

Network Attacks & Defenses

EECS 388 F17



Administrivia

Web project due

Homework 3 is available at <https://eeecs388.org>

Office Hours: by appt

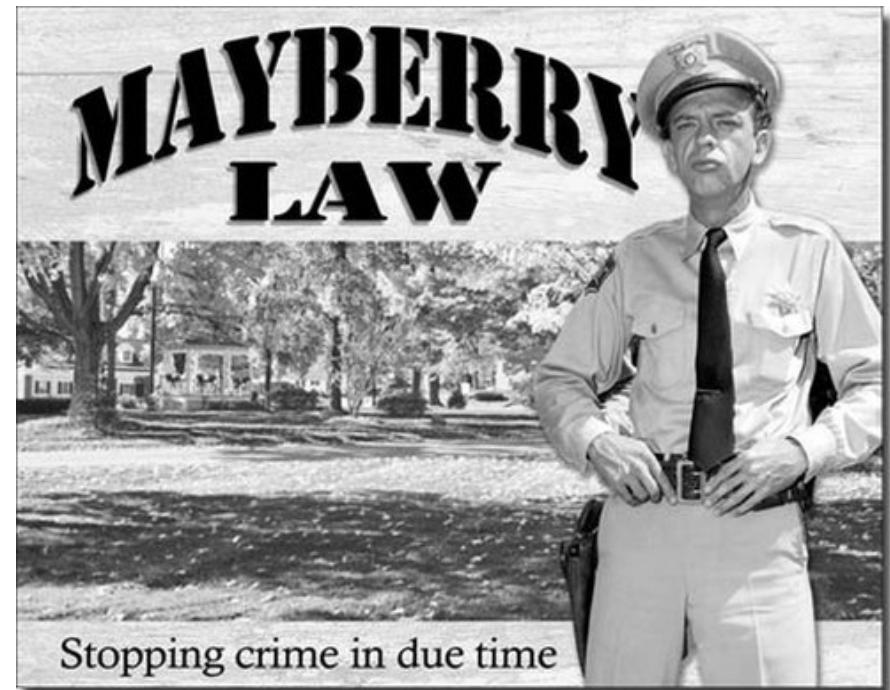
Back In The Day

The Internet was a small town

HTTP

SMTP

NTP



Well, let's just make secure things!

Layers are great!

Layers are a pain!

Application
Presentation
Session
Transport
Network
Link
Physical

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

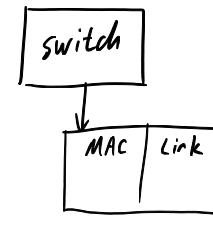
Open networks: anyone in range can listen

Secure protocols:

- WEP -> lol
- WPA -> WPA2

Wired Networks

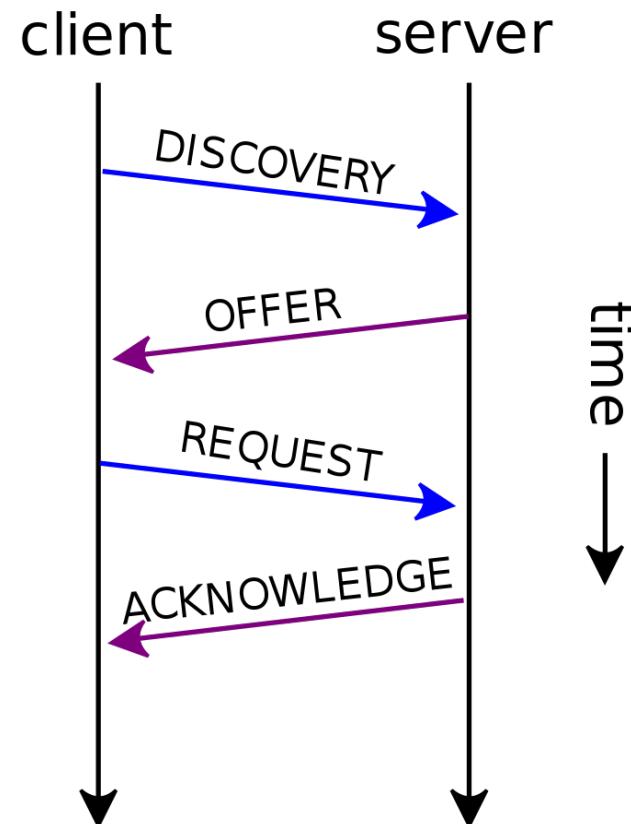
Hub vs. switch



If table full, switch
turns to hub.

Hub: broadcast

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?

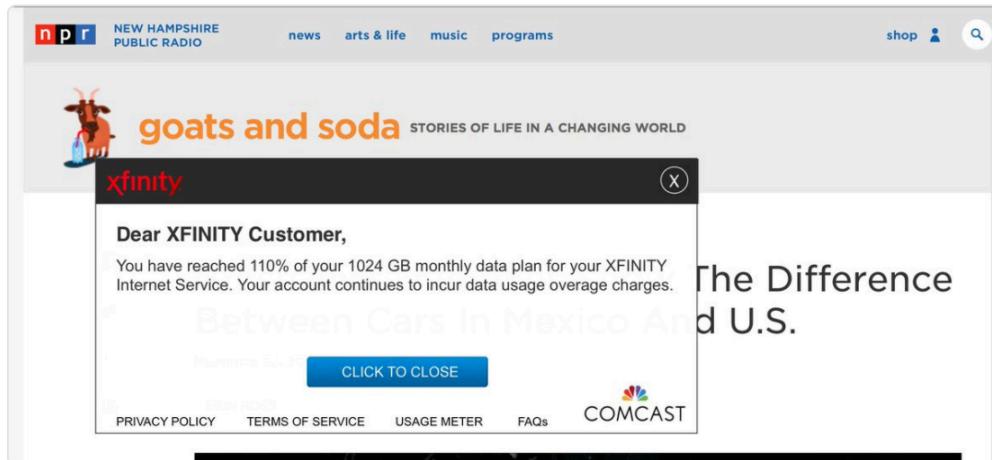
F'ing Comcast



Chris Dzombak
@cdzombak

Following

Comcast is MITMING my shit 😠



9:46 AM - 21 Nov 2016



9

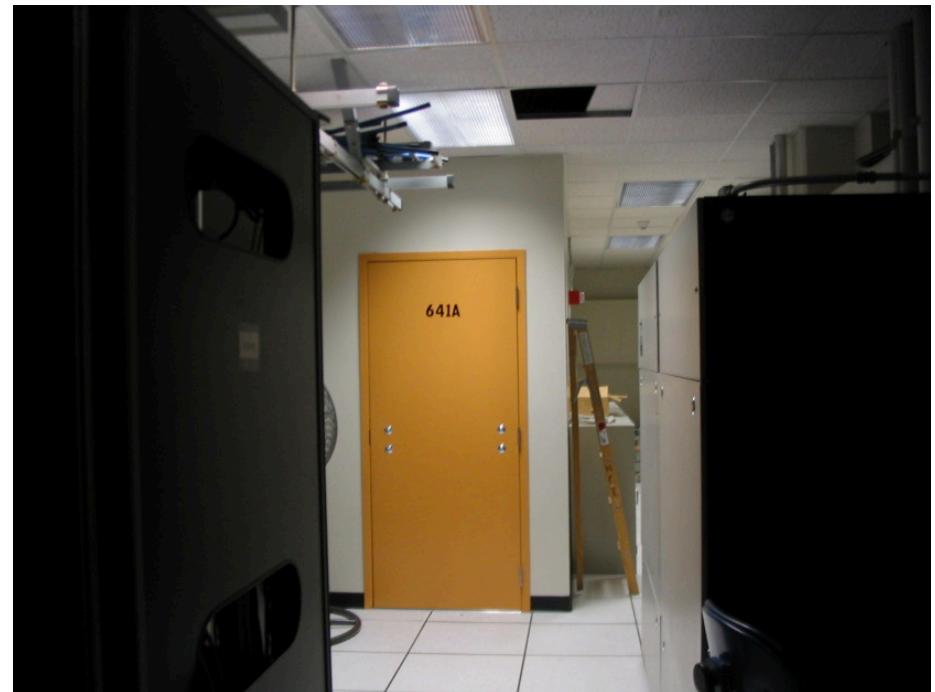
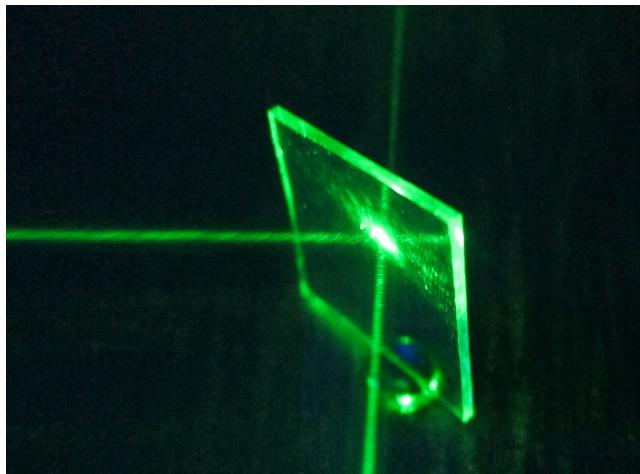


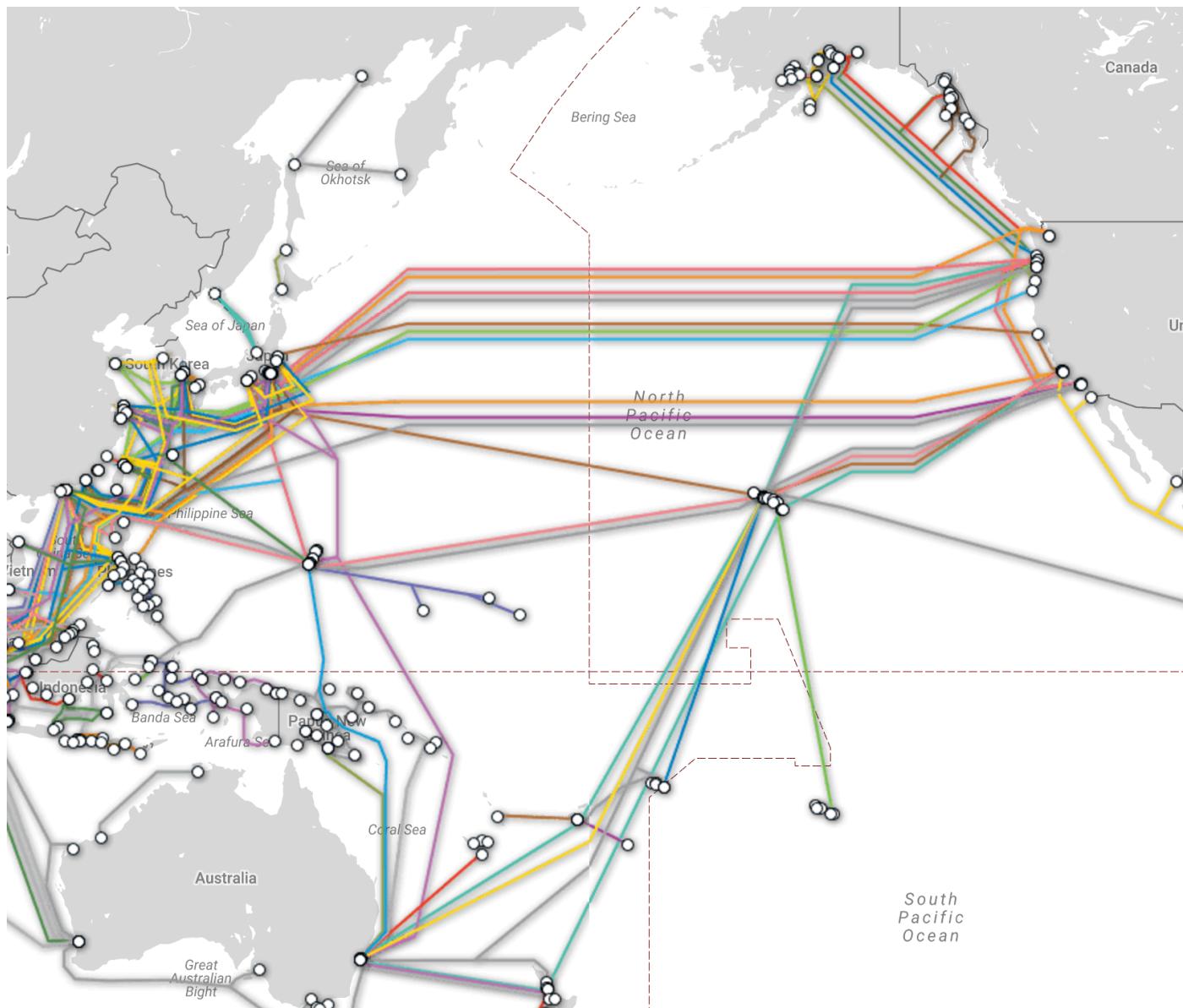
1



Large-Scale Attacks?

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







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

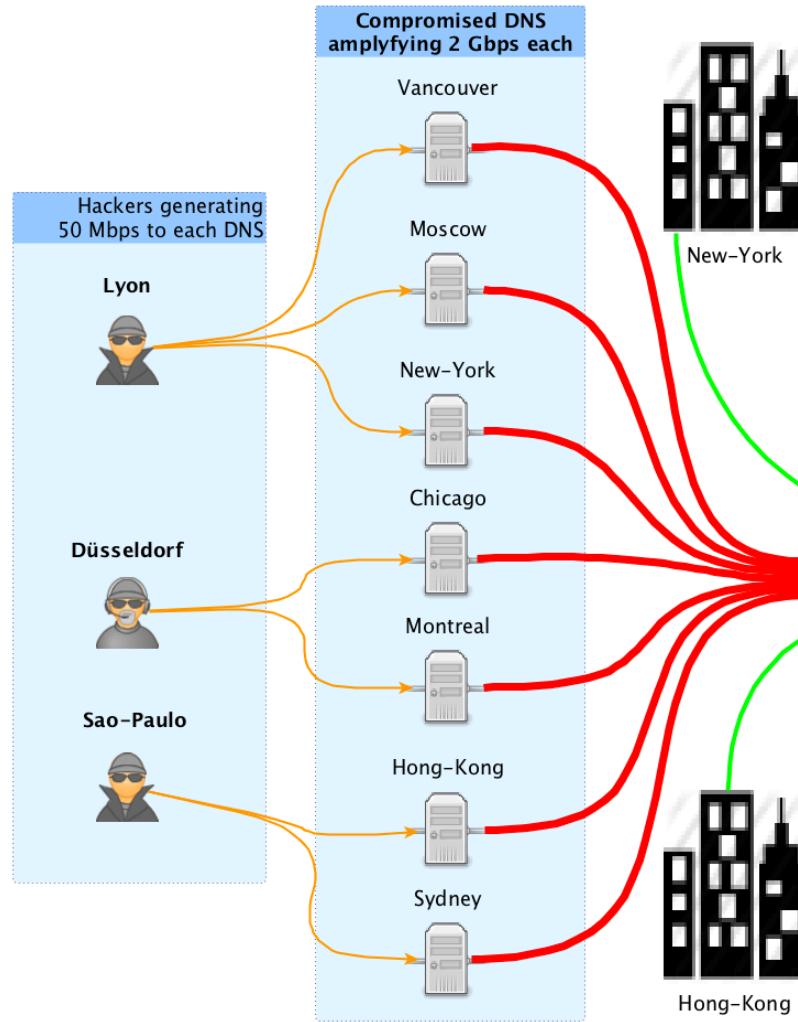
Fix: randomization of source port

How many possibilities now?

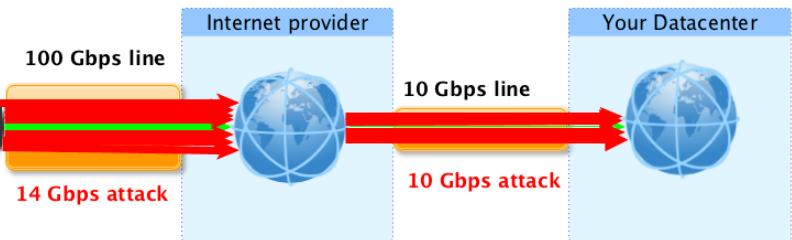
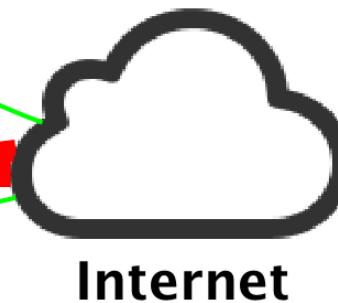
Reflection

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.



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”

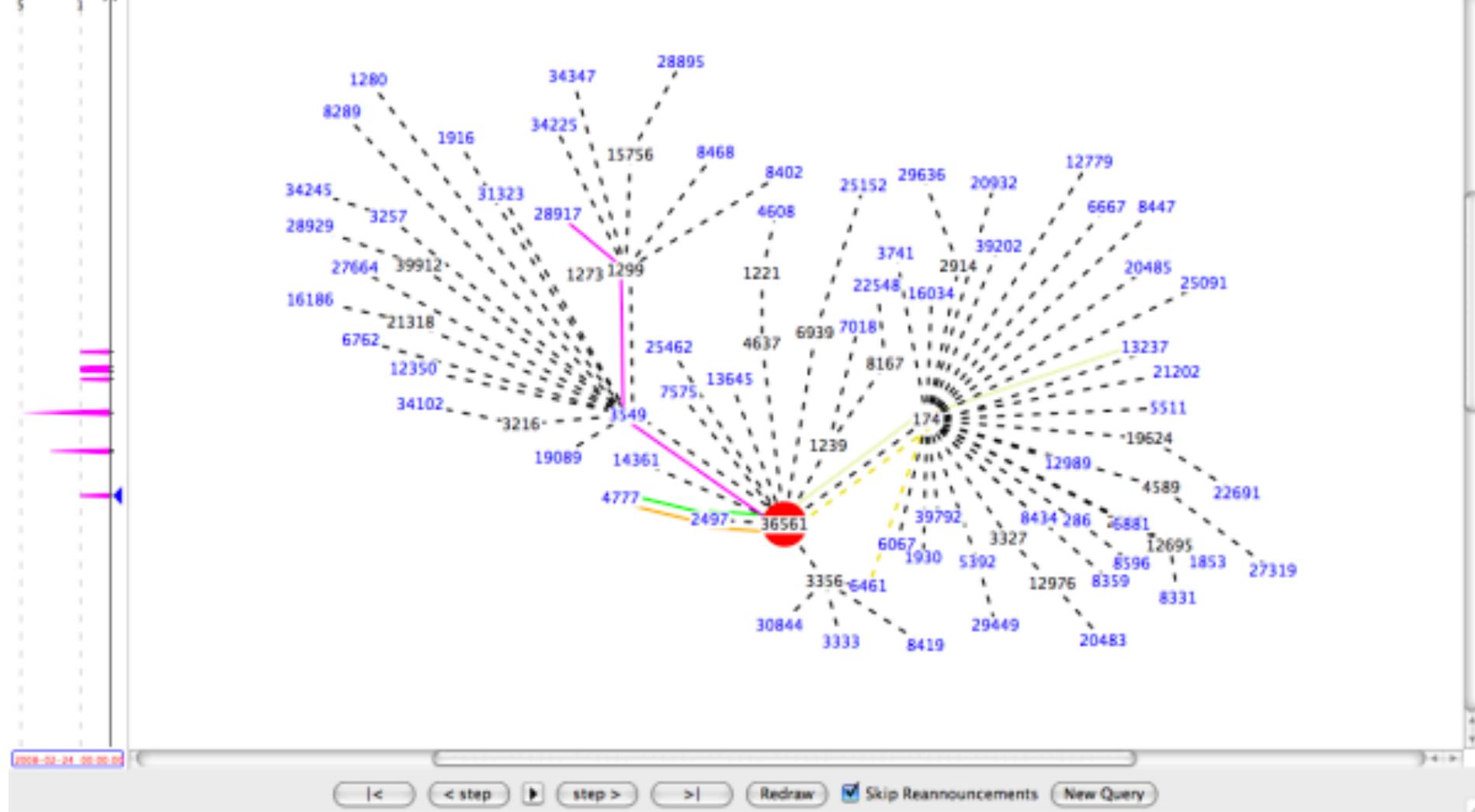
BGPlay: changes to prefix 208.65.152.0/22 from 2008-02-24 00:00:00 to 2008-02-26 00:00:00 UTC

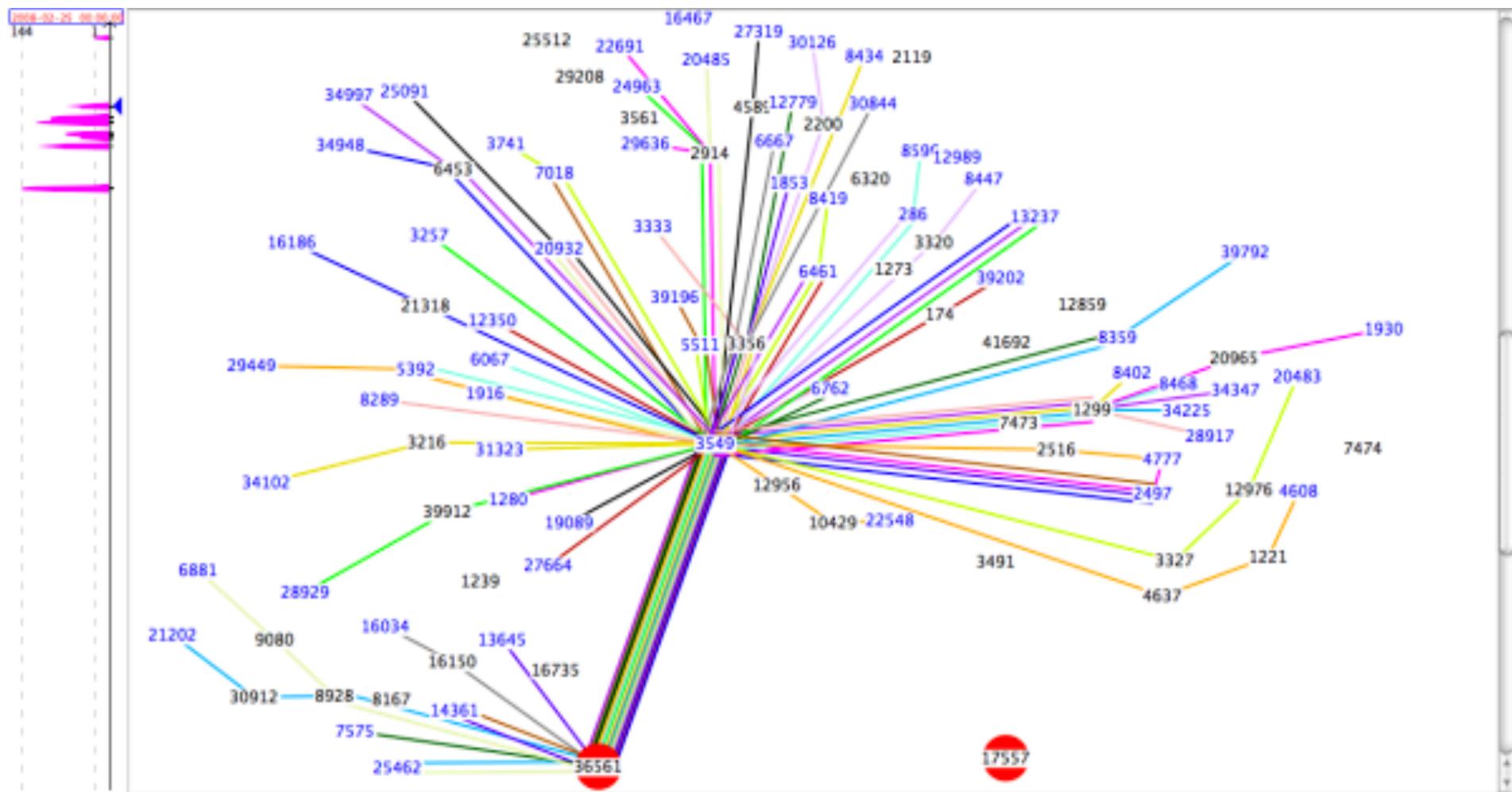
1/12 2008-02-24 16:06:02 Route Re-announcement 6667 174 36561

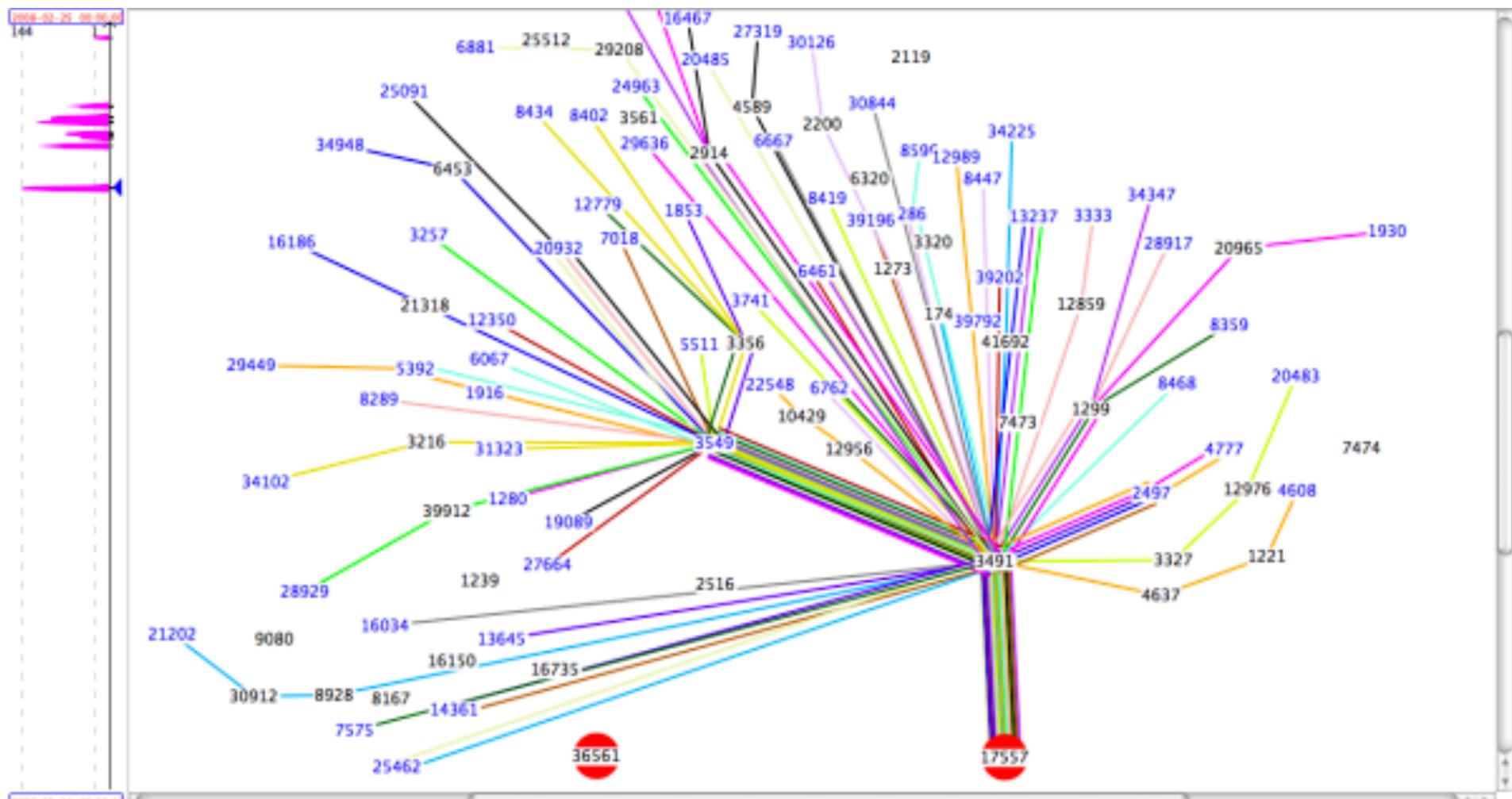
frcc07 194.68.123.136

AS36561 YOUTUBE - YouTube, Inc.

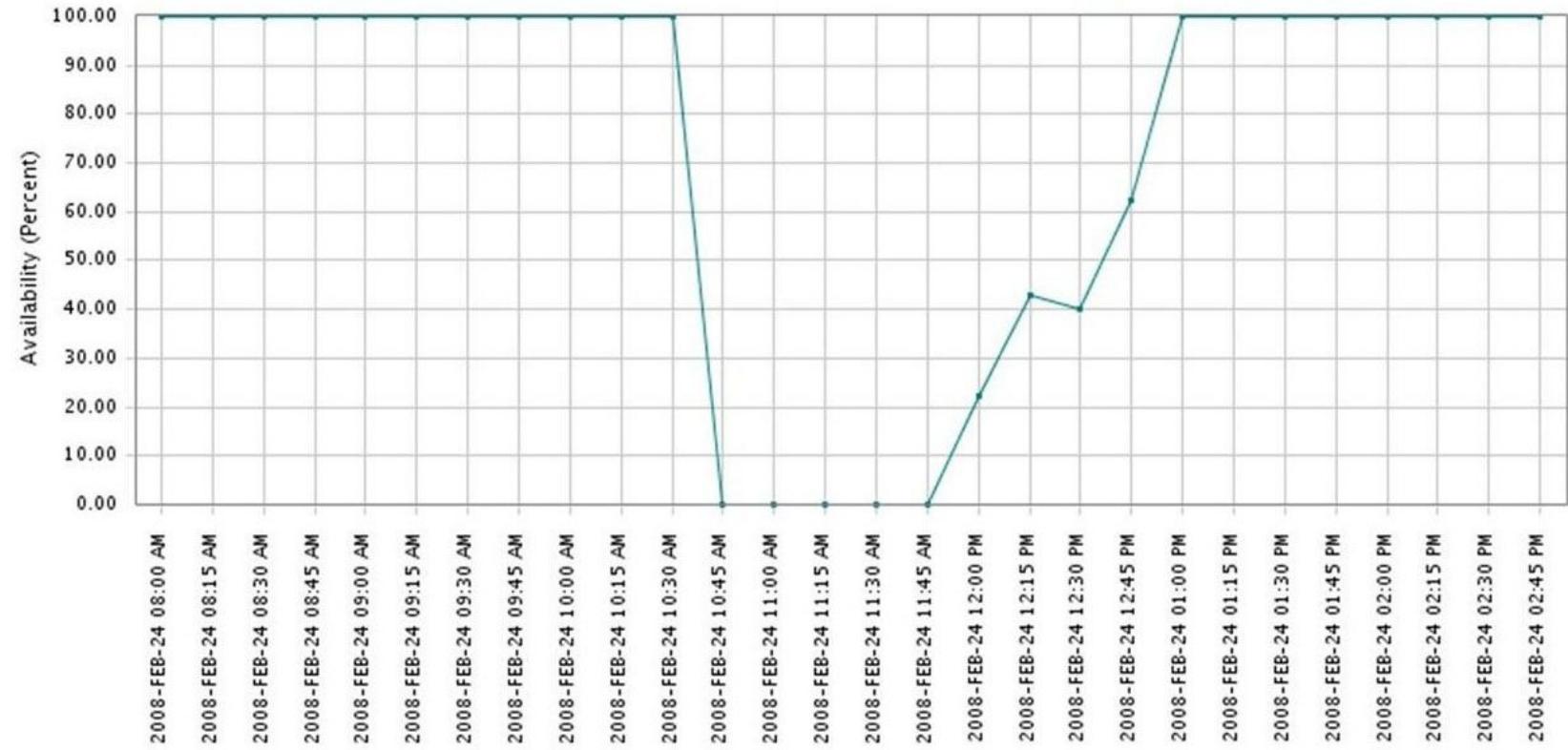
2009-03-26 10:00



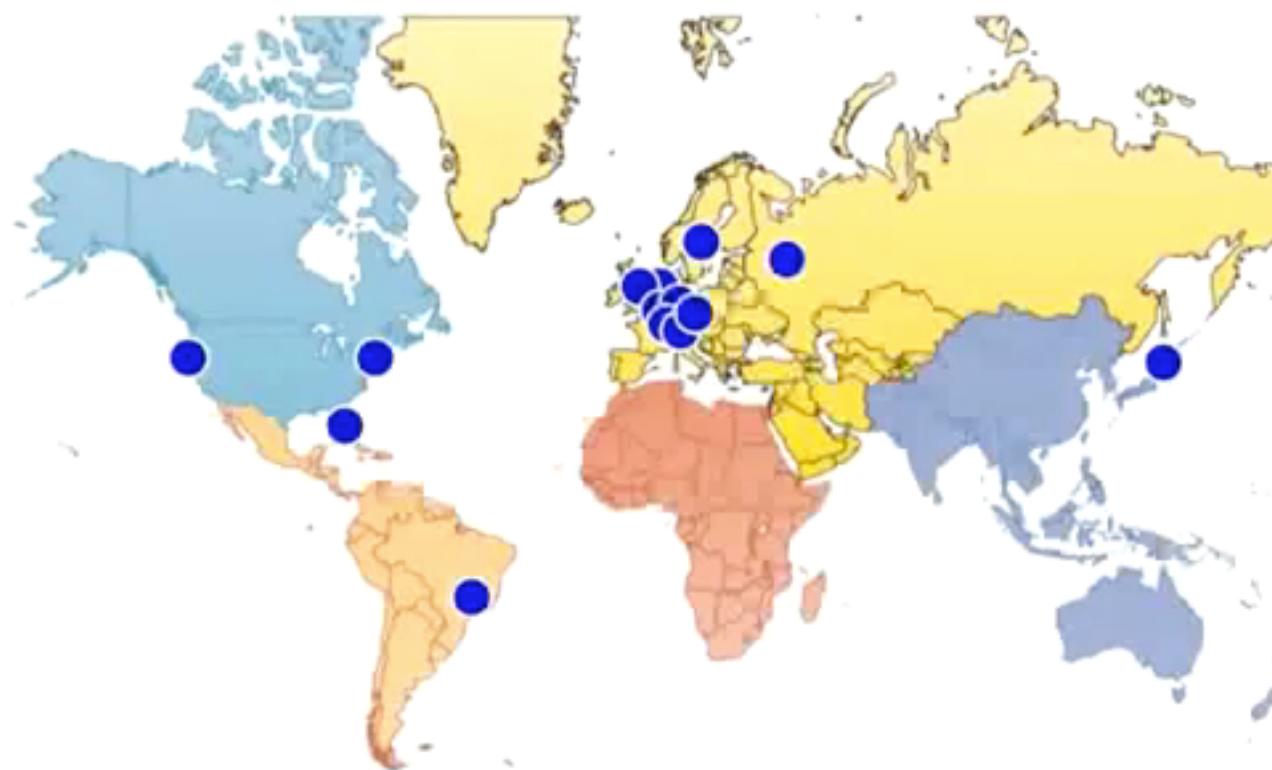




Two minutes later ...



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

Application
Presentation
Session
Transport
Network
Link
Physical

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 from inside that have outside source address.

BGP route hijacking

DNS spoofing

Application
Presentation
Session
Transport
Network
Link
Physical

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?

Application
Presentation
Session
Transport
Network
Link
Physical

Layer 4 (Transport) — UDP

UDP Amplification

DNS, NTP

Don't need a response!

Application
Presentation
Session
Transport
Network
Link
Physical

Layer 7 (Application)

DNS maps names to IPs

BGP maps routers to IPs

Application
Presentation
Session
Transport
Network
Link
Physical

Getting Security

We can build security on top of untrusted layers!

Next Week...

Authenticating users