Echo Request/Reply for Enabled In-situ OAM Capabilities

draft-xiao-ippm-ioam-conf-state-08

Xiao Min	ZTE
Greg Mirsky	ZTE
Lei Bo	China Telecom

Main updates from -07 to -08

- Analyzed use cases for approaches based on Netconf/YANG, IGP, and Echo Request/Reply. Concluded that:
  - Netconf/YANG is most suitable if the IOAM domain is administered by a centralized controller
  - Use of Netconf/YANG is problematic without the centralized controller. Flooding IGP domain with IOAM information may be excessive. Hence, using Echo Request/Reply-based mechanism is reasonable in some cases
- Added IANA registries for SoR/TSF+TSL Capability
  - Also explain why we don't have IANA registry for new types and sub-types
- Improved the Security Considerations section

Netconf/YANG's Limitations

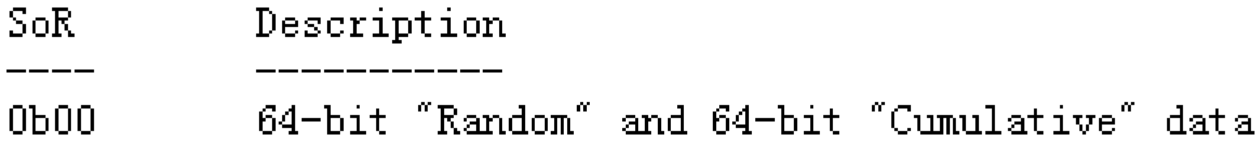
- When Netconf/YANG is used in an IOAM domain where no centralized controller exists:
  - Each IOAM encapsulating node needs to implement a Netconf Client, each IOAM transit node and IOAM decapsulating node needs to implement a Netconf Server, the complexity can be an issue
  - Each IOAM encapsulating node needs to establish Netconf Connection with each IOAM transit node and IOAM decapsulating node, the scalability can be an issue

IGP’s Limitations

- When IGP is used in an IOAM domain where no centralized controller exists:
  - An IGP domain and an IOAM domain don't always have the same coverage. For example, when the IOAM encapsulating node or the IOAM decapsulating node is a host, the availability can be an issue
  - Furthermore, it might be too challenging to reflect IOAM capabilities at the IOAM transit node and/or the IOAM decapsulating node if these are controlled by a local policy depending on the identity of the IOAM encapsulating node

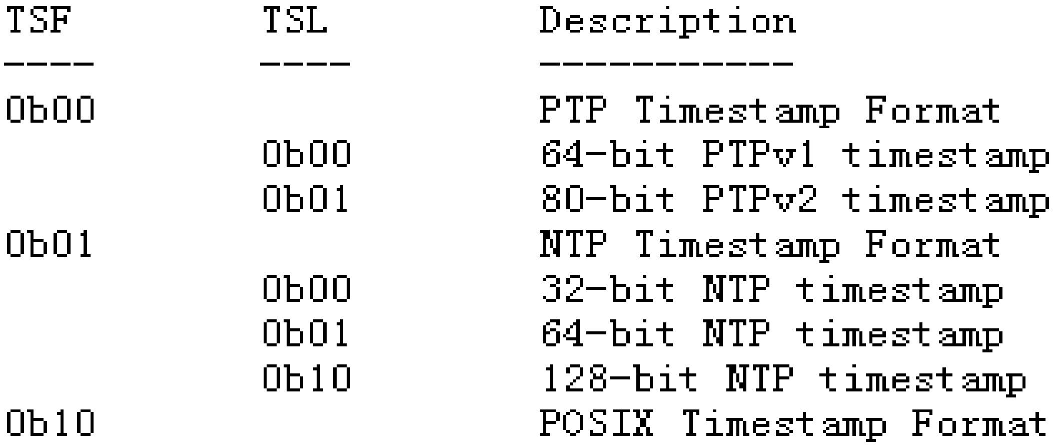
IANA registries for SoR and TSF+TSL Capability

- IOAM SoR Capability identifies the size of "Random" and "Cumulative" data:



SoR	Description
0b00	64-bit “Random” and 64-bit “Cumulative” data

- IOAM TSF+TSL Capability identifies the timestamp format and the timestamp length:



TSF	TSL	Description
0b00		PTP Timestamp Format
	0b00	64-bit PTPv1 timestamp
	0b01	80-bit PTPv2 timestamp
0b01		NTP Timestamp Format
	0b00	32-bit NTP timestamp
	0b01	64-bit NTP timestamp
	0b10	128-bit NTP timestamp
0b10		POSIX Timestamp Format

Improve the Security Considerations

- Several methods are suggested for the implementer and operator to use:
  - Authentication of echo request/reply that includes the IOAM Capabilities TLV
  - A means of filtering based on the source address of the received echo request/reply
  - The security mechanism of underlay data plane can also be employed, e.g. within an IPv6 network
    - ✓ IP Authentication Header [RFC4302] can be used to provide integrity protection
    - ✓ IP Encapsulating Security Payload Header [RFC4303] can be used to provide both integrity protection and confidentiality

Next steps

- Ask for WG adoption