ja pbNHCg==

;; ADDITIONAL SECTION:
a.ns.se.                172800  IN      A       192.36.144.107
a.ns.se.                172800  IN      AAAA    2a01:3f0:0:301::53
b.ns.se.                172800  IN      A       192.36.133.107
c.ns.se.                172800  IN      A       192.36.135.107
d.ns.se.                172800  IN      A       81.228.8.16
e.ns.se.                172800  IN      A       81.228.10.57
f.ns.se.                172800  IN      A       192.71.53.53
g.ns.se.                172800  IN      A       130.239.5.114
g.ns.se.                172800  IN      AAAA    2001:6b0:e:3::1
i.ns.se.                172800  IN      A       194.146.106.22
i.ns.se.                172800  IN      AAAA    2001:67c:1010:5::53
j.ns.se.                172800  IN      A       199.254.63.1
j.ns.se.                172800  IN      AAAA    2001:500:2c::1
```

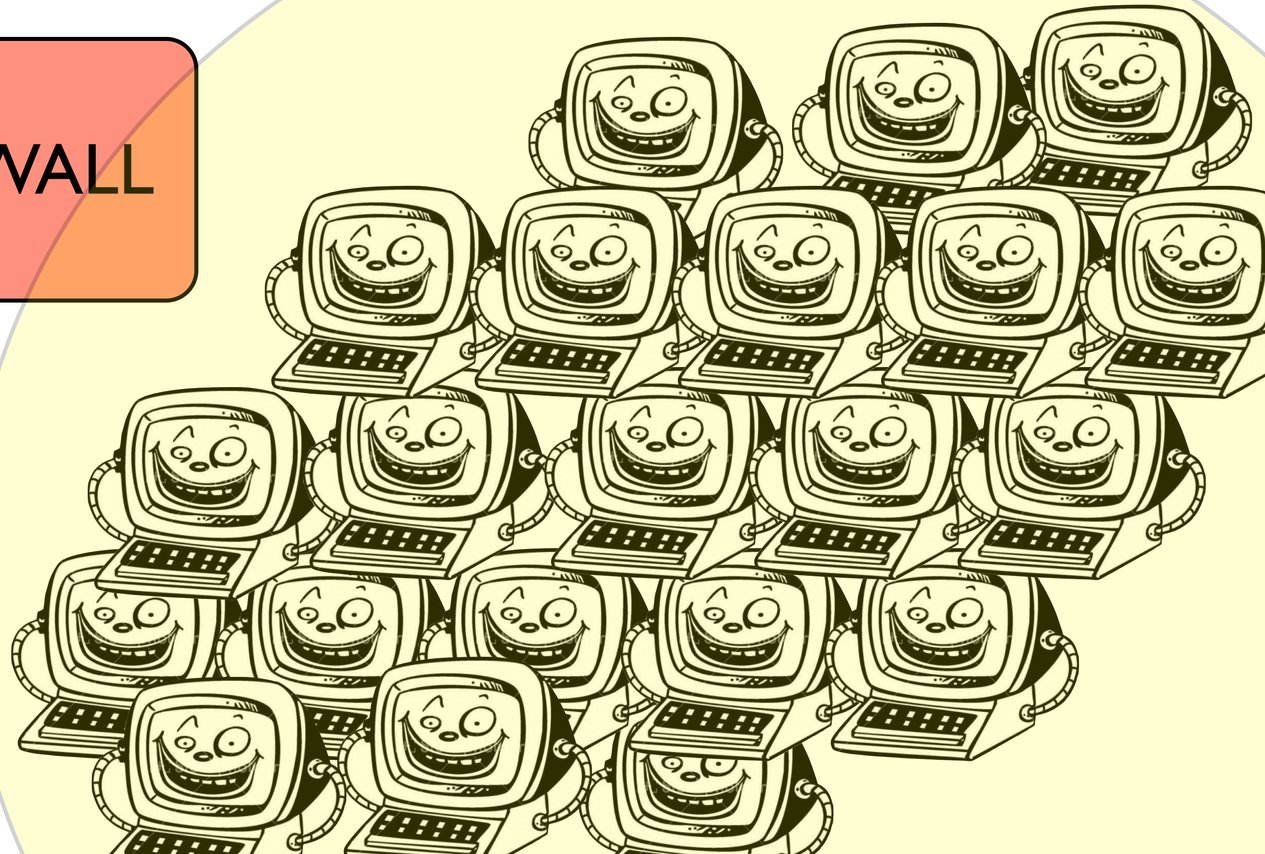
```
j.ns.se.                172800  IN      AAAA    2001:500:2c::1
a.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120926094152 20120912121101 58656 se. cB0VnZRRe7GmP+Ild4rNmQJefMQKx+HOq26gCs+k3q7ZttetdFtqZQa7 hGEkWnALljwqIFgxQucnMRrSVso0uZI21zCe7katSYyK9wJSG1dpsk/G QYcMJc/
EA0deKIVkmA77TWeAi9AtI3cfgDUsibmmCJ08qp34zdoe8wBM fG0=
a.ns.se.                172800  IN      RRSIG   AAAA 5 3 172800 20120926005130 20120913041101 58656 se. pat/9jqrPpm/AP2czFcNCt477zy9wGgnngeuuI+mJsN5l46py+4x0dVS 1dp25uI7BS4nwI/I1yBcvxhPf2bavfLKOqV16p+/yfcBE9Inw8p0O13B
J9Ad87Lb+4rD2NeiFxAoj210pyR4OzsbLwjs1vcIqEAzPHh+r66IFuV0 Udg=
b.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120927063649 20120913021101 58656 se. U8gZpgfj2wCWMrSgnKLyR9VPRyiojP4IGHWlSpeyvu3KTZBSzU7Xw/tu QWORTwjxBkdgTSXNcKJDkQPe8PkMKzPjj/aB6w5dU/QXx7fdyGBYHqlC 2nbc5IIiG6+/
aV2Eg5T5LiRj2+RWJnQWxyh6TxtccKa5SdZ8aVz+bMGw IIE=
c.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120925203628 20120913081101 58656 se. oqrUBu72ccG3moTYF8mENrp0d3D/n0Z9GX3tHLpu3+kckgAZEMahYeB3 VhESvysenqXHy9K++STBH/c/BpZJnOnV109mctZX691/NC7A0cUWk8cE
v2PYkSkRATryT2V4soJWbX1kGrc40UMLatqh6gY7tJPLvnkgeXOu1Fy8 Rjo=
d.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120925050254 20120912181102 58656 se. CqEp4MhqEMzW+Tvg5wTSIy/zqMoFBKNvIwr1590yShYfhtLQpXxKquLe IlHtXbY+kSaA8nKw7rhPGI06QRbW8FYYIWyP/3KSoBsVTr+ZZ19A+1wd
dK20GMC6SjAKRU4HE4vVFSZJm5lvtm5RPSzQxlT19tCwNc1Ggj5ZYaAV uj4=
e.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120926152155 20120913021101 58656 se. qoZASSLoC2MN0bxYc8eTNWjNAIbhSzTyKgBbj4akMDyRQxTeA+YtdURZ lf/5gvDjOOE7yNojuuAzHD8g+dyn5Z7cgmjLIyiIo59huDUkSO0bQZsz
PBLouj9+7NMt2Q5tILJG2a9+BRFpsIE+nAxXMQRpldqJ2l+Zde+DNLU/ XTI=
f.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120926062907 20120913041101 58656 se. kzQMEZB1F5KX06I0TrKgcqKC8Nip3J5/FyTR0O86TdffnIKjQ4Eg83/u yP1kr1LNxCKp8BFHbQKwb50WbxCW0V/BBfWU6L2jeJxz5N1r+zvCzC0v
4AnfNQhJtE3jR6d6RG4DCurkAheFcaPZtmEbYu+jaZi3xLTcw+jEQIE+ d+A=
g.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120923205729 20120910221101 58656 se. h/pT8oAz0YJI7kN7u1Ez6EGFyco56yFNEOJn0lUuJIaKXoiCWxpa4GoV sWMUQOkffPpfZbOqZf8srgQjKmjhkJwGCn+detbGu9znamKVD1oaYbwG XT3Dn27XEBPVr0dwS5seddbKWCZm1O2v
MTl4cGp1wfuQrkmU9NfJs h0k=
g.ns.se.                172800  IN      RRSIG   AAAA 5 3 172800 20120924031728 20120910161101 58656 se. EIU7iR+eAImNWeCGpLxE3998OWAyKOGsDnEgcGF9fyhcxFgw3sDB5kGR /iMGM12RhuK33S3u8te/KQ5DlByeR7Mfj+L7TJR4q1p4rwrxyl6WC45O 9wZRUtBZu/
Zv7UlvVOJDKzGdCaphqj5ey1LI14pyg8QsBPqH2KzbJ8WE VYU=
i.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120926182411 20120912221101 58656 se. YrdQpeZ1iZKYAos1jw6tRrE6uO/jH/EqkgdW8k8BVJPITQq66bwelEdn LDYTn7i8QoOJPPlNbiNjAJxXa15pLqIE2PLZdwq9Qzf3ytg04Tctn6FV 3P+fX7aI6aZuzAjZnm6/
cBigP2s+Pq96xQbAaqTEqXid5MuKDk2k6NMd QCg=
i.ns.se.                172800  IN      RRSIG   AAAA 5 3 172800 20120924081359 20120911001101 58656 se. OBy/eN25dUM/kZMsY2oJb6R/VYrQmhPXt3Px401lr1HBv4YJ3HddW5fX ZHgO95CLHDMQX3VQf0zTvHeyKb5rqk/EtZwF6hk/1h6HL7FGytXlzGEb ABr/rU74yk6LU2aDJ5ThE0793dz8ijfj2F/
gu+WDpWP7zp3s+l9naiTM vE0=
j.ns.se.                172800  IN      RRSIG   A 5 3 172800 20120923152202 20120910141102 58656 se. hFM3pC0tgLGzik7ppcGQrtMDFXTxSKUGqTtbpRtTmEnRHzm3btpdtOg1 lG2YHyFaD/dIKA0wa9qQqjGaifQCc8xY+MkvqFU2MEO83F/tIgmSC+un bWrbytxCXhaKjaU2Zl5/Mk5GsfvB/
fNIBBPIZ5RbrohAbXUQlK6Uz44v yQA=

;; Query time: 126 msec
;; SERVER: 192.36.144.107#53(192.36.144.107)
;; WHEN: Thu Sep 13 06:20:08 2012
```

;; MSG SIZE rcvd: 4073

How to mitigate network attacks?



FIREWALL



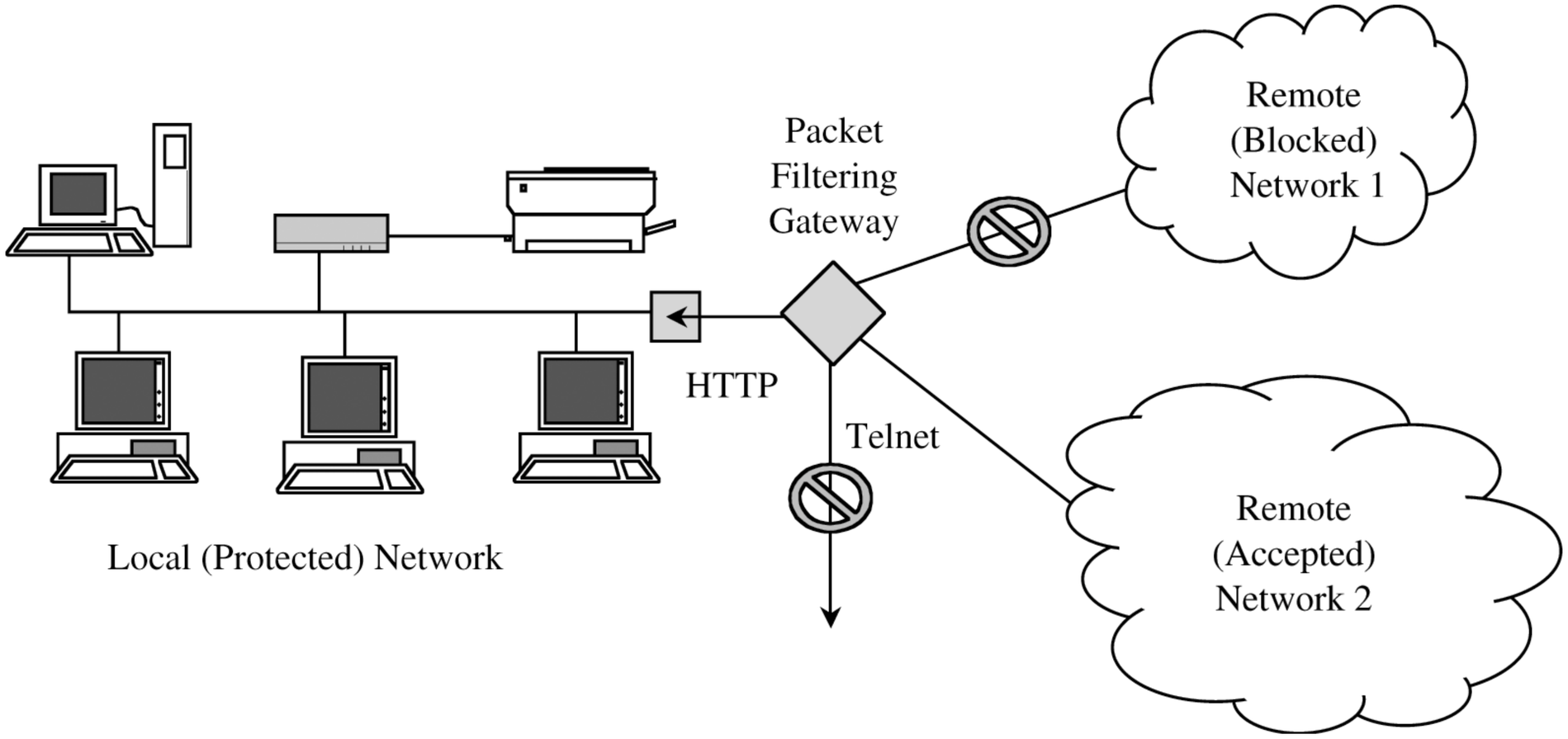
Firewalls

Stateless Packet Filter	Rules based on addr/port + header info
Statefull Packet Filter	above + state between each packet
Statefull Packet Inspection	above + can inspect the data of the package

StateLESS Packet Filter

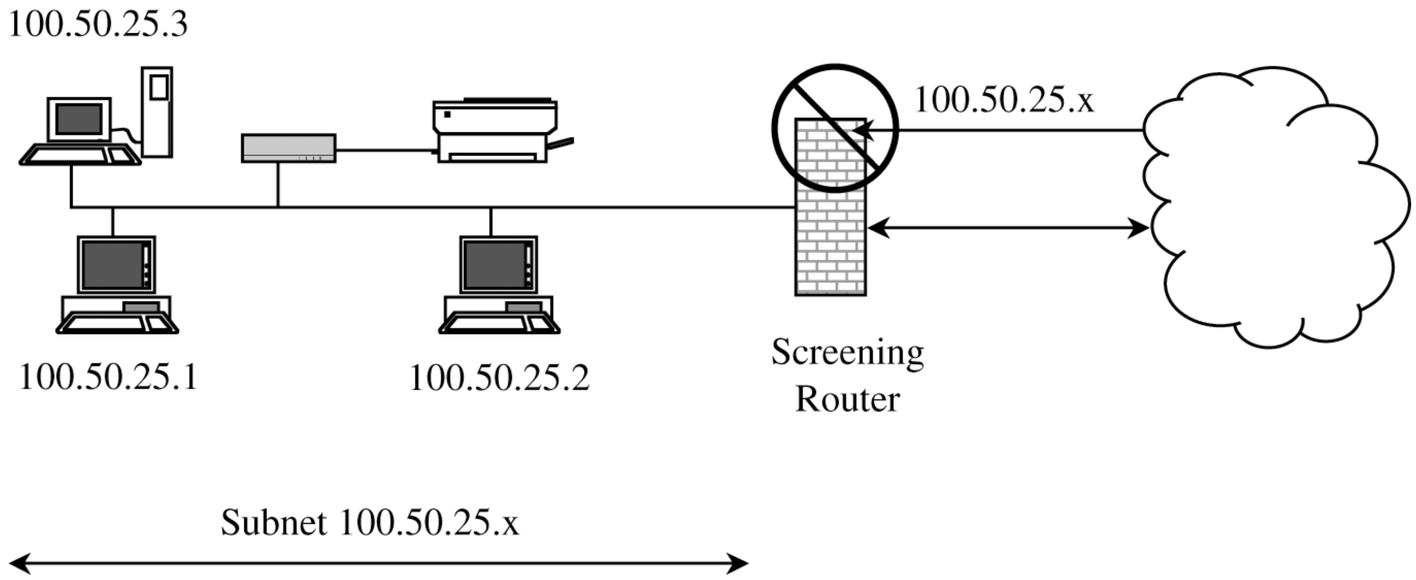
Rules based on addr/port + header info

Look at the packet and decide immediately whether to drop or forward.



•Local subnet has all traffic from remote network 1 blocks (say, network with IP address 253.128.x.x)

• Allow some traffic from Remote Network 2 (say, 253.127.x.x), but only if it is destined for port 80 (web-traffic), Drop all other ports



prevent external traffic from “spoofing” internal addresses.

StateFULL Packet Filter

Rules based on addr/port + header info

networks scans can be detected and stopped

detect invalid tcp packets

Statefull Packet Inspection

can filter for known attacks/shellcode