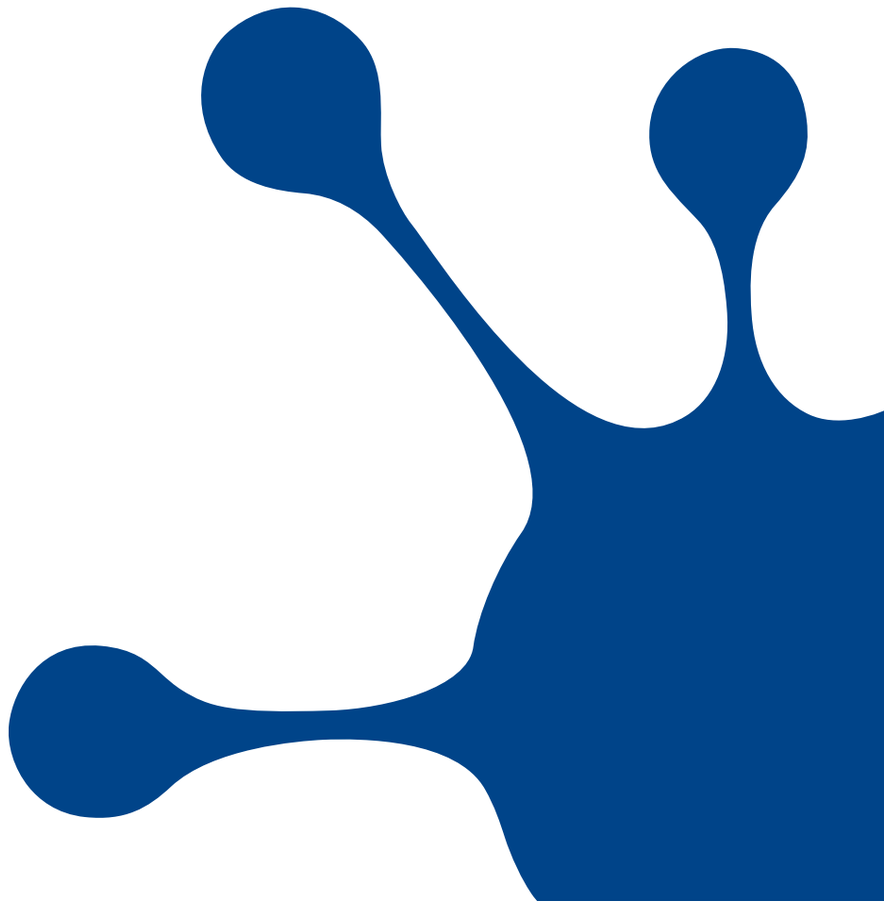
Lars-Johan Liman, M.Sc.
Senior Systems Specialist
Netnod



Overview

What's Netnod?

What do you mean DDoS?

Why is DNS such a popular DDoS tool?

What types of attacks do we see?

Why don’t you just stop it?

What’s wrong with TCP?

What is Netnod, and what do we do?

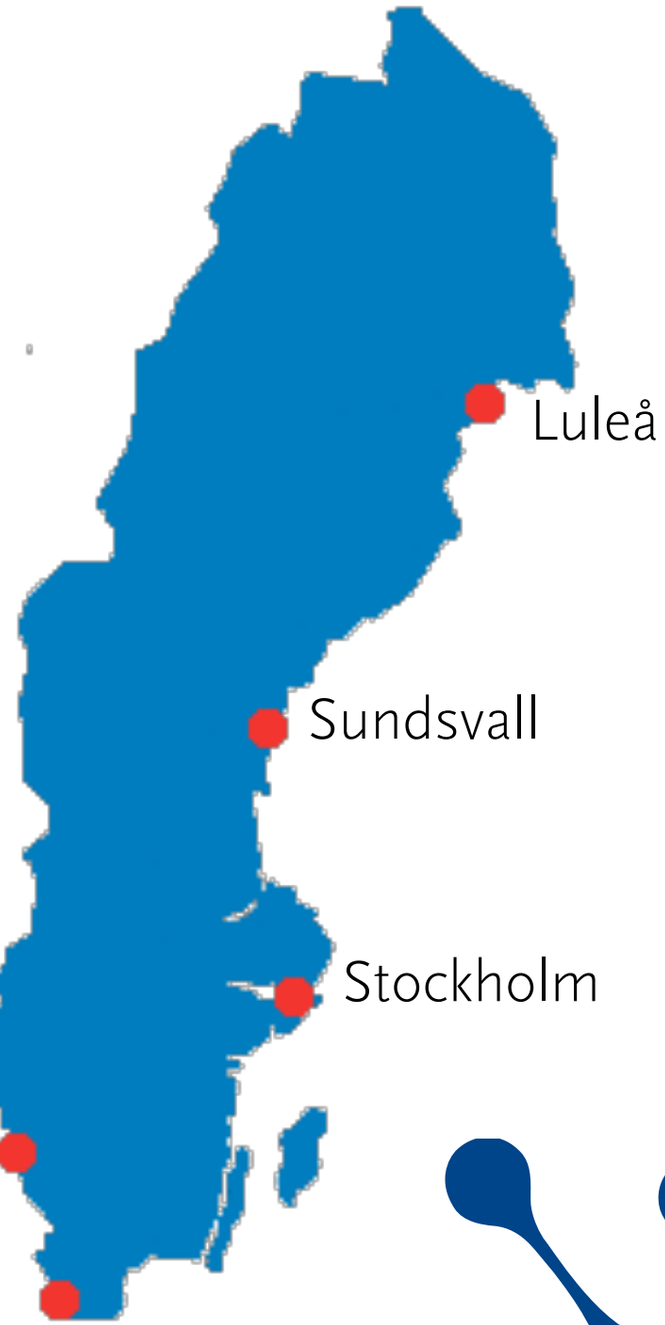
Limited corporation fully owned by a foundation.

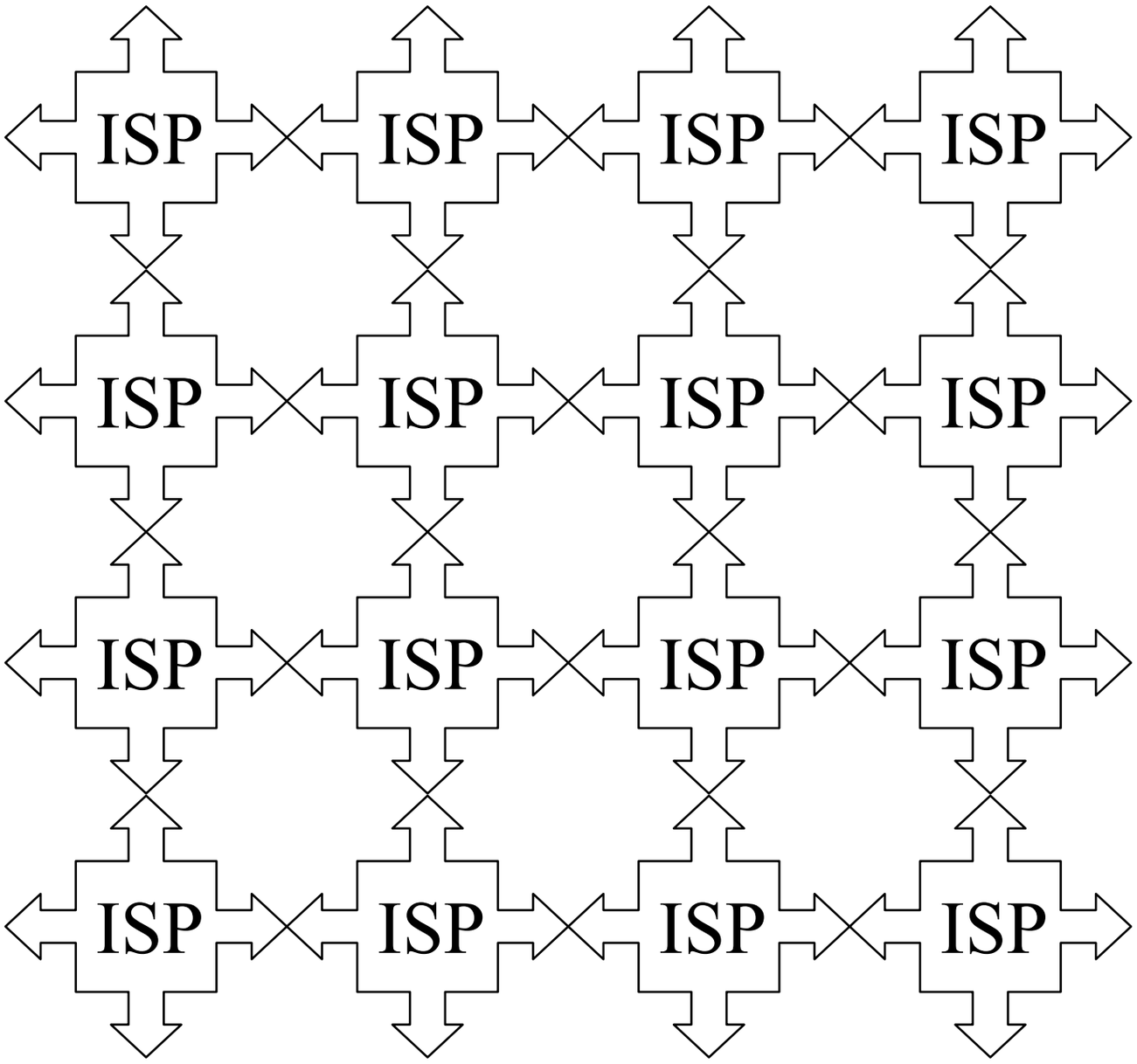
Not for profit.

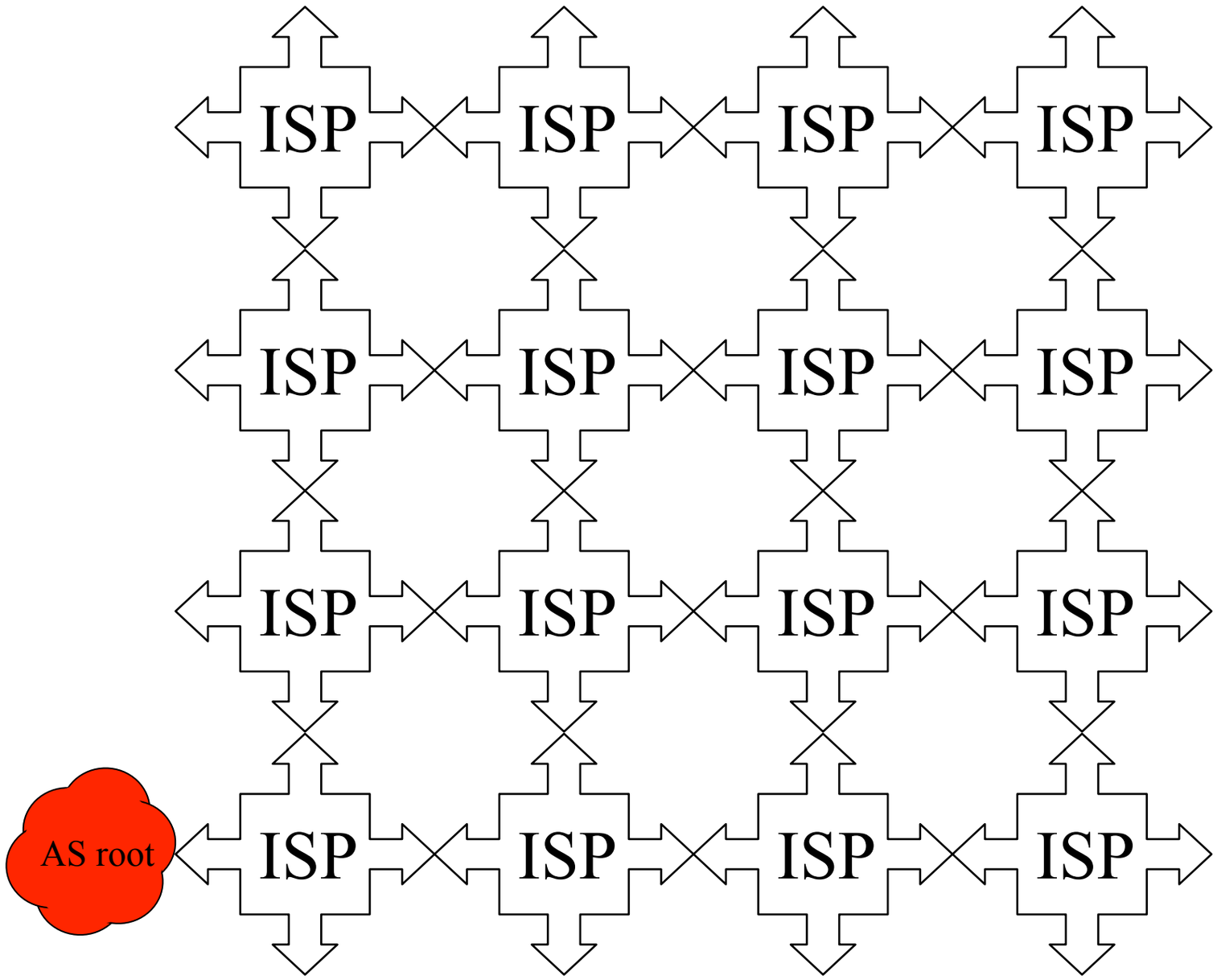
Staff of 16 people. Based in Stockholm, Sweden.

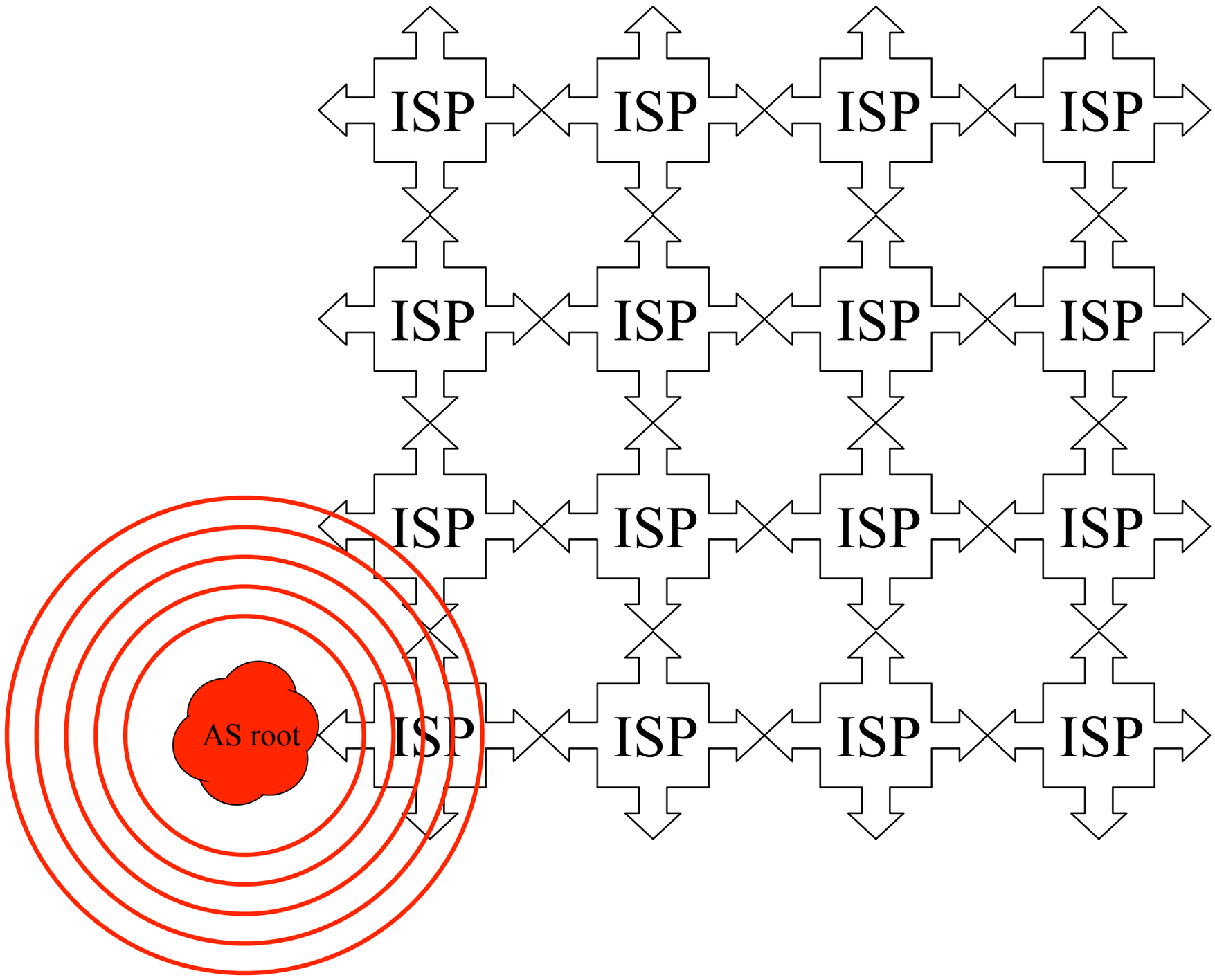
Provides Internet infrastructure services.

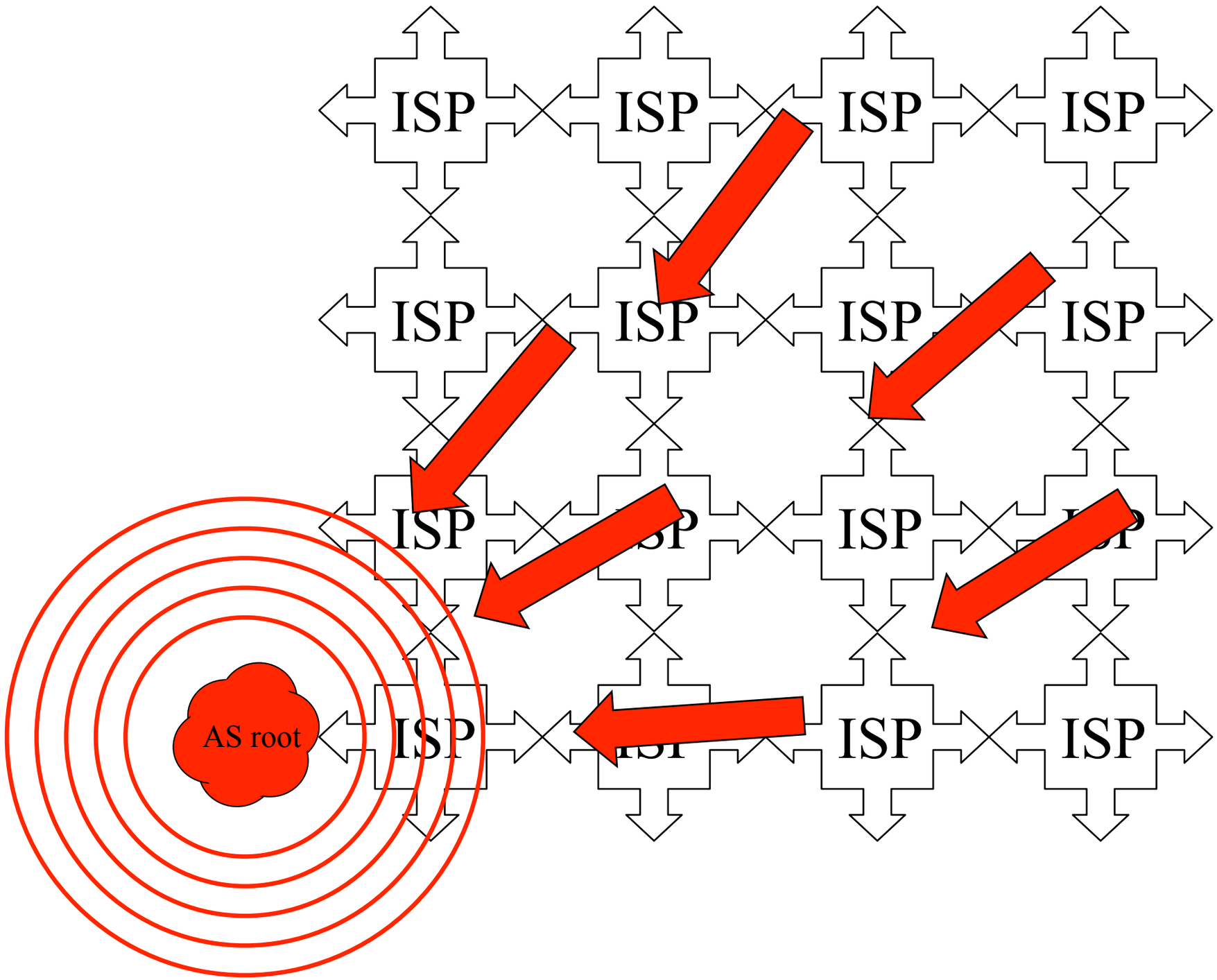
- **Internet exchange points in 6 locations.**
- **DNS authoritative service in 40+ locations using "anycast".**
  - **One of 13 root servers, i-root**
  - **Slave service for ~40 ccTLDs**
- **NTP-service in 4 locations**
  - **Stratum 1 clocks directly synchronised with Swedish stratum 0.**

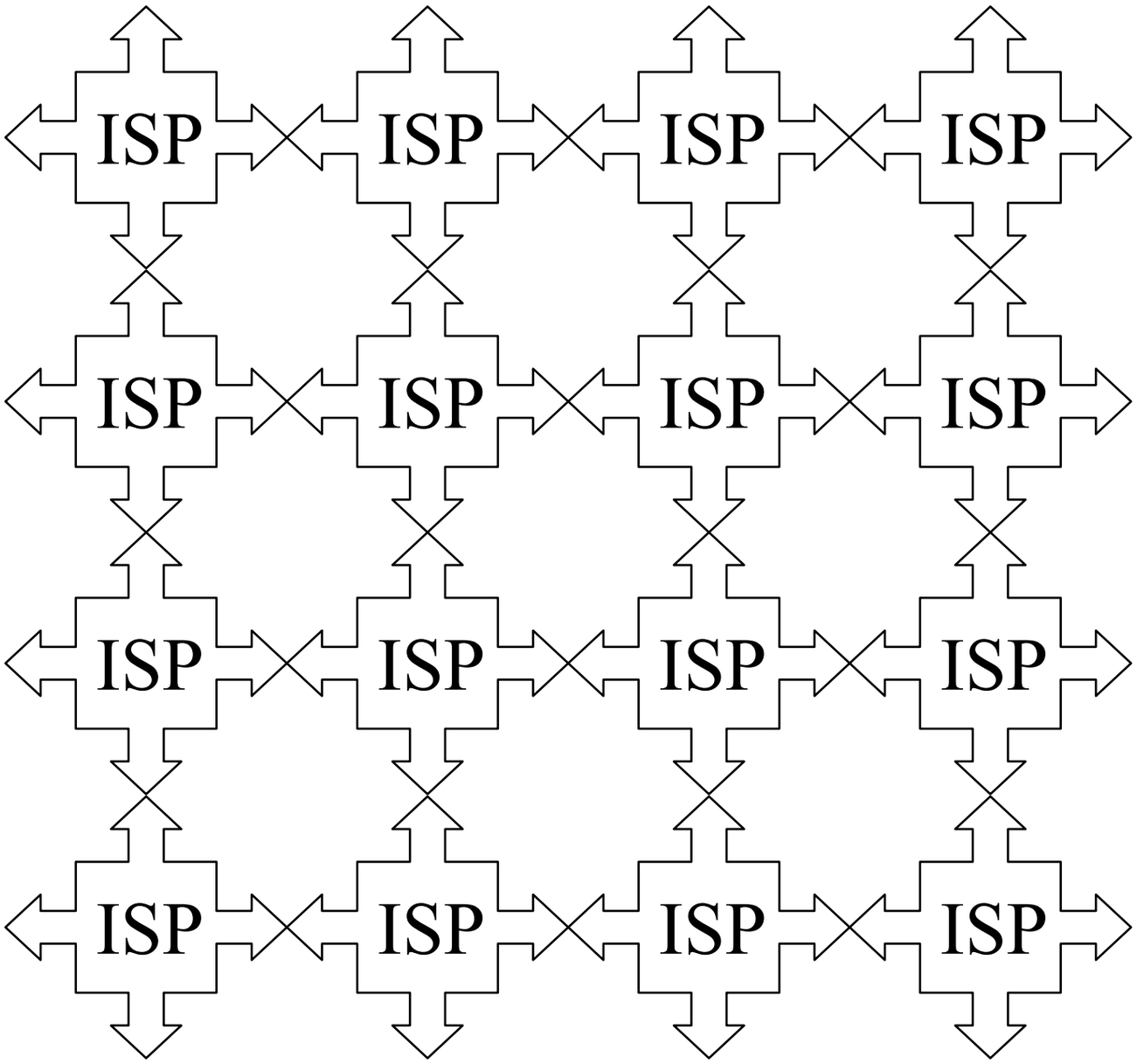


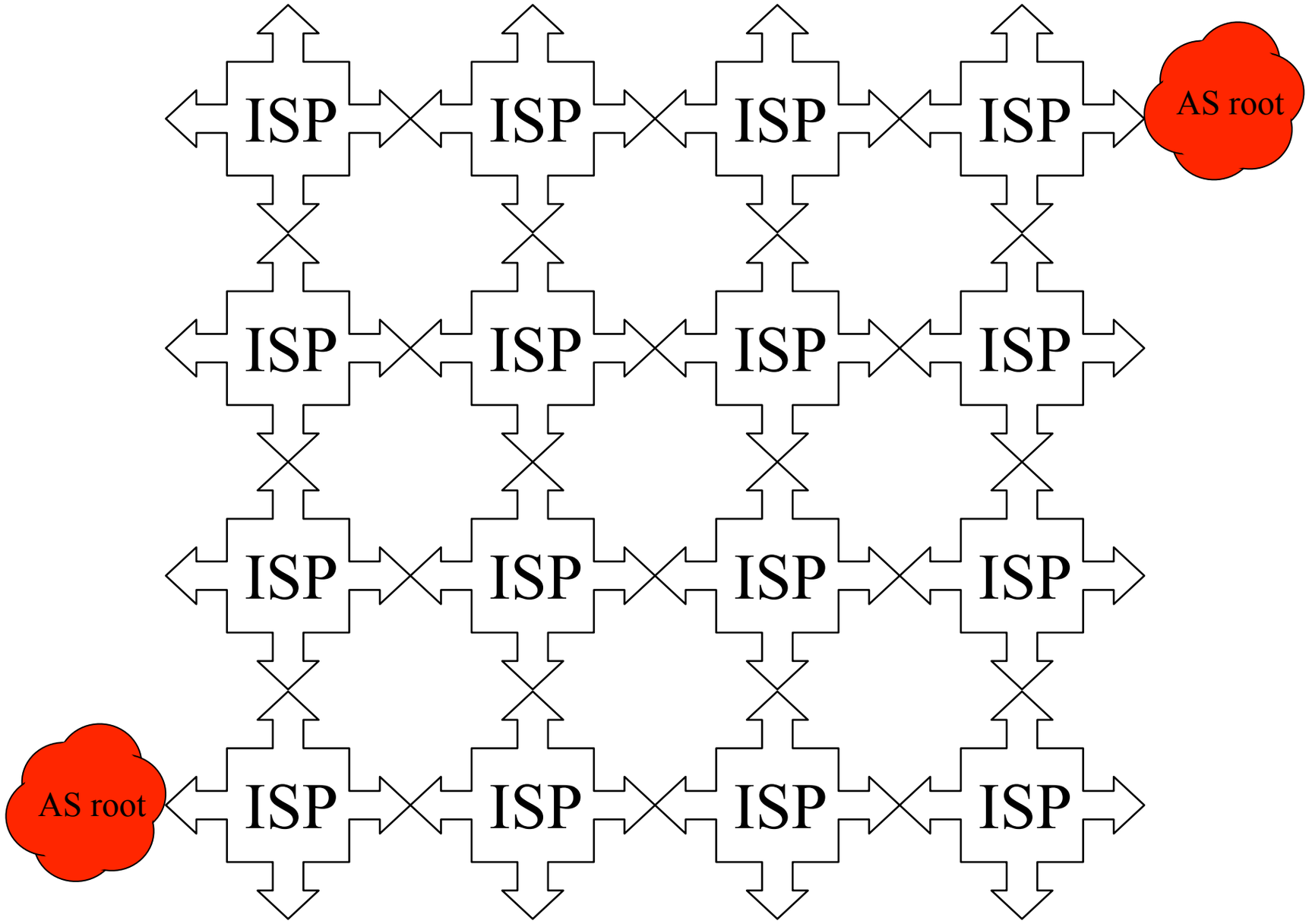

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP

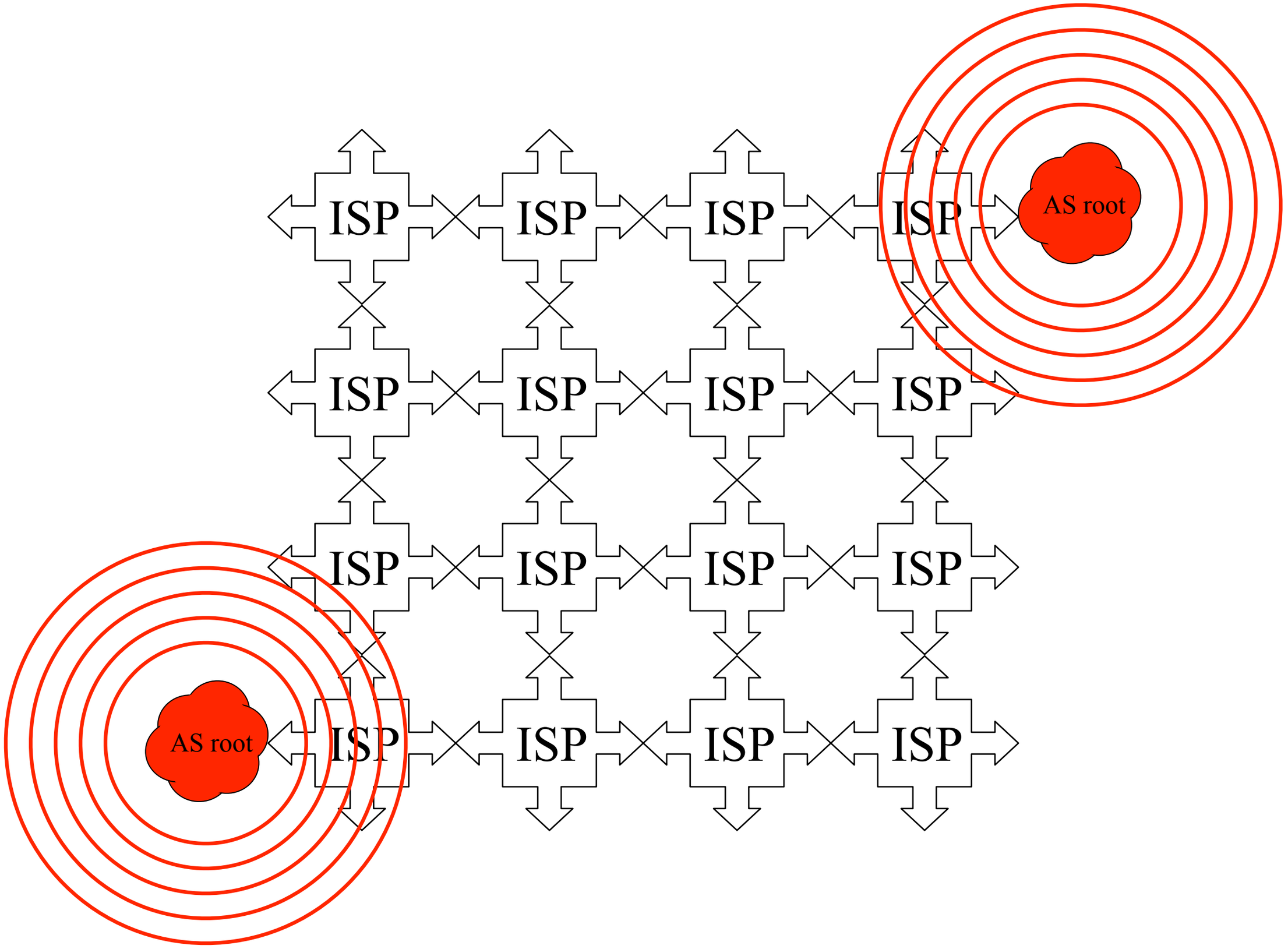

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root

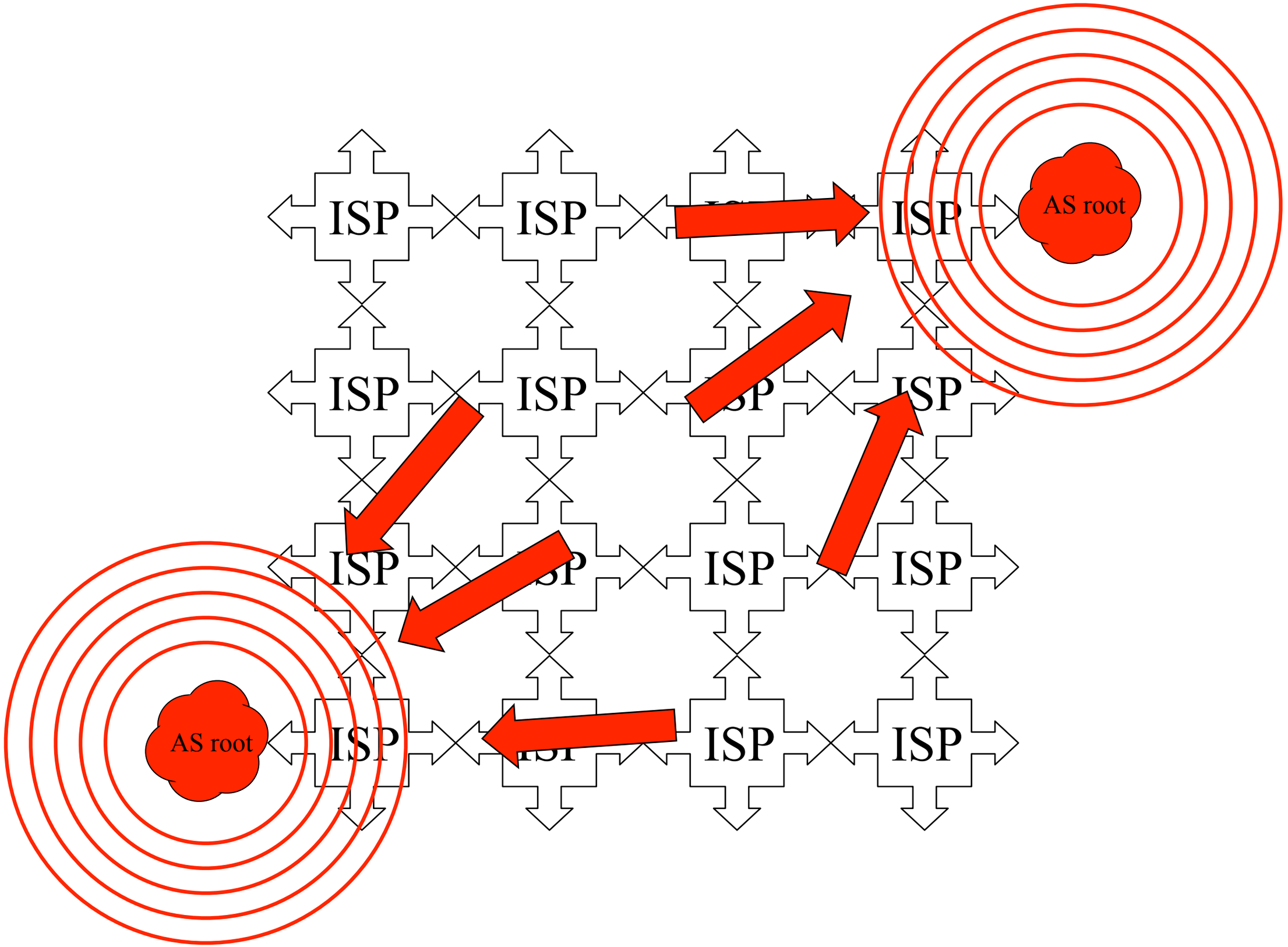

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root

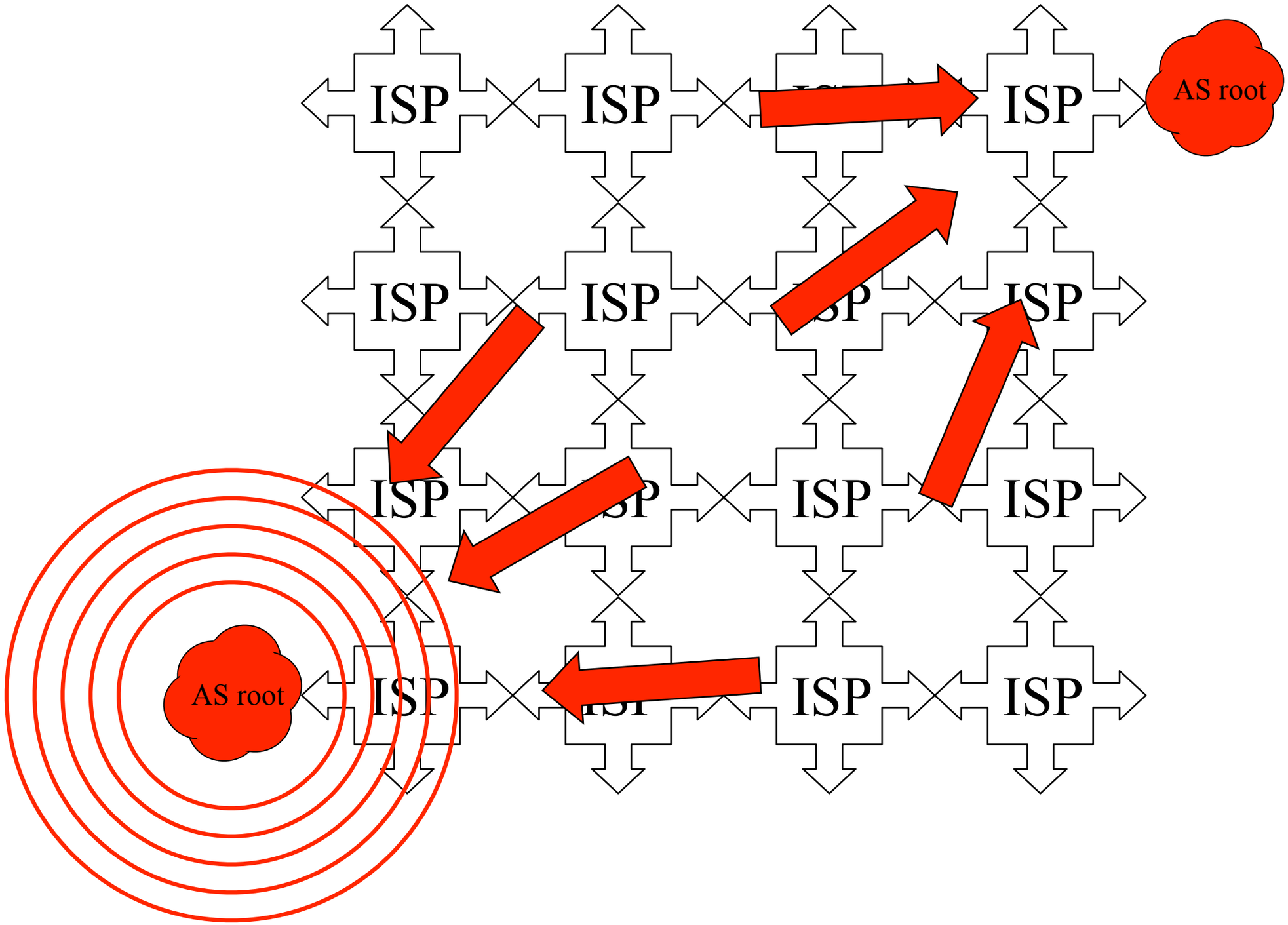

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
AS root

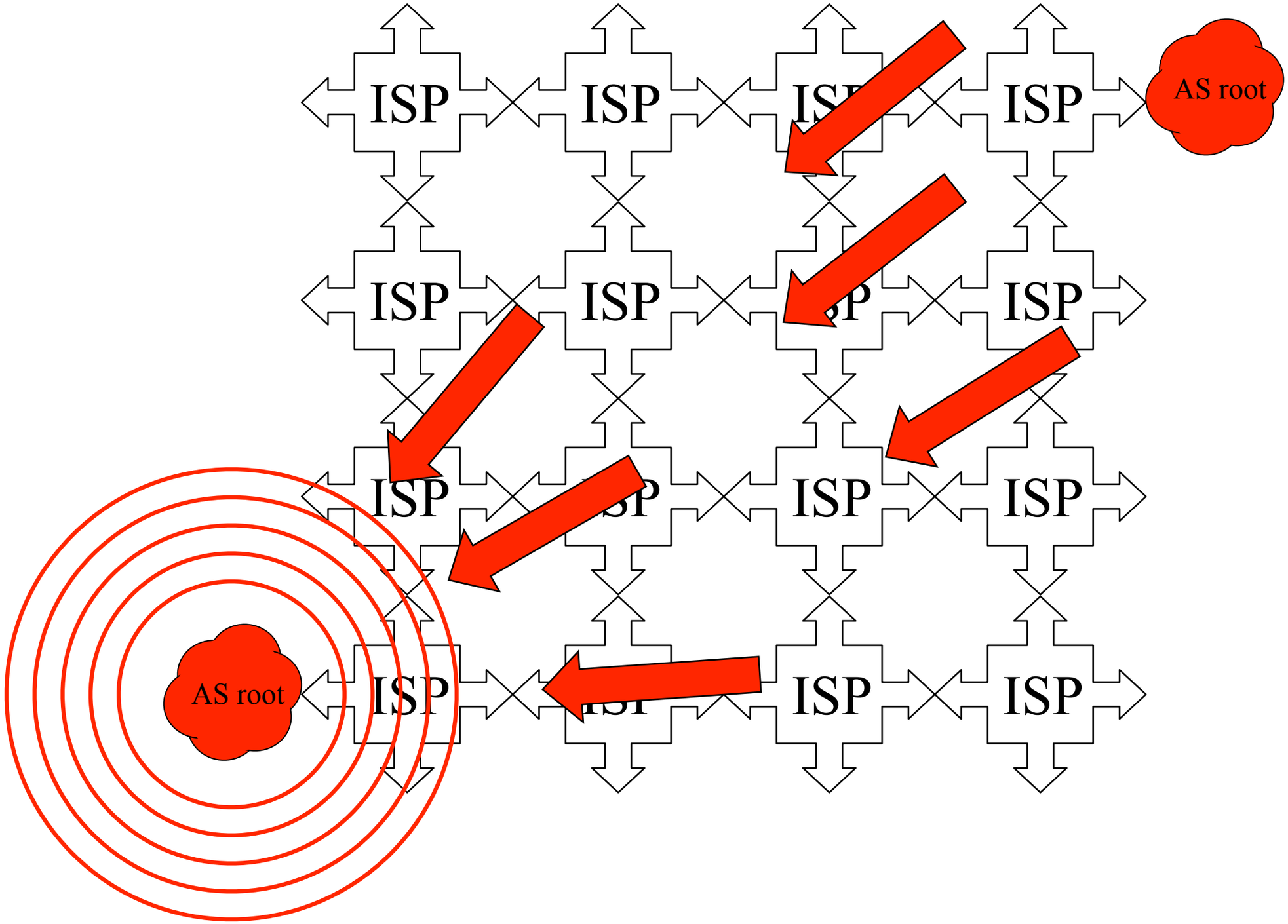

ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP


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


ISP
ISP
ISP
AS root
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

Denial of Service Attacks

As you probably know …

Denial of Service Attacks (DoS):

- Make someone's systems unusable by putting them under extreme load.
- … while not wasting your own resources.
- Create a software virus and build up a fleet of infected machines that act on your order, a.k.a. "bots".
  - This is sold as a service on the black market.
  - Controlled from a command and control center ("C&C") – often itself a bot.
  - Requires large botnets to be effective. Home computers often have limited upstream bandwidth, and you don't want the bandwidth consumption to give away that the computer is infected.
- Hmm … want more bandwidth …

Mirror attacks

Improve effectiveness of attack by involving an “amplifying mirror”.

- Small packet in – from a bot.
- Large packet out – towards primary victim.

Mirror becomes involuntary accomplice, but also a secondary victim.

Good mirrors are

- large servers
- with lots of upstream bandwidth
- serving old “insecure” protocols.

DNS: the perfect naïve accomplice!

- DNS uses UDP – no handshake between client and server. One packet to query, one (or a few) packets to respond.
- It's easy for bots to lie about the source address.
  - Not verified by Internet service providers! BCP 38 (RFC 2827) not enforced!
- DNS queries are considered "innocent".
- Traffic volumes are small (= unnoticed) for queries.
- Amplification is considerable.
  - E.g.: asking a .SE server for all records for "se." with DNSSEC enabled yields a 56x amplification (i.e., outgoing packets are (in total) 56 times bigger than the incoming packet).

Scenario 1: Classic network traffic overload

Attacker:

- Forged source IP address.
- General DNS query (probably requesting DNSSEC).

Mirror:

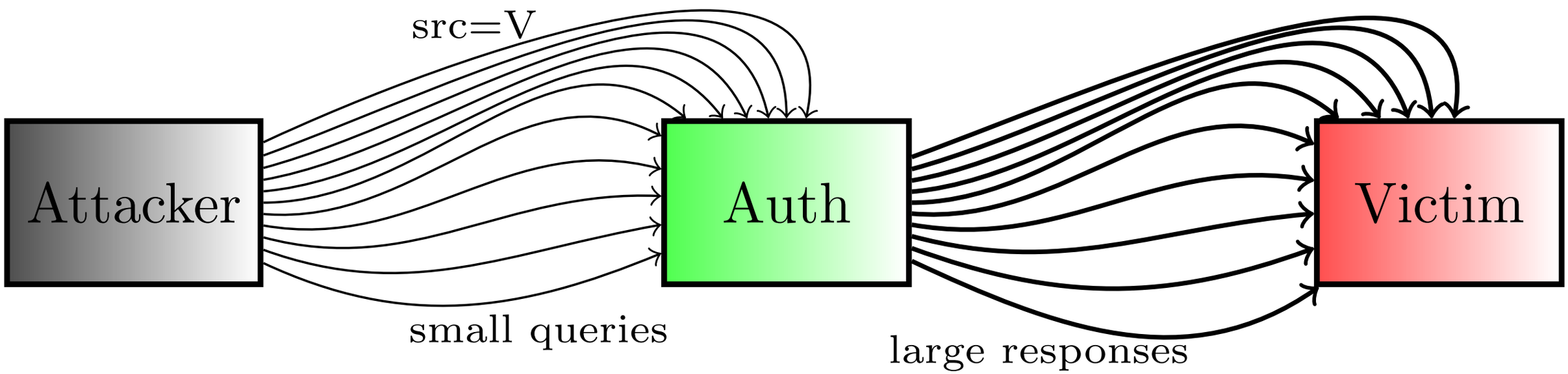
- DNS name server (authoritative or recursive).

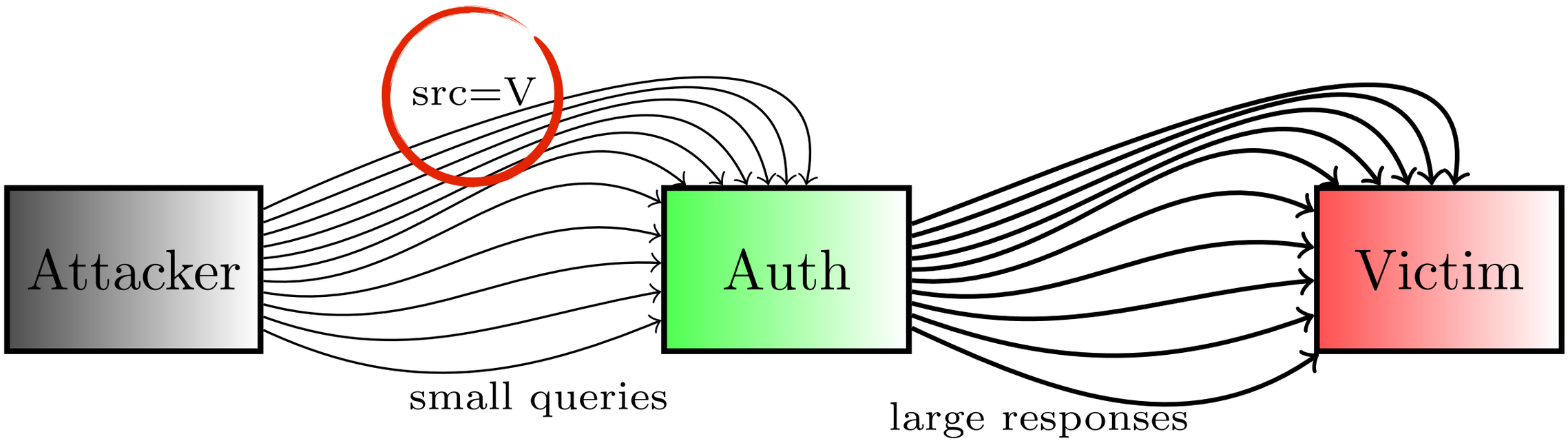
Target:

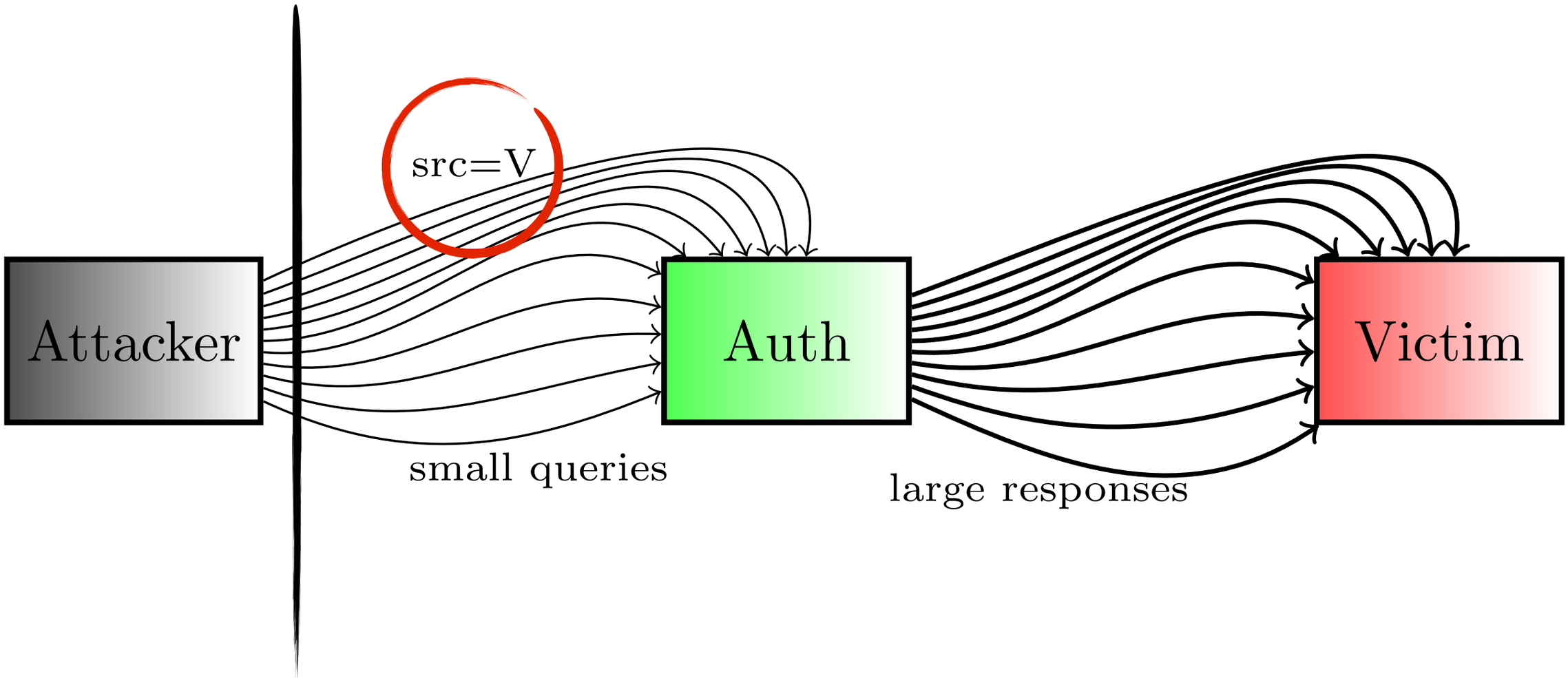
- Anything – web server, payment server, name server, telephony service.

Sought effect:

- Use raw “fire power” from DNS server to create network/packet/processing overload at target, thus depriving its users of service.


src=V
Attacker
Auth
Victim
small queries
large responses


src=V
Attacker
Auth
Victim
small queries
large responses


src=V
Attacker
Auth
Victim
small queries
large responses

Scenario 2: DNS overload

Attacker:

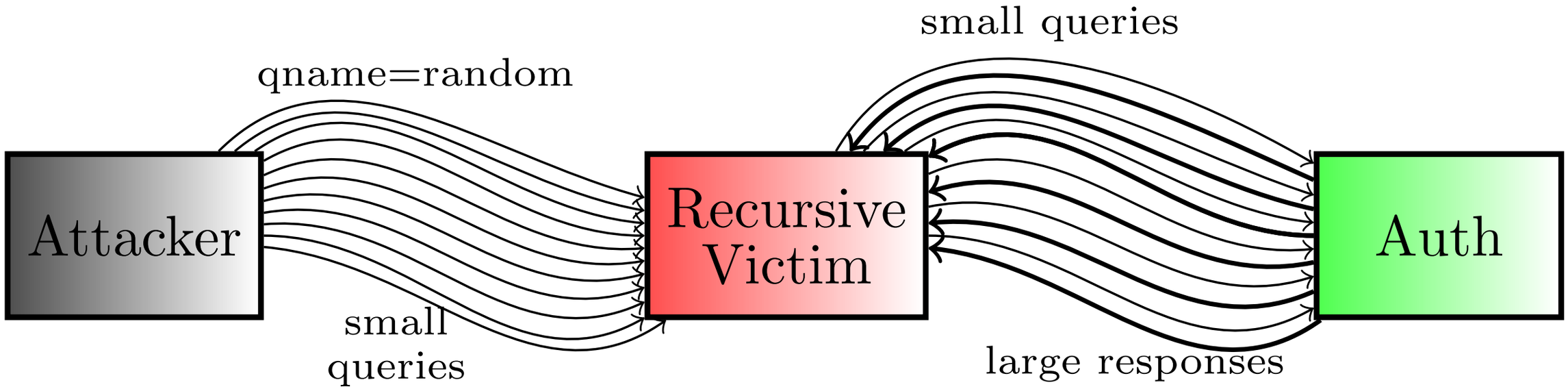
- Real or forged source IP address.
- General DNS query, random query string changing with every query.

Mirror = target

- DNS recursive name server (= victim).

Sought effect:

- Waste computational load on recursive DNS to create processing overload, thus depriving its users of service.


small queries
qname=random
Attacker
Recursive
Victim
Auth
small
queries
large responses

Scenario 3: Authoritative DNS server overload

Attacker:

- Typically botnet.
- Several forged source IP addresses matching existing recursive DNS server clients.
- General DNS query.

Mirror

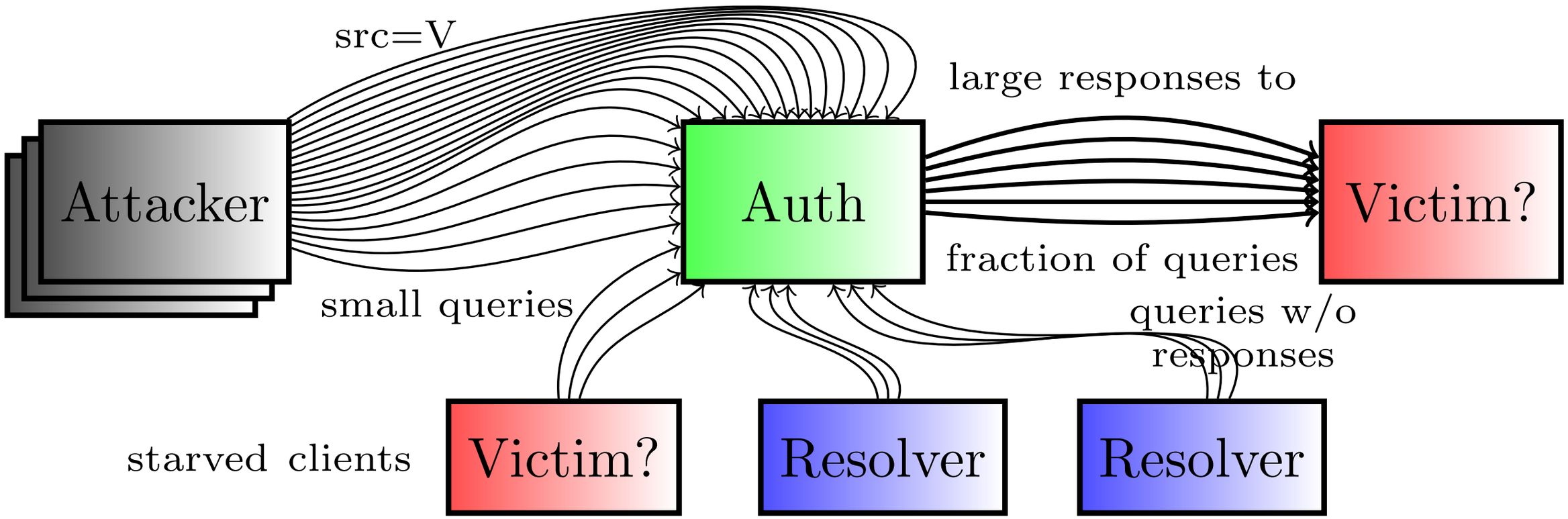
- DNS authoritative name server (which may or may not be the victim).

Target

- Authoritative DNS server or recursive DNS server clients.

Sought effect:

- Either to harm the authoritative DNS provider, or
- To "starve" recursive DNS server clients, hindering them from


src=V
Attacker
Auth
large responses to
Victim?
fraction of queries
small queries
queries w/o
responses
starved clients
Victim?
Resolver
Resolver

Root and TLD servers as mirrors

Root and TLD servers often chosen as mirrors, because

- High up in the food chain, easy to find.
- Overprovisioned due to DNS being primary business.
  - Lots of horse power.
- Well connected.
- Obliged to "love all, serve all".
- Often anycast --> distributed fire power.

(Crux: anycast is a way to defend against DDoS aiming at the root/TLD server, but increases problem when the attack aims at someone else.)

Ways to mitigate?

- Ingress filtering (BCP 38). Not much happening there ...
- Smaller packets? Go back from DNSSEC? Not feasible.
- Block traffic? Leaves innocent clients in the dark.
- Rate limit? Works ... sorts of.
- TCP? Yeah, would work for this particular class of problems, but has other baggage.

Efforts at Netnod

Technical:

- Monitor using our own monitoring systems.
  - Query load, BGP sessions, zone transfer delays, query delay (probes), etc ...
- Collect incoming queries at all anycast nodes continuously.
- PacketQ – flexible database tool to access and investigate query data.
- Rate limit incoming traffic for a few special cases, and on a customer by customer basis.
  - To protect our own systems, and thereby the service provided to our customers.
  - To the extent possible, always coordinate with the customer.
  - Manual configuration based on database investigations.
  - Looking at programmatic Response Rate Limiting (RRL).

Efforts at Netnod

Organisational/procedural:

- Participate in OARC DITL collections and submit data to provide research data.
- Maintain a close relationship with the DNS software community, and participate in the development of ideas and test new code (in our labs).
- Engage in DNS operations related fora, discussing new and improved procedures and best current practice.
- Coordinate with other root and TLD operators (no surprise).
- Establish channels to Swedish law enforcement, Europol, and Interpol.
- Be an active member in the Swedish National Telecommunications Coordination Group for crisis management.
- Have a strong presence in Internet governance circles.
  - IGF – MAG
  - ICANN – SSAC/RSSAC

The future?

Where's my crystal bowl when I need it ... ?

- Some more BCP 38. (Not much hope, though ...)
- More TCP based DNS traffic.
  - Challenge: provide for TCP base service. [Can be done.]
  - Challenge: get to a tipping point where we can turn off UDP.
- ... and we really need a "next generation DNS" ... or, rather, ... a next generation network based data lookup protocol.
  - Apart from IPv4 itself (and UDP and TCP), few active protocols outdate the DNS.

Thank you!

Lars-Johan Liman, M.Sc.
Senior Systems Specialist
Netnod

e-mail/xmpp/sip: liman@netnod.se
tel: +46–8–562 860 12

http://www.netnod.se/

This presentation will be available at

http://www.netnod.se/liman/presentations/denic/20130926-denic.pdf