

ICANN86 Policy Forum in Seville, Spain

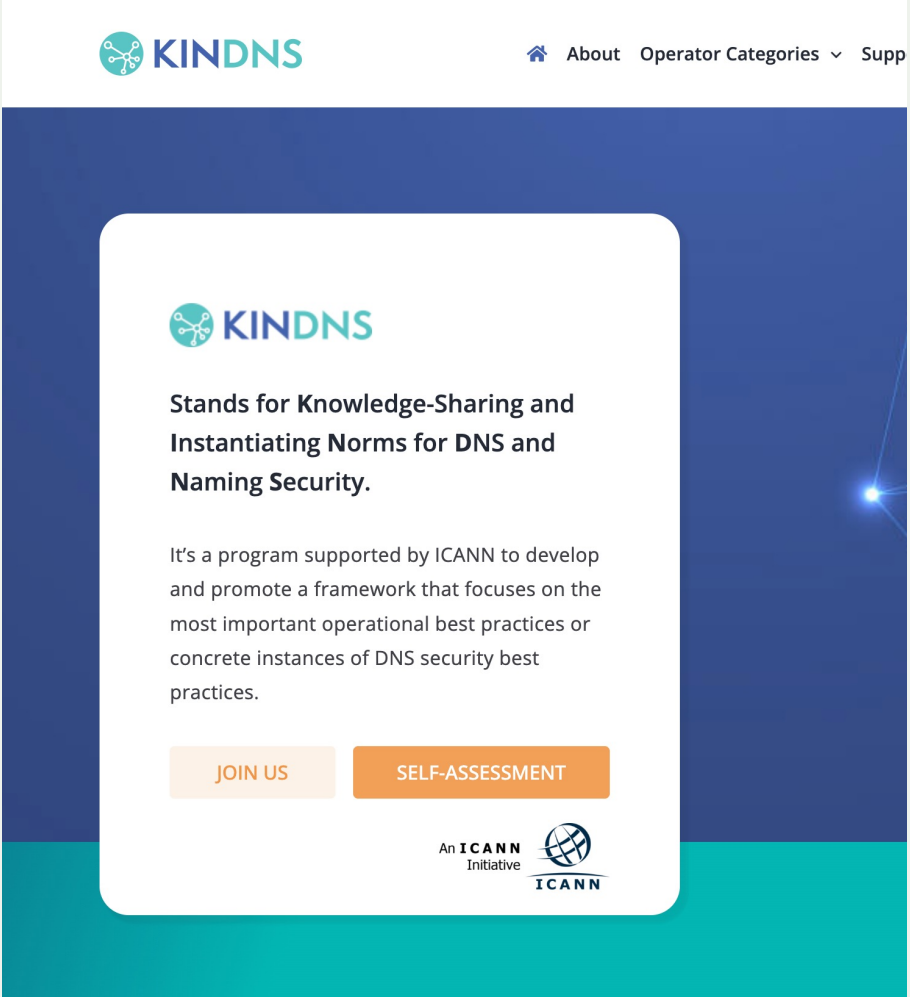
Evidence-based DNS Resilience

Amreesh Phokeer



DNS Resilience

- Internet is increasingly hosting mission-critical applications and services
- Regulations such as NIS2 (EU) and CSF2 (US) to protect critical infrastructures
- We use the KINDNS framework to evaluate the measurable practices of DNS Resilience (both authoritative and recursive)

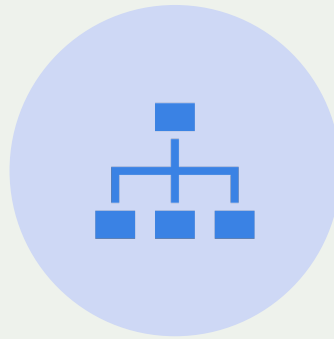


The screenshot shows the KINDNS website landing page. At the top left is the KINDNS logo, and at the top right are navigation links: a home icon, 'About', 'Operator Categories' with a dropdown arrow, and 'Supp'. The main content area has a dark blue background with a white rounded rectangle in the center. Inside this rectangle, the KINDNS logo is repeated, followed by the text 'Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.' Below this is a paragraph: 'It's a program supported by ICANN to develop and promote a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.' At the bottom of the white rectangle are two orange buttons: 'JOIN US' and 'SELF-ASSESSMENT'. In the bottom right corner of the white rectangle is the ICANN logo with the text 'An ICANN Initiative'.

Resilience metrics



MEASURABLE VS NON-MEASURABLE PRACTICES



ORGANIZATIONAL PROCESSES ARE USUALLY NOT MEASURABLE






FOCUS ON OBSERVABLE CHARACTERISTICS



Authoritative DNS Resilience



KINDNS Measurable practices

Authoritative Server operators	TLDs, SLDs and Critical Zones
Practice 1 – DNSSEC and Key management	Covered
Practice 2 – Limited zone transfer	Covered
Practice 4 – Authoritative and recursive on different servers	Covered
Practice 5 – Two distinct name servers	Covered
Practice 6 – <ul data-bbox="264 1070 831 1254" style="list-style-type: none">• Software diversity • Network diversity • Geographic Diversity 	Partly

Different **measures** for different threats

Metric	Resilience against	Dataset
# auth. NSes	node failures	active scans [5]
# IP addr. of auth Nses	node failures	active scans [5]
# of ASes of NS IP addr.	routing issues	PFX2AS [6]
# of anycast addresses	site failures, DDoS	MANycast2 [4], IPInfo [7]
# of TLDs of NS names	NS parent zone failures	active scans [5]
# of server locations	site failures, geofencing	IPInfo Location [7]

[4] Sommesse et al., "MANycast2: Using Anycast to Measure Anycast", IMC, 2020

[5] Steurer et al., "A Tree in a Tree: Measuring Biases of Partial DNS Tree Exploration ", PAM, 2025

[6] CAIDA UCSD, RouteViews prefix2as dataset. <https://www.caida.org/catalog/datasets/routeviews-prefix2as/>, 2008

[7] IPInfo, *Trusted IP Data Provider from IPv6 to IPv4*. <https://ipinfo.io>, 2025

Data Collection

- **ct**: Names from unexpired certificates from Certificate Transparency logs: Argon, Xenon, Oak, Sectico Sabre, CloudFlare Nimbus, DigiCert Nessie, DigiCert Yeti, and TrustAsia.
- **zf**: Zone files from ICANN's Centralized Zone Data Service (CZDS) and available TLDs (.se, .nu, .ee, .ch, and .li).
- **opendata**: Names from the open-data efforts of AFNIC [2] and SK-NIC.
- **Top-lists**: Names from the corresponding domain top-list such as tranco, majestic, radar, umbrella:

Open **INTEL** in numbers:

308
MILLION

domains measured on a
daily basis

5.9
BILLION

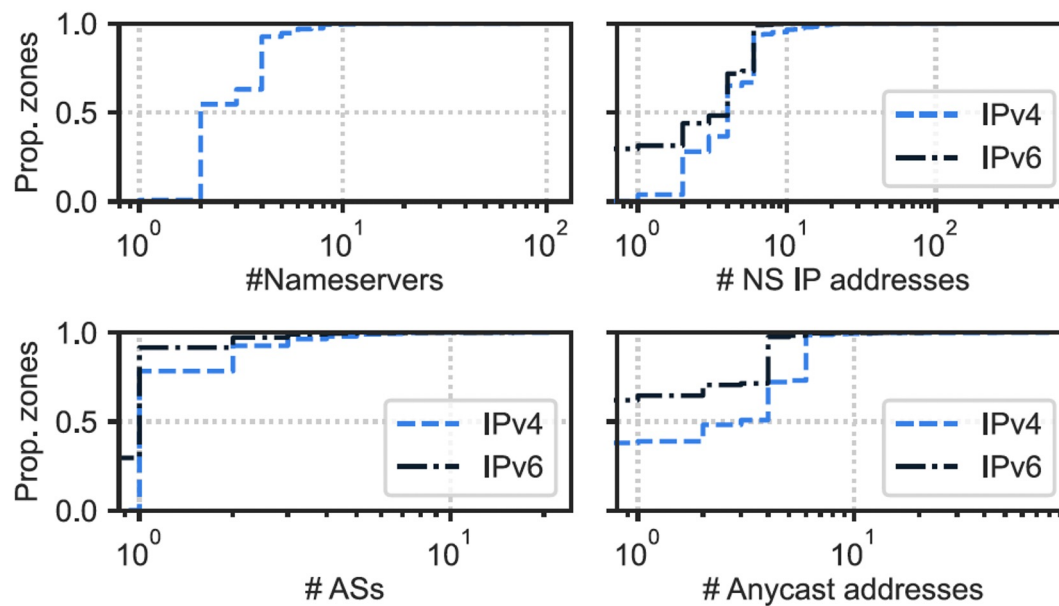
data points collected daily

13.6
TRILLION

data points collected since
the start in 2015

Direct metrics

- Resilience metrics for the Tranco Top 1M domains [2]
- IPv6 deployments include fewer addresses, ASes, and rely less on anycast



Dashboard (Work in Progress)



Country Code Top Level Domain Details

Explore DNS infrastructure and compliance data for country-specific top-level domains.

- A ccTLD zone represents the DNS namespace assigned to a specific country or territory (e.g., `.in`, `.ru`).
- It contains authoritative nameserver records ensuring proper domain resolution within that country's domain space.
- ccTLD zones are essential for national identity, localised control, and reliable DNS infrastructure.

in

36 of 238 countries

- Argentina `.AR`
- Benin `.BJ`
- China `.CN`
- Dominican Republic `.DO`
- Spain `.ES`
- Finland `.FI`
- Indonesia `.ID`
- India `.IN`**
- British Indian Ocean Territory `.IO`
- Papua New Guinea `.PG`
- Philippines `.PH`

[← Back to ccTLD Overview](#)

India
`.IN` ISO IN

NAMESERVERS 4	REGISTERED SLDS 8,469	ASNS AS393818, AS63363, AS42	NS COUNTRIES US, CA
-------------------------	---------------------------------	--	-------------------------------

Compliance Summary

KINDNS best-practice checks

DNSSEC	✓ Compliant
AXFR Security	✓ Compliant
No Recursion	✓ Compliant
NS Redundancy	✓ Compliant
Network / Geographic Diversity	✓ Compliant

Nameserver Details

4 unique nameservers

NAMESERVER	IPV4	IPV6
<code>ns01.trs-dns.com</code>	64.96.1.1	2620:57:4001::1
<code>ns01.trs-dns.net</code>	64.96.2.1	2620:57:4002::1
<code>ns10.trs-dns.info</code>	64.78.204.1	2620:171:812:1534:8::1
<code>ns10.trs-dns.org</code>	64.78.205.1	2620:171:813:1534:8::1

Recursive Resolver Resilience



DNS Resilience Evaluation System Features





Feature	Implementation	Requirements	Related Work
BCP38 compliant	fetch public data	Fetching public data	
QMIN	resolver scans with zmap or custom go tool	Nameserver, scan server, wild-card queries, list of resolver for testing	A Second Look at DNS QNAME Minimization
MANRS compliant	Is network part of route leaks/hijacks? ROV? RPKI?	(note: distance to affected networks)	Measuring MANRS ecosystem GRIP (georgia tech) ROVISTA, geoff huston
Software diversity	SNMP, dig, fpdns2		
Allow DNS traffic only	port scan of selected ports/services	Scan server (22,23,25,80,110,143,...) → use a list of 10-20 ports (have proxying in mind)	
DNSSEC validation		Setup DNSSEC signed domain + NS with "tampered" records	Geoff Huston's DNSSEC measurements

DNS Resilience Evaluation System Features

Feature	Implementation	Requirements	Related Work
Geographical diversity			
Topological diversity	Measuring inside networks? Hard to measure	what are good patterns for running reliable rec. DNS server that are also measurable (probably out of scope for this work)	
Caching best practices	Query popular domain names → TTL values Instrument max. caching time?		Open Intel data
Anycast	https://github.com/ut-dacs/anycast-census and manycast.net		<u>LACeS: An Open, Fast, Responsible, and Efficient Longitudinal Anycast Census System</u>
Consolidation effect	Open DNS API data		

DNS Resilience Evaluation System

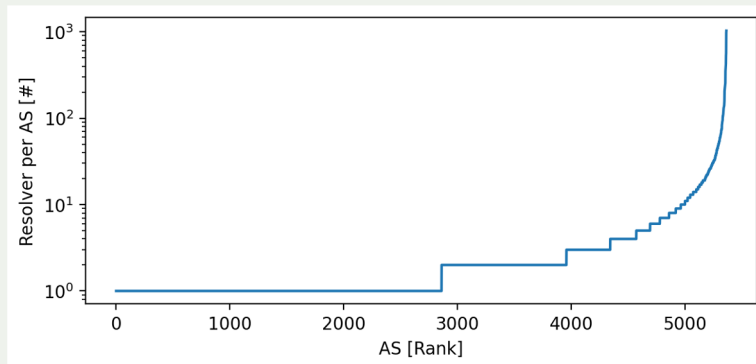
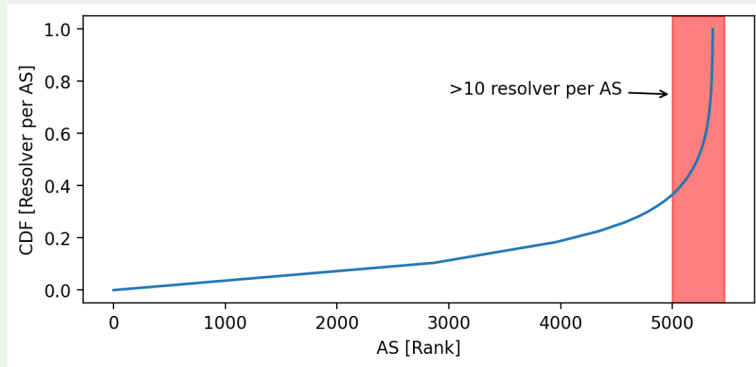
Data sources

Data source	Public?	Update interval	Content	Link
Open DNS API		Weekly updates	Open resolver and forwarder	https://odns-data.netd.cs.tu-dresden.de
CAIDA Spoofer		Daily updates	AS and prefix list that allow for spoofing	https://api.spoofers.caida.org/
Open Intel data		Daily updates	Domain names, real time zone feeds	https://openintel.nl/data/
DNSSEC validation		Daily updates	Network level overview of DNSSEC validation (there is a parser available) (How to get access to that?)	https://stats.labs.apnic.net/dnssec

Measurement vantage points Infrastructure

Vantage point	Probes	Costs	Country	Limitations	Measurements
TU Dresden	1	–	DE	No	Internet-wide
HAW Hamburg	1	–	DE	No	Internet-wide
BCIX	1	–	DE	No	Internet-wide
RIPE Atlas	>1k	Credits	World-wide		Enrich set of resolvers
Proxies	?	Varying	World-wide	Ethics	Proxy measurements already running Maybe for cross validation
VPNs	?	Varying	World-wide	Keep in mind that they might lie about their location	First test from TUD vantage point, then run over VPN

Open resolver report

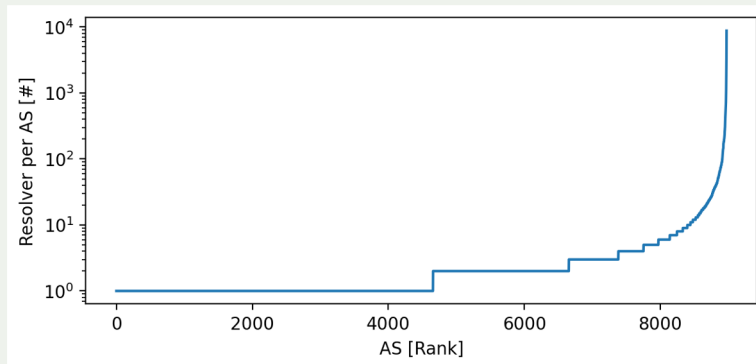
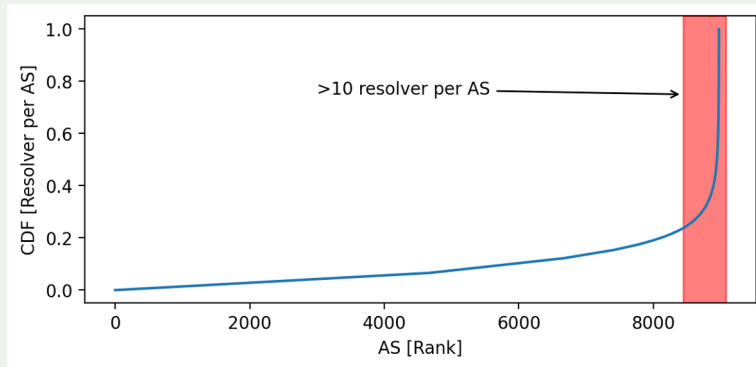


93% of ASes with open resolvers host less than 10 open resolvers.

We observe only a single open resolver per AS for 46% of the ASes.

We observe **28k** open resolvers in **5.4k** ASes and **183** countries.

Closed resolver report



We observe in 94% of ASes with closed resolvers host less than 10 instances.

We observe only a single closed resolver per AS for 48% of the ASes.

We observe **72k** closed resolvers in **9k** ASes and **212** countries*.

*unique country codes, not necessarily independent nations

Overview of spoofing networks

Open DNS API (Transparent forwarders):

ASes that allow spoofing: **2280**

Distributed in **98** countries, affecting **5.6k** BGP announced prefixes.

CAIDA Spoofer:

ASes that allow spoofing: **672**

Distributed in **98** countries, affecting **2k** networks prefixes.

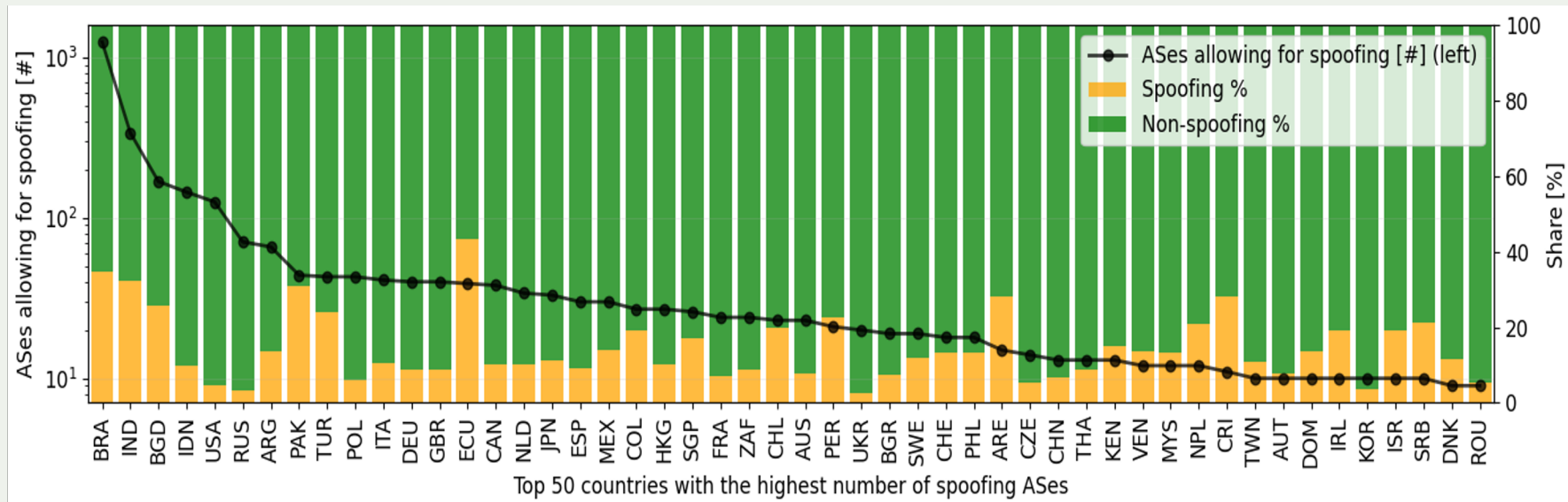
Overlap with CAIDA Spoofer:

98 ASes (4.3%)

66 countries (67%)

Spoofing networks

Overview

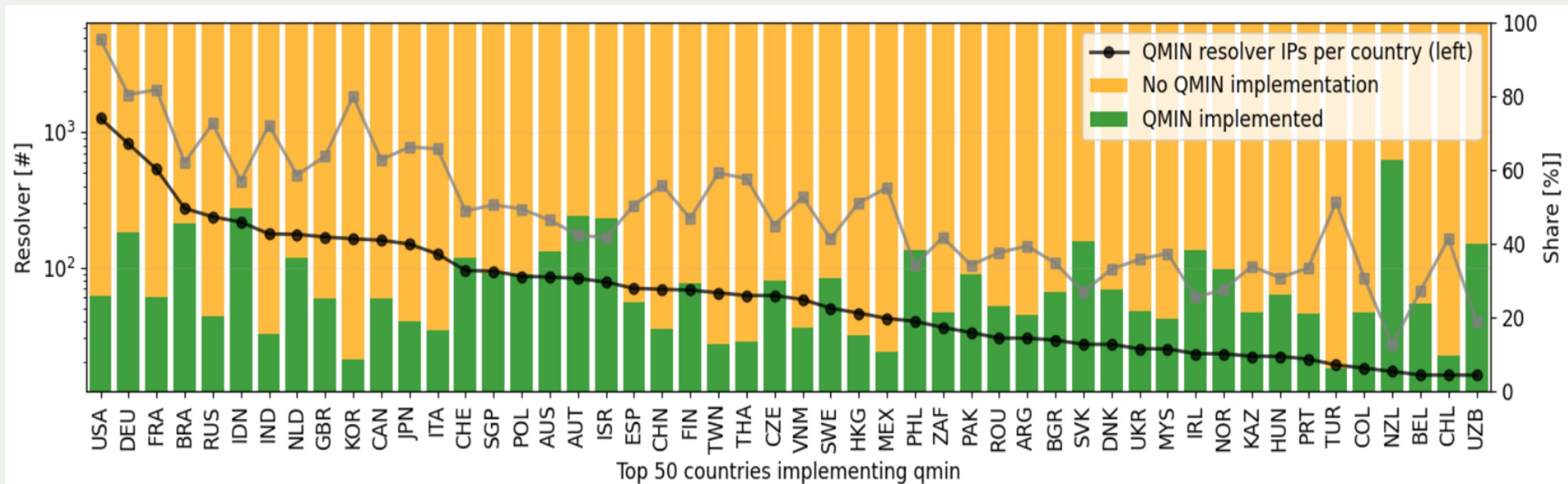


index	queried_ip_country	spoofing_asn_count	spoofing_asn_relative_amount
0	BRA	1,250	36.55
1	IND	340	9.94
2	BGD	169	4.94
3	IDN	145	4.24
4	USA	126	3.68

QMIN measurements

First results

- ~26k open resolvers tested
- 6.4k (25%) implement qmin
- 13.6k (52%) do not implement qmin
- ambiguous for remaining 6k



Thank you

phokeer@isoc.org