# QUIC Version Stuff

draft-duke-quic-v2-01
draft-duke-quic-version-aliasing-06
draft-duke-quic-protected-initial-02

# QUIC v2

Purposes:

- Exercise the VN mechanism
- Template for new version drafts

Adopt? Or just use for exercises?

# Interesting Questions

- Version numbers: incremental or random?
- ALPN? The -applicability draft used to say

> Applications could define an alternate endpoint discovery mechanism to allow the usage of ports other than the default. For example, HTTP/3 (Sections 3.2 and 3.3 of [QUIC-HTTP]) specifies the use of HTTP Alternative Services for an HTTP origin to advertise the availability of an equivalent HTTP/3 endpoint on a certain UDP port by using the "h3" ALPN token. Note that **HTTP/3's ALPN token ("h3") identifies not only the version of the application protocol, but also the version of QUIC itself**; this approach allows unambiguous agreement between the endpoints on the protocol stack in use.

On the one hand, this avoids some VN… on the other hand,...

‘h3-0x385af930’, ‘doq-0x385af930’, ...

Or does quic v2 have to “update” HTTP/3 to use ‘h3’?

```
Updates: 3261, 3329, 3436, 3470, 3501, 3552,
         3568, 3656, 3749, 3767, 3856, 3871,
         3887, 3903, 3943, 3983, 4097, 4111,
         4162, 4168, 4217, 4235, 4261, 4279,
         4497, 4513, 4531, 4540, 4582, 4616,
         4642, 4680, 4681, 4712, 4732, 4743,
         4744, 4785, 4791, 4823, 4851, 4964,
         4975, 4976, 4992, 5018, 5019, 5023,
         5024, 5049, 5054, 5091, 5158, 5216,
         5238, 5263, 5281, 5364, 5415, 5422,
         5456, 5734, 5878, 5953, 6012, 6042,
         6083, 6084, 6176, 6347, 6353, 6367,
         6460, 6614, 6739, 6749, 6750, 7030,
         7465, 7525, 7562, 7568, 8261, 8422
Category: Best Current Practice
```

# Proposal #3a - Edit ALPN Registry

QUIC Versions

| | | | |
|---|---|---|---|
| HTTP/3 | 0x68 0x33 ("h3") | 00000001, ab38347f, 324ab071 | [RFC-ietf-quic-http-34] |
| SMB2 | 0x73 0x6D 0x62 ("smb") | N/A | [https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/5606ad47-5ee0-437a-817e-70c366052962] |
| IRC | 0x69 0x72 0x63 ("irc") | N/A | [RFC1459] |
| DoQ | 0x64 0x6f 0x71 (“doq”) | 00000001, ab38347f | RFC XXXX |

# Proposal #3b - Edit QUIC Version Registry

ALPNs

| Value | Status | Specification | Date | Change Controller | Contact | Notes | |
|---|---|---|---|---|---|---|---|
| 0x00000000 | permanent | [RFC9000] | 2021-02-11 | IETF | [QUIC_WG] | Reserved for Version Negotiation | N/A |
| 0x00000001 | permanent | [RFC9000] | 2021-02-11 | IETF | [QUIC_WG] | | h3, doq |

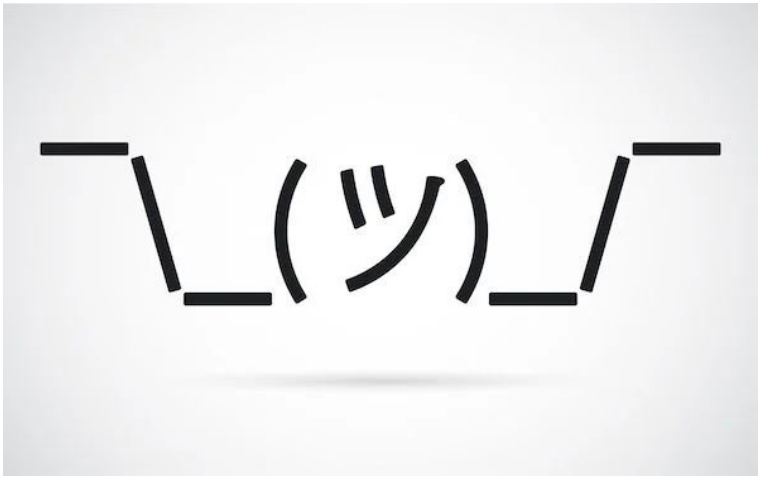
0xab38347f
0x324ab071

h3, doq

h3

3c,3d: list unsupported versions/ALPNs

# Proposal #4




Just do the best we can in the document text

- New applications describe known supported QUIC versions
- New versions describe supported ALPNs

# Version Aliasing & Protected Initials

- Version Aliasing: positive response at IETF 109, but few reviews
- Redesigned the fallback mechanism
- First connection problem: ECH, or “Protected Initials”

| Property | ECH | Protected Initials | Version Aliasing |
|---|---|---|---|
| Fields Protected | Some of Client Hello | All Initial Payloads | All Initial Payloads |
| Delay when server loses its keys | 1 RTT | 2 RTT | 2 RTT |
| Works with TLS over TCP | Yes | No | No |
| First-connection protection | Yes | Yes | No |
| Prevents Initial packet injection attacks | No | Yes | Yes |
| Symmetric Encryption Only | No | No | Yes |
| Greases the Version Field | No | No | Yes |
| Prevents Retry injection attacks | No | No | Yes |
| No trial decryption | No | No | Yes |

# Next steps

- Reviews (especially security reviews) -- are PIs worth it?
- Adoption?
- Implementation?

# Option 1: ALPN includes QUIC version

| | | |
|---|---|---|
| SunRPC | 0x73 0x75 0x6e 0x72 0x70 0x63 ("sunrpc") | [RFC-ietf-nfsv4-rpc-tls-10] |
| HTTP/3 | 0x68 0x33 ("h3") | [RFC-ietf-quic-http-34] |
| SMB2 | 0x73 0x6D 0x62 ("smb") | [https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/5606ad47-5ee0-437a-817e-70c366052962] |
| IRC | 0x69 0x72 0x63 ("irc") | [RFC1459] |

| | | |
|---|---|---|
| DoQ | 0x64 0x6f 0x71 (“doq”) | RFC AAAA |
| HTTP/3 - QUICv04ac27d4 | 0x68 0x33 0x2d 0x30 0x34 0x61 0x63 0x32 0x37 0x64 0x34 (“h3-04ac27d4”) | RFC BBBB |
| DoQ - QUICv04ac27d4 | 0x64 0x6f 0x71 0x2d 0x30 0x34 0x61 0x63 0x32 0x37 0x64 0x34 (“doq-04ac27d4”) | RFC BBBB |
| PRVideo - QUICv1 | 0x70 0x72 0x75 0x69 0x64 0x65 0x6f (“prvideo”) | RFC CCCC |
| PRVideo -QUICv054ac27d4 | 0x70 0x72 0x75 0x69 0x64 0x65 0x6f 0x2d 0x30 0x34 0x61 0x63 0x32 0x37 0x64 0x34 (“prvideo-04ac27d4”) | RFC CCCC |
| HTTP/3 - QUICva745f001 | 0x68 0x33 0x2d 0x61 0x37 0x34 0x35 0x66 0x30 0x30 0x31 (“h3-a745f001”) | RFC DDDD |
| DoQ - QUICva745f001 | 0x64 0x6f 0x71 0x2d 0x61 0x37 0x34 0x35 0x66 0x30 0x30 0x31 (“doq-a745f001”) | RFC DDDD |
| PRVideo - QUICva745f001 | 0x70 0x72 0x75 0x69 0x64 0x65 0x6f 0x2d 0x61 0x37 0x34 0x35 0x66 0x30 0x30 0x31 (“prvideo-a745f001”) | RFC DDDD |

Alt-Svc basically gives us the right version - very little VN

Either: applications know what versions are available to request the right ALPN, or QUIC implementations take the root from the application and append the version