DNS OUT THERE ...

Lars-Johan Liman, M.Sc.
Sr. Systems Specialist
Netnod Internet Exchange

BEAR IN MIND ...

One DB to Rule Them All ...

DNS is a database.

DNS is ***one*** database ...

- **... that is distributed over many servers,**
- **... that can contain a variety of information,**
- **... that is hierarchical, but**

It is ***ONE*** database.

The full service resolver (local nameserver) hides the complexity of the server tree from the stub resolver (end client).

DNS – Fair and Equal

ALL domain names are treated equal!

- There is ***NO*** structural difference between
  `arpa.`
  `lab.csc.kth.se.`
  `www.volvo.se.`
  `10.23.19.8.in-addr.arpa.`
  `10.ugly.23.hack.55.to.33.confuse.12.students.se.`

(or even)

.

Trick Questions

Can you have an A record for SE. ?

Trick Questions

Can you have an A record for SE. ?

- **YES!**

se. 3600 IN A 10.23.19.2

Trick Questions

Can you have a PTR record for kth.se. ?

Trick Questions

Can you have a PTR record for kth.se. ?

- **YES!**

kth.se. 600 IN PTR server14.kth.se.

(OK. Not very useful, but the DNS system doesn't mind!)

Trick Questions

Can you have an MX record for "." ?

Trick Questions

Can you have an MX record for "." ?

- **YES, of course you can!**

```
.                   86400   IN      MX      10  smtp.cafax.se.
```

(And yes, the mail system will not cooperate, but the DNS system doesn't mind.)

Categories of Record Types

The DNS uses its own records to maintain the structure of the database itself.

Two categories of records:

- **Data carrying records: Used by applications to reach various resources.**
  A, AAAA, MX, PTR, SRV, NAPTR, ...
- **Structure carrying records: Only used by the DNS system itself to locate the sought data records.**
  SOA, NS, CNAME, DNAME, ...

(The meat and the bones of the “body”.)

Cacheing is Vital

The cacheing mechanism in the full service resolver helps off-load traffic from the root name servers.

- **The higher up, the more traffic (almost ...).**
- **Without cacheing, every query would have to start at the root.**
- **Not A Good Idea™**
- **The root servers receive enough junk as it is ...**

SPEAKING OF ROOT NAME SERVERS

Root Name Servers

So what's the deal?

- **What, why, who, where, when?**

13 root name servers on the Internet:

- **X.root-servers.net. (where X ∈ { a, b, ..., m })**

Operated by 12 organisations.

- **i.root-servers.net is operated by Netnod.**
- **Verisign operates 2 letters: a and j.**

Overview:

- **http://www.root-servers.ORG/**

Root Server System Expansion

15 years ago it was 13 machines.

- **10 x USA + Sweden + UK + Japan.**

Big nations started to complain.

- **China, India, France, Germany, ...**

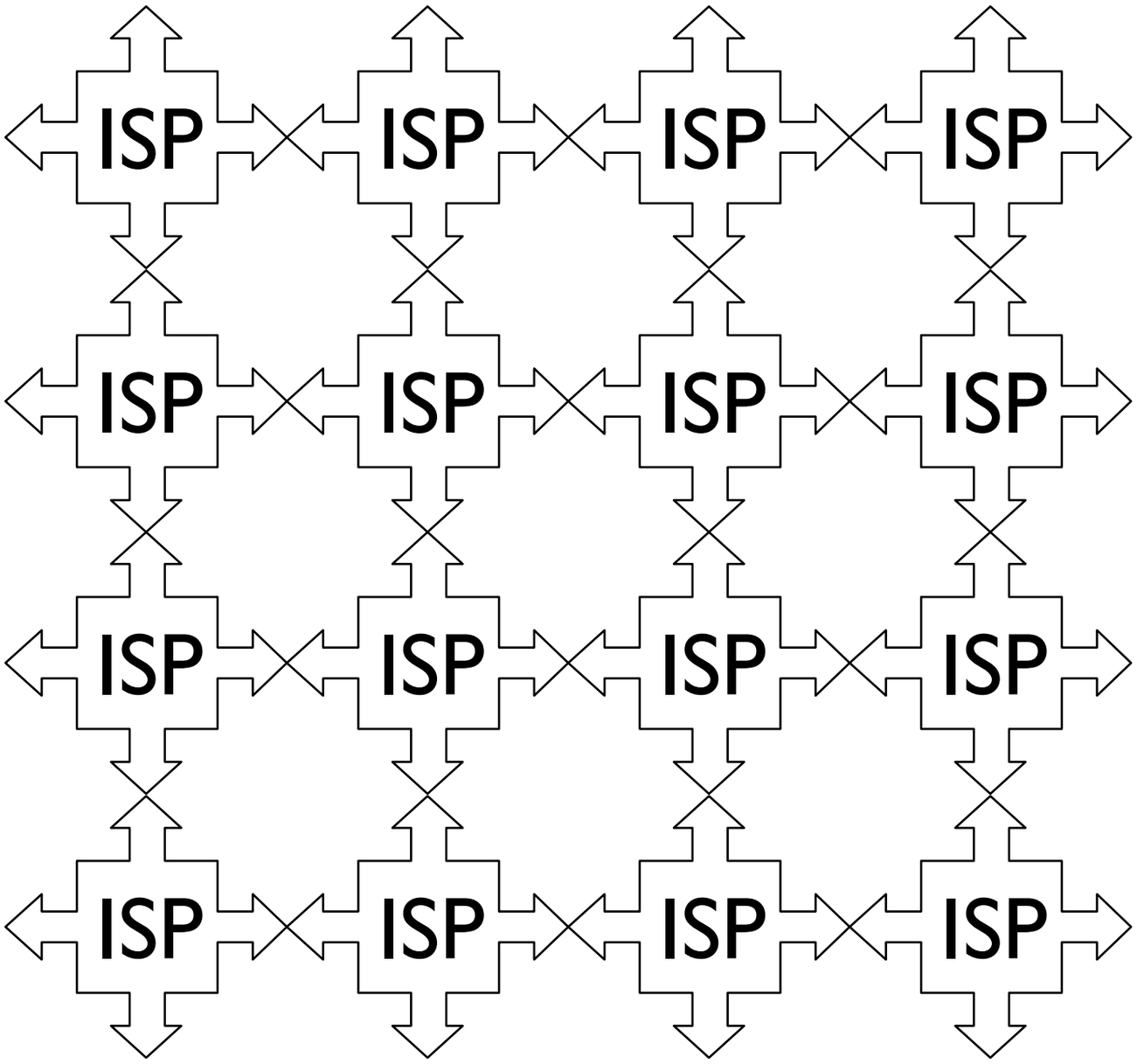
Technical limitation on the number of servers!

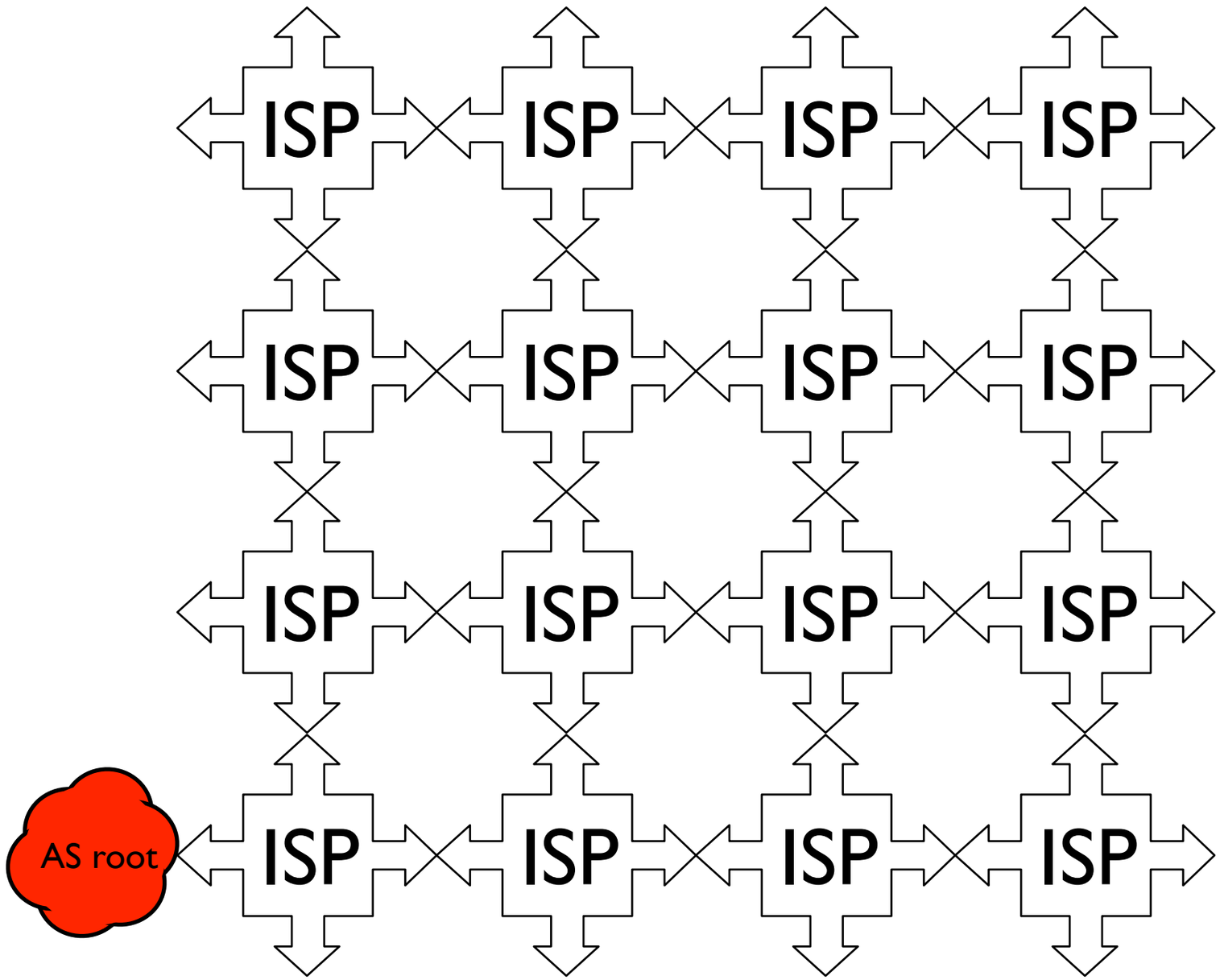
- **What to do?**

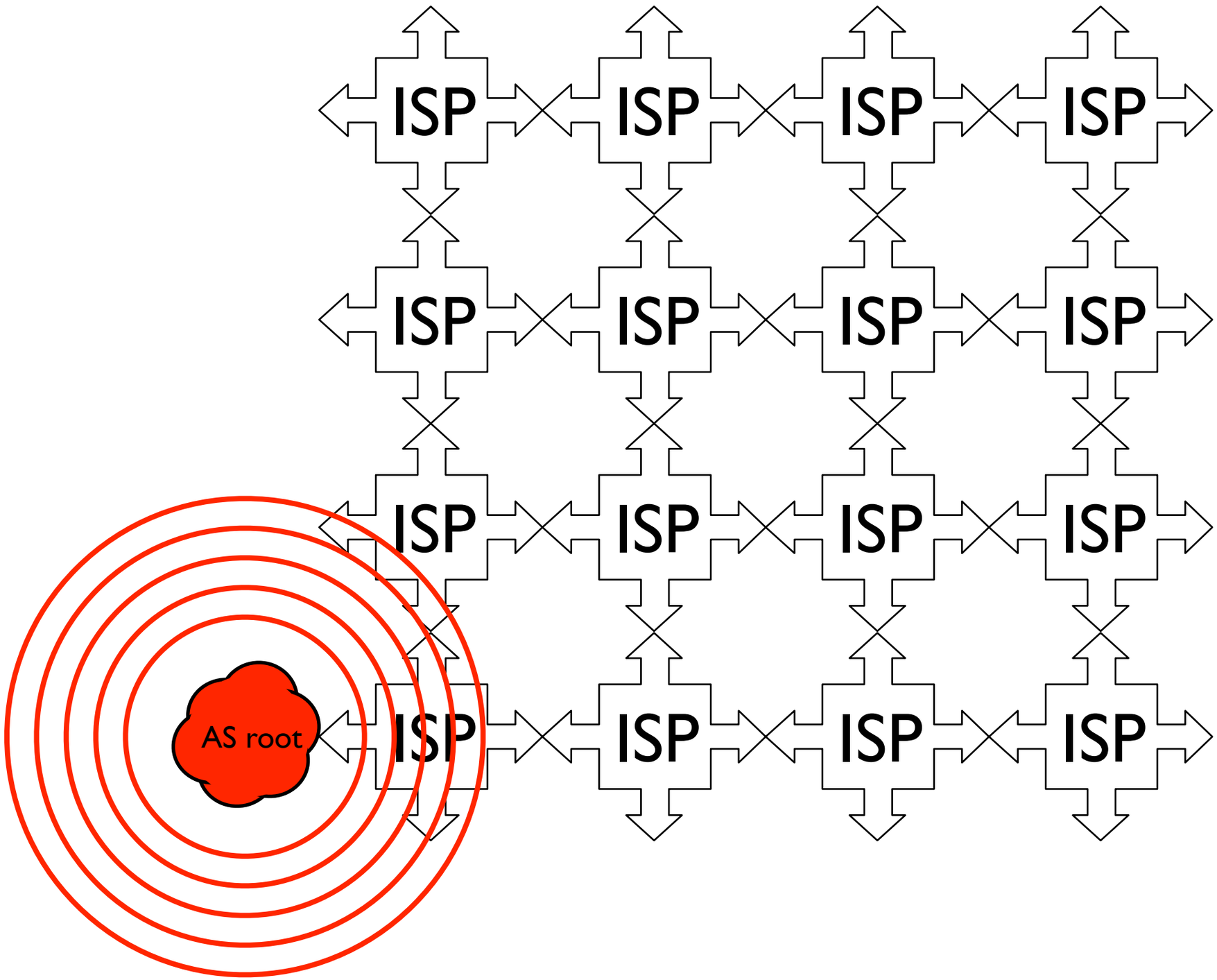
Ugly hack: **ANYCAST!**

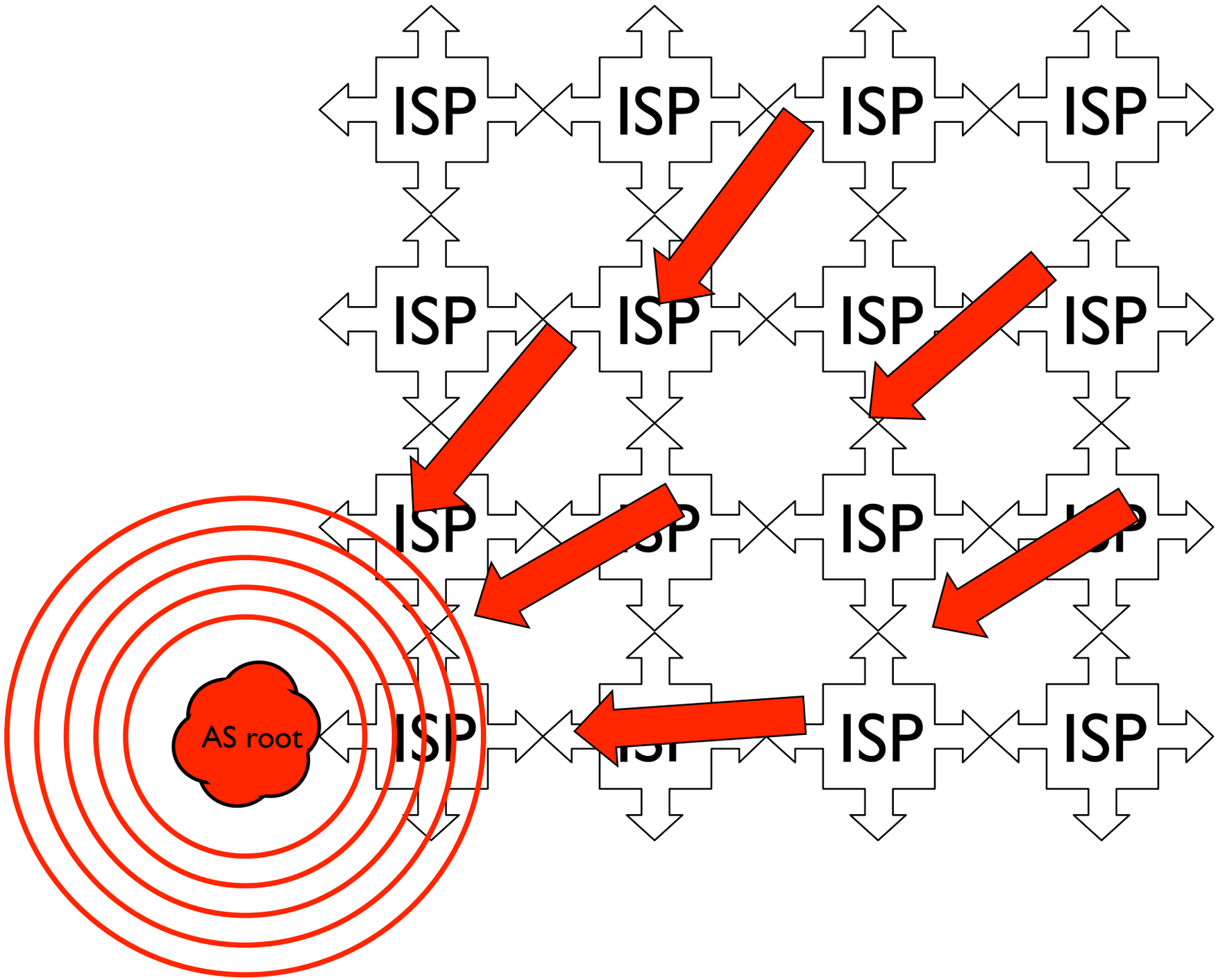
- **Now 300+ sites in total!**

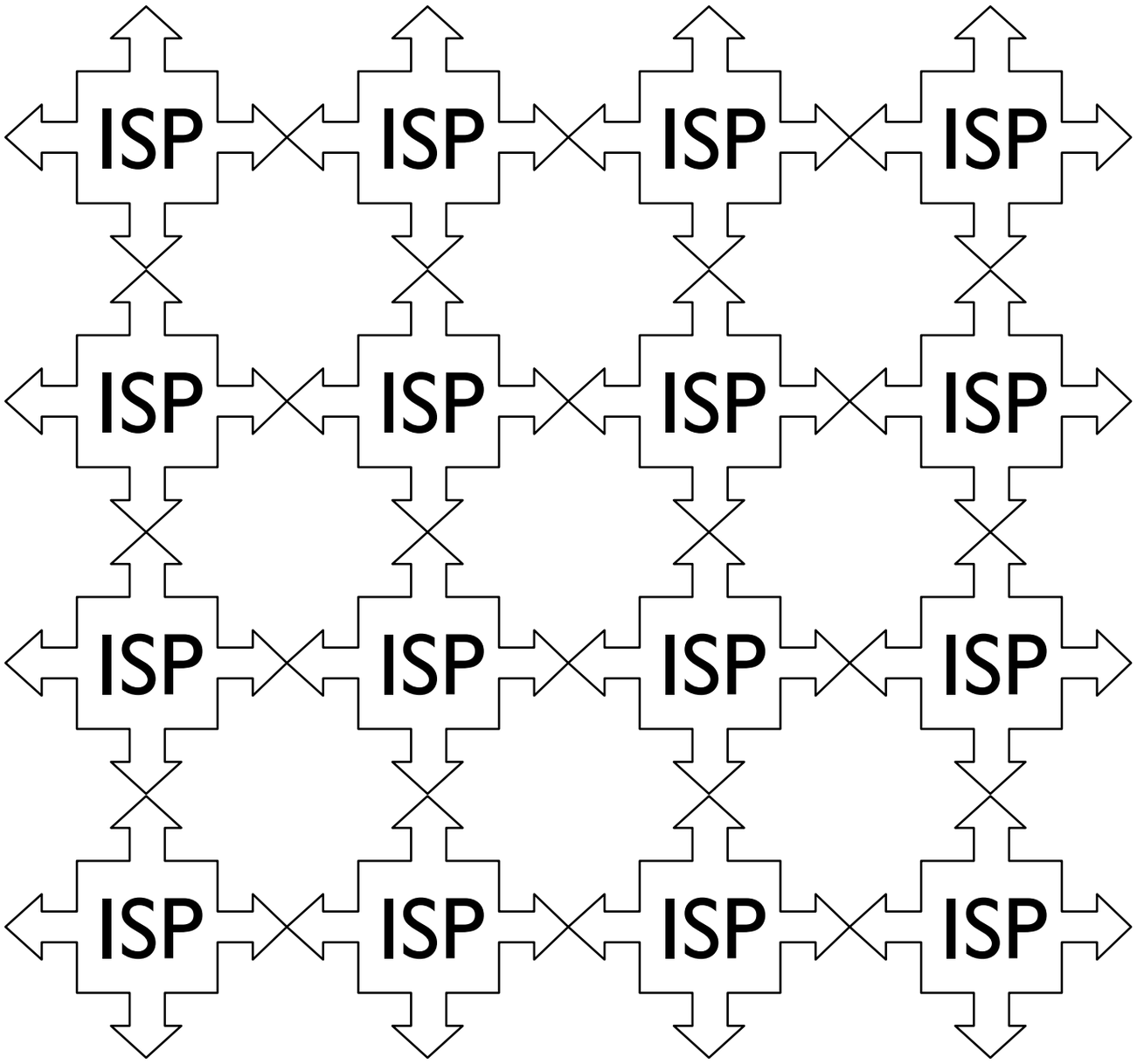
ANYCAST

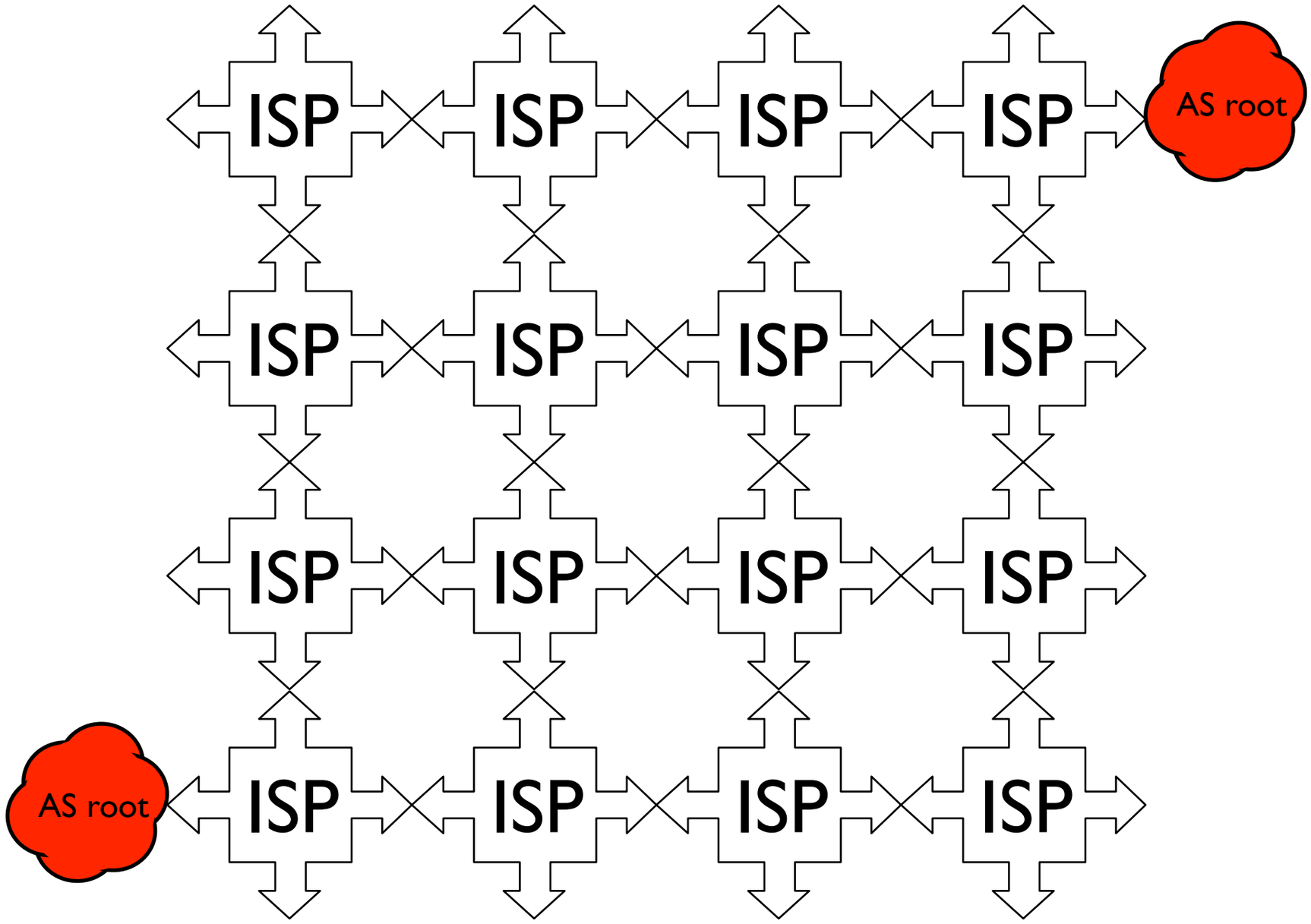

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP

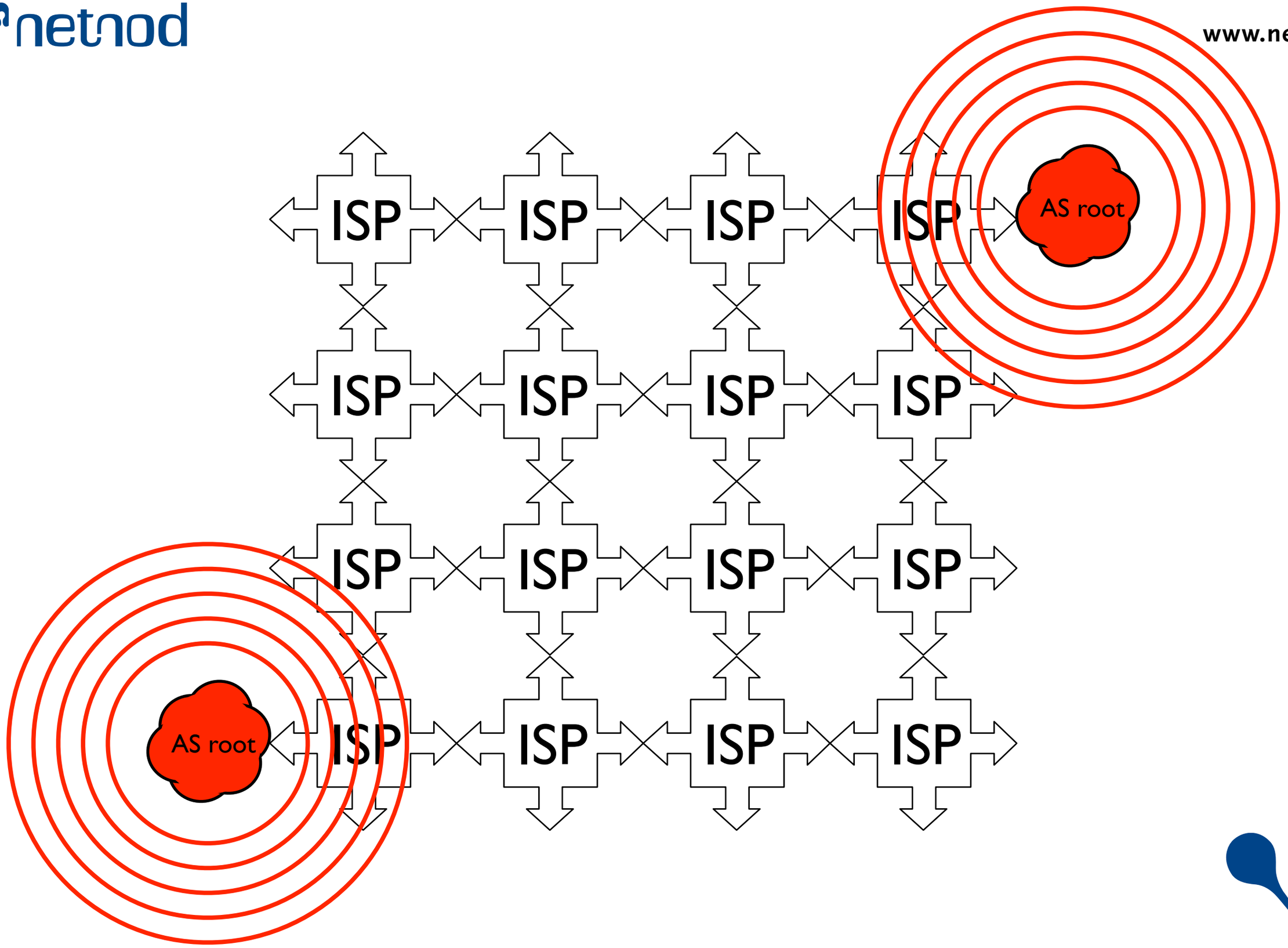

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP

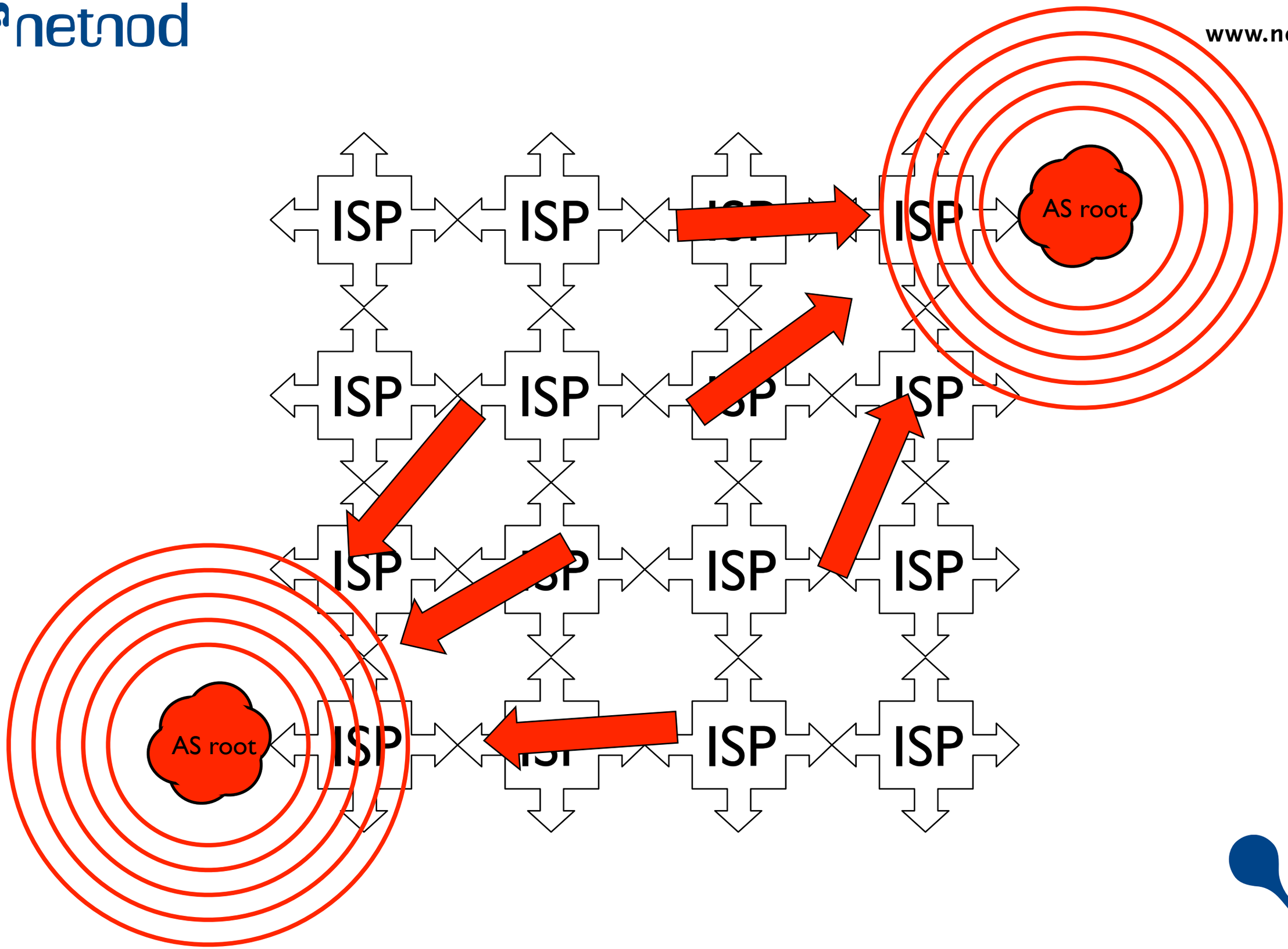

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root

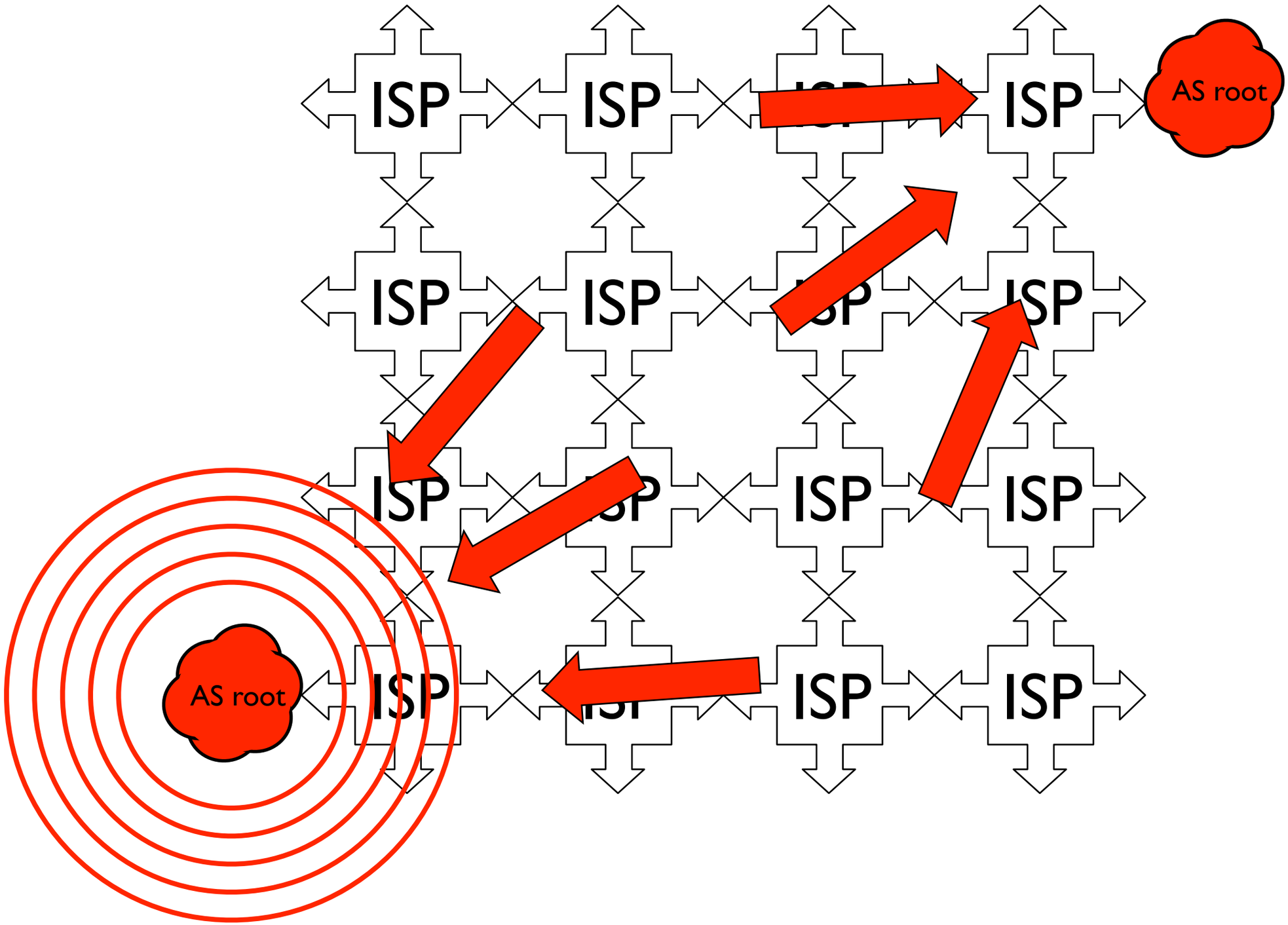

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root

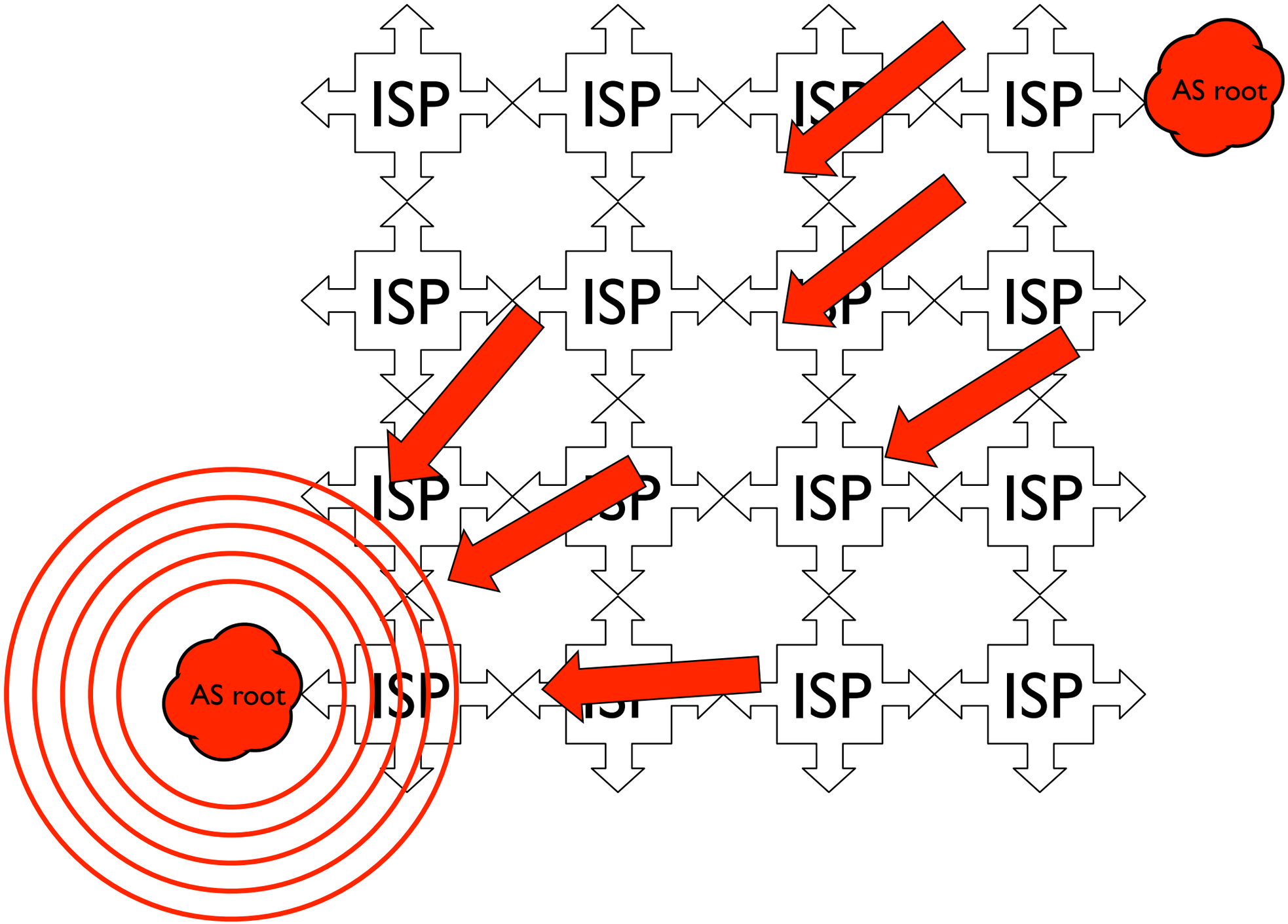

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP


ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP

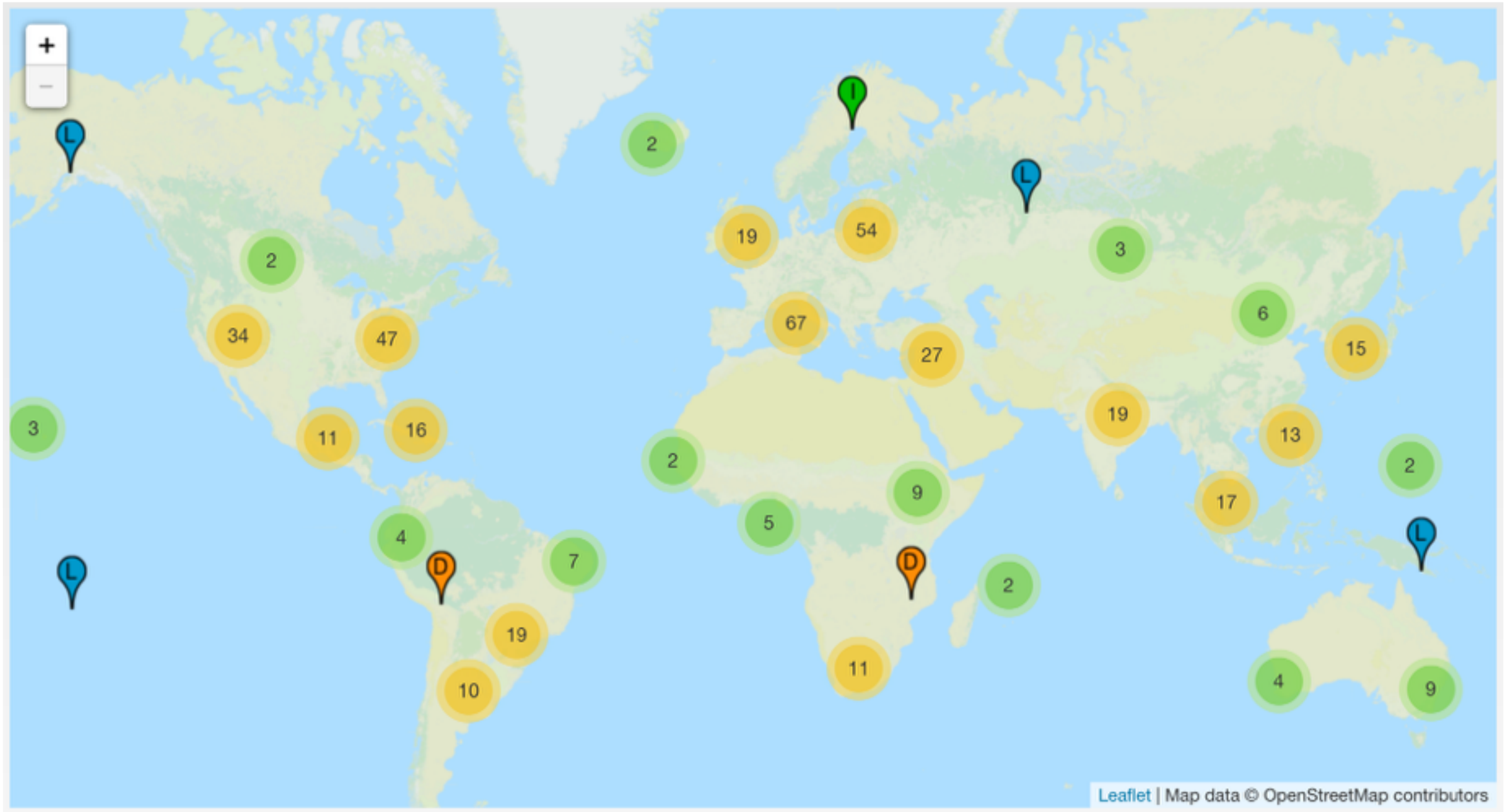

ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP

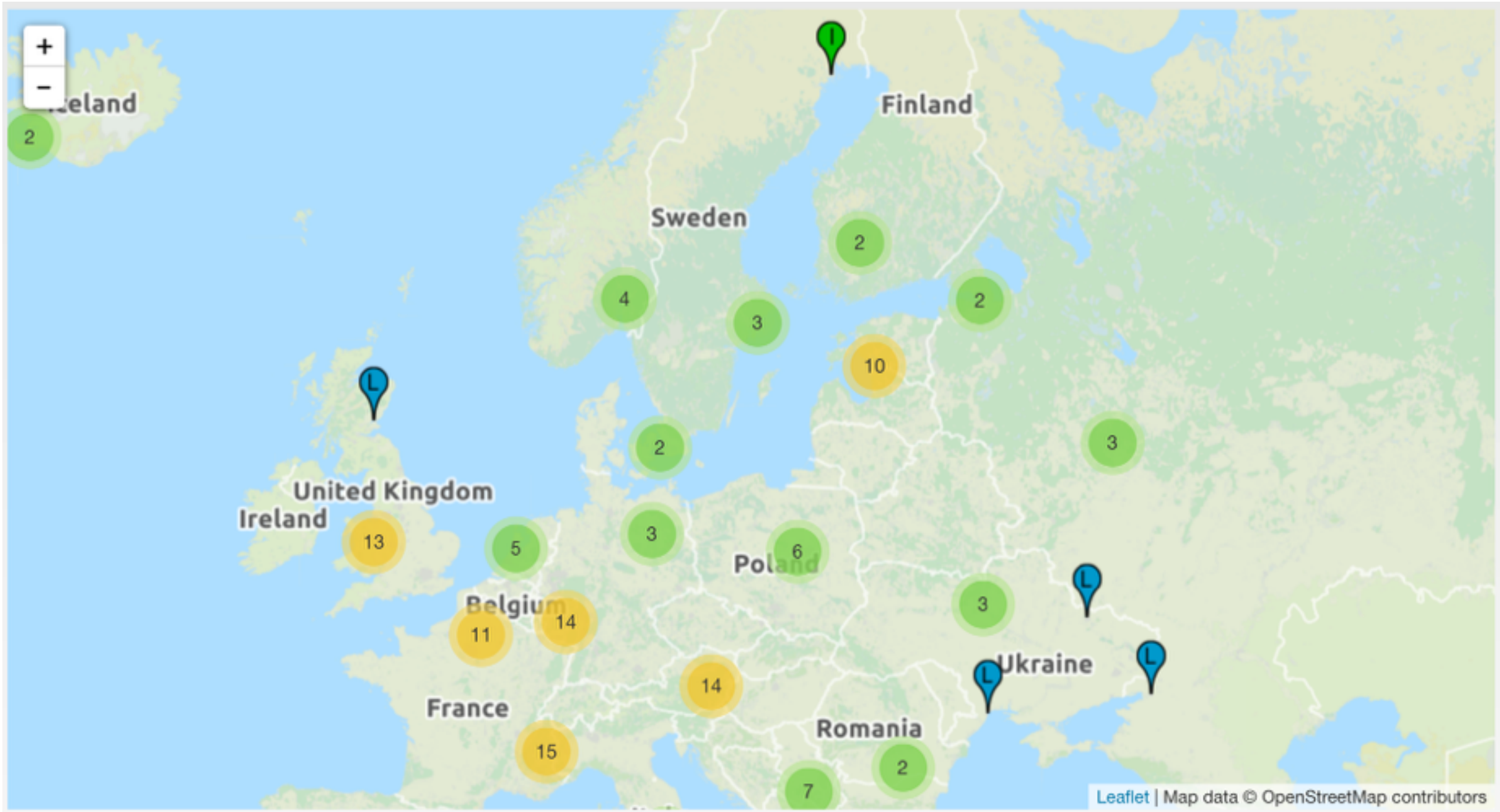

ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP


ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP


ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root
ISP
ISP
ISP


Map
Satellite
Hybrid
Greenland
Iceland
Suomi (Finland)
Россия (Russia)
Canada
United States
México
North Atlantic Ocean
Kazakhstan
Mongolia
中国 (China)
대한민국 (South Korea)
Algeria
Libya
(Egypt)
Saudi Arabia
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
DR Congo
Tanzania
Angola
Namibia
Madagascar
South Africa
Indian Ocean
Indonesia
Papua New Guinea
Australia
New Zealand
Venezuela
Colombia
Perú
Bolivia
Brasil (Brazil)
Argentina
South Atlantic Ocean
Legend
Multiple instances
Single instance
POWERED BY Google
Imagery ©2011 NASA, TerraMetrics, Map data ©2011 Geocentre Consulting, MapLink, Tele Atlas - Terms of Use


+
−
L
I
L
L
D
D
L
2
19
54
3
2
34
47
67
27
6
15
3
11
16
19
13
2
2
9
5
17
4
7
2
L
19
10
11
4
9
Leaflet | Map data © OpenStreetMap contributors


Finland
Sweden
United Kingdom
Ireland
Belgium
France
Poland
Ukraine
Romania
Leaflet | Map data © OpenStreetMap contributors

ROOT ZONE ADMINISTRATION

The Good Old Days™

Used to be Jon Postel (RIP), head of the IANA (Internet Assigned Numbers Authority).

- **... and that was that.**
- **... and then he died!**

Jon initiatied the creation of an organisation for the purpose.

- **This has developed into ICANN (Internet Corporation for Assigned Names and Numbers).**
- **The IANA is now a subdivision of ICANN.**

ICANN

ICANN was designed as a multi-stakeholder, bottom-up organisation.

- **Tried to let everyone have a say – from single citizens to business, and governments.**
- **This works only so-so.**

ICANN is a policy organisation, and it sets policies for new TLDs, and decides which to establish.

New gTLD program established under which hundreds of new TLDs are established.

1974!

ARPANET DIRECTORY
NIC 19275
Jan. 1974

HOST NAMES

HOST NAMES

HOSTNAME	HOST ADDR (Dec)	LIAISON	STATUS
AFWL-TIP	176	D Hyde (505)247-1711 x3803	TIP, Up 3-74
ALOHA-TIP	164	R Binder (808)948-7066	TIP
AMES-11	208	J Hart (415)965-5935	USER, up 12-73
AMES-67	16	W Hathaway (415)965-6033	SERVER
AMES-TIP	144	W Hathaway (415)965-6033	TIP
ANL	2	L Amiot (312)739-7711 x4309	SERVER, up 2-74
ARPA-DMS	28	S Crocker (202)694-5037	USER, Agency use only
ARPA-TIP	156	S Crocker (202)694-5037	TIP
BBN-11X	5	R Thomas (617)491-1850 x483	Peripheral processor for #69, up 12-73
BBN-1D	232	A McKenzie (617)491-1850 x441	USER
BBN-NCC	40	A McKenzie (617)491-1850 x441	USER
BBN-TENEX	69	R Thomas (617)491-1850 x483	SERVER
BBN-TENEXB	133	R Thomas (617)491-1850 x483	SERVER, Limited
BBN-TESTIP	158	A McKenzie (617)491-1850 x441	TIP (magtape)
BELVOIR	27	W Andrews (703)664-5511	USER, up 6-74
BRL	29	M Romanelli (301)278-4574	USER
CASE-10	13	J Calvin (216)368-2984	SERVER
CCA-TENEX	31	R Winter (617)491-3670	SERVER
CCA-TIP	159	R Winter (617)491-3670	TIP
CMU-10A	78	H Van Zoeren (412)621-2600 x160	SERVER
CMU-10B	14	H Van Zoeren (412)621-2600,x160	SERVER
CMU-11	142	C Pierson (412)621-2600 x130	USER, up Spring 74
CMU-CC	206	D King (412)621-2600 x2683	USER, up Spring 74
DOCB-TIP	153	S Stevenson (303)499-1000 x3138	TIP
EGLIN	?	E Blackwell (904)882-3734	Up 3/74
ETAC	20	G Petregal (202)433-3911	USER, up Spring 74
ETAC-TIP	148	G Petregal (202)433-3911	TIP (magtape)
FNWC	33	M Reese (408)646-2817	USER, up 2-74
FNWC-TIP	161	M Reese (408)646-2817	TIP
GWC-TIP	152	A Wells(402)294-2968	TIP (magtape)
HARV-1	73	B Reussow (617)495-4147	USER
HARV-10	9	B Reussow (617)495-4147	SERVER
HARV-11	137	S Bradner (617)495-3864	USER
HASKINS	197	F Cooper (203)865-6163	USER (VDH), up Spring 74
HAWAII-500	100	J Davidson (808)944-7455	SERVER, up 1-74
HAWAII-ALOHA	36	R Binder (808)948-7066	USER, Up 12-73
I4-TENEX	15	J McConnell (408)735-0635	SERVER
I4-TENEXA	79	J McConnell (408)735-0635	Peripheral processor for #15
ILL-CAC	12	T Milke (217)333-8469	USER
ILL-NTS	76	T Milke (217)333-8469	USER
ISI-DEVTENEX	150	R Hoffman (213)822-1511 x190	USER, up 1-74
ISI-SPEECH11	22	R Hoffman (213)822-1511 x190	USER, up 1-74

55

2015: Current Chairman of ICANN

The IANA

The IANA is an administrative function that is regulated by a contract with the US Dept of Commerce*. (This may come to and end “soon”.)

The IANA manages (among other things) the contents of the TLD database, under policies set by ICANN.

The IANA sends requests for update of the root zone to …

*) Specifically its National Telecommunications and Information Administration (NTIA)

The DoC (NTIA) and Verisign

NTIA must approve any changes

- **… before they can be implemented by …**

Verisign, who

- **Generate DNSSEC signature, and**
- **Change the actual root zone file.**

The root server operators …

- **… pick up the root zone file from Verisign.**
- **The root zone is publicly available at ftp://ftp.internic.net/domain/root.zone**

Root Server Operators

12 separate organisations

- **Great variety: from military, via universities, to commercial, to not-for-profits.**

No formal relationship with

- **DoC (except for Verisign)**
- **IANA (except for Verisign)**
- **ICANN**
- **each other**
- **any parent organisation (none exists!)**

Technically very well coordinated!

Root Server Operators

Go by old gentlemen's agreements

- **... with Jon Postel (RIP), former head of IANA.**
- **There is no process to change the set of root ops!**

Vast experience in DNS, routing and system administration.
100,00 % uptime* on the system as a whole for more than 15 years.
Meet 3 times/year for coordination.

*) Knock on wood ...

i.root-servers.net

Ordinary DNS servers.

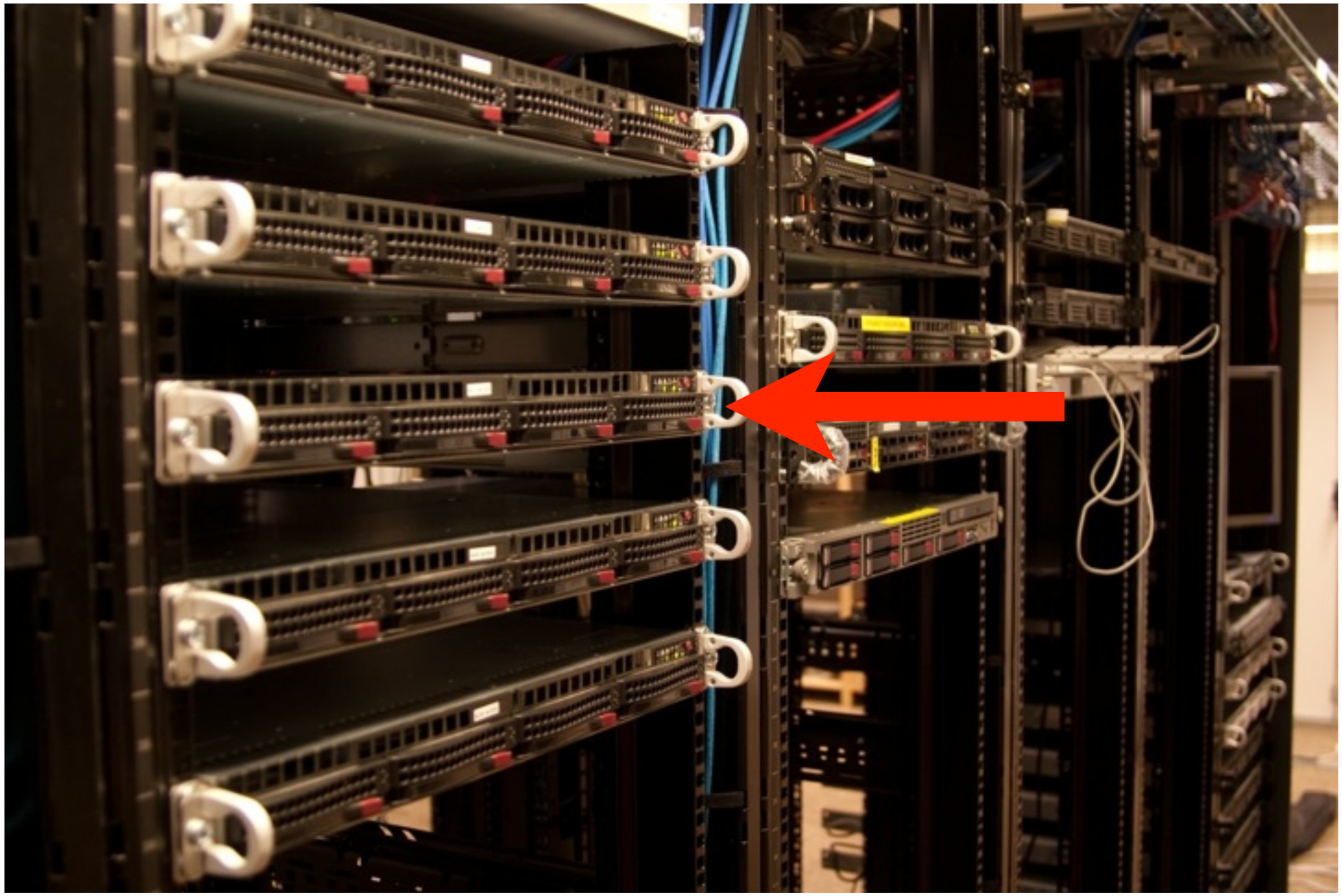
- **Serves the "." zone.**
- **Stockholm: located in communications bunkers provided by PTS.**

Anycast

- **50+ places across the globe.**
- **From Stockholm to Johannesburg, from Wellington to San Francisco …**
- **… including odd places like Colombo, Katmandu, Yerevan, Thimphu, Port Vila**

Serves ~4.5 billion queries/day … to the root zone alone.

s1.sth



Which Node?

How do I know which node I'm using?

```
$ dig  @i.root-servers.net.  \
   hostname.bind.  TXT  CHAOS  \
   +short
```

"s1.sth"

A Few Words About DNSSEC

Upside

- Crypto signatures – validation of data.
- Protects against cache pollutioning (“Kaminski attacks”).
- Can be used to authenticate host keys (i.e., no more web certificates!).

WAY COOL!!

Downside

- Complex administration (use tools!).
- Time sensitive.
- More effective reflection attacks (use rate limiting!).

- SO: GOOD SH*T, BUT USE IT RIGHT!

Contact Information

Lars-Johan Liman
Netnod Internet Exchange
Box 30194
104 25 Stockholm
Sweden

Tel: +46–8–562 860 12
E-mail: liman@netnod.se

Slides available at:
http://www.netnod.se/liman/presentations/kth/201510-ipop-DNS-liman.pdf