Сизов И.М., Сулимов А.Д. Использование LLDP в отечественных ОС на ядре LINUX // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 1(51) с. 16–27

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.738

ИСПОЛЬЗОВАНИЕ LLDP В ОТЕЧЕСТВЕННЫХ ОС НА ЯДРЕ LINUX

[1]Сизов И.М., Сулимов А.Д.
ФГАОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" , Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: [1]goga.sizov.04@mail.ru

Протокол LLDP (Link Layer Discovery Protocol) представляет собой стандарт сетевого взаимодействия, который позволяет производить обмен информацией между устройствами. Использование данного протокола помогает упростить настройку и мониторинг сетевых соединений. В настоящее время активно развиваются отечественные операционные системы на базе ядра Linux, что напрямую связано с импортозамещением и обеспечением технологической независимости. Использование протокола LLDP также упрощает процесс построения гибких и управляемых сетей, соответствующих современным требованиям. Цель исследования заключается в анализе особенностей использования протокола LLDP в отечественных ОС на ядре Linux и выявлении недостатков использования данного протокола.

Ключевые слова: LLDP, соседние устройства, коммутатор, локальная сеть, AutoAttach-таблица, перехват пакетов.

USING LLDP IN DOMESTIC OS BASED ON THE LINUX KERNEL

[1]Sizov I.M., Sulimov A.D.
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky prospekt, 65 k. 1), e-mail: [1]wild.alex2016@yandex.ru

The LLDP Protocol (Link Layer Discovery Protocol) is a network communication standard that allows the exchange of information between devices. Using this protocol helps simplify the configuration and monitoring of network connections. Currently, domestic operating systems based on the Linux kernel are actively developing, which is directly related to import substitution and ensuring technological independence. Using the LLDP protocol also simplifies the process of building flexible and managed networks that meet modern requirements. The purpose of the study is to analyze the features of using the LLDP protocol in domestic OS based on the Linux kernel and identify the disadvantages of using this protocol.

Keywords: LLDP, neighboring devices, switch, LAN, AutoAttach table, packet interception.

Теоретическая основа

LLDP (Link Layer Discovery Protocol) - протокол канального уровня, позволяющий коммутатору оповещать информацию о своем существовании в локальной сети и передавать эту информацию, аналогично он может и получать сведения от другого устройства. Каждое устройство LLDP может отправлять информацию о себе соседям независимо друг от друга. Устройство хранит информацию о соседях, но не перенаправляет её. [2, с. 1]

Для LLDP зарезервирован специальный MAC-адрес, коммутаторы с таким адресом получателя не будут передавать его дальше.

LLDP использует атрибуты, которые содержат описание типа, длины и значения. Они называются TLV (тип, длина, значение). Устройства, поддерживающие LLDP, используют TLV для отправки и получения информации своим непосредственно подключенным соседям. Вот пример некоторых основных TLV: описание порта TLV, имя системы TLV, описание системы TLV, возможности системы TLV, TLV-адрес управления.

Некоторые сетевые конечные устройства могут использовать LLDP для назначения VLAN или требований PoE (Power over Ethernet). Для этого было сделано усовершенствование, которое называется MED (Media Endpoint Discovery). Обычно это называется LLDP-MED. LLDP позволяет определить физическую топологию соединений устройств и визуализировать ее в удобном для восприятия человеком виде [1, с. 144].

Методы исследования

Тип исследования

Исследование носит экспериментально-аналитический характер. Эксперимент будет направлен на настройку и проверку работы протокола LLDP в локальной сети на примере двух устройств, функционирующих в роли коммутаторов. Конфигурация будет выполняться с использованием Open vSwitch (OVS) с предварительной установкой необходимых пакетов LLDP. После установки необходимых пакетов и проверки работы протокола будет сымитирована атака на пакеты протокола LLDP.

Характеристика выборки

В рамках исследования была сформирована выборка оборудования и программного обеспечения:

- Два коммутатора
- Отечественные операционные системы на базе ядра Linux: Альт, РЕД ОС, ROSA Linux, Astra Linux
- Установленный пакет Open vSwitch (OVS) для настройки виртуальных коммутаторов
- Пакет LLDP для обеспечения поддержки протокола LLDP и возможности использования команды
- Инструмент Wireshark для захвата и анализа сетевого трафика

Методы сбора данных

Для сбора данных в рамках эксперимента использовались следующие методы:

- Была настроена сеть, состоящая из двух виртуальных коммутаторов на основе Open vSwitch (OVS), с включенной поддержкой LLDP.
- Был произведен сбор данных о работе протокола LLDP с использованием встроенных инструментов, таких как lldpctl, а также команд управления конфигурацией OVS (ovs-vsctl).
- Были проанализированы передаваемые LLDP-пакеты между коммутаторами.
- Было произведено описание устройств и имени системы через AutoAttach-таблицу.
- Была зафиксирована информация о соседних устройствах на каждом коммутаторе.

- Был произведен перехват пакетов с третьего устройства, просмотр данных пакетов и сброс трафика.

Описание процедуры проведения исследования

Для проведения исследования была подготовлена тестовая среда, состоящая из двух коммутаторов, работающих на основе Open vSwitch (OVS). Настройка протокола LLDP включала включение LLDP на сетевых интерфейсах коммутаторов с помощью команды `ovs-vsctl`. Далее проводилась оценка работы и надежности LLDP. Оценка работы LLDP в сети проводилась на основе данных о корректности отображения информации о соседних устройствах, анализе структуры передаваемых LLDP-сообщений. Оценка надежности работы LLDP проводилась путем просмотра перехваченных пакетов с использованием инструмента Wireshark сбросом трафика.

Методы обработки данных

- Проведен анализ работы протокола LLDP на каждом из двух коммутаторов.
- Просмотрена в ходе эксперимента информация о работе LLDP, такая как таблциа AutoAttach, отображаемая информация о соседних устройствах.
- Выявлены рекомендации в ходе имитированной атаки на пакеты протокола.

Проведение исследования

Для проведения эксперимента будет реализована топология, изображенная на Рисунке 1. Для начала эксперимент будет проведен на операционной системе Альт. Топология включает в себя подключение коммутаторов друг к другу с использованием прямых соединений. Каждый коммутатор будет настроен для передачи и приема LLDP-сообщений, а также для отображения информации о соседних устройствах.

Рисунок 1. – Топология проведения эксперимента

Для начала настроим оба устройства в качестве коммутаторов. Для этого будет использоваться пакет Open vSwitch. С помощью следующих команд на машинах Альт произведем установку пакета:

```
apt-get update
apt-get install openvswitch –y
```

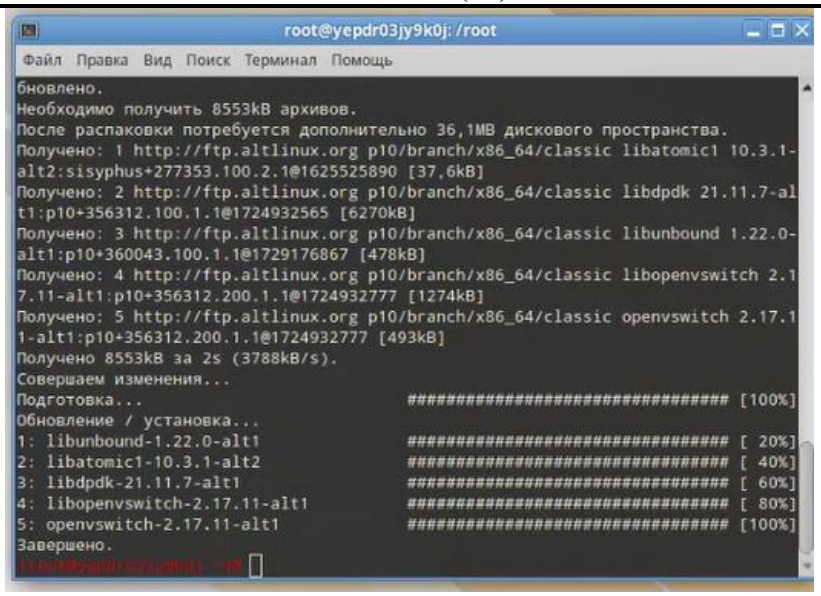

Рисунок 2 – Установка пакета Open vSwitch (Альт)

Далее произведем непосредственно настройку самих коммутаторов. Выполняется это с помощью следующих команд:

```
systemctl start openvswitch.service
ovs-vsctl add-br ovs0
ovs-vsctl add-port ovs0 enp0s3
```

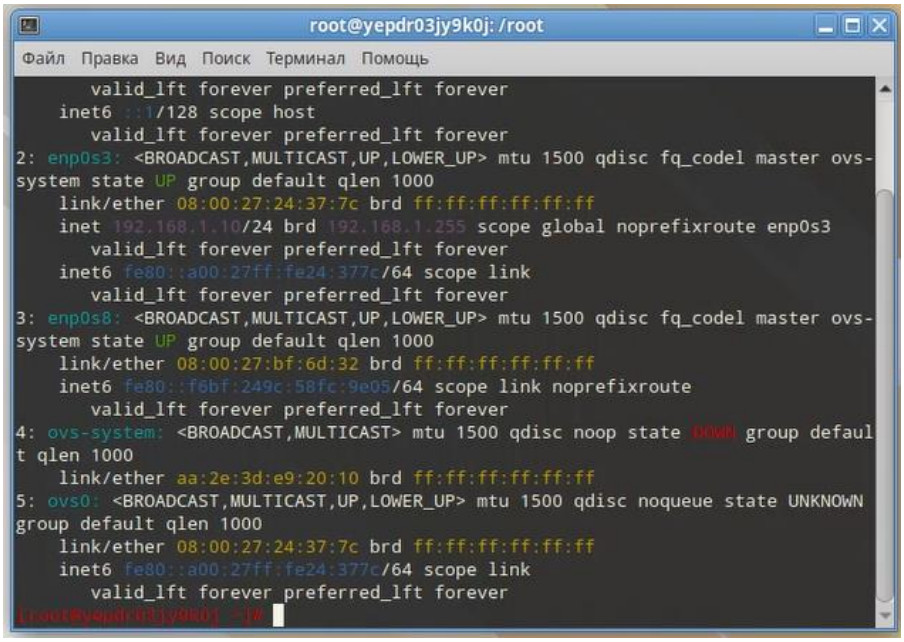

Рисунок 3 – Просмотр настройки коммутатора (Альт)

Чтобы начать настройку LLDP необходимо установить пакет на машину. Используем для этого следующие команды:

```
apt-get update
apt-get install lldpd
systemctl start lldpd
```

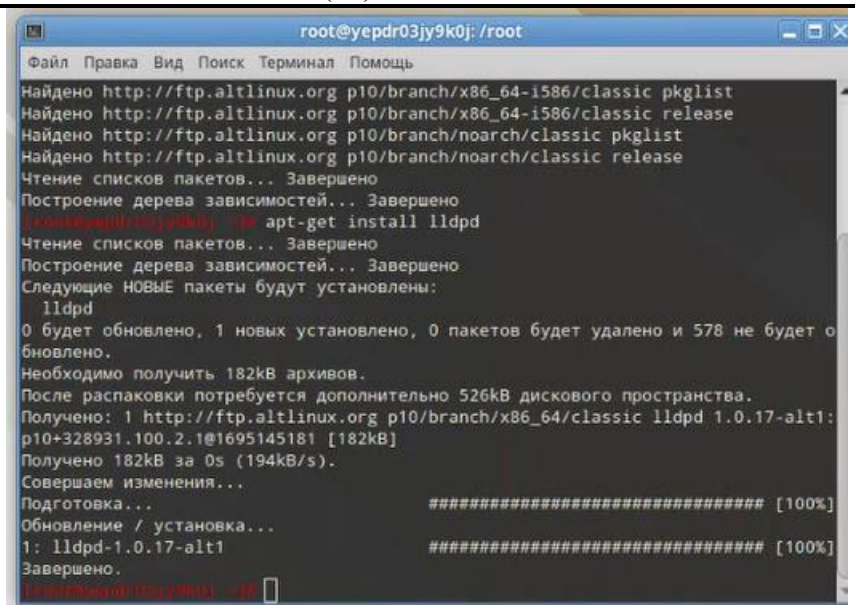

Рисунок 4 – Установка пакета lldp (Альт)

Следующий шаг – произвести настройку LLDP на устройствах. Для этого нужно выполнить следующие команды:

ovs-vsctl set interface enp0s3 lldp:enable=true

ovs-vsctl add-aa-mapping ovs0 0 0

ovs-vsctl set AutoAttach . system_name=”ovs_ALT1”

ovs-vsctl set AutoAttach . system_description=” The_OVS_on_ALT1”

ovs-vsctl list AutoAttach

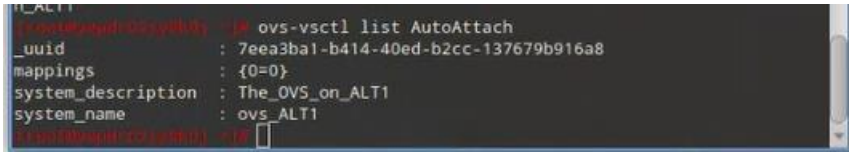

Рисунок 5 – Просмотр настройки таблицы AutoAttach (Альт)

Данные настройки производятся на обоих устройствах. Для просмотра информации о соседе используется команда lldpctl show portlist enp0s3:

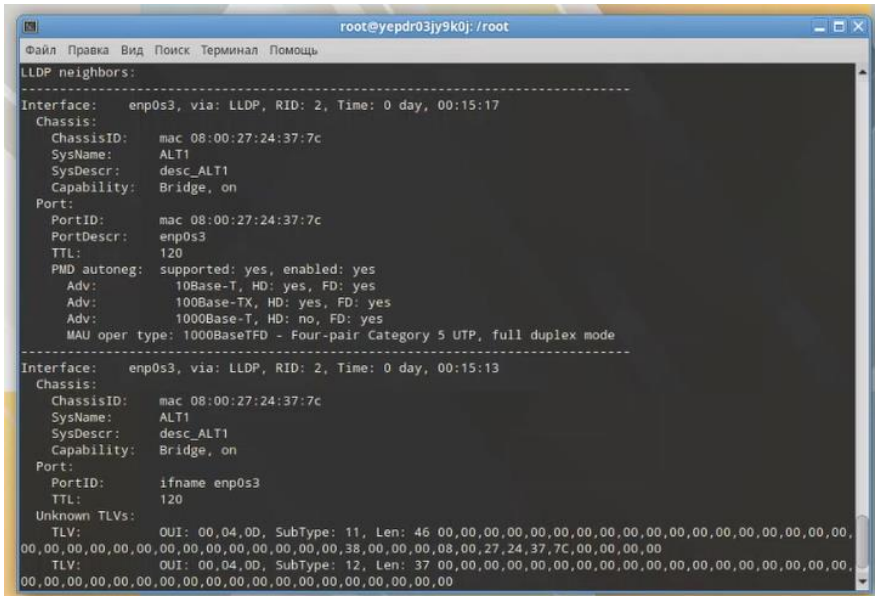

Рисунок 6 – Просмотр информации о соседе (Альт)

Со стороннего устройства выполним атаку на данный протокол. Для начала произведем перехват пакетов, далее выполним их просмотр и произведем сброс трафика. [3]

Для просмотра передаваемых пакетов необходимо на третье устройство установить Wireshark. С помощью следующих команд произведем установку:

sudo apt-get update

sudo apt-get install wireshark

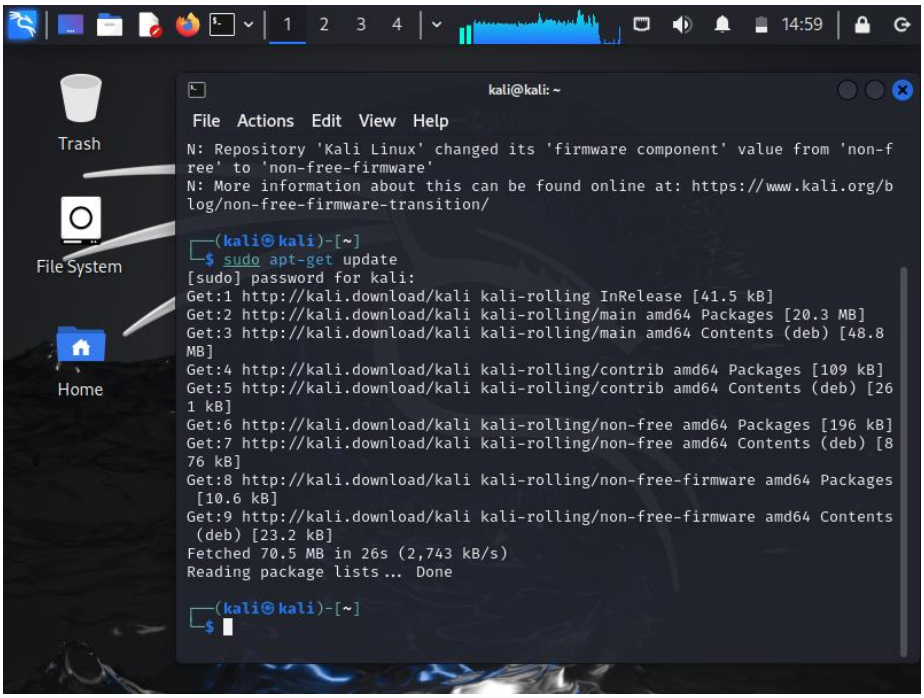

Рисунок 7 – Установка Wireshark

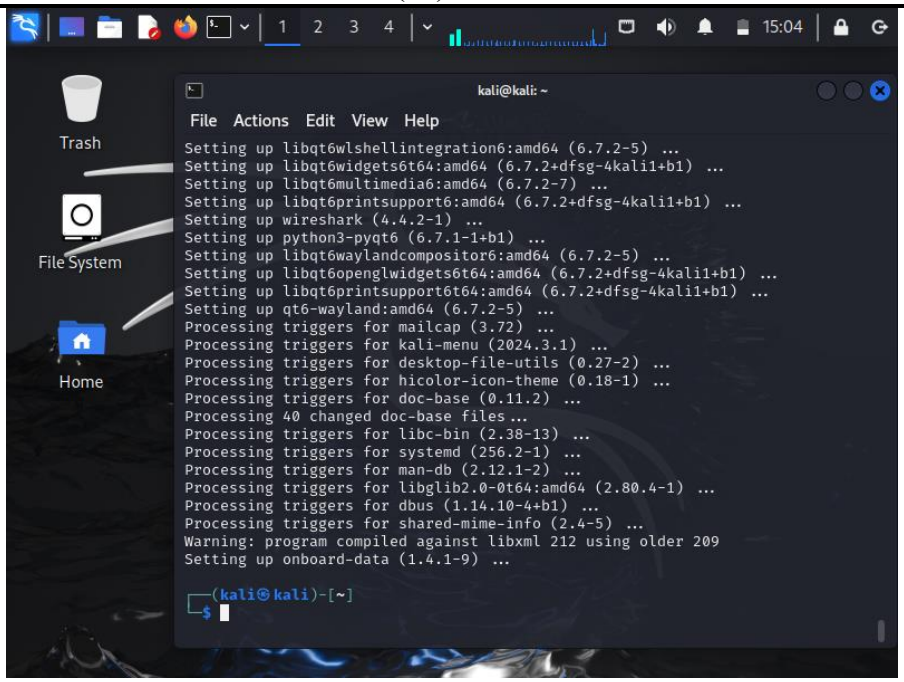

Рисунок 8 – Установка Wireshark

Теперь в самой программе просмотрим пакеты протокола LLDP.

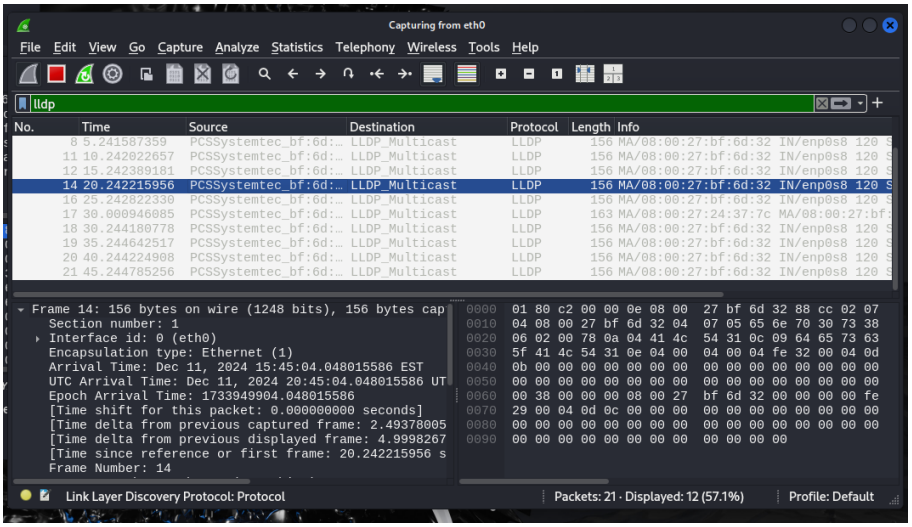

Рисунок 9 – LLDP-пакеты

Последним шагом остается сброс трафика LLDP.

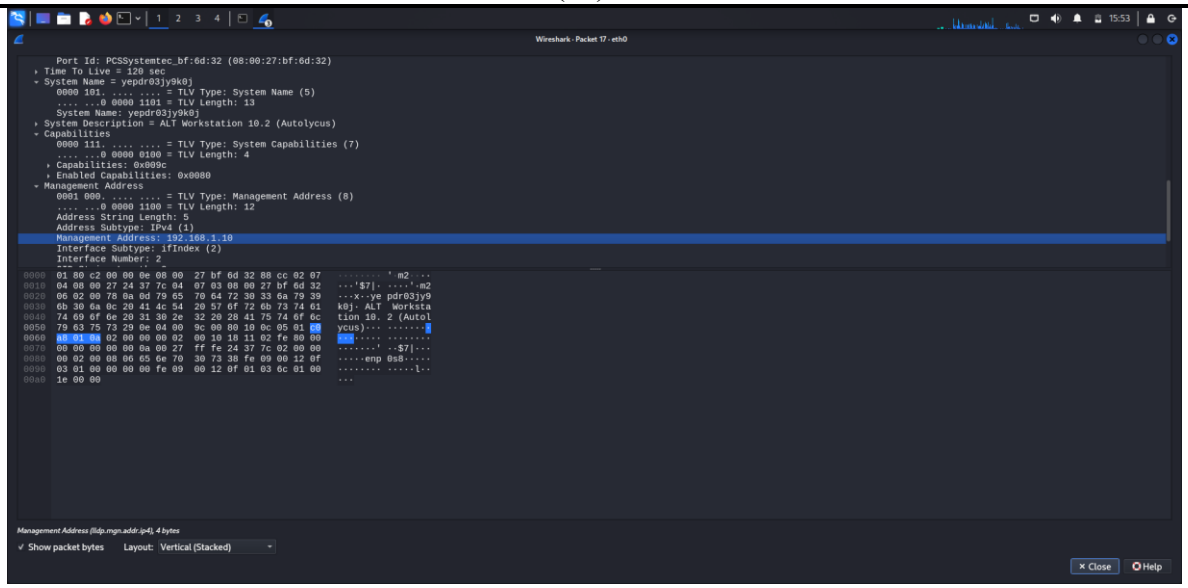

Рисунок 10 – Сброс трафика LLDP

Рассмотрим настройку LLDP на других отечественных операционных системах. Начнем с РЕД ОС. Для настройки коммутаторов и пакета LLDP будут использованы аналогичные команды [5]. Настройка коммутаторов:

sudo yum install openvswitch
sudo systemctl start openvswitch
sudo ovs-vsctl add-br br0
sudo ovs-vsctl add-port br0 enp0s3

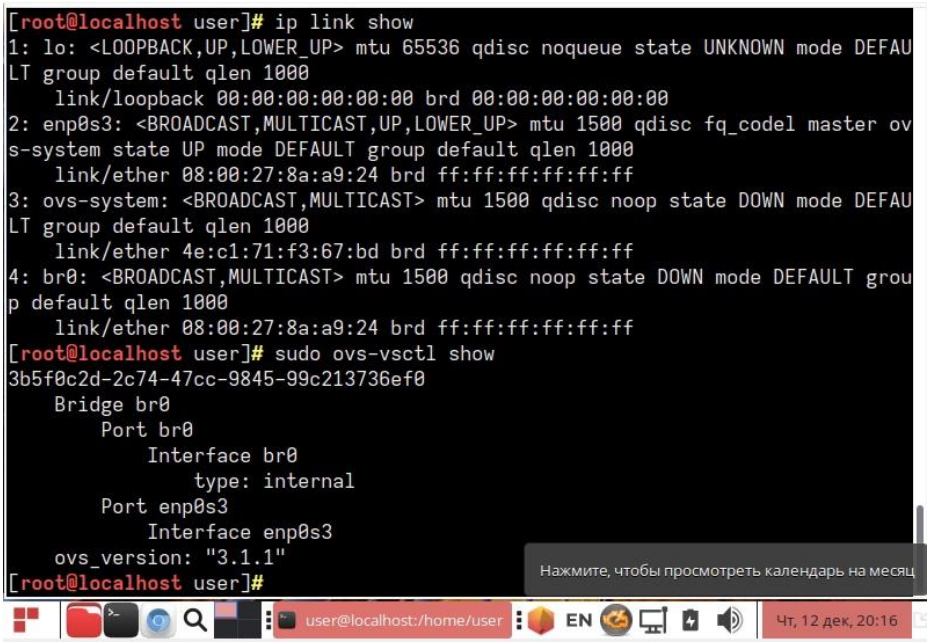

Рисунок 11 – Настройка коммутатора (РЕД ОС)

Для настройки LLDP выполним следующие команды:

sudo yum update
sudo yum install lldpd

sudo systemctl start lldpd

sudo ovs-vsctl set interface <имя_вашего_интерфейса> lldp:enable=true

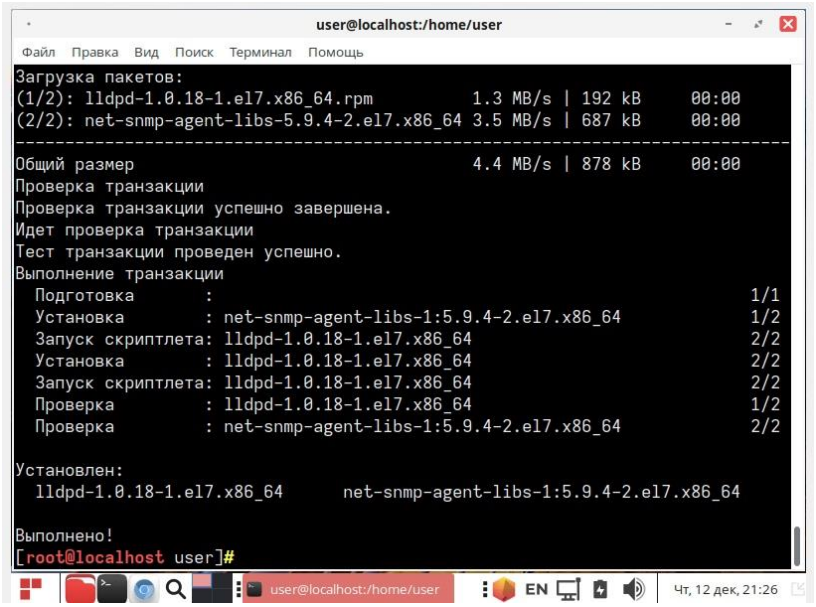

Рисунок 12 – Установка LLDP (РЕД ОС)

С помощью команды lldpctl show enp0s3 просмотрим информацию о соседнем устройстве:

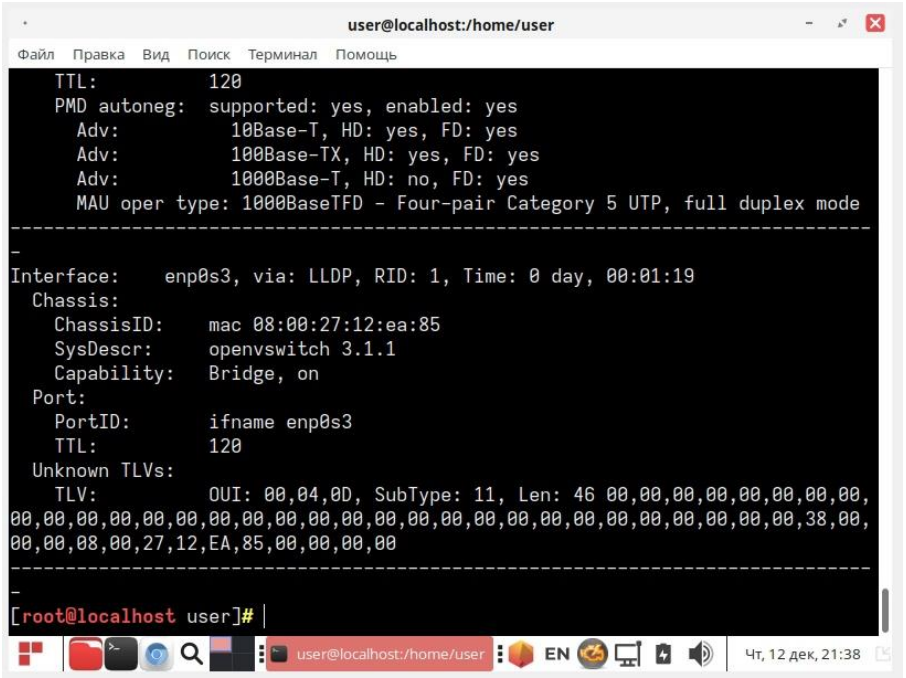

Рисунок 13 – Просмотр информации о соседе (РЕД ОС)

Настройка топологии и протокола LLDP на операционных системах ROSA Linux [7] и Astra Linux [6] производится с помощью аналогичных команд:

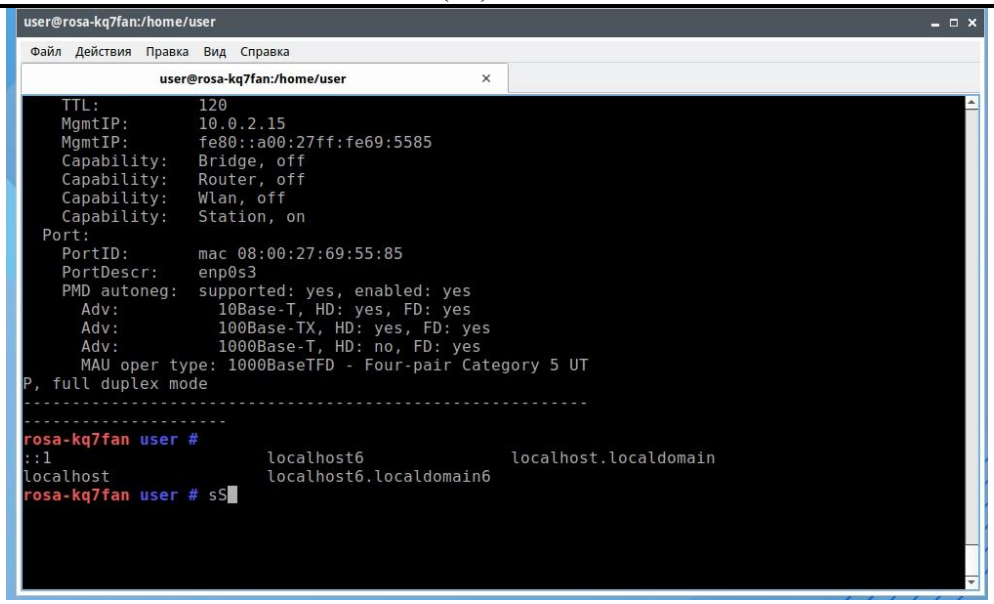

Рисунок 14 – Просмотр информации о соседе (ROSA Linux)

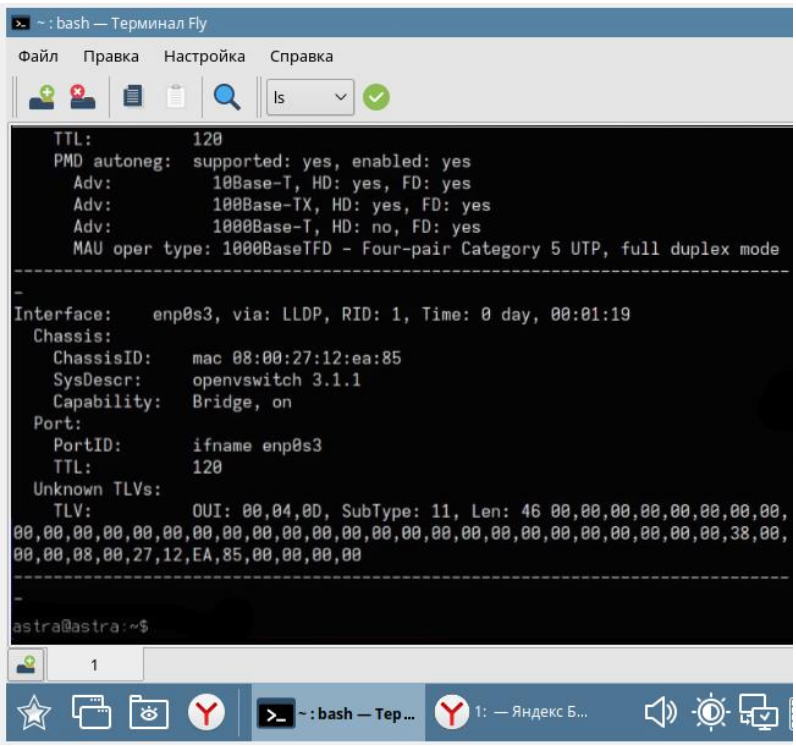

Рисунок 15 – Просмотр информации о соседе (Astra Linux)

Заключение

В ходе данного эксперимента была выполнена реализация работы протокола LLDP на устройствах с установленной на ними отечественными операционными системами Альт, РЕД ОС, ROSA Linux, Astra Linux. Было показано, что протокол LLDP позволяет получать и просматривать информацию о соседних устройствах в сети. В данной части эксперимента так же было замечено, что AutoAttach - является не частью стандартной установки, а специфичной настройкой для операционной системы Альт. Другие дистрибутивы не имеют AutoAttach по умолчанию.

Второй частью данного эксперимента была произведенная на протокол атака, в ходе которой удалось просмотреть перехваченные пакеты и произвести сброс трафика. Это приводит к мысли о том, что в ходе подобной атаки злоумышленник может получить полезную для него информацию, выявить уязвимости коммутатора, которые он будет использовать в дальнейших целях. В связи с этим, будут предложены следующие рекомендации. В гостевых сетях протокол LLDP может быть включен по умолчанию, поэтому стоит его отключать на неиспользуемых интерфейсах. Таким образом, удастся прекратить транслирование данных и обеспечить защиту.

Список литературы

1. Компьютерные сети. L2–технологии : практикум / А.Г. Уймин. — Москва : Ай Пи Ар Медиа, 2024. — 191 с. (дата обращения: 29.11.2024)
2. Определение топологии с помощью протокола LLDP в сетях Juniper / Лагутин И.А. [Электронный ресурс]. URL: https://www.elibrary.ru/ (дата обращения: 10.12.2024)
3. 5 Простых методов защиты маршрутизатора - включая атаку и анализ пакетов / Брэндон Хитцель [Электронный ресурс]. URL: https://www.networkdefenseblog.com/post/ (дата обращения: 10.12.2024)
4. Документация NAG [Электронный ресурс]. URL: https://nag.wiki/ (дата обращения: 10.12.2024)
5. База знаний РЕД ОС [Электронный ресурс]. URL: https://redos.red-soft.ru/base/ (дата обращения: 10.12.2024)
6. База знаний Астра [Электронный ресурс]. URL: https://wiki.astralinux.ru/kb/alfavitnyj-ukazatel-190914856.html (дата обращения: 10.12.2024)
7. Системное Администрирование ОС Роса «Хром» / Мирзоян А.В. [Электронный ресурс]. URL: https://stage.rosalinux.ru/media/2024/05/rosa_basics.pdf (дата обращения: 10.12.2024)
8. Перехват и анализ сетевого трафика с помощью «Wireshark» / Мешкова Елена Владимировна [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=27443875 (дата обращения: 10.12.2024)

References

1. Computer networks. L2 technologies : a practical course / A.G. Uimin. — Moscow : AI Pi Ar Media, 2024. — 191 p. (accessed: 11/29/2024)
2. Topology determination using the LLDP protocol in Juniper networks / Lagutin I.A. [Electronic resource]. URL: https://www.elibrary.ru / (date of request: 10.12.2024)
3. 5 Simple methods of router protection - including attack and packet analysis / Brandon Hitzel [Electronic resource]. URL: https://www.networkdefenseblog.com/post / (date of request: 10.12.2024)
4. NAG Documentation [Electronic resource]. URL: https://nag.wiki / (date of request: 10.12.2024)
5. Knowledge base of the RED OS [Electronic resource]. URL: https://redos.red-soft.ru/base / (date of request: 10.12.2024)
6. Astra knowledge base [Electronic resource]. URL: https://wiki.astralinux.ru/kb/alfavitnyj-ukazatel-190914856.html (date of application: 10.12.2024)

7. System Administration of Rosa "Chrome" OS / Mirzoyan A.V. [Electronic resource]. URL: https://stage.rosalinux.ru/media/2024/05/rosa_basics.pdf (date of application: 10.12.2024)
8. Interception and analysis of network traffic using Wireshark / Meshkova Elena Vladimirovna [Electronic resource]. URL: https://elibrary.ru/item.asp?id=27443875 (date of application: 10.12.2024)