DHS - September 2013

Jeff.Moss@icann.org

What I have been thinking about

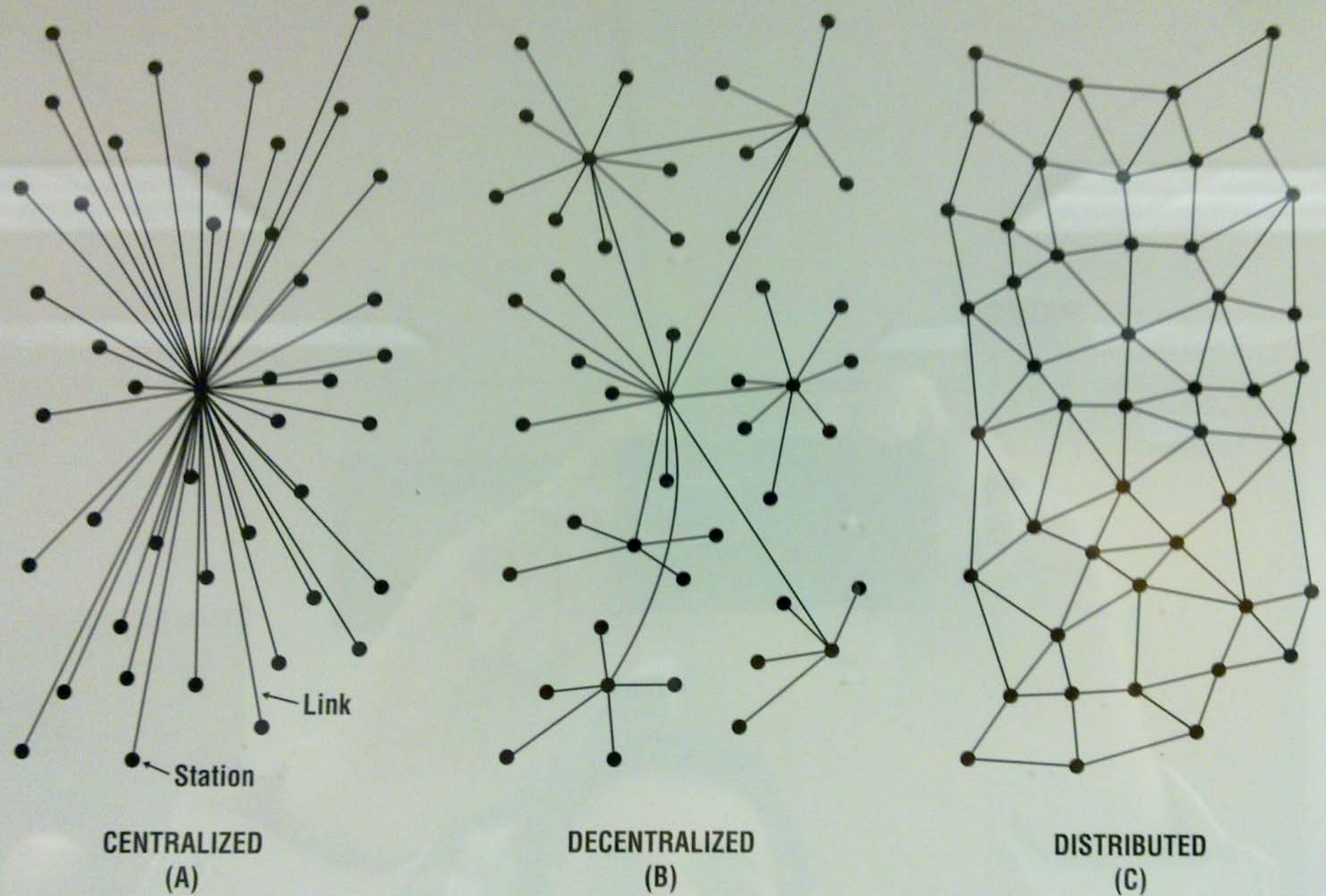
- Complexity
- Internet actors
- Growing DDOS volume
- Issues around the root of in the DNS

  (And the vulnerability market, nation state threats, layer 8 politics, cyber legislation, etc.)

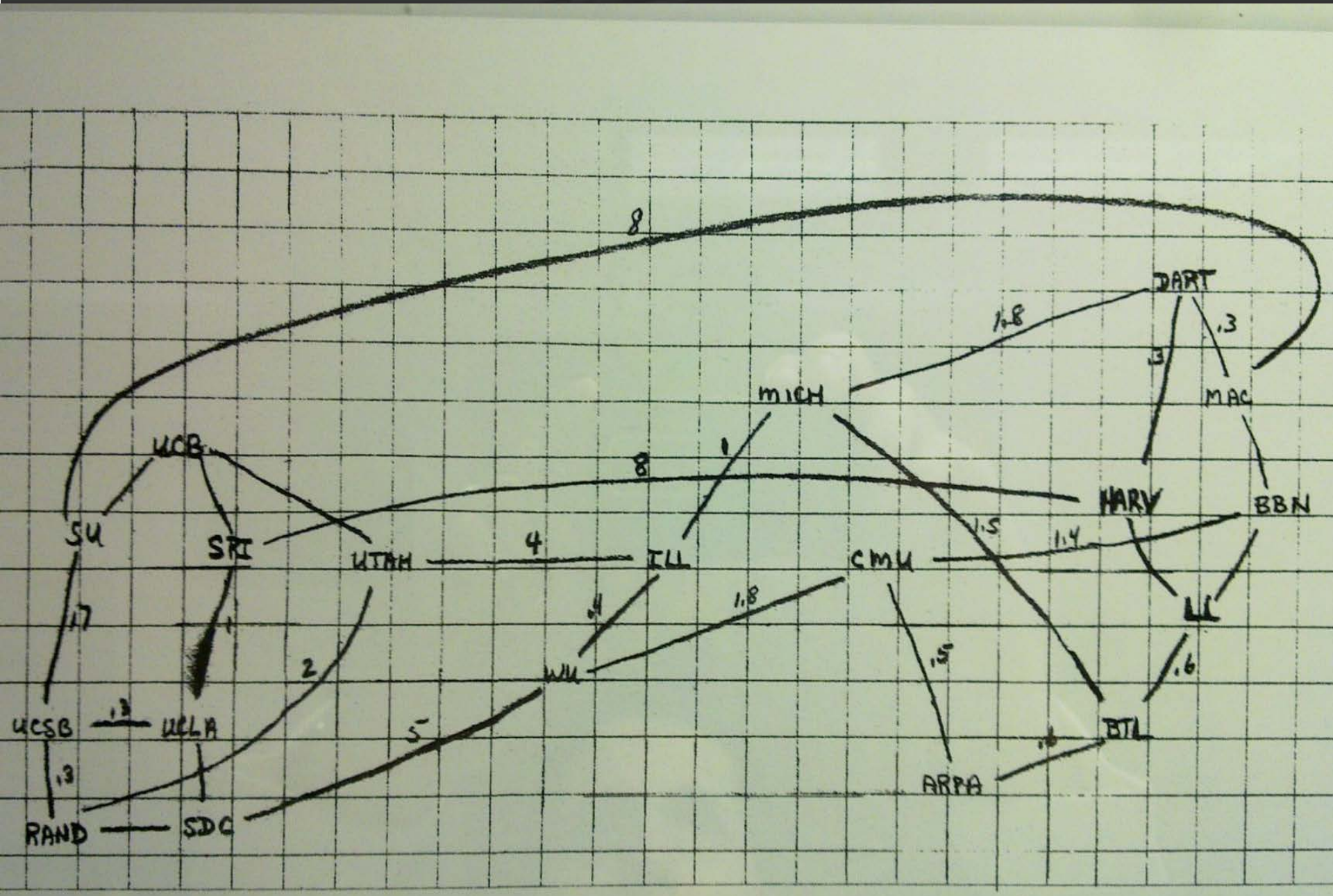

Industrialization


Information Age

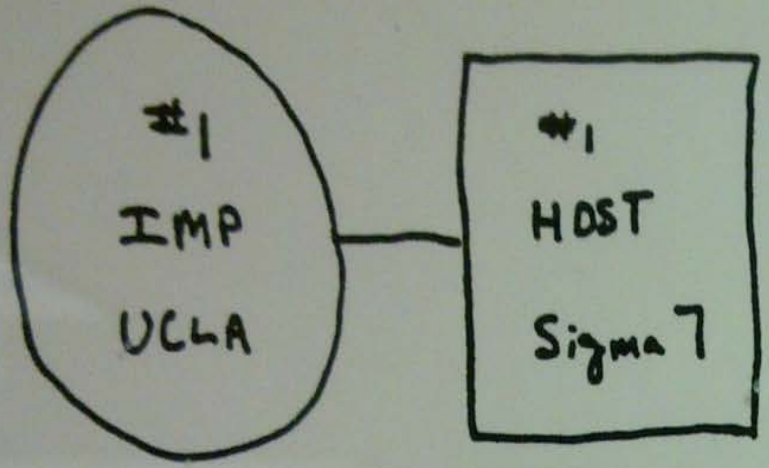
1964 – Network Topologies by Paul Baran



1969 Proposed ARPANET topology by Larry Roberts



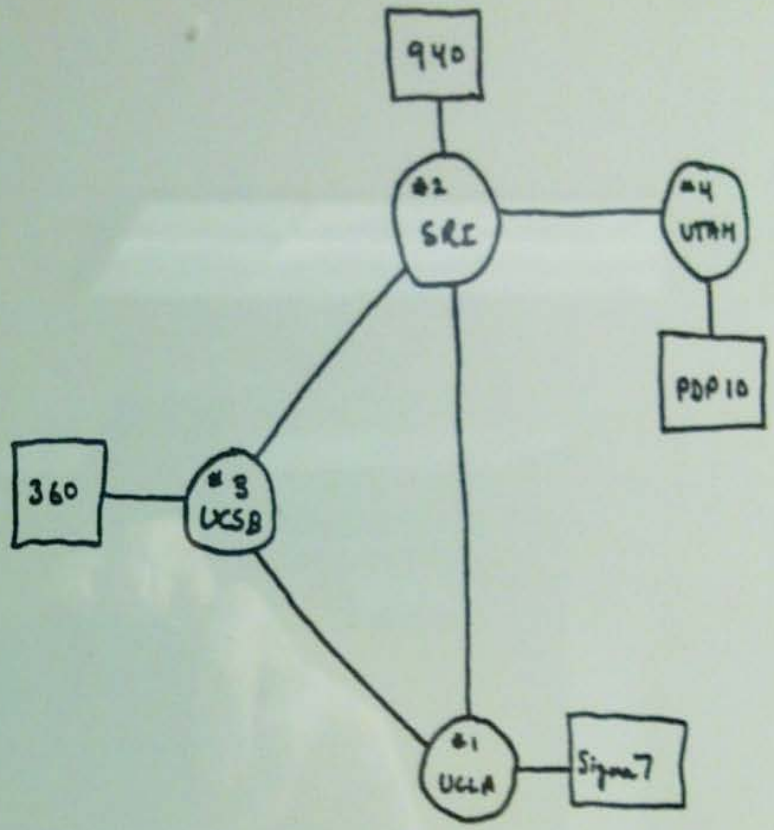
Sept 1969 ARPA network



THE ARPA NETWORK

SEPT 1969

1 NODE

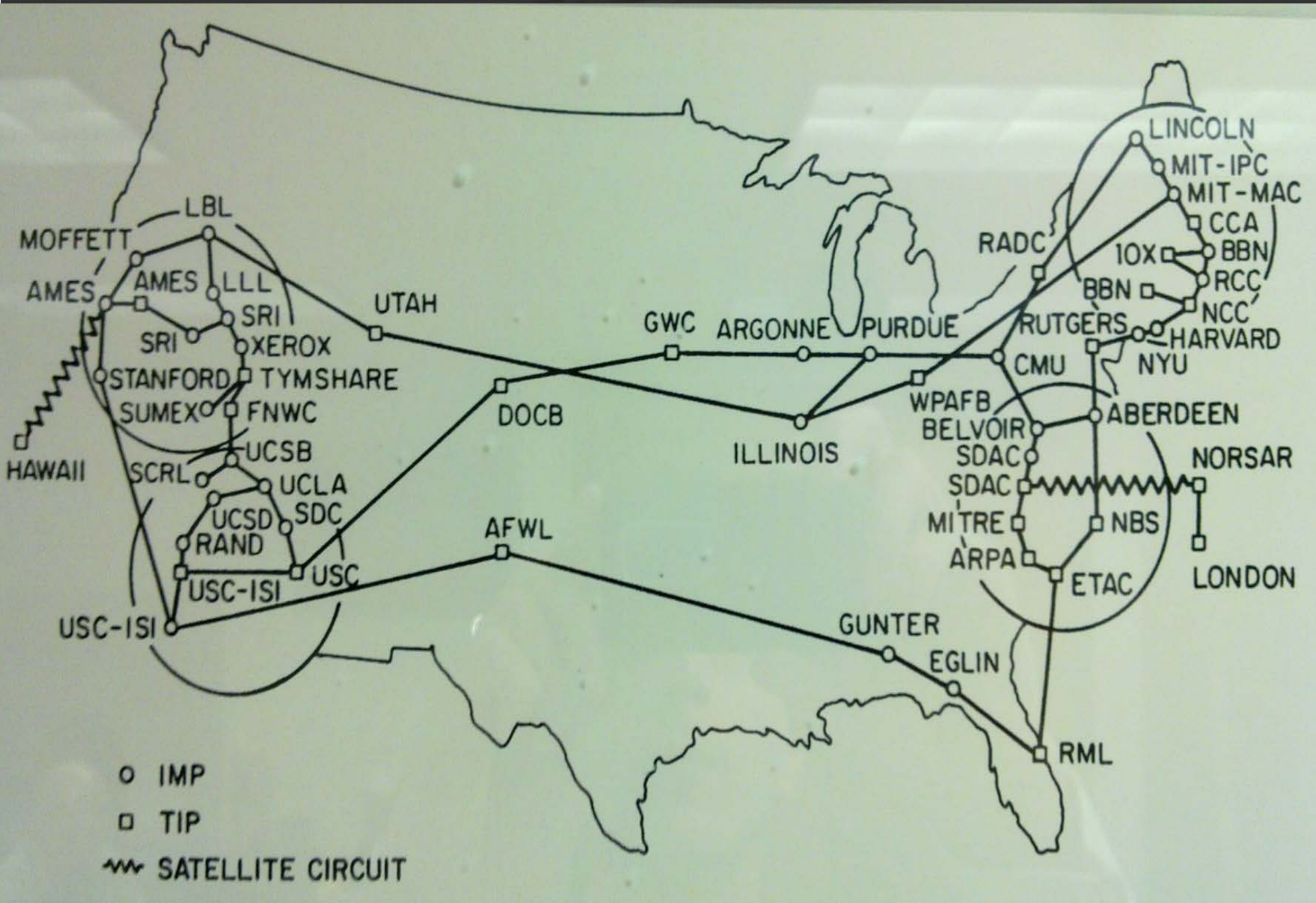


THE ARPA NETWORK

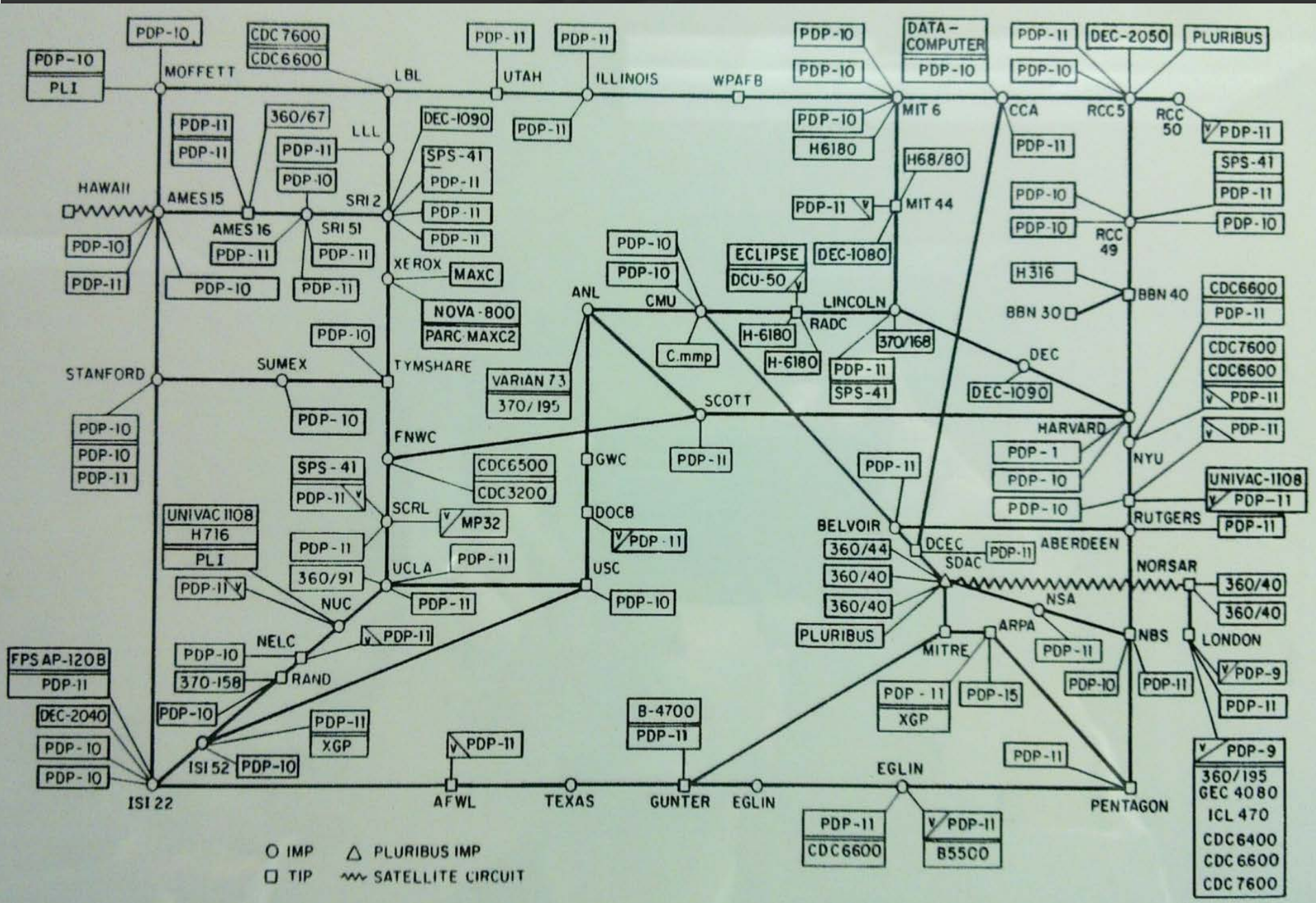
DEC 1969

4 NODES

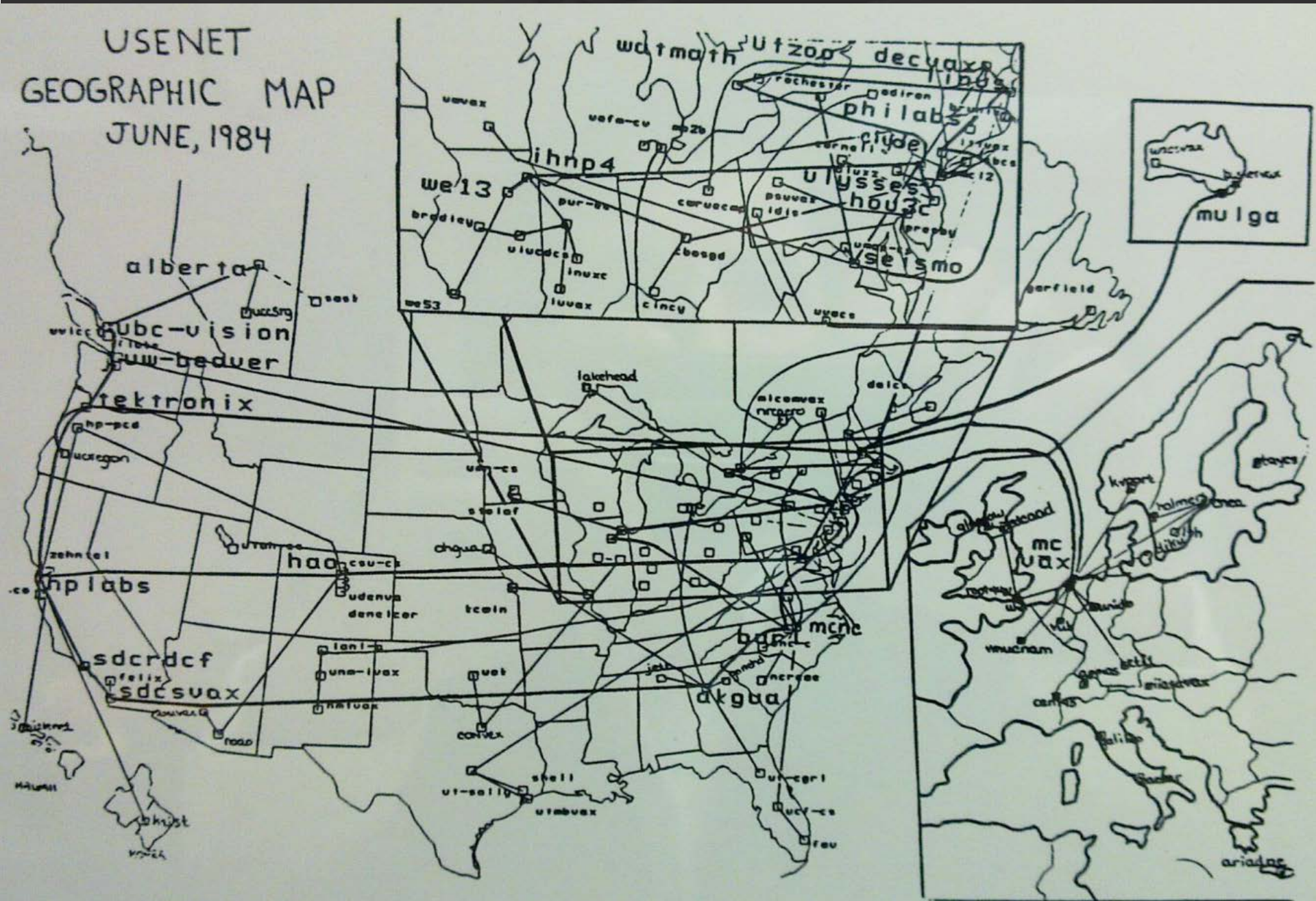
June 1975 ARPA network



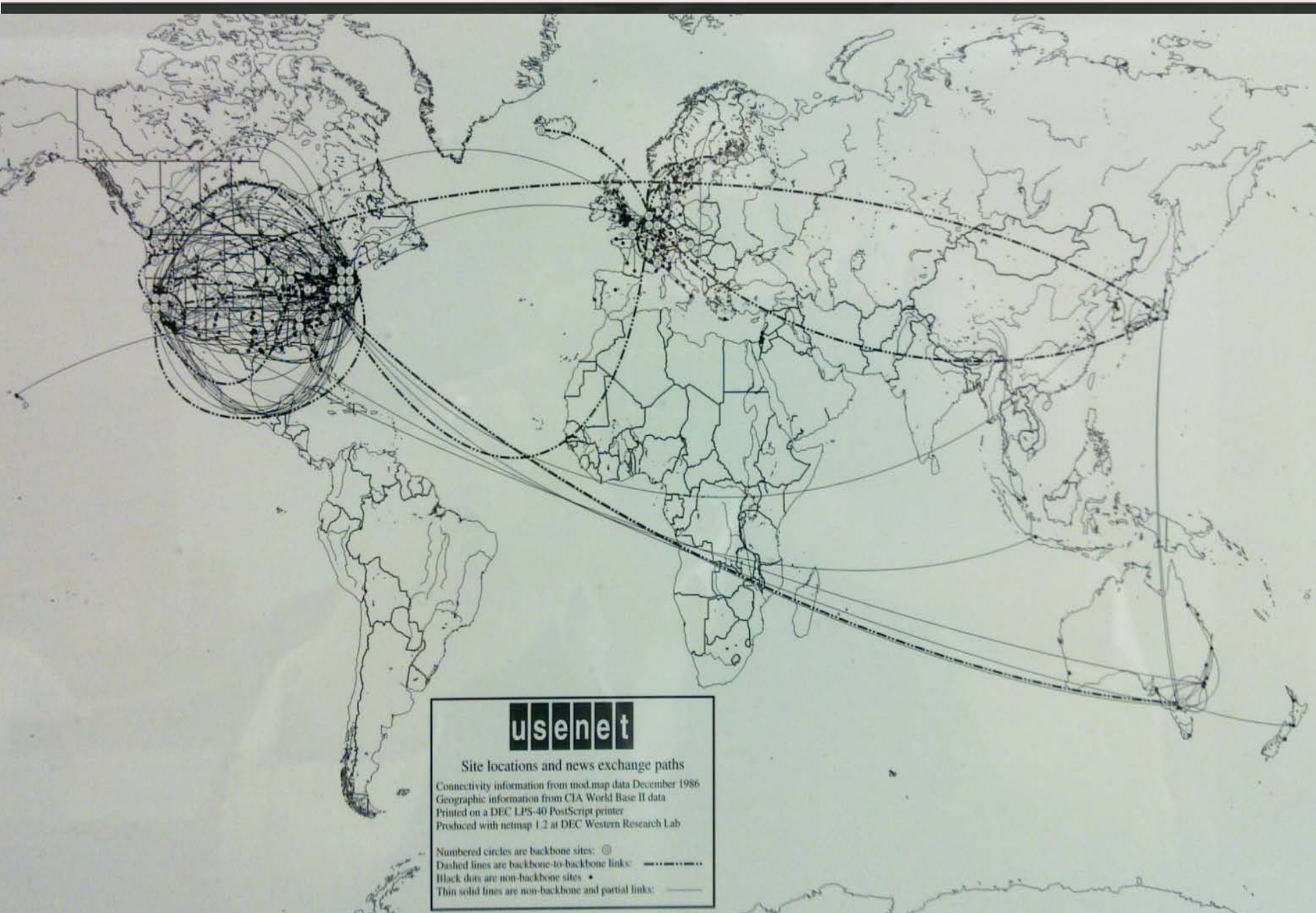
1977 March Logical diagram of ARPANET by BBN



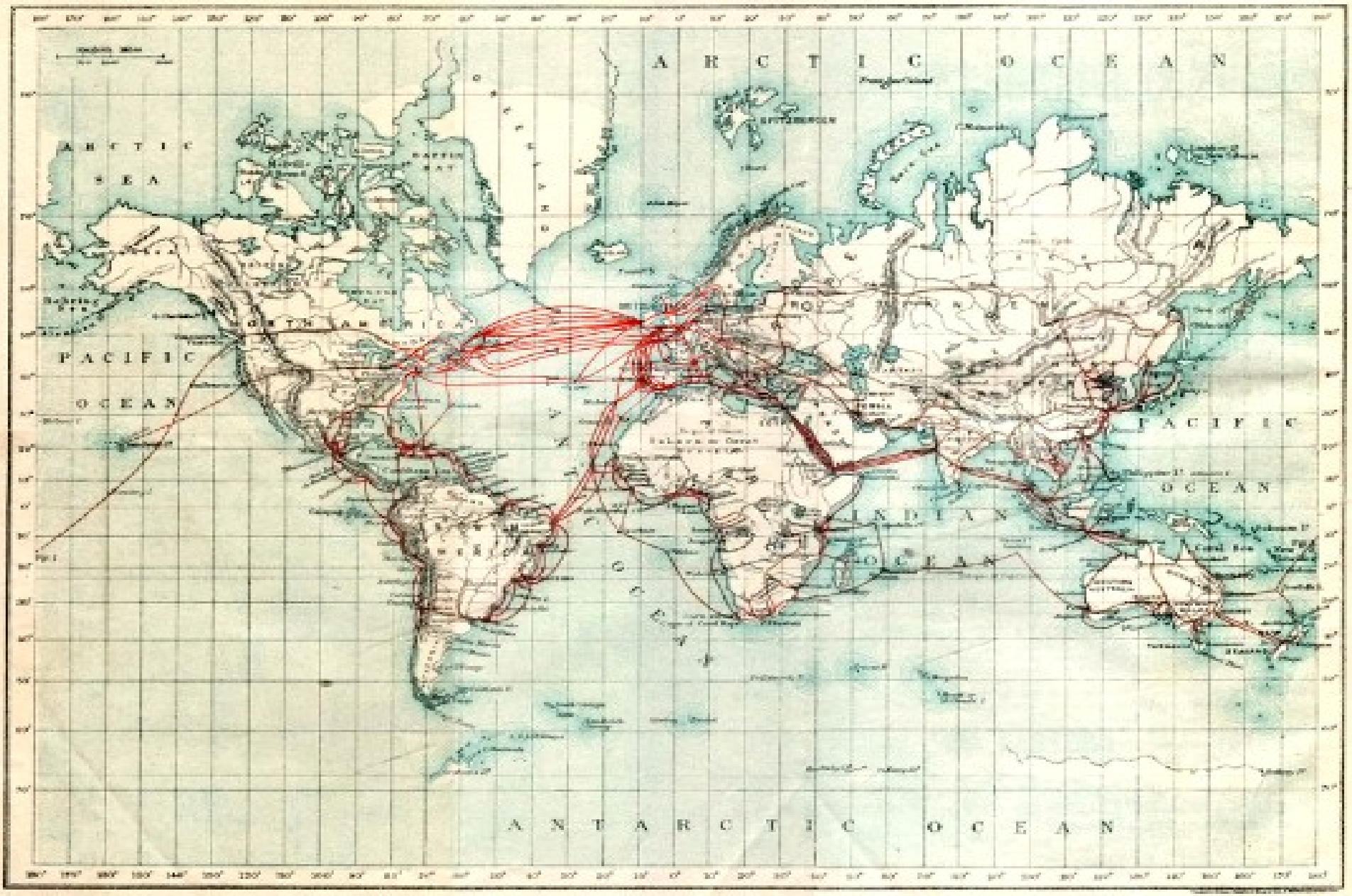
June 1984 USENET map

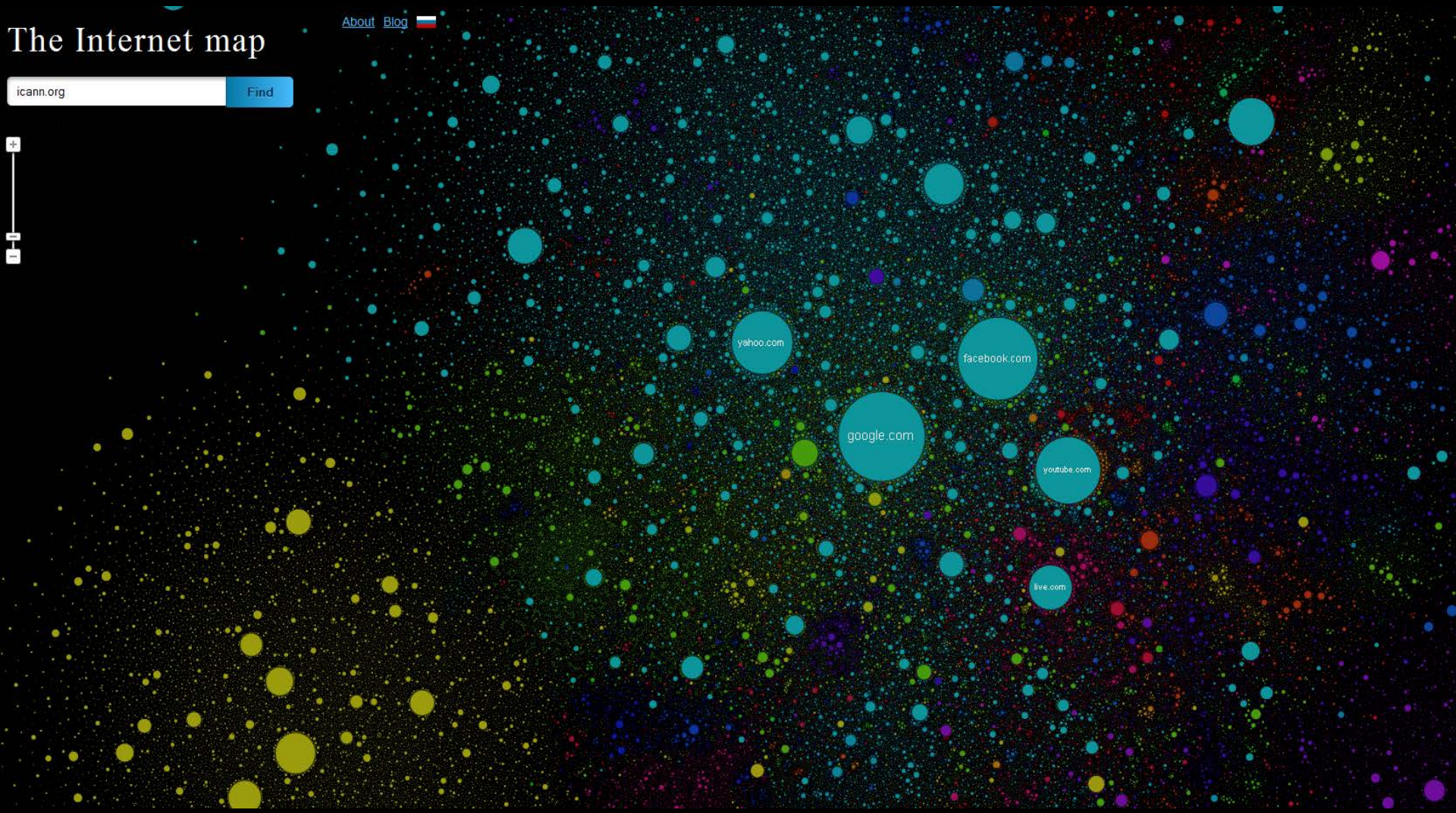


1977 MARCH Logical diagram of ARPANET by BBN



2007 Country interconnect map


EASTERN TELEGRAPH Cº's SYSTEM AND ITS GENERAL CONNECTIONS.
ARCTIC OCEAN
ARCTIC SEA
PACIFIC OCEAN
PACIFIC OCEAN
INDIAN OCEAN
ANTARCTIC OCEAN


The Internet map
About
Blog
icann.org
Find
yahoo.com
facebook.com
google.com
youtube.com
live.com


Specialization
Is
the
key to progress

When investing:

Specialize for larger risk / returns

When investing:

Specialize for larger risk / returns

Diversify to reduce risk / returns


Specialization leads
to Complexity

The failure modes of Complex systems are impossible to predict


ZU 0666', 0, 0); DROP DATABASE TABLICE
DW 530GS
ZWOLNIJ

We now have clouds of complexity

We have *virtual* clouds of complexity

We are moving so fast that we never secured the fundamentals!

A focus on the fundaments, please!

SECURE DNS:

1997	DNSSEC	RFC #2065
1999	DNSSEC	RFC #2535
2005	DNSSEC.BIS	RFC #4035

Encrypted E-mail:

1999	SMTP-TLS	RFC #2487
2002	Service Extension for SMTP over TLS	RFC #3207

Secure Web Browsing:

1991	SSL version 3.0	Netscape
1999	The TLS Protocol	RFC #2246
2000	HTTP over TLS 1.0	RFC #2818
2006	TLS 1.1	RFC #4346
2008	TLS 1.2	RFC #5246

The year is 2013

You still can’t send email securely

You can’t have a secure mobile phone call

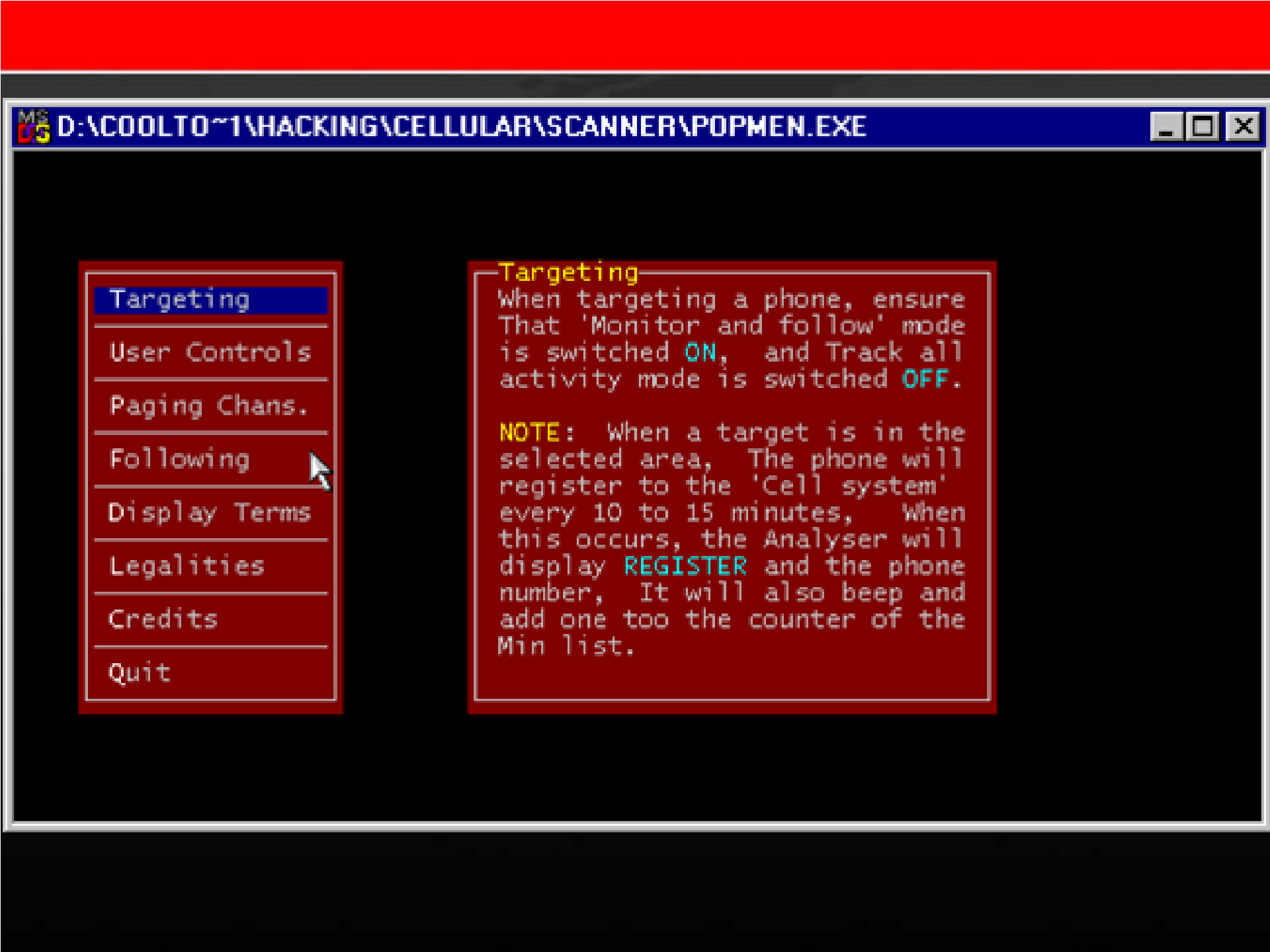
Web browsing securely is essentially impossible

Name resolution is insecure (but getting better)

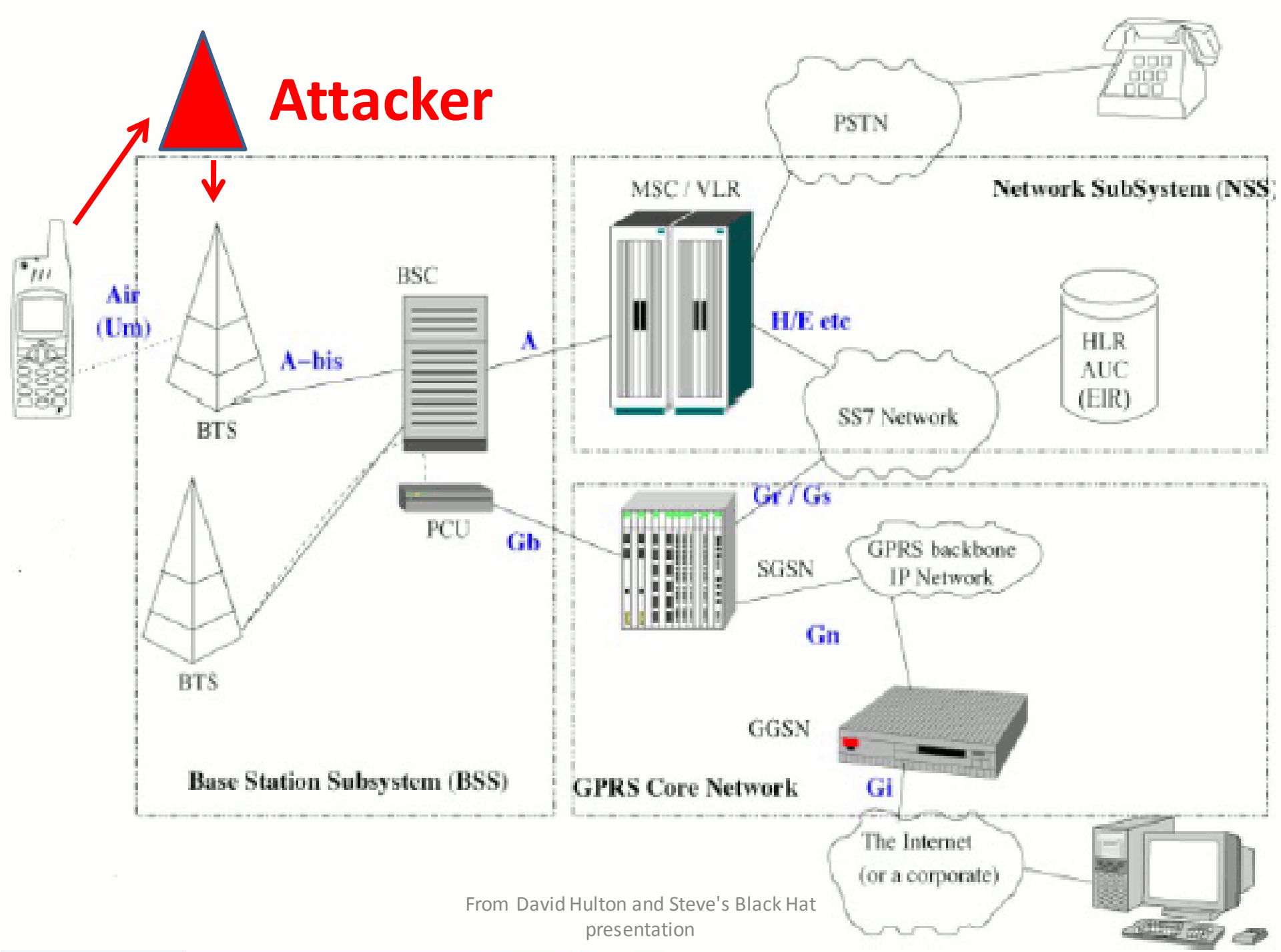
… and we are moving to “cloud” very quickly

Do you trust your cell phone?

1993


D:\COOLTO~1\HACKING\CELLULAR\SCANNER\POPMEN.EXE
Targeting
User Controls
Paging Chans.
Following
Display Terms
Legalities
Credits
Quit
Targeting
When targeting a phone, ensure That 'Monitor and follow' mode is switched ON, and Track all activity mode is switched OFF.
NOTE: When a target is in the selected area, The phone will register to the 'Cell system' every 10 to 15 minutes, When this occurs, the Analyser will display REGISTER and the phone number, It will also beep and add one too the counter of the Min list.

Then GSM came along



From David Hulton and Steve's Black Hat presentation

Digital Lifestyle > News

DEFCON: Hacker snoops on GSM mobile phones in demo

Sun, 01 Aug 2010

Intercepts mobile-phone data on the GSM networks used by AT&T and T-Mobile

Robert McMillan

Despite concerns that federal authorities might fine or arrest him, hacker Chris Paget went ahead with a live demonstration of mobile phone interception at the Defcon hacking conference Saturday.

Using several thousand dollars worth of equipment, Paget was able to intercept mobile-phone data on the GSM (Global System for Mobile Communications) networks used by AT&T and T-Mobile. He did this using a home-made system he calls an IMSI (International Mobile Subscriber Identity) catcher.

Within minutes of activating his IMSI catcher in test mode, Paget had 30 phones connected to the system. Then, with a few keystrokes, he quickly configured the device to spoof an AT&T cell tower.

"As far as your cell phones are concerned I am now indistinguishable from AT&T," he said. He predicted that every AT&T device in the room would connect to his tower, within the next half hour.

Mobile phone interception is illegal in the U.S. And while the U.S. Federal Communications Commission had raised questions about his talk, Paget believes that his demonstration was legal because his device was operating in the 900MHz band used by Ham radio devices. Coincidentally, that 900MHz band is used by GSM devices in Europe "As far as your cell pones are concerned I am a European radio transmitter."

I wonder what the state of the art is for criminals?

1. Nation States want SECRETS

1. Nation States want SECRETS
2. Organized Criminals want MONEY

1. Nation States want SECRETS
2. Organized Criminals want MONEY
3. Protesters want ATTENTION

1. Nation States want SECRETS
2. Organized Criminals want MONEY
3. Protesters want ATTENTION
4. Hackers & researchers want KNOWLEDGE

1. Nation States want SECRETS
2. Organized Criminals want MONEY
3. Protesters want ATTENTION
4. Hackers & researchers want KNOWLEDGE

Hackers & Researchers point the way!

- Discover new classes of vulnerabilities
- Expose poor product security
- Spur public debate

Hackers & Researchers point the way!

- Discover new classes of vulnerabilities
- Expose poor product security
- Spur public debate

Criminals and Governments don't do this

All these groups need the net to work

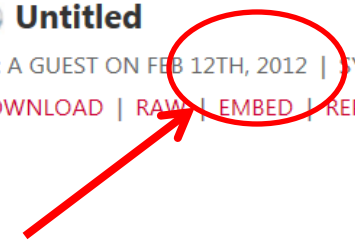
Q: Is there a group that doesn’t?


?
ANONYMOUS

Untitled

BY: A GUEST ON FEB 12TH, 2012 | SYNTAX: NONE | SIZE: 5.86 KB | HITS: 193,937 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE



```
1.  ----------------------------------------------------------------------
2.  01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
3.  01101110  01000111 01101100 01101111 01100010 01100001 01101100
4.  01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
5.  ----------------------------------------------------------------------
6.    ___                    _   _             ___ _     _         _
7.   / _ \ _ __  ___ _ _ __ _| |_(_)___ _ _    / __| |___| |__  __ _| |
8.  | (_) | '_ \/ -_) '_/ _` |  _| / _ \ ' \  | (_ | / _ \ '_ \/ _` | |
9.   \___/| .__/\___|_| \__,_|\__|_\___/_||_|  \___|_\___/_.__/\__,_|_|
10.       |_|
11.   ___ _         _            _
12.  | _ ) |__ _ __| |_____ _  _| |_
13.  | _ \ / _` / _| / / _ \ || |  _|
14.  |___/_\__,_\__|_\_\___/\_,_|\__|
15.
16. ----------------------------------------------------------------------
17. 01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
```

ICANN BYLAWS

ARTICLE I: MISSION AND CORE VALUES

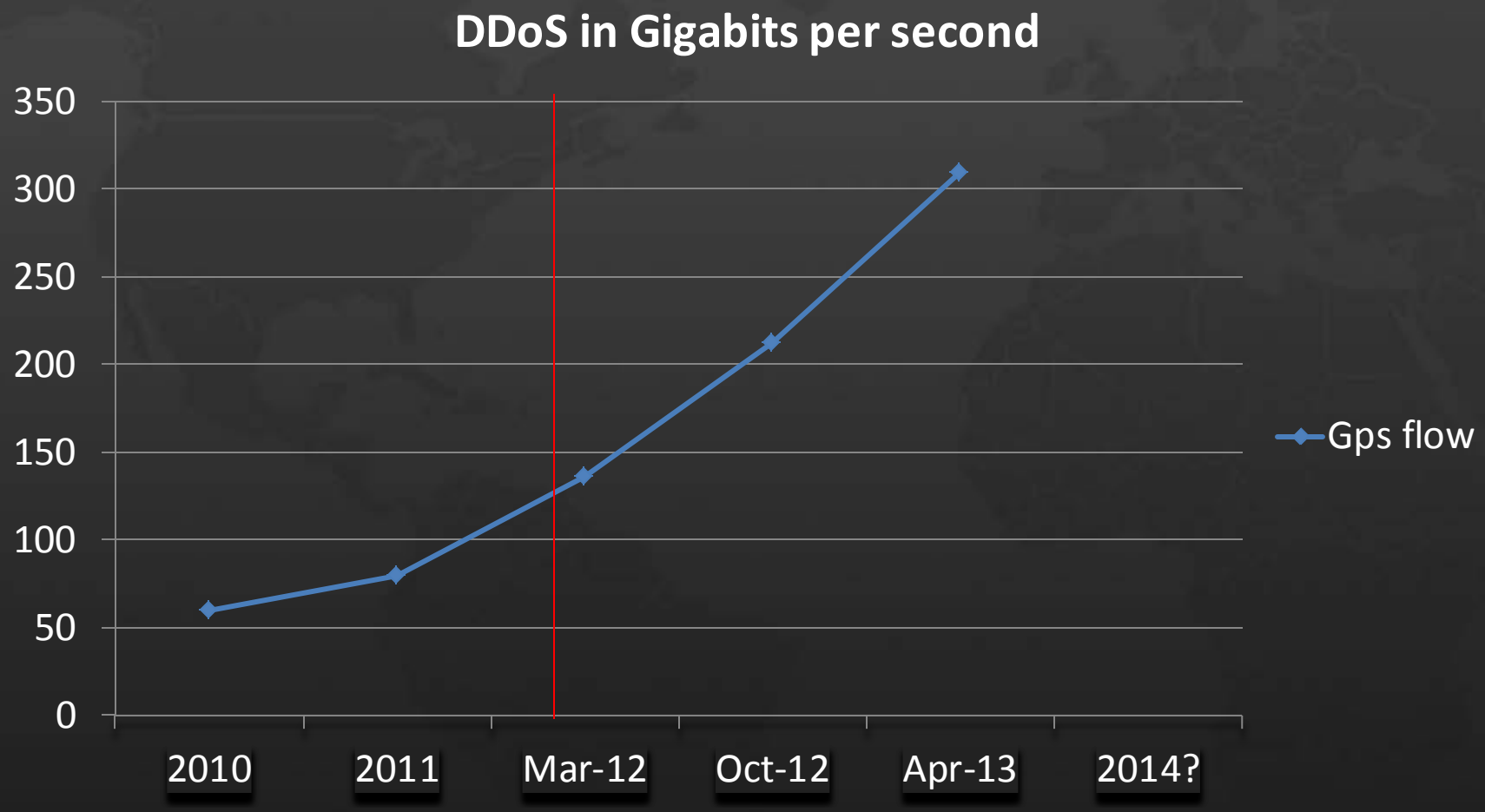
The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, ***and in particular to ensure the stable and secure operation of the Internet's unique identifier systems***…

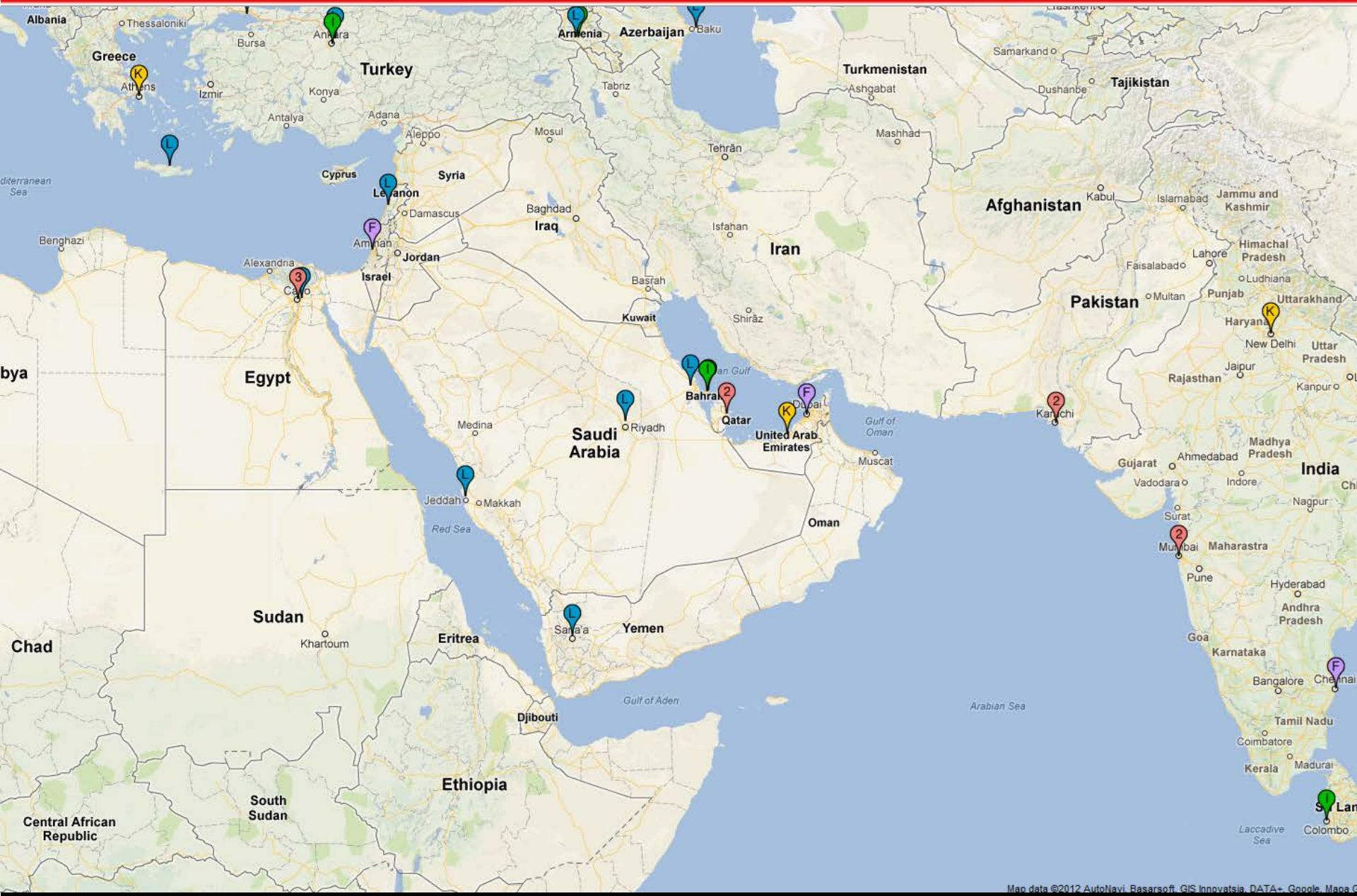
There are 13 root servers

What if a server, or three, fail?

Who knows?

Denial of service is increasing





http://www.root-servers.org/map/

“Get me the internet!”

WHO RUNS THE INTERNET?

NO ONE PERSON, COMPANY, ORGANIZATION OR GOVERNMENT RUNS THE INTERNET.

The Internet itself is a globally distributed computer network comprised of many voluntarily interconnected autonomous networks. Similarly, its governance is conducted by a decentralized and international multi-stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities, and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good.

WHO IS INVOLVED:

IAB A C P S R
INTERNET ARCHITECTURE BOARD
Oversees the technical and engineering development of the IETF and IRTF.
www.iab.org

ICANN C O P V
INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
Coordinates the Internet's systems of unique identifiers: IP addresses, protocol parameter registries, top-level domain space (DNS root zone).
www.icann.org

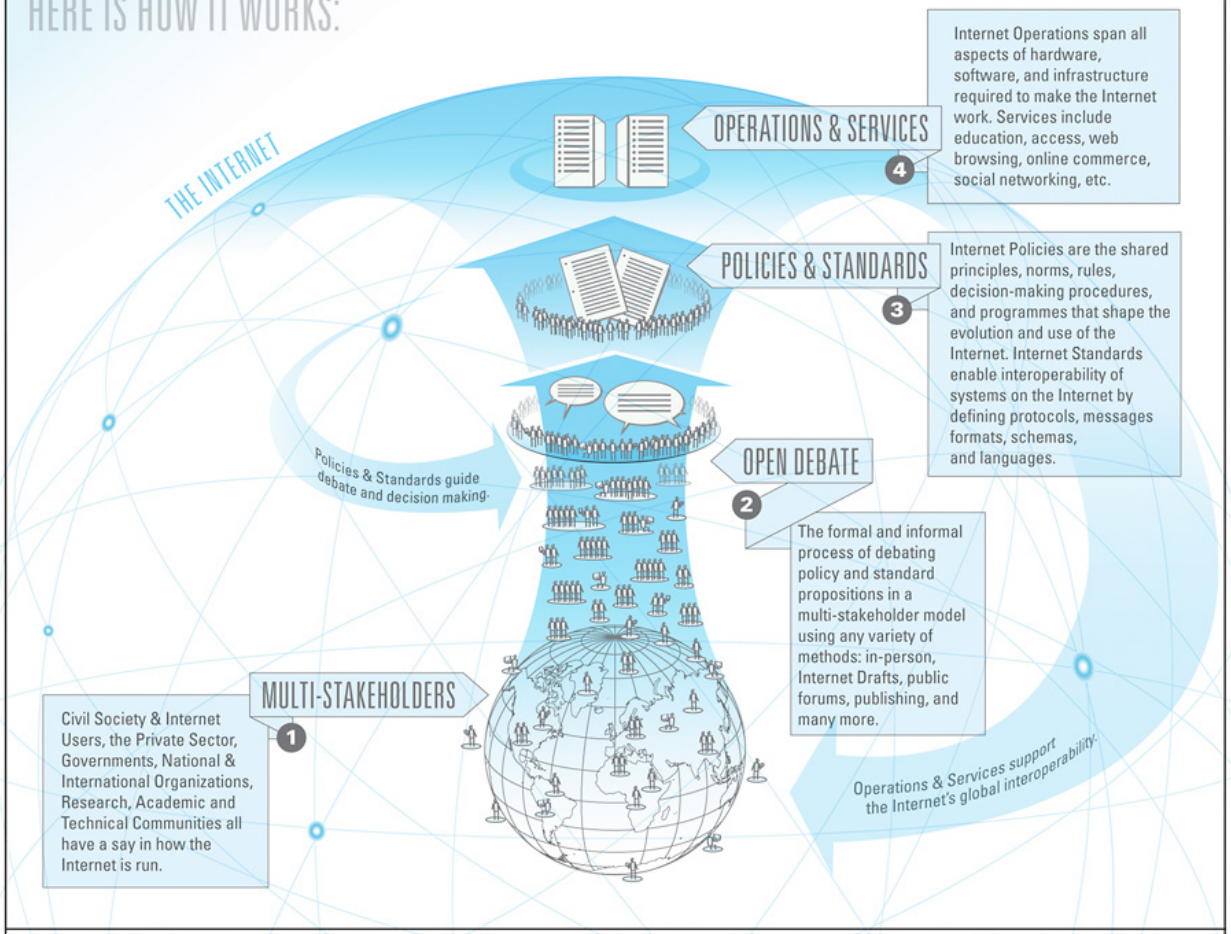
IETF C P S
INTERNET ENGINEERING TASK FORCE
Develops and promotes a wide range of Internet standards dealing in particular with standards of the Internet protocol suite. Their technical documents influence the way people design, use, and manage the Internet.
www.ietf.org

IGF A C P
INTERNET GOVERNANCE FORUM
A multi-stakeholder open forum for debate on issues related to Internet governance.
www.intgovforum.org

IRTF R
INTERNET RESEARCH TASK FORCE
Promotes research of the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.
www.irtf.org

GOVERNMENTS AND INTER-GOVERNMENTAL ORGANIZATIONS C P
Develop laws, regulations and policies applicable to the Internet within their jurisdictions; participants in multilateral and multi-stakeholder regional and international fora on Internet governance.

HERE IS HOW IT WORKS:



LEGEND: A Advice | C Community Engagement | E Education | O Operations | P Policy | R Research | S Standards | V Services

WHO IS INVOLVED:

ISO 3166 MA S
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, MAINTENANCE AGENCY
Defines names and postal codes of countries, dependent territories, special areas of geographic significance.
www.iso.org/iso/country_codes.htm

ISOC C E P V
INTERNET SOCIETY
Assure the open development, evolution and use of the Internet for the benefit of all people throughout the world. Currently ISOC has over 90 chapters in around 80 countries.
www.internetsociety.org

RIRs O P V
5 REGIONAL INTERNET REGISTRIES
Manage the allocation and registration of Internet number resources, such as IP addresses, within geographic regions of the world.

www.afrinic.net	Africa
www.apnic.net	Asia Pacific
www.arin.net	Canada & United States
www.lacnic.net	Latin America & Caribbean
www.ripe.net	Europe, the Middle East & parts of Central Asia

W3C S
WORLD WIDE WEB CONSORTIUM
Create standards for the world wide web that enable an Open Web Platform, for example, by focusing on issues of accessibility, internationalization, and mobile web solutions.
www.w3.org

INTERNET NETWORK OPERATORS' GROUPS A O V
Discuss and influence matters related to Internet operations and regulation within informal fora made up of Internet Service Providers (ISPs), Internet Exchange Points (IXPs), and others.

This graphic is a living document, designed to provide a high level view of how the Internet is run. It is not intended to be a definitive guide. Please provide feedback at www.xplanations.com/whorunstheinternet

http://icann.xplane.com/questionaire/internet_governance

L Root - Before

L Root - Now

http://www.root-servers.org/map/?letter=L

All Roots - Now

http://www.root-servers.org/map/

The 13 Root Servers

- A = 8 VeriSign
- B = 1 U of SoCal
- C = 6 Cogent
- D = 1 U of Maryland
- E = 12 NASA Ames
- F = 49 ISC
- G = 6 US DOD NIC

H = 2 US Army Research Lab

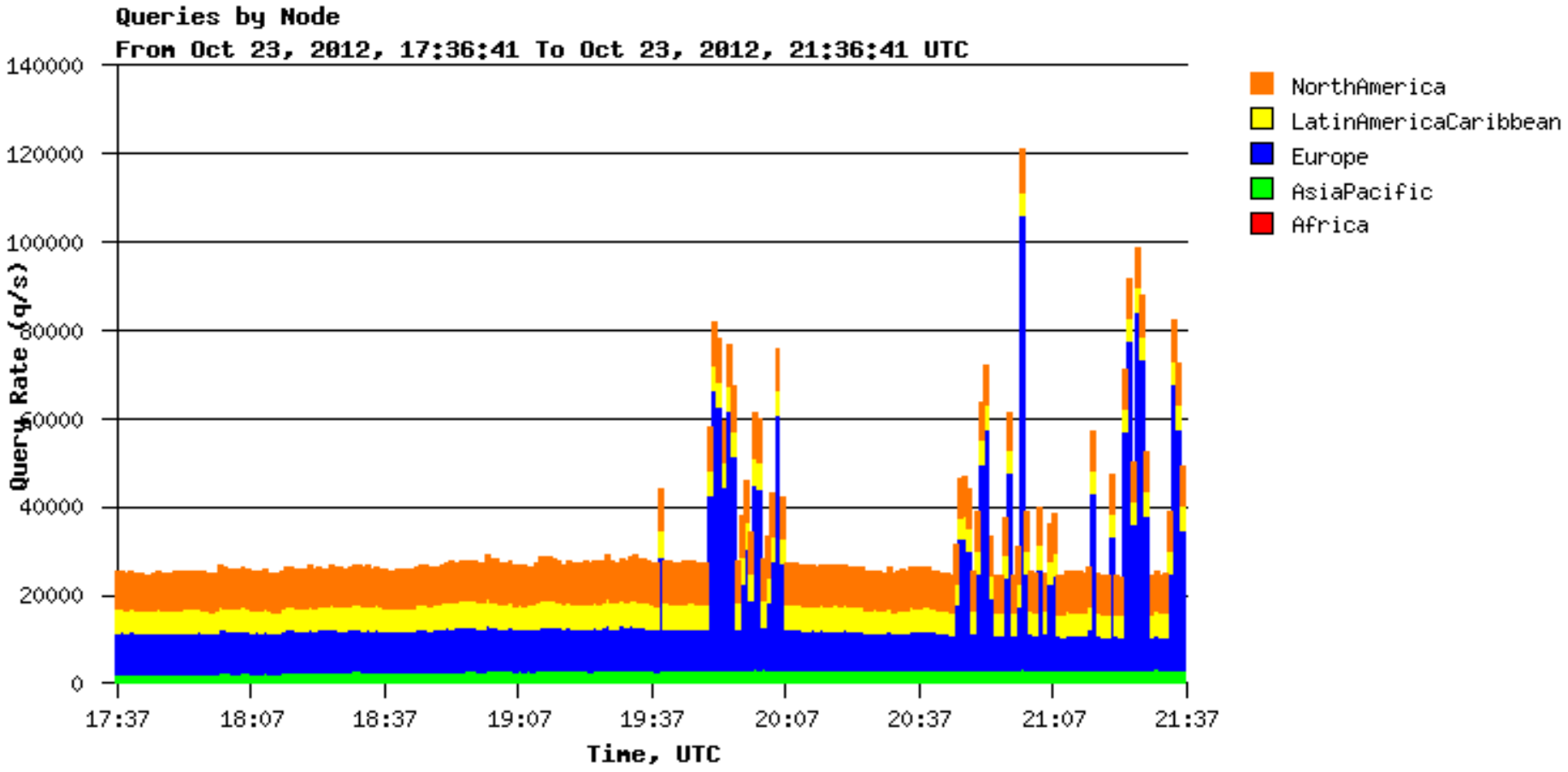
I = 43 Netnod in Sweden

J = 70 VeriSign

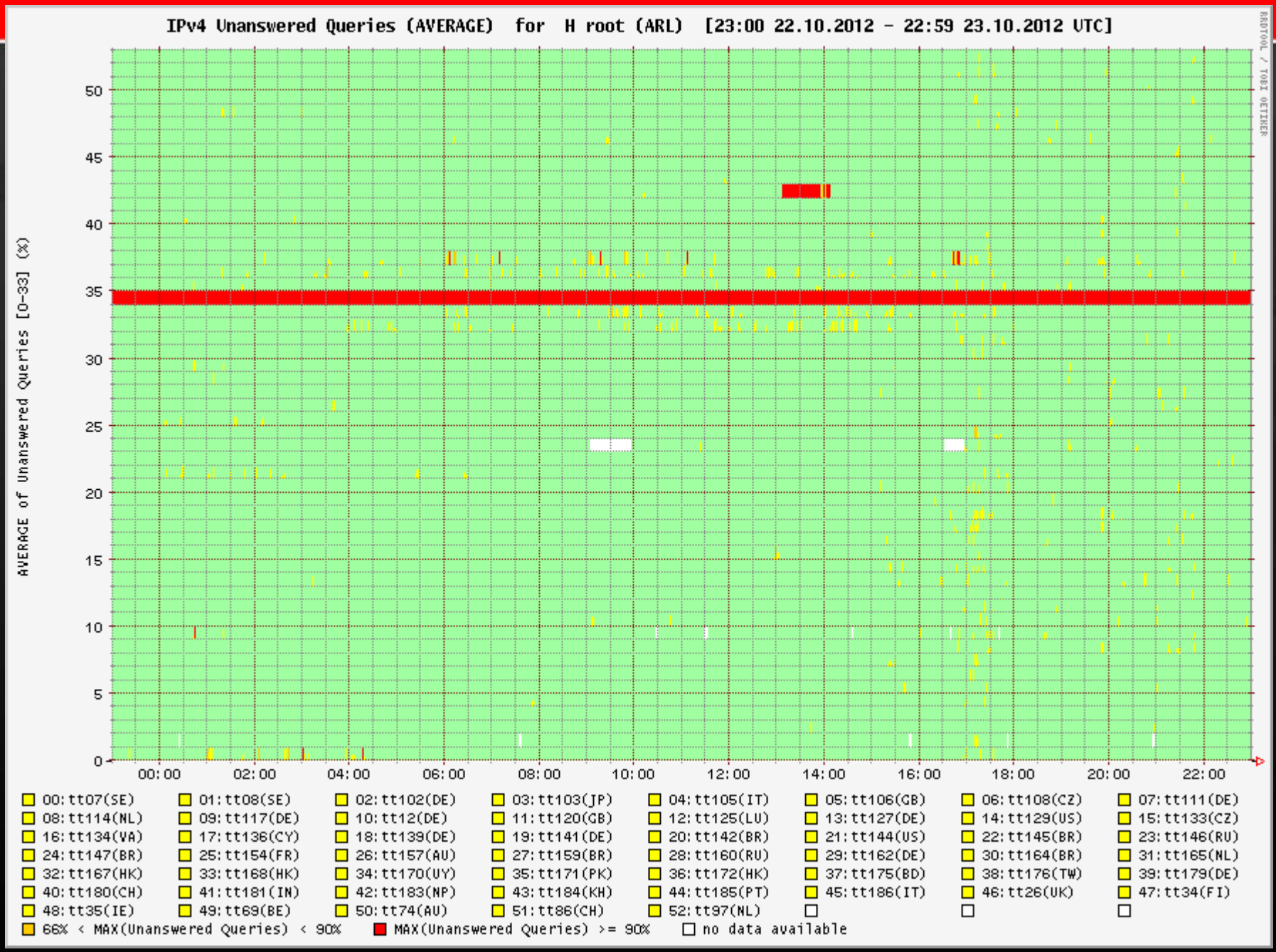
K = 17 RIPE NCC in Netherlands

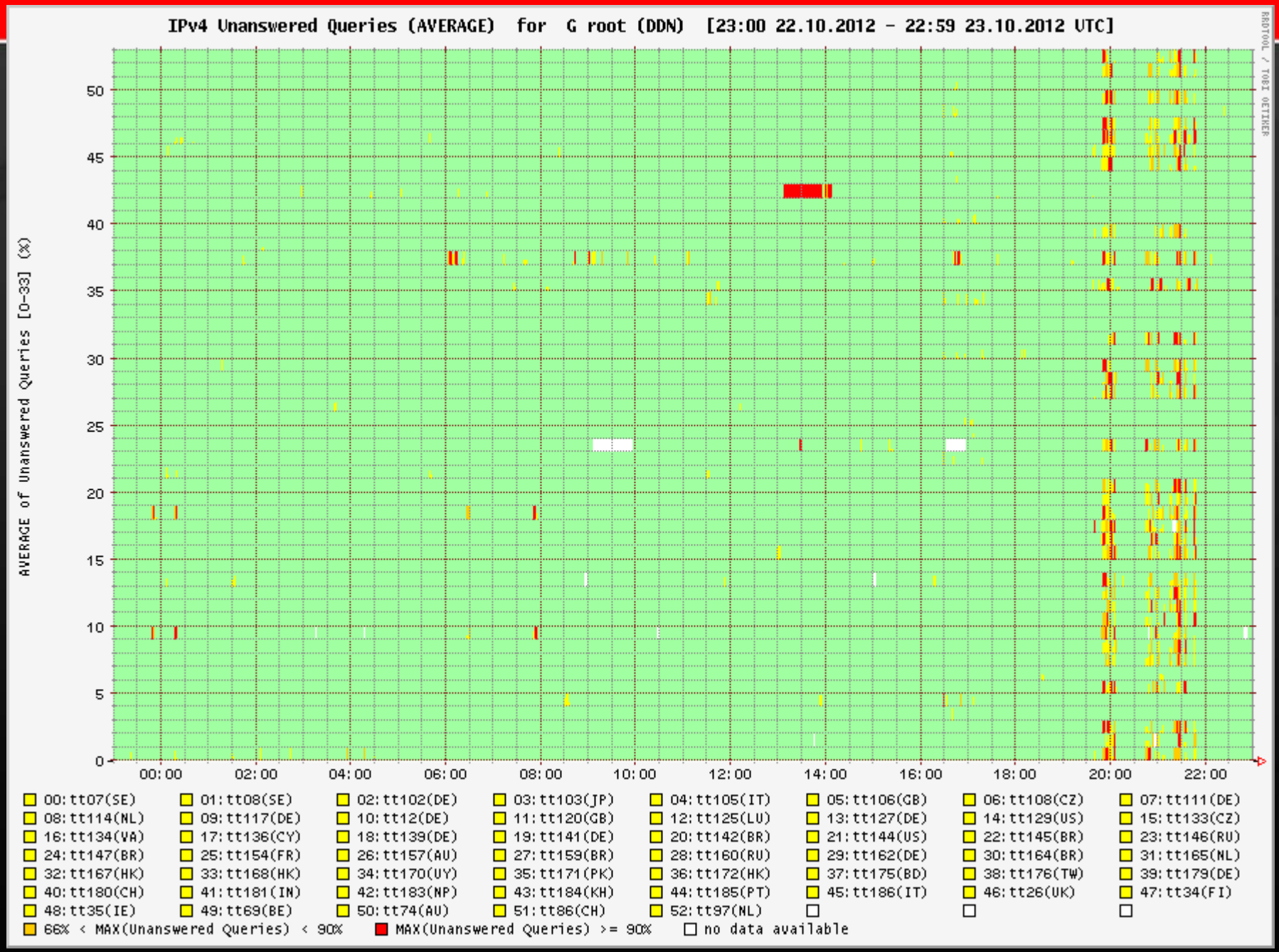
L = 143 ICANN

M = 6 WIDE in Japan



The Queries by Node plot shows the amount of queries coming from each node in the server cluster.


IPv4 Unanswered Queries (AVERAGE) for H root (ARL) [23:00 22.10.2012 - 22:59 23.10.2012 UTC]
AVERAGE of Unanswered Queries [0-33] (%)
0
5
10
15
20
25
30
35
40
45
50
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00: tt07(SE)
01: tt08(SE)
02: tt102(DE)
03: tt103(JP)
04: tt105(IT)
05: tt106(GB)
06: tt108(CZ)
07: tt111(DE)
08: tt114(NL)
09: tt117(DE)
10: tt12(DE)
11: tt120(GB)
12: tt125(LU)
13: tt127(DE)
14: tt129(US)
15: tt133(CZ)
16: tt134(VA)
17: tt136(CY)
18: tt139(DE)
19: tt141(DE)
20: tt142(BR)
21: tt144(US)
22: tt145(BR)
23: tt146(RU)
24: tt147(BR)
25: tt154(FR)
26: tt157(AU)
27: tt159(BR)
28: tt160(RU)
29: tt162(DE)
30: tt164(BR)
31: tt165(NL)
32: tt167(HK)
33: tt168(HK)
34: tt170(UY)
35: tt171(PK)
36: tt172(HK)
37: tt175(BD)
38: tt176(TW)
39: tt179(DE)
40: tt180(CH)
41: tt181(IN)
42: tt183(NP)
43: tt184(KH)
44: tt185(PT)
45: tt186(IT)
46: tt26(UK)
47: tt34(FI)
48: tt35(IE)
49: tt69(BE)
50: tt74(AU)
51: tt86(CH)
52: tt97(NL)
66% < MAX(Unanswered Queries) < 90%
MAX(Unanswered Queries) >= 90%
no data available


IPv4 Unanswered Queries (AVERAGE) for G root (DDN) [23:00 22.10.2012 - 22:59 23.10.2012 UTC]
AVERAGE of Unanswered Queries [0-33] (%)
0
5
10
15
20
25
30
35
40
45
50
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:tt07(SE)
01:tt08(SE)
02:tt102(DE)
03:tt103(JP)
04:tt105(IT)
05:tt106(GB)
06:tt108(CZ)
07:tt111(DE)
08:tt114(NL)
09:tt117(DE)
10:tt12(DE)
11:tt120(GB)
12:tt125(LU)
13:tt127(DE)
14:tt129(US)
15:tt133(CZ)
16:tt134(VA)
17:tt136(CY)
18:tt139(DE)
19:tt141(DE)
20:tt142(BR)
21:tt144(US)
22:tt145(BR)
23:tt146(RU)
24:tt147(BR)
25:tt154(FR)
26:tt157(AU)
27:tt159(BR)
28:tt160(RU)
29:tt162(DE)
30:tt164(BR)
31:tt165(NL)
32:tt167(HK)
33:tt168(HK)
34:tt170(UY)
35:tt171(PK)
36:tt172(HK)
37:tt175(BD)
38:tt176(TW)
39:tt179(DE)
40:tt180(CH)
41:tt181(IN)
42:tt183(NP)
43:tt184(KH)
44:tt185(PT)
45:tt186(IT)
46:tt26(UK)
47:tt34(FI)
48:tt35(IE)
49:tt69(BE)
50:tt74(AU)
51:tt86(CH)
52:tt97(NL)
66% < MAX(Unanswered Queries) < 90%
MAX(Unanswered Queries) >= 90%
no data available
RRDTOOL / TOBI OETIKER

What makes these attacks possible?

What makes these attacks possible?

Bot Nets + Open Recursive DNS Servers

RISK ASSESSMENT / SECURITY & HACKTIVISM

Meet the network operators helping to fuel the spike in big DDoS attacks

SoftLayer, GoDaddy, AT&T, and iWeb make a list of top 10 most abused networks.

by Dan Goodin - Oct 31, 2012 7:43 pm UTC

INTERNET CRIME 44

# of Open Resolvers	AS Number	Network Name
3359	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited
2992	3462	HINET Data Communication Business Group
1431	9394	CRNET CHINA RAILWAY Internet(CRNET)
1403	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.
1323	4134	CHINANET-BACKBONE No.31, Jin-rong Street
1120	36351	SOFTLAYER - SoftLayer Technologies Inc.
1112	4713	OCN NTT Communications Corporation
1039	26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC
980	7018	ATT-INTERNET4 - AT&T Services, Inc.
852	32613	IWEB-AS - iWeb Technologies Inc.

Enlarge / A list of the the 10 network operators with the highest number of open DNS resolvers, as measured by CloudFlare. Over the past three weeks, third-party attackers have been abusing them around the clock in an attempt to knock a website offline.

CloudFlare

A company that helps secure websites has compiled a list of some of the Internet's biggest network nuisances—operators that run open servers that can be abused to significantly aggravate the crippling effects of distributed denial-of-service attacks on innocent bystanders.

http://arstechnica.com/security/2012/10/meet-the-network-operators-helping-fuel-the-spike-in-big-ddos-attacks/

DNS SURVEY: OPEN RESOLVERS

ABOUT

We have an ongoing survey that looks for open DNS resolvers. A DNS resolver is *open* if it provides recursive name resolution for clients outside of its administrative domain. Open DNS resolvers are a bad idea for a few reasons:

- They allow outsiders to consume resources that do not belong to them.
- Attackers may be able to poison the cache of an open resolver.
- Open resolvers are being used in widespread DDoS attacks with spoofed source addresses and large DNS reply messages.

As with open SMTP relays, open DNS resolvers are now being abused by miscreants to further pollute the Internet.

http://dns.measurement-factory.com/surveys/openresolvers.html

This table shows the number of known open resolvers for each autonomous system as of Sun Mar 24 06:00:01 UTC 2013.

count	asn	name
3199	8167	TELESC - Telecomunicacoes de Santa Catarina SA
2088	4713	-Allocated by APNIC-
1961	3462	HINET Data Communication Business Group
1917	7418	Terra Networks Chile S.A.
1673	4766	KIXS-AS-KR Korea Telecom
1439	21844	THEPLANET-AS - THE PLANET
1043	1659	ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information C
1004	2516	JPNIC-ASBLOCK-AP JPNIC
903	17974	TELKOMNET-AS2-AP PT TELEKOMUNIKASI INDONESIA
864	10834	Telefonica Data Argentina S.A.
786	4134	CHINANET-BACKBONE No.31,Jin-rong Street
763	36692	OPENDNS - Freedom Networks LLC
732	16276	OVH OVH
716	2514	JPNIC-ASBLOCK-AP JPNIC
701	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.
700	3786	LGDACOM LG DACOM Corporation
698	9318	HANARO-AS Hanaro Telecom Inc.
652	14992	CRYSTALTECH - CrystalTech Web Hosting Inc.
633	209	ASN-QWEST - Qwest
626	23352	SERVERCENTRAL - Server Central Network
613	15418	FASTHOSTS-INTERNET Fasthosts Internet Ltd. Gloucester, UK.
607	5617	TPNET Polish Telecom_s commercial IP network
605	3320	DTAG Deutsche Telekom AG
591	23966	DANCOM-AS-AP Dancom Online Services
565	4323	TWTC - Time Warner Telecom, Inc.
552	17813	MTNL-AP Mahanagar Telephone Nigam Ltd.
509	4538	ERX-CERNET-BKB China Education and Research Network Center
499	701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Busi
494	18403	FPT-AS-AP The Corporation for Financing & Promoting Technolo
493	9121	TTNET TTnet Autonomous System
492	25847	SERVINT - ServInt Corporation
490	25653	FORTRESSITX - FortressITX
488	36351	SOFTLAYER - SoftLayer Technologies Inc.
484	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited
471	4230	Embratel

http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html

This table shows the number of known open resolvers for each autonomous system as of Sun Mar 24 06:00:01 UTC 2013.

count	asn	name	
3199	8167	TELESC - Telecomunicacoes de Santa Catarina SA	Brazil
2088	4713	-Allocated by APNIC-	Asia Pacific Region
1961	3462	HINET Data Communication Business Group	Taiwan
1917	7418	Terra Networks Chile S.A.	Chile
1673	4766	KIXS-AS-KR Korea Telecom	Korea
1439	21844	THEPLANET-AS - THE PLANET	Soft Layer – Texas USA
1043	1659	ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information C	Taiwan
1004	2516	JPNIC-ASBLOCK-AP JPNIC	Japan
903	17974	TELKOMNET-AS2-AP PT TELEKOMUNIKASI INDONESIA	Indonesia
864	10834	Telefonica Data Argentina S.A.	Argentina
786	4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
763	36692	OPENDNS - Freedom Networks LLC	
732	16276	OVH OVH	
716	2514	JPNIC-ASBLOCK-AP JPNIC	
701	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	
700	3786	LGDACOM LG DACOM Corporation	
698	9318	HANARO-AS Hanaro Telecom Inc.	
652	14992	CRYSTALTECH - CrystalTech Web Hosting Inc.	
633	209	ASN-QWEST - Qwest	
626	23352	SERVERCENTRAL - Server Central Network	
613	15418	FASTHOSTS-INTERNET Fasthosts Internet Ltd. Gloucester, UK.	
607	5617	TPNET Polish Telecom_s commercial IP network	
605	3320	DTAG Deutsche Telekom AG	
591	23966	DANCOM-AS-AP Dancom Online Services	
565	4323	TWTC - Time Warner Telecom, Inc.	
552	17813	MTNL-AP Mahanagar Telephone Nigam Ltd.	
509	4538	ERX-CERNET-BKB China Education and Research Network Center	
499	701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Busi	
494	18403	FPT-AS-AP The Corporation for Financing & Promoting Technolo	
493	9121	TTNET TTnet Autonomous System	
492	25847	SERVINT - ServInt Corporation	
490	25653	FORTRESSITX - FortressITX	
488	36351	SOFTLAYER - SoftLayer Technologies Inc.	
484	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	
471	4230	Embratel	

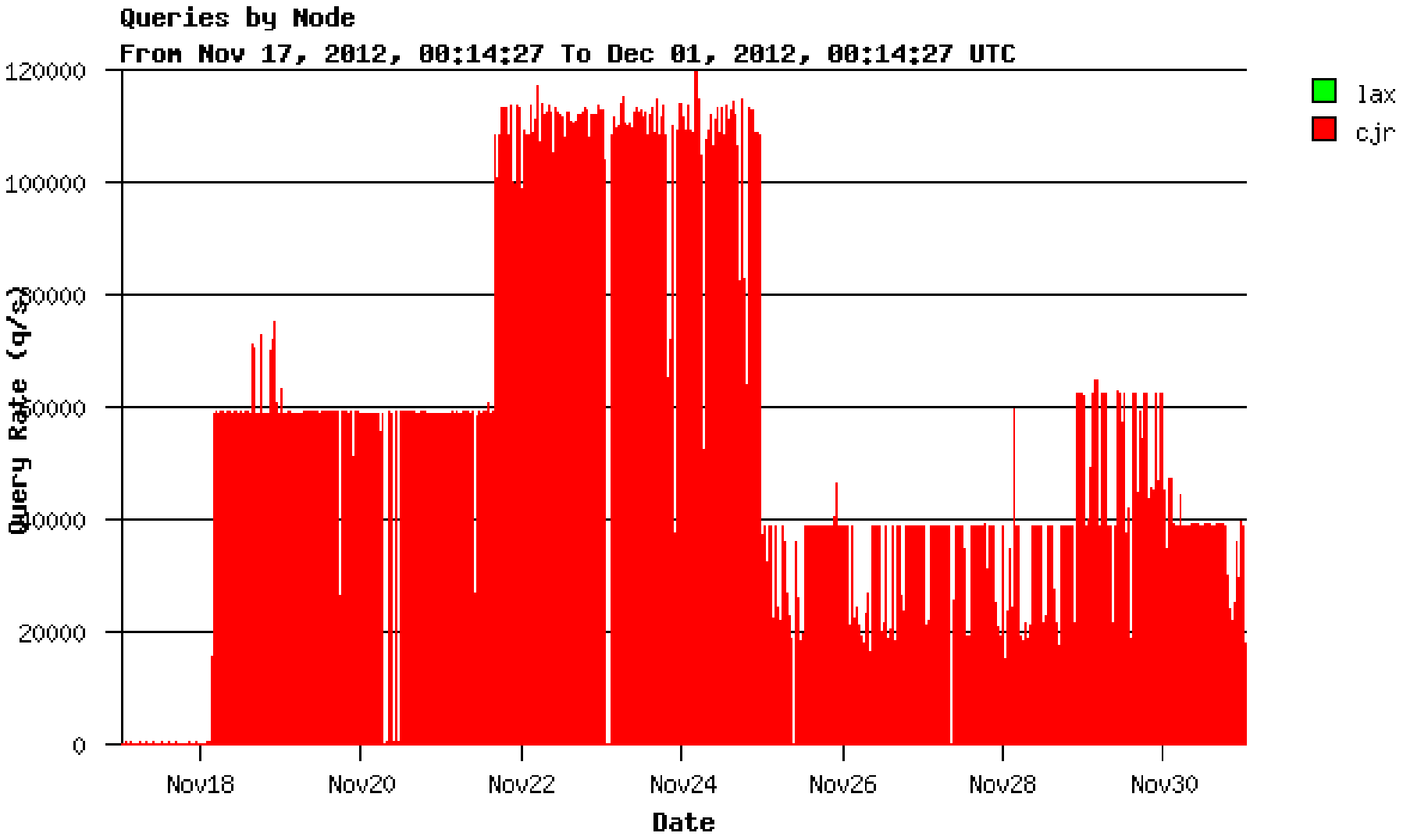
http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html

This table shows the number of known open resolvers for each autonomous system as of Sun Mar 24 06:00:01 UTC 2013.

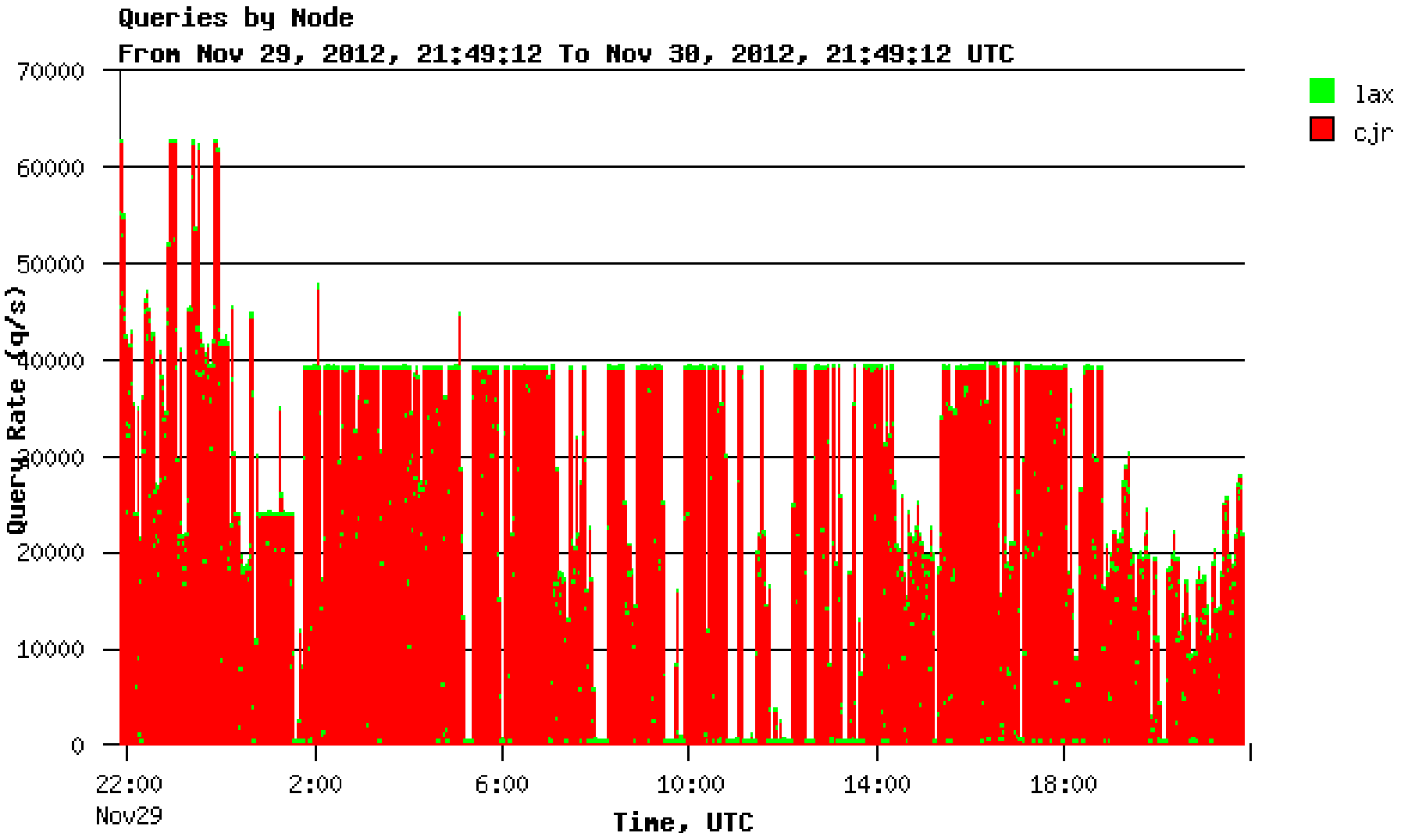
	count	asn	name	
	3199	8167	TELESC - Telecomunicacoes de Santa Catarina SA	Brazil
+976	2088	4713	-Allocated by APNIC-	Asia Pacific Region
-1,031	1961	3462	HINET Data Communication Business Group	Taiwan
	1917	7418	Terra Networks Chile S.A.	Chile
	1673	4766	KIXS-AS-KR Korea Telecom	Korea
+36	1439	21844	THEPLANET-AS - THE PLANET	Soft Layer – Texas USA
	1043	1659	ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information C	Taiwan
	1004	2516	JPNIC-ASBLOCK-AP JPNIC	Japan
	903	17974	TELKOMNET-AS2-AP PT TELEKOMUNIKASI INDONESIA	Indonesia
	864	10834	Telefonica Data Argentina S.A.	Argentina
-653	786	4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
	763	36692	OPENDNS - Freedom Networks LLC	
	732	16276	OVH OVH	
	716	2514	JPNIC-ASBLOCK-AP JPNIC	
	701	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	
	700	3786	LGDACOM LG DACOM Corporation	
	698	9318	HANARO-AS Hanaro Telecom Inc.	
	652	14992	CRYSTALTECH - CrystalTech Web Hosting Inc.	
	633	209	ASN-QWEST - Qwest	
	626	23352	SERVERCENTRAL - Server Central Network	
	613	15418	FASTHOSTS-INTERNET Fasthosts Internet Ltd. Gloucester, UK.	
	607	5617	TPNET Polish Telecom_s commercial IP network	
	605	3320	DTAG Deutsche Telekom AG	
	591	23966	DANCOM-AS-AP Dancom Online Services	
	565	4323	TWTC - Time Warner Telecom, Inc.	
	552	17813	MTNL-AP Mahanagar Telephone Nigam Ltd.	
	509	4538	ERX-CERNET-BKB China Education and Research Network Center	
	499	701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Busi	
	494	18403	FPT-AS-AP The Corporation for Financing & Promoting Technolo	
	493	9121	TTNET TTnet Autonomous System	
-2,875 !!	492	25847	SERVINT - ServInt Corporation	
	490	25653	FORTRESSITX - FortressITX	
-632	488	36351	SOFTLAYER - SoftLayer Technologies Inc.	
	484	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	
	471	4230	Embratel	

http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html

Supply side..


Queries by Node
From Nov 17, 2012, 00:14:27 To Dec 01, 2012, 00:14:27 UTC
120000
100000
80000
60000
40000
20000
0
Query Rate (q/s)
Nov18
Nov20
Nov22
Nov24
Nov26
Nov28
Nov30
Date
lax
cjr

Supply side answer = RRL



What about tampering?

RIPE Atlas

With your help, the RIPE NCC is building the largest Internet measurement network ever made. RIPE Atlas employs a global network of probes that measure Internet connectivity and reachability, providing an unprecedented understanding of the state of the Internet in real time.

Find out how to get involved →

About RIPE Atlas

- FAQ
- Documentation
- Announcements
- Roadmap
- Future Plans
- RIPE Atlas Anchors

LEARN MORE →

Get Involved

- Host a Probe
- Become a Sponsor
- RIPE NCC Members
- Community
- Feedback

LEARN MORE →

Results

- Internet Maps
- Coverage & Statistics
- Analyses & Use Cases
- Graphs

LEARN MORE →

System Statistics

Probes connected to RIPE Atlas: 3895

Measurements currently running: 1931

Current Sponsors

AS34288 CONNECTING EDUCATION TO THE WORLD

BECOME A RIPE ATLAS SPONSOR →

On RIPE Labs

RIPE Atlas Anchors Pilot: Summary and Next Steps >
Sep 16, 2013

Further Virtualisation Testing for the RIPE Atlas Anchor >

Using RIPE Atlas: A DENIC Case Study

by Peter Koch Sep 25, 2012

OR

What has the Beijing DNS server been up to?

"218 (of 1,762) probes, marked red, either received modified or inconsistent results"

https://atlas.ripe.net/contrib/denic_study.html

https://atlas.ripe.net/

Security Today

Email	Nameserver	Web
SMTP-TLS		HTTPS
SPF Record		HSTS Header
DKIM Record		

Security Tomorrow

Email	Nameserver	Web
SMTP-TLS		HTTPS
	DNSSEC	
SPF Record		HSTS Header
DKIM Record		Host Key Pinning
SMIME_A Record		DANE TLS_A
DMARC		

Finally

Internet Update

- Now until 2016+

  DNSSEC = You can trust the answers from DNS

  DANE = Risk of rogue SSL CAs virtually eliminated

  IPv6 = IPSEC support, less NAT, future growth

- ~2015 to 2018+
  - Signed resource directory (RPKI)
  - Beware policy implications…

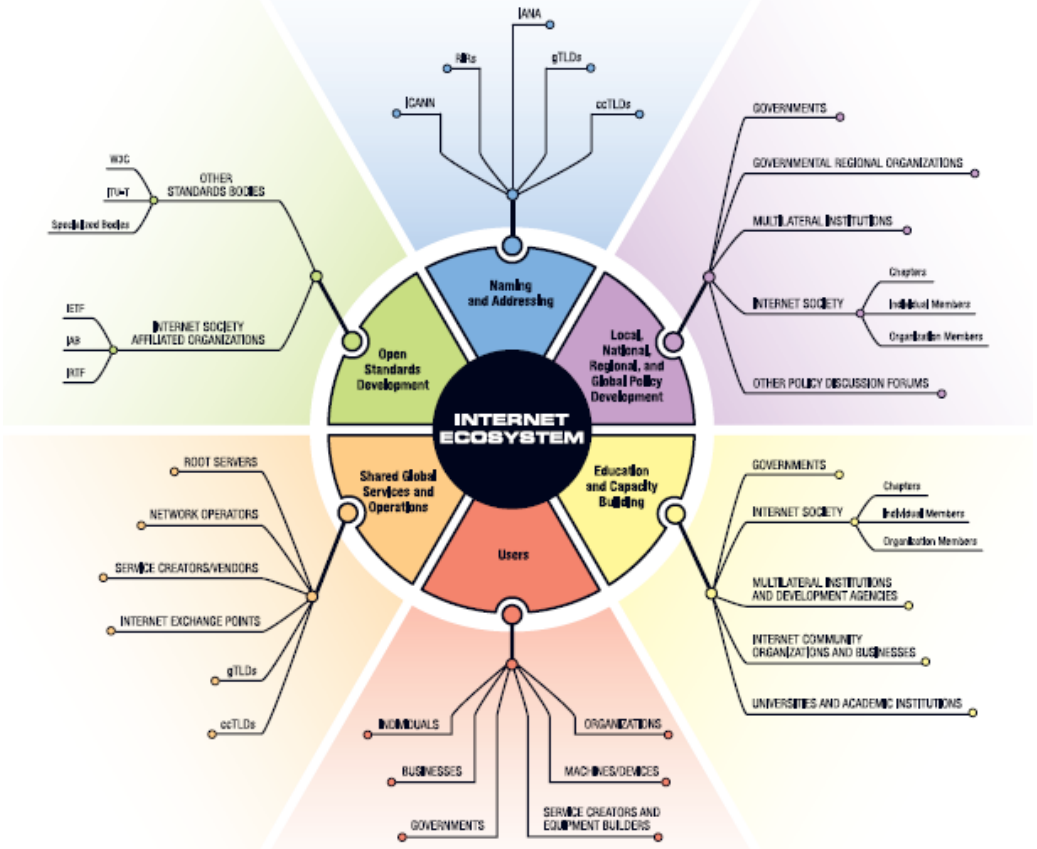
Big questions unanswered

- How do we protect against huge DDOS?
- Role of companies vs. governments
- What is considered Critical Infrastructure?
- What are international norms of behavior?
  - (Double Illegal)

The Internet Ecosystem

The Internet is successful in large part due to its unique model: shared global ownership, development based on open standards, and freely accessible processes for technology and policy development.

The Internet's unprecedented success continues to thrive because the Internet model is open, transparent, and collaborative. The model relies on processes and products that are local, bottom-up, and accessible to users around the world.



http://www.isoc.org/pubpolpillar/docs/internetmodel.pdf

TEAM CYMRU
DNS Name Server Status Summary

[team-cymru@cymru.com] [HOME]

All data is current as of **Sat Dec 1 06:41:02 2012 GMT**
[root] [arpa] [asia] [biz] [com] [edu] [gov] [info] [int] [mil] [name] [net] [org]

DNS Legend:
- response time is within normal parameters
- response time is slightly higher than normal
- response time is much higher than normal
- no query response or route error
- probe data is stale
- no probe data received

Network Legend:
- IP/Prefix/ASN is normal
- Net info has changed within last 15 days
- Net info has changed within last 48 hours
- IP/Prefix/ASN is no longer present

root servers [top]

server	net status			dns response time									
	IP	Prefix	ASN	as174 Paris, FR	as1224 Urbana, IL US	as3265 Amsterdam, NL	as4808 Beijing, CN	as5486 Tel-Aviv, IL	as12513 Oxford, UK	as12824 Szczecin, PL	as24047 Tokyo, JP	as29748 Ashburn, VA US	as39655 Brasov, RO
a.root-servers.net	OK	OK	OK	325 ms	31 ms	9 ms	285 ms	393 ms	94 ms	334 ms	67 ms	8 ms	368 ms
b.root-servers.net	OK	OK	OK	142 ms	60 ms	160 ms	212 ms	204 ms	164 ms	182 ms	118 ms	68 ms	188 ms
c.root-servers.net	OK	OK	OK	11 ms	6 ms	12 ms	215 ms	181 ms	40 ms	23 ms	114 ms	2 ms	38 ms
d.root-servers.net	OK	OK	OK	80 ms	25 ms	92 ms	278 ms	170 ms	101 ms	114 ms	173 ms	4 ms	126 ms
e.root-servers.net	OK	OK	OK	163 ms	4 ms	9 ms	216 ms	77 ms	208 ms	206 ms	120 ms	33 ms	49 ms
f.root-servers.net	OK	OK	OK	156 ms	37 ms	170 ms	4 ms	3 ms	25 ms	182 ms	3 ms	76 ms	189 ms
g.root-servers.net	OK	OK	OK	164 ms	191 ms	278 ms	-- no data --	186 ms	282 ms	144 ms	21 ms	196 ms	318 ms
h.root-servers.net	OK	OK	OK	86 ms	25 ms	96 ms	277 ms	655 ms	101 ms	116 ms	189 ms	10 ms	143 ms
i.root-servers.net	OK	OK	OK	12 ms	4 ms	1 ms	366 ms	75 ms	27 ms	42 ms	19 ms	74 ms	4 ms
j.root-servers.net	OK	OK	OK	43 ms	90 ms	126 ms	4 ms	86 ms	65 ms	1 ms	11 ms	8 ms	19 ms
k.root-servers.net	OK	OK	OK	104 ms	102 ms	4 ms	133 ms	76 ms	129 ms	24 ms	11 ms	598 ms	40 ms
l.root-servers.net	OK	OK	OK	26 ms	54 ms	17 ms	264 ms	98 ms	161 ms	19 ms	9 ms	76 ms	38 ms
m.root-servers.net	OK	OK	OK	2 ms	210 ms	24 ms	104 ms	84 ms	32 ms	270 ms	10 ms	70 ms	301 ms

arpa servers [top]

server	net status			dns response time									
	IP	Prefix	ASN	as174 Paris, FR	as1224 Urbana, IL US	as3265 Amsterdam, NL	as4808 Beijing, CN	as5486 Tel-Aviv, IL	as12513 Oxford, UK	as12824 Szczecin, PL	as24047 Tokyo, JP	as29748 Ashburn, VA US	as39655 Brasov, RO
a.root-servers.net	OK	OK	OK	325 ms	31 ms	9 ms	285 ms	393 ms	94 ms	334 ms	67 ms	8 ms	368 ms
b.root-servers.net	OK	OK	OK	142 ms	60 ms	160 ms	212 ms	204 ms	164 ms	182 ms	118 ms	68 ms	188 ms
c.root-servers.net	OK	OK	OK	11 ms	6 ms	12 ms	215 ms	181 ms	40 ms	23 ms	114 ms	2 ms	38 ms
d.root-servers.net	OK	OK	OK	80 ms	25 ms	92 ms	278 ms	170 ms	101 ms	114 ms	173 ms	4 ms	126 ms
e.root-servers.net	OK	OK	OK	163 ms	4 ms	9 ms	216 ms	77 ms	208 ms	206 ms	120 ms	33 ms	49 ms
f.root-servers.net	OK	OK	OK	156 ms	37 ms	170 ms	4 ms	3 ms	25 ms	182 ms	3 ms	76 ms	189 ms
g.root-servers.net	OK	OK	OK	164 ms	191 ms	278 ms	-- no data --	186 ms	282 ms	144 ms	21 ms	196 ms	318 ms
h.root-servers.net	OK	OK	OK	86 ms	25 ms	96 ms	277 ms	655 ms	101 ms	116 ms	189 ms	10 ms	143 ms
i.root-servers.net	OK	OK	OK	12 ms	4 ms	1 ms	366 ms	75 ms	27 ms	42 ms	19 ms	74 ms	4 ms
k.root-servers.net	OK	OK	OK	104 ms	102 ms	4 ms	133 ms	76 ms	129 ms	24 ms	11 ms	598 ms	40 ms
l.root-servers.net	OK	OK	OK	26 ms	54 ms	17 ms	264 ms	98 ms	161 ms	19 ms	9 ms	76 ms	38 ms
m.root-servers.net	OK	OK	OK	2 ms	210 ms	24 ms	104 ms	84 ms	32 ms	270 ms	10 ms	70 ms	301 ms

asia servers [top]

server	net status			dns response time									
	IP	Prefix	ASN	as174 Paris, FR	as1224 Urbana, IL US	as3265 Amsterdam, NL	as4808 Beijing, CN	as5486 Tel-Aviv, IL	as12513 Oxford, UK	as12824 Szczecin, PL	as24047 Tokyo, JP	as29748 Ashburn, VA US	as39655 Brasov, RO
a0.asia.afilias-nst.info	OK	OK	OK	95 ms	240 ms	318 ms	267 ms	170 ms	125 ms	332 ms	69 ms	234 ms	316 ms
a2.asia.afilias-nst.info	OK	OK	OK	18 ms	31 ms	13 ms	269 ms	79 ms	104 ms	1 ms	10 ms	73 ms	34 ms
b0.asia.afilias-nst.asia	OK	OK	OK	307 ms	243 ms	320 ms	301 ms	340 ms	138 ms	336 ms	63 ms	232 ms	304 ms
b2.asia.afilias-nst.org	OK	OK	OK	1 ms	6 ms	76 ms	188 ms	82 ms	34 ms	109 ms	176 ms	1 ms	41 ms
c0.asia.afilias-nst.info	OK	OK	OK	95 ms	110 ms	2 ms	267 ms	85 ms	32 ms	35 ms	268 ms	17 ms	41 ms
d0.asia.afilias-nst.asia	OK	OK	OK	170 ms	126 ms	207 ms	347 ms	220 ms	178 ms	190 ms	125 ms	115 ms	190 ms

http://www.cymru.com/monitoring/dnssumm/index.html

SSAC Advisory SAC008
DNS Distributed Denial of Service (DDoS) Attacks

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
March 2006

http://www.icann.org/en/groups/ssac/dns-ddos-advisory-31mar06-en.pdf

- Security and Stability Advisory Committee (SSAC)
- What is the SSAC?

- The Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.

- **Recommendation (1):** For the long term, SSAC recommends that the most effective
- means of mitigating the effects of this and numerous DoS attacks is to adopt source IP
- address verification.

Paul Vixie, ISC

Securing the Edge

Abstract

At every edge of the global Internet are the hosts who generate and consume the packet flows which, together, form the overall Internet traffic load. By number, most of these hosts are not secure, leading to dangerous, untraceable traffic flows which can be used to attack other hosts. This memo describes some of the security problems "at the edge" and makes some recommendations for improvement.

1 - Connection Taxonomy

1.1. The Internet is a "network of networks", where the component networks are called Autonomous Systems (AS), each having a unique AS Number (ASN).

1.2. Connections inside an AS are called "Interior" (or sometimes "backbone"), and their security policies are set according to local needs, usually based on business or technical requirements.

1.3. Connections between ASs are called "Border" (or sometimes "peering"), and their security policies are set bilaterally according to the joint needs of the interconnecting parties.

1.4. Connections between an AS and its traffic sources (generators) and traffic sinks (consumers) are called "Edge" (or sometimes "customer"), and their security policies are generally, by long standing tradition, inconsistent.

2 - DDoS Vulnerability

2.1. The most common attack on Internet hosts or infrastructure at the time of this writing is to cause the receipt of too much traffic, consuming all available resources on a victim's host or Internet connection. This is often called a "Denial of Service" (DoS) attack.

2.2. For a DoS attack to succeed, the source or "launch point" must not be trivially detectable. Therefore, successful attacks employ large numbers of weak attackers. An attack launched from ten thousand hosts who each sent ten packets per second would be called a Distributed Denial of Service (DDoS) attack.

Network Working Group
Request for Comments: 2827
Obsoletes: 2267
BCP: 38
Category: Best Current Practice

P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.

May 2000

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

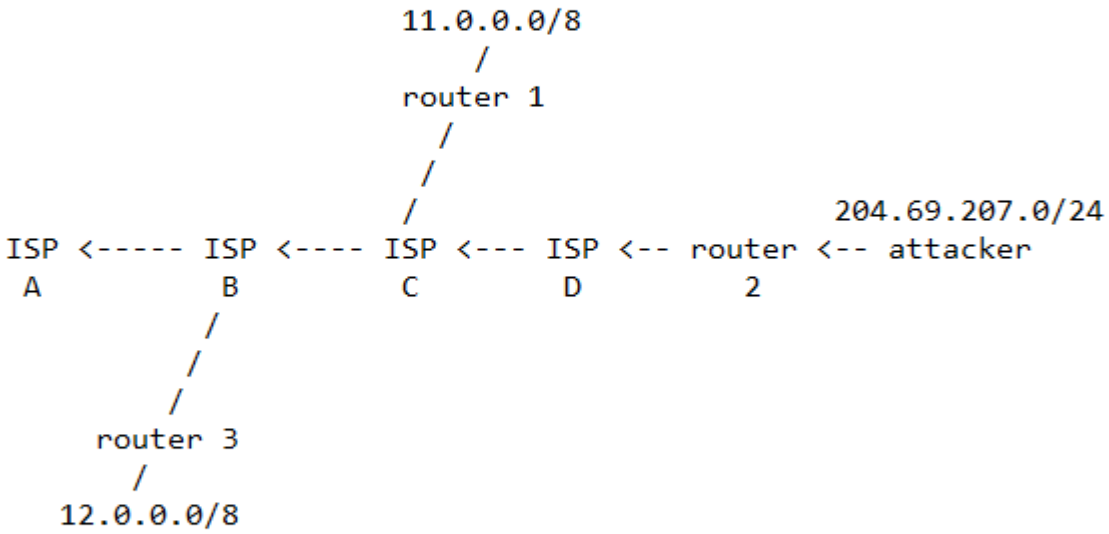
Abstract

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

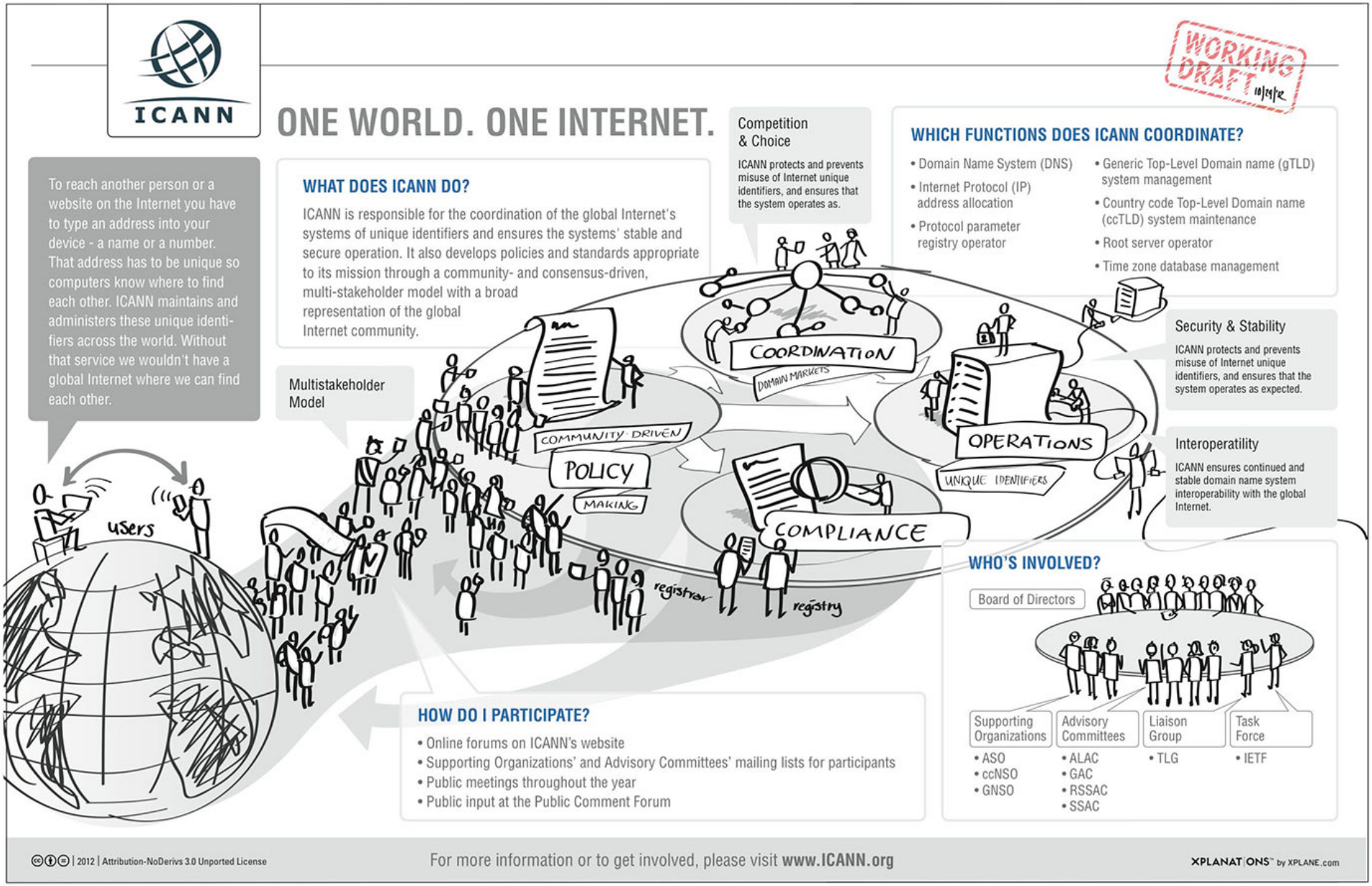
Table of Contents

3. Restricting forged traffic

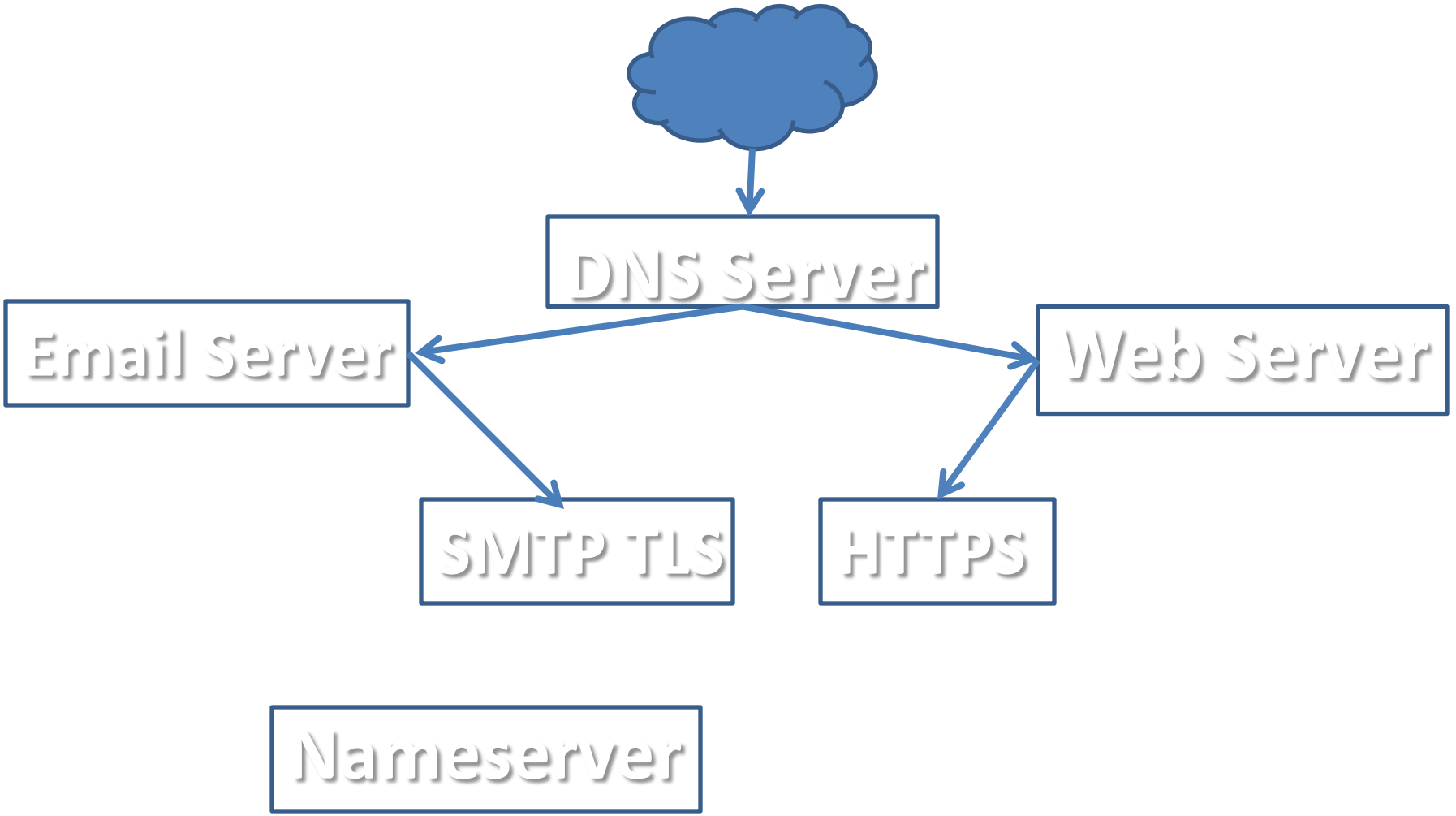
The problems encountered with this type of attack are numerous, and involve shortcomings in host software implementations, routing methodologies, and the TCP/IP protocols themselves. However, by restricting transit traffic which originates from a downstream network to known, and intentionally advertised, prefix(es), the problem of source address spoofing can be virtually eliminated in this attack scenario.



In the example above, the attacker resides within 204.69.207.0/24, which is provided Internet connectivity by ISP D. An input traffic filter on the ingress (input) link of "router 2", which provides connectivity to the attacker's network, restricts traffic to allow only traffic originating from source addresses within the 204.69.207.0/24 prefix, and prohibits an attacker from using "invalid" source addresses which reside outside of this prefix range.



http://icann.xplane.com/questionaire/ecosystem


DNS Server
Email Server
Web Server
SMTP TLS
HTTPS
Nameserver