Hot Topics in
Internet Infrastructure Systems and Security

IIT CS 542 Computer Networking with Professor Nik Sultana
March 31 2025

Guest Lecturer: John Kristoff

Agenda

- Introduction
- DNS centralization, security, and privacy
- BGP routing security and the RPKI
- Internet censorship and fragmentation

Internet Infrastructure Systems

- System of subsystems
    - Naming, Routing
    - Cabling, Airspace, Facilities
    - PKI
    - Number allocation and management
    - ...

Underlying themes

- Few know infrastructure subsystems well
- Fewer talk to the press about them
- Very few are operationally involved in events
- Change is hard and slow
- Never underestimate the installed base

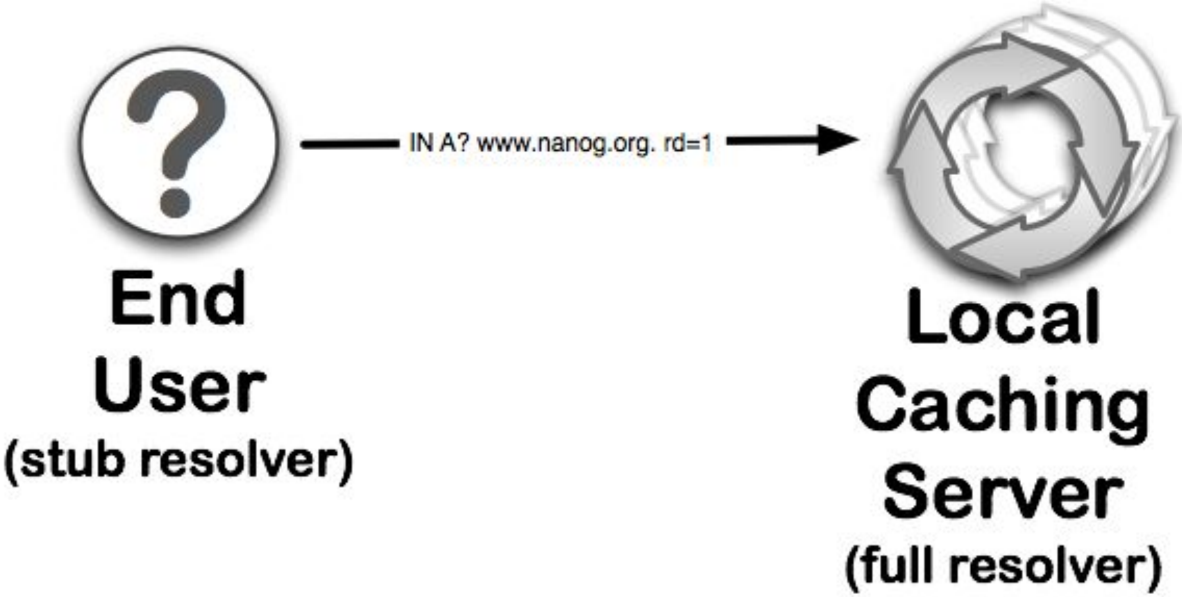
It's not DNS. It's YOU.

Caveats (DNS)

- The DNS is not so simple anymore was it ever?
  - DNS over HTTPS (DoH)
  - QNAME minimization
  - DNSSEC

What is the IPv4 address for www.nanog.org?

Do all the work for me (recursion desired).

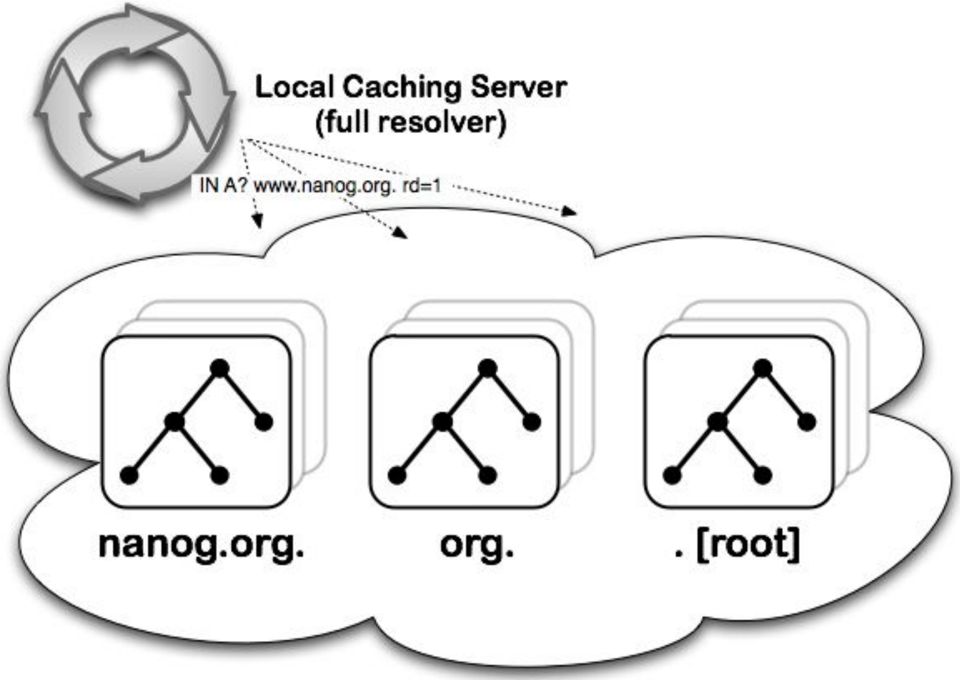


IN A? www.nanog.org. rd=1

End User
(stub resolver)

Local Caching Server
(full resolver)

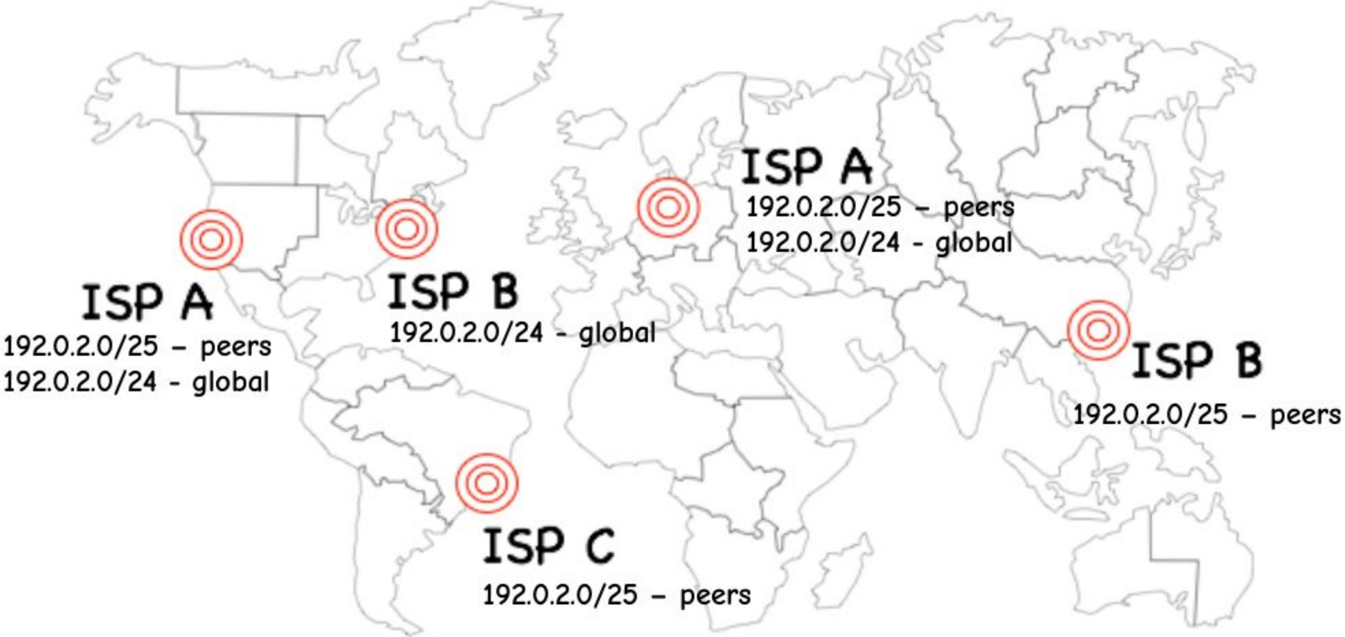
1. Check cache, supply answer if available, or
2. Follow delegation from most specific cached parent, or
3. Start at root if cache is empty.



Query privacy and control

- ISPs historically provided the resolvers
- OpenDNS created a market
    - Google/Cloudflare now own it
- Pros / Cons ?

Shared unicast addressing



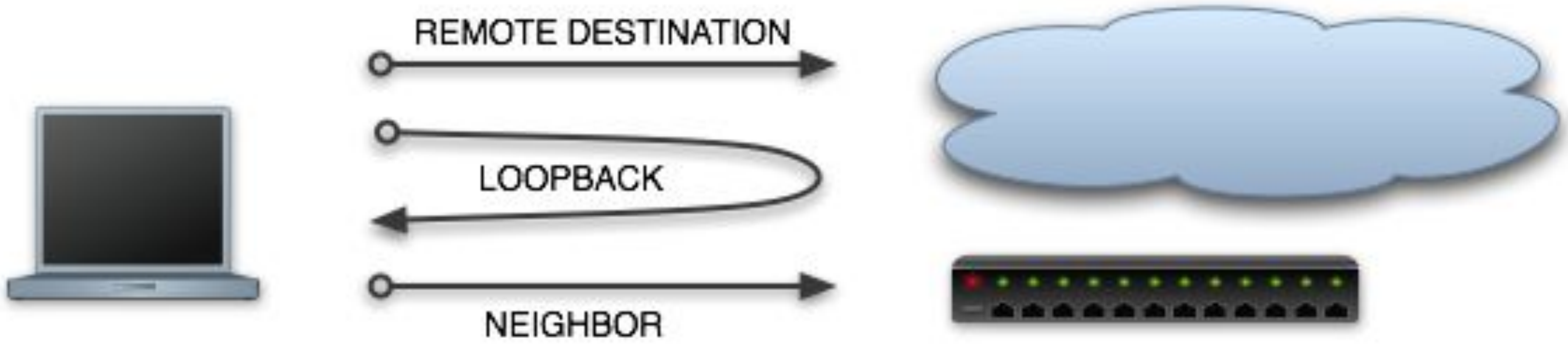
Reading

- “Clouding up the Internet: how centralized is DNS traffic becoming?” (IMC ‘20) Moura, et al.
- “Measuring DNS-over-HTTPS performance around the world” (IMC ‘21) Chhabra, et al.
- “An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?” (IMC ‘19) Lu, et al.

What routers do

192.0.2.0/24
0.0.0.0/0
10.0.0.0/8
1

Who routes?



Must-haves for routing

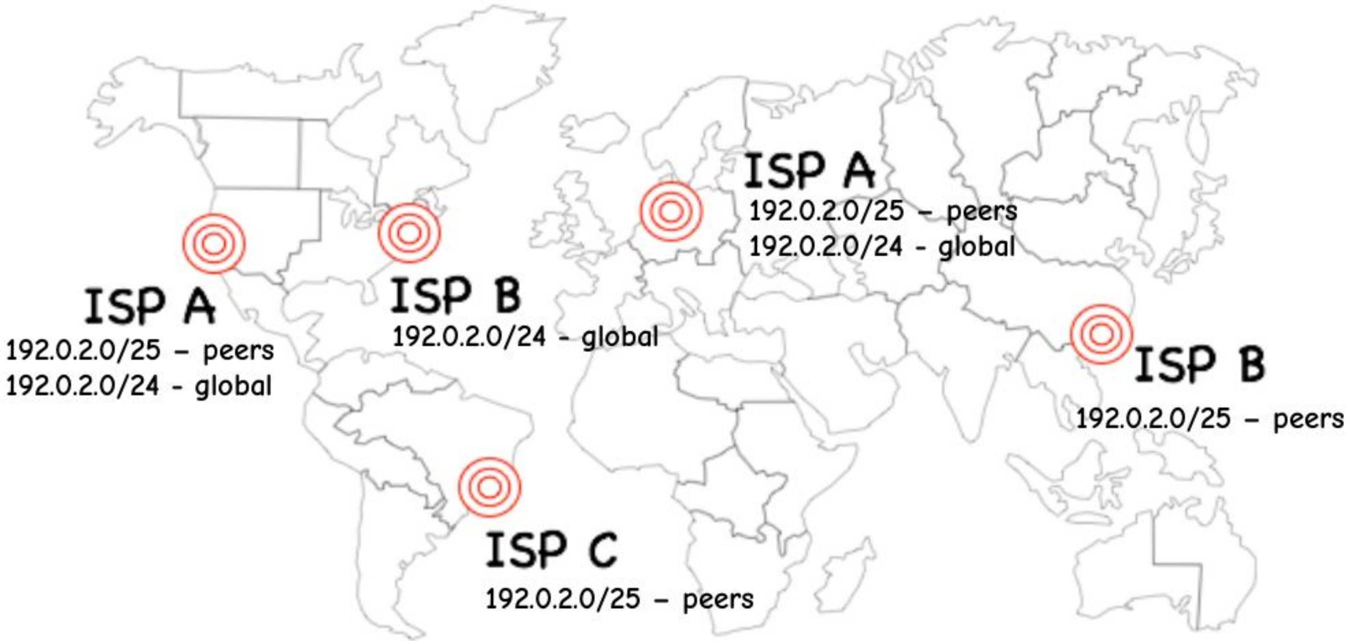
- Destination address
- TTL / hop limit

Key to BGP

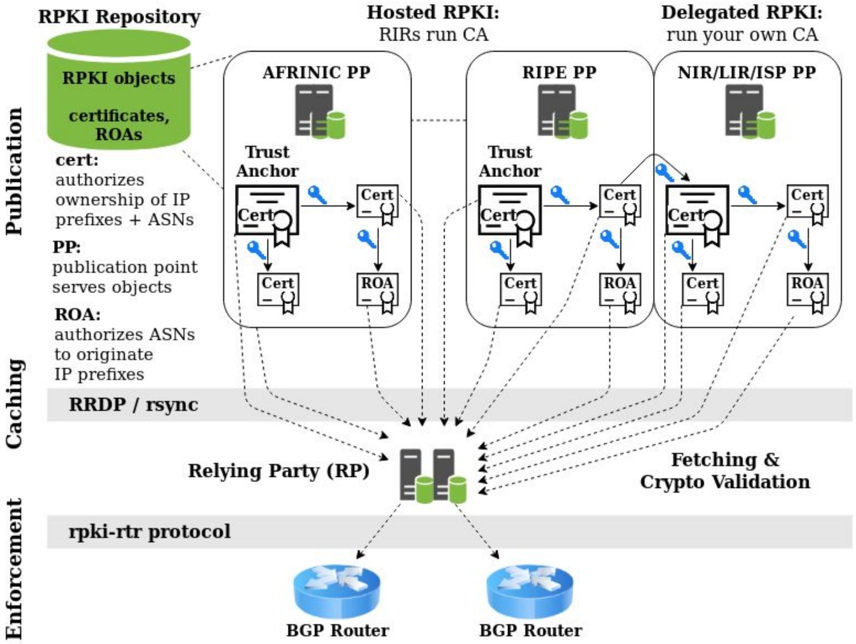
*And the Internet, in practice

- Autonomy
  - Everyone’s view of the world is distinct
  - Policy

Shared unicast addressing



Resource Public Key Infrastructure



Reading

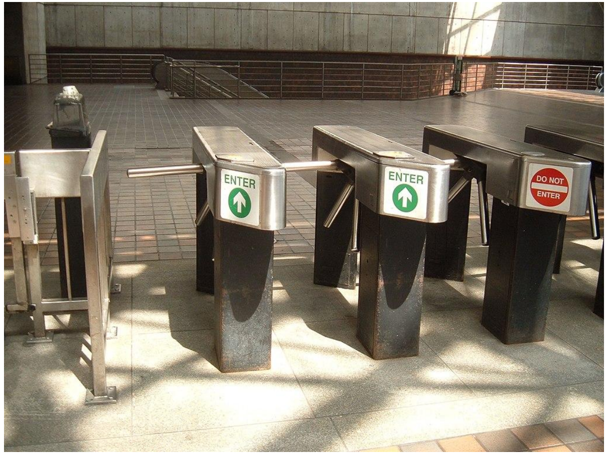
- “Mind your MANRS: measuring the MANRS ecosystem” (IMC ‘22) Du, et al.
- IETF RFC 4593 - Generic Threats to Routing Protocols
- “Securing BGP - A Literature Survey” (IEEE Communications Surveys & Tutorials) Huston, et al.

Internet Censorship and Fragmentation

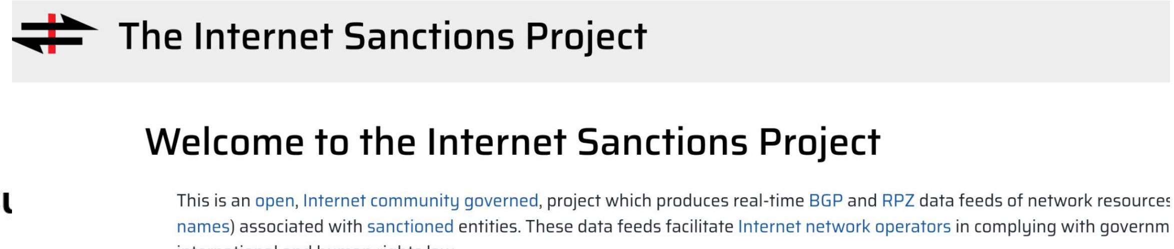
- aka Splintering
- Walled Gardens
- Firewalls and block lists
- Hijacks
- Shutdowns

Walls

Admission Control



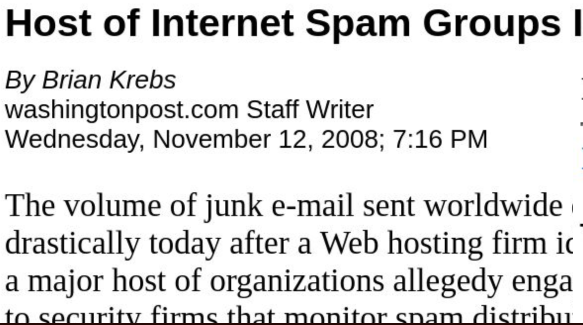
Blockades



The Internet Sanctions Project

Welcome to the Internet Sanctions Project

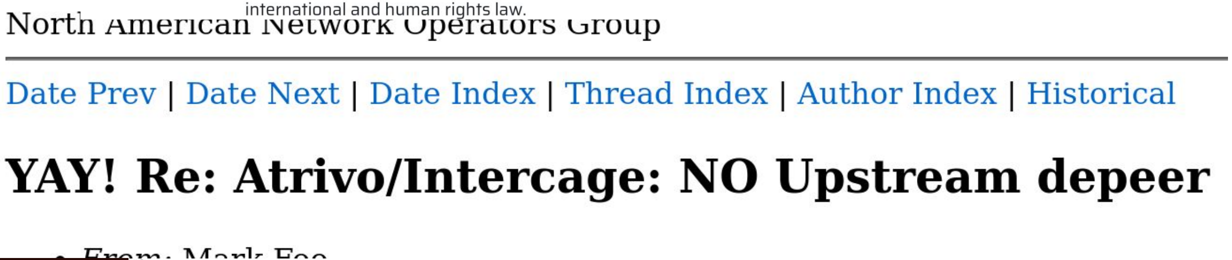
This is an open, Internet community governed, project which produces real-time BGP and RPZ data feeds of network resources
names) associated with sanctioned entities. These data feeds facilitate Internet network operators in complying with governm
international and human rights law.



Host of Internet Spam Groups Is Cu

By Brian Krebs
washingtonpost.com Staff Writer
Wednesday, November 12, 2008; 7:16 PM

The volume of junk e-mail sent worldwide
drastically today after a Web hosting firm id
a major host of organizations allegedy enga
to security firms that monitor spam distribu

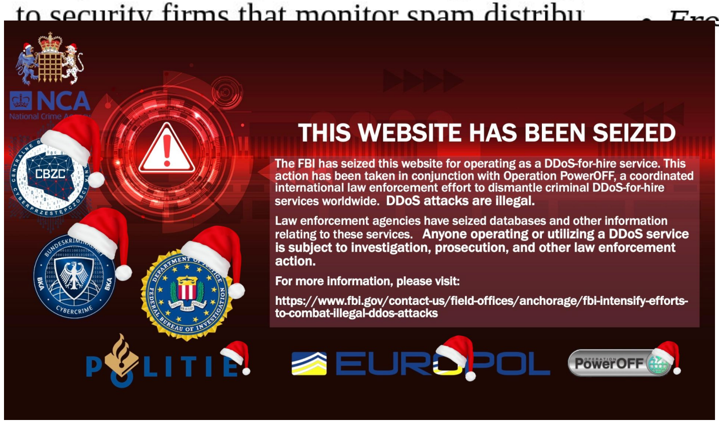


North American Network Operators Group

Date Prev | Date Next | Date Index | Thread Index | Author Index | Historical

YAY! Re: Atrivo/Intercage: NO Upstream depeer

- *From:* Mark Foo

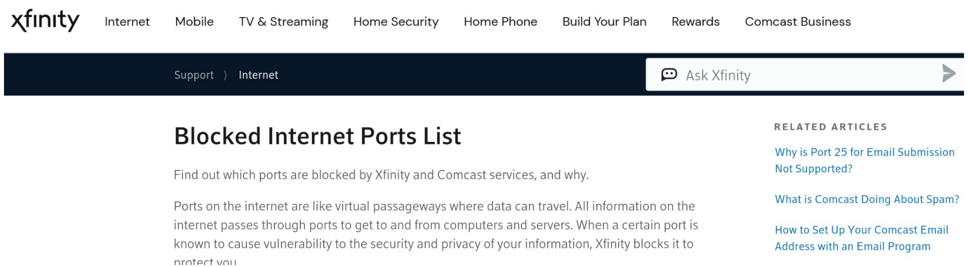


THIS WEBSITE HAS BEEN SEIZED

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. **DDoS attacks are illegal.**

Law enforcement agencies have seized databases and other information relating to these services. **Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.**

For more information, please visit:
https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks



Blocked Internet Ports List

Find out which ports are blocked by Xfinity and Comcast services, and why.

Ports on the internet are like virtual passageways where data can travel. All information on the internet passes through ports to get to and from computers and servers. When a certain port is known to cause vulnerability to the security and privacy of your information, Xfinity blocks it to protect you.

RELATED ARTICLES

Why is Port 25 for Email Submission Not Supported?

What is Comcast Doing About Spam?

How to Set Up Your Comcast Email Address with an Email Program

The GFW is more (less) than a FW

- HTTP fetches with “bad text ” in URLs
- Tor blocking
- “Western” content/service censorship
- 8.8.8.8 hijacking and answer injection
- Oh… and HTTP/TCP reflection/amplification! Oops

Shutdowns

Egypt Leaves The Internet

Jim Cowie

NANOG51, Miami
1 February 2011

Techno-Nationalism

- We’re beginning to see Internet versions all over
  - Various UN committee efforts
  - DNS4EU
  - EU tech alternatives movement
- There are rogue actors too
  - e.g.,threats to standards, governance, RIRs

Border Disputes

Border Changes

New Borders

Reading

- “Internet Sanctions on Russian Media: Actions and Effects” (FOCI ‘24) Kristoff, et al.
- OONI research reports https://ooni.org/reports/
- “Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet” (Council on Foreign Relations Task Force Report), Fick et al.

Reading

- “Internet Sanctions on Russian Media: Actions and Effects” (FOCI ‘24) Kristoff, et al.
- OONI research reports https://ooni.org/reports/
- “Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet” (Council on Foreign Relations Task Force Report), Fick et al.

Thank you, contact information

Contact: John Kristoff

jtk@dataplane.org

https://dataplane.org/jtk/

https://infosec.exchange/@jtk