Ilya Moiseenko
Dave Oran

Path Steering in CCNx and NDN *a Refresher*

draft-oran-icnrg-pathsteering-05

Outline

- Introduction
- Design
- Packet Encoding
- Security Considerations

I. INTRODUCTION

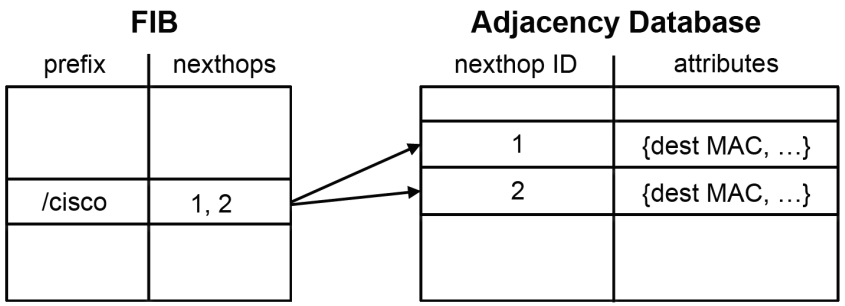
Problem Statement

- ICN communication is inherently multi-path and potentially multi-destination.
- No mechanism for consumers to direct Interest traffic onto a specific path.
  - Forwarding Strategies in ICN forwarders can spray Interests onto various paths
  - Consumers have a hard time interpreting failures and performance glitches
  - Troubleshooting and performance tools need path visibility and control to find problems and do simple measurements.

Motivations for Path Steering

- Discover, monitor and troubleshoot multipath network connectivity based on names and name prefixes:
  - Ping
  - Traceroute
- Accurately measure a performance of a specific network path.
- Multipath Congestion control needs to:
  - Estimate/Count number of available paths
  - Reliably identify a path
  - Allocate traffic to each path
- Traffic Engineering and SDN
  - Externally programmable end-to-end paths for Data Center and Service Provider networks

II. Design

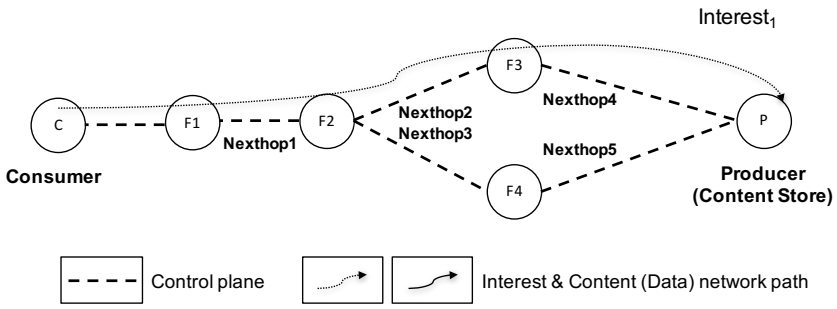


How to label paths?

What is a path label? One or more nexthop IDs

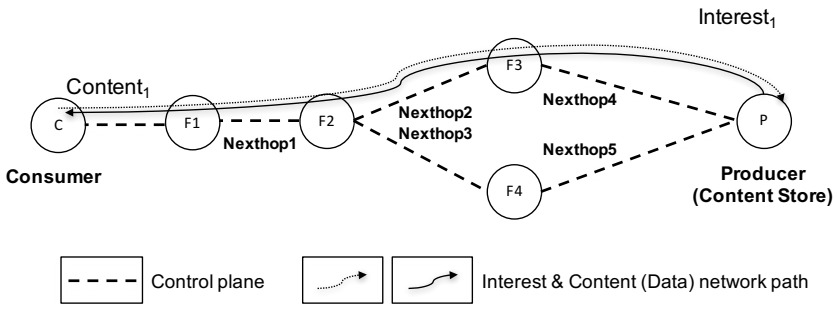
Encoding options:

- Bloom filter
- Pairing function
- Label Stack (similar to MPLS label stack)
- **Fixed size labels – This is what we chose (see later slide)**



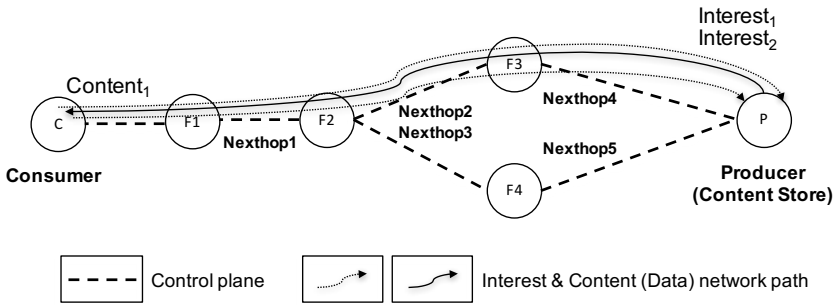
Path discovery and steering

Interest$_1$ contains a path label marked as **DiscoveryMode** and is forwarded with LPNM in the FIB



Path discovery and steering

Content$_1$ carries a path label modified on each hop.



Path discovery and steering

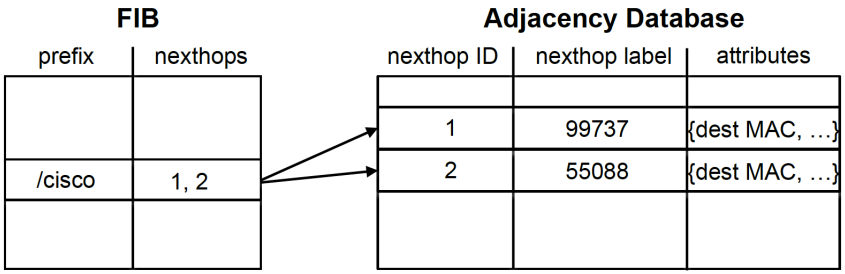
Interest$_2$ has a path label obtained from the earlier returned Data Packet. This a marked as not **DiscoveryMode** and is forwarded with LPNM FIB + nexthop selection.

Advantages

- ICN **Ping** application can reliably measure path RTT
- ICN **Traceroute** application can iteratively discover multiple network paths
- Consumer multipath-aware **congestion control** can discover and distribute load across paths
- Consumer can mitigate **content poisoning** attacks
- **Traffic engineering** (TE) and SDN solutions can be built

Route updates

- With path steering, LNPM FIB lookup still used to find the set of nexthops from which the path' nexthop is chosen.
- If nexthop selection fails:
  - Interest-Return (NACK) carrying a new "Invalid path label" error code
  - or silently forward an Interest through any available nexthop
  - Behavior can be controlled through consumer options on Interests:
    - StrictMode
    - FallbackMode
    - DiscoveryMode



Handling Route updates

- New nexthop label(s) assigned every time FIB entry changes
- On reverse path, Data or NACK is dropped
- On forward path, Interest is NACK'ed

III. Packet Encoding

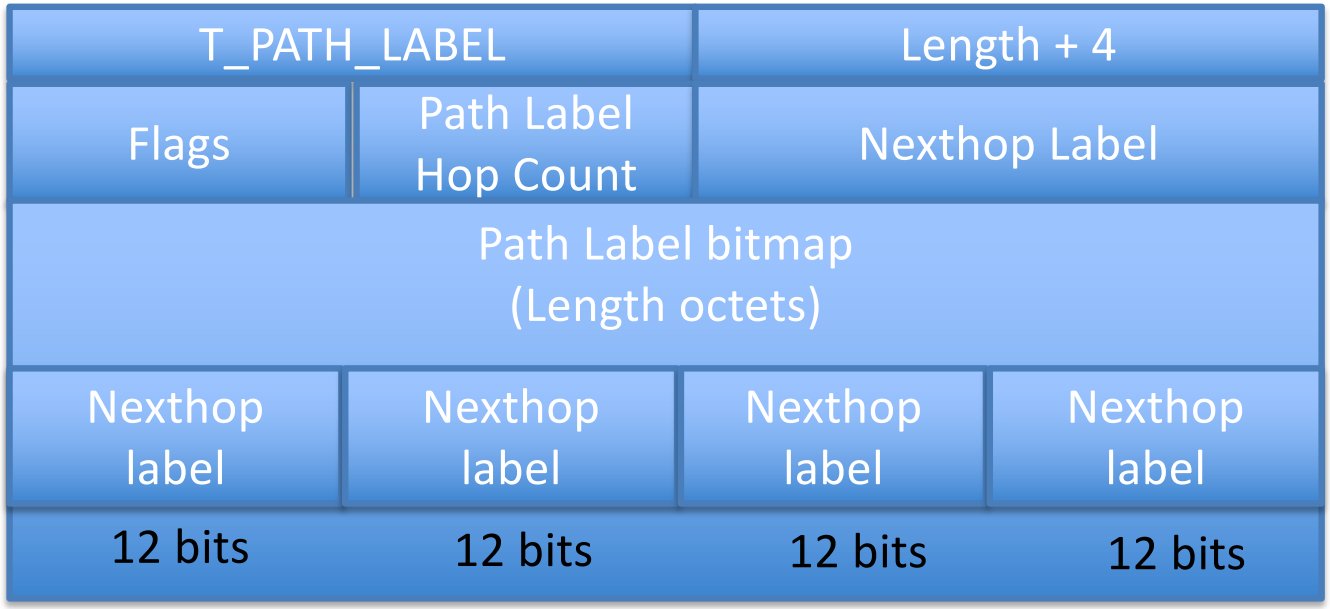
Additions to CCNx Packet format (RFC8609)

- New Error Code: T_RETURN_INVALID_PATH_LABEL for Interest Return Packet
- New hop-by-hop header TLV: T_PATH_LABEL
- New Registry for Path Label Field TLVs:
  - PATH-LABEL-TYPE
  - PATH-LABEL-BITMAP-TYPE
  - PATH-LABEL-NEXTHOP-LABEL-TYPE
  - PATH-LABEL-HOP-COUNT-TYPE

Proposed NDN Packet encoding

- New NDN Packet TLV: PATH-LABEL
  - Note: define in main NDN Packet spec rather than NDNLPv2 since it is hop-by-hop mutable like the recently introduced HopLimit TLV
- Consists of the following:
  - PATH-LABEL-FLAGS-TYPE TLV-LENGTH ; == 1 OCTET
  - PATH-LABEL-NEXTHOP-LABEL-TYPE TLV-LENGTH ; == 2 2 OCTET
  - PATH-LABEL-HOP-COUNT-TYPE TLV-LENGTH ; == 1 OCTET
  - PATH-LABEL-BITMAP-TYPE TLV-LENGTH ; == 64 64 OCTET

Path Label Syntax



This design allocates 12 bits (i.e. 4095 as a *generator polynomial*) to each intermediate ICN forwarder. This should match the scalability of today's commercial routers that support up to 4096 physical and logical interfaces and usually do not have more than a few hundred active ones.

IV. Security considerations

Malicious mis-steering

Consumer can use probing with Interests to discover path labels and then steer packets over wrong paths or to wrong destinations to mount a DoS attack.

- 12-bit nexthop label requires only average 2^{12} Interests to discover by malicious consumer
- Mitigation: periodically update nexthop labels to limit the maximum lifetime of paths
- To foil divide-and-conquer, use a void Hop Count field in “Invalid path label” Interest-Return (NACK) message
- Path label can be encrypted hop-by-hop on the reverse path

Cache pollution

Malicious consumer & producer can inject an off-path and potentially bogus object in on-path caches.

- Mitigation: Cache entries must be annotated with the corresponding path label and only used to satisfy Interests with a matching path label.
- Mitigation: Cache entries must not evict entries for the same object with no path label, or a different path label.

Thanks! Questions?