МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

ФАКУЛЬТЕТ ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Кафедра «Аппаратное и программное обеспечение систем управления в телекоммуникации»

Р.П.Абдурахмонов, Б.У.Акмурадов, Х.Х.Ахмедова

МЕТОДИЧЕСКОЕ ПОСОБИЕ
по выполнению лабораторных работ по предмету

УПРАВЛЕНИЕ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

ЧАСТЬ 1

Ташкент 2023

Авторы: Р.П.Абдурахмонов, У.М.Абдуллаев, Х.Х.Ахмедова

Методическое пособие по выполнению лабораторных работ по предмету " Управление телекоммуникационными сетями " часть 1. -Ташкент: ТУИТ. 2023. - 116 стр.

В методическом пособии представлены указания по знакомству со средой построения виртуальных компьютерных сетей и объединения локальной компьютерной сети на базе коммутаторов, настройка протоколов Telnet, GVRP, STP/RSTP, создание и настройка VLAN, объединение локальных вычислительных сетей на базе маршрутизаторов и с использованием статической маршрутизации. Оно включает в себя название лабораторной работы, цель работы, теоретическую часть, задание, порядок выполнения работы и контрольные вопросы.

Методическое пособие предназначено для бакалавров направления 5350100 – Телекоммуникационные технологии ("Телекоммуникации") для применения в учебном процессе.

Решением научно-методического совета Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий методическое пособие рекомендуется для публикации. ("___" - протоколом "___" _____ 2023 год).

Ташкентский университет информационных технологий имени Мухаммада Ал-Хоразмий, 2023

ВВЕДЕНИЕ

Развитие информационно-коммуникационных услуг, наряду с эффективным управлением информационными ресурсами, требует таких решений, как расширение функциональных возможностей сети связи. В свою очередь, внедрение и развитие новых технологий в сфере телекоммуникаций требует от операторов связи обеспечения качества услуг, установления взаимодействия между протоколами, обеспечения надежного транспорта, определения набора услуг, что указывает на наличие некоторых проблем. Это основная причина увеличения потребности в информационных ресурсах в условиях современного бурного развития телекоммуникаций. В то же время возросла потребность пользователей в получении необходимой им информации качественным, надежным, быстрым и удобным в использовании способом. В таких условиях большое значение приобретают системы и технологии управления сетями и услугами, а их протокол, алгоритм и реализация являются важной частью современных сетей и требуют изучения аспектов управления.

Huawei, глобальный поставщик ИКТ-решений, разработал открытую платформу моделирования корпоративных сетей (eNSP). Платформа представляет собой симулятор реальных сетевых устройств и дает представление о линейке продуктов Huawei для передачи данных. Сетевой симулятор помогает пользователям понять возможности новых технологий и сетей в виртуальной среде, получая четкое представление о поведении и производительности топологии при обновлении или масштабировании устройств, протоколов, каналов связи и приложений.

Данное методическое пособие служит подробным справочно-методическим обеспечением для выполнения лабораторных работ по предмету «Управление телекоммуникационными сетями ».

Лабораторная работа №1.

Знакомство со средой построения виртуальных компьютерных сетей и объединения локальной компьютерной сети на базе коммутаторов.

Цель работы: Познакомиться со средой построения виртуальных компьютерных сетей, изучить ее возможности, научиться интегрировать локальную компьютерную сеть на базе коммутаторов и производить в них первоначальные настройки.

Теоретическая часть

На сегодняшний день существует множество платформ сетевого моделирования: Одной из них является Enterprise Network Simulation Platform (eNSP), бесплатный графический симулятор сети, разработанный Huawei. Эта платформа позволяет специалистам в области ИКТ и клиентам ближе познакомиться с коммуникационными продуктами Huawei, понять работу и настройку маршрутизаторов и коммутаторов Huawei для передачи данных, а также смоделировать реальные сетевые устройства, такие как маршрутизаторы и коммутаторы, чтобы помочь им освоить методы устранения неполадок.

Платформа также помогает специалистам в области ИКТ и клиентам приобретать и улучшать свои навыки планирования, создания, эксплуатации и обслуживания сетей ИКТ для предприятий, тем самым помогая предприятиям создавать более совершенные сети с более высокой эффективностью.

VRP (Versatile Routing Platform) Huawei, являющаяся результатом многолетних исследований и опыта применения Huawei в области сетей, включает в себя запатентованную интеллектуальную собственность Huawei и способна поддерживать многие сетевые системы Huawei. Он имеет мощный

механизм IP-транспорта в качестве ядра и идеальную интеграцию различных технологий сетевых приложений с помощью технологии ОС в реальном времени, технологии управления устройствами и сетью, а также передового дизайна архитектуры. Как расширяемая платформа, способная к стабильной эволюции с открытыми интерфейсами, она поддерживает большое количество протоколов и функций с большой гибкостью. С помощью этой платформы вы можете построить идеальную безопасную сеть с высокой производительностью, превосходным интеллектом и простым управлением.

Особенности симулятора eNSP:

- Имитирует многие функции и возможности маршрутизаторов Huawei AR и коммутаторов серии x7;

- моделирует компьютеры, концентраторы, облачные устройства и коммутаторы;

- Имитирует функции конфигурации устройства для изучения команд устройства Huawei;

- моделирует крупномасштабное построение сети;

- использует настоящие сетевые карты для подключения к реальным сетевым устройствам;

- имитирует запись пакетов на интерфейс для визуального воспроизведения процесса взаимодействия с протоколом;

- графический пользовательский интерфейс;

- Операционная система VRP (универсальная платформа маршрутизации).

Платформа eNSP — это бесплатное программное обеспечение с открытым исходным кодом для общего пользования. Эту платформу могут использовать пользователи с разным уровнем подготовки.

Сетевой концентратор (английское название «концентратор») — это устройство, предназначенное для соединения компьютеров в сетях Ethernet. Сетевой концентратор работает на физическом (первом) уровне сетевой модели OSI, передавая сигнал с одного порта на все остальные

(подключенные) порты. В настоящее время это устройство заменено сетевыми коммутаторами.

Сетевой коммутатор (англ. switch) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне сетевой модели OSI. Коммутаторы разработаны с использованием мостовых технологий и часто называются многопортовыми мостами.

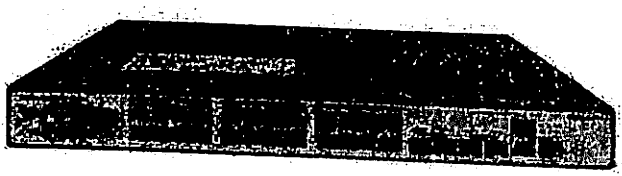

Рис. 1.1 Устройство коммутатора

Принцип работы коммутатора

Коммутатор хранит таблицу коммутации в памяти (называемой ассоциативной памятью), которая указывает, какой узел соответствует порту. Эта таблица пуста, когда коммутатор запущен и работает в режиме обучения. В этом режиме входящие данные на любой порт перенаправляются на все остальные порты коммутатора. В этом случае коммутатор анализирует фрейм и определяет MAC-адрес хоста-отправителя (FF:FF:FF:FF:FF:FF) и заносит его в таблицу в ближайшее время. Затем, если один из портов коммутатора получает кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр пересылается только через порт, указанный в таблице. Со временем коммутатор создает таблицу для всех активных MAC-адресов, что приводит к локализации трафика. В отличие от концентратора коммутатор передает данные непосредственно на приемник. Это повышает производительность и безопасность сети, устраняя необходимость (и возможность) для остальной части сети обрабатывать

данные, которые не предназначены для остальной части сети. Коммутаторы позволяют отправлять пакеты между несколькими сегментами сети.

Режимы коммутации

Существует три способа переключения. Каждый из них представляет собой комбинацию таких параметров, как задержка и надежность передачи.

1. Коммутация с хранением и передачей (Store and Forward). Коммутатор считывает все данные из фрейма (копирует в память коммутатора), проверяет их на наличие ошибок (Cyclic Redundancy Check (CRC)) (при обнаружении ошибок фрейм Ethernet отбрасывается), если ошибок не обнаружено, выбирает порт коммутатора, а затем получает и отправляет кадр в пункт назначения.

2. Промежуточная (сквозная) коммутация. Коммутатор считывает только адрес назначения в кадре и выполняет переключение. В этом случае коммутатор пересылает пакеты или фреймы адресату сразу после обработки адреса получателя, не дожидаясь получения всех данных. Этот режим уменьшает задержки передачи, но не имеет метода обнаружения ошибок.

3. Безфрагментная (бесперебойная коммутация) коммутация. Этот режим является модификацией промежуточного режима переключения. Передача осуществляется после фильтрации фрагментов коллизии (64-байтовый кадр обрабатывается по технологии store-and-forward, остальная часть обрабатывается по технологии промежуточной коммутации).

Задержка, «Решение о коммутации», добавляется ко времени, которое требуется кадру для входа и выхода из порта коммутатора, и вместе с ним определяет общую задержку коммутатора.

Симметричная и асимметричная коммутация

Симметричная коммутация обеспечивает коммутируемые соединения между портами с одинаковой пропускной способностью, например, если все порты имеют пропускную способность 10 Мбит/с или 100 Мбит/с.

Асимметричная коммутация обеспечивает коммутируемые соединения между портами с разной пропускной способностью, например, 10 Мбит/с или комбинацией портов с пропускной способностью 100 Мбит/с и 1000 Мбит/с.

Асимметричная коммутация позволяет серверу выделять порту коммутации большую пропускную способность, чтобы избежать перегрузки. Это обеспечивает плавный поток трафика при одновременном подключении нескольких клиентов к серверу. Буферизация памяти требуется при асимметричном переключении. Чтобы коммутатор мог работать с разными скоростями передачи данных на разных портах, целые кадры хранятся в буфере памяти и перемещаются по одному порту за раз по мере необходимости.

Буферизация памяти

Коммутатор может использовать буферизацию для временного хранения кадров, а затем отправлять их в нужное место назначения. Буферизацию можно использовать, даже когда принимающий порт занят. Буфер — это область памяти, в которой коммутатор хранит данные для передачи.

Буфер памяти может использовать два метода хранения и отправки кадров: буферизация портов и буферизация разделяемой памяти.

При буферизации портов пакеты сохраняются в очередях, связанных с отдельными входными портами. Пакет перенаправляется на выходной порт только после успешной передачи всех последующих кадров. В этом случае один кадр может задержать всю очередь, потому что его принимающий порт занят.

При буферизации с общей памятью все кадры сохраняются в буфере с общей памятью, который используется всеми портами коммутатора. Объем памяти, выделенной порту, определяется его требуемым объемом. Этот метод называется динамическим выделением буфера памяти. После этого кадры в буфере памяти динамически распределяются по выходным портам. Это позволяет вам получать кадр на один порт и отправлять его на другой

порт без очереди. Коммутатор поддерживает (хранит) карту портов, на которые следует отправлять кадры. Эта карта очищается только после успешной отправки кадра. Поскольку буферная память является общей, размер кадра ограничен размером всего буфера, а не его частью, выделенной конкретному порту. Это означает, что большие кадры могут передаваться с меньшими потерями, что особенно важно при асимметричной коммутации, когда порт с пропускной способностью 100 Мбит/с должен отправлять пакеты на порт с пропускной способностью 10 Мбит/с.

Особенности и виды коммутаторов

Коммутаторы делятся на управляемые и неуправляемые (наиболее простые) типы. Более сложные коммутаторы позволяют управлять коммутацией на сетевом (третьем) уровне модели OSI. Их обычно называют «Коммутатор уровня 3» или «Коммутатор L3». Коммутатором можно управлять через веб-интерфейс, интерфейс командной строки (CLI), протокол SNMP, RMON и т. д. Многие управляемые коммутаторы позволяют настроить дополнительные функции: VLAN, QoS, агрегацию, зеркалирование и т.д.

Ниже приведены основные команды для настройки начальной конфигурации коммутатора:

- [Quidway] display current-configuration//просмотр конфигурации коммутатора;

- [Quidway] отображать интерфейсы // видеть состояние интерфейса и основные рабочие параметры;

- [Quidway] display interfaces // просмотреть информацию о вланах;

- [Quidway] display version//просмотр версии прошивки коммутатора;

- [Quidway] display patch // Просмотр версии патча DT;

- [Quidway] super password // установить пароль для изменения привилегий пользователя;

- [Quidway] sysname // установить имя коммутатора (системы);

- [Quidway] interface ethernet 0/0/1 // переход в меню настроек интерфейса (просмотр интерфейса);

- [Quidway] interface vlanif x // Переходим в меню настройки логического L3 интерфейса, связанного с vlan;

- [Quidway-Vlan-interfacex] ip address 10.65.1.1 255.255.0.0 // Установить IP-адрес VLAN, если логический интерфейс L3;

- [Quidway] ip route-static 0.0.0.0 0.0.0.0 10.65.1.2 // настраиваем статический маршрут, в примере - указан маршрут по умолчанию;

- [Quidway] user-interface vty 0 4 // настроить интерфейс виртуального терминала;

- [Quidway-ui-vty0-4] authentication-mode password // изменить тип аутентификации на пароль;

- [Quidway-ui-vty0-4] set authentication-mode password simple 222 // установить пароль;

- [Quidway-ui-vty0-4] user privilege level 3 // показать (отметить) уровень привилегий пользователя;

- [Quidway] interface ethernet 0/0/1 // входим в конфигурацию интерфейса;

- [Quidway-Ethernet0/1] duplex {half|full|auto} // устанавливаем режим работы порта;

- [Quidway-Ethernet0/1] speed {10|100|auto} // устанавливаем скорость порта;

- [Quidway-Ethernet0/1] flow-control // настроить управление потоком;

- [Quidway-Ethernet0/1] port link-type {trunk|access|hybrid} // устанавливаем режим работы vlan текущего порта;

- [Quidway-Ethernet0/1] port default vlan 3 // настройки порта в режиме обработки VLAN - доступ, default vid 3;

- [Quidway-Ethernet0/2] port trunk allow-pass vlan {ID|All} // установить список разрешенных вланов на транковом (транковом) порту;

- [Quidway-Ethernet0/3] port trunk pvid vlan 3 // устанавливаем PVID на основной (транковый) порт;

- [Quidway-Ethernet0/1] shutdown // физическое отключение порта;

- [Quidway-Ethernet0/1] undo shutdown // физически включить порт;

- [Quidway-Ethernet0/1] quit // вернуться в предыдущее меню.

Задание:

Студенты строят и настраивают сеть, используя параметры, перечисленные в таблице 1.1.

Таблица 1.1. Варианты задания

№	Задание
1.	Построить сеть, состоящую из 2 коммутаторов, 4 ПК. Настройте безопасность порта на LSW2 (3 ПК).
2.	Коммутатор LSW3 и LSW4, построить сеть из 5 ПК. Настройте безопасность портов на LSW4 (2 ПК).
3.	Коммутатор LSW3 и LSW2, построить сеть из 5 ПК. Настройте безопасность портов на LSW2 (2 ПК).
4.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте безопасность портов на LSW3 (2 ПК).
5.	LSW3 и LSW2 переключаются, строят сеть из 5 ПК. Настройте безопасность портов на LSW2 (2 ПК).
6.	Коммутатор LSW4 и LSW2, построить сеть из 6 ПК. Настройте безопасность портов на LSW2 (4 ПК).
7.	Коммутатор LSW5 и LSW2, построить сеть из 4-х ПК. Настройте безопасность портов на LSW2 (2 ПК).
8.	Коммутатор LSW1 и LSW2, построить сеть из 7 ПК. Настройте безопасность порта на LSW2 (3 ПК).
9.	Коммутатор LSW1 и LSW2, построить сеть из 5 ПК. Настройте безопасность порта на LSW2 (3 ПК).
10.	Коммутатор LSW1 и LSW2, построить сеть из 7 ПК. Настройте безопасность порта на LSW2 (5 ПК).
11.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте безопасность портов на коммутаторах LSW2 и LSW3.

12.	Коммутаторы LSW5 и LSW6, строят сеть, состоящую из 8 ПК. Настройте безопасность портов на LSW2 (6 ПК).
13.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте безопасность портов на LSW4 (2 ПК).
14.	Построить сеть, состоящую из 4 коммутаторов, 8 ПК. Настройте безопасность портов на LSW2 (6 ПК).
15.	Построить сеть, состоящую из 3 коммутаторов, 6 ПК. Настройте безопасность портов на LSW2 (6 ПК).
16.	Построить сеть, состоящую из 3 коммутаторов, 5 ПК. Настройте безопасность порта на LSW2 (3 ПК).
17.	Коммутатор LSW3 и LSW4, построить сеть из 5 ПК. Настройте безопасность портов на LSW3 (3 ПК).
18.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Настройте безопасность портов на LSW2 и LSW3 (4 ПК).
19.	Построить сеть, состоящую из 2 коммутаторов и 6 ПК. Настройте безопасность портов на LSW3 (3 ПК).
20.	Коммутатор LSW3 и LSW2, построить сеть из 6 ПК. Настройте безопасность порта на LSW2 (3 ПК).
21.	Коммутатор LSW4 и LSW2, построить сеть из 6 ПК. Настройте безопасность порта на LSW4 (3 ПК).
22.	Коммутатор LSW1 и LSW2, построить сеть из 4-х ПК. Настройте безопасность порта на LSW1 (2 ПК).
23.	Коммутатор LSW1 и LSW2, построить сеть из 5 ПК. Настройте безопасность порта на LSW2 (3 ПК).
24.	Коммутатор LSW1 и LSW2, построить сеть из 3-х ПК. Настройте безопасность портов на LSW2 (2 ПК).
25.	Коммутатор LSW1 и LSW2, построить сеть из 6 ПК. Настройте безопасность портов на LSW2 (2 ПК).
26.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте безопасность портов на коммутаторах LSW1 и LSW2.
27.	Коммутаторы LSW5 и LSW6, строят сеть, состоящую из 6 ПК. Настройте безопасность портов на LSW2 (4 ПК).
28.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Настройте безопасность портов на LSW3 (4 ПК).
29.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте безопасность портов на LSW3 (2 ПК).
30.	Построить сеть, состоящую из 3 коммутаторов и 8 ПК. Настройте безопасность портов на LSW3 (3 ПК).

В данной лабораторной работе решаются следующие задачи:

- установка симулятора eNSP и изучение его возможностей;
- настроить системные параметры устройства, такие как имя устройства, системное время и системный часовой пояс;
- конфигурация входных данных (header shell);
- поставить пароль на консольный порт;
- установка времени блокировки (idle-time-out);
- сохранять файлы конфигурации;
- Перезагрузите устройство с помощью VRP;
- Привязка MAC-адреса (port security).

Порядок работы

Сначала установим и запустим симулятор eNSP.

Шаг 1.

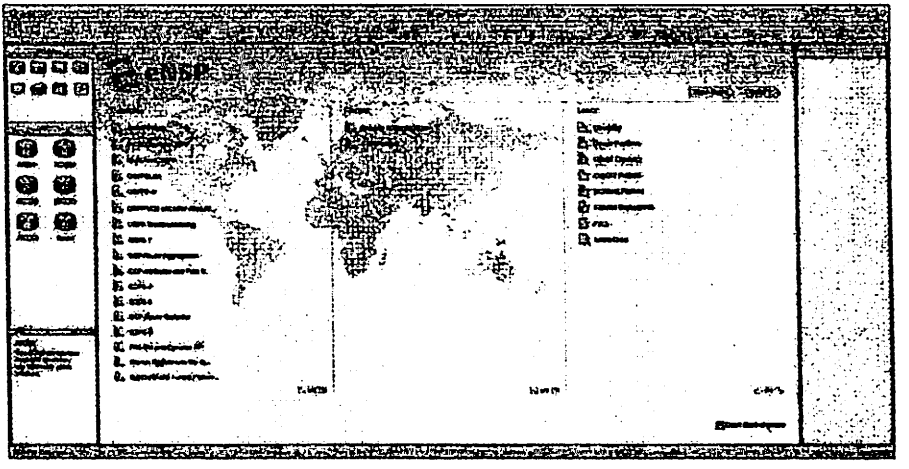

Рисунок 1.2. Окно симулятора eNSP

Типы устройств, доступные в симуляторе eNSP, перечислены ниже:

- маршрутизаторы (routers);
- коммутаторы (switches);

- устройства беспроводной локальной сети WLAN (Wireless Local Area Network);
- Устройство Firewall (FireWall);
- оконечные устройства (End Devices);
- Другие устройства (Other Devices);
- пользовательский тип устройства (Custom Device Type);
- соединения (Connections).

Шаг 2.

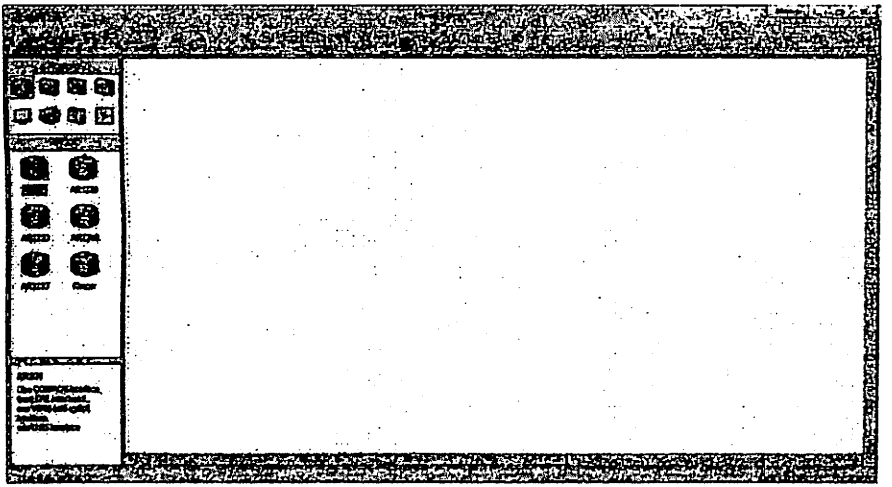

Рисунок 1.3. Окно «Устройства маршрутизатора»

Шаг 3.

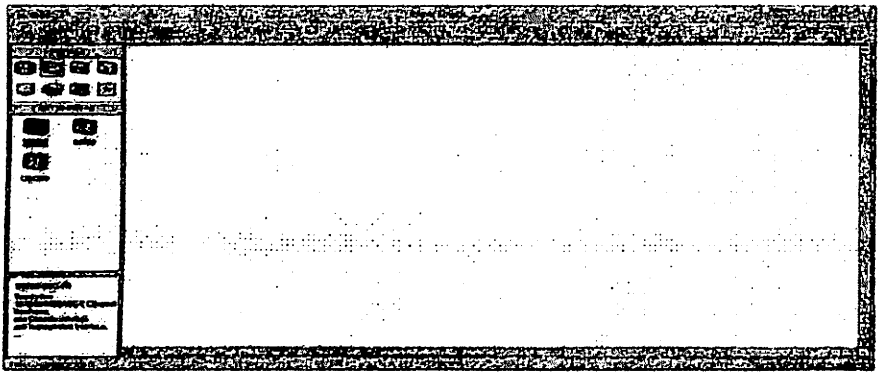

Рисунок 1.4. Окно «Устройства коммутатора»

Шаг 4.

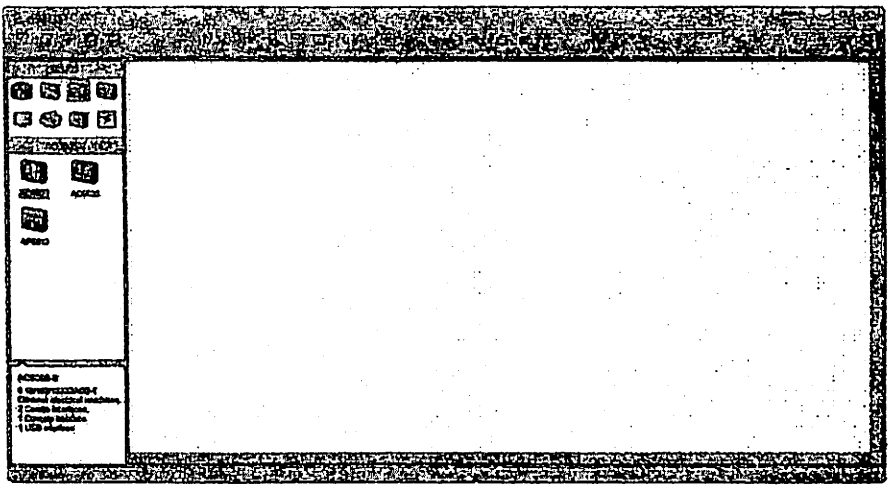

Рисунок 1.5. Окно «Устройства WLAN»

Шаг 5.

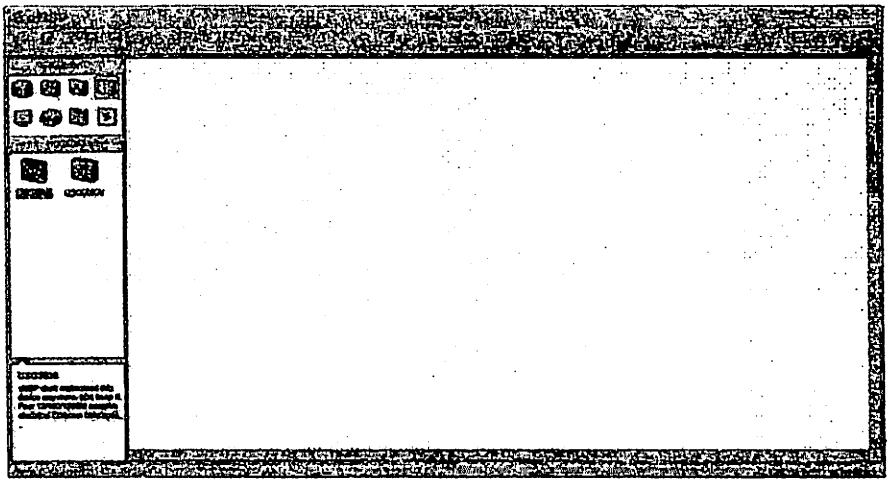

Рисунок 1.6. Окно «Устройства FireWall»

Шаг 6.

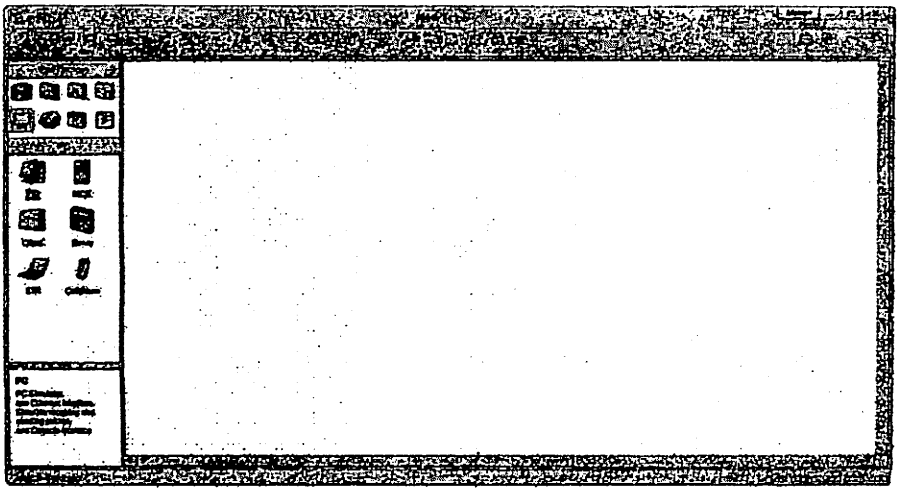

Рисунок 1.7. Окно «Оконечные устройства»

Шаг 7.

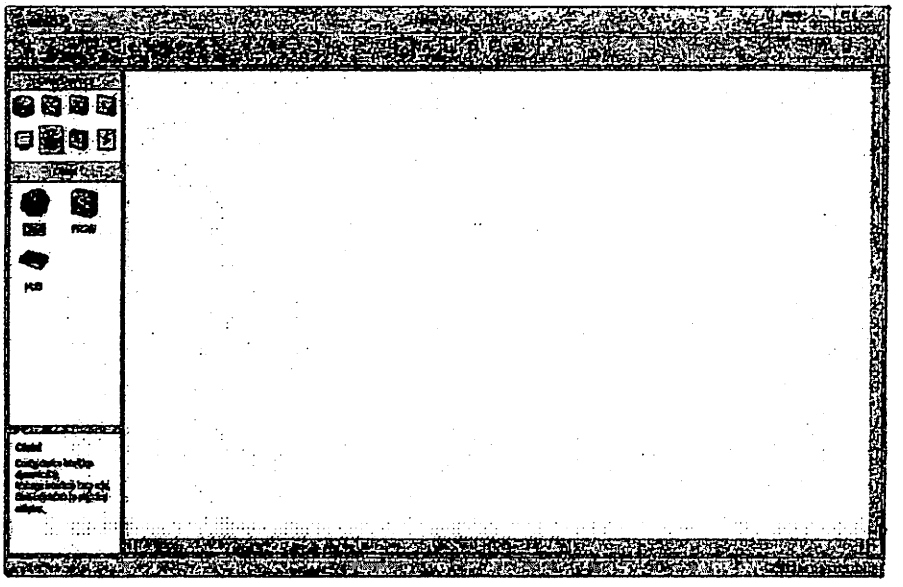

Рисунок 1.8 Окно «Другие устройства»

Шаг 8.

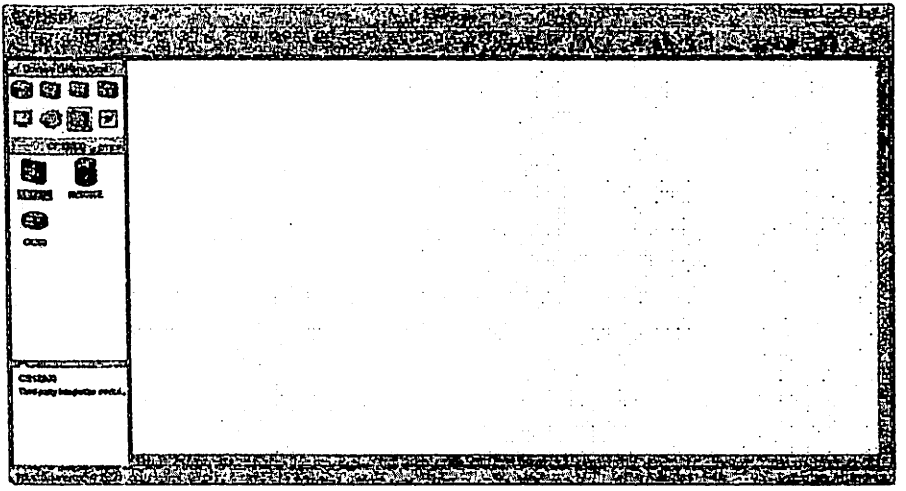

Рисунок 1.9. Окно «Пользовательский тип устройства»

Шаг 9.

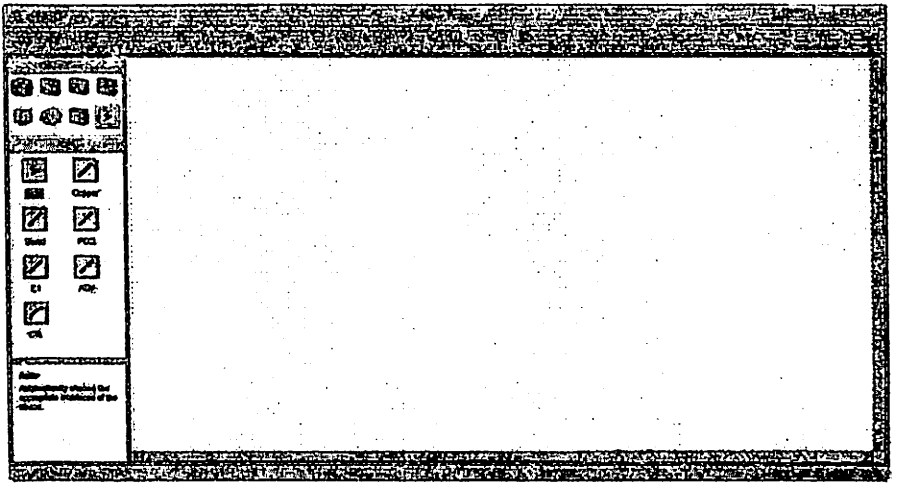

Рисунок 1.10. Окно «Соединения»

Например, рассмотрим подключение двух персональных компьютеров к одной сети:

Для этого в окне «оконечные устройства» выбираем 2 персональных компьютера и соединяем их на основе простой топологии одноранговой (peer-to-peer) сети. Для подключения используем кабель Ethernet.

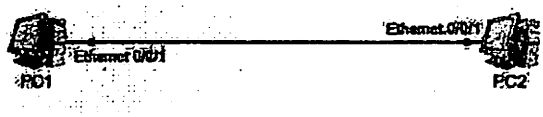

Рисунок 1.11. топология peer-to-peer сети

Затем запускаем два компьютера. После этого даем IP адреса. Назовем первый персональный компьютер и дадим ему IP-адрес.

Шаг 10.

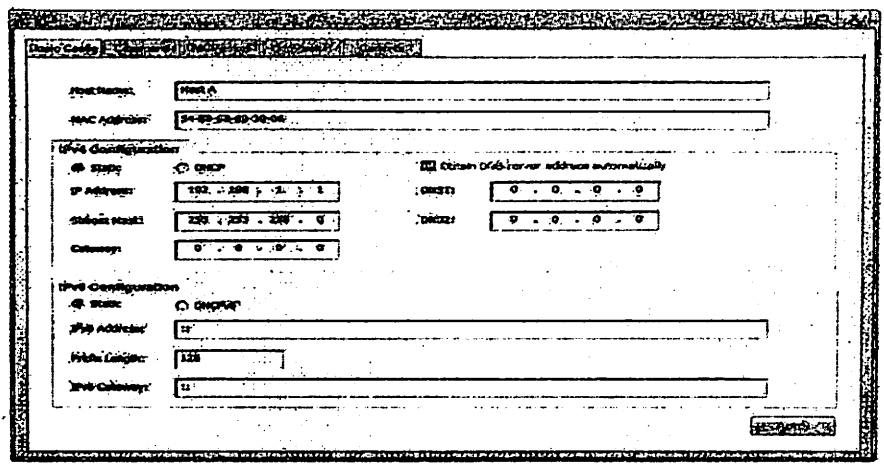

Рисунок 1.12. Даем PC1 имя, IP адрес и маску

После добавления IP-адреса нажмите кнопку «Применить», и он примет IP-адрес и место назначения, которые мы указали. Теперь давайте назовем второй компьютер и дадим ему IP-адрес (рис.1.13)

Шаг 11.

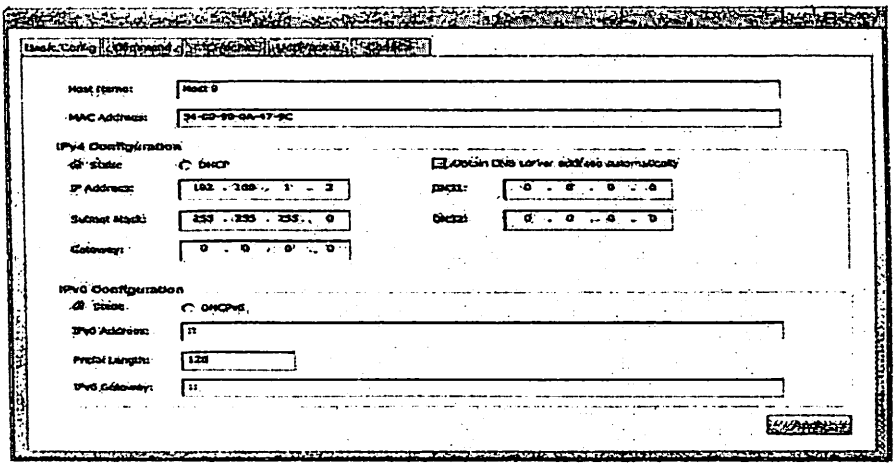

Рисунок 1.13. Даем PC2 имя, IP адрес и маску

Мы можем проверить, установлено ли соединение с помощью команды ping.

Шаг 12.

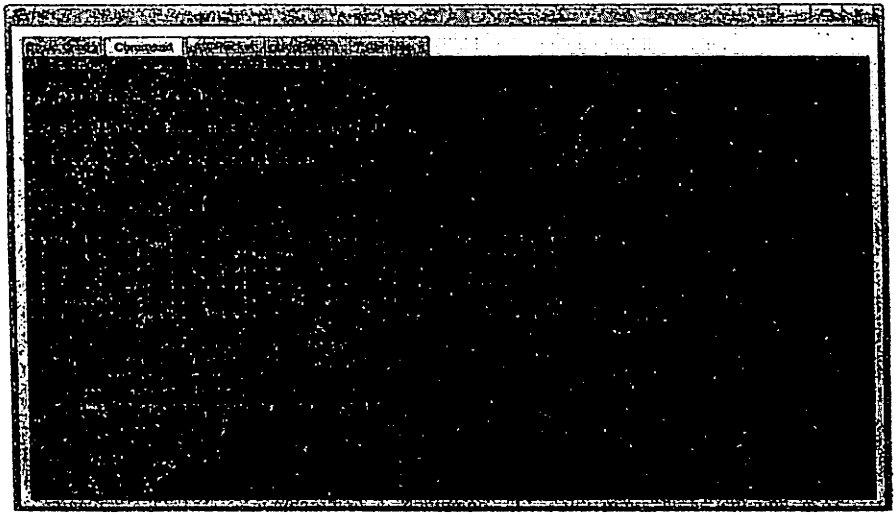

Рисунок 1.14 проверяем сетевое соединение с помощью команды ping

Теперь мы научимся интегрировать, настраивать и работать в сети на основе коммутаторов.

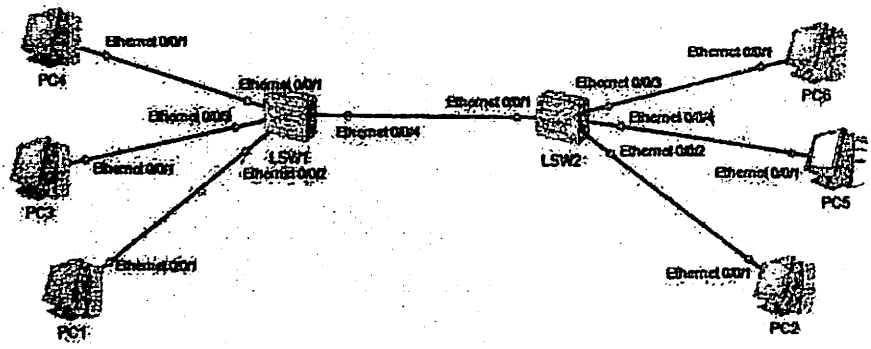

Рисунок 1.15. Исследуемая структура сети

Сначала запустим все устройства. Присвоим каждому персональному компьютеру IP-адрес:

Например: ПК1 — 192.168.1.1/255.255.255.0

Шаг 13.

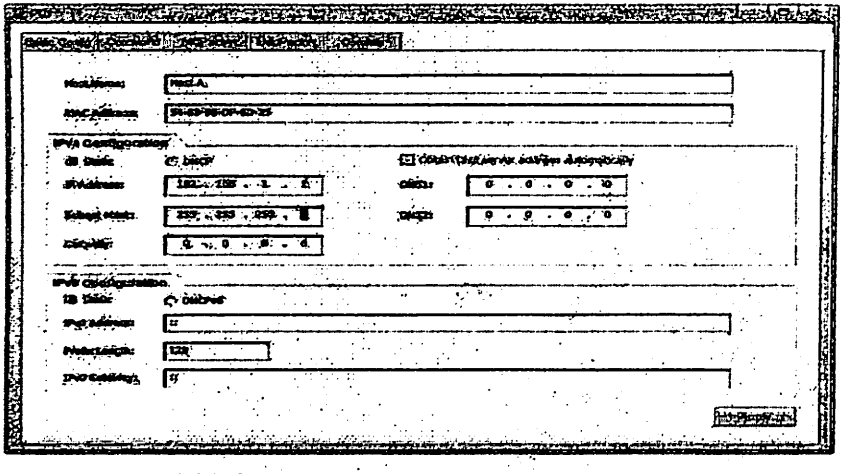

Рисунок 1.16. Окно назначения IP-адреса и маски персональному компьютеру (ПК1).

Всем остальным персональным компьютерам присваивается тот же IP-адрес и маска.

ПК2 — 192.168.1.2/255.255.255.0

ПК3 — 192.168.1.3/255.255.255.0

ПК4 — 192.168.1.4/255.255.255.0

ПК5 — 192.168.1.5/255.255.255.0

ПК6 — 192.168.1.6/255.255.255.0

Запускаем коммутационное устройство и делаем необходимые начальные настройки.

Шаг 14.

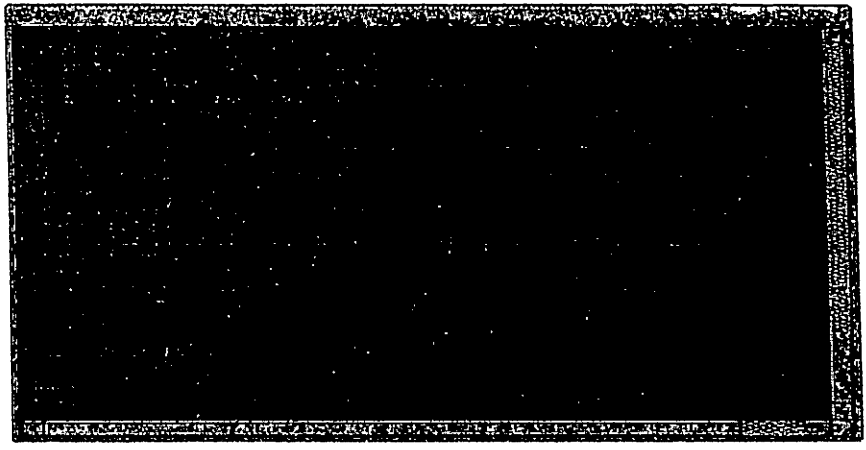

Рисунок 1.17. Переключить окно CLI устройства

Чтобы просмотреть информацию о версии системы, введите следующую команду:

<Huawei> display version

```
<Huawei>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (S3700 V200R001C00)
Copyright (c) 2000-2011 HUAWEI TECH CO., LTD

Quidway S3700-26C-HI Routing Switch uptime is 2 week, 30
day, 1 hour, 1 minute
```

Рисунок 1.18. Информация о версии системы

```
Directory of flash:/

  Idx  Attr      Size(Byte)  Date         Time        FileName
    0  drw-               -  Aug 06 2015 21:26:42    src
    1  drw-               -  Feb 02 2022 12:53:37
compatible

32,004 KB total (31,972 KB free)
```

Рисунок 1.24. Список сохраненных файлов

Управление файлами конфигурации устройства. Чтобы просмотреть сохраненные файлы конфигурации, введите следующую команду:

<LSW1>display saved-configuration

Если файл не сохранен, данные не выводятся. Чтобы сохранить текущую конфигурацию, введите следующую команду:

<LSW1>save

```
<LSW1>save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Info: Please input the file name ( *.cfg, *.zip )
[vrpcfg.zip]:
Jan 20 2022 13:20:41+08:00 LSW1 %%01CFM/4/SAVE(l)[2]:The
user chose Y when deciding whether to save the configuration
to the device.
Now saving the current configuration to the slot 0..
Save the configuration successfully.
<LSW1>
```

Рисунок 1.25. Результат сохранения файла

Если мы сохраним текущую конфигурацию с помощью команды «save», конфигурация будет сохранена на устройстве. Если мы хотим сохранить его во Flash-памяти, то используем следующую команду:

<LSW1>save huawei.cfg

Чтобы просмотреть сохраненную информацию о конфигурации, мы снова запускаем следующую команду:

<LSW1>display saved-configuration

Чтобы просмотреть текущую информацию о конфигурации, введите следующую команду:

<LSW1>display current-configuration

Чтобы удалить файлы конфигурации из флэш-памяти, введите следующую команду:

<LSW1>reset saved-configuration

Если мы хотим снова сохранить файл конфигурации во флэш-памяти, мы вводим указанную выше команду и «dir», чтобы увидеть файлы, сохраненные на текущем устройстве:

<LSW1>dir

Чтобы указать файл конфигурации для следующего запуска, мы вводим следующую команду:

<LSW1>startup saved-configuration huawei.cfg

Во время перезагрузки коммутатор автоматически загружает указанный файл конфигурации. Поэтому данные конфигурации не будут потеряны после перезагрузки.

Введите следующую команду, чтобы перезагрузить устройство:

<LSW1>reboot

Настройка функции привязки MAC-адреса.

MAC-адрес каждого устройства, подключенного к сети, используется для передачи данных по сети. Каждый сетевой адаптер имеет свой собственный 6-байтовый MAC-адрес. MAC-адрес (управление доступом к среде) записывается в виде 12 шестнадцатеричных цифр, разделенных на группы по две с помощью символа «-» или «:».

Например: 10:F1:0E:23:D0.

Вы можете настроить безопасность порта и установить максимальное количество безопасных MAC-адресов, которые интерфейс может узнать в сетях, требующих высокой безопасности доступа. Безопасность портов позволяет коммутатору превращать MAC-адреса, полученные через интерфейс, в безопасные MAC-адреса и прекращать изучение новых MAC-адресов при достижении максимального количества изученных MAC-адресов. После включения защиты портов коммутатор может обмениваться данными только с устройствами с определенными MAC-адресами. Если

интерфейс получает пакеты с исходным MAC-адресом, который не существует после того, как количество защищенных MAC-адресов достигает предела, коммутатор считает, что пакеты исходят от неавторизованного пользователя, и выполняет действие, настроенное для интерфейса. Это предотвращает доступ ненадежных пользователей к этим интерфейсам, повышая безопасность коммутатора и сети. В таблице ниже описаны действия по обеспечению безопасности порта.

Таблица 1.1 Режимы безопасности портов

Функция	Описание
Restrict(граница)	Отбрасывает пакеты с несуществующим MAC-адресом источника и создает ловушку. Это действие рекомендуется.
Protect (защита)	Отбрасывает пакеты, не имеющие MAC-адреса, но не перехватывает.
Shutdown (удаление)	Переводит интерфейс в состояние ошибки и создает ловушку. Обычно интерфейс в состоянии ошибки можно восстановить только с помощью команды перезапуска в представлении интерфейса.
Shutdown (удаление)	Чтобы разрешить сбойному интерфейсу автоматически подниматься вверх по истечении заданного времени, вам необходимо запустить в системном представлении команду auto-recovery call port-security-interval value. Значение интервала в этой команде указывает время, в течение которого интерфейс может автоматически переключиться в состояние Up.

Функция фиксированного MAC-адреса обычно используется в сетях, где пользователи редко меняются. Его можно прикрепить 2-мя разными способами.

[LSW1]interface Ethernet 0/0/4

[LSW1-Ethernet0/0/4]port-security enable

[LSW1-Ethernet0/0/4]port-security max-mac-num 2

[LSW1-Ethernet0/0/4]port-security mac-address sticky

[LSW1-Ethernet0/0/4]port-security protect-action shutdown

<LSW1>save

<LSW1>display interface brief

<LSW1>display mac-address

Результат настройки безопасности порта показан на рисунке 1.26.

Шаг 17.

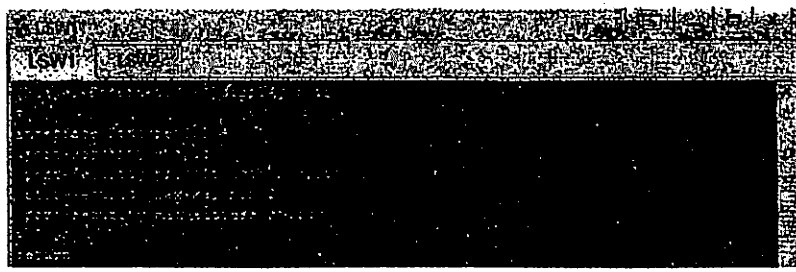

Рисунок 1.26. Проверьте настройку безопасности порта

Теперь давайте проверим безопасность порта. Для этого мы дадим компьютерам 192.168.1.0 (необязательно) сетевые IP-адреса (например, ПК1 будет использовать 192.168.1.1 маску 255.255.255.0, ПК5 будет использовать 192.168.1.5 маску 255.255.255.0). Для проверки работы отправляем пинги с 2-х произвольных ПК, пинги проходят, а MAC-таблица коммутатора запоминает MAC-адреса этих 2-х устройств. Если мы отправим пинг с третьего ПК, то сеть отключится (мы выбрали режим выключения). Сначала мы пингуем ПК 4 (IP-адрес 192.168.1.4/24) на ПК 6 (IP-адрес 192.168.1.6/24). Затем отправляем пинг с ПК 4 на ПК 5 (IP-адрес 192.168.1.5/24). Коммутационное устройство (таблица MAC-адресов) запоминает MAC-адреса этих двух устройств (ПК 6 и ПК 5). Это не позволяет другим устройствам обмениваться пакетами. Пропингуем ПК 4 до ПК 6.

Шаг 18.

Рисунок 1.27. Закрепите MAC-адрес устройства с помощью эхо-запроса

Отправим ping с ПК 4 на ПК 5

Шаг 19.

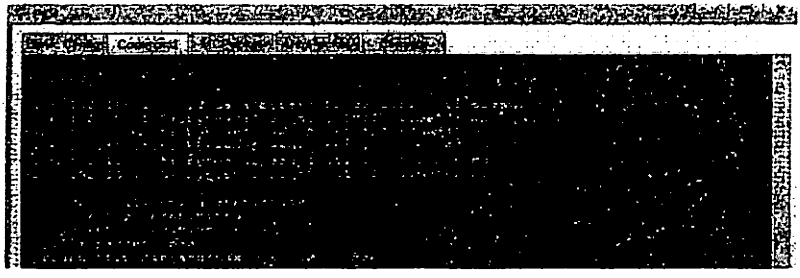

Рисунок 1.28. Закрепление MAC-адрес устройства с помощью Ping

Не удается отправить ping с ПК 4 на ПК 2, поскольку таблица MAC-адресов коммутатора помнит 2 MAC-адреса. Порт отключается т.к. режим shutdown включен.

Шаг 20.

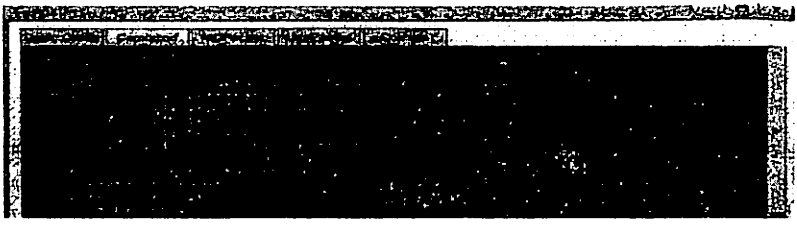

Рисунок 1.29. Не удалось закрепить MAC-адрес устройства с помощью ping

Чтобы проверить MAC-адреса, подключенные к порту Ethernet 0/0/4, мы используем команду «display mac-address sticky».

Шаг 21.

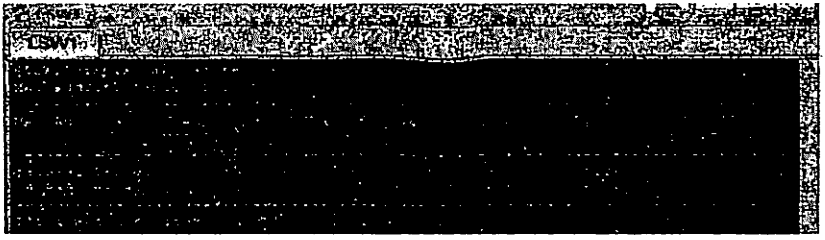

Рисунок 1.30. MAC-адреса, подключенные к порту Ethernet 0/0/4

Чтобы перезапустить сеть, вам нужно войти в интерфейс и ввести следующую команду.

[LSW1]interface Ethernet 0/0/4

[LSW1-Ethernet0/0/4]undo shutdown

Вы также можете вводить MAC-адреса статически. Для этого необходимо знать MAC-адреса устройств (ПК). Следующая команда используется для статического ввода MAC-адресов.

[LSW1-Ethernet0/0/4]port-security mac-address sticky 5489-98FC-1170

При привязке статического MAC-адреса 6-значный адрес объединяется в 3 значные цифры.

Отчет должен состоять из:

1. Названия лабораторной работы, цель работы, краткие теоретические сведения;

2. Построить сеть по заданному варианту и произвести необходимые настройки;

3. Включить результаты в отчет;

4. Выводы

Контрольные вопросы

1. Возможности эмулятора eNSP.
2. Маршрутизаторы серии AR.
3. Возможности коммутационных устройств.
4. Задача программы WinPcap.
5. Программная задача Wireshark.
6. Функции и возможности программы VirtualBox.
7. Функция коммутационного аппарата.
8. Типы коммутационных устройств.
9. Как изменить имя устройства?
10. Зачем нужна безопасность портов и как она реализуется?
11. Как поставить пароль на консольный порт?
12. Какие есть способы создать заголовочную оболочку?
13. Как сохранить текущую настройку?
14. Как удалить настройки?
15. Варианты коммутатора, работающего на уровне L3.
16. Как статически привязать MAC-адрес?.
17. Какова цель команды *port-security mac-address sticky*?
18. Для чего используется команда *undo shutdown*?
19. Какова цель команды *undo terminal monitor*?
20. Какова цель команды *port-security max-mac-num 2*?

Лабораторная работа №2

Настройка протокола Telnet

Цель работы: Изучение настройки протокола Telnet и использования для удаленного доступа к сетевым устройствам.

Теоретическая часть

Telnet — это сетевой протокол, используемый для подключения к удаленному (дистанционному) компьютеру по сети или через Интернет и управления этой системой с помощью удаленных команд. Telnet — это основной сетевой протокол, используемый для виртуальной связи с удаленной системой с помощью текстового терминала. Telnet — это сетевой протокол, используемый для двусторонней связи между двумя удаленными хостами по сети или через Интернет.

Рисунок 2.1. Задача протокола Telnet

Используя этот протокол, пользователи могут входить в удаленную систему и общаться с помощью виртуального терминала, но он небезопасен для использования в ненадежных сетях, таких как Интернет.

Telnet обменивается данными в виде простого текста, поэтому он не подходит для отправки конфиденциальной информации, включая имена пользователей и пароли, с использованием этого протокола, поскольку любой другой может прочитать текст, которым обмениваются, и легко перехватить сообщения. Telnet обычно обменивается данными через TCP через порт 23, а также может получать доступ к другим портам и службам. Его можно использовать в частных сетях из-за более низкой безопасности.

Рисунок 2.2. Работа протокола Telnet

Задание:

Студенты будут строить и настраивать сеть, используя параметры, перечисленные в Таблице 2.1.

Таблица 2.1. Варианты задания

№	Задание
1.	Построить сеть, состоящую из 2 коммутаторов и 4 ПК. Настройте протокол telnet на коммутаторах.
2.	Построить сеть из 5 ПК и коммутаторов LSW3 и LSW4,. Настройте протокол telnet на коммутаторах.
3.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте протокол telnet на LSW2 и LSW3.
4.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте протокол telnet на LSW1 и LSW2.
5.	Построить сеть из 5 ПК и коммутаторов LSW3 и LSW2,. Настройте протокол telnet на коммутаторах.
6.	Построить сеть из 6 ПК и коммутаторов LSW4 и LSW2,. Настройте протокол telnet на коммутаторах.
7.	Построить сеть из 4 ПК и коммутаторов LSW5 и LSW2,. Настройте протокол telnet на коммутаторах.
8.	Построить сеть из 7 ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
9.	Построить сеть из 5ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
10.	Построить сеть из 7 ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
11.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте протокол telnet на LSW2 и LSW3.
12.	Построить сеть из 8 ПК и коммутаторов LSW5 и LSW6,. Настройте протокол telnet на коммутаторах.

13.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте протокол telnet на коммутаторах LSW3 и LSW4.
14.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте протокол telnet на коммутаторах LSW3 и LSW4.
15.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте протокол telnet на коммутаторах LSW1 и LSW3.
16.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте протокол telnet на коммутаторах LSW2 и LSW3.
17.	Построить сеть из 5 ПК и коммутаторов LSW3 и LSW4,. Настройте протокол telnet на коммутаторах.
18.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Настройте протокол telnet на коммутаторах LSW2 и LSW3.
19.	Построить сеть, состоящую из 2 коммутаторов и 6 ПК. Настройте протокол telnet на коммутаторах.
20.	Построить сеть из 6 ПК и коммутаторов LSW3 и LSW2,. Настройте протокол telnet на коммутаторах.
21.	Построить сеть из 6 ПК и коммутаторов LSW4 и LSW2,. Настройте протокол telnet на коммутаторах.
22.	Построить сеть из 4 ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
23.	Построить сеть из 5 ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
24.	Построить сеть из 3 ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
25.	Построить сеть из 6 ПК и коммутаторов LSW1 и LSW2,. Настройте протокол telnet на коммутаторах.
26.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте протокол telnet на коммутаторах LSW1 и LSW2.
27.	Построить сеть из 6 ПК и коммутаторов LSW5 и LSW6,. Настройте протокол telnet на коммутаторах.
28.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Настройте протокол telnet на коммутаторах LSW1 и LSW3.
29.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте протокол telnet на коммутаторах LSW2 va LSW4.
30.	Построен комплект, состоящий из 3 переключателей, 8 шт. Настройте протокол telnet на коммутаторах LSW1 va LSW3

В данной лабораторной работе решаются следующие задачи:

- настроить коммутаторы LSW1, LSW2 согласно топологии, показанной на рисунке 2.3;
- отрегулируйте настройки AAA;
- настроить виртуальный терминал VTY;
- настроить Telnet-сервер;
- настройка данных для входа пользователя;
- проверка доступа к удаленному устройству с помощью Telnet

Порядок выполнения работы

Настройте базовые конфигурации коммутаторов LSW1, LSW2 в соответствии с топологией, показанной на рис. 2.3.

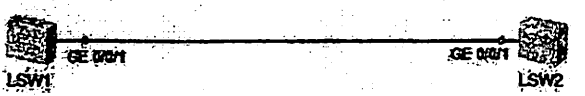

Рисунок 2.3. Исследуемая сетевая структура

Переименуем коммутатор LSW1 и настроим IP-адрес.

<Huawei>system-view

[Huawei]sysname LSW1

[LSW1]int vlanif 1

[LSW1-Vlanif1]ip address 192.168.1.1 24

Чтобы увидеть текущие настройки, нужно запустить команду «display this».

[LSW1-Vlanif1]display this

[LSW1-Vlanif1]quit

Ставим пароль на консольный порт. Установка пароля на консольный порт необязательна при настройке протокола Telnet. В предыдущей лабораторной работе мы использовали пароль в качестве аутентификации. В

этой лабораторной работе мы будем использовать «AAA» в качестве аутентификации (также при настройке протокола telnet).

[LSW1]user-interface console 0

[LSW1-ui-console0]authentication-mode aaa

[LSW1-ui-console0]idle-timeout 15

Чтобы увидеть результат настройки консольного порта, необходимо выполнить команду «display this » (рис. 2.4).

[LSW1-ui-console0]display this

```
[LSW1-ui-console0]display this
#
user-interface con 0
authentication-mode aaa
idle-timeout 15 0
user-interface vty 0 4
#
return
```

Рисунок 2.4. Результат настройки консольного порта

Следующая команда используется для выхода из настроек консольного порта:

[LSW1-ui-console0]quit

Настроим виртуальный терминал VTY.

[LSW1]user-interface vty 0 4

[LSW1-ui-vty0-4]authentication-mode aaa

[LSW1-ui-vty0-4]protocol inbound telnet

[LSW1-ui-vty0-4]idle-timeout 15

Чтобы увидеть результат текущих настроек, нужно запустить команду «display this»

[LSW1-ui-vty0-4]display this

Команда «quit» используется для выхода из настроек консольного порта.

[LSW1-ui-vty0-4]quit

Настроим сервер Telnet.

[LSW1]telnet server enable

[LSW1]aaa

[LSW1-aaa]local-user consolelsw1 password cipher user privilege level 15

[LSW1-aaa]local-user consolelsw1 service-type terminal

Чтобы увидеть результат настройки telnet-сервера на LSW1 (рисунок 2.5), нужно выполнить команду «display this»

[LSW1-aaa]display this

```
[LSW1-aaa]display this
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
 local-user consolelsw1 password cipher VY^NCQZ_aQ5NZPO3JBXBHA!!
 local-user consolelsw1 privilege level 15
#
return
```

Рисунок 2.5. Результат текущих настроек

Команда «quit» используется для выхода из настроек сервера Telnet.

[LSW1-aaa]quit

[LSW1]quit

<LSW1>quit

Выход и повторный вход в систему позволит вам войти в систему, введя свое имя пользователя и пароль.

Информация для входа пользователя настроена следующим образом:

[LSW1]aaa

[LSW1-aaa]local-user telnetlsw1 password cipher admin privilege level 15

[LSW1-aaa]local-user telnetlsw1 service-type telnet

Чтобы увидеть результат текущих настроек, нужно запустить команду «display this»

[LSW1-aaa]display this

[LSW1-aaa]quit

Чтобы увидеть все настройки, запустите команду «display current-configuration».

[LSW1]display current-configuration

Теперь приступим к настройке второго коммутатора. Переименуем коммутатор LSW2 и настроим IP-адрес.

<Huawei>system-view

[Huawei]sysname LSW2

[LSW2]int vlanif 1

[LSW2-Vlanif1]ip address 192.168.1.2 24

[LSW2-vlanif1]quit

Ставим пароль на консольный порт. Используем AAA в качестве аутентификации.

[LSW2]user-interface console 0

[LSW2-ui-console0]authentication-mode aaa

[LSW2-ui-console0]idle-timeout 15

[LSW2-ui-console0]display this

[LSW2-ui-console0]quit

Настроим виртуальный терминал VTY.

[LSW2]user-interface vty 0 4

[LSW2-ui-vty0-4]authentication-mode aaa

[LSW2-ui-vty0-4]protocol inbound telnet

[LSW2-ui-vty0-4]idle-timeout 15

[LSW2-ui-vty0-4]quit

Настроим Telnet-сервер.

[LSW2]telnet server enable

[LSW2]aaa

[LSW2-aaa]local-user telnetlsw2 password cipher admin privilege level 15

[LSW2-aaa]local-user telnetlsw2 service-type telnet

Чтобы увидеть результат настройки telnet-сервера (рисунок 2.6) на LSW2, необходимо выполнить команду «display this»

[LSW2-aaa]display this

```
[LSW2-aaa]display this
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
 local-user telnetlsw2 password cipher VY^NCQZ_aQ5NZPO3JBXBHA!!
 local-user telnetlsw2 privilege level 15
 local-user telnetlsw2 service-type telnet
 local-user consolelsw2 password cipher VY^NCQZ_aQ5NZPO3JBXBHA!!
 local-user consolelsw2 privilege level 15
 local-user consolelsw2 service-type terminal
#
return
```

Рисунок 2.6. Результат настройки сервера telnet на LSW2

Настроим данные для входа пользователя.

[LSW2]aaa

[LSW2-aaa]local-user consolelsw2 password cipher user privilege level 15

[LSW2-aaa]local-user consolelsw2 service-type terminal

[LSW2-aaa]quit

[LSW2]quit

<LSW2>quit

При выходе из системы и повторном входе вам будет предложено ввести имя пользователя и пароль.

Username:consolelsw2

Password:

<LSW2>system-view

[LSW2]aaa

Используйте команду «display this», чтобы увидеть текущие настройки.

[LSW2-aaa]display this

[LSW2-aaa]quit #

Теперь проверим соединение между двумя коммутаторами с помощью команды ping.

[LSW2]ping 192.168.1.2

Результат обмена данными между коммутаторами LSW2 и LSW1 показан на рисунке 2.7.

```
[LSW2]ping 192.168.1.1
  PING 192.168.1.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=280 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=255 time=10 ms
```

Рисунок 2.7. Результат связи между коммутаторами LSW2 и LSW1

Результат обмена данными между коммутаторами LSW1 и LSW2 показан на рисунке 2.8.

```
[LSW1]ping 192.168.1.2
  PING 192.168.1.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.2: bytes=56 Sequence=1 ttl=255 time=390 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 192.168.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.1.2: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 192.168.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
```

Рисунок 2.8. Результат связи между коммутаторами LSW1 и LSW2

Подключаемся от коммутатора LSW1 к коммутатору LSW2 по протоколу Telnet.

Подключение от коммутатора LSW1 к коммутатору LSW2 по протоколу Telnet осуществляется следующим образом:

<LSW1>telnet 192.168.1.2

Мы подключились от коммутатора LSW1 к коммутатору LSW2, используя протокол Telnet. Мы можем видеть результат (рис.2.9).

Шаг 1.

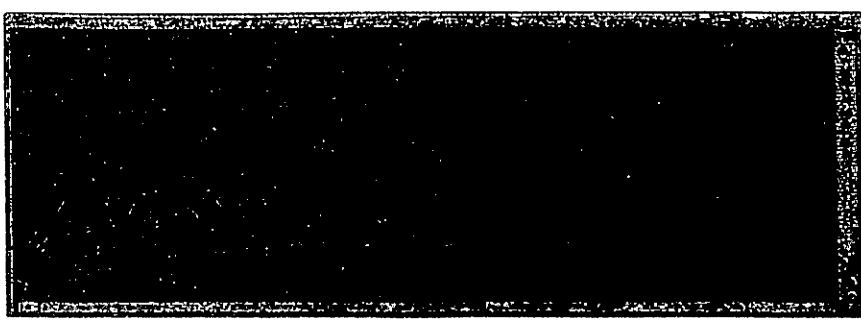

Рисунок 2.9. Результат подключения коммутатора LSW1 к коммутатору LSW2 по протоколу Telnet

Подключение к коммутатору LSW2 по протоколу Telnet успешно выполнено.

Пример 2

На рис. 2.10 показана структура исследуемой сети. В этом примере настраивается протокол Telnet между двумя коммутаторами (LSW1 и LSW2). В этом примере консольный порт не защищен паролем.

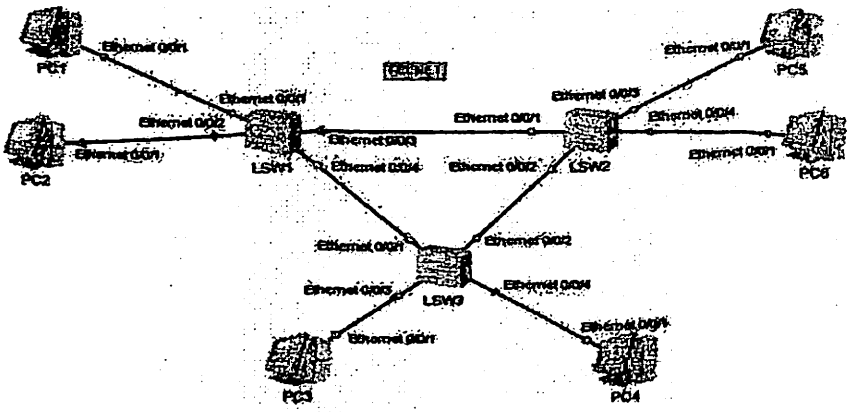

Рисунок 2.10. Исследуемая структура сети

Коммутатору LSW1 дается имя и настраивается IP-адрес..

<Huawei>system-view

[Huawei]sysname LSW1

[LSW1]int vlanif 1

[LSW1-Vlanif1]ip address 192.168.1.1 24

[LSW1-Vlanif1]quit

Дается имя коммутатору LSW2 и настроим IP-адрес .

<Huawei>system-view

[Huawei]sysname LSW2

[LSW2]int vlanif 1

[LSW2-Vlanif1]ip address 192.168.1.2 24

[LSW2-Vlanif1]quit

Настраиваем виртуальный терминал VTY на LSW1. Мы используем AAA в качестве аутентификации

[LSW1]user-interface vty 0 4

[LSW1-ui-vty0-4]authentication-mode aaa

[LSW1-ui-vty0-4]protocol inbound telnet

[LSW1-ui-vty0-4]idle-timeout 15

[LSW1-ui-vty0-4]quit

Настраиваем телнет-сервер на LSW1.

[LSW1]telnet server enable

В LSW1 мы настраиваем данные для входа пользователя

[LSW1]aaa

[LSW1-aaa]local-user ulugbek password cipher 123 privilege level 15

[LSW1-aaa]local-user ulugbek service-type telnet

[LSW1-aaa]quit

Настраиваем виртуальный терминал VTY на LSW2

[LSW2]user-interface vty 0 4

[LSW2-ui-vty0-4]authentication-mode aaa

[LSW2-ui-vty0-4]protocol inbound telnet

[LSW2-ui-vty0-4]idle-timeout 15

[LSW2-ui-vty0-4]quit

Настраиваем сервер Telnet на LSW2

[LSW2]telnet server enable

В LSW2 мы настраиваем информацию для входа пользователя.

[LSW2]aaa

[LSW2-aaa]local-user ulugbek2 password cipher 123 privilege level 15

[LSW2-aaa]local-user ulugbek2 service-type telnet

Подключаемся от коммутатора LSW1 к коммутатору LSW2 по протоколу Telnet. Для этого вводим следующую команду

<LSW1>telnet 192.168.1.2

Мы сделали подключение от коммутатора LSW1 к коммутатору LSW2 по протоколу Telnet. Результат показан на рисунке 2.11.

Шаг 2.

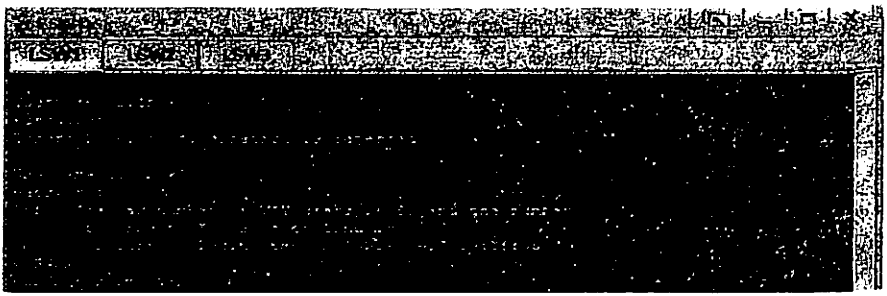

Рисунок 2.11. Результат telnet-подключения к коммутатору LSW2

Telnet-подключение к коммутатору LSW2 прошло успешно.

Отчет должен состоять из:

1. Название лабораторной работы, цель работы, краткие теоретические сведения;
2. Построить сеть по заданному варианту и произвести необходимые настройки;
3. Включите результаты в отчет;
4. Выводы

Контрольные вопросы

1. Объясните принцип работы протокола Telnet.
2. Какова функция протокола Telnet?
3. Через какой порт TCP осуществляется связь по Telnet?
4. Что такое AAA?
5. Что такое VTY?
6. В чем разница между протоколом Telnet и протоколом SSH?
7. Какой порт указан для протокола Telnet?
8. Какая команда используется для подключения по протоколу Telnet?

Лабораторная работа №3

Создание и настройка VLAN

Цель работы: Получите практические навыки по созданию и настройки VLAN.

Теоретическая часть

VLAN (Virtual Local Area Network, виртуальная локальная сеть) — это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе (Ethernet, Wi-Fi интерфейсе) создать несколько виртуальных локальных сетей. VLAN используют для создания логической топологии сети, которая никак не зависит от физической топологии.

Примеры использования VLAN:

- Объединение в единую сеть компьютеров, подключенных к разным коммутаторам.

Допустим, у вас есть компьютеры, которые подключены к разным свитчам, но их нужно объединить в одну сеть. Одни компьютеры мы объединим в виртуальную локальную сеть VLAN 1, а другие — в сеть VLAN 2. Благодаря функции VLAN компьютеры в каждой виртуальной сети будут работать, словно подключены к одному и тому же свитчу. Компьютеры из разных виртуальных сетей VLAN 1 и VLAN 2 будут невидимы друг для друга.

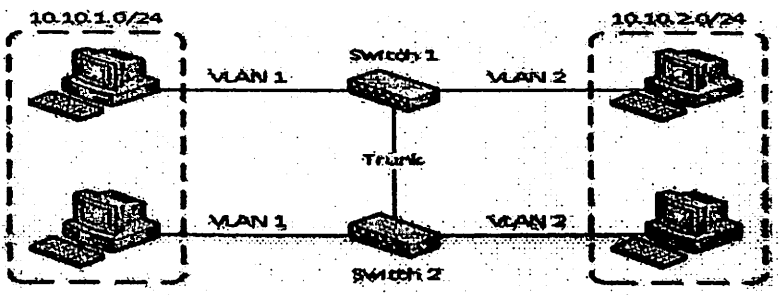

Рисунок 13.1. Разделение в разные подсети компьютеров, подключенных к одному коммутатору

- Разделение компьютеров, подключенных к одному коммутатору, на разные подсети.

На рисунке 3.2 компьютеры физически подключены к одному свитчу, но разделены в разные виртуальные сети VLAN 1 и VLAN 2. Компьютеры из разных виртуальных подсетей будут невидимы друг для друга.

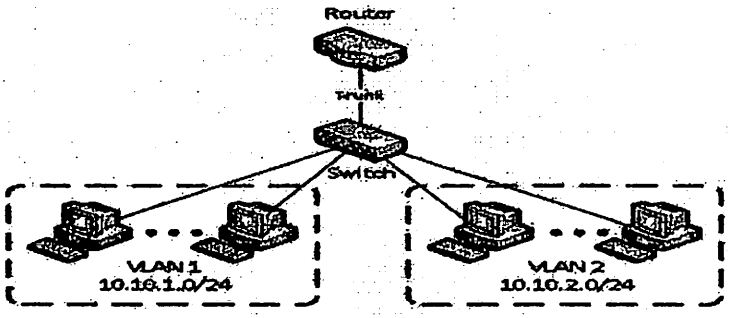

Рисунок 3.2. Разделение компьютеров, подключенных к одному коммутатору, в разные подсети

- Разделение гостевой Wi-Fi сети и Wi-Fi сети предприятия.

На рисунке 3.3 к маршрутизатору (router) подключена физически одна Wi-Fi точка доступа.

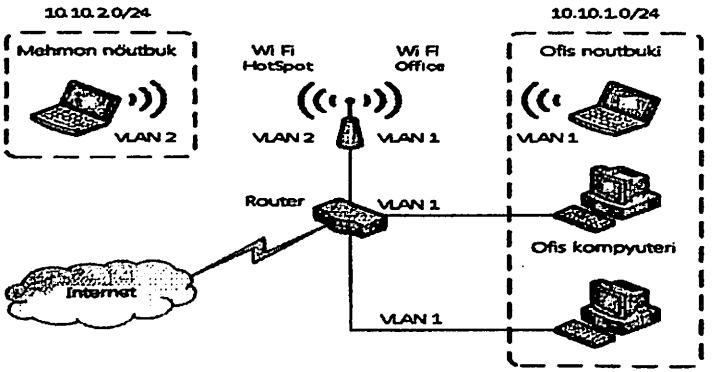

Рисунок 3.3. Разделение гостевой сети Wi-Fi и корпоративной сети Wi-Fi на VLAN

На точке созданы две виртуальные Wi-Fi точки с названиями HotSpot и Office. К HotSpot будут подключаться по Wi-Fi гостевые ноутбуки для доступа к интернету, а к Office — ноутбуки предприятия. В целях безопасности необходимо, чтобы гостевые ноутбуки не имели доступ к сети предприятия. Для этого компьютеры предприятия и виртуальная Wi-Fi точка Office объединены в виртуальную локальную сеть VLAN 1, а гостевые ноутбуки будут находиться в виртуальной сети VLAN 2. Гостевые ноутбуки из сети VLAN 2 не будут иметь доступ к сети предприятия VLAN 1.

Достоинства испольвования VLAN

- Гибкое разделение устройств на группы.

Как правило, одному VLAN соответствует одна подсеть. Компьютеры, находящиеся в разных VLAN, будут изолированы друг от друга. Также можно объединить в одну виртуальную сеть компьютеры, подключенные к разным коммутаторам.

- Уменьшение широковещательного трафика в сети.

Каждый VLAN представляет отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN. Если на разных коммутаторах настроить один и тот же VLAN, то порты разных коммутаторов будут образовывать один широковещательный домен.

- Увеличение безопасности и управляемости сети.

В сети, разбитой на виртуальные подсети, удобно применять политики и правила безопасности для каждого VLAN. Политика будет применена к целой подсети, а не к отдельному устройству.

- Уменьшение количества оборудования и сетевого кабеля.

Для создания новой виртуальной локальной сети не требуется покупка коммутатора и прокладка сетевого кабеля. Однако вы должны использовать более дорогие управляемые коммутаторы с поддержкой VLAN.

Характеристики технологии VLAN

Максимальное количество VLAN в системе — 4096 (VLAN 0 и VLAN 4095 зарезервированы).

Максимальное количество интерфейсов VLANIF в системе — 4094..

Как правило, каждый порт коммутатора имеет VLAN 1 или управляющую VLAN. Сеть управления нельзя отключить, но можно создать дополнительные сети VLAN и назначить дополнительные порты для этих альтернативных сетей VLAN.

Назначение VLAN может быть выполнено на основе одного из пяти методов, включая порт, MAC-адрес, IP-подсеть, протокол и реализацию на основе политики. Метод на основе портов является стандартным и наиболее распространенным методом назначения VLAN. С помощью этого метода VLAN классифицируются на основе номеров портов на коммутаторе.

Задание:

Студенты строят и настраивают сеть, используя параметры, перечисленные в Таблице 3.1.

Таблица 3.1. Варианты задания

№	Задание
1.	Построить сеть, состоящую из 2 коммутаторов и 4 ПК. Создайте и настройте Vlan10 и Vlan20.
2.	Построить сеть из LSW3 и LSW4 и из 5 ПК. Создайте и настройте Vlan15 и Vlan20.
3.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Создайте и настройте Vlan10, Vlan15 и Vlan5.
4.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Создайте и настройте Vlan30 и Vlan40.
5.	Построить сеть из LSW2 и LSW3 и из 5 ПК. Создайте и

	настройте Vlan12 и Vlan26.
6.	Построить сеть из LSW4 и LSW2 и из 6 ПК. Создайте и настройте Vlan6 и Vlan7.
7.	Построить сеть из LSW5 и LSW2 и из 4 ПК. Создайте и настройте Vlan10 и Vlan20.
8.	Построить сеть из LSW1 и LSW2 и из 7 ПК. Создайте и настройте Vlan5 и Vlan10.
9.	Построить сеть из LSW1 и LSW2 и из 5 ПК. Создайте и настройте Vlan20 и Vlan30.
10.	Построить сеть из LSW1 и LSW2 и из 7 ПК. Создайте и настройте Vlan13 и Vlan15.
11.	Построить сеть, состоящую из 3 коммутаторов и из 5 ПК. Создайте и настройте Vlan10 и Vlan20 на LSW2 и LSW3.
12.	Построить сеть из LSW5 и LSW6 и из 8 ПК. Создайте и настройте Vlan10 и Vlan25.
13.	Построить сеть из 4 коммутаторов и 4 ПК. Создайте и настройте Vlan15 и Vlan20 на LSW3 и LSW4 .
14.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Создайте и настройте Vlan30 и Vlan50 на LSW3 и LSW4.
15.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Создайте и настройте Vlan14 и Vlan24 на LSW1 и LSW3.
16.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Создайте и настройте Vlan7 и Vlan12 на LSW2 и LSW3.
17.	Построить сеть из LSW3 и LSW4 и из 5 ПК. Создайте и настройте Vlan10 и Vlan20.
18.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Создайте и настройте Vlan20 и Vlan25 на LSW2 и LSW3.
19.	Построить сеть, состоящую из 2 коммутаторов и 6 ПК. Создайте и настройте Vlan5 и Vlan10.
20.	Построить сеть из LSW3 и LSW2 и из 6 ПК. Создайте и

	настройте Vlan10 и Vlan20.
21.	Построить сеть из LSW4 и LSW2 и из 6 ПК. Создайте и настройте Vlan17 и Vlan20.
22.	Построить сеть из LSW1 и LSW2 и из 4 ПК. Создайте и настройте Vlan15 и Vlan25.
23.	Построить сеть из LSW1 и LSW2 и из 5 ПК. Создайте и настройте Vlan18 и Vlan28.
24.	Построить сеть из LSW1 и LSW2 и из 3 ПК. Создайте и настройте Vlan18 и Vlan20.
25.	Построить сеть из LSW1 и LSW2 и из 6 ПК. Создайте и настройте Vlan16 и Vlan22.
26.	Построить сеть, состоящую из 3 коммутаторов и из 5 ПК. Создайте и настройте Vlan19 и Vlan20 на LSW1 и LSW2.
27.	Построить сеть из LSW5 и LSW6 и из 6 ПК. Создайте и настройте Vlan5 и Vlan9.
28.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Создайте и настройте Vlan16 и Vlan24 на LSW1 и LSW3.
29.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Создайте и настройте Vlan17 и Vlan27 на LSW2 и LSW4.
30.	Построить сеть, состоящую из 3 коммутаторов и 8 ПК. Создайте и настройте Vlan50 и Vlan100 на LSW1 и LSW3.

В данной лабораторной работе решаются следующие задачи:

- Настроить интерфейсы устройств, как показано на рисунке 3.4;

- Определить интерфейсы портов, как порты доступа и магистральные порты;

- создать VLAN;

- Настроить теги VLAN на портах, используя тип подключения к транковому порту;

- Настроить VLAN по умолчанию для интерфейса, используя VLAN ID порта;

- Проверить связь между VLAN.

Порядок выполнения работы

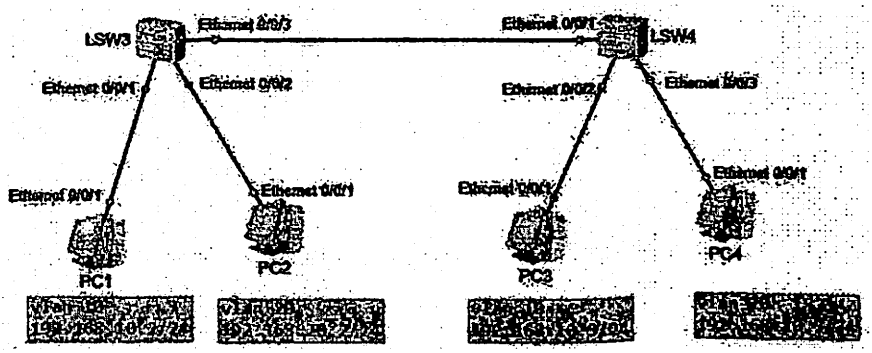

Рисунок 3.4. Исследуемая топология сети

Создаем VLAN вводом коммутатора LSW3. Именуем коммутатор и создаем vlan 10.

<Huawei>system-view

[Huawei]sysname LSW3

[LSW3]vlan 10

[LSW3-vlan10]quit

Создаем vlan 20 на коммутаторе LSW3.

[LSW3]vlan 20

[LSW3-vlan20]quit

[LSW3]interface Ethernet 0/0/1

[LSW3-Ethernet0/0/1]port link-type access

[LSW3-Ethernet0/0/1]port default vlan 10

[LSW3-Ethernet0/0/1]quit

[LSW3]interface Ethernet 0/0/2

[LSW3-Ethernet0/0/2]port link-type access

[LSW3-Ethernet0/0/2]port default vlan 20

[LSW3-Ethernet0/0/2]quit

Мы создаем VLAN, войдя в коммутатор LSW4. Именуем коммутатор и создаем vlan 10.

<Huawei>system-view

[Huawei]sysname LSW4

[LSW4]vlan 10

[LSW4-vlan10]quit

Создаем vlan 20 на коммутаторе LSW4.

[LSW4]vlan 20

[LSW4-vlan20]quit

Настроим тип привязки портов и назначаем VLAN на порты.

[LSW4]interface Ethernet 0/0/2

[LSW4-Ethernet0/0/2]port link-type access

[LSW4-Ethernet0/0/2]port default vlan 10

[LSW4-Ethernet0/0/2]quit

[LSW4]interface Ethernet 0/0/3

[LSW4-Ethernet0/0/3]port link-type access

[LSW4-Ethernet0/0/3]port default vlan 20

[LSW4-Ethernet0/0/3]quit

Теперь мы указываем тип соединения портов между двумя коммутаторами и какому VLANу разрешено проходить через это магистральное соединение.

Настроим LSW3.

[LSW3]interface Ethernet 0/0/3

[LSW3-Ethernet0/0/3]port link-type trunk

[LSW3-Ethernet0/0/3]port trunk allow vlan 10 20

[LSW3-Ethernet0/0/3]quit

Настроим LSW4.

[LSW4]interface Ethernet 0/0/1

[LSW4-Ethernet0/0/1]port link-type trunk

[LSW4-Ethernet0/0/1]port trunk allow vlan 10 20

[LSW4-Ethernet0/0/1]quit

Проверим связь между VLAN . Для этого входим в каждый персональный компьютер и назначаем IP-адреса, как показано на рисунке 3.4.

PC1 ga – 192.168.10.2 /255.255.255.0

PC2 ga – 192.168.20.2 /255.255.255.0

PC3 ga – 192.168.10.3 /255.255.255.0

PC4 ga – 192.168.20.3 /255.255.255.0

Проверим, правильно ли настроены VLAN. Для этого отправляем ping с ПК1 (VLAN 10/192.168.10.2) на ПК3 (VLAN 10/192.168.10.3).

Шаг 1.

Рисунок 3.5. Проверка связи между VLAN 10

Мы видим, что VLAN настроены правильно.

Отчет должен состоять из:

1. Название лабораторной работы, цель работы, краткие теоретические сведения;
2. Построить сеть по заданному варианту и произвести необходимые настройки;
3. Включить результаты в отчет;
4. Выводы.

Контрольные вопросы

1. Что такое VLAN?
2. Какова цель создания VLAN?
3. Какие возможности предоставляет VLAN?
4. Каково максимальное количество VLAN?
5. Для чего используется режим доступа?
6. Что такое ствол?
7. Для чего используется режим доступа?
8. Перечислите типы VLAN.

Лабораторная работа №4.

Настройка протокола GVRP и изучение принципа его работы.

Цель работы: Развить практические навыки настройки и применения протокола GVRP.

Теоретическая часть

GARP VLAN Registration Protocol (GVRP) — это протокол канального уровня модели OSI, основанный на стандарте IEEE 802.1p, который позволяет коммутаторам в локальных сетях динамически регистрировать VLAN.

Основная цель GVRP — позволить коммутаторам автоматически обнаруживать информацию о VLAN, которую в противном случае пришлось бы настраивать вручную для каждого коммутатора. Этого можно достичь путем распределения идентификаторов VLAN по локальной сети (используя GVRP). GVRP также можно использовать на сетевых серверах. Эти серверы обычно настроены на присоединение к нескольким VLAN, а затем сообщают коммутаторам, к каким VLAN они хотят присоединиться. Другая функция GVRP используется для регистрации и отмены регистрации атрибутов VLAN. GARP идентифицирует приложения по их MAC-адресам. IEEE Std назначает 01-80-C2-00-00-21 реализации 802.1Q VLAN (GVRP).

GARP-сообщения

Члены GARP обмениваются информацией VLAN посредством сообщений GARP. Основными сообщениями GARP являются сообщения о присоединении, сообщения о выходе и сообщения о выходе из группы.

Сообщение присоединения (join message)

Когда член GARP ожидает, пока другие устройства зарегистрируют его атрибуты, он отправляет сообщения о присоединении к другим устройствам. Когда член GARP получает сообщение о присоединении от другого члена или он статически настроен с атрибутами, он отправляет сообщения о присоединении на другие устройства, чтобы устройства могли зарегистрировать новые атрибуты.

Существует два типа сообщений о присоединении:

Сообщение JoinEmpty: объявляет незарегистрированный атрибут;

Сообщение JoinIn: объявляет объединенный атрибут.

Сообщение Leave (leave message)

Член GARP отправляет сообщения Leave другим устройствам, когда он ожидает, пока другие устройства удалят (удаляют) его атрибуты из списка. Когда участник GARP получает сообщение о выходе от другого участника или когда некоторые из его атрибутов статически аннулируются, он также отправляет сообщения о выходе на другие устройства.

Сообщения Leave делятся на два типа:

Сообщение LeaveEmpty: удаляет незарегистрированный атрибут из списка.

Сообщение LeaveIn: удаляет зарегистрированный атрибут из списка.

Сообщения LeaveAll (LeaveAll messages)

Когда участник запускается, он запускает таймер LeaveAll. По истечении времени таймера LeaveAll участник отправляет сообщения LeaveAll на другие устройства. Член отправляет сообщения LeaveAll, чтобы отменить регистрацию всех атрибутов, чтобы другие участники могли повторно зарегистрировать атрибуты локального члена. Сообщения LeaveAll иногда используются для удаления ненужных атрибутов из сети. Например, атрибут участника удален (удален).

GARP-таймеры

GARP определяет четыре таймера:

- присоединиться к таймеру (Join timer);
- удерживать таймер (Hold timer);
- убрать таймер (Leave timer);
- удалить все таймеры (LeaveAll timer).

Режимы регистрации

Настроенная вручную VLAN — это статическая VLAN, а VLAN, созданная с использованием GVRP, — это динамическая VLAN. GVRP предоставляет три режима регистрации. Статические VLAN и динамические VLAN работают по-разному в каждом режиме ведения журнала. Режимы регистрации GVRP следующие:

Normal: В этом режиме динамические VLAN могут быть зарегистрированы на интерфейсах, а интерфейсы могут анонсировать динамические VLAN и статические VLAN.

Fixed: В этом режиме динамические VLAN не могут быть зарегистрированы на интерфейсе, а интерфейсы могут анонсировать статические VLAN.

Forbidden: В этом режиме нельзя зарегистрировать динамические VLAN, все VLAN, кроме VLAN 1, удаляются из интерфейсов, а интерфейсы могут объявлять только информацию о VLAN 1.

Чтобы настроить VLAN на всех устройствах в сети, сетевой администратор должен вручную создать ее на каждом устройстве. На рис. 4.1 четыре коммутатора соединены магистралью.

Задание:

Студенты строят и настраивают сеть, используя параметры, перечисленные в Таблице 4.1.

Таблица 4.1. Варианты задания

№	Задание
1.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Создайте Vlan10 и Vlan20 и настройте GVRP.
2.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Создайте Vlan15 и Vlan20 и настройте GVRP.
3.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Создайте Vlan10, Vlan15 и Vlan5 и настройте GVRP.
4.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Создайте Vlan30 и Vlan40 и настройте GVRP.
5.	Построить сеть, состоящую из 5 коммутаторов и 5 ПК. Создайте Vlan12 и Vlan26 и настройте GVRP.
6.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Создайте Vlan6 и Vlan7 и настройте GVRP.
7.	Построить сеть, состоящую из 5 коммутаторов и 4 ПК. Создайте Vlan10 и Vlan20 и настройте GVRP.
8.	Построить сеть из 7 ПК и коммутатор LSW1 и LSW2. Создайте Vlan5 и Vlan10 и настройте GVRP.
9.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Создайте Vlan20 и Vlan30 и настройте GVRP.
10.	Построить сеть, состоящую из 4 коммутаторов и 7 ПК. Создайте Vlan13 и Vlan15 и настройте GVRP.
11.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Создайте Vlan10 и Vlan20 на LSW2 и LSW3 и настройте GVRP.
12.	Построить сеть, состоящую из 5 коммутаторов и 8 ПК. Создайте Vlan10 и Vlan25 и настройте GVRP.

13.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Создайте Vlan15 и Vlan20 на LSW3 и LSW4 и настройте GVRP.
14.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Создайте Vlan30 и Vlan50 на LSW3 и LSW4 и настройте GVRP.
15.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Создайте Vlan14 и Vlan24 на LSW1 и LSW3 и настройте GVRP.
16.	Построить сеть, состоящую из 5 коммутаторов и 5 ПК. Создайте Vlan7 и Vlan12 на LSW2 и LSW3 и настройте GVRP.
17.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Создайте Vlan10 и Vlan20 и настройте GVRP.
18.	Построить сеть, состоящую из 5 коммутаторов и 9 ПК. Создайте Vlan20 и Vlan25 на LSW2 и LSW3 и настройте GVRP.
19.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Создайте Vlan5 и Vlan10 и настройте GVRP.
20.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Создайте Vlan10 и Vlan20 и настройте GVRP.
21.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Создайте Vlan17 и Vlan20 и настройте GVRP.
22.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Создайте Vlan15 и Vlan25 и настройте GVRP.
23.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Создайте Vlan18 и Vlan28 и настройте GVRP.
24.	Построить сеть, состоящую из 4 коммутаторов и 3 ПК. Создайте Vlan18 и Vlan20 и настройте GVRP.
25.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Создайте Vlan16 и Vlan22 и настройте GVRP.
26.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Создайте Vlan19 и Vlan20 на LSW1 и LSW2 и настройте GVRP.
27.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Создайте Vlan5 и Vlan9 и настройте GVRP.
28.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Создайте Vlan16 и Vlan24 на LSW1 и LSW3 и настройте GVRP.
29.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Создайте Vlan17 и Vlan27 на LSW2, LSW4 и настройте GVRP.
30.	Построить сеть, состоящую из 3 коммутаторов и 8 ПК. Создайте Vlan50 и Vlan100 на LSW1 и LSW3 и настройте GVRP.

В данной лабораторной работе решаются следующие задачи:

- Настройте интерфейсы устройств, как показано на рисунке 4.1;
- настроить GVRP;
- Установить режим регистрации GVRP.

Порядок работы

Исследуемая топология сети показана на рис. 4.1.

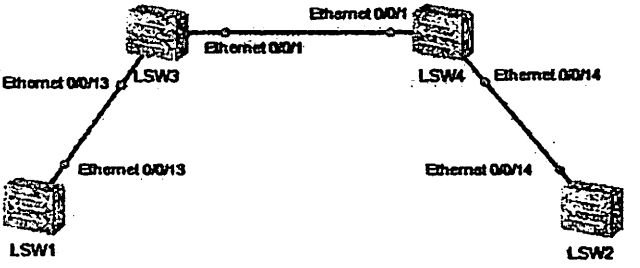

Рисунок 4.1. Исследуемая структура сети

Корпоративная сеть содержит несколько коммутаторов, которыми необходимо регулярно управлять. Виртуальные локальные сети следует применять и удалять по мере необходимости на всех коммутаторах, но обычно это трудоемкая задача для администратора, а ошибки конфигурации часто возникают из-за человеческого фактора. Администратор хочет упростить процесс управления VLAN и попросил включить GVRP на всех коммутаторах и установить режим логирования на интерфейсах.

Настроим устройства. Называем устройства.

Для коммутатора LSW1:

<Huawei>system-view

[Huawei]sysname LSW1

Для коммутатора LSW2:

<Huawei>system-view

[Huawei]sysname LSW2

Для коммутатора LSW3:

<Huawei>system-view

[Huawei]sysname LSW3

Для коммутатора LSW4:

<Huawei>system-view

[Huawei]sysname LSW4

Настраиваем магистральные соединения(trunk) между коммутаторами:

Для коммутатора LSW1:

[LSW1]interface ethernet 0/0/13

[LSW1-Ethernet0/0/13]port link-type trunk

[LSW1-Ethernet0/0/13]port trunk allow-pass vlan all

Для коммутатора LSW3:

[LSW3]interface Ethernet 0/0/13

[LSW3-Ethernet0/0/13]port link-type trunk

[LSW3-Ethernet0/0/13]port trunk allow-pass vlan all

[LSW3]interface ethernet 0/0/1

[LSW3-Ethernet0/0/1]port link-type trunk

[LSW3-Ethernet0/0/1]port trunk allow-pass vlan all

Для коммутатора LSW4:

[LSW4]interface ethernet 0/0/14

[LSW4-Ethernet0/0/14]port link-type trunk

[LSW4-Ethernet0/0/14]port trunk allow-pass vlan all

[LSW4-Ethernet0/0/14]quit

[LSW4]interface ethernet 0/0/1

[LSW4-Ethernet0/0/1]port link-type trunk

[LSW4-Ethernet0/0/1]port trunk allow-pass vlan all

[LSW2]interface Ethernet 0/0/14

[LSW2-Ethernet0/0/14]port link-type trunk

[LSW2-Ethernet0/0/14]port trunk allow-pass vlan all

Настроим GVRP на всех соответствующих интерфейсах:

Для коммутатора LSW1:

[LSW1]gvrp

[LSW1]interface ethernet 0/0/13

[LSW1-Ethernet0/0/13]gvrp

Для коммутатора LSW3:

[LSW3]gvrp

[LSW3]interface ethernet 0/0/13

[LSW3-Ethernet0/0/13]gvrp

[LSW3-Ethernet0/0/13]quit

[LSW3]interface ethernet 0/0/1

[LSW3-Ethernet0/0/1]gvrp

Для коммутатора LSW2:

[LSW2]gvrp

[LSW2]interface ethernet 0/0/14

[LSW2-Ethernet0/0/14]gvrp

Для коммутатора LSW4:

[LSW4]gvrp

[LSW4]interface ethernet 0/0/14

[LSW4-Ethernet0/0/14]gvrp

[LSW4-Ethernet0/0/14]quit

[LSW4]interface ethernet 0/0/1

[LSW4-Ethernet0/0/1]gvrp

Создаем VLAN 100 на LSW1, VLAN 200 на LSW2 и VLAN 2 на LSW1, LSW2, LSW3 и LSW4.

Для коммутатора LSW1:

[LSW1]vlan batch 2 100

Для коммутатора LSW2:

[LSW2]vlan batch 2 200

Для коммутатора LSW3:

[LSW3]vlan 2

Для коммутатора LSW4:

[LSW4]vlan 2

Чтобы просмотреть статистику GVRP на LSW3 и LSW4 запустите команду отображения статистики ("display gvrp statistics"). Статистика gvrp для LSW3 показана на рис. 4.2.

[LSW3]display gvrp statistics

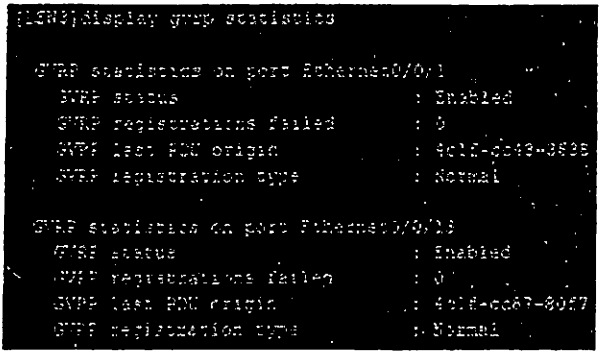

Рисунок 4.2. Статистика gvrp на LSW3

[LSW4]display gvrp statistics

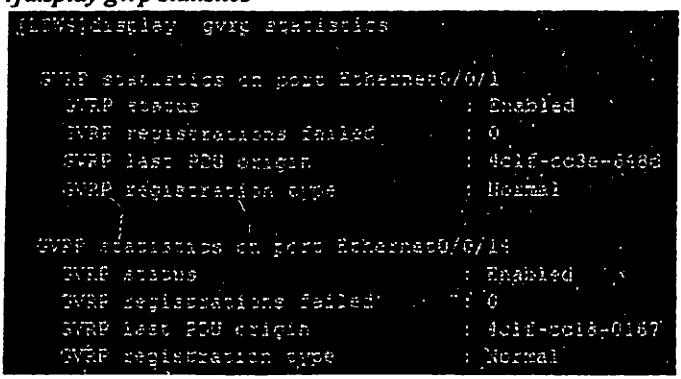

Рисунок 4.3. Статистика gvrp на LSW4

По умолчанию тип регистрации устанавливается как обычно. Мы используем команду «display vlan» для проверки конфигурации VLAN на LSW3 и LSW4. Результат настройки VLAN в LSW3 показан на рисунке 4.4.

[LSW3]display vlan

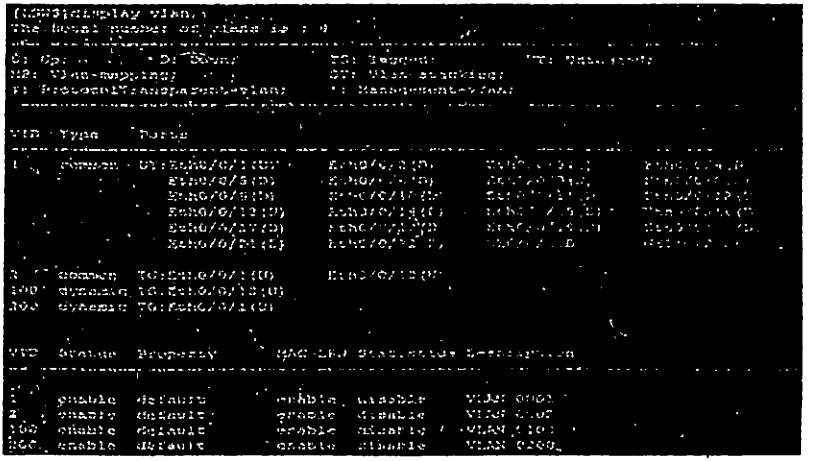

Рисунок 4.4. Проверка настроек VLAN на LSW3

Результат настройки VLAN в LSW4 показан на рисунке 4.5.

[LSW3]display vlan

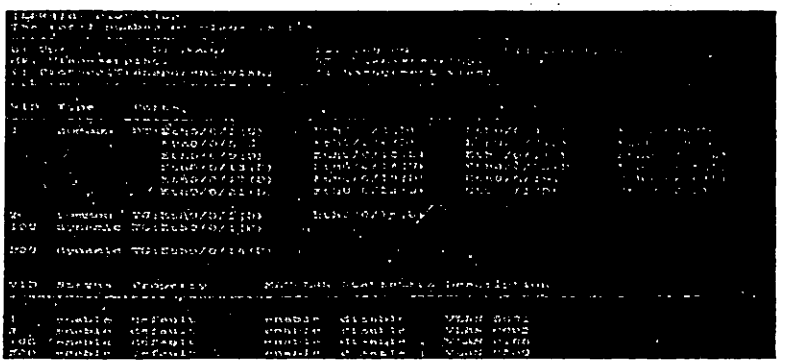

Рисунок 4.5. Проверка настроек VLAN на LSW4

LSW3 и LSW4 динамически изучают VLAN 100 и VLAN 200, но только в одном направлении. VLAN 2 определяется статически. Чтобы включить двунаправленное распространение, мы создаем VLAN 200 на LSW1 и VLAN 100 на LSW2.

Для коммутатора LSW1:

[LSW1]vlan 200

Для коммутатора LSW2:

[LSW2]vlan 100

Запускаем команду "display vlan" на LSW3 и LSW4 для проверки конфигурации.

[LSW3]display vlan

Результат настройки VLAN в LSW3 показан на рисунке 4.6.

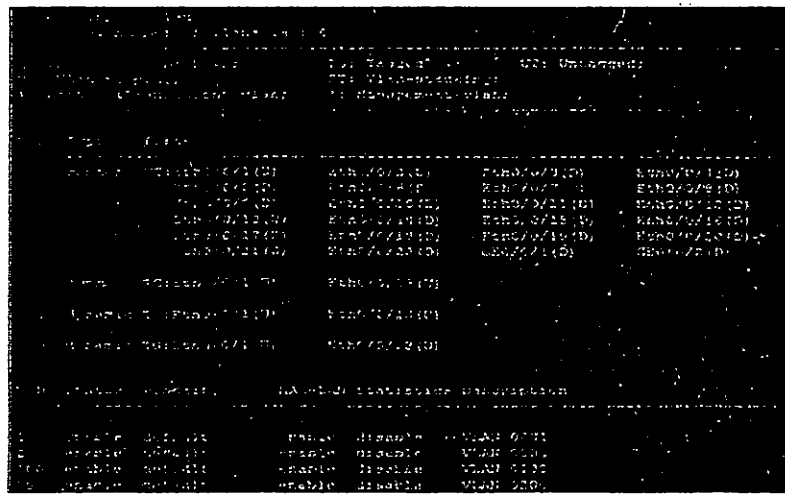

Рисунок 4.6. Проверка настроек VLAN на LSW3

Результат настройки VLAN в LSW4 показан на рисунке 4.7.

[LSW4]display vlan

Рисунок 4.7. Проверка настроек VLAN на LSW4

Выделенные записи показывают интерфейсы, добавленные в VLAN 100 и VLAN 200 на LSW3 и LSW4.

Изменяем тип регистрации для интерфейсов.

На LSW3 мы меняем тип регистрации Ethernet 0/0/1 на «fixed». Те же шаги можно выполнить на интерфейсе Ethernet 0/0/1 LSW4.

[LSW3]interface ethernet 0/0/1

[LSW3-Ethernet0/0/1]gvrp registration fixed

Запустите команду отображения статистики "display gvrp statistics" на LSW3 и LSW4, чтобы увидеть изменения. Рис. 4.8

[LSW3-Ethernet0/0/1]display gvrp statistics interface Ethernet 0/0/1

[LSW4-Ethernet0/0/1]display gvrp statistics interface Ethernet 0/0/1

Шаг 7.

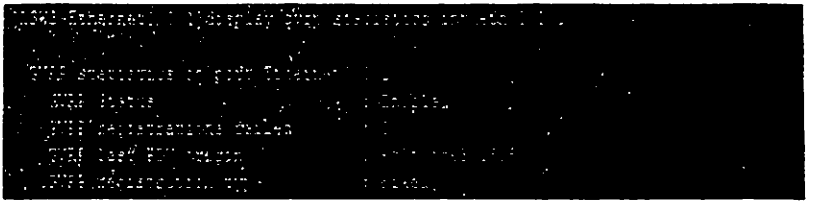

Рисунок 4.8. Результат установки фиксированного режима

Тип регистрации GVRP проверяется как установленный на интерфейсе Ethernet 0/0/1. Динамические VLAN не могут регистрироваться на этом интерфейсе. Давайте запустим команду display vlan, чтобы увидеть эффект фиксированного типа ведения журнала.

Отмеченные записи означают, что интерфейс Ethernet 0/0/1 не зарегистрирован в динамических VLAN 100 и VLAN 200. Рис. 4.9

[LSW3]display vlan

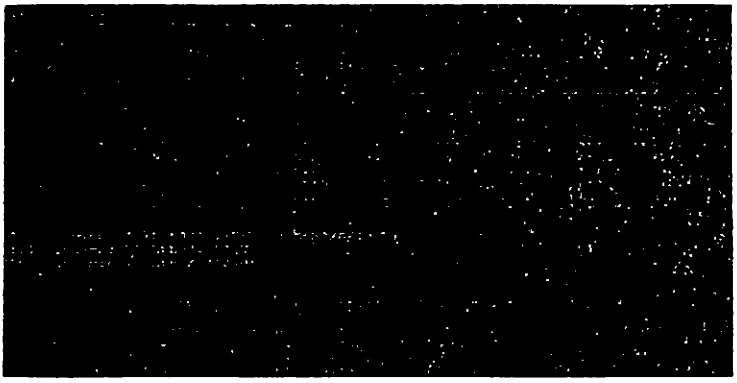

Рисунок 4.9. Проверка VLAN на LSW3 после установки режима fixed

Теперь настроим интерфейс Ethernet 0/0/1 LSW3 для использования следующего типа регистрации. Второй тип регистрации — «запрещенный», его мы и настроим. Те же шаги можно выполнить на интерфейсе Ethernet 0/0/1 LSW4.

[LSW3]interface ethernet 0/0/1

[LSW3-Ethernet0/0/1]gvrp registration forbidden

Чтобы увидеть изменения GVRP, запускаем команду "display gvrp statistics"

[LSW3]display gvrp statistics interface ethernet 0/0/1

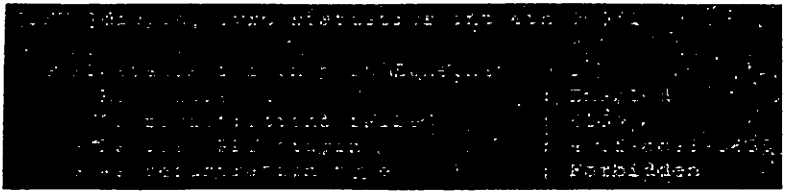

Рисунок 4.10. Результат режима Forbidden

Мы видим, что для типа регистрации GVRP установлено значение «запрещено» на интерфейсе Ethernet 0/0/1.

В режиме «Forbidden» только VLAN1 разрешено проходить через интерфейс Ethernet 0/0/1, а все остальные VLAN ограничены.

Чтобы просмотреть всю конфигурацию, используйте команду "display current-configuration".

Для проверки режима регистрации " Forbidden " выполните команду "display vlan" ".

[LSW3]display vlan

На рис. 4.11 показаны результаты VLAN на LSW3 после установки режима Forbidden.

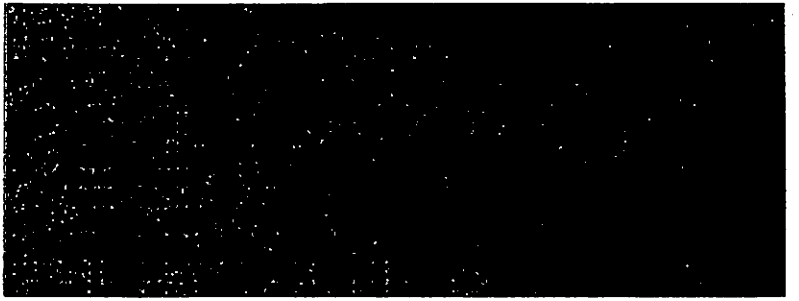

Рисунок 4.11. Проверка VLAN на LSW3 после установки режима forbidden

Отчет должен состоять из:

1. Название лабораторной работы, цель работы, краткие теоретические сведения;

2. Построить сеть по заданному варианту и произвести необходимые настройки;

3. Включите результаты в отчет;

4. Выводы.

Контрольные вопросы

1. Какова цель протокола GVRP?

2. Какие есть режимы регистрации в GVRP?

3. Какова функция режима Normal?

4. Какова функция режима Fixed?

5. Что делает режим Forbidden?

6. Что такое GARP и его функции.

7. Перечислите типы сообщений GARP.

8. Разница между Fixed и Forbidden режимами?

5-Лабораторная работа.

Настройка протокола STP/RSTP и изучение принципа его работы

Цель работы: Изучить принцип работы протоколов канального уровня STP/RSTP и их настройку.

Теоретическая часть

Протокол STP представляет собой пошаговый протокол модели OSI и основан на стандарте IEEE 802.1d. Протокол STP был разработан в 1985 году Радиа Перлман. Протокол имеет следующие характеристики: VBST (VLAN-Based Spanning Tree),RSTP, MSTP, STP.

Основное назначение протокола STP — сеть Ethernet.В произвольной топологии он предназначен для предотвращения образования петли в канале между несколькими коммутаторами, соединенными друг с другом. Протокол STP основан на создании логического дерева соединений между коммутаторами в сети. На вершине дерева находится корневой коммутатор (Root switch), а на следующих ветвях (ответвления), т.е. некорневые коммутаторы. Когда коммутаторы соединены друг с другом, использование основного магистрального канала позволяет физически подключить другие каналы, но логически автоматически заблокировать их (рис. 5.1). Процесс построения дерева состоит из следующих шагов:

- Выберите корневой коммутатор;
- Выбор корневых портов;
- Выбор назначенных портов.

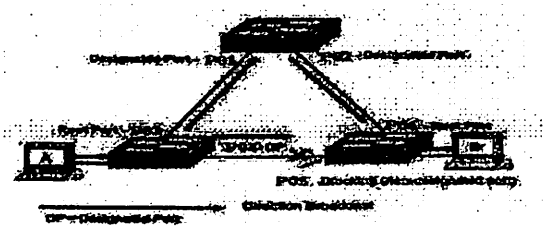

Рисунок 5.1. Типы портов в протоколе STP

При выборе нужного корневого коммутатора коммутатор выбирается на основе самого низкого значения приоритета или значения его идентификатора. Здесь значение идентификатора представляет собой MAC-адрес коммутатора, т. е. наименьшее значение — это корневой коммутатор в сети. Коммутаторы отправляют друг другу кадры Hello BPDU каждые 2 секунды и определяют, какой из них является корневым коммутатором. Значения привилегии и идентификатора идентификатора кадров, полученных от соседей, сравниваются и, если их значения выше, перестают претендовать на корневую позицию и начинают раздавать сообщение Hello BPDU победителю. Нам нужно знать, что если при сравнении привилегии остаются равнозначными, то корневой коммутатор выбирается путем сравнения их идентификаторов.

Протокол множественного связующего дерева (MSTP) описан в стандарте IEEE 802.1s и позже был дополнен IEEE 802.1Q-2003. Протокол MSTP — это улучшенная версия стандарта IEEE 802.1w (RSTP) для поддержки нескольких копий протокола STP. Это позволяет сети работать быстрее, балансируя нагрузку на сконфигурированную сеть VLAN. 802.1s Дополнение к стандарту MSTP является дополнением к стандарту 802.1Q.

Как правило, в коммутируемых сетях Ethernet резервные каналы используются для повышения надежности сети и для резервирования каналов. Однако использование избыточных каналов может создавать петли, которые дестабилизируют таблицу MAC-адресов и вызывают широковещательные штормы. В результате качество связи может ухудшиться, а услуги связи могут быть прерваны. Протокол связующего дерева (STP) используется для решения этих проблем. STP предотвращает образование петель. Устройства с активным STP обнаруживают сетевые петли, взаимодействуя друг с другом, и блокируют определенные порты для устранения петель. Результаты сравнения протоколов STP, RSTP и MSTP представлены в таблице 5.1.

Таблица 5.1 Результаты сравнения протоколов STP, RSTP и MSTP

[illegible]	[illegible]	[illegible]
STP	- создает дерево без петель, чтобы избежать широковещательных штормов и избыточных реализаций; - обеспечивает медленную сходимость.	Нет необходимости различать пользовательский или служебный трафик, и все VLAN имеют связующее дерево..
RSTP	- создает дерево без петель, чтобы избежать широковещательных штормов и избыточных реализаций; - обеспечивает быструю сходимость.	
MSTP	- создает несколько связующих деревьев, чтобы избежать широковещательных штормов и избыточных реализаций; - обеспечивает быструю сходимость; - Выполняет балансировку нагрузки между VLAN и перенаправляет трафик из разных VLAN по разным путям.	Пользовательский или служебный трафик должен быть дифференцированным и сбалансированным по нагрузке. Трафик из разных VLAN маршрутизируется через независимые связующие деревья..

Чтобы реализовать резервирование в сложной сети, сетевые администраторы обычно устанавливают несколько физических каналов связи между двумя устройствами, один из которых является основным каналом, а другие — резервными. Могут возникать широковещательные штормы или петли, вызывающие нестабильность таблицы MAC-адресов. Сетевой администратор может настроить RSTP для предотвращения образования петель после настройки сети. Когда в сети возникают петли, RSTP блокирует

порт для предотвращения образования петель. Протокол RSTP предотвращает бесконечное зацикливание пакетов, позволяя коммутатору обрабатывать пакеты.

Задание:

Учащиеся будут строить и настраивать сеть, используя параметры, перечисленные в Таблице 5.2.

Таблица 5.2. Варианты задания

№	
1.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
2.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
3.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
4.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
5.	Построить сеть, состоящую из 5 коммутаторов и 5 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
6.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
7.	Построить сеть, состоящую из 5 коммутаторов и 4 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
8.	Настройте сеть из 7 ПК и коммутаторов LSW1 и LSW2, LSW1 в качестве основного и LSW2 в качестве резервного (STP).
9.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
10.	Построить сеть, состоящую из 4 коммутаторов и 7 ПК. Настройте LSW1 как основной, LSW2 как резервный (STP).
11.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте LSW2 как основной, LSW3 как резервный (RSTP).
12.	Построить сеть, состоящую из 5 коммутаторов и 8 ПК. Настройте LSW2 как основной, LSW3 как резервный (RSTP).
13.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте LSW3 в качестве основного, LSW4 в качестве резервного (RSTP).

14.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте LSW3 в качестве основного, LSW4 в качестве резервного (RSTP).
15.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте LSW3 в качестве основного, LSW1 в качестве резервного (RSTP).
16.	Построить сеть, состоящую из 5 коммутаторов и 5 ПК. Настройте LSW2 как основной, LSW4 как резервный (RSTP).
17.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Настройте LSW1 как основной, LSW4 как резервный (RSTP).
18.	Построить сеть, состоящую из 5 коммутаторов и 9 ПК. Настройте LSW3 в качестве основного, LSW2 в качестве резервного (RSTP).
19.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте LSW4 как основной, LSW3 как резервный (RSTP).
20.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте LSW3 в качестве основного, LSW4 в качестве резервного (RSTP).
21.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте LSW3 в качестве основного, LSW4 в качестве резервного (STP).
22.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте LSW1 как основной, LSW2 как резервный (RSTP).
23.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Настройте LSW1 в качестве основного, LSW3 в качестве резервного (STP).
24.	Построить сеть, состоящую из 4 коммутаторов и 3 ПК. Настройте LSW2 как основной, LSW4 как резервный (RSTP).
25.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте LSW1 как основной, LSW3 как резервный (RSTP).
26.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте LSW3 в качестве основного, LSW1 в качестве резервного (STP).
27.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте LSW2 как основной, LSW3 как резервный (RSTP).
28.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Настройте LSW3 в качестве основного, LSW2 в качестве резервного (STP).

29.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте LSW1 как основной, LSW4 как резервный (RSTP).
30.	Построить сеть, состоящую из 3 коммутаторов и 8 ПК. Настройте LSW2 в качестве основного, LSW1 в качестве резервного (STP).

В данной лабораторной работе выполняются следующие задачи.

Назначение протокола STP (протокол связующего дерева):

- Настроить и проверить интерфейсы коммутатора LSW1, LSW2, LSW3 и LSW4, как показано на рисунке 5.2;

- настроить и проверить корневой коммутатор и корневые вторичные коммутаторы по протоколу STP;

- сделать каждый коммутатор корневым коммутатор (root) и изменить направления движения фрейма;

- Проанализируйте результаты каждой конфигурации коммутатора.

Назначение протокола RSTP (протокол связующего дерева):

- настроить и проверить интерфейсы коммутатора LSW1, LSW2, LSW3 и LSW4, как показано на рисунке 5.6;

- включить протокол RSTP;

- настроить и проверить основной (корневой) и резервный (корневой вторичный) коммутаторы;

- настроить значение пути для порта, чтобы порт был заблокирован;

- настройте RSTP, чтобы избежать зацикливания;

- включить функции безопасности;

- анализировать результаты каждой конфигурации коммутатора.

Порядок выполнения работы

Настройте базовые конфигурации коммутаторов LSW1, LSW2, LSW3, LSW4 в соответствии с топологией, показанной на рис. 5.2.

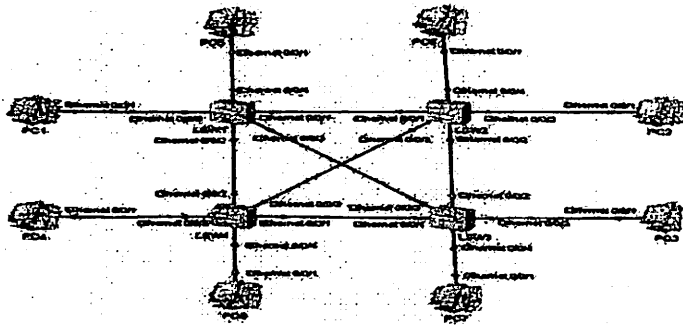

Рисунок 5.2. Исследуемая структура сети

Обычно функция STP коммутатора включена. Если STP выключен, включите его с помощью команды stp enable. Использование режимов STP {mstp, rstp, stp} Вы можете установить профили MSTP, RSTP, STP. Режим по умолчанию — MSTP.

Существует несколько способов определения коммутатора (корневого коммутатора), который является базовым в топологии сети:

- четкое назначение главного выключателя в сети;

- саф

Способ 1 Четко обозначьте коммутатор, который является ключевым для сети:

- stp root primar- используется для указания коммутатора (корневого коммутатора), который является основным для сети (например, [LSW1] stp root primary)

- stp root secondary- используется для указания резервного коммутатора для коммутатора (корневого коммутатора), который является основным для сети (например, [LSW2] stp root secondary).

Способ 2 Обозначте основному коммутатору приоритета коммутатора:

- stp priority priority - используется для обозначения коммутатора (корневого коммутатора), который является основным. Коммутатор у

которого приоритет ниже является основным коммутатором (например, *stp priority 4096*).

При установке приоритета обращают внимание на количество шагов, т.е. длина каждого шага 4096. Значение приоритета от 0 до 61440. В исходном случае все коммутаторы в сети будут иметь одинаковый (стандартный) приоритет (приоритет 32768). Устройство с одинаковыми значениями CIST Bridge и CIST Root/ERPC является корневым коммутатором.

При выполнении основной команды stp root значение приоритета корневого коммутатора автоматически устанавливается равным 0. Вы больше не можете изменить приоритет корневого устройства с помощью команды stp priority.

В этой лабораторной работе мы определяем коммутатор LSW1 как основной корневой коммутатор, а LSW2 — как резервный коммутатор. Сперва включим режим STP на всех коммутаторах.

Настраиваем коммутатор LSW1.

<Huawei>system-view

[Huawei]sysname LSW1

[LSW1]stp mode stp

Настраиваем коммутатор LSW2.

<Huawei>system-view

[Huawei]sysname LSW2

[LSW2]stp mode stp

Настраиваем коммутатор LSW3.

<Huawei>system-view

[Huawei]sysname LSW3

[LSW3]stp mode stp

Настраиваем коммутатор LSW4.

<Huawei>system-view

[Huawei]sysname LSW4

[LSW4]stp mode stp

Даже если STP автоматически выберет корневой коммутатор, мы сначала назначим коммутатор, расположенный ближе к центру сети. Среди коммутаторов в сетевой топологии, упомянутых выше, основным корневым коммутатором (root) является LSW1. Потому что в этой топологии MAC-адрес LACW1 меньше, чем у других коммутаторов. Для проверки это делается в LSW1 с помощью команды display stp. В результате мы можем узнать является MAC-адрес коммутатора LSW1 или основного коммутатора (CIST Bridge) (рис. 5.3).

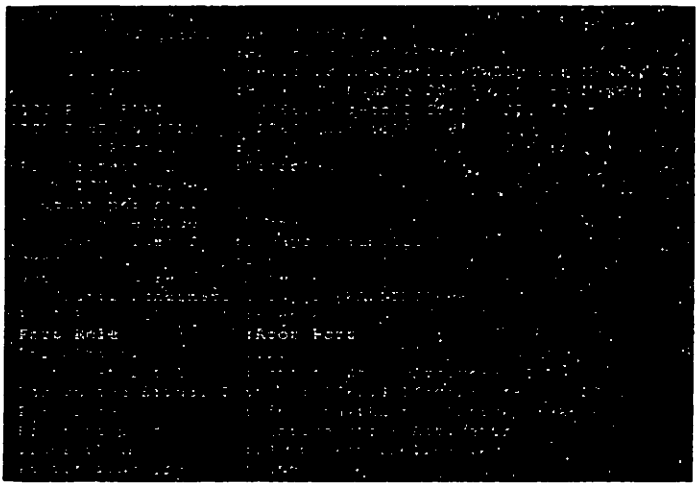

Рисунок 5.3. Результаты Stp на LSW1

Теперь мы настраиваем коммутатор LSW1 в качестве корневого (root) коммутатора и LSW2 в качестве резервного коммутатора..

[LSW1]stp root primary

[LSW2]stp root secondary

Чтобы просмотреть краткое описание STP, запустите «display stp brief». Информация о протоколе STP в коммутаторе LSW1 показана на рис. 5.4, а в коммутаторе LSW2 показана на рис. 5.5.

Рисунок 5.4. Stp данные на коммутаторе LSW1

Рисунок 5.5. Stp данные на коммутаторе LSW2

Чтобы просмотреть состояние STP порта, отобразите «display stp interface Ethernet 0/0/1».используется команда.

Как только вышеуказанные сетевые параметры установлены, коммутаторы отправляют сообщение друг другу и выбирают корневой коммутатор для сети LAN. Для просмотра текущих конфигураций коммутатор использует команду display stp.

Пример протокола RSTP

Настройте интерфейсы коммутатора LSW1, LSW2, LSW3 и LSW4, как показано на рис. 5.6.

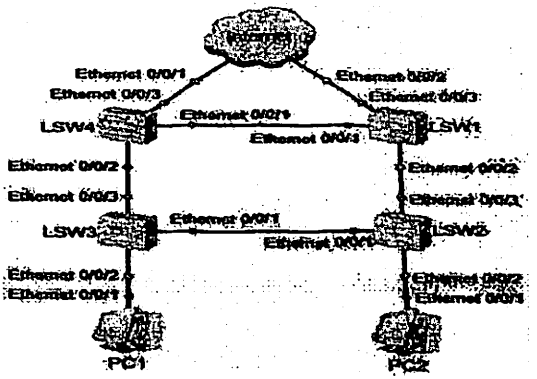

Рисунок 5.6. Исследовал топологию сети

Давайте настроим основные функции RSTP. Настраиваем протокол RSTP на коммутаторах LSW1, LSW2, LSW3 и LSW4.

Настраиваем LSW1 для работы в режиме RSTP

<Huawei>system-view

[Huawei]sysname LSW1

[LSW1]stp mode rstp

Настраиваем LSW2 для работы в режиме RSTP

<Huawei>system-view

[Huawei]sysname LSW2

[LSW2]stp mode rstp

Настраиваем LSW3 для работы в режиме RSTP

<Huawei>system-view

[Huawei]sysname LSW3

[LSW3]stp mode rstp

Настраиваем LSW4 для работы в режиме RSTP

<Huawei>system-view

[Huawei]sysname LSW4

[LSW4]stp mode rstp

Настраиваем основной (root) и резервный (root secondary) коммутаторы. Мы настраиваем LSW1 в качестве основного коммутатора и LSW4 в качестве резервного коммутатора.

Установим LSW1 в качестве основного.

[LSW1]stp root primary

Команда display stp используется для проверки того, чтобы LSW1 был установлен как ведущий. Результат STP на LSW1 показан на рисунке 5.7.

[LSW1]display stp

Рисунок 5.7. Результат STP на LSW1

Установим LSW4 в качестве резервной копии

[LSW4]stp root secondary

Команда display stp используется для проверки настроек stp на коммутаторе LSW4. Результат STP в LSW4 показан на рисунке 5.7.

[LSW4]display stp

Рисунок 5.8. Результат STP на LSW4

Настройка пути для порта, который будет заблокирован.

Диапазон значений пути зависит от алгоритма. В качестве примера используется запатентованный алгоритм Huawei. Мы указываем 20000 в качестве значения пути для блокируемых портов. Устройства-коммутаторы в одной сети должны использовать один и тот же алгоритм для расчета значения пути порта.

Настраиваем LSW1 для расчета значения пути

[LSW1]stp pathcost-standart legacy

Результат значения пути в LSW1 (показан на рис. 5.9) можно просмотреть с помощью команды "display this".

Рисунок 5.9. Просмотр значения пути в LSW1

Мы настраиваем LSW2 для вычисления значения пути.

[LSW2]stp pathcost-standart legacy

Настраиваем LSW3 для расчета значения пути

[LSW3]stp pathcost-standart legacy

Установите значение пути Ethernet0/0/1 на 20000 на LSW3.

[LSW3]interface Ethernet 0/0/1

[LSW3-Ethernet0/0/1]stp cost 20000

[LSW3-Ethernet0/0/1]quit

Результат значения пути в LSW3 показан на рисунке 5.10.

Рисунок 5.10. Просмотр значения пути в LSW3

Мы настраиваем LSW4 для вычисления значения пути.

[LSW4]stp pathcost-standart legacy

Чтобы избежать петли, мы включаем RSTP. Мы устанавливаем порты, подключенные к компьютеру, как edged-порты. На LSW2 настраиваем Ethernet 0/0/2 как пограничный порт .

[LSW2]interface Ethernet 0/0/2

[LSW2-Ethernet0/0/2]stp edged-port enable

[LSW2-Ethernet0/0/2]quit

(Произвольно) Настройте безопасность BPDU на коммутаторе LSW2.

[LSW2]stp bpdu-protection

На LSW3 настраиваем Ethernet 0/0/2 как пограничный порт.

[LSW3]interface Ethernet 0/0/2

[LSW3-Ethernet0/0/2]stp edged-port enable

[LSW3-Ethernet0/0/2]quit

(Произвольно) Настройте безопасность BPDU на коммутаторе LSW3.

[LSW3]stp bpdu-protection

Если граничные порты подключены к сетевым устройствам с включенной защитой STP и BPDU, граничные порты отключаются, а их атрибуты остаются неизменными после получения BPDU. RSTP включен на каждом коммутационном устройстве (например, [LSW1] stp enable).

Включаем функции безопасности. Корневая защита используется для порта, назначенного корневым коммутатором.

Настраиваем безопасность на интерфейсе Ethernet0/0/1 главного коммутатора LSW1

[LSW1]interface Ethernet 0/0/1

[LSW1-Ethernet0/0/1]stp root-protection

[LSW1-Ethernet0/0/1]quit

Настраиваем безопасность на интерфейсе Ethernet0/0/2 главного коммутатора LSW1

[LSW1]interface Ethernet 0/0/2

[LSW1-Ethernet0/0/2]stp root-protection

[LSW1-Ethernet0/0/2]quit

После завершения настройки и стабильной топологии сети выполните следующие действия, чтобы проверить конфигурацию. Мы запускаем команду «display stp brief» на LSW1, чтобы увидеть состояние и тип безопасности портов. Результат защиты порта на коммутаторе LSW1 показан на рисунке 5.11.

Рисунок 5.11. Проверка безопасности порта на LSW1

После настройки LSW1 в качестве основного коммутатора порты Ethernet0/0/2 и Ethernet0/0/1, подключенные к LSW2 и LSW4, становятся защищенными портами. Чтобы проверить состояние Ethernet0/0/1, мы

запускаем команду «display stp interface Ethernet0/0/1 brief» на LSW2. (рис. 5.12)

Рисунок 5.12. Проверка состояния порта на LSW2

Ethernet0/0/1 становится назначенным портом и находится в состоянии FORWARDING. Для проверки состояния порта на LSW3 запускаем команду "display stp brief "

Рисунок 5.13. Проверка состояния порта на LSW3

Мы видим, что Ethernet0/0/1 становится альтернативным портом и находится в состоянии DISCARDING, Ethernet0/0/3 становится корневым портом и находится в состоянии FORWARDING.

Отчет должен состоять из:

1. Название лабораторной работы, цель работы, краткие теоретические сведения;

2. Построить сеть по заданному варианту и произвести необходимые настройки;

3. Включить результаты в отчет;

4. Выводы.

Контрольные вопросы

1. Назначение и виды протокола STP.

2. Как установить главный выключатель?

3. Как назначить резервный переключатель?

4. Как выбрать главный выключатель?

5. Объясните корневой порт.

6. Объясните назначенный порт.

7. Объясните альтернативный порт.

8. Зачем нужна защита BPDU?

6-Лабораторная работа.

Интерфейс Ethernet и конфигурация link

Цель работы: Изучить интерфейс Ethernet и настроить конфигурацию канала.

Теоретическая часть

Объединение каналов (link aggregation), также называемая Eth-Trunk, представляет собой технологию, которая позволяет объединять несколько физических каналов в один логический канал. Такое сочетание позволяет повысить пропускную способность и надежность канала. Объединение каналов можно настроить между двумя коммутаторами, между коммутатором и маршрутизатором, а также между коммутатором и хостом. Соответствующие каналы перекрывают друг друга и повышают надежность.

По мере расширения сети пользователи предъявляют все более высокие требования к пропускной способности и надежности магистрали Ethernet. Первоначально пользователи использовали высокоскоростные устройства для замены старых устройств, чтобы увеличить пропускную способность сети. Однако это решение дорого и негибко.

Объединение каналов помогает увеличить пропускную способность за счет объединения группы физических интерфейсов в один логический интерфейс без обновления устройства. Кроме того, агрегация каналов обеспечивает механизмы резервирования каналов, что значительно повышает их надежность.

Объединение каналов имеет следующие преимущества:

- увеличивается пропускная способность;

- пропускная способность интерфейса объединения каналов является суммой пропускных способностей интерфейсов-участников;

- высокая надежность;

Когда количество активных интерфейсов падает ниже этого порога, Eth-Trunk отключается. Это гарантирует минимальную доступную пропускную способность сети для Eth-Trunk.

Например, если Eth-Trunk должен обеспечивать минимальную пропускную способность 2 Гбит/с, а каждый канал-член имеет пропускную способность 1 Гбит/с, минимальное количество каналов-членов Up равно 2 или должно быть больше.

- Режим объединения соединений;

Существует два режима агрегации каналов: ручной и LACP (протокол управления агрегацией каналов). Различия (сравнения) режимов объединения каналов представлены в таблице 6.1.

. Таблица 6.1 Различия между режимами объединения каналов

[illegible]	Ручной режим	Режим LACP
Описание	Вы должны вручную создать Eth-Trunk и добавить в Eth-Trunk интерфейсы-члены. В этом режиме LACP не требуется.	Eth-Trunk создан на основе LACP. LACP предоставляет стандартный механизм согласования для коммутационного устройства, так что коммутационное устройство может автоматически создавать и инициализировать агрегированные каналы в соответствии со своей конфигурацией. Как только объединенный канал установлен, LACP отвечает за поддержание состояния канала. Когда условие агрегации каналов изменяется, LACP изменяет или удаляет агрегированные каналы.
LACP требуется	Нет	Да
Обмен данными	По умолчанию все каналы являются	Как правило, некоторые каналы являются активными.

	активными каналами. В передаче данных участвуют все активные каналы. При отказе одного активного канала трафик распределяется между оставшимися активными каналами..	В передаче данных участвуют все активные каналы. Если активный канал выходит из строя, система выбирает канал среди неактивных каналов в качестве активного канала. То есть количество каналов, задействованных в передаче данных, остается неизменным.
Поддержка объединения каналов между устройствами	Нет	Да
Определение ошибок (неисправностей).	Этот режим может обнаруживать только сбои в каналах-членах, но не может обнаруживать другие ошибки, такие как сбои стека каналов и неправильные соединения каналов..	Этот режим может обнаруживать пропадание каналов и другие ошибки, такие как сбои стека каналов и неправильные соединения каналов..

- Режимы объединения каналов, поддерживаемые устройством;

Внутри устройство — интерфейсы-члены Eth-Trunk расположены на одном устройстве.

Межстековое устройство — интерфейсы-члены Eth-Trunk расположены на устройствах-членах стека.

Между устройствами (Inter-device): Объединение каналов между устройствами принадлежит E-Trunk. E-Trunk позволяет объединять каналы между несколькими устройствами на основе протокола LACP.

Задание:

Студенты будут строить и настраивать сеть, используя параметры, перечисленные в Таблице 6.2.

Таблица 6.2. Параметры задания

№	Задание
1.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте режим LACP между LSW1 и LSW2.
2.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте режим LACP между LSW1 и LSW2.
3.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте режим LACP между LSW2 и LSW3.
4.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте режим LACP между LSW2 и LSW3.
5.	Построить сеть, состоящую из 5 коммутаторов и 5 ПК. Настройте режим LACP между LSW3 и LSW2.
6.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте режим LACP между LSW3 и LSW4.
7.	Построить сеть, состоящую из 5 коммутаторов и 4 ПК. Настройте режим LACP между LSW1 и LSW2.
8.	Построить сеть, состоящую из 2 коммутаторов и 7 ПК. Настройте режим LACP между LSW1 и LSW2.
9.	Построить сеть, состоящую из 4 коммутаторов, 5 ПК. Настройте режим LACP между LSW1 и LSW2.
10.	Построить сеть, состоящую из 4 коммутаторов и 7 ПК. Настройте режим LACP между LSW3 и LSW4.
11.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте режим LACP между LSW2 и LSW3.
12.	Построить сеть, состоящую из 5 коммутаторов и 8 ПК. Настройте режим LACP между LSW4 и LSW3.
13.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте режим LACP между LSW3 и LSW4.
14.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте режим LACP между LSW1 и LSW2.
15.	Построить сеть, состоящую из 3 коммутаторов и 6 ПК. Настройте режим LACP между LSW1 и LSW3.
16.	Построить сеть, состоящую из 5 коммутаторов и 5 ПК. Настройте режим LACP между LSW3 и LSW5.
17.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Настройте режим LACP между LSW4 и LSW2.
18.	Построить сеть, состоящую из 5 коммутаторов и 9 ПК. Настройте режим LACP между LSW4 и LSW2.

19.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте режим LACP между LSW1 и LSW2.
20.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте режим LACP между LSW1 и LSW3.
21.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте режим LACP между LSW1 и LSW2.
22.	Построить сеть, состоящую из 4 коммутаторов и 4 ПК. Настройте режим LACP между LSW3 и LSW4.
23.	Построить сеть, состоящую из 4 коммутаторов и 5 ПК. Настройте режим LACP между LSW1 и LSW2.
24.	Построить сеть, состоящую из 4 коммутаторов и 3 ПК. Настройте режим LACP между LSW3 и LSW2.
25.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте режим LACP между LSW2 и LSW3.
26.	Построить сеть, состоящую из 3 коммутаторов и 5 ПК. Настройте режим LACP между LSW1 и LSW3.
27.	Построить сеть, состоящую из 4 коммутаторов и 6 ПК. Настройте режим LACP между LSW1 и LSW2.
28.	Построить сеть, состоящую из 3 коммутаторов и 9 ПК. Настройте режим LACP между LSW2 и LSW1.
29.	Построить сеть, состоящую из 4 коммутаторов и 8 ПК. Настройте режим LACP между LSW4 и LSW2.
30.	Построить сеть, состоящую из 3 коммутаторов и 8 ПК. Настройте режим LACP между LSW1 и LSW2.

В данной лабораторной работе решаются следующие задачи:

- Настроить и проверить интерфейсы коммутаторов LSW3 и LSW4, как показано на рисунке 6.3;

- Создать Eth-Trunk и настроить Eth-Trunk для работы в режиме LACP для выполнения объединения каналов;

- Добавление интерфейсов-членов в Eth-Trunk;

- Установить приоритет системы LACP;

- Установить верхний предел количества активных интерфейсов для повышения надежности;

- Дать приоритет интерфейсу LACP и определить активные интерфейсы, чтобы интерфейсы с более высоким приоритетом выбирались в качестве активных интерфейсов.

Порядок выполнения работы

В настоящее время корпоративная сеть работает в едином широковещательном домене, в результате чего все узлы сети получают большой объем трафика. Администратор должен попытаться контролировать поток трафика на канальном уровне, применяемом к коммутаторам LSW3 и LSW4.

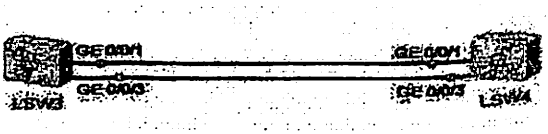

Рисунок 6.3. Исследуемая структура сети

Настроим коммутатор LSW3.

Создаем Eth-Trunk 1 на коммутаторе LSW3 и настраиваем Eth-Trunk 1 для работы в режиме LACP.

<HUAWEI> system-view

[HUAWEI] sysname LSW3

[LSW3] interface eth-trunk 1

[LSW3-Eth-Trunk1] mode lacp-static

[LSW3-Eth-Trunk1] quit

Добавьте интерфейсы-участники в Eth-Trunk 1 на LSW3.

[LSW3] interface gigabitethernet 0/0/1

[LSW3-GigabitEthernet1/0/1] eth-trunk 1

[LSW3-GigabitEthernet1/0/1] quit

[LSW3] interface gigabitethernet 0/0/3

[LSW3-GigabitEthernet0/0/3] eth-trunk 1

[LSW3-GigabitEthernet0/0/3] quit

Чтобы сделать LSW3 основным (Actor), устанавливаем приоритет LACP на коммутаторе LSW3 равным 100.

[LSW3] lacp priority 100

Устанавливаем верхний предел количества активных интерфейсов на коммутаторе LSW3 равным 2.

[LSW3] interface eth-trunk 1

[LSW3-Eth-Trunk1] max active-linknumber 2

[LSW3-Eth-Trunk1] quit

Выставляем LACP приоритет интерфейса и определяем активные каналы на коммутаторе LSW3

[LSW3] интерфейс gigabitethernet 1/0/1

[LSW3-GigabitEthernet1/0/1] приоритет lacp 100

[LSW3-GigabitEthernet1/0/1] выйти

[LSW3] интерфейс gigabitethernet 1/0/2

[LSW3-GigabitEthernet1/0/2] приоритет lacp 100

[LSW3-GigabitEthernet1/0/2] выйти

Используем команду "display eth-trunk 1" для проверки настроек. Результат настроек в LSW3 показан на рисунке 6.4.

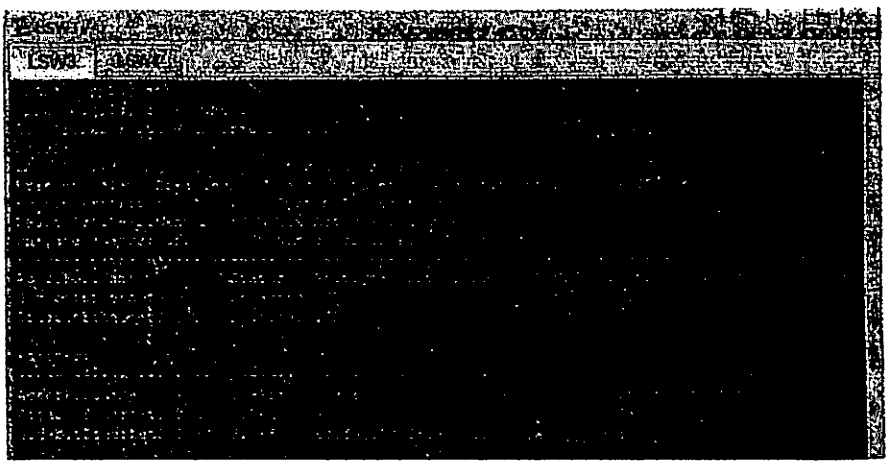

Рисунок 6.4. Проверка настроек в LSW3

Настроим коммутатор LSW4.

Создаем Eth-Trunk 1 на коммутаторе LSW4 и настраиваем Eth-Trunk 1 для работы в режиме LACP.

<HUAWEI> system-view

[HUAWEI] sysname LSW4

[LSW4] interface eth-trunk 1

[LSW4-Eth-Trunk1] mode lacp-static

[LSW4-Eth-Trunk1] quit

Добавьте интерфейсы-участники в Eth-Trunk 1 на LSW4.

[LSW4] interface gigabitethernet 0/0/1

[LSW4-GigabitEthernet1/0/1] eth-trunk 1

[LSW4-GigabitEthernet1/0/1] quit

[LSW4] interface gigabitethernet 0/0/3

[LSW4-GigabitEthernet0/0/3] eth-trunk 1

[LSW4-GigabitEthernet0/0/3] quit

Используем команду "display eth-trunk 1" для проверки настроек. Результат настроек в LSW4 показан на рисунке 6.5.

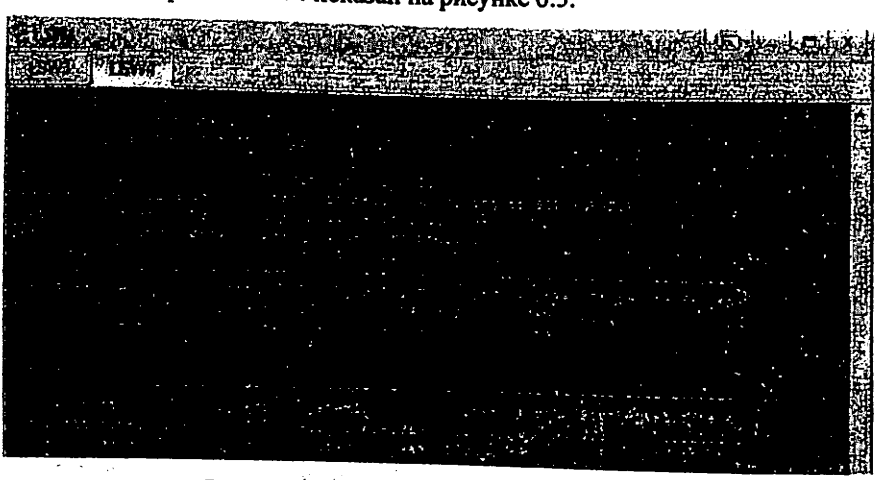

Рисунок 6.5. Проверка настроек на LSW4

Предыдущие данные показывают, что системный приоритет LACP LSW3 выше системного приоритета LACP LSW4. Мы видим, что активные интерфейсы GigabitEthernet0/0/1 и GigabitEthernet0/0/3 находятся в выбранном состоянии.

Отчет должен состоять из:

1. Название лабораторной работы, цель работы, краткие теоретические сведения;

2. Построить сеть по заданному варианту и произвести необходимые настройки;

3. Включить результаты в отчет;

4. Выводы

Контрольные вопросы

1. Что такое конфигурация ссылок?
2. Что такое протокол LACP?
3. Зачем нужно объединять каналы?
4. Какие еще протоколы, похожие на LACP, вы знаете?
5. Как статически настроен LACP?
6. Как установить системный приоритет в LACP?
7. Какая команда используется для проверки eth-trunk?
8. Как добавить интерфейсы в eth-trunk?
9. Как влияет на состояние канала увеличение количества Eth-транков?
10. В чем разница между режимом ручной настройки и режимом LACP?
11. Какова функция команды "*mode lacp-static*" ?
12. Какова функция команды "*lacp priority 100*" ?
13. Что делает команда "*eth-trunk 1*" ?
14. Какова функция команды "*max active-linknumber 2*" ?
15. Какова цель команды "*interface eth-trunk 1*" ?

Лабораторная работа №7

Объединение локальных вычислительных сетей на базе маршрутизаторов и использование статической маршрутизации.

Цель работы: Объединение локальных вычислительных сетей на базе маршрутизаторов с использованием статической маршрутизации.

Теоретическая часть

Маршрутизаторы (уровень 3 сетевой модели OSI) используются для соединения нескольких сетей на уровне сети. Стек протоколов TCP/IP обеспечивает два типа маршрутизации: статическую и динамическую.

Статическая маршрутизация означает, что таблицы маршрутизации настраиваются системным администратором вручную на основе команды route. Этот тип метода маршрутизации рекомендуется, когда сеть взаимодействует с одной или двумя другими сетями. Однако если сеть подключена к большому количеству сетей, то количество шлюзов резко возрастает, а ручное обслуживание таблиц маршрутизации занимает значительное время. При динамической маршрутизации таблицы маршрутизации автоматически обновляются демонами (постоянно (непрерывно) работающим программным обеспечением, определяющим сетевые маршруты для передачи данных). Демоны маршрутизации постоянно получают уведомления от других демонов маршрутизации, поэтому они постоянно обновляют свои таблицы маршрутизации. Gated и routed являются примерами стандартных программ этого типа.

В отличие от динамической маршрутизации, статические маршруты фиксированы и не меняются при изменении или перенастройке сети. Статическая маршрутизация и динамическая маршрутизация не исключают друг друга.

Статическая маршрутизация и динамическая маршрутизация не исключают друг друга. Как динамическая маршрутизация, так и статическая маршрутизация обычно используются на маршрутизаторе, чтобы максимизировать эффективность маршрутизации и обеспечить резервное копирование в случае невозможности обмена информацией динамической маршрутизации.

На сегодняшний день существует два типа IP-адресов (интернет-протокола): IPv4 (интернет-протокол версии 4) и IPv6 (интернет-протокол версии 6). По этому протоколу можно не только обращаться к элементам сети Интернет, но и назначать уникальные адреса пользователям в локальной сети. Благодаря адресации пользователи сети отличаются друг от друга, и пакеты гарантированно доходят до указанного пользователя. В версии 4 протокола IP (IPv4) сетевой адрес имеет длину 32 бита. Количество доступных адресов составляет 232 уровня. Для удобства чтения сетевые адреса IPv4 разделены на 4 байта (октета) с помощью точек, и каждый байт в IP-адресе записывается как десятичное число. Сетевой адрес (IP-адрес) должен состоять из двух частей: номера сети и номера узла в этой сети. IP-адреса делятся на 5 классов (классы A, B, C, D и E), каждый из которых имеет ограничение на количество сетей и номер узла.

Таблица 7.1

Класс	Деление	Диапазон	Адрес сети	Адрес узла
A	0111 1111	1.0.0.0 126.255.255.255	исходный 8 bit	последний 24 bit
B	1011 1111	128.0.0.0 191.255.255.255	исходный 16 bit	последний 16 bit
C	1101 1111	192.0.0.0	исходный 24 bit	последний 8

		223.255.255.255		bit
D	1110 1111	224.0.0.0 239.255.255.255	Адреса отправки многоадресных данных	
E	1111 1111	240.0.0.0 255.255.255.255	Зарезервированные адреса	

IP-адреса класса A зарезервированы для очень больших сетей, IP-адреса класса B предназначены для сетей среднего размера, а IP-адреса класса C являются наиболее часто используемыми адресами и зарезервированы для небольших сетей (известных как локальные сети). Например, 192.168.10.1/24.

Протокол IPv6 считается протоколом нового поколения и имеет широкий спектр возможностей, в отличие от протокола IPv4. В версии 6 протокола IP (IPv6) сетевой адрес имеет длину 128 бит. Количество доступных адресов составляет 2128 уровней. В IPv6 сетевые адреса делятся на 8 групп (октетов) по 16 байтов в каждой с использованием точек. Также каждый байт в IP-адресе записывается в шестнадцатеричном формате, в отличие от IPv4 (из-за большого количества доступных адресов и неудобства предыдущего формата записи). Например, 8000:0000:0000:0000:0127:AB68:CD45:EF15.

Расчет количества хостов и подсетей на основе IP-адреса и маски

IP-адреса используются для идентификации устройств в сети. Каждому сетевому устройству (включая компьютеры, серверы, маршрутизаторы, принтеры и т. д.) должен быть присвоен IP-адрес для связи с другими устройствами по сети. Такие устройства в сети называются хостами. Маска подсети определяет максимальное количество хостов, которые могут быть в данной сети. Кроме того, маски подсети позволяют разделить одну сеть на несколько подсетей (подсетей).

Представляем IP-адреса

Одна часть IP-адреса — это номер сети, а другая часть — идентификатор хоста. Точно так же, как разные дома на одной улице имеют

одно и то же название улицы по своему адресу, хосты в сети имеют общий сетевой номер по своему адресу. Точно так же, как разные дома имеют свой номер дома, каждый хост в сети имеет уникальный идентификационный номер — идентификатор хоста. Номер сети используется маршрутизаторами (маршрутизаторами, интернет-концентраторами) для маршрутизации (пересылки) пакетов в нужные сети, а идентификатор хоста идентифицирует конкретное устройство в сети, на которое должны быть доставлены пакеты.

Структура IP-адреса

IP-адрес состоит из четырех частей, записанных в виде десятичных чисел, разделенных точками (например, 192.168.1.1). Каждая из этих четырех частей называется октетом. Октет — это восемь двоичных цифр (например, 11000000 или 192 в десятичном виде). Таким образом, каждый октет может принимать двоичные (числовые) значения от 00000000 до 11111111 или от 0 до 255 в десятичном виде. На рис. 7.1 показан пример IP-адреса, где первые три октета (192.168.1) — это номер сети, а четвертый октет (16) — идентификатор хоста.

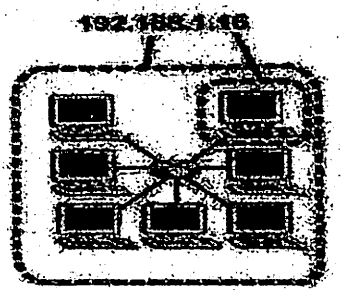

Рисунок 7.1. Номер сети и идентификатор хоста

Количество двоичных цифр в IP-адресе, соответствующем номеру сети, и количество цифр в адресе, соответствующем каждому идентификатору хоста, могут различаться в зависимости от маски подсети.

Частные IP-адреса

Каждый хост в Интернете должен иметь уникальный адрес. Если ваши сети изолированы от Интернета (например, соединение двух филиалов), вы без проблем можете использовать любой IP-адрес для хостов. Однако организация IANA (Управление по присвоению номеров в Интернете) выделила следующие три блока IP-адресов для определенных сетей:

А/10.0.0.0 - 10.255.255.255

Б/172.16.0.0 - 172.31.255.255

С/192.168.0.0 - 192.168.255.255

Назначенные частные IP-адреса подсети иногда называют «серыми» адресами.

IP-адреса можно получить от IANA, интернет-провайдера (ISP), или вы можете назначить свои собственные из диапазона адресов частной сети.

Сетевые маски

Маска сети используется для определения того, какие биты являются частью номера сети, а какие — частью идентификатора хоста (с помощью логической операции И).

Маска подсети содержит 32 бита. Если бит в маске подсети равен «1», соответствующий бит в IP-адресе является частью номера сети. Если бит в маске подсети равен «0», соответствующий бит в IP-адресе является частью идентификатора хоста.

Пример извлечения номера сети и идентификатора хоста из IP-адреса (например, 192.168.1.2) приведен в таблице 7.2.

Таблица 7.2

	1-й октет (192)	2-й октет (168)	3-й октет (1)	4-й октет (2)
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Сетевая маска	11111111	11111111	11111111	00000000
Номер сети	11000000	10101000	00000001	
Идентификатор хоста				00000010

Маски подсети всегда состоят из набора единиц, начиная с крайнего левого бита маски, за которым следует ряд нулей, всего 32 бита. Сетевую маску можно определить как количество битов в адресе, представляющем номер сети (количество битов со значением «1»).

Например, «8-битная маска» — это маска, в которой 8 бит равны 1, а остальные 24 бита равны 0 (11111111.00000000.00000000.00000000).

Маски подсети пишутся через точку с запятой, как и IP-адреса. В следующих примерах показаны двоичные и десятичные представления 8-битных, 16-битных, 24-битных и 29-битных масок подсети (таблица 7.3).

Таблица 7.3

	1-й октет в двоичном	2-й октет в двоичном	3-й октет в двоичном	4-й октет в двоичном	в десятичном
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
25-битная маска	11111111	11111111	11111111	10000000	255.255.255.128
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248
30-битная маска	11111111	11111111	11111111	11111100	255.255.255.252

Размер сети

Количество битов в номере сети определяет максимальное количество хостов, которые могут быть в этой сети. Чем больше битов в номере сети, тем меньше битов остается для идентификатора хоста в адресе. IP-адрес с

идентификатором хоста, состоящим из одних нулей, является IP-адресом сети (например, 192.168.1.0 /24-битная маска подсети). IP-адрес со всеми идентификаторами узлов является широковещательным адресом этой сети (например, 192.168.1.255 / с 24-битной маской подсети). Поскольку эти два IP-адреса нельзя использовать в качестве индивидуальных идентификаторов узлов, максимально возможное количество узлов в сети рассчитывается следующим образом (таблица 7.4).

Таблица 7.4

Сетевая маска		Размер идентификатора хоста		Максимальное количество хостов
8 bit	255.0.0.0	24 bit	2^{24}-2	16777214
16 bit	255.255.0.0	16 bit	2^{16}-2	65534
24 bit	255.255.255.0	8 bit	2^{8}-2	254
25 bit	255.255.255.128	7 bit	2^{7}-2	126
29 bit	255.255.255.248	3 bit	2^{3}-2	6
30 bit	255.255.255.252	2 bit	2^{2}-2	2

Формат записи

Поскольку маска всегда представляет собой левостороннюю последовательность единиц, дополненную до 32 битов нулями, вы можете просто отображать количество единиц вместо того, чтобы записывать значение каждого октета. Обычно это записывается как «/» после количества битов 1 в адресе и маске.

Например, адрес 192.1.1.0/25 (адрес 192.1.1.0 с маской 255.255.255.128). Возможные маски подсети в обоих форматах показаны в таблице 7.5.

Таблица 7.5

Сетевая маска	Формат записи	Последний октет	Полный октет

		(в двоичном формате)	(в десятичной системе)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Формирование сетей (subnet).

Одну сеть можно разделить на несколько с помощью сетей. В следующем примере сетевой администратор создает две сети, чтобы изолировать группу серверов от других устройств в целях безопасности. В этом примере сеть компании имеет адрес 192.168.1.0.

Первые три октета адреса (192.168.1) — это номер сети, а остальные октеты — идентификатор хоста, что позволяет максимальное количество хостов в сети 28 — 2 = 254. Изображение сети компании до ее разделения на малые сети показано на рисунке 7.2 ниже.

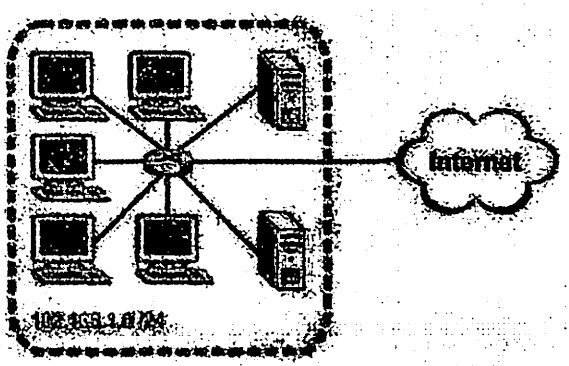

Рисунок 7.2. Пример формирования сети: ее состояние до разделения на мелкие сети

Вы можете немного «позаимствовать» идентификатор хоста, чтобы разделить сеть 192.168.1.0 на две отдельные подсети. В этом случае маска подсети становится 25-битной (255.255.255.128 или /25).

Бит «заимствованного» идентификатора хоста может быть равен нулю или единице, что дает нам две подсети: 192.168.1.0/25 и 192.168.1.128/25.

Состояние сети компании после разделения на малые сети показано на рис. 7.3. Теперь он содержит две подсети: A и B.

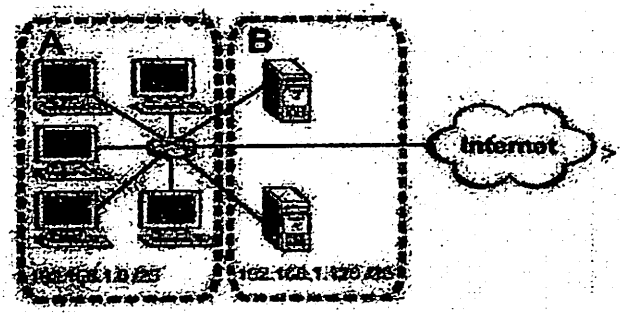

Рисунок 7.3. Состояние после разделения на сети

В 25-битной подсети 7 бит зарезервированы для идентификатора хоста, поэтому в каждой подсети может быть максимум 27 - 2 = 126 хостов (все нули — это идентификатор хоста самой подсети, а все единицы — broadcast адрес). Адрес 192.168.1.0 с маской 255.255.255.128 — это адрес сети A, адрес 192.168.1.127 с маской 255.255.255.128 — ее broadcast адрес. Таким образом, наименьший IP-адрес, который может быть назначен текущему хосту в сети A, равен 192.168.1.1, а наибольший — 192.168.1.126. Точно так же диапазон идентификаторов хостов для сети B может быть указан от 192.168.1.129 до 192.168.1.254.

Пример: Разделить на четыре подсети

В предыдущем примере рассматривалось использование 25-битной сетевой маски для разделения 24-битного адреса на две сети. Точно так же для разделения 24-битного адреса на четыре сектора требуется

«заимствование» двух битов идентификатора хоста для получения четырех возможных комбинаций (00, 01, 10 и 11).

Маска сети состоит из 26 бит, т.е. 255.255.255.192 (11111111.11111111.11111111.11000000). Каждая сеть содержит 6 бит идентификатора хоста, что дает в общей сложности 26 - 2 = 62 хоста на сеть (идентификатор хоста, состоящий из всех нулей, — это сама сеть, а все единицы — сетевой broadcast адрес). Первый сетевой адрес указан в таблице 7.6.

Таблица 7.6

IP-адрес/сетевая маска	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	00000000
Сетевая маска (в двоичном формате)	11111111.11111111.11111111.	11000000
Сетевой адрес 192.168.1.0	Наименьший идентификатор хоста: 192.168.1.1.	
Адрес Broadcast 192.168.1.63	Самый большой идентификатор хоста — 192.168.1.62.	

Второй сетевой адрес указан в таблице 7.7.

Таблица 7.7

IP-адрес/сетевая маска	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	01000000
Сетевая маска (в двоичном формате)	11111111.11111111.11111111.	11000000
Сетевой адрес 192.168.1.64.	Наименьший идентификатор хоста: 192.168.1.65.	
Broadcast адрес: 192.168.1.127.	Самый большой идентификатор хоста — 192.168.1.126.	

Третий сетевой адрес приведен в таблице 7.8.

Таблица 7.8

IP-адрес/сетевая маска	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	01000000
Сетевая маска (в двоичном формате)	11111111.11111111.11111111.	11000000
Сетевой адрес 192.168.1.128.	Наименьший идентификатор хоста: 192.168.1.129.	
Broadcast адрес: 192.168.1.191.	Самый большой идентификатор хоста — 192.168.1.190.	

Четвертый сетевой адрес приведен в таблице 7.9.

IP-адрес/сетевая маска	Номер сети	Значение последнего октета
IP-адрес (десятичный)	192.168.1.	192
IP-адрес (двоичный)	11000000.10101000.00000001.	11000000
Сетевая маска (в двоичном формате)	11111111.11111111.11111111.	11000000
Сетевой адрес 192.168.1.128.	Наименьший идентификатор хоста: 192.168.1.193.	
Broadcast адрес: 192.168.1.191.	Самый большой идентификатор хоста — 192.168.1.254.	

Пример: Разделить на восемь сеток

Точно так же 27-битная маска (000, 001, 010, 011, 100, 101, 110 и 111) используется для создания восьми сеток. Значения последнего октета IP-адреса для каждой сети показаны в таблице 7.10 ниже.

Таблица 7.10

Сеть	Сетевой адрес	Первый адрес	Последний адрес	Broadcast адрес
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191

7	192	193	222	223
8	224	225	254	255

Планирование сети

Для сети с 24-битным сетевым номером сводка по сетевому планированию представлена в таблице 7.11.

Таблица 7.11

Количество зарезервированных битов идентификатора хоста	Сеть маска	Количество сетей	Количество хостов в сети
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Вот пример расчета количества сетей и хостов для сети 59.124.163.151/27.

/27 - сетевой префикс или маска сети

В двоичном формате 11111111 11111111 11111111 11100000 255.255.255.224 в десятичном формате

В четвертом поле (последний октет) 11100000 первые 3 бита определяют количество секторов, в нашем примере 23=8.

В четвертом поле (последний октет) 11100000 последние 5 бит определяют количество хостов в сети, в нашем примере 25 = 32.

Диапазон IP-адресов первой сети — от 0 до 31 (32 хоста), но 0 — это сеть, а 31 — broadcast адрес. Таким образом, максимальное количество хостов в данной сети равно 30.

Диапазон IP-адресов второй сети — от 59.124.163.32 до 59.124.163.63.

Второй сетевой адрес: 59.124.163.32

Второй сетевой broadcast адрес: 59.124.163.63

Мы можем рассчитать диапазон IP-адресов восьмой сети от 59.124.163.224 до 59.124.163.255.

Восьмой сетевой адрес: 59.124.163.224

адрес восьмой broadcast сети: 59.124.163.255

В нашем примере IP-адрес 59.124.163.151 находится в пятой сети.

Пятый сетевой адрес: 59.124.163.128/27

Диапазон IP-адресов пятой сети — от 59.124.163.128 до 59.124.163.159.

адрес пятой broadcast сети: 59.124.163.159.

Задание:

Учащиеся строят и настраивают сеть, используя параметры, указанные в таблице 7.12.

Таблица - 7.12. Варианты задания

№	Задание
1.	Построить сеть, состоящую из 4-х маршрутизаторов , 4-х коммутаторов, 4-х ПК. Настройте статические и резервные маршруты.
2.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 5 ПК. Настройте статические и резервные маршруты.
3.	Построить сеть, состоящую из 4 маршрутизаторов , 4 коммутаторов, 8 ПК. Настройте статические и резервные маршруты.
4.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 6 ПК. Настройте статические и резервные

	маршруты.
5.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 5 ПК. Настройте статические и резервные маршруты.
6.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
7.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 4 ПК. Настройте статические и резервные маршруты.
8.	Построить сеть, состоящую из 6 маршрутизаторов , 6 коммутаторов, 7 ПК. Настройте статические и резервные маршруты.
9.	Построить сеть, состоящую из 4-х маршрутизаторов , 4-х коммутаторов, 5-ти ПК. Настройте статические и резервные маршруты.
10.	Построить сеть, состоящую из 4 маршрутизаторов , 4 коммутаторов, 7 ПК. Настройте статические и резервные маршруты.
11.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 5 ПК. Настройте статические и резервные маршруты.
12.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 8 ПК. Настройте статические и резервные маршруты.
13.	Построить сеть, состоящую из 4-х маршрутизаторов , 4-х коммутаторов, 4-х ПК. Настройте статические и резервные маршруты.
14.	Построить сеть, состоящую из 4 маршрутизаторов , 4 коммутаторов, 8 ПК. Настройте статические и резервные маршруты.
15.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
16.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 5 ПК. Настройте статические и резервные маршруты.
17.	Построить сеть, состоящую из 6 маршрутизаторов , 6

	коммутаторов, 5 ПК. Настройте статические и резервные маршруты.
18.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 9 ПК. Настройте статические и резервные маршруты.
19.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
20.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
21.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
22.	Построить сеть, состоящую из 4-х маршрутизаторов , 4-х коммутаторов, 4-х ПК. Настройте статические и резервные маршруты.
23.	Построить сеть, состоящую из 4-х маршрутизаторов , 4-х коммутаторов, 5-ти ПК. Настройте статические и резервные маршруты.
24.	Построить сеть, состоящую из 4-х маршрутизаторов , 4-х коммутаторов, 3-х ПК. Настройте статические и резервные маршруты.
25.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
26.	Построить сеть, состоящую из 6 маршрутизаторов , 6 коммутаторов, 5 ПК. Настройте статические и резервные маршруты.
27.	Постройте сеть, состоящую из 4 маршрутизаторов, 4 коммутаторов, 6 ПК. Настройте статические и резервные маршруты.
28.	Построить сеть, состоящую из 6 маршрутизаторов , 6 коммутаторов, 9 ПК. Настройте статические и резервные маршруты.
29.	Построить сеть, состоящую из 4 маршрутизаторов , 4 коммутаторов, 8 ПК. Настройте статические и резервные маршруты.

30.	Построить сеть, состоящую из 5 маршрутизаторов , 5 коммутаторов, 8 ПК. Настройте статические и резервные маршруты.

В этой лабораторной работе необходимо выполнить следующие задания:

- настроить и проверить интерфейсы маршрутизаторов R1, R2, R3 и коммутаторов LSW1, LSW2, LSW3, как показано на рисунке 3.1;

- настроить статический маршрут в качестве следующего перехода, используя интерфейс и IP-адрес;

- проверить работу статического маршрута;

- Осуществлять связь между локальной и внешней сетями с использованием стандартного маршрута;

- установить резервный статический маршрут на маршрутизаторе.

Порядок выполнения работы

Настройте базовые конфигурации для коммутаторов LSW1, LSW2, LSW3, R1, R2, R3 в соответствии с топологией, показанной на рисунке 3.1.

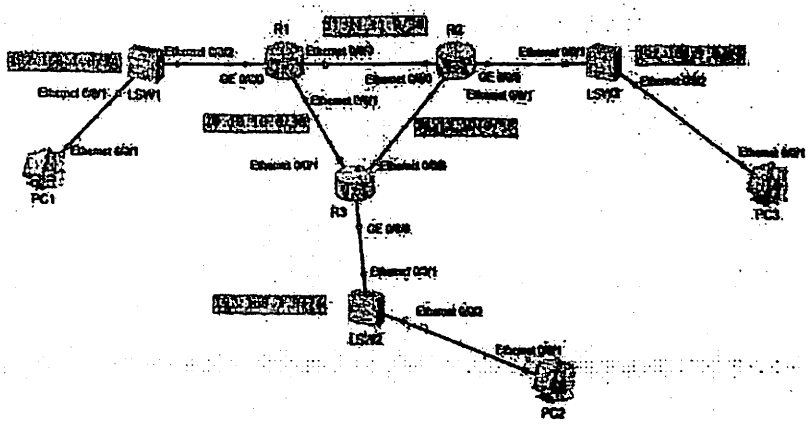

Рисунок 3.1. Исследуемая сетевая структура

1. Основные настройки системы и настройка IP-адресов. Для R1, R2 и R3 мы настроим сетевые IP-адреса на имена устройств и интерфейсы.

Настроим маршрутизатор R1:

<Huawei>system-view

[Huawei]sysname R1

[R1]interface Ethernet 0/0/0

[R1-Ethernet0/0/0]ip address 11.11.11.1 255.255.255.252

[R1-Ethernet0/0/0]quit

[R1]interface Ethernet 0/0/1

[R1-Ethernet0/0/1]ip address 10.10.10.1 255.255.255.252

[R1-Ethernet0/0/1]quit

[R1]interface GigabitEthernet 0/0/0

[R1- GigabitEthernet]ip address 192.168.1.1 255.255.255.0

[R1- GigabitEthernet]quit

Чтобы просмотреть текущую конфигурацию, вводим следующую команду:

<R1>display ip interface brief

Результат текущих настроек на маршрутизаторе R1 показан на рисунке 7.5.

Interface	IP Address/Mask	Physical	Protocol
Ethernet0/0/0	11.11.11.1/30	up	up
Ethernet0/0/1	10.10.10.1/30	up	up
GigabitEthernet0/0/0	192.168.1.1/24	up	up
GigabitEthernet0/0/1	unassigned	down	down
GigabitEthernet0/0/2	unassigned	down	down
GigabitEthernet0/0/3	unassigned	down	down
NULL0	unassigned	up	up(s)
Serial0/0/0	unassigned	down	down
Serial0/0/1	unassigned	down	down
Serial0/0/2	unassigned	down	down
Serial0/0/3	unassigned	down	down

Рисунок 7.5. Результат текущих настроек на маршрутизаторе R1

Настроим маршрутизатор R2:

<Huawei>system-view

[Huawei]sysname R2

[R2]interface Ethernet 0/0/0

[R2-Ethernet0/0/0]ip address 11.11.11.2 255.255.255.252

[R2-Ethernet0/0/0]quit

[R2]interface Ethernet 0/0/1

[R2-Ethernet0/0/1]ip address 12.12.12.1 255.255.255.252

[R2-Ethernet0/0/1]quit

[R2]interface GigabitEthernet 0/0/0

[R2- GigabitEthernet]ip address 192.168.2.1 255.255.255.0

[R2- GigabitEthernet]quit

Чтобы просмотреть текущую конфигурацию, вводим следующую команду:

<R2>display ip interface brief

Результат текущих настроек на маршрутизаторе R2 показан на рисунке 7.6.

Interface	IP Address/Mask	Physical	Protocol
Ethernet0/0/0	11.11.11.2/30	up	up
Ethernet0/0/1	12.12.12.1/30	up	up
GigabitEthernet0/0/0	192.168.2.1/24	up	up
GigabitEthernet0/0/1	unassigned	down	down
GigabitEthernet0/0/2	unassigned	down	down
GigabitEthernet0/0/3	unassigned	down	down
NULL0	unassigned	up	up(s)
Serial0/0/0	unassigned	down	down
Serial0/0/1	unassigned	down	down
Serial0/0/2	unassigned	down	down
Serial0/0/3	unassigned	down	down

Рисунок 7.6. Результат текущих настроек на маршрутизаторе R2

Настроим маршрутизатор **R3**:

<Huawei>system-view

[Huawei]sysname R2

[R3]interface Ethernet 0/0/0

[R3-Ethernet0/0/0]ip address 12.12.12.2 255.255.255.252

[R3-Ethernet0/0/0]quit

[R3]interface Ethernet 0/0/1

[R3-Ethernet0/0/1]ip address 10.10.10.2 255.255.255.252

[R3-Ethernet0/0/1]quit

[R3]interface GigabitEthernet 0/0/0

[R3- GigabitEthernet]ip address 192.168.3.1 255.255.255.0

[R3- GigabitEthernet]quit

Joriy konfiguratsiyani ko'rish uchun quyidagi buyruqdan foydalaniladi.

<R3>display ip interface brief

Чтобы просмотреть текущую конфигурацию, вводим следующую команду:

<R3>display ip interface brief

Результат текущих настроек на маршрутизаторе R3 показан на рисунке 7.7.

Interface	IP Address/Mask	Physical	Protocol
Ethernet0/0/0	12.12.12.2/30	up	up
Ethernet0/0/1	10.10.10.2/30	up	up
GigabitEthernet0/0/0	192.168.3.1/24	up	up
GigabitEthernet0/0/1	unassigned	down	down
GigabitEthernet0/0/2	unassigned	down	down
GigabitEthernet0/0/3	unassigned	down	down
NULL0	unassigned	up	up(s)
Serial0/0/0	unassigned	down	down
Serial0/0/1	unassigned	down	down

Рисунок 7.7. Результат текущих настроек на роутере R3

Теперь мы входим в каждый коммутатор, даем им названия и входим в интерфейс vlan и настроим IP-адреса.

Настроим коммутатор **LSW1**:

<Huawei>system-view

<Huawei>sysname LSW1

[LSW1]interface Vlanif1

[LSW1-Vlanif1]ip address 192.168.1.100 255.255.255.0

Настроим коммутатор **LSW2**:

<Huawei>system-view

<Huawei>sysname LSW2

[LSW2]interface Vlanif1

[LSW2-Vlanif1]ip address 192.168.2.100 255.255.255.0

Настроим коммутатор **LSW3**:

<Huawei>system-view

<Huawei>sysname LSW3

[LSW3]interface Vlanif1

[LSW3-Vlanif1]ip address 192.168.3.100 255.255.255.0

3. Настроим статические маршруты.

Для маршрутизатора **R1**:

[R1]ip route-static 192.168.2.0 255.255.255.0 11.11.11.2

[R1]ip route-static 192.168.3.0 255.255.255.0 10.10.10.2

Для маршрутизатора **R2**:

[R2]ip route-static 192.168.1.0 255.255.255.0 11.11.11.1

[R2]ip route-static 192.168.3.0 255.255.255.0 12.12.12.2

Для маршрутизатора **R3**:

[R3]ip route-static 192.168.1.0 255.255.255.0 10.10.10.1

[R3]ip route-static 192.168.2.0 255.255.255.0 12.12.12.1

4. Теперь настроим резервные маршруты.

Для маршрутизатора **R1**:

[R1]ip route-static 192.168.2.0 255.255.255.0 11.11.11.2 preference 1

[R1]ip route-static 192.168.2.0 255.255.255.0 10.10.10.2 preference 5

preference 5

Для маршрутизатора **R2**:

[R2]ip route-static 192.168.1.0 255.255.255.0 11.11.11.1 preference 1

[R2]ip route-static 192.168.1.0 255.255.255.0 12.12.12.2 preference 5

Для маршрутизатора **R3**:

[R3]ip route-static 192.168.1.0 255.255.255.0 10.10.10.1 preference 1

[R3]ip route-static 192.168.2.0 255.255.255.0 12.12.12.1 preference 5

2. Мы можем использовать команду ping для проверки сетевого соединения между R1 и R3. Отправляем ping с R1 на R3. Результат эхо-запроса от R1 до R3 показан на рис. 7.8.

```
<R1>ping 192.168.3.1
  PING 192.168.3.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=255 time=590 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=255 time=50 ms
  --- 192.168.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

Рисунок 7.8. Результат проверки соединения путем эхо-запроса R1 на R3.

Контрольные вопросы

1. Что такое статическая маршрутизация?
2. Как реализована статическая маршрутизация?
3. Зачем нужны резервные маршруты?
4. Как настроить резервные маршруты?
5. Классы протокола IPv4.
6. Бесплатные IP-адреса для использования в локальной сети.
7. Объясните структуру протокола IPv6.
8. Как определяется broadcast адрес?
9. Объясните маски подсети.
10. Как разделить сеть на маленькую сеть?
11. Как определяется сетевой адрес?
12. Какова цель команды "display ip interface Brief"?
13. Какова цель команды "ip route-static"?.

СПИСОК ЛИТЕРАТУРЫ

1. Network Management for the Mid-Market. Greg Shields, Solar winds, Network Management Solutions, San Francisco, CA (PRWEB) march 14, 2007.

2. HCNA-HNTD Huawei Networking Technology and Device. Entry Lab Guide. Version 2.1, 2014.

3. Alexander Clemm. Network Management Fundamentals. Cisco Press, 2014, ISBN-13: 978-1587201370.

4. Фокин В.Г. Управление телекоммуникационными сетями. Учебное пособие. Изд. СибГУТИ 2011

Интернет-ресурсы

1. https://habr.com/ru/post/419491/

2. https://support.huawei.com/enterprise/en/doc/EDOC1100008283/971e500a/traffic-filter-interface-view

3. https://support.huawei.com/enterprise/en/doc/EDOC1100086647

4. https://forum.huawei.com/enterprise/ru

5. https://selectel.ru/blog/dhcp-protocol/

Оглавление

Введение		3
Лабораторная работа №1	Знакомство со средой построения виртуальных компьютерных сетей и объединения локальной компьютерной сети на базе коммутаторов	4
Лабораторная работа №2	Настроить протокол Telnet	32
Лабораторная работа №3	Создание и настройка VLAN	44
Лабораторная работа №4	Настройка протокола GVRP и изучение принципа его работы	53
Лабораторная работа №5	Настройка протокола STP/RSTP и изучение принципа его работы	68
Лабораторная работа №6	Интерфейс Ethernet и конфигурация канала	83
Лабораторная работа №7	Объединение локальных вычислительных сетей на базе маршрутизаторов и с использованием статической маршрутизации	94
СПИСОК ЛИТЕРАТУРЫ		115

Методическое пособие разработанное для лабораторных работ по предмету "Управление телекоммуникационными сетями" часть 1 предназначено для бакалавров направления 5350100 – Телекоммуникационные технологии ("Телекоммуникации")

Методическое пособие обсуждено на совещании заседании кафедры "АПОСУТ" №___ от ___ _____ 2023 года и рекомендовано для изучения в научно-методическом совете факультета.

Методическое пособие обсуждено на совещании факультета "Телекоммуникационные технологии" №___ от ____ _____ 2023 года и рекомендовано для изучения в научно-методическом совете университета.

Методическое пособие обсуждено на совещании научно-методического совета ТУИТ №___ от __ _____ 2023 года и рекомендовано для печати.

Авторы: Р.П.Абдурахмонов

Б.У.Акмурадов

Х.Х.Ахмедова

Рецензенты: PhD. Д.Т.Хасанов

PhD О.У.Аскаралиев

Ответственный редактор: PhD М.Б.Мирзаева

Корректор: С.Х.Абдуллаева

Формат 60x84 1/16. Печ.лист 7,5.
Заказ №108. Тираж 10.
Отпечатано в «Редакционно издательском»
отделе при ТУИТ.
Ташкент ул. Амир Темур, 108.