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

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

L. Ciavattone, A. Morton
Protocol: Setup and Activate Test

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

Communication to Well-Known Port (optional AUTH)

Communication to Ephemeral Port: Offered Testing Parameters

Load PDUs: Time stamps, SeqNums

Setup Exchange

Test Activation Exchange

Check AUTH
Allocate Test Socket and Reply:
Includes Ephemeral Port

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

Feedback:
Measurements (loss, delay, Rcv Rate)
OR Sending Rate Structure

Request PDU
Response PDU

Not shown:
-Timeouts
-Rejects
-Test STOP

(Such that IESG SEC Rvw = Ship it!)
New Security Modes (A thru F)

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)

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)

How should the protocol operate in diff modes?
BACKUP
Protocol: Setup and Activate Test

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

Communication to Well-Known Port

Communication to Ephemeral Port

Load PDUs

Request PDU

Response PDU

Client

Server

Setup Exchange

Check AUTH
Allocate Test Socket and Reply,
Including Ephemeral Port

Setup Timeout

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

Test Activation Exchange

Test Activation Timeout

Feedback

Test Stream & Feedback

RTT Is a factor only in these exchanges

What Security Features Needed?
Receiver Rate Measurement

Sender

Receiver

Trial Interval

Sub-Interval

Test Interval

IP-Layer Capacity

Time = T + 1

T

$dt$

$dt_n$ $dt_n$ $dt_n$ …

$n=1$ $n=2$ $n=3$ …

Sub-Intervals

$C_{max}$

Load PDU

Status Feedback PDU
## Key Parameters (4)

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

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