EUROPEAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND MANAGEMENT STUDIES

TYPE Original Research
PAGE NO. 143-148
DOI 10.55640/eijmrms-05-02-28

Systematizing the Regulation of Local Networks

Qalandarov Jamil Jalolovich

System Administrator, Digital Infrastructure Development Center, TATU named after Muhammad al-Xorazmiy, Uzbekistan

Akmalov Elyor Ilxomovich

IT Developer, Director of Active Service LLC, Uzbekistan

Omonov Zokir Hojiboy o`g`li

Network Administrator, Digital Infrastructure Development Center, TATU named after Muhammad al-Xorazmiy, Uzbekistan

OPEN ACCESS

SUBMITED 24 December 2024
ACCEPTED 26 January 2025
PUBLISHED 28 February 2025
VOLUME Vol.05 Issue02 2025

Abstract: In this article, when the LLDP and SNMP protocols are used together, they provide network engineers with a powerful set of tools. Data collection from devices via SNMP enables continuous monitoring of the network's performance, while LLDP automatically identifies the network topology and facilitates understanding of the connections between network devices.

The combined use of these protocols allows administrators to quickly and accurately assess the network's status, prevent potential issues, or resolve them promptly. To enhance network efficiency and reduce operational problems, it is crucial to use these protocols properly. The article outlines effective methods for utilizing these protocols.

Keywords: LLDP, SNMP, local network, LAN, SNMP, CDP, EDP, FDP, LLTD.

Introduction: The Relevance of Regulating and Systematizing Local Networks

The relevance of regulating and systematizing local networks is very important in today's era of advancing technology. Local networks (Local Area Networks, LAN) are systems that connect computers and other devices located within a limited area, such as an office building, manufacturing facility, or educational institution. By properly regulating and systematizing networks, it is possible to prevent data theft and misuse.

Implementing security policies and technologies, along with measures such as encryption and access control systems, is essential.

Systematizing local networks facilitates the seamless exchange of data between various devices and applications, which in turn helps to optimize business processes and enhance operational efficiency. Overall, the regulation and systematization of local networks are crucial for improving the effectiveness of data integration and management processes.

This is particularly an important issue for large organizations and corporations, as all these measures help manage data effectively and enhance production efficiency. Data integration enables the merging of data obtained from various sources and its utilization in a common format. This process facilitates data exchange among numerous systems and platforms while ensuring data consistency within the organization. Data management involves optimizing the processes of storing, regulating, analyzing, and using data. This allows organizations to manage data efficiently, ensure its security, and control access to it [2]. By properly organizing and regularly updating the system, the reliability and stability of the network are ensured. This, in turn, prevents downtime and guarantees the continuous operation of the system. Network reliability refers to the network's ability to transmit data accurately and error-free. Reliable local networks must have the ability to withstand unexpected malfunctions and recover quickly from them. Network redundancy includes having backup network devices and communication channels, such as using two servers or two internet connections. Monitoring and diagnostics ensure the reliable operation of the network by continuously tracking its status, promptly identifying issues, regularly creating backups of critical information, and securely storing them. Proper organization of the network allows for efficient management of servers, storage devices, and other resources. This helps in optimizing resource usage and improving operational efficiency. The issue of organizing and structuring local networks is particularly important at the corporate and organizational levels. It is one of the key factors in ensuring the efficient allocation of resources and the stable operation of the network. Optimal resource distribution—such as effectively sharing network resources like speed, memory, and storage capacity—not only enhances system performance but also enables better service delivery to users. Organizing local networks also aids in effectively implementing security policies and protecting data. Efficient sharing of network resources facilitates scalability, meaning it becomes easier to expand the network or connect new devices. Properly designing the network simplifies future expansion and modernization. The benefits of organizing and structuring local networks are primarily associated with two key aspects: scalability (the ability to increase capacity) and flexibility (the ability to adapt to different situations). These two aspects are particularly important in today's rapidly changing technological environment. Scalability refers to the network's ability to adapt to growth. This includes tasks such as adding new devices to the network, supporting a larger number of users, and enhancing the capability to process and manage data. By ensuring scalability and flexibility, organizations can effectively respond to evolving demands and technological advancements without significant disruptions to their existing infrastructure. Considering scalability in organizing local networks provides the opportunity to adapt the network to future growth and technological advancements. Flexibility , on the other hand, refers to the network's ability to work with various technologies, software, and operating systems. This includes adapting the network to use new software or accommodate varying workloads. Flexible networks also simplify integration between different technologies and platforms, which helps organizations efficiently manage their business processes. In today’s dynamic environment, having a network that is both scalable and flexible ensures that businesses can seamlessly incorporate new solutions, adjust to changing demands, and maintain high performance without significant disruptions. This approach not only enhances operational efficiency but also prepares the organization for long-term success in an ever-evolving technological landscape.

The process of organizing and structuring local networks plays a crucial role in enhancing the efficiency of businesses' and organizations' IT infrastructure. While organizing and structuring local networks can be a multi-step and complex process, one of its key components is identifying needs. This primarily involves improving network efficiency, ensuring security, and considering future expansion possibilities. By properly planning and implementing this process, organizations can achieve a more reliable, scalable, and secure IT environment. This not only helps meet current demands but also prepares the infrastructure for future technological advancements and business growth, ensuring long-term effectiveness and adaptability. Assessing the current state involves analyzing the existing network infrastructure, including hardware and software, as well as the network's current performance metrics. Identifying user needs is another critical part of this process, which focuses on understanding the requirements and expectations of network users

(employees, customers, partners). This helps anticipate network loads and prevent unexpected outages. Determining the requirements for hardware and software involves specifying the needs for network devices such as routers, switches, firewalls, and software (operating systems, network management tools). This step helps avoid the use of inappropriate or inadequate equipment that does not meet network demands. Selecting the right topology plays a crucial role in organizing and structuring local networks. The choice of topology significantly impacts network performance, reliability, and scalability. An appropriate topology ensures efficient data flow, minimizes potential bottlenecks, and enhances overall network efficiency. By carefully evaluating these factors, organizations can design a network that aligns with their current and future needs while maintaining stability and security.

Topology is the scheme of physical or logical connections between devices in a network. The most commonly used topologies for local networks include star, ring, bus, mesh, and hybrid topologies. In the star topology , all devices are connected to a central point (for example, a switch or router). This topology is easy to manage because each device is only connected to the central point. If one device fails, it does not affect the operation of other devices. However, if the central device fails, the entire network will stop functioning.

In the ring topology, each device is directly connected to two neighboring devices, forming a ring.

Data is sent in one direction around a loop in a ring topology. This topology is simple and reliable, but if one device in the ring fails, the entire network may stop functioning. In a bus topology, all devices are connected to a single shared transmission channel. Data is broadcast through this channel. The advantage of this topology is that new devices can be added easily. However, if there is a problem with the channel, it could affect the entire network. In a mesh topology, each device is connected directly to one or several other devices. This topology provides the highest level of reliability and flexibility.

Network Protocols in Regulating Local Networks

In managing and monitoring local networks, protocols such as SNMP (Simple Network Management Protocol) and LLDP (Link Layer Discovery Protocol) play a crucial role. These protocols are essential for overseeing the network and monitoring its operational status. SNMP is used for data exchange among network devices (for example, routers, switches, servers, and workstations). It allows for collecting information for network management and sending commands to devices. With SNMP, administrators can monitor the performance of devices on the network to ensure they operate correctly and optimally. LLDP is an open standard used for data exchange between network devices. With this protocol, network devices (such as routers, bridges, switches, servers, phones, and other devices) can identify each other and exchange information about the network topology. LLDP helps administrators quickly and efficiently describe the network infrastructure, thereby facilitating network management and troubleshooting. The main functions of LLDP are as follows:

Device detection: Using LLDP, network devices can automatically recognize each other. This is especially useful for identifying the location of devices in large and complex networks.

Information haring: Using LLDP, configuration data—including s device name, port identifier, and device types—is exchanged among devices.

Network diagnostics: LLDP provides network administrators with precise information about the status of devices and their interconnections, thereby facilitating network management as well as the detection and resolution of potential issues. LLDP operates in two main modes: transmitter and receiver.

Transmitter mode: In transmitter mode, the device operating in this mode regularly sends its own data—including identification information, port information, and capabilities—via LLDP packets to other devices. This information is used to detect newly connected devices in other parts of the network and to understand their configuration.

Receiver mode: In receiver mode, a device operating in this mode receives LLDP packets from other devices and analyzes them. Based on the received data, the device can build the network topology and establish communication with other devices. LLDP can operate in a bidirectional mode, meaning that a device can function as both sender and receiver simultaneously. This enables effective management and monitoring of a scalable network.

LLDP Packet Structure

LLDP packets consist of TLV (Type, Length, Value) blocks, which serve as the primary mechanism for carrying protocol data. Each TLV contains three main components:

1. Type: The type of the TLV. This part indicates what kind of data it contains, such as a device identifier, port identifier, device capabilities, etc.

2. Length: The length of the Value part in bytes. It shows the size of the data block.

3. Value: The data itself. Depending on the type of information, this part can include various data such as the device name, physical address, port name, etc.

LLDP packets are sent at regular intervals, allowing for the discovery of newly connected devices and the determination of the network topology.

LLDP Packet Blocks

LLDP packets primarily consist of the following TLV blocks:

- **Chassis ID TLV:** The general identifier of the device. This information enables the device to be uniquely identified on the network.
- **Port ID TLV:** The general identifier of the port. This information is used to uniquely identify the port.
- **TTL TLV:** The packet's "time-to-live." After this time elapses, the information is considered outdated.
- **Port Description TLV:** A description of the port. This information provides details about the port's characteristics and other important data.
- **System Name TLV:** The system's name. This is the general name or description of the device.
- **System Description TLV:** A detailed description of the system. This includes, for example, information about the software in use and hardware characteristics.
- **System Capabilities TLV:** The capabilities of the system. This information indicates what the device is capable of, such as functioning as a router or a switch.
- [1,4].

Below is an example of LLDP packets between two devices in JSON format (Figure 1). In this example, you can observe the connection between two switches, SW1 and SW2. Each switch sends its own LLDP packet, which contains the device identifier, port identifier, TTL, port and system description, as well as the system capabilities. These JSON examples demonstrate the LLDP protocol's ability to exchange data and its effectiveness in identifying interconnections between network devices. Additionally, there are software libraries available that provide high-level support for this protocol, which simplify the work of programmers and network administrators. Below is an automatic diagram of the network device map created using a python3 program with the LLDP protocol[5].


```
{
   "LLDP_Packet_1": {
      "Chassis_ID":"00:1A:2B:3C:4D:5E",
      "Port_ID":"GigabitEthernet1/0/1",
      "TTL":120,
      "Port_Description":"To switch SW2, port Gi1/0/2",
      "System_Name":"SW1",
      "System_Description":"Layer 2 Switch, Model HPE5130",
      "System_Capabilities":"Bridge, Router"
   },
   "LLDP_Packet_2": {
      "Chassis_ID":"00:1A:2B:3C:4D:5F",
      "Port_ID":"GigabitEthernet1/0/2",
      "TTL":120,
      "Port_Description":"To switch SW1, port Gi1/0/1",
      "System_Name":"SW2",
      "System_Description":"Layer 2 Switch, Model ZYXEL",
      "System_Capabilities":"Bridge"
   }
}
```


Figure 1. LLDP packets between two devices in JSON format.

Bu pratokol yordamida TATUda mavjud kommutatorlarning xaritasi avtomatik xolda yaratilgan. LLDP protokol yordamida tartibga solinmagan va juda ko‘p mexnat talab qilinadigan tarmoqlarni tartiblashtirish, tarmoq xaritalarini shakllantirish, tizimlashtirish uchun juda katta amaliy yordam berishimi mumkin. Shuningdek. bazi ishlab chiqaruvchilar tomonidan LLDP protokoliga o‘xshash bazi protokollar yaratilgan ularni bazilarini ko‘rib o‘tamiz.

- Cisco Discovery Protocol (CDP): A protocol developed by Cisco and primarily used on Cisco devices. CDP is also

used to discover network devices and obtain information about them, but it is limited to Cisco devices only. This protocol, like LLDP, transmits information in TLV format.

- Extreme Discovery Protocol (EDP): A protocol developed by Extreme Networks, designed specifically for the company's devices. It is similar to CDP, but it can only operate with Extreme devices.
- Foundry Discovery Protocol (FDP): A protocol developed by Foundry Networks (currently under Brocade Communications Systems) and used for its devices.
- Link Layer Topology Discovery (LLTD): A protocol developed by Microsoft for the Windows operating system. It is primarily used in home and small office networks.

- Link Layer Topology Discovery (LLTD): A protocol developed by Microsoft for the Windows operating system. It is primarily used in home and small office networks.

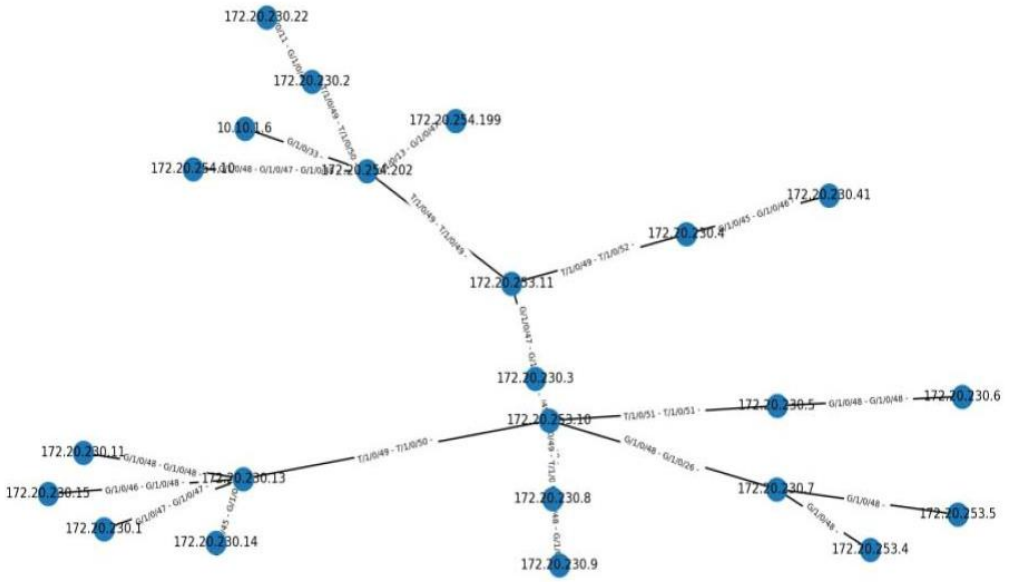

Figure 2. Automatically creating a network map using the LLDP protocol

LLDP is an open protocol standardized by IEEE that can be used on devices from various manufacturers. CDP, on the other hand, is designed for Cisco devices and may not be compatible with other brands. LLDP is developed in accordance with international standards, ensuring compatibility with a wider range of devices. Other manufacturers have their own proprietary protocols, such as EDP and FDP, which offer optimized functions and features for their devices. However, the drawback of these protocols is that they only work with their own manufacturers' devices and are not mutually compatible [1,3].

CONCLUSION

Data security can be ensured through the effective regulation of local networks. This is particularly necessary to protect against cyberattacks and to prevent unauthorized access to data. Through systematized networks, work can be managed effectively and resources can be utilized efficiently, which helps to increase work productivity and enhance the overall performance of the organization.

Regulating local networks also enables the monitoring and management of network traffic. In turn, this contributes to the reliable operation of the network and the optimal allocation of resources. Systematized networks allow for the delivery of high-quality services to users, thereby improving their work experience and reinforcing trust in the organization.

Moreover, by regulating and systematizing local networks, it becomes possible to identify technical issues and resolve them quickly, ensuring the stable operation of the network. In conclusion, regulating and systematizing local networks offers a range of significant benefits, including ensuring data security, enhancing work efficiency, controlling traffic, improving service quality for users, and promptly addressing technical problems.

REFERENCES

IEEE 802.3 Frame Expansion Study Group, Ottawa, Sept 30, 2004

Gary A. Donahue. Network Warrior, Second Edition, 2011, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, pp.759.

https://www.geeksforgeeks.org/link-layer-discovery-protocol-lldp/

https://learningnetwork.cisco.com/s/article/link-layer-discovery-protocol-lldp-x

https://codereview.stackexchange.com/questions/238781/find-neighbours-of-a-switch-using-python-and-snmp-lldp