Regarding ntpv5

Doug Arnold
2021-02-03
Ntpv4 works well for general IT

- Server, router logfile event timestamps
- Certificate, key, ticket lifetimes in security protocols
  - although start-up issue not solved
- Setting PC & laptop clocks
- Unicast client-server mode security is updated by NTS
Why ntpv5?

Some proposed answers from the email reflector:
• Greater accuracy
• Flexibility for a variety of use cases
• Mandatory security to push users to adopt security
• Uniform, monotonic timescale like TAI to avoid leap seconds
• Simplify ntp world by moving everyone to client-server mode
Current proposals

- Draft-grueessing-ntp-ntpv5-requirements-01
- Draft mlichvar-ntp-ntpv5-01
- Both of these are incomplete works in progress

<table>
<thead>
<tr>
<th>Feature</th>
<th>Gruessing requirements draft</th>
<th>Mlichvar draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved accuracy</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Flexibility for variety of use cases</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Mandatory security</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Monotonic timescale</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Client server only</td>
<td></td>
<td>√</td>
</tr>
</tbody>
</table>
Improved Accuracy

- Non-fully-compliant versions of ntpv4 exist specifically to address this need
  - Different algorithms
  - Higher message rates
  - 50 ns clock agreement can be achieved in small networks
  - Popular in financial data centers
- Mlichvar draft includes ability for on-path support
  - Correction Extension Field would work similar to Transparent clocks in PTP
Flexibility for variety of use cases

• Why?
  • Needed to support high accuracy use cases in LANs
  • May be needed to support IoT use cases with devices that have limited processing power
  • Allow high reliability implementations, for example Chronos

• How
  • Separation of algorithms from over the wire protocol supported in both drafts
  • General purpose extension field mechanism in Mlichvar draft

• To make sure it solves the general IT case a document could be created with recommended algorithms
Mandatory Security

• Would encourage faster adoption of security
  • This approach has worked for other protocols
  • Likely to be viewed as positive in the long run

• Cons
  • Goes against flexibility for niche applications
    • Maybe some applications do not need security
    • Security needs for some applications might look very different from others. For example, time from the internet vs high accuracy LAN
  • Security is the fastest changing aspect of networking – so keeping it separate might make it easier to keep standards up to date
Montonic Timescale

• Best choice would probably be TAI
• Pro: No leap seconds in the protocol
• Cons
  • Current software expects OS time to include leap seconds
  • Some legal requirements mandate UTC
  • Many technical standards mandate UTC
  • Some network operator with niche applications want to distribute uncommon timescales like UT1
• Both drafts propose allowing multiple timescale choices
  • Gruessing draft requires the ability to determine UTC
  • Mlichvar proposes enumerated variable in ntp messages indicating timescale in use
Unicast client-server only

• Pro
  • Most deployed ntp devices use this
  • Support for multiple modes makes implementations more complex
  • No up-to-date security standards for other modes

• Con
  • Other modes are used in some networks
  • Might go against flexibility for niche applications