SEC-DIR Response & Encrypted Mode Discussion:

“Test Protocol for One-way IP Capacity Measurement”

draft-ietf-ippm-capacity-metric-protocol-03

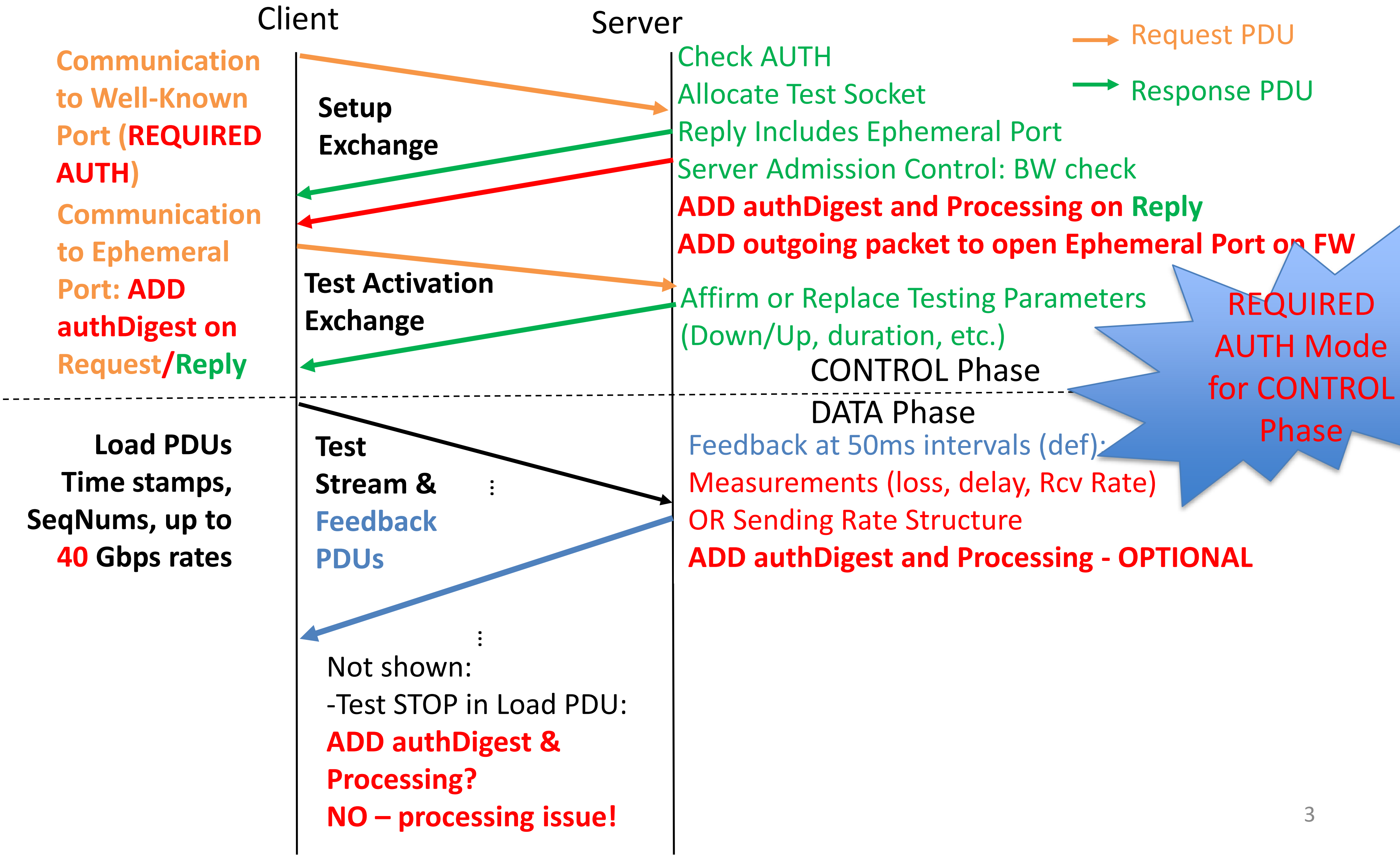
L. Ciavattone, A. Morton

Implemented extensive changes in -protocol-03, including:

- 1. Adoption of 4 new modes of security operation
- 2. Expansion of the now-Required Authenticated mode coverage to the entire Control phase packet exchanges. The server can reply with an error message only when the authentication of a request is valid, otherwise the request terminates silently.
- 3. Addition of a new Optional mode for Authentication of the Status feedback messages during the Data phase packet exchanges.
- 4. New Sections on Key Management and Firewall Configuration
- 5. New sub-section outlines for the Test Setup, Test Activation, and Status Feedback section, aligning with each step of the host processing for this protocol.
- 6. New Security Considerations on attacks the WG discussed @IETF-114
- 7. Expanded IANA section requesting a new Registry group to support future expansion of this protocol.

Protocol: Setup and Test Phases

draft-ietf-ippm-capacity-metric-protocol-03



Client

Server

Request PDU

Response PDU

Communication to Well-Known Port (**REQUIRED AUTH**)

Setup Exchange

Check AUTH

Allocate Test Socket

Reply Includes Ephemeral Port

Server Admission Control: BW check

ADD authDigest and Processing on Reply

ADD outgoing packet to open Ephemeral Port on FW

Communication to Ephemeral Port: **ADD authDigest on Request/Reply**

Test Activation Exchange

Affirm or Replace Testing Parameters (Down/Up, duration, etc.)

CONTROL Phase

DATA Phase

REQUIRED AUTH Mode for CONTROL Phase

Load PDUs Time stamps, SeqNums, up to 40 Gbps rates

Test Stream & Feedback PDUs

⋮

Feedback at 50ms intervals (def):

Measurements (loss, delay, Rcv Rate)

OR Sending Rate Structure

ADD authDigest and Processing - OPTIONAL

⋮

Not shown:

-Test STOP in Load PDU:

ADD authDigest & Processing?

NO – processing issue!

DTLS doesn't encrypt key info, and has other limits

- Could use DTLS during the Control phase (Test Setup and Test Activation)
- However, info exchanged in the Control phase is of limited value
  - A test is starting
  - Configuration of the test system
  - Easy to finger-print traffic to reveal a "measurement"
  - No measurements/results in Control phase

- Can't use DTLS in the Data phase – retransmissions and ordered delivery are un-helpful
- So, The most valuable info communicated -- the measurements and the send-rate structure -- cannot be encrypted using DTLS

~~IF we~~ Encrypt all exchanges – one approach

(exposed measurements and rate-control messages seem to REQUIRE this)

- A simple solution to "encrypt all the things" is to **operate the protocol within an encrypted tunnel**.
- Bilateral Agreement: Tests are point-to-point, allowing **choice of encrypted tunnel and keys** between the parties seeking to use encryption.
- There is considerable support for independent tunnel implementation in Linux hosts, etc.
- There is some HW support for stand-alone tunnels, e.g., smart NICs, data centers
- There is no need to modify this protocol to use the encrypted tunnel.
- Some may want to **characterize** or measure the tunnel tech. they chose: **Leave the tunnel choice to the USERS**.
- The Emphasis in IPPM is accuracy
  - Recommend to run some Unauthenticated tests first, with NO Tunnel – see if tunnel has negative impact & purposefully characterize the encryption tunnel itself.
- A Recommendation would be to use Unauthenticated mode in the encrypted tunnel, to maximize server and client performance.
- There might be reasons to use Authenticated mode: still an option.
- MTU is reduced in the tunnel (but 1222 byte datagram or 1250 IP-Layer bytes leaves lots of room for encapsulation headers).

So, leave the encrypted tunnel choice and instantiation to the Users – say so in the draft!

Next Steps

- More SEC AD and/or SEC-DIR interactions (hopefully)
- Implement WG-agreed proposal for fully encrypted Mode in the draft, Ideally in the next Revision
- The bottom line:
    - AFAIK, full encryption is not widely activated in measurement protocols used at scale
    - OWAMP and TWAMP had it...
- WG Last Call in January 2023?
    - Maybe sooner if Encryption solution is simple.
- Note: lots of measurements shared on the ippm-list:
    - Comparisons with RFC 9097 Capacity and RTT under Working Load