CCNx Specification Changes

Overview of Changes

- Optional header expansion
  - Content object hash specification
- New hash rules for agility
  - Multiple hash restrictions
  - Restrictions identify explicit hash algorithm
- Nameless object inclusion
  - Clear definition of nameless objects
  - Clear interest<->content matching rules

New Optional Headers

Name	Type	Value
SHA256 ContentObjectHash	T_HASH_SHA256 (0x00)	32-byte hash
SHA512 ContentObjectHash	T_HASH_SHA512 (0x01)	64-byte hash

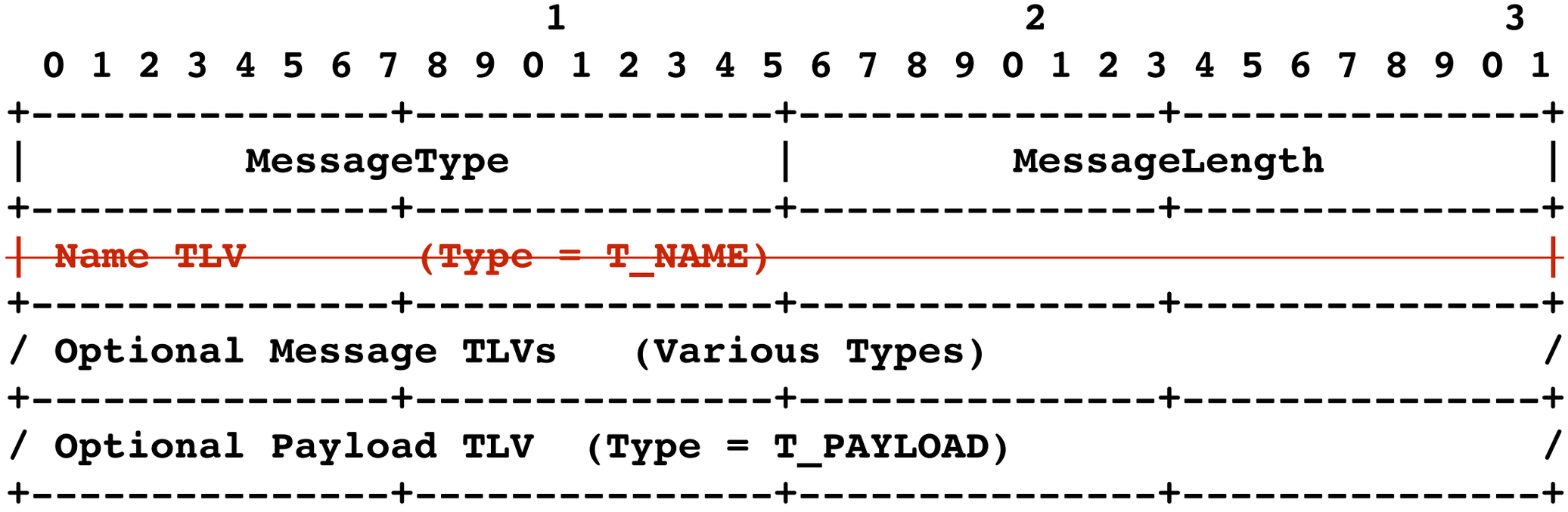
Currently, only SHA-256 is supported for the ContentObjectHash

Modified Hash Rules

- Interests:
  - T_OBJHASHRESTR would be recast to:
    - T_OBJECTHASHRESTR_SHA256
    - T_OBJECTHASHRESTR_SHA512
      - Interests can specify more than one hash restriction (if known) and routers match against the strongest restriction.
        - If both SHA512 and SHA256 restrictions are provided routers will give the SHA512 hash priority
- Content Objects:
  - Routers may optionally check verify the COH against the Interest restriction
  - If a Content Object doesn't carry a T_HASH_* optional header, the hash must be computed
  - If a Content Object carries a T_HASH_* optional header, the hash can be used outright or re-computed
- Goal: producers or border routers can pre-compute the hash(es) of a Content Object and put them in packet to minimize work done in the core

Nameless Objects

Nameless objects are content objects with **no name TLV**



CCN Matching Rules

Content / Interest	Name	Name, Keyld	Name, Hash	Name, Keyld, Hash	Keyld	Hash	Keyld, Hash
Name	(1)	(1)	(1)	(1)	~	~	~
Name, Keyld	(1)	(2)	(1)	(2)	~	~	~
Name, Hash	(3)	(3)	(3)	(3)	(4)	(4)	(4)
Name, Keyld, Hash	(3)	(3)	(3)	(5)	(4)	(4)	(4)

~ = matching not possible

Rule Set

Rule ID	Description
1	Match on Name equality
2	Match on Name and KeyId equality
3	Match on Name and Hash equality (computing the hash if necessary)
4	Match on Hash equality (computing the hash if necessary)
5	Match on Name, KeyId, and Hash equality (computing the hash if necessary)