Отчёт по лабораторной работе №5

Администрирование локальных сетей

Бансимба Клодели Дьегра, НПИбд-02-22

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Получить основные навыки по настройке VLAN на коммутаторах сети.

# 2 Выполнение лабораторной работы

Откроем проект с названием lab\_PT-04.pkt и сохраним под названием lab\_PT-05.pkt. После чего откроем его для дальнейшего редактирования (рис. fig. 1).



Рис. 1: Открытие проекта lab\_PT-05.pkt

Используя приведённую в лабораторной работе последовательность команд из примера по конфигурации Trunk-порта на интерфейсе g0/1 коммутатора mskdonskaya-sw-1, настроим Trunk-порты на соответствующих интерфейсах всех коммутаторов

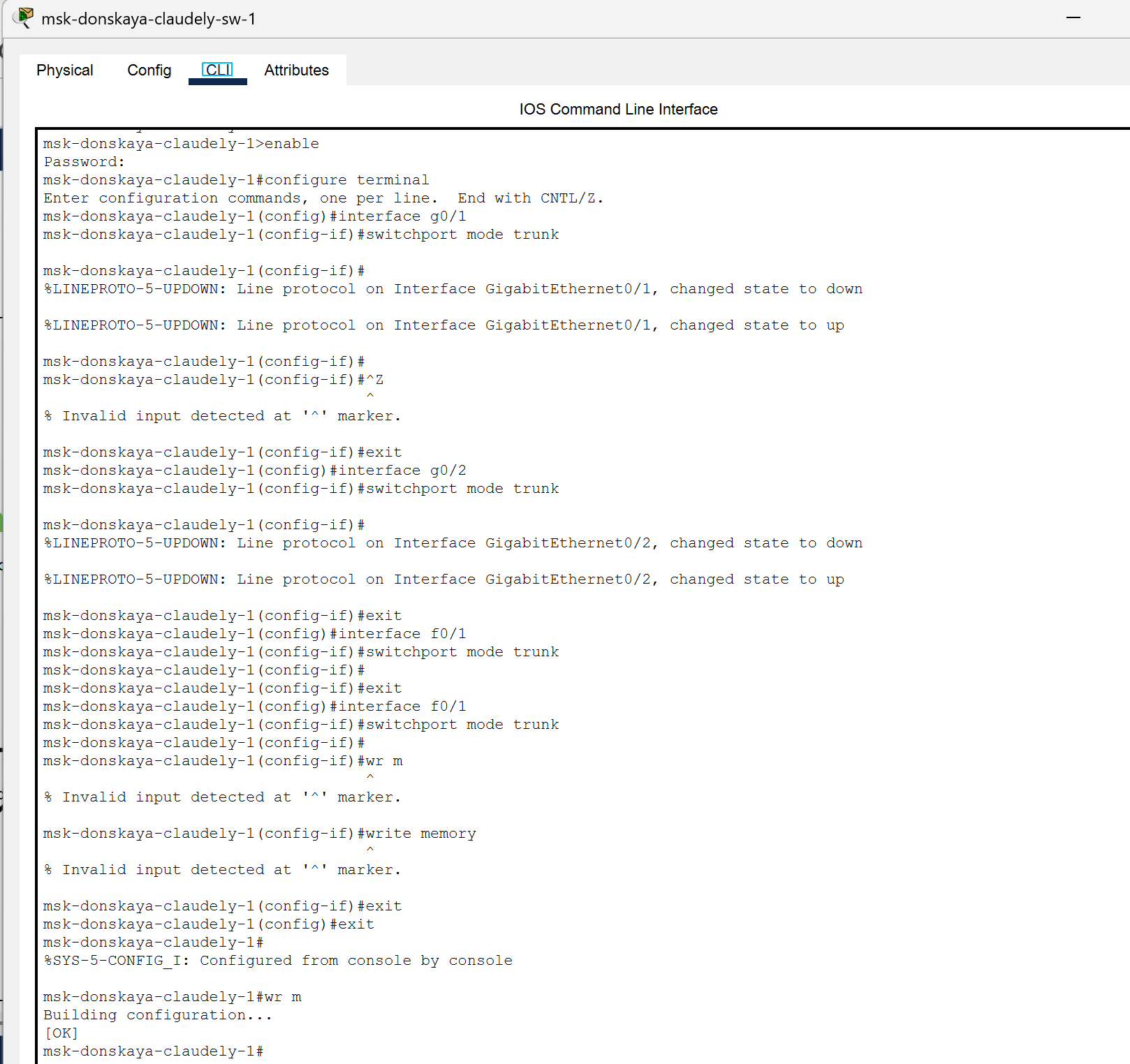


Рис. 2: Настройка Trunk-портов на коммутаторе msk-donskaya-claudely-sw-1.

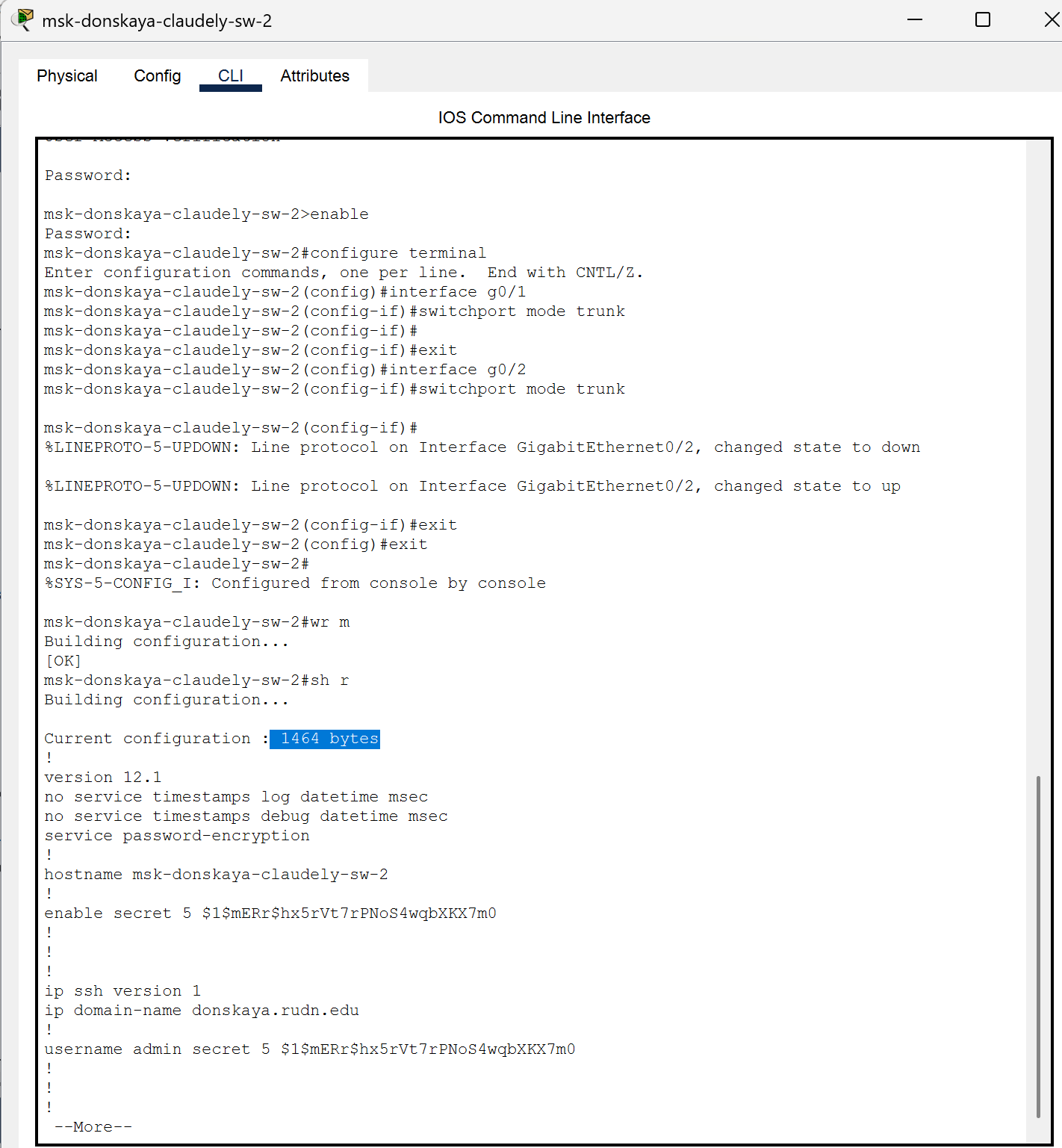


Рис. 3: Настройка Trunk-портов на коммутаторе msk-donskaya-claudely-sw-2.

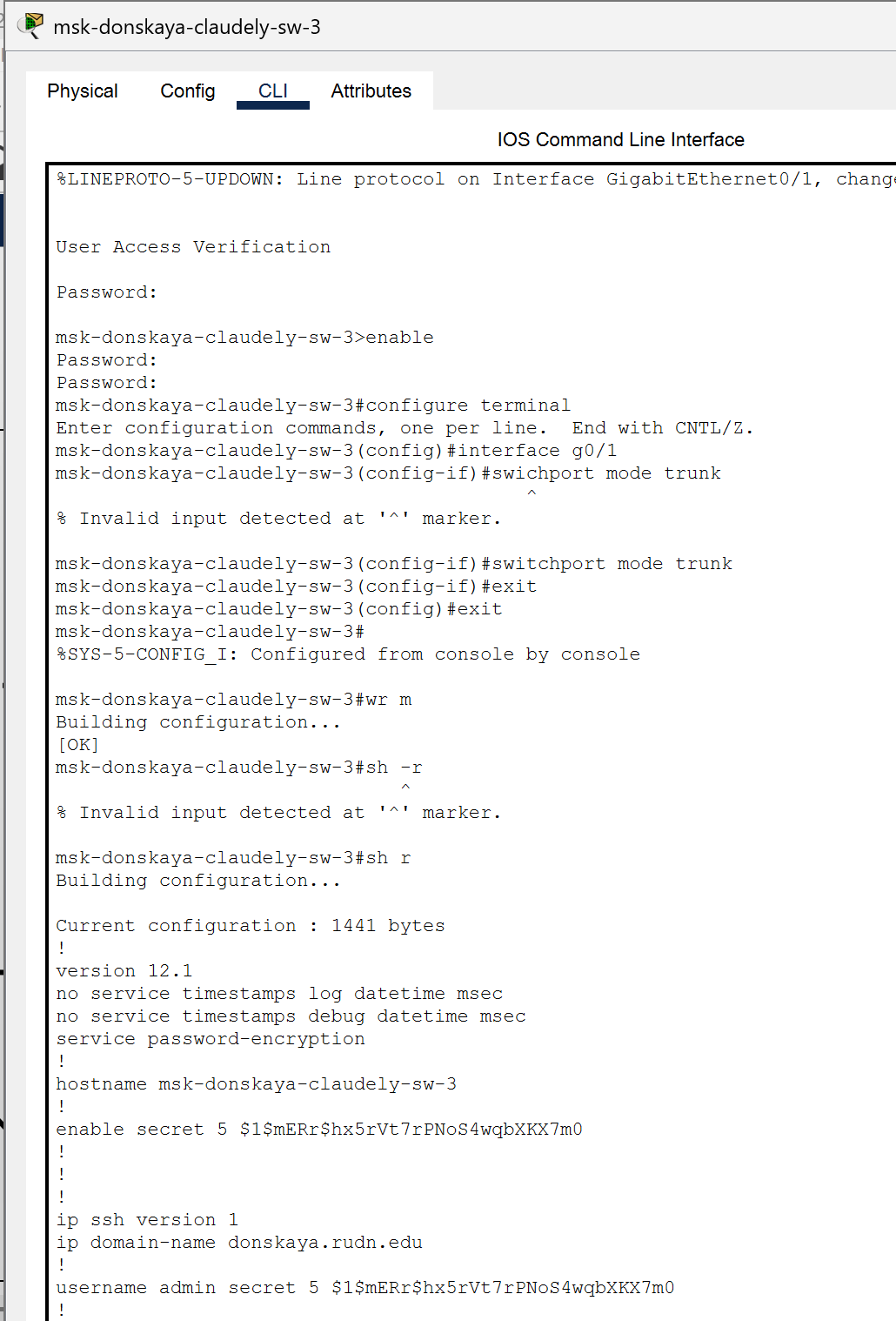


Рис. 4: Настройка Trunk-портов на коммутаторе msk-donskaya-claudely-sw-3.



Рис. 5: Настройка Trunk-портов на коммутаторе msk-donskaya-claudely-sw-4.



Рис. 6: Настройка Trunk-портов на коммутаторе msk-pavlovskaya-claudely-sw-1.

Далее настроим коммутатор msk-donskaya-claudely-sw-1 как VTP-сервер и пропишем на нём номера и названия VLAN (рис. fig. 7).

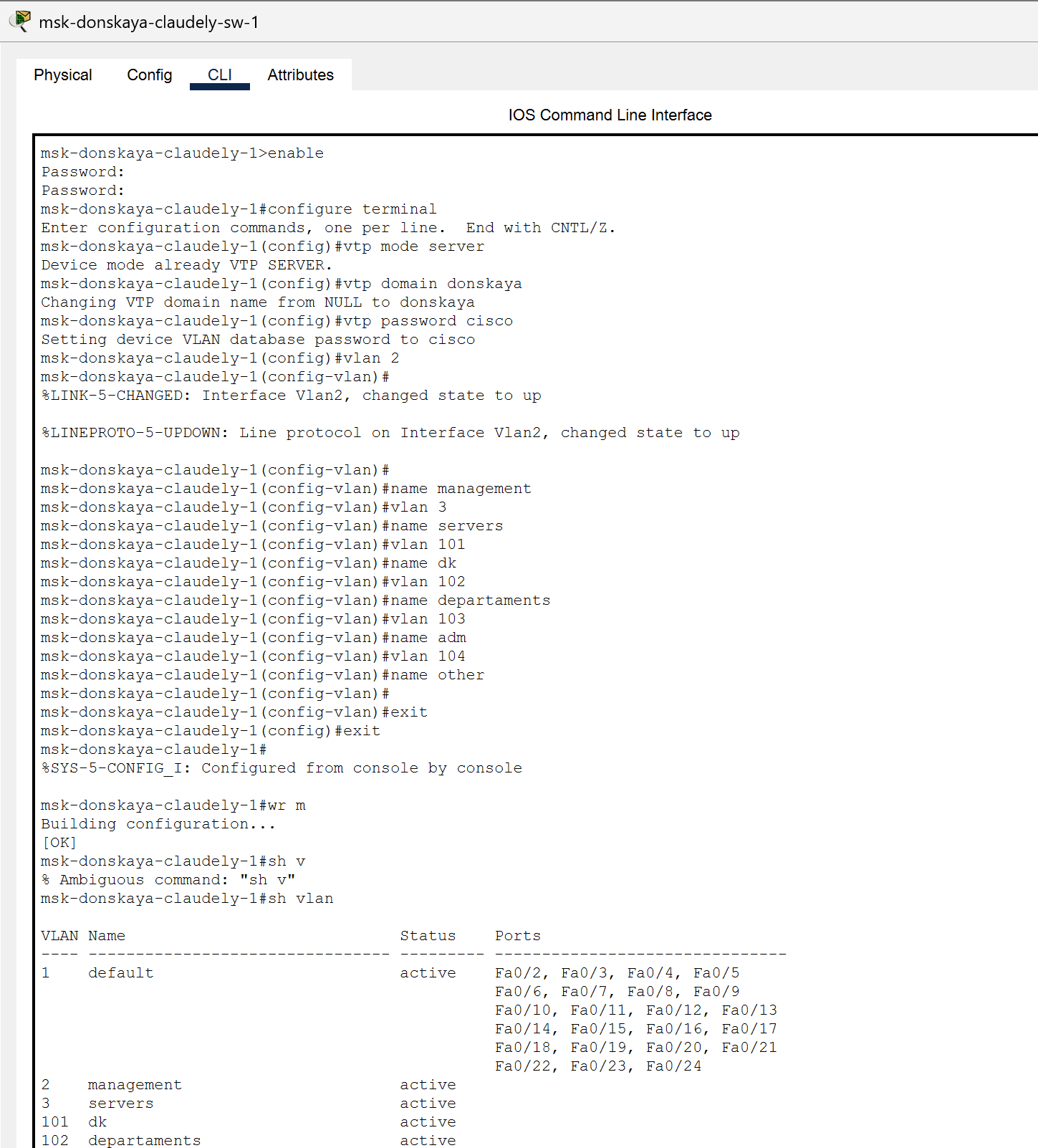


Рис. 7: Настройка коммутатора msk-donskaya-claudely-sw-1 как VTP-сервера, добавление номеров и названий VLAN.

Теперь настроим коммутаторы msk-donskaya-claudely-sw-2, msk-donskaya-claudely-sw-3, msk-donskaya-claudely-sw-4 и msk-pavlovskaya-claudely-sw-1 как VTP-клиенты и на интерфейсах укажем принадлежность к VLAN



Рис. 8: Настройка коммутатора msk-donskaya-claudely-sw-2 как VTP-клиента и указание принадлежности к VLAN.



Рис. 9: Настройка коммутатора msk-donskaya-claudely-sw-3 как VTP-клиента и указание принадлежности к VLAN.

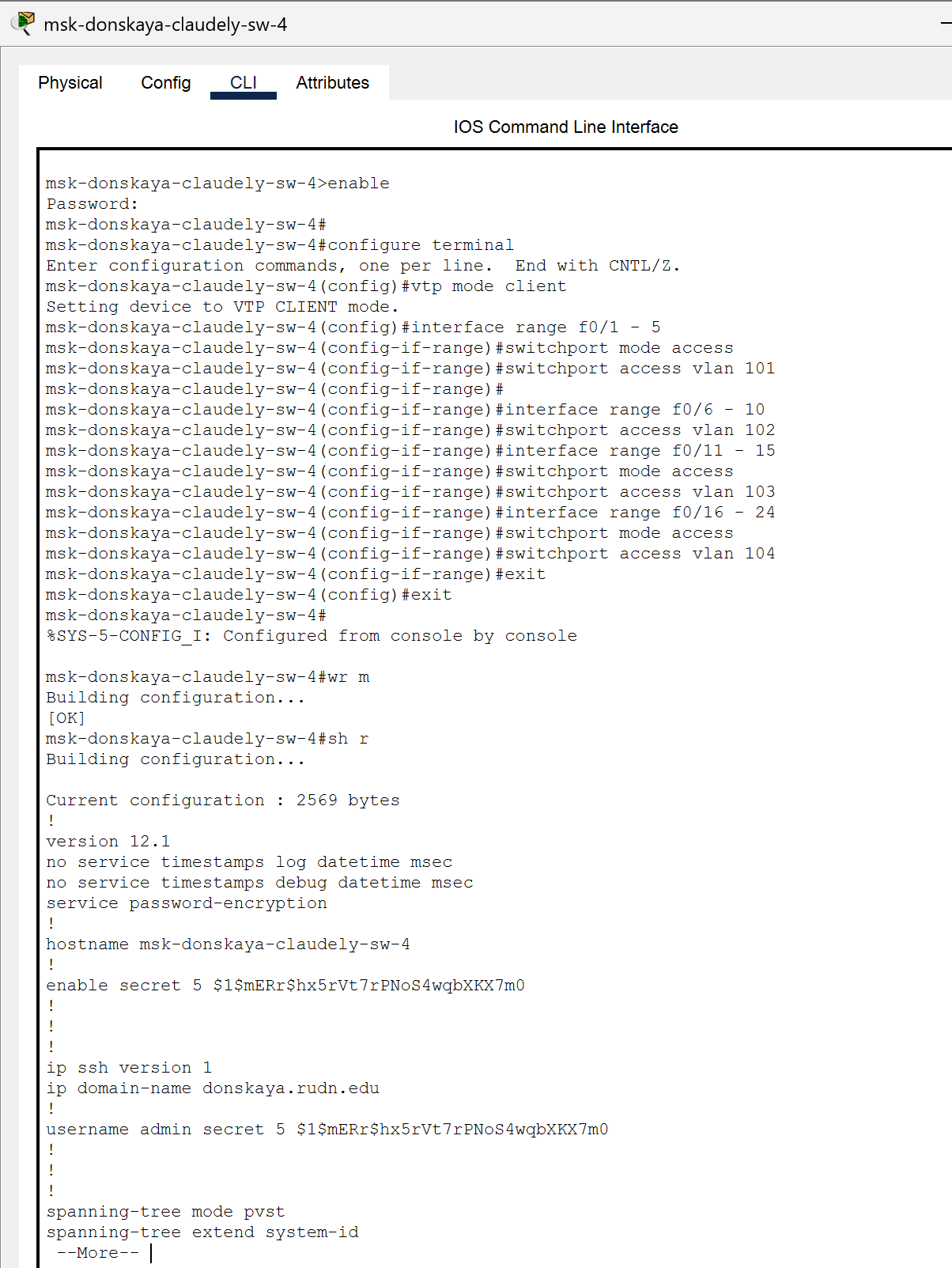


Рис. 10: Настройка коммутатора msk-donskaya-claudely-sw-4 как VTP-клиента и указание принадлежности к VLAN.



Рис. 11: Настройка коммутатора msk-pavlovskaya-claudely-sw-1 как VTP-клиента и указание принадлежности к VLAN.

Затем требуется указать статические IP-адреса на оконечных устройствах

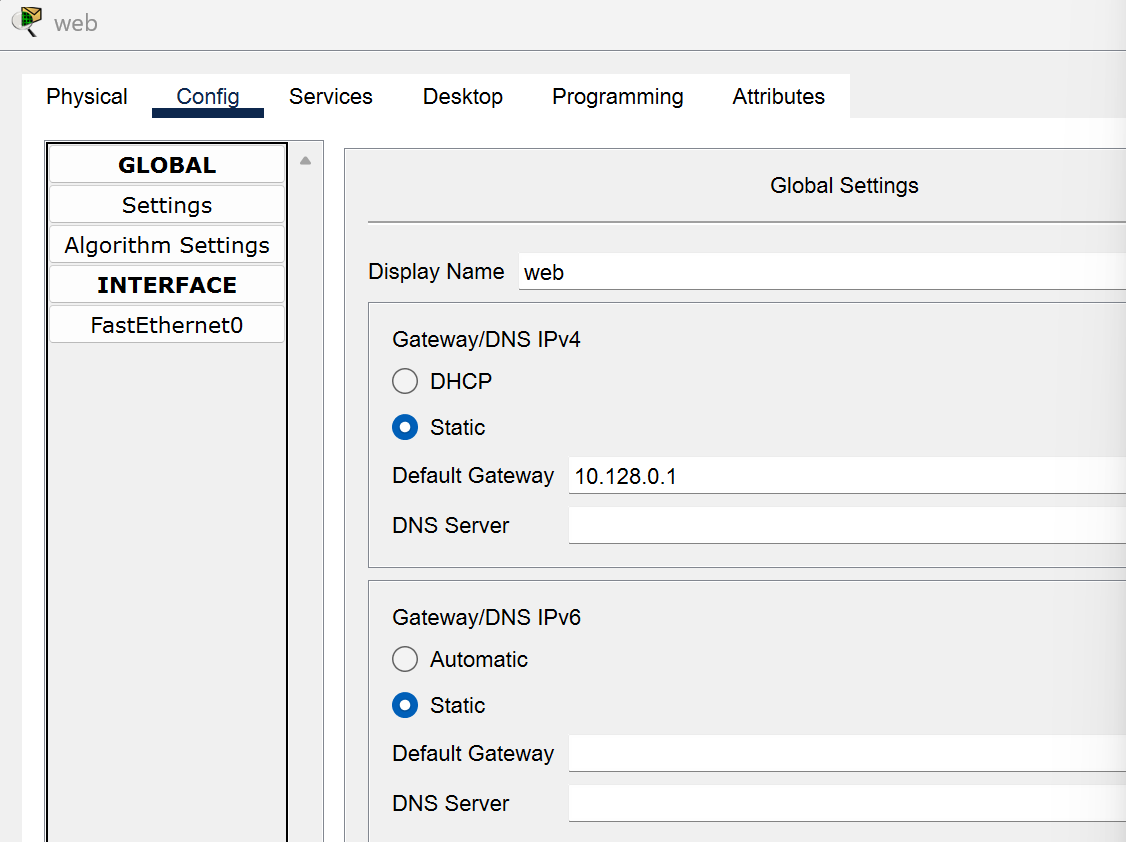


Рис. 12: Пример указания статического IP-адреса на оконечном устройстве (Default Gateway).

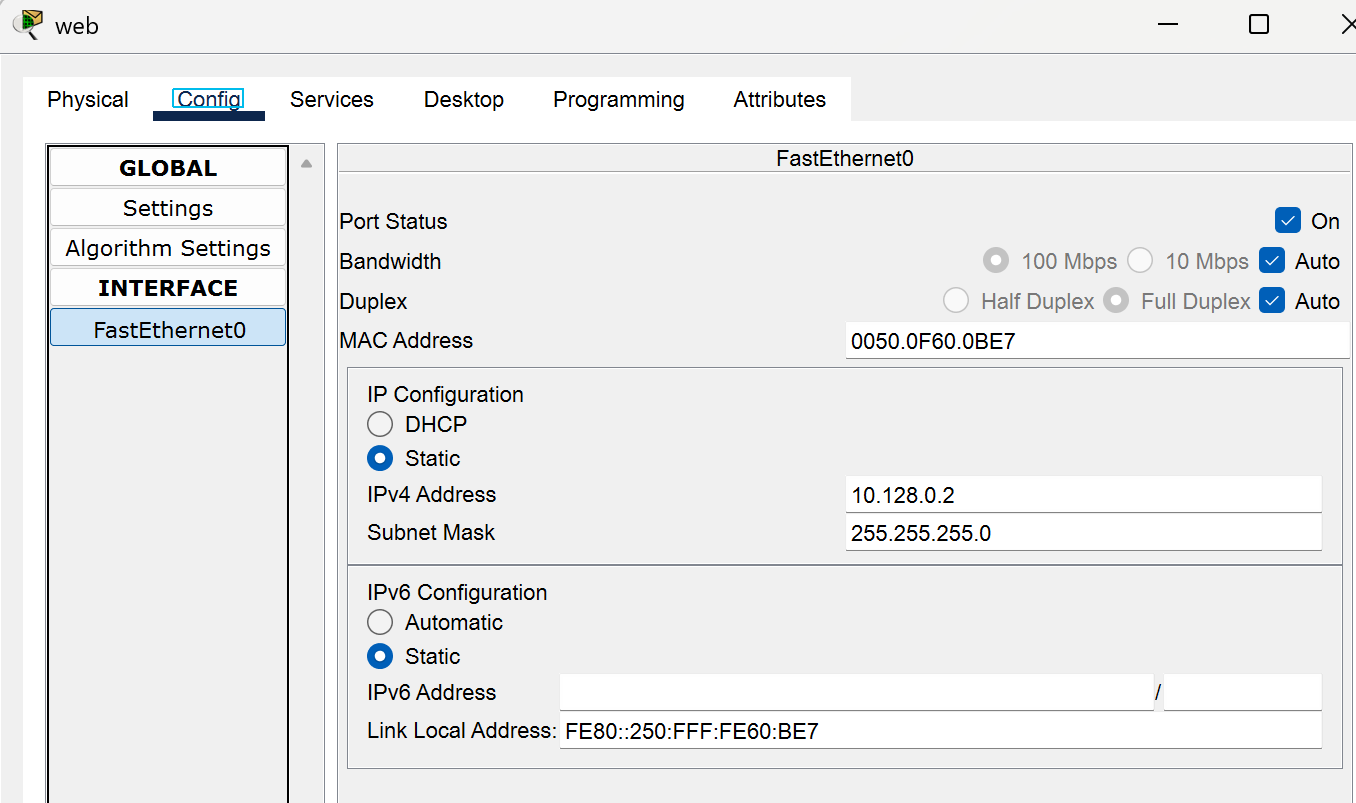


Рис. 13: Пример указания статического IP-адреса на оконечном устройстве (IP Configuration).

Используя режим симуляции в Packet Tracer, изучим процесс передвижения пакета ICMP по сети

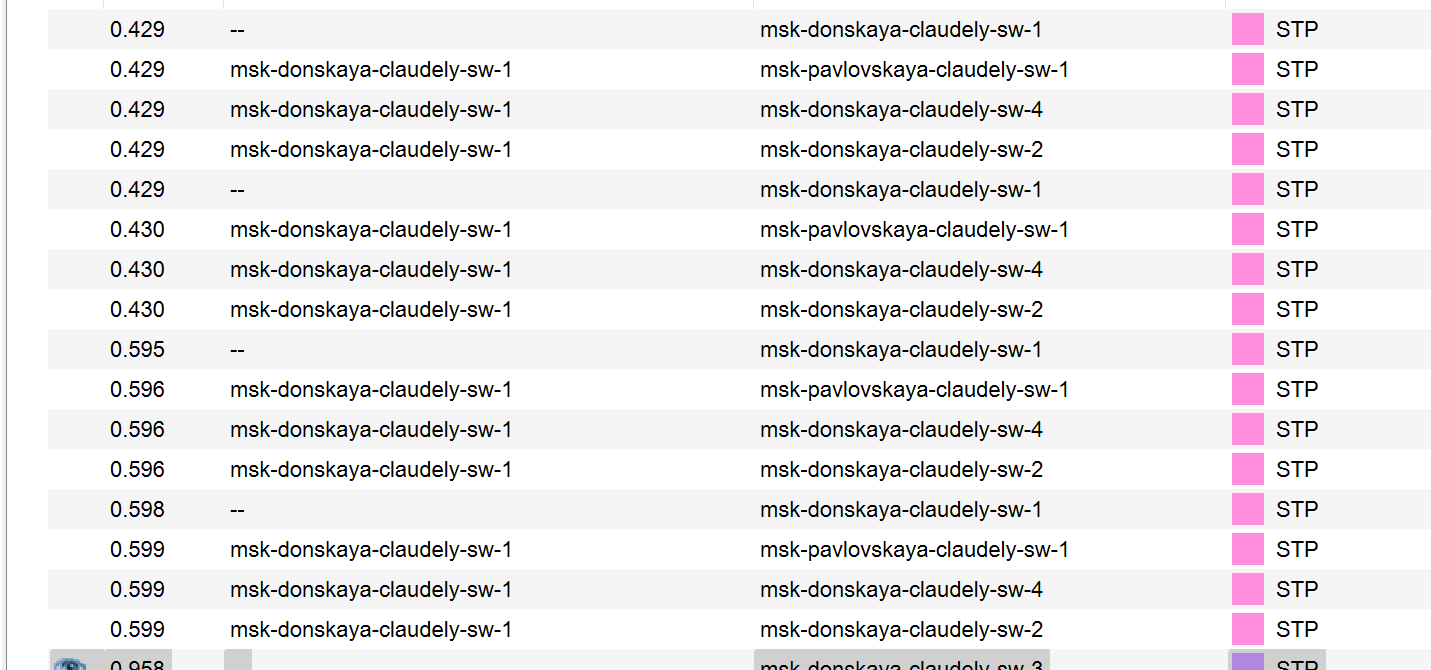


Рис. 14: Изучение процесса передвижения пакета ICMP по сети в режиме симуляции в Packet Tracer.

# 3 Выводы

В ходе выполнения лабораторной работы мы получили основные навыки по настройке VLAN на коммутаторах сети.

# 4 Ответы на контрольные вопросы:

1. Какая команда используется для просмотра списка VLAN на сетевом устройстве? - show vlan
2. Охарактеризуйте VLAN Trunking Protocol (VTP). Приведите перечень команд с пояснениями для настройки и просмотра информации о VLAN. – switchport mode trunk/access: switchport mode trunk: устанавливает порт в режим транка (trunk), который передает данные для нескольких VLAN через один физический интерфейс. switchport mode access: устанавливает порт в режим доступа (access), который предназначен для работы с одним определенным VLAN. switchport access vlan : назначает определенный VLAN для порта в режиме доступа. vtp mode server/client: vtp mode server: устанавливает коммутатор в режим сервера VTP, позволяя ему рассылать информацию о VLAN другим коммутаторам в сети. vtp mode client: устанавливает коммутатор в режим клиента VTP, что позволяет ему принимать информацию о VLAN от серверов VTP. vtp domain : устанавливает домен VTP, в котором находится коммутатор. Для синхронизации информации о VLAN, все коммутаторы в сети должны находиться в одном домене VTP с одинаковым именем. vtp password : устанавливает пароль VTP для доступа к домену VTP. Это помогает обеспечить безопасность и предотвратить несанкционированные изменения конфигурации VLAN. vlan : создает новый VLAN с указанным номером. name : присваивает имя VLAN, что делает его более понятным для администраторов сети.
3. Охарактеризуйте Internet Control Message Protocol (ICMP). Опишите формат пакета ICMP. – Это протокол в семействе протоколов интернета, который используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных в компьютерных сетях. ICMP также выполняет некоторые сервисные функции, такие как проверка доступности хостов и диагностика сетевых проблем. Формат пакета ICMP обычно состоит из заголовка и полезной нагрузки, которая может включать в себя различные поля, зависящие от типа сообщения ICMP. Основные поля заголовка ICMP включают в себя: Тип: определяет тип сообщения ICMP, например, сообщение об ошибках, запрос эхо и т. д. Код: подтип сообщения, который помогает уточнить тип сообщения. Например, для сообщения об ошибке этот код может указывать на конкретный тип ошибки. Контрольная сумма: используется для обеспечения целостности пакета ICMP. Дополнительные данные: в зависимости от типа и кода сообщения, может содержать дополнительные поля с информацией о сетевой проблеме или другой полезной информацией.
4. Охарактеризуйте Address Resolution Protocol (ARP). Опишите формат пакета ARP. - Это протокол, используемый в компьютерных сетях для связывания IP-адресов с физическими MAC-адресами устройств в локальной сети. Он позволяет устройствам в сети определять MAC-адреса других устройств на основе их IP-адресов. Когда устройству требуется отправить пакет данных другому устройству в сети, оно сначала проверяет свою локальную таблицу ARP, чтобы узнать MAC-адрес получателя. Если необходимый MAC-адрес отсутствует в таблице ARP, устройство отправляет ARP-запрос на всю сеть, запрашивая MAC-адрес соответствующего IP-адреса. Устройство, которое имеет этот IP-адрес, отвечает на запрос, предоставляя свой MAC-адрес. Формат пакета ARP обычно состоит из следующих полей: Тип аппаратного адреса: определяет тип физического аппаратного адреса в сети, такой как Ethernet (значение 1). Тип протокола: указывает на протокол сетевого уровня, для которого запрашивается соответствие адресов, обычно IPv4 (значение 0x0800). Длина аппаратного адреса: указывает на размер физического адреса, обычно 6 байт для MAC-адресов Ethernet. Длина адреса протокола: указывает на размер адреса протокола, обычно 4 байта для IPv4. Код операции: определяет тип операции ARP, например, запрос (значение 1) или ответ (значение 2). MAC-адрес отправителя: физический адрес отправителя. IP-адрес отправителя: IP-адрес отправителя. MAC-адрес получателя: физический адрес получателя (обычно пустой в ARP-запросах). IP-адрес получателя: IP-адрес получателя, для которого запрашивается соответствие MAC-адреса.
5. Что такое MAC-адрес? Какова его структура? - MAC-адрес (Media Access Control address) - Это уникальный идентификатор, присваиваемый каждому устройству или интерфейсу активного оборудования в компьютерных сетях Ethernet. Этот адрес используется для уникальной идентификации устройства в сети и обеспечения корректной передачи данных между устройствами. Структура MAC-адреса следующая: MAC-адрес состоит из 6 байт (или 48 бит). Каждый байт разбивается на две части: Префикс: это первые три байта (24 бита) MAC-адреса. Префикс обычно определяет производителя устройства (Organizationally Unique Identifier, OUI). Это уникальный идентификатор, выданный Институтом инженеров электротехники и электроники (IEEE) производителям сетевого оборудования. Идентификатор устройства: это оставшиеся три байта (24 бита) MAC-адреса. Идентификатор устройства является уникальным номером, присвоенным самим производителем идентификатора. MAC-адрес записывается в шестнадцатеричной системе счисления и обычно разделяется двоеточием или дефисом между каждыми двумя байтами (например, 01:23:45:67:89:ab). Использование уникальных MAC-адресов позволяет коммутирующим устройствам в сети Ethernet правильно маршрутизировать кадры данных и устанавливать точные соединения между устройствами в сети.

# Список литературы