

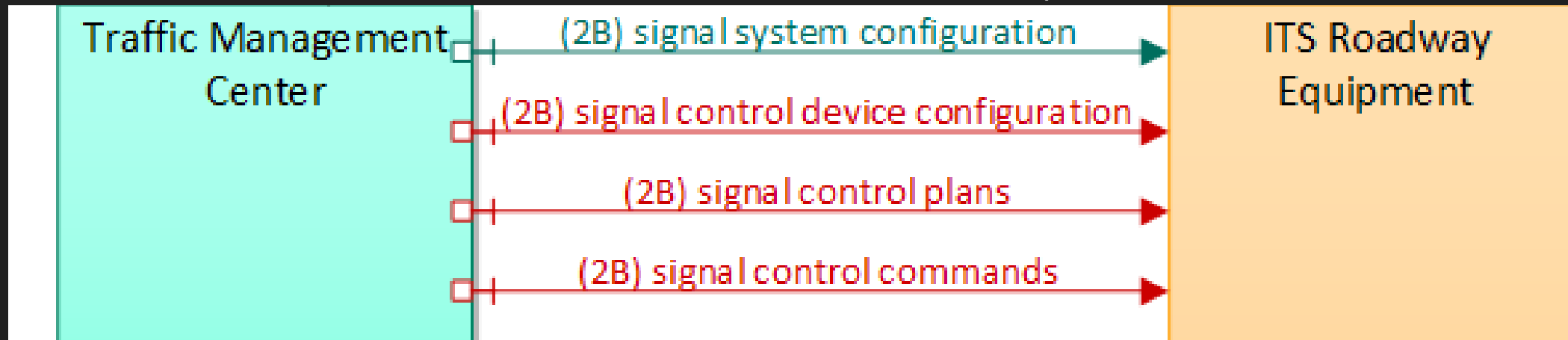
Securing field communications within intelligent transportation systems (ITS): SNMP and TLS1.3

9 November 2021, for IETF Operations and Maintenance Area WG

K. Vaughn M. Vanderveen

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



Change overview

- Changes necessitating a new document
 - Update fingerprint algorithm and related MIB objects to reflect 2-octet cipher suite
 - Alternative: Require IANA to maintain 1-octet hash ID for (D)TLS 1.3; clarify rules for fingerprint
- Other clarifications needed as part of update
 - Update references (e.g., (D)TLS 1.3 vs (D)TLS 1.2)
 - Clarify that authentication and privacy are always provided (i.e., a part of 1.3)

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

Major Questions to Resolve

- Does the OPSAWG wish to adopt this work?
- How to best address the fingerprint issue
 - Revise MIB
 - Require IANA to maintain 1-octet hash identifier
- Document format
 - Update to RFC 6353
 - Obsolete RFC 6353 and replace
 - New RFC without obsoleting RFC 6353

Can be resolved via the reflector