How do we BEGIN Test processes?

What info is communicated to activate a test?

Security for “Test Protocol for One-way IP Capacity Measurement”

draft-morton-ippm-capacity-metric-protocol-01

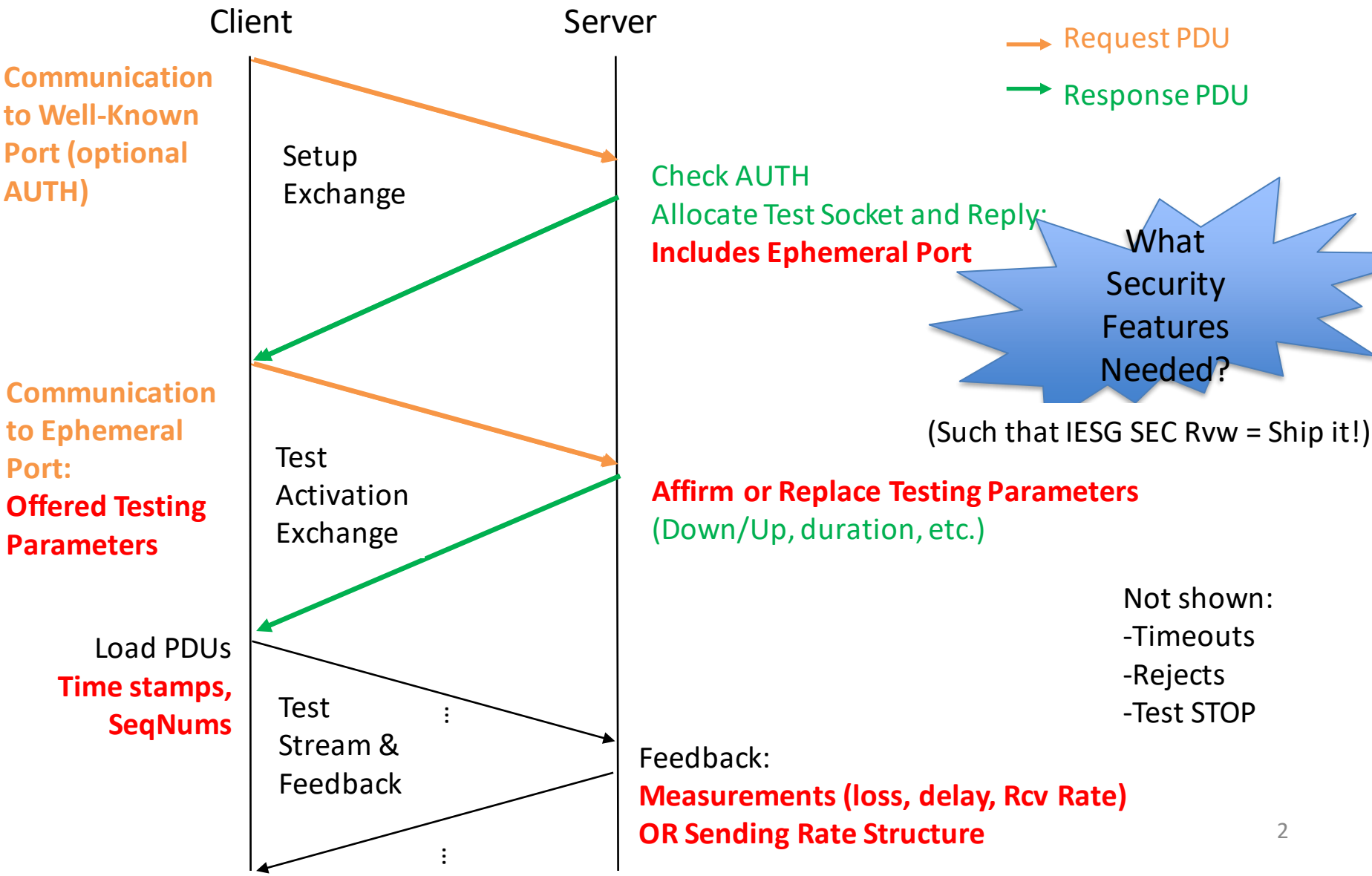
L. Ciavattone, A. Morton

What Security Features are Needed?

How should the protocol operate in diff modes?

Protocol: Setup and Activate Test

draft-morton-ippm-capacity-metric-protocol-01



Not shown:
-Timeouts
-Rejects
-Test STOP

New Security Modes (A thru F)

How should the protocol operate in diff modes?

PHASES

- Setup Exchange ONLY
- Setup and Test Activation
- Test Stream and Feedback

MODES

A. Unauthenticated mode (for all phases)

AND

B. OPTIONAL Authenticated set-up only

SHA-256 HMAC time-window verification (5 min time stamp verification)

(Currently in the running code, could add silent failure option)

-=-=-=-=-=-=-=-=-=-

C. Encrypted setup and test-activation

(currently using OpenSSL Library in AUTH above, so KISS, but may be too slow for test packets)

-=-=-=-=--=- Old/low-power host performance impacts -=-=-=-=-=-=-

D. Encrypted feedback messages (20 pps)

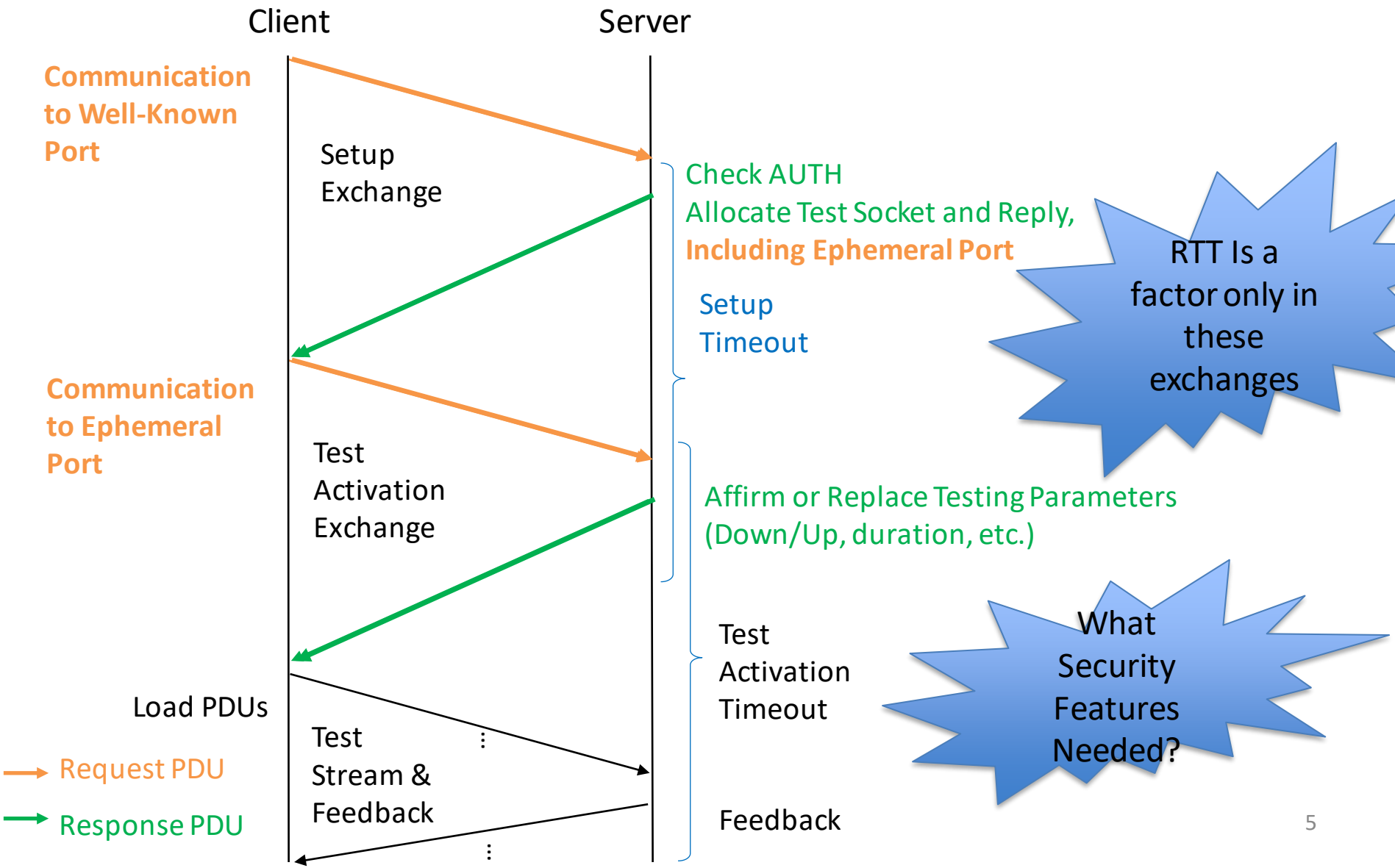
E. Integrity protection for test packets (SHA-256 HMAC) >80k pps @1G

F. Encrypted test packets (maybe also valuable to defeat compression on links)

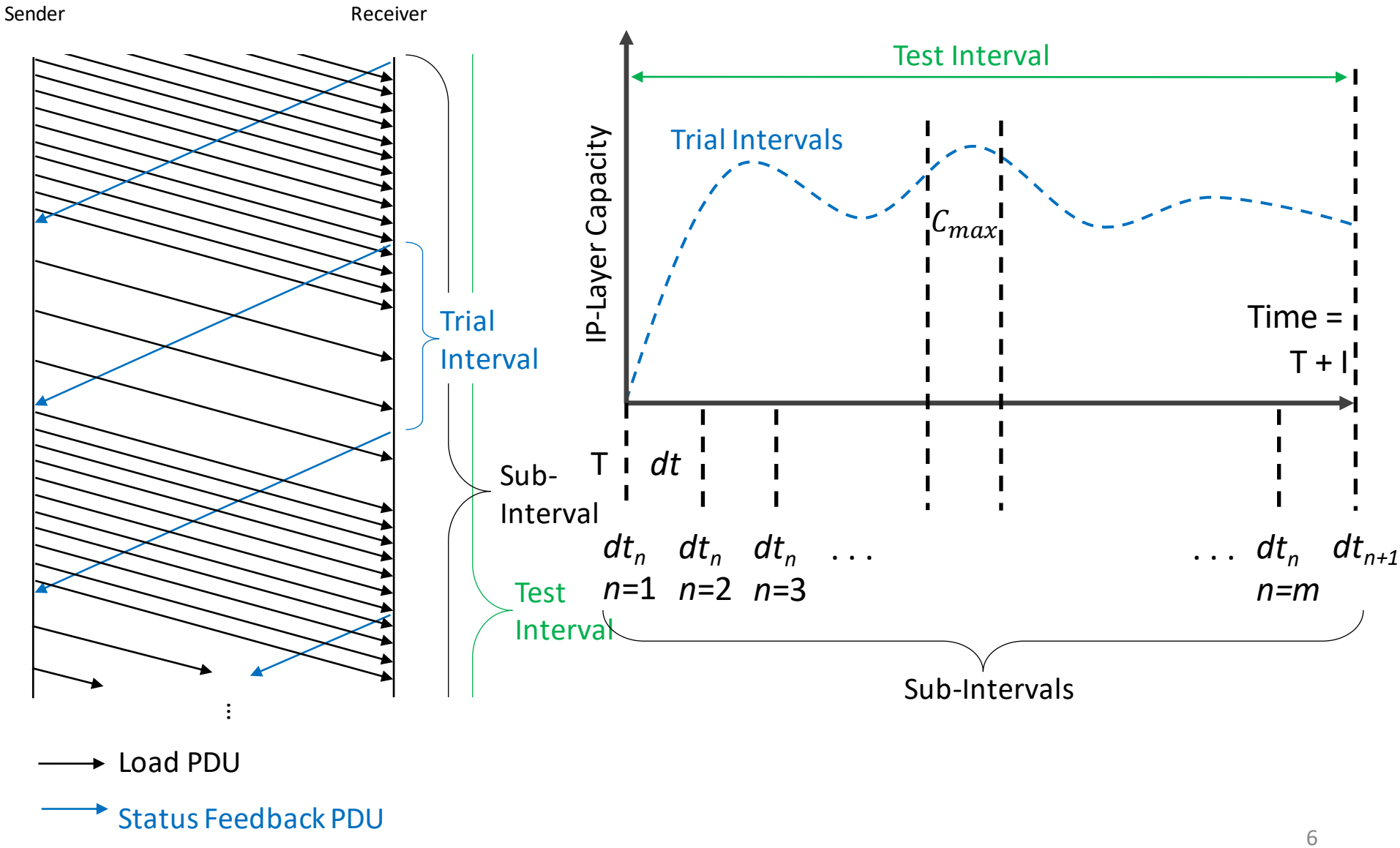
BACKUP

Protocol: Setup and Activate Test

draft-morton-ippm-capacity-metric-protocol-01



Receiver Rate Measurement



Key Parameters (4)

- Load-Rate Alg: Seq. Errors, Delay Range Thresh

Parameter	Default	Tested Range or values	Expected Safe Range (not entirely tested, other values NOT RECOMMENDED)
low delay range threshold	30ms	5ms, 30ms	same as tested
high delay range threshold	90ms	10ms, 90ms	same as tested
sequence error threshold	0	0, 100	same as tested
consecutive errored status	2	2	Use values >1 to avoid misinterpreting transient loss