

DNS Blocking

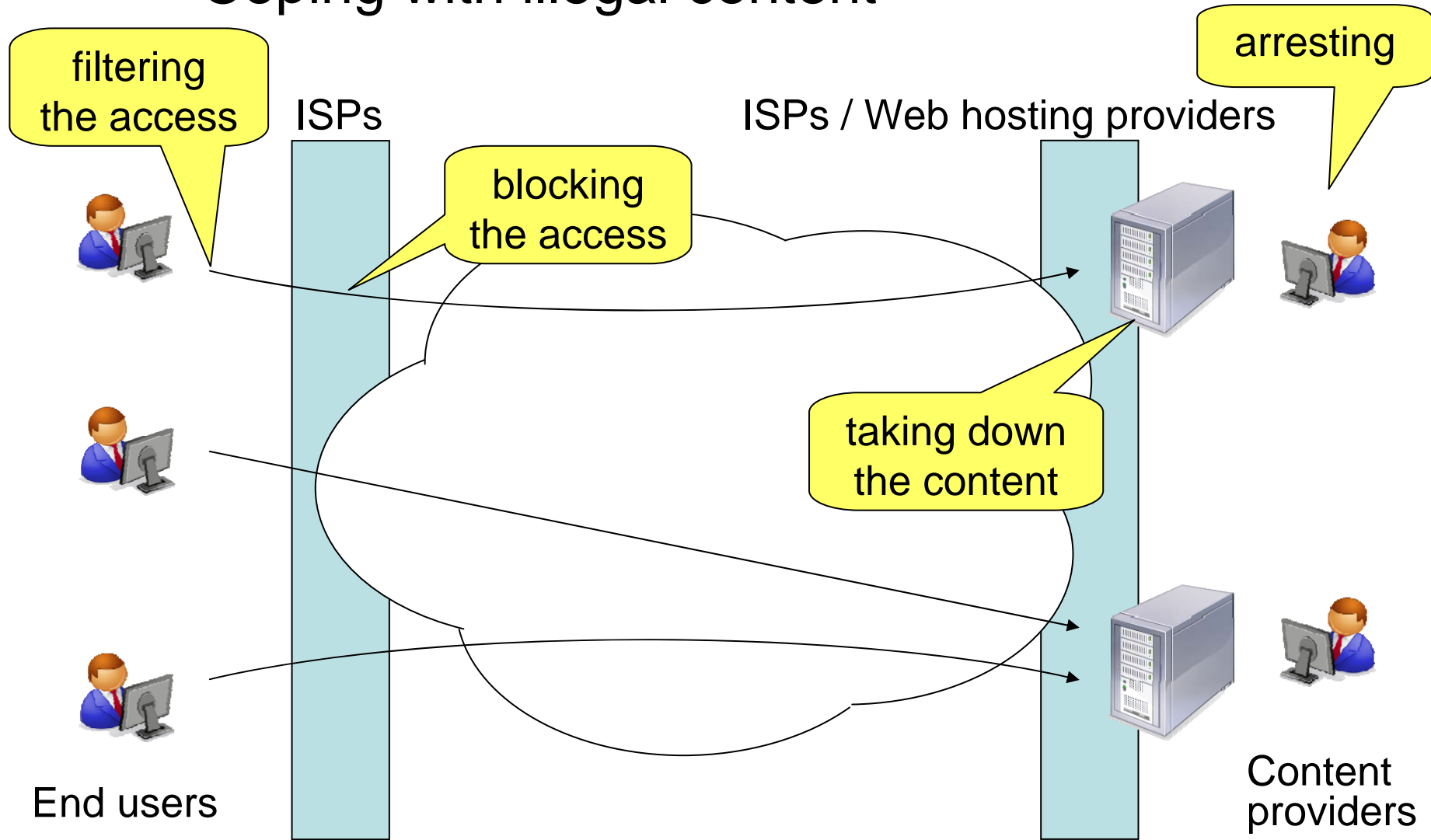
against illegal/inappropriate content

APTLD Meeting
November 1, 2010
Hiro Hotta, JPRS

Purpose of this presentation

- to share the status of DNS blocking against illegal content in Japan
 - still under investigation on what can/should be done by various players
- to share the concerns about DNS blocking

Coping with illegal content



Taking down the content

- Registry (JPRS)
 - informs the Registrar that the usage of the domain name under its management was reported illegal/inappropriate
 - asks the Registrar whether the registration information of the domain name is correct
 - ask the registrar to send a modify/delete request of the domain name to Registry if the domain name registration is inappropriate
- Registrars
 - follow the above procedure and/or
 - take down the web-site following their agreement with customers
- ISPs / Web hosting providers (they are Registrars in many cases)
 - usually have agreement with their customers prescribing "if its content is illegal or inappropriate, the web site is taken down"
 - take down web sites

Filtering the access

- ISPs
 - provide filtering services to its subscribers
- End Users
 - install filtering software to their PCs
 - subscribe filtering service from their ISPs

Blocking the access

- solution with most efficiency / effectiveness
- 4 ways have been suggested in the report from "child pornography prevention investigation team" in Japan
 - DNS poisoning
 - packet filtering (at devices such as routers)
 - blocking within proxy servers
 - hybrid filtering (e.g., DNS poisoning + proxy blocking)
- by DNS poisoning
 - overwriting the original DNS record with a record that navigates to a "warning page",
 - redirecting access to "an illegal/inappropriate web-page" to a "warning page" is achievable

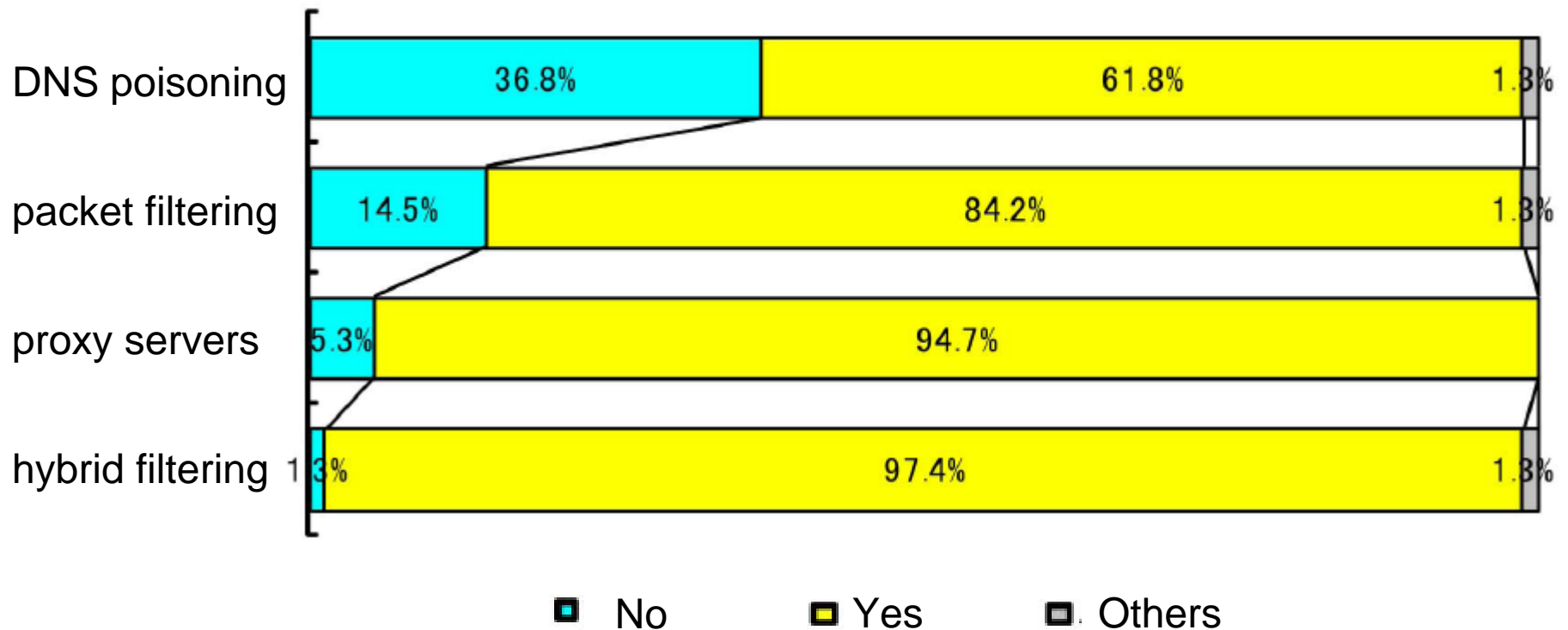
Blocking the access - continued -

- against "privacy of communications" established in "Constitution of Japan"?
 - without consent of communicating entities
- targeted especially at "child pornography"
 - at this moment
- ISP association basically agrees to the blocking because of
 - immense harm of the crime
 - technical feasibility of blocking
 - immediate blocking is avoided
 - order of "taking down" precedes "blocking"

Blocking the access - continued -

- the list of sites to be blocked is created and maintained by a private-sector organization
 - with help of police department and Internet Hotline Center
- concerns of ISPs
 - over-blocking
 - reliability of the list of sites to be blocked
- blocking is done without consent of
 - end users
 - content providers

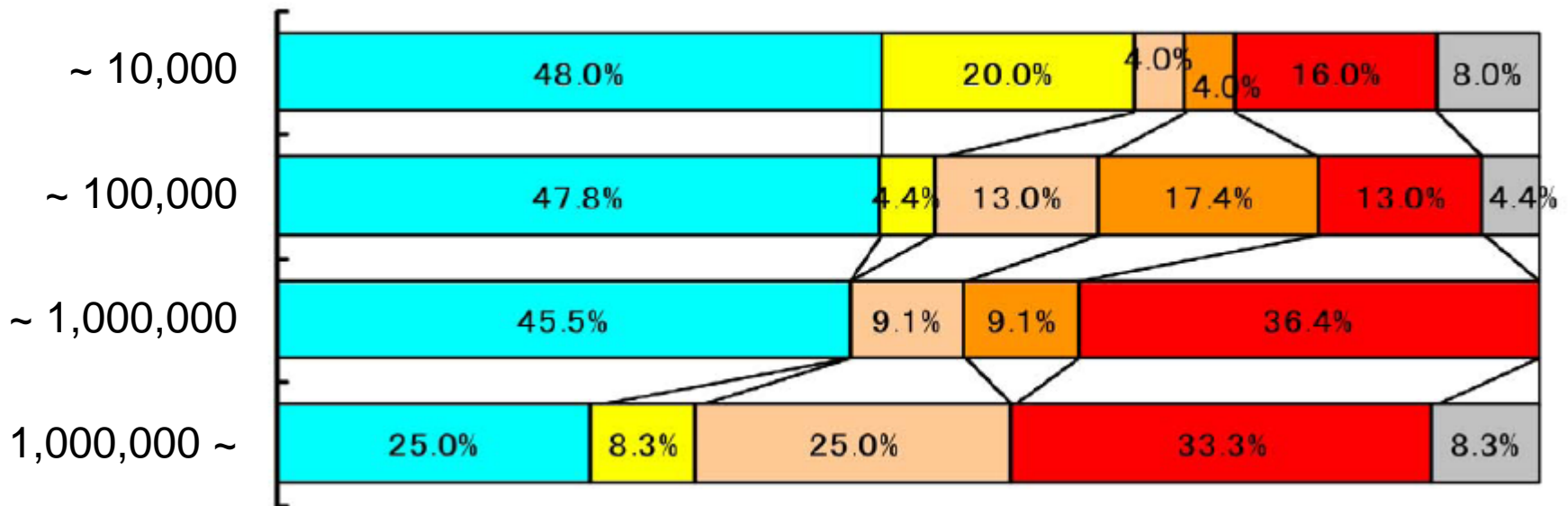
ISP survey (necessity of new investment on equipment)



source) meeting on blocking on the Internet, JAIPA
http://www.jaipa.or.jp/event/adla/100910_isp_swg.pdf

ISP survey (feasible solutions)

of subscribers



- DNS poisoning
- packet filtering
- proxy servers
- hybrid filtering
- none of them
- No answer

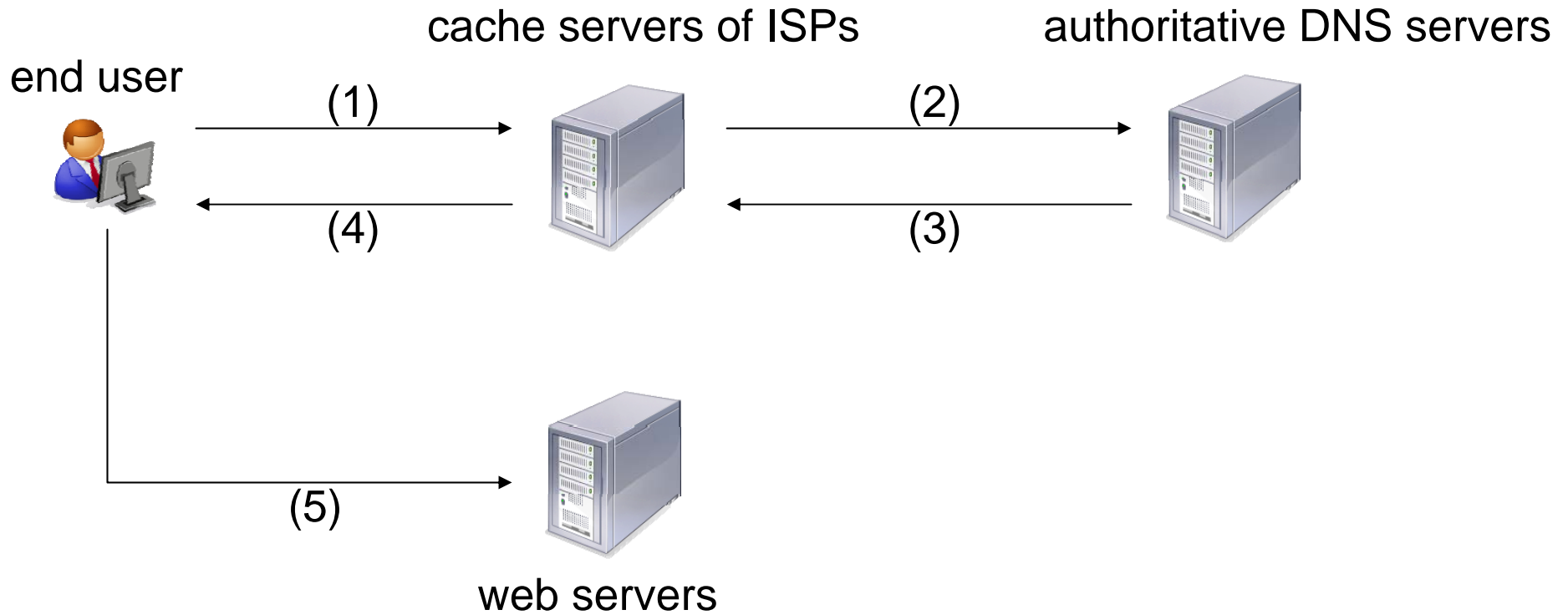
source) meeting on blocking on the Internet, JAIPA
http://www.jaipa.or.jp/event/adla/100910_isp_swg.pdf

DNS Poisoning for DNS blocking

- DNS poisoning is considered as the most promising way for ISPs
 - lowest cost
 - fast to introduce
 - especially initial cost for small ISPs is smallest
- results of the access to blocked pages
 - a "warning" page that some authority put up
 - by redirection of the access
 - a "page not existent" page that browsers display
 - by NXDOMAIN value

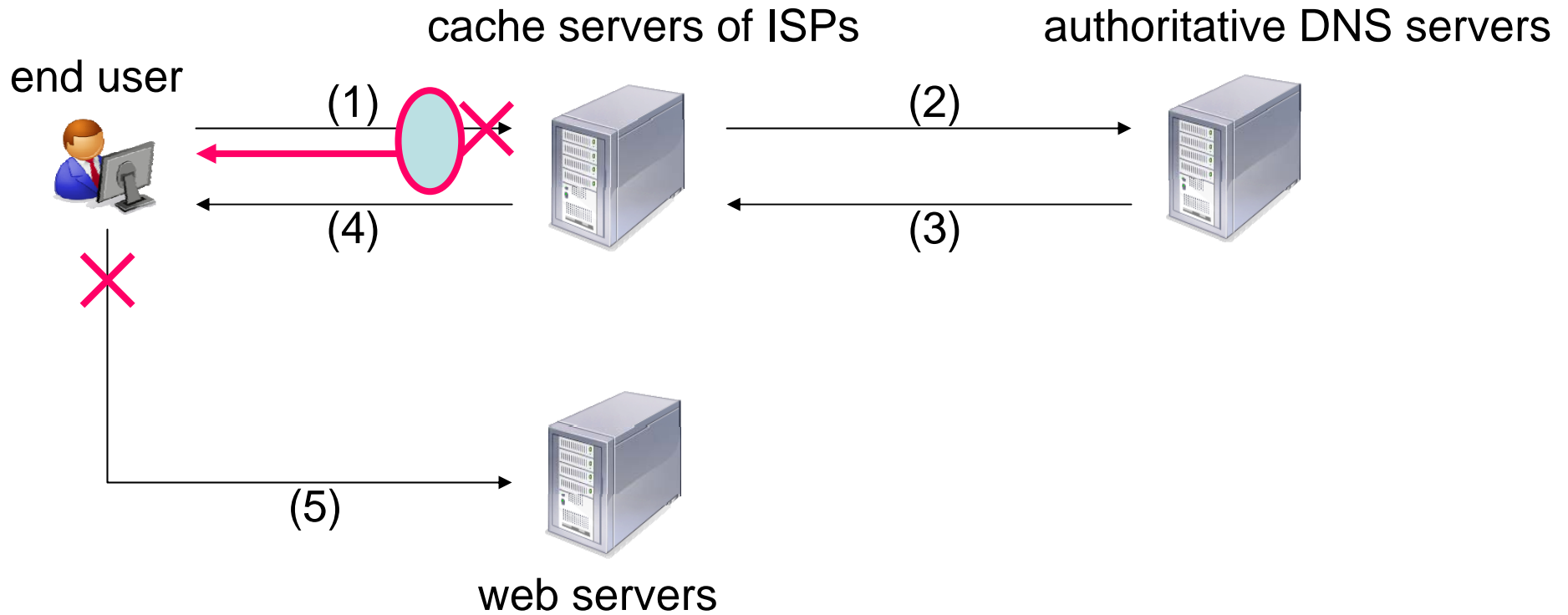
Points of DNS Blocking

<usual access>

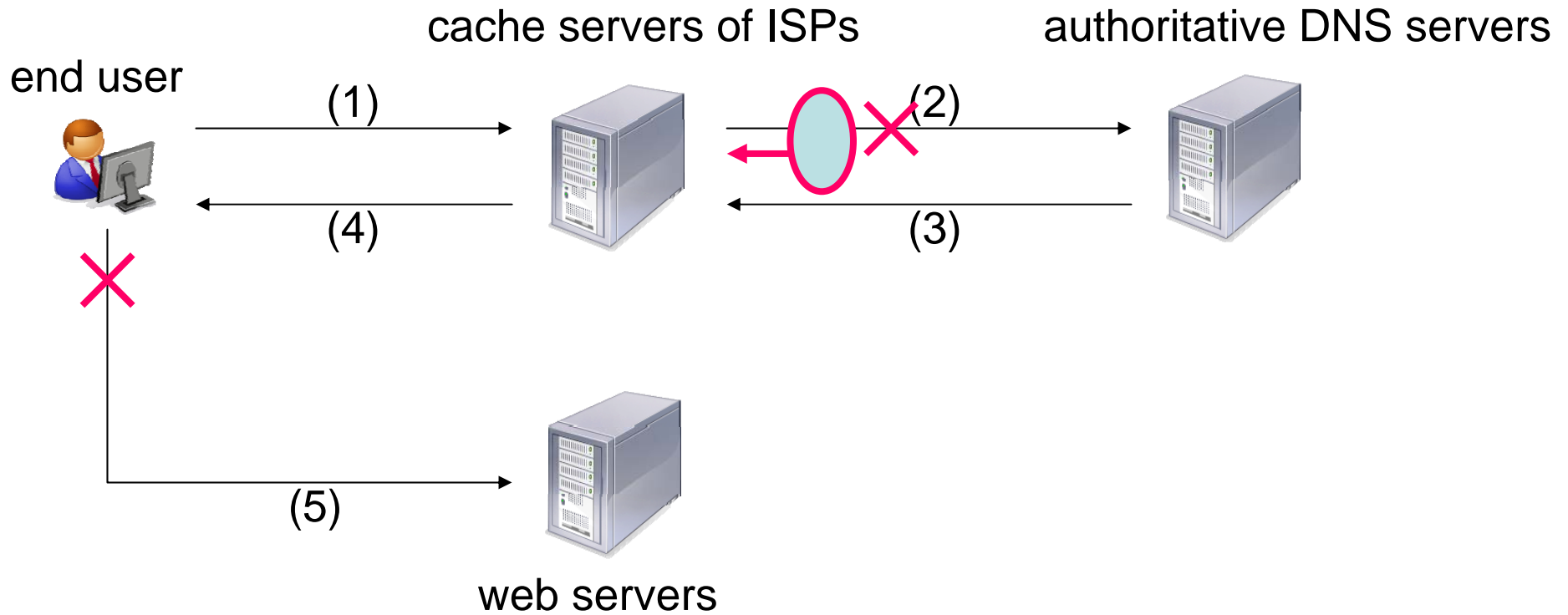


Points of DNS Blocking

<A>

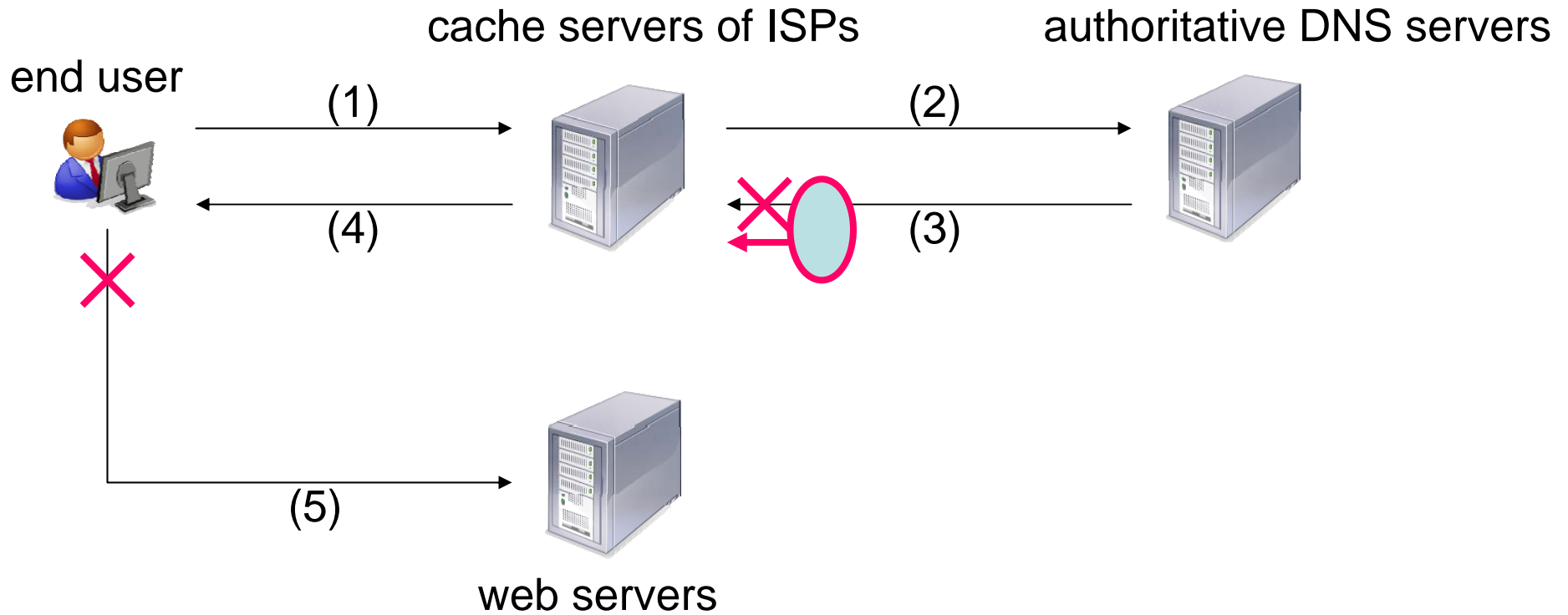


Points of DNS Blocking



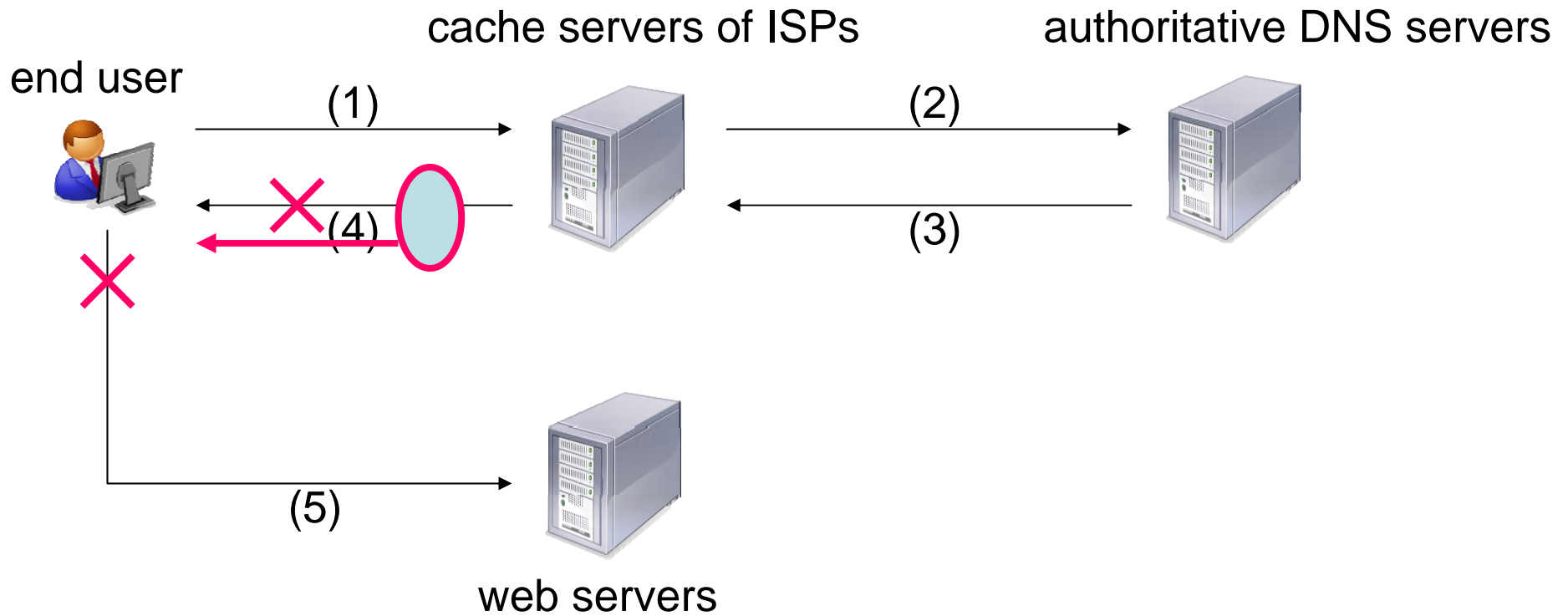
Points of DNS Blocking

<C>

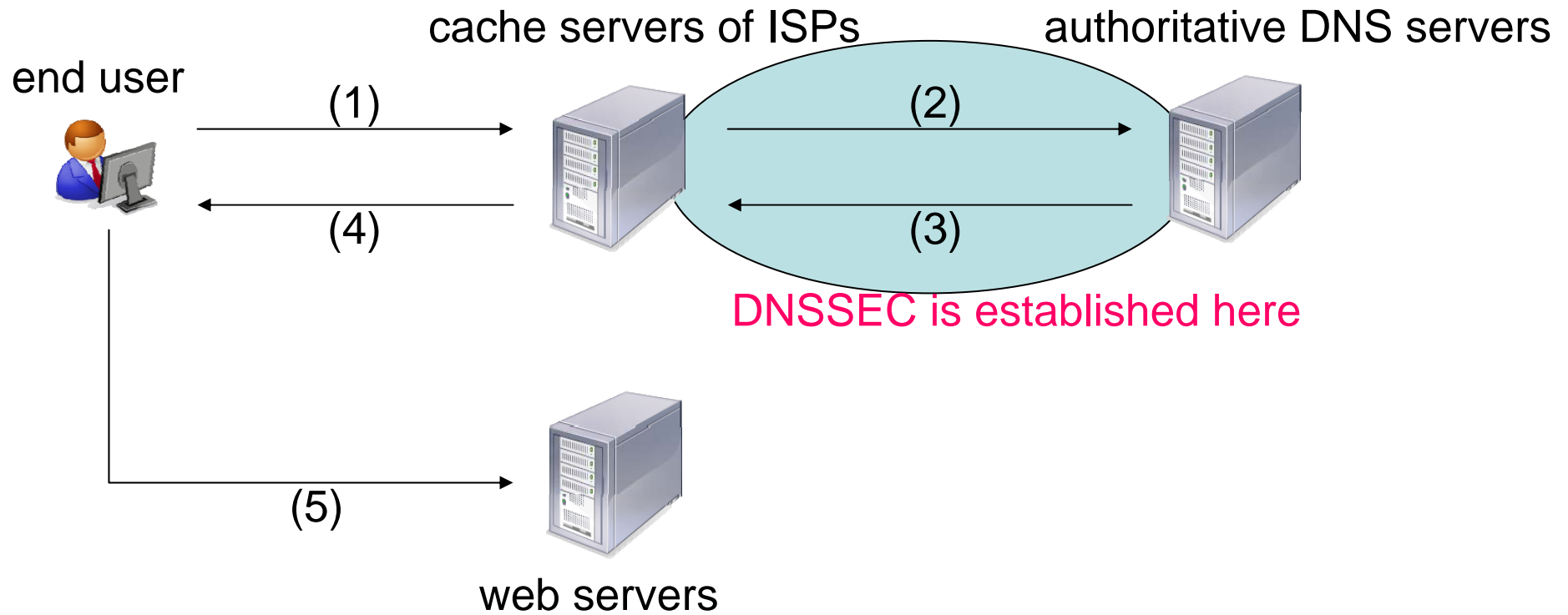


Points of DNS Blocking

<D>



DNSSEC



Incompatibility between DNS blocking and DNSSEC

- and <C> are incompatible with DNSSEC
 - breaking the trust chain
 - redirecting "access to illegal/inappropriate web-page" to a "warning page" is not achievable (just regarded as "nonexistent") (*)
- <D> is inefficient
 - discarding the result of elaborated DNS query-response
- so; <A> is most promising
- however the report from "child pornography prevention team in Japan" presents methods such as <C> and <D> as examples.

(*) some may argue that it doesn't matter whether web pages with illegal content results in "warning page" or "page not existent"

Worries of a Registry

- DNS data modification by DNS poisoning
 - authoritative DNS data are not the answers to the DNS queries - against registrants' will
 - can this win the understanding of registrants and end users?
 - blocking (by reason of content) should be done in upper layers than DNS?
- inconsistency between DNS blocking and DNS-layer services provided by Registries
 - registries must be heard in the process of finding solutions
 - but... want to stay away from content-level discussion - at least in early phases
 - but... uncomfortable with DNS level solution
 - and... incompatibility with other services must be avoided
 - anyway, JPRS published the way how DNSSEC and DNS blocking coexist

Q&A