Monitoring Recursive DNS in China

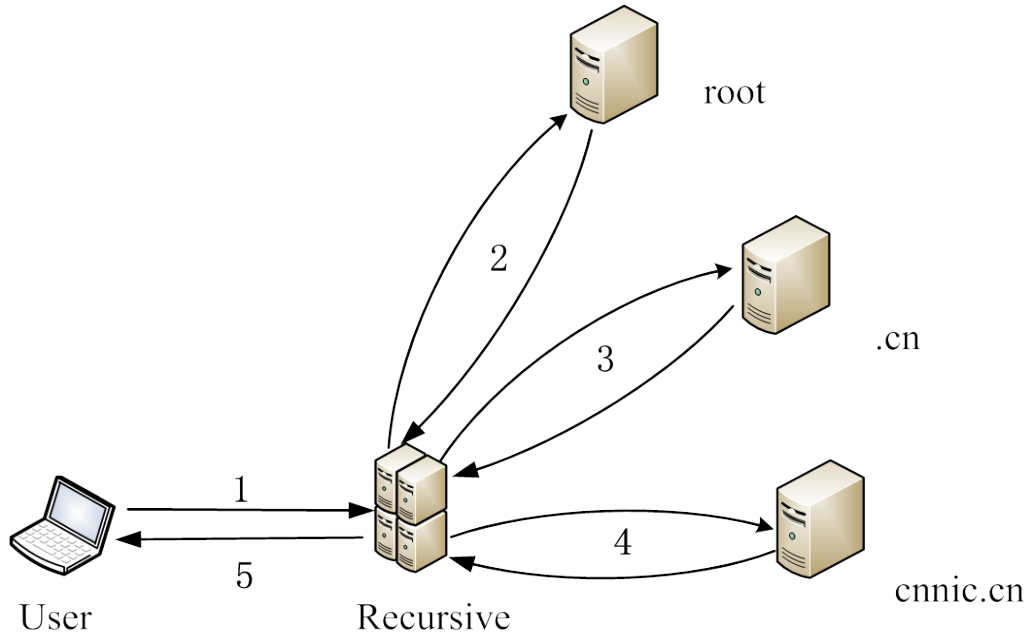
YUCHI Xuebiao

yuchixuebiao@cnnic.cn

May 12, 2013

Why we do this

- Recursive DNS is used to resolve other people's domains.
- The majority of DNS query responses are generated from the recursive DNS.
- If your recursive DNS goes down, your internet connection will, too.



Why we do this

- However, Recursive DNS are usually paid less attention than the authoritative ones.
- The cyber-criminals of today started to focus efforts on this central part of the internet infrastructure.
- In order to investigate the security, stability and resiliency of recursive DNS used in China, we built a nationwide distributed platform to monitor the status of recursive DNS
  - including all recursive DNS deployed by the three largest ISPs in China.

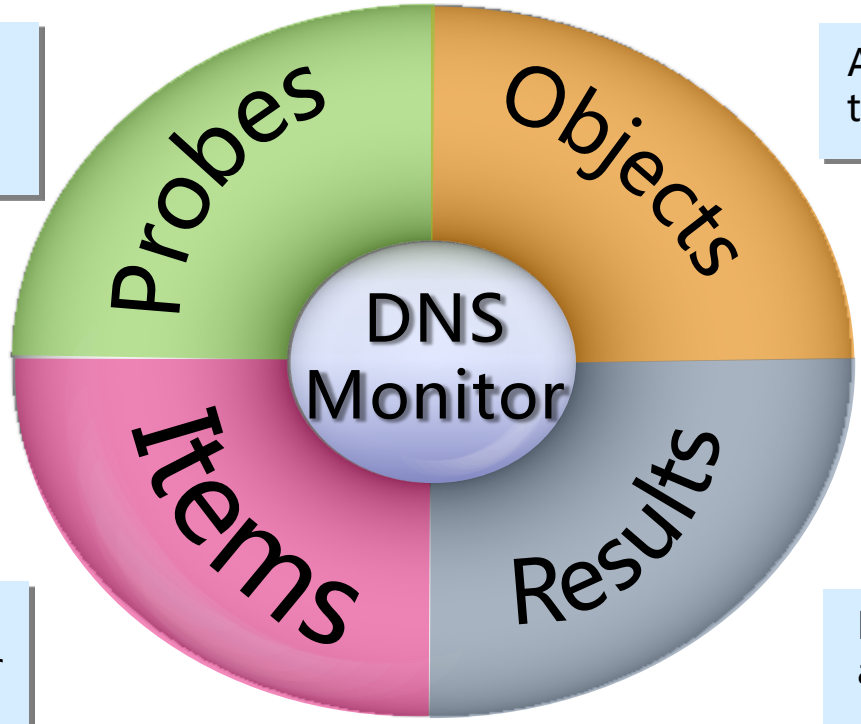
DNS Monitor

Probes

39 probes in China, 2 more overseas in this year

Objects

All root, TLD, SLD, Recursive that we can identify



Items

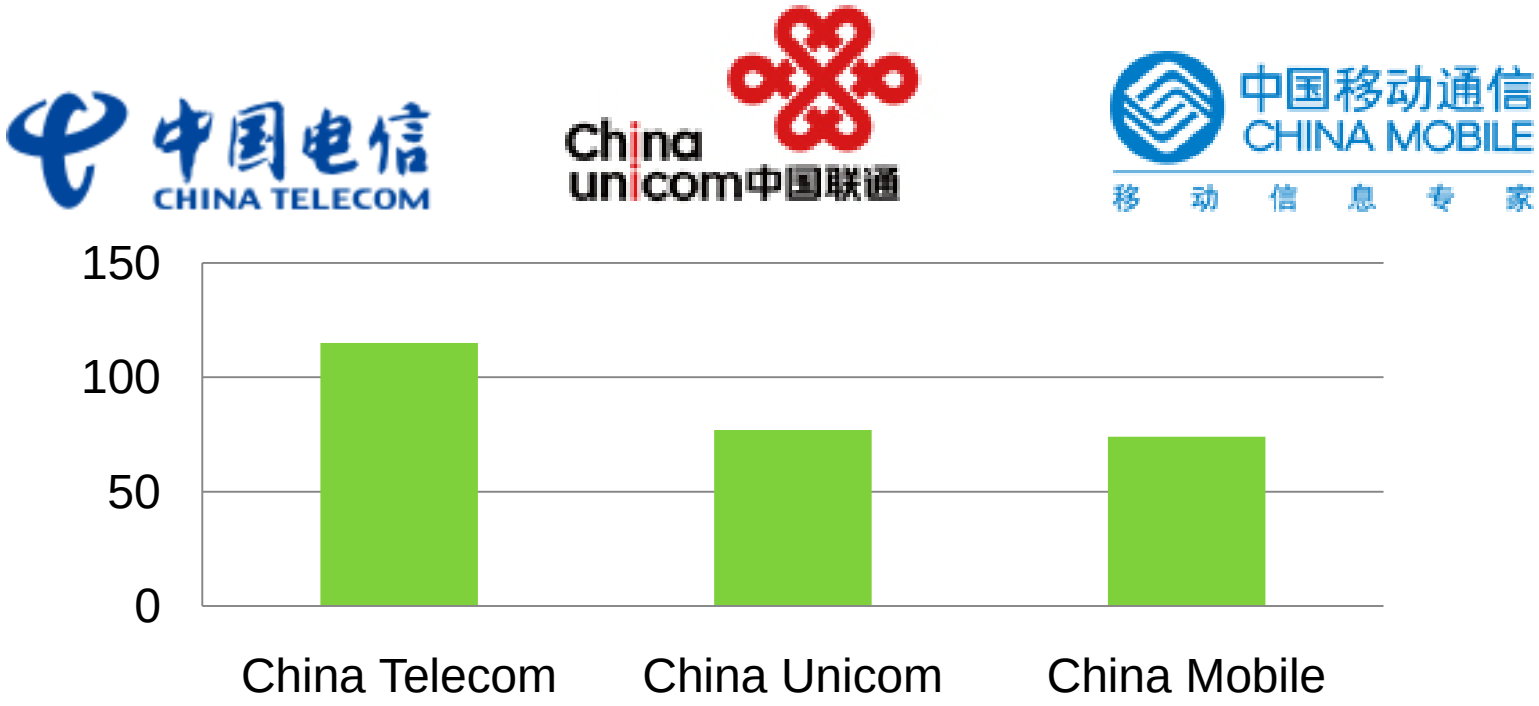
21 items related to Configuration, Failure, Flow, Performance, Security

Results

Publish DNS security report annually

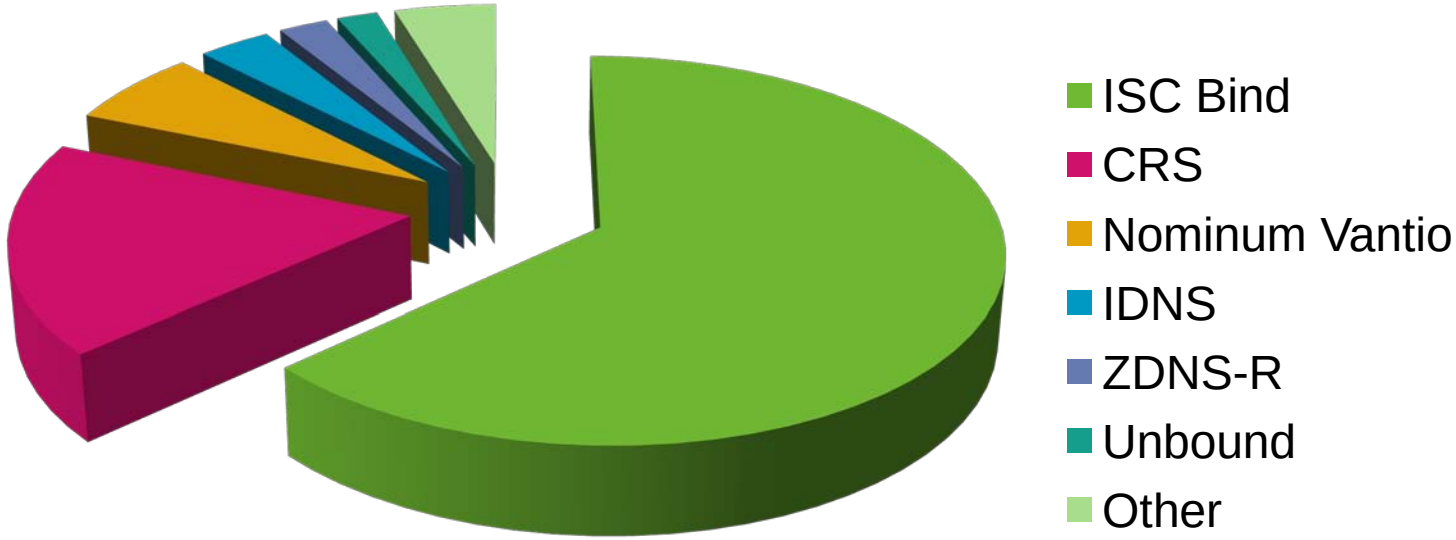
Coverage

- Nearly 300 recursive servers deployed by the three largest ISPs in China
- Distributed in all provinces of China Mainland.

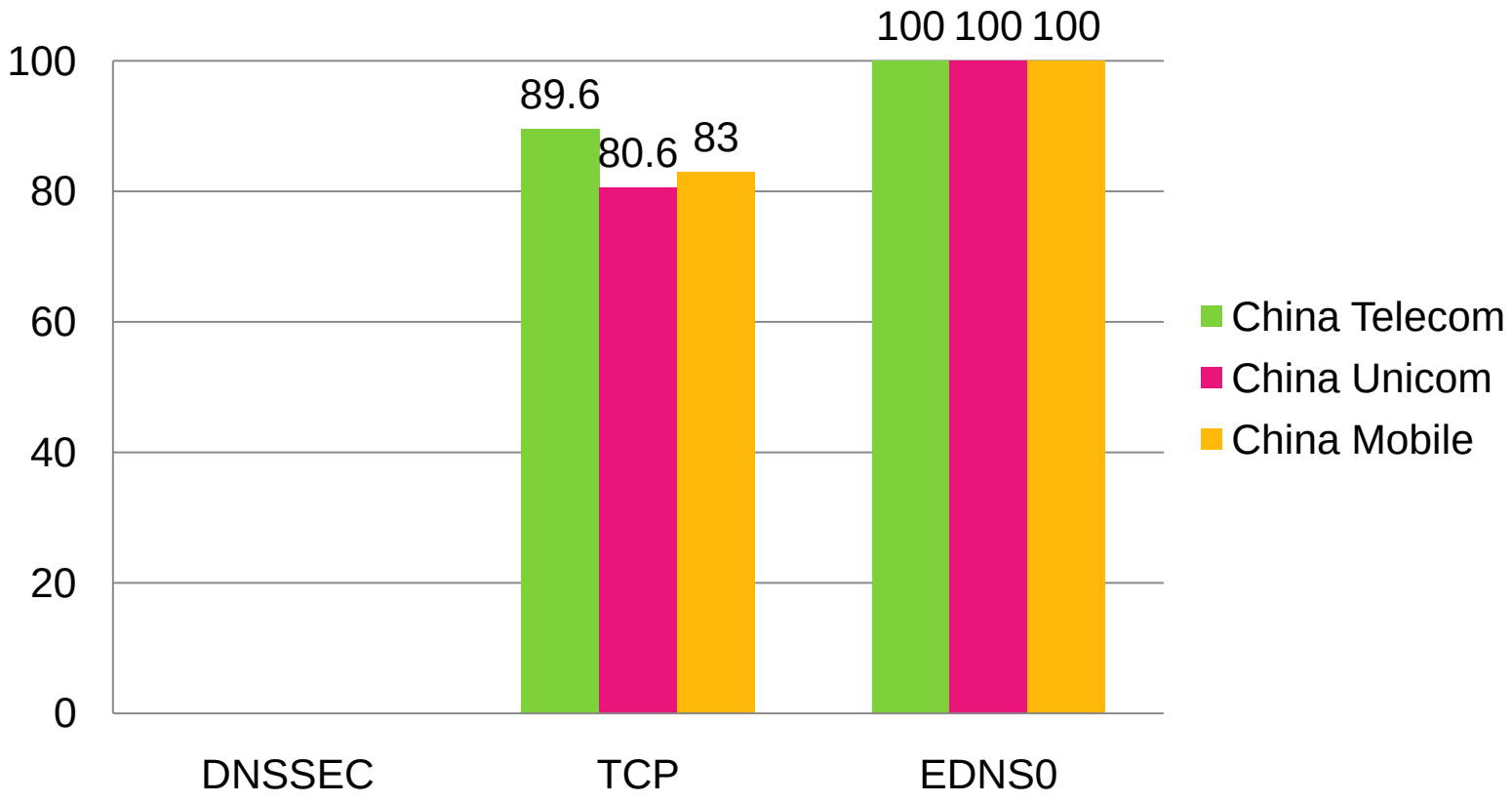


Software

- OS
  - Linux 53.9%, others are Unix
- DNS software
  - 63.3% are Bind, with 36.1% of them outdated.

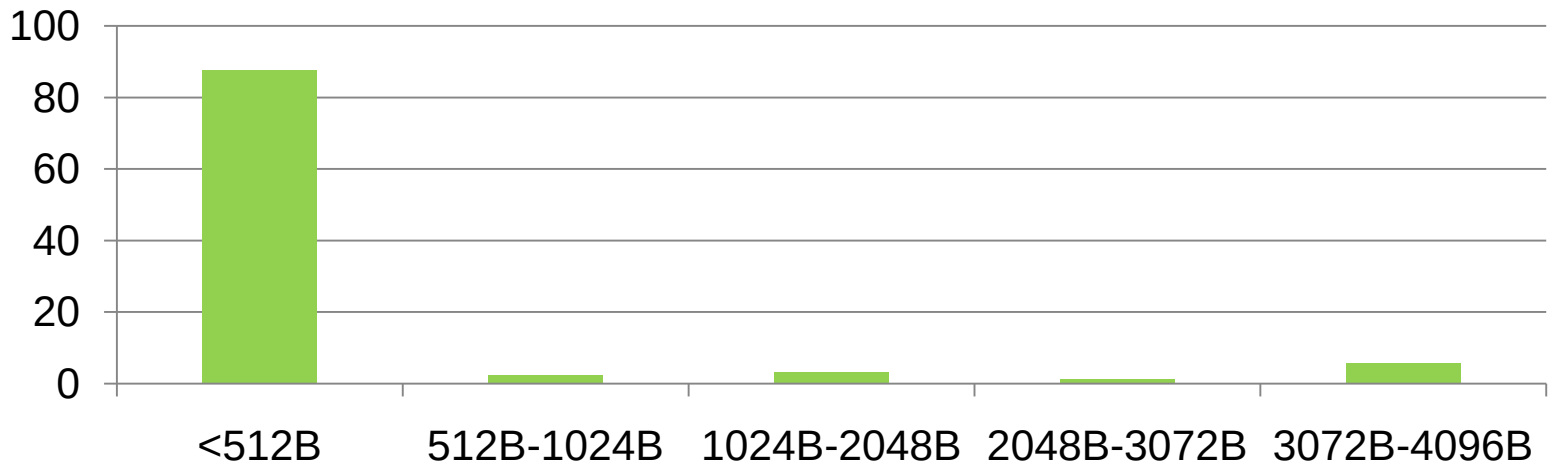


Protocol


100
80
60
40
20
0
89.6
80.6
83
100 100 100
DNSSEC
TCP
EDNS0
China Telecom
China Unicom
China Mobile

Protocol

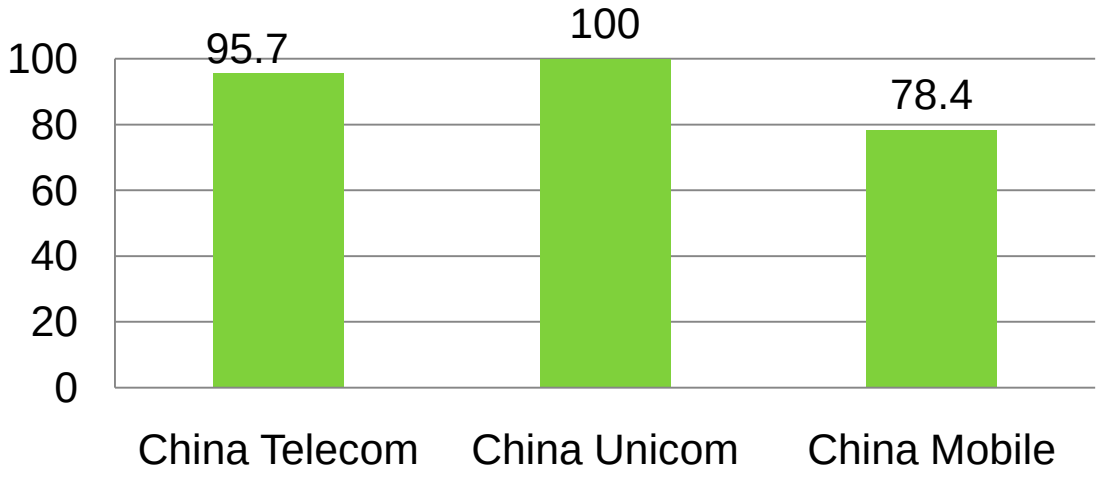
- maximum UDP packet size specified



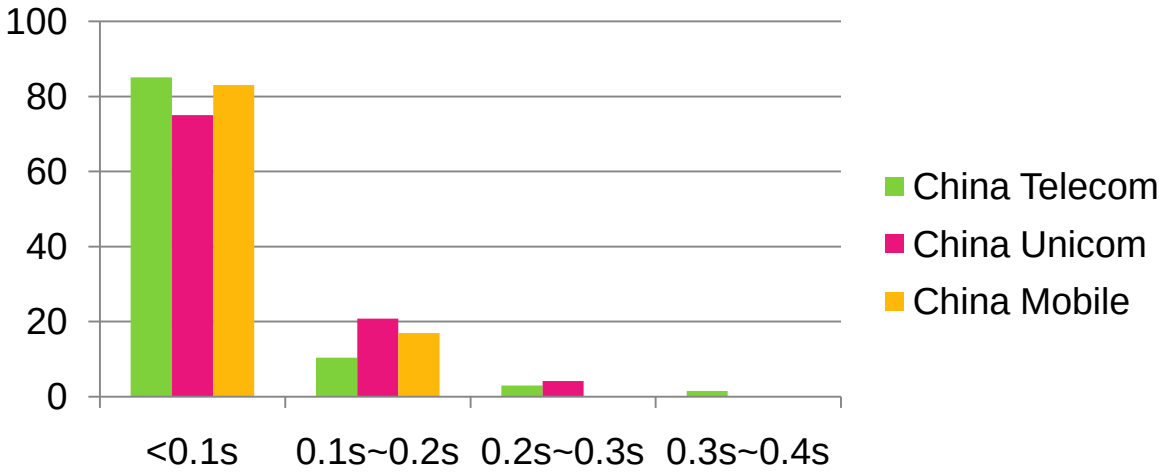
- All their port randomness are excellent.
  - dig @IP-of-server +short porttest.dns-oarc.net TXT

Performance

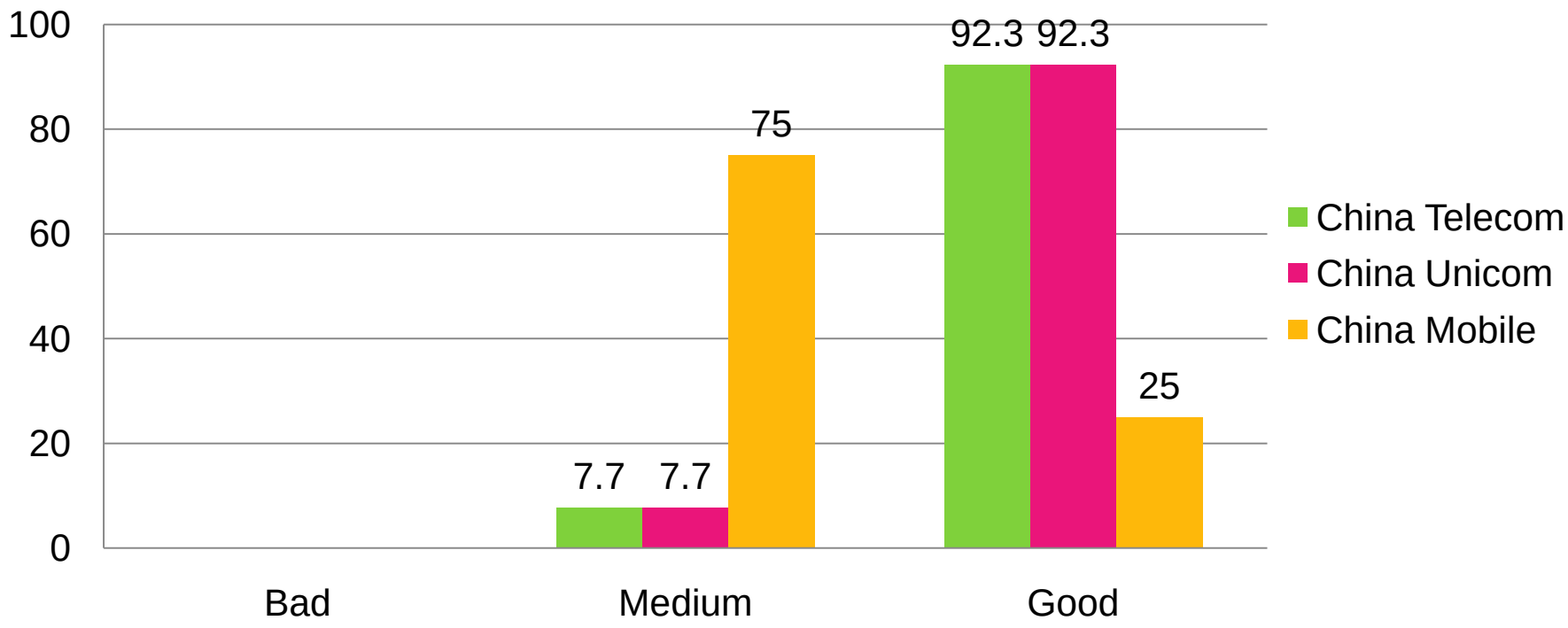
- Redundancy
  - 92.1% are clustered



- Response Latency
  - mostly within 100ms



Evaluation


100
80
60
40
20
0
92.3
92.3
75
25
7.7
7.7
Bad
Medium
Good
China Telecom
China Unicom
China Mobile

Findings

- Most of recursive DNS in China are configured properly, while others are not.
- Linux and BIND are the favorite OS and DNS software.
- A large portion of BIND are outdated.
- DNSSEC validation is currently not supported.
- EDNS0 is supported, but not configured properly yet.

Future Work

- More probes will be planted.
- More items will be monitored.
- More servers will be covered.
  - e.g. public recursive DNS

Thank you !