# Securing field communications within intelligent transportation systems (ITS): SNMP and TLS1.3

26 July 2021, for IETF Security Area

K. Vaughn  M. Vanderveen

# Purpose

- Background for requesting update for RFC 6353
- Review of changes needed
- Identify path forward

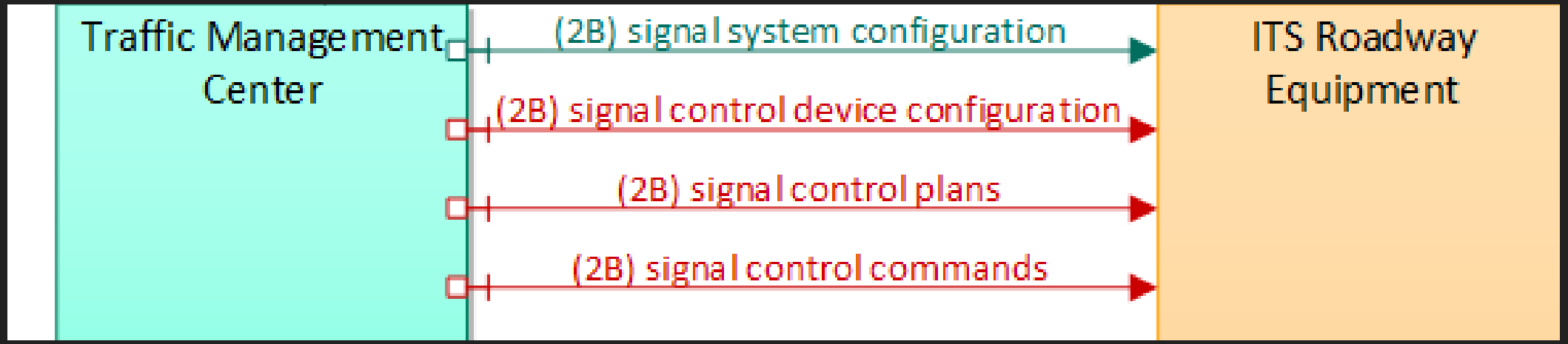
# Background

Why the ITS community is interested in an update to RFC 6353

# Existing usage of SNMP within ITS

- Primary protocol for ITS field devices
  - Center-to-field
  - Field-to-field
- Used Internationally
- Includes safety-critical data

- Many types of devices, including:
  - Signal controllers
  - Electronic signage
  - Various sensors
  - Highway lighting
  - Ramp meters



# Secure SNMP deployment (2018)


- SNMPv3 over (D)TLS using RFC 6353
  - Uses the (D)TLS X.509 certificate for access control
  - Uses bi-directional X.509 certificates
  - Uses TLSv1.2

- (D)TLSv1.2 has known security vulnerabilities

# Potential solutions

- Migrate to an alternative protocol
  - Experts have recently reasserted their support for using SNMP
    - Supported by both private and public sector
    - Deemed SNMP to be an appropriate design for our environment
    - Cost to migrate to different protocol would be high
- Update RFC 6353 recommendations
  - Not currently being addressed within IETF
  - ITS experts interested in working with IETF
    - Could develop as NTCIP standard, if needed

# Status

- ITS experts have drafted an initial, preliminary update for RFC 6353

# Review changes needed

TLS 1.3 cipher suite

# Change overview

- Changes necessitating a new document
  - Update fingerprint algorithm and related MIB objects to reflect 2-octet cipher suite
- Other clarifications needed as part of update
  - Clarify that authentication and privacy are always provided (i.e., a part of 1.3)
  - Update references (e.g., TLS 1.3 vs TLS 1.2)

# Change overview

- Subjective changes
  - Prohibit use of 0-RTT mode of TLS 1.3 to prevent playback attacks
  - Recommend disabling of USM
  - Mandate previous recommendations
    - Prohibit the use of SSL or TLS versions prior to 1.2
    - Prohibit use of prior versions of SNMP over TLSTM
    - Requiring each command generator to have its own certificate
    - Prohibit use of CommonNames
- Subjective non-changes
  - Retain use of same port numbers

# Path forward

Is the IETF interested?

# Optional paths to deployment

Is the IETF security area interested in advancing such a document assuming editor support is provided?

Standards Track (proposed)

Track Experimental

Informational Track

Non-IETF publication

# Format of document

- Two Possible Approaches
  - Replacement of RFC 6353
    - Reflected in draft 00 (which removed support for DTLS)
  - Update to RFC 6353
    - Reflected in current draft 01, which supports DTLS 1.3 now that it is being finalized
- The update cuts the document length in half, but it is still 40+ pages due to the 30 page MIB