Dealing with fragmentation in EDNS0
Proposal for a recommendation

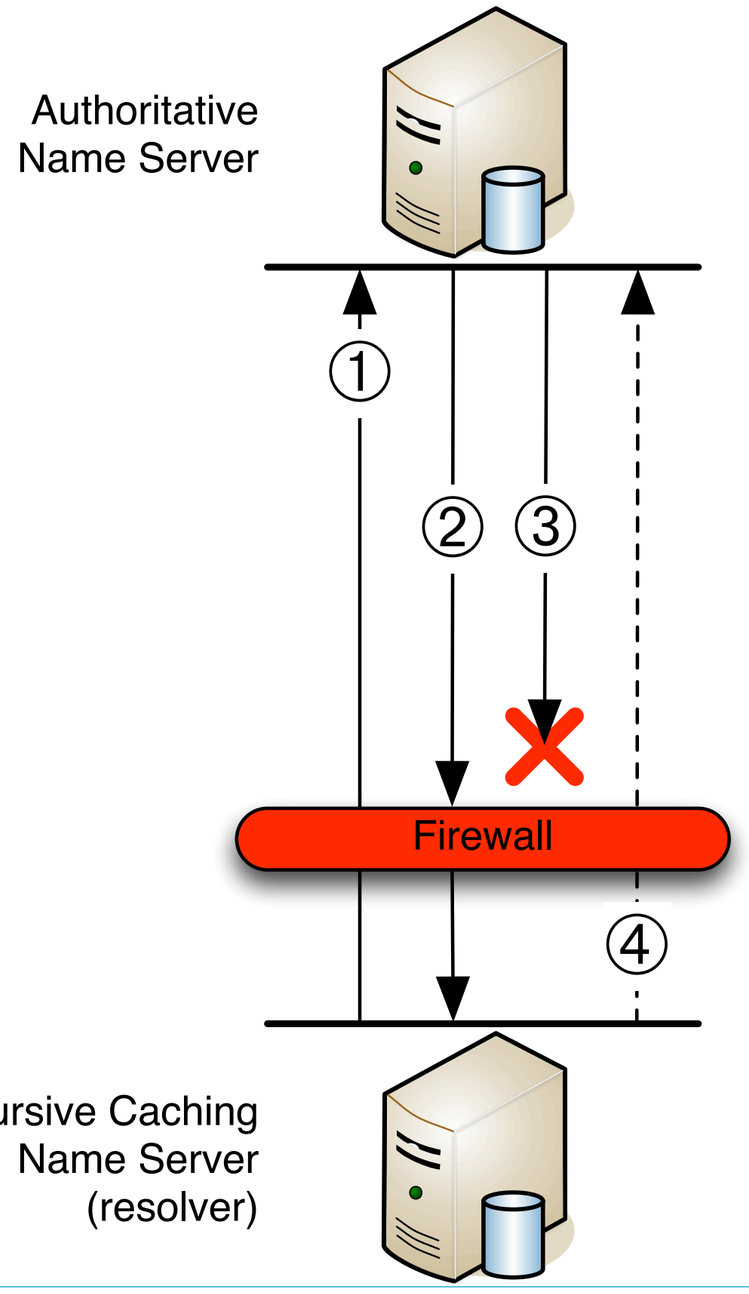
Sean McAfee (AP)

Roland van Rijswijk - Deij

roland.vanrijswijk@surfnet.nl

SURFNET

Problem recap



Extent of the problem

- 9% of all internet hosts may have problems receiving fragmented UDP messages [1];

- 2% – 10% of all resolving name servers experience problems receiving fragmented DNS responses [2]

[1] Weaver, N., Kreibich, C., Nechaev, B., and Paxson, V.: Implications of Netalyzr's DNS Measurements. In: Proceedings of the First Workshop on Securing and Trusting Internet Names (SATIN), Teddington, United Kingdom, (2011).

[2] Van den Broek, J., Van Rijswijk, R., Pras, A., Sperotto, A., "DNSSEC and firewalls - Deployment problems and solutions", Private Communication, Pending Publication, (2012).

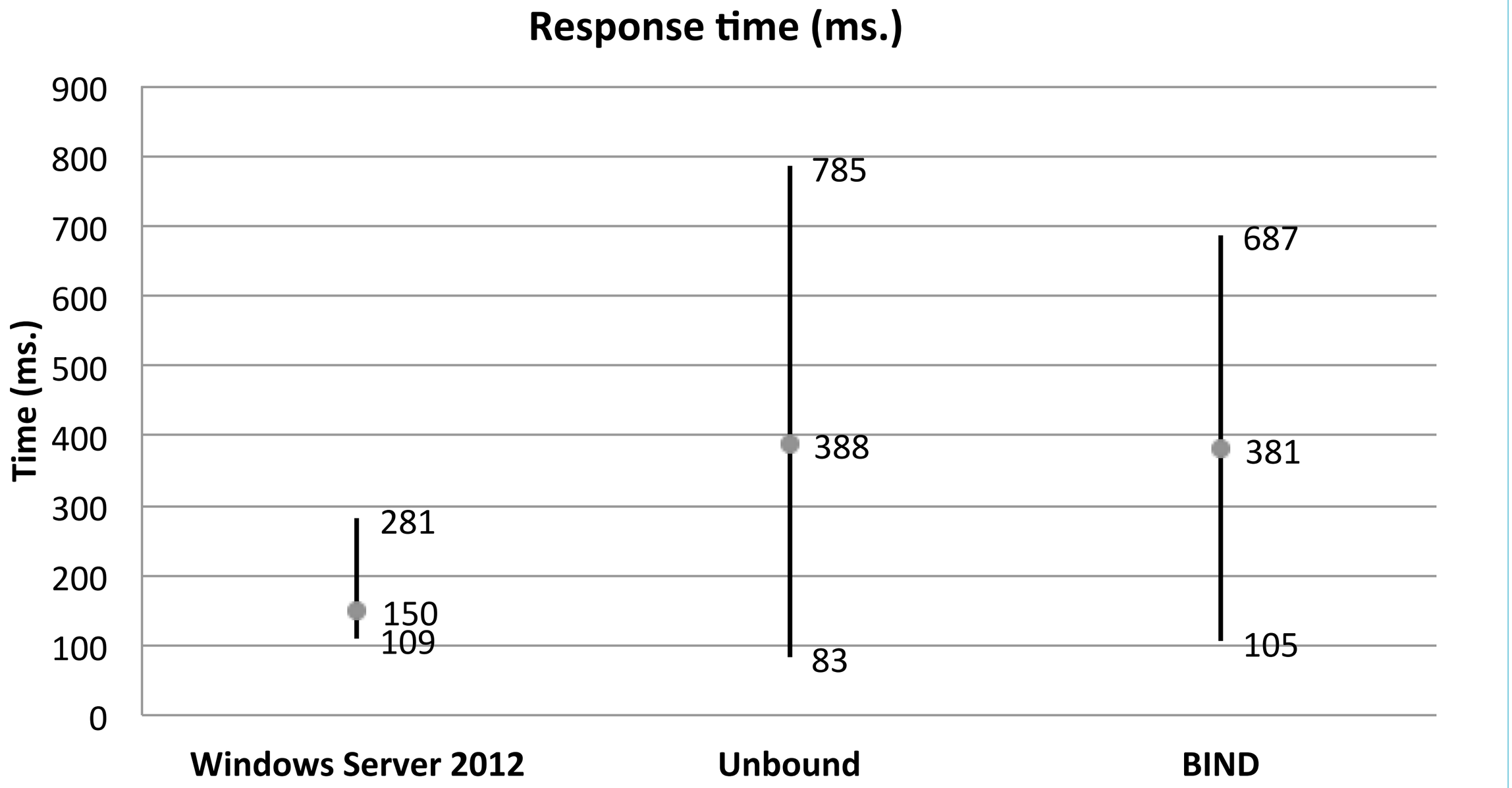
Solutions

- Resolving name servers should advertise a proper max. response size to avoid fragmentation issues [RFC 2671BIS (DRAFT)];

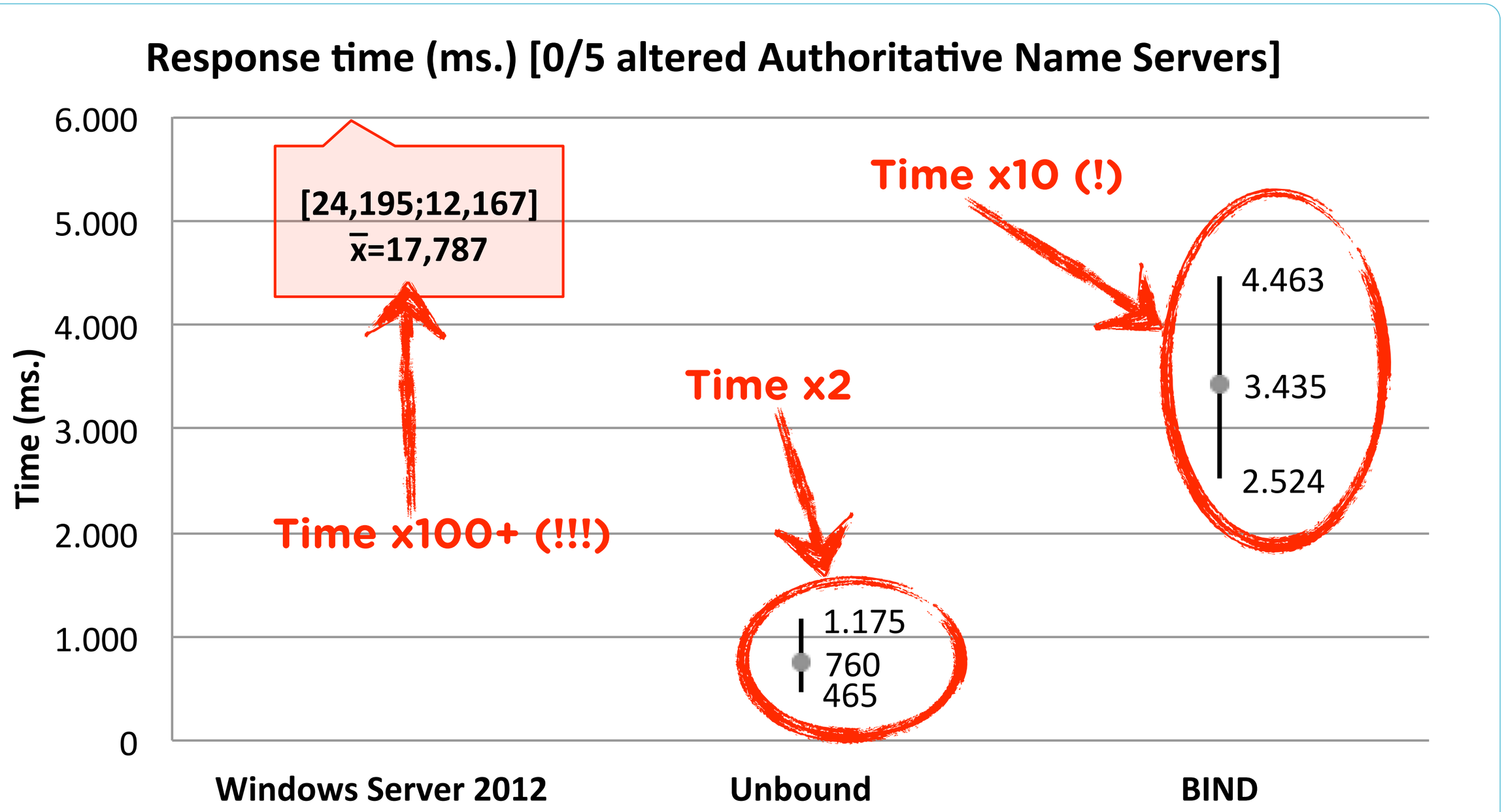
  Not explicitly stated in standards yet, nor widely implemented;

- Until then: set maximum response size at some authoritative name servers

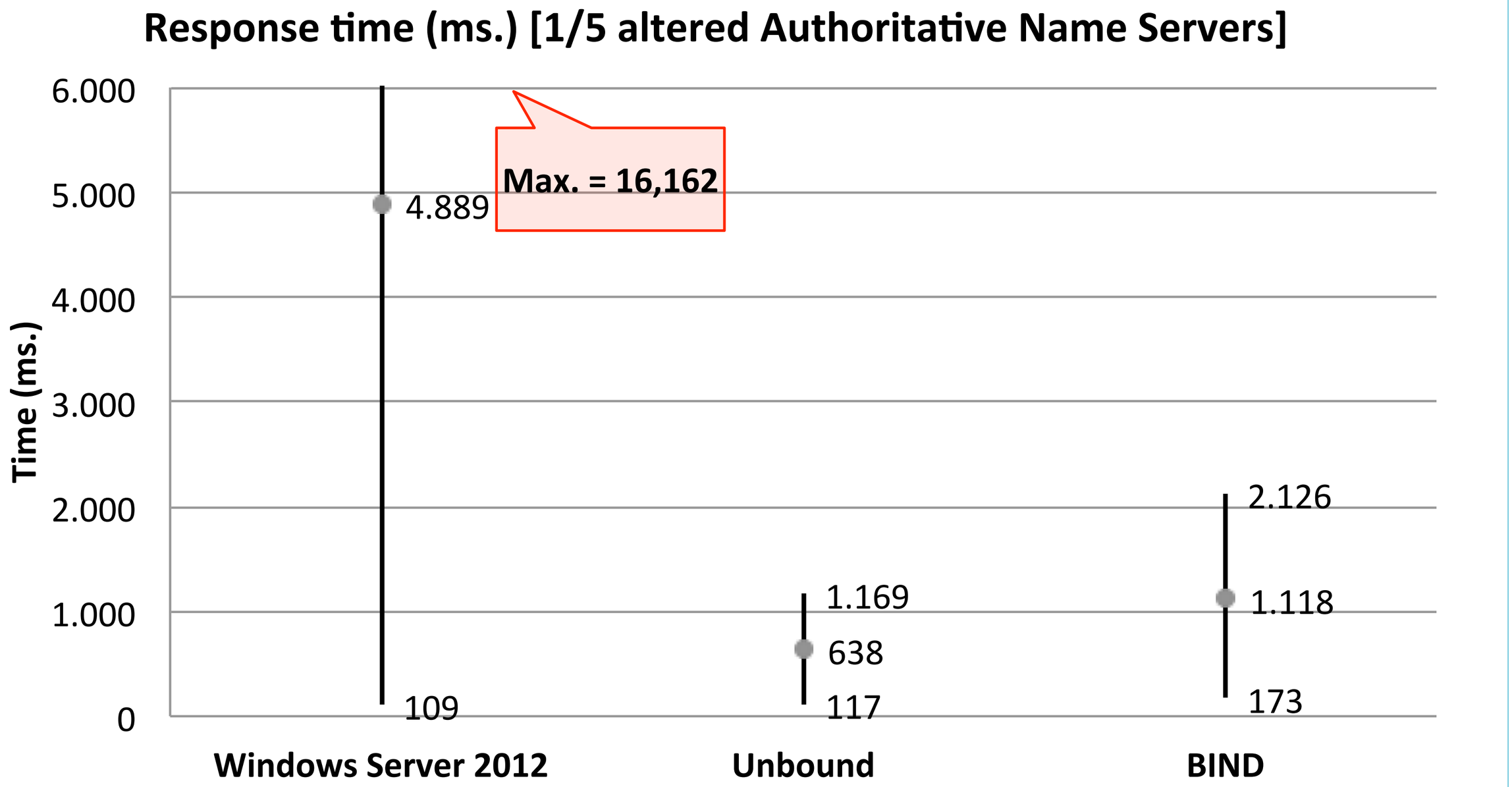
Resolver experiments (1)
Normal operations



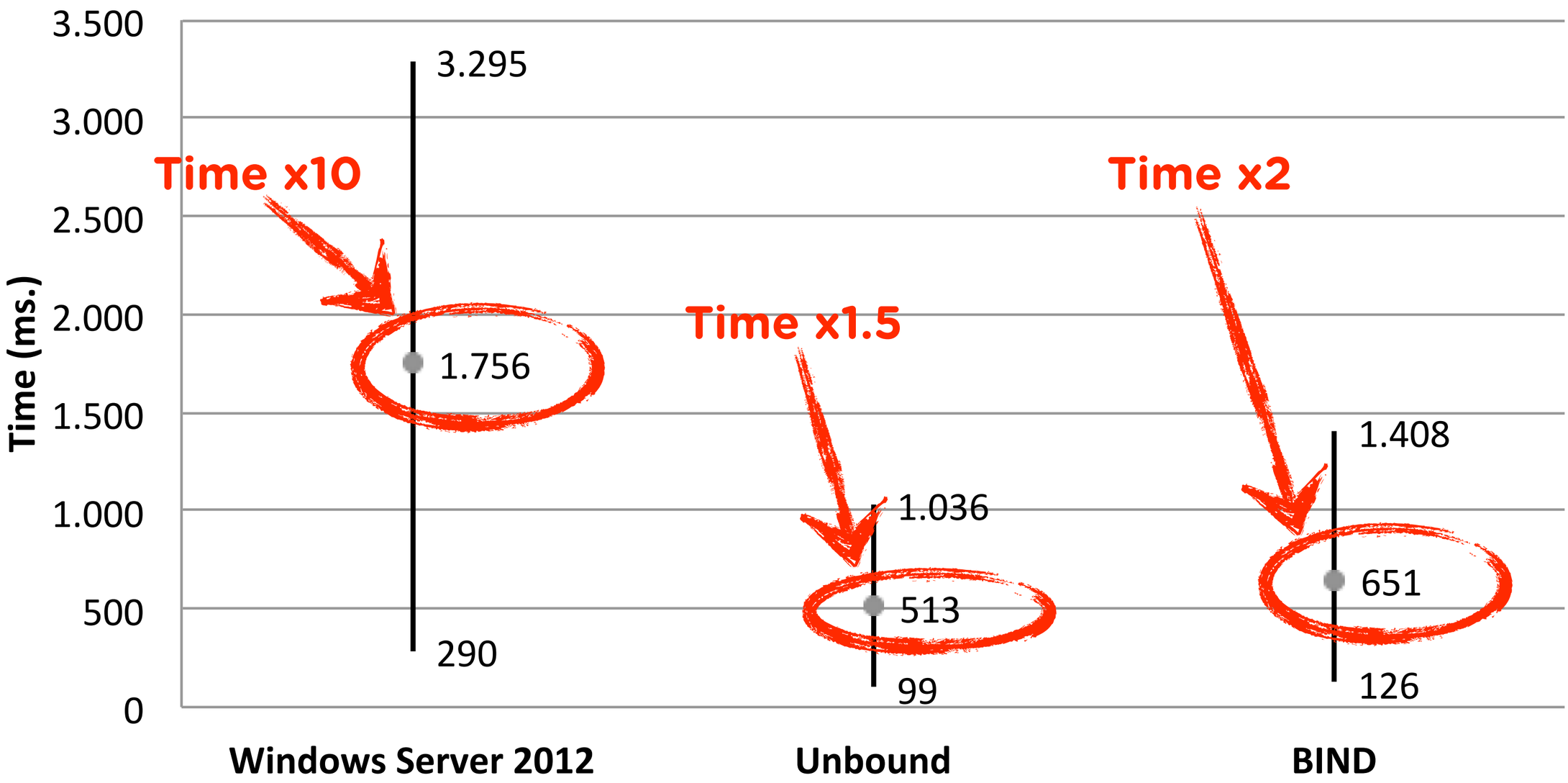
Resolver experiments (2)
Blocking fragments



Resolver experiments (3)
Max. resp. size on 1 authNS



Resolver experiments (4)
Max. resp. size on 2 authNS



Experiment on live authNS

Traffic (IPv4 + IPv6)	Normal Operations	Max. response size 1232 bytes
Fragmented responses	28.9%	0.0%*
Fragment receiving resolvers	57.3%	0.0%*
Truncated UDP responses	0.8%	0.9%
ICMP FRTE messages	5649/h	< 1/h*
ICMP FRTE sending resolvers	1.3%	0.0%*
Total retries	25.8%	25.5%

*Statistically significant difference between experiments

Rise in truncated answers

- Experiment:
  - Querying 995 zones in .com, .edu, .mil, .net and .nl
  - All zones are signed and have a www-node
  - Results:

Max. response	A for www	AAAA for www	DNSKEY
4096	0.0%	0.0%	0.0%
1472	1.8%	1.8%	8.1%
1232	2.9%	3.5%	**40.0%**

  - 30% truncations were expected for a maximum response size of 1232 bytes by Rikitake, K., Nogawa, H., Tanaka, T., Nakao, K. and Shimojo, S. “An Analysis of DNSSEC Transport Overhead Increase”, IPSJ SIG Technical Reports 2005-CSEC-28, Vol. 2005, No. 33, pp. 345-350, ISSN 0919-6072, 2005

Proposed recommendation

1. At least 50% of all authoritative name servers for a zone **SHOULD** be set to limit the overall response size to 1472 bytes, but **MAY** be set as low as 1232 bytes;

2. At least 50% of all in-zone authoritative name servers for a zone **SHOULD** be set to limit the overall response size to 1472 bytes, but **MAY** be set as low as 1232 bytes;

3. Authoritative name servers to which the above recommendations are applied **MUST** accept DNS queries over TCP.

roland.vanrijswijk@surfnet.nl

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

Questions? Remarks?