Connect by Name
What does it mean to setup a connection?

- Using modern standards...
- Securely
- Privately

```c
  c = connectByName("dns.quad9.net", "doh");
```
Step 1: Happy Eyeballs

- Lookup IPv6 of dns.quad9.net
- Lookup IPv4 of dns.quad9.net

Simultaneously

IPv6 arrived?

Wait 25ms

ipv6 arrived?

Wait 25ms

Setup TLS

Try in turn...

late arrivals

2620:fe::9
9.9.9.9
2620:fe::fe
149.112.112.112

Setup TLS

Try in turn...

late arrivals

9.9.9.9
2620:fe::9
149.112.112.112
2620:fe::fe
$ dig dns.quad9.net AAAA +dnssec

; <><> DiG 9.16.6-Ubuntu <><> dns.quad9.net AAAA +dnssec
; global options: +cmd
; Got answer:
; >>>HEADER<<< opcode: QUERY, status: NOERROR, id: 11598
; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; QUESTION SECTION:
; dns.quad9.net.

; ANSWER SECTION:
dns.quad9.net. 994 IN AAAA 2620:fe::9
dns.quad9.net. 994 IN AAAA 2620:fe::fe
dns.quad9.net. 994 IN RRSIG AAAA 8 3 1200 20201223190000 202 01206190000 61069 quad9.net. PWS+67FpGquaK4uGFr3qVyRh58bFSVB+RPlFRQj1kOMr/iIVwLWvD3 MSDKhsz53TTZU48ZCw9PcMbtXw5d4at4I5xUgkkfktq6XQLhLDFa ZAhUasHRaP3945Wq1 Kxy8C6h6U3HLC3JAXArM6Javlv/L4j2XvYohAiGa c0MQW84QJTFjrBWLG4wYmEKpX6WBrx2R85C7UNU LKke7ywGKGtQ2ZkD+ 7xLvnKJCuVqV5j/0mLytZkwL2BeK9pSxG1y08FvdWJTlMpb/7nNnn6I FvfXXL FCIKBVKEhu5uFJRL/e/GyhnrxwJE4SnR6hlIj3qylkp0/L8mgn YyfgdG=

; Query time: 8 msec
; SERVER: fd06:5431:4e7b::1#53(fd06:5431:4e7b::1)
; WHEN: wo dec 09 12:46:17 CET 2020
; MSG SIZE  rcvd: 395
DANE
Happy Eyeballs, DNSSEC & DANE

Step 1:

- Lookup IPv6 of dns.quad9.net +dnssec
- Lookup IPv4 of dns.quad9.net +dnssec
- Lookup _443._tcp.dns.quad9.net TLSA +dnssec
DNSSEC Chain TLS Extension

- DANE Embedded in the TLS Handshake:

- _443._tcp.dns.quad9.net. TLSA
- quad9.net. DNSKEY
- quad9.net. DS
- net. DNSKEY
- net. DS
- . DNSKEY

Diagram:

- TLS Chain extension? (yes)
  - Abort DANE Lookup Use Chain extension
  - DANE Authenticate TLS (yes)
  - PKIX Authenticate TLS (no)
- DANE records? (no)
Zero config DNSSEC

System requirement for DNSSEC:

- root KSK

Alternatively, from application fetch:

- RFC7958

validate with ICANN CA
Happy Eyeballs, DNSSEC & DANE + fetching/renewing DNSSEC TA

Step 1:

dns.quad9.net AAAA →
dns.quad9.net A →
_443._tcp.quad9.net TLSA →
data.iana.org AAAA →
data.iana.org A →

connect port 80  fetch anchors

TLS 🌟  Communicate...

Beware! This is the happy path.
DNS-over-TLS (DoT)
DNS-over-HTTPS (DoH)

• Do all DNS lookups *privately*

• Setting up DoT or DoH in itself involves:
  - Happy Eyeballs
  - DANE Authentication
    • With DNSSEC Chain, or
    • DANE records acquired over the as of yet unauthenticated DoT or DoH session
Much, much, more ...

- DNSSEC Roadblock avoidance  RFC8027
- DNSSEC with DNS64 / NAT64  RFC7050
- DNS-over-Quick (DoQ)
- Oblivious DNS-over-HTTPS (ODoH)
- Multiple Provisioning Domains  RFC7556
- etc.
What does it mean to setup a connection?

- Using modern standards...
- Securely
- Privately
What is Connect by Name?

Turn this:

Into this: