DNS @ IETF

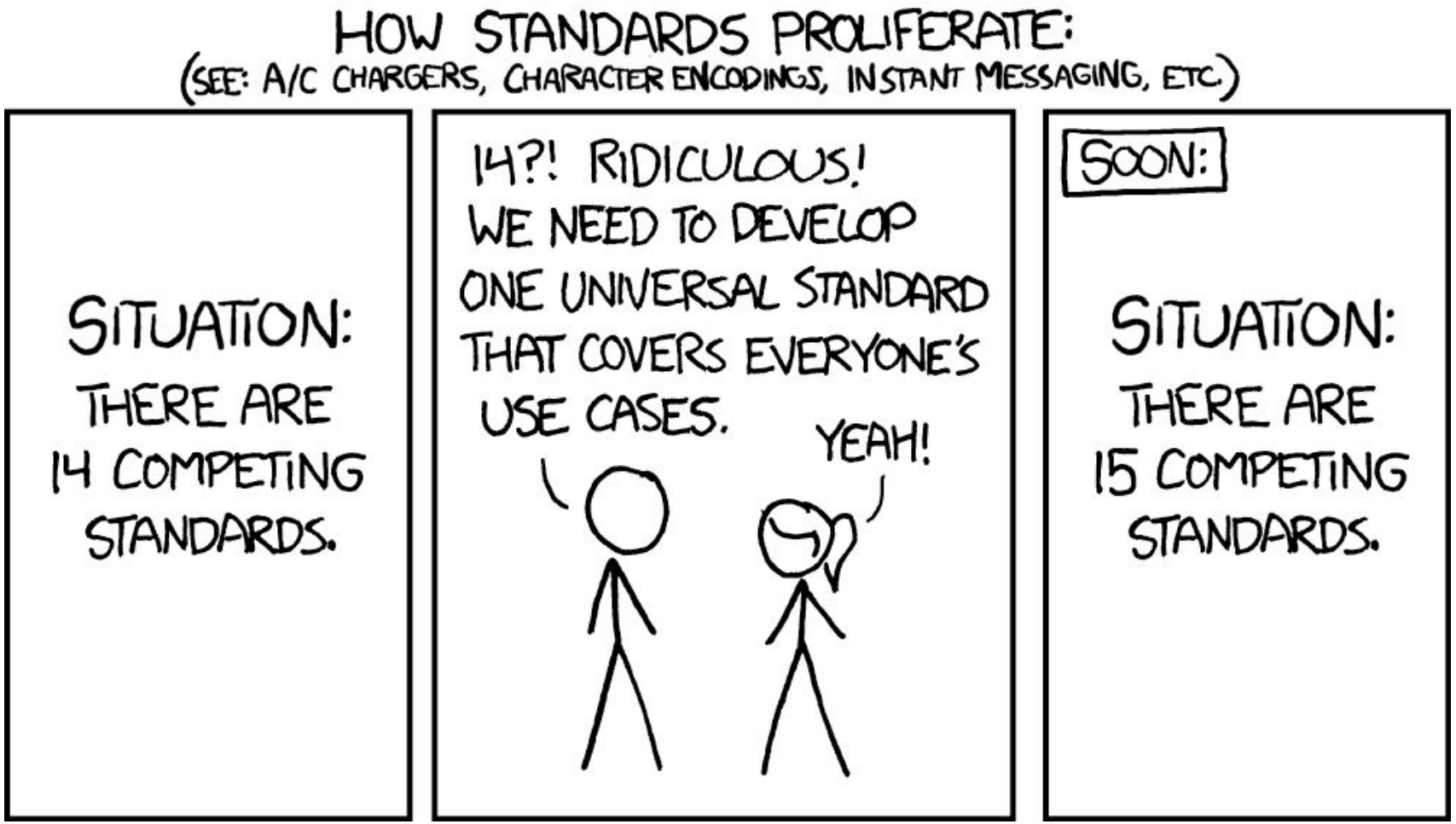
DNS Standards Work-of-Interest

David Lawrence <d.lawrence@salesforce.com>

NANOG 91, Kansas City, June 2024

A very brief history of the IETF

- Standards Developing Organization (SDO)
  - Akin to ITU, IEEE, WHO, ASME …
  - Voluntary, international, individual membership
- An ancient body, from the adolescence of the pre-commercial Internet.
  - First met in 1986, nearly 40 years ago (4 days before the Challenger disaster)
- Formed to coordinate interoperability in a heterogeneous environment
- Core principles
  - open, consensus-driven process
  - freely available standards
  - non-proprietary for implementation
  - planned security
  - planned privacy
- No direct certification / enforcement powers



https://xkcd.com/927/

So, why am I here?

- Surprisingly little overlap between standards writers and operators
- Charges of Ivory Towerism are not completely unwarranted
- Increased outreach to the operator community
  - Can identify practical spec problems earlier
  - Could help adoption of new technologies

Overview of the IETF's Structure

- Areas
  - Applications and Real-Time Area (art): Higher level, like email, calendaring and telephony
  - General Area (gen): Work about the IETF itself, like tools and processes
  - Internet Area (int): Core Internet tech like IP, DNS, NTP, and DHCP
  - Operations and Management Area (ops): Topics such as configuration and management
  - Routing Area (rtg): BGP, RPKI, MPLS, et cetera
  - Security Area (sec): Crypto algorithms, key management, identities, TLS, and so on
  - Web and Internet Transport (wit): HTTP, QUIC, and other web-focused services
- Working Groups
  - More narrowly focused topics within each area, eg just the DNS registry/registrar protocol
  - Boundaries can be a little fuzzy, such as DNS protocol work in the dnsop wg in ops
- Internet Engineering Steering Group (IESG) is all Area Directors
- Internet Architecture Board (IAB) provides top level leadership

The IETF's Output

- Document Types
  - Standards Track: Proposed Standard or Internet Standard, to be broadly implemented
  - Best Current Practice (BCP): Operational advice
  - Informational: External protocols or non-protocol documents
  - Historic: Obsolete protocols
- Document Streams
  - IETF stream, produced through working group collaboration and IESG review
  - IAB stream, for documents produced by the IAB, mostly about the standards process
  - IRTF (Internet Research Task Force) stream, for research-focused documents
  - Independent Submission Stream, for documents outside of the above
    - April 1st RFCs
    - Jon Postel's eulogy
    - Non-IETF protocol descriptions
    - Informational, Experimental or Historic, NEVER Standards Track nor BCP

DNS Working Groups

- dnsop, for core operations and protocol work
  - historic: dnsext/namedroppers
- dprive, focused on privacy enhancements for the DNS
- dnssd, scaling the DNS service discovery protocol
- add, guiding resolver selection protocols for clients
- deleg, investigating a new delegation mechanism

dnsop recent notable work

- RFC 9520, Negative Caching of DNS Resolution Failures
  - Reduces aggressive retry in the absence of explicit TTL information
  - Recommends exponential backoff to a maximum of five minutes
- RFC 9460, Service Binding and Parameter Specification via the DNS
  - New records, SVCB and HTTPS, that helps facilitate independent service operators
  - Addresses the problem where a CNAME can't coexist with other records at zone apex
  - Helps support efficient initiation of TLS sessions
- RFC 9432, DNS Catalog Zones
  - Secondary nameservers need not have out-of-band configuration of new zones at primary
- RFC 8901, Multi-Signer DNSSEC Models
  - From 2020, but now finally seeing implementation from, eg, Cloudflare and NS1
- RFC 8914, Extended DNS Errors
  - Optional, allowing for descriptions on answers like policy blocking, DNSSEC errors, or stale data
- RFC 9567, DNS Error Reporting
  - Allows configuration of an email address for resolver error reports, eg DNSSEC failure

dnsop current notable work

- Structured Error Data for Filtered DNS
  - Leverages RFC 8914 extended errors to add JSON-formatted additional information
  - Primary use case is for user feedback about policy blocked responses
- Automatic DNSSEC Bootstrapping using Authenticated Signals
  - Another attempt to address the lack of an operator role in the ICANN model
- Domain Control Validation using DNS
  - Analyses various in-band ownership validation approaches and recommends best practices
  - Hope to cut down on enormous apex TXT record sets (many now force TCP lookups)
- IP Fragmentation Avoidance in DNS over UDP
  - Recommends techniques to reduce the risk of fragmenting UDP responses
- Generalized DNS Notifications
  - Expands DNS NOTIFY operation beyond signaling zone transfers
  - Initial use case is for DNSSEC key-related updates with parent

dprive recent and notable work

- RFC 9103, DNS Zone Transfer over TLS
  - Guards against third-party observation of zone data during secondary refresh
- RFC 9250, DNS over Dedicated QUIC Connections
  - DoQ, akin to DoT (DNS over TLS) but with QUIC efficiencies
  - General purpose for both client to resolver and resolver to authority
  - Doesn't address discovery, just the query/response mechanism
- RFC 9539, Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS
  - Approaches to probing for DoT / DoQ support at authorities
- Using Early Data in DNS over TLS
  - 0-RTT session resumption is susceptible to replay attacks; this proposes mitigations

dnssd recent and notable work

- RFC 8765, DNS Push Notifications
  - Allows client subscription to monitor changes to specific records of interest
- An EDNS(0) option to negotiate Leases on DNS Updates
  - Adds leases to Dynamic DNS registrations to allow for expiry
- Service Registration Protocol for DNS-Based Service Discovery
  - Simplifies service setup and related dynamic DNS update
  - Significant initial use case is to make printer setup easier
  - Implemented by the Matter spec for IoT devices
- DNS Multiple QTYPEs
  - A way to ask for multiple record types at a name in one go, such as A, AAAA and MX
  - In dnssd because they want it to minimize packets on low-power Thread meshes
  - Thread clients want both SRV and TXT records

add recent and notable work

- RFC 9461, Service Binding Mapping for DNS Servers
  - Extends the RFC 9460 SVCB record to identify DNS server capabilities
  - Can specify a server runs an encrypted transport, and on what port
- RFC 9462, Discovery of Designated Resolvers
  - DDR, for clients to identify a resolver's encrypted DNS configuration
- RFC 9463, DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers
  - DNR, Local encrypted resolver setup via DHCP or router advertisement
- DNS Resolver Information
  - An extensible type, RESINFO, for specifying the details of a resolver's feature support
- Establishing Local DNS Authority in Validated Split-Horizon Environments
  - Enterprise DNS and internal/external views of zone data has long complicated DNS setups
  - Provides a trust mechanism to assert when domains need internal resolution

deleg, a new IETF working group

- My aspirational talk at NANOG 90 ran headlong into Real World Process
- To recap, a cross-section of the DNS industry wants to provide more information about the authoritative servers for a zone
- Initial use cases are to indicate DoT/DoQ/DoH, and operator indirection
- Likely the biggest change to DNS since DNSSEC
- "Birds of a Feather" in March at Brisbane IETF showed support to pursue it
- Working group still needs final IESG approval, expected next week
- First draft on the problem statement and requirements by end of the month
- Inaugural meeting at Vancouver IETF in July

Thank you