Network Attacks & Defenses

EECS 388 F17

Administrivia

Web project due

Homework 3 is available at https://eecs388.org

Office Hours: by appt

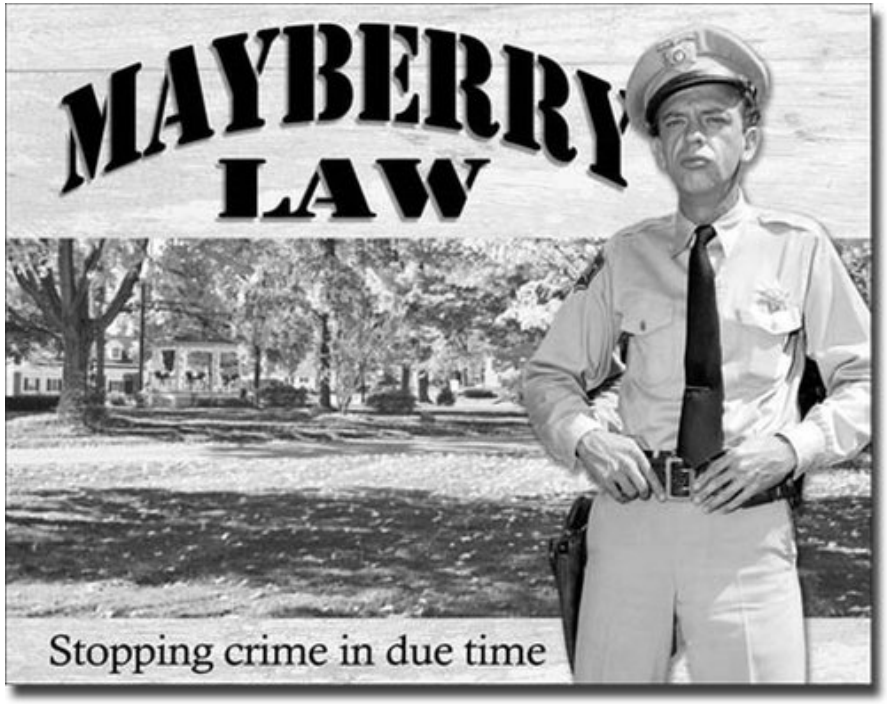
Back In The Day

The Internet was a small town

HTTP

SMTP

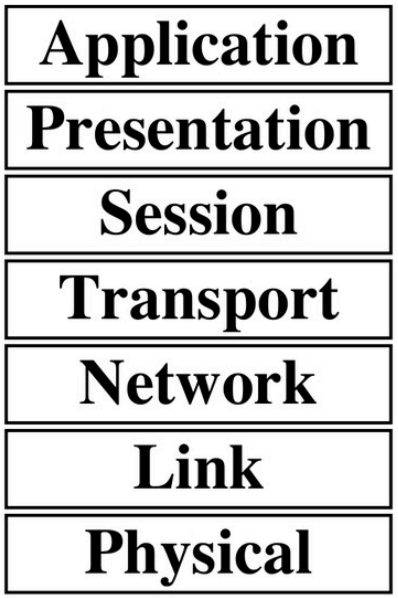
NTP



Well, let's just make secure things!

Layers are great!

Layers are a pain!



Classes of Network Vulnerabilities

- Unencrypted transmission
- No source authentication
- No integrity
- No built-in bandwidth control

Two Types of Attackers

- Eve the Eavesdropper
- Mallory the Man In The Middle

How?

Wireless Networks

Open networks: anyone in range can listen

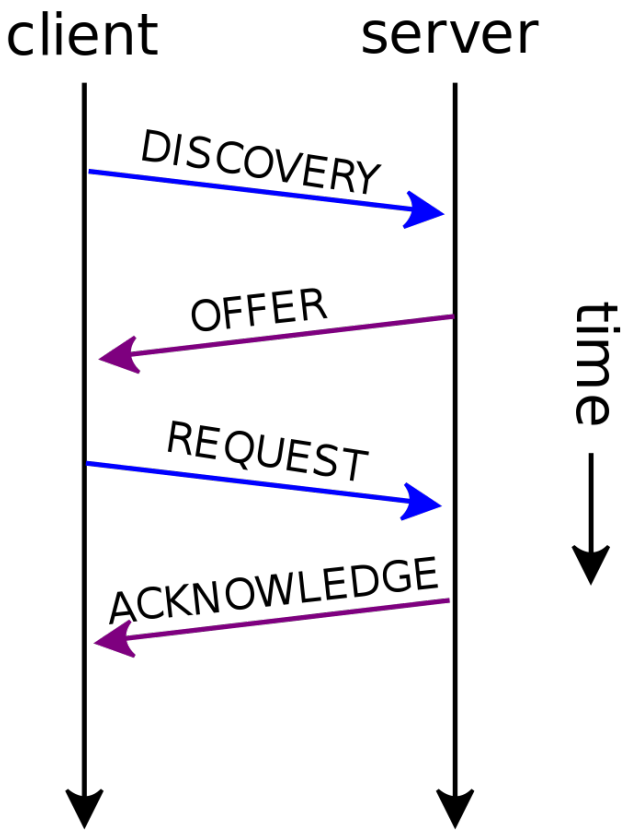
Secure protocols:

- WEP -> lol
- WPA -> WPA2

Wired Networks

Hub vs. switch

Dynamic Host Configuration Protocol



Address Resolution Protocol (ARP)

Internet Protocol (IPv4) over Ethernet ARP packet		
octet offset	**0**	**1**
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

Wired Networks

How does a client know its gateway to the Internet?

Dynamic Host Configuration Protocol

How does a switch know where to send traffic?

Address Resolution Protocol

ARP Spoofing

ARP isn't authenticated

Shout loud enough and you get the traffic

QED

How could we authenticate ARP?

How could we otherwise defend against ARP spoofing?

Tools?

tcpdump

Wireshark

dSniff

Okay, so what can we do?

Capture

Sensitive data

Session data

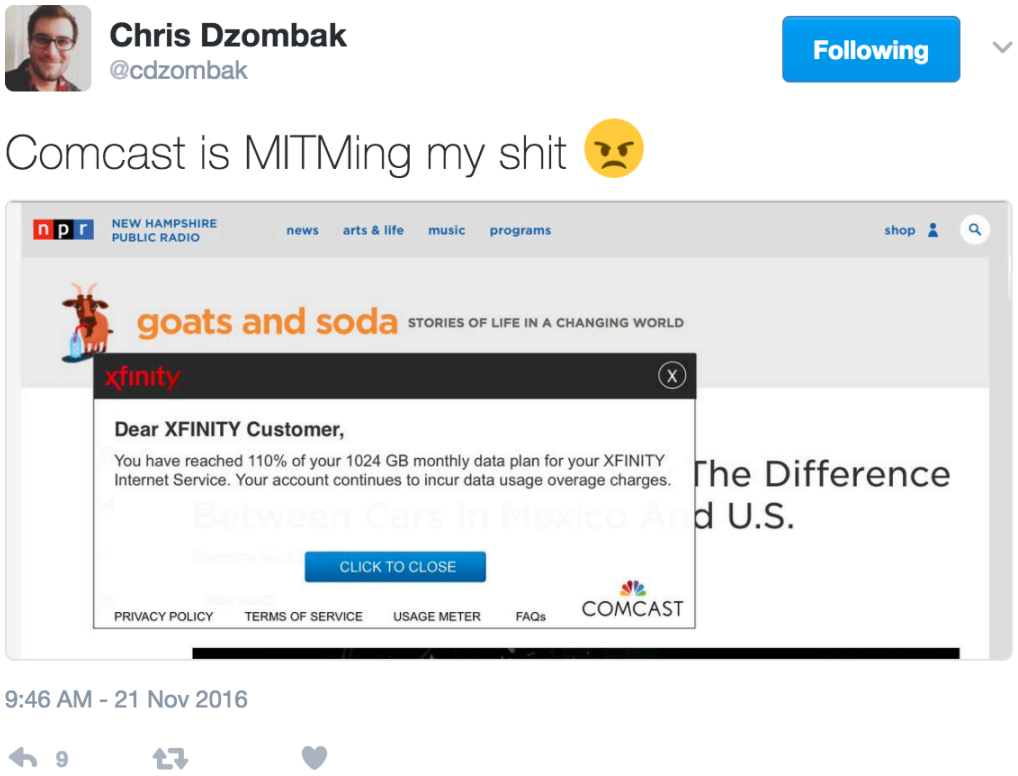
Modify

Infect executables

Inject content

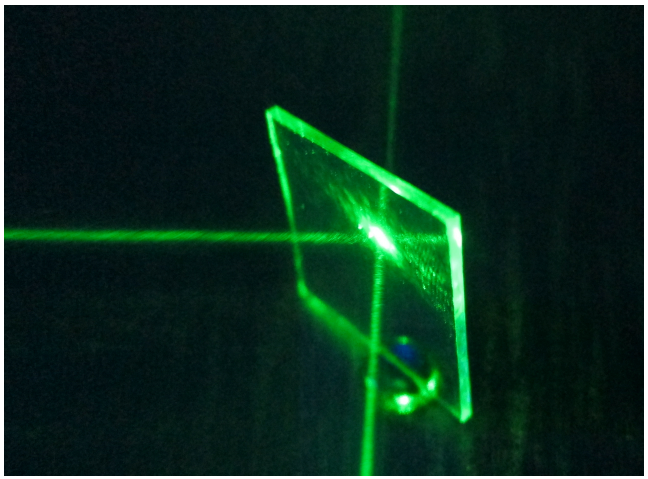
What kind of content would be interesting to inject?

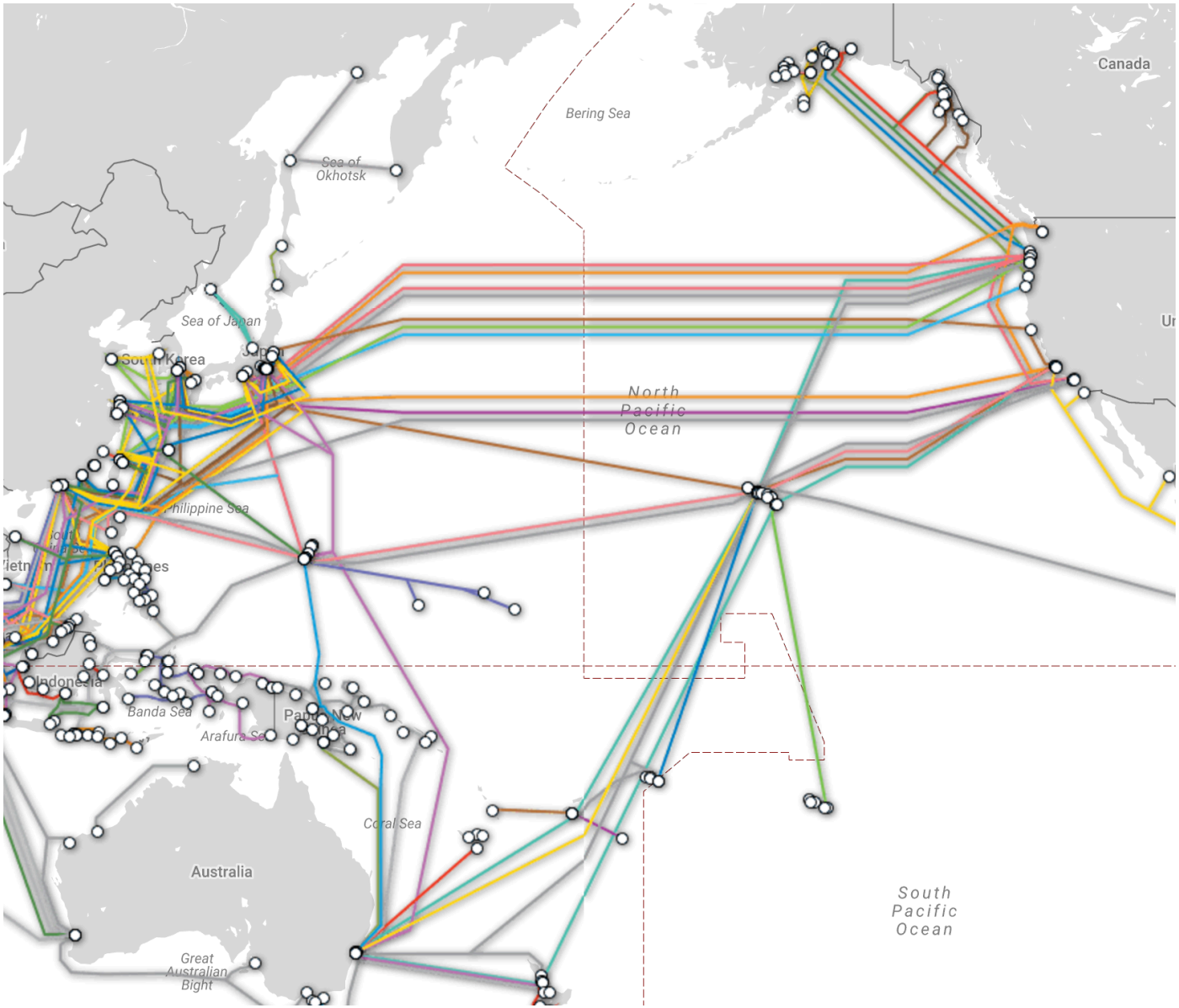
F’ing Comcast



Large-Scale Attacks?

What can you learn if you passively read all data that goes through an ISP?




Canada
Bering Sea
Sea of Okhotsk
Sea of Japan
South Korea
North Pacific Ocean
Philippine Sea
Indonesia
Banda Sea
Arafura Sea
Coral Sea
Australia
Great Australian Bight
South Pacific Ocean

Okay, so what can we do?

Solutions?

Secure protocols (TLS, SSH, etc.)

VPN

Wireless: WPA2

IP: No Source Authentication

Can’t Trust Source IP

IP Raw Sockets

You pick the Layer 4 protocol (or do it yourself)

Why is IP spoofing less effective for TCP than UDP?

DNS: Kaminsky Attack

DNS Transaction IDs

16 bit field -> only 2^{16} possible transaction IDs

Dan Kaminsky: just shout loud enough and wait

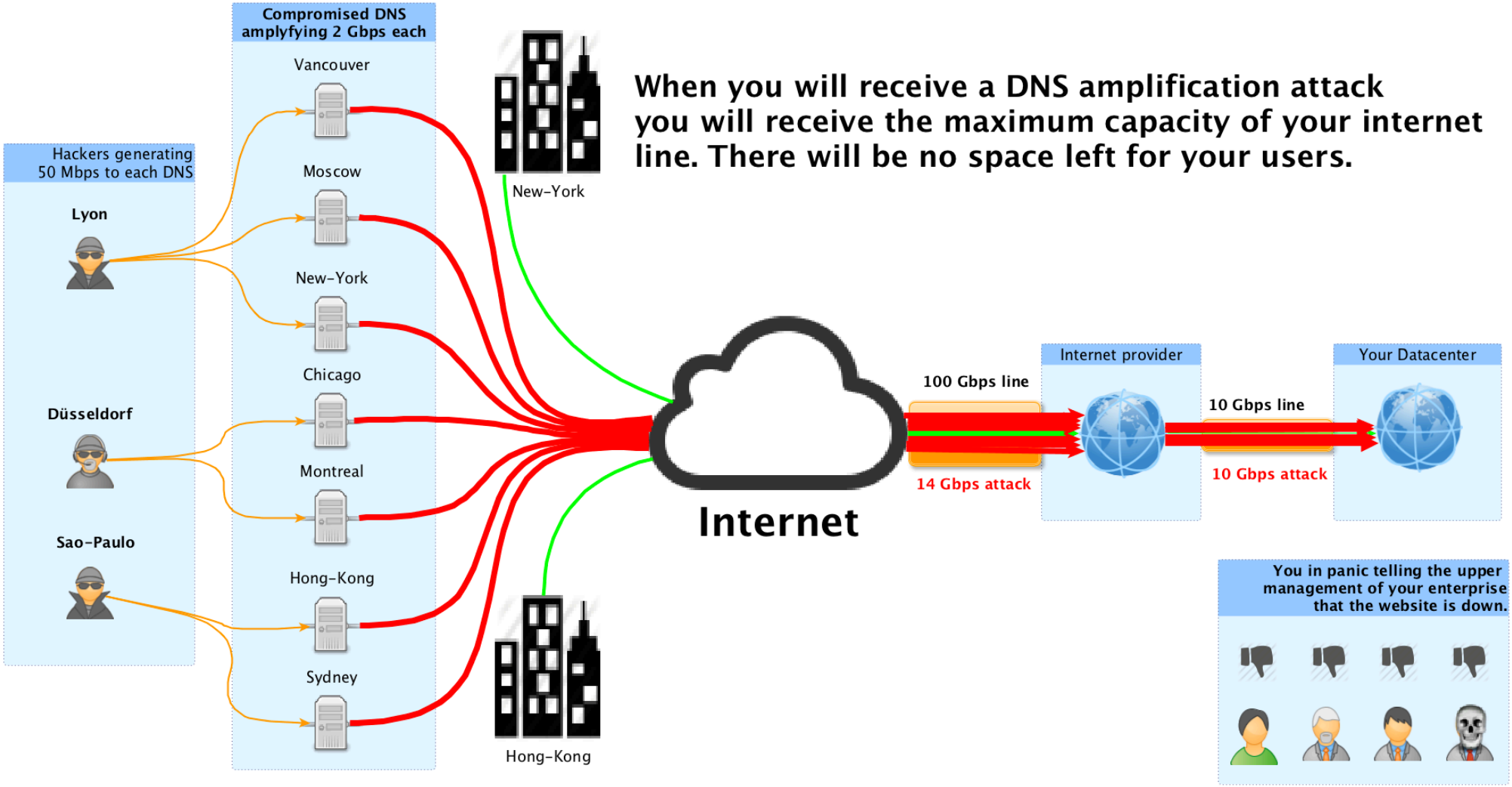
Fix: randomization of source port

How many possibilities now?

Reflection

UDP: to, from, data

UDP protocols that provide services: NTP, DNS


When you will receive a DNS amplification attack you will receive the maximum capacity of your internet line. There will be no space left for your users.
Hackers generating 50 Mbps to each DNS
Lyon
Düsseldorf
Sao-Paulo
Compromised DNS amplyfying 2 Gbps each
Vancouver
Moscow
New-York
Chicago
Montreal
Hong-Kong
Sydney
New-York
Hong-Kong
Internet
100 Gbps line
14 Gbps attack
Internet provider
10 Gbps line
10 Gbps attack
Your Datacenter
You in panic telling the upper management of your enterprise that the website is down.

BGP:
Border Gateway Protocol

BGP:
Border Gullible Protocol

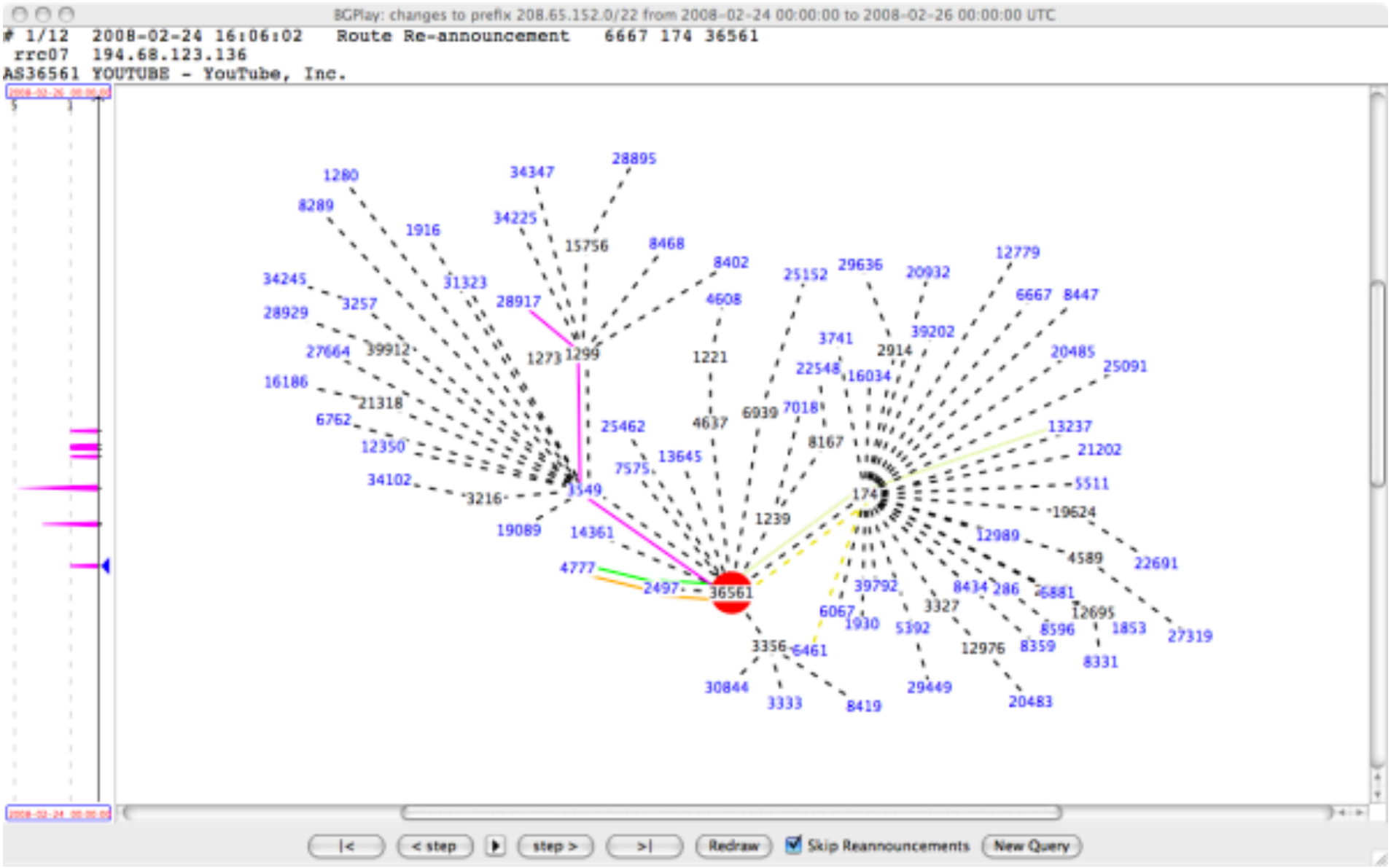
Routing

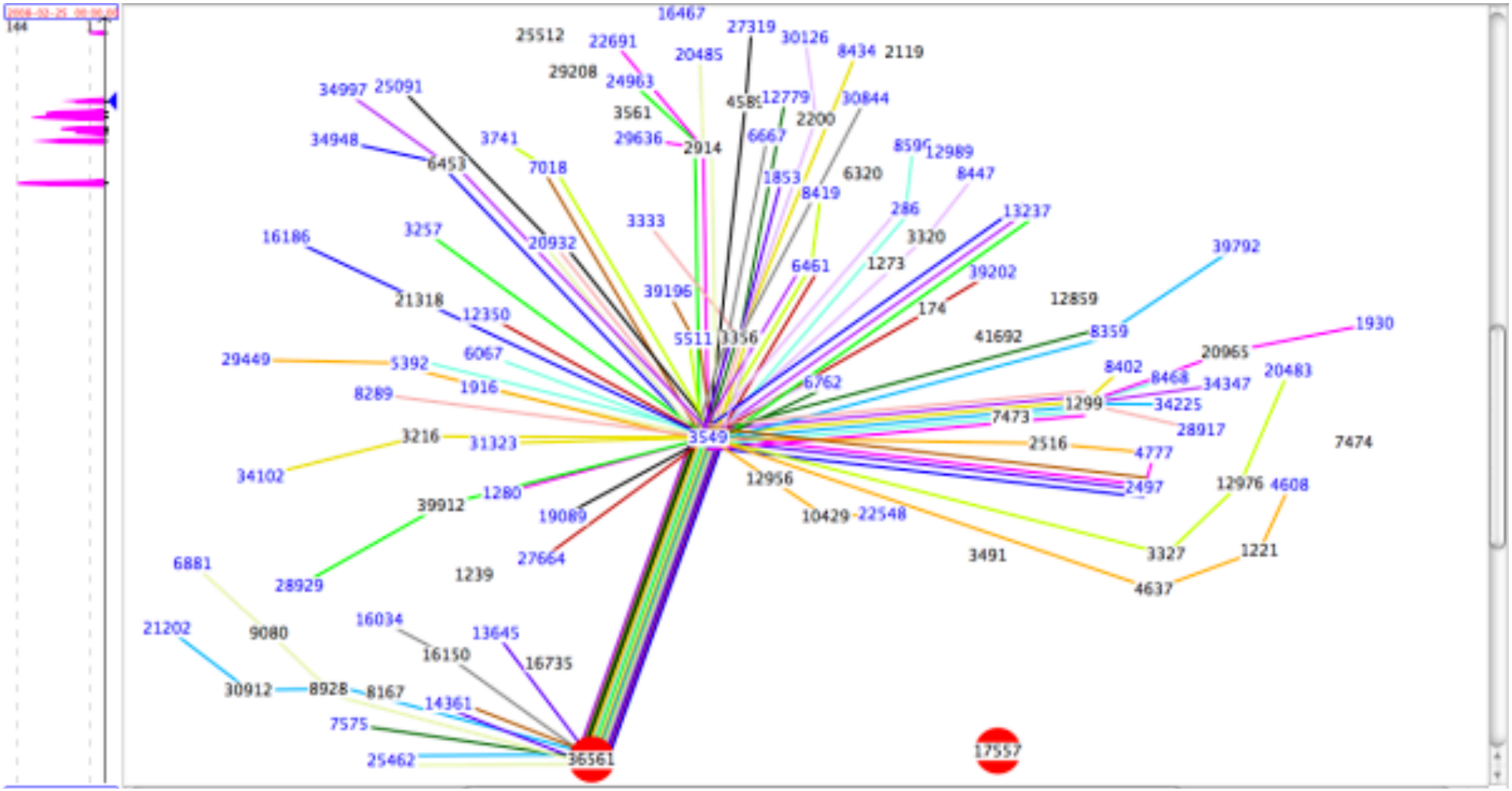
BGP

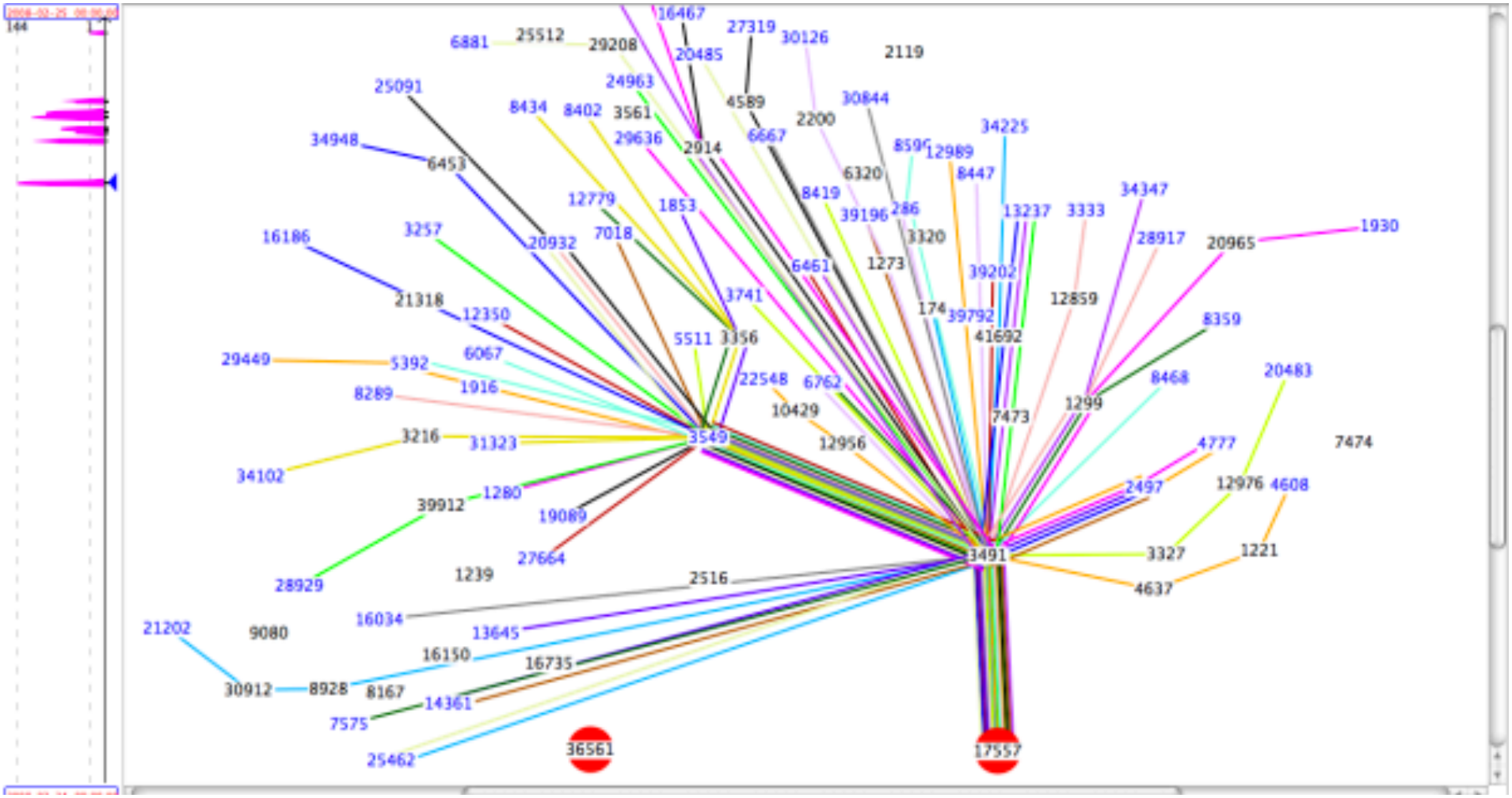
ASes advertise their connectivity to blocks of IP addresses

BGP uses route advertisements to form forwarding tables, loads them into edge routers

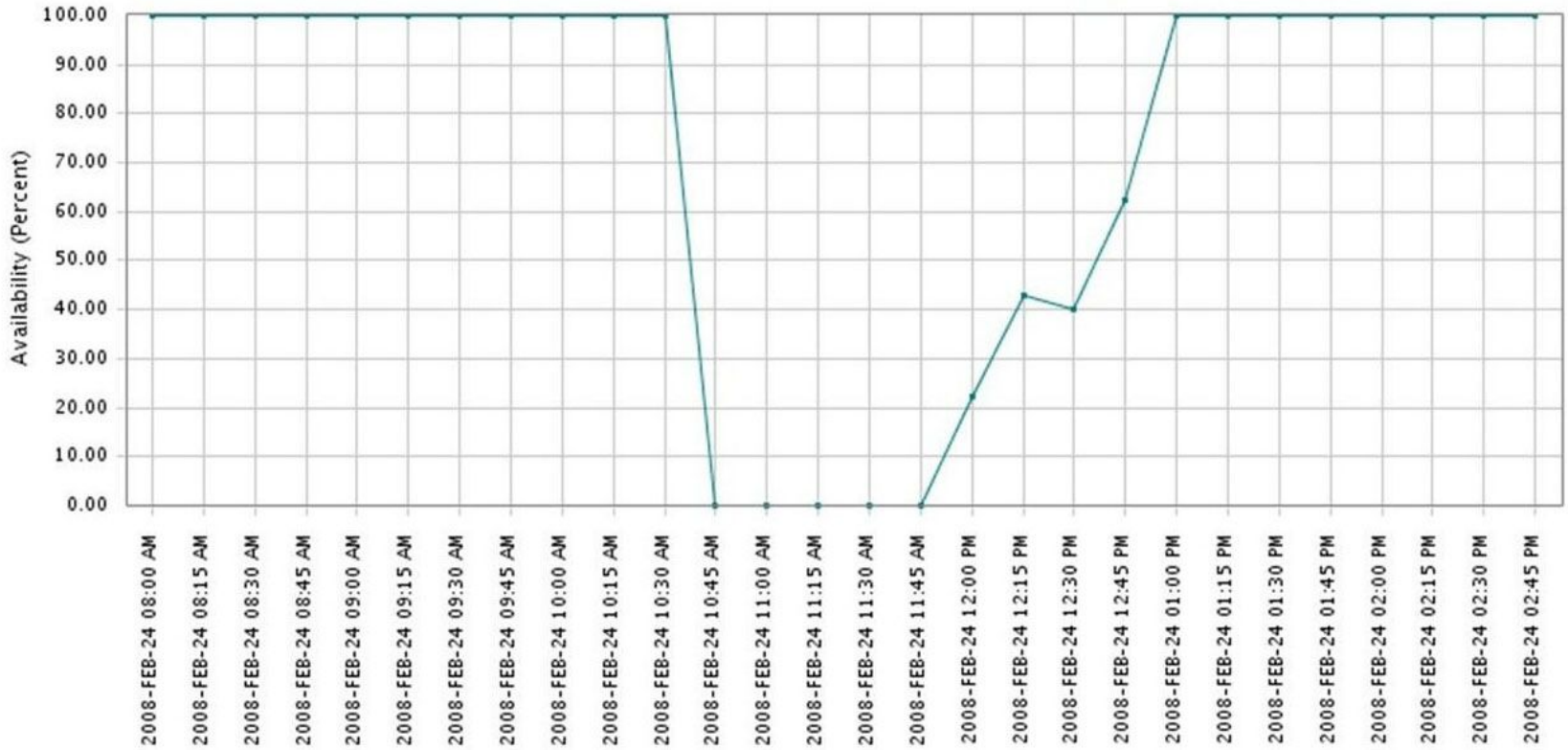
May be multiple routes to some AS. Q: How decide which route to use? A: Heuristics like “more specific address block”


BGPlay: changes to prefix 208.65.152.0/22 from 2008-02-24 00:00:00 to 2008-02-26 00:00:00 UTC
1/12 2008-02-24 16:06:02 Route Re-announcement 6667 174 36561
rrc07 194.68.123.136
AS36561 YOUTUBE - YouTube, Inc.
1280
8289
1916
34347
28895
34225
15756
8468
8402
34245
3257
31323
28917
4608
25152
29636
20932
12779
28929
27664
39912
1273
1299
1221
3741
2914
39202
6667
8447
16186
21318
22548
16034
20485
25091
6762
25462
4637
6939
7018
12350
13645
8167
13237
7575
21202
34102
3216
3549
174
5511
19089
14361
1239
19624
12989
4589
22691
4777
2497
36561
39792
8414
286
6881
6067
1930
3327
5392
12695
1853
27319
8596
3356
6461
12976
8359
8331
30844
3333
8419
29449
20483
|<
< step
step >
>|
Redraw
Skip Reannouncements
New Query

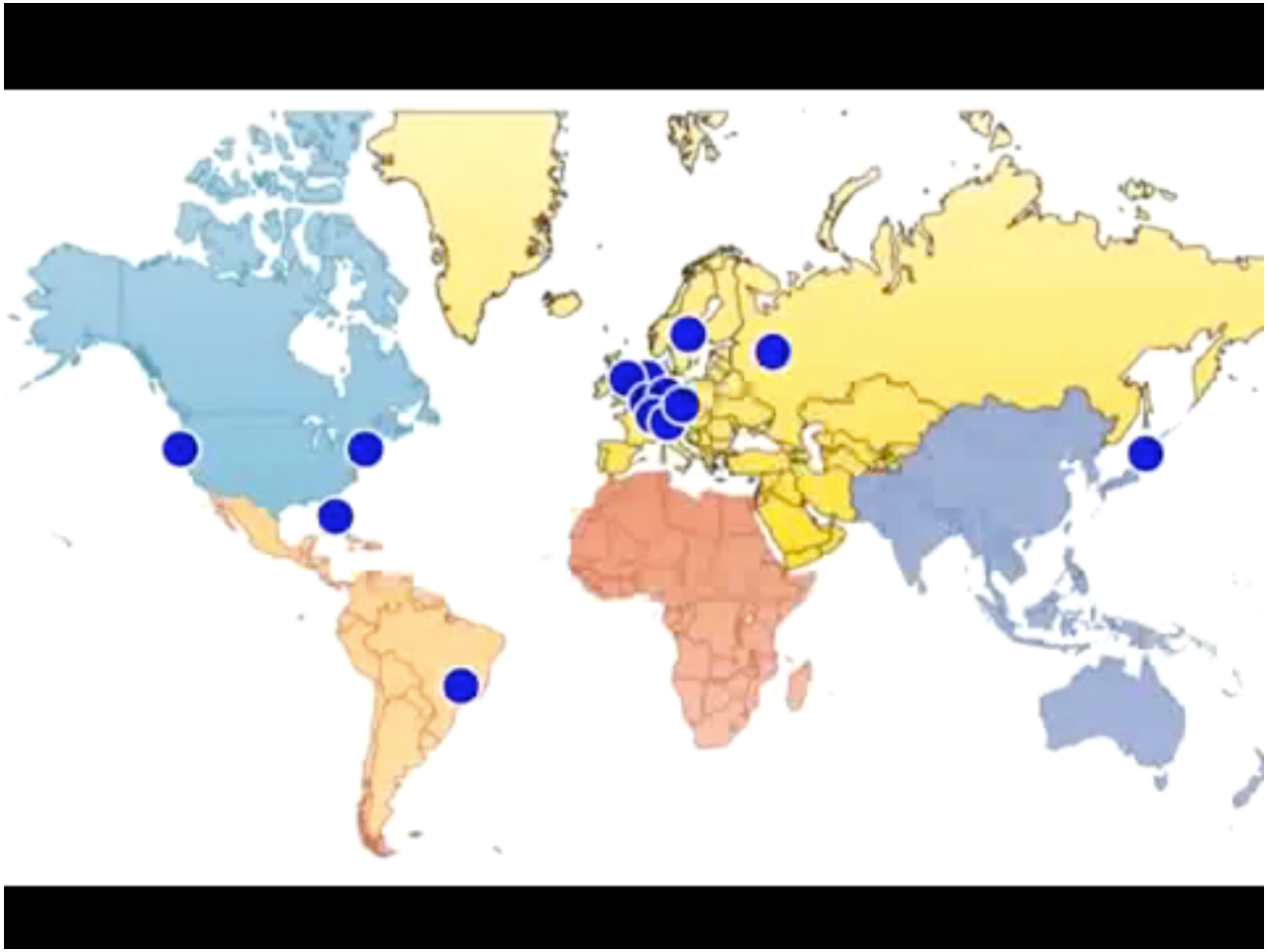

144
16467
25512
22691
27319
30126
20485
8434
2119
29208
24963
34997
25091
4585
12779
30844
3561
2200
34948
3741
29636
2914
6667
6453
7018
1853
6320
8596
12989
8447
8419
3333
286
13237
16186
3257
20932
3320
6461
1273
39792
39196
19202
21318
12350
174
12859
5511
1356
41692
8359
1930
29449
5392
6067
20965
8402
8468
34347
20483
8289
1916
6762
1299
34225
7473
28917
3216
31323
3549
2516
4777
7474
34102
12956
2497
12976
4608
39912
1280
19089
10429
22548
27664
3491
3327
1221
6881
1239
4637
28929
16034
21202
9080
13645
16150
16735
30912
8928
8167
14361
7575
25462
36561
17557


144
16467
27319
30126
6881
25512
29208
20485
2119
25091
24963
4589
30844
8434
8402
3561
2200
34225
34948
29636
2914
6667
8596
12989
6453
6320
8447
12779
8419
34347
1853
39196
286
13237
3333
16186
3257
20932
7018
3320
28917
20965
1930
6461
1273
39202
21318
3741
12859
12350
174
39792
41692
8359
5511
3356
29449
5392
6067
22548
6762
8468
20483
1916
8289
10429
1299
7473
3216
31323
3549
12956
4777
7474
34102
2497
12976
4608
1280
39912
19089
3491
3327
1221
27664
1239
2516
4637
28929
16034
13645
21202
9080
16150
16735
30912
8928
8167
14361
7575
25462
36561
17557

Two minutes later …



RIPE NCC video



Sign All the Things!

Nothing stops this type of hijacking

DNSSEC: signing DNS records

Exploits

sick h4x

Virus: exploit that attaches onto another file or program

Worm: self-propagating exploit

Trojan: exploit disguised as something of interest

Worms

How do worms propagate?

- Scanning for vulnerable hosts
- Sending to everyone in email/chat contacts

Worms

What do worms do?

- Blackmail/ransomware
- Exfiltrate data
- Corrupt files
- Bot

Botnet

Permanently compromised systems with communications

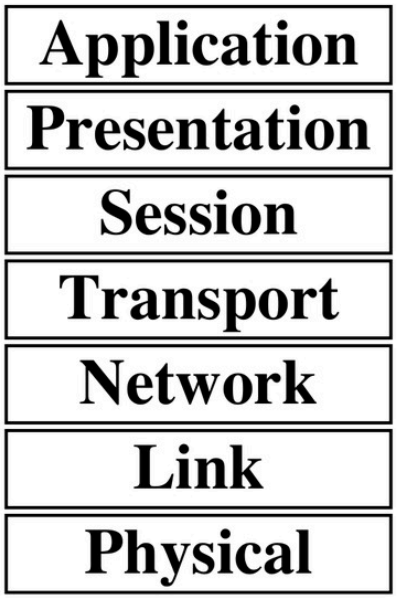
Spam, DDoS, bitcoin mining, etc.

Summary:
Attacking Each Layer

Layer 2 (Link) — Ethernet

ARP Spoofing

Only works on local network



Layer 3 (Network) — IP

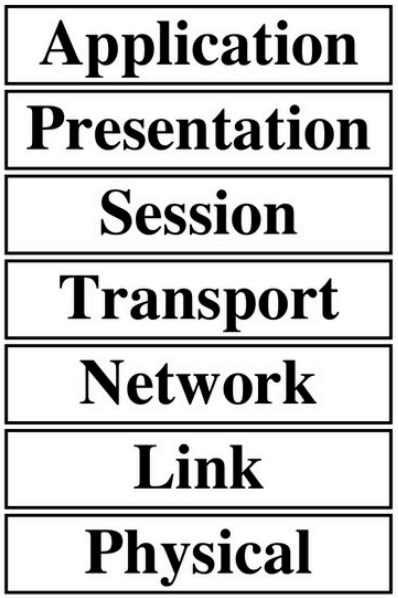
IP Spoofing

Can/should be filtered at the edge

- Ingress filtering: don't forward packets from outside that have inside source address
- Egress filtering: don't forward packets packets from inside that have outside source address.

BGP route hijacking

DNS spoofing



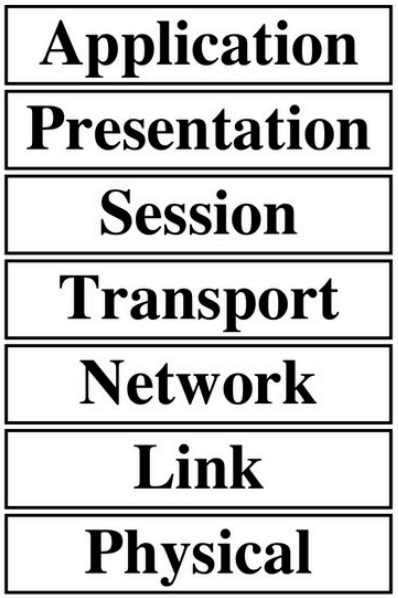
Layer 4 (Transport) — TCP

TCP injection: guess sequence numbers, use IP spoofing

E.g., DoS: TCP RST

Edge filtering

Why don't we do more edge filtering?

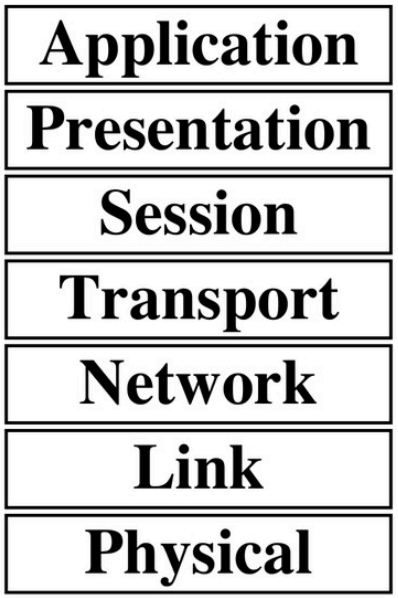


Layer 4 (Transport) — UDP

UDP Amplification

DNS, NTP

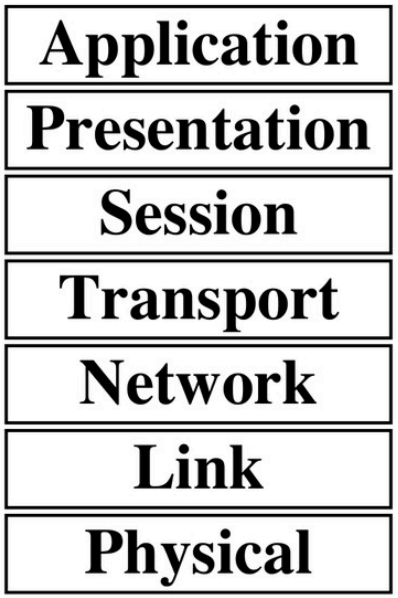
Don’t need a response!



Layer 7 (Application)

DNS maps names to IPs

BGP maps routers to IPs



Getting Security

We can build security on top of untrusted layers!

Next Week…

Authenticating users