Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По практической работе №2**

Студент: Смирнов Алексей Игоревич

Дисциплина/Профессиональный модуль: Инфокоммуникационные системы и сети

Выполнил студент

Группы: 3ПКС-220

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2023г.**

**СОДЕРЖАНИЕ**

[Лабораторная работа №1 3](#_Toc137504154)

[Лабораторная работа №2 11](#_Toc137504155)

[Лабораторная работа №3 14](#_Toc137504156)

[Лабораторная работа №4 18](#_Toc137504157)

[Лабораторная работа №5 20](#_Toc137504158)

[Лабораторная работа №6 23](#_Toc137504159)

# **Лабораторная работа №1**

**Исследование интерфейса программы Cisco Packet Tracer**

**Цель работы:** изучить интерфейс программы Cisco Packet Tracer, научиться назначать статические и динамические IP-адреса в новом интерфейсе, изучить работу DHCP-сервера.

**Ход работы:**

Задание 1. Необходимо построить сеть, назначить статические IP-адреса компьютерам, проверить соединение между компьютерами (доступность каждого интерфейса) в программе Cisco Packet Tracer.

Изображение выглядит как диаграмма, линия, снимок экрана

Автоматически созданное описание

Рисунок 1. Построенная сеть

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 2. IP-адрес 1 компьютера

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 3. IP-адрес 2 компьютера

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 4. IP-адрес 3 компьютера

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 5. IP-адрес 4 компьютера

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок 6. Проверка соединения

Задание 2. Необходимо построить сеть, назначить динамические IP-адреса компьютерам с помощью DHCP-сервера, проверить соединение между компьютерами (доступность каждого интерфейса) в программе Cisco Packet Tracer.

Изображение выглядит как диаграмма, линия, снимок экрана, круг

Автоматически созданное описание

Рисунок 7. Построенная сеть

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 8. Назначение IP-адреса серверу

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Рисунок 9. Активирование функции DHCP на сервере

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 10. Автоматическая конфигурация IP-адреса

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 11. Проверка соединения между PC5 (192.168.0.10) и PC7 (192.168.0.12)

**Контрольные вопросы:**

1. Чем отличается соединение устройств с помощью Copper Straight-Through (прямого) и Cross-Over (кроссоверного, обратного) кабеля?

Прямой кабель (Copper Straight-Through) используется для прямого соединения устройств различного типа. В этом кабеле проводники соединяются один к одному по соответствующим контактам на каждом конце кабеля. Кроссоверный кабель (Cross-Over) используется для соединения устройств одного типа, например, компьютера с компьютером или коммутатора с коммутатором. В этом кабеле проводники перекрещиваются, то есть проводник 1 на одном конце кабеля будет соединен с проводником 3 на другом конце, проводник 2 - с проводником 6 и так далее.

1. С помощью какой команды командной строки можно выяснить IP-адрес компьютера?

Для выяснения IP-адреса компьютера в командной строке можно использовать команду ipconfig.

1. В чем разница между статическим и динамическим адресом?

Статический IP-адрес назначается вручную администратором или сетевым администратором. Динамический IP-адрес назначается автоматически через протокол DHCP (Dynamic Host Configuration Protocol).

1. Что означает параметр TTL в результатах команды ping?

Параметр TTL (Time to Live) в результатах команды ping означает время жизни пакета данных в сети. Этот параметр определяет количество промежуточных узлов (коммутаторов, маршрутизаторов), которые пакет может пройти перед тем, как быть отброшенным.

1. Почему в результатах команды ping Вы наблюдаете 4 пакета?

Когда вы выполняете команду ping, по умолчанию отправляется несколько ICMP-пакетов (обычно 4) на указанный узел или хост в сети. Каждый пакет имеет уникальный идентификатор, и отправитель ожидает получить ответ на каждый из них. Это делается для обеспечения достоверности результатов и обнаружения потери пакетов или проблем на маршруте.

1. Каким параметром можно изменить количество пакетов в команде ping?

Чтобы изменить количество пакетов, используйте параметр -n с указанием желаемого числа пакетов. Например: ping -n 10 google.com отправит 10 пакетов на адрес google.com.

1. Можно ли изменить количество байт в передаваемом пакете команды ping? Если да, каким параметром?

Да, в некоторых операционных системах можно изменить размер передаваемого пакета в команде ping. Чтобы изменить размер пакета, используйте параметр -l с указанием желаемого размера пакета в байтах. Например: ping -l 100 google.com отправит пакет размером 100 байт на адрес google.com.

1. Зачем в результатах команды ping выводится статистика?

Для проверки доступности узла, оценки качества связи, отслеживания потери пакетов, определения стабильности сети.

1. На что затрачивается время передачи, выводимое в результатах команды ping? Какие узлы при этом прошѐл пакет?

Время передачи, выводимое в результатах команды ping, представляет собой время, затраченное на отправку ICMP-запроса от вашего компьютера до целевого узла (хоста или IP-адреса) и получение ответа обратно. Что касается узлов, которые пакет проходит по пути, вывод команды ping не предоставляет прямой информации о промежуточных узлах. Он показывает только время передачи и возможные потери пакетов.

1. Что такое пул адресов DHCP-сервера?

Пул адресов DHCP-сервера (Dynamic Host Configuration Protocol) - это диапазон IP-адресов, который DHCP-сервер может выделять и назначать автоматически устройствам в сети, которые запрашивают IP-конфигурацию. DHCP-серверы используются для автоматической конфигурации сетевых параметров, включая IP-адреса, подсети, шлюзы по умолчанию и DNS-серверы.

**Вывод:** в проделанной работе научился строить сети в программе Cisco Packet Tracer, назначать динамические IP-адреса компьютерам с помощью DHCP-сервера и простым способом, а также проверять соединение между компьютерами.

# **Лабораторная работа №2**

**Базовая настройка коммутатора Cisco**

**Цель работы:** получение базовых навыков по работе с командным интерфейсом коммутаторов Cisco, настройка базовой конфигурации коммутатора.

**Ход работы:**

**Контексты командной строки Cisco IOS**

**Контекст пользователя** открывается при подсоединении к маршрутизатору; обычно при подключении через сеть требуется пароль, а при подключении через консольный порт пароль не нужен. В этот же контекст командная строка автоматически переходит при продолжительном отсутствии ввода в контексте администратора. В контексте пользователя доступны только простые команды (некоторые базовые операции для мониторинга), не влияющие на конфигурацию маршрутизатора. Вид приглашения командной строки: switch>

**Контекст администратора** (контекст "exec", привилегированный режим) открывается командой enable, поданной в контексте пользователя; при этом обычно требуется пароль администратора. В контексте администратора доступны команды, позволяющие получить полную информацию о конфигурации маршрутизатора и его состоянии, команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Вид приглашения командной строки: switch#

**Глобальный контекст** конфигурирования открывается командой config terminal ("конфигурировать через терминал"), поданной в контексте администратора. Глобальный контекст конфигурирования содержит как непосредственно команды конфигурирования коммутатора, так и команды перехода в контексты конфигурирования подсистем коммутатора.

**Контекст конфигурирования интерфейса** открывается командой interface имя\_интерфейса (например, interface fa0/1), поданной в глобальном контексте конфигурирования.

**Контрольные вопросы:**

1. Нужна ли настройка ip-адреса VLAN1 для отправки эхо-запроса с PC0 на PC1?

Да, для отправки эхо-запроса с одного устройства на другое в разных VLAN требуется настройка IP-адресов на соответствующих интерфейсах в каждом VLAN. В случае, когда вы хотите отправить эхо-запрос с PC0 в VLAN1 на PC1 в другом VLAN, вам потребуется присвоить IP-адрес каждому из этих устройств в соответствующих VLAN.

1. Что произойдет, если 5 человек попытаются создать сеанс Telnet с любым из двух коммутаторов?

Если 5 человек одновременно попытаются создать сеанс Telnet с одним из двух коммутаторов, в зависимости от конфигурации коммутаторов и доступных ресурсов, могут произойти следующие варианты:

1. Если коммутаторы настроены для поддержки множества одновременных Telnet-сеансов и имеют достаточные ресурсы (такие как процессор и память) для обработки всех запросов, то все 5 человек смогут успешно создать сеансы Telnet с коммутаторами.
2. Если коммутаторы ограничивают количество одновременных Telnet-соединений и это ограничение уже достигнуто (например, только 3 одновременных сеанса Telnet), то первые 3 человека смогут успешно создать сеансы Telnet, а оставшиеся 2 человека будут отклонены до освобождения ресурсов.
3. Если коммутаторы не поддерживают Telnet-соединения или данная функция отключена, все 5 попыток будут отклонены.
4. Команда "enable password" создает незашифрованный пароль. Какая команда позволяет создать зашифрованный пароль для доступа в привилегированный режим?

Команда "enable secret" позволяет задать пароль, который будет зашифрован с использованием односторонней хэш-функции. Зашифрованный пароль хранится в конфигурационном файле коммутатора или маршрутизатора, обеспечивая более высокий уровень безопасности, поскольку невозможно восстановить исходный пароль из его зашифрованного значения.

1. Какова роль протокола ARP в процессе обмена данными по протоколу ICMP между устройствами?

Протокол ARP (Address Resolution Protocol) играет важную роль в процессе обмена данными по протоколу ICMP (Internet Control Message Protocol) между устройствами. Вот как он влияет на этот процесс:

1. Определение MAC-адреса: Протокол ARP используется для определения MAC-адреса устройства, имеющего определенный IP-адрес в локальной сети. Когда устройство, например, отправляет ICMP-сообщение другому устройству в той же локальной сети, оно должно знать MAC-адрес получателя, чтобы правильно доставить пакет по сети.
2. ARP-запрос: Если отправитель не знает MAC-адреса получателя, он отправляет ARP-запрос (broadcast) на локальную сеть, содержащий IP-адрес получателя. Запрос также содержит MAC-адрес отправителя.
3. ARP-ответ: Устройство, имеющее запрашиваемый IP-адрес, отвечает на ARP-запрос, предоставляя свой MAC-адрес отправителю.
4. Кэширование ARP: После получения ARP-ответа, отправитель кэширует пару IP-адреса и MAC-адреса получателя на некоторое время (обычно несколько минут). Это позволяет избежать повторных ARP-запросов для того же IP-адреса в ближайшем будущем, что повышает эффективность обмена данными.

**Вывод:** в проделанной работе получил базовые навыки по работе с командным интерфейсом коммутаторов Cisco, теоретически познакомился с настройкой базовой конфигурации коммутатора.

# **Лабораторная работа №3**

**Настройка VLAN на коммутаторах Cisco**

**Цель работы:** получение базовых навыков по работе с VLAN, научиться настраивать VLAN на оборудовании Cisco.

**Ход работы:**

PC0, PC4 и PC5 имеют VLAN 8; PC1 и PC2 имеют VLAN 4;

PC3 и PC7 имеют VLAN 3; PC6 имеет VLAN 4

**Изображение выглядит как диаграмма, линия, снимок экрана

Автоматически созданное описание**

Рисунок 1. Схема сети с VLAN

**Контрольные вопросы:**

1. Назовите причины использования VLAN.

VLAN (Virtual Local Area Network) - это технология, которая позволяет разбивать физическую сеть на логически отдельные сегменты. Использование VLAN может быть обусловлено несколькими причинами:

1. Управление трафиком: VLAN позволяют разделить сеть на группы устройств, которые имеют схожие требования к сетевому трафику. Это помогает ограничить размеры широковещательного домена и уменьшить количество лишнего трафика, улучшая производительность и безопасность сети.
2. Управление безопасностью: VLAN позволяют ограничивать доступ к определенным сегментам сети. Это позволяет создавать изолированные сетевые сегменты для групп пользователей или приложений, обеспечивая более высокий уровень безопасности и предотвращая несанкционированный доступ.
3. Упрощение управления сетью: С использованием VLAN можно легко группировать устройства и ресурсы по логическим параметрам в соответствии с требованиями организации. Это упрощает администрирование сети, позволяет быстро настраивать правила доступа и упрощает масштабирование сети при необходимости.
4. Повышение гибкости: VLAN обеспечивают гибкость в изменении конфигурации сети без физического перекаблирования. Пользователи и ресурсы могут быть перемещены между VLAN, не требуя физической перенастройки сети.
5. Оптимизация использования сетевых ресурсов: VLAN позволяют эффективно использовать доступные сетевые ресурсы. Ресурсы можно легко выделить для конкретных групп пользователей или приложений, что способствует оптимальному использованию пропускной способности и улучшению качества обслуживания.
6. В чём разница между тегированным и нетегированным трафиком?

Нетегированный трафик: В нетегированном режиме коммутаторы не добавляют VLAN-тег к сетевым кадрам. Трафик, отправляемый на порт, настроенный в режиме нетегированного доступа (untagged), считается принадлежащим к определенной VLAN. Это означает, что порт работает в рамках определенной VLAN и все кадры, полученные с этого порта, не имеют VLAN-тега. Нетегированный трафик используется внутри одной VLAN для связи между устройствами внутри сегмента сети. Тегированный трафик: В тегированном режиме коммутаторы добавляют VLAN-тег к сетевым кадрам. Кадры, отправляемые на порт, настроенный в режиме тегированного доступа (tagged), содержат VLAN-тег, который указывает идентификатор VLAN, к которой они принадлежат. Тегированный трафик используется для передачи данных между различными VLAN и коммутаторами. При получении тегированного трафика коммутаторы считывают VLAN-тег и пересылают кадр в соответствующую VLAN.

1. Сколько бит содержит VID?

Наиболее распространенный протокол тегирования VLAN - IEEE 802.1Q. В рамках этого протокола поле VID составляет 12 бит.

1. Какие устройства подключает access-порт?

Access-порт в сетевых коммутаторах используется для подключения конечных устройств (host devices), таких как компьютеры, серверы, принтеры или IP-телефоны, к сети. Access-порт предоставляет подключение устройствам, которым требуется только одна VLAN (нетегированный трафик). Основная функция access-порта заключается в передаче сетевого трафика от подключенного устройства до коммутатора и обратно. Коммутатор принимает трафик от подключенного устройства и пересылает его в соответствующую VLAN.

1. Как называется порт, передающий трафик нескольких VLAN?

Порт, который передает трафик нескольких VLAN, называется trunk-порт (транковый порт).

1. Какой командой можно посмотреть информацию о настроенных VLAN?

show vlan brief: Команда show vlan brief предоставляет более подробную информацию о настроенных VLAN, включая список портов, принадлежащих каждой VLAN, типы портов (access или trunk) и другие свойства VLAN.

1. Какой командой можно запретить передачу трафика VLAN 70 через транковый порт?

interface <имя\_транкового\_порта>

switchport trunk allowed vlan remove 70

1. Какой командой можно посмотреть информацию о настроенных транковых портах?

show interfaces trunk: Эта команда отображает информацию о настроенных транковых портах на коммутаторе, включая список портов, их статус (вкл/выкл), разрешенные VLAN и другие свойства.

1. Будут ли пинговаться устройства одной VLAN, подключенные к разным коммутаторам, между которыми не назначен транковый порт?

Если между двумя коммутаторами, к которым подключены устройства одной VLAN, не настроен транковый порт, то устройства в этой VLAN не смогут обмениваться трафиком напрямую между коммутаторами. Пинги или другие сетевые соединения между этими устройствами не будут успешными.

**Вывод:** в проделанной работе получил базовые навыки по работе с VLAN, научился настраивать VLAN на оборудовании Cisco.

# **Лабораторная работа №4**

**Принцип работы протокола покрывающего дерева STP**

**Цель работы:** исследовать принцип работы протокола STP; сравнить процесс конвергенции протоколов STP и RSTP.

**Ход работы:**

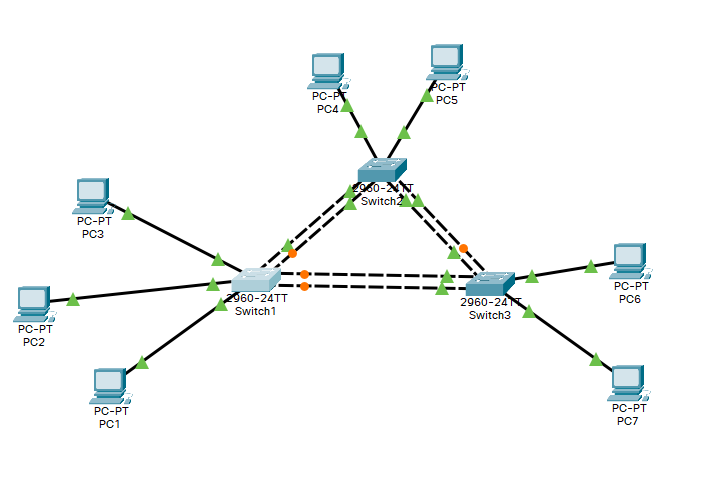


Рисунок 1. Схема сети с индикацией портов

**Контрольные вопросы:**

1. Для чего используется технология PortFast?

Для портов, к которым подключены не коммутаторы, конечные устройства (компьютеры, телефоны и др.), для быстрого перехода в состояние передачи (без прохода через состояния listening и learning), Cisco разработала технологию PortFast. Устройство, подключенное к порту с включенным PortFast, сразу может передавать данные.

1. Дать определение протоколу RSTP.

Rapid spanning tree protocol (RSTP) – общедоступный протокол. Включает расширения Cisco BackboneFast, UplinkFast и PortFast. Имеет меньшее время сходимости по сравнению с STP.

1. Какие бывают виды и модификации протокола STP?
2. Per-VLAN spanning tree protocol (PVST)
3. Per-VLAN spanning tree protocol plus (PVST+)
4. Rapid per-VLAN spanning tree protocol (rapid PVST+)
5. Rapid spanning tree protocol (RSTP)
6. Multiple STP (MSTP)
7. От чего защищает протокол STP в сетях Ethernet при наличии кольцевых топологий?

Протокол STP позволяет в сети с избыточными соединениями использовать только один логический путь, блокируя избыточные пути, которые могут привести к образованию петель.

В случае если один из участков пути будет недоступен, протокол STP вычислит новый путь и разблокирует один из заблокированных участков.

**Вывод:** в проделанной работе я исследовал принцип работы протокола STP; сравнить процесс конвергенции протоколов STP и RSTP.

# **Лабораторная работа №5**

**Настройка агрегации линий связи**

**Цель работы:** исследовать назначение агрегации каналов и протоколов агрегирования, научиться настраивать агрегированные каналы на оборудовании Cisco.

**Ход работы:**

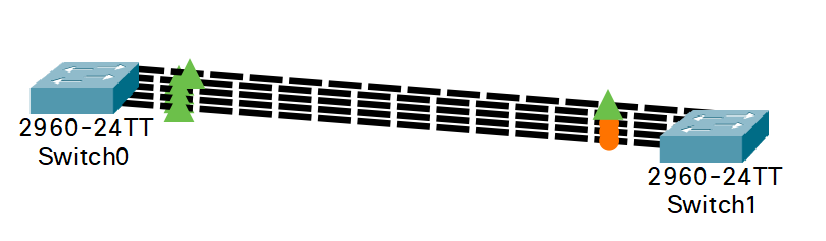


Рисунок 1. Схема построенной сети

**Контрольные вопросы:**

1. Сравните функции коммутатора: STP и агрегацию портов.

Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов, передаваться данные будут только через один интерфейс, который не заблокирован STP. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность. Без использования STP такое избыточное соединение создаст петлю в сети.

1. Сравните протокол LACP и статическое агрегирование.

Статическое агрегирование:

* Преимущества:

1. Не вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек
2. Вариант, который рекомендует использовать Cisco

* Недостатки:

1. Нет согласования настроек с удаленной стороной. Ошибки в настройке могут привести к образованию петель

Агрегирование с помощью LACP:

* Преимущества:

1. Согласование настроек с удаленной стороной позволяет избежать ошибок и петель в сети.
2. Поддержка standby-интерфейсов позволяет агрегировать до 16ти портов, 8 из которых будут активными, а остальные в режиме standby

* Недостатки:

1. Вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек
2. Будет ли работать агрегирование, если на обоих портах линии настроить режим auto?

Нет

1. Будет ли работать агрегирование, если на обоих портах линии настроить режим desirable?

Да

1. Будет ли работать агрегирование, если на обоих портах линии настроить режим active?

Да

1. Будет ли работать агрегирование, если на обоих портах линии настроить режим passive?

Нет

1. Перечислите методы балансировки нагрузки.

В зависимости от модели коммутатора, могут поддерживаться такие методы балансировки:

* по MAC-адресу отправителя или MAC-адресу получателя или учитывая оба адреса
* по IP-адресу отправителя или IP-адресу получателя или учитывая оба адреса
* по номеру порта отправителя или номеру порта получателя или учитывая оба порта

**Вывод:** в проделанной работе я исследовал назначение агрегации каналов и протоколов агрегирования, научиться настраивать агрегированные каналы на оборудовании Cisco.

# **Лабораторная работа №6**

**Назначение IPv6-адресов на сетевом оборудовании**

**Цель работы:** получить навыки по настройке IPv6-адресов на сетевых устройствах, разобраться в разных типах индивидуальных IPv6-адресов.

**Ход работы:**

**Задание 1.**

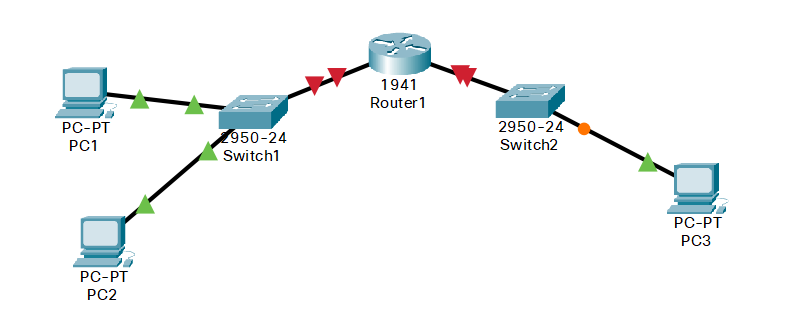


Рисунок 1. Сеть для настройки IPv6-адресации

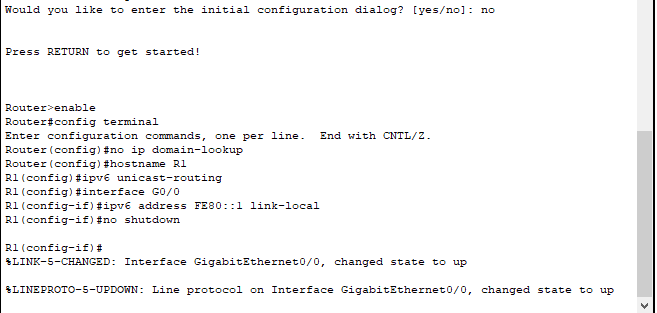


Рисунок 2. Настройка локального IPv6-адреса в подсети А

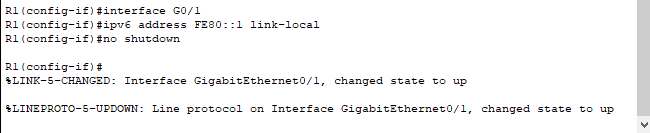


Рисунок 3. Настройка локального IPv6-адреса в подсети B

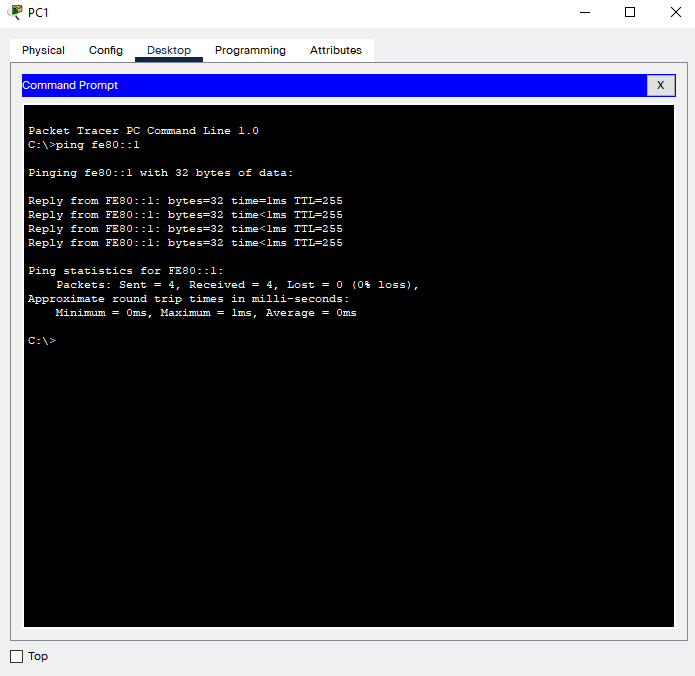


Рисунок 4. Проверка доступности интерфейса G0/0

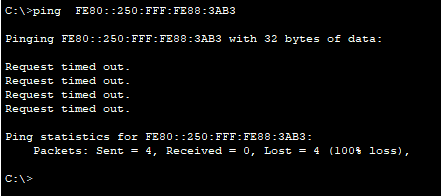


Рисунок 5. Проверка доступности интерфейса PC3 с PC1 по локальному адресу

|  |  |  |  |
| --- | --- | --- | --- |
| Проверить доступность | | | Успешный результат команды ping (да/нет) |
| от интерфейса | до интерфейса | |
| Название устройства | Название устройства | Локальный IPv6-адрес |
| PC1 | R1 (G0/0) | FE80::1 | Да |
| PC2 | R1 (G0/0) | FE80::1 | Да |
| PC3 | R1 (G0/1) | FE80::1 | Да |

|  |  |  |  |
| --- | --- | --- | --- |
| Проверить доступность | | | Успешный результат команды ping (да/нет) |
| от интерфейса | до интерфейса | |
| Название устройства | Название устройства | Локальный IPv6-адрес |
| PC1 | PC2 | FE80::20C:85FF:FE6E:7288 | Да |
| PC2 | PC3 | FE80::250:FFF:FE88:3AB3 | Нет |
| PC3 | PC3 | FE80::250:FFF:FE88:3AB3 | Да |

**Задание 2.**

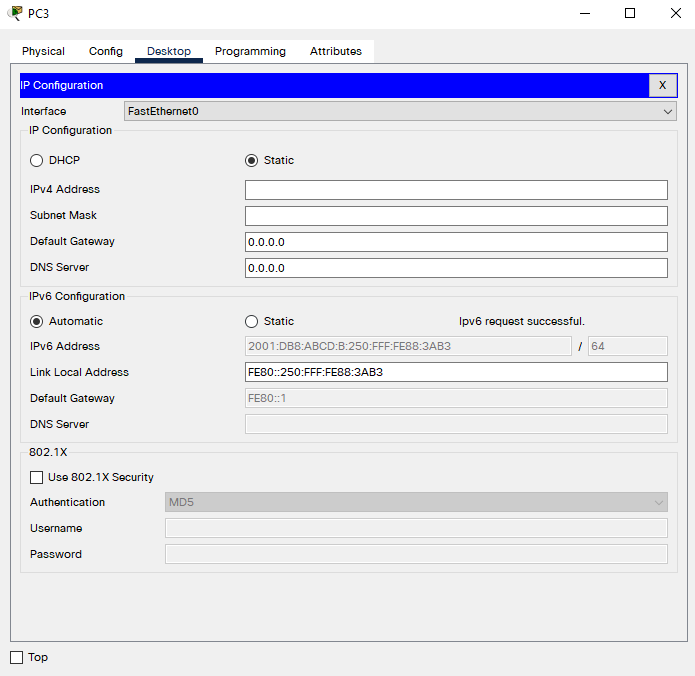
****

Рисунок 6. Автоматическая настройка IPv6-адреса с помощью маршрутизатора на PC3

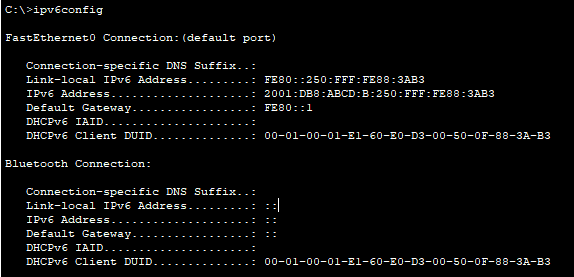
****

Рисунок 7. Глобальный IPv6-адрес PC3

**Контрольные вопросы:**

1. Приведите пример локального адреса.

FE80::20C:85FF:FE6E:7288

1. Приведите пример глобального IPv6-адреса.

2001:DB8:ABCD:B:250:FFF:FE88:3AB3

1. Объясните, почему по локальному адресу невозможно связаться с устройством, находящимся в другой сети.

Так как локальные адреса существуют только в пределах одной подсети.

1. Переведите MAC-адрес по варианту в IPv6-адрес (табл. 7). Запишите решение и получившийся IPv6-адрес.

fe80::23da:76ff:fe54:de12

**Вывод:** в проделанной работе я получил навыки по настройке IPv6-адресов на сетевых устройствах, разобраться в разных типах индивидуальных IPv6-адресов.