Hybrid Information-Centric Networking

ICN with IPv6

Luca Muscariello, Giovanna Carofiglio, Jordan Augé, Michele Papalini

INTAREA WG Meeting IETF 102- Montreal -16th of July 2018

Outline

- Motivation
- Naming data with IPv6
- The network architecture
- Application support

Motivation

- Insert ICN into the Internet Protocol
- Evolutionary implementation
- Shorter time to deployment
- Minimize standardization effort
- Minimize clean-slate work in routers and end-hosts
- Enable hybrid deployment and interconnection of IPv6 and hICN
- hICN as an overset of IPv6

What is ICN in the first place?

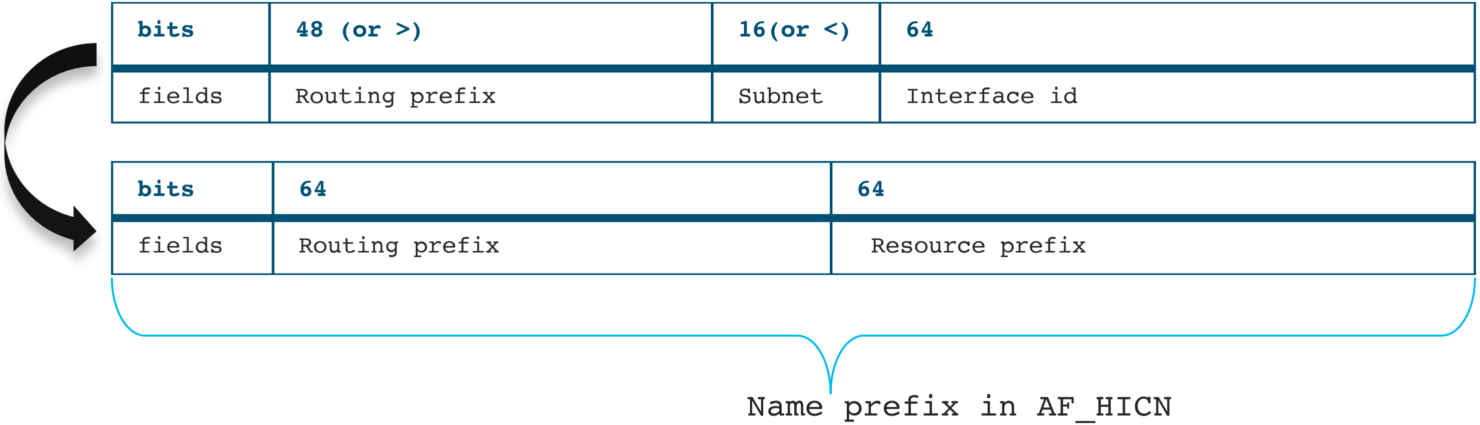
- A network architecture to transport many different kinds of applications from real-time to content-distribution;
- enables connection-less and location-independent communications by identifying data with unambiguous names;
- hICN is based on request/reply semantics and an hICN node accepts data from an input interface if and only if there is a pending request for it (local flow balance principle).
- Data integrity and authentication of the data producer is built in (data-centric security)

Name prefixes in IPv6 numbers

- location-independent identifiers for data sources
- An RTP media source
- An HTTP service
- A video object
- An end host
- A service

Naming data with the Internet Protocol

- Definitions:
  - Name prefix: encoded as an IPv6 128 bits word and carried in IPv6 header fields
  - Name suffix: encoded in transport headers fields such as TCP
  - Name: hierarchical concatenation of name prefix and suffix



bits	48 (or >)	16(or <)	64
fields	Routing prefix	Subnet	Interface id

bits	64	64
fields	Routing prefix	Resource prefix

IPv6 prefixes for data names

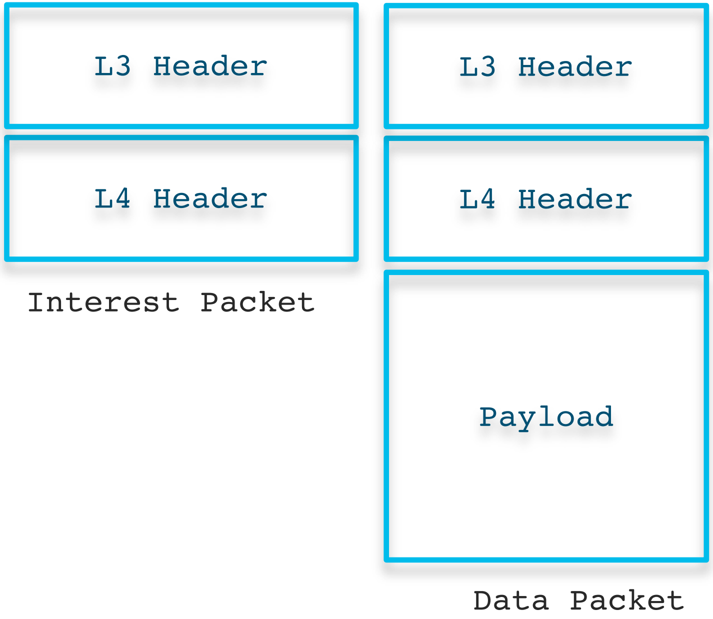
- It is an open problem to determine which IPv6 prefixes should be used as name prefixes: several options are possible.
- It is desirable to be able to recognize that an IPv6 prefix is a name prefix, e.g. with an address family
- However this can be determined and distributed by a control plane to configure routers

1. a new IPv6 address family AF_HICN, b001::/16
2. Let the management and control plane to locally configure HICN prefixes and announce them to neighbors for interconnection. A prefix owner can reuse existing prefixes
3. Other solutions…

Packet format

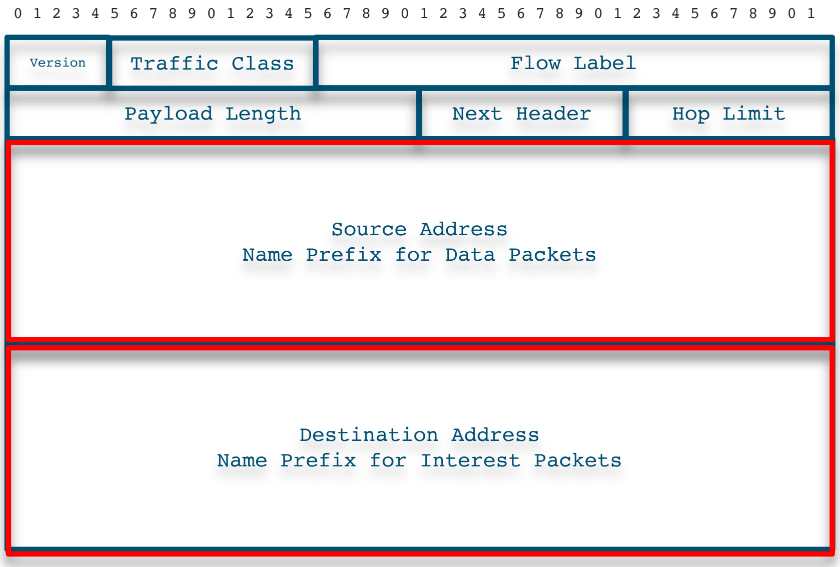
Packet format: two protocol data units

- The protocol semantic is request/reply
- Two protocol data units: Interest/Data
- Interest is used to query Data with a 1:1 match
- The semantics are unchanged w.r.t. NDN/CCN
- draft-irtf-icnrg-ccnxmessages-08
- draft-irtf-icnrg-ccnxsemantics-09



Packet format L3

- The name prefix is stored in the **DST** address field to exploit IP routing/forwarding of the **requests**
- The name prefix is stored in the **SRC** address field as **replies** are not routed by name
- SRC and DST in Interest/Data are valid IPv6 addresses (locators), i.e. identifiers of network interfaces



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version

Traffic Class

Flow Label

Payload Length

Next Header

Hop Limit

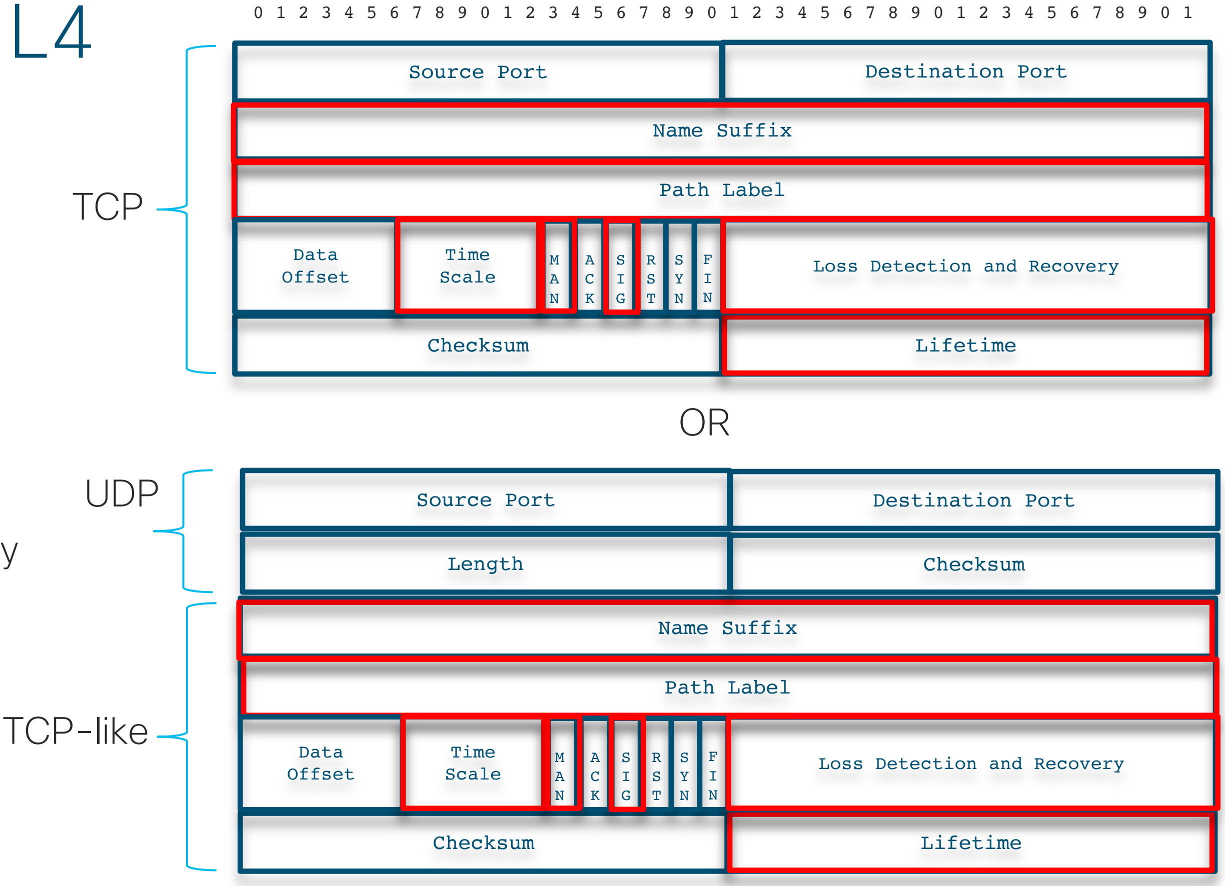
Source Address
Name Prefix for Data Packets

Destination Address
Name Prefix for Interest Packets

Packet format L4

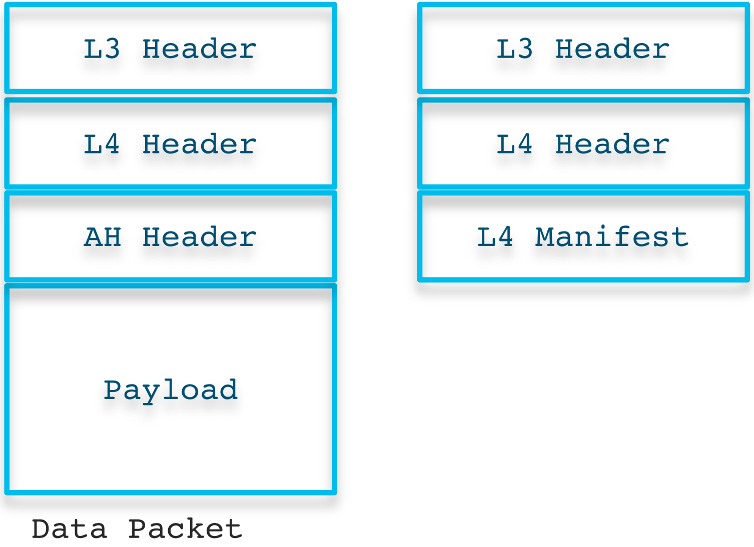
- Use the TCP header by default
- Keep SRC/DST ports
- e.g. for HTTP

- But also UDP header to carry a hICN L4 header
- e.g. for RTP

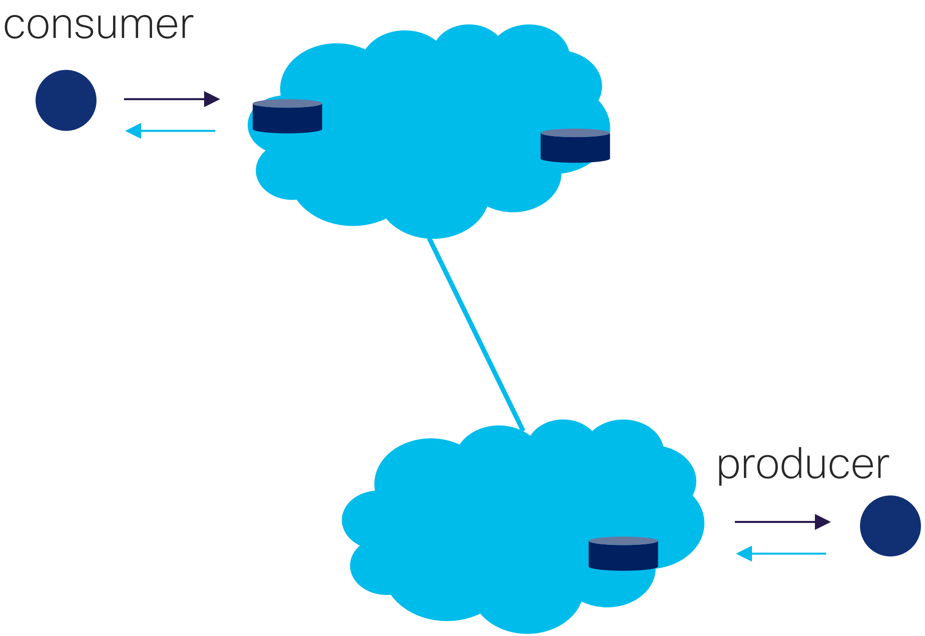


Security: authentication and integrity

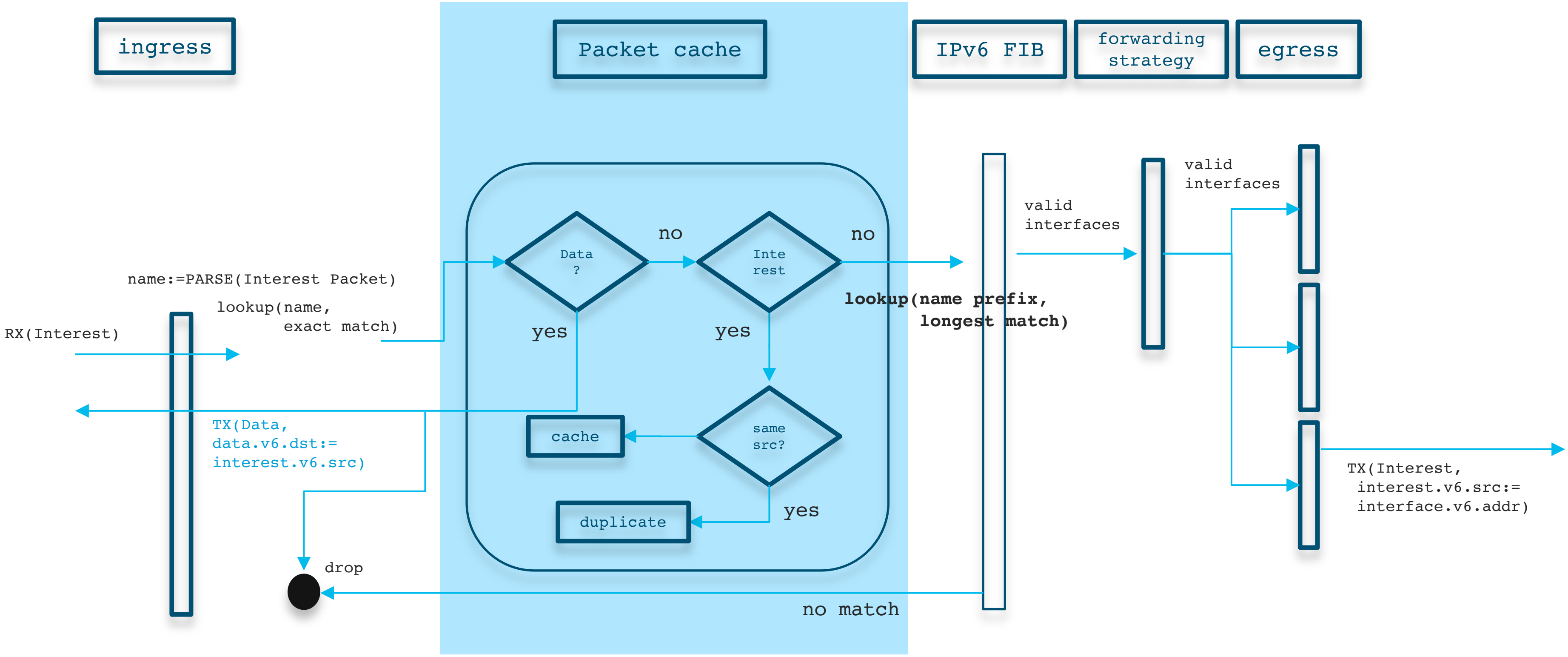
- Authenticity and Integrity provided by using crypto signatures
- Two signature envelops: a single data packet or the transport manifest
- In the first case the signature is carried by the IP authentication header
- In the second case the transport manifest is the only signed unit
- Definition of L4 Manifest
  - A low level index of names of a collection of data packets
  - Carries hashes of data for integrity
  - Carries the signature of the manifest for authentication



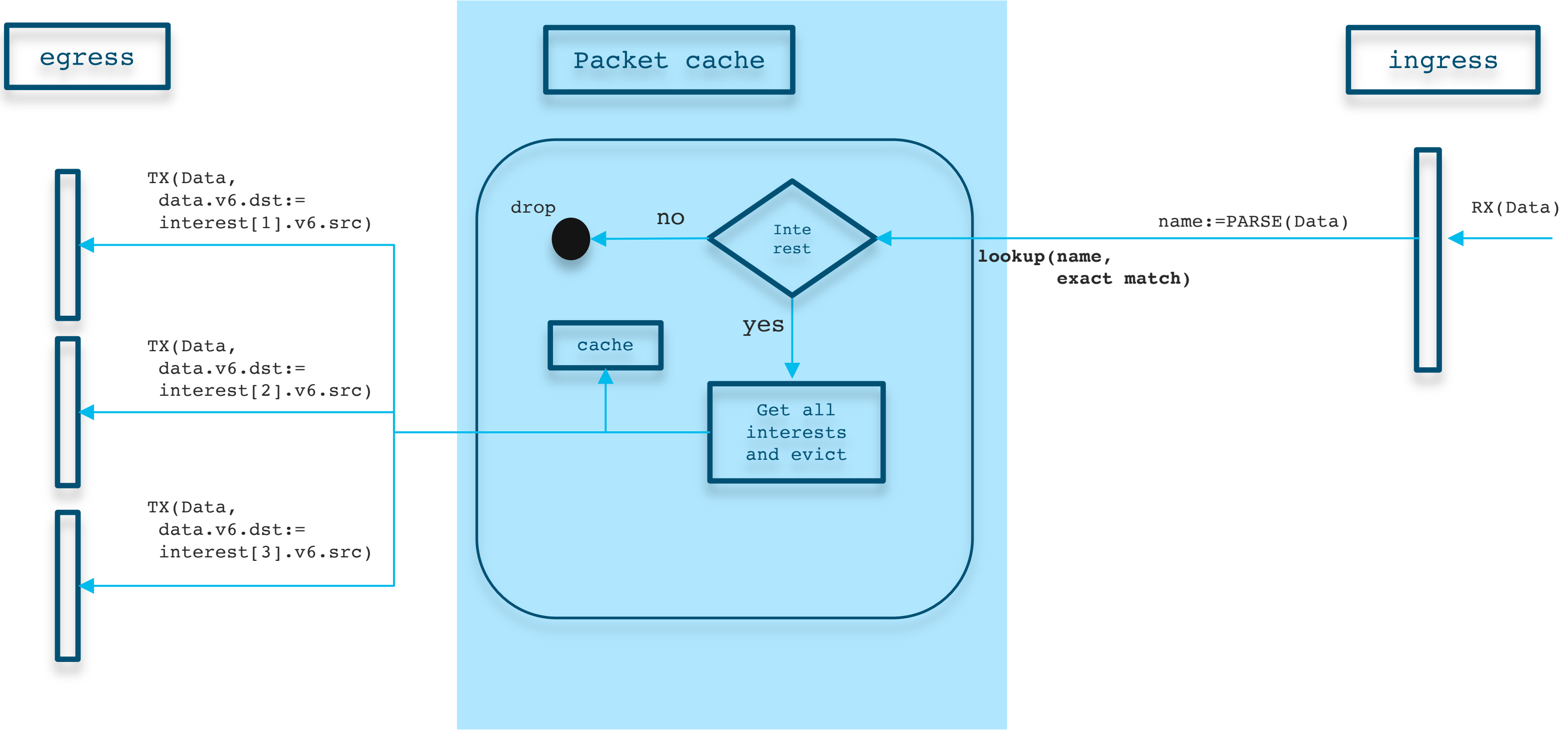
Forwarding path



hICN protocol semantics: the interest path



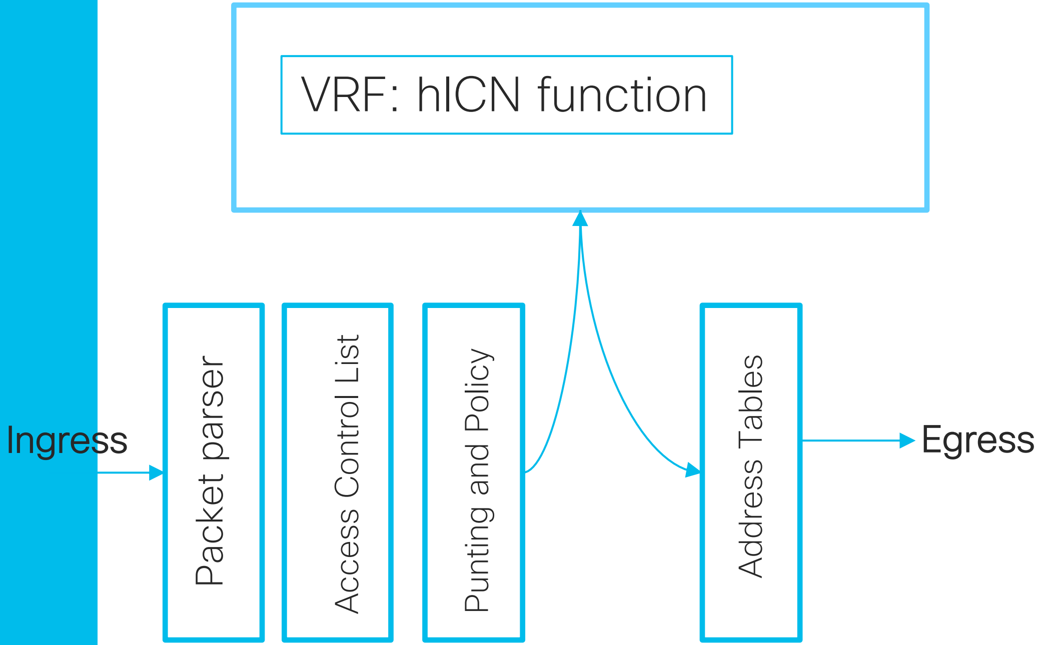
hICN protocol semantics: the data path



Punting

- hICN traffic requires a punting rule
- Has to be efficient and easy to manage
- AF_HICN putting using ACL
- Explicitly flag hICN traffic, how?

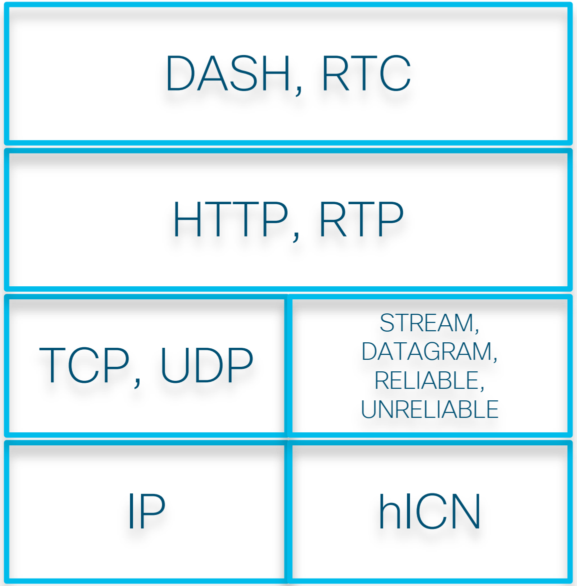
  Port numbers?



Application Support

Transport Layer and Socket API

- An INET like Socket API and a post-socket API
- Unidirectional sockets: producer and consumers
- Socket identifiers based on name prefixes
- Segmentation and signature computation at the producer
- Reassembly and signature verification at the consumer
- DATAGRAM or STREAM transport
- Reliable or unreliable
- Support of current applications: HTTP, RTP



DASH, RTC

HTTP, RTP

TCP, UDP

STREAM, DATAGRAM, RELIABLE, UNRELIABLE

IP

hICN

Conclusion

- It is possible to deploy ICN now using hICN for IPv6
- No tradeoffs in terms of ICN features
- Prototype available at Cisco with focus on HTTP and RTP
- Novel transport services and socket API (based on TAPS)