IMPLEMENTATION OF THE LLDP PROTOCOL ACROSS VARIOUS VENDORS AND PROBLEMS IN GENERALIZATION.

Qalandarov Jamil Jalolovich

Muhammad al-Khwarizmi Tashkent University of Information Technologies, Center for Digital Infrastructure Development, First-category engineer programmer

djamic@gmail.com

Omonov Zokirjon Hojiboy ugli

Muhammad al-Khwarizmi Tashkent University of Information Technologies, Center for Digital Infrastructure Development, Head of IT Infrastructure Development Department omonov@eipublication.com

Akmalov Elyor Ilxomovich

Center for Digitalization and Certification, System Administrator

akmalov@eipublication.com

Abstract. *Modern telecommunication networks are complex systems composed of devices from various manufacturers (Cisco, Huawei, HP, MikroTik, and others). In such environments, the Link Layer Discovery Protocol (LLDP), defined by the IEEE 802.1AB standard, is considered the primary tool for automatically discovering and monitoring network topology. This thesis analyzes the implementation of the LLDP protocol across different vendors, the impact of proprietary extensions on interoperability, and the challenges of standardizing data into a unified format.*

Introduction. In the era of modern information technologies, the heterogeneity (diversity) of corporate and provider-level networks is increasing sharply. It has become common for devices from multiple vendors, including manufacturers such as Cisco, Huawei, HP, and MikroTik, to coexist within a single network segment. In such a multi-vendor environment, standardized inter-device communication protocols are necessary to ensure network integrity, automatically discover topology, and rapidly troubleshoot faults.

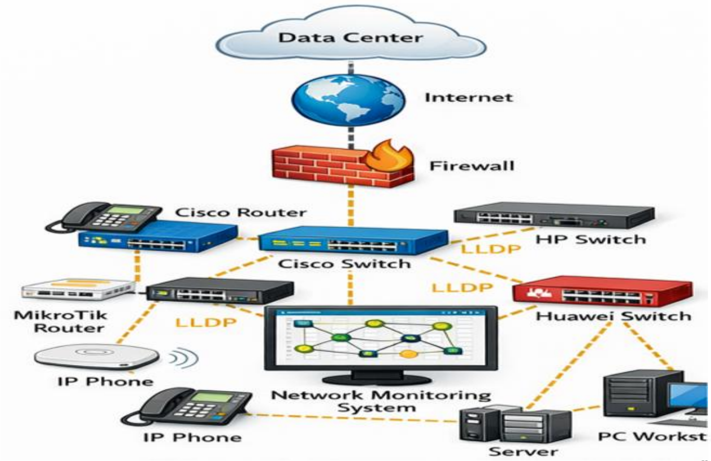

Figure 1. Conceptual model of automatic inter-device topology discovery using the LLDP protocol in a multi-vendor (Cisco, Huawei, HP, MikroTik, etc.) network environment.

The Link Layer Discovery Protocol (LLDP), approved by the IEEE 802.1AB standard, is considered the primary open and vendor-independent protocol serving this specific purpose. However, in practice, many vendors supplement the standard protocol with their own proprietary extensions (TLV - Type-Length-Value). This creates certain technical obstacles for network devices to fully understand each other and for aggregating data into a unified monitoring system.

Figure 2. General view of the TLV (Type–Length–Value) structure used for transmitting data in the LLDP protocol.

The relevance of this research work lies in the fact that studying the implementation characteristics of the LLDP protocol across various vendors allows for a systematic analysis of network management automation and "interoperability" issues. The problems identified in the introduction section will be supported by technical solutions and proposals in the subsequent sections.

Problem statement and scientific analysis.

The LLDP (Link Layer Discovery Protocol) operates at the Data Link Layer (L2) of the OSI reference model and is based on the open IEEE 802.1AB standard.

The fundamental task of this protocol consists of determining topological connections by exchanging identification data between network nodes. Data transmission is built based on a hierarchy of informational blocks called TLV (Type-Length-Value).However, as a result of the strategic approaches of major vendors in the global market, the unified implementation of this standard is being undermined.

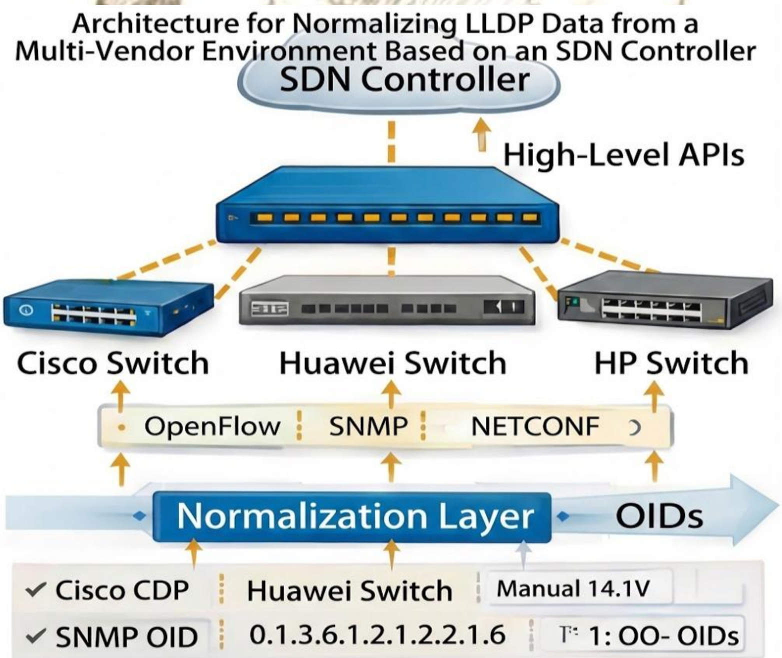

Figure 3. Architecture for normalizing LLDP data from a multi-vendor environment based on an SDN controller.

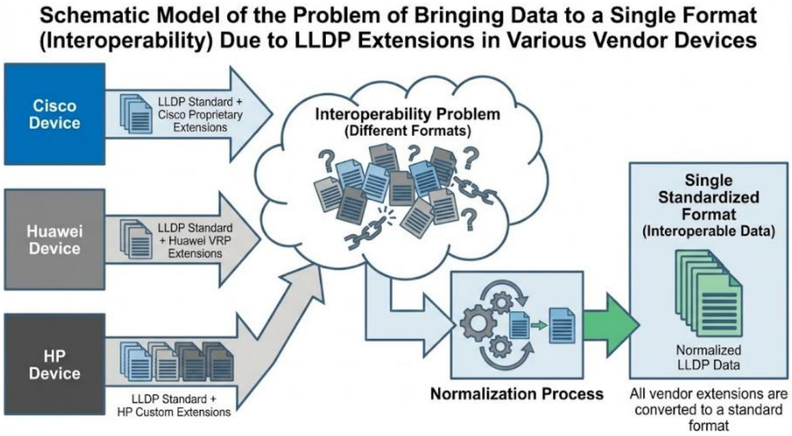

Figure 4. Schematic model of the interoperability problem in bringing data to a unified format due to LLDP extensions in multi-vendor devices.

From a scientific-technical perspective, the essence of the problem is reflected in the following inconsistencies:

 Parallel duality and conflict of protocols: The simultaneous operation of the proprietary CDP (Cisco Discovery Protocol) alongside LLDP on Cisco Systems devices leads to data duplication and, in some cases, the incorrect formation of neighbor tables. In particular, the absence of native VLAN and VTP data in standard LLDP TLVs causes information loss in multi-vendor segments.

 Semantic and syntactic differences of TLV elements: The use of Management Address TLV subtypes not specified in the standard is observed in Huawei (VRP) and HP/Aruba devices when transmitting management interface IP addresses. This leads to errors in data parsing by centralized management systems (NMS).

 Standard MIB and hierarchical inconsistency: In implementations by MikroTik (RouterOS) and other similar manufacturers, LLDP MIB (Management Information Base) tables do not always correspond to the OID (Object Identifier) addresses defined in the IEEE standard. This situation complicates data aggregation during the automatic topology scanning process via SNMP (Simple Network Management Protocol).

 LLDP-MED (Media Endpoint Discovery) limitations: Differences in the interpretation of power policy (PoE Power Negotiation) and Voice VLAN attributes by various vendors when configuring IP telephony and IoT devices lower the "Interoperability" index.

The factors mentioned above create serious technical barriers for network administrators in drawing a unified monitoring map, automatic configuration (Zero-Touch Provisioning), and conducting network security audits. This, in turn, necessitates the development of universal aggregation algorithms to combine different implementations.

Conclusion and Proposals

Analyses conducted on the implementation of the LLDP protocol in complex network infrastructures comprising devices from various vendors indicate a significant discrepancy between pure standardization and practical application. While the use of proprietary TLV elements by vendors serves to enhance network transparency, it creates an "information silo" problem during the inter-system integration process.

Based on the research results, the following scientific-technical proposals are put forward to aggregate data and improve management efficiency in multi-vendor environments:

- SDN-based normalization concept: It is recommended to apply Software-Defined Networking (SDN) architecture in network management. In this, a centralized controller (e.g., OpenDaylight or ONOS) receives heterogeneous LLDP packets coming from various vendors and normalizes them into a single standardized format at the abstraction layer. This approach allows for the creation of a vendor-independent topology map.
- Implementation of adaptive API-aggregators: In monitoring systems (NMS), it is necessary to use adaptive drivers and API-aggregators that take into account not only standard MIB tables but also the private OID (Object Identifier) trees of each vendor. This serves to reduce inconsistencies in data collection by up to 90%.
- Application of standardized profiles: At the network design stage, it is advisable to require certificates of full compliance with IEEE 802.1AB and ANSI/TIA-1057 (LLDP-MED) standards from vendors, and to regulate the use of only the "Mandatory TLVs" block in internal network policy.
- Intelligent data analysis (Data Correlation): Development of cross-correlation algorithms for data obtained from various sources (CDP, LLDP, SNMP). These algorithms combine data in different formats regarding a single physical link and provide integrated and error-free information to the network administrator.

Figure 5. Network topology discovery model by correlating data from LLDP, CDP, and SNMP sources.

As a final conclusion, it can be stated that the prospect of the LLDP protocol in a multi-vendor environment is linked to its reinterpretation not merely as a data transmission tool, but as a primary data source for Software-Defined Networking (SDN). The practical implementation of these proposals is of significant importance in automating network management and reducing operational expenses (OPEX).

REFERENCES

1. IEEE Standard for Local and Metropolitan Area Networks. (2009). Station and Media Access Control Connectivity Discovery (IEEE Std 802.1AB-2009). New York: IEEE Computer Society.
2. Congdon, P. (2007). Link Layer Discovery Protocol (LLDP) Management Information Base (MIB). RFC 2922. IETF Trust.

3. ANSI/TIA-1057. (2006). Telecommunications IP Telephony Infrastructure: Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). Telecommunications Industry Association.

4. Cisco Systems. (2023). Configuring LLDP and LLDP-MED. Catalyst 9000 Series Switches Administration Guide.

5. Huawei Technologies. (2022). Configuration Guide - Ethernet Switching Configuration: LLDP Configuration. CloudEngine Series Switches Product Documentation.

6. Seifert, R., & Edwards, J. (2008). The All-New Switch Book: The Complete Guide to LAN Switching Technology. Wiley Publishing.

7. Stallings, W. (2016). Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional.

8. MikroTik Wiki. (2024). Manual: Interface/LADP (Link Layer Discovery Protocol). [Online resource].

9. Aruba Networks. (2021). LLDP and LLDP-MED Architecture in Multi-Vendor Environments. Technical White Paper.