



101st IETF/IRTF, Mar. 2018, London

# CCNinfo: Discovering Content and Network Information in Content-Centric Networks

---

draft-asaeda-icnrg-ccninfo-00

Hitoshi Asaeda (NICT)

Xun Shao (KIT)

# Changes

---

- Replace Contrace with CCNinfo
  - Old: “Contrace: Traceroute Facility for Content-Centric Network”
    - <https://tools.ietf.org/html/draft-asaeda-icnrg-contrace-04>
  - New: “CCNinfo: Collecting Content and Network Information in Content-Centric Networks”
    - <https://tools.ietf.org/html/draft-asaeda-icnrg-ccninfo-00>
    - Several small changes from contrace-04

# Brief introduction of CCNinfo

---

- What is CCNinfo?
  - CCNinfo aims for discovering/retrieving information about the network (incl. multi-path) topology and in-network cache in CCN
- CCNinfo collects the information
  - Caching router (per prefix)
  - Number of hops from consumer to caching router / publisher
  - RTT between consumer and caching router / publisher
  - Cache hit ratio
    - Number of the accesses (i.e., received Interests) per cache / chunk
  - Lifetime and expiration time per cache / chunk
  - Path stretch ("d / P")
    - where "d" is the hop count of the data and "P" is the hop count from the consumer to the publisher

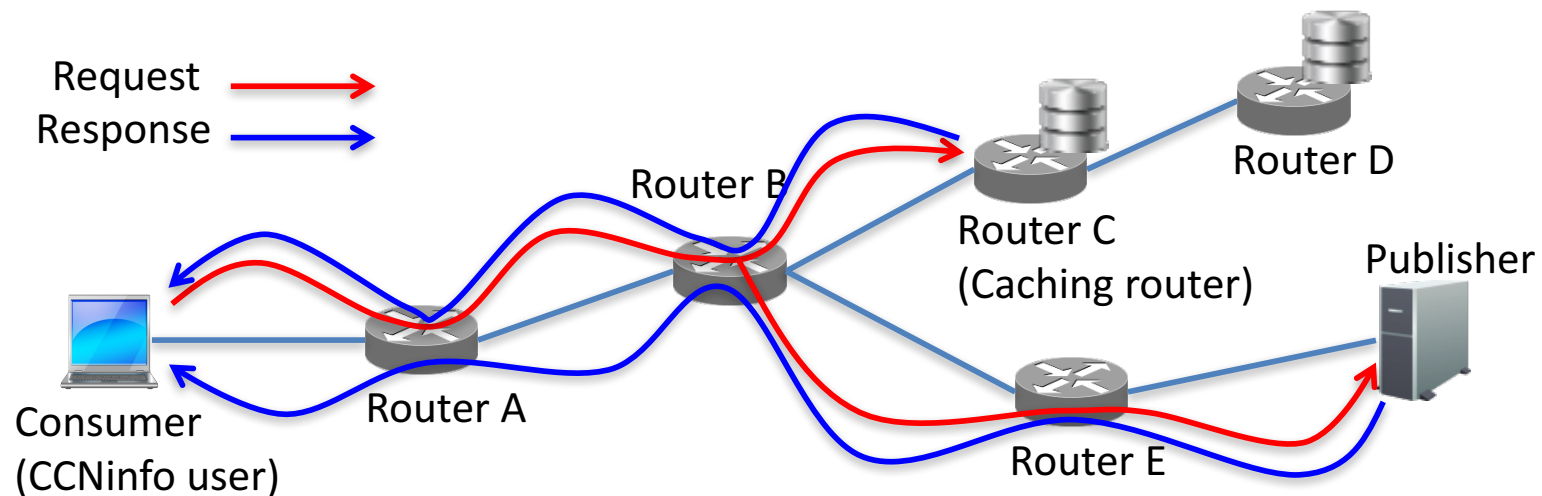
# Brief introduction of CCNinfo – cont'd

---

- Why is CCNinfo needed? What is the benefit?
  - For protocol analysis
    - Effectiveness, robustness, and cost of designed networks
      - Hop count / RTT for content retrieval, multipath, in-network caching algorithm
    - Characteristics of content
      - Content popularity, cache hit ratio
  - As an OAM tool
    - Operation
      - Cache lifetime or expiration time
    - Monitoring
      - CS capacity and usage at router, num. of interests per content
    - Trouble shooting
      - Availability of caching routers and publishers
  - Yet, policy-based information provisioning
    - Fine-grained access control and policy configuration for information disclosure highly required

# CCNinfo Basic Behavior

- **Request message** is initiated by CCNinfo user and forwarded toward caching router or publisher based on the FIB in a hop-by-hop manner
- Request message includes **Request block** and **Report block(s)**
- **Reply message** is initiated by caching router or publisher and forwarded toward CCNinfo user based on the PIT entry
- Reply message includes **Reply block** and **Reply sub-block(s)**

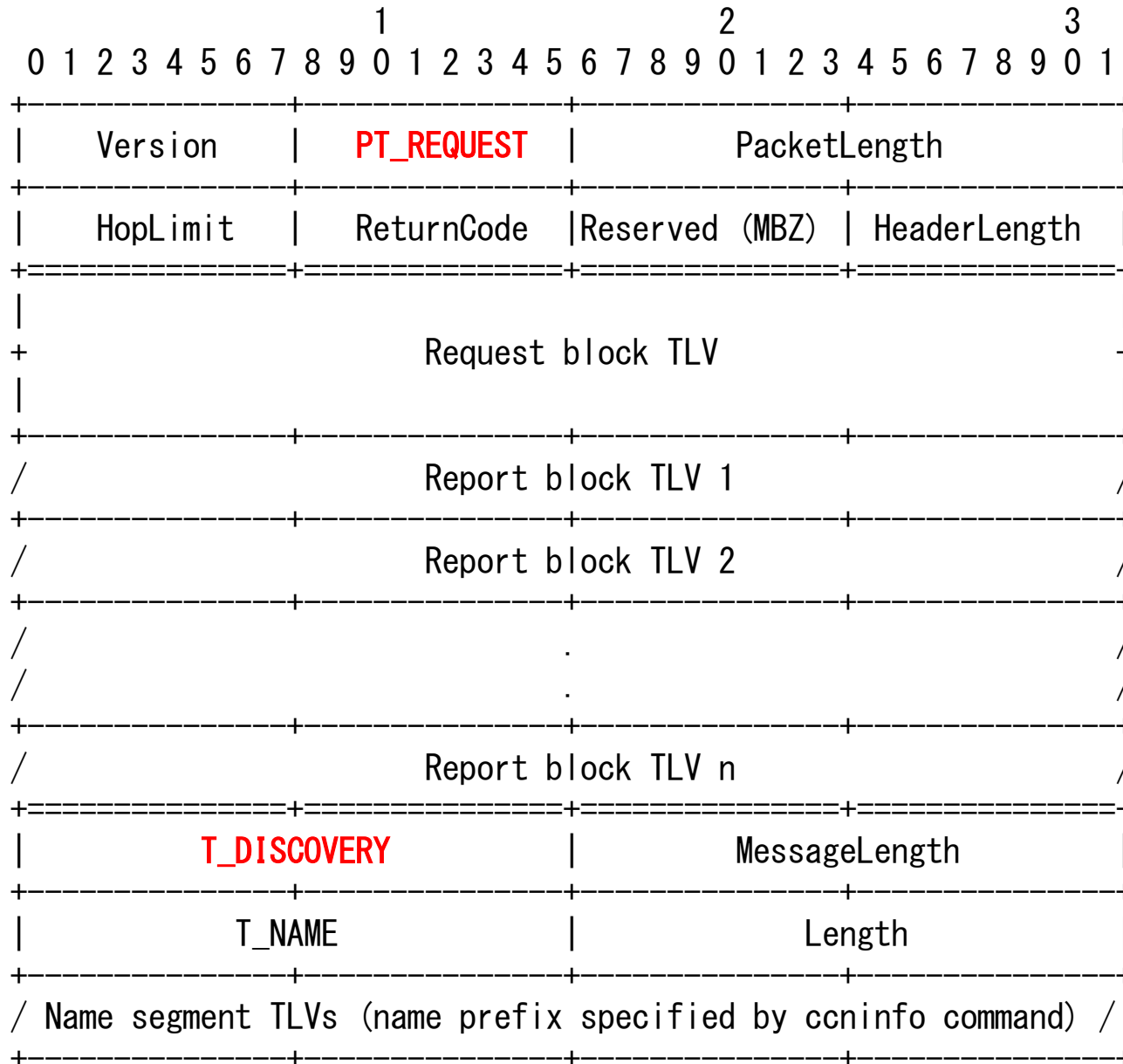


# CCNinfo Request/Reply Messages

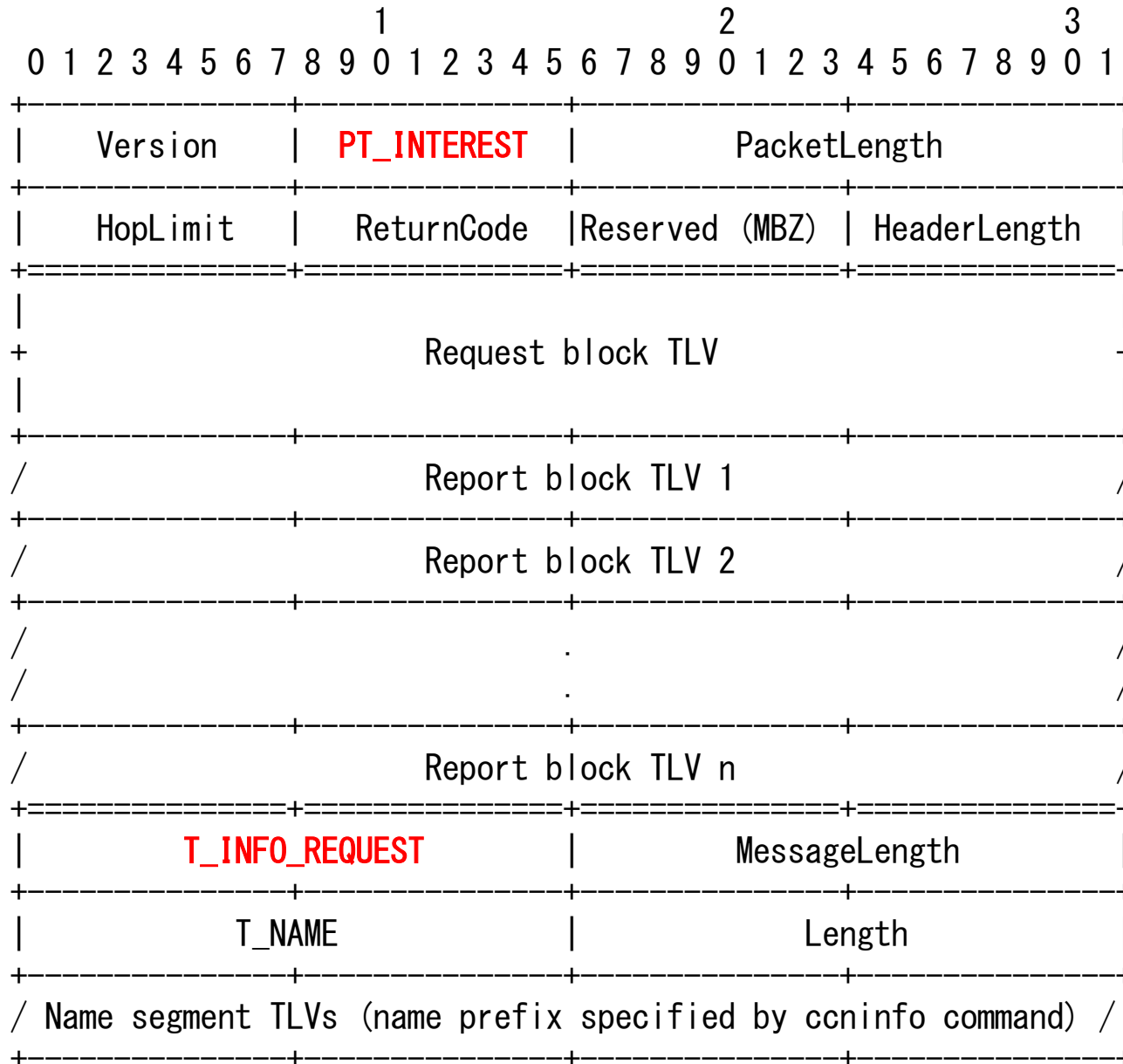
---

- Compatible with CCNx-1.0 TLV format
- CCNinfo Request Message
  - Request message consists of a fixed header, Request block TLV, Report block TLV(s), and Name TLV
- CCNinfo Reply Message
  - Reply message consists of a fixed header, Request block TLV, Report block TLV(s), Name TLV, and Reply block/sub-block TLV(s)
- **Case 1 (defined in the current I-D)**: New Request type (PT\_REQUEST) and Reply type (PT\_REPLY) values in the fixed header are used
- **Case 2**: No new protocol type, but new message type values (T\_INFO\_REQUEST / T\_INFO\_REPLY) for interest / data are required
  - PT\_INTEREST and PT\_CONTENT are used

# Case 1: Request Message

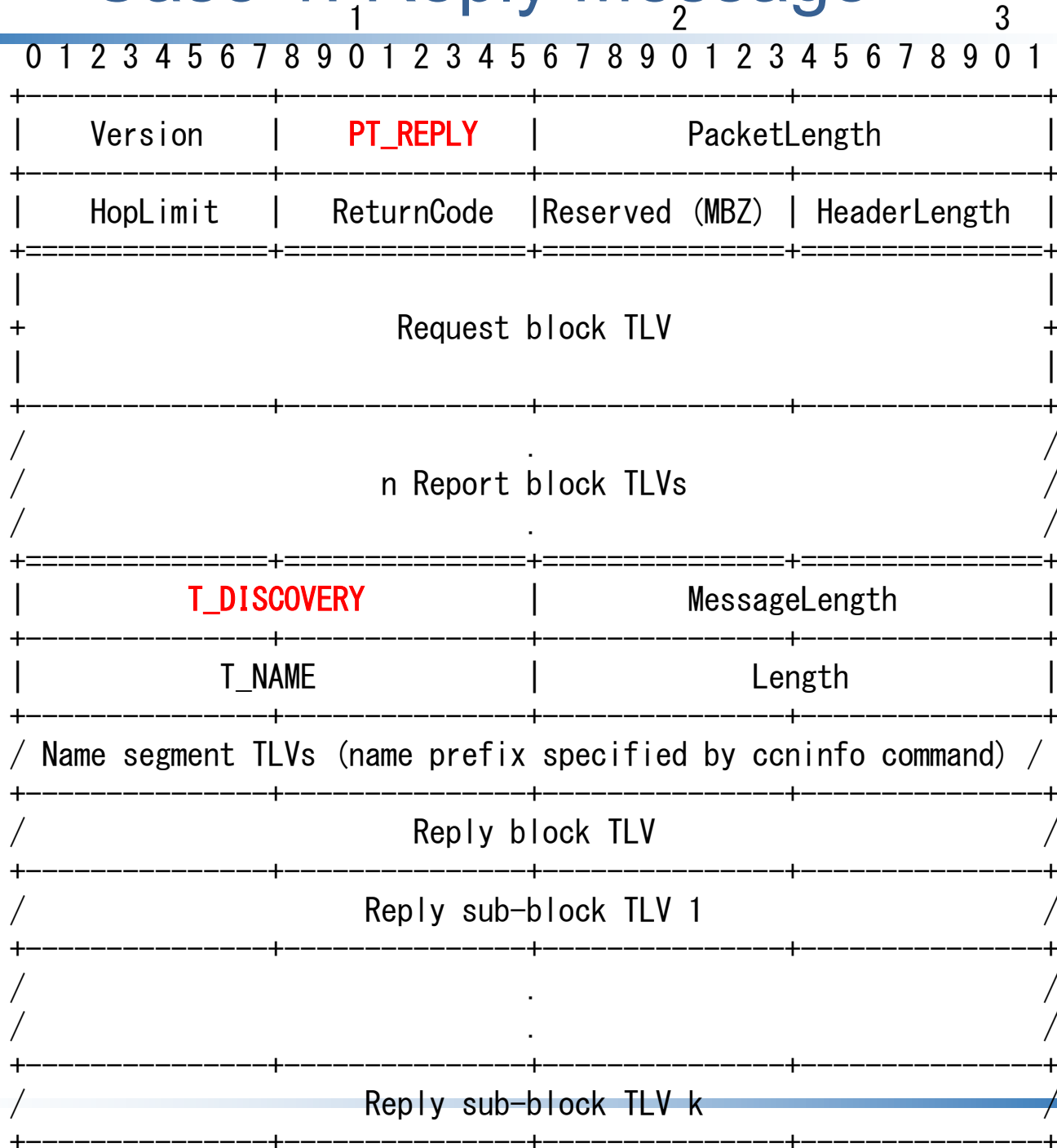


# Case 2: Request Message

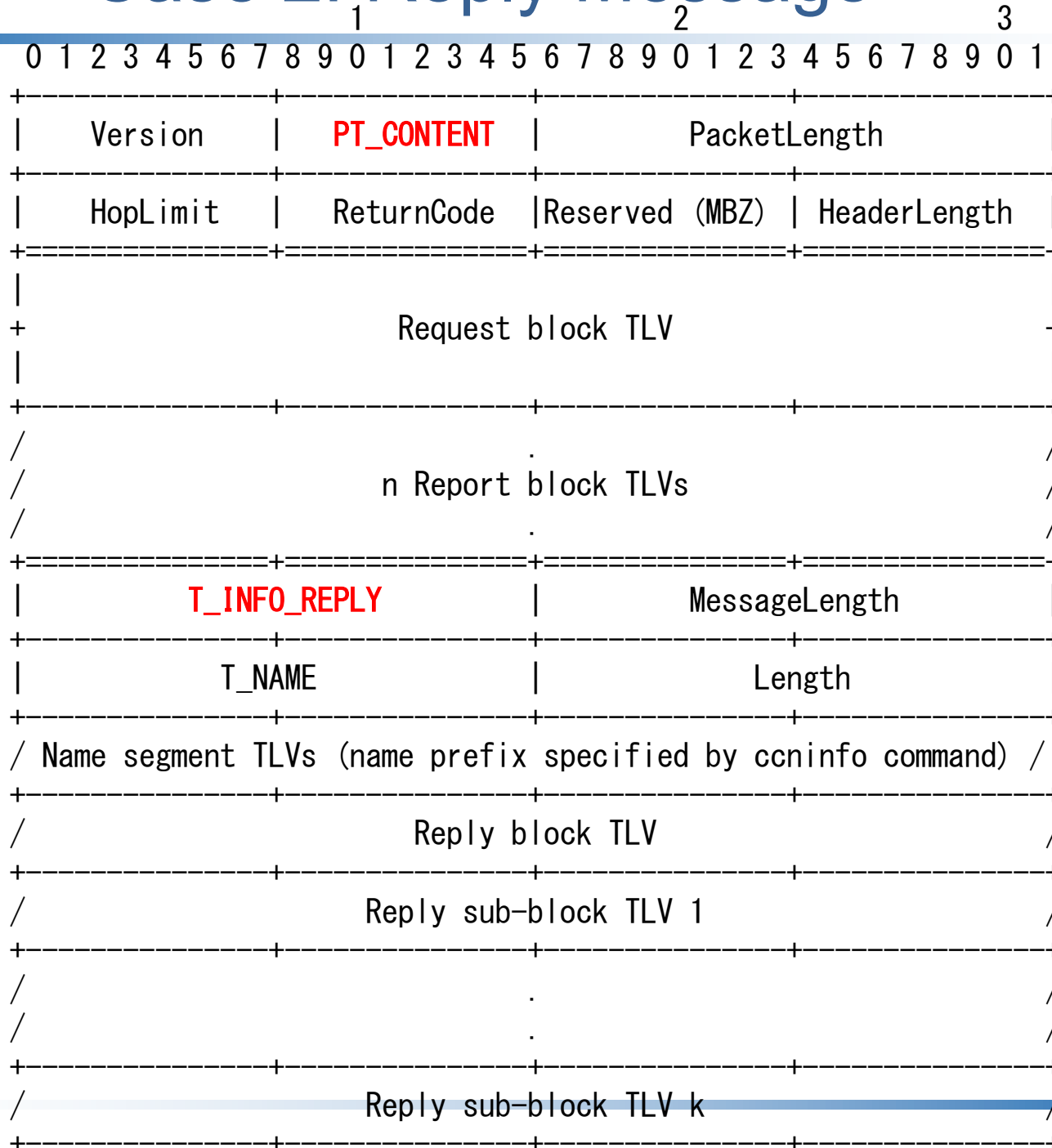




# Case 1: Reply Message



# Case 2: Reply Message



## Case 1 vs. Case 2

---

- Different operations from the regular Interest / Data are required (= less trouble, easy-to-understand implementation)
  - Routers SHOULD NOT remove the PIT entry created by the CCNinfo Request until timeout value expires.
  - CCNinfo Requests SHOULD NOT result in PIT aggregation in routers during the Request message transmission.
  - CCNinfo Replies MUST NOT be cached in routers upon the Reply message transmission.

## Case 1 vs. Case 2 – cont'd

---

- Policy-based information provisioning: different and fine-grained access control for authorized / unauthorized Requests are required, for example,
  - Router SHOULD forward the Request message to the upstream router toward the content forwarder
  - However, according to the “Node Identifier” in the Request block or “Signature” in the ValidationAlgorithm TLV, router SHOULD configure either of:
    - (1) All (all cache information is disclosed)
    - (2) Partial (cache information with the particular name prefix can (or cannot) be disclosed), or
    - (3) Deny (no cache information is disclosed)

# A brief comparison with ICN traceroute

	CCNinfo	ICN traceroute
Objective	Collect comprehensive information to support diagnostic test and statistical analysis	Obtain limited information of specific route for debug and diagnosis
Methodology	Explore the tree structure from the consumer to the routers and the producer	Explore the basic information of specific route between the consumer and the producer
Algorithm	Interest-like requests, but waiting for the reply until time-out	Iterative algorithm similar with IP traceroute
Multipath	Works like ordinary interests	Possibly, but not specified
Protocol type	<b>Case 1:</b> New protocol types required <b>Case 2:</b> No new protocol type, but new type values for interest/data required	No new protocol type
Reserved name	No reserved name	Reserve “traceroute” suffix

# Summary

---

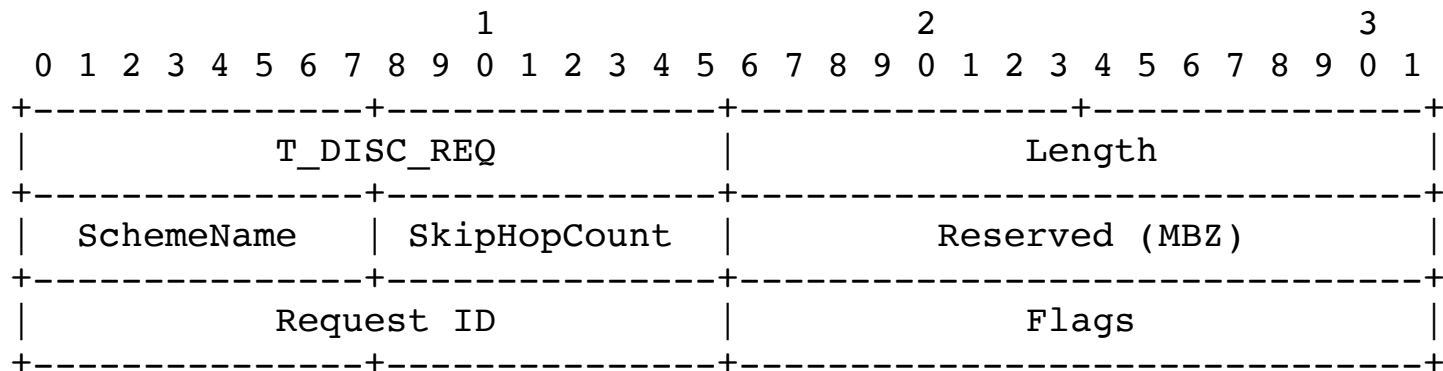
- CCNinfo, which is compatible with CCNx-1.0 TLV format, is a powerful network tool providing various information
- RG draft?
  - We'll then start discussion more on new message types, etc.

# Backup

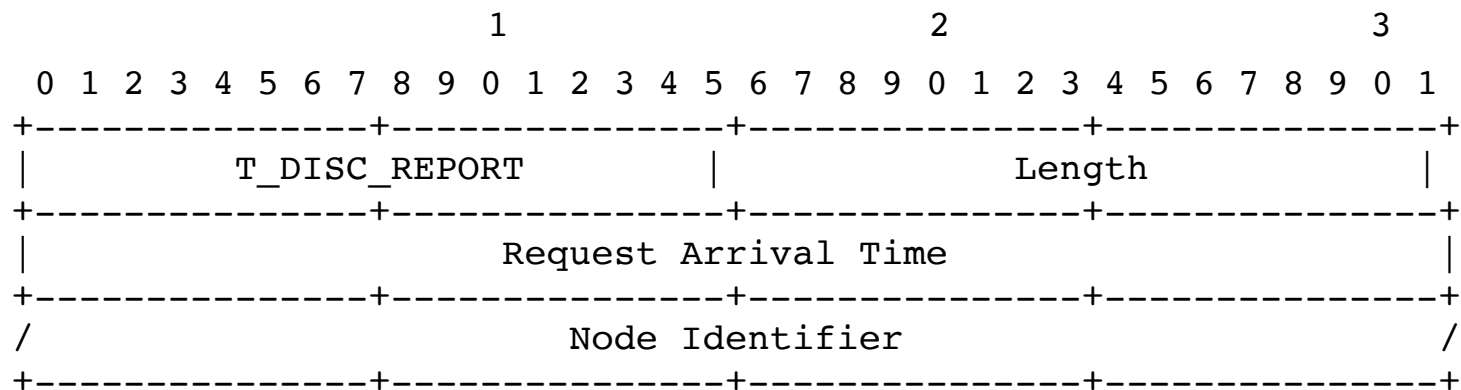
---

# Request Block and Report Block

- Request block



- Report block

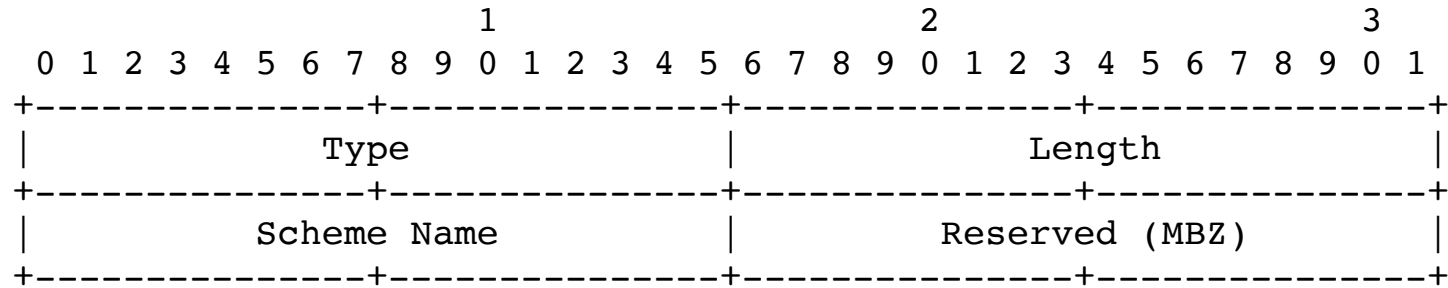




# Reply Sub-Block for T\_DISC\_CONTENT and T\_DISC\_CONENT\_OWNER

1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type										Length											
Content Size																					
Object Count																					
# Received Interest																					
First Seqnum																					
Last Seqnum																					
Cache Lifetime																					
Remain Cache Lifetime																					
T_NAME										Length											
/ Name segment TLVs (name prefix partially/exactly matched) /																					

# Reply Sub-Block for T\_DISC\_GATEWAY



# Security Considerations

---

- Policy-Based Information Provisioning for Request
  - Routers can reply the CCNInfo Reply with the ADMIN\_PROHIB return code without appending any Reply (sub-)block TLV
  - Permission, whether (1) All (all cache information is disclosed), (2) Partial (cache information with the particular name prefix can (or cannot) be disclosed), or (3) Deny (no cache information is disclosed), can be defined at routers
- Filtering of CCNInfo Users Located in Invalid Networks
  - Routers may support an access control mechanism to filter out Requests from invalid CCNInfo users located in invalid networks

# Security Considerations – cont'd

---

- Topology Discovery
  - If a network topology is a secret, CCNinfo Requests may be restricted at the border of the domain, using the ADMIN\_PROHIB return code
- Characteristics of Content
  - If publisher or content information is secret, CCNinfo Requests may be restricted at the border of the domain, using the ADMIN\_PROHIB return code
- Shortening CCNinfo Reply Timeout
  - Routers may configure the shorter timeout value to time out the Request
- Limiting Request Rates
  - Routers may rate-limit CCNinfo Requests by ignoring some of the consecutive messages.

# Security Considerations – cont'd

---

- Limiting Reply Rates
  - Routers in the traced path may rate-limit CCNInfo Replies.
- Adjacency Verification
  - Forwarding CCNInfo messages given from non-adjacent neighbor nodes/routers must be prohibited
  - Defining the secure way to verify the adjacency cannot rely on the way specified in CCNx message format or semantics; therefore a new TLV for adjacency verification using hop-by-hop TLV header will be defined in a separate document.