DNS on FreeBSD

Erwin Lansing, DK Hostmaster A/S
FreeBSD 10.0

- unbound
- ldns
- host-wrapper, drill

- Simple setup
  - For complicated setup, install package
- Local caching recursor daemon only
  - Any resolver supported as 3rd party package
  - Any authoritative server supported as 3rd party package
- Forwarder
- DNSSEC validating
- SSHFP
- DANE
FreeBSD 10.1

- minor issues resolved
- local unbound as install time option
  - default off
FreeBSD 11.0

- local unbound as install time option
  - default on
Experience

• NTP
• “Starbucks effect”
  • extra records in root
  • EDNS0
  • fragmentation
  • TCP

• Protocol is right, it’s broken.
• User is unhappy
• permissive mode? dnssec-trigger? prompt user?
Future

• getdns-api

• Capsicum / Casper
  • compartmentalised service
  • applications don’t need to know
    • DNS
    • crypto
    • DNSSEC
    • TLS
    • certificates
    • DANE
    • ...
  • “Give me an encrypted socket to www.facebook.com”
    • OS does the rest
    • show proof
    • OS-wide policy
Questions?

erwin@dk-hostmaster.dk
erwin@FreeBSD.org

Wiki:
https://wiki.freebsd.org/DNSBase

Slides:
http://people.freebsd.org/~erwin/presentations/20141015-ICANN-FreeBSD-DNS.pdf