**Protocol Orchestrator Node (PON) - Gateway Communication Standards Document**

**1. Introduction** This document establishes the communication standards between the **Protocol Orchestrator Node (PON)** and **Edge Gateways** in an IoT network. The objective is to ensure reliable, secure, and efficient communication for dynamic protocol switching, network monitoring, and device status reporting. This standard outlines message structures, transmission protocols, security requirements, workflows, and error-handling mechanisms.

**2. Scope** This standard applies to all communication between the PON and Edge Gateways in an IoT network. The focus is on protocol-switching instructions, status reporting from Gateways, acknowledgment of commands, retransmission mechanisms, and security measures. These guidelines ensure consistency in communication, integrity of messages, and proper monitoring of network health.

**3. Communication Architecture** The communication between the PON and Edge Gateways is structured into distinct roles. The PON serves as the central authority for protocol decisions, while the Edge Gateway operates as an intermediary node enforcing these directives and managing local network conditions. Communication takes place using lightweight messaging protocols, such as MQTT and CoAP, transmitted over secure transport layers like TLS and DTLS.

The Edge Gateway listens for commands from the PON, executes protocol-switching directives, and sends periodic status updates back to the PON. Additionally, acknowledgments are used to confirm the successful execution of instructions.

+--------------------------+

| Protocol Orchestrator |

| Node (PON) |

+------------+------------+

|

▼

+------------+------------+

| Edge Gateway |

| (Protocol Management,|

| Data Aggregation, |

| Status Reporting) |

+------------+------------+

|

▼

+--------------------------+

| IoT Devices |

| (Sensors, Actuators) |

+--------------------------+

**4. Message Types** Communication between the PON and Edge Gateway is categorized into **Update Messages**, **Status Messages**, and **Acknowledgment Messages (ACK)**. Each message type uses a predefined binary format for consistency and efficiency.

**4.1 Update Message** Update messages are sent from the PON to instruct the Gateway to switch between SLAAC and DHCPv6 protocols.

A screenshot of a black and white table

Description automatically generated

**4.1.1 Message ID** The Message ID is a **32-bit** unique identifier assigned to each Update Message. It ensures every message can be accurately tracked and matched with acknowledgments.

**4.1.2 Message Type** The Message Type is **2 bits** and identifies the message as an Update message.

**4.1.3 Protocol** The Protocol is **1 bit** and indicates the selected protocol: 0 for SLAAC and 1 for DHCPv6.

**4.1.4 Elapsed Time** The Elapsed Time is **16 bits** and indicates the time, in seconds, since the last Update message was sent.

**4.1.5 Timestamp** The Timestamp is **64 bits** and provides the Unix Epoch time when the Update message was generated.

**4.1.6 Reserved** The Reserved field is **64 bits**, reserved for future use, and must be set to 0.

**4.2 Status Message** Status messages are periodically sent from the Edge Gateway to the PON, providing updates on protocol states and overall system health.

A black and white table with white text

Description automatically generated

**4.2.1 Message ID** The Message ID is **32 bits** and uniquely identifies each Status Message.

**4.2.2 Message Type** The Message Type is **2 bits** and identifies the message as a Status message.

**4.2.3 Protocol** The Protocol is **1 bit** and indicates the active protocol.

**4.2.4 Status** The Status is **2 bits** and indicates operational health.

**4.2.5 Elapsed Time** The Elapsed Time is **16 bits** and tracks time since the last status update.

**4.2.6 Uptime** The Uptime is **16 bits** and measures active duration.

**4.2.7 Timestamp** The Timestamp is **64 bits** and logs the message time.

**4.2.8 Reserved** The Reserved field is **64 bits**, reserved for future use.

**4.3 Acknowledgment Message (ACK)** Acknowledgment messages are sent from the Gateway to the PON to confirm the successful execution of an Update Message.

A black table with white text

Description automatically generated

**4.3.1 Message ID** The Message ID is **32 bits** and uniquely identifies each ACK message.

**4.3.2 Message Type** The Message Type is **2 bits** and identifies the message as an ACK.

**4.3.3 Protocol** The Protocol is **1 bit** and indicates the protocol associated with the acknowledgment.

**4.3.4 Status** The Status is **2 bits** and indicates if the Update Message succeeded or failed.

**4.3.5 Elapsed Time** The Elapsed Time is **16 bits** and represents time since acknowledgment.

**4.3.6 Timestamp** The Timestamp is **64 bits** and logs the acknowledgment time.

**4.3.7 Reserved** The Reserved field is **64 bits**, reserved for future use.

**5. Retransmission Standards Retransmission mechanisms ensure message reliability in scenarios where messages are delayed, lost, or corrupted. Each message type adheres to the following retransmission rules:**

**5.1 Retry Limit Update and ACK messages may be retransmitted up to 3 times to ensure message delivery.**

**5.2 Timeout Interval If no acknowledgment (ACK) is received within 5 seconds of sending an Update message, retransmission is triggered.**

**5.3 Exponential Backoff Each retransmission attempt uses an exponential backoff mechanism, where the wait time doubles after each failed attempt.**

**5.4 Failure Handling If all retransmission attempts fail after three tries, the PON raises an error alert, and the Gateway logs the failure for diagnostic purposes.**

**5.5 Message Tracking Retransmitted messages retain their original Message ID to ensure accurate matching with corresponding ACKs.**

**5.6 Monitoring and Logging All retransmission events, including failures, must be logged for analysis. Logs must include timestamps, message IDs, and retransmission counts.**

**5.7 Adaptive Retransmission Mechanism The system may use adaptive retransmission intervals based on network conditions, dynamically adjusting timeout values to optimize delivery performance.**

**6. Security Standards Security measures ensure message confidentiality, integrity, and authenticity. The following measures must be implemented:**

**6.1 Encryption All communication must be encrypted using TLS (MQTT) or DTLS (CoAP) protocols to prevent unauthorized interception.**

**6.2 Authentication Devices must authenticate using pre-shared keys (PSK) or digital certificates before communication is established.**

**6.3 Integrity Checks Every message must include an HMAC (Hash-based Message Authentication Code) to verify data integrity.**

**6.4 Key Rotation Policies Encryption keys and authentication credentials must be rotated periodically to minimize exposure risks.**

**6.5 Access Control Strict Access Control Lists (ACLs) must be enforced on both the PON and Gateway nodes to ensure that only authorized devices can access critical network resources.**

**6.6 Audit Logging Security-related events, including failed authentication attempts, retransmission failures, and unauthorized access attempts, must be logged.**

**6.7 Secure Bootstrapping New devices must undergo a secure bootstrapping process, including authentication and provisioning, before integration into the network.**

**6.8 Intrusion Detection and Prevention (IDPS) The system must include Intrusion Detection and Prevention Systems to monitor traffic anomalies, detect malicious patterns, and prevent attacks.**

**6.9 Firmware Integrity Checks Devices must validate firmware integrity during startup and periodically to detect unauthorized modifications.**

**6.10 Security Audits Regular security audits must be conducted to assess vulnerabilities and ensure compliance with established protocols.**

**6.11 Threat Modeling A threat modeling framework must be used to identify and mitigate potential vulnerabilities across the communication lifecycle.**

**6.12 Network Segmentation IoT devices, gateways, and controllers must be segmented into logical networks to contain potential breaches.**

**6.13 Disaster Recovery Plan A disaster recovery plan must be established to ensure rapid restoration of secure communication after critical failures.**

**6.14 Incident Response Plan An incident response plan must define clear protocols for addressing and mitigating security breaches.**

**7 document versions:**

**1.0 – initial version**

**End of Document**