# draft-ietf-quic-applicability-12
# draft-ietf-quic-manageability-12

Mirja Kühlewind and Brian Trammell
July, 2021, online IETF-111 meeting

# What happened so far...

- 1. WGLC in Feb 2021
  - Lots of input and some discussion at IETF-110 in March
  - Thanks for all the reviews!
- -11 submitted in April
- 2. WGLC in April 2021
  - Again quite a bit of input but only few actually non-editorial changes (see next slides)
  - Thanks again for all the re-reviews!
- -12 submitted in June
- One new issue on GitHub since… see later slides

# Updates to applicability statement in -12

- Discussion and clarification about use of ALPN token “h3” (PR #375)
  - Thanks Martin Duke and Lucas!
- Refined guidance on use of DSCP (PR #383)
  - Thanks Gorry!
- Refined text on ACK frequency (for constraint networks) (PR #386)
  - Thanks Gorry, Martin Thomson, Ian, and Lucas!

# Updates to manageability statement in -12

- Clarified guidance on PMTUD (PR #370)
  - Thanks Gorry!
- SNI parsing clarified (PR#388) and appendix A removed
  - Thanks David and Ian! (one more editorial PR ready to merge...)

# New issue(s)

- (We need to double-check contributors and the acknowledgement section!)
- New PR on source port recommendations (PR #392)
  - Raised by mnot on list
  - Discussion also on-going in tsvwg
  - **Is this guidance QUIC-specific?**
  - **Should we add it?**
  - **Is there also NAT guidance needed in the manageability statement?**
- Also: More guidance about server privacy after resumption or migration?
  - This came up in another recent discussion on the mailing list
  - But belonged in transport draft…?

```
+ ## Source Port Selection
+
+ Some UDP protocols are vulnerable to reflection attacks, where an attacker is
+ able to direct traffic to a third party as a denial of service. For example,
+ these source ports are associated with applications known to be vulnerable to
+ reflection attacks (often due to server misconfiguration):
+
+ * port 53 - DNS {{?RFC1034}}
+ * port 123 - NTP {{?RFC5905}}
+ * port 1900 - SSDP {{SSDP}}
+ * port 5353 - mDNS {{?RFC6762}}
+ * port 11211 - memcached
+
+ Services might block source ports of protocols known to be vulnerable to
+ reflection, to avoid the overhead of processing large numbers of packets by
+ their QUIC implementations. However, this practice has negative effects on
+ clients: not only does it require establishment of a new connection, but in
+ some instances, might cause the client to avoid using QUIC for that service for
+ a period of time, downgrading to a non-UDP protocol (see {{fallback}}).
+
+ As a result, client implementations are encouraged to avoid using source ports
+ associated with protocols known to be vulnerable to reflection attacks.
```