

PRP A PROTOCOL ATLAS

References → discovery → authenticated relationships → selected trajectories

Architecture, component protocols and selected binary layouts

01 / NAME

SCIR

SELF-CERTIFYING IDENTIFIER REFERENCES

A compact reference commits to canonical material. Identity proof remains a separate protocol operation.

00 IDENTITY

Public-key commitment

01 ALIAS

Shared rendezvous reference

02 MULTICAST

Logical one-way transmission

03 GROUPCAST

Group and participation state

02 / FIND

Discovery

CARRIER HINTS + PROTECTED LOOKUP

Local enumeration identifies candidates. Protected discovery combines directional policy, Bloom views and exact lookup.

01 Carrier-local hints

02 Sharded Bloom / microshards

03 Exact target lookup

04 Destination proof

Bloom positive = candidate, not authority.

03 / AUTHENTICATE

HS2 successor

FOUR-FLIGHT ARCHITECTURAL FLOW

M1 →

Nonidentifying initiation

M2 ←

Protected destination proof + PoW*

M3 →

Protected client proof + solution*

M4 ←

Authenticated admission result

* When required by admission policy.

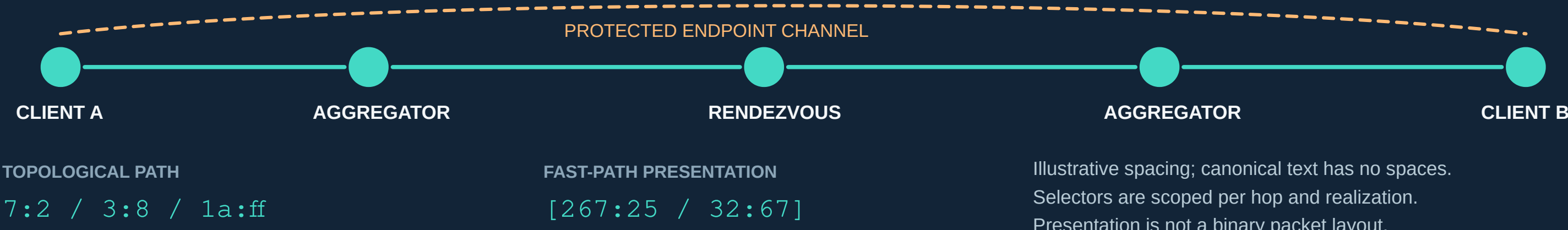
Flight labels are not wire-v4 opcodes.

04 / REACH

TPA + protected fast paths

RELATIVE TOPOLOGY • LOCAL SELECTORS • DISTINCT IDENTITY SCOPES

The client selects its trajectory. Each hop interprets a local context; an aggregator’s adjacency identity does not reveal the identity carried inside the protected final channel.



05 / MAINTAIN

Relationships

LIFECYCLE • DTN • CUSTODY

Membership and policy survive session changes. Rekey, path replacement and retention have separate scope and lifetime rules. Availability and transport capacity are negotiated toward the rendezvous.*

06 / DISTRIBUTE

Multicast + groupcast

ONE TRANSMISSION • MULTIPLE SENDERS

Multicast identifies a logical transmission. Groupcast composes independently governed participation and multiple transmissions. Aggregation replicates delivery; it does not take ownership of endpoint identities.

07 / ADAPT

Carriers + resources

DIRECTION • GENERATIONS • OBSERVATIONS

Carrier readiness is directional. Volatile selectors require current generations. Resource reports expose local observations: queues, loss and residual capacity. An observed rate is not itself a reservation.

WIRE NOTEBOOK

Exact layouts below belong to named working-draft profiles; widths are in octets.

SCIR / canonical reference

reference_header	reference_suite	identifier
1 • class in bits 1..0	2 • unsigned big-endian	L • suite-defined; current L = 32 or 48

PROTECTED DISCOVERY v1 / 36-octet header + payload

version	kind	flags	control gen.	subject gen.	correlation	length	reserved
1	1	2	4	8	16	2	2

Canonical inner payload follows. Generation binding and exact length are checked before use.

AOP / Adjacent Operation Packet

Successor session record: the complete protected packet

sequence	ciphertext	authentication tag
8 • unsigned big-endian	encrypted RRL: count + records + padding	tau • session-defined

Experimental ChaCha20-Poly1305: tau = 16; nonce = derived 4-byte prefix + sequence. Nonce is not sent again.



RRL / Route-Record List

The operation container inside AOP — one authenticated list, multiple scoped records

record_count	records	opaque_padding
2 • decode exactly N	record 1 record 2 ... record N	remaining plaintext

EACH RECORD

route_alias	kind	flags	body_length	body
2 • local session scope	1 • operation type	1	2 • exact body size	variable • kind-specific content

Fixed record header: 6 octets. Padding is not another record. Authenticate the AOP before dispatching operations.

READING KEY

HS2 / TPA: architectural direction; successor integration remains a separate scope.

AOP successor: sequence[8] + ciphertext + tag[tau]. Historical AOP: nonce[12] + ciphertext + tag[16].

SCIR, discovery and RRL are versioned formats; diagram widths are illustrative, not byte-proportional.

* Capacity negotiation: protocol-author clarification, 23 Oct 2026. Wire snapshot: 24 Oct 2026.