

# Trusted Path Routing

draft-voit-rats-trustworthy-path-routing-00

Eric Voit

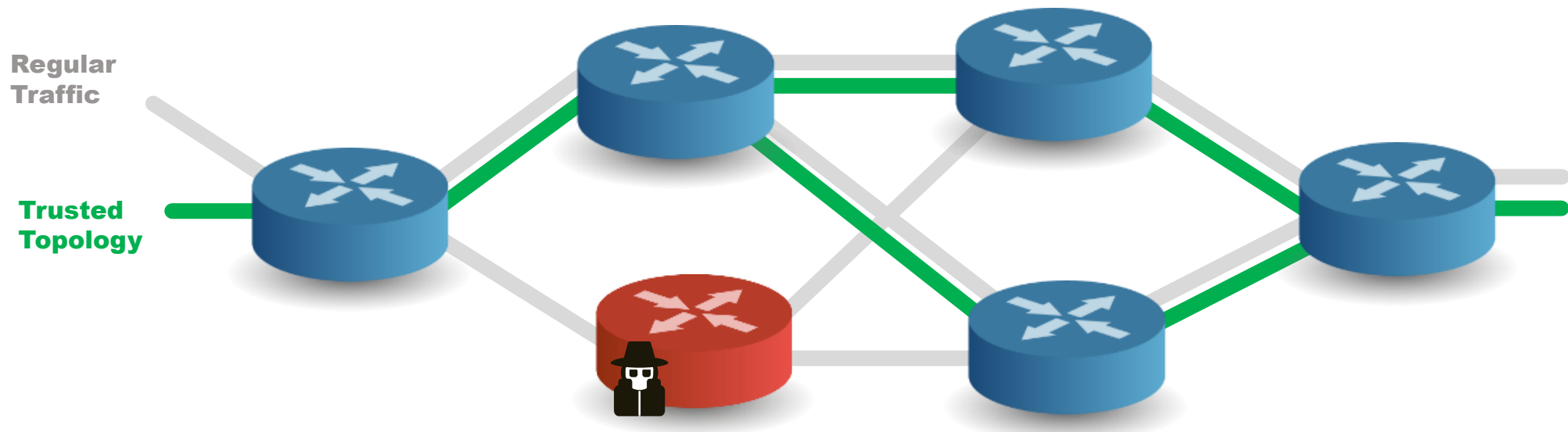
[evoit@cisco.com](mailto:evoit@cisco.com)

Cisco Systems, Inc.

IETF 108, July 29<sup>th</sup> 2020, RATS WG

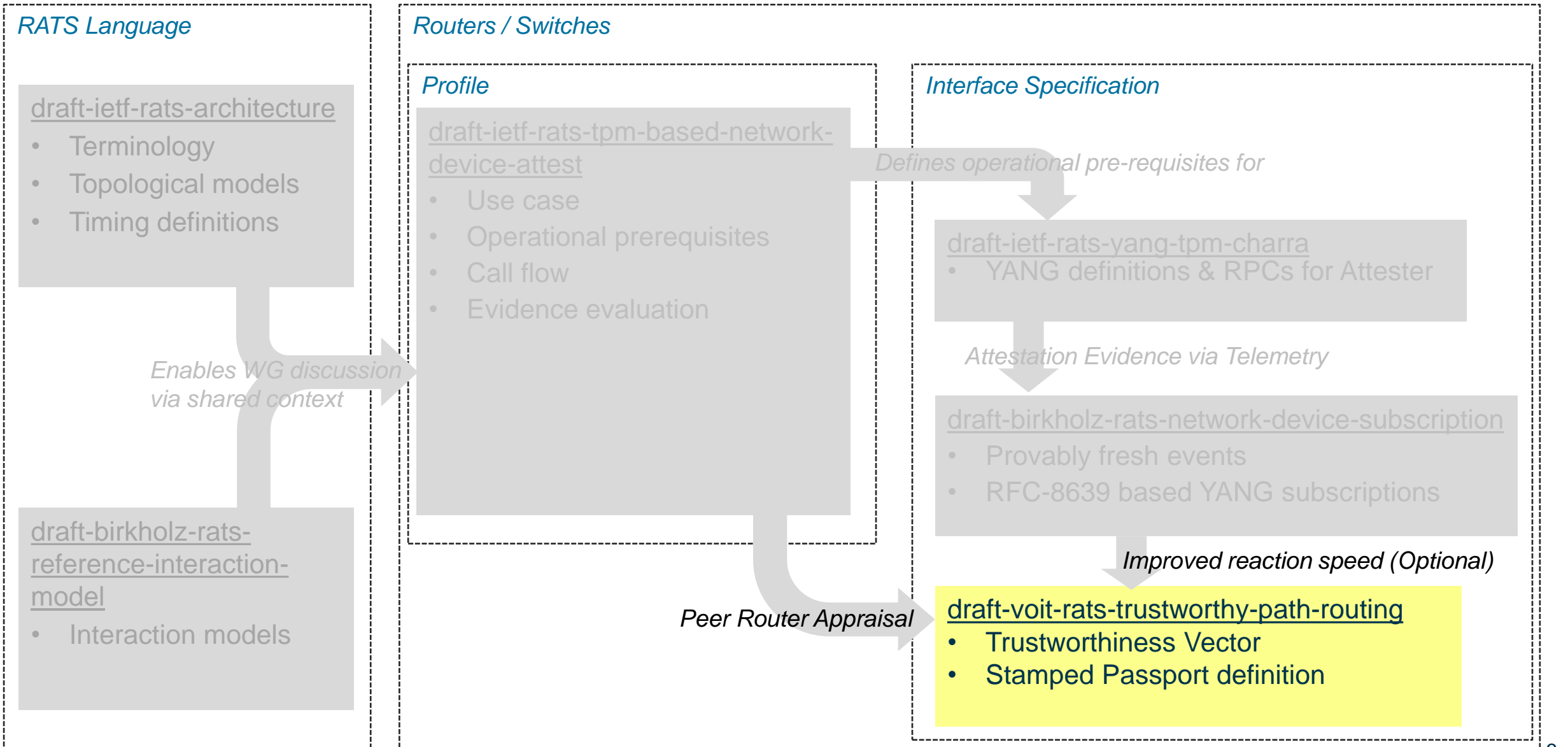
# Trusted Path Routing

- Trusted Topology dynamically maintained based on Attestation Results
- Sensitive flows bypass insecure / potentially compromised network devices



- Boot integrity not verified
- Actively exhibits Indicators of Compromise
- Software isn't patched
- Doesn't have hardware cryptoprocessor
- Currently unattested

# Relationship to other RATS drafts



# Trustworthiness Level

An assertion from a Verifier that is *externally actionable*:

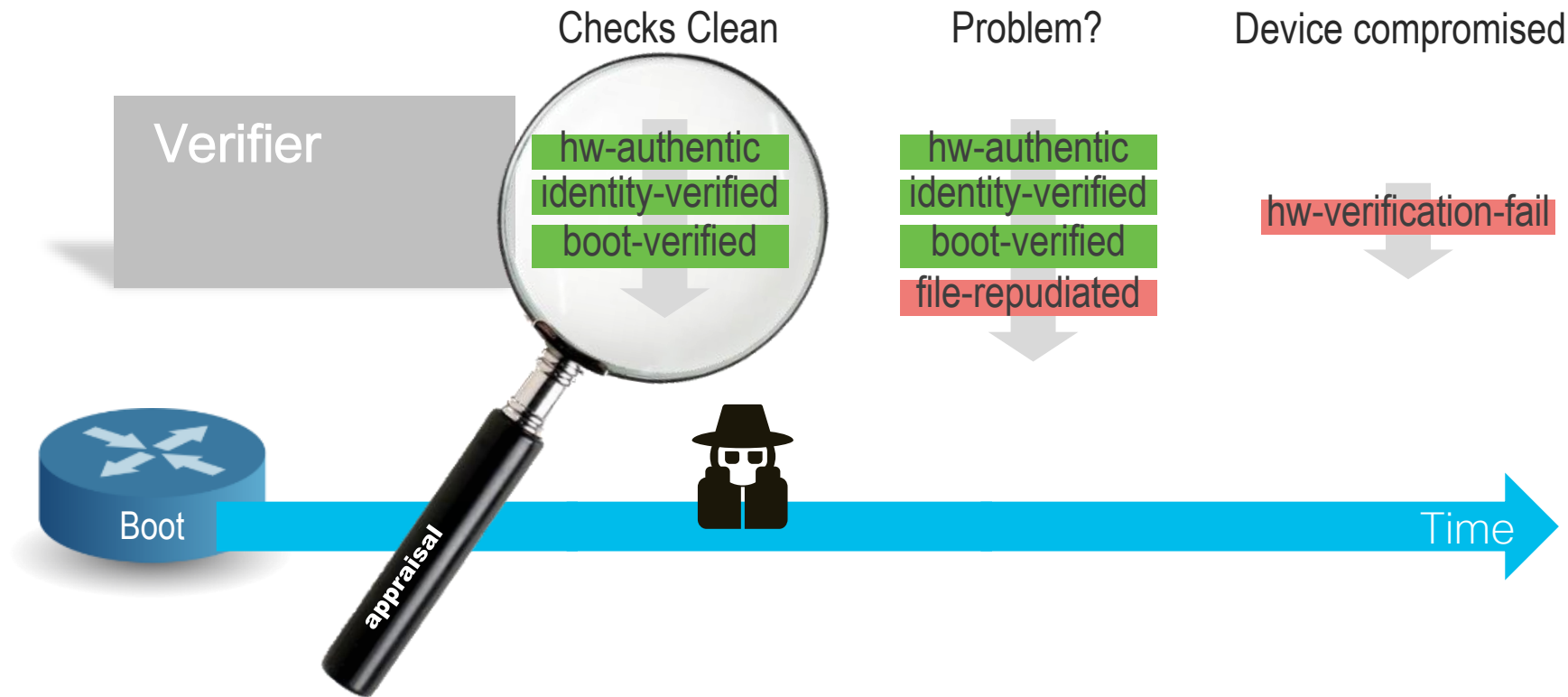
HW Integrity	hw-authentic	Device has authentic hardware
	fw-authentic	Device has authentic firmware
	hw-verification-fail	Device has failed its hardware or firmware verification
Unique Identity	identity-verified	Device has a verified unique identity
	identity-fail	Can't verify a Device's unique identity
Boot Integrity	boot-verified	Device is Boot Integrity Verified
	boot-verification-fail	Device has failed its Boot Integrity verification
Filesystem Integrity	files-verified	All relevant files in file system recognized
	file-repudiated	File(s) exist which should not be present



- These could also be encoded as EAT
- Does the WG want to standardize Appraisal Results & encodings?

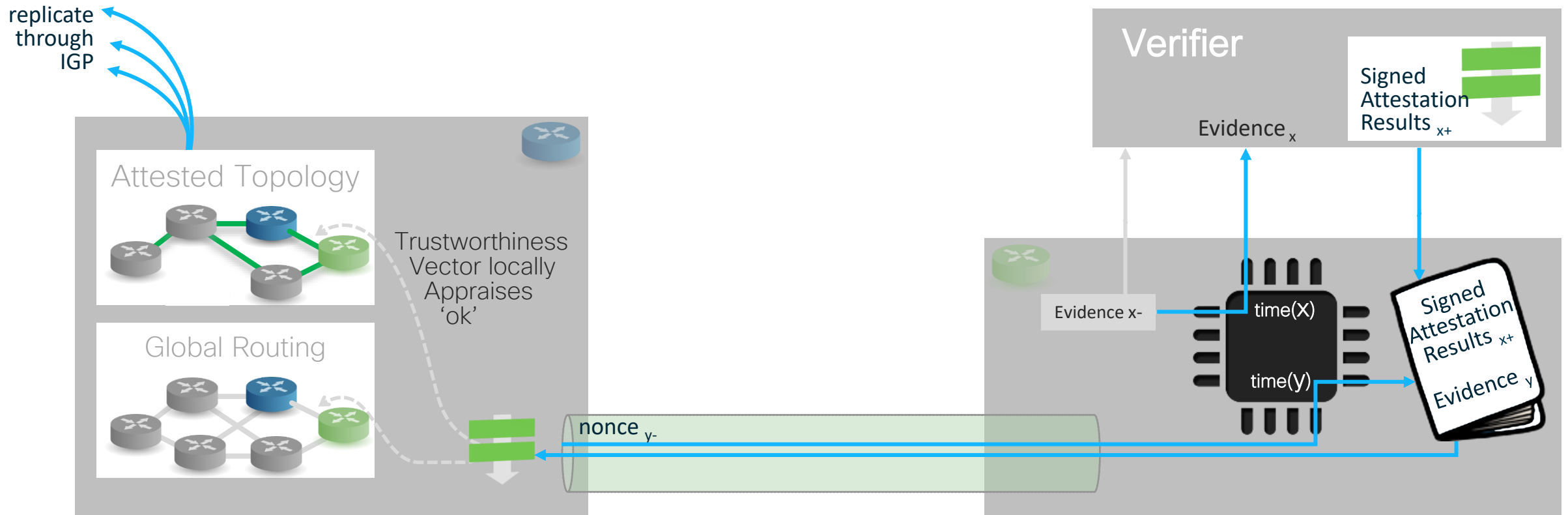
# Trustworthiness Vector

- One to Many Trustworthiness Levels assigned during an appraisal cycle.
- Verifier signs Vector and pushes to Router at each appraisal



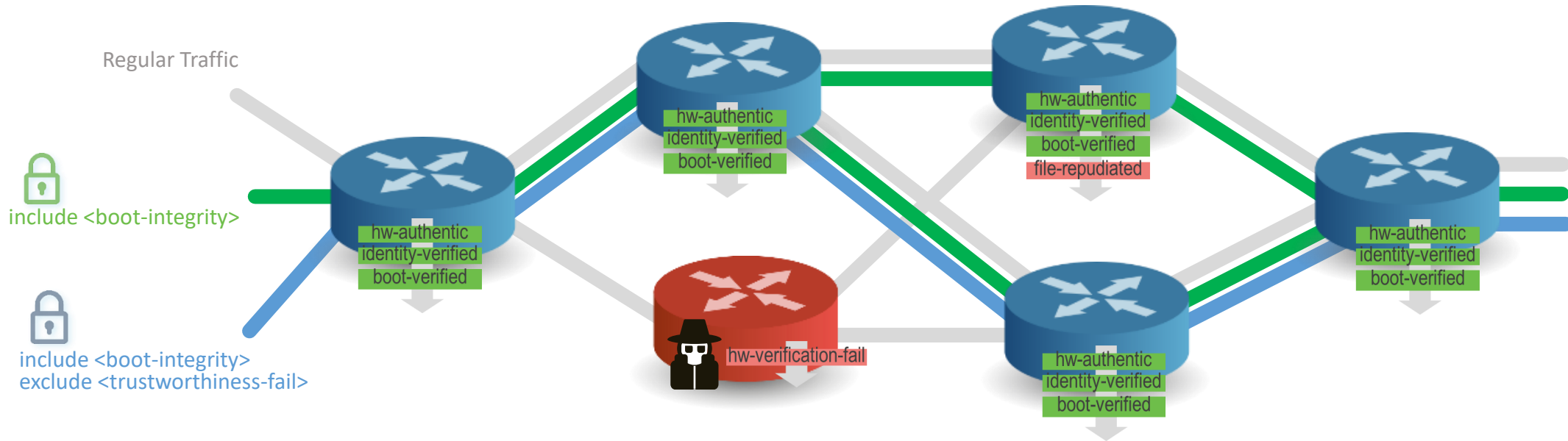
# Trusted Path Routing

- Link adjacencies added to Trusted Topology based on latest appraisal
- Existing routing protocol distribution



# Trusted Path Routing

- Custom Trusted Topologies can be dynamically maintained based on Attestation Results



# Next

- Does the WG want to standardize Appraisal Results & encodings?
- Definition of EAP payload
- Is there WG interest in progression and eventual adoption?