Latest Measurements on DNS Privacy

Sinodun

Sara Dickinson sara@sinodun.com (Presenter)
John Dickinson jad@sinodun.com
Jim Hague jim@sinodun.com

Agenda

- Two topics
  - Summary of initial benchmarking work on TCP/TLS for recursive resolvers
  - (Time permitting) Brief look at level of implementation & deployment of both DNS over TLS & HTTP

Benchmarking

Partly funded by a grant from the Open Technology Fund
(and NLnet Foundation)

- GOALS of this initial work:
  - **Understand characteristics** of how existing recursive servers handle TCP and TLS loads
  - **Looking at relative performance** cf. UDP more than absolute at this stage

Benchmarking

Partly funded by a grant from the Open Technology Fund
(and NLnet Foundation)

- GOALS of this initial work:
  - **Understand characteristics** of how existing recursive servers handle TCP and TLS loads
  - **Looking at relative performance** cf. UDP more than absolute at this stage

Much more complex than UPD…
Many more parameters…

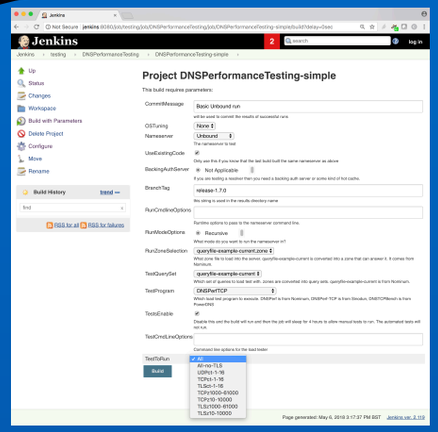
Nameservers tested

- **Bind 9.12.1 (No TLS)**
- **Unbound 1.7.0**
- **Knot Resolver 2.3.0**
- **dnsdist 1.3.0**

Other nameservers are available….

Test setup - Hardware

‘Out of the box’ testing



- 2*8 core Intel Xenon @ 2.1Ghz, 32Gb RAM
- Ubuntu 18.04
- Only basic OS and NS tuning
- NS locked to 4 cores (threads)
- Hot cache

Test setup - Software

GitHub: sinodun/dnsperf-tcp

- **dnsperf**: from Nominum/Akamai (not resperf)
- **dnsperf-tcp:** fork of dnsperf with tcp support
- **dnsperf-tls**: branch with tls support but..
  - implementation issues due to threading

Test setup - Software

GitHub: sinodun/dnsperf-tcp

- **dnsperf**: from Nominum/Akamai (not resperf)
- **dnsperf-tcp:** fork of dnsperf with tcp support
- **dnsperf-tls**: branch with tls support but..
  - implementation issues due to threading

TLS 1.2,
No TFO, TLS SR,…

Test setup - Software

GitHub: sinodun/dnsperf-tcp

- **dnsperf**: from Nominum/Akamai (not resperf)
- **dnsperf-tcp:** fork of dnsperf with tcp support
- **dnsperf-tls**: branch with tls support but..
  - implementation issues due to threading

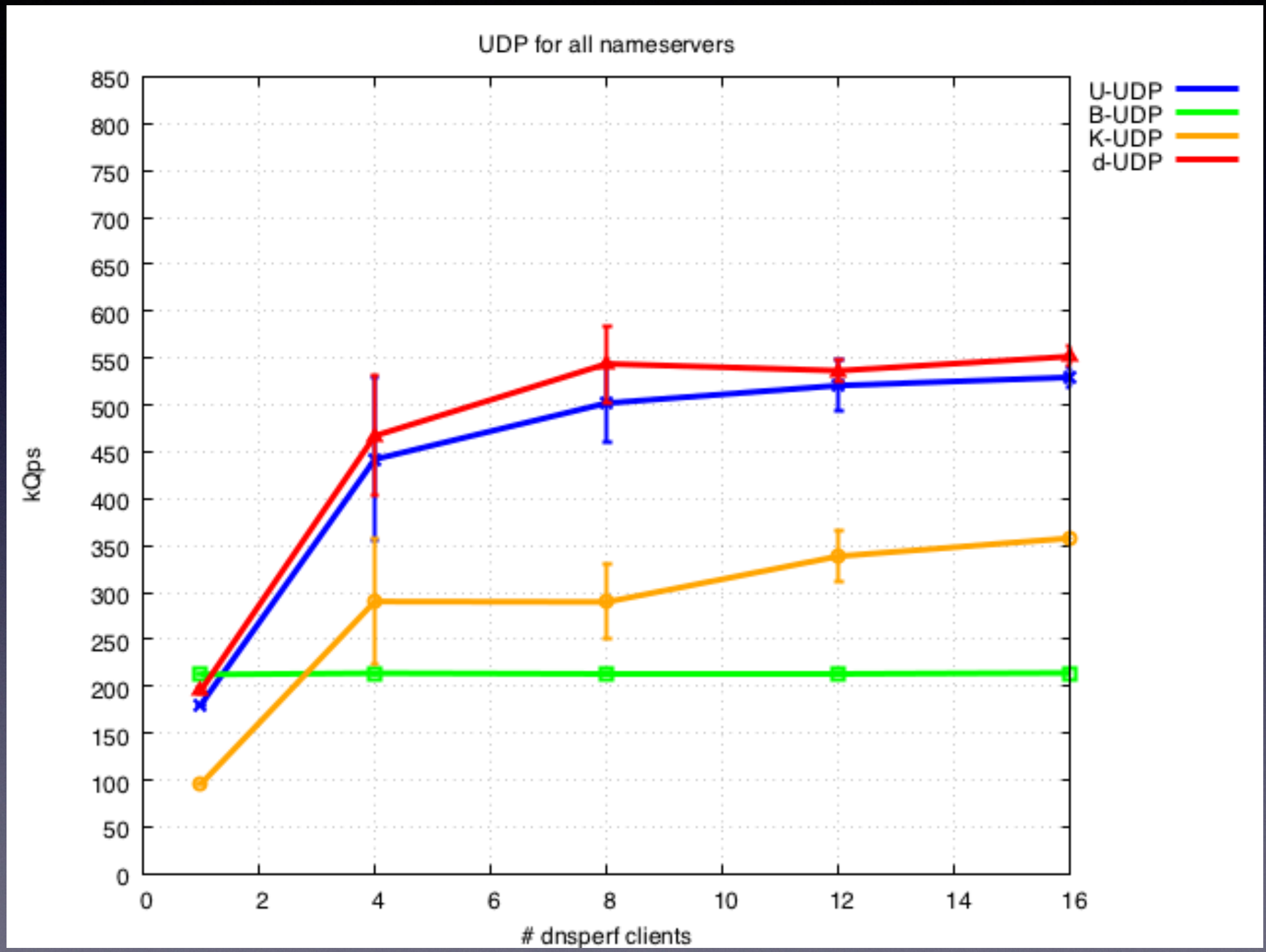
TLS 1.2,
No TFO, TLS SR,…

Focus on few clients,
Varying q per conn

- Increasing load by adding clients

UDP

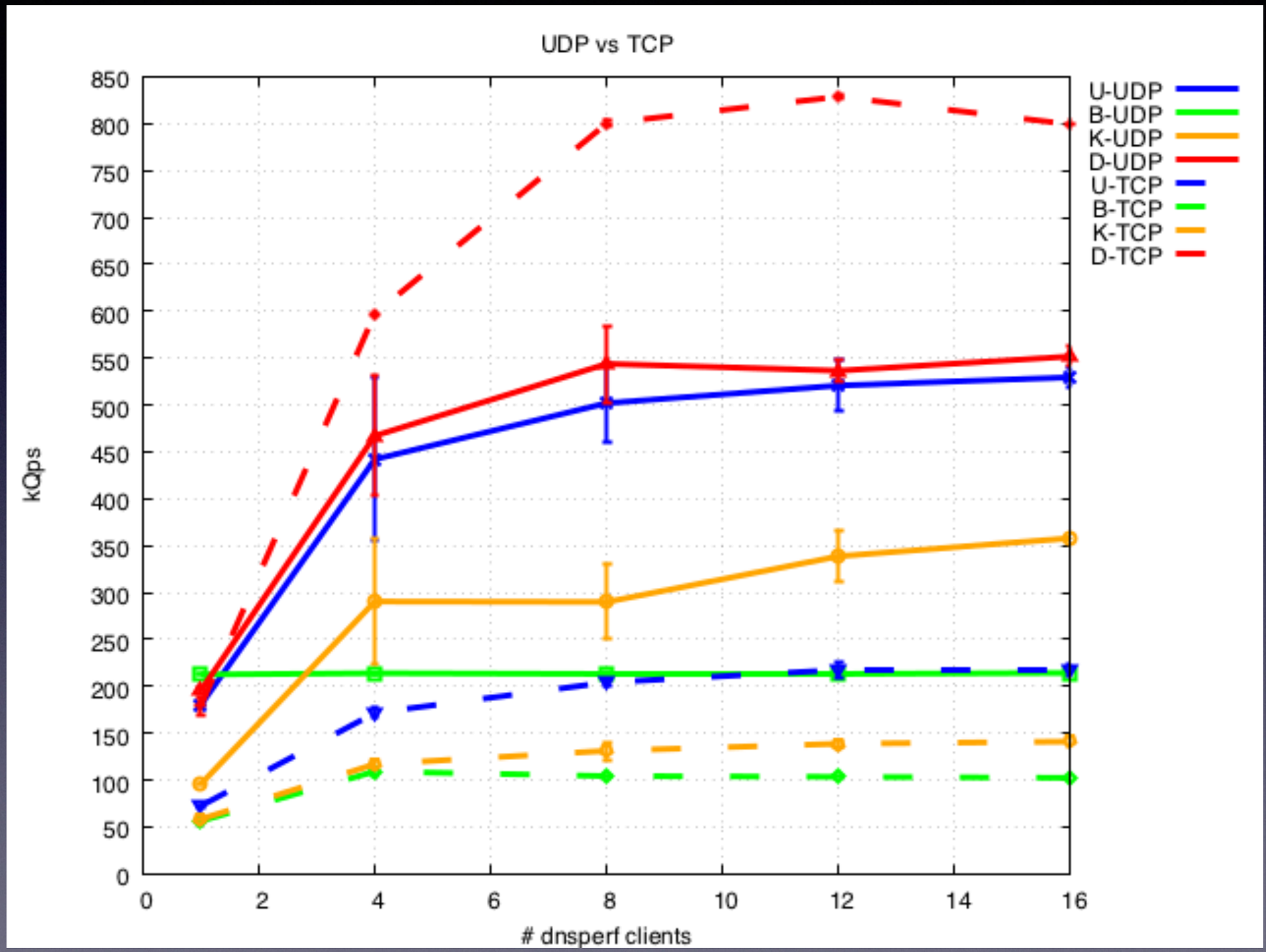
- Unbound & dnsdist similar
- Bind very flat



- Increasing load by adding clients
- 20,000 q per conn

UDP vs TCP

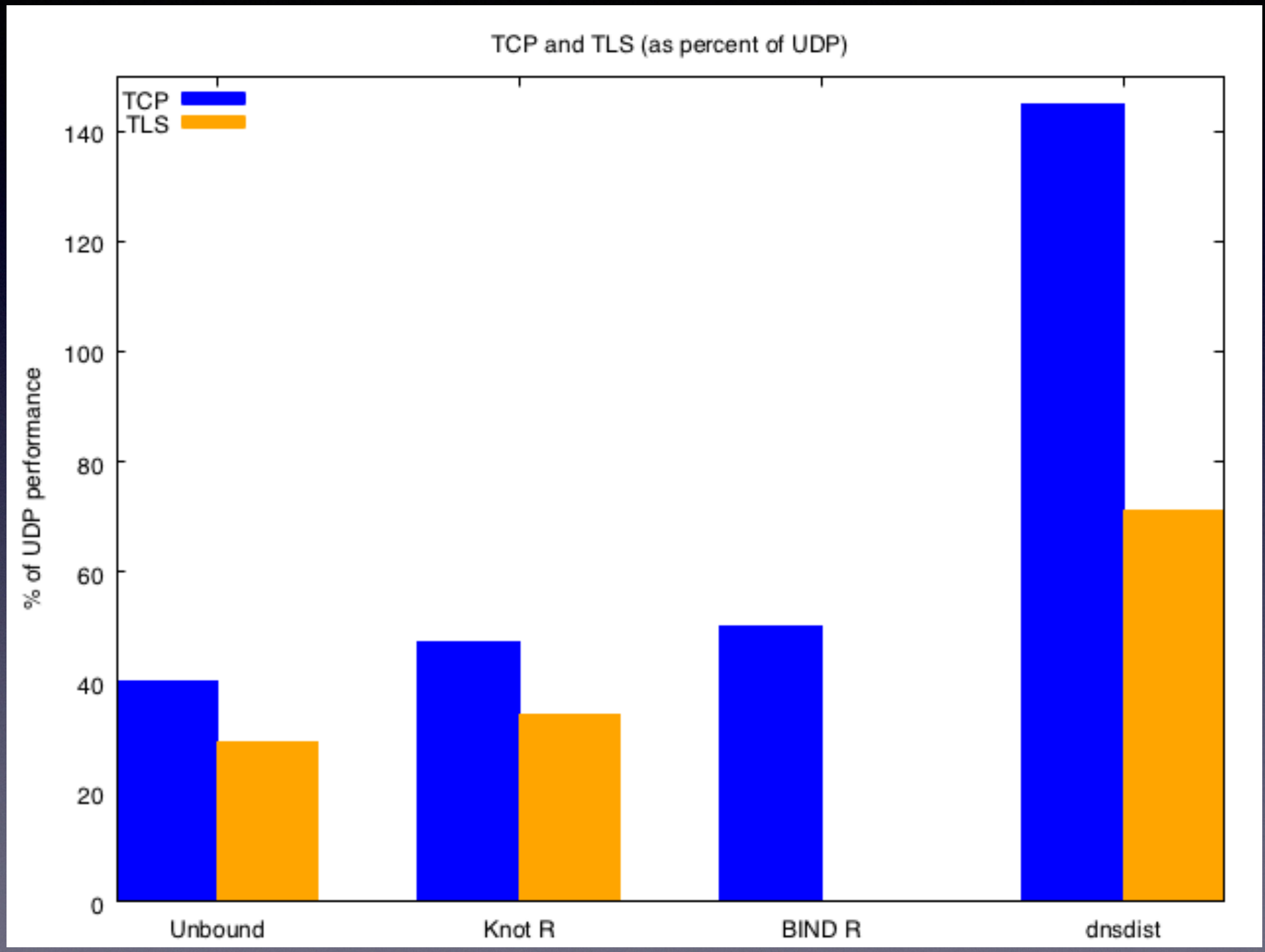
- dnsdist TCP better than UPD (but threading is diff)!
- Others similar reduction



- 8 clients
- 20,000 q per conn

% of UDP

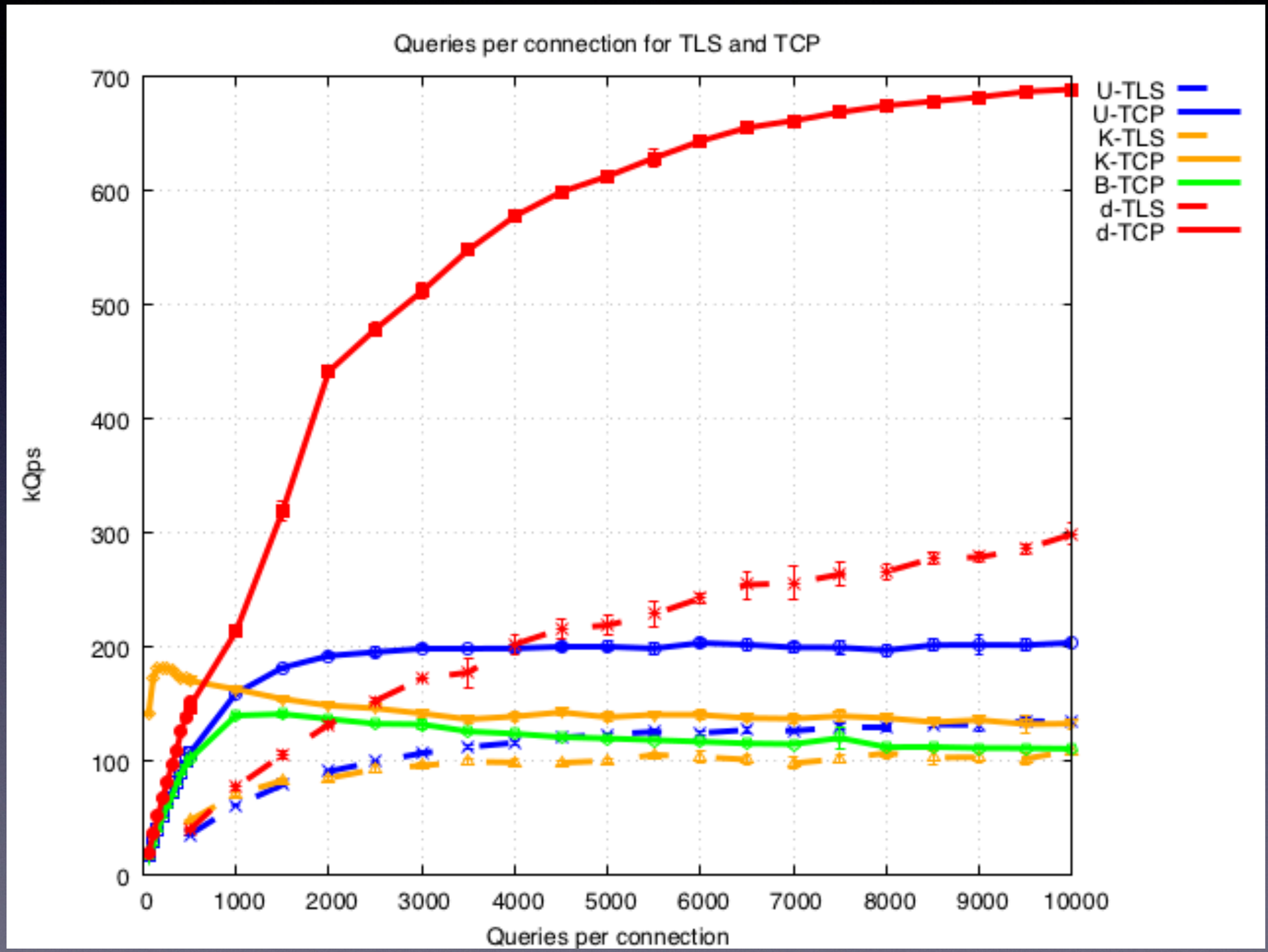
- dnsdist best
- Unbound does not do concurrent processing



- Using 8 clients
- Solid line is TCP, doted is TLS

Low q/conn

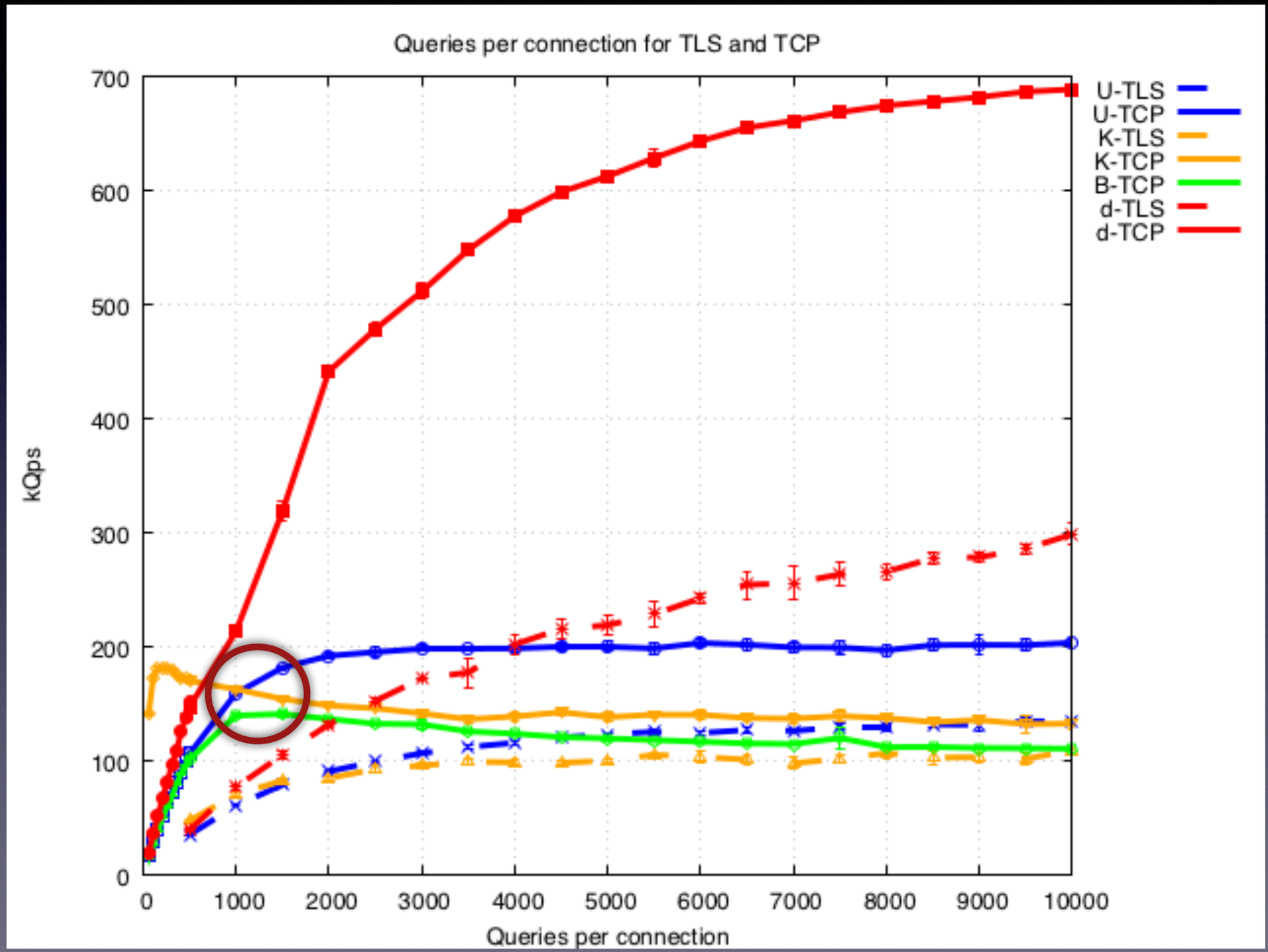
- dnsdist fall-off ~2000
- U & B fall-off ~1000
- Knot TCP is very flat



- Using 8 clients
- Solid line is TCP, doted is TLS

Low q/conn

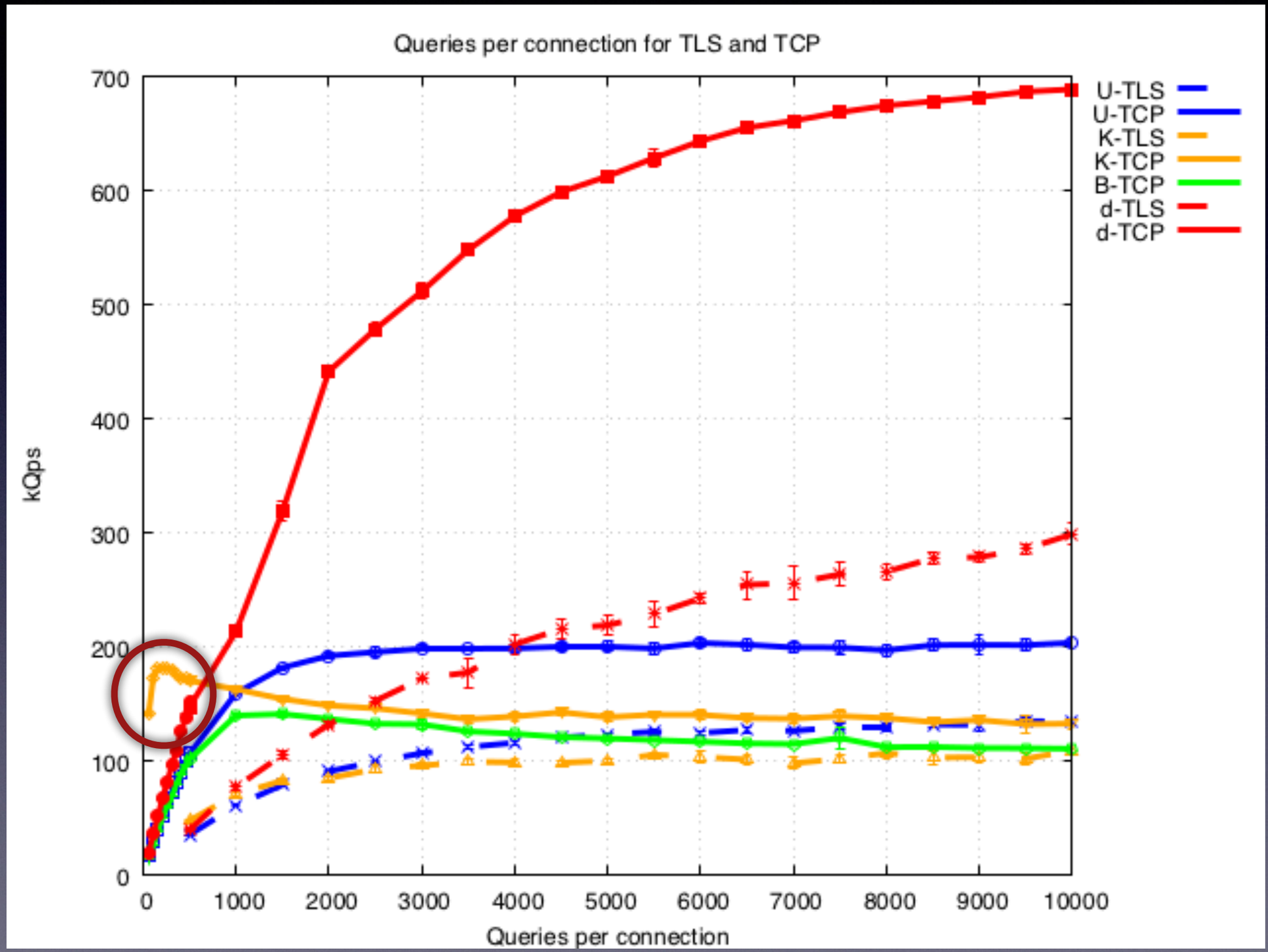
- dnsdist fall-off ~2000
- U & B fall-off ~1000
- Knot TCP is very flat



- Using 8 clients
- Solid line is TCP, doted is TLS

Low q/conn

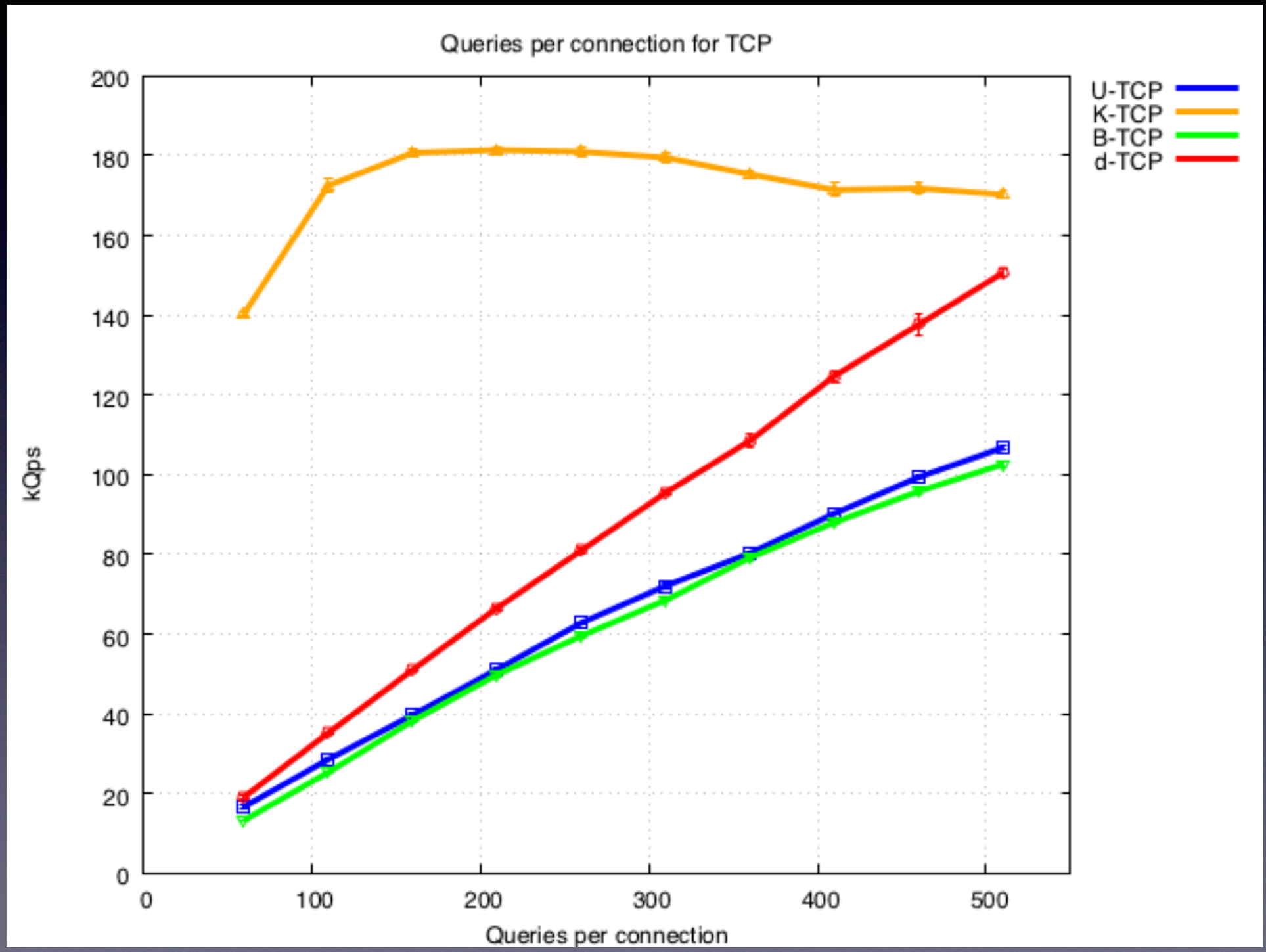
- dnsdist fall-off ~2000
- U & B fall-off ~1000
- Knot TCP is very flat



- Using 8 clients
- Current test system hits issues…

Low q/conn

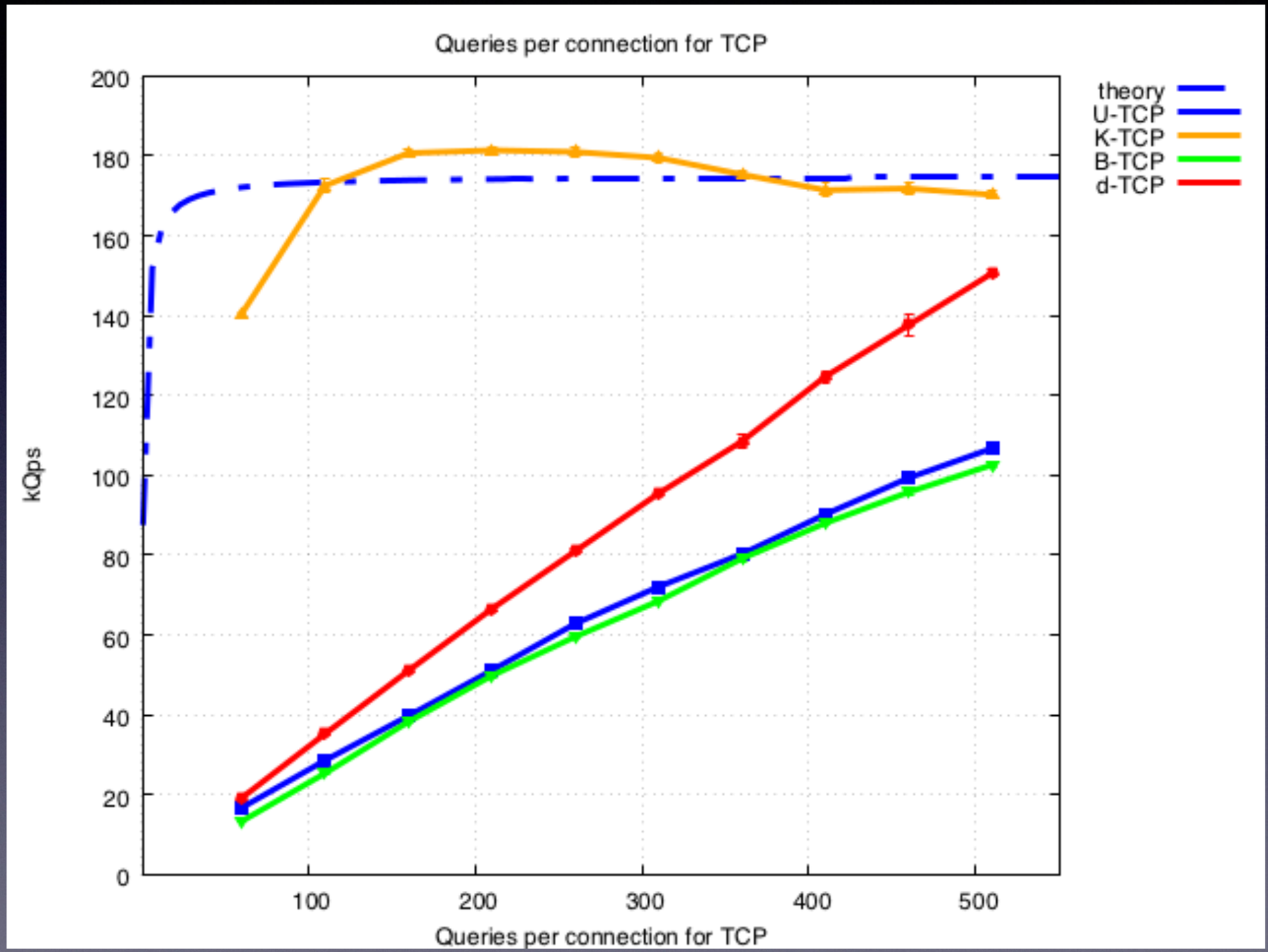
- Knot flat till ~100 q/conn
- Others linear decline
- (1 + N)/N dips ~ 100



- Using 8 clients
- Current test system hits issues…

Low q/conn

- Knot flat till ~100 q/conn
- Others linear decline
- (1 + N)/N dips ~ 100



Full report on dnsprivacy.org

TODO list

- Understand implementations better
- OS + NS tuning
- Drill to lower q/conn for TCP and TLS
  - Add tricks: TFO, TLS Session Resumption, TLS 1.3,…
- Scale to MANY clients
- Compare to TLS proxy e.g. nginx, haproxy
- Add concurrent processing to Unbound
- Use new/different test tool?

Deployment & Implementation

DOT: DNS-over-TLS
DOH: DNS-over-HTTPS (WIP)

Implementation

	Client	Recursive Resolver
DOT	• Stubby • Unbound/Knot resolver (fwd) • Android system (dev) • systemd (PR)	• Unbound, Knot Resolver, dnsdist + CoreDNS, Tenta • BIND on the way?
DOH*	• Android Intra App • Firefox config option • Stubby (next release) • Various experimental	• Various experimental

* 10+ implementations (see DOH mailing list and IETF 101 Hackathon)

Recursive Resolver Deployment

	Standalone	Large Scale
DOT	• 19 test servers	• Quad9 (9.9.9.9) • Cloudflare (1.1.1.1)
DOH*	• Google https://dns.google.com/experimental • Few other test servers	• Cloudflare https://cloudflare-dns.com/dns-query

* Experimental, some support JSON as well as wireformat

Stub to recursive is changing

- DOH draft is in WGLC
- Expect browsers to adopt DOH (default?), other apps?
- System components to use either DOT or DOH…?
- What does this mean for users
  - Privacy (yeah!) but…
  - Multiple config points (transport & DNSSEC), multiple recursives, monitoring?

Stub to recursive is changing

- DOH draft is in WGLC
- Expect browsers to adopt DOH (default?), other apps?
- System components to use either DOT or DOH…?
- What does this mean for users
  - Privacy (yeah!) but…
  - Multiple config points (transport & DNSSEC), multiple recursives, monitoring?

Thank you!

More information at:
dnsprivacy.org