draft-ietf-6tisch-minimal-security

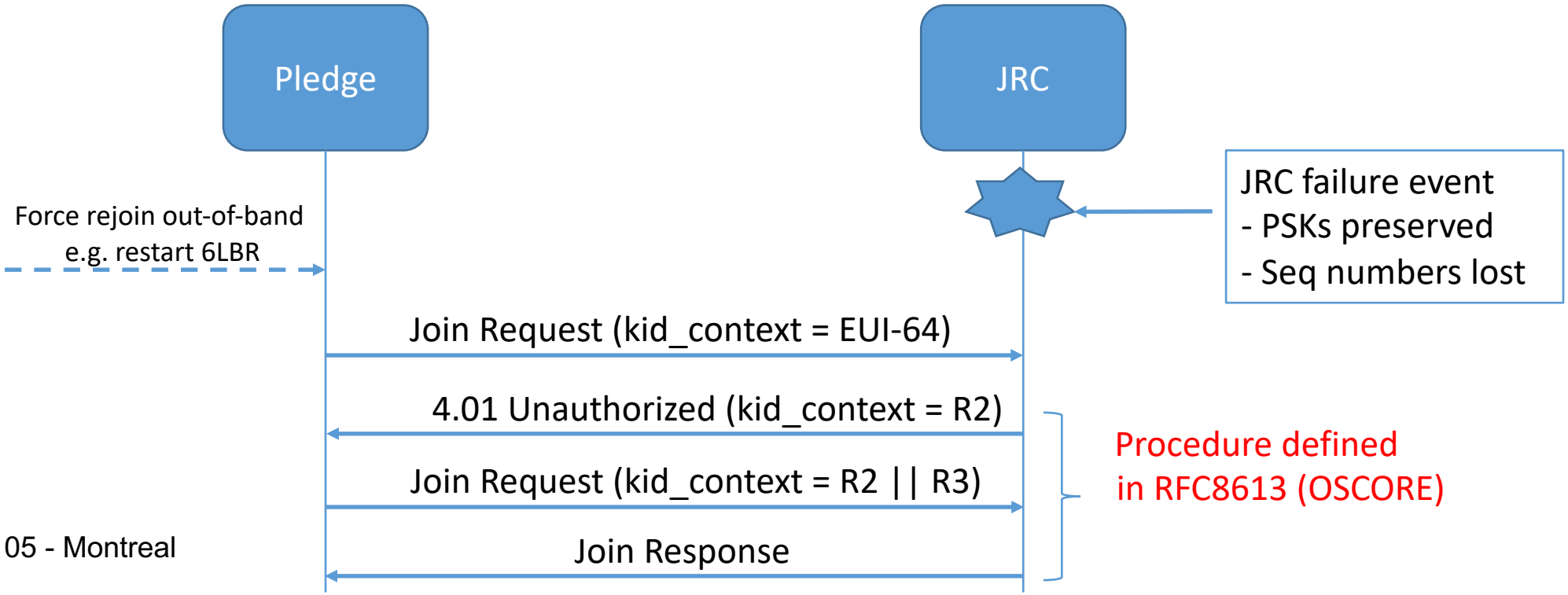
- Authors: Mališa Vučinić (Ed.)
  Jonathan Simon
  Kris Pister
  Michael Richardson

Status

- Published -10 after Prague and -11 after shepherd's review
- Shipped to AD
- Goal of the presentation
  - Summary of changes in -10 and -11
  - Discuss ASN replay attack

Updates in -10

- Failure handling after Göran Selander's 2nd WGLC review
  - Expanded Section 8.3.3.
  - RECOMMEND usage of OSCORE Appendix B.2 to renegotiate context ID



Updates in -10

- CoJP Error handling
  - Christian Amssus' comment on the ML
  - Redefined CBOR parameters
  - CoAP request now carries self-contained CBOR object describing the error
  - Malformed and Unsupported parameters
- Editorial: Rekeying process is now a separate section

```
Unsupported_Configuration = [
       + parameter            : Unsupported_Parameter
]

Unsupported_Parameter = (
         code                 : int,
         parameter_label      : int,
         parameter_addinfo    : nil / any
)
```

Name	Value	Description	Reference
Unsupported	0	The indicated setting is not supported by the networking stack implementation.	[[this document]]
Malformed	1	The indicated parameter value is malformed.	[[this document]]

Updates in -11

- Pascal Thubert's shepherd review
- Update RFC6775 reference to RFC8505
- Editorial:
  - Elaborate on SHOULDs in Section 6.1.2 on setting DSCP code points
  - Nits

Latest discussions on the ML

Background:
L2 nonce in IEEE 802.15.4 TSCH

Octets: 8	5
Source Address	ASN

Figure 9-2—CCM* nonce in TSCH mode

Absolute slot number
Local notion of time

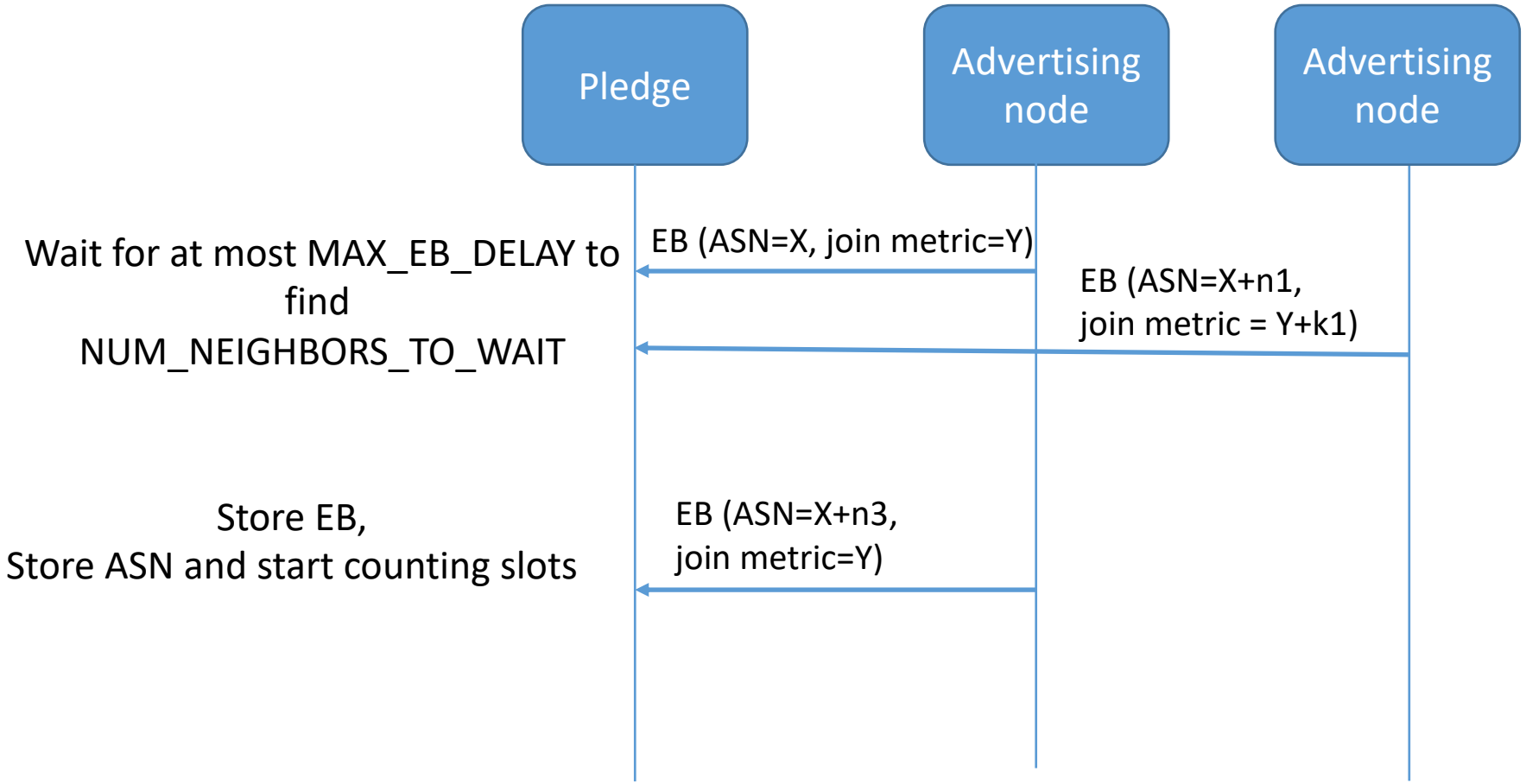
8-byte globally
unique EUI-64

Octets: 3	1	2	2
IEEE 802.15 CID	0x00	PAN ID	Short address

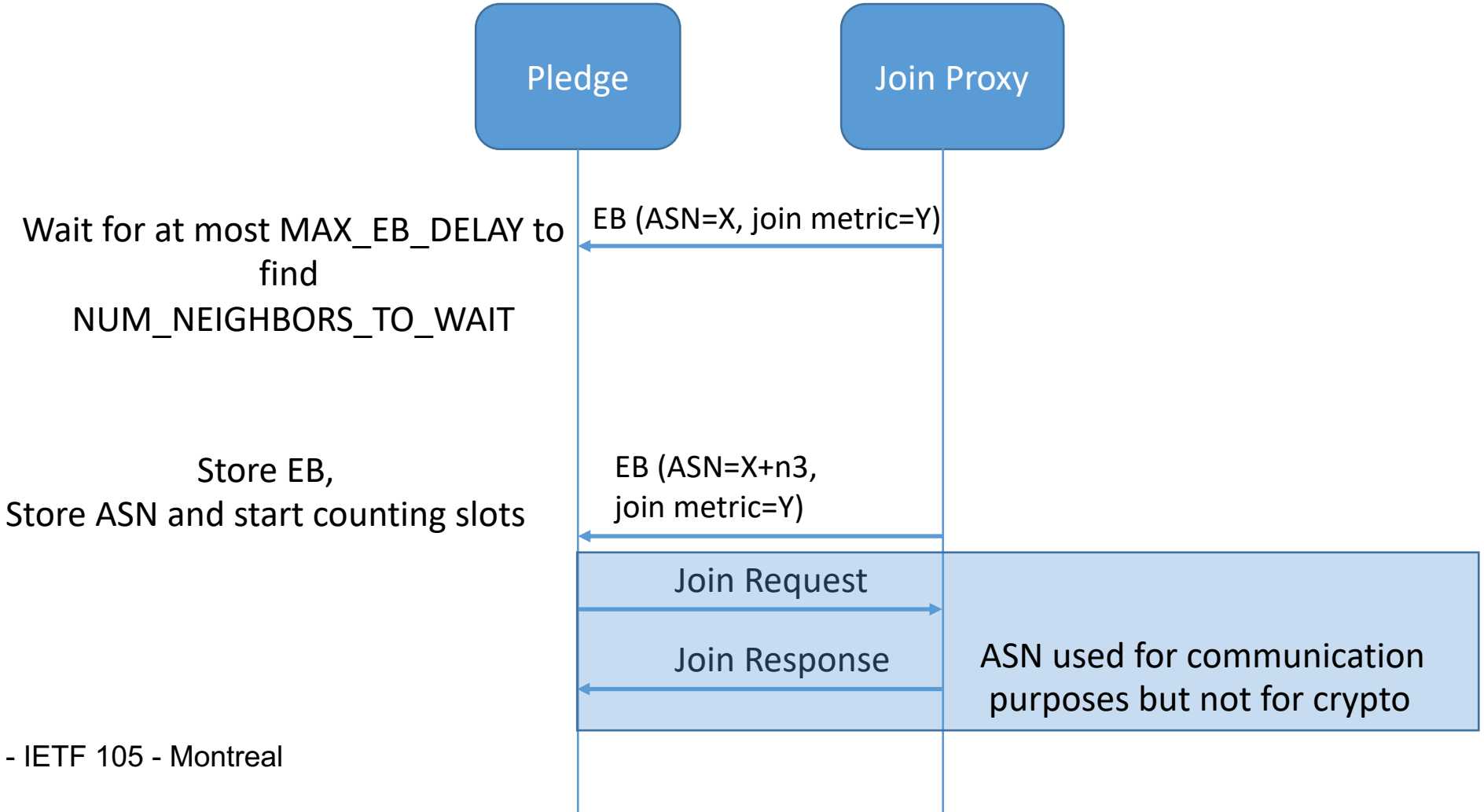
Figure 9-3—Source Address field for TSCH mode with short addressing

Locally unique 2-byte address

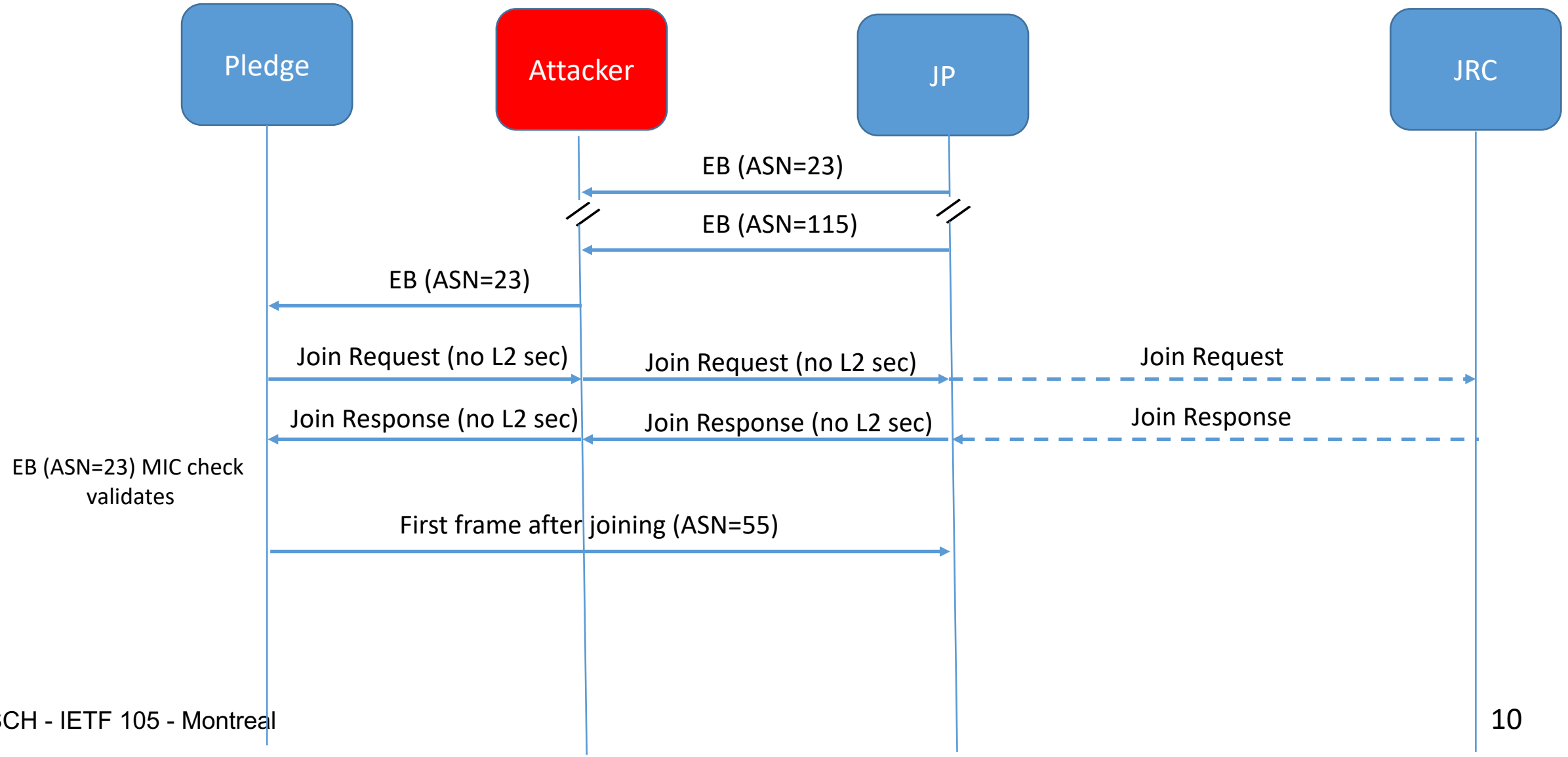
Background: Distribution of ASN in IEEE 802.15.4 TSCH and 6TiSCH



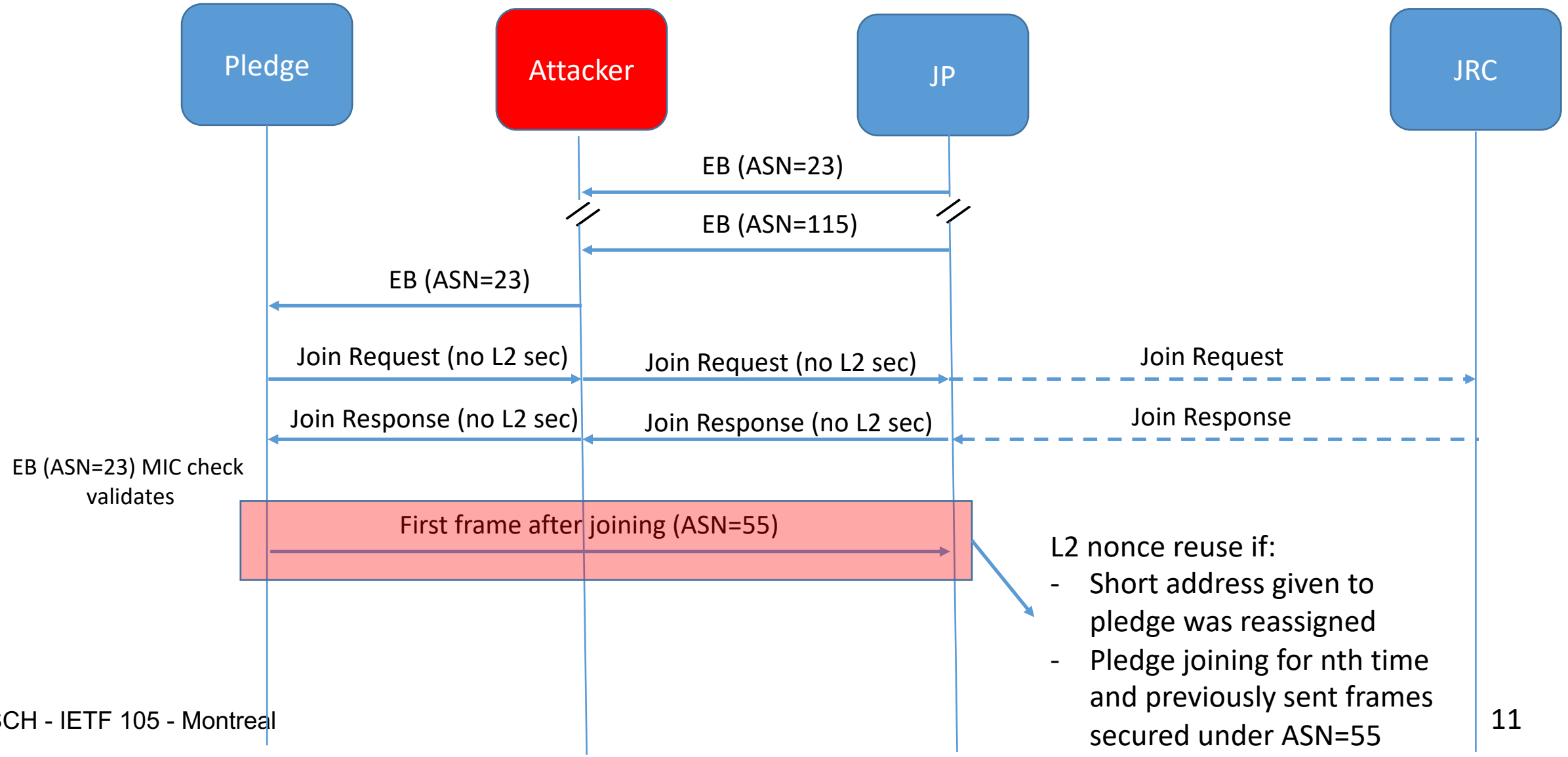
Background: Distribution of ASN in IEEE 802.15.4 TSCH and 6TiSCH



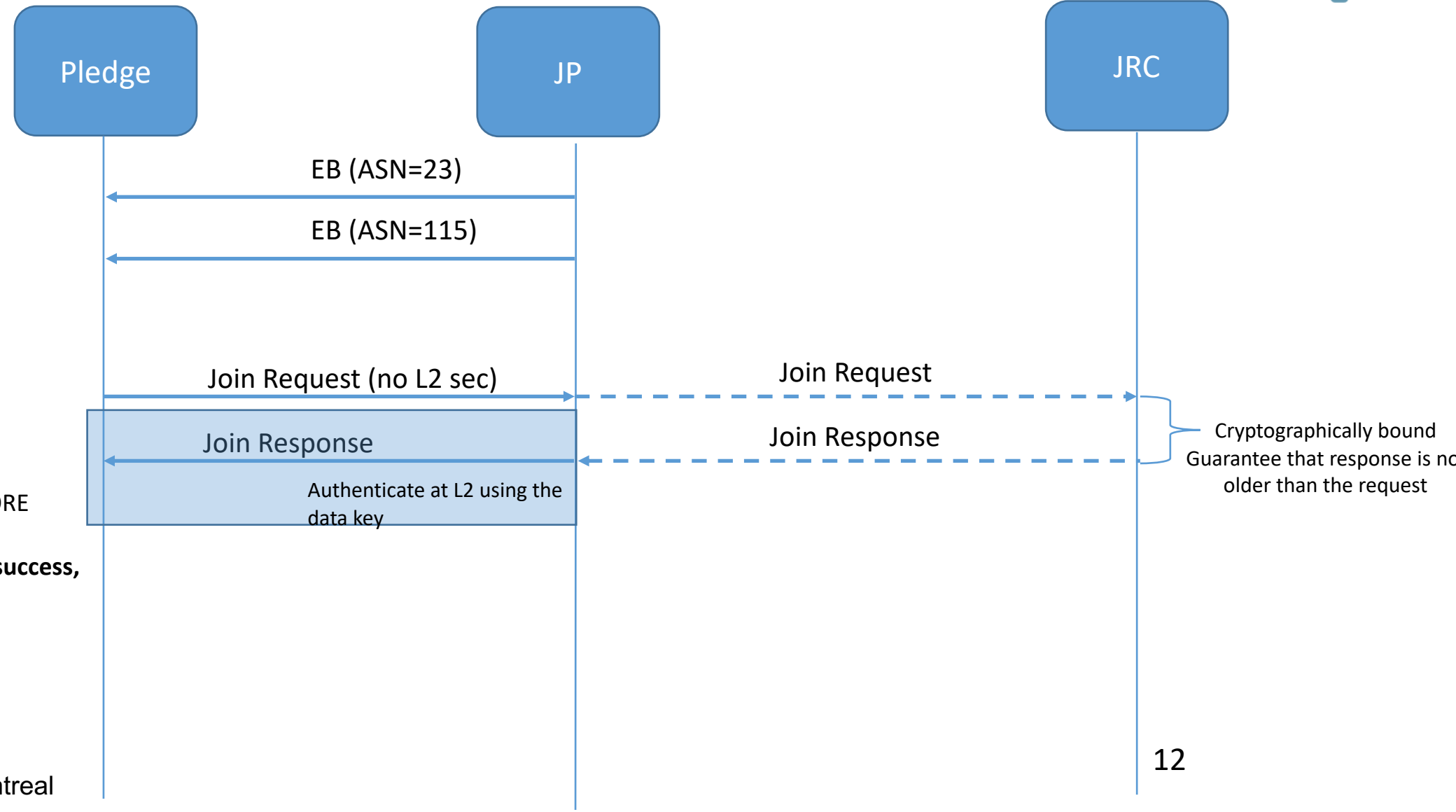
ASN replay attack



ASN replay attack



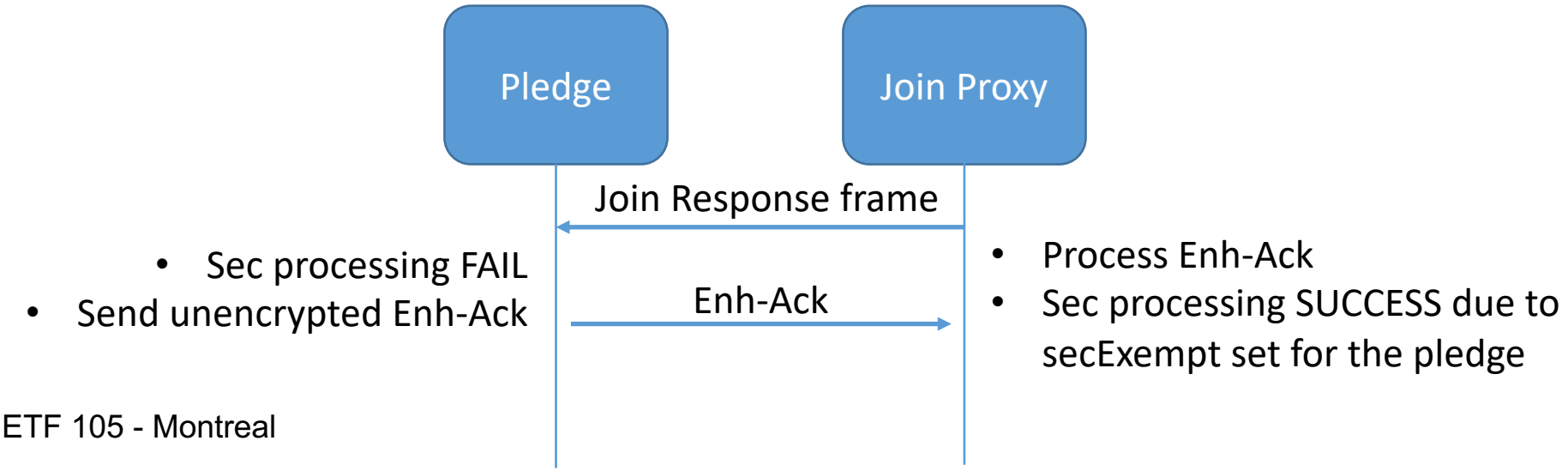
Proposed resolution



1. Discard L2 verification
2. Decrypt & verify OSCORE
3. Get the L2 keys
4. **Verify L2 MIC and on success, declare ASN as valid**

Proposed resolution - Caveats

- Reception of the Join Response at Pledge
  - Security processing at L2 fails due to the missing key
  - Use 802.15.4 *promiscuous* mode during the join process at the pledge
  - Will pass the frame to the upper layer in any case
- L2 ACK of the Join Response



TSCH and CCM security proofs

- *CCM** security proofs apply if nonce contains the security level
- Not the case with TSCH nonce (see Slide 7)
- Security proofs of *CCM* still apply
- Limitation is that a single key can only be used with fixed-length authentication tags

Proposed resolution:
Implementations MUST use different link-layer keys when using different authentication tag (MIC) lengths, as using the same key with different authentication tag lengths might be unsafe.
For example, this prohibits the usage of the same key for both MIC-32 and MIC-64 levels.
See Annex B.4.3 of {{IEEE802.15.4}} for more information.

Conclusion

- Shipped to AD already
- Note on ASN replay attack resolution needed
- Publish in -12