КГКП «АЛМАТИНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ И МАШИНОСТРОЕНИЯ»

«УТВЕРЖДАЮ»
Директор АКТиМ
_____ А.Б.Коджахметова
«___» _____ 2024г.

Учебное пособие по использованию eNSP (Enterprise Network Simulation Platform)

Специальность - 07140900 «Радиотехника, электроника и телекоммуникации»
Квалификация - 3W07140901 «Электромонтажник-наладчик телекоммуникационного оборудования и каналов»

Алматы, 2024 г.

Учебное пособие разработано в соответствии с типовыми учебными планами и предметной программы по специальности 07140900 «Радиотехника, электроника и телекоммуникация»

Учебное пособие рассмотрено и одорено на заседании предметно-цикловой комиссии «Энергетика и связь»
протокол №2 от "18" 09 2024 г.

Руководитель ПЦК Тұрсынғаликызы Ж.

Учебное пособие рассмотрено на методическом совете Алматинского колледжа телекоммуникаций и машиностроения
протокол №2 от "19" 09 2024 г.

И.о. заместителя директора по УМР Қайыпбаева Л.М.

Составители: мастера производственного обучения Салибаева У.Р., Кыдырбеков О. Н., Әшірбаев А.А., преподаватель специальных дисциплин Марат Г.С.

СОДЕРЖАНИЕ

Кабельная информационная сеть представляет собой сложную и многоуровневую систему, обеспечивающую передачу данных с высокой скоростью и надежностью. Каждый элемент этой сети, от витой пары до оптоволоконных линий, играет свою уникальную роль в создании инфраструктуры, обеспечивающей современное общество.

Современные кабельные сети требуют тщательной проектировки и регулярного обслуживания. Они включают в себя не только физические компоненты, но и программное обеспечение, которое управляет потоками информации. Развитие технологий позволяет значительно повысить пропускную способность сетей, что, в свою очередь, способствует реализации новых сервисов и технологий, таких как облачные вычисления и Интернет вещей.

Одной из ключевых задач является обеспечение кибербезопасности данных, что требует внедрения современных систем шифрования и защиты. Компании всё чаще обращаются к инновационным решениям, чтобы гарантировать безопасность и целостность передаваемой информации.

Кабельные информационные сети продолжают эволюционировать, адаптируясь к изменениям в технологической среде и потребностях пользователей, создавая надежную основу для будущих коммуникационных решений.

Волоконно-оптические линии связи являются основой современного сетевого взаимодействия, обеспечивая высокую скорость передачи данных. Важным элементом этой инфраструктуры выступают сетевые шкафы, которые организуют и защищают компоненты сети. Оснащенные особыми системными кабелями, шкафы облегчают управление соединениями и упрощают техническое обслуживание.

Распространенные разъемы для системных кабелей, такие как LC, SC и ST, разработаны для обеспечения надежного соединения и минимизации потерь сигнала. Для их установки и подключения необходимы общие инструменты, которые позволяют проводить гибкую и эффективную прокладку системных приборов.

Проектирование подсистем аппаратных цехов требует четкого понимания принципов работы кабельных систем и их интеграции в общую инфраструктуру. Приемка работ по прокладке кабелей осуществляется с акцентом на соответствие стандартам качества.

Основы цифровой коммутации и маршрутизации, включая протоколы OSPF и STP, играют ключевую роль в организации сети. Непременным условием для эффективного функционирования является также использование протоколов DHCP и PPP, а также понимание основ VLAN и агрегации каналов, что позволяет оптимизировать трафик и повысить безопасность сетевой среды.

КАБЕЛЬНАЯ ИНФОРМАЦИОННАЯ СЕТЬ

1. Понятие о сетевых шкафах

Сетевые шкафы представляют собой неотъемлемую часть современного информационного пространства, обеспечивая организацию и защиту сетевых компонентов. Они служат не только для размещения серверов и сетевого оборудования, но и для управления кабельной инфраструктурой, что позволяет оптимизировать пространство и повышать эффективность охлаждения.

Конструкция сетевых шкафов варьируется в зависимости от требований конкретного проекта. Стандартные размеры, такие как 19 дюймов для установки оборудования, дополняются различными решениями по климат-контролю, системам безопасности и бесперебойному питанию. Важно отметить, что правильный выбор сетевого шкафа не только улучшает доступ к оборудованию, но и снижает риски, связанные с перегревом и физическими повреждениями (рисунок 1).

Рисунок 1 - Сетевые шкафы

Кроме того, современные сетевые шкафы предлагают интеграцию с системами мониторинга и контроля, что позволяет администраторам оперативно отслеживать состояние оборудования и предотвращать возможные неисправности. Таким образом, сетевые шкафы не просто хранилища, а ключевые элементы инфраструктуры, обеспечивающие стабильность и постоянство работы информационных систем в организации.

2. Понятие о сетевых кабелях

Сетевой кабель - это физический канал связи, используемый для передачи данных между устройствами в компьютерной сети. Он состоит из нескольких проводов, заключенных в изоляционную оболочку.

Основные типы сетевых кабелей:

1) Коаксиальный кабель:

1. Состоит из центрального проводника, окруженного изоляцией, оплеткой и внешней изоляцией.
2. Используется для передачи аналоговых сигналов, в том числе для кабельного телевидения.
3. Низкая скорость передачи данных, подвержен помехам.

2) Витая пара:

1. Состоит из двух изолированных проводов, скрученных вместе.
2. Используется для передачи цифровых сигналов.
3. Различается по категориям (Cat5, Cat6, Cat7), определяющим скорость передачи данных и частоту.
4. Более защищен от помех, чем коаксиальный кабель.

3) Оптоволоконный кабель:

1. Состоит из тонкого стеклянного или пластикового волокна, по которому передаются световые импульсы.
2. Обеспечивает высокую скорость передачи данных, не подвержен помехам.
3. Дорогостоящий, требует специального оборудования для подключения.

Основные характеристики сетевых кабелей:

- Скорость передачи данных: Определяет максимальную скорость передачи информации по кабелю.
- Частота: Максимальная частота сигнала, которую может передавать кабель.
- Пропускная способность: Количество данных, которое может быть передано за единицу времени.
- Длина: Максимальная длина кабеля, на которой гарантируется качественная передача данных.
- Сопротивление: Сопротивление кабеля электрическому току.
- Помехоустойчивость: Способность кабеля противостоять внешним помехам.

Применение сетевых кабелей:

- Локальные сети (LAN): Для подключения компьютеров, принтеров, серверов и других устройств в пределах одного здания.
- Глобальные сети (WAN): Для соединения локальных сетей друг с другом на больших расстояниях.
- Интернет: Для подключения к сети Интернет.
- Телефония: Для передачи голосовых сигналов по IP-телефонии.
- Кабельное телевидение: Для передачи аналоговых и цифровых телевизионных сигналов.

Выбор сетевого кабеля:

Выбор сетевого кабеля зависит от конкретных потребностей, таких как скорость передачи данных, длина кабеля, бюджет и другие факторы.

Важно:

1. Правильно выбрать категорию кабеля в зависимости от необходимой скорости передачи данных.
2. Использовать качественные кабели от проверенных производителей.
3. Правильно подключить кабель к устройствам.
4. Обеспечить правильную прокладку кабеля для предотвращения повреждений и помех.

3. Понятие о распространенных разъемах для системных кабелей

Современные системы передачи данных требуют надежных и высокоскоростных соединений, что делает выбор разъемов для системных кабелей особенно важным. Наиболее распространёнными являются RJ-45, используемые в сетях Ethernet, и USB, популярные в мобильных устройствах и компьютерной технике. Разъемы типа HDMI обеспечивают передачу видео и аудио сигналов, что делает их незаменимыми в области мультимедиа.

Другие важные разъемы включают в себя LC и SC для оптического волокна, которые обеспечивают высокую пропускную способность и низкие уровни затухания. Разъемы SATA и PCIe играют ключевую роль в подключении накопителей и графических карт, соответственно, обеспечивая быстродействие и эффективное охлаждение систем.

Наконец, стоит упомянуть о разъемах питания, таких как ATX и Molex, которые обеспечивают необходимое энергоснабжение для работы комплектующих. Каждый тип разъема имеет свои преимущества и области применения, что позволяет инженерам и пользователям подобрать оптимальные решения для своих задач. Таким образом, глубокое понимание характеристик и возможностей распространенных разъемов является важным фактором в разработке и эксплуатации современных вычислительных систем.

4. Понятие о общих инструментах для прокладки системных приборов

В современном мире промышленные системы и приборы становятся все более сложными и взаимосвязанными. Эффективная прокладка системных приборов требует использования различных инструментов, которые помогают обеспечить надежность и функциональность. В этой статье мы рассмотрим общие инструменты, используемые для прокладки системных приборов, и уделим внимание их функциям, типам, а также рекомендациям по эффективному использованию.

Зачем нужны инструменты для прокладки системных приборов?

Прокладка системных приборов — это процесс монтажа, настройки и тестирования оборудования, который включает в себя не только электрику, но и механические, а также программные компоненты. Для успешного выполнения этих задач требуется специализированный инструмент. Их использование приносит множество преимуществ:

1. **Эффективность**: Использование специализированных инструментов позволяет сэкономить время, а также уменьшить вероятность ошибок при установке.
2. **Безопасность**: Правильные инструменты помогают избежать несчастных случаев, связанных с работой с электрическими и механическими системами.
3. **Качество**: Хорошие инструменты обеспечивают надежное соединение и функционирование приборов, что минимизирует риски сбоя в работе.
4. **Удобство**: Многие инструменты разрабатываются так, чтобы быть удобными для работы, что снижает утомляемость оператора.

Виды инструментов для прокладки системных приборов

Электрические инструменты

Электрические инструменты играют ключевую роль в прокладке системных приборов. Они обеспечивают высокую скорость и точность монтажа. Среди наиболее распространенных электрических инструментов можно выделить:

• **Электродрели**: Используются для сверления отверстий в различных материалах. Современные электродрели могут иметь различные режимы работы, что делает их универсальными.

• **Кабельные стрипперы**: Эти инструменты необходимы для снятия изоляции с проводов. Это позволяет подготовить провода к подключению к системным приборам.

• **Ударные отвертки**: Они помогают быстро закручивать и раскручивать винты, что особенно важно на больших строительных площадках.

Эти инструменты играют важную роль в процессе укладки электрических проводов и соединений. Правильный выбор электрических инструментов существенно повышает качество и скорость работы.

Ручные инструменты

Несмотря на распространение электрических инструментов, ручные инструменты остаются незаменимыми в процессе прокладки системных приборов. Они часто используются для более точной работы, где требуется ручная сила и ловкость. К основным ручным инструментам можно отнести:

• **Плоскогубцы**: Необходимы для захвата, удерживания и изгиба проводов, особенно в труднодоступных местах.

• **Кусачки**: Используются для обрезки проводов. Кусачки должны быть довольно острыми, чтобы с легкостью справляться с различными типами проводов.

• **Отвертки**: Различные типы отверток необходимы для работы с различными крепежными элементами. Наличие отверток с различными насадками позволяет работать с несколькими типами винтов.

Эта категория инструментов предназначена для более точных и детализированных операций, что особенно важно при работе с маленькими и хрупкими компонентами системных приборов.

Измерительные инструменты

Измерительные инструменты обеспечивают точность при прокладке системных приборов. Без них невозможно гарантировать, что все соединения и установки выполнены правильно. К таким инструментам относятся:

• **Мультиметры**: Они используются для измерения напряжения, тока и сопротивления, необходимы для проверки исправности электрических цепей.

• **Уровни**: Уровни помогают убедиться, что приборы установлены горизонтально или вертикально, что критически важно для их корректной работы.

• **Лазерные дальномеры**: Эти устройства помогают точно измерять расстояния, что особенно полезно при установке сложных систем.

Измерительные инструменты значительно облегчают работу и повышают ее качество. Без точных измерений невозможно обеспечить надежность и долговечность систем.

Технологические новшества в инструментах для прокладки

Современные инструменты для прокладки системных приборов постоянно развиваются. Производители внедряют новые технологии, чтобы сделать их более эффективными и удобными в использовании. Некоторые из технологических новшеств включают:

• **Литий-ионные аккумуляторы**: Они обеспечивают долгую работу инструментов без подзарядки, что особенно удобно на больших строящихся объектах.

• **Интеллектуальные системы диагностики**: Различные инструменты могут оснащаться системами, которые позволяют проводить диагностику всех функций. Это позволяет заранее выявлять потенциальные проблемы.

• **Эргономичный дизайн**: Современные инструменты разрабатываются с учетом комфорта пользователя. Удобные рукоятки и легкий вес значительно снижают утомляемость.

Постоянное развитие технологий делает инструменты более удобными и многофункциональными, что позволяет направить усилия на решение более важных задач.

Подбор инструментов в зависимости от задачи

Правильный выбор инструментов — ключевой аспект успешной прокладки системных приборов. Необходимо учитывать специфические требования проекта и характеристики используемых приборов. При выборе инструментов полезно учитывать следующие моменты:

1. **Тип оборудования**: Разное оборудование требует различных инструментов. Например, для работы с тяжелыми электроприборами могут понадобиться одни инструменты, тогда как для легких — совершенно другие.
2. **Условия работы**: В зависимости от условий прокладки (доступность, место работы и т.д.) будут необходимы различные инструменты.
3. **Квалификация персонала**: Лучше всего подбирать инструменты с учетом уровня квалификации работников, которые будут их использовать. Это поможет избежать несчастных случаев и повысить производительность.

Системный подход к выбору инструментов позволяет значительно повысить эффективность прокладки системных приборов.

Важность регулярного обслуживания инструментов

Для того чтобы обеспечить долговечность и надежность инструментов, необходимо проводить регулярное обслуживание. Правильный уход увеличивает срок службы и эффективность инструмента:

• **Чистка инструментов**: После каждого использования необходимо очищать инструменты от грязи и остатков материалов.

• **Проверка состояния**: Регулярно проверяйте инструменты на предмет износа или повреждений. Замена или ремонт поврежденных инструментов предотвращает случаи, когда они могут повредить оборудование или привести к травмам.

• **Правильное хранение**: Сохраняйте инструменты в специальных контейнерах или на полках, чтобы избежать их повреждения и потери.

Таким образом, регулярное обслуживание инструментов является залогом их надежной и продолжительной работы.

Использование общих инструментов для прокладки системных приборов — это не просто обязательный этап работы, но и важный фактор, определяющий качество, безопасность и эффективность установок. Понимание функций и типов инструментов поможет вам избежать ошибок и повысить производительность вашей работы.

Правильный выбор, регулярное обслуживание и современный подход позволят вам успешно справляться с задачами любой сложности, обеспечивая надежную работу системных приборов в долгосрочной перспективе. Помните, что качество работы напрямую зависит от инструментов, которые вы применяете, поэтому уделяйте этому аспекту внимания.

5. Правила приемки и методы контроля прокладки кабельных линий

Приемка в эксплуатацию кабельных линий производится после окончания работ по прокладке кабелей и монтажу соединительных и концевых муфт. Все работы выполняют в соответствии с утвержденным и согласованным проектом, инструкцией Госстроя по

прокладке кабелей напряжением до 110 кВ (СН 85 — 74) и действующей технической документацией на муфты для кабелей с бумажной и пластмассовой изоляцией.

Кабельные линии при приемке в эксплуатацию подвергают осмотрам и электрическим испытаниям. Кабели скрытых прокладок (в траншеях, блоках и т. п.) не могут быть осмотрены после окончания всех работ на трассах, а существующие методы электрических испытаний не дают возможности выявить все дефекты в проложенной линии. Поэтому, для того чтобы обеспечить хорошее качество работ, необходимо контролировать прокладку кабеля и монтаж муфт во время их производства, т. е. осуществлять технический надзор.

В технический надзор входят: проверка кабельных сооружений и траншей; ознакомление с заводскими протоколами испытаний кабеля и его состоянием; проверка качества работ во время прокладки кабеля и монтажа муфт; контроль за наличием у монтажного персонала удостоверений, разрешающих им выполнять указанные работы. Его осуществляет та организация, которая будет эксплуатировать проложенный кабель.

Траншеи, каналы, туннели и другие кабельные сооружения выполняют с учетом минимально допустимых радиусов и изгибов кабелей, приведенных в таблица – 5.1.

Примечание. DK— наружный диаметр кабеля.

При осмотре кабельных сооружений должны быть проверены: наличие уклонов для стока воды, электрическое освещение, вентиляция и водооткачка, соответствие внутренних размеров проекту, состояние железобетонных конструкций и др.

Проверка качества работ при прокладке кабеля включает: контроль по динамометру за усилием тяжения кабеля; определение допустимых радиусов изгибов, глубины прокладки и расстояний между параллельно уложенными кабелями, а также расстояний между крайними кабелями и стенами сооружений; определение расстояний на пересечениях и сближениях кабелей с различными сооружениями; контроль за наличием песчаной подушки под кабель, защитных покрытий, запасов кабеля перед муфтами, маркировочных бирок.

Таблица – 5.1. Минимально допустимые радиусы изгиба кабелей при прокладке

Наименование	**Минимальный нару жный радиус изгиба *DK***
Кабели с бумажной пропитанной изоляцией (вязкая пропитка) и с бумажной изоляцией, пропитанной нестекающим составом:	
многожильные в свинцовой оболочке	15 *Я*
одножильные в алюминиевой или свинцовой оболочке	25
многожильные в алюминиевой оболочке	25
Кабели с пластмассовой изоляцией в алюминиевой оболочке	15
Кабели с пластмассовой и резиновой изоляцией: одножильные	10
многожильные	7,5

Контроль за монтажом муфт включает проверку: соответствия типоразмера муфты сечению кабеля; наличия кондиционных и не просроченных (срок годности) комплектующих материалов; наличия соответствующего инструмента и приспособлений; соблюдения обязательной технологии и последовательности монтажа.

На маркировочных бирках обозначают их марку, номинальное напряжение, число и сечение жил, номер или наименование кабельной линии. На бирках соединительных муфт силовых кабелей, кроме того, указывают дату монтажа и фамилию электромонтажника-кабельщика; а на бирках концевых заделок — конечные пункты (откуда и куда проложен кабель).

6. Основа цифровой коммутации

Цифровая коммутация лежит в основе современных телекоммуникационных систем. Это технология, которая позволяет передавать информацию в цифровом формате, обеспечивая надежную, гибкую и эффективную связь. Понимание принципов цифровой коммутации имеет решающее значение для специалистов в области информационных технологий и телекоммуникаций. Протоколы коммутации (рисунок-1)..

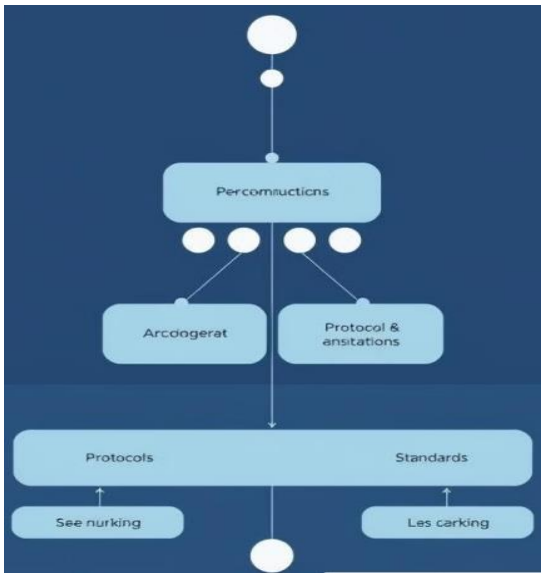


Рисунок – 1. Протоколы коммутации

Протоколы коммутации

TCP/IP

Набор основных протоколов, обеспечивающих передачу данных в сетях, включая IP для адресации имаршрутизации, а также TCP для надежной доставки пакетов.

Ethernet

Широко распространенный стандарт локальных сетей, определяющий физический и канальный уровни взаимодействия сетевых устройств.

ATM

Асинхронный режим передачи данных, основанный накоммутации ячеек. Применялся в высокоскоростных сетях связи, но постепенно вытесняется протоколами Ethernet и IP.

			
Коммутторы	**Маршрутизторы**	**Межсетевые экраны**	**VPN - концепторы**
Сетевые устройства, обеспечивающие передачу данных междупортами на основе MAC-адресов, создавая временные виртуальныеканалы связи	Устройства, принимающие решения о выборе оптимального пути для передачи пакетов данных между сетевыми сегментами наоснове IP-адресов.	Системы безопасности, контролирующие и фильтрующие сетевой трафик в соответствии с заданными правилами	Устройства, обеспечивающие безопасное удаленное подключение к корпоративной сети через зашифрованные виртуальные частные каналы.

Коммутация на канальном уровне

MAC-адресация

На канальном уровне устройства используют уникальные физические адреса (MAC-адреса) для идентификации сетевых интерфейсов и коммутации трафика между ними.

Коммутация кадров

Коммутаторы анализируют заголовки кадров Ethernet, содержащие MAC-адреса источника и получателя, для динамической маршрутизации трафика между портами.

Таблицы коммутации

Коммутаторы поддерживают внутренние таблицы, сопоставляющие MAC-адреса с портами, что позволяет им эффективно направлять трафик по назначению.

VLAN

Технология виртуальных локальных сетей (VLAN) дает возможность логически разделять коммутируемые сегменты, повышая безопасность и гибкость сетевой инфраструктуры.

Маршрутизация на сетевом уровне:

1. Адресация

Маршрутизаторы используют IP-адреса для идентификации сетевых интерфейсов и определения оптимального пути для передачи пакетов между подсетями.

2. Таблицы маршрутизации

Маршрутизаторы поддерживают таблицы маршрутизации, содержащие информацию о доступных сетевых сегментах и соответствующих интерфейсах для пересылки трафика.

3. Протоколы маршрутизации

Для обмена информацией о доступных маршрутах маршрутизаторы используют специальные протоколы, такие как RIP, OSPF и BGP (рисунок-2).

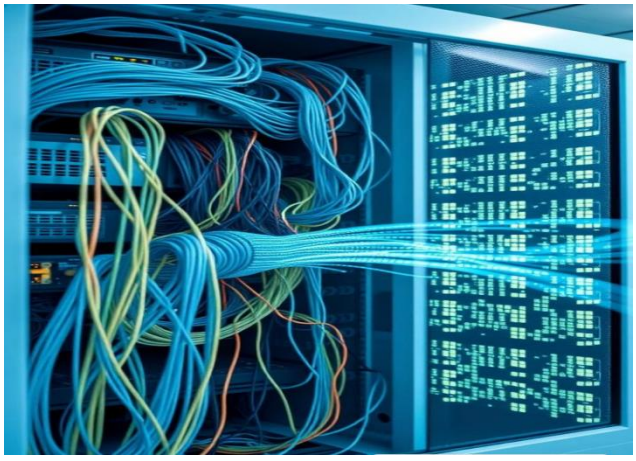


Рисунок-2. Шкаф маршрутизатора

Конвергенция технологий:

IP – телефония - Голосовая связь поверх IP-сетей с использованием протоколов, таких как SIP и H.323, обеспечивает интеграциютелефонии и данных.

IPTV - Технология доставки телевизионного контента по IP-сетям позволяет объединить услуги видео, голоса и данных в единую конвергентную платформу.

Unified Communications - Концепция объединенных коммуникаций предполагает интеграцию различных каналов связи (голос, видео, сообщения) в единое пользовательское решение приведенных в таблица –6. 1.

Таблица – 6.1. Будущее цифровой коммутации

5G	Высокоскоростные мобильные сети 5-го поколения, обеспечивающие беспрецедентную пропускную способность и низкие задержки для широкого спектра приложений.
SDN/NFV	Программно-определяемые сети и виртуализация сетевых функций, позволяющие гибко настраивать и масштабировать сетевые службы.
IoT	Интернет вещей, объединяющий миллиарды подключенных устройств, которые требуют надежной, масштабируемой и адаптивной коммутационной инфраструктуры.

Агрегация каналов

Агрегация каналов представляет собой сложный и многослойный процесс, который включает в себя объединение различных потоков данных и информации для создания единого и более эффективного канала коммуникации. В условиях современного мира, где информация поступает с разных платформ и устройств, необходимость в агрегировании становится особенно актуальной.

Процесс агрегации позволяет не только упростить доступ к информации, но и улучшить качество взаимодействия с пользователями. Объединяя различные источники, такие как социальные сети, новостные ленты и корпоративные системы, можно создать гибкую и интегрированную экосистему, способную адаптироваться к уникальным потребностям бизнеса и его клиентов.

Кроме того, агрегация каналов способствует более глубокой аналитике данных, позволяя выявлять тренды и предпочтения аудитории. Это, в свою очередь, открывает новые горизонты для разработки целевых стратегий маркетинга и повышения уровня клиентской удовлетворенности.

Преимущества агрегации очевидны – она способствует оптимизации процессов, повышает эффективность обмена информацией и обеспечивает большей прозрачности в работе компании, создавая тем самым позитивный имидж в глазах потребителей.

7. Руководство по установке eNSP (Enterprise Network Simulation Platform)

Huawei eNSP (Enterprise Network Simulation Platform) - эмулятор сети передачи данных, позволяет делать работоспособные модели сети, настраивать маршрутизаторы и коммутаторы, взаимодействовать с реальными сетями, отслеживать трейсы пакетов с помощью Wireshark.

В данной статье будет производиться установка eNSP версии **1.3.00.100** и настройка вложенной виртуализации в случае использования не Windows систем.

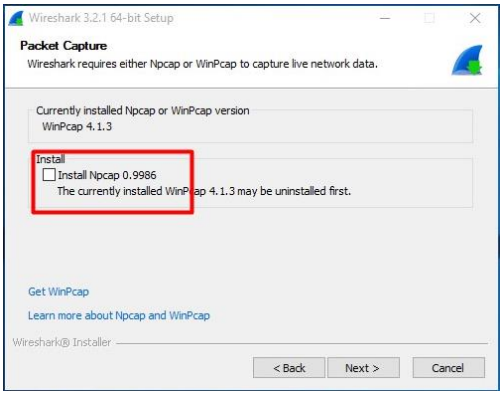
Установка eNSP

Для начала исходя из статьи "Основные проблемы при запуске симуляции в eNSP", необходимо убедиться во включённой виртуализации в BIOS и выключенном гипервизоре Hyper - V.

После:

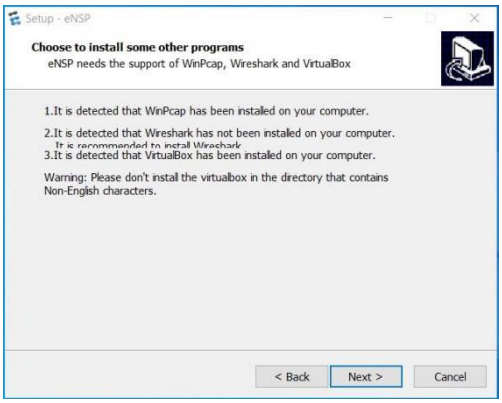
1. Скачиваем и инсталируем WinPcap: https://www.winpcap.org/install/default.htm
2. Скачиваем иинсталируем Wireshark: https://www.wireshark.org/download.html

При установке Wireshark обязательно убрать галку в чекбоксе с предложением установки Npcap:



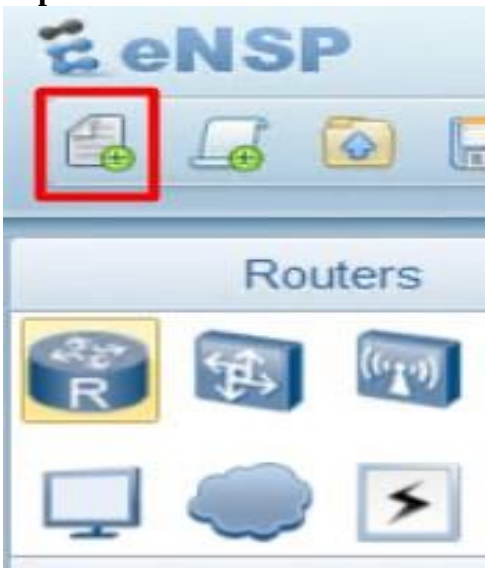
3. Скачиваем и инсталируем VirtualBox пятой версии (на данный момент, это единственная версия с которой работает eNSP), также *очень важно не устанавливать* VirtualBox в директорию содержащую не английские символы в названии).

4. Запускаем установку eNSP, жмём далее, убеждаемся что eNSP обнаружил всё зависимое ПО:



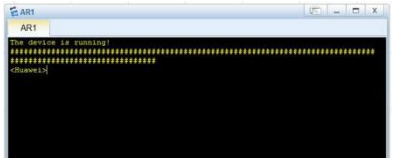
Проверить работоспособность можно создав новую топологию и запустить один из роутеров.

Нажмём кнопку **New Topo**:



В пункте **Routers** выбираем нужный нам роутер:

В пункте **Routers** перетащите на поле, например, роутер AR2220 и запустите его нажав по нему правой кнопкой мыши и нажав "Start". Далее если несколько раз нажать на роутер, то откроется окно терминала со статусом его загрузки и конечным приглашением для ввода команд:



Если CLI прогрузилось и отобразил <Huawei> - значит eNSP работает корректно.

Вложенная виртуализация для запуска eNSP

Если не получается из-за конфигурации компьютера запустить или установить eNSP и необходимые для него компоненты, можно воспользоваться чистой ОС в виде виртуальной машины, куда можно установить eNSP. Для запуска eNSP и firewall's для него внутри виртуальной машины, можно воспользоваться вложенной (Nested) виртуализацией.

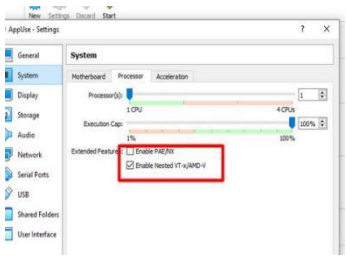
Для операционной системы Windows:

cd C:\Program Files\Oracle\VirtualBox

VBoxManage.exe list vms

VBoxManage.exe modifyvm "имя виртуальной машины" --nested-hw-virt on

В VirtualBox открываем настройки необходимой виртуальной машину для eNSP **Система -> Процессор**, включаем Nested VT-x/AMD-V:



Для операционной системы Linux:

vboxmanage list vms

VBoxManage modifyvm "имя виртуальной машины" --nested-hw-virt on

8. Команды eNSP (Enterprise Network Simulation Platform)

8.1 Общие команды для устройств Huawei

Вид пользователя：	< Huawei>
Вид системы：	< Huawei>system-view/sys [Huawei]
Вид интерфейса：	< Huawei>systemview/sys [Huawei]interface/int Ethernet0/0/1 [Huawei- Ethernet0/0/1]
Вид протокола маршрутизации：	[Huawei]isis [Huawei- isis-1]
Установка имени устройства:	< Huawei> system-view
Изменение имени устройства:	[Huawei] sysname Switch [Switch]

✓ Основые команды

1. < Huawei> quit ─возврат к предыдущему виду

2. < Huawei> return - Возврат непосредственно к пользовательскому представлению

3. < Huawei> save - Используется в режиме просмотра пользователя < Huawei> для сохранения конфигурации

4. < Huawei> reboot - перезагрузка

5. < Huawei> shutdown закрыть порт, undo shutdown порт активации

6. < Huawei> undo - Используется для восстановления ситуации по умолчанию (например, для установки имени устройства)

< Huawei> system-view

[Huawei] sysname Switch[Switch] undo sysname восстановление ситуации по умолчанию

[Huawei]

Используется для отключения какой-либо функции (например, ftp)

< Huawei> system-view

[Huawei] ftp server enable

[Huawei] undo ftp server Отключение функции ftp в устройстве

Чтобы удалить настройку undo, за которой следует информация о настройке команды, можно удалить связанную с ней конфигурацию

✓ Установите ip-адрес и маску подсети интерфейса устройства

[Huawei] interface - вход в вид интерфейс

[Huawei- Ethernet0/0/1]ip address - маска подсети ip-адреса

Конфигурирование ip-адреса и маски подсети

[Huawei- Ethernet0/0/1]undo shutdown - завести интерфейс

[Huawei- Ethernet0/0/1]display interface - просмотр состояния интерфейса

[Huawei] undo info-center enable - закрыть терминал для отображения информации об отправке центра сообщений

8.2 IP-адрес

IP-адрес (от англ. Internet Protocol) - уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.

В сети Интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети. В версии протокола IPv4 IP - адрес имеет длину 4 байта, а в версии протокола IPv6 - 16 байт.

Иногда встречается запись IP-адресов вида «192.168.5.0/24». Данный вид записи заменяет собой указание диапазона IP-адресов. Число после косой черты означает количество единичных разрядов в маске подсети. Для приведённого примера маска подсети будет иметь двоичный вид 11111111 11111111 11111111 00000000 или то же самое в маршрутизаторе в десятичном виде: «255.255.255.0». 24 разряда IP-адреса отводятся под номер сети, а остальные 8 разрядов полного адреса - под адреса хостов этой сети, адрес этой сети и широковещательный адрес этой сети. Итого, 192.168.5.0/24 означает диапазон адресов хостов от 192.168.5.1 до 192.168.5.254, а также 192.168.5.0 - адрес сети и 192.168.5.255 - широковещательный адрес сети. Для вычисления адреса сети и широковещательного адреса сети используются формулы:

- адрес сети = IP.любого_компьютера_этой_сети AND MASK (адрес сети позволяет определить, что компьютеры в одной сети)
- широковещательный адрес сети = IP.любого компьютера этой сети OR NOT(MASK) (широковещательный адрес сети воспринимается всеми компьютерами сети как дополнительный свой адрес, то есть пакет на этот адрес получат все хосты сети как адресованные лично им. Если на сетевой интерфейс хоста, который не является маршрутизатором пакетов, попадёт пакет, адресованный не ему, то он будет отброшен).

Запись адресов IP с указанием маски подсети переменной длины (записывается после адрес через косую дробную черту - «слэш») также называют бесклассовой адресацией (**CIDR**), в противоположность записи без указания маски, именуемой классовой адресацией:

- ✓ 192.0.2.2 и 100.64.2.2 - классовая запись адреса;
- ✓ 192.0.2.2/24 и 100.64.2.2/16 - бесклассовая запись CIDR тех же адресов и подсетей;

Классификация IP-адресов:
A(0）：8 bit， 0.0.0.0~127.255.255.255/8
Категория A (первый бит 0): номер сети 8 бит
B（10）：16 bit，128.0.0.0~191.255.255.255/16
Категория B (первые две цифры равны 10): номер сети 16 бит
C（110）：24 bit，192.0.0.0~223.255.255.255/24
Категория C (первые три цифры 110): номер сети 24 бит
Указанные адреса назначается хосту
D（1110）：224.0.0.0~239.255.255.255
Категория D (первые четыре цифры - 1110) Для многоадресной рассылки
E（1111）：240.0.0.0~255.255.255.255 исследование пользователей
Категория E (первые четыре цифры - 1111)

Отличие:
CIDR - это формирование нескольких стандартных сетей в одну большую сеть
VLSM - разделение стандартной сети на несколько меньших сетей (подсетей).
CIDR - перемещение маски подсети влево, VLSM - перемещение маски подсети вправо.

Специальные IP-адреса
1. В мире компьютеров не существует представления 0.
2. 255.255.255.255 Ограниченный широковещательный адрес, указывает на адрес назначения широковещательного уровня 3, все хосты в том же диапазоне

широковещательного домена получат этот пакет, диапазон широковещательного домена является переменным, связанным с делением подсети.

3. 169.254.0.0/16 использует DHCP для автоматического получения IP-адреса. При сбое в работе DHCP-сервера или превышении таймаута ответа система присваивает вам такой адрес, и вы не можете получить нормальный доступ в Интернет.

4. 127.0.0.0/8 (127.0.0.1-127.255.255.255) Локальный loopback-адрес, в основном используется для тестирования или управления сетью, а также для обновления маршрутизации, более стабилен, чем физический порт.

5. RFC1918 частный 1P-адрес 1PV4 адресное пространство в части специального мазка адреса, стать частным IP-адресом, частный IP-адрес не может быть непосредственно в соответствии с доступом к сети общего пользования (Internet 〉 IP, может быть использован только локально.

1 A: 10.0.0.0/8(10.0.0.1-10.255.255.255)
категория A: 10.0.0.0/8 (10.0.0.1-10.255.255.255) 1 сайт категория A
2 B: 172.16.0.0/12(172.16.0.1-172.31.255.255) 16 B
категория B: 172.16.0.0/12 (172.16.0.1-172.31.255.255) 16 категорий B
3 C : 192.168.0.0/16(192.168.0.1-192.168.255.255)256 C
категория C: 192.168.0.0/16 (192.168.0.1 - 192.168.255.255) 256 категорий C

6. Общая многоадресная рассылка
224.0.0.1 Все хост
224.0.0.2 Все маршрутизаторы
224.0.0.5 Все удаленные маршрутизаторы OSPF
224.0.0.6 Адрес многоадресного приема для DR и BDR
224.0.0.9 Адрес приема многоадресной рассылки RIPvz
224.0.0.18 дрес многоадресной рассылки VRRP

9. Основные принцины маршрутизатора и коммутатора, соединение сетей в программе eNSP

Маршрутиза́тор, **ро́утер** (транслит.от англ. *router*), также **роутер** (от англ. *router* /ˈɹuːtə(ɹ)/или /ˈɹaʊtəɹ/[1], /ˈɹaʊtɚ/) - специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации.

Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

Маршрутизаторы работают на «сетевом» (третьем) уровне сетевой модели OSI, в отличие от коммутаторов (свитчей) L2 уровня OSI и концентраторов (хабов), которые работают соответственно на втором и первом уровнях модели OSI.

Выберите маршрутизатор: AR2240

<huawei>system-view - перейдите в режим просмотра системы
[huawei]sysname R1 - дать названия маршрутизатору

[R1]undo info-center enable- настройка шрифтов, отображение интерфейсов, сохранение.

Tab - использование «Табуляция, клавиши вверх и вниз

[R1] int g0/0/x - вход в режим просмотра интерфейса

[R1 int g0/0/x]ip add x.x.x.x 24 - настройка IP-адреса в режиме просмотра интерфейса

[R1]quit - выход из системы

<R1> save - сохронить настройки

<R1> dis this, dis cu - запрос текущей конфигурации

<R1>dis ip int bri - запрос состояния интерфейса

<R1>dis ip rou - запрос таблицы маршрутизации

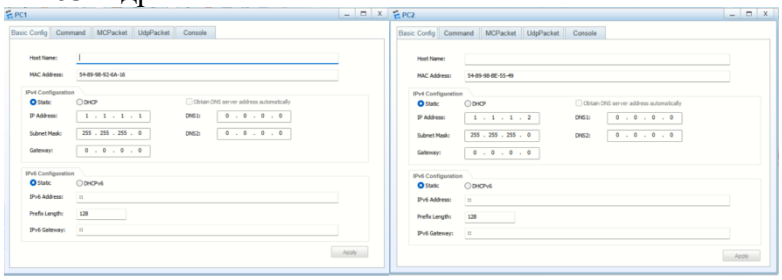
<R1> dis arp - запрос таблицы маршрутизации

<R2>- конфигурация R2 одинакова

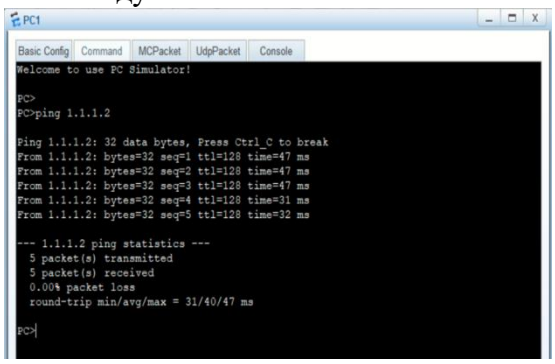
<R1> ping 172.16.12.2 - проверить связь между маршрутизаторми R1 с R2.

Сетевой коммутатор (жарг. ***свитч***, ***свич*** от англ. *switch* «переключатель») - 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 были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI).

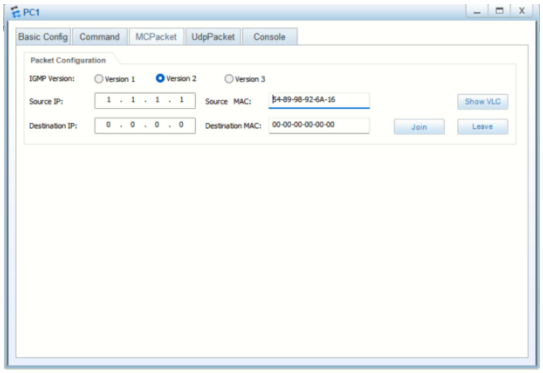
Вводим IP и Mask адрес на PC1 и PC2:



Проверить соединение между PC1 на PC2 с помошью команды `PC>ping 1.1.1.2`



MAC-адрес записывается в аппаратное обеспечение и поэтому также называется аппаратным адресом. MAC-адрес служит идентификатором адреса устройства передачи данных и должен быть уникальным для каждого MAC-адреса в сети:



Адреса различаются по своей природе MAC-адреса - это физические адреса, а IP-адреса - логические адреса. Изменчивость различна MAC-адрес имеет уникальность, MAC-адрес каждой аппаратной фабрики фиксирован; IP-адрес не имеет уникальности.

Рабочие уровни различны. Уровень 2 пересылает кадры данных на основе MAC-адресов, а уровень 3 - сообщения на основе IP-адресов. Коммутаторы второго уровня пересылают данные на основе таблицы MAC-адресов, а маршрутизаторы - на основе таблицы маршрутизации (IP-адреса).

определение длины отличается. MAC-адрес - это адрес на Ethernet-карте, длиной 48 бит, IP-адрес в настоящее время является мейнстримом длиной 32 бита. IP-адрес и MAC-адрес через протокол ARP связаны между собой.

Основа распределения различна. Распределение IP-адресов основано на топологии сети, а распределение MAC-адресов - на производителе.

Прежде всего, следует отметить, что не для всех видов передачи данных между сетями требуются mac-адреса и ip-адреса. Например, нет MAC-адресов для связи между линиями "точка-точка", и нет ip-адресов, когда на сетевом уровне используется протокол ipx. Но в современных магистральных сетях мы все используем ip-адреса и mac-адреса.

mac-адрес подобен идентификационному номеру человека, идентификационный номер человека связан с городом, в котором находится его счет, датой рождения, но он не имеет отношения к местонахождению человека, человек перемещается, знание идентификационного номера человека не позволяет найти его. mac-адрес аналогичен, он связан с производителем устройства, партией, датой и так далее, знание mac устройства не позволяет отправлять ему данные по сети, если оно не находится в той же сети, что и отправитель. Знание mac устройства не позволяет отправлять ему данные по сети, если оно не находится в той же сети, что и отправитель.

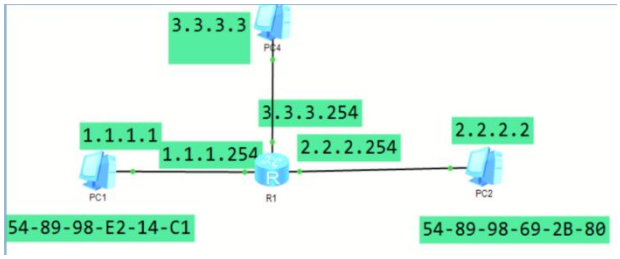
Поэтому для обеспечения связи между машинами нам также необходимо понятие ip-адреса, который выражает местоположение текущей машины в сети, аналогично понятию названия города + номера дороги + номера дома. Благодаря ip-уровню адресации мы можем знать, по какому пути передавать данные между любыми двумя машинами в Интернете в мире.

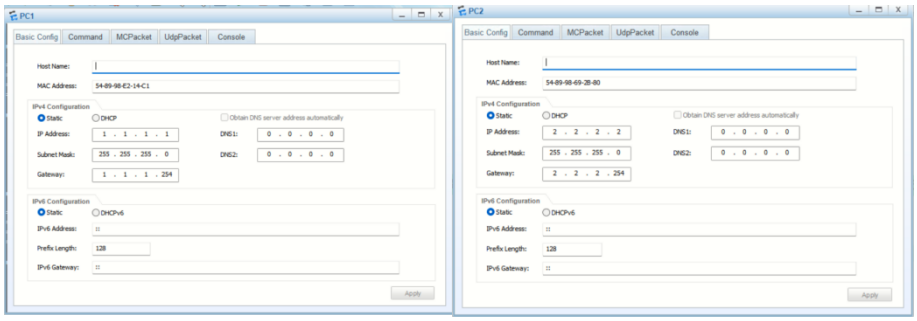
1. исторические причины В ранних Ethernet был только концентратор (hub), коммутатора (switch) не было, поэтому отправляемый пакет могли прослушивать все машины внутри Ethernet, поэтому для сопровождения MAC-адреса каждая машина должна принимать только те пакеты, которые соответствуют ее собственному MAC-адресу. До появления ip-адресов уже использовались mac-адреса

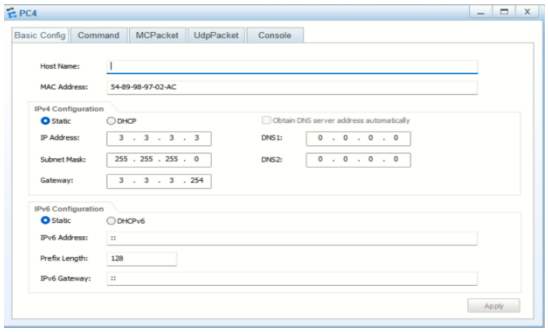
2. многоуровневая модель сетевой архитектуры, в которой многоуровневость позволяет более гибко заменять протоколы на сетевом и канальном уровнях

3. передача информации, которую необходимо знать, фактически представляет собой два адреса: адрес конечной точки, адрес следующего хопа. ip-адрес - это, по сути, адрес конечной точки, он не меняется при переходе через маршрутизатор, в то время как

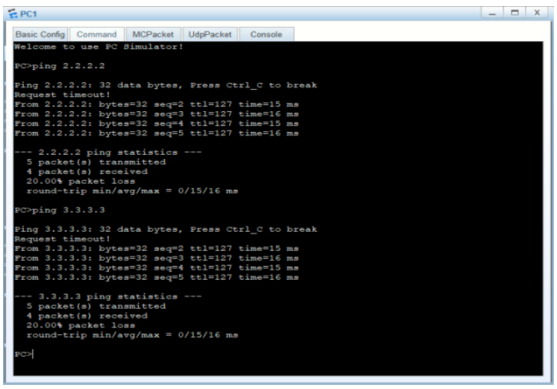
MAC-адрес - это адрес следующего хопа, при каждом переходе через маршрутизатор он будет меняться. MAC-адрес играет роль в записи информации о следующем хопе.







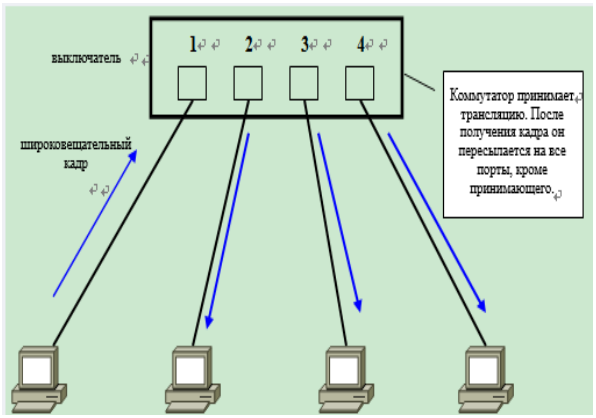

```
<R1>sys
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip address 1.1.1.254 24
[R1-GigabitEthernet0/0/0]int g0/0/1
[R1-GigabitEthernet0/0/1]ip address 2.2.2.254 24
[R1-GigabitEthernet0/0/1]int g0/0/2
[R1-GigabitEthernet0/0/2]ip address 3.3.3.254 24
```



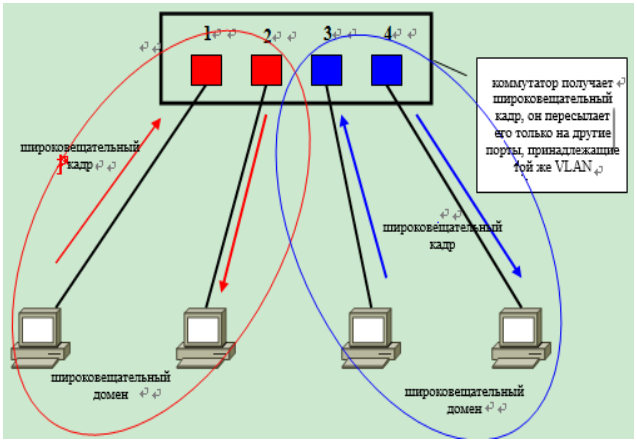
10. Основа виртуальной локальной компьютерной сети (VLAN)

VLAN (аббр. от англ. *Virtual Local Area Network*) - виртуальная локальная компьютерная сеть. Представляет собой группу хостов с общим набором требований [*источник не указан 1260 дней*], которые взаимодействуют так, как если бы они были подключены к широковещательному домену независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

Механизм



Любые широковещательные кадры пересылаются на все остальные порты, кроме принимающего порта



После этого коммутатор будет пересылать его только на другие порты, принадлежащие к той же VLAN

Особенности VLAN

Физическая локальная сеть может быть разделена на несколько VLAN, а в одной VLAN могут находиться устройства из нескольких физических сетей.

Все устройства в VLAN находятся в одном широковещательном домене, и широковещательные сообщения не могут распространяться через VLAN.

Сообщения второго уровня между VLAN изолированы друг от друга.

Связь между виртуальными локальными сетями может осуществляться только с помощью технологии маршрутизации третьего уровня (которая реализуется сетевыми устройствами третьего уровня, такими как маршрутизаторы или коммутаторы третьего уровня).

VLAN отличаются друг от друга номерами VLAN, которые могут принимать значения от 1 до 4094.

VLAN работают на уровне 2 (канальный уровень) эталонной модели

1 VLAN = 1 широковещательный домен = один логический сегмент (подсеть)

Access - Интерфейсы, обычно используемые на коммутаторах для подключения конечных устройств, таких как пользовательские ПК, серверы и т.д. Сетевые карты этих устройств, к которым подключены интерфейсы Access, обычно отправляют и получают только нетегированные кадры. Интерфейс Access может присоединиться только к одной VLAN.

Trunk - Магистральный интерфейс

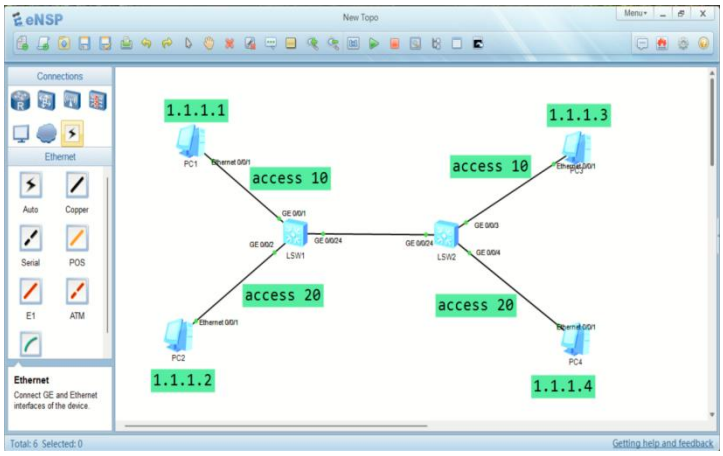
Магистральные интерфейсы позволяют пропускать кадры данных из нескольких VLAN, которые

различаются тегами 802.1Q. Магистральные интерфейсы обычно используются для взаимодействия между коммутаторами, а также для подключения субинтерфейсов маршрутизаторов, межсетевых экранов и других устройств.

Hybrid - Гибридные интерфейсы похожи на магистральные тем, что через них также могут проходить кадры данных из нескольких VLAN, причем эти кадры различаются по меткам 802.1Q. Пользователи имеют возможность указать, будет ли гибридный интерфейс передавать метку при отправке кадров данных для определенной VLAN (или определенных VLAN).

Создать виртуальной локальной компьютерной сети (VLAN)

```
<Huawei>sys
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys sw1
[sw1]vlan batch 10 20
Info: This operation may take a few seconds. Please wait for a
moment...done.
[sw1]
```

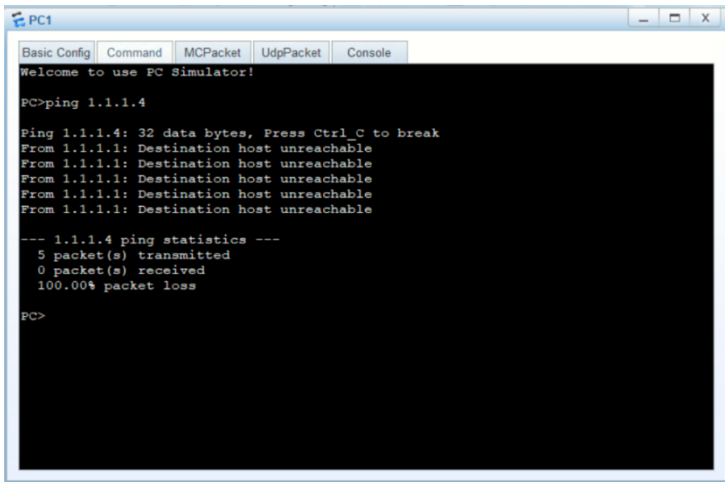



```
[sw1]dis vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
-
U: Up;          D: Down;          TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                 ST: Vlan-stacking;
#: ProtocolTransparent-vlan;      *: Management-vlan;
--------------------------------------------------------------------------------
-
VID  Type    Ports
--------------------------------------------------------------------------------
-
1    common  UT:GE0/0/1(U)       GE0/0/2(U)       GE0/0/3(D)       GE0/0/4(D)
                GE0/0/5(D)       GE0/0/6(D)       GE0/0/7(D)       GE0/0/8(D)
                GE0/0/9(D)       GE0/0/10(D)      GE0/0/11(D)      GE0/0/12(D)
```

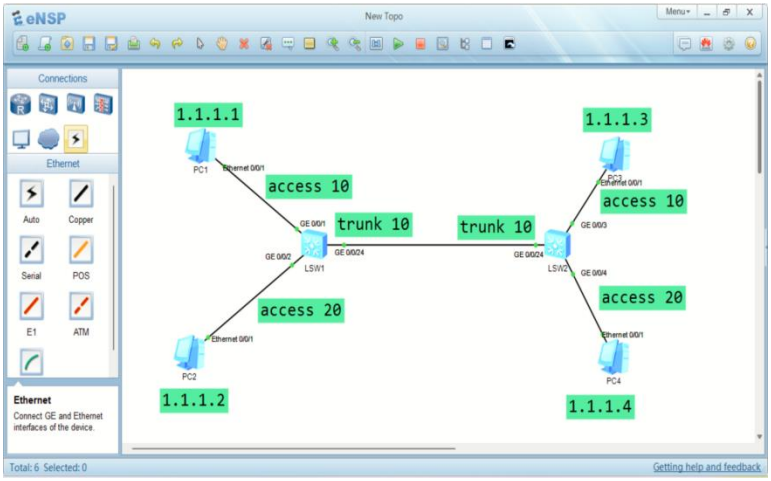
```
               GE0/0/13(D)     GE0/0/14(D)     GE0/0/15(D)     GE0/0/16(D)
               GE0/0/17(D)     GE0/0/18(D)     GE0/0/19(D)     GE0/0/20(D)
               GE0/0/21(D)     GE0/0/22(D)     GE0/0/23(D)     GE0/0/24(U)

10   common
20   common

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
-
1    enable  default       enable  disable    VLAN 0001
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
[sw1]int g0/0/1
[sw1-GigabitEthernet0/0/1]port link-type access
[sw1-GigabitEthernet0/0/1]port default vlan 10
[sw1-GigabitEthernet0/0/1]int g0/0/2
[sw1-GigabitEthernet0/0/2]port link-type access
[sw1-GigabitEthernet0/0/2]port default vlan 20
[sw1-GigabitEthernet0/0/2]dis port vlan active
T=TAG U=UNTAG
--------------------------------------------------------------------------------
Port                Link Type    PVID    VLAN List
--------------------------------------------------------------------------------
GE0/0/1             access       10      U: 10
GE0/0/2             access       20      U: 20
GE0/0/3             hybrid       1       U: 1
GE0/0/4             hybrid       1       U: 1
GE0/0/5             hybrid       1       U: 1
GE0/0/6             hybrid       1       U: 1
GE0/0/7             hybrid       1       U: 1
GE0/0/8             hybrid       1       U: 1
GE0/0/9             hybrid       1       U: 1
GE0/0/10            hybrid       1       U: 1
GE0/0/11            hybrid       1       U: 1
GE0/0/12            hybrid       1       U: 1
GE0/0/13            hybrid       1       U: 1
GE0/0/14            hybrid       1       U: 1
GE0/0/15            hybrid       1       U: 1
GE0/0/16            hybrid       1       U: 1
GE0/0/17            hybrid       1       U: 1
GE0/0/18            hybrid       1       U: 1
GE0/0/19            hybrid       1       U: 1
GE0/0/20            hybrid       1       U: 1
GE0/0/21            hybrid       1       U: 1
GE0/0/22            hybrid       1       U: 1
GE0/0/23            hybrid       1       U: 1
GE0/0/24            hybrid       1       U: 1
[sw1-GigabitEthernet0/0/2]
[sw1-GigabitEthernet0/0/2]q
[sw1]q
<sw1>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]:


<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys sw2
[sw2]un in en
Info: Information center is disabled.
[sw2]vlan batch 10 20
```

```
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw2]dis vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
-
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
-

VID  Type    Ports
--------------------------------------------------------------------------------
-

1    common  UT:GE0/0/1(D)      GE0/0/2(D)      GE0/0/3(U)      GE0/0/4(U)
                GE0/0/5(D)      GE0/0/6(D)      GE0/0/7(D)      GE0/0/8(D)
                GE0/0/9(D)      GE0/0/10(D)     GE0/0/11(D)     GE0/0/12(D)
                GE0/0/13(D)     GE0/0/14(D)     GE0/0/15(D)     GE0/0/16(D)
                GE0/0/17(D)     GE0/0/18(D)     GE0/0/19(D)     GE0/0/20(D)
                GE0/0/21(D)     GE0/0/22(D)     GE0/0/23(D)     GE0/0/24(U)
10   common
20   common

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
-
1    enable  default       enable  disable    VLAN 0001
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020

[sw2]int g0/0/3
[sw2-GigabitEthernet0/0/3]port link-type  access
[sw2-GigabitEthernet0/0/3]port default vlan 10
[sw2-GigabitEthernet0/0/3]int g0/0/4
[sw2-GigabitEthernet0/0/4]port link-type access
[sw2-GigabitEthernet0/0/4]port default vlan 20
[sw2-GigabitEthernet0/0/4]dis port vlan active
T=TAG U=UNTAG
--------------------------------------------------------------------------------
Port                Link Type    PVID    VLAN List
--------------------------------------------------------------------------------
GE0/0/1             hybrid       1       U: 1
GE0/0/2             hybrid       1       U: 1
GE0/0/3             access       10      U: 10
GE0/0/4             access       20      U: 20
GE0/0/5             hybrid       1       U: 1
GE0/0/6             hybrid       1       U: 1
GE0/0/7             hybrid       1       U: 1
GE0/0/8             hybrid       1       U: 1
GE0/0/9             hybrid       1       U: 1
GE0/0/10            hybrid       1       U: 1
GE0/0/11            hybrid       1       U: 1
GE0/0/12            hybrid       1       U: 1
GE0/0/13            hybrid       1       U: 1
GE0/0/14            hybrid       1       U: 1
GE0/0/15            hybrid       1       U: 1
GE0/0/16            hybrid       1       U: 1
GE0/0/17            hybrid       1       U: 1
GE0/0/18            hybrid       1       U: 1
GE0/0/19            hybrid       1       U: 1
GE0/0/20            hybrid       1       U: 1
GE0/0/21            hybrid       1       U: 1
```

```
GE0/0/22            hybrid       1       U: 1
GE0/0/23            hybrid       1       U: 1
GE0/0/24            hybrid       1       U: 1
[sw2-GigabitEthernet0/0/4]
[sw2-GigabitEthernet0/0/4]q
[sw2]q
<sw2>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]:
Now saving the current configuration to the slot 0.
Save the configuration successfully.
```




```
<sw2>sys
Enter system view, return user view with Ctrl+Z.
[sw2]int g0/0/24
[sw2-GigabitEthernet0/0/24]port link-type trunk
[sw2-GigabitEthernet0/0/24]port trunk allow-pass vlan 10
[sw2-GigabitEthernet0/0/24]dis this
#
interface GigabitEthernet0/0/24
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
[sw2-GigabitEthernet0/0/24]port link-type trunk
[sw2-GigabitEthernet0/0/24]port trunk allow-pass vlan 20
[sw2-GigabitEthernet0/0/24]dis this
#
interface GigabitEthernet0/0/24
 port link-type trunk
 port trunk allow-pass vlan 10 20
```



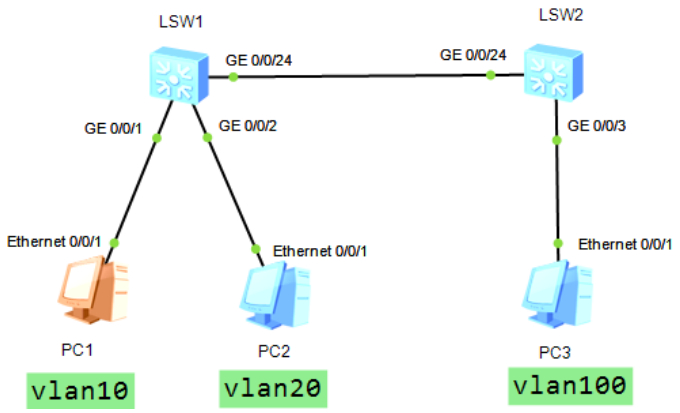

```
vlan batch 10 20
interface GigabitEthernet0/0/x
 port link-type trunk
 port trunk allow-pass vlan  x
dis port vlan active
dis vlan
----------------------------
port trunk pvid vlan x
```

измените G0/0/24 на SW1 и SW2 на гибридный тип.

```
dis this
undo  port trunk allow-pass vlan 10 20
undo  port trunk pvid vlan
undo port link-type
 port link-type hybrid
 port hybrid untagged vlan 10
 port hybrid tagged vlan 20
```

Измените порт G0/0/1 коммутатора SW1 на гибридный тип в соответствии со следующей конфигурацией, а затем pc1 пропингует pc3

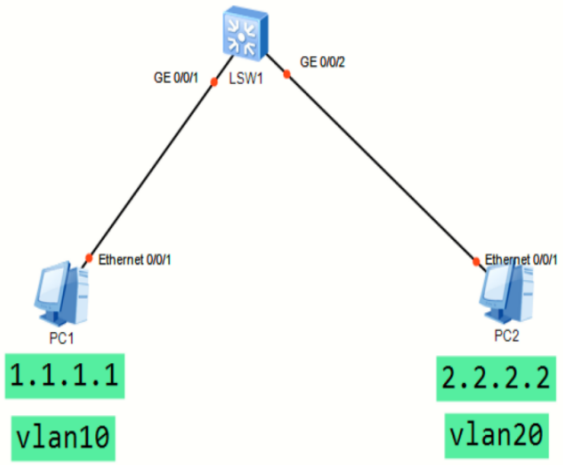
```
[SW1-GigabitEthernet0/0/1]undo port default vlan
[SW1-GigabitEthernet0/0/1]undo port link-type
[SW1-GigabitEthernet0/0/1]port link-type hybrid
[SW1-GigabitEthernet0/0/1]port hybrid untagged vlan 10
```



В соответствии с левым рисунком завершить конфигурирование, требования pc1 ping pc2 не проходит, но может ping pc3, написать команду конфигурации, описать весь процесс взаимодействия.

```
[SW1] vlan batch 10 20 100
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SW1-GigabitEthernet0/0/1] port hybrid untagged vlan 10 100
[SW1-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type hybrid
[SW1-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 20 100
[SW1-GigabitEthernet0/0/2] interface GigabitEthernet 0/0/24
[SW1-GigabitEthernet0/0/24] port link-type hybrid
[SW1-GigabitEthernet0/0/24] port hybrid tagged vlan 10 20 100

[SW2] vlan batch 10 20 100
[SW2] interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3] port link-type hybrid
[SW2-GigabitEthernet0/0/3] port hybrid pvid vlan 100
[SW2-GigabitEthernet0/0/3] port hybrid untagged vlan 10  20 100
[SW2-GigabitEthernet0/0/3] interface GigabitEthernet 0/0/24
[SW2-GigabitEthernet0/0/24] port link-type hybrid
[SW2-GigabitEthernet0/0/24] port hybrid tagged vlan 10 20 100
```

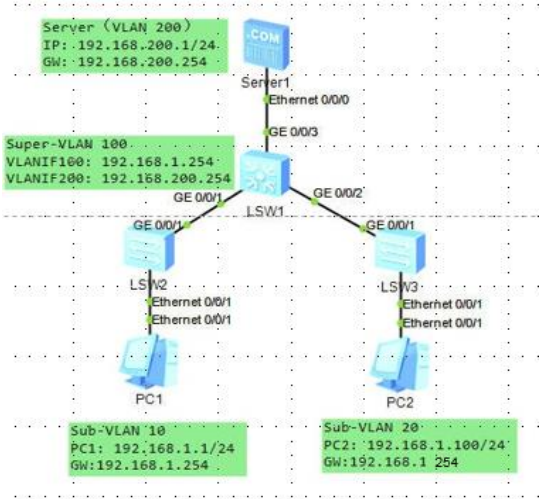
Межсетевое взаимодействие VLAN



Команды конфигурации

```
[SW1]vlan batch 10 20
[SW1]int g0/0/1
[SW1-GigabitEthernet0/0/1]port link-type access
[SW1-GigabitEthernet0/0/1]port default vlan 10
[SW1]int g0/0/2
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 20
[SW1]int vlanif10
[SW1-Vlanif10]ip add 172.16.12.254 24
[SW1]int vlanif20
[SW1-Vlanif20]ip add 192.168.12.254 24
[SW1]dis ip int bri
[SW1]dis ip rou
```

Передовые технологии VLAN




```
<SW1>
[SW1] vlan batch 10 20 #创建 Sub-VLAN
[SW1] interface GigabitEthernet0/0/1
[SW1-GigabitEthernet0/0/1] port link-type trunk
[SW1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SW1] interface GigabitEthernet0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[SW1] vlan 100 Super-VLAN
[SW1-vlan100] aggregate-vlan
[SW1-vlan100] access-vlan 10 20 VLAN100 Sub-VLAN
[SW1] interface vlanif 100
[SW1-vlanif100] ip address 192.168.1.254 24
[SW1-vlanif100] arp-proxy inter-sub-vlan-proxy enable Sub-VLAN Proxy ARP


[SW1] vlan 200
[SW1] interface GigabitEthernet0/0/3
[SW1-GigabitEthernet0/0/3] port link-type access
[SW1-GigabitEthernet0/0/3] port default vlan 200
[SW1] interface vlanif 200
[SW1-VLANIF200] ip address 192.168.200.254 24


SW2
[SW2] vlan 10
[SW2] interface GigabitEthernet0/0/1
[SW2-GigabitEthernet0/0/1] port link-type trunk
[SW2-GigabitEthernet0/0/1] ] port trunk allow-pass vlan 10
[SW2] interface Ethernet 0/0/1
[SW2-Ethernet0/0/1] port link-type access
[SW2-Ethernet0/0/1port default vlan 10


SW3
[SW3] vlan 20
[SW3] interface GigabitEthernet0/0/1
[SW3-GigabitEthernet0/0/1] port link-type trunk
[SW3-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[SW3] interface Ethernet 0/0/1
[SW3-Ethernet0/0/1] port link-type access
[SW3-Ethernet0/0/1] port default vlan 20
```

11. Протокол STP (802.1D)

Протокол STP (Spanning Tree Protocol) является ключевым механизмом для предотвращения петель в локальных сетях Ethernet. В этом разделе мы рассмотрим, как работает STP в симуляторе eNSP, и изучим основные концепции, лежащие в его основе.

Базовые понятия STP.

Корневой мост

Ключевым элементом STP является корневой мост - коммутатор, который выбирается в качестве центра топологии. Этот коммутатор становится точкой отсчета для вычисления кратчайших путей до остальных устройств сети.

Порты коммутатора

Каждый порт коммутатора может находиться в одном из четырех состояний: корневой, назначенный, альтернативный или отключенный. Эти состояния определяют роль порта в топологии STP.

Стоимость пути - Каждому порту назначается определенная стоимость пути, которая зависит от скорости линка. STP выбирает пути с наименьшей совокупной стоимостью для предотвращения петель.

Настройка и наблюдение STP в eNSP

Включение STP

Для активации STP необходимо выполнить команду "stp enable" в режиме конфигурации интерфейса или всего коммутатора.

Просмотр информации

Используйте команды "display stp" и "display stp brief" для получения подробной информации о состоянии STP, включая выбранный корневой мост, стоимости путей и состояния порт

Настройка приоритетов

Приоритет коммутатора в STP можно изменить командой "stp priority", что позволяет влиять на выбор корневого моста.

Отладка

Для более глубокого анализа STP можно использовать команды "debugging stp" и "debugging stp event".

Защита STP от атак

Атаки на корневой мост

Злоумышленники могут попытаться подделать идентификатор корневого моста, чтобы перенаправить трафик через контролируемые ими устройства. Для защиты необходимо использовать аутентификацию BPDU.

Атаки на порты

Злоумышленники могут пытаться вывести из строя отдельные порты, чтобы вызвать перестройку топологии. Защититься можно с помощью BPDU Guard и Root Guard.

Атаки на сообщения BPDU

Подмена BPDU-сообщений может привести к нарушению работы STP. Для защиты используются аутентификация и ограничение BPDU.

Расширенные возможности STP:

RSTP - Rapid Spanning Tree Protocol (RSTP) улучшенная версия STP, которая обеспечивает более быструю сходимость топологии и поддерживает гибридные сети.

MSTP - Multiple Spanning Tree Protocol (MSTP) позволяет создавать несколько независимых экземпляров STP, каждый из которых отвечает за свой набор VLAN.

PVST+ - Per-VLAN Spanning Tree Plus (PVST+) поддерживает отдельные экземпляры STP для каждого VLAN, обеспечивая гибкость и производительность.

Лучшие практики STP

Оптимизация приоритетов

Тщательно настраивайте приоритеты коммутаторов, чтобы обеспечить желаемый выбор корневого моста и эффективную топологию.

Ограничение портов

Используйте BPDU Guard и Root Guard для защиты от атак на порты и предотвращения неправильной перестройки сети.

Мониторинг и отладка

Регулярно проверяйте состояние STP, используя команды просмотра и отладки, чтобы выявлять и устранять проблемы.

Безопасность BPDU

Внедряйте аутентификацию BPDU, чтобы предотвратить подмену сообщений и повысить общую безопасность.

Таблица – 11.1. Устранение неполадок STP

Проблема	**Возможные причины**	**Рекомендации по устранению**
Неправильный выбор корневого моста	- Неверные приоритеты коммутаторов - Нарушение физического подключения	- Настройка приоритетов коммутаторов - Проверка физических линков
Неактивные порты	- Неверная конфигурация портов - Конфликты с другими протоколами	- Проверка состояния и настроек портов - Устранение конфликтов с другими протоколами
Перестройка топологии	- Атаки на сообщения BPDU - Проблемы с физическими линками	- Внедрение аутентификации BPDU - Поиск и устранение проблем с линками

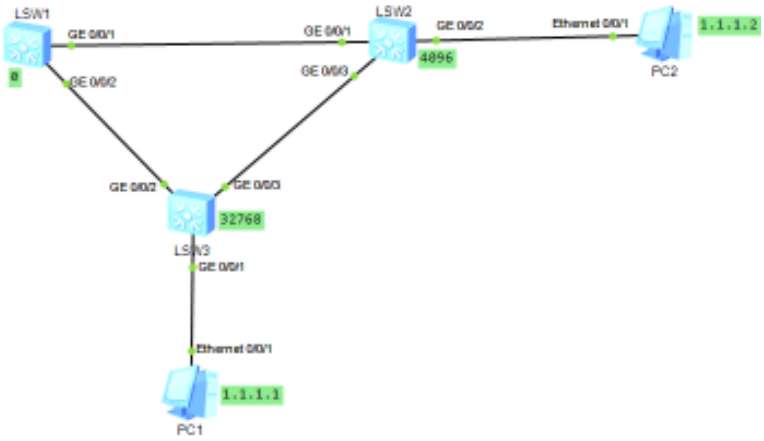
Протокол STP играет ключевую роль в предотвращении петель в локальных сетях Ethernet. Понимание базовых концепций STP, включая выбор корневого моста и состояния портов, позволяет эффективно настраивать и обслуживать сетевую инфраструктуру. Кроме того, важно применять передовые методы защиты STP от различных атак и проблем, чтобы обеспечить надежность и масштабируемость сети. Использование eNSP позволяет практически отрабатывать навыки работы с STP в безопасной виртуальной среде.

STP протокол связующего дерева, разработан для блокировки интерфейса, чтобы сеть больше не формировалась. В отличие от ручного выключения интерфейса, STP не отключает питание интерфейса, а блокирует пересылку пакетов, кроме пакетов STP.

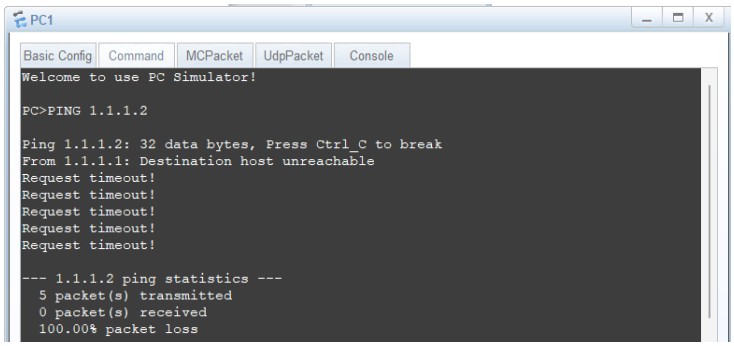
Как работает STP?

STP определяет пять состояний переадресации интерфейса, пересылку, обучение, прослушивание, блокировку и отключение, а также три роли интерфейса, назначенный порт, корневой порт и заблокированный порт.

Топология дерева должна иметь корень. Как определено в STP, устройство, которое функционирует как корень древовидной сети, называется корневым мостом. Во всей сети STP есть только один корневой мост. Хотя корневой мост не обязательно находится в физическом центре сети, он функционирует как ее логический центр. Корневой мост динамически изменяется в зависимости от топологии сети. После конвергенции сети корневой мост генерирует конфигурационные BPDU и отправляет их другим устройствам через определенные промежутки времени. Другие устройства обрабатывают и пересылают конфигурационные BPDU, чтобы сообщить об изменениях топологии нисходящим устройствам.

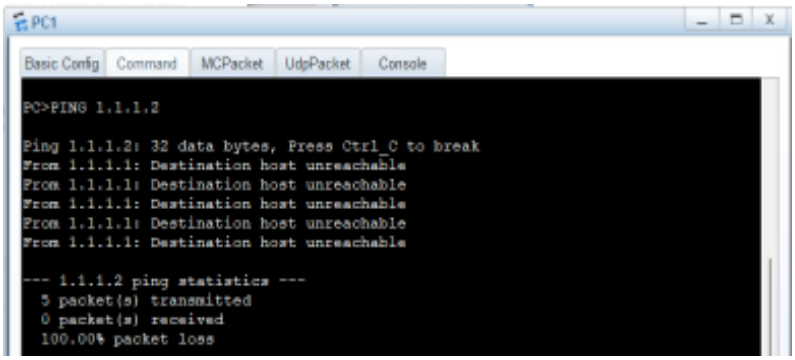



```
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys sw1
[sw1]stp disable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.

The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys sw2
[sw2]stp disable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.

The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys sw3
[sw3]stp disable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.

<PC1> ping 1.1.1.2
```




```
[sw1]dis
[sw1]display mac-vlan
[sw1]display mac-address
```

```
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
5489-9880-3012 1           -      -      GE0/0/1         dynamic   0/-
5489-98f9-5657 1           -      -      GE0/0/1         dynamic   0/-
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 2


[sw1]stp enable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw1] User interface con0 is available

[sw2] display mac-vlan
[sw2]display mac-address
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
5489-9880-3012 1           -      -      GE0/0/3         dynamic   0/-
5489-98f9-5657 1           -      -      GE0/0/2         dynamic   0/-
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 2

[sw2]stp enable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw2] User interface con0 is available


[sw3]display mac-vlan
[sw3]display mac-address
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/LSR-ID
               VSI/SI                                              MAC-Tunnel
-------------------------------------------------------------------------------
5489-9880-3012 1           -      -      GE0/0/3         dynamic   0/-
5489-98f9-5657 1           -      -      GE0/0/3         dynamic   0/-
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 2

[sw3]stp enable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.

<PC1>ping 1.1.1.2
```

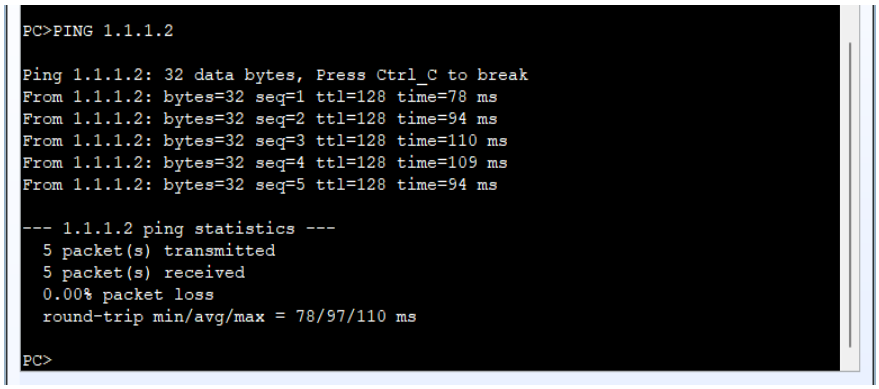


```
[sw1]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
[sw1]stp priority 0
[sw1]q
<sw1>
```

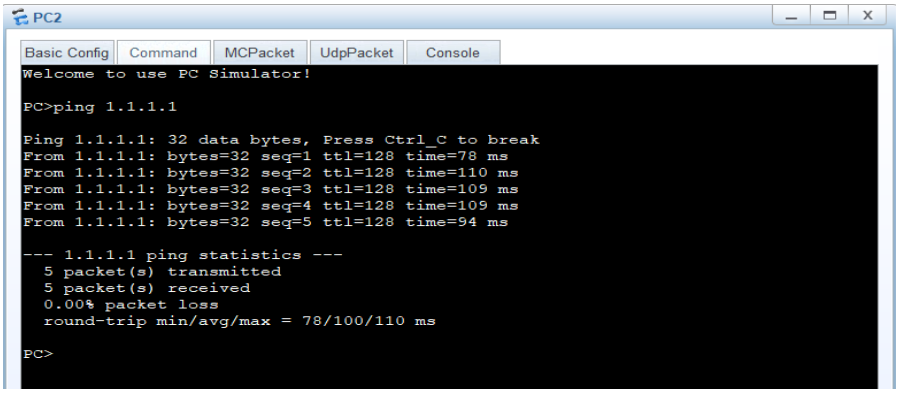
```
[sw2]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  LEARNING        NONE
   0    GigabitEthernet0/0/3        ALTE  DISCARDING      NONE
[sw2]stp priority 4096
[sw2]q
<sw2>
```

```
[SW3]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/3        ALTE  DISCARDING      NONE
[SW3]stp priority 32768
[SW3]q
<SW3>
```

```
<PC1>ping 1.1.1.2
```




```
<PC2>ping 1.1.1.1
```



12. Основы протокола OSPF

Открытая кратчайшая трассировка стоп-сигналов (OSPF - Open Shortest Path First) - это динамический протокол маршрутизации, который широко используется в современных корпоративных и провайдерских сетях. Понимание фундаментальных принципов OSPF является ключевым для дизайна, настройки и управления маршрутизацией в сложных сетевых средах.

OSPF - протокол динамической маршрутизации, который автоматически находит и перестраивает маршруты при изменениях в сети. Он постоянно анализирует состояние всех доступных маршрутов и с помощью алгоритма выбирает лучший. Благодаря этому OSPF особенно эффективен в высоконагруженных сетях, где необходимо бесперебойно и без задержек передавать большие объёмы данных.

Архитектура OSPF:

Области (Areas) - Сеть OSPF разделяется на логические области для масштабируемости и избежания чрезмерной нагрузки на маршрутизаторы. Каждая область имеет свою базу данных состояния канала связи, что позволяет ограничить распространение информации о маршрутах только внутри области.

Пограничные маршрутизаторы - Пограничные маршрутизаторы соединяют области OSPF и отвечают за агрегацию и распространение маршрутной информации между ними. Они играют ключевую роль в обеспечении масштабируемости и управляемости сетью.

Центральные маршрутизаторы - Центральные маршрутизаторы отвечают за построение и поддержание базы данных топологии внутри своей области. Они обмениваются информацией о состоянии каналов с другими маршрутизаторами в области для расчета оптимальных маршрутов.

Процесс сходимости OSPF:

Обнаружение соседей

Маршрутизаторы OSPF обнаруживают своих соседей, используя протокол приветствия (hello). Этот шаг устанавливает соседние отношения и определяет параметры соседства, такие как идентификаторы, интервалы приветствий, ключи аутентификации и др.

Выборы DR/BDR

На многоточечных сетях (например, Ethernet) маршрутизаторы OSPF выбирают Назначенного Маршрутизатора (DR) и Резервного Назначенного Маршрутизатора (BDR). Эти роли отвечают за эффективную рассылку и обновление информации о состоянии каналов.

Распространение LSA

Маршрутизаторы OSPF обмениваются пакетами состояния каналов (Link State Advertisements - LSA), которые содержат информацию об их подключенных интерфейсах. Этот процесс позволяет построить базу данных топологии сети.

Маршрутизация в OSPF:

Стоимость каналов - OSPF использует метрику стоимости каналов для определения оптимальных маршрутов. Чем ниже стоимость, тем предпочтительнее канал. Администраторы могут настраивать стоимость вручную для балансировки нагрузки.

Внутренние и внешние маршруты - OSPF различает внутренние маршруты (внутри одной области) и внешние маршруты (между областями). Внутренние маршруты имеют приоритет перед внешними, что обеспечивает предсказуемость маршрутизации.

Вычисление маршрутов - На основе полученной базы данных топологии OSPF использует алгоритм Дейкстры для вычисления кратчайших путей до всех известных сетей. Эти оптимальные маршруты заносятся в таблицу маршрутизации (таблица – 12.1).

Таблица – 12.1. Типы пакетов OSPF

Приветствие (Hello)	**Обновление состояния канала (LSU)**	**Запрос состояния канала (LSR)**	**Подтверждение состояния канала (LSAck)**
Пакеты приветствия используются для обнаружения соседних маршрутизаторов и установления соседских отношений.	Пакеты обновления состояния канала (Link State Update) используются для распространения информации о состоянии каналов между маршрутизаторами.	Пакеты запроса состояния канала (Link State Request) используются для запроса недостающей информации о состоянии каналов.	Пакеты подтверждения состояния канала (Link State Acknowledgment) используются для подтверждения получения пакетов обновления состояния канала.

Конфигурация OSPF

1) Настройка интерфейсов - Первым шагом является настройка OSPF на интерфейсах маршрутизаторов, включая назначение области, стоимости канала, идентификатора маршрутизатора и других параметров.

2) Определение областей - Следующим шагом является разделение сети на логические области OSPF, определение пограничных маршрутизаторов и настройка параметров межобластной маршрутизации.

3) Оптимизация параметров - Для повышения производительности и надежности OSPF можно настроить дополнительные параметры, такие как интервалы приветствий, таймеры сходимости, Authentication и т.д.

Преимущества OSPF

1) Масштабируемость

Архитектура OSPF с разбиением на области позволяет масштабировать сети до огромных размеров без потери производительности.

2) Быстрая сходимость

OSPF использует эффективные алгоритмы обнаружения изменений в топологии и быстрого распространения обновлений, что обеспечивает быструю сходимость маршрутной информации.

3) Безопасность

OSPF поддерживает механизмы аутентификации, шифрования и защиты от несанкционированного доступа, что повышает безопасность сети.

4) Гибкость

OSPF предоставляет богатый набор возможностей по настройке метрик, фильтрации маршрутов, балансировке нагрузки и другим аспектам маршрутизации.

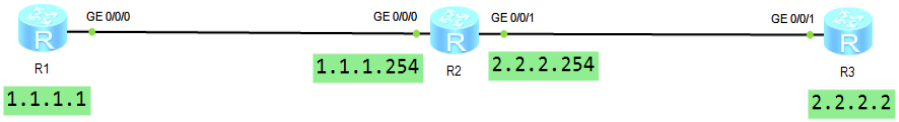
Таблица – 12.2. Применение OSPF

Корпоративные сети	OSPF широко применяется для построения маршрутизации в крупных корпоративных сетях, обеспечивая масштабируемость, отказоустойчивость и гибкость управления.
Сети провайдеров	Магистральные сети провайдеров часто используют OSPF для динамической маршрутизации между точками присутствия и филиалами клиентов.
Гибридные облачные сети	OSPF помогает интегрировать локальные корпоративные сети с облачными сервисами, обеспечивая единое пространство маршрутизации.

Данные между устройствами передаются через сеть, которая бывает глобальной или локальной (LAN) - в пределах дома или офиса. Чтобы данные достигли адресата, их нужно направлять по правильному пути. За это отвечает система маршрутизации, выполняющая

роль навигатора для сетевого оборудования. Маршрутизация может быть статической или динамической.

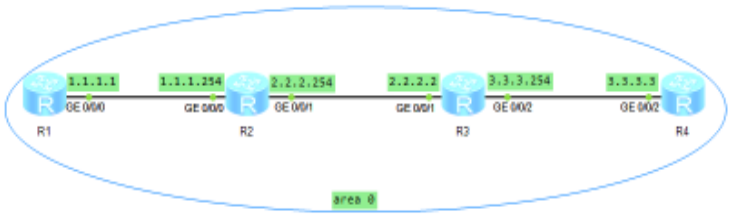
Первый эксперимент




```
R1
<Huawei>system-view
Enter system view, return user view with Ctrl+Z
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysname R1
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 1.1.1.1 24
[R1-GigabitEthernet0/0/0]q

R2
<Huawei>system-view
Enter system view, return user view with Ctrl+Z
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysname R2
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 1.1.1.254 24
[R2-GigabitEthernet0/0/0]int g0/0/1
[R2-GigabitEthernet0/0/1]ip add 2.2.2.254 24
[R2-GigabitEthernet0/0/1]dis ip int bri
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 8
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 8

Interface                         IP Address/Mask      Physical   Protocol
Ethernet0/0/0                     unassigned           down       down
Ethernet0/0/1                     unassigned           down       down
GigabitEthernet0/0/0              1.1.1.254/24         up         up
GigabitEthernet0/0/1              2.2.2.254/24         up         up
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
[R2-GigabitEthernet0/0/1]


R3
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
```

```
Info: Information center is disabled.
[Huawei]sysname R3
[R3]int g0/0/1
[R3-GigabitEthernet0/0/1]ip add 2.2.2.2 24
[R3-GigabitEthernet0/0/1]q
[R3]ip route-static 1.1.1.0 24 2.2.2.254
[R3]


R1
[R1]ip route-static 2.2.2.0 24 1.1.1.254
[R1]dis ip rou 2.2.2.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        2.2.2.0/24  Static  60   0           RD   1.1.1.254
GigabitEthernet
0/0/0

[R1]ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=254 time=120 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=254 time=60 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=254 time=50 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=254 time=40 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/62/120 ms
[R1]
```

Второй эксперимент




```
R1
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R1
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 1.1.1.1 24
[R1-GigabitEthernet0/0/0]

R2
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
```

```
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R2
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 1.1.1.254 24
[R2-GigabitEthernet0/0/0]int g0/0/1
[R2-GigabitEthernet0/0/1]ip add 2.2.2.254 24
[R2-GigabitEthernet0/0/1
```

```
R3
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R3
[R3]INT G0/0/1
[R3-GigabitEthernet0/0/1]ip add 2.2.2.2 24
[R3-GigabitEthernet0/0/1]int g0/0/2
[R3-GigabitEthernet0/0/2]ip add 3.3.3.254 24
[R3-GigabitEthernet0/0/2]
```

```
R4
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R4
[R4]int g0/0/2
[R4-GigabitEthernet0/0/2]ip add 3.3.3.3 24
[R4-GigabitEthernet0/0/2]
```

```
R1
[R1-GigabitEthernet0/0/0]q
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]dis ip int bri
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 9
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 9

Interface                         IP Address/Mask      Physical   Protocol
Ethernet0/0/0                     unassigned           down       down
Ethernet0/0/1                     unassigned           down       down
GigabitEthernet0/0/0              1.1.1.1/24           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
[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.255
```

```
[R1-ospf-1-area-0.0.0.0]dis this
#
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
#
return
[R1-ospf-1-area-0.0.0.0]q
[R1-ospf-1]q
[R1]
```

```
R2
[R2-GigabitEthernet0/0/1]q
[R2]ospf 1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 1.1.1.254 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 2.2.2.254 0.0.0.255
[R2-ospf-1-area-0.0.0.0]q
[R2-ospf-1]q
[R2]

R3
[R3-GigabitEthernet0/0/2]q
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 3.3.3.254 0.0.0.255
[R3-ospf-1-area-0.0.0.0]q
[R3-ospf-1]q
[R3]

R4
[R4-GigabitEthernet0/0/2]q
[R4]ospf 1
[R4-ospf-1]area 0
[R4-ospf-1-area-0.0.0.0]network 3.3.3.3 0.0.0.255
[R4-ospf-1-area-0.0.0.0]q
[R4-ospf-1]q
[R4]

R1
[R1]ping 3.3.3.3
  PING 3.3.3.3: 56  data bytes, press CTRL_C to break
    Reply from 3.3.3.3: bytes=56 Sequence=1 ttl=253 time=50 ms
    Reply from 3.3.3.3: bytes=56 Sequence=2 ttl=253 time=80 ms
    Reply from 3.3.3.3: bytes=56 Sequence=3 ttl=253 time=80 ms
    Reply from 3.3.3.3: bytes=56 Sequence=4 ttl=253 time=70 ms

  --- 3.3.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/68/80 ms
[R1]
```

13. Списки контроля доступа ACL

Списки контроля доступа (Access Control Lists, ACL) представляют собой мощный инструмент управления доступом в современных сетевых средах. Они позволяют системным администраторам и специалистам по кибербезопасности тонко настраивать разрешения и ограничения для различных пользователей, групп и сетевых объектов, обеспечивая надежную защиту информационных ресурсов.

Основные понятия и концепции ACL

1) Субъекты и объекты

Субъекты - это пользователи, группы, процессы или другие сущности, которым необходим доступ к ресурсам. Объекты - это файлы, каталоги, сетевые устройства, базы данных и другие ресурсы, к которым применяются правила доступа.

2) Разрешения и запреты

ACL определяют, какие конкретно действия (чтение, запись, выполнение и т.д.) разрешены или запрещены для каждого субъекта в отношении каждого объекта.

3) Модели управления доступом

Существует несколько моделей управления доступом, таких как дискреционное управление доступом (DAC), мандатное управление доступом (MAC) и управление доступом на основе ролей (RBAC). Каждая модель имеет свои особенности и предназначена для решения различных задач.

Применение ACL в различных средах

1) Сетевая безопасность - В сетевой безопасности ACL используются для фильтрации трафика, ограничения доступа к сетевым сервисам и устройствам, а также для обеспечения разграничения полномочий между пользователями и группами.

2) Безопасность операционных систем - На уровне операционных систем ACL применяются для настройки разрешений на файлы, каталоги и другие объекты, обеспечивая контроль доступа к критически важным ресурсам.

3) Безопасность облачных сред - В облачных средах ACL используются для управления доступом к облачным ресурсам, таким как виртуальные машины, хранилища данных, сетевые компоненты и службы.

Принципы эффективного управления ACL

1) Принцип наименьших полномочий

Предоставляйте пользователям и процессам только те права, которые необходимы для выполнения их задач. Это позволяет минимизировать риски, связанные с несанкционированным доступом.

2) Регулярный аудит

Периодически анализируйте и пересматривайте действующие ACL, чтобы выявлять и устранять устаревшие или избыточные правила, а также обеспечивать соответствие политикам безопасности.

3) Автоматизация управления

Используйте инструменты и скрипты для автоматизации процессов создания, обновления и применения ACL. Это позволяет снизить вероятность ошибок и обеспечить согласованность правил во всей инфраструктуре.

Лучшие практики конфигурации ACL

1) Наследование политик

Используйте наследование политик для повторного использования и распространения ACL-правил на множество объектов. Это позволяет поддерживать последовательность и единообразие в управлении доступом.

2) Гранулярность правил

Создавайте максимально детализированные и конкретные ACL-правила. Это помогает избежать избыточных разрешений и обеспечивает точный контроль доступа.

3) Интеграция с другими системами

Интегрируйте ACL с другими компонентами безопасности, такими как системы управления личными данными, решения для аутентификации и авторизации. Это повышает общую эффективность системы управления доступом.

Практические примеры применения ACL

1) Контроль доступа к файлам

Использование ACL для ограничения доступа к конфиденциальным файлам и каталогам на файловых серверах, обеспечивая соответствие политикам безопасности.

2) Фильтрация сетевого трафика

Применение ACL на сетевых устройствах для контроля входящих и исходящих соединений, блокирования нежелательного трафика и предотвращения несанкционированного доступа.

3) Управление облачными ресурсами

Использование ACL для предоставления доступа к виртуальным машинам, хранилищам данных и другим облачным сервисам в соответствии с ролями и правами пользователей.

Решение распространенных проблем с ACL

1) Конфликтующие правила

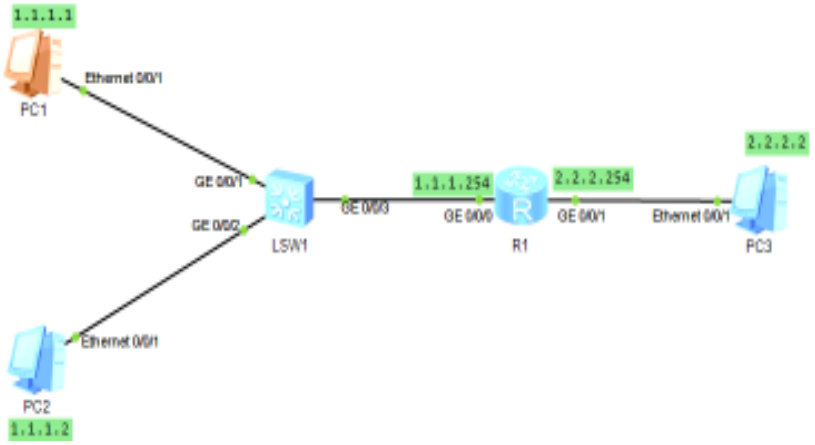
Регулярно проверяйте ACL на наличие противоречивых или перекрывающихся правил, которые могут привести к непредсказуемым результатам. Используйте инструменты для анализа и выявления таких конфликтов.

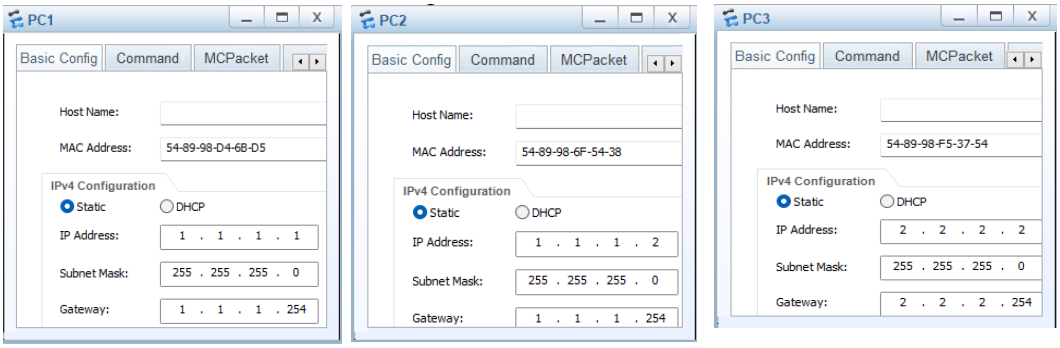
2) Снижение производительности

Следите за тем, чтобы правила ACL не становились слишком громоздкими и не оказывали негативного влияния на производительность систем. При необходимости оптимизируйте и упрощайте ACL-конфигурации.

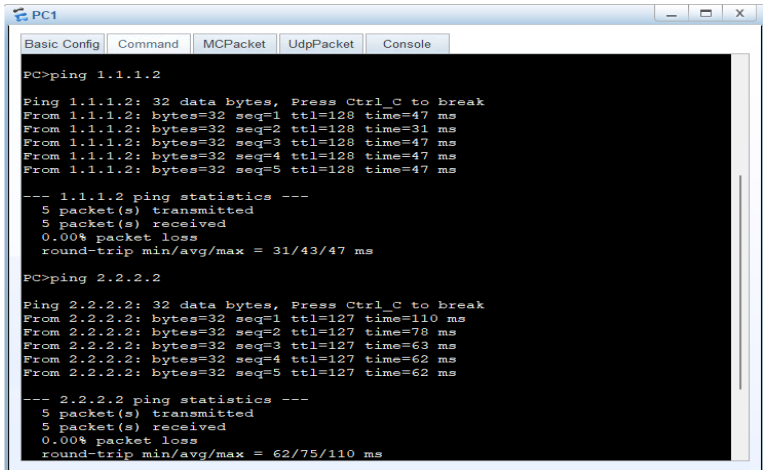
3) Аудит и отчетность

Регулярно проводите аудит существующих ACL, чтобы выявлять неиспользуемые или устаревшие правила, а также обеспечивать соответствие требованиям безопасности и нормативным актам.






```
R1
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R1
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 1.1.1.254 24
[R1-GigabitEthernet0/0/0]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 2.2.2.254 24
[R1-GigabitEthernet0/0/0]q
[R1]acl 2000
[R1-acl-basic-2000]undo rule 5
Error: The ACL subitem number does not exist!
[R1-acl-basic-2000]rule 5 deny source 1.1.1.1 0.0.0.0
[R1-acl-basic-2000]rule 10 deny source 1.1.1.3 0.0.0.0
[R1-acl-basic-2000]q
[R1-GigabitEthernet0/0/1]q
[R1]acl 2000
```



14. Трансляция сетевых адресов (NAT)

Трансляция сетевых адресов (NAT) используется многими сервис провайдерами и частными пользователями для решения проблемы нехватки реальных IP-адресов и обеспечения безопасности локальных сетей подключенных к Интернету. Например. Предприятие может иметь выделенный диапазон реальных IP-адресов, но гораздо большее количество компьютеров имеющих локальные IP-адреса которым необходим доступ в Интернет. Для решения этой проблемы используется технология трансляции адресов,

которая позволяет компьютерам локальной сети взаимодействовать с сетью Интернет, используя всего один внешний реальный IP-адрес.

NAT решает эту проблему с помощью подстановки общедоступного IP- адреса вместо локального IP-адреса Подставляя внутренний IP-адрес и порт вместо внешнего IP-адреса и порта, NAT сохраняет таблицу соответствия, затем при получении ответного пакета производится обратное преобразование.

К локальным IP-адресам относятся следующие диапазоны адресов: 10.xxx.xxx.xxx, 192.168.xxx.xxx, 172.16.xxx.xxx - 172.32.xxx.xxx.

Типы трансляторов сетевых адресов (NAT)

Трансляторы адресов подразделяются на 4 типа:

1. Symmetric NAT.
2. Full Cone NAT.
3. Address Restricted Cone NAT (он же Restricted NAT).
4. Port Restricted Cone NAT (или Port Restricted NAT)

В первых трех типах NATа разные IP-адреса внешней сети могут взаимодействовать с адресом из локальной сети используя один и тот же внешний порт. Четвертый тип, для каждого адреса и порта использует отдельный внешний порт.

NATы не имеют статической таблицы соответствия адресов и портов. Отображение открывается, когда первый пакет посылается из локальной сети наружу через NAT и действует определенный промежуток времени (как правило, 1-3 минуты), если пакеты через этот порт не проходят, то порт удаляется из таблицы соответствия. Обычно NAT распределяют внешние порты динамически, используется диапазон выше 1024.

1. Symmetric NAT

До недавнего времени это была наиболее распространённая реализация. Его характерная особенность – в таблице NAT маппинг адреса IL на адрес IG жёстко привязан к адресу OG, то есть к адресу назначения, который был указан в исходящем пакете, инициировавшем этот маппинг. При указанной реализации NAT в нашем примере хост 192.168.0.141 получит оттранслированные входящие UDP-пакеты только от хоста 1.2.3.4 и строго с портом источника 53 и портом назначения 1053 – ни от кого более. Пакеты от других хостов, даже если указанные в пакете адрес назначения и порт назначения присутствуют в таблице NAT, будут уничтожаться маршрутизатором. Это наиболее параноидальная реализация NAT, обеспечивающая более высокую безопасность для хостов локальной сети, но в некоторых случаях сильно усложняющая жизнь системных администраторов. Да и пользователей тоже.

2. Full Cone NAT

Эта реализация NAT – полная противоположность предыдущей. При Full Cone NAT входящие пакеты от любого внешнего хоста будут оттранслированы и переправлены соответствующему хосту в локальной сети, если в таблице NAT присутствует соответствующая запись. Более того, номер порта источника в этом случае тоже не имеет значения – он может быть и 53, и 54, и вообще каким угодно.

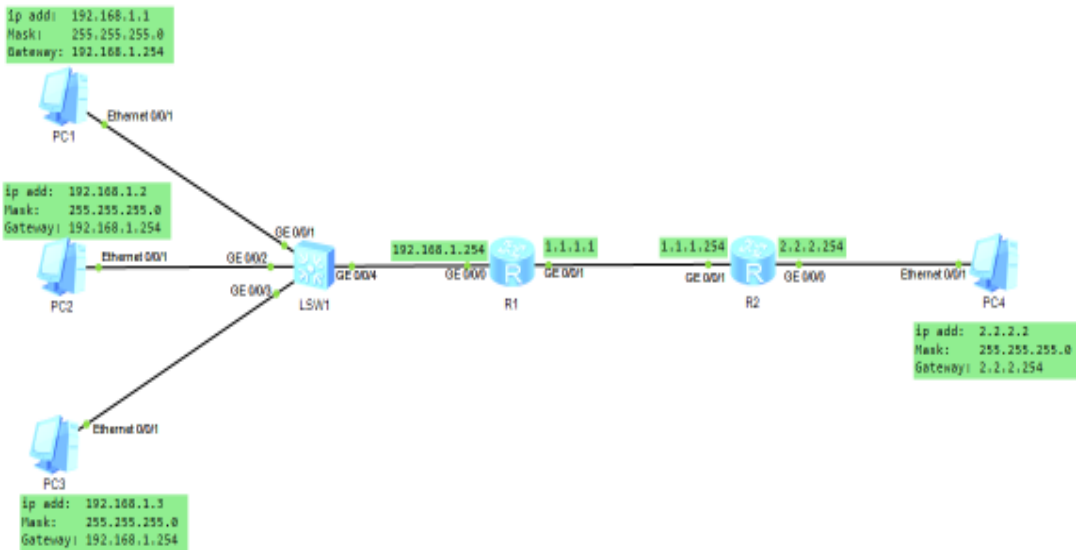
Например, если некое приложение, запущенное на компьютере в локальной сети, инициировало получение пакетов UDP от внешнего хоста 1.2.3.4 на локальный порт 4444, то пакеты UDP для этого приложения смогут слать также и 1.2.3.5, и 1.2.3.6, и вообще все до тех пор, пока запись в таблице NAT не будет по какой-либо причине удалена. Ещё раз: в этой реализации NAT во входящих пакетах проверяется только транспортный протокол, адрес назначения и порт назначения, адрес и порт источника значения не имеют.

3. Address Restricted Cone NAT (он же Restricted NAT)

Эта реализация занимает промежуточное положение между Symmetric и Full Cone реализациями NAT – маршрутизатор будет транслировать входящие пакеты только с определенного адреса источника (в нашем случае 1.2.3.4), но номер порта источника при этом может быть любым.

4. Port Restricted Cone NAT (или Port Restricted NAT)

То же, что и Address Restricted Cone NAT, но в этом случае маршрутизатор обращает внимание на соответствие номера порта источника и не обращает внимания на адрес источника. В нашем примере маршрутизатор будет транслировать входящие пакеты с любым адресом источника, но порт источника при этом обязан быть 53, в противном случае пакет будет уничтожен маршрутизатором.




```
R1
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R1
[R1]INT G0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.1.254 24
[R1-GigabitEthernet0/0/0]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 1.1.1.1 24
[R1-GigabitEthernet0/0/1]q
[R1]
```

```
R2
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys R2
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ip add 1.1.1.254 24
[R2-GigabitEthernet0/0/1]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 2.2.2.254 24
[R2-GigabitEthernet0/0/0]q
```

```
[R2]q
[R1]
[R1]ip route-static 2.2.2.0 24 1.1.1.254
[R1]q
<R1>ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=127 time=110 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=60 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=127 time=60 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/74/110 ms

<R1>
```

Теперь протокол NAT адрес

```
<R1>sys
Enter system view, return user view with Ctrl+Z.
[R1]nat address-group 1 1.1.1.2 1.1.1.10
[R1]acl 2000
[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000]q
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1
[R1-GigabitEthernet0/0/1]q
[R1]q

<R1>ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=60 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=80 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=127 time=60 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 60/67/80 ms

<R1>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=128 time=110 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=128 time=60 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=128 time=70 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=128 time=60 ms
    Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=128 time=60 ms

  --- 192.168.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/72/110 ms

<R1>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=128 time=90 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2 ttl=128 time=60 ms
    Reply from 192.168.1.2: bytes=56 Sequence=3 ttl=128 time=50 ms
    Reply from 192.168.1.2: bytes=56 Sequence=4 ttl=128 time=40 ms
    Reply from 192.168.1.2: bytes=56 Sequence=5 ttl=128 time=40 ms

  --- 192.168.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/56/90 ms

<R1>ping 192.168.1.3
  PING 192.168.1.3: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.3: bytes=56 Sequence=1 ttl=128 time=110 ms
    Reply from 192.168.1.3: bytes=56 Sequence=2 ttl=128 time=60 ms
    Reply from 192.168.1.3: bytes=56 Sequence=3 ttl=128 time=80 ms
    Reply from 192.168.1.3: bytes=56 Sequence=4 ttl=128 time=50 ms
    Reply from 192.168.1.3: bytes=56 Sequence=5 ttl=128 time=60 ms

  --- 192.168.1.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/72/110 ms

<R1>
```

15. Протокол DHCP

Для выхода в сеть любому устройству (компьютеру, смартфону) нужен IP-адрес. В зависимости от способа подключения он может быть постоянным или меняющимся. В первом случае адрес присваивается на постоянной основе, а во втором – действует только в течение одного подключения. Такое подключение работает по протоколу DHCP. В статье мы расскажем, что это за протокол и как он работает, а также покажем, как подключить DHCP на Windows.

Какой IP-адрес может быть у устройства

IP-адрес устройства может быть статическим или динамическим.

Статический адрес присваивается на постоянной основе, а динамический выдается на время (например, на одну сессию). Для автоматической выдачи динамических адресов используется прокол DHCP.

Чтобы получить статический адрес, нужно заказать его у своего интернет-провайдера. В этом случае к сети вы будете всегда подключаться под одним и тем же IP-адресом. Если вы не заказывали эту услугу, то каждый раз при выходе в сеть будете подключаться под разными IP.

В первом случае пользователь с правами администратора сети делает настройку сетевого адаптера вручную — задает ему статический адрес. Во втором — динамический IP присваивается автоматически через протокол DHCP.

Что такое Dynamic Host Configuration Protocol (DHCP)

DHCP - это протокол прикладного уровня, который помогает назначать IP-адреса устройствам при подключении к серверу. Протокол DHCP автоматизирует выдачу адресов, а также их передачу следующим пользователям после отключения устройств или их перехода из одной подсети в другую. Протокол динамического присвоения IP-адресов

функционирует по принципу DORA. **DORA** - это аббревиатура, которая обозначает названия этапов работы протокола DHCP:

- **D** – Discovery (обнаружение);
- **O** – Offer (предложение);
- **R** – Request (запрос);
- **A** – Acknowledge (подтверждение).

Протокол DHCP (принцип работы)

1. **Discovery (обнаружение)**. На первом этапе сервер проверяет, в сети ли устройство. Технически этот процесс выглядит, как отправка отдельного запроса на универсальный адрес 255.255.255.255. Поскольку на этапе обнаружения у нового пользователя отсутствует свой IP, с его стороны отправляется MAC-адрес (уникальный идентификатор устройства) и IP 0.0.0.0.

2. **Offer (предложение)**. На втором этапе подключения подбираются доступные варианты сетевой конфигурации присоединенного устройства. Сервер, работающий по протоколу DHCP, подбирает предложения с возможными подключениями и отправляет их на устройство по его уникальному MAC-адресу. По итогу для подключения выбирается только один вариант (чаще всего именно последний доступный вариант присоединения к сети).

3. **Request (запрос)**. На третьем этапе подключения по DHCP отправляется запрос на подключение с устройства клиента. После того как клиент получил предложение со стороны сетевого адаптера, он отправляет запрос на присоединение к сети. Запрос включает в себя MAC-адрес клиента и IP, который отправил сервер на предыдущем этапе.

4. **Acknowledge (подтверждение)**. На четвертом этапе сервер подтверждает подключение устройства. Он отправляет по MAC-адресу клиента сообщения с данными параметров, с помощью которых устройство будет авторизовано в сети. После успешной автоматической проверки соответствия всех настроек, соединение становится активным. С этого момента устройство может обмениваться данными с сервером.

5. **Особенности протокола**

Плюс DHCP в том, что IP-адреса распределяются автоматически между устройствами, что облегчает работу администратора. Однако у протокола есть уязвимость: при распределении IP злоумышленник может перехватить данные или подставить свои. Несмотря на это, протокол повсеместно применяется во всем мире, так как на данный момент DHCP - это единственное решение для выдачи динамических IP-адресов при администрировании серверов.

Как работает протокол DHCP при обновлении арендных IP-адресов

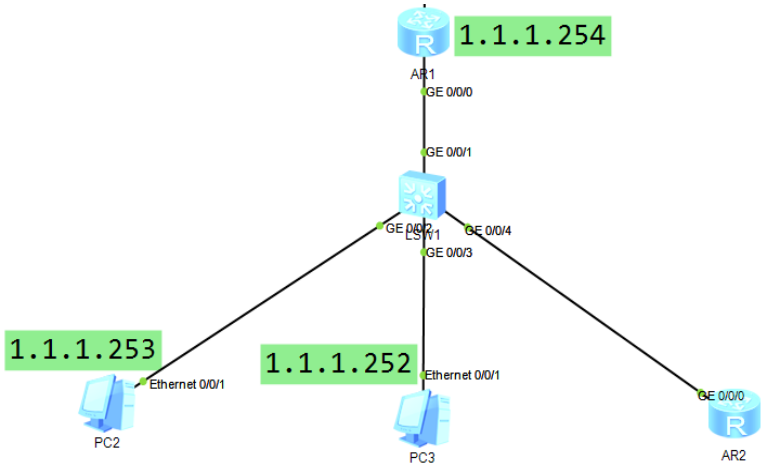
Сервер, работающий по протоколу DHCP, присваивает IP-адреса устройствам в момент их подключения к сети. Затем происходит обмен данными. Однако система динамического образования подразумевает, что адреса выдаются в своего рода аренду на ограниченный период времени. Время, на которое сервер выдает устройству IP-адрес, настраивается администратором. Оно может быть равно как нескольким минутам, так и месяцам.

Можно подумать, что недостаток протокола DHCP - необходимость отключать пользователя от сети каждый раз, когда время действия выданного IP-адреса закончится. Однако это не так: обновить IP-адрес можно без разрыва соединения. Этот процесс проходит в два этапа:

- изменение адреса,
- изменение настроек подключения.

После того как половина времени, отведенного на действие выданного IP-адреса, истечет, система автоматически подаст запрос на обновление. Технически это происходит так же, как и подключение по принципу DORA. Только процедура сразу начинается с этапа отправки запроса.

Если по запросу на обновление адреса от сервера не приходит ответная информация, то система продолжает отправлять запросы. Если пройдет 87,5% времени аренды IP-адреса, но он так и не обновится, система заново выполнит алгоритм подключения по принципу DORA с самого первого этапа. Это поможет избежать ситуации, когда под одним адресом одновременно синхронизируются два клиента.



Первый эксперимент

LSW1

```
<Huawei>
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys sw1
[sw1]stp disable
Warning: The global STP state will be changed. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw1]
<sw1>sa
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]:
<sw1>
```

AR1

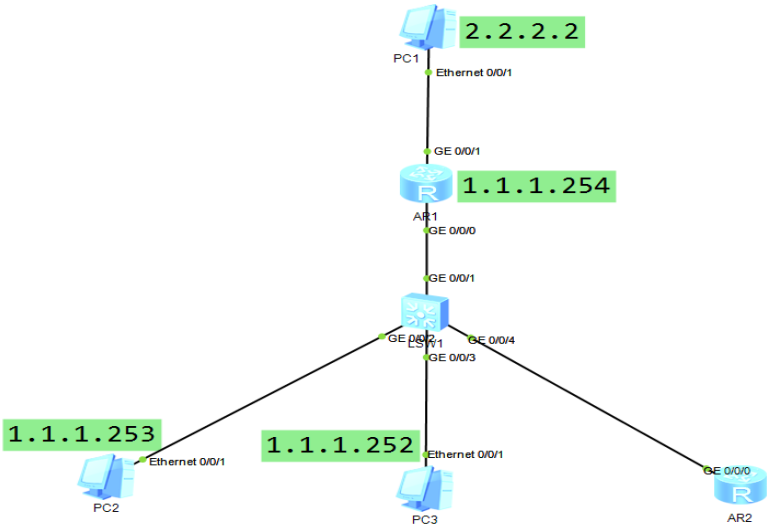
```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]
[R1]un in en
Info: Information center is disabled.
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 1.1.1.254 24
[R1-GigabitEthernet0/0/0]q
[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]dhcp select interface
[R1-GigabitEthernet0/0/0]
```

Введите PC2, выберите command и напишите
PC2>Видим IP адреса с помощью ipconfig, адрес даётся
`PC2>ping 1.1.1.252` (работает)

Введите PC3, выберите command и напишите
PC3> Видим IP адреса с помощью ipconfig, адрес даётся
PC3>ping 1.1.1.253 (работает)

AR2

```
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]un in en
Info: Information center is disabled.
[R2]dis ip int bri (IP-адрес не указан)
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              unassigned           up         down
GigabitEthernet0/0/1              unassigned           down       down
GigabitEthernet0/0/2              unassigned           down       down
NULL0                             unassigned           up         up(s)
TAM.....................................
[R2]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip address dhcp-alloc
[R2-GigabitEthernet0/0/0]dis ip int bri (енді IP адрес берілді)
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              1.1.1.251/24         up         up
GigabitEthernet0/0/1              unassigned           down       down
GigabitEthernet0/0/2              unassigned           down       down
NULL0                             unassigned           up         up(s)
HO.....................................
[R2-GigabitEthernet0/0/0]ping 2.2.2.2 (істемей тұр)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

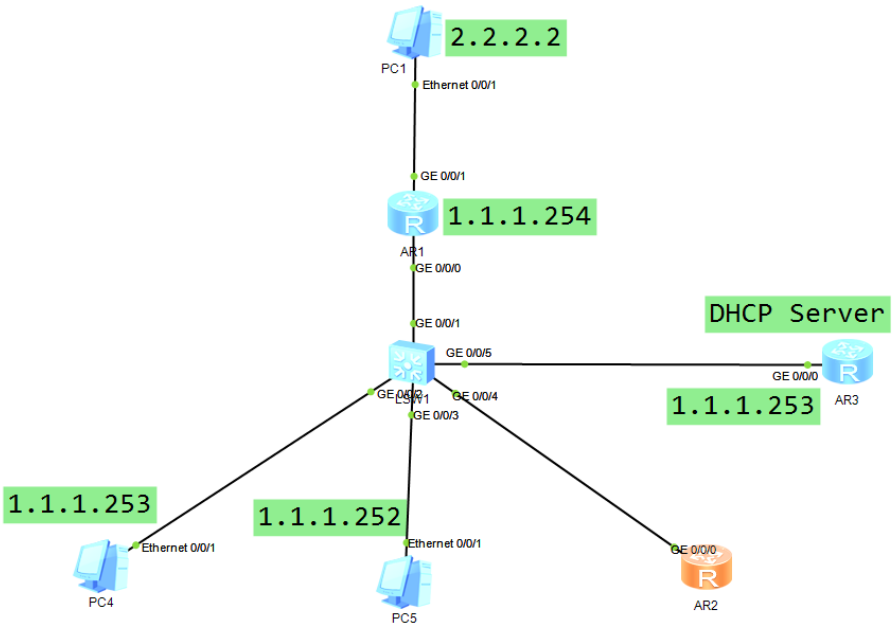


Второй эксперимент, подключаем PC1-компьютер

```
<R1>
<R1>sys
Enter system view, return user view with Ctrl+Z.
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 2.2.2.254 24
[R1-GigabitEthernet0/0/1]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

<R1>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
```

Теперь давайте проверим R2 (работает)

```
[R2-GigabitEthernet0/0/0]ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=30 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=30 ms
  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 30/42/70 ms

[R2-GigabitEthernet0/0/0]q
[R2]ping 1.1.1.252 (істеп тұр)
  PING 1.1.1.252: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.252: bytes=56 Sequence=1 ttl=128 time=90 ms
    Reply from 1.1.1.252: bytes=56 Sequence=2 ttl=128 time=40 ms
    Reply from 1.1.1.252: bytes=56 Sequence=3 ttl=128 time=50 ms
    Reply from 1.1.1.252: bytes=56 Sequence=4 ttl=128 time=50 ms
  --- 1.1.1.252 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/54/90 ms
[R2]ping 1.1.1.253 (істеп тұр)
  PING 1.1.1.253: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.253: bytes=56 Sequence=1 ttl=128 time=90 ms
    Reply from 1.1.1.253: bytes=56 Sequence=2 ttl=128 time=50 ms
    Reply from 1.1.1.253: bytes=56 Sequence=3 ttl=128 time=30 ms
    Reply from 1.1.1.253: bytes=56 Sequence=4 ttl=128 time=40 ms

  --- 1.1.1.253 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/52/90 ms
<R2>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
```



AR1

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]
[R1]un in en
Info: Information center is disabled.
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 1.1.1.254 24
[R1-GigabitEthernet0/0/0]q
[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]dhcp select interface
[R1-GigabitEthernet0/0/0]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on
<R1>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
```

AR2

```
The device is running!
####################
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]un in en
Info: Information center is disabled.
[R2]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip address dhcp-alloc
[R2-GigabitEthernet0/0/0]dis ip int bri (IP адрес тексеру, адрес берілді)

Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              1.1.1.251/24         up         up
```

```
GigabitEthernet0/0/1                unassigned           down       down
GigabitEthernet0/0/2                unassigned           down       down
NULL0                               unassigned           up         up(s)
[R2-GigabitEthernet0/0/0]
[R2-GigabitEthernet0/0/0]ping 2.2.2.2 (істеп тұрған жоқ)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Итак, давайте сделаем следующее для AR1:

```
[R1-GigabitEthernet0/0/0]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 2.2.2.254 24
[R1-GigabitEthernet0/0/1]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on
<R1>
<R1>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
```

Теперь зайдем в AR2 и проверим:

```
 [R2-GigabitEthernet0/0/0]ping 2.2.2.2 (енді істеп тұр)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=30 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 30/42/70 ms

[R2-GigabitEthernet0/0/0]ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=40 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=50 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=40 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=127 time=60 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 40/47/60 ms

<R2>sys
Enter system view, return user view with Ctrl+Z.
```

```
[R2]ping 1.1.1.252
  PING 1.1.1.252: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.252: bytes=56 Sequence=1 ttl=128 time=90 ms
    Reply from 1.1.1.252: bytes=56 Sequence=2 ttl=128 time=40 ms
    Reply from 1.1.1.252: bytes=56 Sequence=3 ttl=128 time=50 ms
  --- 1.1.1.252 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/54/90 ms


[R2]ping 1.1.1.253
  PING 1.1.1.253: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.253: bytes=56 Sequence=1 ttl=128 time=90 ms
    Reply from 1.1.1.253: bytes=56 Sequence=2 ttl=128 time=50 ms
    Reply from 1.1.1.253: bytes=56 Sequence=3 ttl=128 time=30 ms
  --- 1.1.1.253 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/52/90 ms
```

Теперь давайте поместим это в AR3:

```
Please press enter to start cmd line!
################################################################################
##########################################
<Huawei>
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R3
[R3]UN IN EN
Info: Information center is disabled.
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]ip add 1.1.1.253 24
[R3-GigabitEthernet0/0/0]q
[R3]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R3]ip pool 1
Info: It's successful to create an IP address pool.
[R3-ip-pool-1]network 1.1.1.0 mask 24
[R3-ip-pool-1]gateway-list 1.1.1.254
[R3-ip-pool-1]excluded-ip-address 1.1.1.10
[R3-ip-pool-1]dns-list 8.8.8.8
[R3-ip-pool-1]q
[R3]ip pool 1
[R3-ip-pool-1]lease day 3
[R3-ip-pool-1]int g0/0/0
[R3-GigabitEthernet0/0/0]dhcp select global
[R3-GigabitEthernet0/0/0]
[R3-GigabitEthernet0/0/0]dis this (орындаған командаларымызды тексеру)
[V200R003C00]
#
interface GigabitEthernet0/0/0
 ip address 1.1.1.253 255.255.255.0
 dhcp select global
#
return
[R3-GigabitEthernet0/0/0]q
[R3]dhcp enable
[R3]
```

```
  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on
```

Проверим, работает

```
<R3>ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

<R3>sys
Enter system view, return user view with Ctrl+Z.
[R3]
[R3]ip route-s
[R3]ip route-static 0.0.0.0 0 1.1.1.254


Енді тексереміз, (работает)
[R3]ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=40 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=50 ms
     --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 40/50/70 ms

[R3]
  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on


<R2>ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=127 time=150 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=50 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=70 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=60 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=127 time=50 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/76/150 ms

<R2>

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on
```

16. Протокол PPP

Протокол "точка-точка" (PPP) - набор стандартных протоколов, обеспечивающих взаимодействие программного обеспечения удаленного доступа от различных поставщиков. При помощи подключения с поддержкой PPP можно производить подключения к удаленным сетям через любой сервер PPP, поддерживающий этот промышленный стандарт. PPP также позволяет компьютеру, на котором функционирует служба удаленного доступа Windows 2000 Server, принимать запросы и обеспечивать доступ к сети клиентам с программным обеспечением удаленного доступа третьих фирм, соответствующим стандартам PPP.

Стандарты PPP также открывают дополнительные возможности, недоступные при более старых стандартах, например SLiP. PPP поддерживает несколько методов аутентификации, сжатие и шифрование данных.- Большинство реализаций PPP позволяет полностью автоматизировать последовательность входа в систему.

PPP также поддерживает несколько сетевых протоколов, в качестве которых могут выступать TCP/iP, iPX или NetbEUi.

PPP — основа для протоколов PPTP и L2TP, которые используются в VPN-соединениях. PPP — эталон для большинства приложений удаленного доступа.

Работа PPP и протоколы. Реализация протокола двухточечного соединения (Point-to-Point Protocol, PPP) должна твердо придерживаться стандартов, установленных в RfC по PPP. Ниже дан краткий обзор механизмов функционирования PPP и протоколов, используемых в PPP-соединении.

Последовательность установления соединения PPP. После начального соединения с удаленным сервером PPP производятся следующие переговоры по установлению PPP-соединения:

Установление протоколов управления связью (Link Control Protocols, LCP). Протоколы LCP служат для установления и настройки связи и параметров окон передачи данных, например, максимальный размер окна.

Установление протоколов аутентификации. Протоколы аутентификации служат для определения используемого сервером удаленного доступа уровня безопасности. Уровень безопасности может изменяться от незашифрованного (аутентификация при помощи пароля, передаваемого открытым текстом) до сильно зашифрованного (аутентификация при помощи смарт-карт).

Установление протоколов управления сетью (Network Control Protocols, NCP). Протоколы NCP служат для установления и настройки различных параметров сетевых протоколов (iP, iPX и NetbEUi) (параметры сжатия заголовков протокола и протоколы управления сжатием).

Установленное в результате переговоров соединение будет оставаться активным до его разрыва по одной из следующих причин:

- Пользователь явно разорвал соединение
- Истекло время простоя
- Администратор разорвал соединение
- Произошла неустранимая ошибка связи

Протоколы управления связью. Протоколы управления связью (Link Control Protocols, LCP) устанавливают и настраивают *кадрирование* (framing) PPP. Кадрирование PPP определяет, как формируются данные перед передачей по глобальной сети. Стандарт кадрирования PPP гарантирует, что программное обеспечение удаленного доступа любых производителей может передавать и распознавать пакеты данных от любого программного обеспечения удаленного доступа, которое твердо придерживается стандартов PPP. PPP и Windows 2000 используют модификацию кадрирования HDLC (Высокоуровневое

управление каналом передачи данных, High-level Data Link Control) для последовательного доступа или iSDN.

Протоколы управления сетью. Протоколы управления сетью (таблица - 16.1) устанавливают и настраивают различные параметры сетевых протоколов (TCP/iP, iPX, NetbEUi и AppleTalk).

Таблица - 16.1. Протоколы управления сетью

Протокол управления сетью	Описание
IP Control Protocol (Протокол управления IP, IPC)	Служит для конфигурирования, разрешения и запрещения модулей iP на обоих концах соединения
IPX Control Protocol (Протокол управления IPX, iPXCP)	Служит для конфигурирования, разрешения и запрещения модулей iPX на обоих концах соединения
NetbEUi Control Protocol (Протокол управления NetbEUi, NbTP)	Служит для конфигурирования, разрешения и запрещения модулей NetbEUi на обоих концах соединения
AppleTalk Control Protocol (Протокол управления AppleTalk, ATCP)	Служит для конфигурирования, разрешения и запрещения модулей AppleTalk на обоих концах соединения

Использование PPP для подключения к Интернету. Протокол PPP используется в Windows 2000 по умолчанию. Автономный компьютер под управлением Windows 2000 Server, настроенный на прием входящих подключений, не требует никаких специальных настроек для поддержки входящих подключений с использованием PPP. Если подключение сконфигурировано должным образом, запрос на подключение по PPP автоматически будет удовлетворен.

Если происходит подключение к удаленному PPP-серверу, обычно подходят настройки по умолчанию и не требуется дополнительное конфигурирование. Однако, если требуется, можно настраивать дополнительные параметры PPP для исходящего или входящего подключения.

Первый эксперимент

```
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]un in en
Info: Information center is disabled.
[R2]aaa
[R2-aaa]local-user huawei password cipher 12345678
Info: Add a new user.
[R2-aaa]int s0/0/0
[R2-Serial0/0/0]ppp aut
[R2-Serial0/0/0]ip add 1.1.1.254 24
[R2-Serial0/0/0]ppp authentication-mode pap
```

```
[R2-Serial0/0/0]aaa
[R2-aaa]ping 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=30 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=30 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/26/30 ms

[R2-aaa]
Please Press ENTER.
```

Второй эксперимент

```
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]un in en
Info: Information center is disabled.
[R1]int s0/0/0
[R1-Serial0/0/0]ip add 1.1.1.1 24
[R1-Serial0/0/0]ppp pap local-user huawei password cipher 1234567
[R1-Serial0/0/0]
[R1-Serial0/0/0]ping 2.2.2.2 (не работает)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

[R1-Serial0/0/0]shutdown
[R1-Serial0/0/0]undo shutdown
 [R1-Serial0/0/0]ppp pap local-user huawei password cipher 12345678
[R1-Serial0/0/0]
[R1-Serial0/0/0]ping 2.2.2.2 (не работает)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

[R1-Serial0/0/0]undo ppp pap local-user
[R1-Serial0/0/0]ppp pap local-user huawei password cipher 12345678
[R1-Serial0/0/0]
```

```
[R1-Serial0/0/0]ping 2.2.2.2 (не работает)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

[R1-Serial0/0/0]shutdown
[R1-Serial0/0/0]undo shutdown
[R1-Serial0/0/0]
[R1-Serial0/0/0]
[R1-Serial0/0/0]ping 2.2.2.2  (не работает)
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

[R1-Serial0/0/0]
```

Третий эксперимент

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]un in en
Info: Information center is disabled.
[R1]int s0/0/0
[R1-Serial0/0/0]ip add 1.1.1.1 24
[R1-Serial0/0/0]ppp pap local-user huawei password cipher 12345678
[R1-Serial0/0/0]undo ppp pap local-user
[R1-Serial0/0/0]ppp chap local-user huawei
[R1-Serial0/0/0]ppp chap user huawei
[R1-Serial0/0/0]ppp chap password cipher 12345678
[R1-Serial0/0/0]shutdown
[R1-Serial0/0/0]undo shutdown
[R1-Serial0/0/0]

  [R1-Serial0/0/0]ping 1.1.1.254 (работает)
  PING 1.1.1.254: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.254: bytes=56 Sequence=1 ttl=255 time=20 ms
    Reply from 1.1.1.254: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 1.1.1.254: bytes=56 Sequence=3 ttl=255 time=30 ms
```

```
    Reply from 1.1.1.254: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 1.1.1.254: bytes=56 Sequence=5 ttl=255 time=30 ms
    Reply from 1.1.1.254: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 1.1.1.254: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 1.1.1.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/28/30 ms

[R1-Serial0/0/0]
```

Четвертый эксперимент

```
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]un in en
Info: Information center is disabled.
[R2]aaa
[R2-aaa]local-user huawei password cipher 12345678
Info: Add a new user.
[R2-aaa]int s0/0/0
[R2-Serial0/0/0]ip add 1.1.1.254 24
[R2-Serial0/0/0]ppp authentication-mode pap
[R2-Serial0/0/0]ppp auth
[R2-Serial0/0/0]ppp authentication-mode chap
[R2-Serial0/0/0]shutdown
[R2-Serial0/0/0]undo shutdown
[R2-Serial0/0/0]
[R2-Serial0/0/0]ping 1.1.1.1 (работает)
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=30 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/16/30 ms

[R2-Serial0/0/0]
```

17. Протокол PPPoE

Что такое протокол PPPoE

PPPoE расшифровывается как Point-to-point-protocol over Ethernet. Это сетевой протокол, который используется для установления и управления соединениями между двумя сетевыми узлами Ethernet. PPPoE работает на канальном уровне модели OSI, требует ввода имени пользователя и пароля для аутентификации и установления соединения с провайдером.

Протокол PPPoE имеет несколько особенностей:

- он работает поверх протокола Ethernet;
- для установки соединения используется имя пользователя и пароль;
- PPPoE поддерживает шифрование данных с помощью протокола PAP или CHAP.

Протокол «точка-точка» (PPP) — это модуль связи между узлами, например, клиент-сервер.

При PPPoE-соединении компьютер или сетевое устройство клиента подключается к сети провайдера через DSL-модем. Соединение инкапсулируется с помощью PPP, который затем инкапсулируется в кадры Ethernet для передачи по локальной сети.

Первоначальное назначение PPPoE — более простое соединение между устройствами с использованием фрейминга ISO 3309. С тех пор были разработаны другие методы, включая PPP через ATM (PPPoA), PPP через SONET/SDH (POS) и PPP.

Для чего используется PPPoE

Протокол используют провайдеры для предоставления доступа в интернет своим клиентам по DSL. В этих типах соединений DSL-модем устанавливает PPPoE-соединение с сетью провайдера, что позволяет компьютеру клиента получить доступ в интернет.

PPPoE обычно используется в ситуациях, когда широкополосное соединение необходимо разделить между несколькими устройствами или пользователями. Например, в домашней сети маршрутизатор может использовать PPPoE для установления соединения с провайдером, а затем передавать это соединение всем устройствам, подключенным к сети.

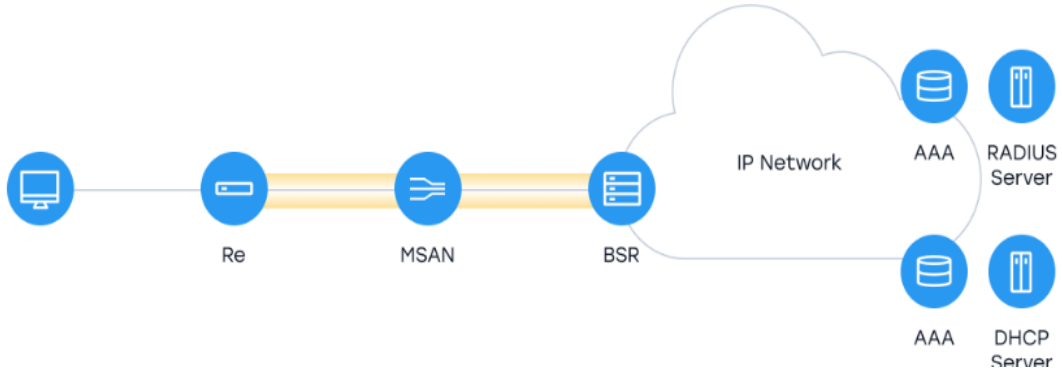
Как работает PPPoE

Первым шагом процесса является создание PPPoE-соединения в соответствии со стандартом RFC 2516.

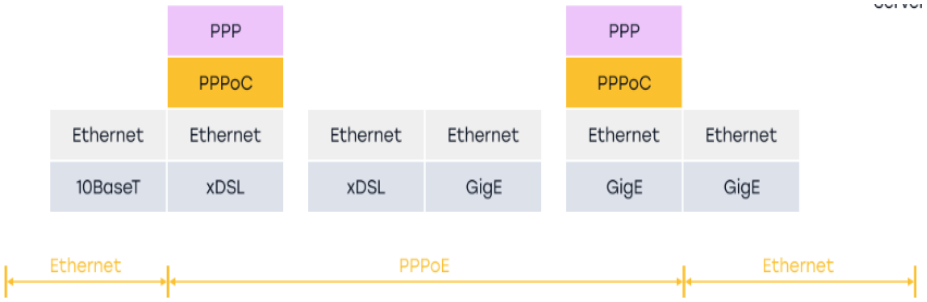
Второй шаг — создание соединения через протокол управления соединением (LCP) для согласования параметров, например, аутентификации.

Третий шаг — аутентификация абонента с помощью Challenge Handshake Authentication Protocol (CHAP). Другие протоколы аутентификации, которые могут быть использованы, включают расширяемый протокол аутентификации (EAP).

Наконец, IP-адреса назначаются с помощью протокола управления интернет-протоколом (IPCP). После этих шагов сеть становится доступной для абонента.



Есть еще один важный аспект этого процесса — мониторинг сеанса PPPoE. Эта функция использует PPP keepalives для мониторинга сессий с обеих конечных точек.



Авторизация PPPoE происходит на странице Ethernet, где в разделе «аутентификация у провайдера» в поле «тип авторизации» необходимо указать PPPoE, затем ввести логин и пароль, предоставленные провайдером для подключения к интернету.

Преимущества PPPoE

Из плюсов протокола PPPoE можно выделить следующие:

- двухуровневая инкапсуляция L2;
- одноадресные соединения;
- уникальные идентификаторы сеанса;
- поддержка различных сетевых протоколов, включая IPv4, IPv6 и IPX;
- настройка политик контроля доступа.

Отличия PPPoE и PPTP

PPTP (Point-to-Point Tunneling Protocol) — это протокол для создания безопасной виртуальной сети через интернет. Он позволяет удаленным пользователям безопасно подключаться к частной сети через публичную. PPTP используется для создания безопасных соединений между удаленными пользователями и частной сетью. PPPoE используется для доступа в интернет для отдельных клиентов.

Разница также заключается в безопасности. Считается, что PPTP менее безопасен, чем другие VPN-протоколы, например, OpenVPN или IPsec, потому что у него есть уязвимости. PPPoE считается безопасным для пользователей, которым нужен доступ в интернет, потому что он защищен аутентификацией и шифрованием.

Разница между протоколами L2TP и PPPoE

L2TP также используют для создания VPN. L2TP — это комбинация двух других протоколов: PPTP и L2F (Layer 2 Forwarding Protocol). Так же как и PPTP, L2TP использует протокол туннелирования для инкапсуляции пакетов PPP в пакеты IP для передачи через интернет.

L2TP может использоваться с различными типами сетей, в то время как PPPoE предназначен только для сетей Ethernet. L2TP также обеспечивает более надежные функции безопасности, чем PPPoE, включая возможность шифрования данных, передаваемых по VPN.

Сравнение PPPoE, PPTP и L2TP

PPPoE, PPTP и L2TP — сетевые протоколы, используемые для разных целей. Каждый протокол имеет свои сильные и слабые стороны с точки зрения безопасности, совместимости и сферы применения.

Стоит добавить, что по сравнению с PPTP и L2TP, протокол PPPoE считается более эффективным и безопасным, поскольку он шифрует передаваемые по сети пакеты данных. Кроме того, его легче настроить на маршрутизаторе, для этого требуется ввести имя пользователя и пароль.

Протоколы	Назначение	Инкапсуляция	Безопасность
PPPoE	предоставление доступа в интернет отдельным клиентам через Ethernet	PPP-пакеты в кадры Ethernet для передачи по сетям Ethernet	безопасная аутентификация и шифрование для индивидуальных соединений клиентов
PPTP	создание VPN-соединения через интернет	PPP-пакеты в IP-пакеты для передачи через интернет	не рекомендуется для использования в средах с высокими требованиями к безопасности
L2TP	создание безопасного VPN-соединения между двумя сетями	PPP-пакеты в IP-пакеты для передачи через интернет или другие типы сетей	надежное шифрование и аутентификация для VPN-соединений

Различия PPPoE и DHCP в конфигурации маршрутизатора

PPPoE и DHCP — протоколы, которые обычно используются в конфигурациях маршрутизаторов для обеспечения доступа в интернет. Их основные различия в конфигурации маршрутизатора.

Аутентификация:

- PPPoE требует аутентификации у провайдера для установления соединения;
- DHCP не требует аутентификации.

Конфигурация:

- для установления соединения PPPoE требует от пользователя ввода имени и пароля, предоставленных провайдером;
- DHCP назначает IP-адреса устройствам автоматически, не требуя ввода данных пользователем.

Примеры использования:

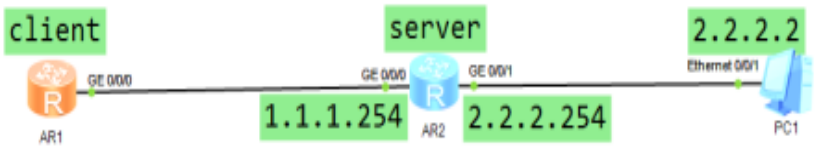
- PPPoE используют провайдеры для предоставления доступа в интернет отдельным клиентам через Ethernet;
- DHCP используют провайдеры для автоматического назначения IP-адресов устройствам в сети.

Ограничения:

- PPPoE ограничен сетями Ethernet и может иметь проблемы с производительностью в больших сетях;
- DHCP — централизованная система, если сервер DHCP выйдет из строя, клиенты не смогут получить IP-адреса.

Безопасность:

- PPPoE обеспечивает безопасную аутентификацию и шифрование для отдельных клиентских соединений;
- DHCP не обеспечивает аутентификацию и шифрование.



Первый эксперимент

```
Please press enter to start cmd line!
##################
```

```
<Huawei>
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]un in en
Info: Information center is disabled.
[R2]ip pool 1
Info: It's successful to create an IP address pool.
[R2-ip-pool-1]network 1.1.1.0 mask 24
[R2-ip-pool-1]gateway-list 1.1.1.254
[R2-ip-pool-1]q
[R2]int Virtual-Template  1
[R2-Virtual-Template1]ppp authentication-mode chap
[R2-Virtual-Template1]ip address 1.1.1.254 24
[R2-Virtual-Template1]remote address pool 1
[R2-Virtual-Template1]int g0/0/0
[R2-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[R2-GigabitEthernet0/0/0]aaa
[R2-aaa]local-user huawei password cipher 123
Info: Add a new user.
[R2-aaa]local-user huawei service-type ppp
[R2-aaa]q
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ip add 2.2.2.254 24
[R2-GigabitEthernet0/0/1]q
[R2]
  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on
<R2>ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=128 time=40 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=128 time=20 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=128 time=20 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=128 time=20 ms
     --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/22/40 ms

<R2>dis ip int b

Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              unassigned           up         down
GigabitEthernet0/0/1              2.2.2.254/24         up         up
GigabitEthernet0/0/2              unassigned           down       down
NULL0                             unassigned           up         up(s)
Virtual-Template1                 1.1.1.254/24         up         up
<R2>

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

<R2>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
```

Второй эксперимент

```
Please press enter to start cmd line!
################################################################################
```

```
<Huawei>
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]un in en
Info: Information center is disabled.
[R1]int Dialer1
[R1-Dialer1]dialer user huawei
[R1-Dialer1]dialer bundle 1
[R1-Dialer1]ppp chap user huawei
[R1-Dialer1]ppp chap password cipher 123
[R1-Dialer1]ip address ppp-negotiate
[R1-Dialer1]int g0/0/0
[R1-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
[R1-GigabitEthernet0/0/0]q
[R1]ip route-static 0.0.0.0 0 Dialer 1
[R1]
[R1]ping 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=127 time=50 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=127 time=40 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=127 time=20 ms
    Reply from 2.2.2.2: bytes=56 Sequence=5 ttl=127 time=30 ms

  --- 2.2.2.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 20/35/50 ms

[R1]dis ip int bri
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 3

Interface                         IP Address/Mask      Physical   Protocol
Dialer1                           1.1.1.253/32         up         up(s)
GigabitEthernet0/0/0              unassigned           up         down
GigabitEthernet0/0/1              unassigned           down       down
GigabitEthernet0/0/2              unassigned           down       down
NULL0                             unassigned           up         up(s)
[R1]

  Please check whether system data has been changed, and save data in time

  Configuration console time out, please press any key to log on

<R1>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated

<R1>
```

18. Беспроводная локальная сеть (WLAN)

Беспроводная локальная сеть (WLAN) - локальная сеть, в которой соединения между сетевыми устройствами выполнялись без использования проводов. Термин Wi-Fi (хотя первоначально это было название только одного продукта, использующего определенный стандарт WLAN) используется в качестве синонима для термина WLAN.

Беспроводная локальная сеть (WLAN)

Характеристики:

Эти типы сетей чаще всего создаются с использованием микроволн в качестве среды передачи сигнала, а также с использованием инфракрасного излучения. Они разработаны на основе стандарта IEEE 802.11 , который описывает физический и MAC- уровни.

Для связи через микроволны используется диапазон 2,4 ГГц [в стандартах: 802.11, 802.11b, 802.11g, 802.11n, 802.11ac и 802.15.1 (bluetooth)] или 5 ГГц (в стандартах 802.11a, 802.11n, 802.11 переменный ток). В Европе полоса 2,4 ГГц разделена на 13 каналов в диапазоне 2400–2483,5 МГц с шагом 5 МГц (центральная частота первого канала составляет 2412 МГц). Однако полоса пропускания, занимаемая одной сетью, составляет около 20 МГц, поэтому на практике только три сети могут работать без взаимных помех, поскольку каналы перекрываются. Каждый канал имеет свою собственную несущую частоту, которая модулируется при передаче информации.

Скорость передачи данных зависит от используемого стандарта и расстояния между используемыми устройствами и обычно составляет 11 (802.11b) или 54, 108 (802.11a / g) Мбит / с.

WLAN (Wireless Local Area Network) - вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами СВЧ радиоволны, а не кабель. Это гибкая система передачи данных, которая применяется как расширение или альтернатива кабельной локальной сети и применяется в пределах одной территории внутри зданий (дом, школа, офис...). Всё это даёт возможность пользователям перемещаться в зоне обслуживания сети. В качестве центральной точки в WLAN сетях, применяют точки доступа или беспроводные Wi-Fi маршрутизаторы.

Компания Huawei

Huawei подвела первые итоги программы сертификации экспертов по беспроводным технологиям.

Компания Huawei подвела промежуточные итоги программы сертификации экспертов по беспроводным технологиям – HCIE WLAN. Целью программы является формирование на рынке пула экспертов, способных обеспечить высокоуровневую работу

сетей и интеграцию технологий Huawei для решения актуальных бизнес-задач. К декабрю 2021г. компании удалось подготовить к сертификации 80 специалистов уровня HCIE WLAN, 71 из них уже успешно сдали квалификационный экзамен.

Пристальное внимание подготовке профильных ИКТ-специалистов обусловлено не только масштабностью и глубиной проникновения цифровых технологий в бизнес, но и их возрастающей сложностью. Так, в рамках проекта, реализованного компанией Huawei для X5 Group (владеет торговыми сетями «Пятерочка», «Перекресток», «Карусель» и другими), перед Huawei стояла задача по развертыванию высокоскоростных сетей Wi-Fi на нескольких десятках тысяч объектов, причем управление политиками и сервисами всей сети должно было осуществляться централизованно. «Решение такого уровня требует как наличия технологий, базирующихся на использовании искусственного интеллекта, так привлечения специалистов, способных спроектировать подобную сеть и интегрировать ее в существующую ИТ-инфраструктуру. Это еще один довод в пользу подготовки и развития квалифицированных экспертов, умеющих работать с оборудованием Huawei», – отметил ведущий менеджер по продуктам Huawei Datacom-Network **Антон Печенев**.

Беспроводные сети также широко применяются для оптимизации процессов в логистике, при эксплуатации smart-офисов, в здравоохранении и образовании. По словам заместителя руководителя Huawei OpenLab Москва **Виктора Смоковдина**, особенно высоких результатов позволяет добиться конвергентная архитектура Wi-Fi и IoT «Интернет вещей». Она дает возможность создавать эффективные интеллектуальные решения для навигации внутри помещений, инвентаризации и управления электронными ценниками в магазинах. Развитие таких решений является одним из ключевых направлений работы Huawei.

«Компания Huawei активно инвестирует в разработку новых беспроводных решений, чтобы постоянно повышать качество выпускаемых продуктов, увеличивать их пропускную способность, уменьшать задержки при передаче данных и обеспечивать параллелизм операций. При этом для нас важно не просто предоставлять нашим российским клиентам высокотехнологичное оборудование, а развивать сам рынок ИКТ. Вместе с нашими локальными партнерами мы строим инфраструктуру, которая является основой для предоставления новых услуг и развития цифровой экономики в целом. В России мы участвуем в реализации большого количества крупных инфраструктурных проектов, разрабатываем новые решения в сотрудничестве с российскими ИТ-компаниями, а также инвестируем в образовательные инициативы, потому что у нас есть четкое понимание – какими бы умными ни были технологии, именно люди обеспечивают их правильное функционирование», – прокомментировал директор департамента сетевых решений Huawei Enterprise в России **Чжао Шаоци** (Zhao Shaoqi).

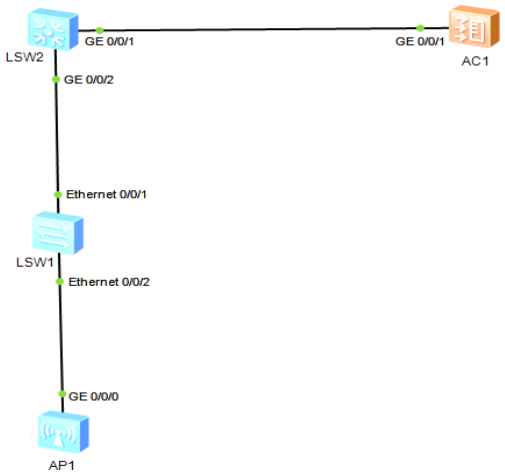
Свою экосистему подготовки экспертов в области ИКТ Huawei развивает на протяжении нескольких лет. Подготовка к сертификации охватывает учащихся и специалистов и разделяется на три уровня: базовый, профессиональный и экспертный. Базовый уровень сертификации (HCIA WLAN) предполагает обучение по направлению эксплуатации беспроводных сетей. Второй уровень (HCIP WLAN) включает развитие навыков планирования, проектирования и развертывания. Преимущество же высшего уровня (HCIE WLAN) заключается в том, что специалисты учатся оптимизировать крупномасштабные сети с различным набором сценариев.

В 2020 г, компания Huawei запустила стратегический проект HCIE 1000, цель которого – подготовить в России 1000 экспертов высшего уровня к 2023 г, (сюда входят как эксперты по беспроводным технологиям, так и специалисты, выбравшие другие направления: облачные вычисления, искусственный интеллект, Big Data, хранение данных).

На сегодняшний день обучение по различным направлениям уже прошли 750 человек. Подобных высоких показателей удалось добиться в том числе благодаря локализации и уникальному проекту по подготовке специалистов HCIE CAMP, который в этом году был запущен по трем направлениям: коммутация и маршрутизация (routing and

switching), системы хранения данных (storage), беспроводные сети (WLAN). Обучение 80 WLAN экспертов состоялось как раз в рамках проекта HCIE CAMP совместно с УЦ Микротест. На сегодняшний день Россия занимает первое место в мире по числу HCIE WLAN специалистов.

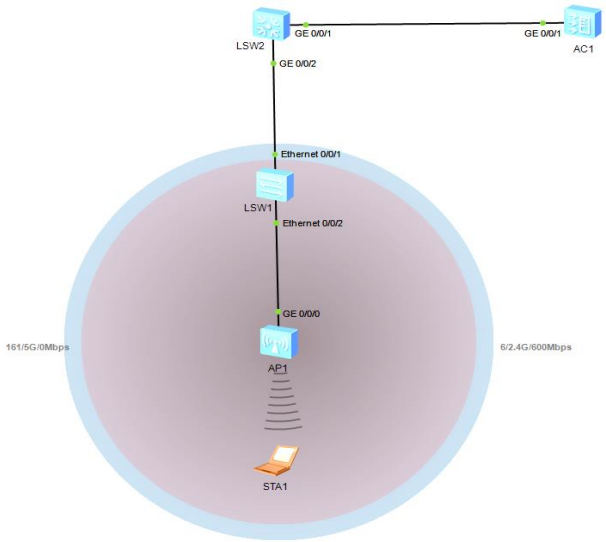
При этом Huawei не только развивает профессиональные компетенции действующих участников рынка, но и занимается подготовкой студентов и обучением молодых специалистов с нуля. Компания активно сотрудничает с российскими вузами, открывая на их базе Академии информационно-коммуникационных технологий Huawei.



Первый эксперимент

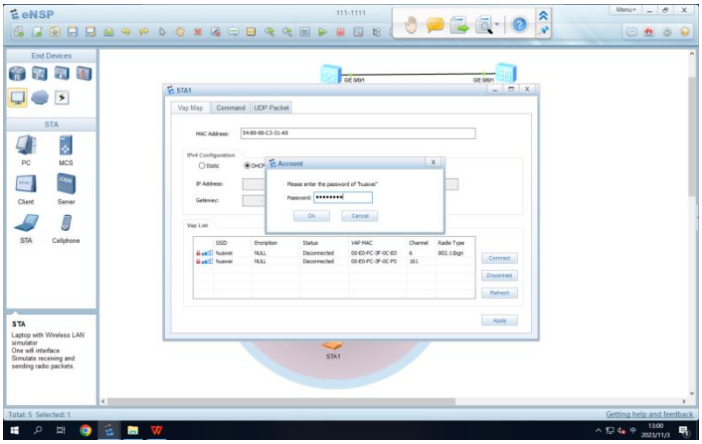
```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sys sw1
 [sw1]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw1]int e0/0/2
[sw1-Ethernet0/0/2]port link-type trunk
[sw1-Ethernet0/0/2]port trunk allow-pass vlan all
[sw1-Ethernet0/0/2]int e0/0/1
[sw1-Ethernet0/0/1]port link-type trunk
[sw1-Ethernet0/0/1]port trunk allow-pass vlan all
[sw1-Ethernet0/0/1]int e0/0/2
[sw1-Ethernet0/0/2]port trunk pvid vlan 100

<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys sw2
[sw2]un in en
Info: Information center is disabled.
[sw2]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw2]int g0/0/2
[sw2-GigabitEthernet0/0/2]port link-type trunk
[sw2-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[sw2-GigabitEthernet0/0/2]int g0/0/1
[sw2-GigabitEthernet0/0/1]port link-type trunk
[sw2-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[sw2-GigabitEthernet0/0/1]q
[sw2]int LoopBack 0
[sw2-LoopBack0]ip add 2.2.2.2 32
```

```
[sw2-LoopBack0]


The device is running!
##########
<AC6605>sys
Enter system view, return user view with Ctrl+Z.
[AC6605]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC6605]int g0/0/1
[AC6605-GigabitEthernet0/0/1]port link-type trunk
[AC6605-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[AC6605-GigabitEthernet0/0/1]q
[AC6605]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[AC6605]int vlanif100
[AC6605-Vlanif100]ip add 10.23.100.1 24
[AC6605-Vlanif100]dhcp select interface
[AC6605-Vlanif100]q
[AC6605]capwap source interface Vlanif100
[AC6605]wlan
[AC6605-wlan-view]ap auth-mode no-auth
Warning: It is insecure to configure none authentication mode.
 [AC6605-wlan-view]dis ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal          [1]
--------------------------------------------------------------------------------
---------------------
ID   MAC            Name           Group   IP            Type            State
S
TA Uptime
--------------------------------------------------------------------------------
---------------------
0    00e0-fc3f-0ce0 00e0-fc3f-0ce0 default 10.23.100.191 AP2050DN        nor
0
   29S
--------------------------------------------------------------------------------
---------------------
Total: 1
[AC6605-wlan-view]
```

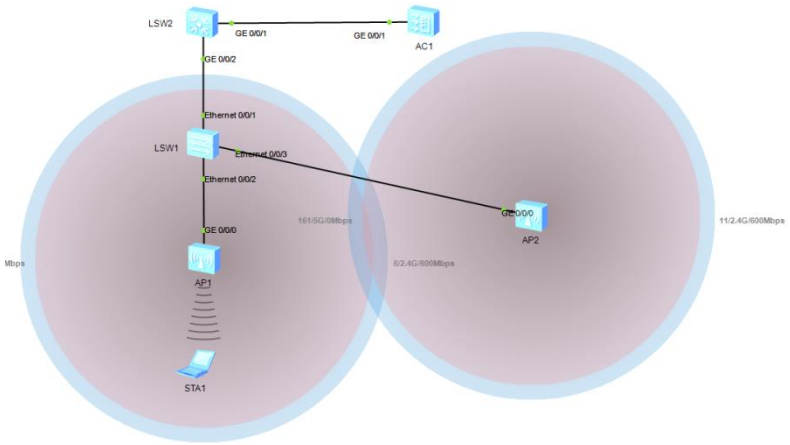



```
<AC6605>sys
Enter system view, return user view with Ctrl+Z.
```

```
[AC6605]wlan
[AC6605-wlan-view]ssid-profile name ssid1
[AC6605-wlan-ssid-prof-ssid1]ssid huawei
Info: This operation may take a few seconds, please wait.done.
[AC6605-wlan-ssid-prof-ssid1]q
[AC6605-wlan-view]security-profile name sec1
[AC6605-wlan-sec-prof-sec1]security wpa-wpa2 psk pass-phrase a1234567 aes
[AC6605-wlan-sec-prof-sec1]q
[AC6605-wlan-view]vap-profile name vap1
[AC6605-wlan-vap-prof-vap1]security-profile sec1
Info: This operation may take a few seconds, please wait.done.
[AC6605-wlan-vap-prof-vap1]ssid-profile ssid1
Info: This operation may take a few seconds, please wait.done.
[AC6605-wlan-vap-prof-vap1]forward-mode direct-forward
[AC6605-wlan-vap-prof-vap1]service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait.done.
[AC6605-wlan-vap-prof-vap1]q
[AC6605-wlan-view]ap-group name default
[AC6605-wlan-ap-group-default]vap-profile vap1 wlan 1 radio all
Info: This operation may take a few seconds, please wait...done.
[AC6605-wlan-ap-group-default]
[AC6605-wlan-ap-group-default]
```



Второй эксперимент

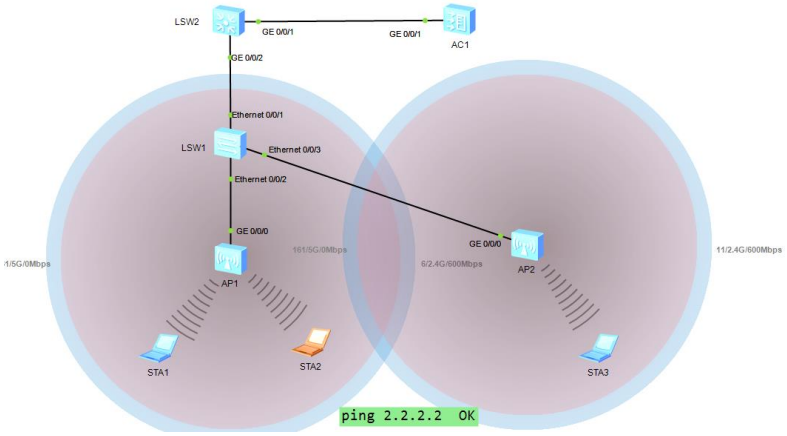


<sw1> (следуя командам в первом эксперименте)

```
<sw1>sys
```

```
Enter system view, return user view with Ctrl+Z.
[sw1]int e0/0/3
[sw1-Ethernet0/0/3]port link-type trunk
[sw1-Ethernet0/0/3]port trunk pvid vlan 100
[sw1-Ethernet0/0/3]port trunk allow-pass vlan 2  4094
[sw1-Ethernet0/0/3]
```

Третий эксперимент




```
Please press enter to start cmd line!

<sw1>sys
Enter system view, return user view with Ctrl+Z.
[sw1]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw1]int e0/0/2
[sw1-Ethernet0/0/2]port link-type trunk
[sw1-Ethernet0/0/2]port trunk allow-pass vlan all
[sw1-Ethernet0/0/2]int e0/0/1
[sw1-Ethernet0/0/1]port link-type trunk
[sw1-Ethernet0/0/1]port trunk allow-pass vlan all
[sw1-Ethernet0/0/1]int e0/0/2
[sw1-Ethernet0/0/2]port trunk pvid vlan 100
[sw1-Ethernet0/0/2]q
[sw1]int e0/0/3
[sw1-Ethernet0/0/3]port link-type trunk
[sw1-Ethernet0/0/3]port trunk pvid vlan 100
[sw1-Ethernet0/0/3]port trunk allow-pass vlan 2 4094
[sw1-Ethernet0/0/3] User interface con0 is available

Please press enter to start cmd line!
################################################
<AC6605>sys
Enter system view, return user view with Ctrl+Z.
[AC6605]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC6605]int g0/0/1
[AC6605-GigabitEthernet0/0/1]port link-type trunk
[AC6605-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[AC6605-GigabitEthernet0/0/1]q
[AC6605]dhcp enable
[AC6605]int vlanif100
[AC6605-Vlanif100]ip address 10.23.100.1 24
[AC6605-Vlanif100]dhcp select interface
[AC6605-Vlanif100]q
```

```
[AC6605]capwap source interface Vlanif100
[AC6605]wlan
[AC6605-wlan-view]ap auth-mode no-auth
[AC6605-wlan-view]q
<AC6605>dis ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
idle : idle            [1]
nor  : normal          [1]
--------------------------------------------------------------------------------
---------------------
ID   MAC            Name           Group   IP            Type            State
S
TA Uptime
--------------------------------------------------------------------------------
---------------------
0    00e0-fcb1-1e70 00e0-fcb1-1e70 default 10.23.100.198 AP2050DN        nor
0
   2M:29S
1    00e0-fcfa-3ff0 00e0-fcfa-3ff0 default -             AP2050DN        idle
0
   --------------------------------------------------------------------------------
-------------------------
Total: 2
```

Когда подключен второй WI-FI

```
<AC6605>sys
Enter system view, return user view with Ctrl+Z.
[AC6605]wlan
[AC6605-wlan-view]ssid-profile name ssid1
[AC6605-wlan-ssid-prof-ssid1]ssid huawei
[AC6605-wlan-ssid-prof-ssid1]q
[AC6605-wlan-view]security-profile name sec1
[AC6605-wlan-sec-prof-sec1]security-profile name sec1
[AC6605-wlan-sec-prof-sec1]security wpa-wpa2 psk pass-phrase a1234567 aes
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[AC6605-wlan-sec-prof-sec1]q
[AC6605-wlan-view]vap-profile name vap1
[AC6605-wlan-vap-prof-vap1]security-profile sec1
[AC6605-wlan-vap-prof-vap1]ssid-profile ssid1
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait...done.
[AC6605-wlan-vap-prof-vap1]forward-mode direct-forward
[AC6605-wlan-vap-prof-vap1]service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait...done.
[AC6605-wlan-vap-prof-vap1]q
[AC6605-wlan-view]ap-group name default
[AC6605-wlan-ap-group-default]vap-profile vap1 wlan 1 radio all
[AC6605-wlan-ap-group-default]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

<AC6605>

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on


Please press enter to start cmd line!
```

```
################################################
<sw2>sys
Enter system view, return user view with Ctrl+Z.
[sw2]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[sw2]int g0/0/2
[sw2-GigabitEthernet0/0/2]port link-type trunk
[sw2-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[sw2-GigabitEthernet0/0/2]int g0/0/1
[sw2-GigabitEthernet0/0/1]port link-type trunk
[sw2-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[sw2-GigabitEthernet0/0/1]q
[sw2]int LoopBack 0
[sw2-LoopBack0]ip add 2.2.2.2 32
[sw2]q
[sw2]int vlanif101
[sw2-Vlanif101]
[sw2-Vlanif101]dis this
#
interface Vlanif101
 ip address 10.23.101.1 255.255.255.0
#
return

[sw2-Vlanif101]dhcp select interface
[sw2-Vlanif101] User interface con0 is available

Please Press ENTER.
```

Предоставление паролей компьютерам `a1234567`

```
Commandka kirip


STA>ipconfig
Link local IPv6 address...........: ::
IPv6 address......................: :: / 128
IPv6 gateway......................: ::
IPv4 address......................: 10.23.101.253
Subnet mask.......................: 255.255.255.0
Gateway...........................: 10.23.101.1
Physical address..................: 54-89-98-C5-79-0C
DNS server........................:


Welcome to use STA Simulator!
STA>ping 2.2.2.2
Ping 2.2.2.2: 32 data bytes, Press Ctrl_C to break
From 2.2.2.2: bytes=32 seq=1 ttl=255 time=141 ms
From 2.2.2.2: bytes=32 seq=2 ttl=255 time=141 ms
From 2.2.2.2: bytes=32 seq=3 ttl=255 time=125 ms
From 2.2.2.2: bytes=32 seq=4 ttl=255 time=125 ms
From 2.2.2.2: bytes=32 seq=5 ttl=255 time=125 ms

--- 2.2.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 125/131/141 ms

STA>
```

IPv6 (англ. *Internet Protocol version 6*) - новая версия интернет-протокола (IP), призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете, за счёт целого ряда принципиальных изменений. Протокол был разработан IETF. Длина адреса IPv6 составляет 128 бит, в отличие от адреса IPv4, длина которого равна 32 битам.

На конец 2012 года доля IPv6 в сетевом трафике составляла около 5 %. К концу 2013 года ожидался рост на 3 %. Согласно статистике Google по всему миру на январь 2024 года процент пользователей, которые получают доступ к Google по протоколу IPv6, составлял около 41 %. В России коммерческое использование операторами связи невелико (не более 4,5 % пользователей). DNS-серверы многих российских регистраторов доменов и хостинг-провайдеров используют IPv6.

После того, как адресное пространство в IPv4 закончилось, используется два стека протоколов - IPv6 и IPv4 параллельно (англ. *dual stack*), с постепенным увеличением доли трафика IPv6, по сравнению с IPv4. Такая ситуация стала возможной из-за наличия огромного количества устройств, в том числе устаревших, не поддерживающих IPv6 и требующих специального преобразования для работы с устройствами, использующими только IPv6.

История создания - В конце 1980-х стала очевидна необходимость разработки способов сохранения адресного пространства Интернета. В начале 1990-х, несмотря на внедрение бесклассовой адресации, стало ясно, что этого недостаточно для предотвращения исчерпания адресов и необходимы дальнейшие изменения инфраструктуры Интернета. К началу 1992 года появилось несколько предложений, и к концу 1992 года IETF объявила конкурс для рабочих групп на создание интернет-протокола следующего поколения (англ. IP Next Generation - IPng). 25 июля 1994 года IETF утвердила модель IPng, с образованием нескольких рабочих групп IPng. К 1996 году была выпущена серия RFC, определяющих Интернет-протокол версии 6, начиная с RFC 1883.

IETF назначила новому протоколу версию 6, так как версия 5 была ранее назначена экспериментальному протоколу, предназначенному для передачи видео и аудио.

Исчерпание IPv4-адресов

Основная статья: ***Исчерпание IPv4-адресов***

Оценки времени полного исчерпания IPv4-адресов различались в 2000-х. Так, в 2003 году директор APNIC Пол Уилсон (англ. *Paul Wilson*) заявил, что, основываясь на темпах развёртывания сети Интернет того времени, свободного адресного пространства хватит на одно—два десятилетия. В сентябре 2005 года Cisco Systems предположила, что пула доступных адресов хватит на 4—5 лет.

3 февраля 2011 агентство IANA распределило последние пять блоков /8 IPv4 региональным интернет-регистраторам. На этот момент ожидалось, что общий запас свободных блоков адресов у региональных интернет-регистраторов (RIR) закончится в течение срока от полугода (APNIC) до пяти лет (AfriNIC)[4].

По состоянию на сентябрь 2015 года об исчерпании общего запаса свободных блоков IPv4-адресов и ограничениях на выдачу новых диапазонов адресов объявили все региональные регистраторы, кроме AfriNIC; ARIN объявил о полном исчерпании свободных IPv4-адресов, а для остальных регистраторов этот момент прогнозируется начиная с 2017 года. Выделение IPv4-адресов в Европе, Азии и Латинской Америке (регистраторы APNIC, RIPE NCC и LACNIC) продолжается блоками /22 (по 1024 адреса).

Основы адресации IPv6

Основная статья: ***IPv6-адрес***

Существуют различные типы адресов IPv6: одноадресные (Unicast), групповые (Anycast) и многоадресные (Multicast).

Адреса типа Unicast хорошо всем известны. Пакет, посланный на такой адрес, достигает в точности интерфейса, который этому адресу соответствует.

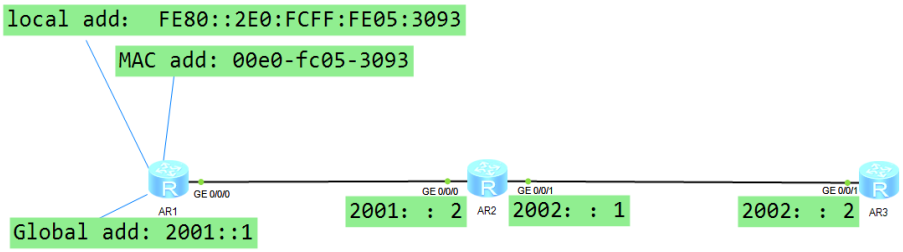
Адреса типа Anycast синтаксически неотличимы от адресов Unicast, но они адресуют группу интерфейсов. Пакет, направленный такому адресу, попадёт в ближайший (согласно метрике маршрутизатора) интерфейс. Адреса Anycast могут использоваться только маршрутизаторами.

Адреса типа Multicast идентифицируют группу интерфейсов. Пакет, посланный на такой адрес, достигнет всех интерфейсов, привязанных к группе многоадресного вещания.

Широковещательные адреса IPv4 (обычно xxx.xxx.xxx.255) выражаются адресами многоадресного вещания IPv6. Крайние адреса подсети IPv6 (например, xxxx: xxxx: xxxx: xxxx:0:0:0:0 и xxxx: xxxx: xxxx: xxxx: ffff: ffff: ffff: ffff для подсети /64) являются полноправными адресами и могут использоваться наравне с остальными.

Группы цифр в адресе разделяются двоеточиями (например, fe80:0:0:0:200:f8ff:fe21:67cf). Незначащие старшие нули в группах могут быть опущены. Большое количество нулевых групп может быть пропущено с помощью двойного двоеточия (fe80::200:f8ff:fe21:67cf). Такой пропуск должен быть единственным в адресе.

Первый эксперимент



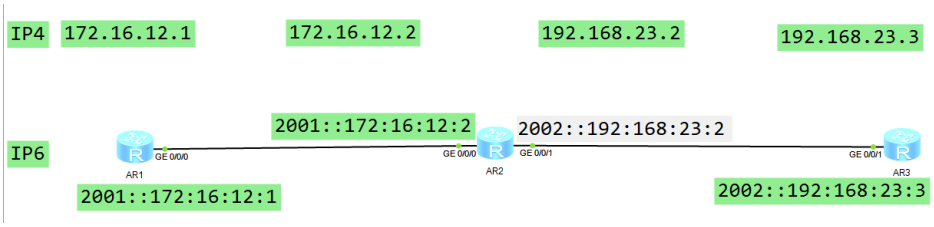

```
Please press enter to start cmd line!
########
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R1
[R1]un in en
Info: Information center is disabled.
[R1]ipv6
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ipv6 enable
[R1-GigabitEthernet0/0/0]ipv6 address 2001::1 64
[R1-GigabitEthernet0/0/0]dis ipv6 int
GigabitEthernet0/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE05:3093
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::2
    FF02::1
    FF02::1:FF05:3093
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
```

```
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses

<R1>sys
Enter system view, return user view with Ctrl+Z.
[R1]ipv route-static 2002::2 64 2001::2
Info: The destination address and mask of the configured static route
mismatched, and the static route 2002::/64 was generated.
R1]ping ipv6 2002::2
  PING 2002::2 : 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 2002::2
    bytes=56 Sequence=2 hop limit=63  time = 50 ms
    Reply from 2002::2
    bytes=56 Sequence=3 hop limit=63  time = 30 ms
    Reply from 2002::2
    bytes=56 Sequence=4 hop limit=63  time = 20 ms
    Reply from 2002::2

  --- 2002::2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 20/30/50 ms

[R1]q
<R1>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<R1>

The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]un in en
Info: Information center is disabled.
[R2]ipv6
[R2]int g0/0/0

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

[R2-GigabitEthernet0/0/0]ipv6 enable
[R2-GigabitEthernet0/0/0]ipv6 address 2001::2 64
[R2-GigabitEthernet0/0/0]q
[R2]ipv6
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ipv6 enable
[R2-GigabitEthernet0/0/1]ipv6 address 2002::1 64
[R2-GigabitEthernet0/0/1]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

The device is running!

<Huawei>sys
Enter system view, return user view with Ctrl+Z.
```

```
[Huawei]sys R3
[R3]UN IN EN
Info: Information center is disabled.
[R3]ipv6
[R3]int g0/0/1
[R3-GigabitEthernet0/0/1]ipv6 enable
[R3-GigabitEthernet0/0/1]ipv6 address 2002::2 64
[R3-GigabitEthernet0/0/1]q

[R3]ipv6
[R3]ipv route-static 2001::1 64 2002::1
Info: The destination address and mask of the configured static route
mismatched, and the static route 2001::/64 was generated.
[R3]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

<R3>sa
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.......
  Configuration file had been saved successfully
```

Note: The configuration file will take effect after being activated

Второй эксперимент




```
The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]un in en
Info: Information center is disabled.
[R1]ipv6
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ipv6 enable
[R1-GigabitEthernet0/0/0]ipv6 address 2001::172:16:12:1 64
[R1-GigabitEthernet0/0/0]

  Please check whether system data has been changed, and save data in time
  Configuration console time out, please press any key to log on

[R1]ipv6 route-static 2002::192:168:23:3 64 2001::172:16:12:2
Info: The destination address and mask of the configured static route
mismatched
, and the static route 2002::/64 was generated.
[R1]ping ipv6 2002::192:168:23:3
  PING 2002::192:168:23:3 : 56  data bytes, press CTRL_C to break
    Reply from 2002::192:168:23:3
    bytes=56 Sequence=1 hop limit=63  time = 30 ms
    Reply from 2002::192:168:23:3
    bytes=56 Sequence=2 hop limit=63  time = 40 ms
    Reply from 2002::192:168:23:3
```

```
    bytes=56 Sequence=3 hop limit=63  time = 40 ms
    Reply from 2002::192:168:23:3

  --- 2002::192:168:23:3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
   round-trip min/avg/max = 30/34/40 ms
[R1]

The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R2
[R2]UN IN EN
Info: Information center is disabled.
[R2]ipv6
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ipv6 enable
[R2-GigabitEthernet0/0/0]ipv6 address 2001::172:16:12:2 64
[R2-GigabitEthernet0/0/0]q
[R2]ipv6
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ipv6 enable
[R2-GigabitEthernet0/0/1]ipv6 address 2002::192:168:23:2 64
[R2-GigabitEthernet0/0/1]q
[R2]ping ipv6 2002::192:168:23:3
  PING 2002::192:168:23:3 : 56  data bytes, press CTRL_C to break
    Reply from 2002::192:168:23:3
    bytes=56 Sequence=1 hop limit=64  time = 50 ms
    Reply from 2002::192:168:23:3
    bytes=56 Sequence=2 hop limit=64  time = 20 ms
    Reply from 2002::192:168:23:3

  --- 2002::192:168:23:3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/30/50 ms
[R2]

The device is running!
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys R3
[R3]un in en
Info: Information center is disabled.
[R3]ipv6
[R3]int g0/0/1
[R3-GigabitEthernet0/0/1]ipv6 enable
[R3-GigabitEthernet0/0/1]ipv6 address 2002::192:168:23:3 64
[R3-GigabitEthernet0/0/1]q
[R3]ipv6 route-s
[R3]ipv6 route-static 2002::192:168:23:2 64 2001::172:16:12:1
Info: The destination address and mask of the configured static route
mismatched
, and the static route 2002::/64 was generated.
[R3]ipv6 route-static 2001::172:16:12:1 64 2002::192:168:23:2
Info: The destination address and mask of the configured static route
mismatched, and the static route 2001::/64 was generated.
[R3]
```

СПИСОК ЛИТЕРАТУРЫ

1. Семенов А.Б. Волоконная оптика в локальных и корпоративных сетях связи. – М.:КомпьютерПресс. 1998г.
2. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы. М.: ДМК-Пресс, 2002г.
3. Гроднев И.И., Мурадян А.Г. Шарафутдинов Р.М. И ДР. Волоконно-оптические передачи и кабели. – М: Р/с., 1993г.
4. Understanding Rapid Spanning Tree Protocol (802.1w) - объяснение принципов работы RSTP на сайте cisco.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2016г.
6. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи СПб. БХВ-Петербург, 2010г.
7. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. СПб.: БХВ-Петербург, 2014г.
8. Деарт В.Ю. Мультисервисные сети связи. Транспортные сети и сети доступа. М.: Брис-М, 2014г.
9. Configuration Guide - IP Routing. Huawei Technologies Co., Ltd. – 2011г.
10. Configuration Guide - Ethernet. Huawei Technologies Co., Ltd. – 2011г.
11. Васин Н.Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов. М.: ИНТУИТ, БИНОМ, 2011г.
12. Васин Н.Н. Системы и сети пакетной коммутации. Часть 1.Основы построения сетей пакетной коммутации: Учебное пособие. Самара: ПГУТИ, ИУНЛ, 2015г.
13. Васин Н.Н. Системы и сети пакетной коммутации. Часть 2. Маршрутизация и коммутация: Учебное пособие. Самара: ПГУТИ, ИУНЛ, 2015г.
14. IPv6: A 2012 Report Card Архивная копия от 10 сентября 2013 на Wayback Machine (англ.)
15. ↑ IPv6 in 2013: Where Are We Now? - InternetNews. www.internetnews.com. Дата обращения: 14 февраля 2019. Архивировано 4 ноября 2018 года.
16. ↑ IPv6 – Google (англ.). www.google.com. Дата обращения: 9 февраля 2024. Архивировано 5 февраля 2024 года.