Міністерство освіти і науки України
Державний університет телекомунікацій

Гніденко М.П.
Гайдур Г.І.
Сєрих С.О.

Перспективні компоненти та засоби інфокомунікаційних технологій

Навчальний посібник

Київ - 2017

УДК 004.7(075)

Гриф надано Державним університетом телекомунікацій

Рецензенти: **Прокопов С.В**., кандидат технічних наук, доцент, начальник відділу дослідження змісту вищої освіти Інституту модернізації змісту освіти.
Приходько Ю.І., кандидат технічних наук, доцент, головний науковий співробітник Науково-методичного центру Національного університета оборони України

Гніденко М.П., Гайдур Г.І., Сєрих С.О.
Перспективні компоненти та засоби інфокомунікаційних технологій. – Навчальний посібник. – Київ: ДУТ, 2017. – 168 с. (на російській мові)

На ринку інформаційних технологій (IT) дуже динамічно просуває свої досягнення в області мережевих технологій компанія Hewlett-Packard (HP), в якості світового лідера виробництва мережевого обладнання для проектування, розгортання і експлуатації мереж на основі відкритих стандартів і конвергентної інфраструктури. Завдяки використанню мережевого обладнання компанії Hewlett-Packard (HP), можна істотно підвищити оперативність малого і середнього бізнесу, зменшити вимоги до обслуговування і знизити витрати на утримання IT-середовища.

У навчальному посібнику розглядаються питання проектування і впровадження мережевих рішень компанії Hewlett-Packard (HP) на основі таких понять як основи мережевих технологій і мережевого обладнання, інфраструктури дротових і бездротових мереж, протоколів TCP/IP, комутації та маршрутизації, адміністрування та управління мережами, безпеки мереж, усунення несправностей, оптимізації, доступності і надійності мереж. Всі питання мають прикладний характер і пояснюються на практичних прикладах.

Матеріали навчального посібника є основою для переходу до оволодіння відкритих стандартизованих рішень, як архітектура: таких HP FlexNetwork з єдиною системою управління та моніторингу HP Intelligent Management Center (IMC HP), а також програмно-визначених мереж SDN (Software Defined Networking).

Навчальний посібник призначено для студентів, аспірантів і викладачів, які планують підготуватися до міжнародної сертифікації рівня HP Accredited Technical Associate (HP ATA) – Networks.

Содержание

Введение

Компьютерные информационные технологии используются во всех областях научной и производственной деятельности. Компьютеризации подверглись такие области деятельности как автоматизация процессов управления сложных производств, системы моделирования и численные методы исследования природных явлений, системы коммуникаций и связи, системы накопления и хранения знаний, электронные информационные системы. Новые достижения в развитии этих систем стали возможны благодаря их интеграции с сетевыми технологиями.

Это учебное пособие является результатом опыта преподавания авторами курсов сетевых технологий компания Hewlett Packard Enterprise в Государственном университете телекоммуникаций.

Hewlett Packard Enterprise помогает заказчикам в построении эффективной, продуктивной и безопасной ИТ-среды посредством соединения традиционных подходов с новыми, что позволяет компаниям быстро реагировать на идеи создавая, используя и развивая новые решения на основе лучшего опыта и лучших бизнес-моделей. Новые подходы помогают выбрать и внедрить вычислительные мощности, которые могут оказать значительное влияние на результатыи эффективность бизнеса, построить хранилище, способное «думать» в не меньшей степени, чем хранить, использовать сети, осуществляющие обмен данными быстрее и безопаснее, чем когда либо.

Интенсивное развитие и внедрение новых сетевых технологий последние годы потребовало не только притока большого числа специалистов по разработке и проектированию систем, но и существенно изменило требования к уровню подготовки пользователей.

Этими фактами обусловлен повышенный спрос к учебным программам и курсам по различным направлениям информационных технологий, что в свою очередь требует наличия большого числа учебно-методического материала.

Учебное пособие предлагает материал по сетевым технологиям как с точки зрения теоретических основ сетевых технологий и сетевого оборудования, так и практических рекомедаций по их использованию. Такой подход может быть полезен как начинающих осваивать новый вид деяльности, так и специалистам, которым необходимо освежить знания и повысить квалификацию.

Глава 1:
Основы сетевых технологий

Введение

В начале развития компьютерных сетей, проблема совместимости между оборудованием различных производителей была актуальной как никогда. Существовало несколько несовместимых стандартов подключения компьютеров, форматирования данных и приложения передаваемых данных. Ранние модели сети были основаны на этих оригинальных концепциях. Очень быстро стала очевидной потребность в общих стандартах. В этой главе мы введем основные понятия сетей и сетевых стандартов. Начнем с принятого базового стандарта – семиуровневой модели взаимодействия открытых систем (OSI). Затем мы сравним модель OSI с наиболее распространенной реализацией используемой в настоящее время, моделью TCP/IP. Мы рассмотрим практическое применение Ethernet и беспроводных технологий. Также кратко рассмотрим некоторые стандарты, более высокого уровня, используемые для реализации адресации, основной сетевой безопасности и виртуальных локальных сетей (VLAN).

Цели

В этой главе вы изучите:

- Описани семиуровневой модели OSI.
- Сравнение и сопоставление моделей OSI и TCP/IP.
- Пояснение цели и использования назначения различных методов адресации.
- Определение общих технологий Ethernet.
- Определение общих беспроводных технологий.
- Пояснение основных концепций безопасности.

Модель OSI

Международная организация по стандартизации (ISO) представила модель OSI (рис. 1-1), как способ решения дилеммы(необходимости выбора) стандартов, вызванной использованием множественых несовместимых стандартов в прошлом. Модель OSI является семиуровневой моделью, которая организует и описывает сетевые функции и интерфейсы. Модель достигла своей нынешней формы в 1983 году.

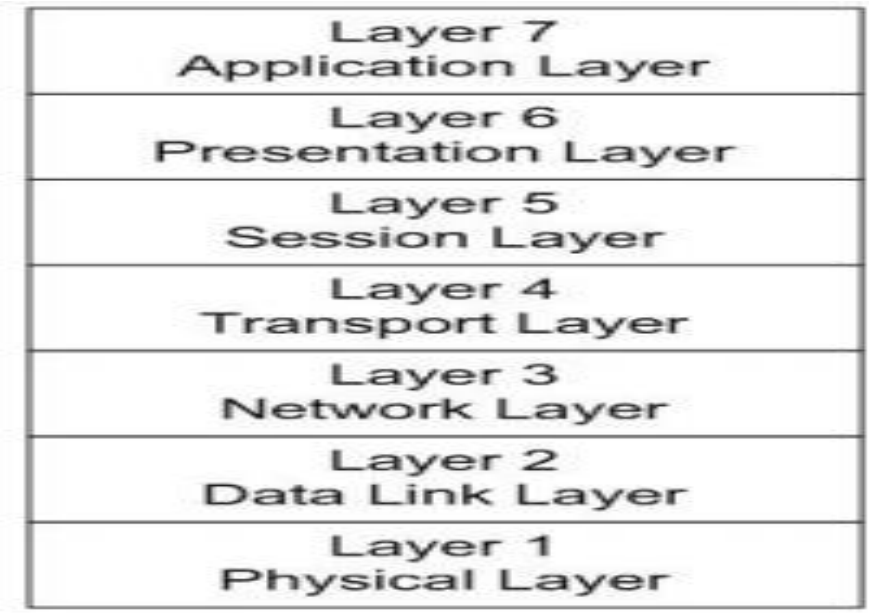


Рис. 1.1 – Модель OSI

Модель OSI состоит из слудующих уровней: физического, канального, сетевого, транспортного, сеансового, уровня представления и уровня приложений. За исключением физического уровня, каждый из уровней может взаимодействовать только с уровнем расположеным непосредственно выше или ниже него. Физический уровень одного сетевого устройства, может взаимодействовать с физическим уровнем другого сетевого устройства.

Модель OSI обеспечивает стандарты руководства, а не строгие правила реализации сети. Другие организации по стандартизации как правило, следуют этой модели, чтобы обеспечить функциональную сеть. Например, IEEE разработал подробные стандарты протоколов, реализованных на уровнях 1 и 2: 802.3 (Ethernet) и 82.011 (беспроводные технологии).

Institute of Electrical and Electronics Engineers (институт инженеров электорехники и электроники) (IEEE) - техническая организация, которая способствует развитию и публикаций стандартов.

Протокол - набор правил, которые устройства используют для взаэмодействия. Каждый из уровней использует собственные протоколы для обеспечения сеанса связи.

Одной из сильных сторон модели OSI является то, что она обеспечивает общий контекст для описания сетей и сетевых устройств. Утверждая, что устройство работает на определенном уровне, имеется ввиду что устройство включает

в себя функционал всех предведущих уровней. Например, многие переключатели описаны в уровне 3, это означает, что устройство реализует функциональные возможности сетевого уровня. Также это означает что в нем реализована функциональность канала передачи данных и физического уровня.

Коммутатор (switch) - сетевое устройство связи, что пропускает данне из порта источника к порту назначения.

Уровень 1 - Физический уровень

Физический уровень отвечаетственый за передачу и прием данных по среде передачи. информация рассматривается как неструктурированный поток исходных данных сигнала. Передача может быть осуществлена на физическом носителе, например по медному проводу или оптоволокну, или же по беспроводной сети с помощью радиоволн.

Среда передачи - тот путь данных, по которому осуществляется передача данных. В проводной сети медные кабеля используются наиболее часто.

Физический уровень обеспечивает прямую связь между узлами. Кроме того, этот слой лучше всего определяется и наиболее последовательно реализуется.

Узел – этот термин используется для обозначения точки подключения к сети, как правило, это компьютер или другое сетевое устройство.

Физическая середа

Физическая среда это путь, по которому передаются данные. Физический уровень определяет тип среды которая используется. Он также определяет, как устройства физически подключены к среде, в том числе типа разъема, номер контакта, и так далее.

В случае проводной сети, требуются определенные виды разьемов. Определяется тип носителя: медного или волоконно-оптического кабеля. Также определяется мощность сигнала.

Опто-волоконный кабель - кабель из стекла или пластиковых волокон, который передает сигнал в виде световых лучей.

Для беспроводных устройств, для передачи и приема задается частота. Стандарты указывают частоту, которая будет использоваться и рекомендуемые уровни передачи.

Передача данных

Технические характеристики, указанные на физическом уровне определяют кодировку данных – как данные преобразуются в сочитаемую форму для передачи. Кодирование данных включает в себя представление данных в виде 1 или 0, определяет как начать сначала и до конца кадра, и как данные синхронизировать.

Кодирование данных - преобразование данных из потока данных в другой формат. В контексте физического уровня, это относится к конвектированию данных в формат пригодный для передачи.

Характеристики физического слоя также определяют метод передачи. Данные могут быть отправлены с использовать либо цифровую или аналоговую передачу. Системы передачи по оптоволокну, для примера, используют цифровую передачу. В волоконно-оптических системах передачи, наличие или отсутствие света используется для выражения двух состояний цифровой передачи: 0 или 1. Беспроводная передача являются аналоговой передачей по самой своей природе, потому что она использует радио частоты передачи.

Цифровой сигнал - сигнал с двумя различными состояниями, представленый в виде значений 0 и 1 для передачи данных.

Аналоговый сигнал характеризуется постоянно меняющейся амплитудой сигнала (высота волны), частотой (скорось изменения), или обеих составляющих.

Основано на обычае радиопередачи и сигнал генерируется, когда воспроизводиться.

Технология передачи - передача данных либо в качестве аналогового или цифрового сигнала.

Уровень 2 – Канальный

Канальный уровень несет ответственность за обеспечение того ,что данные передаються между узлами без ошибок. Передача данных без ошибок есть конечной целью этого уровня, но это не всегда достигается. До сих пор, с использованием современных технологий передачи, большинство передач часто очень близки к безошибочным. Такая точность осуществляется с помощью следующих методов:

- Управления ссылками - устанавливает логическую связь между узлами и затем устраняет соединение, когда это уже не нужно.
- Контроль трафика - управляет передачей кадров и отключает узел передачи, когда данные не доступны для отправки.
  - Секвенирование - гарантирует, что кадры посылаются (и получаются) последовательно.
  - Подтверждение - признает получение кадров, как способ обнаружения потерянных или поврежденных кадров.
  - Определение границ - определяет форматы кадра, и признает эти границы на полученных кадрах.
  - Коррекция ошибок - проверяет целостность кадра.
  - Управление доступом - определяет, какой узел может использовать носитель для передачи.

Каждый узел однозначно определены на канальном уровне через уникальный адрес который известен как адрес управления доступом к среде (MAC-адрес).

MAC-адрес - адрес, который однозначно идентифицирует узел сети на 2 уровне модели OSI.

MAC-адрес обычно записывается как 12-значное шестнадцатеричное число. Первые шесть цифр идентифицируют производителя сетевого интерфейса. Остальные цифры представляют собой уникальный адрес адаптера. Это актуально как для проводных, так и для беспроводных сетевых адаптеров. В некоторых случаях, например, когда сети реализованы на виртуальной машине, MAC-адрес генерируется с помощью программного обеспечения.

Виртуальная машина - компьютер в памяти физического компьютера, что позволяет представлять один компьютер в качестве несколько отдельных компьютеров, выполняющих изолированные функции.

Протоколы передачи низкого уровня, такие как Ethernet и Token Ring, определяются на обоих слоях – физическом и канальном. Эти два протокола несовместимы. Они не могут интерпретировать данные друг друга, потому что их кадры строятся по-разному. Они также имеют различные определения для типов физических носителей и характеристик сигнала.

Ethernet - наиболее распространенный протокол передачи низкого уровня. Иногда также упоминается как транспортный протокол.

Token Ring - собственный протокол низкого канального уровня, который наиболее часто используется в реализации сети IBM.

Вы можете получить MAC-адрес для сетевого Ethernet адаптера в Windows, выполнив команду **IPCONFIG** (Рисунок 1-2).

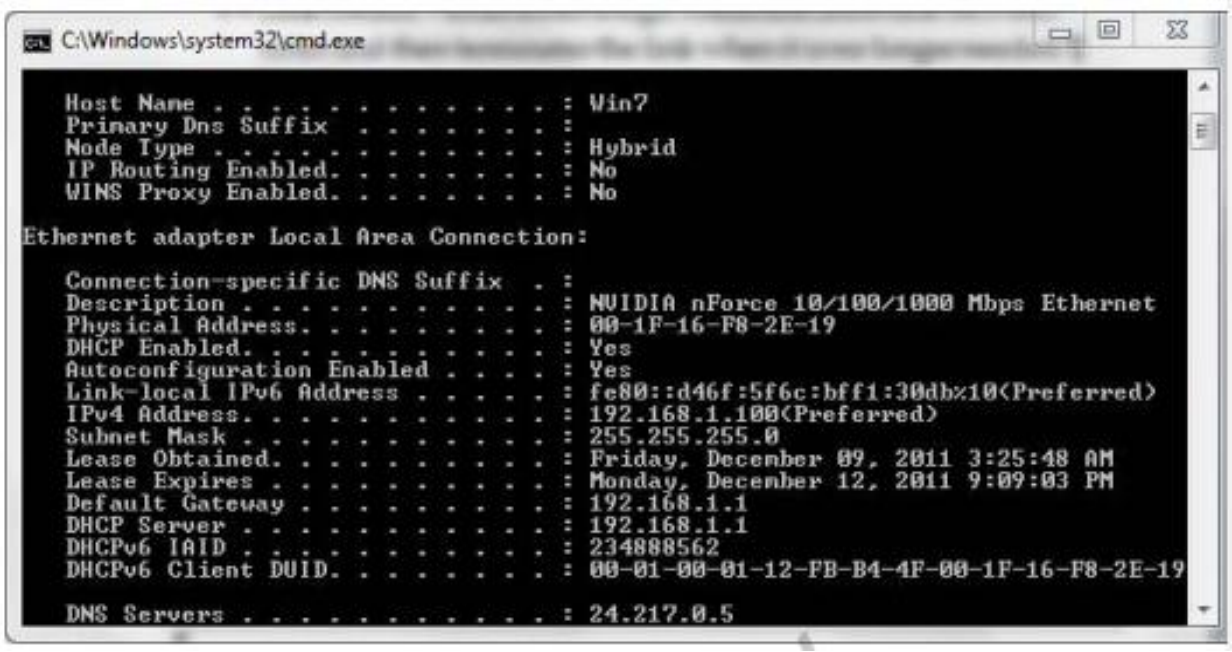


Рис. 1.2 – Просмотр MAC-адреса

MAC-адрес будет указан в конфигурации адаптера Ethernet. Он в списке физического адрес адаптера. В этом случае, адрес:

00-1F-16-F8-2E-19

Уровень 3 - Сетевой уровень.

Сетевой уровень производит маршрутизацию в сети возможной. Каждый узелсеть идентифицируется по уникальному адресу, который состоит из адреса сети и адреса узла (Рисунок 1-3). К протоколам сетевого уровня также относятся логические имена устройств (такие как CopyRoomPC) для сетевых адресов.

Рис. 1-3 – Адрес Ipv4

Вместо того, чтобы быть жестко(hard-coded)* фиксированным для узла, как MAC-адрес, сетевой адрес определяется через конфигурации устройства. Адрес может быть либо настроен на узле или применяться автоматически, когда узел подключается к сети.

Болие детально формат адреса IPv4 мі рассмотрим в дальнейшем курсе, но, как небольшое примечание, адрес идентифицирует узел и подсеть, на которой он расположен. Значение, известное как маска подсети определяет, какие биты используется для каждой части адреса.

Маршрутизаторы отвечают за пересылку трафика между сетями. Маршрутизаторы отвечают за то, чтобы данные следующим образом прокладывали путь к правильному адресату. Они также несут ответственность за управление фрагментацией.

Маршрутизатор (router) - устройство отвечает за направление трафика на основе сетевого адреса.

Фрагментация - процесс деления сетевого пакета на пакеты меньшего размера для сборки в пункте назначения.

Фрагментация необходима из-за того, что некоторые маршрутизаторы имеют меньший размер MTU чем другие. Когда маршрутизатор с большим MTU передает кадр к маршрутизатору с меньшим MTU, он должен разбить кадр так, чтоб он мог быть собран после принимающего узла.

Максимальный блок передачи (MTU - maximum transmission unit) - крупнейший размер пакета или кадра, с которым маршрутизатор может справиться.

(hard-coded)* -данные находящиеся в самом коде.

Уровень 4 – Транспортный

Транспортный уровень отвечает за безошибочную доставку сообщения. Конкретные функции, реализованные в соответствии с протоколом на транспортном уровне несколько зависят от качества передачи и условий проверок на ошибки на сетевом уровне и ниже. Основные функции аналогичны тем, которые предусмотрены для кадров канального уровня, но на более высоком уровне. К ним относятся:

- Сегментация - разбивает сообщение (если необходимо) для сборки получения транспортного уровня.
- Подтверждение - использует подтверждения, чтобы обеспечить надежную доставку.
- Контроль трафика - обеспечивает передачу только тогда, когда имеется сообщение.
- Мультиплексирование - управляет передачей нескольких сообщений.
- Транспортный уровень добавляет информацию заголовка, которая позволяет собрать сообщение при получении. Это включает в себя нумерацию, если это не предусмотрено в нижних слоях.

Уровень 5 – Сеансовый.

Сеансовый уровень отвечает за установление и поддержку сесий между хостами, а также завершение сеанса, когда он перестаёт быть необходим. Протоколы сеансового уровня также предоставляют функции для поддержки сессии, включая безопасность, распознавание между хостами и запись сессии.

Сессия - ряд взаимодействий, которые происходят между двумя узлами в ходе подключения.

Уровень 6 – Уровень представления

Уровень представления отвечает за форматирования данных из уровня приложений, так что данные могут быть переданы или так, чтобы данные могут быть обознаны уровнем приложений. Это делается с помощью перевода данных, который включает:

- Перевод символов - обычно ASCII или EBCDIC.
- Преобразование - по мере необходимости, в том числе порядок битов, форматирование конца строки, и так далее.

- Сжатие - применения алгоритмов сжатия данных для уменьшения размеров передаваемых данных.
- Шифрование - шифрование/дешифрование данных для обеспечения безопасности данных.

Американский стандартный код для обмена информацией (ASCII - American Standard Code for Information Interchange) - способ кодирования символов, который используется чтобы предоставить 128 символов, 7-ми битными значениями. Чаще всего используется в операционной системе UNIX и некоторыми устаревшими приложениями на DOS основе.

Расширенный двоично-десятичный код обмена (EBCDIC - Extended Binary Coded Decimal Interchange Code) - двоичный код для символьного кодирования, разработаный IBM и, прежде всего, используется в ЭВМ.

Даже тогда, когда данные передаются в открытом виде, шифрование данных, как правило, применяется к любым паролям, передаваемых между узлами.

Уровень 7 – Уровень приложений

Пользователи и приложения обеспечивают доступ к сетевым службам через уровень приложений. Все сетевые услуги знакомые вам осуществляются через уровень приложений, в том числе:

- Дистанционный доступ к файлам и к принтеру.
- Совместное использование ресурсов.
- Связь между процессами, работающими на различных компьютерах.
- Электронные сообщения и электронная почта.
- Службы каталогов.
- Просмотр веб-страниц.

Процесс – в этом контексте, процесс относится к случаю, когда программа выполняется на компьютере.

Управление сетью осуществляется также на уровне приложений. Несколько специализированных протоколов управления реализуют управление сетью.

Модель TCP/IP

Transmission Control Protoco/Internet Protocol (TCP/IP) стек сетевых протоколов, который в настоящее время чаще всего используется. Он используется в большинстве локальных и глобальных сетях, и это является основным протокол поддержки в Интернете.

Локальная сеть (LAN) – соединённые компьютеры в рамках небольшой географической области, как правило, одного офиса или здания.

Глобальная сеть (WAN) - компьютеры, подключённые в более широком географическом районе. Интернет является примером WAN.

Модель TCP / IP основана на четырех слоях DARPA модели. Рисунок 1.4 показывает, как TCP / IP модель отображается на модели OSI. Функциональность обеспечивается с помощью различных протоколов, реализованных в каждом из уровней.

DARPA (Defense Advanced Research Projects Agency) - проекты перспективных исследований агентства обороны. Независимые исследования агентства, финансируемого Департаментом обороны США.

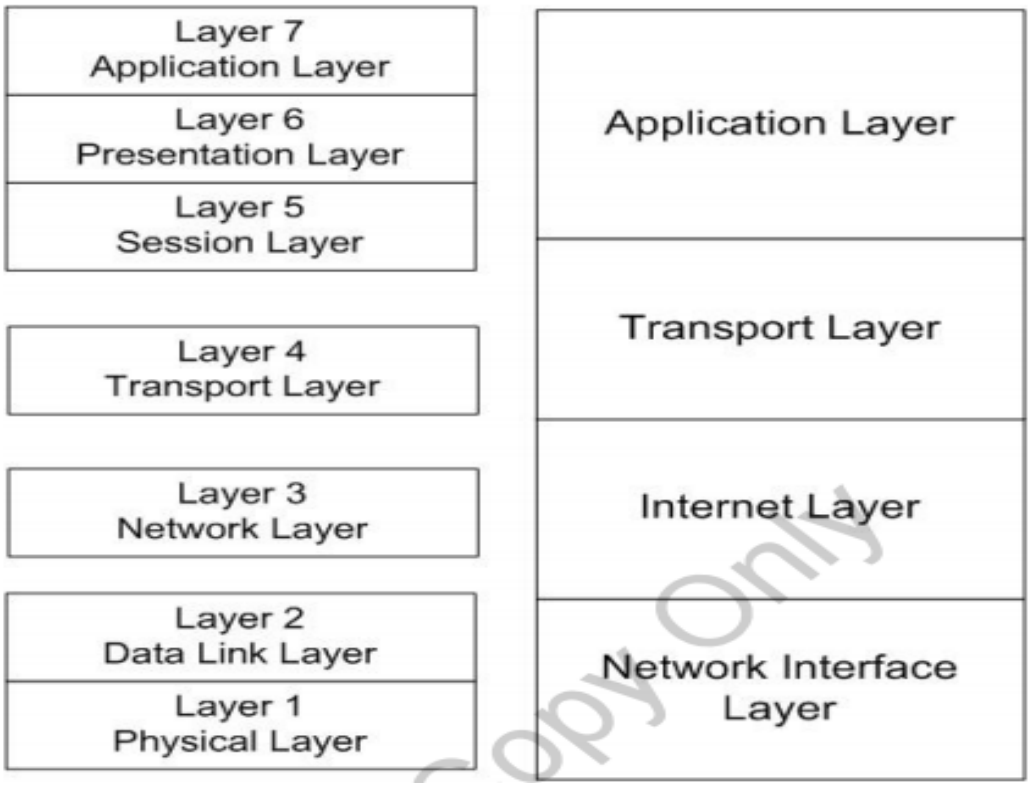


Рис. 1.4 – Сетевая модель TCP/IP

Уровень сетевого интерфейса

Уровень сетевого интерфейса (также известный как слой доступа к сети) реализует большую часть функциональности физического и канального уроней модели OSI. Как и в модели OSI, отдельные узлы идентифицированы MAC-адресами, реализуемые на уровне сетевого интерфейса.

Хост - термин используется для обозначения узлов в TCP/IP сети.

Как упоминалось ранее, транспортные протоколы низкого уровня, такие как Ethernet и 802.11 беспроводных сетей реализуются на этом уровне.

Модель TCP / IP была разработана, чтобы работать независимо от сети коммуникационных технологий. Из-за этого, она может быть приспособлена, чтобы поддерживать широкий спектр протоколов, в том числе протоколов WAN, таких как Frame Relay, в слое сетевого интерфейса. Такая гибкость позволяет TCP / IP быть адаптированой для поддержки новых сетевых коммуникационных технологий.

Frame Relay – (ретрансляция кадров) - формат передачи низкого уровня предназначен для поддержания связи между локальными сетями и между конечными точками WAN.

Уровень сетевого интерфейса не поддерживает последовательности и признание определенного на канальном уровне OSI. Когда модель TCP / IP была впервые разработана, предполагалось, что связь на уровне сетевого интерфейса будет ненадежной. Вместо этого, функциональные возможности, необходимые для поддержки надежной связи осуществляется на уровнях транспорта и приложений.

Интернет Уровень

Уровень Интернет TCP/IP обеспечивает ту же функциональность, что и сетевой уровень модели OSI. В своей текущей реализации, Интернет слой выполнен из двух слоев, действующих параллельно:

- Уровень Интернет-протокола версии 4 (IPv4)
- Уровень Интернет-протокола версии 6 (IPv6)

Оба несут ответственность за адресацию хостов, сетевую адресацию, маршрутизацию и упаковку данных для передачи. В дальнейшем, каждый из них будет обсуждаться, но опишем их.

Интернет-протокол, IPv4 или IPv6, несет ответственность за фрагментацию пакетов для передачи и сборку пакетов после получения. Оба протокола обеспечивают надежную доставку без установления соединения.

Установления соединения - между двумя хостами происходит без предварительной договоренности (без установления сеанса).

Основное различие между ними состоит в формате адреса. IPv4, оригинальный протокол Интернет, использует 32-битный адрес. Его, как правило, записывают в десятичной нотации, как показано ниже:

192.168.10.42

IPv4 по-прежнему используется в большинстве случаев, Интернет прекращает работать с адресацией IPv4, поскольку она доступна для назначения. По этой причине был разработан протокол IPv6 , он расширяет адресное пространство, обеспечивая 128-битный адрес, представленный в виде серии шестнадцатеричных чисел:

fe80:d46f:5f6c:bff1:30db

Цель реализации TCP/IP, в том числе в Интернете, является постепенный переход от IPv4 к IPv6. Большинство сетевых устройств в настоящее время поддерживает как IPv4, так и IPv6. Компьютерные операционные системы настраивают хосты как с IPv4, так и с IPv6. Тем не менее, адреса IPv6 в значительной степени игнорируются, поскольку они в настоящее веремя не требуется в большинстве сетевых сред.

Для поддержки IPv4 или IPv6 протоколы, реализуемые на более высоких уровнях модели TCP/IP не нужно изменять, если они не дают информации об адресе.

ARP

Один из протоколов, выполнен на Интернет уровне, который заслуживает особого упоминания, является ARP. Есть версии ARP : в IPv4, так и IPv6. В каждом случае, его основная функция состоит в отображении IP-адресов в MAC-адресах.

Address Resolution Protocol (ARP) - протокол TCP / IP предназначен для обеспечения IP адреса / разрешение MAC-адресов.

Информацию MAC-адресов собирают путем использования широковещательных передач. Чтобы уменьшить количество передач, каждый хост имеет свой собственный кэш ARP. Вы можете ввести информацию об адресе в кэше статически, но большая часть информации сохраняется динамически в результате трансляции ARP.

Трансляция - один-ко-многим без установления соединения связи.

Вы можете просмотреть содержимое ARP кэша, выполнив следующую команду:

arp – a

Результаты будут уникальны для каждого узла, но список типичных результатов даст вам представление о том, чего ожидать.

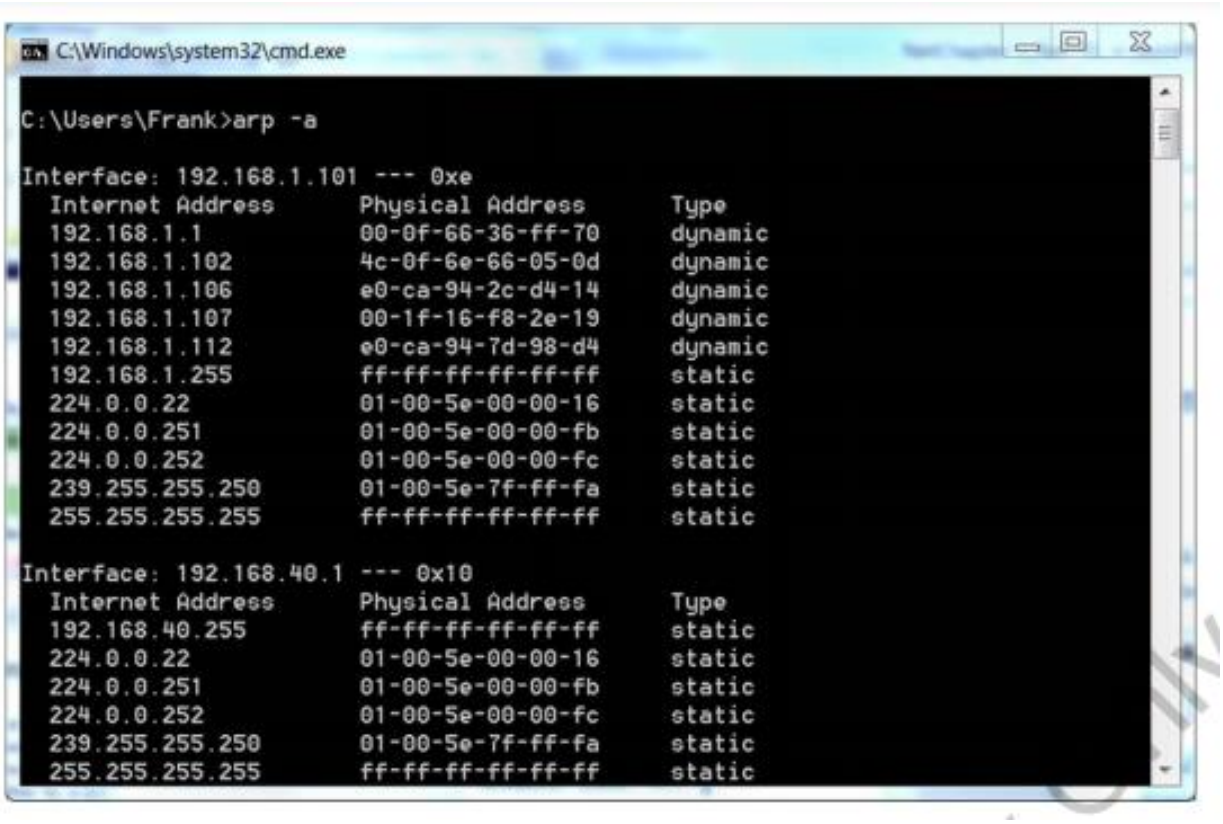


Рис. 1.5 - Пример КЭШа ARP

Обратите внимание, что каждая запись идентифицирует IPv4-адрес, физический адрес (MAC-адрес), и тип адреса: динамический или статический. Адреса назначаются либо динамически, или они сконфигурированы как статический адрес.

Транспортный уровень

Транспортный уровень TCP/IP (также известный как хост-хост транспортного уровня) несет ответственность за ту же функциональность, что и транспортный уровень модели OSI. Некоторые функции сеансового уровня OSI также обеспечивается через транспортный уровень. Транспортный уровень TCP/IP обеспечивает сессии и дейтаграммные услуги для TCP / IP прикладного уровня.

Дейтаграмма - пакет данных, содержащий пункт назначения и информацию маршрутизации.

Два основных протокола реализуют на уровнях TCP/IP:

- транспортный протокол управления (TCP)
- протокол дейтаграмм пользователя (UDP)

Оба они могут быть реализованы по протоколам IPv4 и IPv6. TCP и UDP будут детально обсуждены далее, но их быстрый обзор поможет вам понять, что происходит на этом уровне.

TCP

TCP является протоколом, ориентированным на соединение. Другими словами, это обеспечивает надежную связь (один к одному) между двумя узлами сети.

- Установление соединения между хостами
- Подтверждение последовательностей пакетов, пересылаемых между хостами
- Восстановление потерянных пакетов (через ретрансляцию)

Для обеспечения доставки данных, TCP используется всякий раз, когда это необходимо.

UDP

UDP является протоколом без установления соединения. Он может быть использован в режиме передачи один-к-одному или один-ко-многим (трансляция). Поскольку UDP не требует соединения, он не гарантирует надежную доставку, хотя надежная связь может быть реализована с помощью протоколов более высокого уровня, которые используют UDP для поставки. Как правило, UDP используется, при малых обьемах данных (не более одного пакета).

Уровень приложений

Уровень приложений отвечает за функциональные возможности, предоставляемых сеансовым уровнем, уровнем представления, и уровнем приложений модели OSI. Это интерфейс между пользователями и приложениями компьютера и сетевых услуг, предоставляемых TCP / IP. Большое количество протоколов реализованы на этом уровне. Некоторые из наиболее известных имеют дело с обменом информацией, включая HTTP, который является частью основного фундамента World Wide Web (WWW).

Протокол передачи гипертекста (HTTP) - протокол высокого уровня TCP/IP, что позволяет использовать веб-браузер для запроса и получать данные с веб-сайта.

Уровень приложений также включает в себя несколько протоколов управления, используемые для таких целей, как:

- Разрешение имен хостов в IP-адреса.
- Поддержание и обмен информацией о маршруте между маршрутизаторами
- Автоматическое предоставления информации о конфигурации сети для хост-компьютера

Протоколы реализованные на уровне приложений могут позволять создавать даже каталог устройств развернутых в сети. Эта возможность позволяет сетевому администратору создать карту сети.

Технологии Ethernet

Ethernet представляет собой протокол связи низкого уровня, которая реализуется на физическом и канальном уровне модели OSI или на уровне сетевого интерфейса модели TCP / IP, в зависимости от контекста. Это означает, что Ethernet отвечает за определение такой стандартной информации, как:

- средства передачи и типы разъемов;
- длина кабеля сегмента;
- передачи сигналов (прочность и формат);
- формат кадра;
- метод доступа к сети.

Ethernet, в настоящее время, наиболее часто используемый стандарт обмена данными для технологий локальных сетей. Одной из причин этого является то, что Ethernet, в его нынешнем виде, это стандартизированная технология, основанная на стандарте IEEE 802.3. Ethernet впервые был введен в систему собственной связи. Первыми разработчикамя является компания Xerox. В дальнейшем Intel, Digital Equipment Corporation (DEC) и Xerox работали вместе, для продвижения Ethernet в качестве стандарта, по сравнению с конкурирующими технологиями, в том числе Token Ring (IBM).

К 1980 году, Ethernet был явным победителем. Сегодня, редко можно встретить другие протоколы низкого уровня, и только в очень специализированных сетях, например на некоторых системах управления производственным процессом.

Ethernet стал настолько распространенным, что большинство производителей встраивают сетевой адаптер Ethernet (или NIC) непосредственно в материнскую плату компьютера для настольных и переносных компьютеров.

Network interface card (NIC) - сетевой адаптер связи.

Технические характеристики Ethernet

В оригинальных реализациях Ethernet используется коаксиальный кабель. Эти первые стандарты были известны как:

- 10Base5 - Толстый Ethernet или Thicknet
- 10Base2 - Тонкий Ethernet или Thinnet

Коаксиальный кабель - кабель с центральным металлическим сердечником, который переносит сигнал, окруженный изолятором и металлической оболочкой.

Термины Thicknet и Thinnet обозначают толщину коаксиального кабеля. Оба стандарта поддерживают скорость передачи данных до 10 мегабит в секунду (Mbps). Типы 10Base5 и 10Base2 использовать различные соединители. 10Base5 использует подключение AUX, а 10Base2 использует разъем BNC.

Рис. 1.6 – Сетевой адаптер

Вы врядли когда либо сталкивались с сетью использующую Ethernet через коаксиальный кабель. Сейчас стандартом является Ethernet по медной витой паре, хотя оптоволоконный кабель также используется в высокоскоростных сетях и сетях с высоким уровнем безопасности.

По этому сетевые платы Ethernet больше не поставляются с AUX или BNC соединителями, они имеют RJ-45 модульный адаптер (как показано на рисунке 1.6), волоконно-оптический адаптер, или оба адаптера. Новые компьютеры имеют RJ-45 разъем, который встроенный в материнскую плату, и они могут также иметь оптический соединитель.

Первый стандарт Ethernet который использует витую пару был известен как StarLAN и был ограничен скоростью 1 Mbps. Поскольку технологии улучшились, и потребности пользователей эволюционировали, образовалось множество Ethernet стандартов. Популярные стандарты приведены в таблице 1.1:

Табл. 1.1 - Популярные стандарты

Name	Data rate	IEEE Standard	Note
10BaseT	10 Mbps	802.3i	Requires two twisted pairs
100BaseT	100 Mbps	802.3u	Requires two twisted pairs
1000BaseT	1 Gbps	802.3ab	Requires four twisted pairs
10GBaseT	10 Gbps	802.3an	Requires four twisted pairs

Большинство коммутаторов разработаны, чтобы позволить вам использовать кросове рили кабель прямого подключения. ПИН-аут для витой пары зависит от применения кабелей.

В кабеле прямых подключений, пары на прием и передачу подключаются к таким же контактам на обоих концах, как показано на Рис. 1.7.

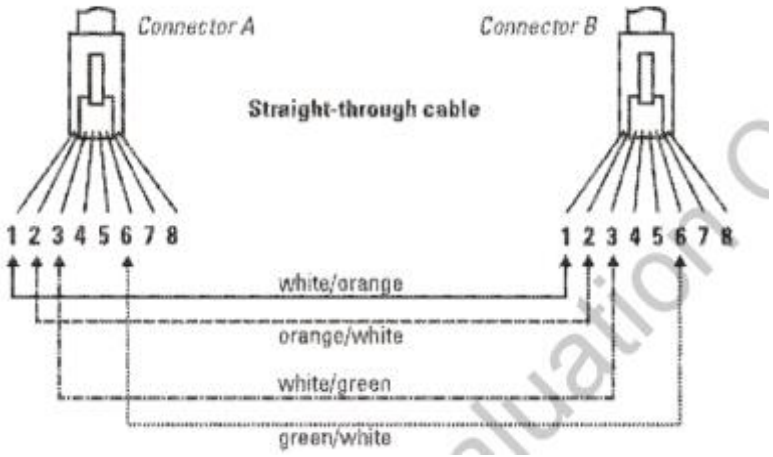


Рис. 1.7 – Прямое подключение кабеля

При прямом подключении кабеля, функции (прием или передача) противоположны на каждом конце RJ-45 (Рис. 1.8).

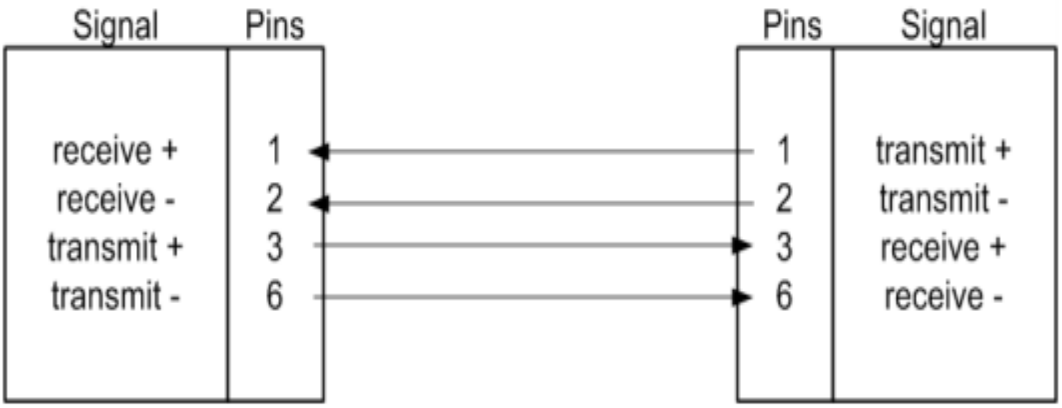


Рис. 1-8 – Схема контактов при прямом подключении

Прямое подключение контактов используется с четырьмя витыми парами, то есть используются все восемь контактов (рис 1.9).

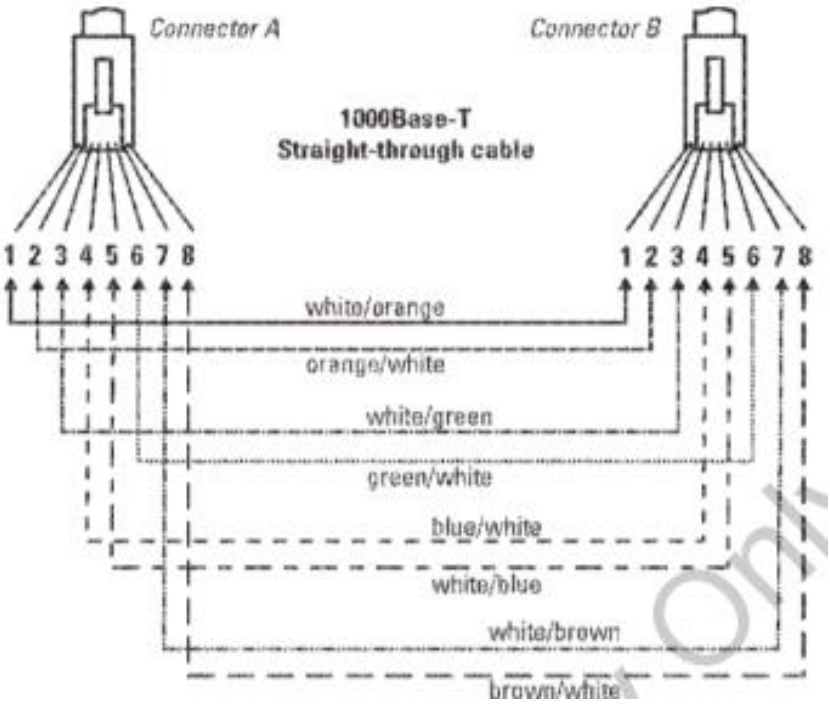


Рис.1.9 – Стандарт 1000BaseT с прямым подключением кабеля

При перекрестным подключение кабеля (рис 1.10) пары отправки и получения обмениваются местами, так что пара передачи на одном конце подключена как пара приема на другом конце.

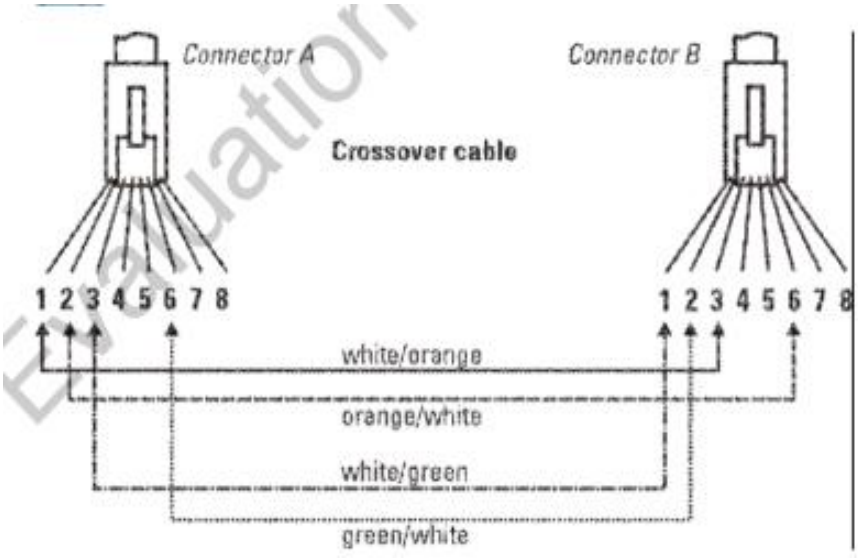


Рис.1.10 – Перекрестное подключение

При использовании кросовера, штырковый вывод RJ-45 определяеться расположение контактов определяется на обоих концах. Провода которые на одном конце есть передающими, на другом являются приемными (рис 1-11).

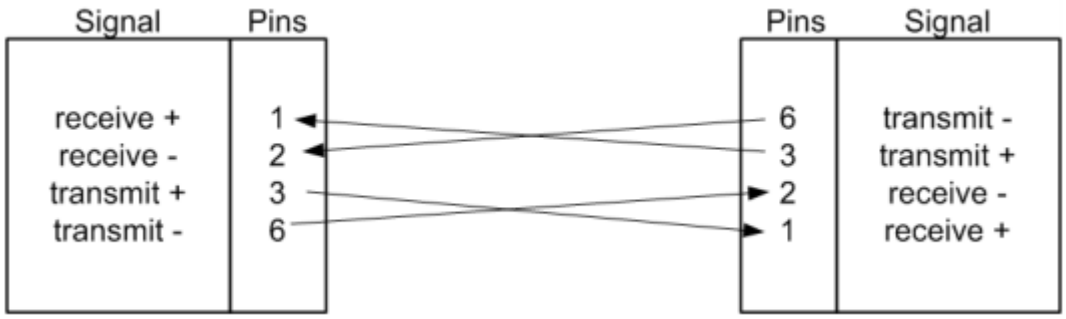


Рис. 1.11 – Схема контактов при перекрестном подключении

Стандарты Ethernet на 40 Гбит и 100 Гбит находятся в стадии разработки.
Существуют такие же стандарты для Ethernet по оптоволоконному кабелю. Волоконно-оптический кабель имеет ряд приемуществ: более высокая скорость, устойчивость к ЭМП, длинна кабельных сегментов более 20 км в длину.

Электромагнитные помехи (ЭМП) - электромагнитное поле радиочастотного спектра, вызывающее помехи.

Типы трафика Ethernet

Прежде чем мы рассмотрим как управляется связь Ethernet, мы сделаем быстрый обзор видов Ethernet трафика. Есть четыре основных типа трафика:

Unicast (Одноадресный) - посылаемый по одному конкретному хосту, идентифицированного по определенному адресу.
Broadcast (Широковещательный) - посылаемый по всем узлам сети или сегмента сети без учета адреса узла.
Multicast (Многоадресный) - посылаемый по идентифицированной группе хостов в группе многоадресной рассылки, это эффективная группа рассылки.
Anycast - посылаемый первому серверу в группе распределения, а не всем членам группы.

Как правило, большая часть трафика в сети это одноадресный трафик, связь между узлами строится по принципу один-к-одному. В коммутируемой сети, трафик фильтруют и направляют на коммутатор.
Широковещательный трафик, как правило, связан с сетевой управленческой деятельностью. Все хосты могут потенциально получать и, в свою очередь, обрабатывать трафик. ARP, например, использует передачу для разрешения MAC-адресов.
Многоадресный трафик похож на широковещательный трафик, он строится по типу один-ко-многим. Разница между ними состоит в том, что данные в многоадресном трафике предназначены для конкретных хостов. Преимущество многоадресного

трафика перед одноадресным трафиком является то, за одну передачу передаются данные сразу нескольким адресатам.
Anycast трафик также отправляется в группу рассылки, которая представляет собой набор узлов, любое устройство которых имеет одинаковый адрес назначения. Тем не менее, трафик обрабатывается первым хостом приема передачи. Anycast наиболее часто используется в управлении информацию о маршруте и доступности маршрутизатора.

Связь с помошью Ethernet

Для передачи по Ethernet данные форматируются в кадры, как показано на рисунке 1.12

Рис. 1.12 – кадр Ethernet

Каждый кадр начинается с преамбулы и разделителя начала кадра. Это продолжается MAC-адресами источника и назначения. Кадр может также включать в себя тег определения принадлежности VLAN. Кадр также идентифицирует тип протокола, встроенного в полезную нагрузку, за которым следуют полезные данные.
Стандаром для кадров есть до 1500 байт полезной нагрузки, которая является частью данных кадра Ethernet. Весь размер кадра 1518 байт. Новые устройства, в том числе коммутаторы Gigabit Ethernet, поддерживают большие кадры до 9000 байт данных.

Jumbo Frame - кадр Ethernet, что используется с IPv4 и IPv6, имеет возможность переносить до 9000 байт данных.

Неспособность большинства сетевых устройств поддерживать Jumbo кадры задержало их применение в большинстве сетей.
Данные следуют за 32-битовым CRC значением, которое используется для обнаружения ошибок. Наконец, кадр должен заканчиваться 96 битами состояния простоя, перед тем, как хост будет отправлять следующий кадр.
Циклический контроль избыточности (CRC) - способ проверки целостности данных на основе значений что генерируется из данных до передачи.

CSMA/CD

Ethernet использует метод доступа к сети, известный как CSMA/CD. С CSMA/CD, хост сначала обнаруживает передает ли в данный момент другой хост. Если среда свободна, он будет передавать свой кадр. Это было большой проблемой в первоначальных сетях Ethernet, которые разделяли соединение коаксиального кабеля или, были подключены через концентратор.
Множественный доступ к несущей с обнаружением коллизий (CSMA/CD) - метод доступа к сети, используемый протоколом Ethernet, поддерживающий общий доступ к средствам массовой передачи.
Главный недостаток CSMA/CD в том, что несколько узлов пытаются передавать одновременно. Это известно как коллизия и приводит к повреждению всех кадров, переданных в то время.
Когда происходит коллизия:

Все задействованные хосты прекращают передачу.
Оба кадры отбрасываются.
Обе станции будут ждать в течении рандомного времени и будут пытаться передавать,пока не передадут кадр успешно.
Как правило, хост настроен на максимальное количество попыток передачи. Если этот показатель будет достигнут в течение одного кадра, кадр отбрасывается и передача данных прерывается.
Сегодня большинство сетей Ethernet построены с применением коммутаторов, так что этот общий метод доступа к среде не применяется. Трафик передается через соответствующий порт на коммутаторе, так что другие устройства не разделяют соединительный кабель к месту назначения.

Основные сетевые устройства

Если сеть становится все больше, с большим количеством (и более активных) хостов, коллизия может стать серьезной проблемой и значительно ухудшить производительность сети. Тем не менее, вы можете контролировать и разделять сетевой трафик, создавая домены коллизий через устройства связи установленные в сети.

Домен коллизий - группа Ethernet узлов напрямую связанных на физическом уровне, которые могут помешать коммуникациям друг друга.

В большинстве базовых конфигураций, все компьютеры в сети подключаются непосредственно к сети. Каждый узел имеет равный доступ к сети. Весь трафик передается с конца в конец по сети кабельного сегмента.
Когда вы сегментируете сеть с помощью устройств уровня 2 или уровня 3, необходимо создать домен коллизий. С помощью сегментирования сети по этой методике,

устройства будут распространять трафика через сеть, избегая столкновений. Домены коллизий могут значительно улучшить производительность сети.
Традиционно, домены коллизий устанавливаются на основе физического расположения хостов. Каждый хост расположен по одной или другой стороне устройства. Переключатели также могут позволить вам создавать домены коллизий определенных портов на коммутаторе. Тем не менее, переключатели пошли еще дальше в предотвращении столкновений при буферизации трафика в порту.
Устройства, которые работают на физическом уровне для предотвращения коллизий ничего не делают. Наиболее распространенными устройствами этого типа являются повторители и концентраторы. Оба устройства передавать трафик без учета адреса назначения.
Устройства, которые работают на канальном уровне управлять трафиком на основе MAC-адреса. Устройства на этом уровне включают шлюзы и коммутаторы уровня 2. Эти устройства могут пропускать или блокировать трафик на основе MAC-адреса назначения. Устройства второго уровня, как правило, пропускают весь широковещательный трафик.
Устройства, которые работают на сетевом уровне управляют трафиком на основе сетевого адреса. В случае TCP/IP, управление трафиком производится на основе IP-адреса. Трафик направляется, проходит, или блокируется на основе адреса назначения. По умолчанию, маршрутизатор блокирует большинство (или весь) широковещательный трафик, создавая широковещательные домены.

Широковещательный домен - область сети, в котором распространяется вещания.

Беспроводные технологи

Беспроводные сети работают по воздуху, или, точнее, передача радиоволн осуществляется по воздуху, он выступает в качестве их средства передачи. Эта особенность дает вам возможность развернуть сети там, где невозможно провести кабель и обеспечивает ранее невообразимую гибкость в поиске и подключении к сети.
Современные беспроводные локальные сети основаны на стандартах IEEE 802.11. Как и 802.3, спецификация 802.11 определяет несколько стандартов. Спецификации 802.11 часто дает устройсту потенциал для поддержки более одного стандарта одновременно. Вы чаще слышим термин Wi-Fi, используемый для описания сети, основаной на стандартах 802.11
Первоначально беспроводные сети 802.11 были развернуты в первую очередь как частные сети, либо сети внутри дома или в офисе. За последние несколько лет общественные Wireless Fidelity (Wi-Fi) сети (горячие точки) стали обычным явлением. Большинство учебных заведений, много ресторанов (в том числе рестораны быстрого питания), и другие общественные места, например библиотеки и аэропорты, дают доступ общественности к Интернету через их точи доступа Wi-Fi.
Использование широкополосного беспроводного подключения к Интернету в настоящее время стали очень распространенным явлением. Эта беспроводная технология основана

на мобильных технологиях 3G (третьего поколения) и 4G (четвертого поколения). Устройства подключаются к Интернету через беспроводные сети сотовой связи. Стандарт 3G разработан для поддержки теоретической максимальной пропускной способности 100 Мбит/с. В практических приложениях его эффективная пропускная способность значительно меньше, а максимальная пропускная способность редко превышает 47 Мбит/с. Устройства 4G имеют максимальную пропускную способность при движении (например, в транспортном средстве) 100 Мбит/с, а при неподвижном состоянии их максимальная пропускная способность составляет 1 Гбит/с. Этот дизайн поддерживает бесшовную передачу, так как устройство перемещается по географической области, что позволяет устройству никогда не терять соединение до тех пор, пока оно остается в зоне обслуживания.

Основы коммуникаций

Беспроводная сетевая плата состоит из радиопередатчика и приемника которые работают в определенном диапазоне частот, в зависимости от стандарта или стандартов, которые поддерживает беспроводная сеть. Мобильные компьютеры и большинство настольных компьютеров поставляются со встроенным Wi-Fi модулем. Другие устройства, такие как медиа-плееры и смартфоны, также в настоящее время широко поддерживают Wi-Fi сети, а также широкополосный доступ 3G или 4G.

Частота - скорость, с которой сигнал осциллирует, измеряется в герцах (Гц).
Смартфон - мобильный телефон, который работает на мобильной вычислительной платформе, обеспечивая работу компьютера через телефон.

Все беспроводные устройства могут принимать передачу, но могут они что-либо делать с передаваемой информацией или нет зависит от конфигурации устройства и сети. Большинство конфигураций беспроводной сети 802,11 основаны на одной или более точек доступа (AP). AP выступает в качестве центральной точки доступа для беспроводных хостов. Вместо прямой связи друг с другом, хосты взаимодействуют через точку доступа.
Количество и размещение точек в сети в первую очередь зависит от количества и размещения беспроводных устройств. AP также может подсоединять компьютеры к беспроводной сети. Они также позволяют компьютерам в проводной сети взаимодействовать друг с другом.

Стандарты беспроводных сетей

Стандарты 802.11 перечислены в таблице 1.2.

Табл. 1.2 - Стандарты беспроводных сетей

802.11 Standard	Frequency	Maximum data rate
802.11a	5 MHz	54 Mbps
802.11b	2.4 MHz	11 Mbps
802.11g	2.4 MHz	54 Mbps
802.11n	2.4/5 MHz	Up to 600 Mbps

Скорости передачи данных основаны на идеальных условиях. Типичные скорости передачи данных в большинстве реализаций будут меньше, чем максимальные. Устройства 802.11g совместимы с устройствами стандарта 802.11b. Устройства 802.11n совместимы с устройствами 802.11a, 802.11b, 802.11g.
Всякий раз, используя полосу 2,4 МГц, существует потенциал для помех с другими устройствами, работающими на той же частоте. Это включает в себя устройства Bluetooth, беспроводные клавиатуры, беспроводные мыши и мониторы безопасности, микроволновые печи.

CSMA/CA

Как и Ethernet, устройства 802.11 передают данные в виде кадров. Они похожи на кадры данных Ethernet и выполняют ту же функцию. Они предназначены для организации данных для передачи.
Метод доступа к сети используемый 802.11 является CSMA/CA, который работает несколько, как CSMA/CD. Причина, по которой CSMA/CD не используется, то что передающая станция не может обнаружить коллизию.
Множественный доступ к несущей с избежанием коллизий (CSMA/CA) - метод доступа к сети, используется в беспроводных сетях стандарта 802.11, который позволяет устройствам разделять частотный диапазон общей среды передачи.
При CSMA/CA, хост прослушивает в течение заданного периода времени, чтобы обеспечить наличие канала, который он будет использовать для передачи. В большинстве реализаций, отправляется просьба об отправке сигнала (PTC) - информирования других узлов о своем намерении передать. Посылающий хост ждет сигнал (CTS - clear-to-send) для начала передачи.

Основы безопасности

Безопасность является постояной проблемой в почти любой сетевой среде,учитывая это , безопасность будет рассмотрена несколько позже в течение этого курса. В данное время, наша дискуссия ограничится кратким введением в концепции безопасности. Мы ориентируемся на двух ключевых областях:

Аутентификация и ресурс доступа.
Данные и безопасность святи.

В реальных приложениях, вы увидите, что эти две составляющие часто пересекаются и не могут быть легко разделённы.

Основы аутентификации

Если вы когда-либо входили на компьютер с помощью пароля, вы приняли участие в процессе аутентификации. Имя пользователя и пароль, которые вы вводили сравниваются с сохраненной информацией. Некоторые формы аутентификации обычно требуются при подключении к сети, запуске утилит управления, или попытке получить доступ к ресурсам, таким как файлы. Довольно часто различные виды деятельности требуют различных уровней доступа и, в свою очередь, отдельный аутентификации.
Для пользователей, аутентификация, как правило, на основывается на следующем:
Что вы знаете.
Что у вас есть.
Кто вы.

"То, что вы знаете," как правило, относится к паролю, PIN-коде или другой информации, которую знаете только вы. Специалисты, для обеспечения безопасности, не используют однофакторную аутентификацию как единый способ защиты. Пароли не сложно подобрать, особенно когда пользователи выбирают простые, легкие для подбора пароли. Персональный идентификационный номер (PIN-код) - числовое значение используется для проверки идентичности.
Однофакторная аутентификация - аутентификация на основе только одного типа фактора аутентификации.
"То, что у вас есть" относится к какому-то типу маркера физической безопасности, например смарт-карты, удостоверение, ключ, или другое физическое устройство. Вы должны предоставить один из этих физических устройств, перед процедурой аутентификации.
"Кто вы" относится к биометрической информации. Сканеры отпечатков пальцев и сетчатки становятся обычным явлением в приложениях среднего и высокого уровня безопасности. Некоторые устройства безопасности даже рассчитаны на последовательностях ДНК. Многие ноутбуки и клавиатуры теперь поставляются с встроенным сканером отпечатков пальцев.

Биометрическая информация - информация основана на физических характеристиках.

Иногда используется четвертый фактор, используемый для аутентификации "то, что вы можете сделать", он базируется на признании тебя по деятельности.
Общий подход к повышению безопасности полагается на многофакторную аутентификация. Например, можно требовать смарт-карту и пароль, или удостоверение и отпечаток, прежде чем разрешить доступ.

Многофакторная аутентификация - аутентификация требует, по крайней мере два типа проверки подлинности учетных данных для выполнения проверки подлинности. Например, то, что вы знаете, (ПИН-код) и что-то у вас есть (смарт-карта).

Большинство систем защиты сети определяют, к каким ресурсам вы можете получить доступ и какие уровни доступа доступны для вас. Вам можете быть предоставлен доступ на уровне чтение / запись ваших собственных файлов, хранящимся в сети, но ограничен доступ на чтение других файлов. Как правило, вы не будете иметь доступа к большенству файлов.
Аутентификация не ограничивает пользователей. Многие современные сетевые активыне программы прежде чем разрешить компьютерам установить сеанс связи проверяют компьютеры на подлинность. Беспроводные сетевые точки доступа обычно настроены на требование проверки подлинности хоста, прежде чем разрешить подключение.

Введение в Безопасность Данных

В широком смысле, безопасность данных связана с:
Предотвращением воздействия на данные
Предотвращением повреждения данных

В большинстве сетевых систем использование шифрования данных играет центральную роль в обеспечении безопасности.
Данные сохраняются в зашифрованном виде на диске. Даже если неавторизованный пользователь (или программа) получили доступ к месту хранения файла, файл по-прежнему будет защищен через шифрование.

Шифрование - процесс представления данных в нечитабельный вид с использованием алгоритма, с использованием технологий и знаний, необходимых для обращения вспять процесса.

Безопасность связи может также предотвратить несанкционированный доступ к данным. Некоторые сетевые протоколы, например HTTP, FTP, передают данные в виде текста. Тем не менее, этот формат не является безопасным, поскольку данные могут быть перехвачены третьей стороной. В правильно защищенной сети, принимаются меры для того, чтобы данные были зашифрованы для передачи, даже когда осуществляется передача по внутренней кабельной сети.

HTTPS и FTPS являются защищенными версиями этих протоколов.

Протокол передачи файлов (FTP) - по своей сути небезопасный протокол передачи данных, обычно используется для загрузки файлов из и на сервера в Интернете.

Введение в VLAN

В начале работы сети, может быть организовано только физическое местоположение сетевых узлов. Это ограничение было преодолено с введением VLAN. Старые сетевые проекты используют шлюзы и маршрутизаторы для создания границ между хостами. Современные коммутаторы обеспечивают сегментацию через VLAN. VLAN выглядит как маршрутизируемая подсеть, также называемая подсетью третьего слоя, к остальной части сети. Каждая сеть VLAN имеет свой собственный IP-адрес сети в целях маршрутизации.

Статическая VLAN является простейшим типом VLAN. В этой конфигурации, порты коммутатора назначены VLANy, создавая эквивалент подсети третьего слоя. Когда устройство подключено к порту, оно становится частью локальной сети для которой порт назначен.

Как правило, коммутатор сконфигурирован по умолчанию как единый VLAN. Для создания новых сетей VLAN, вы должны сначала удалить порты из VLAN по умолчанию. Вы даже можете определить порты из разных переключателей как часть той же VLAN.

VLAN также могут быть созданы и управляются динамически. Вы можете назначить порты к VLAN на основе таких факторов, как MAC-адрес подключенного компьютера или имя пользователя, используемого при входе на компьютер.

При использовании сетей VLAN в сети Ethernet, каждый кадр включает в себя тег 802.1Q в каждом кадре Ethernet, это приводит к увеличению общего размера кадра до максимального 1522 байт. Информация в теге идентифицирует кадр как кадр VLAN и включает в себя информацию идентификатора VLAN, чтобы помочь кадру достичь правильного назначения.

Глава 2:
Основы сетевого оборудования

Введение

Семиуровневая модель OSI обеспечивает стандартизированную структуру для сетевых устройств, а также их функциональность. В этой главе мы рассмотрим практическое применение модели OSI и устройств работающих на разных уровнях.

Мы обратим внимание на один конкретный тип устройств – коммутатор. За последние несколько лет большинство коммутаторов расширили свои возможности за счет добавления функций 2 и 3 уровней, сочетающих свойства концентраторов, мостов, маршрутизаторов и других устройств. Широкая распространённость коммутаторов в современных сетях делает их одним из ключевых объектов для исследования.

В ходе прохождения этого курса, Вы ознакомитесь с различными моделями коммутаторов фирмы Hewlett Packard. Большинство команд управления, а также интерфейс командной строки являются одинаковыми для различных коммутаторов.

Цели

В этой главе вы узнаете, как:
Определить назначение и использование общего сетевого оборудования, такого как:
сетевая карта;
ретранслятор;
концентратор;
шлюз;
коммутатор;
маршрутизатор;
Построить карту апаратных устройств для любого из уровней модели OSI.
Рассмотрите процедуры управления коммутатором.
Определите интерфейс управления.
Опишите назначение и использование журналов событий.

Распространённое сетевое оборудование

Одним из критериев классификации сетевого оборудования может выступать уровень модели OSI, на котором непосредственно работает устройство. Например:

Сетевой адаптер - работает на физическом и канальном уровнях (1 и 2 уровни).
Ретранслятор - работает на физическом уровне (1 уровень).

Необходимо акцентировать внимание студентов на то, что они должны будут знать описание сетевых устройств. Когда мы говорим , что это устройство работает на определенном уровне, то это означает, что оно также реализует функциональные возмо жности всех нижестоящих уровней.

Концентратор - работает на физическом уровне (1 уровень).
Шлюз - работает на канальном уровне (2 уровень).
Коммутатор - традиционно работает на канальном уровне (уровень 2), а также выполняет вспомогательные функции на сетевом уровне (3 уровень).

Маршрутизатор - работает на сетевом уровне (3 уровень). Когда устройство сообщает, что работает на определенном уровне, оно реализует функциональные возможности всех нижестоящих уровней. Например, мост работает на канальном уровне. Тем не менее, он был бы бесполезным, если бы он не включал в себя функционалы первого уровня, которые дают возможность подключаться и взаимодействовать, используя сети общего доступа.

Мы начинаем эту главу с обсуждения самых распространенных видов сетевого оборудования, а также их функционала. Это важно, так как мы будем ссылаться на эти устройства в течение всего курса.

Сетевой адаптер

На заре сетевых технологий сетевые адаптеры (сетевые платы) наиболее часто реализовывались в качестве дополнительных плат расширения. Они были относительно дорогими и часто вызывали затруднение в настройке. Как только сетевые компьютеры стали более распространены, и промышленность обосновалась на сетевых стандартах, цены значительно снизились.

Уже через несколько лет, сети стали настолько распространенными, что настольные и портативные компьютеры имеют, по меньшей мере, один встроенный сетевой адаптер. Настольные ПК в основном имеют уже встроенный Ethernet адаптер и порт RJ45. В ноутбуках же обычно встроен как проводной, так и беспроводной адаптер.

Развлечения, в том числе компьютерные игры, являются основной движущей силой технических инноваций. Многие компьютеры, предназначены для серьезных профессиональных игр, чтобы соответствовать мощности обработки некоторых серверов.

Вы до сих пор можете купить карты расширения, которые позволят вам оборудовать ваш компьютер дополнительными проводными или волоконно-оптическими Ethernet адаптерами. Некоторые конфигурации системы требуют несколько сетевых адаптеров. Например, если вы планируете использовать ПК в качестве проводного сетевого маршрутизатора, вам потребуется как минимум два сетевых адаптера, каждый из которых обладает собственным сетевым адресом.

Одной из причин для установки нового сетевого адаптера, может выступать увеличение производительности сети. Например, вы можете обновить компьютеры, построенные на поддержку 100Base-T, таким образом, что они смогут поддерживать 1000BASE-T.

Также вы можете увидеть сетевой адаптер в виде платы расширения при добавлении беспроводного сетевого адаптера (Рис. 2.1).

Рис. 2.1 - Беспроводной адаптер

Наиболее часто используемый способ расширения сетевой платы на ПК является подключение беспроводного сетевого адаптера в USB порт (Рис. 2.2). Как правило, установка заключается только в подключении адаптера к компьютеру, после чего компьютер сам выполнит распознание и настройку.

Рис. 2.2 – USB адаптер

Вне зависимости от того встроенный он или добавлен, сетевой адаптер выполняет те же функции для компьютера, что и другие сетевые устройства. Сетевой адаптер имеет, как минимум, MAC (Media Access Control) адрес, используемый для идентификации и подключения устройства к сети передачи данных.

Повторитель

Повторитель, по своей сути, является просто усилителем. Он работает на физическом уровне, принимая сигнал, ретранслирует его усиленным в другой сегмент кабеля. Традиционный повторитель имеет свойственный ему недостаток, который заключается в том, что он усиливает все, что получает. Если принимаемый сигнал с помехами, повторитель усиливает как сигнал и шумы.

Шумы негативно влияют на полезный сигнал, так как они могут поглощать отражённый сигнал или вступать в интерференцию с полезным сигналом, что негативно сказывается на качестве конечного (полученного) сигнала.

Ретрансляторы используют для увеличения длинны сегмента сети. В зависимости от типа сети, существуют различные правила, формирования количества повторителей между конечными точками, или узлами, в сети. На начальном этапе развития Ethernet, возможно было подключить до пяти отрезков кабеля с четырьмя повторителями (Рисунок 2-3). Только три сегмента могли иметь все подключенные устройства, и они должны были быть разделены по сегментам, без подключенных устройств. Иногда это правило называют «5 - 4 - 3». Правило Ethernet для использования ретрансляторов: пять сегментов, соединенных четырьмя повторителями с не более чем тремя сегментами с подключенными к ним устройствами.

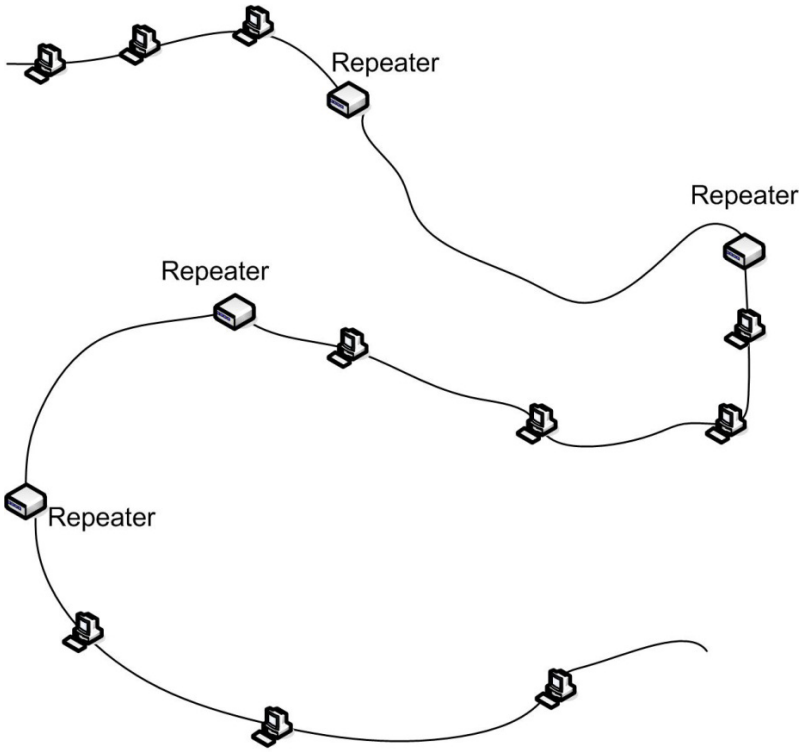


Рис. 2-3: Ретрансляторы (5-4-3)

На сегодня Вы ещё можете увидеть ретрансляторы в современных сетях, но это довольно таки редкое явление. Так как оптико-волоконный кабель является невосприимчивым к электромагнитному излучению, в отличии от медного кабеля, то сигнал на входе ретранслятора имеет лучшие показатели. Исходя из этого, один из вариантов использования повторителей в локальной сети является расширение кабельных сегментов для волоконно-оптических сетей.

Сетевой концентратор

Сетевой концентратор - устройство, работающее на первом уровне модели OSI. Концентратор представляет собой центральную точку для подключения кабелей сетевых устройств (Рис. 2.4). Он выполняет функцию объединения устройств вместе на электронном уровне, что дает им равный доступ к сети. Кроме того, сигнал не только регенерируется, как в случае со стандартным аналоговым ретранслятором, но и усиливается. С точки зрения передачи и возможных коллизий, концентратор работает так же, как устройства, использующие коаксиальный кабель.

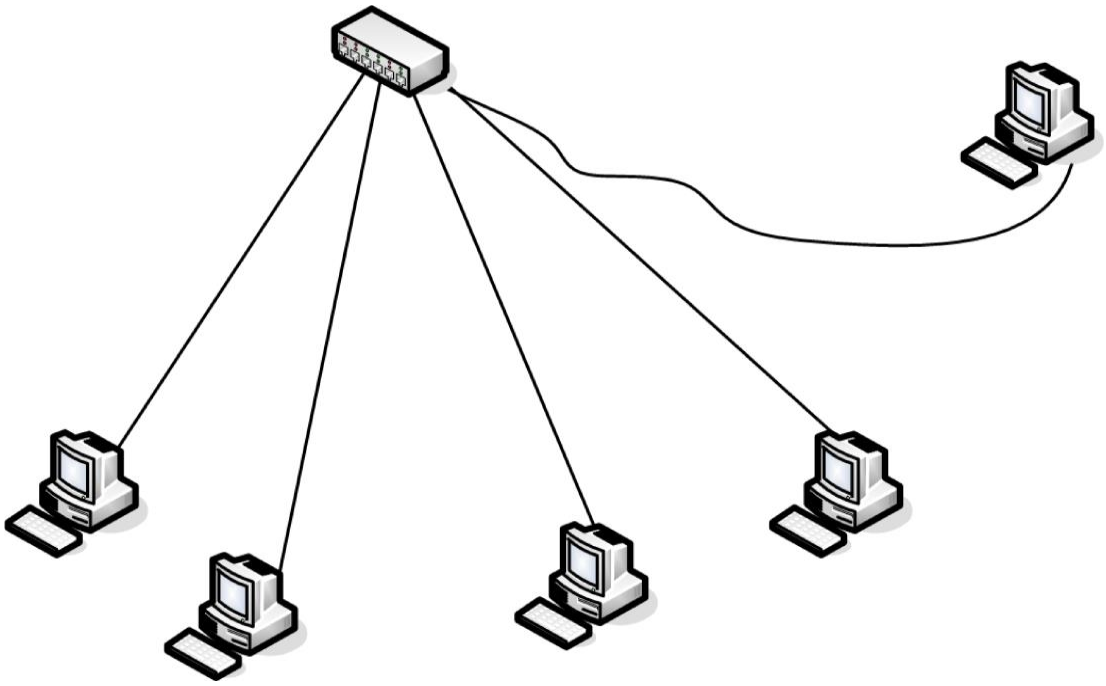


Рис. 2.4 – Концентратор

Термин, который мы должны объяснить в надлежащем контексте это - порт. Вы узнали в предыдущей главе, что порт может быть использован вместе с IP-адресом, чтобы определить конечную точку для передачи. При обсуждении концентраторов и коммутаторов, порт необходим для реализации физической связи сетевых устройств.

Порт - обычно используется для обозначения точки подключения (как правило соединения RJ45) сетевых устройств Ethernet к концентратору или коммутатору.

Большинство концентраторов имеют в своём составе порт для каскадного соединения связи, что позволяет расширить свою сеть путем подключения к другим сетевым устройствам (Рис. 2.5).

Порт для каскадного соединения обеспечивает, и поддерживает связь с другими сетями соединительных устройств.

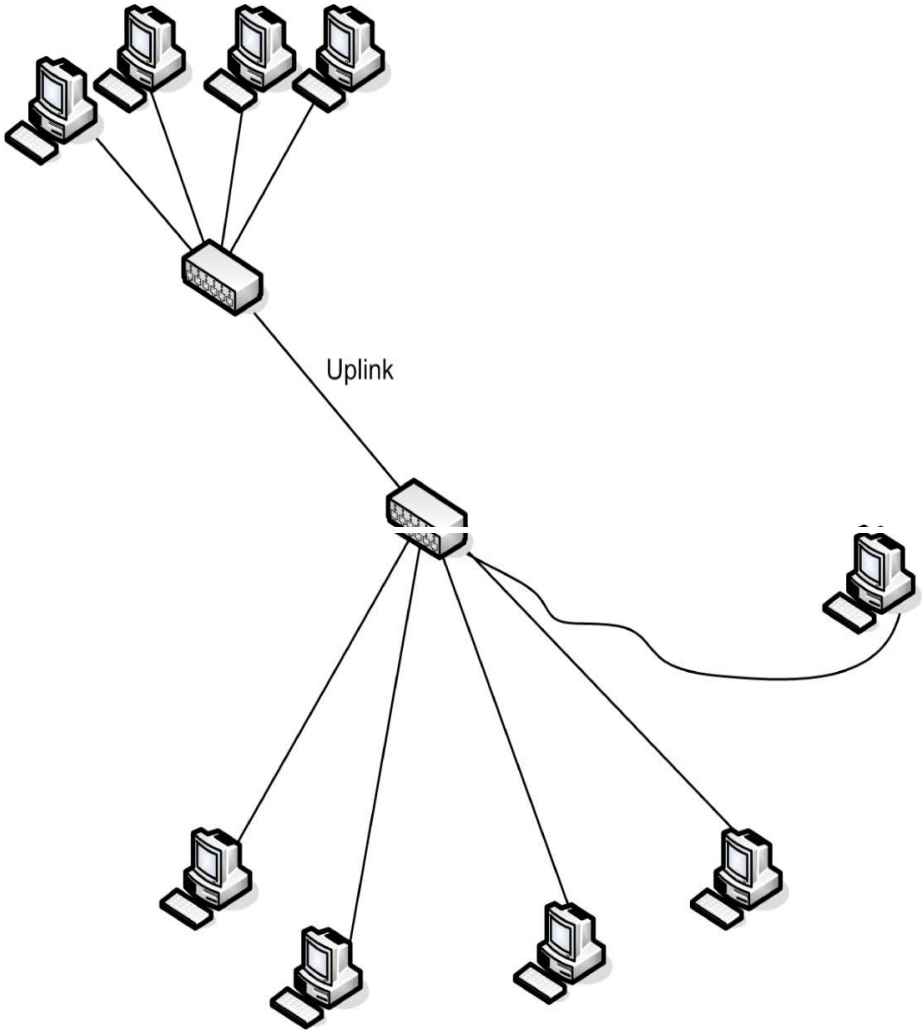


Рис. 2.5 - Хабы соединены восходящей линией порта.

Иногда вы можете увидеть традиционные центры, именуемые неуправляемыми узлами. В таком центре отсутствует возможность, какого либо изменения параметров узла.

На сегодняшний день Вы редко увидите концентратор в его классическом определении. Большинство современных концентраторов имеют ряд дополнительных функций. Например, концентратор обнаруживает скорость, с которой работает сетевой адаптер и компенсирует её, чтобы позволить компьютерам связываться друг с другом, даже когда компьютеры используют различные скорости передачи. Некоторые концентраторы также поддерживает функции удаленного управления, такие, как возможность отключения порта. Например, вы могли бы применить это в случае если на компьютер, подключенный к нему, не удается отправить безыскажённые данные. При отключении порта, можно изолировать компьютер так, чтобы он не мешал работе сети. Часто, это может быть сделано удаленно, и при этом нет необходимости физически отключать компьютер.

Уточним, что сетевой коммутатор это другое устройство, хотя оба находятся на 2 уровне модели OSI. Функционал мостов обычно входит в сетевые коммутаторы.

Мост

Мост работает на втором уровне эталонной модели взаимодействия открытых систем. Традиционно, его цель состоит в том, чтобы соединить различные виды медиа в единую логическую сеть. Одним из вариантов использования может выступать необходимость объединения сегментов сети, работающих с разными типами кабеля (коаксиальный и витая пара) в одной подсети с общим сетевым адресом.

Подсеть - область сети, имеющей уникальный сетевой адрес. Все узлы в подсети будет иметь тот же сетевой адрес.

Мост принимает кадры от одного подключенного сегмента и определяет, передавать ли повторно кадр на другие подключенные сегменты. Мостовые фильтры направляют на основе MAC-адреса назначения.

Рассмотрим ситуацию, в которой компьютер сегмента A передает кадр и пункт назначения к другому компьютеру в том же сегменте. Мост получает кадр, но, так как адресат находится на том же сегменте, а не в сегменте B, то выполняется его уничтожение, а не передача на сегмент B (Рис. 2.6). Тем не менее, если мост видит, что MAC-адрес назначения находится в сегменте B, или, если он не признаёт назначения, он пересылает кадр в сегмент B.

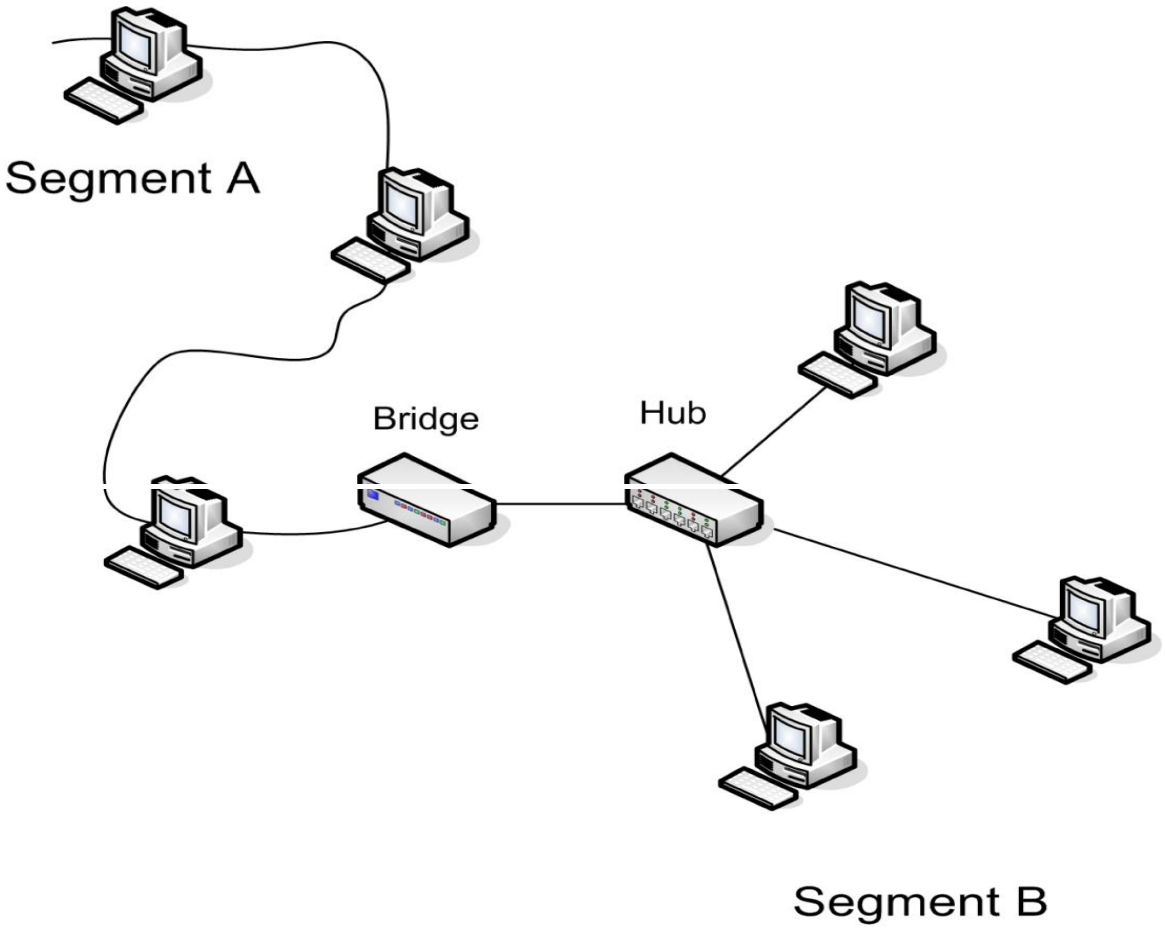


Рис. 2.6 - Сегменты моста

В процессе мост создает домены коллизий, поскольку кадры восстановлены, а не только проходят через мост. На рисунке 2-6, данные компьютеров на отрезке А могут войти в коллизию с данными других компьютеров того же сегмента, или со моста, но не с данными сегмента В.

Мост также выполняет функции ретранслятора между сегментами, потому что исходящий кадр повторно передаётся, а сигнал - просто регенерируется.

Мосты помогают управлять сетевым трафиком, но не во всех ситуациях. Широковещательный трафик не фильтруется Мостами. К сожалению, иногда устройства неверно названы производителями. В течение многих лет, устройства, которые на самом деле являлись мостами, были названы концентраторами (Рис. 2.7).

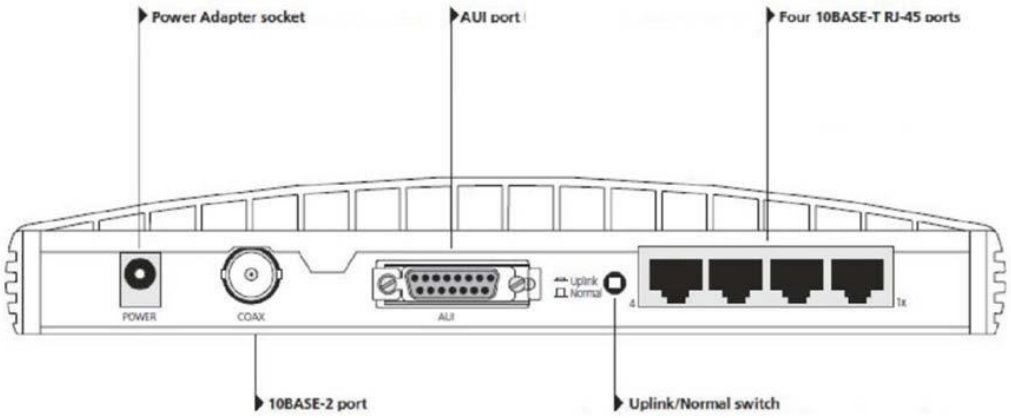


Рис. 2.7 – Мост

Устройство на Рис. 2.7 является мостом, в классическом понимании, он позволяет подключать 10base2, 10base5 (через порт AUI) и 10Base-T сегменты сети.

Коммутатор

Коммутатор быстро стал популярным в современной сети. Большинство современных коммутаторов поддерживают функциональность на 2 и 3 уровнях модели OSI, что означает, что в других устройствах зачастую нет необходимости, особенно в сетях малого и среднего бизнеса.

На первый взгляд, многие небольшие коммутаторы выглядят как шлюзы. Однако внутри они существенно отличаются друг от друга. Вместо того чтобы просто связывать порты вместе в электронном виде, коммутатор действует как мультипортовый мост. Это реализуется с помощью буфера трафика между портами, используя технологию, известную как «store and forward» (сохранить и передать), что исключает столкновения. Коммутатор поддерживает таблицу, которая отслеживает MAC-адреса. Он определяет адрес назначения и перенаправляет трафик туда на основе MAC-адреса. Она также

позволяет настроить виртуальные локальные сети для управления сетевым трафиком и безопасностью.

Маршрутизаторы третьего уровня модели OSI - устройства, которые работают на сетевом уровне. Маршрутизаторы и коммутаторы третьего уровня требуются, если вы хотите разделить сеть на подсети. Маршрутизаторы устанавливают границы между подсетями и несут ответственность за обеспечение того, чтобы пакеты нашли свой правильный путь к нужным подсетям для доставки. Маршрутизаторы и маршрутизация подробно рассматриваются в главе 6. Большинство коммутаторов 2 и 3 уровня - устройства которые включают в себя возможности маршрутизации.

Коммутатор третьего уровня модели OSI может быть настроен для передачи трафика из одной подсети в другую. Коммутатор, который включает в себя возможности третьего уровня, иногда называют «routing switch» (коммутатор маршрутизации).

Большие коммутаторы, как правило, являют собой модульные устройства (Рис. 2.8), которые позволяют настроить коммутатор для ваших нужд на основе установленных модулей. Вы можете начать с малого - одного или двух модулей, а также расширить коммутатор по мере роста сети.

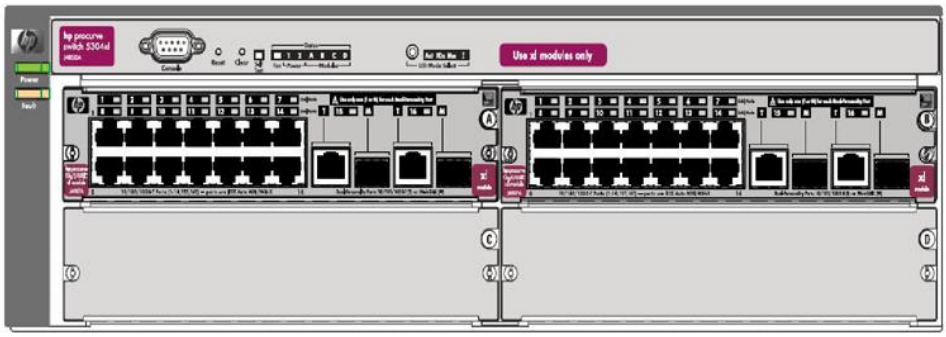


Рис. 2.8 - Коммутатор

Брандмауэр

Межсетевые экраны рассматриваются в главе 3, но вы можете перенести его сюда для пояснения возможностей маршрутизатора.

Большинство коммутаторов предназначены для поддержки удаленного управления. Это означает, что вы можете удаленно управлять конфигурациями, а также обновить программное обеспечение коммутатора, произвести резервное копирование информации, управление деятельностью портов и так далее. Многие коммутаторы также обеспечивают высокий уровень безопасной связи путем шифрования связи с подключенными устройствами.

Маршрутизатор

В простейшем виде, направляющая сеть построена из двух или более адресуемых сетей 3 уровня, соединенных между собой маршрутизаторами (Рис. 2.9). Каждый маршрутизатор имеет, по крайней мере, два порта (также называемые интерфейсами), каждый из которых имеет свой сетевой адрес. Маршрутизаторы, предназначенные для использования по ссылкам WAN, как правило,

поддерживают дополнительные функции, такие как способность действовать в качестве межсетевого экрана или VPN конечной точки.

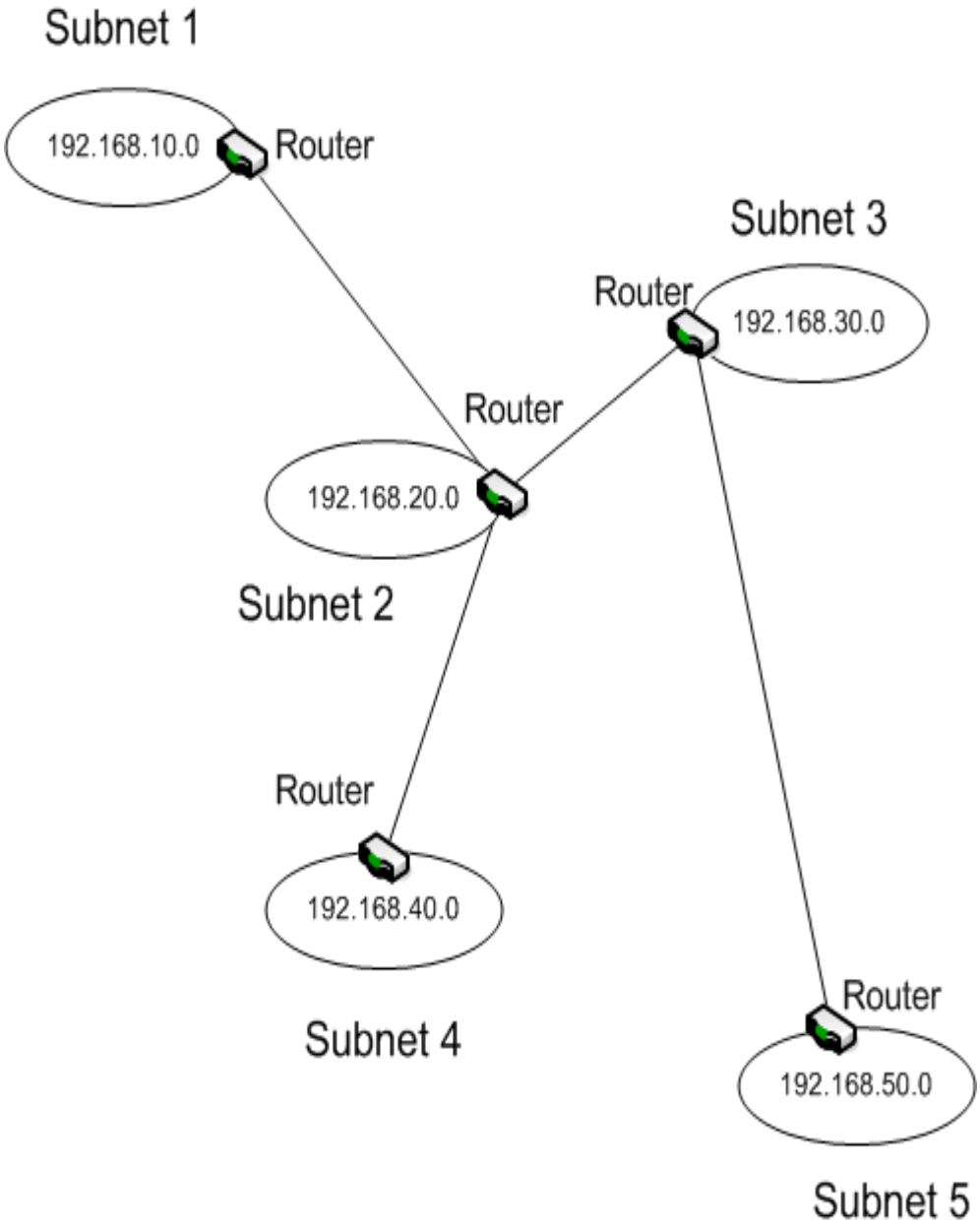


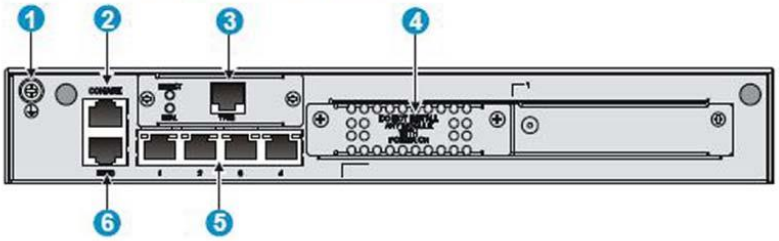
Рис. 2.9 - Топология сети

В примере, показанном на Рис. 2.9, маршрутизатор в подсети 3 имеет три доступных порта, что позволяет подключить к IPv4 подсети 2, 3 и 5. Маршрутизатору в подсети 2 потребуется четыре порта для подсетей 1, 2, 3 и 4.

Когда пакет приходит на маршрутизатор, он определяет адрес назначения и пересылает пакет через соответствующий порт в сети назначения для доставки. В зависимости от типа маршрутизатора, его действия могут отличаться. Они зависят от информации в пакете, такой как адрес источника или данных, содержащихся в пакете.

(1) Power switch	(2) Power receptacle	(3) USB port
(4) Reset button		

Figure 10 A-MSR20-12-T rear panel



(1) Grounding screw	(2) Console/AUX port	(3) T1 port TPRI0
(4) SIC/DSIC slot	(5) Ethernet LAN ports (ETH1 to ETH4)	(6) Ethernet WAN port ETH0

Рис. 2.10 – Маршрутизатор

Маршрутизатор, который изображён на Рис. 2.10, имеет пять портов Ethernet. Четыре из них доступны как порты LAN (обозначены номером 5 на рис 2-10). Каждый порт определяет разные подсети в локальной сети. Пятый порт - WAN-порт поддерживает широкие связи зоны (маркированные как номер 6 на рисунке 2-10). Обратите внимание, что консольный порт на этом маршрутизаторе (помеченный как № 2 на Рис. 2.10) является разъем RJ45, вместо последовательного порта.

Из-за того, что маршрутизатор включает в себя функции устройств более низкого уровня, например, такого как мост, а также устанавливает границу для доменов коллизий в сети. Информация от устройств в одной подсети не может столкнуться с информацией других подсетей. Кроме того, маршрутизатор обрабатывает каждый пакет, чтобы определить наилучший путь доставки, так что повышает уровень сигнала ретрансляции каждого пакета.

Маршрутизатор также устанавливает границу для широковещательных доменов. Маршрутизаторы не распространяют широковещательный трафик, за исключением передачи DHCP/BOOTP. Большинство маршрутизаторов не проводят эти трансляции по умолчанию, но Вы имеете возможность включить эту функцию, работая с некоторыми маршрутизаторами. Как правило, маршрутизатор настроен в режим "модуля поддержки IP-адреса", которая позволяет маршрутизатору изменить трансляцию на одноадресную для пересылки DHCP-сервера. Потому что DHCP-сервер получает адрес DHCP-клиента, как часть запроса, он отвечает маршрутизатору однонаправленной передачей пакета, а маршрутизатор пересылает DHCP ответ клиенту.

DHCP/Bootp

Специальные трансляции, используемые с автоматическим присвоением IP-адресов (DHCP) и удаленной загрузки для устройств, которые не имеют загрузочные файлы на локальном диске (BOOTP).Многие коммутаторы спроектированы таким образом, что они могут также быть сконфигурированы для работы в качестве маршрутизаторов.

Другие распространенные устройства

Существуют и другие сетевые устройства, не упомянутые здесь. Нередко сеть будет иметь один или несколько серверов, которые предоставляют особые услуги сети. Иногда вы будете встречать устройства, разработанные специально, чтобы позволить внутренним компьютерам безопасно общаться с внешним миром.

Другие распространенные устройства - другие устройства будут рассмотрены более подробно ниже в данном курсе.

Ещё одно устройство, которое действительно заслуживает особого внимания - беспроводная точка доступа «AP» (Access Point), иногда упоминается как WAP. Как уже упоминалось в предыдущей главе, точка доступа выступает в качестве центральной точки соединения для беспроводных устройств. Она также выступает в качестве шлюза, соединяющего беспроводные устройства с проводной сетью (Рис. 2.11).

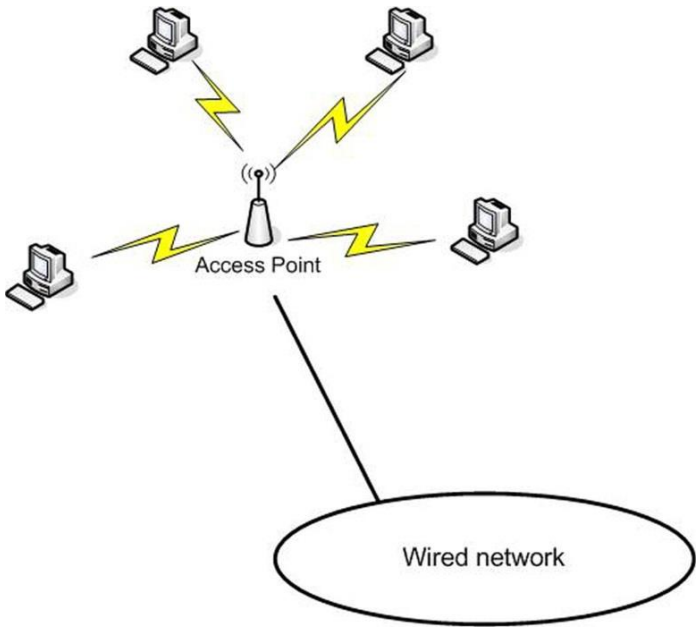


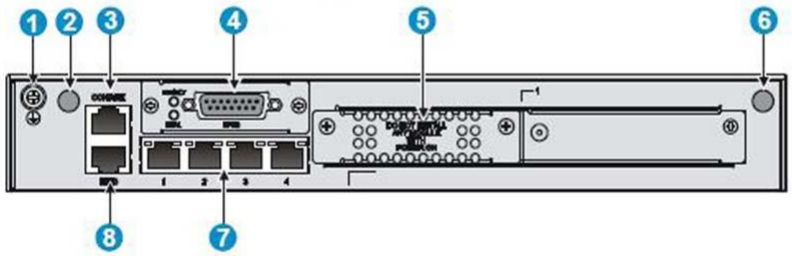
Рис. 2.11 - Точка доступа

В большинстве сетей, аутентификация, связь и безопасность для беспроводных клиентов осуществляется через точки доступа. Как и в других соединительных устройствах, большинство точек доступа поддерживают удаленное управление, часто через веб-интерфейс. В крупной беспроводной сети вы, вероятно, найдете точки доступа, управляемые через центральный беспроводной контроллер, что делает ненужным (в большинстве случаев) индивидуальную настройку и управление точкой доступа.

Возможно, одно устройство, которое создало наибольшую революцию, как для домашнего использования, так и в малом бизнесе, сети является беспроводной маршрутизатор (Рис. 2.12). Беспроводной маршрутизатор сочетает в себе шлюз, маршрутизатор, коммутатор и функциональность беспроводной точки доступа наряду с автоматическим присвоением IP-адреса, беспроводной безопасности, и, в некоторых случаях, даже других функций. Помните, что беспроводной маршрутизатор не проводит маршрутизацию беспроводных сигналов. Он пересылает трафик с помощью беспроводной сети 802.11 Wi-Fi к адресатам, которые, как правило, пользуются интернетом.

(1) Power switch	(2) Power receptacle	(3) USB port
(4) Reset button		

Figure 8 A-MSR20-12-W rear panel



(1) Grounding screw	(2) Antenna port	(3) Console/AUX port
(4) E1 port EPRI0	(5) SIC/DSIC slot	(6) Antenna port
(7) Ethernet LAN ports (ETH1 to ETH4)	(8) Ethernet WAN port ETH0	

Рис. 2.12 - Беспроводной маршрутизатор

Обратите внимание, что конфигурация беспроводного маршрутизатора очень похожа на конфигурацию проводного маршрутизатора, о котором было рассказано выше, с теми же проводными сетевыми портами и портом WAN. Основное отличие заключается в том, что этот маршрутизатор также включает в себя встроенный радиомодем, а также имеет внешний порт антенны.

Одна из причин популярности беспроводных маршрутизаторов является то, что они дают простой способ подключения к высокоскоростному интернету (Рис. 2.13).

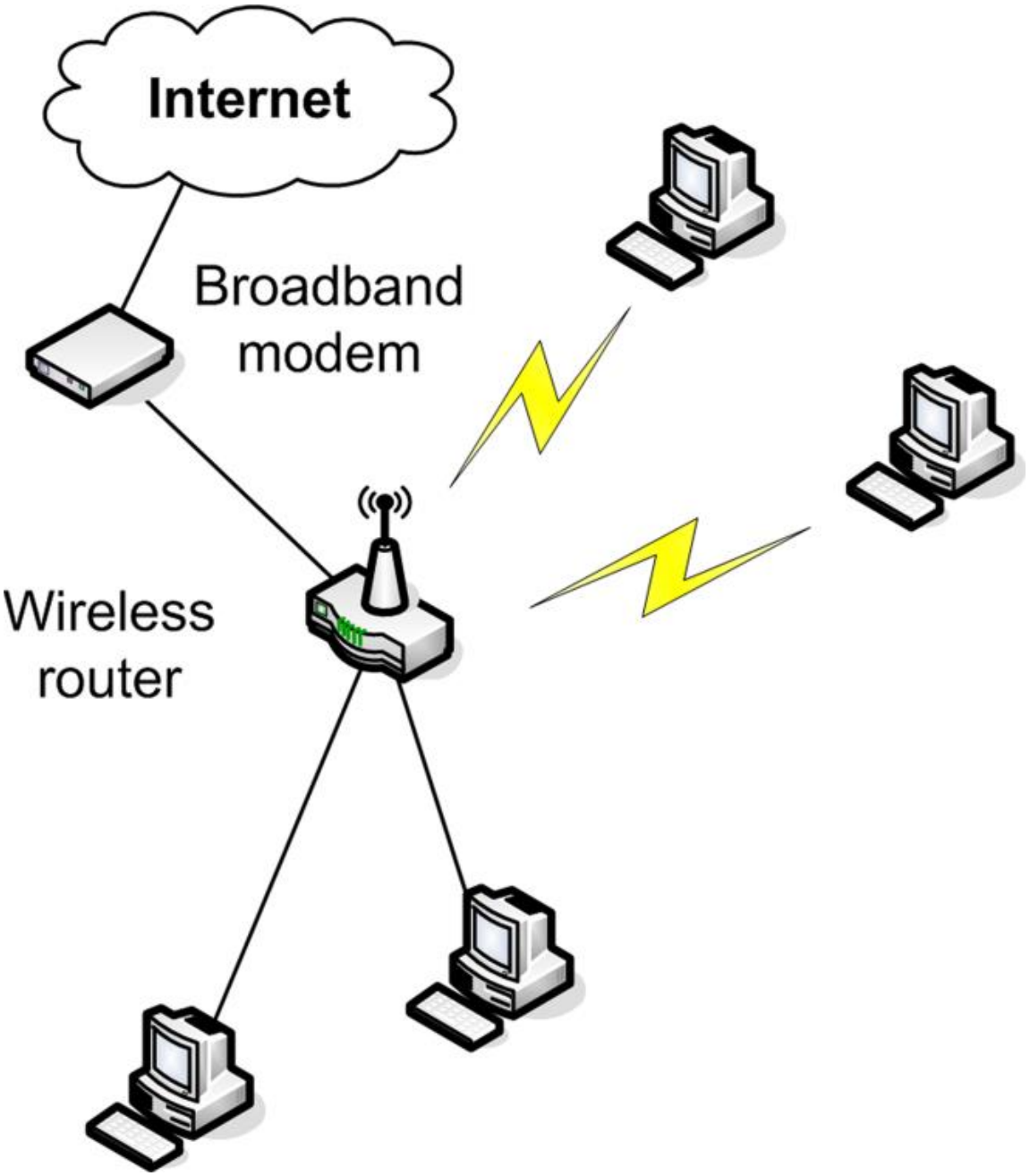


Рис. 2.13 - Использование беспроводного маршрутизатора

В одной общей конфигурации, высокоскоростное устройство, как правило, DSL или кабельный модем, подключается к порту по восходящей линии связи беспроводного маршрутизатора к общему доступу с помощью проводных клиентов портов и беспроводных клиентов. Беспроводной маршрутизатор также предназначен для определения IP-адреса подключенных клиентов и управляет преобразованием адресов для доступа в интернет. Сетевые устройства, как правило, предназначены для поддержки небольшого количества подключенных компьютеров. Для дома или малого бизнеса, вы, возможно, увидите DSL модем с возможностью беспроводного использования.

Модем - *сокращение от модулятор / демодулятор. Это устройство, которое преобразовывает цифрой сигнал в аналоговый.*

Цифровая абонентская линия (DSL) - *технология, которая обеспечивает связь цифровых данных по стандартным телефонным линиям.*

Кабельный модем *- устройство, которое обеспечивает доступ в Интернет через коаксиальные линий кабельного телевидения.*

Сценарий: GoShop, Inc.

GoShop, Inc разрабатывает свою новую сеть. Сеть будет стартовать менее чем с 20 компьютеров, но, как ожидается, вырастет с течением времени. Сеть будет развёрнута в районе, который может поддерживать проводное или беспроводное подключение, но кабель ещё не был проложен. Клиентские компьютеры будут рабо тать на ОС Windows или Linux. Все будут получать TCP / IP адреса IPv4 автоматически. Целью компании является, исключить возможность получать какой-либо доступ к сети. Рассмотрите сетевые параметры и соединительные устройства которые вы будите использовать.

Основы коммутатора

Сейчас подробней рассмотрим коммутатор, и разберемся в особенностях управления коммутатором. Сейчас мы рассмотрим коммутатор не вдаваясь в подробности, позже, в этом курсе, мы рассмотрим его более детально. *Управление коммутатором раскрыто более подробно в главе 4 и последующих главах.*

Ориентация коммутатора

Прежде чем мы рассмотрим управление коммутатором, мы должны изучить само устройство. Физически, большинство коммутаторов очень похожи функционалом, но они могут различаться количеством портов. Некоторые коммутаторы, особенно менее дорогие, имеют фиксированные конфигурации (Рис. 2.14).

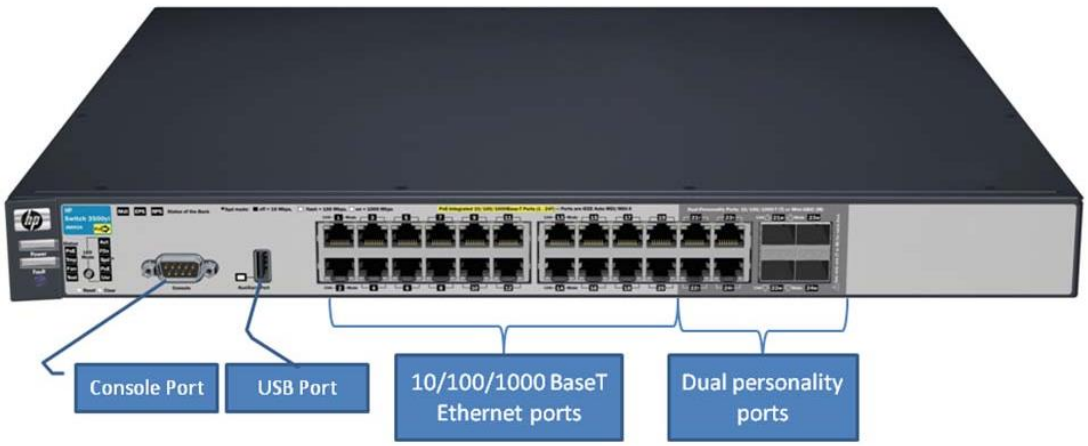


Рис. 2.14 - HP E3500-24G-PoE yl

Консоль порт последовательного порта, может быть использован для управления коммутатором. Коммутатор также имеет порт USB, который может использоваться для загрузки нового программного обеспечения или резервного копирования конфигурации коммутатора. Эта конфигурация коммутатора дает Вам 20 портов 10/100/1000 Base-T и 8 портов HP двойного назначения, которые поддерживают мини-GBIC или 10/100/1000 Base-T, давая вам возможность выбора типа кабеля (проводной или оптический). Shared порт – порт двойного

назначения. Если трансивер вставлен - коллективный 10/100/1000 Base-T RJ-45 порт отключается.

Питание через Ethernet (PoE)

Wired Ethernet network technology - сетевая технология, что позволяет устройствам получить электрический ток, который позволяет им работать через кабель для передачи данных, без отдельного силового кабеля.

Преобразователь интерфейса Gigabit (GBIC)

Приемопередатчик (трансивер) - устройство, которое сочетает в себе функциональность передатчика и приемника в одном устройстве.

Приемопередатчик - преобразует электрический сигнал в оптический и оптический в электрический.

Четыре порта на правой стороне коммутатора на Рис. 2.14 являются восходящей линией портов. Они позволяют вам расширить свою конфигурацию подключения коммутатора к другим коммутаторам или другим устройствам, таким как маршрутизатор. Higher-end switches, как правило, имеет модульную конструкцию (Рис. 2.15). Вы можете изменить функциональность коммутатора путем изменения модулей установленных в нём.

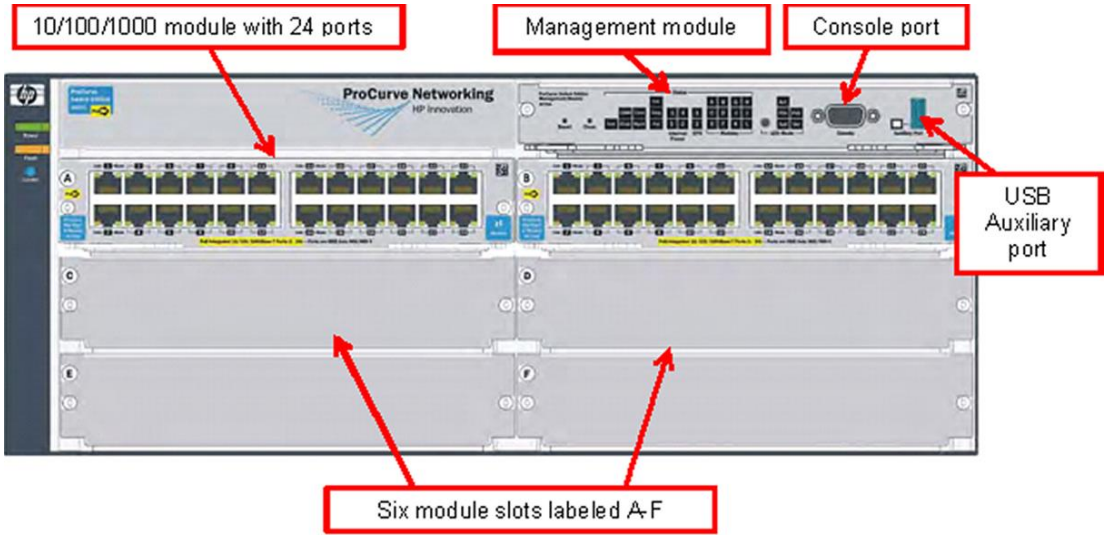


Рис. 2.15 - HP 5406zl-48G

Управления модулем осуществляется через консоль или USB порт. Также имеется индикатор светодиодов, которые предоставляют информацию о коммутаторе и статусе установленных модулей. Эта модель коммутатора обеспечивают установку до шести модулей.

Образец на Рис. 2.15 имеет только два установленных модуля. Вы можете установить дополнительные модули портов, в случае необходимости (Рис. 2.16). Вы можете выбрать модуль для установки имеющегося восходящего порта, для дальнейшего расширения. Во многих коммутаторах, модули обладают возможностью горячей замены.

Горячая замена *- относится к компонентам устройств и модулей, которые могут быть изменены без выключения устройства. Любой из модулей может быть заменён, в то время, как остальные будут продолжать работу.*

Стандартный модуль имеет 24 порта с нечетными номерами портов в верхней строке и четными номерами портов в нижней строке (Рис. 2.16).

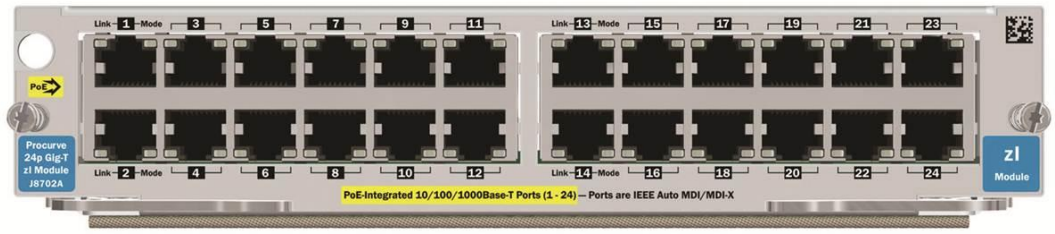


Рис. 2.16 - Модуль с 24 портами

Порты в модуле называются идентификатором слота (обычно буква) и номер порта. Если вы установили этот модуль в слот A, порт на левом верхнем углу этого модуля будет порт A1, и порт на правой нижней части будет A24.

Варианты управления коммутатором

Коммутаторы HP обладают тремя вариантами интерфейса управления:

Интерфейс командной строки (CLI);
Меню;
Веб-интерфейс.

CLI является самым мощным, но это также самый сложный в использовании тип управления. Интерфейс меню проще в использовании, потому что вы выберите команды из меню, а не вводите их. Тем не менее, интерфейс меню ограничивает команды управления, к которым у вас есть доступ, что делает его менее мощным. Веб-интерфейс наименее мощный, но зато самый простой в использовании. Веб-интерфейс дает вам простой способ проверить состояние коммутатора из любой точки сети.

CLI (Интерфейс командной строки)

Доступ к CLI осуществляется при подключении к порту консоли, с ПК под управлением эмулятора терминала или с помощью VT-100 терминала (Рис. 2.17). Очевидным недостатком является то, что вы должны находится в непосредственной близости к коммутатору, а также иметь в наличии 9-контактный последовательный кабель. Самым большим преимуществом является то, что Вы можете подключиться к коммутатору и открыть командную строку, даже если это не может быть достигнуто через сеть.

Например, Вам придется использовать консольное подключение, если коммутатор не имеет действующий IP-адрес.

Эмулятор терминала *- программа, которая позволяет ПК эмулировать функциональность последовательный терминалов.*

VT-100 *- общие положения последовательного терминала.*

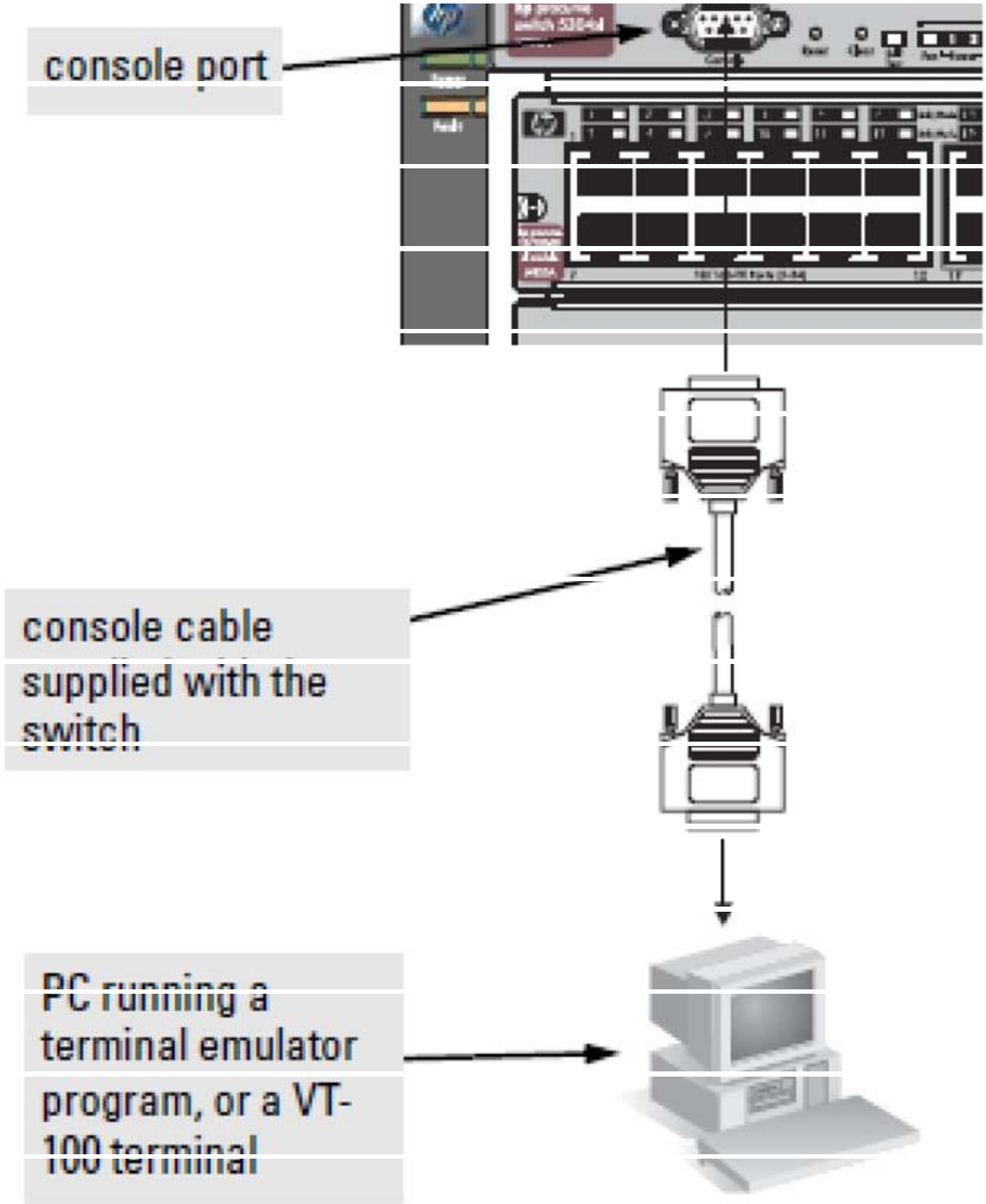


Рис. 2.17 - Подключение консоли

Другим вариантом является запуск Telnet сессии и подключения к коммутатору. Для того, чтобы сделать это, выполните команду Telnet и укажите имя переключателя или IP-адрес (Рис. 2.18). Telnet по умолчанию, использует хорошо известный порт приложений 23 для общения, но может быть указан альтернативный порт.

Убедитесь, что студенты поняли, что порт 23 - порт TCP / IP связи, а не физический порт на коммутаторе.

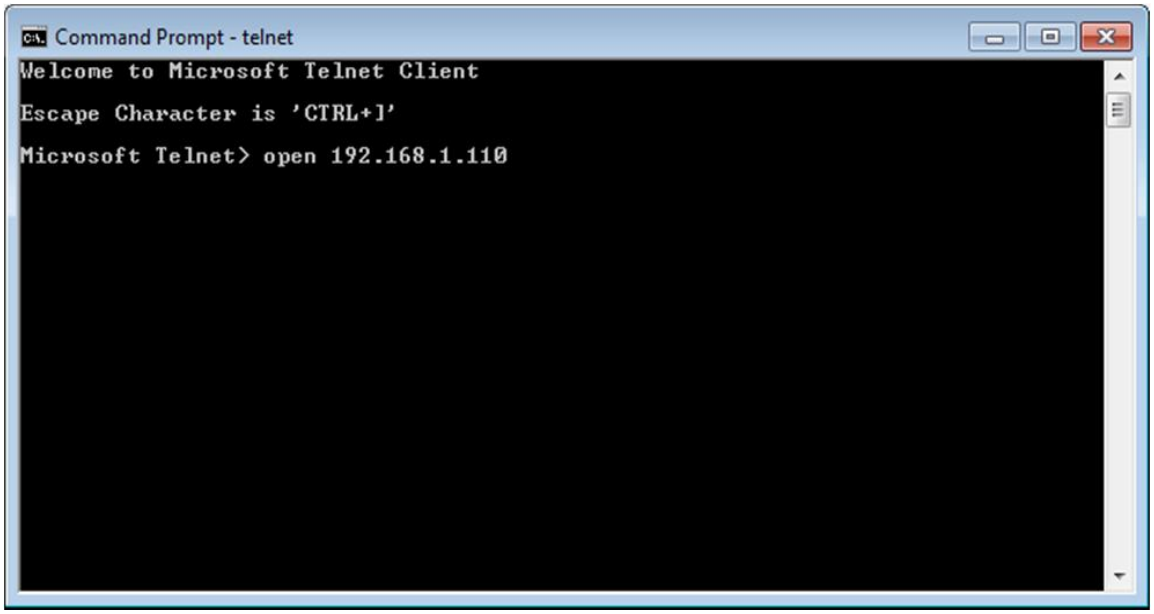


Рис. 2.18 - Подключение к коммутатору по Telnet

Telnet *- применение слоя TCP / IP-утилиты / протокол, который позволяет выполнять команды на удаленном устройстве.*

Использование Telnet для подключения к коммутатору по сети действительно несет неотъемлемый риск безопасности. Все данные, передаваемые во время сессии Telnet, передается в открытом виде. Одной из целей получения доступа злоумышленниками может быть перехват управленческой деятельности.

При подключении, коммутатор отображает авторские права и сообщает свои характеристики (Рис. 2.19). Скриншот экрана, показанный на Рис. 2.19, был сделан из коммутатора HP - 24G 3500yl. Вы можете увидеть другие версии этих заявлений. Нажмите любую клавишу для продолжения в командной строке CLI.

Рис. 2.19 - Начальное подключение

Укажите, что оператор может просматривать, но не изменять параметры конфигурации. По умолчанию в строке указано, что коммутатор устарел.

Менеджер и режим оператора

По умолчанию CLI проводит быструю перекличку номеров модели коммутатора (Рис. 2.20). Вы изначально подключаете уровень менеджера, который позволяет вам выполнять все команды, поддерживаемые CLI.

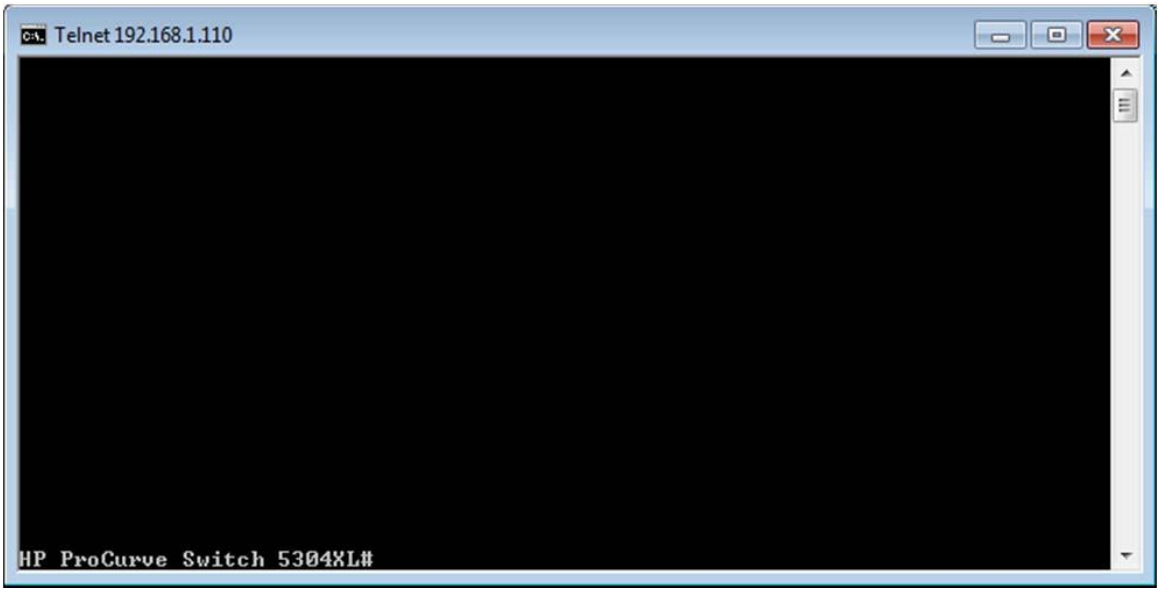


Рис. 2.20 - Менеджер командной строки

В этом случае менеджер сообщает:

```
HP ProCurve Switch 5304#
```

Чтобы выполнить команду, введите её в командную строку и нажмите клавишу Enter. Если ввести «выход» в командной строке и нажать клавишу Enter, то это направит Вас в строку оператора. Изменения командной строки для:

```
HP ProCurve Switch 5304>
```

Запустите команду, что позволит вернуться к уровню менеджера.

Пусть студенты знают, что CLI документация включена в руководствах продукта, а также присутствует в Интернете на веб-сайте HP. Рис. 2.21 показывает конфигурацию роботы устарелого модульного коммутатора.

Просмотр активной конфигурации

Для просмотра информации о конфигурации выполните следующую команду:

```
show running-config
```

Результат выполнения команды показывает активные сведения о конфигурации, в том числе типа модуля, VLAN, и информацию порта (Рис. 2.21).

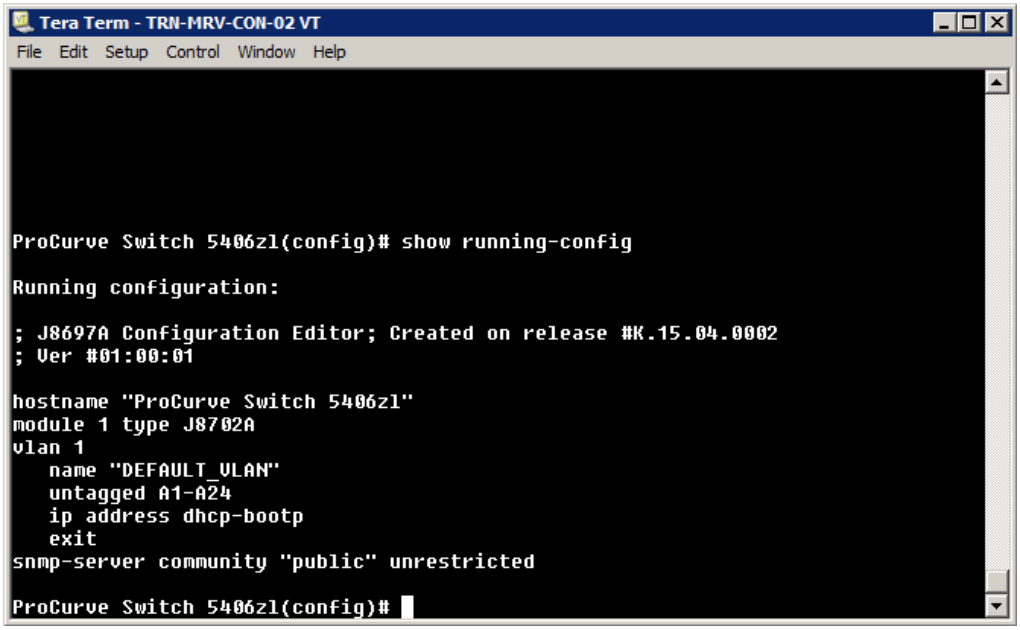


Рис. 2.21 - Активные конфигурации

При запуске этой команды ещё рас модульный коммутатор перечислит все установленные модули и их тип (Рис. 2.22).

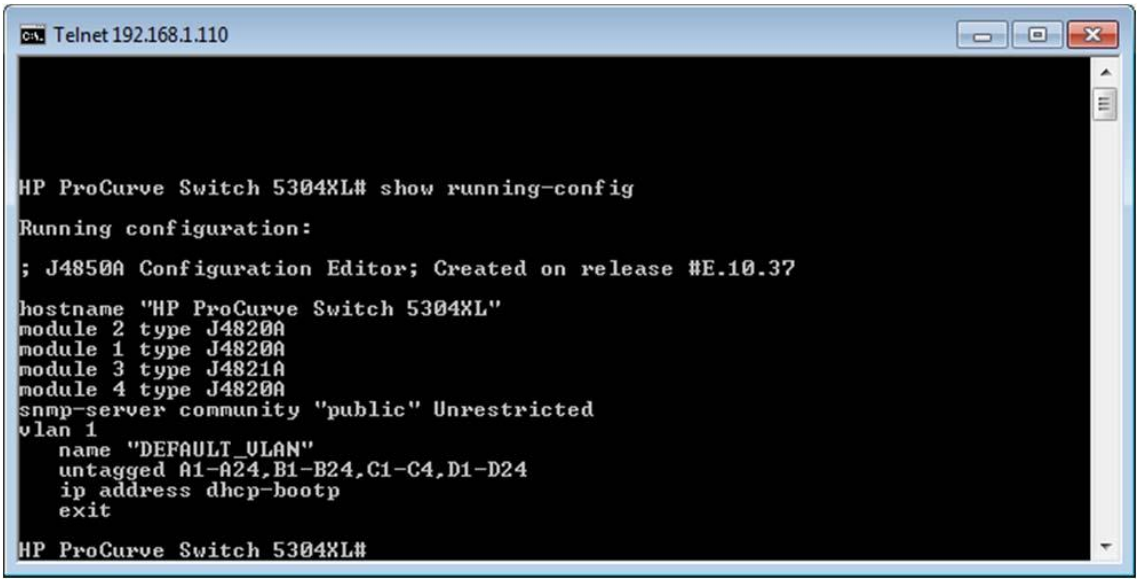


Рис. 2.22 - Модульный коммутатор

CLI имеет большое количество поддерживаемых команд, многие из которых имеют свой набор функций.

Команды не чувствительны к регистру. Самыми главными командами являются «show running-config» и «ShOw RUNNING-config».

Получение справки

Одним из первых вещей, которые вы должны сделать, это просмотреть список доступных команд. Для этого введите или нажмите клавишу Tab в командной строке (Рис. 2.23).

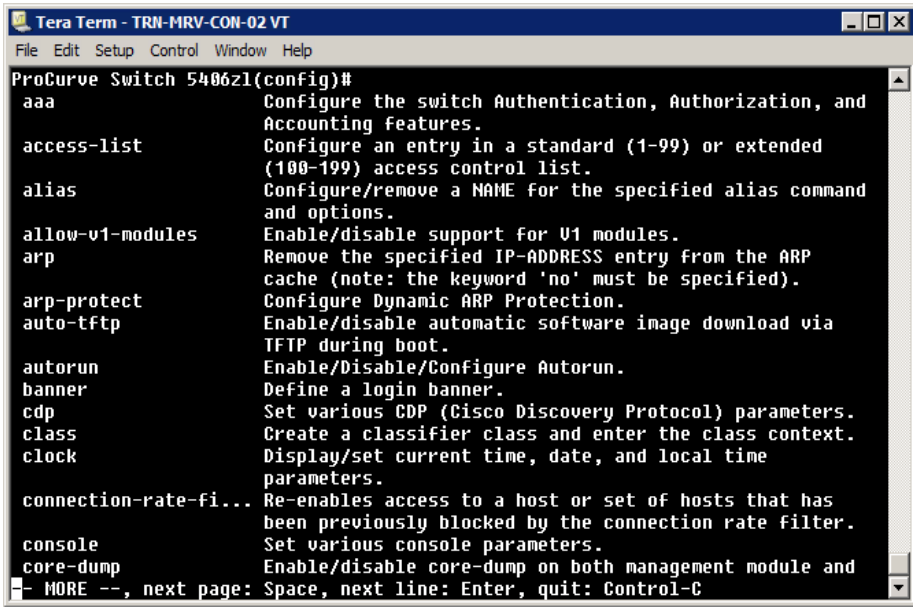


Рис. 2.23 - Диспетчерские команды

Список доступных команд ограничен во время работы в режиме оператора (Рис. 2.24).

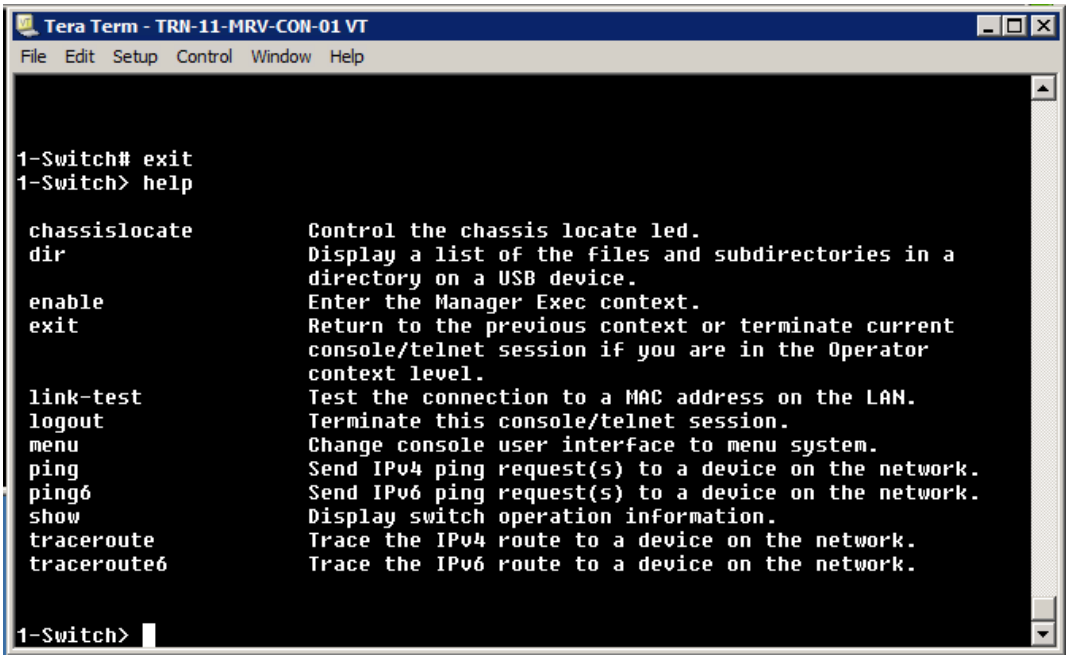


Рис. 2.24 - Список команд оператора

Некоторые команды поддерживают подкоманды. Одним из примеров этого является команды шоу, которое вы видели раньше. Для получения списка поддерживаемых команд, шоу типа в командной строке, а затем введите или нажмите клавишу Tab (Рис. 2.25).

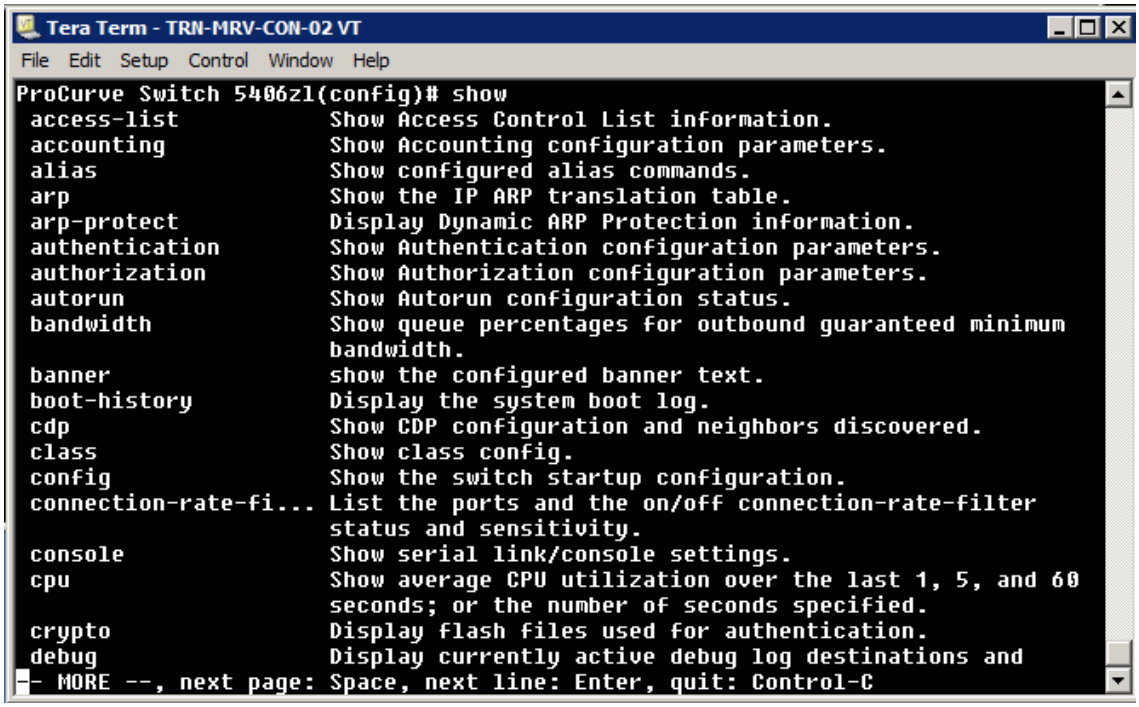


Рис. 2.25 – Команды

Чтобы узнать больше о любой из этих команд, типа шоу, имя команды, помощь, а затем нажмите клавишу Enter. Например:

```
show arp help
```

Это действие отображает описание команды и каких-либо дополнительных опций, если они поддерживаются (Рис. 2.26).

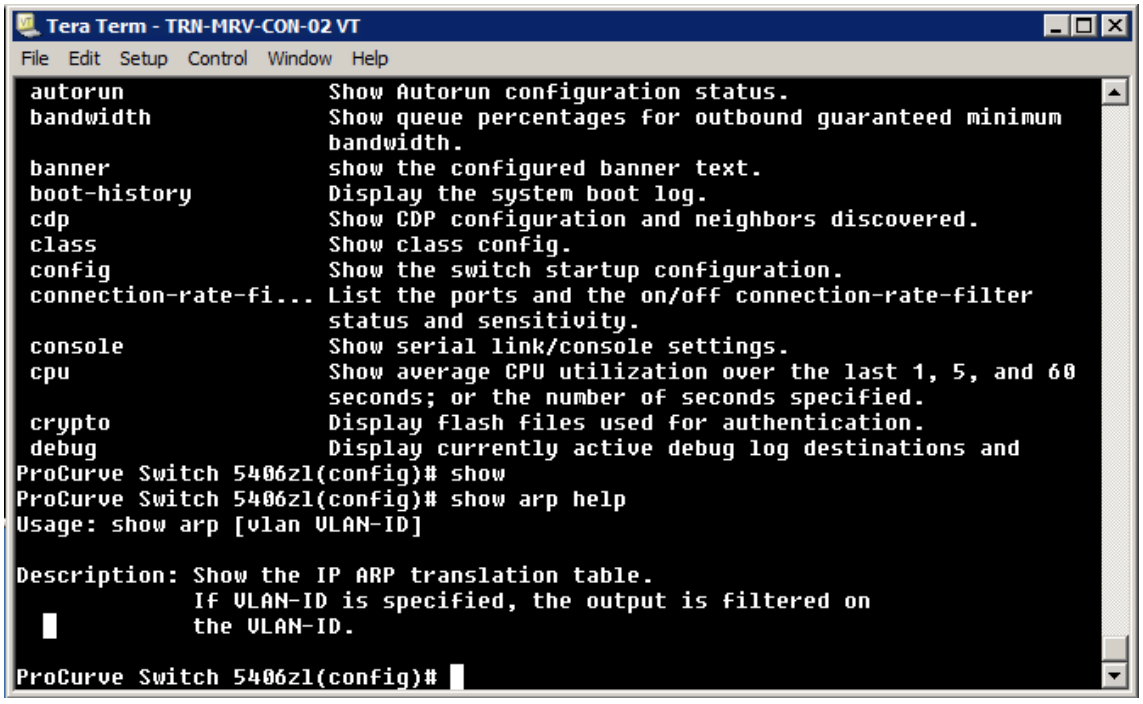


Рис. 2.26 - Показать команду помощи

Для большинства других команд, вы можете просто ввести имя команды с последующей подсказкой, или <Tab> и нажмите клавишу Enter для получения дополнительной информации о команде и командных опций. Например, если вы хотите узнать больше о команде TraceRoute которую вы видели ранее, вы должны ввести:

```
traceroute help
```

Эта команда возвращает список опций команд с описаниями (Рис. 2.27).

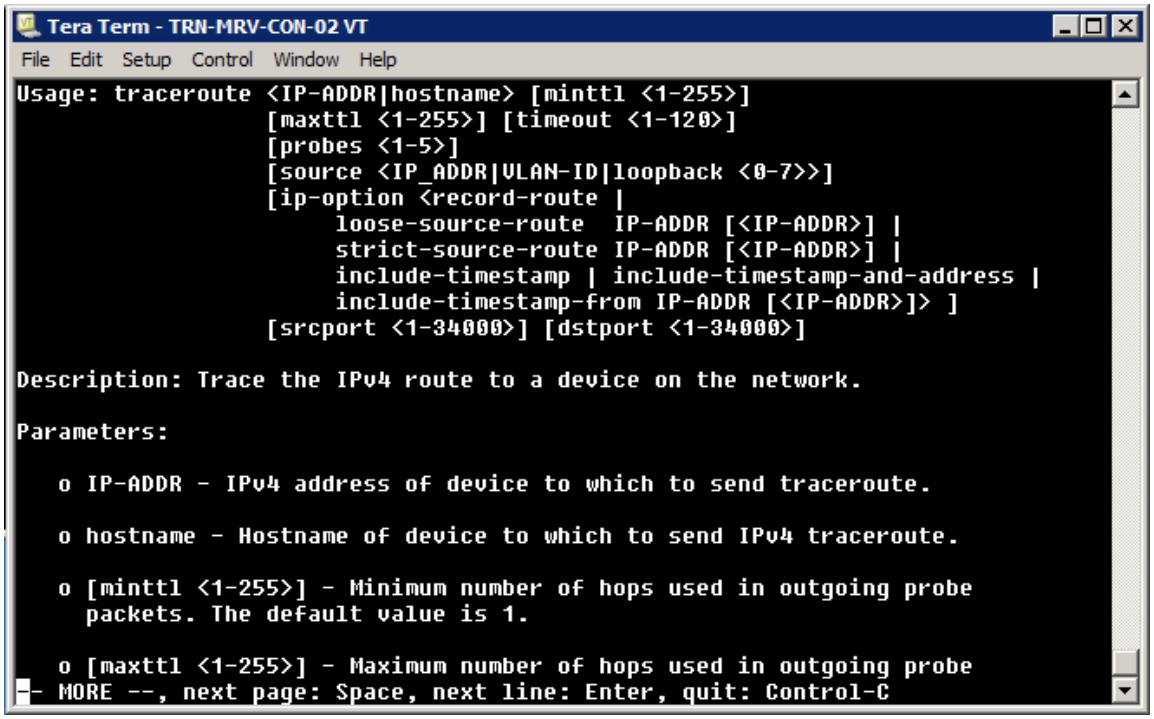


Рис. 2.27 - Трассировка, команда помощи

Команды контекста

Некоторые команды изменяют контекст командной строки. Например, если вы запустите команду (config), стремительные изменения включают в себя (конфигурации), и вы можете выполнять команды конфигурации (Рис. 2.28).

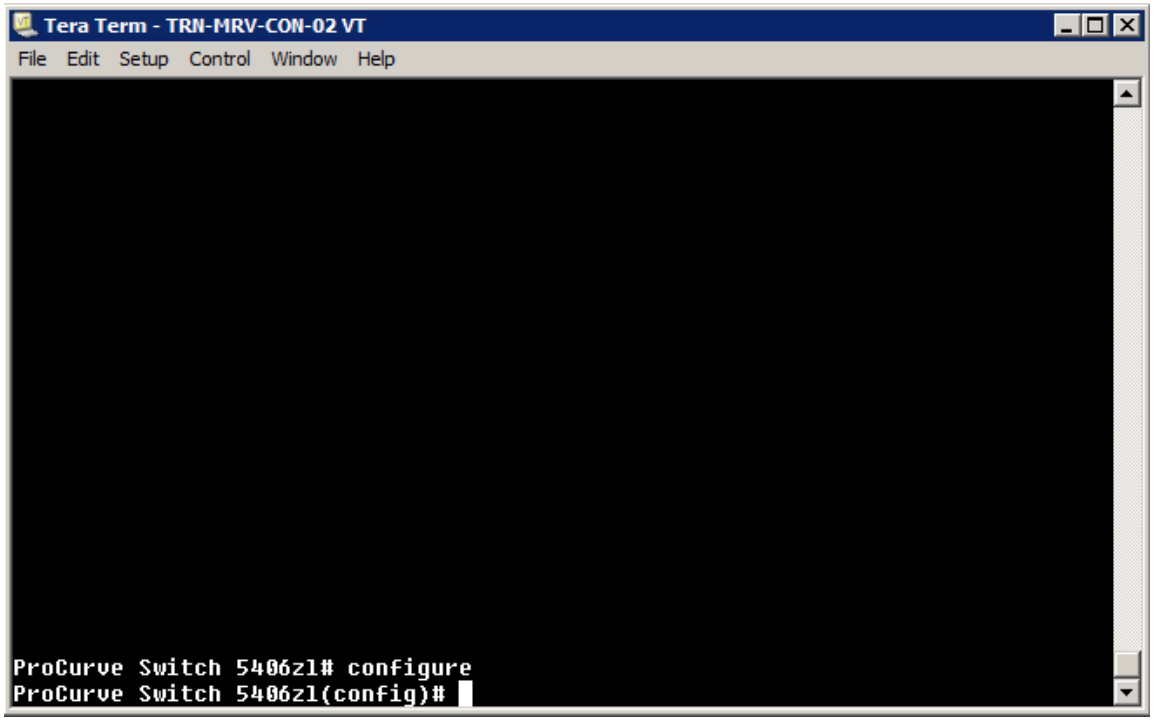


Рис. 2.28 - Конфигурация Контекста

Теперь, при вводе, вы получите список команд конфигурации (Рис. 2.29).

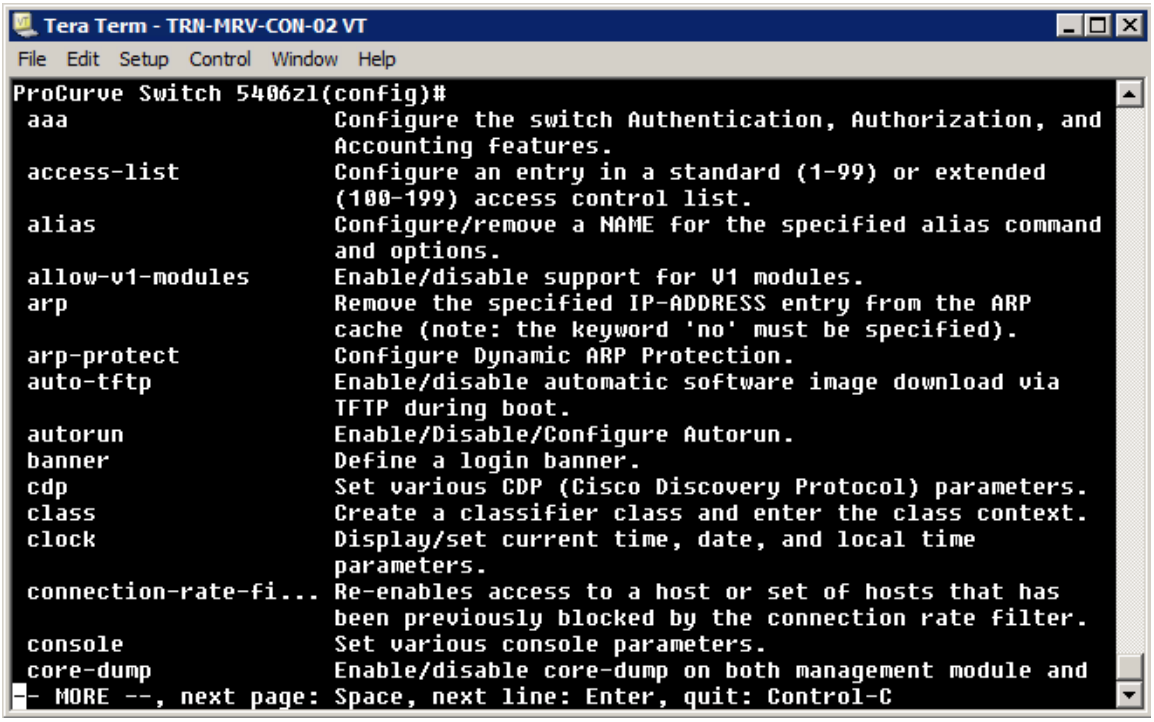


Рис. 2.29 - Команды конфигурации

Наберите Exit в (config) командной строки, чтобы выйти из контекста конфигурации.

Интерфейс меню

Прежде чем вы сможете запустить интерфейс меню, необходимо подключить к коммутатору и открыть CLI (Рис. 2.30), необходимо запустить команду «Menu» в командной строке.

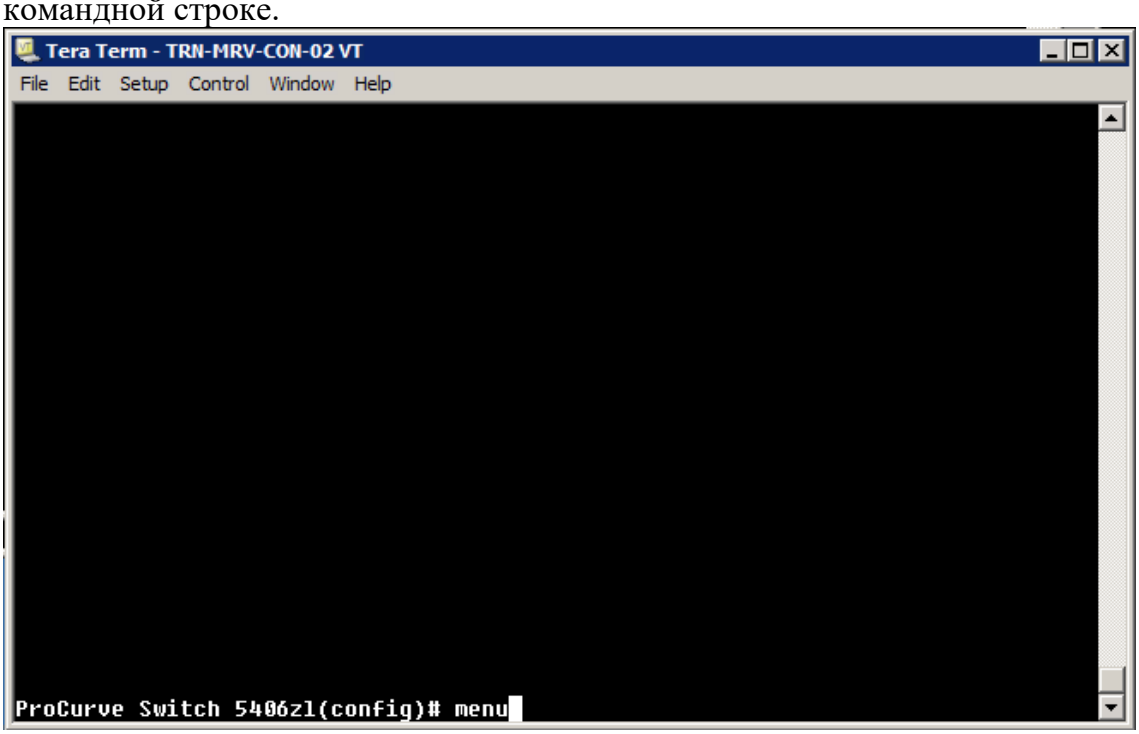


Рис. 2.30 - Команда «Menu»

Это открывает главное меню по умолчанию (Рис. 2.31).

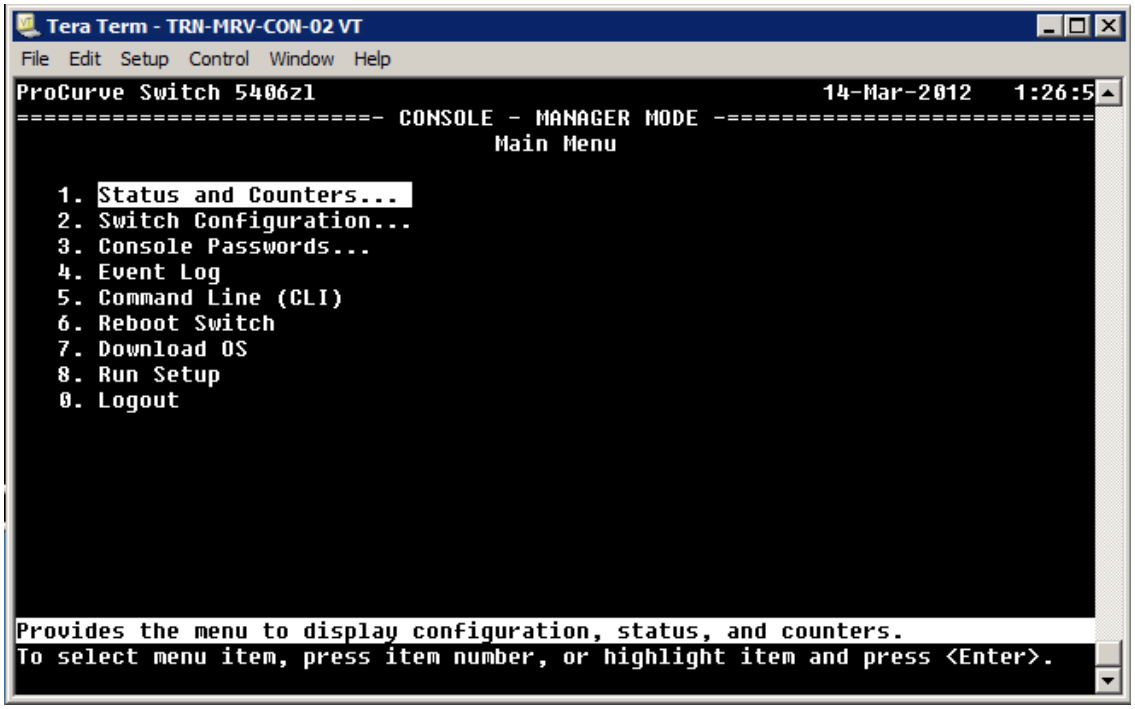


Рис. 2.31 - Главное меню

Нажмите номер пункта или используйте клавиши со стрелками, чтобы выбрать пункт меню, затем нажмите клавишу Enter. Например, «Status and Counters» направит вас к «Status and Counters Menu» (Рис. 2.32).

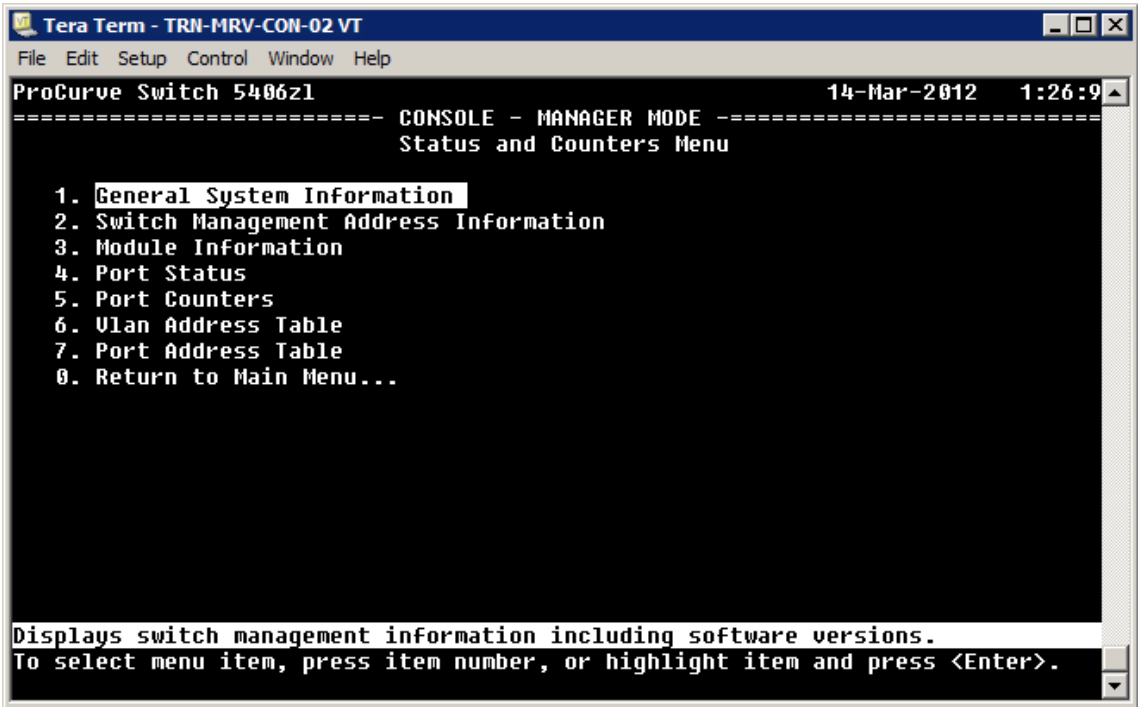


Рис. 2.32 - Status and Counters Menu

В каждом из подменю, выбор номера 0, Вас возвращает к меню более высокого уровня. Отсюда вы можете просматривать общую информацию о системе (выбор 1). Введите «1» или нажмите клавишу «Enter», чтобы вывести общую информацию на экран (Рис. 2.33).

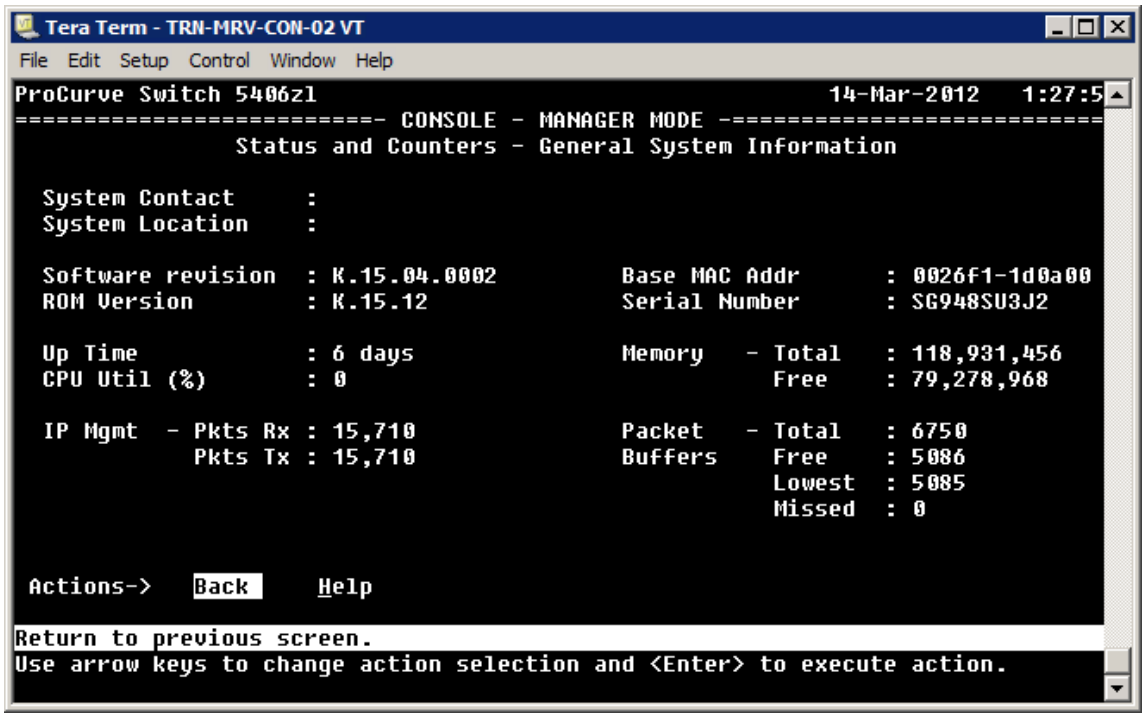


Рис. 2.33 - Общая Информация о системе

Для того чтобы увидеть информацию о конфигурации системы, выберите пункт «2». Переключение конфигураций (Switch Configuration), на «1». Сведения о системе (System Information). Эта команда выведет на монитор сводку о системе (Рис. 2.34).

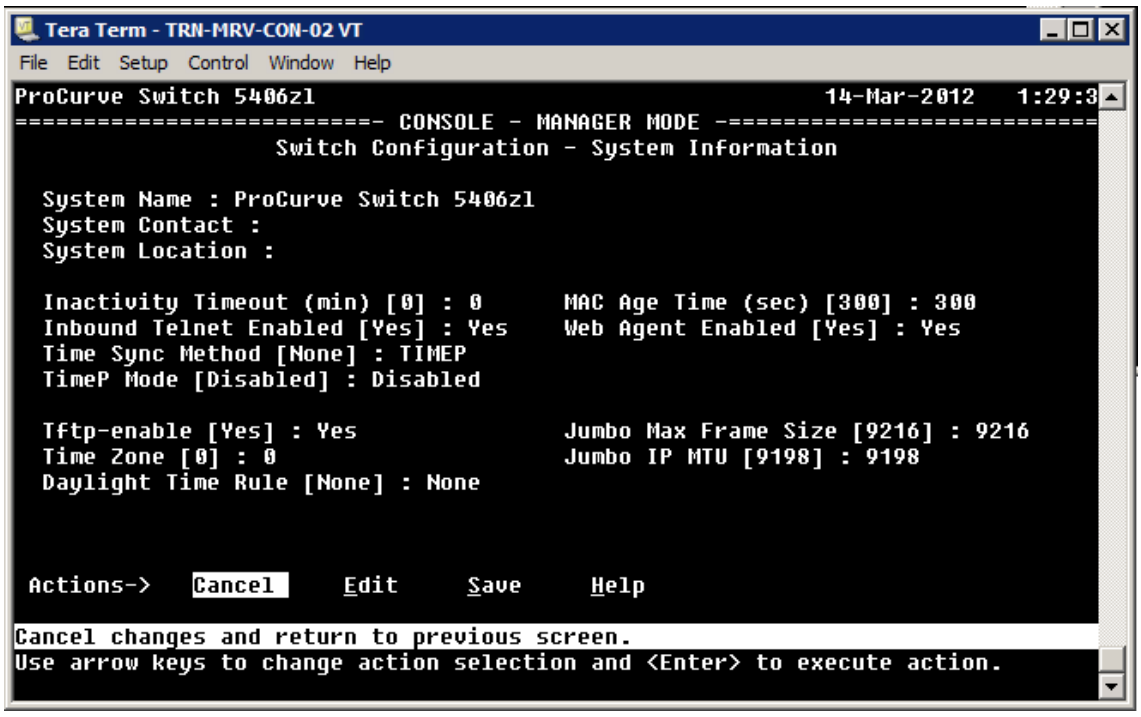


Рис. 2.34 - Коммутатор, Сводка конфигурации (Switch Configuration Summary)

Напомните студентам, что для Telnet и Веб-интерфейса управлением соединением клиент / хост должены быть в той же подсети, что и коммутатор или маршрутизарот должны быть подключены к коммутатору.

Запуск интерфейса меню с оператором CLI строке, подразумевает более ограниченный выбор меню (Рис. 2.35).

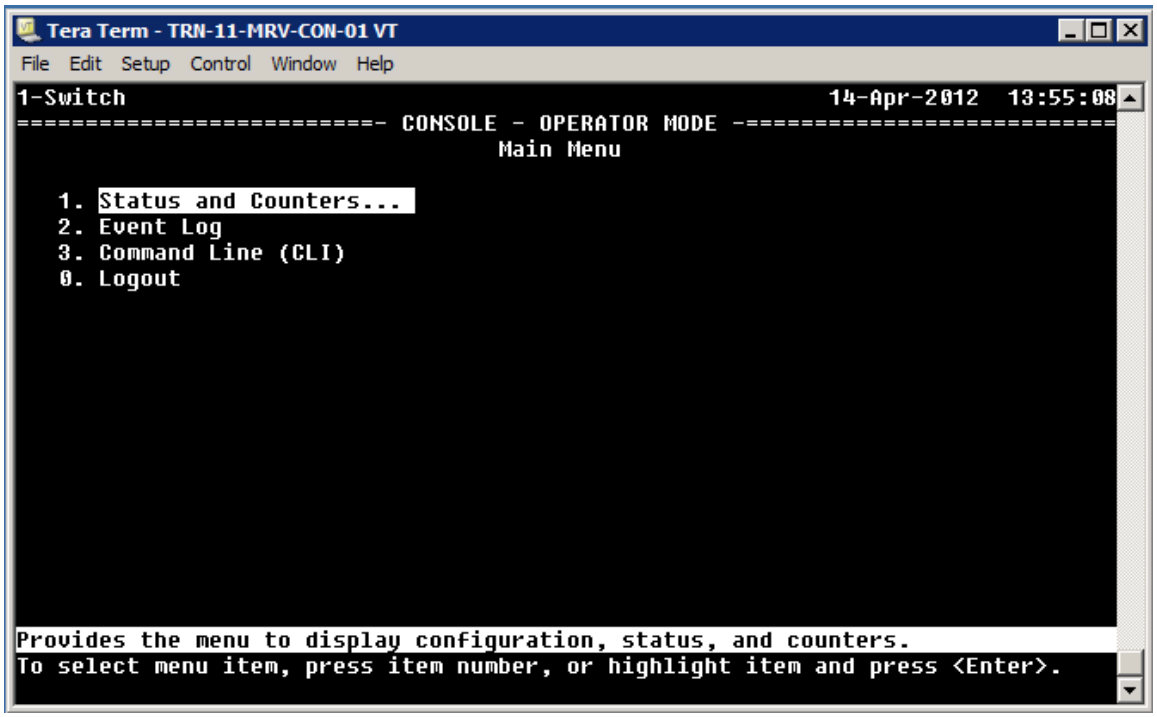


Рис. 2.35 - Оператор Меню (Manu)

У вас есть доступ к подменю «Status and Counters», можно просмотреть содержимое журнала событий, вернуться к CLI или выйти из вашеей Telnet сессии.

Веб-интерфейс

Для запуска веб-интерфейса, введите IP-адрес коммутатора в URL строку браузера. Ваш браузер будет подключаться к коммутатору и отобразит полний URL для веб-интерфейса коммутатора, как показано на рисунке Рис. 2.36.

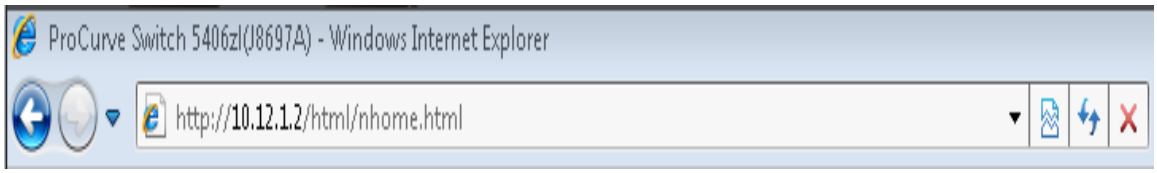


Рис. 2.36 - Подключение к веб-интерфейсу

Веб-интерфейс открывает страницу Состояние (Status) и отображает информацию о состоянии коммутатора (Рис. 2.37). Точное появление страници состояния зависит от модели коммутатора и уровня программного обеспечения. На Рис. 2.37, отображается общая информация о коммутаторе и состоянии порта.

В этом примере ограничивается количиство страниц интерфейса, чтобы дать вам общее представление о том, что вы можете сделать через веб-интерфейс.

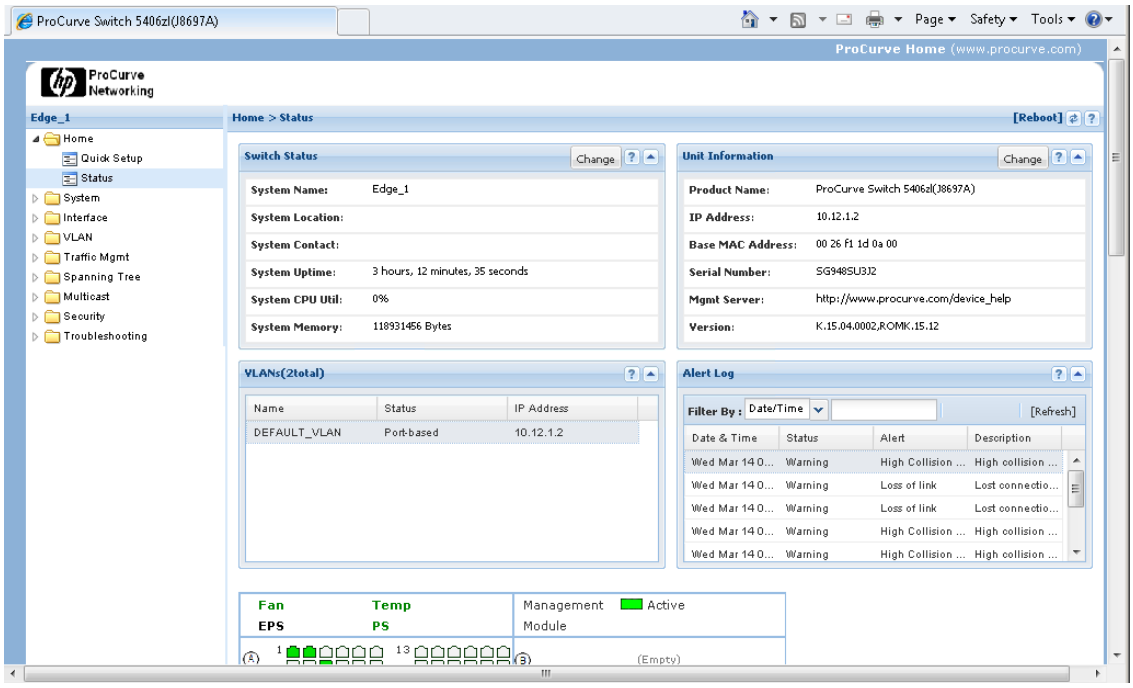


Рис. 2.37 - Страница состояния (Status Page)

Болие детельно про SNMP Вы узнаете в главе 10.

Выберите «Quick Setup», чтобы открыть основные параметры настройки коммутатора (Рис. 2.38).

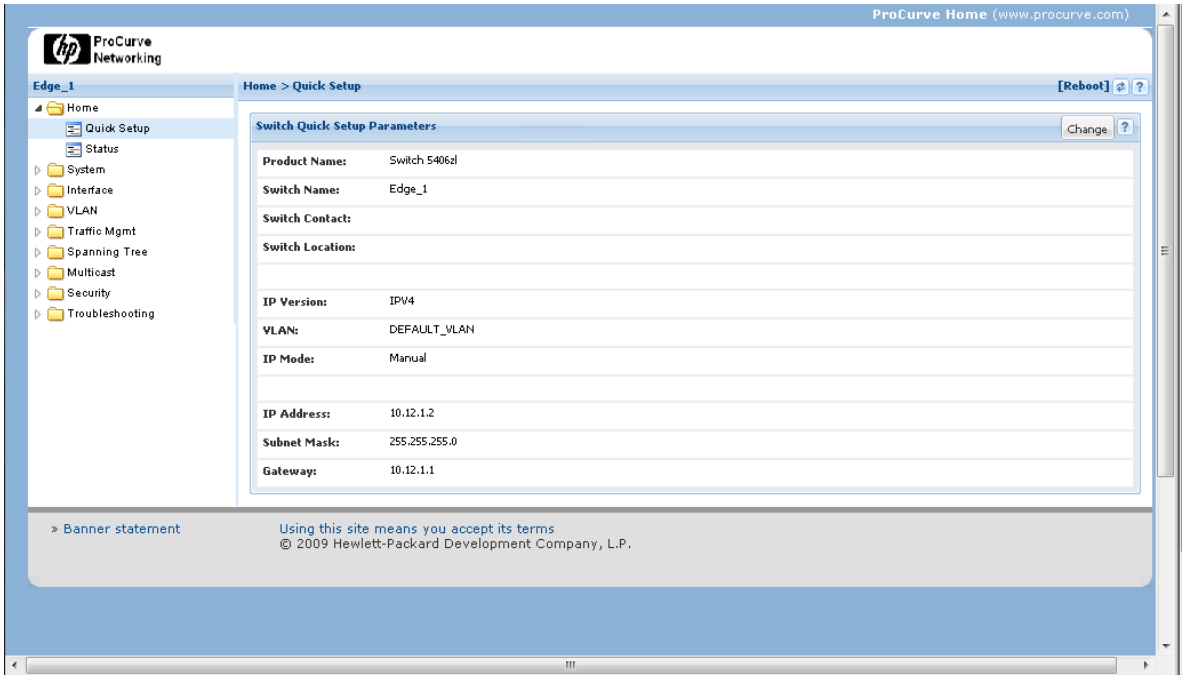


Рис. 2.38 - Быстрая настройка (Quick Setup)

Системные параметры

Разверните папку «System», чтобы получить доступ к «Logging, SNMP» та выберите «Updates/Downloads» экраны. «Logging» отображает журнал коммутатора (Рис. 2.39).

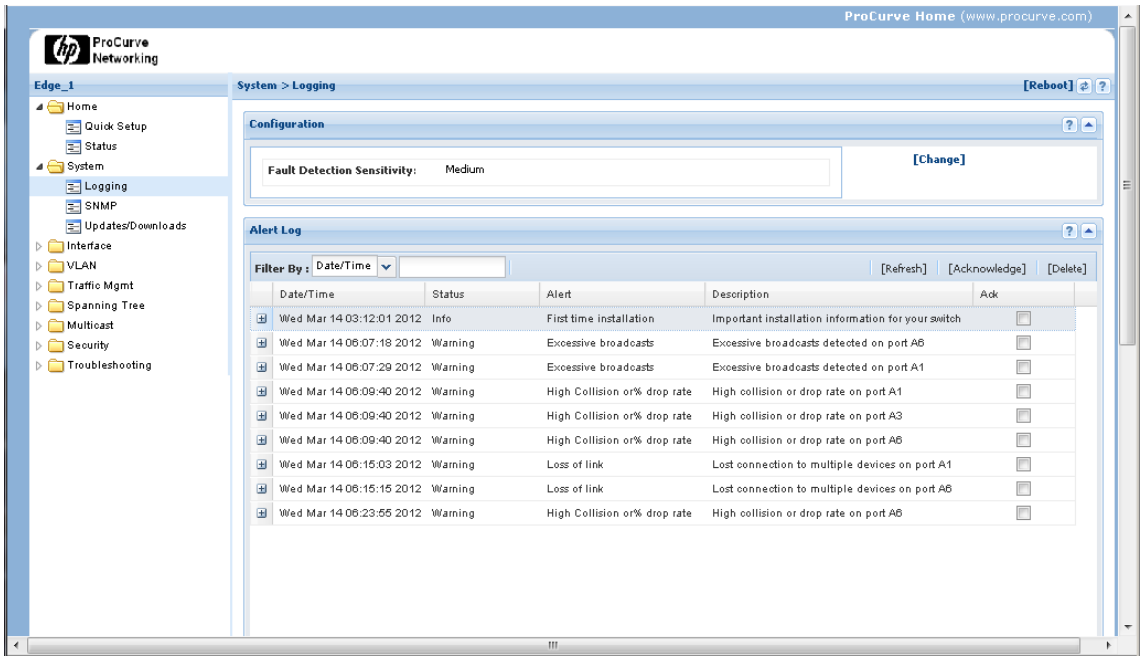


Рис. 2.39 - Вход на страницу (Logging Page)

Откройте страницу «Updates/Downloads» для просмотра и управления образами программного обеспечения и конфигурационных файлов (Рис. 2.40), которые хранятся во флэш-памяти коммутатора. Максимальное количество образов программного обеспечения составляет 2 еденицы, в то время, как количество конфигурационных файлов достигает 3-х. Настройки в файлах конфигурации используются для настройки коммутатора во время запуска.

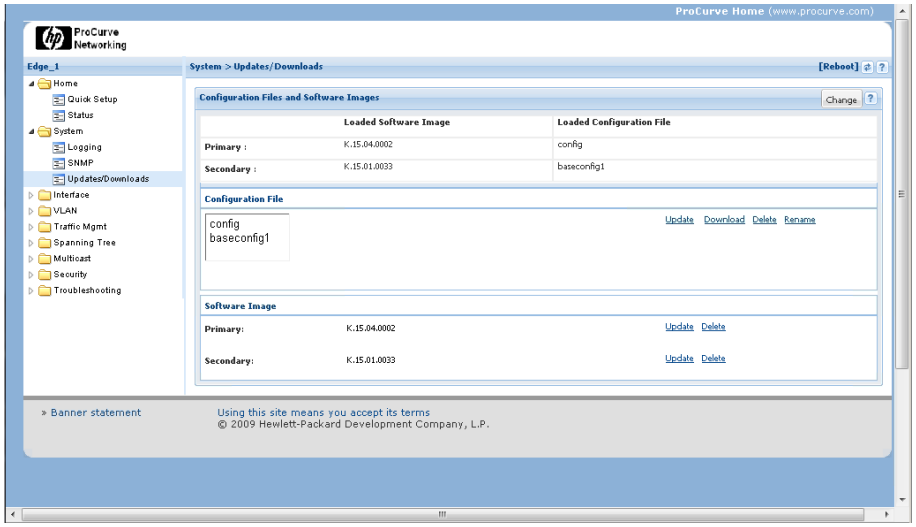


Рис. 2.40 - Updates/Downloads

Параметры интерфейса

Разверните папку «Interface», чтобы получить доступ к странице «Info/Config» и «POE». Страница Порт «Info/Config» (Рис. 2.41) отображает информацию порта конфигурации и позволяет управлять параметрами конфигурации.

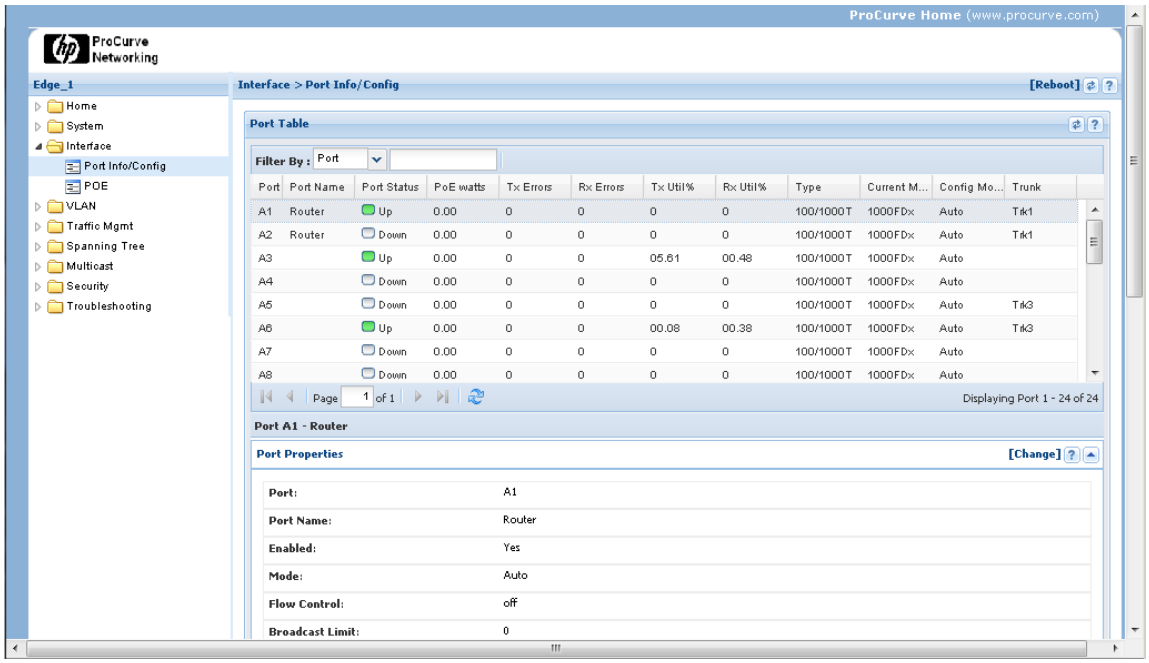


Рис. 2.41 - Порт Info/Config

Подчеркните что устройство, питание которого организовано через POE (Power over Ethernet – по витой паре) обычно не будет иметь возможности альтернативного питания, поэтому POE необходим для устройства.

Страница Port Info/Config также отображает сводную статистику портов коммутатора (Рис. 2.42), которые могут вам понадобиться (прокрутите вниз, чтобы посмотреть).

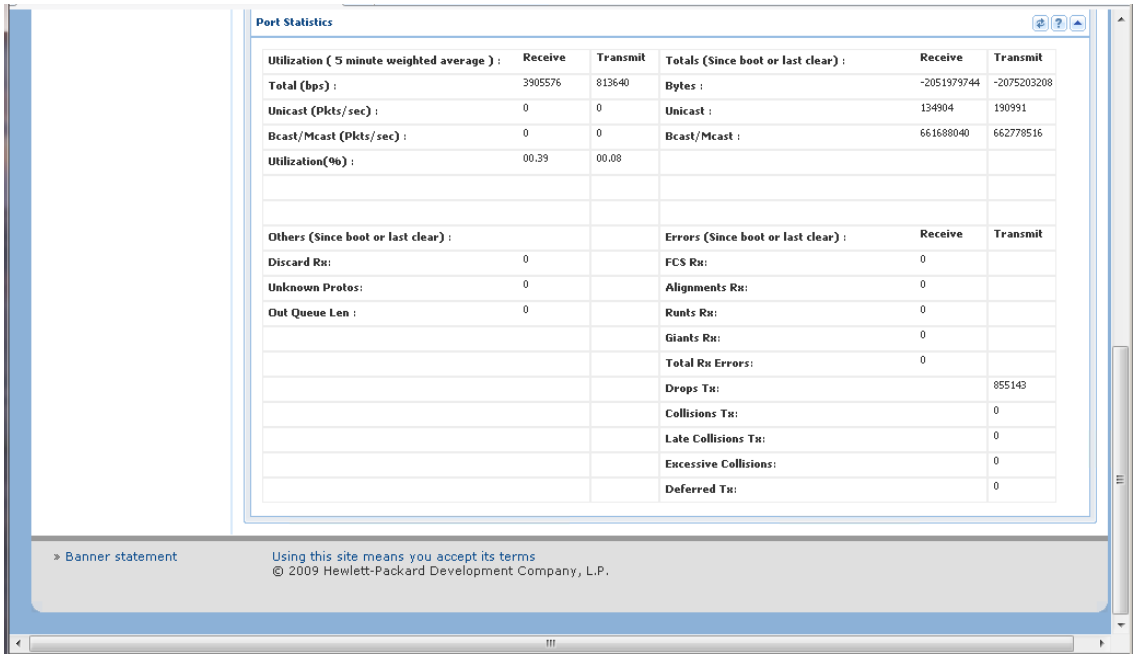


Рис. 2.42 - статистика портов на странице «Port Info/Config»

Нажмите «POE» для просматра и изминения параметров конфигурации POE (Рис. 2.43). Количество доступных устройств POE несколько ограничена, но оно постоянно растет.

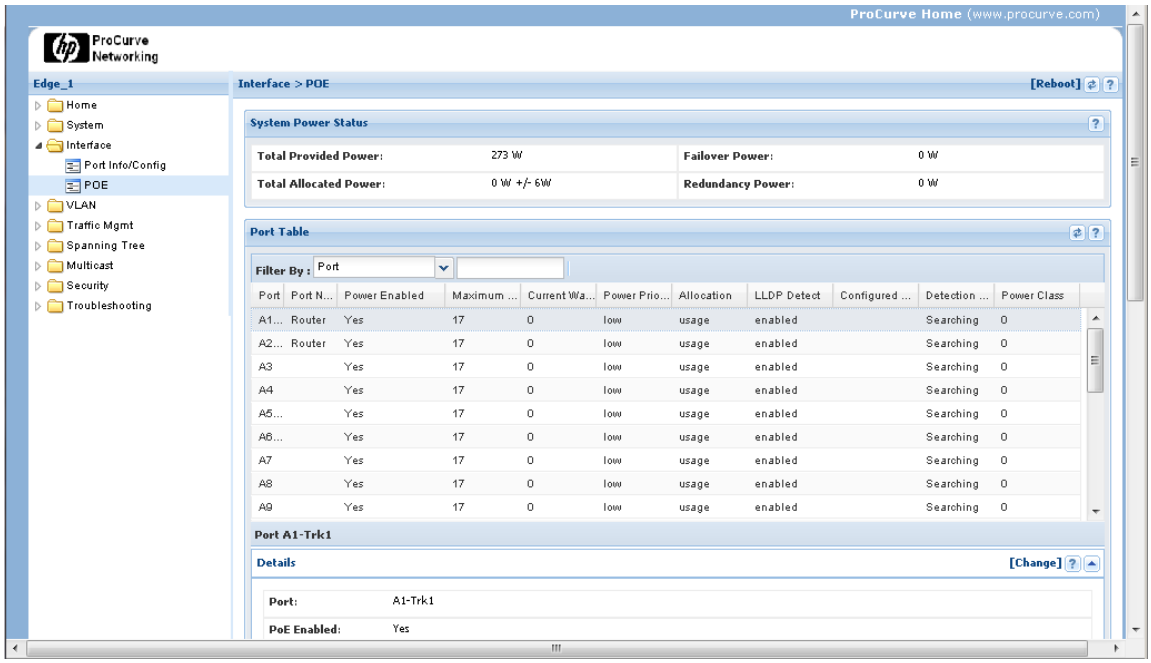


Рис. 2.43 – POE

VLAN опции

Разверните «VLAN» и выберите «VLAN Mgmt» для изменения и просмотра настроек параметров VLAN (Рис. 2.44). Выберите VLAN из таблицы «VLAN» для просмотра свойств, характерных для этой VLAN.

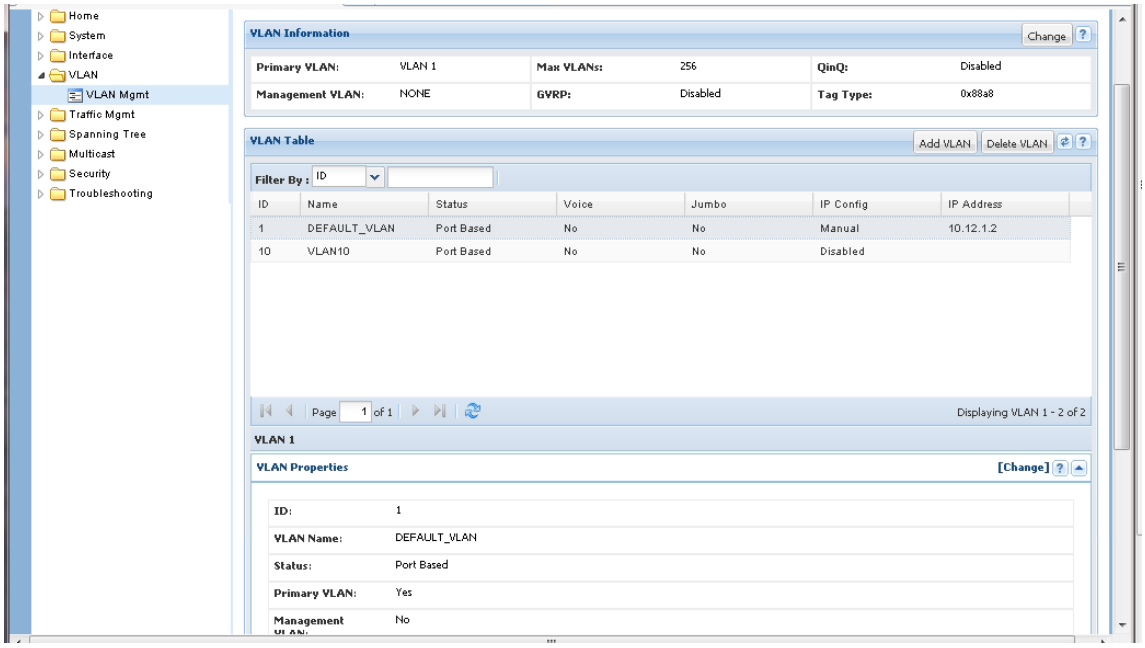


Рис. 2.44 - Управление VLAN

Параметры безопасности

Страница безопасности позволяет настроить параметры безопасности. По умолчанию, коммутатор не защищён. К примеру, по умолчанию, имена и пароли пользователей оператора и менеджера - пустые (Рис. 2.45).

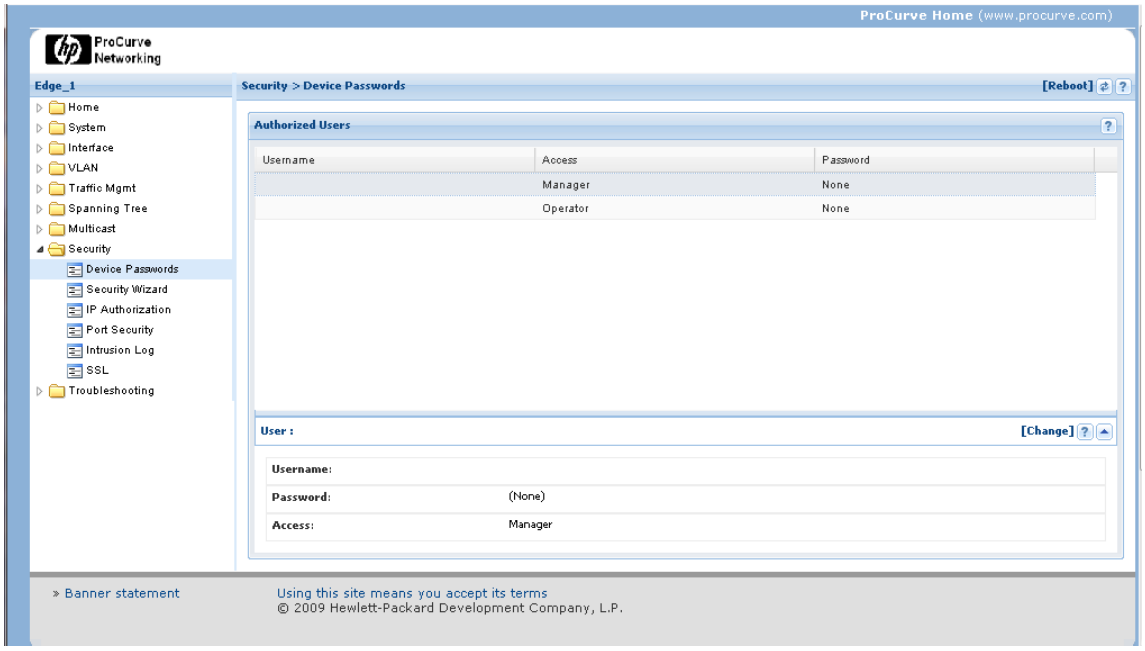


Рис. 2.45 - Пароли устройств

Если позволяет время обсудите с классом, почему это наилучшее предложение с точки зрения практики.

В дополнение к ограничению доступа по имени пользователя и пароля, вы можете ограничить доступ к управлению коммутатором с помощью IP-адреса источника. Таким образом, вы сможете ограничить компьютеры, которые могут запустить сессию Telnet с помощью коммутатора.

Мы настоятельно рекомендуем, при настройке нового коммутатора, первым делом выполнить установку имён пользователей и паролей для оператора и менеджера доступа к коммутатору.

Средства устранения неполадок

Некоторые инструменты поиска неисправностей осуществляется через веб-интерфейс. Ping/Link Test (Рис. 2.46) что позволяет проверить связь с сетевыми устройствами. Вы можете запускать «ping» тесты по IP-адресу и «link» тесты - по MAC адресу.
Некоторые версии веб-интерфейса не включают в себя страницы для устранения неполадок.

Вы также можете включить коммутатор зеркального используя интерфейса командной строки. Настройка коммутатор зеркалирование показана позже.

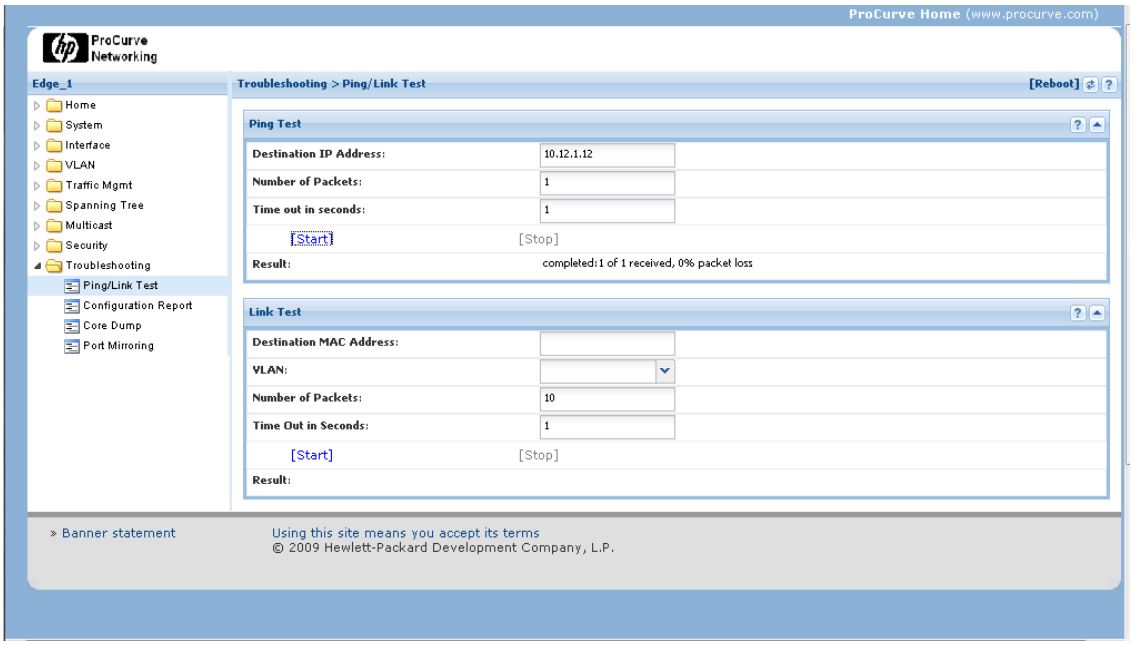


Рис. 2.46 - Ping/Link Test

Выберите «Configuration Report», чтобы просмотреть подробные настройки коммутатора (Рис. 2.47). Страница «Configuration Report» отображает текущую конфигурацию.

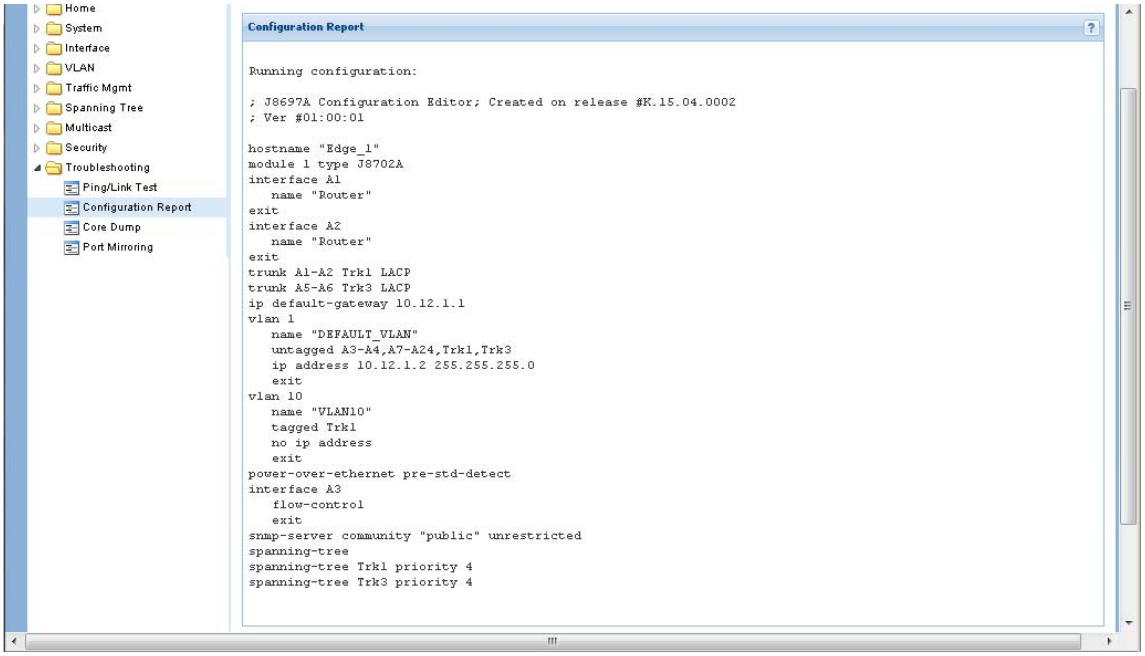


Рис. 2.47 - Configuration Report

Страницы по устранению неполадок также позволяют Вам выполнять сброс системных настроек или памяти, переключиться на анализ. Вы также можете включить коммутатор зеркального отображения для мониторинга трафика.

Одним из преимуществ использования веб-интерфейса является то, что позволяет управлять коммутатором из любого места сети. Еще одним преимуществом является то, что веб-интерфейс это самый простой инструмент управления в

использовании. Самый большой недостаток в том, что веб-интерфейс поддерживает наименьшее количество вариантов управления.

Сценарий: GoShop, Inc.

В GoShop, Inc., процес настройки своей сети, идентичен настройке проводной сети Ethernet. Все соединения устройств подключены к управляемому коммутатору и физически находится в запертом шкафу. Коммутатор имеет два порта модулей с местом для дополнительных портов. Порты b1 через B24 в настоящее время зарезервированы для будущего расширения.

В максимально возможной степени, управления коммутатором следует делать из-за пределов распределительного шкафа. Только администратор сети и персонал технической поддержки должен иметь возможность делать какие-либо изменения в конфигурации коммутаторов.

Обсудите требования к управлению для этой конфигурации. Определите способ удовлетворения требованиям доступа и ограничения безопасности, указанные в этом руководстве.

Управление коммутатором

Перед тем как покинуть тему коммутаторов, мы потратим немного больше время на обсуждение управление коммутатором.

Switch Setup с помощью мастера безопасности Web Interface

Одним из первых вещей, которые необходимо выполнить для нового коммутатора - это настроить основные параметры коммутатора, особенно параметры безопасности. Рассмотрим один из способор реализации этого процеса, с помошью Веб-мастера безопасности (Рис. 2.48).

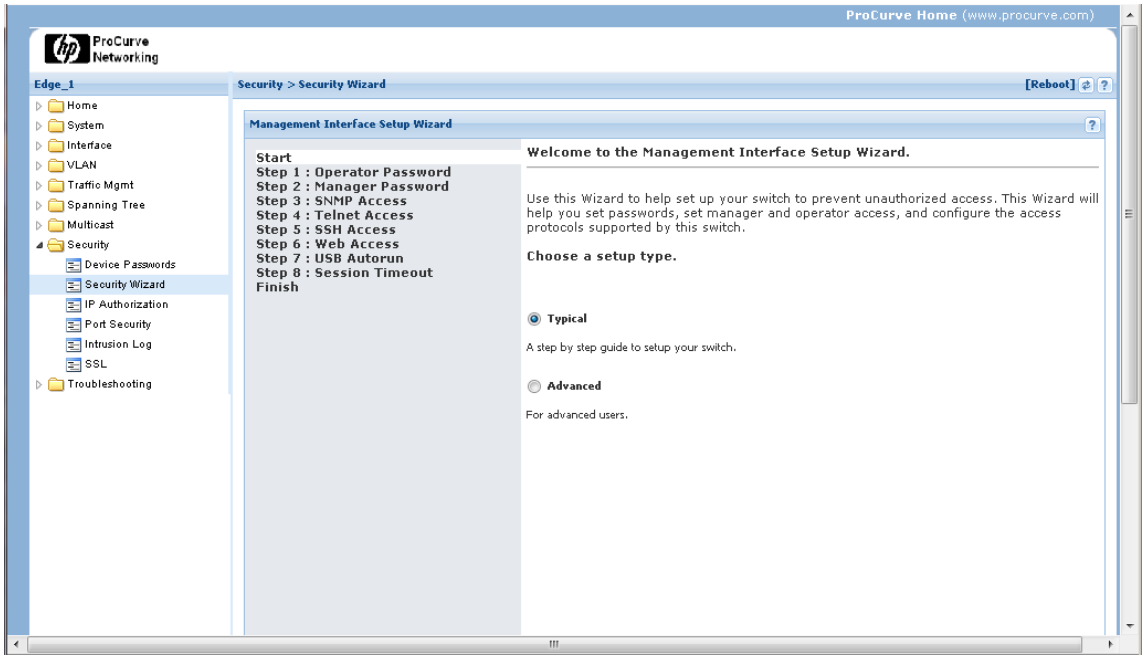


Рис. 2.48 - Мастер безопасности

Типовые настройки конфигурации безопасности включают в себя:

пароль оператора;

пароль управления;

доступ к SNMP;
доступ к Telnet;
доступ к SSH;
веб-доступ;
USB автозапуска;
тайм-аут сессия.

Существуют другие действия, которые вы, скорее всего, захотите выполнить во время первоначальной настройки. Одним из них является отключение DHCP / BOOTP поддержки и назначение статического IP-адреса коммутатора. При включении DHCP / BOOTP, есть шанс, что IP-адрес коммутатора может измениться. Используя статический адрес, вы можите осуществить подключение к коммутатору через Telnet или веб-интерфейс.

Настройка коммутатора при помощи интерфейса командной строки

Команда установки CLI позволяет ввести основную информацию для коммутатора используя интерфейс меню (Рис. 2.49).

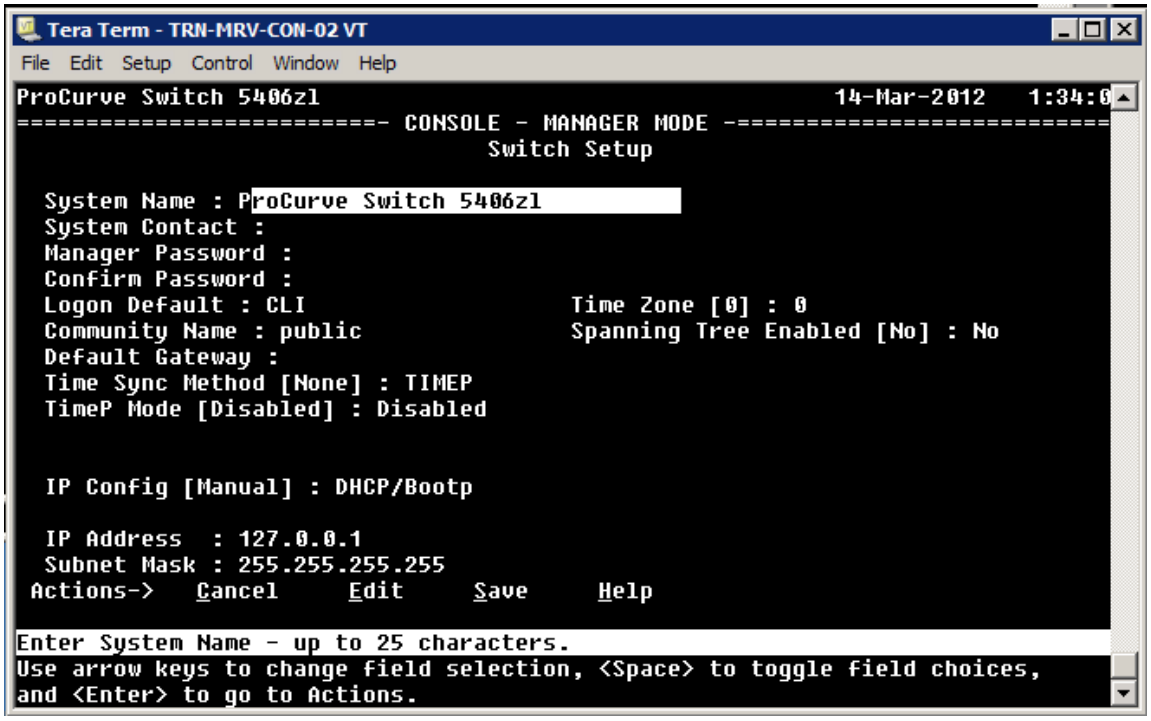


Рис. 2.49 - Экран Switch Setup

Отсюда, вы можете ввести основную информацию установки, например, в качестве контактного лица для коммутатора, менеджер паролей, включить или отключить DHCP / BOOTP, а также IP-адрес. В этом примере предполагается, что коммутатор выполнен с возможностью назаначания IP-адреса - автоматически.

Шлюз по умолчанию относится к маршрутизатору, на который проводится переадресация пакетов, в случае если адресат находится не в локальной сети, то путь к месту назначения - не известен.

Один из шагов, который вы должны выполнить это определение описательного и уникального имени хоста для коммутатора, который необходимо сделать в контексте

конфигурации. Например, если вы хотите назвать коммутатора Switch1, вам потребуется запустить команду «config», чтобы войти в контекст конфигурации, а затем запустить:

```
hostname switch1
```

При настройке хоста для коммутатора, его имя будет отображаться в командной строке CLI вместо числа модели коммутатора.

Вы также можете управлять паролями в контексте конфигурации. Например, если вы хотите установить имя пользователя для доступа к менеджеру как администратора и установить пароль, то необходимо выполнить:

```
password manager user-name admin
```

CLI запросит у вас пароль. Введите пароль и нажмите клавишу Enter.

Чтобы задать имя пользователя и пароль для доступа оператора, вы должны использовать ту же самую команду «password». Для того, чтобы задать имя пользователя как технический оператора, выполните:

```
password operator user-name techie
```

Вас ещё рас попросят ввести пароль.

Для того чтобы очистить оба пароля, тоесть оставить коммутатор не защищённым паролем, выполните:

```
no password all
```

Прежде чем запустить эту команду Вы должны быть подключены к коммутатору с доступом менеджера через Telnet сессию или через консоль.

Многие коммутаторы также имеют кнопку, которую можно использовать для очистки паролей. Нажатие кнопки Clear приведёт к очистке паролей, но не сбросит конфигурацию коммутатора к настройкам по умолчанию.

Команды настройки и управления

Таб. 2.1 - Часто используемые команды конфигурации

Синтаксис команды	Описание
configure	Переход от уровня менеджера к глобальному контексту конфигурации
hostname	Определить имя хоста на коммутаторе
password	Настройка защиты паролем для уровней конфигурации
ip address <subnet mask>	Настройка IP-адреса для интерфейса
interface <int number>	Показать tagged / untagged VLAN статус портов
write memory	Сохранить изменения конфигурации
vlan <vlan-id>	Переход от глобального контекста конфигурации в контексте конфигурации VLAN
logout	Выйти из интерфейса управления
show ip	Показать IP-адрес

show lldp info remote-device	Просмотреть информацию LLDP для подключенного устройства
show interface	Показать информацию о портах Ethernet
exit	Выход из уровня конфигурации. Например, эта команда будет двигаться из контекста конфигурации VLAN к глобальному контексту конфигурации.
enable	Привилегия менеджера уровня доступа

После внесения изменений в конфигурацию, вы должны сохранить их во флэш-памяти коммутатора. Чтобы сделать это, выполните команду:

```
write memory
```

Уровни доступа

Уровни доступа коммутатора являют собой иерархическую структуру (Рис. 2.50). Уровень опеатора обеспечивает доступ только для просмотра информации о коммутаторе. Если вы хотите внести изменения, вы должны быть подключены, по крайней мере, на уровне менеджера.

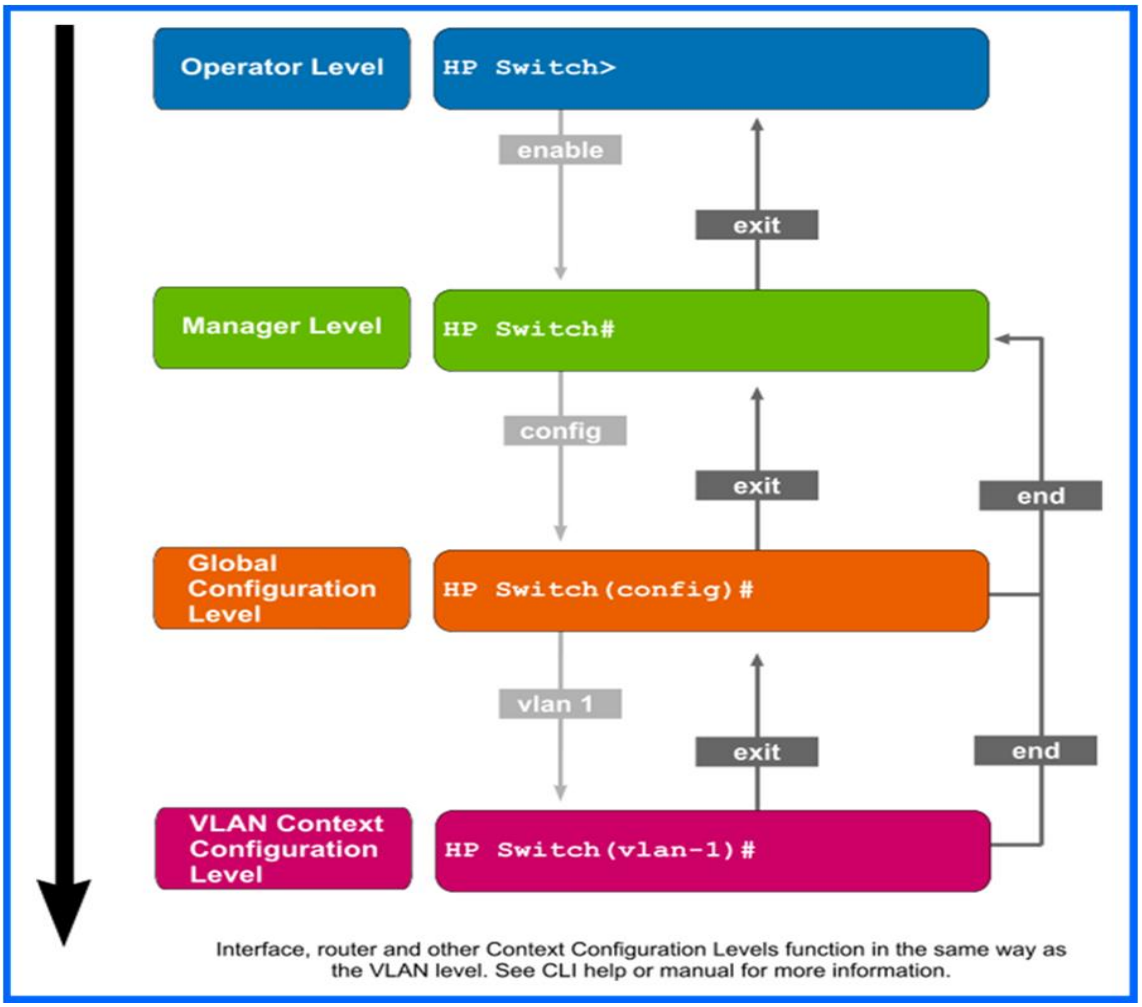


Рис. 2.50 - Уровни доступа

Глобальный уровень конфигурации (контекст config) и VLAN уровня конфигурации контекста (VLAN контекст) даст вам доступ к более мощным, специализированным конфигурациям и командам управления.

Примеры управления

Перед тем как перейти к следующему, мы рассмотрим некоторые дополнительные примеры управления.

Показать примеры команд

Рание мы розсматривали использование команд «show». Команда «show» также позволяет просматривать информацию о различных параметрах конфигурации. Например чтобы увидеть список настроенных VLAN, вы можете запустить:

```
show vlans
```

Чтобы увидеть информацию о маршрутизации с помощью коммутатора, выполните следующую команду:

```
show ip route
```

Вы также можете использовать команду, чтобы просмотреть информацию разделения сетевых коммутаторов, использующих протокол LLDP.

Link Layer Discovery Protocol (LLDP) - TCP / IP протокол канального уровня, используемый устройствами для обмена служемной информацией с месными соседями, такой как: кто они, их возможности, и т. д.

Чтобы увидеть информацию о местных портах и портовых идентификаторов коммутатора, выполните:

```
show lldp info local-device
```

Чтобы увидеть информацию об удаленных коммутаторах, выполните команду:

```
show lldp info remote-device
```

Вы можете получить более подробную информацию о портах, запустив:

```
show interface
```

Эта команда покажет список портов, переданных и полученных пакетов, а также список пакетных ошибок.

Команды глобальной конфигурации контекста

Вы узнали выше что контекст «config» (глобальный контекст конфигурации) дает вам доступ к дополнительным командам конфигурации. Оттуда, вы можете ввести контекст конфигурации для конкретного порта. Если вы хотите, управлять портом A10, вы должны запустить:

```
interface a10
```

Ваша подсказка будет похожа на следующее:

```
switch1(eth-A10)#
```

Некоторые из команд управления включают в себя:

```
enable
```

Включение порта (значение по умолчанию)

```
disable
```

Отключить порт, так что он больше не может быть использован.

```
speed-duplex
```

Определить параметры скорости и дуплекса для порта.

```
mdix-mode
```

Укажите поддержку перекрестного или прямого кабеля.

```
name
```

Укажите имя порта, чтобы определить его по имени, или порт ID.

Duplex.В контексте общения, дуплекс означает, что пользователи, на обоихконцах, могут отправлять и получать информацию одновременно.

Контекст команд VLAN

Если вы хотите запустить дополнительные команды управления VLAN, необходимо ввйоти в виртуальную локальную сеть. При необходимости управления из строки «config», выберете «vlan context» для VLAN. Первоначально коммутатор будет настроен с одной VLAN, VLAN-1.

```
vlan 1
```

Вы можете убедится, что вы находитесь в vlan по строке:

```
switch1(vlan-1)#
```

Используйте команду «IP» для конфигурирования IP в VLAN, например:

```
ip address 192.168.1.14/24
```

Адрес задается с помощью бесклассовой междоменной маршрутизацией (CIDR). О CIDR россказывется позднее в этом курсе, но пару слов, всё таки, сказать стоит: после "/" определяет количество битов в маске подсети номер, так / 24 эквивалентно маске подсети:

```
255.255.255.0
```

Если это по умолчанию VLAN коммутатора, вы меняете IP-адрес коммутатора. Если Вы зашли, чтобы проверить настройки системы в этой точке, вы увидите, что IP Config установлен в ручной режим, а IP-адрес и маска подсети установлены в значения, которые вы указали.

Вы должны сохранить эти изменения, если хотите, чтобы они были применены в следующий раз после сброса. Вы можете сохранить их отсюда, либо с помощью «write memory» в командной строке.

История команд

Вы имеете доступ к недавно выполняемым командам в случае, если есть необходимость использовать их снова. Используйте стрелки вверх и вниз для прокрутки команд. Вы можете редактировать командную строку, если необходимо, нажмите клавишу «Enter», чтобы выполнить команду еще раз. Для просмотра списка истории команд, запустите:

```
show history
```

Будет отображена текущая историю командной строки (Рис. 2.51).

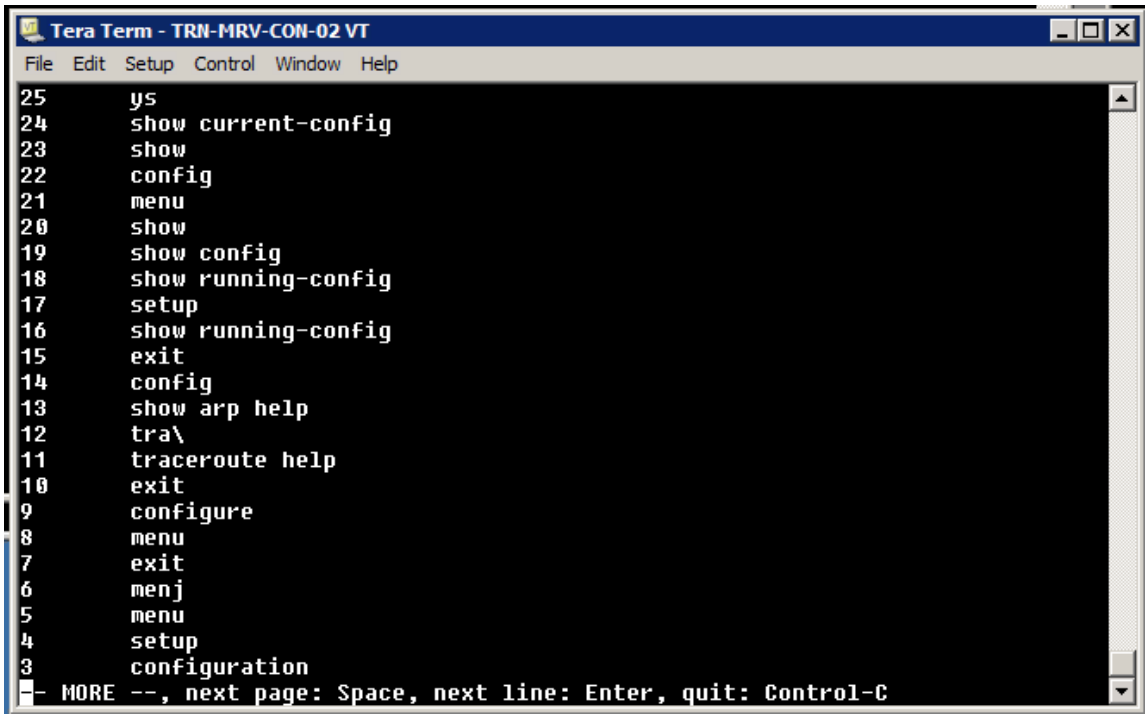


Рис. 2.51 - Список истории команд

Вы можете выполнить команду из истории команд по номеру индекса. Например: `repeat 10`

Журналы событий

Все происходящие события регистрируются в журнале событий коммутатора. Существует пять категорий записей:

Информационные;

Предупредительные;

Важные;

Отладочные;

Ошибки.

Глава 3:
Сетевая инфраструктура

Введение

Прежде чем вы сможете понять, как функционирует сеть в целом, вы должны понять, как работают отдельные сетевые устройства. Тем не менее, чтобы получить реальное представление о сети, вам необходимо узнать, как эти отдельные устройства работают вместе, чтобы сформировать сетевую инфраструктуру. Даже небольшая сеть может быть реализована в различных формах. Важно, понять эти варианты сети, прежде чем рассматривать сетевые устройства более подробно. В этой главе подробно рассматриваются проводные и беспроводные сети.

Мы исследуем сети средств массовой информации и варианты кабельных установок, в том числе топологии и конфигурации, как для проводных, так и беспроводных сетей. В процессе, мы сделаем краткий обзор на вопросы безопасности, относящиеся к сетевым функциям. Мы также потратим немного больше времени о сегментации сети, и поговорим об использовании периметра сети для защиты LAN от вшнешней сети. Эта лекция так же включает в себя обзор на некоторые дополнительные технологии, в том числе трансляция адресов, межсетевые экраны, фаерволы и прокси-серверы.

Цели

В этой главе вы узнаете, как:

• Описать ведущие сетевые характеристики.
• Выбрать подходящий тип кабеля для определенного использования.
• Сравнить и сопоставить ведущие сетевые топологии.
• Описание стандартов для беспроводных сетей и их реализации.
• Сравнить и сопоставить беспроводные варианты сетевой безопасности.
• Сравнить и сопоставить общие изменения беспроводной сети.
• Описание назначения и использования основных сетевых технологий:
Подсети и VLAN

NAT и PAT

Брандмауэры и прокси-серверы

Проводные сети

Основное внимание в этой главе уделяется известным, хорошо устоявшимся технология. В первую очередь мы поговорим о конфгурации сети (LAN конфигурация и подключения локальных сетей по Интернету).

Несмотря на растущую популярность беспроводных сетей на деловых и потребительских рынках, проводные сети продолжают доминировать в бизнесе и промышленности. Большинство новых сооружений и строительные ремонты включают планы кабельных трасс для кабельного оборудования. Вы могли бы задаться вопросом, почему проводные сети продолжают использоваться. Одной из основных причин является то, что сетевые администраторы выполняют и, как правило, используют технологии, которые они уже знают. Проводные сети были на первом месте в течение десятилетий, так что вся промышленность была создана, чтобы держать их функционирование должным образом. Возможно, самым главным является тот факт, что проводные локальные сети Ethernet по-прежнему превышают беспроводные сети в производительности и безопасности, поэтому переход к беспроводной сети не имеет смысла для многих предприятий.

Другие причины для дальнейшего использования проводных сетей включают в себя:

• Доступность

Многие коммерческие здания подключены к сети уже при постройке. Если они еще не подключены, они, по крайней мере сконструированы таким образом, что имеют полное представление о сети(с маршрутами для кабелей и коммутационными шкафами, разработанными в здании).

• Надежность

Компании знают, что они могут рассчитывать на проводные сети. Проводное подключение основано на уже существующих технологиях. Большинство основных технологий существуют на протяжении десятилетий. После их установки, сетевые компоненты, в том числе кабели и разъемы, могут быть нетронутыми на протяжении многих лет. Источники потенциальных проблем связи хорошо известны и, в большинстве случаев их относительно легко исправить или избежать.

• Установленые стандарты

Компоненты, связанные с проводным Ethernet следуют установленным стандартам реализации в основном способе всей отрасли.

• Гибкость

Большинство функций доступны при проектировании и развертывании проводной сети. Вместо того, чтобы создавать конфигурацию с нуля, установленные конструкции могут быть изменены, так, чтобы удовлетворить ваши потребности.

• Безопасность

Во многих смыслах, проводная сеть более безопасна по своей природе, чем беспроводная сеть, по крайней мере, на местном уровне. Подключение через сетевой кабель и его потоки данных являются более тяжелыми для перехвата, нежели перехват радиочастотной передачи.

Преобладание проводных сетей вряд ли существенно изменится в ближайшее время. Некоторые сетевые потребности, такие как дальние, высокоскоростные сетевые соединения, просто не могут быть удовлетворены текущими беспроводными технологиями. Кроме того, даже если большая часть вашей сети развернута в проводной сети, это не единственный вариант конфигурации. Вы можете соединить проводные и беспроводные технологии для дальнейшего расширения ваших вариантов сети.

Микроволновое соединение точка-точка, которое иногда используется для соединения двух мест. С практической точки зрения, оно действует непосредственно как кабель между двумя точками.

Инфраструктура проводной сети

Прежде, чем мы обратим внимание на проводные передатчики информации и проводные сетевые топологии, мы должны сначала рассмотреть несколько моментов о структуре проводов и проводные сетевые стандарты. Мы начнем с введения в кабельную систему. Далее, мы обратим внимание на стандарты Ethernet. Мы ограничим наше обсуждение 802.3 стандартами Ethernet, так как они на сегодняшний день являются наиболее распространенными сетевыми стандартами в эксплуатации.

Топология

- то, каким образом связаны между собой сетевые компоненты. Логическая топология описывает потоки данных в сети, а физическая топология описывает физические взаимосвязи между устройствами.

Кабельная система

- сетевые проводные инфраструктуры.

Кабельная система

Кабельная система это кабели в здании. В общем пользовании, она относится как к сетевым так и к телекоммуникационным (телефонные) кабелям. Она также устанавливает разграничение (или демаркирование) между кабелями в здания и кабелями снаружи здания. Место, где кабели входят в здание иногда называют точкой входа или входом объекта. Это то, где телефон, Интернет и другие телекоммуникационные услуги подключаются к внутренней сети.
Внутри объекта, конкретная реализация кабельной системы может варьироваться, но часто бывают некоторые общие черты. Они, как правило, имеют техническое помещение, компьютерное оборудование, поддерживающие сеть. Там также может быть отдельная комната телекоммуникационной поддержки телефонной системы. Если у вас есть несколько технических помещений и телекоммуникационных помещений, магистральные кабели используются для связи между местами. Например, у вас магистральный кабель может работать между этажами в здании или между зданиями в университетском городке.

Магистральный кабель

- сетевой кабель, используемый в локальных сетях для эффективного соединения на расстоянии.

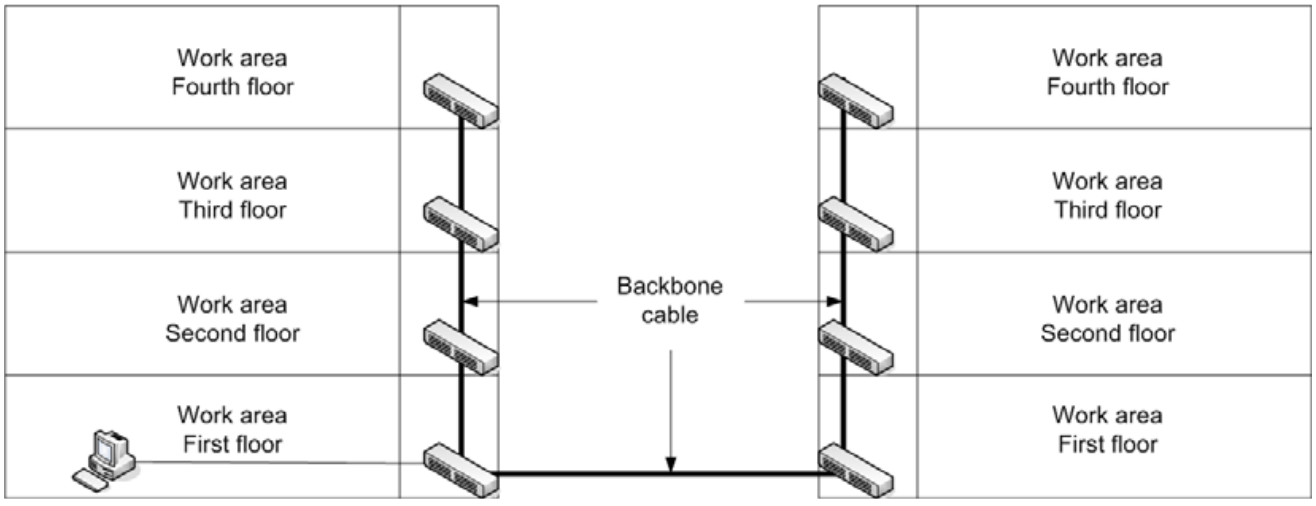


Рисунок 3-1: Магистральные провода

В рабочей среде, например, в качестве офисной площади или этажа здания, кабельная система состоит из горизонтальных компонентов распределения. Это начинается с

распределения фреймов в конечные точки в технической комнате, а оттуда кабели прокладываются в рабочую среду.

Кабели физически направляются в рабочую среду за счет использования каналов, кабельных подвесок, и кабельных лотков. Канал представляет собой пластиковую или металлическую трубу, которая обеспечивает путь для кабеля и физически защищает его. Кабельные лотки и кабельные подвески обеспечивают кабелям маршрут и облегчают физическое напряжение на кабель. Прилягающую площадь, через которую направляется кабель обычно называют пленум (Рисунок 3-2). Площадь пленума может включать в себя пространство над подвесным потолком, область под фальшполом, или открытое пространство между стенами.

Кабельный лоток

- узкий лоток который проходит через области пленума, в котором может быть положен кабель.

Кабельная подвеска

- простые крючки, используются для хранения кабелей в пространстве и обеспечивают разгрузку кабеля.

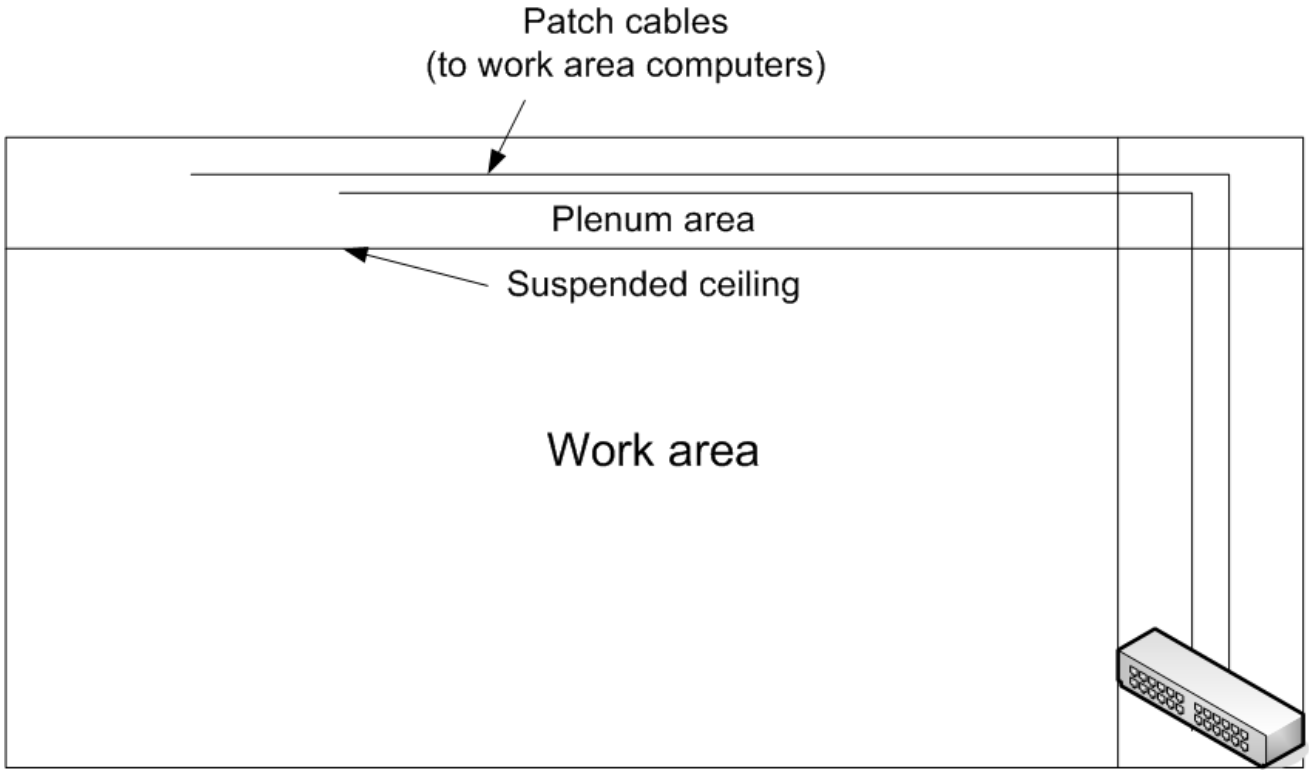


Рисунок 3-2: Пример горизонтальной прокладки

Нельзя запускать сетевые провода через тот же канал где есть электрические кабеля. Это может привести к тому что напряжение с электрических кабелей будет препятствовать коректной передаче информации по сетевым кабелям.

Стандарты Ethernet

Начальные стандарты Ethernet были основаны на коаксиальных кабельных сооружениях.
Было два выходных эталона:

10Base5

10Base2

10Base5, также известный как толстый Ethernet или Thicknet, в первую очередь был использован в магистральных приложениях. 10Base2, также известный как Thin Ethernet или ThinNet, был использован для соединения с отдельными сетевыми устройствами.
Эти унаследованные технологии встречаются редко и не используются в новых устройствах. Большинство сетевых устройств и почти все сетевые платы даже не поддерживают разъемы AUI и BNC используемые в 10Base5 и 10Base2.
Стандартные технологии сегодня используют или витую пару или оптоволоконные кабели. Наиболее распространенными являются кабели на основе стандартов BaseT медные кабеля. Медные кабельные стандарты, которые вы, вероятно, увидите включают в себя:

10BaseT

100BaseT

1000BaseT

10GBaseT

1000Base-LH - стандарт поддерживает работу на растоянии до 80 км в одномодовом волоконном кабеле.

Эти стандарты основаны на использовании витой пары (Рисунок 3-3) .Кабель имеет несколько медных проводов, собранных в пары. Каждая пара будет наполовину скрученна по всей длине проводов, используется для того, чтобы уменьшить шанс вмешательства. Подключение осуществляется через RJ-45 разъем.

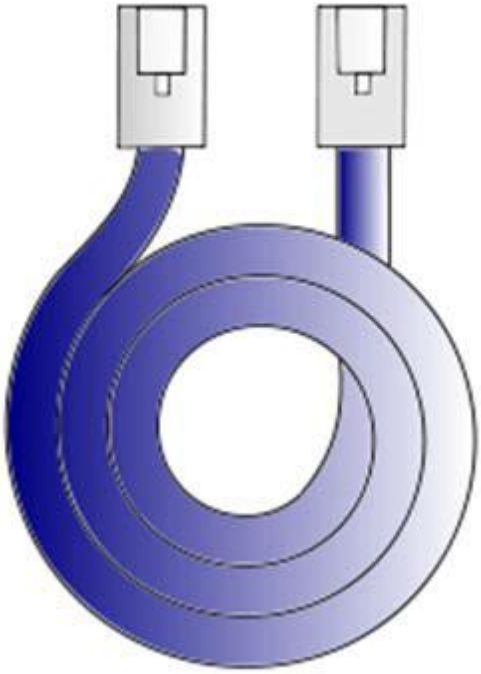


Рисунок 3-3: Витая пара

10BaseT по прежнему поддерживается, но как правило, служит в качестве резервной системы проводки. Большинство сетевых интерфейсов используют 10BaseT только в качестве запасного варианта когда основная система проводки имеет коммуникационные проблемы. Большинство коммутаторов автоматически настраивают скорость передачи данных портов в соответствии с максимальной скоростью, поддерживаемой как переключателем так и подключенным устройством.
Есть также различные стандарты Ethernet для волоконно-оптического кабеля. Старейшим из них является 10Base-FL. Ограничена максимальная скорость передачи данных 10 Мбит, стандарт поддерживает кабельные отрезки до 1 км. Другие волоконные стандарты включают в себя:

1000Base-LX

1000Base-SX

1000Base-ZX

10GBase-X

Эти все стандарты поддерживают скорость передачи данных до 1 Гбит, а для 10GBASE-X - 10 Гбит. Максимальная длина сегмента кабеля отличается между стандартами, максимальная длина 10 км для наиболее распространенных реализаций. Текущие реализации волоконно-оптических связей основаны на стандарте IEEE 802.3ah. Higherspeed стандарты, в том числе 40 Гб и 100 Гб Ethernet, находятся в стадии

разработки, некоторые приборы, работающие на этих скоростях доступны в данный момент. Тем не менее, реализация большинства из этих высоких скоростей зависят от производителя.

Будьте предельно осторожны при выборе конкретного производителя сетей. Могут возникнуть проблемы с функциональной совместимостью с другими производителями товаров

Сетевые средства массовой информации

Как уже упоминалось выше, есть три основных типа проводных сетевых средства массовой информации.

К ним относятся:
Коаксиальный кабель

Витая пара

Волоконно-оптический кабель

Витая пара может быть разделена на STP и UTP. Физическая разница между ними заключается в том, что провода в кабеле STP в окружении металлической оболочкой, обеспечивающей защиту от электромагнитных помех и радиопомех. Ранние использованные термины определены ниже.

Экранированная витая пара (STP)
- две или более пар изолированных медных проводов, окружены металлическим экраном и внешним диэлектриком.

Неэкранированная витая пара (UTP)
- две или более пар изолированных медных проводов, окружены внешним диэлектриком.

Электромагнитные помехи (EMI)

- сигналы помехи, вызванные излучением или созданием электрического тока поперек магнитного поля (электромагнитной индукции) внешнего источника.

Радиочастотные помехи (RFI)
- форма EMI, состоящий из высоко частотных (частоты радиоволн) выбросов.

Коаксиальный кабель

Коаксиальный кабель, показанный на рисунке 3-4, имеет центральный проводник, который несет сигнал данных. Он окружен диэлектриком, а затем металлическим экраном.

Рисунок 3-4: Коаксиальный кабель

Коаксиальный кабель эффективное технологическое наследие для сетей. Он по-прежнему широко используется для кабельного телевидения и для подключения к спутниковой антенне или спутникового модема.

Характеристики необходимого кабеля, зависят от того, что вы используете - 10base2 или 10Base5 Ethernet.

10Base2

RG58 A / U кабель

Длина сегмента максимум 607 футов (около 185 м)

10Base5

RG-11 кабель

Длина сегмента максимум +1640 футов (500 м).

Максимальная длина кабеля любого типа обусловлена физическими характеристиками кабеля и передающимся сигналом. Сигнал теряет силу на расстоянии, это процесс, известный как ослабление (рис 3-5). После прохождения расстояния, сигнал становится не надежным. Это относится как к проводным так и к беспроводным передачам.

Ослабление

- потеря сигнала (амплитуды сигнала) на расстоянии.

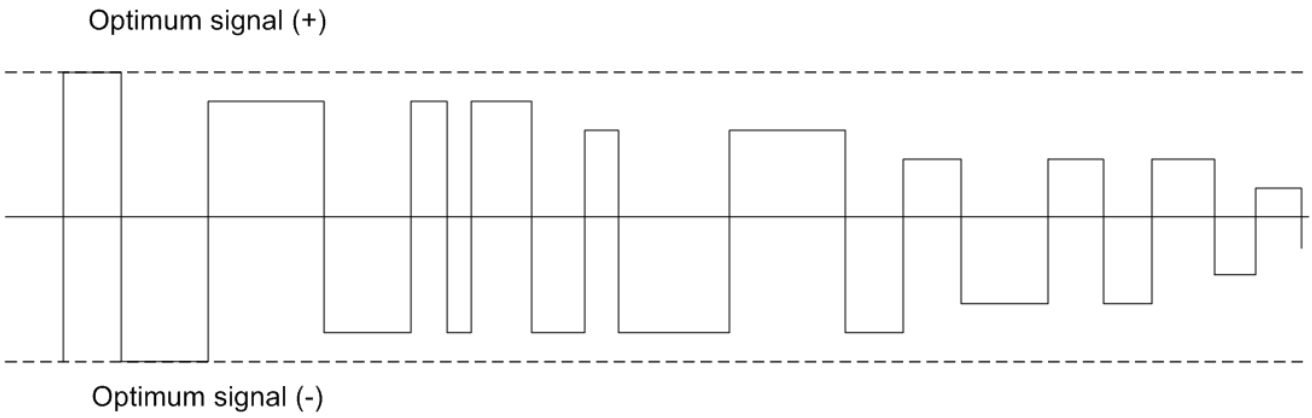


Рисунок 3-5: Ослабление

В примере, пунктирные линии показывают оптимальную силу сигнала. Сигнал начинается в оптимальном состоянии, но ослабляется чем дальше он проходит.

10Base2, является наиболее распространенной реализацией, использовалась когда оба устройства были подключены непосредственно к кабелю или к цепи. Соединения были реализованы с помощью разъема BNC, показанный на рисунке 3-6. На оба типа кабеля

по их концам были установлены резисторы по 50 Ом, чтобы обеспечить качество сигнала.

Рисунок 3-6: BNC розьем

Есть несколько причин, почему коаксиальный кабель потерял рентабельность в сетевых реализациях. По сравнению с витой парой, с ним достаточно трудно работать, коаксиальный кабель не является достаточно гибким, чтобы согнуть его под острым углом. Основные коаксиальные конфигурации также очень сложно устранить. Проблема в любом месте вдоль трассы кабеля, на обоих концах или с любого подключенного устройства может вызвать ошибку сети.

Витая пара

Почти все текущие конфигурации сети использовуют витую пару. Большинство развертывание использовать UTP кабель, который легче в использовании и дешевле, чем STP кабеля. STP кабель обычно используется только тогда, когда экологические факторы требуют этого, например, источники электромагнитных помех, расположенны вблизи кабелей. Витая пара имеет несколько преимуществ по сравнению с коаксиальным кабелем, которые помогли его быстрому внедрению. Основными среди этих преимуществ были стоимость и простота установки. Это было просто дешевле для развертывания сети с помощью витой пары, а не коаксиального кабеля. Кроме того, большинство офисов уже созданы с поддержкой витой пары для работы в офисе телефонных систем.

Телефонные системы использовают более низкое качественную витую пару, чем сетевые системы. Телефонный кабель не должен быть использован для современных сетевых приложений, хотя телефонные системы могут использовать один и тот же UTP кабель, используемый для сетей передачи данных. Кросс-соединения систем на распределение кадров будет сохранять информацию и голосовые провода разделенными. Часто сегодня, телекоммуникационный трафик осуществляется в TCP / IP-пакетов по сетевому кабелю, чтобы голосовые сигналы пускались в сети передачи данных. Это часто упоминается как передача голоса по IP или VoIP.

Кросс-коммутационные системы

- устройство цифрового переключения используется для маршрутизации телекоммуникационного трафика.

Стандарты витой пары

Стандарты витой пары называют кабельными категориями. Есть несколько стандартов по всему миру, которые определяют эти категории. В дополнение к категориям, перечисленным здесь, есть категории, которые пока не (или никогда не были) используемые в сетевых приложениях.
Текущие категории перечислены в таблице 3-1.

Таблица 3-1: категории витых пар

Категория	**Пропускная способность**	
Cat 3	16 MHz	10BaseT
Cat 5/5e	100 MHz	До Gigabit Ethernet
Cat 6	250 MHz	Замена 5e Cat
Cat 6e	500 MHz	До 10 Gigabit Ethernet
Cat 7	600 MHz	10 Gigabit Ethernet

Категориям Cat 5e, Cat 6 и Cat 6e доступен STP или UTP кабель. Cat 7 кабели, как правило, экранированные, а иногда и использовуют нестандартные (не разъем RJ-45) разъемы. Максимальная длина кабеля, как правило, определяется как 100 м (около 300 футов). Более длинные кабеля приведут к деградации сигналов из-за затухания и перекрестных помехами между парами. Эта проблема особенно видна в кабелях, которые содержат несколько пар. Это часто можно увидеть в кабелях, содержащих до 25 пар в профессиональных електропроводах. При необходимости более далеких передач используеться волоконно-оптический кабель вместо витой пары.

Перекрестные помехи
- сигнал помехи между проводами работающими параллельно.

Соединения витых пар

В небольших установках, устройства могут подключаться непосредственно к центральной станции или коммутатору. Это не практично в средних и крупных установках. Вместо этого, соединения обычно выполняются в кроссе с мульти-парных кабелей идущим к стеной плите по всему офису. Окончательный подключение производится с помощью кабеля с разъемом RJ-45 (рис 3-7) на каждом конце.

Рисунок 3-7: Разъем RJ-45

Старые монтажные шкафы иногда имеют один и тот же тип патч-панелей, как для телефона и так и для поддержки сети. Эти панели требуют плинты, чтобы создать соединение. В плинтах закусы очень тесно расположены, для того чтобы проколоть

отдельные провода и чтобы сделать связь. Они несколько сложны в использовании, и также они требуют специальных инструментов для подключения к панели.

Патч-панель

- Центральная точка подключения и панель распределения витых пар, в том числе телефонных систем и сетевого кабеля.

Плинт

- традиционный способ подключения витой пары внутри патч-панели.

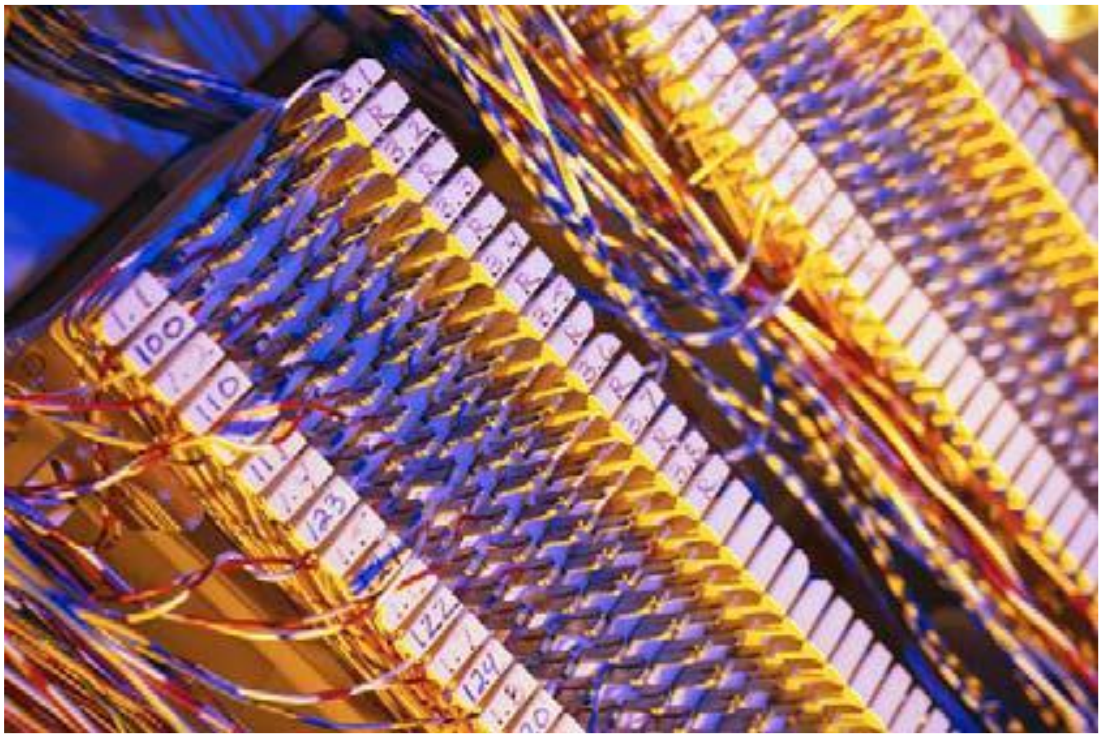


Рисунок 3-8: Плинт

В большинстве современных сетевых установок используются патч-панели с модульными разъемами (рис 3-9). Патч кабели прокладываются между коммутатором и патч-панелью. Отсюда, проводка распространяется по всей территории.

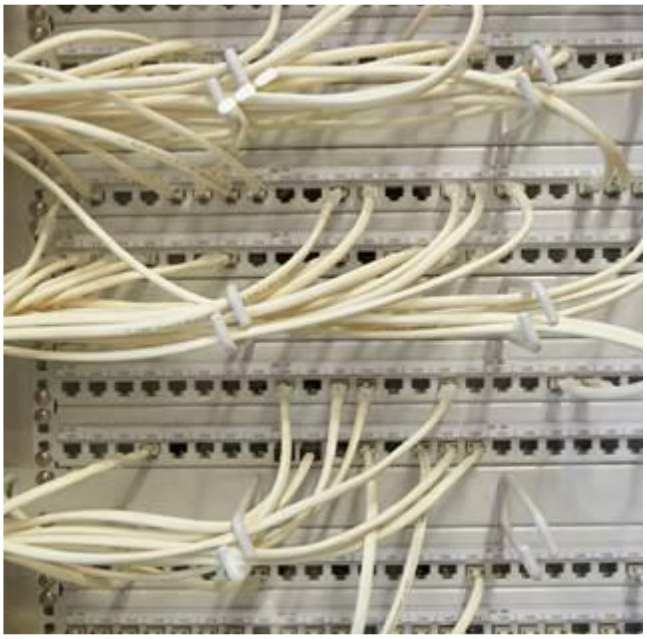


Рисунок 3-9: Модульная патч-панель

Большинство модульных патч-панелей могут быть расширены. Это означает, что вы можете расширить свою сеть, подключив дополнительную панель расширения, вместо того, чтобы покупать и устанавливать полностью новую панель. Большинство также позволяют удалить один или несколько наборов модульных разъемов, чтобы дать вам прямой доступ к коммутационной панели внизу. Иногда это необходимо для устранения неполадок и ремонта или для некоторых специальных применений установки.

Задача: <u>GoShop, Inc.</u>

GoShop, Inc является небольшой сетью розничной торговли, чьи клиенты делают покупки через интернет с веб-сайта компании. Они хотят объединить их офис и склад / отправку в одном месте.

Они расположены в здании, которое будет полностью удовлетворять обе свои потребности и прогнозируемые время в течение следующих нескольких лет. Компания будет нести ответственность за стоимость любого улучшения которое они захотят внести в здание или его инфраструктуру. Так же здание снабжено гнездом с CAT 3 кабелем, находящимся в распределительном шкафу. Физически оно расположено в том месте, которое будет использоваться в качестве склада. Владелец здания оставляет 1-й уровень, так что GoShop,Inc в полном праве использовать хаб для своей сети.

Сравните сильные и слабые стороны использования существующей кабельной системы и инфраструктуры по сравнению с модернизации сети.

Объясните изменения, которые должны быть сделаны для обеспечения безопасной и оптимальной производительности.

Опто-волоконный кабель

Волоконно-оптический кабель, как показано на рисунке 3-10, изначально считается оправданным только в особых случаях, особенно когда очень длинные, очень высокие скорости соединения были необходимы. Он нашел свой путь во многих конфигурациях LAN в ситуациях, когда он лучше подходит, чем медный кабель.

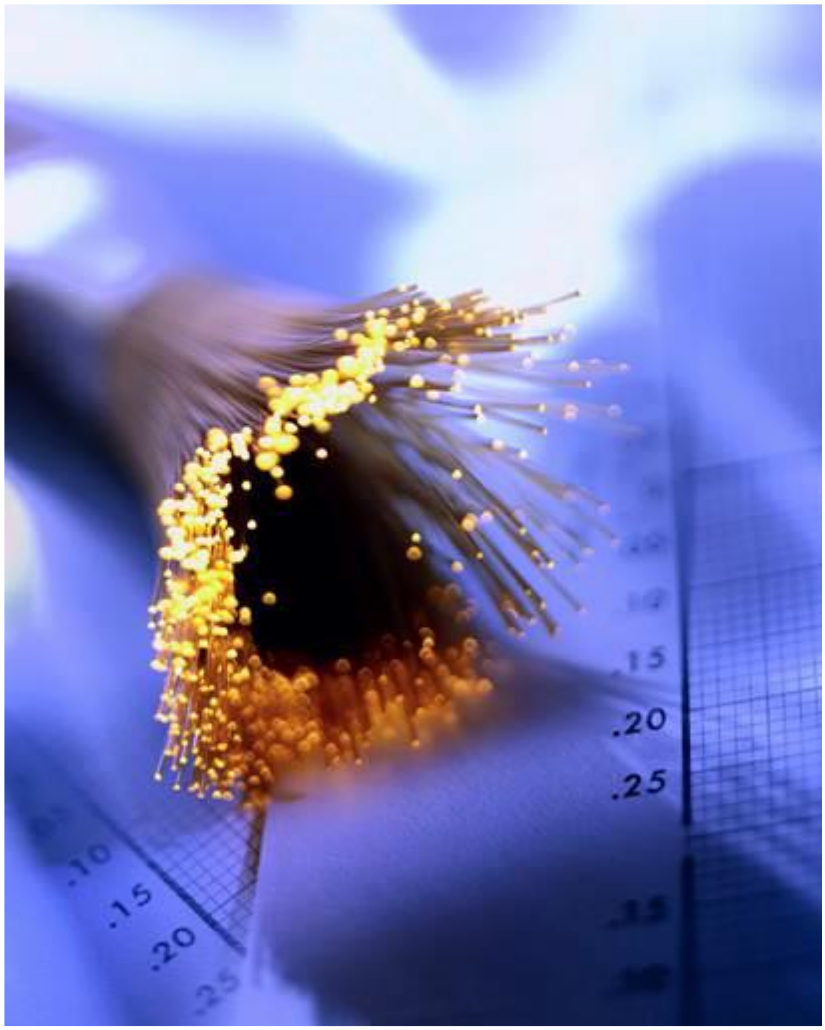


Рисунок 3-10: Волоконно-оптический кабель

Волоконно-оптический кабель используется, когда EMI слишком высока, чтобы использовать медный провод. Достаточно высокий уровень EMI может мешать даже STP кабелям. Он также используется, когда необходимо предоставить надежное и высокоскоростное соединение между сетевыми устройствами. Например, вы могли бы использовать волоконно-оптический кабель для подключения высокопроизводительных серверов прямо к сетевому хранилищу. Волоконно-оптический кабель также выбирается для многих приложений с высоким уровнем безопасности. Подключение в сеть через волоконно-оптическом кабель и перехват данных чрезвычайно трудный. Даже тогда,

когда волоконно-оптический кабель пропускает такие попытки они будут легко обнаружены, так как они сразу же обрывают связь в кабеле. Другой рынок, который является движущей силой принятия оптоволоконного кабеля для сетевых приложений является игровой. Сети, созданные специально для поддержки компьютерных геймеров оптимизированы для максимальной производительности, часто нуждающихся в поддержке типичных скоростей передачи данных, превышающих пиковые скорости передачи данных в большинстве сетей SMB. Волоконно-оптический не является универсальным решением для всех сетевых ситуаций. Он является относительно дорогим. Сам кабель несколько хрупкий, и его трудно правильно установить. Например, некоторые развертывание требуют специальной подготовки, чтобы правильно завершить и подключить кабель.

Использование волоконно-оптических кабелей

Большинство компьютеров не имеют предустановленной волоконно-оптической поддержки, но есть и исключения. Компьютеры, которые выступают в качестве сетевых серверов имеют встроенные (или установленые) волоконно-оптические адаптеры. То же самое можно сказать и о многих топовых игровых машинах.
Волоконно-оптические соединители принимают различные формы в зависимости от того где они конкретно примененяются (рис 3-11). Большинство приложений используют два волокна, один для отправки и другой для получения. Устройства, которые используют волоконно-оптический кабель соединены в конфигурации последовательной цепочки, так что данные проходят через каждое устройство по пути к месту назначения.

Рисунок 3-11: Волоконно-оптический разъем

Одно из преимуществ конфигурации последовательной цепочки заключается в том, что сигнал на каждом устройстве регенерируется. Затухание потенциальная проблема в волоконно-оптическом кабеле, так же как и в медной кабеле. Тем не менее, в отличие от медного провода, сигнал в волоконно-оптическом кабеле обновляется на каждом устройстве и каждой соединенной цепочкой. Оптические соединения обычно используют SFP (или SFP +) трансиверы, показанные на рисунке 3-12, как окончание на

коммутаторе. Есть виды трансиверов, направленные на поддержку общих многомодовых и одномодовых волоконных стандартов.

Рисунок 3-12: HP X130 10G SFP+ LC ER 40km Transceiver

Малый форм-фактор (SFP)

- подключаемый модульный трансивер поддерживает все сетевые интерфейсы и телекоммуникационные приложения. Заменяет более ранний интерфейсный преобразователь Gigabit (GBIC).

Усиленный малый форм-фактора (SFP +)

- улучшенная версия стандарта SFP, предназначенной для поддержки 10 Гбит приложений.

Кабельные сетевые топологии

Ваша сетевая топология несколько зависит от вашего протокола низкого уровня связи. Ethernet был первоначально разработан для использования технологии шины; в то время как Token Ring использует (не удивительно) кольцевую топологию. Прежде чем пытаться разрабатывать или поддерживать сети, вы должны понимать сетевые топологии и как они используются. Наша дискуссия сосредоточена на четырех общих сетевых топологиях:

Звезда

Автобус

Кольцо

Петля

Каждая топология имеет свои сильные и слабые стороны.

Некоторые ранние попытки в соединении компьютеров, использывали топологию точка-точка, которая была на самом деле простым прямым соединением компьютеров друг с другом без какого-либо распределяющего оборудования или центральной точки подключения. Этот метод все еще иногда используется во время программного обеспечения и обновлений операционной системы.

Звезда

В топологии звезда, каждый узел соединяется с центральным узлом через соединение точка-точка, как показано на рисунке 3-13. Метод доступа к сети будет зависеть от использованного протокола низкого уровня развертываня в сети.

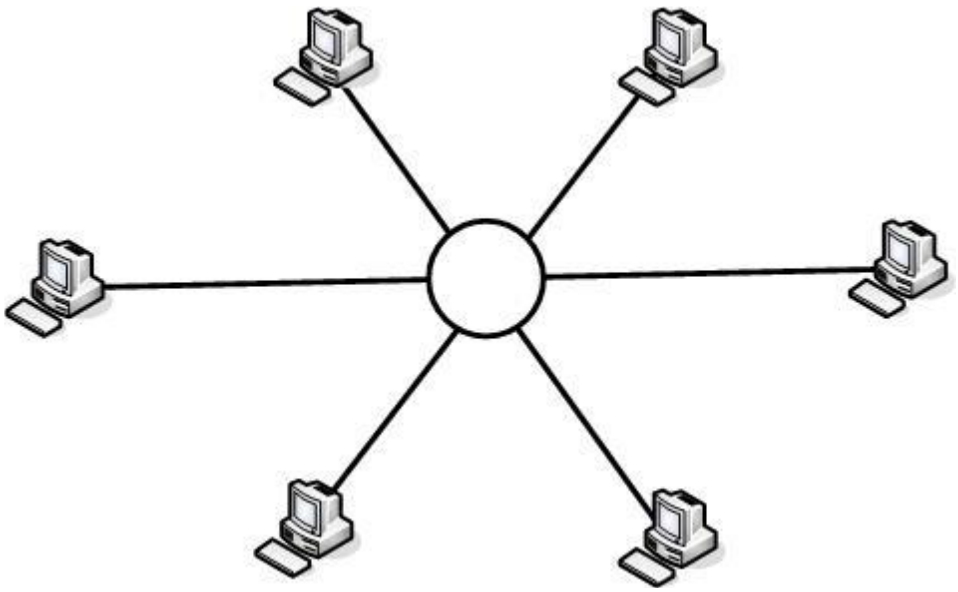


Рисунок 3-13: Топология Звезда

Даже если сеть Ethernet может выглядеть как топология звезда, это не настоящая звезда, из-за того как проходит доступ к сети и управления. Оригинальные

стандарты Ethernet указывают топологию шины, хотя это редко используется на практике.

Частым изменением топологии звезда является распределенная звезда (Рисунок 3-14). В распределенной звезде есть концентраторы, которые соединенны друг с другом, чтобы расширить сеть.

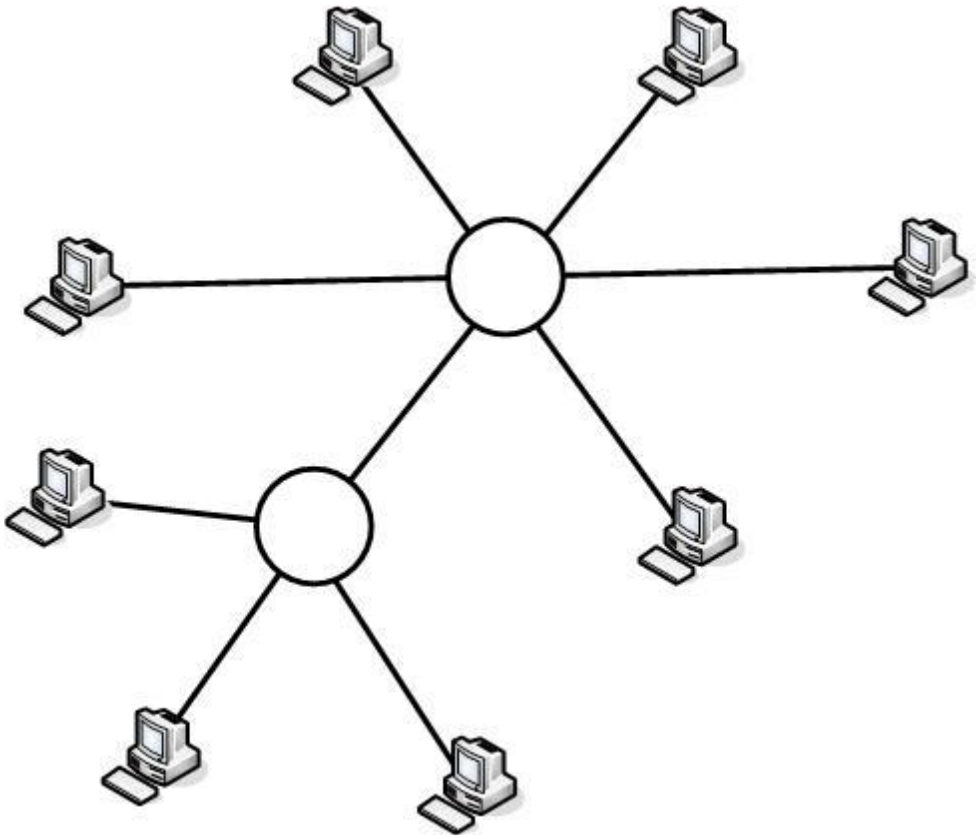


Рисунок 3-14: Топология распределенная звезды

Правда конфигурации топологии звезда очень редко видно в реализациях LAN. Тем не менее, соединения точка-точка, сделанные между хостами и коммутаторами выглядят как звездообразная топология. Центр звезды отличается от коммутатора Ethernet или концентратора тем что трафик управляется в центральном подключении.

Шина

Ethernet был разработан вокруг логической топологии шины (рис 3-15). Все узлы сети подключаются непосредственно к сетевому кабелю. В теории, каждый узел имеет равный, общий доступ к кабельному сегменту. Из-за общего доступа, могут развиться очереди и медленная скорость передачи, когда два узла пытаются передавать информацию одновременно. Каждый конец кабеля сегмента прекращается резистором, чтобы сигнал не отражался назад и вперед по кабелю.

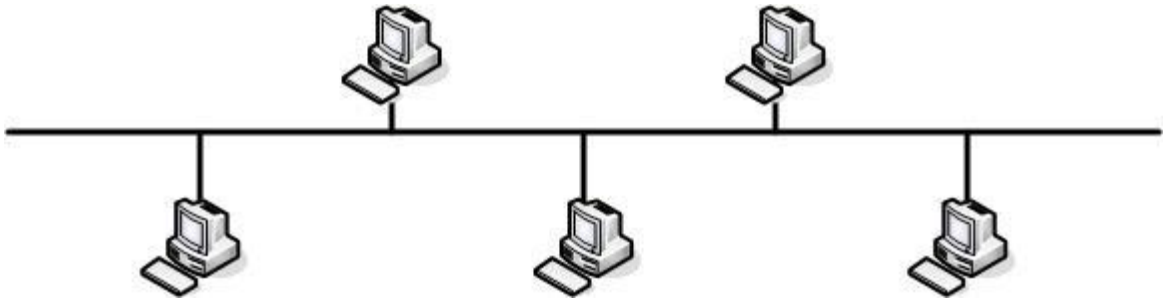


Рисунок 3-15: Топология шины

В топологии шины, при каждой передаче все узлы получают фактически то же самое время. Если передача не адресована конкретному узлу (или адресу в эфире), узел будет игнорировать передачу. Этот тип топологии шины иногда называется линейным. Одна из проблем в этой топологии является то, что проблемы общения трудно устранить. Проблемы с терминатором на любом конце, или короткий перерыв или проблема в любом месте в кабельном сегменте, может вызвать проблемы связи по всему сегменту.

Линейная шина

- топология шины без каких-либо ветвей сходит сегмент кабеля

Как упоминалось ранее, при монтаже с помощью концентратора (или коммутатора), сегмент Ethernet выглядит как физическая звезда. Концентратор имеет внутренне проводную связь, как на шинном подключении в центральной точке. Концентратор выступает в качестве центральной точки подключения.

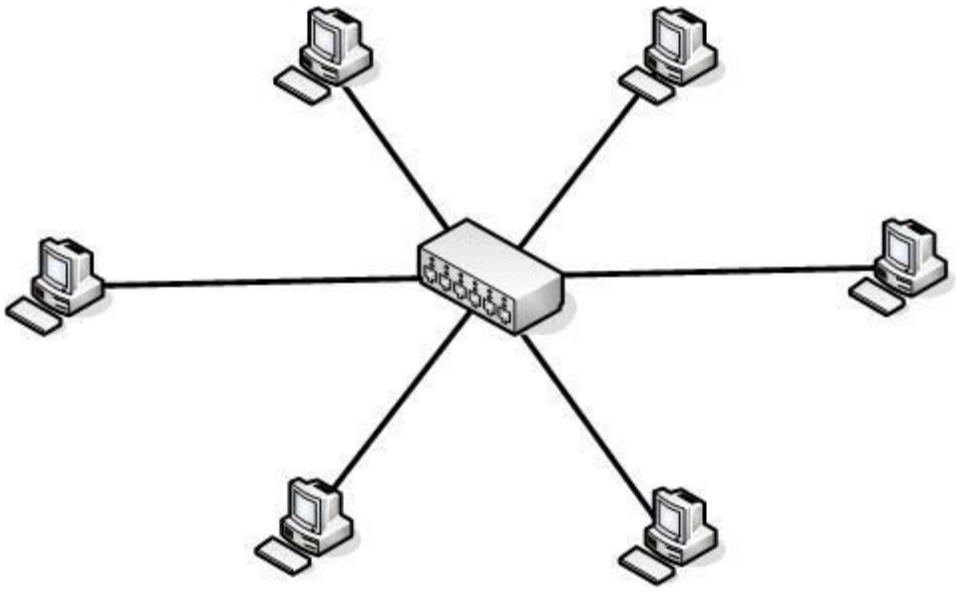


Рисунок 3-16: Подключение с хабом

Когда используется коммутатор, он компенсирует одно из слабых мест топологии шины. Переключатель добавляет контроль трафика по буферизации передачи в порту, тем

самым избегая большинства столкновений. Порты коммутатора можно настроить так, что они действуют как единый сегмент кабеля для целей адресации.

Кольцо

В кольцевой топологии, выход одного узла является входом следующего узла в истинной шлейфовой конфигурации. Каждый узел действует как повторитель, повышая сигнал при передаче к следующему узлу в цепочки.

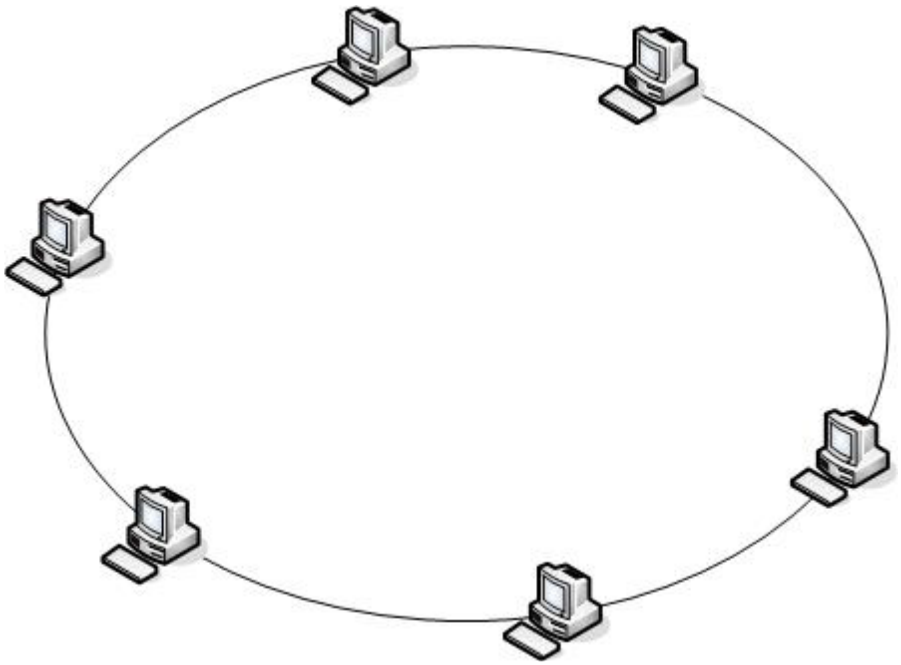


Рисунок 3-17: Топология Кольцо

Протокол от IBM Token Ring использует кольцевую топологию. Пакет данных, известный как маркер, передается от узла к узлу по сети. Узел может загрузить маркер с данными, который передается по всему сегменту, пока не достигнет своей цели. В этот момент, данные выгружаются из маркера и пустой маркер и передается к следующему узлу.
Некоторые топологии "Кольцо" используют двойное кольцо, то есть, два кольца, которые посылают сигналы в противоположных направлениях. Это дает возможность кольцу работать так, чтобы компенсировать разрыв или неисправный узел до тех пор, пока проблема не будет устранена.

Сетка(Сеть)

В полной сетке (рис 3-18), каждый узел в сети связан с каждым другим узлом. Нет центрального узла в данной конфигурации, так же как нет никакого центрального узла в звездной конфигурации. Она предоставляет несколько каналов связи для передачи данных. Она также требует протокол, который управляет маршрутами принятых данных, чтобы избежать петли. Трафик через эти петли, если он не тщательно

контролируется, может привести к поломке сети связи из-за широковещательных штормов.

Петля

- путь связи, где данные идут по кругу без конечного пункта назначения.

Широковещательные штормы

- ситуация, в которой трансляций неоднократно повторно отправляется, потребляя ресурсы сети и предотвращая доставку нормального сетевого трафика.

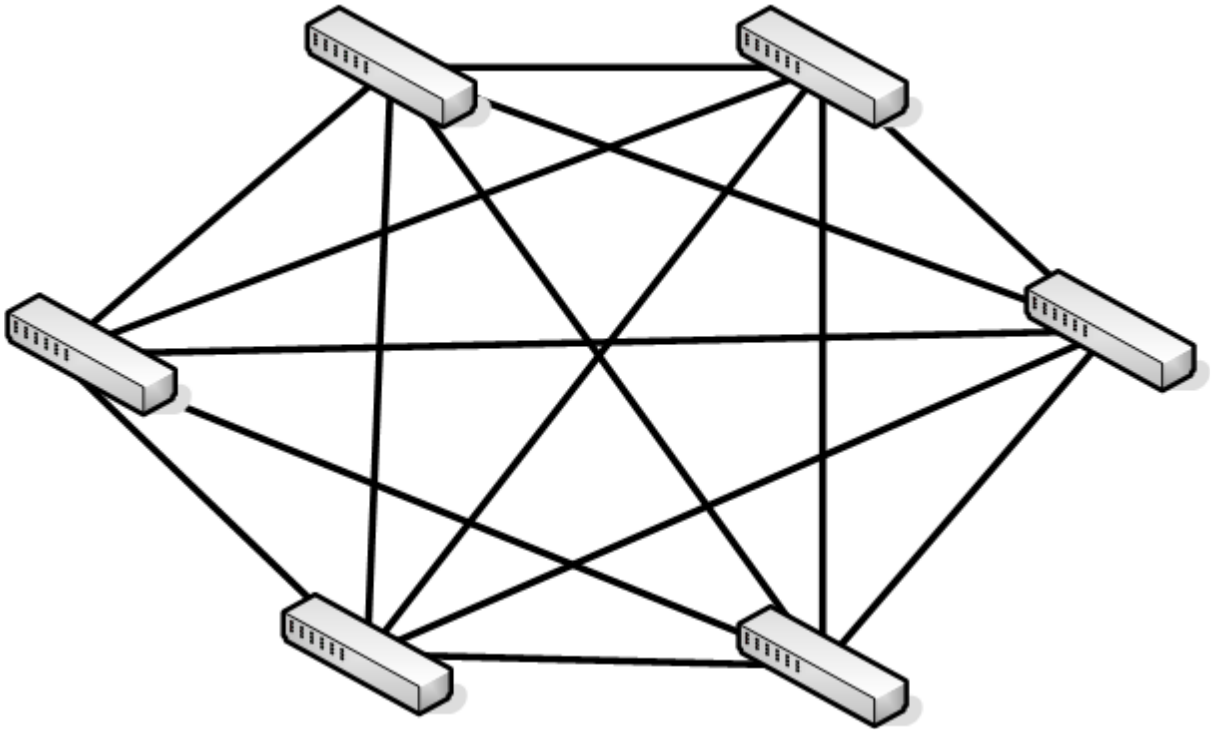


Рисунок 3-18: Сетка сеть

Один из преимуществ этой топологии является то, что она может компенсировать неудачи. Многочисленные соединения позволяют маршрутизацию данных по всем отсутствующим узлам или разрывам в соединительной кабельной системы. Самый известный пример частичтой сети является Интернет с его бесчисленными связями. Во многих случаях, это более ограниченные сетки или частичное сетки (рис 3-19), а не полностью подключенная сеть.

Частичная сетка

-топология сети, где некоторые узлы не подключены к любым другим узлам.

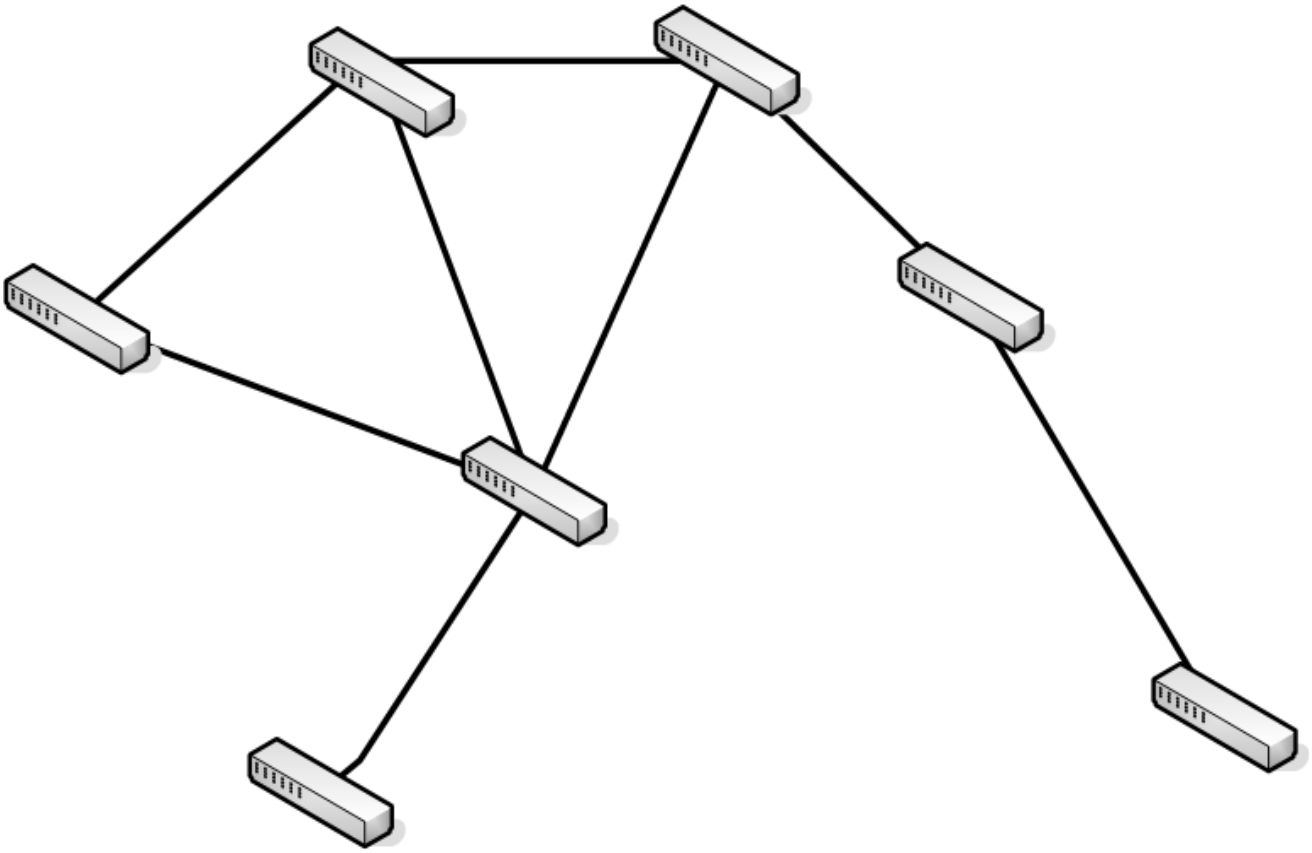


Рисунок 3-19: Частичная сетка

Даже в частичной сетке, все еще существует возможность создания бесконечного цикла.

Обзор безопасности проводной сети

Важной частью любого развертывания сети является предоставление надлежащей безопасности для сети, его компьютеров, и его данных. Большинство мер безопасности реализованы на более высоких уровнях в OSI модели, но есть некоторые вещи, которые можно сделать в кабельной системе.
Вы должны защитить физическую сеть, чтобы предотвратить от несанкционированного перехвата в сети кабельной системы. Открытый кабель должен быть сведен к минимуму. Если ваш объект имеет монтажный шкаф, вам необходимо держать его обеспечение на все время. Вы также должны периодически инвентаризировать сети, чтобы убедиться, что там не было никаких посторонних (и, возможно компрометирующих) изменений.
Вы также должны защищать средства доступа к сети от внешнего мира. Чуть позже в этой главе мы объясним, как реализовать эти меры безопасности.

Беспроводная сеть

Есть большая вероятность, что вы уже используете беспроводную сеть, возможно, даже не осознавая этого. Беспроводные коммуникации являются обычным явлением и для сотовых телефонов системы обеспечивают почти всемирный охват. Системы топологии сетка беспроводной сети с вышек сотовой связи обеспечивают покрытие в большинстве районов.

Беспроводные компьютерные сети теперь стали обычным явлением. Они являются наиболее популярным способом общения в доме, потому что нет необходимости запускать физическую кабельный систему и они пользуются популярностью во многих офисах, особенно из-за их гибкости и относительной легкостью управления. Вы даже можете найти публичные сети Wi-Fi в местах, где люди собираются, таких как библиотеки, колледжи и рестораны (рис 3-20).

Рисунок 3-20: Символ бесплатного Wi-Fi

Wi-Fi точки доступа находятся даже в самых неожиданных местах, например в прачечных. В некоторых городах даже по всему городу есть Wi-Fi, чтобы обеспечить всех граждан бесплатным доступом в Интернет. Новые технологии Wi-Fi и обновленные сетевые устройства выдвигаются на постоянной основе, постоянно расширяя возможности беспроводных сетей.

Горячая точка

- место с беспроводным подключением Wi-Fi.

Вы уже познакомились с беспроводным стандартом 802.11 ранее. Современные беспроводные устройства предназначены для поддержки 802.11n, но в состоянии также поддерживать устройства, которые имеют 802.11a/b/g беспроводные адаптеры. Таким образом, вы можете продолжать использовать старые беспроводные устройства без их модернизации.
Есть несколько потенциальных преимуществ, доступных через беспроводные сети, в том числе:

Простота развертывания

Требования к оборудованию минимальны и нет, как правило, нет необходимости, чтобы прокладывать кабель.
Поддержка мобильных пользователей

Мобильные пользователи или пользователи, которые находятся в офисе, периодически могут легко подключаться к офисной сети.
Взаимосвязь с проводной сетью

У вас есть возможность подключения беспроводных сетевых клиентов с проводной сетью, давая им полный доступ к сетевым ресурсам.

Иногда ограничения, которые требуются, чтобы использовать беспроводную сеть являются законными, а не физическими. Например, вы могли бы быть настроить сеть в историческом здании и юридически запретить делать физические изменения или запуск компьютерного кабеля.

Беспроводные сетевые конфигурации

Для устройства что бы использовать беспроводную сеть необходим беспроводной адаптер. Почти все мобильные компьютеры и смартфоны (многие ноутбуки, планшеты и т.д.) имеют встроенный Wi-Fi адаптер. Многие настольные компьютеры имеют встроенный Wi-Fi адаптер. Есть также различные стили беспроводных адаптеров которые легко доступны.

Рисунок 3-21: USB Wi-Fi адаптер

Хотя вы можете найти беспроводные адаптеры, которые устанавливаются в качестве расширения, они являются более распространенным, выглядят они в качестве устройств, которые подключаются к свободному USB порту (рис 3-21).
Есть два основных варианта конфигурации, поддерживаемые для беспроводных сетей:

Одноранговый режим

Режим инфраструктуры

Выбор режима зависит от ваших требований к сети. Рабочий режим настраивается с помощью свойств беспроводного адаптера.

Одноранговый режим

Одноранговый режим, также известный как режим точка-точка, это самая простая конфигурации для реализации, но не подходит для большинства сред SMB. На самом деле, одноранговая иногда неуместна даже для домашних сетей.

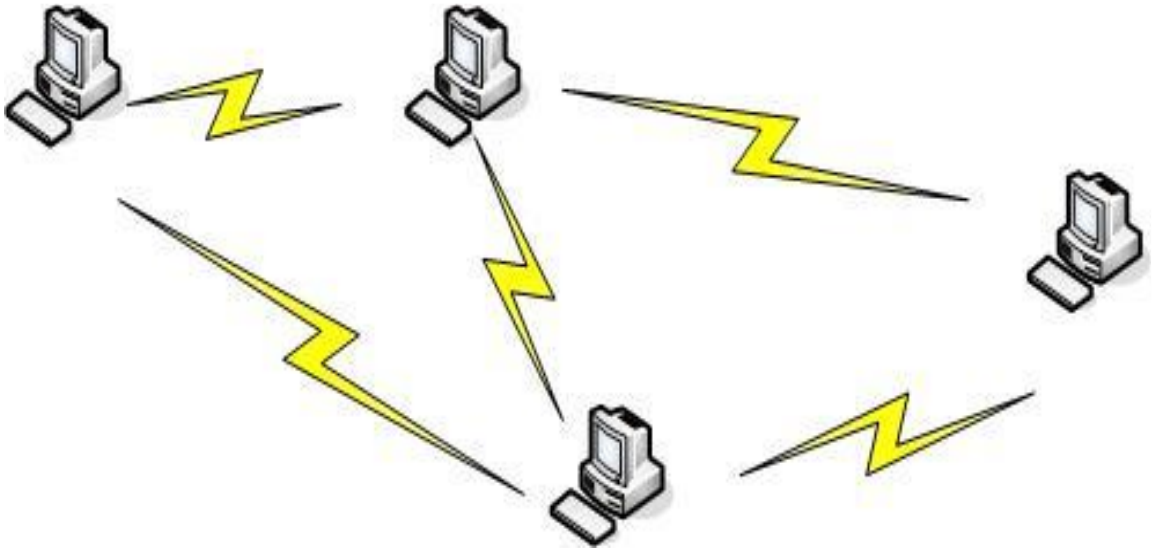


Рисунок 3-22: Режим одноранговая сеть

В одноранговом режиме, беспроводные устройства напрямую общаться друг с другом. Это позволяет устройствам обмениваться файлами и другими ресурсами друг с другом, но не с другими проводными сетевыми устройствами.
Одноранговая сеть ограничивается не более чем девяти клиентскими устройствами. Два устройства должны быть в пределах диапазона покрытия друг от друга, чтобы совместно использовать ресурсы. Там нет организованного метода для преодоления или ретрансляции данных между устройствами. Вы обнаружите, что эффективные конфигурации беспроводной безопасности основаны вокруг использования точки доступа (AP) в качестве центрального контактного пункта для беспроводной связи.

Точка доступа (AP)
- центральный пункт связи для беспроводных сетей. Точка доступа обеспечивает связь между беспроводными устройствами и может поддерживать связь к проводной сети.

Инфраструктурный режим

В стандартной конфигурации для большинства беспроводных адаптеров, поддерживается только инфраструктурный режим . В режиме инфраструктуры беспроводные устройства взаимодействуют через AP (рис 3-23), а не общаться друг с другом напрямую.

Рисунок 3-23: MSM422 точка доступа

Инфраструктурный режим требует по крайней мере одну точку доступа и один компьютер (или другое беспроводное устройство). Конфигурация может включать в себя несколько точек для расширения диапазона сети. Вы также можете подключить AP к проводной сети, чтобы дать беспроводным клиентам доступ к проводным сетевым ресурсам (рис 3-24).

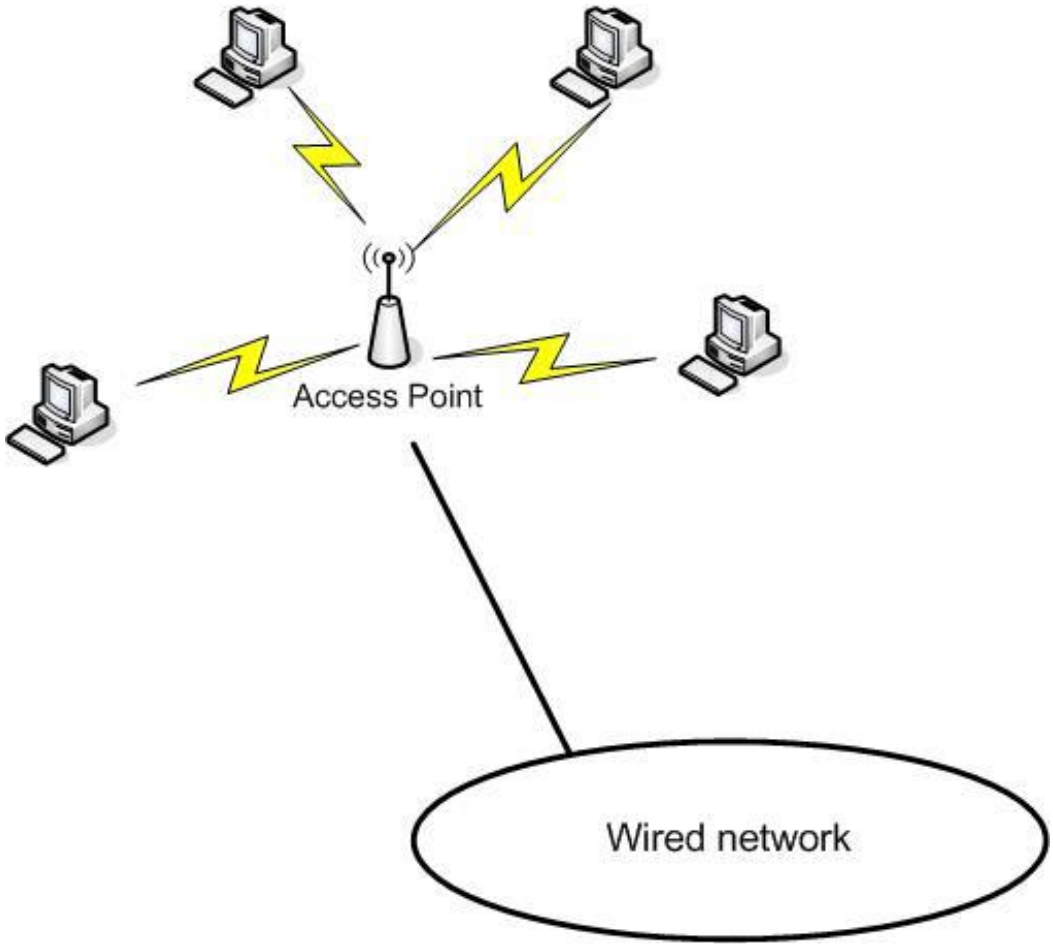


Рисунок 3-24: AP Подключается к проводной сети

Не только эта конфигурация наиболее подходящая для большинства нужд малого и среднего бизнеса, это также самая популярная конфигурация для домашних сетей. Одна из основных причин по которой многие люди используют эту конфигурацию для домашней сети, это то что она позволяет им использовать подключение к Интернету с высокой пропускной способностью с их беспроводных устройств.

В дополнение к компьютерам, домашние сети часто включают в себя принтеры, сканеры и развлекательные устройства, такие как игровые приставки, телевизоры, DVD-и или Blu-Ray проигрыватели дисков. Эти устройства часто предназначены для связи через сеть стандарта Wi-Fi.

Обзор безопасности беспроводной сети

Общей проблемой беспроводных сетей является то, что вы могли бы обеспечивать горячую точку для незнакомцев. Один из способов, который обнаруживает незащищенные или слабо защищенные беспроводные сети это вардрайвинг.

Вардра́йвинг (англ. Wardriving)
— процесс поиска и взлома уязвимых точек доступа беспроводных сетей Wi-Fi человеком либо группой лиц, оснащенных переносным компьютером с Wi-Fi-адаптером. При этом для пространственного поиска и локализации точки используется транспортное средство (отсюда и название — боевое вождение).

Если ваша сеть обнаружена через вардрайвинг, вы можете стать жертвой вархакинга. Если да, то вы найдете этот символ написанный мелом на тротуаре возле вашего офиса:

Рисунок 3-25: Символ вархакинга

Вархакинг

- маркировка доступных беспроводных сетей мелом.

Это символ указывает на незащищенное Wi-Fi соединение, открытое приглашение для людей, чтобы воспользоваться вашей беспроводной сети и, чаще всего, вашей интернет-связь. Как минимум, это может ухудшить производительность сети. В худшем случае, это выставит ваши сетевые ресурсы злоупотреблению и потерям. Несанкционированные пользователи могут украсть или удалить общие данные.

Стандарты 802.11 и 802.1X определяют несколько параметров безопасности, чтобы помочь вам защитить вашу сеть. Реализация этих стандартов не всегда гарантирует, что ваша сеть будет оставаться в безопасности, но они будут проходить долгий путь к защите. Это не мешает вархакингу. Это, тем не менее, изменит статус вашей сети из незащищенного Wi-Fi в защищенный Wi-Fi (рис 3-26).

802.1X - беспроводные стандарты сетевой безопасности.

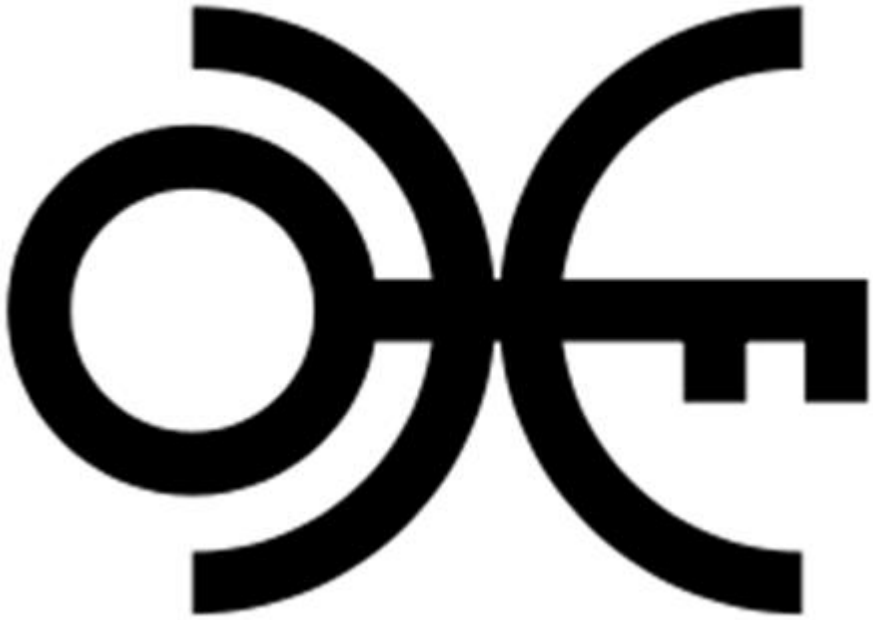


Рисунок 3-26: Защищенный Wi-Fi

Доступные опции безопасности включают в себя:

Фильтрация MAC-адресов

Позволяет или блокирует доступ к точке доступа, основанного на MAC-адресе клиентского компьютера. Это легко обойти, подделкой MAC-адресов.
Wired Equivalent Privacy (WEP)

Метод шифрования данных, используемый для шифрования данных, передаваемых между беспроводными узлами. Шифрование легко взламывается и поэтому не рекомендуется для использования в любом приложении.

Wi-Fi Protected Access (WPA)

Временная аутентификации и шифрование стандартов предназначенных для замены WEP и исправить некоторые из его более важных недостатков.

Wi-Fi Protected Access 2 (WPA2)

Стандарт 802.11i, определяющийся улучшенной сетевой аутентификацией и шифрованием.

Подмена адреса

-процесс настройки несанкционированного компьютера с адресом, который является действительным, авторизированный адрес целевой сети.

Эти защитные и шифровочные методы предназначены для использования с другими методами обеспечения безопасности сети, например, требуя аутентификация пользователя для доступа к сетевым ресурсам, установка безопасности доступа к файлам и другим ресурсам, войдя в сетевую активность, и так далее.

Гибридные сети

Многие сети лучше всего охарактеризовать как гибридные сети, объединяющие различные топологии и даже различные коммуникационные технологии в единое целое. Это становится все более распространенным, так как сети становятся все больше и больше взаимосвязаны.

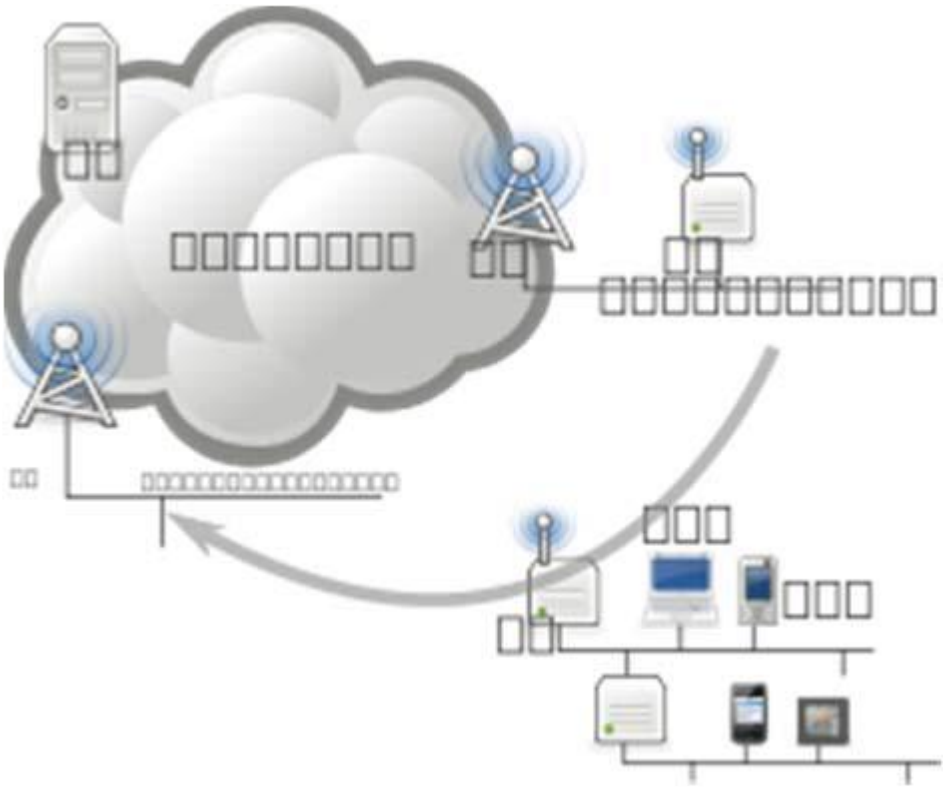


Рисунок 3-27: Гибридная сеть

Очень маленькую сеть Ethernet можно сконфигурировать как одиночную звезду. Поскольку сеть расширяется и сегментируется, она могла бы стать группой шинных сетевых сегментов, соединенных в качестве частичной (или полной) петли. Сеть становится еще более сложной и более гибридной конфигурацией, когда вы добавляете в нее беспроводные сегменты или широкие области связи (рис 3-27).

Задача: GoShop, Inc.

GoShop переместила свою административную и складское в единое место. Это помогло им консолидировать деятельность и значительно сократить их операционные затраты. Место в настоящее время подключен с CAT 6 витая пара подключении к коммутатору уровня 2, физически находящемся в коммутационном шкафу на складском этаже.
Складской персонал жалуется, что выполнение заказов стало слишком громоздким и кропотливым. Они должны либо распечатать копии заказов клиента, отмеченные пункты, а затем генерировать документы к окончательному заказу, или бежать туда обратно к компьютерам расположенным в передней части склада, так как они собирают детали для каждого заказа отдельно.

Обсудить варианты оптимизации процесса наполнения склада заказа.
Какие изменения инфраструктуры будут необходимы для поддержки мобильных ручных компьютеров для складского персонала? Включите все необходимое оборудование и потенциальные проблемы.

Основные сетевые технологии

Мы закончим эту главу с краткого обсуждения некоторых технологий и концепций, которые имеют решающее значение для понимания современных сетевых инфраструктур. Обсуждение призвано служить только в качестве обзора предмета. Эти темы будут рассмотрены более детально в более позднее время на протяжении этого курса.

Сегментация сети

Вы уже имели некоторое введение в идеи сегментации сети. Есть несколько причин, почему вы могли бы рассмотреть сегментации сети, в том числе:

Оптимизация сети связи

Улучшение управления потоком сетевого трафика

Повышение безопасности управления сетью

Есть два основных метода, используемых для сегментации сети, подсетей и виртуальных локальных сетей (рис 3-28). Один из самых существенных различий между ними состоит в том подсети реализуются на уровне 3 модели OSI в, но VLAN, реализуются на уровне 2.

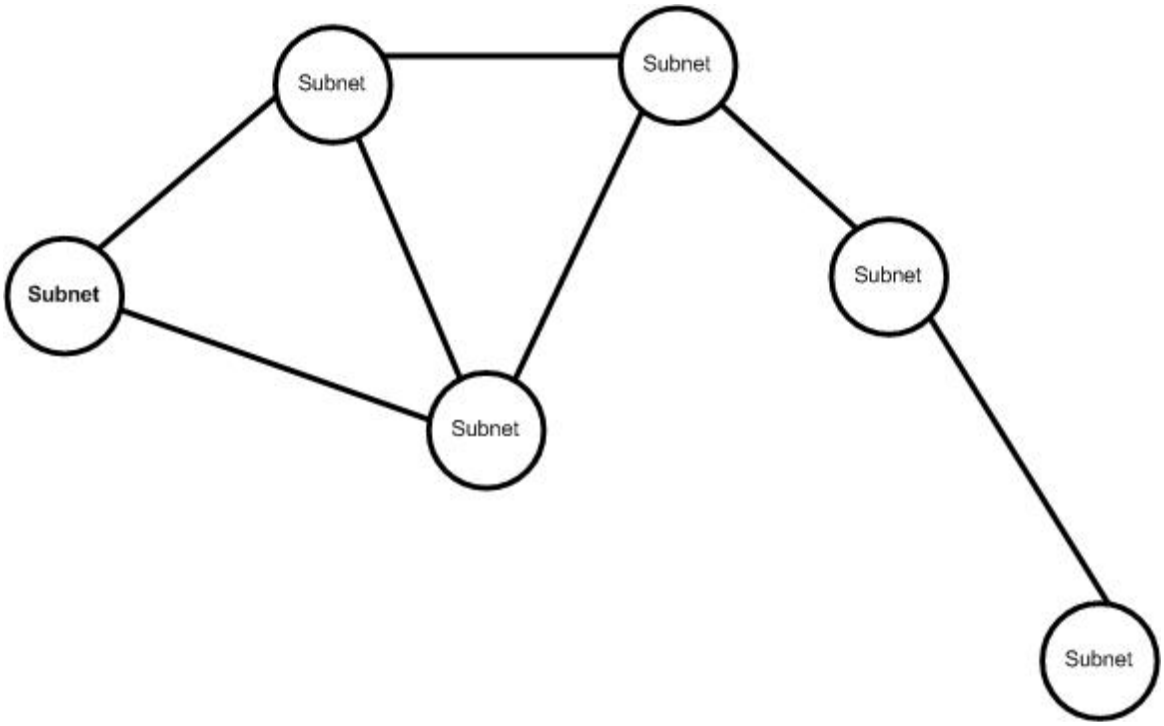


Рисунок 3-28: Несколько подсетей

Маршрутизаторы и коммутаторы маршрутизации требуется при использовании подсетей в сегменте сети. Каждая подсеть должна иметь разный сетевой адрес. При использовании VLAN, коммутатор используются для сегмента сети, а сегментация обычно портом. Сеть VLAN может быть составлена из портов, назначенных от одного коммутатора или состоять из портов, собранных из нескольких коммутаторов. Каждая сеть VLAN будет иметь разный идентификационный номер и другой присвоенный IP-адрес. Сеть VLAN может быть связана с множеством подсетей (рис 3-29).

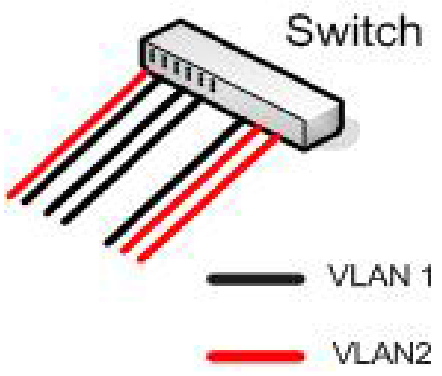


Рисунок 3-29: Коммутатор с двумя VLAN

Сети VLAN стали популярным вариантом сегментации для локальных сетей. Маршрутизаторы по-прежнему являются основным средством сегментации более широкой области.

Периметр сети

Один специализированный тип сегментации сети периметра. Сетевой периметр защищенной подсети, что находится между внутренней локальной сетью и внешним миром, в частности в Интернете. Термин ДМЗ иногда используется, чтобы обратиться к демилитаризованной зоне или экранированной подсети.

Экранированная подсеть
- подсеть изолирована от остальной части сети с трафиком в и из сети фильтруется.

Демилитаризованная зона (ДМЗ)
- в контексте сети, относится к подсети экранированной одним или несколькими межсетевыми экранами.

Сначала нужно ввести понятие брандмауэра. Брандмауэр представляет собой устройство безопасности, которое может фильтровать трафик в или из сети периметра. Брандмауэр может быть отдельным, специализированного устройством или, чаще всего, осуществляться через функциональные возможности, предоставляемые в маршрутизаторе. Брандмауэр действует по фильтрации трафика, что позволяет пройти в любом направлении, как показано на рисунке 3-30. Таким образом, вы можете ограничить трафик на определенные виды связи, блокировать доступ потенциально опасных приложений, и даже устанавливать ограничения на информацию источника и адрес назначения.

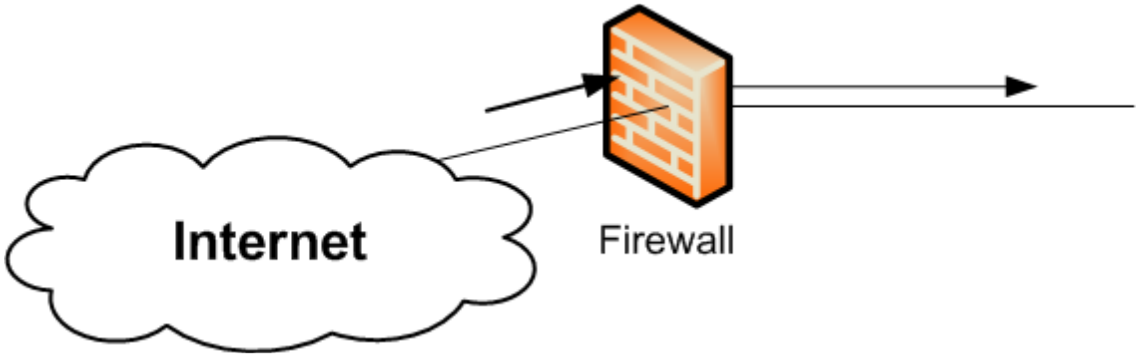


Рисунок 3-30: Брандмауэр

Личные брандмауэры, защищающие один компьютер, также распространены. Они часто реализуются с помощью операционной системы. Персональный брандмауэр фильтрует трафик в и из компьютера, на котором он сконфигурирован.

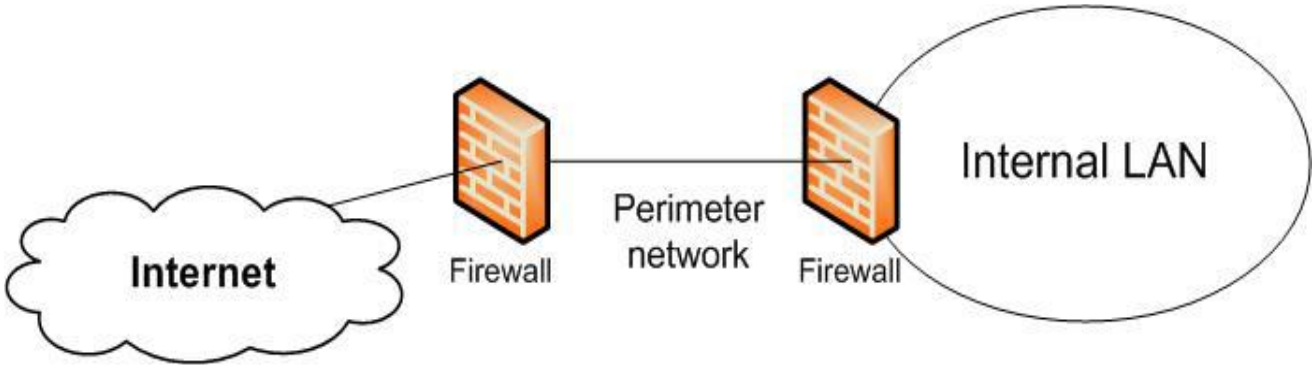


Рисунок 3-31: Периметр сети

Периметр сети выступает в качестве буфера, чтобы защитить вашу сеть. Он предназначен для предотвращения несанкционированного доступа в сети, а также целенаправленные нападения. Одна конфигурация общего сетевого периметра имеет периметр сети, ограниченный с обеих сторон брандмауэрами, как показано на рисунке 3-31.

Основная цель сети периметра, что она дает вам место, чтобы развернуть устройства, которыми вы хотите поделиться с миром в целом. Например, если вы хотите иметь общедоступный веб-сайт и разместить на своем веб-сервере, вы должны развертывание веб-сервера в демилитаризованной зоне. Таким образом, вы сделали бы его доступным для Интернет, не подвергая всю сеть для общественности.

Скрытые подсети

Вы можете увидеть внутренние изменение сети на сети периметра, которое называют просто скрытой подсетью. В этом случае, подсеть является частью вашей внутренней сети, но граница в подсети защищена брандмауэром, как показано на рисунке 3-32. Брандмауэр фильтрует все передачи в и из подсети.

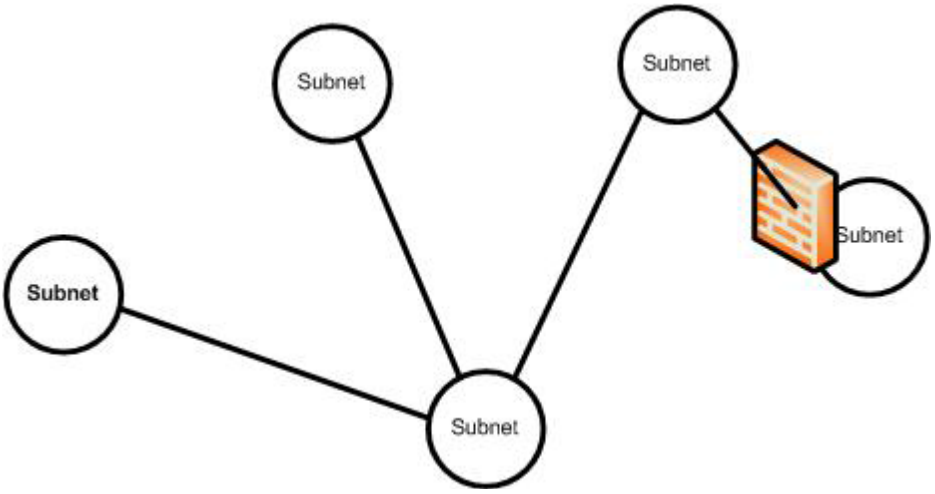


Рисунок 3-32: Скрытая подсеть

Одной из причин для конфигурирования вашей сети этим способом является то, что это обеспечение дополнительной безопасности для компьютеров, размещенных в экранированной подсети. Она также позволяет указать жесткий контроль над пользователями (и какие приложения) могут иметь доступ к ресурсам в защищенной подсети.

Прокси

Один тип специализированного сервера, который вы можете найти в сети периметра, является прокси-сервер. Вместо того, чтобы позволить клиентским компьютерам внутренней сети доступ к серверам напрямую, их запросы обрабатываются через прокси-сервер. Клиенты могут получить доступ к прокси-серверу, проходя через следующие этапы:

Клиент делает запрос к прокси-серверу.

Прокси-сервер запрашивает Интернет-ресурс и извлекает результат.

Прокси-сервер передает результат запрашиваемый клиентом.

Процесс невидим для пользователя, чтобы ничего не указывало что они имеют доступ к Интернету через дополнительное устройство. Использование прокси-сервера позволяет повысить безопасность сети. Он также добавляет слой административного контроля, позволяя вам ограничить доступ пользователей к веб-сайтам, которые вы не хотите что бы их просматривали. Прокси-сервер может сканировать исходящий трафик, а также, как способ предотвращения потерь данных или раскрытия.
Прокси-серверы также помогает уменьшить объем трафика между сетью и Интернетом. Информация извлеченная из Интернета попадает в буфер на прокси-сервер. Если другой клиент запрашивает ту же самую информацию, то она читается из буфера прокси-сервера, а не ищется заново в Интернете.

Преобразование адреса

Перевод адреса еще одна важная технология, когда устройству во внутренней сети необходимо получить доступ к внешнему миру. Чем больше информации потенциальный злоумышленник сможет собрать о вашей локальной сети, тем легче ему или ей будет взломать вашу сеть.

Взлом
- в этом контексте, несанкционированного доступа в сеть и к ее ресурсам.

Таким образом, вы всегда должны скрывать IP-адреса компьютеров в локальной сети. Вы также должны часто использовать личные IP-адреса для конфигурации внутренних хостов. При использовании частных IP-адресов, вы должны использовать трансляцию адреса при доступе к Интернету.

Частные IP-адреса
- IP диапазоны адресов, которые могут быть назначены в качестве внутренних адресов LAN, но не могут быть использованы для общения в Интернете.

Вы можете скрыть IP-адреса локальных компьютеров и использовать личные адреса в вашей сети с помощью сетевых адресов (NAT) сервера или сетевого порта и Address Translation (PAT или NAPT) сервер. NAT-сервер заменяет действительный адрес Интернет на хостовый адрес. Когда ответ возвращается, он направлен на хост. NAPT или PAT сервера используют те же адреса для всех хостов ИТ-услуг и отслеживают, исходящие хосты путем присвоения иного TCP или UDP адреса порта для каждого. Использование NAT или PAT также дает вам дополнительный контроль над фильтрацией порта на ваши брандмауэры, потому что вы можете указать неиспользуемые порты что бы потенциальный злоумышленник не мог войти в вашу сеть. Как с прокси-сервером, процесс является прозрачным для пользователя.

Виртуальная частная сеть (VPN)

VPN-предназначена для обеспечения безопасной, надежной связи менее безопасных средств массовой коммуникации. Наиболее распространенным использование VPN является обеспечение безопасной связи между двумя удаленными узлами, используя Интернет в качестве носителя. С VPN, сеанс связи устанавливается между двумя конечными точками. Два наиболее распространенных сценария LAN-to-LAN связь и компьютер-LAN связь.

Рисунок 3-33: LAN-to-LAN VPN

В связи LAN-to-LAN, вы используете Интернет в качестве канала глобальной связи между локальными сетями, как показано на рисунке 3-33. Этот тип соединения чаще всего является постоянным подключением между локальными сетями. На каждом конце, устройство, как правило, маршрутизатор, сконфигурировано как VPN конечной точки. Связь обычно шифруются только между двумя конечными точками.

Связь компьютер-LAN наиболее часто используется, чтобы обеспечить удаленный пользовательский с доступом к безопасной локальной сети. Компьютер выступает в качестве конечной точки VPN на одном конце. Конечная точка будет создана в конце LAN и примет связь компьютера. Часто, в локальной сети конечная точка будет настроена для поддержки нескольких одновременных подключений VPN. Это часто устанавливается в качестве соединения по требованию, которое не «упадет», когда доступ в Интернет больше не требуется.

Вы можете найти оба типа конечных точек, настроенных на одну локальную сеть. Например, если SMB имеет удаленные офисы, а также удаленных или мобильных пользователей, он может иметь точки для поддержки WAN связи на удаленных местах и конечные точки для поддержки отдельных пользователей.

VPN, основаны на использовании протоколов туннелирования для передачи данных между конечными точками. Конечные точки должны быть способны взаимно аутентифицировать друг друга, когда сеанс связи устанавливается для обеспечения безопасности.

Туннелирование (от англ. tunnelling — «прокладка туннеля» в компьютерных сетях) — процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Туннелирование представляет собой метод построения сетей, при котором один сетевой протокол инкапсулируется в другой.

Глава 4:
Коммутаторы

Введение

Ранее в этом курсе вы уже познакомились с коммутаторами (switches), в том числе с некоторыми процедурами базовой конфигурации. Но сейчас мы возвращаемся к коммутаторам, чтобы более детально рассмотреть их конфигурацию и управление.

Часть нашего внимания будет уделено созданию и управлению основной сетевой безопасности и виртуальных локальных сетей (VLAN), что является основным определением для использования коммутатора многими компаниями. Также мы взглянем по-другому на управление и мониторинг состояния порта. Глава будет включать в себя процедуры для соединения портов и для создания данных с высокой пропускной способностью. Мы узнаем о настройке на сетевом уровне (уровень 3), поддержку маршрутизации в коммутаторе. Закрепим наши знания обсуждением о файлах конфигурации и обновлений программного обеспечения.

В этой главе мы будем использовать CLI (Command Line Interface) и меню интерфейсов для выполнения различных задач управления. Мы делаем так, чтобы дать вам больше опыта работы после изучения каждого из интерфейсов управления.

Цели

В этой главе вы узнаете, как:

Описать распространенные типы переключателей.
Настроить пользовательские сети VLAN.
Управлять IP-адресом для VLAN.
Настроить и управлять сетями VLAN.
Настраивать и управлять портами.
Настраивать агрегацию портов.
Управлять обновлениями программного обеспечения.
Управлять несколькими конфигурациями коммутатора.
Управление коммутатором
Эта глава посвящена процедурам управления коммутатором. Специфика в том, что вы сможете делать, будет напрямую зависеть от коммутатора, они, как правило, могут быть сосредоточены в одном из трех основных категорий:

Неуправляемые коммутаторы (Unmanaged switch)

Полууправляемые коммутаторы (коммутатор с ограниченными возможностями управления, а также известный как веб-управляемый коммутатор - Web Managed Switch)
Управляемые коммутаторы (Managed switch)
Основное внимание мы будем уделять управляемым коммутаторам, или полностью управляемым коммутаторам, которые имеют несколько интерфейсов управления и находятся в широком диапазоне настраиваемых параметров.

Неуправляемые коммутаторы

На нижнем конце доступных коммутаторов есть неуправляемые коммутаторы. Они предназначены для обеспечения связи для небольших сетей. Работают неуправляемые коммутаторы строго на уровне 2 модели OSI. Они имеют ограниченное количество портов, обычно не более 24 (чаще 8 или 16), и нет настраиваемых параметров.

Неуправляемые коммутаторы имеют явное преимущество, если вы хотите создать сеть для малого бизнеса. А все потому, что им присущи не управляемые параметры, так называемое «plug-and-play» (это характеристика устройства, под которой понимают возможность пользованием устройства сразу после подключения и без установки дополнительных драйверов). Подключите коммутатор в розетку, а затем подключите сетевые устройства к нему, и все работает. Неуправляемые коммутаторы обеспечивают основные функциональные возможности, которые можно было бы ожидать на этом уровне, например, возможность буферного трафика, чтобы избежать столкновения, но нет поддержки для более продвинутых функций.

Неуправляемые коммутаторы также не предоставляют никакой информации по сети, только информацию по индикаторам. Вы сможете, как правило, сказать, глядя на состояние индикаторов, обнаружил ли порт подключённоее устройство и есть ли любая деятельность в порту. Вы также можете сказать с какой скоростью эксплуатируется порт и посмотреть дуплексные настройки подключенных устройств.

Но запомните! Вы не сможете создать VLAN на неуправляемому коммутаторе.

Полууправляемые коммутаторы

Полууправляемые коммутаторы, также известны как веб-управляемые коммутаторы (Web Managed Switch), поддерживают ограниченные возможности управления. Однако, они являются более продвинутыми устройствами, чем неуправляемые коммутаторы и обладают дополнительной функциональностью.

Как и неуправляемые коммутаторы, большинство полууправляемых коммутаторов имеют фиксированную физическую конфигурацию. Большинство полууправляемых коммутаторов предоставляют функции на канальном уровне модели OSI, а небольшое

их количество включают некоторую функциональность на сетевом уровне, включая поддержку маршрутизации IP-адреса. Поддержка маршрутизации обычно ограничивается только статическими маршрутами.

Статический маршрут (static route) - вручную настроен маршрут с IP-адресом назначения и маршрутной информацией.

Как и неуправляемые коммутаторы, полууправляемые коммутаторы могут быть, как правило, развернуты как «plug-and-play» устройства, использующих конфигурации рлдууправляемых коммутаторов по умолчанию. Доступ к более продвинутой функциональности, однако, нуждается в пользовательских настройках.

Полууправляемые коммутаторы обеспечивают явные преимущества перед неуправляемыми коммутаторами. Например, полууправляемые коммутаторы имеют доступ к управлению через интерфейс управления на основе браузера, который позволяет смотреть статистику по портам и управлять пользовательскими настройками. Еще одним преимуществом является то, что полууправляемые коммутаторы включают поддержку VLAN. Вы также сможете настроить агрегацию каналов, чтобы обеспечить данные с высокой пропускной способностью. Агрегация каналов (link aggregation) – объединение нескольких физических сетевых подключений параллельно, как один логический путь связи, чтобы обеспечить более высокую пропускную способность и резервирование.

Полууправляемые коммутаторы не обязательно ограничиваются веб-интерфейсом. Большинство коммутаторов этого типа также имеют разъем RJ-45. Некоторые из них также имеют соединение USB, которое может использоваться для прямого подключения к коммутатору. Это аналогично соединению консоли на управляемых коммутаторах, но также может быть использовано для выполнения тех же процедур, как веб-интерфейс.

Полууправляемые коммутаторы также включают ограниченную поддержку SNMP. SNMP устройства управления могут автоматически обнаружить и удаленно контролировать полууправляемые коммутаторы. Тем не менее, полууправляемые коммутаторы не поддерживают дистанционное управление с устройства управления SNMP.

Simple Network Management Protocol (SNMP) - протокол TCP / IP для удаленного мониторинга и управления сетевыми устройствами.

Управляемый коммутатор

Мы уже ранее познакомились с управляемыми коммутаторами. Большинство из них построены на модульной конструкции, что позволяет расширить их, если есть необходимость. Управляемые коммутаторы поддерживают функциональность на канальном уровне модели OSI, а также обеспечивают широкий спектр функциональных возможностей сетевого уровня (такие как динамическая маршрутизация).

Динамическая маршрутизация (dynamic routing) - поддержка динамических обновлений в сети направлений и маршрутов для обеспечения изменений в доступных маршрутах и условий сети.

Управляемые коммутаторы поддерживают различные пользовательские настройки управления, в том числе:

CLI – интерфейс командной строки (консольный порт или по сети)
Интерфейс меню (консольный порт или по сети)
Веб-интерфейс (только через сеть)
Кроме того, большинство управляемых коммутаторов могут быть проверены и настроены через SNMP и консоль управления SNMP. Это не только предоставляет дополнительные возможности управления, кроме этого вы также можете установить порог значения, так что устройство управления SNMP может предупредить вас о ситуациях, которые могут потребовать прямого вмешательства.

Такие продукты, как ProCurve Manager (PCM) являются примерами управления SNMP консолей, которые позволяют вам видеть подключенные устройства и деятельность движения.

Большинство управляемых коммутаторов разработаны для работы с протоколом SNMP. Таким образом, устройство управления знает, какая информация доступна на коммутаторе и какие виды деятельности удаленного управления он поддерживает.

Management Information Base (MBI) информационная база управления – совокупность информации управления об устройстве для использования с управлением SNMP.

Настройки размещения коммутатора внутри сети

Когда вы проектируете сеть, важно понять, что вы можете смешивать типы коммутаторов в одной локальной сети. Вы всегда имеете неуправляемый коммутатор, а потом к нему добавляете полууправляемый коммутатор в сеть, и коммутатор расширяется. В зависимости от потребностей, коммутаторы можно подключать непосредственно друг с другом или через маршрутизатор (коммутатор сетевого уровня, выполненный в виде маршрутизатора, как показано на рисунке 4.1).

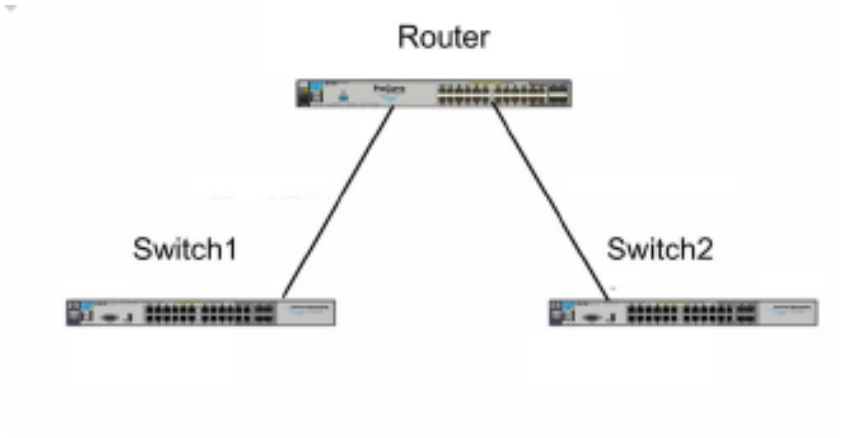


Figure 4-1: Layer 3 Switch Configured as a Router

Рис. 4.1 – Подключение коммутаторов через маршрутизатор

Router (маршрутизатор), Switch1 (коммутатор 1), и Switch2 (коммутатор 2), имена устройств на рисунке 4.1 – коммутаторы.

Коммутатор 1 и коммутатор 2 может быть реализован на уровне 2 модели OSI, но маршрутизатор должен быть также и в конфигурации уровня 3 модели OSI. Вы также можете создать такую конфигурацию для подключения к конечным коммутаторам, использовав раутер вместо коммутатора 3 уровня.

Коммутатор уровня 3 (Layer 3 switch) - переключатель, который поддерживает функциональность уровень 3 модели OSI, в том числе IP-маршрутизацию.

Конечный коммутатор (edge switch) - переключение на границе множества переключателей, соединенных с центральным устройством.

Вы можете развернуть разные типы коммутаторов в различных местах (рис. 4.2). Это позволяет использовать тип, который лучше всего подходит, а также позволяет сэкономить деньги путем развертывания менее дорогих коммутаторов, где дополнительная функциональность не нужна.

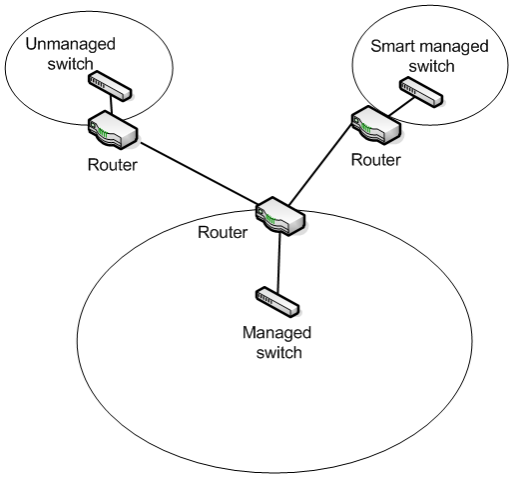


Рис. 4.2 – Пример развертывания

Наряду с потребностями в любой точке, доступность персонала также может быть проблемой. Небольшие удаленные офисы, возможно, не имеют возможности содержать обслуживающий персонал или имеют только вспомогательный персонал, которые проходил минимальное обучение. Тем не менее, даже если никто из персонала не может обеспечить поддержку управления, вы можете рассмотреть полууправляемый коммутатор, ведь коммутатор может быть реализован как удаленный мониторинг, возможны некоторые отдаленные настройки.

Вы также можете смешивать и сочетать различные соединительные устройства, а также развернуть неуправляемые сетевые концентраторы (hubs) вместе с коммутаторами, но это делается редко в современной конфигурации сети. То, что вы, скорее всего, увидите - это сеть с выключателями и беспроводные точки доступа, а также некоторые специальные развертывание приложений, которые имеют коммутаторы, они также работают в качестве точек доступа.

Сетевой неуправляемый концентратор (unmanaged hub) - устройство для объединения компьютеров в сеть Ethernet, который не требует и не поддерживает управление. Устройства подключены по топологии "звезда", но трафик, может быть управляем как в концентраторе при топологии "общая шина".

Виртуальные сети

Подсети и сети VLAN имеют два пути, по которому можно разделить сеть для управления и контроля трафика. Сети VLAN помогают улучшить безопасность сети путем разделения управления, связанного с трафиком от другого сетевого трафика. Например, если сеть поддерживает VoIP, вы можете использовать VLAN для изоляции телефонного трафика из сети данных трафика.

Voice over IP (VoIP) - протокол передачи телефонных сигналов (разговоров) через интернет.

Есть два типа портов (соединений):

Нетегированные (ссылка доступа)
Тегированные (агрегированные соединения)

Нетегированный порт (untagged/access link) - порт связан с сетевым устройством, кроме другого коммутатора.

Тегированный порт(tagged/trunk link) – порт, что связан с другим коммутатором.

Большинство связей – это связи доступа, связи на ПК и другие сетевые узлы устройства. Тегированные соединения также используются для создания связи с высокой пропускной способностью при настройке виртуальной локальной сети с коммутаторами.

Виртуальную локальную сеть можно приравнять к подсети. И VLAN, и подсеть являют собой широковещательный домен. Основная разница между ними в том, что VLAN реализован на уровне 2, а подсеть реализуется на уровне 3. Кроме того, имеет зависимость от местоположения, а VLAN реализуется на основе конфигурации порта.

Простейший тип статического VLAN на основе портов

Членство в сети VLAN зависит исключительно от порта, к которому устройство прилагается.

Статическое определение виртуальной локальной сети включает в себя идентификатор VLAN, имя и связанные с ними порты. Вы также можете включать IP-адрес для VLAN. Это необязательно если вы используете SNMP для сетевого управления. В этом случае, вы должны, по крайней мере, определить IP-адрес для VLAN управления, он должен быть уникальными. Кроме того, если включена маршрутизация на коммутаторе, определяя IP-адрес для каждого VLAN, это позволяет маршрутизировать трафик между VLAN.

Управление виртуальной локальной сетью (management VLAN) – это виртуальная локальная сеть обозначена как VLAN, может быть использована для целей управления коммутатором.

Можно настроить VLAN так, что он будет состоять из портов, расположенных на различных физических коммутаторах. Трафик между портами в той же сети VLAN, даже

если они находятся на разных коммутаторах, соединяется, таким образом, что вещание распространяется через сеть VLAN. Трафик между сетями VLAN направляется, так как широковещательный трафик не пересекает сетей VLAN.Вы также можете иметь динамические конфигурации VLAN на основе различных параметров, такие как вошедшие в использование устройства или MAC-адрес.

Типы виртуальных локальных сетей

В дополнение к управлению трафика путем создания широковещательных доменов, еще одним распространенным использованием сетей VLAN есть умение отделить различные типы трафика от нормального сетевого трафика.

На основе портов VLAN статические типы включают в себя:

По умолчанию
Включает в себя все порты коммутатора, когда находится в режиме по умолчанию. Благодаря этому VLAN осуществляет как и трафик управления, так и стандартный сетевой трафик.
Первичную VLAN
Первоначально, это виртуальна локальная сеть по умолчанию. Вы можете назначить пользовательские VLAN в качестве основного и сделать его ответственным за некоторые функции управления. Для коммутаторов HP, первичная VLAN является единственной VLAN на коммутаторе, которая может принимать генерируемые адреса через DHCP.
Безопасное управление VLAN
При создании в качестве пользовательского VLAN, безопасное управление является изолированной сетью специально для управления коммутатором. Доступ к функциям управления, ограничивается только теми портами, настроенными как безопасные члены управления VLAN. Трафик не может быть направлен к или от этой VLAN.
Voice VLAN
Это виртуальная локальная сеть, которая создается что бы изолировать VoIP трафик от других трафиков.
Это обычная практика, чтобы удалить или переименовать VLAN по умолчанию в целях безопасности. Оставив VLAN по умолчанию, мы можем обеспечить путь для несанкционированного доступа в сеть.

Порт в VLAN может быть тегированным или нетегированным. Тегирование построено на основе стандарта 802.1Q. Один порт может разрешить трафик от нескольких VLAN.

Порт может быть нетегированный для одной виртуальной локальной сети, и при этом может быть тегированным для другой сети (рис 4.3).

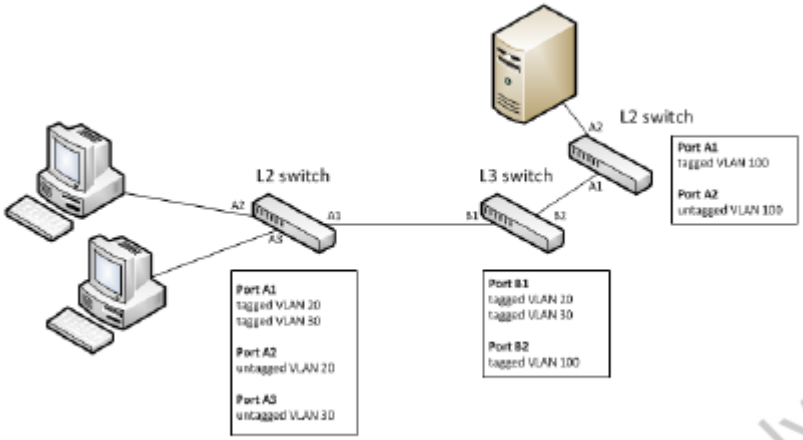


Figure 4-3: Sample Network with Tagged and Untagged VLANs

Рис. 4.3 – Локальная сеть с тегированными и нетегированными портами

Как вы можете видеть, порты A1 и B1 - тегированные порты, которые несут трафик для VLAN 20 и 30 между коммутаторами L2 и L3. Порты A2 и A3 подключают клиентские компьютеры к VLAN, 20 и 30, соответственно, и, таким образом сконфигурирован как нетегированный. Порт B2 на коммутаторе L3 и порт A1 на коммутаторе L2 определяют тегированные порты, которые позволяют осуществляться трафику для VLAN 100 между коммутатором L2 и L3. Нетегированный порт A2 на правому коммутаторе L2 соединяет сервер для VLAN 100.

802.1Q – стандарт для использования тегов VLAN с пакетами Ethernet.

Управление виртуальными локальными сетями

Если коммутатор поддерживает виртуальные локальные сети, то в стандартной конфигурации будет одна виртуальная сеть, к которой привязаны все порты. Она будет иметь индекс VLAN 1. Трафик не сможет маршрутизироваться через VLAN. Чтобы настроить VLAN, вы должны сначала создать новый и удалить порты из VLAN по умолчанию. Любой порт явно не удаляется, а остается частью VLAN по умолчанию.

Основные шаги для создания пользовательского VLAN:

Определите имя и индекс VLAN.
Передача портов от дефолта (или другой) VLAN к новой VLAN
Назначить IP-адрес в сети VLAN (по желанию)
Вы можете выполнять основные шаги для создания VLAN, используя CLI (Command Line Interface) - интерфейс меню или веб-интерфейс. Например, на рисунке 4.4 показана страница веб-интерфейс для управления VLAN.

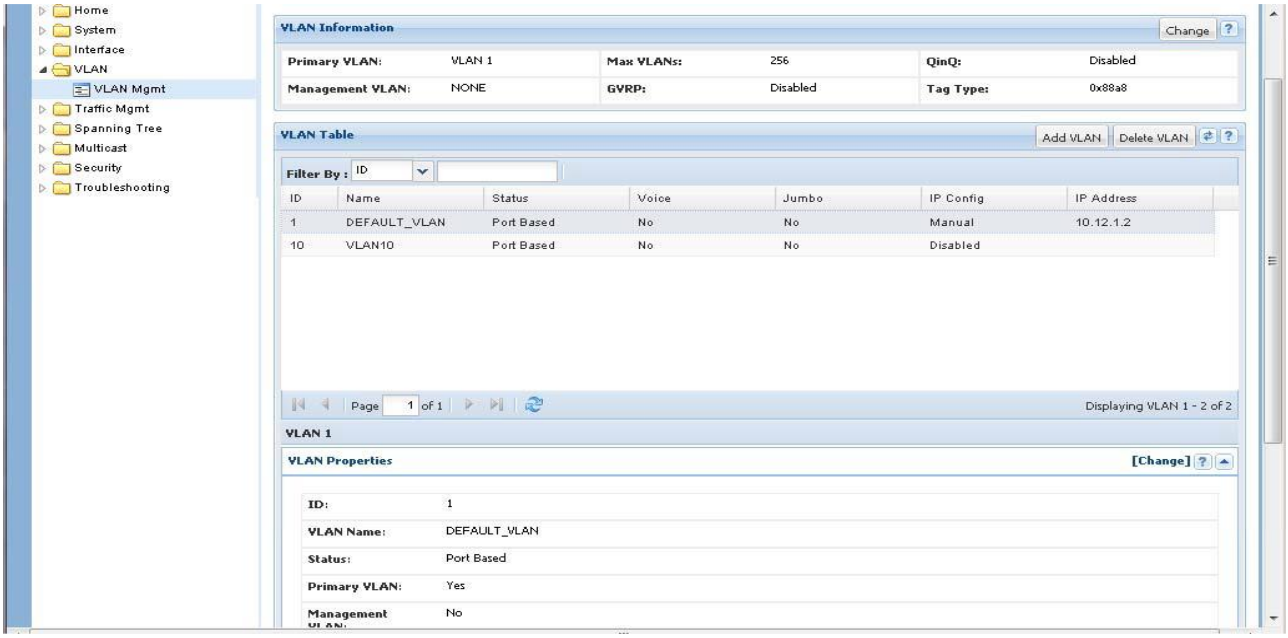


Рис. 4.4 - Страница веб-интерфейс для управления VLAN

Во-первых, мы будем использовать интерфейс меню, чтобы пройти через процесс создания пользовательского VLAN. Запустите интерфейс меню и выберите 2. Switch Configuration из главного меню, чтобы открыть меню конфигурации коммутатора (рис 4.5).

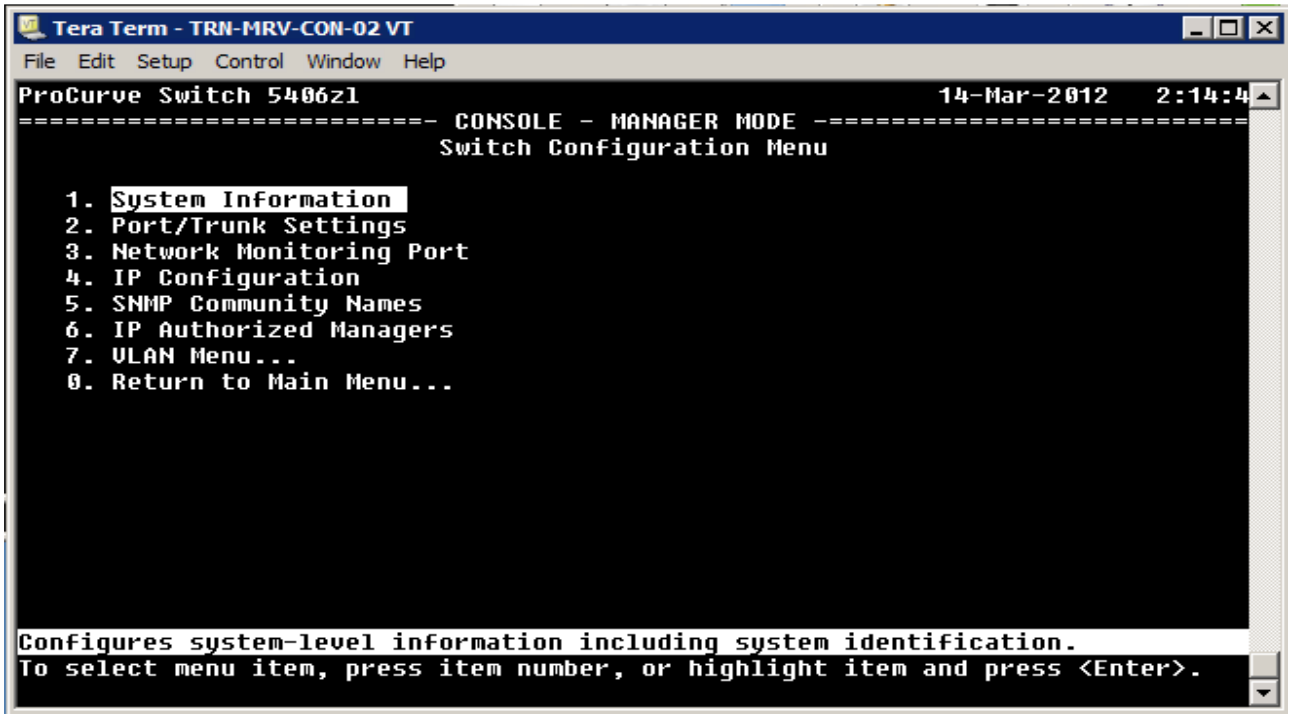


Рис. 4.5 - Меню конфигурации коммутатора

От Switch Configuration Menu, выберите 7. VLAN меню (рисунок 4.6).

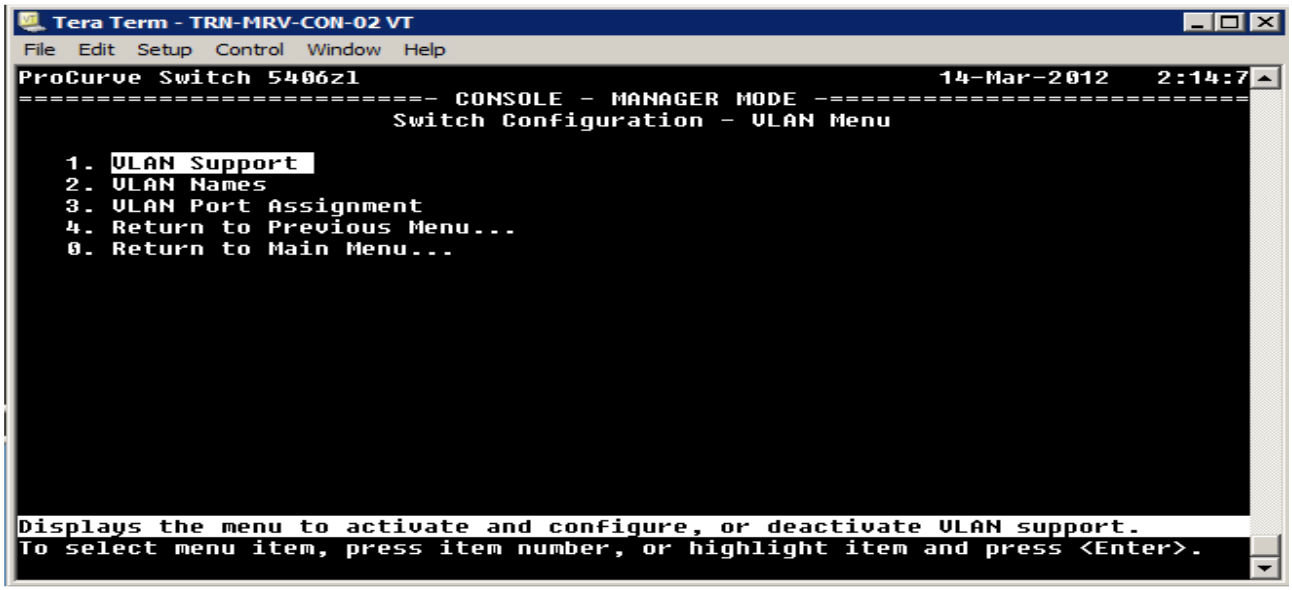


Рис. 4.6 - VLAN меню

Мы начнем с рассмотрения меню опций команд VLAN. Здесь вы можете:

Настраивать параметры поддержки VLAN.
Создавать и управлять именами и идентификаторами VLAN.
Назначать или удалить порты из VLAN.

Начните с выбора 1. VLAN Support, чтобы проверить параметры конфигураций VLAN (Рисунок 4.7).

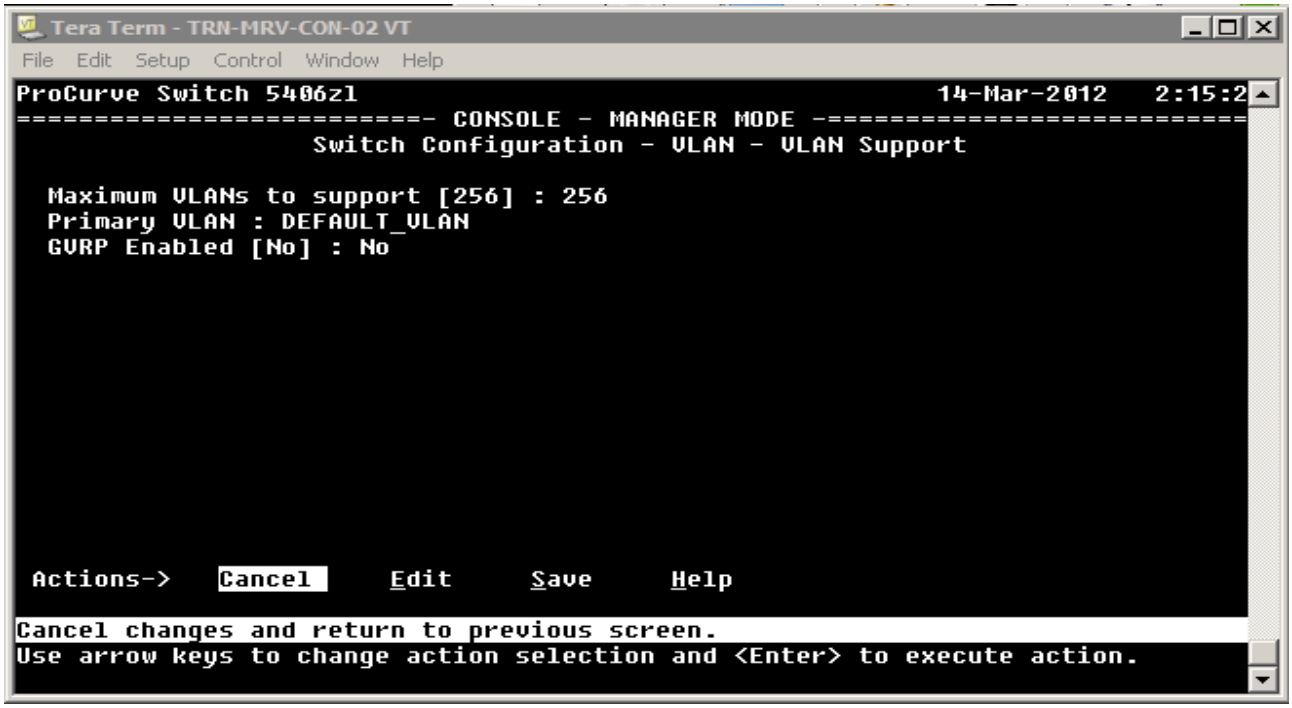


Рис. 4.7 - Параметры конфигураций VLAN

Вы можете видеть, что этот коммутатор поддерживает до 256 виртуальных локальных сетей. Коммутатор, в настоящее время, создан с конфигурацией по умолчанию VLAN, поэтому основная VLAN также по умолчанию (имеет название DEFAULT_VLAN). GVRP, протокол управления VLAN, по умолчанию отключен.

Протокол регистрации GARP VLAN (GVRP) – дополнение в общий протокол регистрации атрибутов (GARP), который используется в создании и управлении сети VLAN. Он динамически создает VLAN на принимающей стороне в соответствии с VLAN, созданными статически на передающей стороне.

Чтобы создать новую VLAN, необходимо ее определить. Выберите Cancel, чтобы вернуться к VLAN Menu и выберите 2. VLAN Names, чтобы открыть экран VLAN Names Configuration (Рисунок 1.8). По умолчанию выбирается меню Actions. Выберите Add из Actions меню и введите информацию.

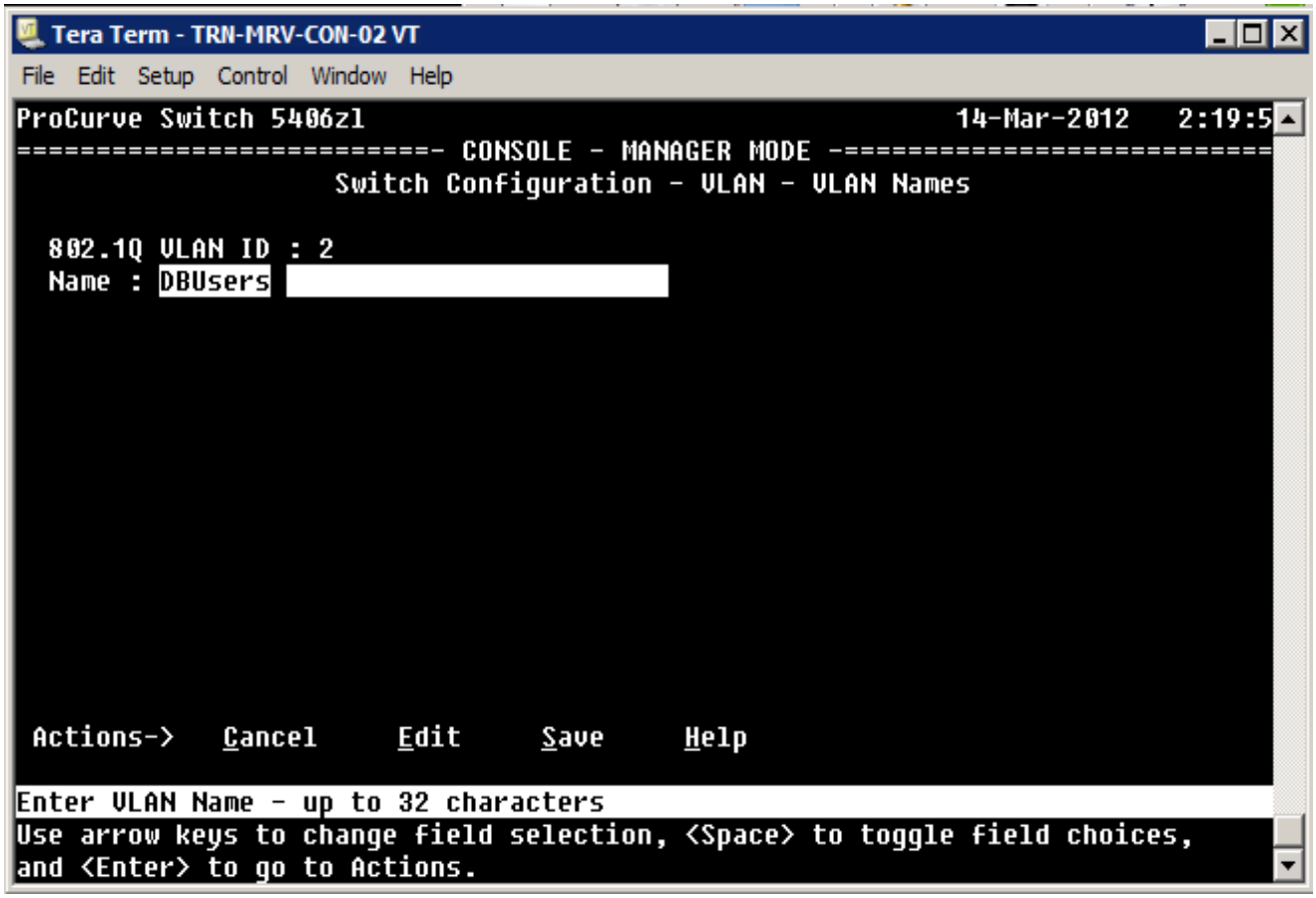


Рис. 4.8 - экран VLAN Names Configuration

Вы можете указать идентификатор и имя. Отсюда вы должны нажать клавишу Enter, чтобы вернуться в Actions меню, и выберите пункт Save, чтобы сохранить новое определение VLAN.

Теперь список имен VLAN включает в себя как DEFAULT_VLAN так и новый, который вы, только что создали (Рисунок 4.9).

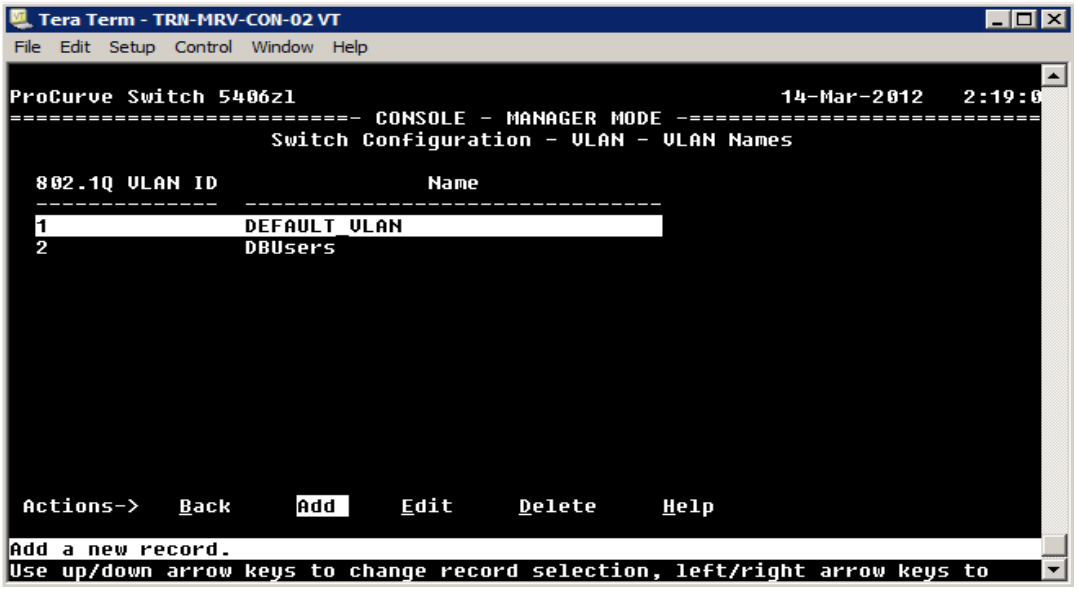


Рис. 4.9 - список имен VLAN

В этот момент, существует вторая VLAN, которая сконфигурирована на коммутаторе. Тем не менее, она не имеет никаких назначенных портов, так что на самом деле ничего не нужно делать. Чтобы добавить порты, выберите 3. VLAN Port Assignment из меню VLAN.

Экран VLAN Port Assignment показывает текущее назначения портов (рис 4.10). В примере показано стандартные привязки портов, где все они привязаны к стандартной VLAN (default VLAN).

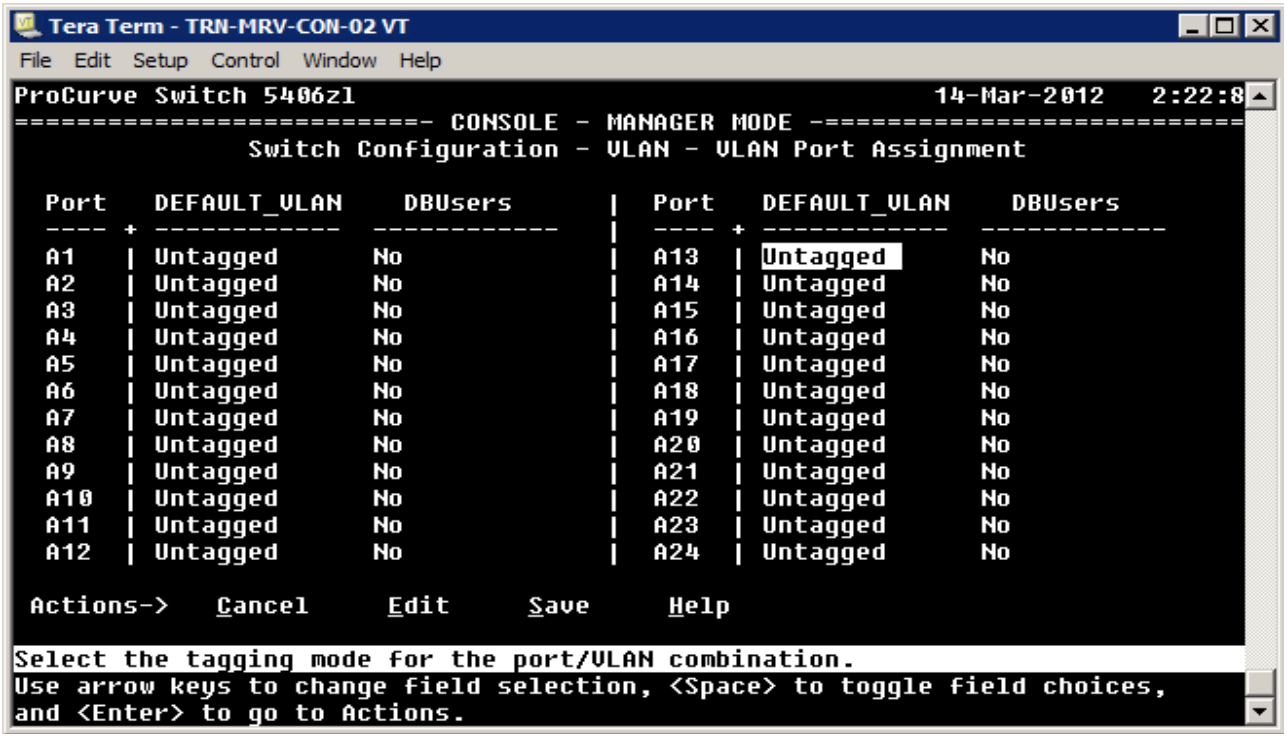


Рис. 4.10 - Экран VLAN Port Assignment

Чтобы изменить порт назначения, выберите Edit в меню Actions и с помощью клавиш со стрелками выберите порт, который вы хотите изменить (Рисунок 4.11).

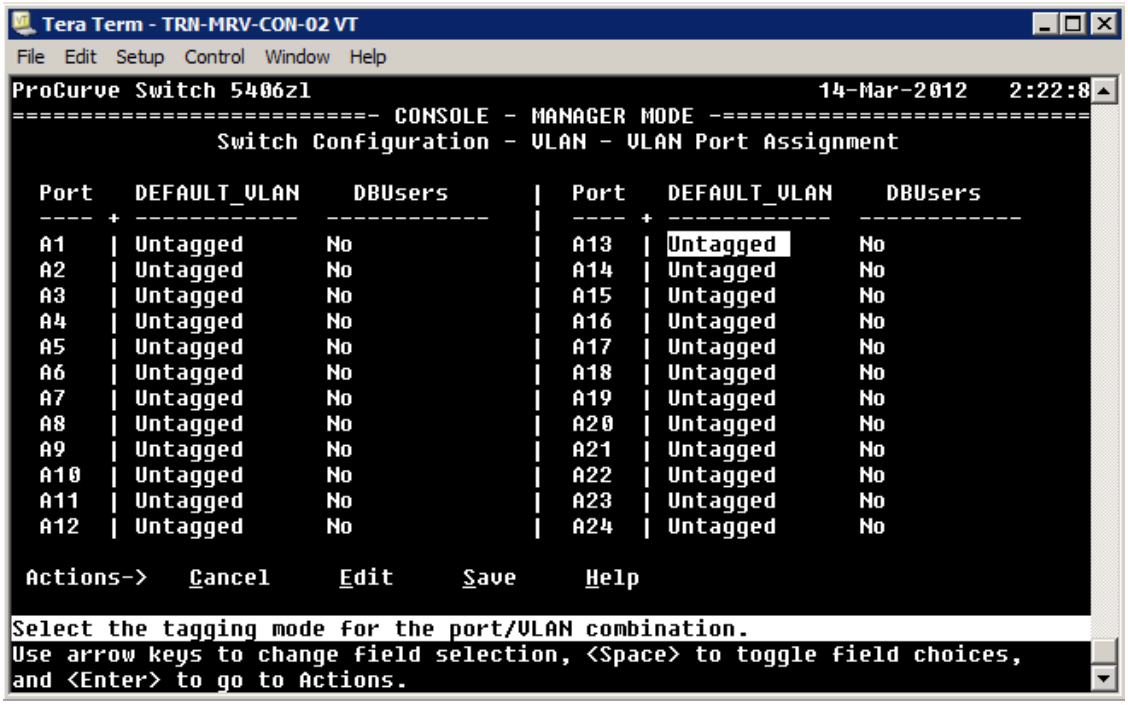


Рис. 4.11 - Меню Actions

Что нужно делать, если вы хотите добавить порты в DBUsers VLAN:

В выбранный порт, в колонке DEFAULT_VLAN, нажмите пробел, пока значение показывает No.

Для этого порта, под DBUsers, нажимайте пробел, пока показывает Untagged (Рисунок 4.12). Продолжайте этот процесс для всех портов, которые вы хотите добавить в сеть VLAN.

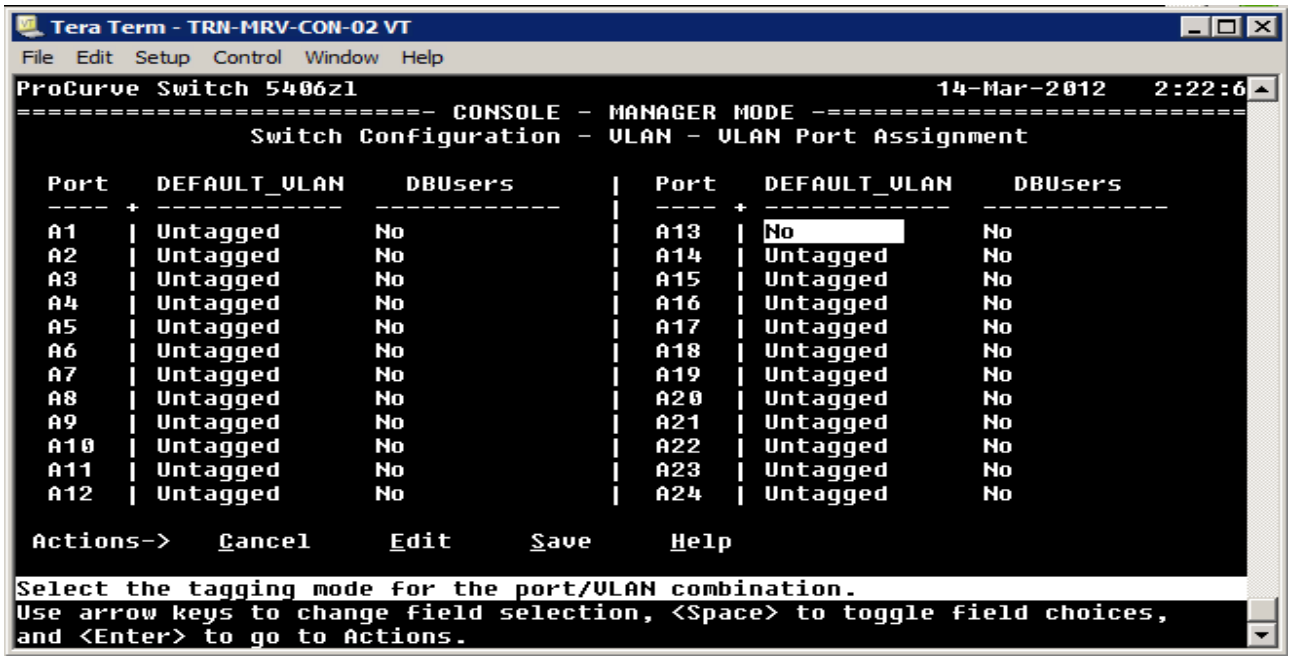


Рис. 4.12 – Добавление портов в сеть VLAN.

Порты также могут быть сконфигурированы как тегированные или запретные. Когда порт устанавливается как запретный, он не вступает в VLAN, которая была динамически создана с помощью протокола GVRP. После того как вы настроили порты, выберите Save из меню Actions.

Ранее мы рассматривали как использовать интерфейс командной строки для установки IP-адреса для VLAN. Это также может быть достигнуто с помощью меню интерфейса. С VLAN Menu, выберите 4. Return to Previous Menu. Это приведет вас обратно к Switch Configuration Menu. Отсюда, выберите 4.

Теперь, когда вы знакомы с процессом, мы можем изучить команды консоли, что вы будете использовать для создания и названия VLAN. Чтобы создать новую сеть, выполните команду виртуальной локальной сети, за которой следует идентификатор VLAN (рис 4.13).

Рис. 4.13 – Создание новой сети

Это создает новую и автоматически переключается в контекст конфигурации для этого VLAN. Как вы можете видеть на рисунке 4.13, вы вернетесь к обновленной командной строке, но никакой дополнительной обратной связи не предусмотрено, если нет ошибки в заданной команде. В этом примере, новая VLAN будет иметь имя по умолчанию VLAN 2 (рис 4.14).

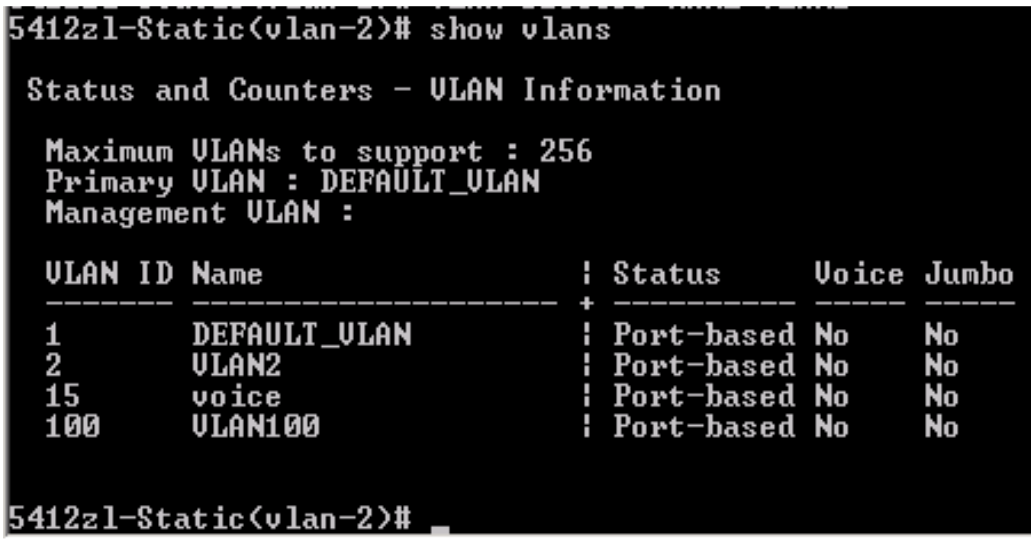


Рис. 4.14 – Имя VLAN по умолчанию

Если вы хотите переименовать VLAN как DBUsers, вы должны зкоманду: vlan VLAN2 name DBUsers

Если нет никаких ошибок, то команда не возвращает никакого ответа, а возвращает в командную строку.

Конфигурация IP

Конфигурация IP отключена по умолчанию для вновь созданного VLAN (рис 4.15). Вы можете достичь этого, выбрав IP Configuration из главного меню. Также можете установить настройки конфигурации IP - DHCP / BOOTP, чтобы автоматически получать IP-адрес от DHCP-сервера, или вы можете вручную настраивать статический адрес конфигурации IP. Выделите значение IP-Config для VLAN и нажмите пробел, чтобы прокрутить доступные варианты.

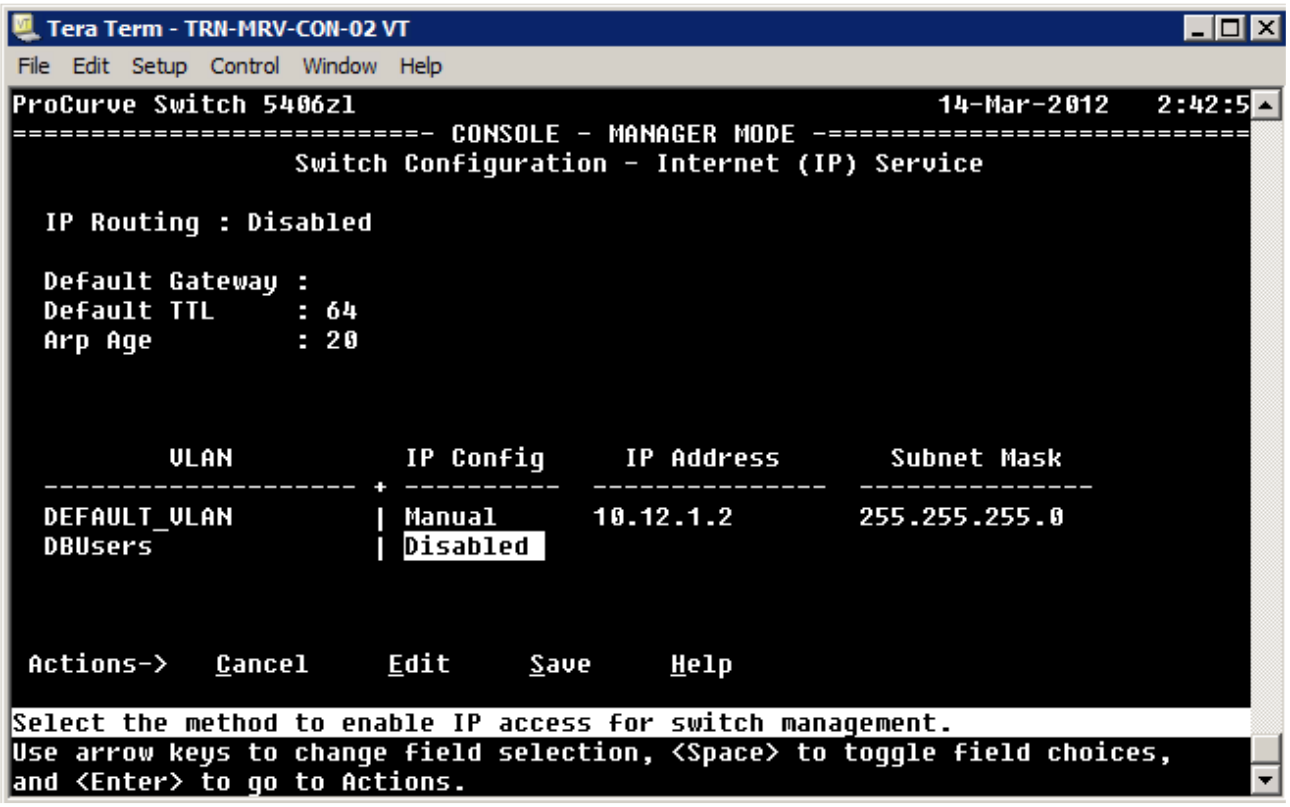


Рис. 4.15 – Стандартная IP конфигурация

Чтобы добраться до экрана управления, выберите Switch Configuration в главном меню, а затем выберите IP Configuration из IP Configuration Menu.

Если вы хотите, чтобы сеть VLAN имела известный IP-адрес, вы можете выбрать настройку статистического IP-адреса (Рис 4.16).

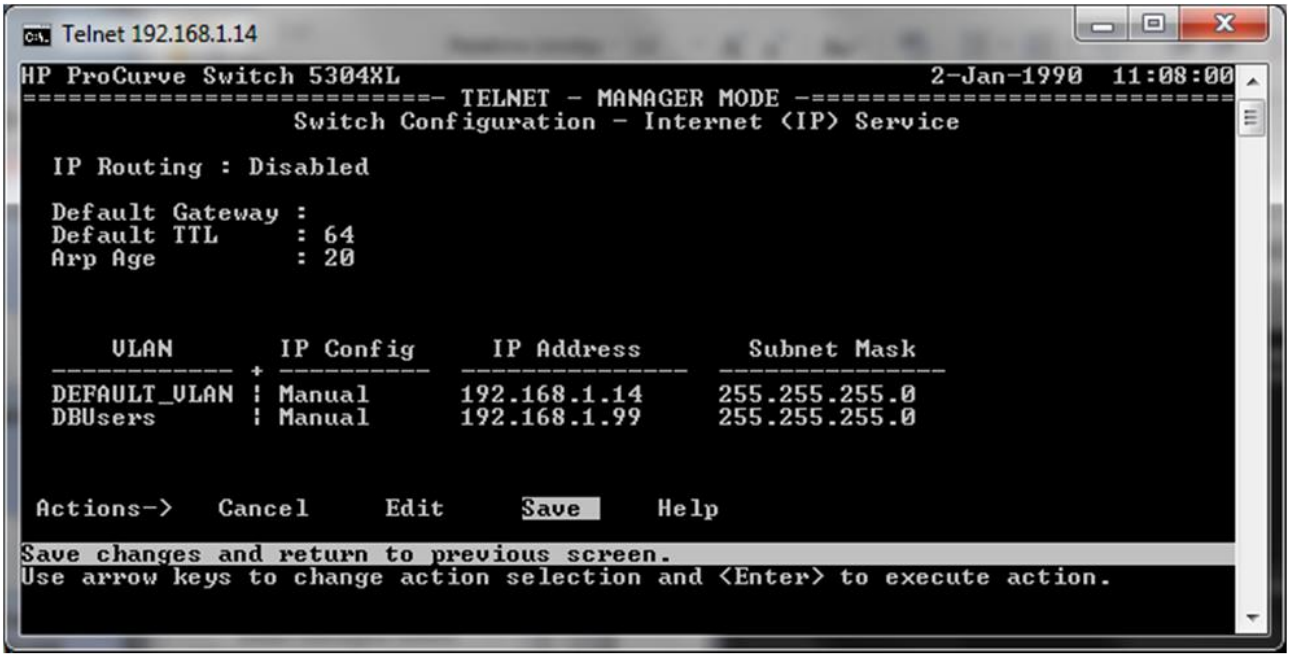


Рис. 4.16 – Статический IP-адрес

Если вы вернетесь к CLI, вы можете запустить следующую команду, чтобы увидеть список сетей VLAN настроенных на коммутаторе вместе с типом VLAN:

show vlans

В этом случае коммутатор сконфигурирован на основе двух портов VLAN (рис 4.17).

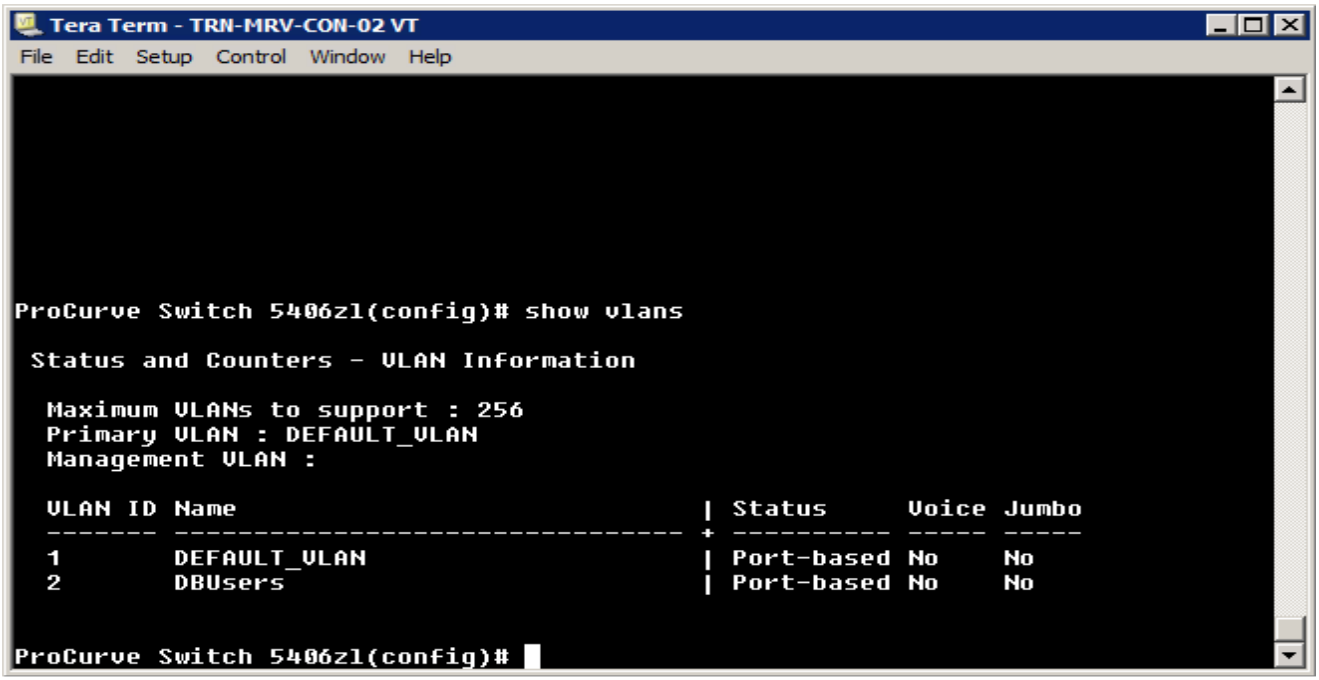


Рис. 4.17 – Список VLAN

Обратите внимание, что DEFAULT_VLAN еще называется первичным VLAN. Там нет определяющей, что означает, что вы можете подключиться к коммутатору из любого порта и осуществлять деятельность по управлению.

Требования к удалению VLAN зависит от коммутатора, а иногда и от версии системного программного обеспечения. С некоторых коммутаторов, вы должны удалить все порты из VLAN, прежде чем она может быть удалена. С другими, вы можете удалить VLAN, и его порты автоматически вернутся к VLAN по умолчанию.

Руководство портами

Управление портами для VLAN делается под виртуальную локальною сеть связи. Тем не менее, вы можете просмотреть информацию порта, включая статистические данные и счетчики, в любом контексте. Для просмотра, выполните следующую команду:

show interface

Если вы хотите увидеть более подробную информацию для одного порта, укажите его номер:

show interface a1

Это даст вам статистику для указанного порта (рис 4.18).

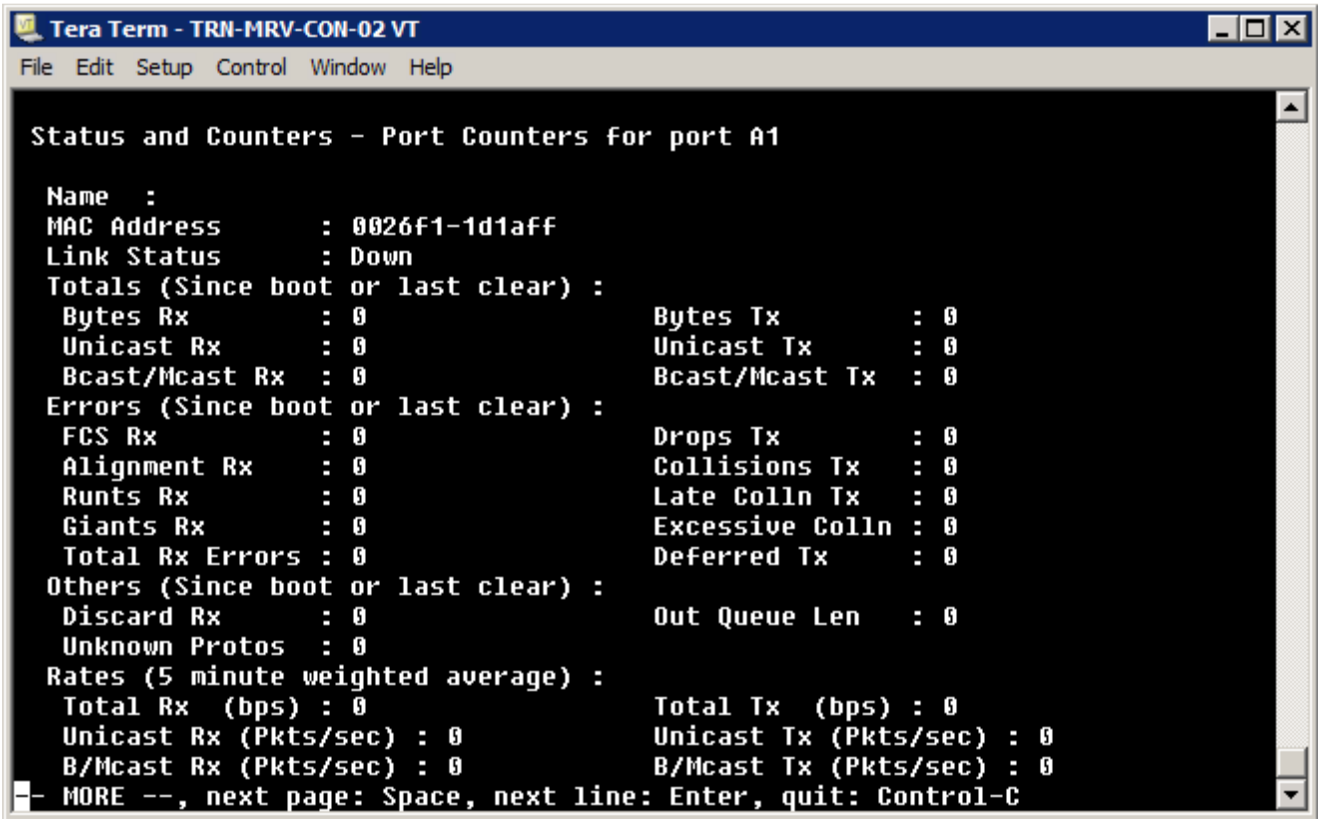


Рис. 4.18 – Статические порты

Предоставляемая информация включает следующее:

1. Статус соединения.

2. Общее число байтов, юникаст, полученные и переданные данные.

3. Скорость приема и передачи

Там нет портов, которые могут быть связанны с вновь созданной VLAN (рис. 4.19). Вы должны сделать порт назначения после создания VLAN.

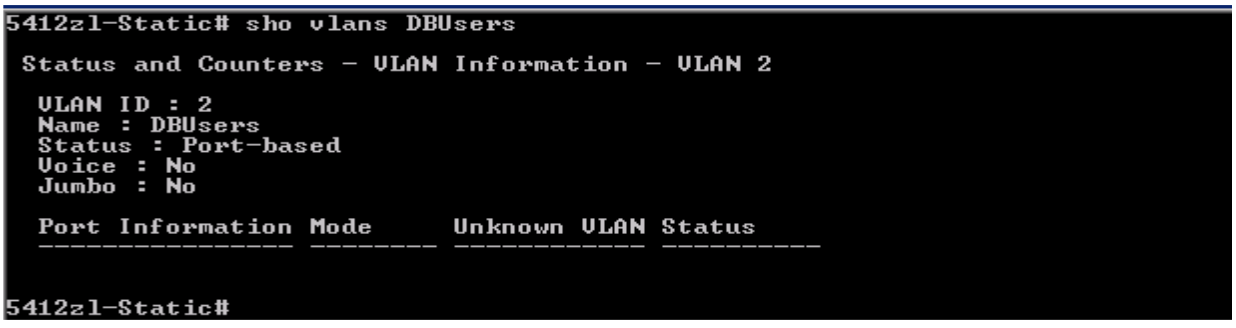


Рис. 4.19 – Порт назначения новой VLAN

Вы должны сначала ввести контекст конфигурации. Затем, вы можете ввести контекст для VLAN, которой вы управляете. Помните, что вы должны ввести идентификатор, когда вы переключаетесь на виртуальной локальной сети связи. Для управления VLAN 2, выполните следующее в контекстной строке конфигурации:

5412zl-Static (config) #vlan 2

Новой командной строкой будет:

5412zl-Static (vlan-10) #

По умолчанию, все порты будут сконфигурированы как нетегированые. Чтобы настроить тегированный порт, выполните следующую команду:

tagged <port>

Помните, что когда вы имеете дело с модульным коммутатором, порт назначения будет выглядеть следующим образом:

tagged b1

Чтобы изменить маркированный порт обратно в нетегированный порт, выполните:

untagged <port>

Вы можете указать один или диапазон портов, как в примере рисунка (Рисунок 4.20).

```
5412zl-Static(vlan-2)# untagged H10
5412zl-Static(vlan-2)# sho vlans DBUsers

 Status and Counters - VLAN Information - VLAN 2

  VLAN ID : 2
  Name : DBUsers
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  H10              Untagged Learn        Down

5412zl-Static(vlan-2)#
```

Рис. 4.20 – Добавление портов

В этом примере, также нужно включить порт. Когда порт сконфигурирован как тегированный член VLAN, его статус (тегированный или нетегированный) в любой другой VLAN остается неизменным.

Когда порт нетегированный, он всегда будет удален от любой другой VLAN, в которой в настоящее время тегированный.

Когда вы изменяете тегированный порт на нетегированный в той же VLAN, этот порт не становится автоматически нетегированным в другой VLAN.

В этом случае, если тегированный порт должен быть нетегированным в другой VLAN, он должен быть вручную помеченный как нетегированный в этой VLAN.

Помните, что вы должны записать изменения в память, чтобы обновить конфигурацию запуска. В противном случае, все несохраненные изменения будут потеряны, если вы перезагрузить коммутатор.

Уровень 3 Управление

Коммутаторы уровня 3 поддерживают широкий спектр конфигурации команды поддержки маршрутизации и помогают обеспечить доступ к сетевым услугам.

Команды маршрутизатора в этом разделе представляют собой команды на коммутатор с названием "Router". В командной строке показывается, как легче это сделать, что бы увидеть контекст команды.

Мы начнем с рассмотрения образца конфигурации сети (рис 4.21). При использовании коммутатора в качестве маршрутизатора, как в этом примере, настраивается маршрутизатор в качестве шлюза по умолчанию для клиентов и передача трафика между настроенными VLAN.

Шлюз по умолчанию (default gateway) – роутер по умолчанию, который используется для передачи трафика, когда конкретный маршрут к назначению не известен или указан.

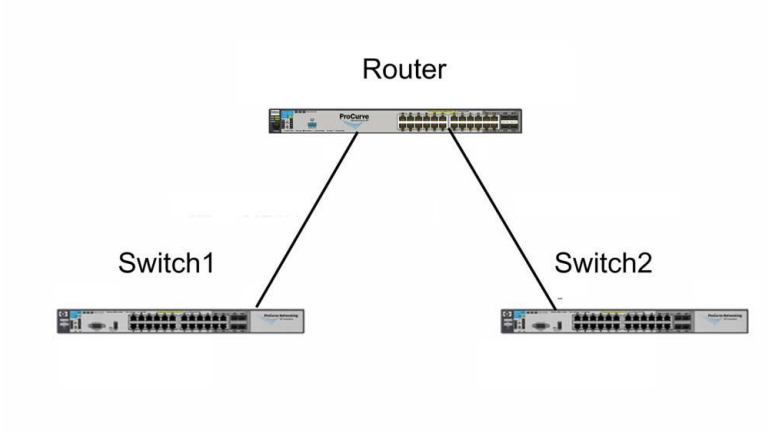


Рис. 4.21 – Образец конфигурации сети

Чтобы использовать коммутатор в качестве маршрутизатора, необходимо сначала включить маршрутизацию. Для этого из контекста конфигурации, выполните следующее:

Router(config) # ip routing

Использование пинга для устранения связи поддерживается как и в меню интерфейс, так и в веб-интерфейсе.

Вы также должны настроить коммутатор со шлюзом по умолчанию для удаленного управления по сети VLAN, которая посвящена для управления устройством. Шлюз по умолчанию должен быть в той же подсети, что и IP-адрес управления коммутатором. Это делается с конечным коммутатором в контексте конфигурации. Предполагая, адрес шлюза по умолчанию в 192.168.10.1, выполните следующее:

Switch1(config) # ip default-gateway 192.168.10.1

Параметр helper-address используется для включения коммутатора, направляющего DHCP запросы от всех VLAN, к DHCP-сервера к другой VLAN. Например, у вас может быть DHCP-сервер в сети VLAN 100 и клиентские компьютеры в сети VLAN 2, 3 и 5. Эта команда должна быть запущена отдельно для каждого VLAN, используя контекст VLAN:

Router(vlan-1)# ip helper-address <ip _address >

Обратите внимание, что в этой команде, вы должны заменить <ip_address> с IP-адреса DHCP-сервера. Helper - address настроен на маршрутизаторе или на уровне 3 коммутатора. Настройка вспомогательного адреса коммутатора на уровне 2 не имеет никакого эффекта.

Например, если клиенты на VLAN 2 должны арендовать IP-адреса из DHCP-сервера с адресом 10.10.5.2,выполните следующее:

Router(vlan2) # ip helper-address 10.10.5.2

Вы можете использовать команду пинг для проверки коммуникаций с коммутатором для подключенного устройства. Чтобы проверить подключение маршрутизатора на устройство, подключенное к одному из конечных коммутаторов, запустите команду, похожую на следующее:

Router # ping 192.168.1.108

Агрегация каналов

Агрегация каналов, или объединение портов, позволяет создать более высокую пропускную способность путем связывания несколько физических портов в один логический канал связи. HP использует стандартный протокол, называемый LACP, чтобы управлять объединения портов в своих коммутаторах.

Объединение портов (port trunking) – известное как агрегация каналов, это сочетание физических портов, чтобы создать один канал связи для обеспечения более высокой пропускной способности связи.

Link Aggregation Control Protocol (LACP) - протокол, используемый для управления объединенных физических портов в качестве одного канала связи. LACP определяется в RFC 802.3ad.

Агрегирование каналов иногда делается для обеспечения более высокой пропускной способности между маршрутизатором и связанными конечными коммутаторами. Оно также может быть использовано для создания магистральной сети с высокой пропускной способностью. Серверные операционные системы также поддерживают агрегацию каналов, что позволяет связать несколько сетевых адаптеров, чтобы улучшить связь с сетевыми серверами.

Настройка агрегации каналов требует контекст конфигурации, для этого введите:

trunk <port_id, port_id> trk<id> lacp

Для ввода фактических значений нужно выполнить следующую строку команд:

trunk a4,a5 trk2 lacp

Чтобы увидеть соединения, которые настроенные на коммутаторе, выполните следующее:

show trunk

Это вернет список соединений и их ассоциированные порты (рис. 4.22).

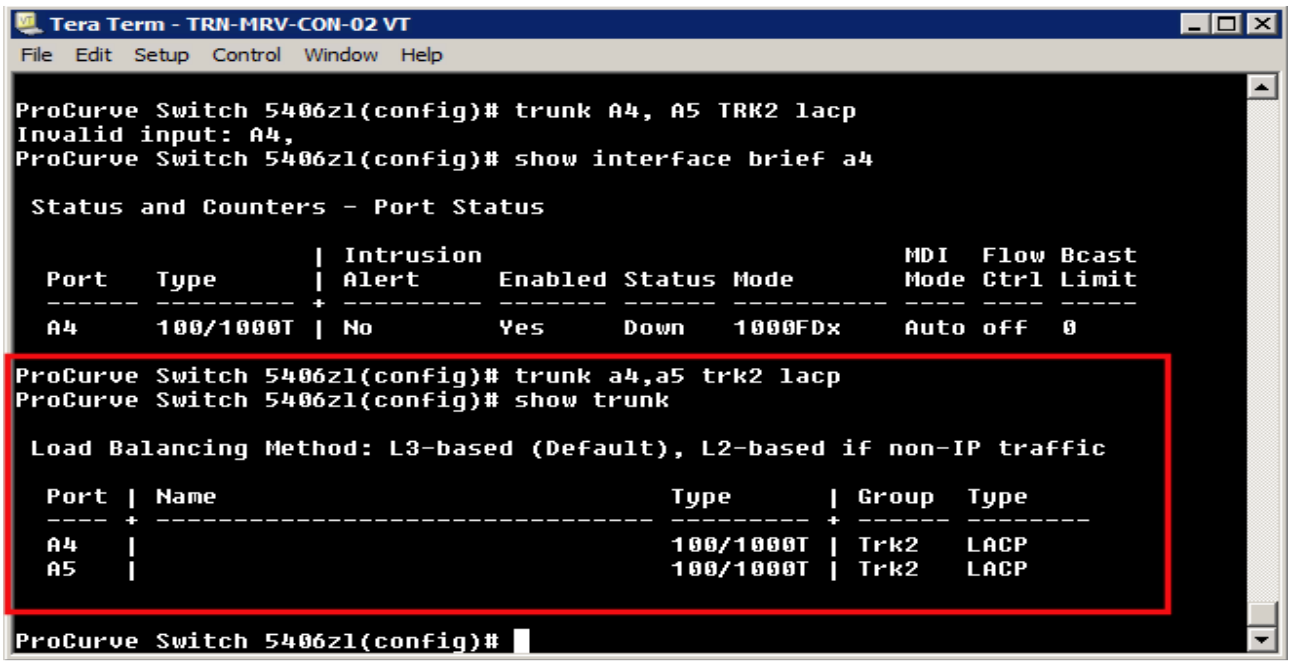


Рис. 4.22 – Настройка шин

Рисунок 4.22 показывает команду объединения и результирующий список. Результат помечены как балансировка нагрузки, которая также упоминается как распределение нагрузки. Это означает, что коммутатор будет пытаться сохранить трафик между двумя портами в том же объеме.

Балансировка нагрузки (load balancing) - процесс обмена трафика в равной степени, когда доступны несколько физических линий связи.

Вы можете получить более подробную информацию о сконфигурированных портах, выполнив следующие действия:

show interface brief a4-a5

Это даст вам краткое изложение информации о порте (рис 4.23).

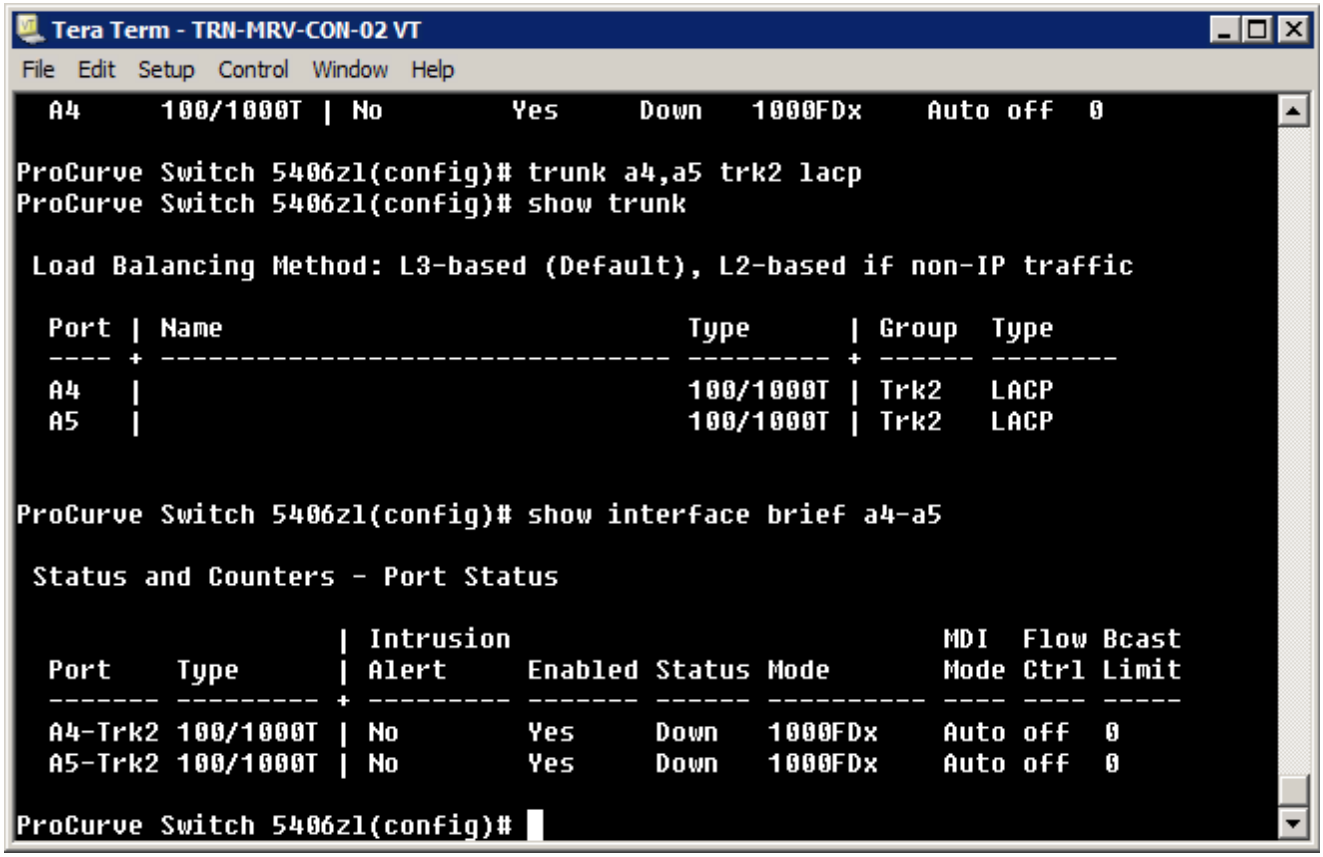


Рис 4.23 – Сводка состояний о портах

В этом примере, оба порта имеют статус Down, так как коммутатор не может физически подключаться к любому из портов.

Чтобы связать объединение с VLAN, выполните следующие действия в контексте конфигурации:

vlan <id> tagged trk<id>

Например, чтобы связать trunk 2 с VLAN 10, выполните следующее:

vlan 10 tagged trk2

Здесь маркировка может стать практической частью вашей конфигурации. Поскольку порты TRK2 тегированные, они могут быть частью нескольких VLAN.

Конфигурация коммутаторов

До этого момента мы имели дело с двумя конфигурациями, текущая конфигурация, которая используется, и конфигурация запуска хранится во флэш-памяти. Изменения в конфигурации сохраняются только в текущей пямяти, пока вы не выполните команду

- write memory. Вы можете создать резервную копию конфигурации на USB или на сервере TFTP.

Вместе с данными конфигурации, образы прошивки, которые используется для загрузки коммутатора, хранятся во флэш-памяти. На самом деле, коммутатор имеет два образа прошивки: первичные и вторичные. Они могут иметь одинаковые или разные версии файла. Они могут быть скопированы с коммутатора на любую флэш-память или сервер TFTP.

Процедуры, обсуждаемые в ходе этого раздела, предполагают доступный USB порт на коммутаторе.

Управление конфигурацией

Перед началом работы с конфигурациями коммутатора, вы должны убедиться, что текущая конфигурация и конфигурация запуска одинаковы. Таким образом, вы начинаете с известного базового уровня. Вы можете просмотреть текущую конфигурацию, выполнив следующие действия:

show running-config

Для сравнения текущей конфигурации с сохраненной конфигурации запуска, выполните следующее:

show running-config status

Если они отличаются, помните, что вы можете написать в память, чтобы сохранить текущую конфигурацию в качестве новой конфигурации запуска.

Резервное копирование файлов конфигурации

Чтобы увидеть файл конфигурации или файлы, хранящиеся во флэш-памяти коммутатора, вы можете запустить следующее:

show config files

Это возвращает список файлов конфигурации. По умолчанию, коммутатор будет иметь одну конфигурацию. Рисунок 4.24 показывает коммутатор, который выполненный с двумя файлами конфигурации.

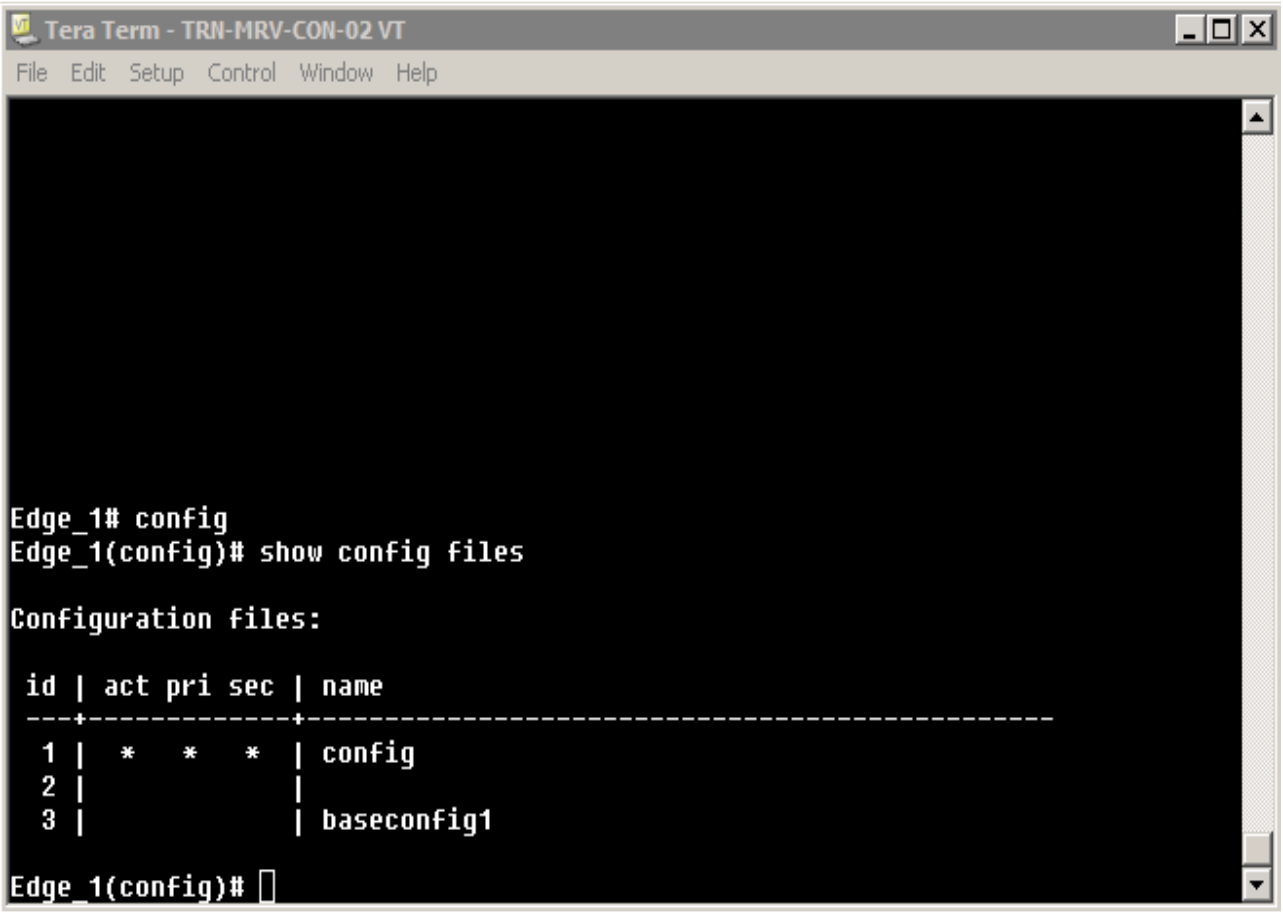


Рис. 4.24 – Файлы во флэш-памяти коммутатора

Там может быть до трех файлов конфигурации. Обратите внимание, что у вас есть три колонки между идентификатором и именем конфигурации. Звездочка указывает на:

act
Активная конфигурация, она используется для загрузки коммутатора

pri
Конфигурация привязывается к первичному образу прошивки

sec
Конфигурация привязывается к вторичному образу прошивки

Вы также можете посмотреть на информацию о конфигурации, которая хранится в файле конфигурации с помощью команды show config с последующим именем файла. В этом случае, выполните следующее:

show config config

Будьте осторожны при указании конфигурации файла. Команды не чувствительны к регистру, только на имена. Это возвращает тот же тип информации, которую вы можете увидеть, если отобразите текущую конфигурацию (рис 4.25).

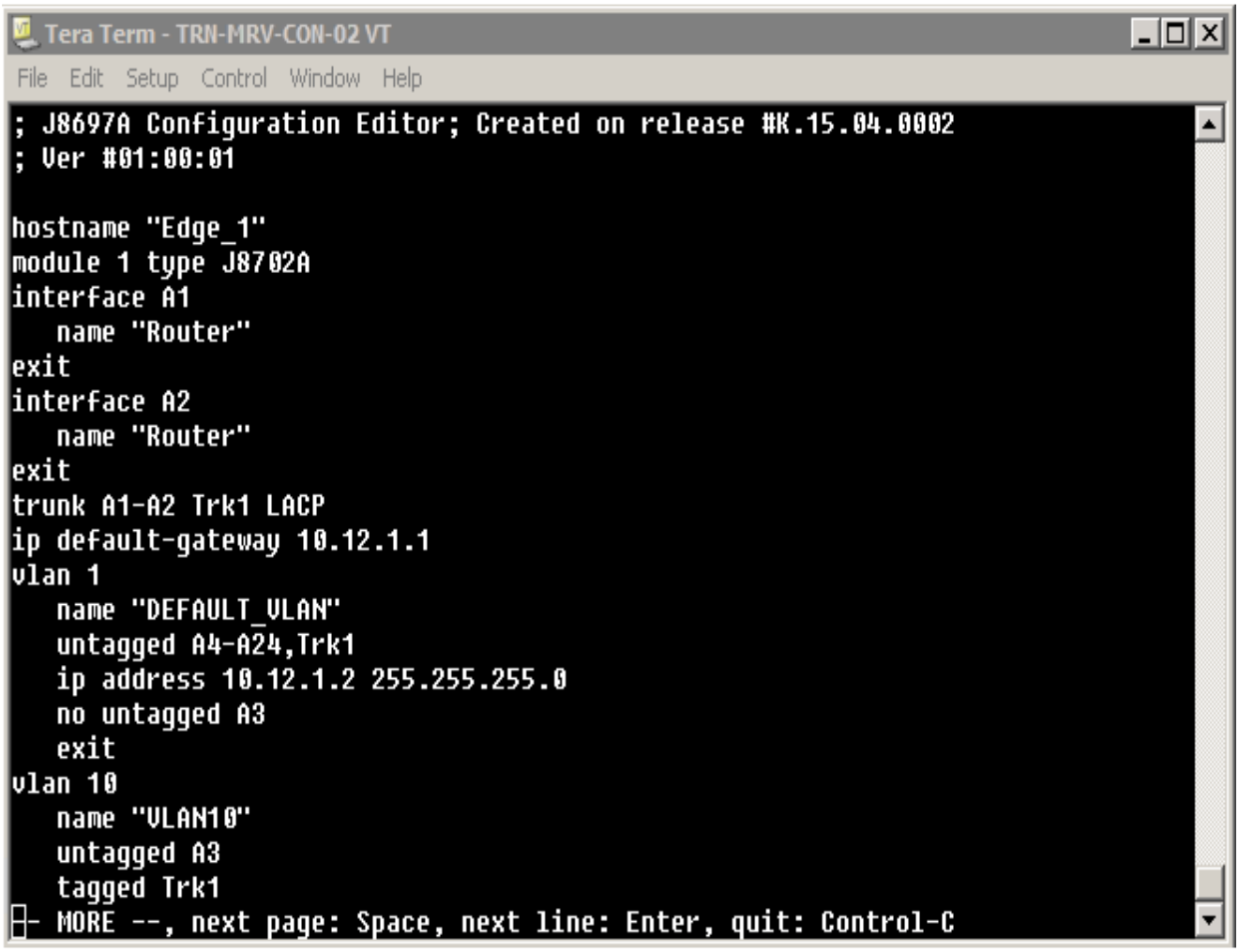


Рис. 4.25 – Текущая кофигурация

Для резервного копирования начальной конфигурации на флэш-накопитель USB, выполните следующее:

copy startup-config usb <filename>.<ext>

Когда вы выполняете эту команду, замените < filename > и < ext > с фактическими значениями. Например:

copy startup-config usb switch1.cfg

Вы можете также производить резервное копирование на сервер TFTP, используя следующее:

copy startup-config tftp <ip_address> <filename>.<ext>

Команда должна быть введена как непрерывная последовательность. Команда иногда может не помещаться в текстовой строке. Чтобы внести команду, просто продолжайте ее ввод, пока не закончите, после чего нажмите клавишу "Enter" для запуска команды.

Управление несколькими файлами конфигурации

У вас также есть возможность хранения нескольких конфигурационных файлов на коммутаторе. Вы можете создать новый путем копирования существующего файла. Рассмотрим следующую команду копирования:

copy config baseconfig1 config baseconfig2

Это создает дубликат baseconfig1 с именем файла baseconfig2. Если вы посмотрите конфигурационные файлы, то вы увидите помеченных три файлы (рис 4.26).

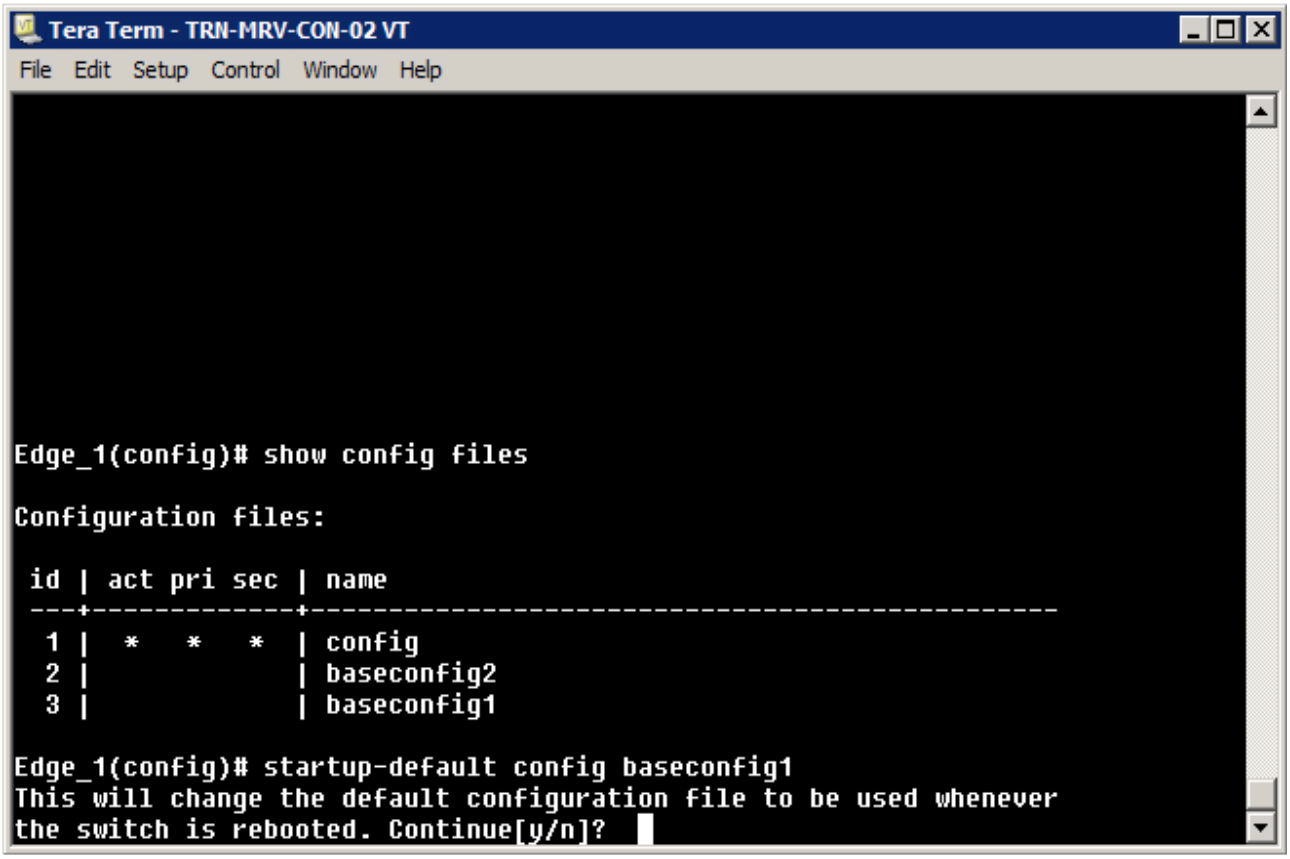


Рис. 4.26 - Конфигурационные файлы

Для того, чтобы новый файл конфигурации стал файлом конфигурации запуска, выполните следующее:

startup-default config <configname>

В этом примере, вы бы выполнили следующее:

startup-default config baseconfig1

Вам будет предложено проверить свое действие. Изменения не вступят в силу до тех пор, пока коммутатор не будет перезапущен.

Команда, которая показана выше, связывает конфигурационный файл baseconfig1 с первичным и вторичным образом прошивки (рис 4.27).

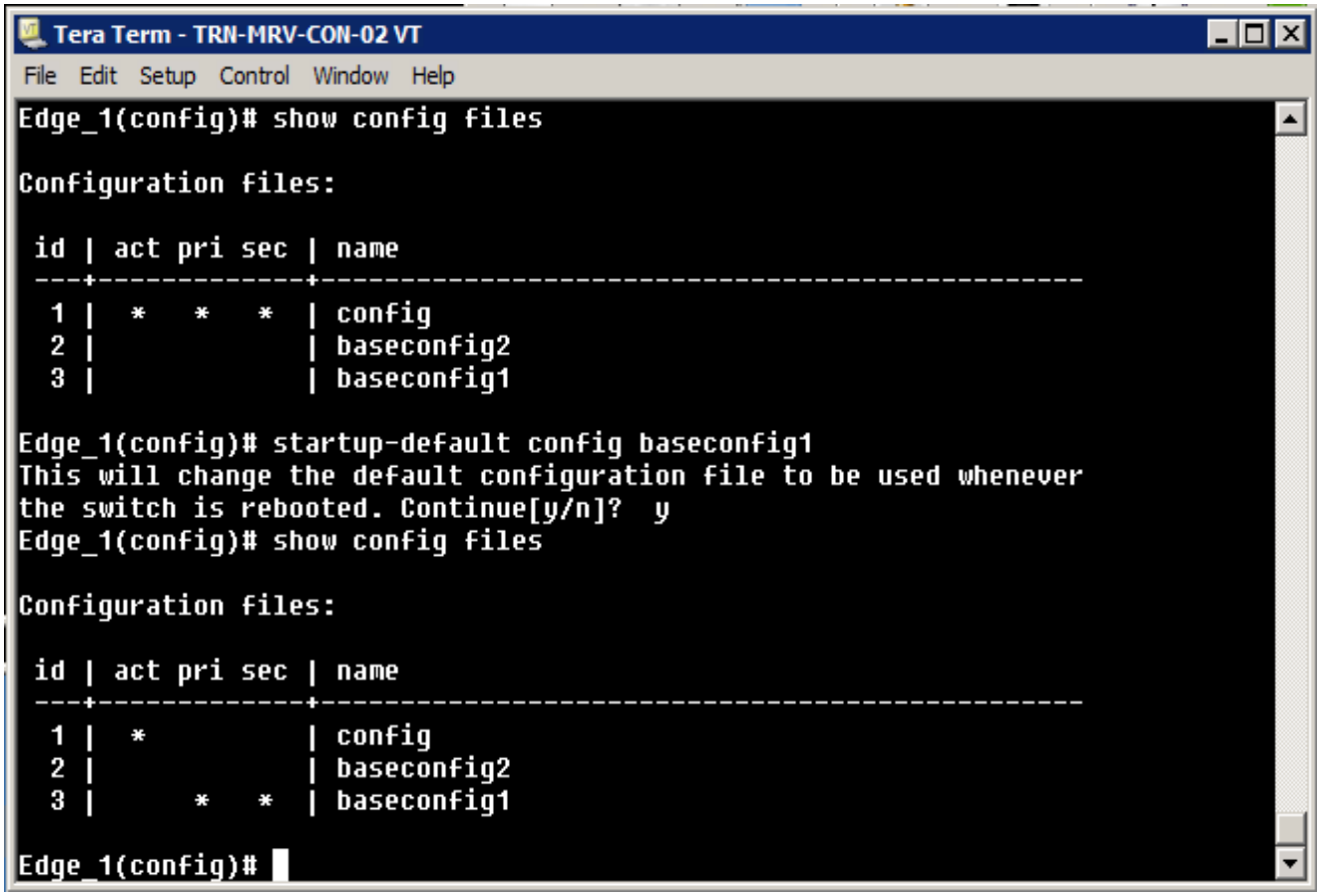


Рис. 4.27 – Связь с первичным и вторичным образом прошивки

В этот момент, конфигурация по-прежнему является активной, потому что она является последней, которая используется для загрузки коммутатора. В следующий раз при загрузке, baseconfig1 будет использоваться в качестве файла конфигурации запуска и начальной запущенной конфигурации.

После перезагрузки, все изменения конфигурации, которые вы внесли в рабочую конфигурацию, сохранятся в "baseconfig 1". Файл конфигурации будет оставаться неизмененным, пока он не будет активным.

Вы также можете связать файлы конфигурации с различными образами прошивки. Например, вы могли бы связать конфигурации начальной прошивки и baseconfig1 с вторичным. Чтобы связать основной образ прошивки только с настройками, выполните следующее:

startup-default primary config config

Это связывает конфигурационный файл с основным, в то время как baseconfig1 до сих пор ассоциируется с вторичным образом прошивки (рис 4.28).

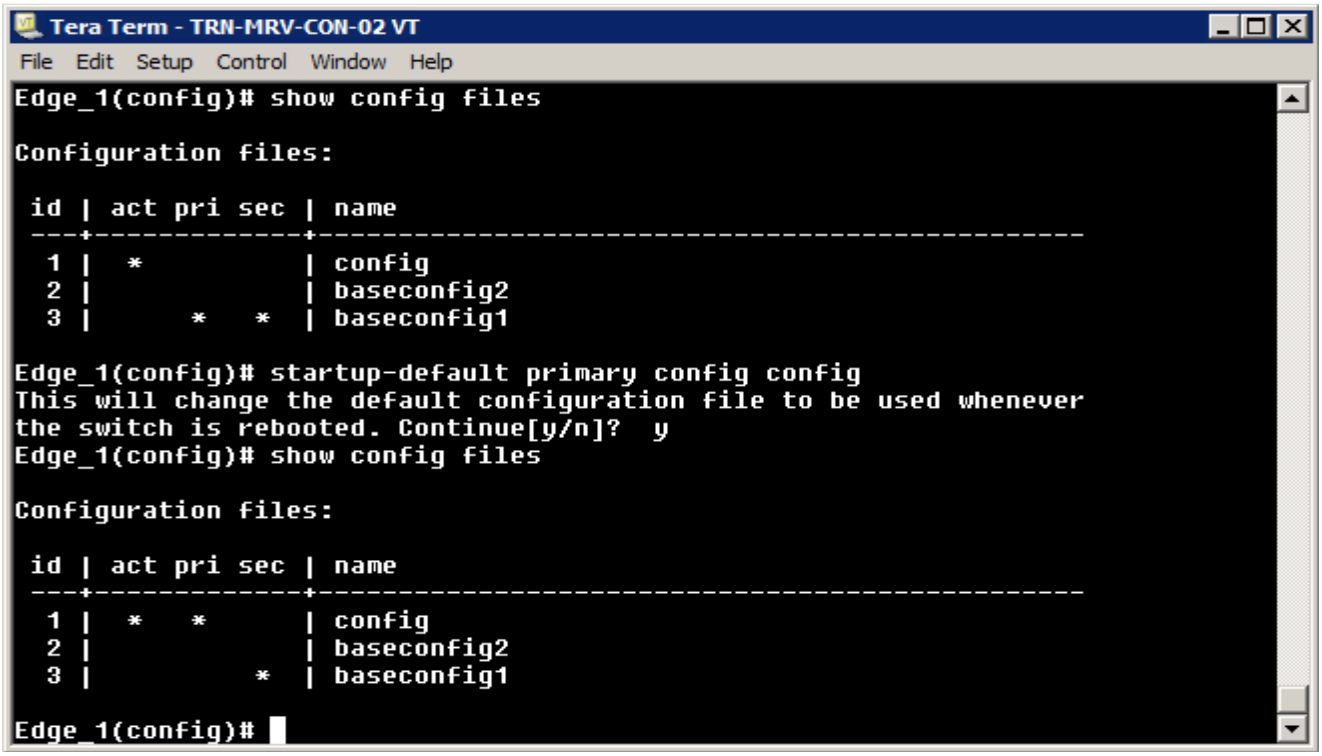


Рис. 4.28 - Связь с первичным и вторичным образом прошивки

Команда erase позволяет удалить файл конфигурации из флэш-памяти. Например, чтобы удалить baseconfig2, выполните следующее:

erase config baseconfig2

Это удаляет файл конфигурации и оставляет открытый файл (рис 4.29).

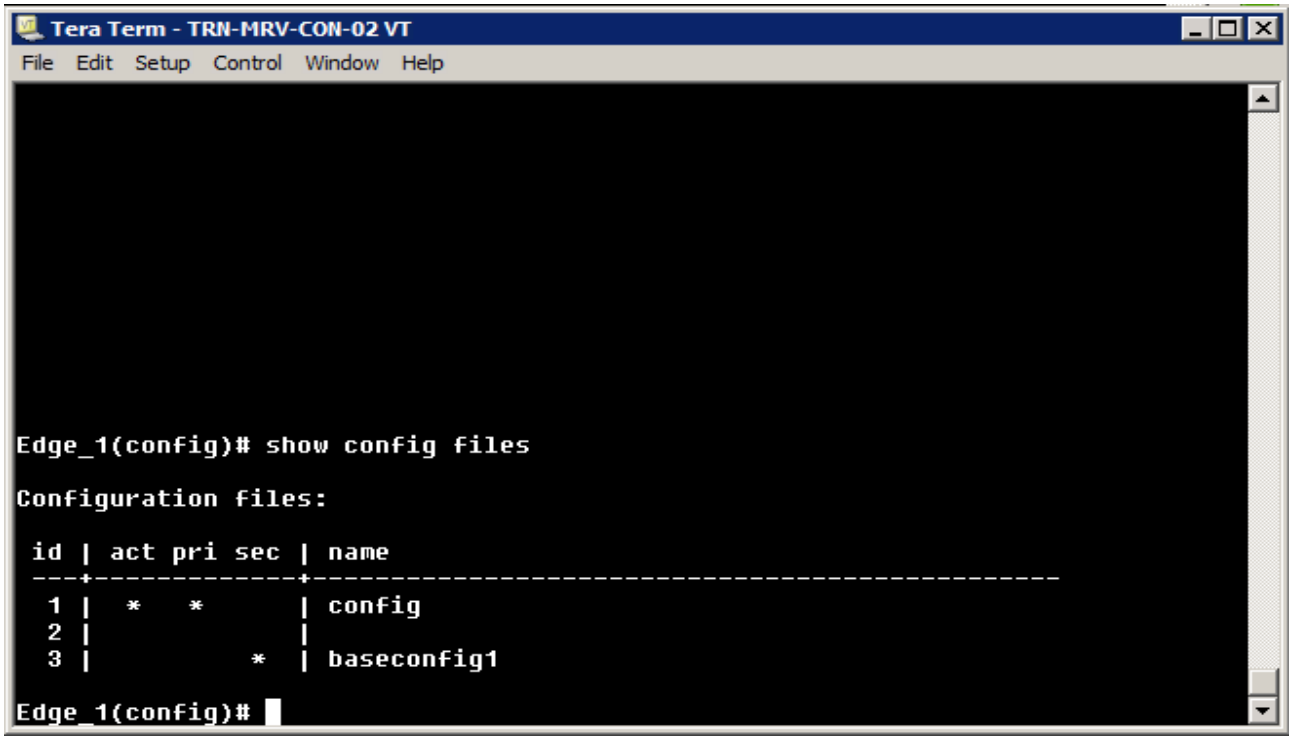


Рис. 4.29 – Удаление образа прошивки

Рис. 4.29 - Если вы удалите активный файл конфигурации, то вам будет предложено заменить его на другой. В этом случае, вы получите следующее сообщение:

The specified configuration file "baseconfig1" is the default configuration for the primary and/or secondary boot image. If it is deleted, the current active configuration file "config" will be set as the default.

Нажмите клавишу “y”, чтобы иметь переконфигурированный файл.

Управление программным обеспечением

Коммутатор программного обеспечения хранится во флэш-памяти вместе с файлом конфигурации запуска (рис 4.30). Есть две программные прошивки, которые определены как первичные и вторичные. По умолчанию, коммутатор настроен на загрузку с основным образом прошивки.

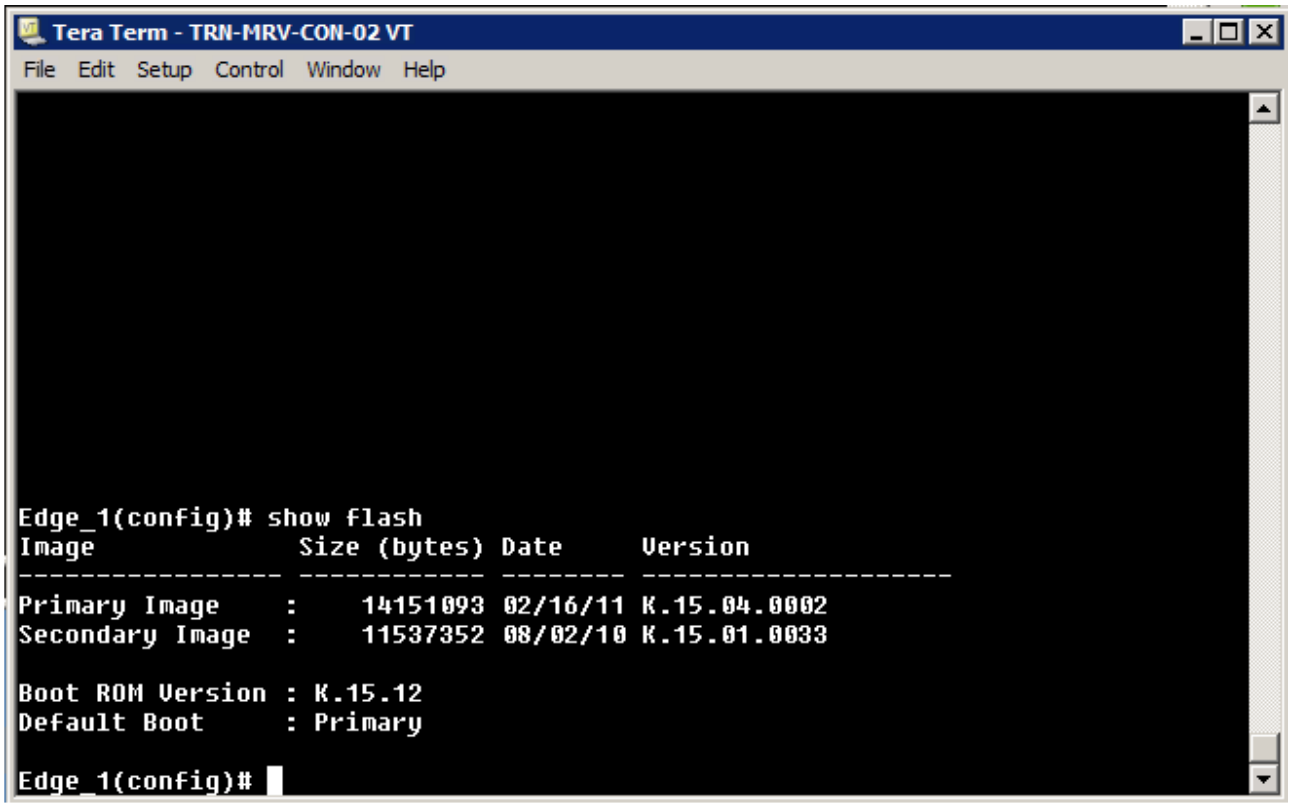


Рис. 4.30 – Образ прошивки программного обеспечения

В этом случае, есть два образа версии прошивки. Чем выше номер версии, тем он указывает на более свежую. Основная прошивка имеет номер версии K.15.04.0002 и является более поздней. Вторичная имеет номер версии K.15.01.0033. Прошивки каждого коммутатора зависят от его серии. “K” образ прошивки есть для коммутаторов 3500yl, 5400zl, 6600 и 8200zl серии.

Рисунок 4.31 показывает информацию о версии для старшей модели коммутатора с более старой версией. Размер файла, в данном случае, значительно меньше, чем более новой версии.

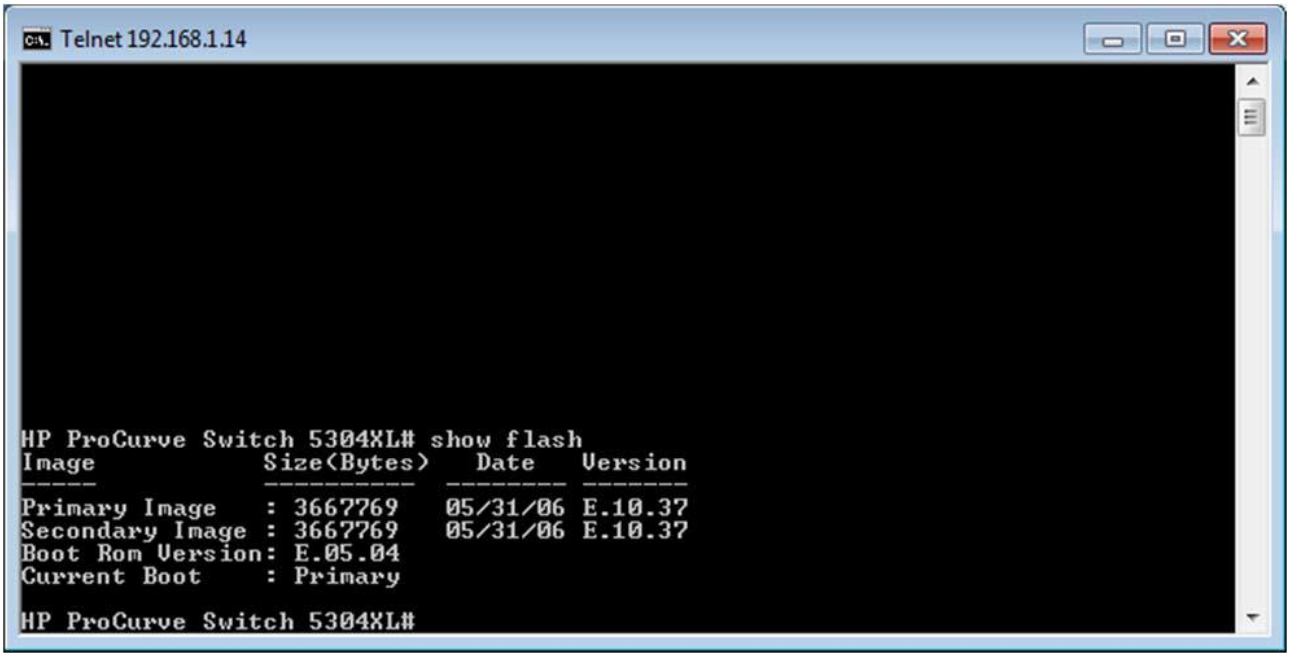


Рис. 4.31 - Информация о версии для старшей модели коммутатора

“E” образ прошивки, как на картинке, показанной в примере, может быть использован только для коммутаторов серии 5300xl.

Одним из вариантов обновления системного ПО, это загрузка файла на диске USB, а затем применяется изображение на флэш-память коммутатора. Чтобы скопировать программное обеспечение в качестве вторичного образа прошивки, выполните следующее:

copy usb flash <filename> secondary

Это оставляет основную копия неизменным. Укажите “primary” в конце строки команды, если вы хотите скопировать файл с диска USB на флэш-память. Это может занять от двух до трех минут, чтобы применить обновленное программное обеспечение.

После копирования образа прошивки в флэш-память, нужно загрузиться с этого образа прошивки, чтобы проверить, все ли работает правильно. Для одноразового запуска вторичного образа, введите следующую команду:

boot system flash secondary

Вам будет предложено проверить свое действие и сохранить конфигурацию в файл конфигурации запуска флэш-памяти. Когда коммутатор перезагрузится, вы потеряете соединение управления к коммутатору. Вам нужно будет восстановить связь после завершения перезагрузки коммутатора.

Глава 6:

Маршрутизация

Введение

Использование термина "маршрутизация" не ограничивается компьютерными сетями. Маршрутизация это выбор сетевого маршрута, через который посылается информация к конечной точке назначения. Это относится, как упоминалось в предыдущих частях, к LAN и WAN, а так же к компьютерным сетям, сетям электронного обмена данными, и даже для физических транспортных сетей.

Наше внимание в этом разделе в основном будет уделено роутерам (маршрутизаторам), как сетевому оборудованию и роли, которую они играют. Мы рассмотрим процесс разделения сетей на подсети и использование роутеров для обеспечения того чтобы информация дошла до места назначения. Мы так же коротко рассмотрим, как управляется информация о маршрутах. Мы так же исследуем специализированные роутеры, в которых реализованы дополнительные возможности, как способ дополнения к сетевой безопасности.

Этот раздел в основном фокусируется на технологиях маршрутизации основанных на IPv4. Тем не менее, большинство тем, описанных здесь, так же применимы к IPv6. Некоторые важные ограничения будут упомянуты как необходимые.

Цели

В этой главе вы узнаете, как:

- Правилам и основам маршрутизируемой сети.
- Перечислять и объяснять некоторые протоколы маршрутизации.
- Распознавать назначения использования специализированных роутеров
    - Firewall
    - Proxy
    - Multicast роутер
    - конечные точки VPN
- Обсудим процедуры развёртывания и управления маршрутизаторами.

Основы маршрутизации

Для компьютерных сетей, маршрутизация находится на Сетевом уровне модели OSI (или на уровне Internet TCP/IP модели). Любой сетевой транспортный протокол, который реализует Сетевой уровень модели OSI, может поддерживать маршрутизацию (рисунок 6-1).

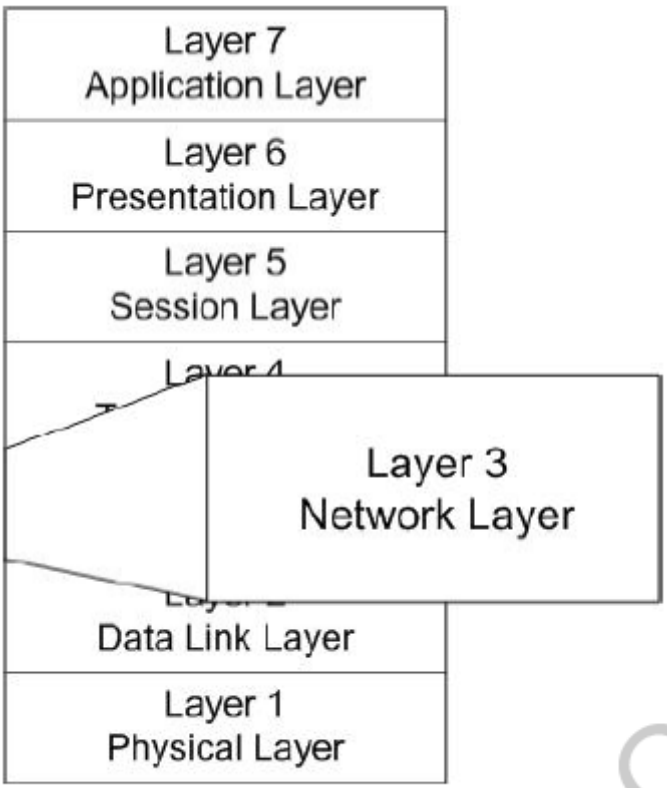


Figure 6-1: OSI Model

Рисунок 6-1: Модель OSI

Современное оборудование поддерживает множество функций. Тем не менее, для прибора, которого называют Роутером (маршрутизатором), одна из функций, которая должна обеспечивается это маршрутизация 3 уровня.

Некоторые старые сетевые протоколы, такие как NetBEUI , иногда называемые NetBIOS кадрами, не включали функциональность Сетевого уровня. На протяжении многих лет, термины NetBEUI и NetBIOS ошибочно использовались как взаимозаменяемые для обозначения сетевого протокола.

NetBIOS Extended User Interface (NetBEUI) - NetBIOS расширенный пользовательский интерфейс
Относится к сетям NetBIOS, основанные на сетевых схемах, которые обеспечивали сессии коммуникации, основанные на символических именах, но не включали протоколы маршрутизации.

Network Basic Input/Output System (NetBIOS)
Обычно относится к Сессионному уровню и системам символьного обозначения, определяющим устройства по 16-битовому имени.

NetBIOS все еще иногда рассматривается как NetBIOS over TCP/IP (NBT) - NetBIOS через TCP/IP. Пользовательские операционные системы продолжают оказывать поддержку для NetBIOS имен. Вы можете отключить поддержку NetBIOS в современных операционных системах семейства Windows, путем изменения свойств TCP/IP.

NetBIOS через TCP/IP (NBT)
Метод инкапсуляции пакетов NetBIOS внутри TCP или UDP пакетов для доставки по маршрутизируемой сети.

Для выключения NetBIOS over TCP/IP на компьютерах с операционной системой Windows 7, выберете **Сети и Интернет** с **Панели Управления**, выберите **Показать состояние сети** и выберите **изменить параметры адаптера**. Потом, правый клик на **сетевой адаптер**. Выберите **Свойства** из списка, выберите **Интернет Протокол IPv4 (TCP/IPv4)** и выберите **Свойства** (Рисунок 6-2)

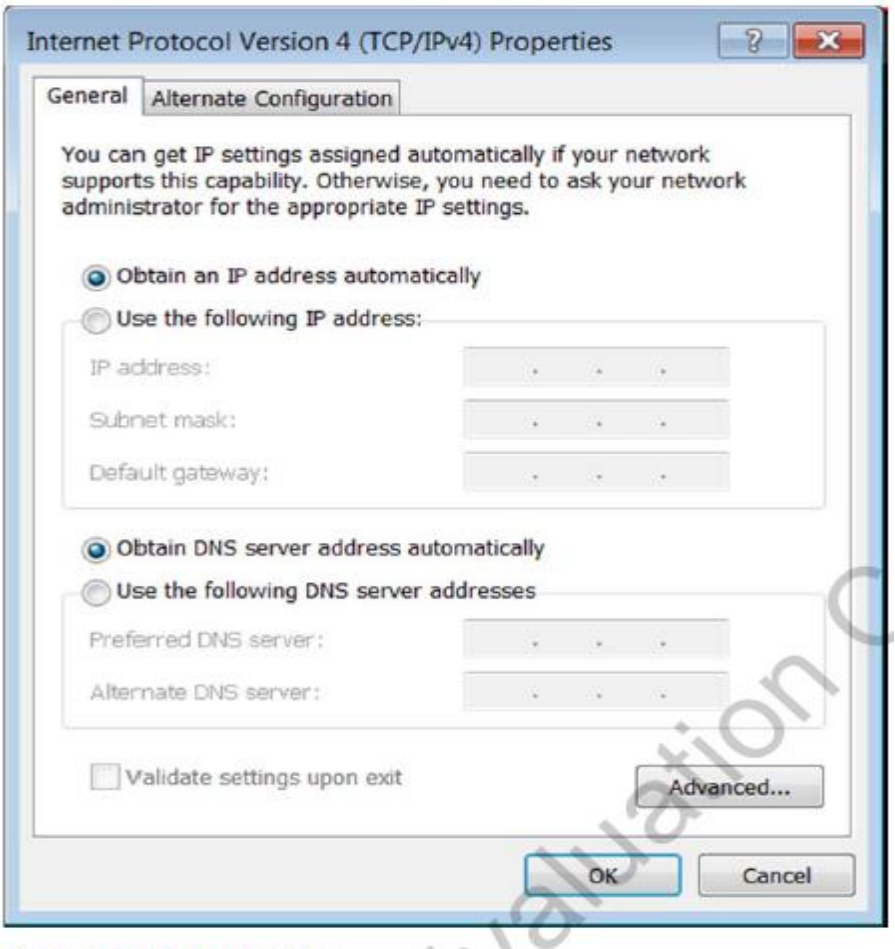


Figure 6-2: IPv4 Properties

Рисунок 6-2: Свойства IPv4

Сейчас, выберите **Дополнительно** для открытия дополнительных свойств и выберите панель **WINS** (Figure 6-3).

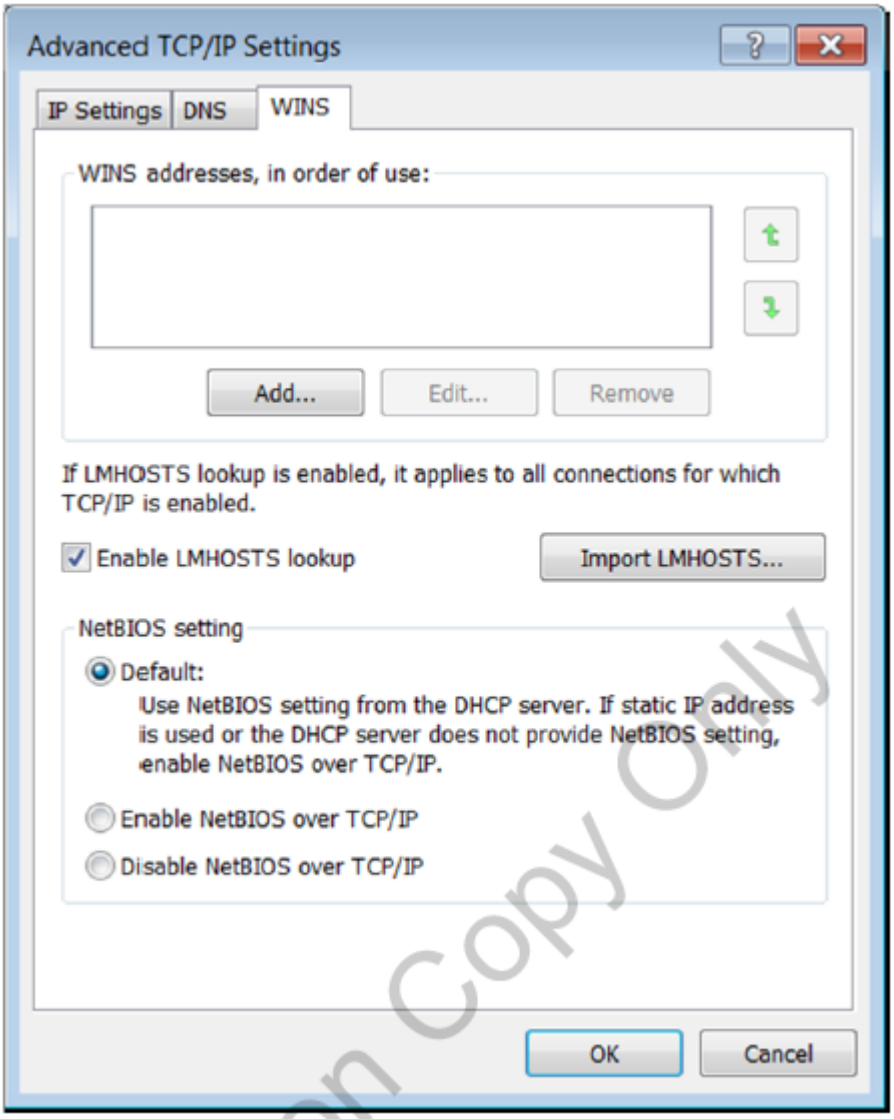


Figure 6-3: NetBIOS Properties

Рисунок 6-3: Свойства NetBIOS

Выберите **Выключить NetBIOS over TCP/IP** чтобы отключить поддержку NBT. Когда настройки по умолчанию включены, вы можете сконфигурировать ваши DHCP серверы так, чтобы NBT был отключен при получении IP адреса.

Маршрутизаторы

Когда мы говорим что маршрутизатор работает на 3 уровне модели OSI . мы имеем ввиду что роутер обеспечивает функциональность через 3 уровень . Например,1 уровень обеспечивает соединение сети к среде передачи. Уровень 2: каждый сетевой интерфейс роутера имеет канально-локальный адрес, или MAC адрес (рисунок 6-4)

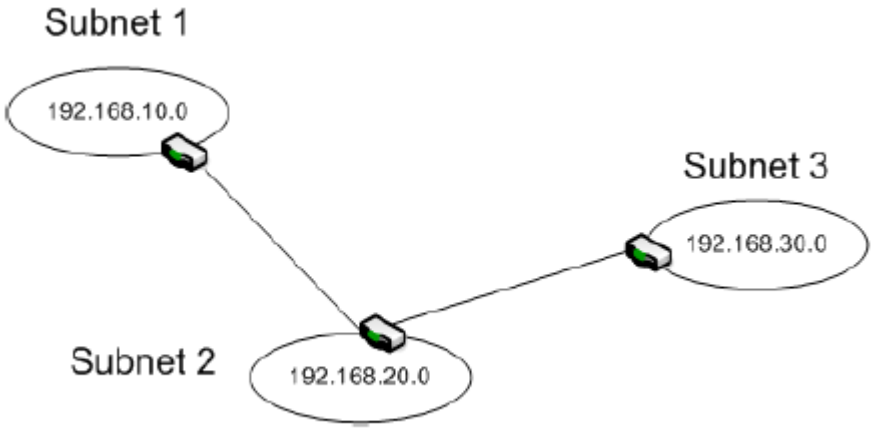


Figure 6-4: Simple Routed Network

Рисунок 6-4: Простая маршрутизируемая сеть

Маршрутизаторы используют, чтобы разделить сеть на разделенные (отдельные) подсети, каждые с уникальными сетевыми адресами. Трафик проходит или не проходит в зависимости от сетевого адреса. Например, если пакет сгенерирован в подсети 1 и предназначен любому другому хосту из той же подсети 1, пакет не будет из нее выпущен (из подсети) ее маршрутизатором.

В сетях TCP/IP, маршрутизатор так же описывается как шлюз по умолчанию. Каждому хосту может быть назначен шлюз по умолчанию, который является роутером по умолчанию, на который посылается информация для дальнейшей маршрутизации.

Маршрутизатор получает пакет, проверяет адрес получателя и, если он подходящий, перепосылает пакет по его пути. В этом случае, роутер ведет себя как повторитель Первого уровня, усиливая (скорее ретранслируя) переданный сигнал и помогая обеспечить наилучшую связность.

Использование Роутера

Обычно, роутеры используются для:

- Управление сетевым трафиком
  Трафик, предназначенный для подсети, остается в подсети, таким образом, уменьшая общесетевой трафик. Роутеры так же могут быть использованы для посылки информации по широкополосным маршрутам, избегая скоплений информации и возможных сбоев сети.
- Изолирование сетевых сегментов
  Роутеры могут быть использованы для улучшения безопасности в сегменте, контролируя трафик, что находится в и вне сегмента

Многие роутеры, помимо их основных функций, были созданы с дополнительным функционалом, и могут в сети выполнять функции:

- NAT
- VPN конечная точка
- Firewall
- Прокси-сервер

Вы так же можете встретить роутеры, которые поддерживают проводные и беспроводные сегменты сети. В такой конфигурации, они ведут себя и как роутеры, и как мосты (bridge), будучи интерфейсом между разными средами передачи.

Типы роутеров

Есть много способов, по которым вы можете классифицировать роутеры, например функциональность и тип предоставляемых сервисов. На данный момент мы рассмотрим самую простую классификацию: по установке и развёртыванию роутеров. Наиболее часто упоминаются роутеры основанные на программном обеспечении (software-based) и основанные на аппаратном обеспечении (hardware-based). Несмотря на то, что эти определения в некоторой степени не точны, они пригодны для наших целей.

Software Router (роутеры, основанные на программном обеспечении)

Когда мы говорим что Роутер - Software Router- мы имеем ввиду что он развернут на стандартном ПК со специальным программным обеспечением, обеспечивающем функции роутера. Например, Windows Server operating systems поддерживают сервис RRAS, что позволяет использовать сервер как роутер.

Маршрутизация и удаленный доступ (Routing and Remote Access, RRAS)

Сетевые системы поставляются с Windows Server operating systems и позволяют вам настроить сервер так, чтобы он работал как роутер. RRAS так же обеспечивает другие сетевые услуги.

Одно из преимуществ использования сервера в качестве роутера это относительно маленькие денежные затраты. Оно основано на том, что используется стандартное аппаратное и программное обеспечение ПК. Вы даже можете установить на ПК такие сервисы как NAT и удаленный доступ.

Потенциальные проблемы это – проблемы безопасности, надежности и эффективности. Так как роутер работает с операционной системой Windows server, роутер восприимчив к таким же рискам, как и другие Windows компьютеры. Это так же имеет влияние на потенциальную надежность роутера. Кроме того, поскольку он работает на операционной системе общего назначения, производительность значительно страдает по сравнению с устройствами, специально предназначенных для работы в

качестве маршрутизаторов. В момент пиковой нагрузки, это может вылиться в полный сбой сети, если роутер не сможет обеспечить необходимую производительность.

Компьютер с RRAS можно так же настроить на обеспечение других сетевых приложений и сервисов. Это не рекомендовано, так как это может повлиять на эффективность роутера, и создает потенциальные проблемы безопасности.

Hardware роутер (аппаратный маршрутизатор)

Hardware роутер (так же называемый Dedicated – выделенный) является, по сути, очень похожим на выше описанный Software роутер. Это специальный компьютер со специальным аппаратным обеспечением, которое было разработано и оптимизировано специально для маршрутизации трафика. Функциональность роутера так же обеспечивается через Софт (программное обеспечение), но Софт предназначен для специальных целей. Это дает производителю возможность решать проблемы, которые могут быть выявлены после выпуска или улучшить роутер с помощью дополнительного функционала.

Выделенный роутер

Сетевой прибор, разработанный специально для целей маршрутизации.

Figure 6-5: HP MSR20 Series Router

Рисунок 6-5: HP MSR20 Series Router

Роутеры сильно различаются в размерах, возможностях и стоимости. Роутер на рисунке 6-5 скорее всего, будет использоваться при развертывании SMB. Большие компании могут легко иметь несколько роутерных стоек, поддерживающих большое множество LAN и WAN каналов, голосовые сервисы, и другие сервисы если нужно.

Дополнительная функциональность зависит от модели роутера и дополнительных опций, которые были заказаны. Это обычная ситуация когда в роутере интегрирована поддержка для VLAN и коммутацию второго уровня, множество сервисов 3-го уровня,

контроль доступа, безопасность передачи информации и интеграцию с другими технологиями.

Маршрутизация

Маршрутизация (довольно просто)- процесс пересылки пакета от источника к месту назначения через маршрутизируемую сеть. Посылающий хост не должен знать ничего о физическом расположении места назначения, только адрес сети и хоста.

Информация для маршрутизации

Роутеры сохраняют информацию про пути в RIB или таблицах маршрутизации. Таблица маршрутизации это обычно таблица, включающая в себя известные этому роутеру подсети, и какой интерфейс роутера должен быть использован, для отправки пакета в определенную подсеть (Рисунок 6-6).

База информации маршрутизации (Routing Information Base, RIB)

Таблица, что поддерживается в маршрутизаторе, который содержит информацию о маршрутах и используется для пересылки пакетов.

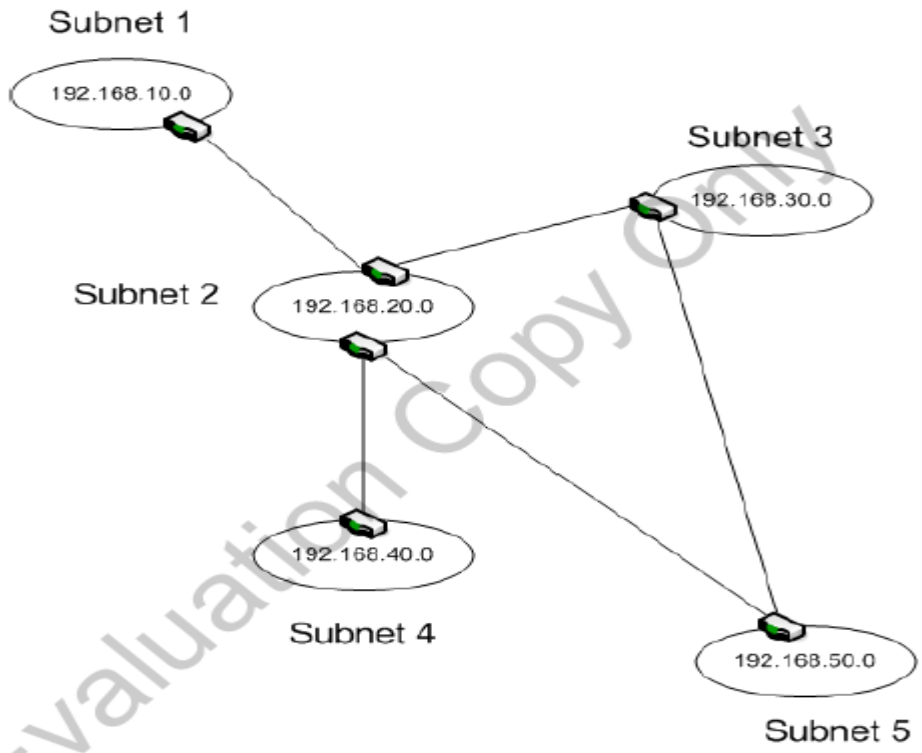


Figure 6-6: Sample Routed Network

Рисунок 6-6: Пример сети с маршрутизацией

Информация о маршрутах может быть введена в таблицу маршрутизации с помощью статического ручного ввода или обновляться динамически. Статические записи настраиваются для маршрутизатора и, как правило, включаются в таблицу

маршрутизации автоматически каждый раз, когда роутер перезагружается. Автоматические обновления посылаются роутерами с помощью специализированных протоколов, которые позволяют роутерам обмениваться информацией.

Как минимум, таблица маршрутизации включает следующие:

- ID адрес сети назначения (IP адрес и маску подсети)
- Стоимость («Вес», используемый для определения лучшего роутера)
- Следующий прыжок (следующий роутер на пути к месту назначения)

Следующий прыжок

Следующий роутер (шлюз по умолчанию) на пути следования пакета к месту назначения.

Вы так же будете сталкиваться с записью с IP адресом сетевого интерфейса, через который нужно посылать пакет. Если место назначения не будет записано в таблице маршрутизации, пакет будет отослан по адресу шлюза по умолчанию.

В таблице маршрутизации для шлюза по умолчанию адрес и маска подсети устанавливаются 0.0.0.0

Процесс маршрутизации

Хост способен распознать, основываясь на адресе назначения, находится или нет хост назначения в той же подсети. Если нет, то хост будет посылать пакет соответствующему маршрутизатору (или шлюзу по умолчанию), который должен перенаправить к конечному пункту назначения.

Точный процесс маршрутизации пакета в некоторой степени зависит от типа передачи. Например:

- Unicast

  Пакет маршрутизируется к одному месту назначения.
- Broadcast

  Пакет, если будет пропущен, отправляется во все возможные подсети.
  Обычно роутеры настроены не пропускать широковещательные пакеты, хотя некоторые будут передавать пакеты, предназначенные для удаленного управления и DHCP.
- Multicast

  Пакет передается для группы хостов, возможно находящихся в разных подсетях.
- Anycast

Пакет предназначен группе хостов, но доставляется только одному хосту, обычно ближайшему к месту отправки.

Рисунок 6-7 иллюстрирует процесс Unicast.

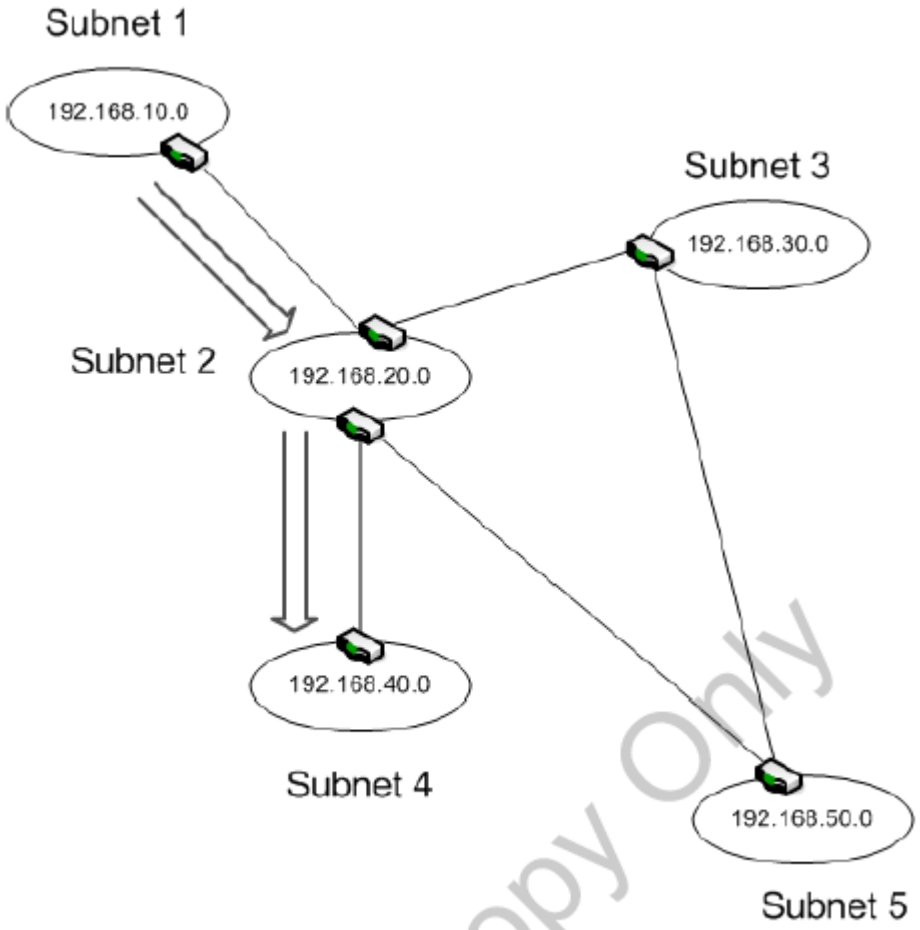


Figure 6-7: Unicast Routing Example

Рисунок 6-7: Пример Unicast маршрутизации

Хост в подсети 1 генерирует пакет с конечным адресом 192.168.40.115. Роутер из подсети 1 посылает пакет на роутер, показанный наверху подсети 2. Из-за того что присутствует множество путей (даже через одну петлю), роутер должен принять решение про лучший маршрут. Он отправит пакет прямо на роутер, показанный снизу подсети 2, который в свою очередь пошлет его подсеть 4 для доставки.

Как делается выбор лучшего маршрута? В протоколах с **distance vector routing** (дистанционно-векторная маршрутизация), путь обычно выбираются по количеству роутеров между источником и местом назначения. В нашем примере пакет мог пройти через подсети 3 и 5, но это добавило бы 2 петли.

Distance vector routing (дистанционно-векторная маршрутизация)

Алгоритм маршрутизации, который строит свои расчеты маршрутов по «стоимости» (кол-ву прыжков) к месту назначения.

Прыжок

Относится к каждому роутеру, который проходит пакет на пути к пункту назначения

При дистанционно-векторной маршрутизации, маршрут основывается на стоимости, выраженной в кол-ве прыжков, к месту назначения. Мы показали очень легкий пример, но маршрут может стать сложнее в большей сети. Чтобы облегчить процесс, каждый роутер обновляет информацию своего соседа информацией о каждом месте назначения, о котором он знает. Роутер использует эту информацию для обновления таблицы маршрутизации, и, в свою очередь, принимает решение о лучшем маршруте.

У роутера настроен путь по умолчанию к другому роутеру. Он используется, как следующий прыжок, когда место назначения не содержится в таблице маршрутизации RIB.

Есть вероятность того что пакет может потеряться в большой сложной сети, что может застрять в петле где не сможет никогда найти свое место назначения. Чтобы избежать этого, у каждого пакета настроено так называемое значение TTL (time-to-live) . Это максимальное количество прыжков (роутеров) через которые пакет может быть послан. С прохождением каждого роутера, значение увеличивается на единицу. Когда счетчик достигает значения TTL, пакет сбрасывается, и ICMP сообщение посылается обратно источнику показывая, что пакет не может быть доставлен.

Повторение IPv4 адресации

IPv4 адресация была рассмотрена детально в предыдущих частях. Сейчас, мы повторим несколько ключевых моментов, так как они относятся к роутерам и процессу маршрутизации.

- Каждое сетевое оборудование имеет свой уникальный IP адрес.
- Маска подсети используется для определения какая часть адреса используется для адреса хоста, а какая для адреса подсети.
- Хосты могут общаться друг с другом в одной подсети, не проходя через роутер.
- Трафик должен проходить через роутер, когда пакет посылается из одной подсети в другую.
- Когда мы используем DHCP/Bootp чтобы дать адрес компьютеру, любой роутер между арендующим (принимающим IP адрес) хостом и DHCP сервером должен быть настроен на передавание DHCP сообщений к DHCP серверу.

- Широковещательные сообщения могут быть потеряны, если на используемом роутере не настроена поддержка Мультикаста.
- Приватные IP адреса не могут быть использованы для связи через Интернет.

Эти моменты в основном касаются IPv4 адресации, но большинство роутеров сейчас поддерживают как IPv4, так и IPv6.

Протоколы маршрутизации

Каждый роутер хранит таблицу маршрутизации, или RIB, которая содержит IP адреса и информацию о маршрутах. Вы можете создавать статические записи в таблице, но это занимает много времени и не эффективно. В дополнение к сказанному, таблица маршрутизации не адаптируется к изменениям в сетевой среде. Для таких случаев, у вас должна быть информация, которая обновляется автоматически.

Откуда роутеры получают информацию для маршрутизации? Она приходит от других роутеров, через динамические обновления через протоколы маршрутизации. Протоколы маршрутизации позволяют роутерам делиться информацией с их таблиц с другими маршрутизаторами.

Есть два основных типа проколов маршрутизации. Протокол маршрутизации обычно касается либо внутренней маршрутизации, либо внешней маршрутизации.

Внутренний протокол маршрутизации (Interior gateway routing protocol, **IGRP**)

Протоколы, разработанные для работы с роутерами развернутыми в LAN и WAN окружениях.

Внешний протокол маршрутизации (Exterior gateway routing protocol, **EGRP**)

Протоколы для обеспечения интернет маршрутов.

Мы будем фокусироваться на протоколах внутренней маршрутизации. Далее протоколы могут быть разделены на маршрутизацию с анализом каналов (link-state routing protocols) и дистанционно-векторную маршрутизацию (distance-vector routing protocols).

Протоколы маршрутизации с анализом каналов

Маршруты основаны на множестве факторов, включая количество прыжков к месту назначения, а так же, полосу пропускания, скопления трафика, и другие факторы которые уменьшают эффективность.

Основные среди внутренних протоколов маршрутизации – RIPv1, RIPv2, RIPng и OSPF.

Протокол информации о маршрутизации версия 1 (Routing Information Protocol version 1, **RIPv1**)

Оригинальная версия протокола RIP.

Протокол информации о маршрутизации версия 2 (Routing Information Protocol version 2, **RIPv2**)

Обновление для протокола RIP, которое поддерживает формат адреса CIDR.

Протокол информации о маршрутизации, новое поколение (Routing Information Protocol, next generation, **RIPng**)

Обновление к RIP, поддерживающие IPv6 адресы.

Протокол маршрутизации с определением кратчайшего пути (Open Shortest Path First, **OSPF)**
Общий протокол с маршрутизацией с анализом каналов (link-state).

Есть еще другие внутренние протоколы которые используются, такие как IS-IS (Intermediate System-Intermediate System – пер. Промежуточная система – Промежуточная система), но детальное обсуждение этого протокола лежит за рамками этого курса.

RIP

RIP обычно достаточно чтобы удовлетворить нужды сетей среднего-малого бизнеса. Его также легко настроить, что делает его популярным выбором для маленьких сетей

Есть 3 версии RIP:

- RIPv1

  Оригинальная версия, разработанная для поддержки только бесклассовых сетей.
- RIPv2

  Выпущенный как замена для первой версии, включает встроенную поддержку CIDR и маски подсети с меняющейся длинной.
- RIPng

Разработан для поддержки IPv6 маршрутизации.

RIP имеет некоторые нерешаемые недостатки. Как результат, медленная конвергенция, особенно в относительно больших сетях. RIP протокол так же ограничен на поддержку не больше 15 прыжков на маршруте. Это лимит сети, которую может поддерживать RIP.

Convergence

Конвергенция – это состояние, в котором все роутеры имеют актуальную информацию для маршрутизации.

RIP использует 3 механизма, чтобы предотвратить рассылку неправильной информации через сеть:

- **Split horizon** (дословно Расщепленный горизонт)

  Когда роутер получает обновление информации через интерфейс, он не будет (интерфейс) посылать свою информацию обратно через тот же интерфейс. Этот механизм разработан для предотвращения петель маршрутизации.
- **Route Poisoning** (дословно «Отравление» маршрута)

  Механизм, используемый для определения роутера как недостижимого. Это делается с помощью выставления маршрутной метрики на значение 16 (которая обозначается как недостижимая) перед тем как послать маршрут. Роутеры, получившие это сообщение, удалят этот маршрут из их таблиц.

- **Holddown** (дословно Придерживать)

  Роутер запускает таймер, как только получает сообщение, что другой роутер недостижим по этому маршруту. Пока таймер считает, роутер будет игнорировать любые сообщения, которые будут говорить, что роутер достижим. Роутер может обновлять информацию о маршруте после того как таймер закончится. Таймер по умолчанию устанавливается на 180сек для RIP.

Сейчас мы тщательнее рассмотрим каждую RIP версию.

RIPv1

RIPv1 имеет несколько недостатков, которые привели к его замене. Среди недостатков: отсутствие поддержки масок подсети с изменяющейся длинной, CIDR, и IPv6 адресации. RIP использует широковещательные сообщения, что может излишне

потреблять полосу пропускания и уменьшает эффективность. Обновления не несут информацию про подсети.

RIPv2

RIPv2 добавил поддержку для масок подсети с меняющейся длинной и CIDR.

Тем не менее, RIPv2 был разработан, чтобы быть обратно совместимым, так же предоставляя поддержку бесклассовой маршрутизации и ограничивая количество прыжков на маршруте 15-ю. RIPv2 посылает обновления через мультикастную передачу на адрес 224.0.0.9, достигая всех смежных роутеров. Каждый принимающий маршрутизатор обрабатывает эти обновления, обновляет свою RIB (при необходимости), а затем отправляет новые обновления соседнему маршрутизатору.

RIPng

RIPng был разработан для обеспечения distance-vector протокола для IPv6 адресов. RIPng так же был разработан как улучшение к RIP2, и не всегда совместим с роутерами использующими только RIP1.

OSPF

OSPF – это наиболее используемый протокол маршрутизации в больших сетях. Он позволяет более эффективную маршрутизации и большую эффективность связи, потому что OSPF так же учитывает такие параметры как полоса пропускания, поддерживаемая различными роутерами. OSPF так же отвечает на изменение сетевой топологии, например неработающий канал или роутер. OSPF способен быстро вычислить и компенсировать эти и другие меняющиеся условия.

Специальные роутеры

Часто бывает, что роутеры выполняют множество действий, чтобы сохранить количество систем, подключенных к Интернет минимальным. Это особенно важно, если они развернуты в сети периметра (perimeter network).

Firewalls (файерволы)

Есть два базовых типа файерволов: host-based и network-based. Host-based файерволы работают на компьютере пользователя и разработаны, чтобы защищать только пользователя. Network-based были разработаны для защиты сетей.

Файрволы были разработаны для защиты хоста или сегмента сети с помощью фильтрации трафика проходящего из и в файервол. Это может осуществляться через порт фильтрации, который блокирует или пропускает трафик, основываясь на номере

порта. Более сложные роутеры управляют трафиком, основываясь на адресах источника и места назначения и даже на основании контента пакета.

Конфигурация файрволов

Две наиболее распространённые конфигурации файрволов это network-based файрволы с двумя сетевыми адаптерами и файрволы с тремя сетевыми адаптерами. Мы рассмотрим общие конфигурации периметр-сетей, чтобы увидеть, как они используются.

На нашем первом примере, периметр-сеть ограничена двумя файрволами (рисунок 6-8). Один находится между периметр-сетью и публичным интернетом. Второй между периметр-сетью и внутренней сетью.

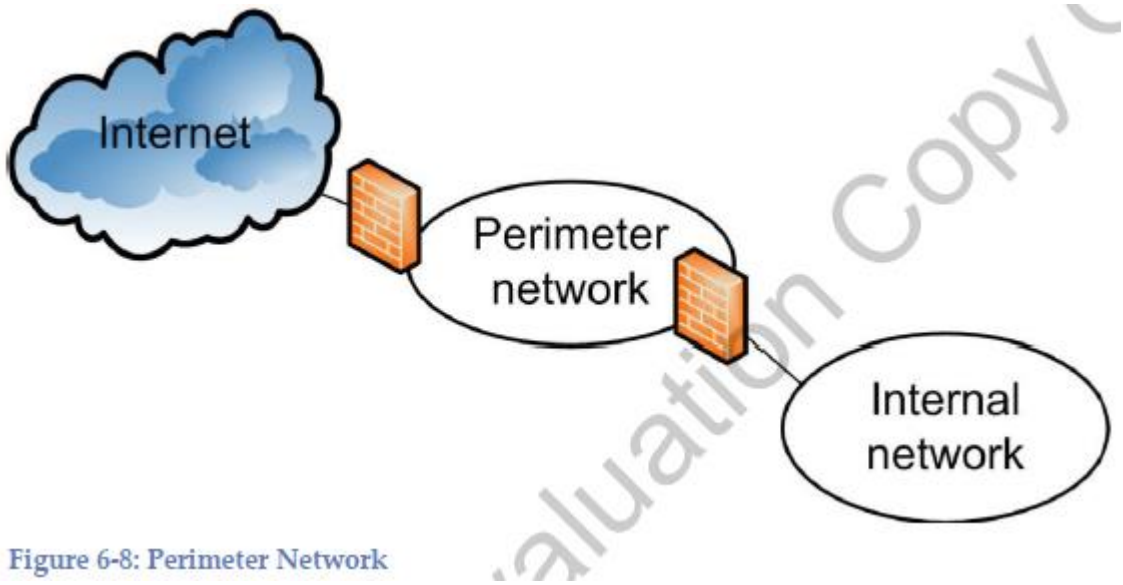


Figure 6-8: Perimeter Network

Рисунок 6-8: Периметр-Сеть

Вам иногда придется столкнуться с периметр-сетью с одним настроенным файрволом. В этом примере файрвол устанавливается с тремя сетевыми адаптерами.

Вы можете встретить эту конфигурацию еще как three-prong firewall (3-х зубцовый файрвол). Один из адаптеров файрвола подключен к интернету, один к периметр-сети и один к внутренней сети. Трафик между любыми двумя должен пройти через файрвол.

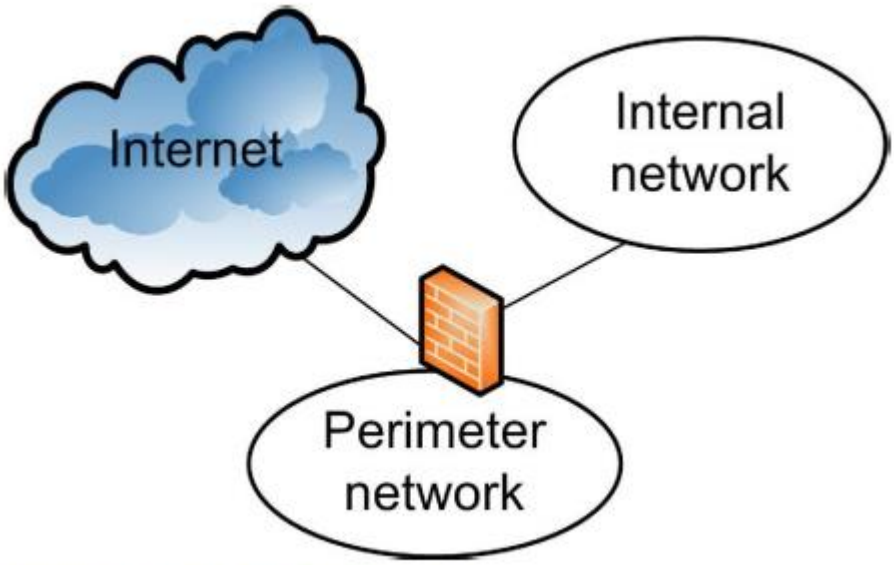


Figure 6-9: Alternate Configuration

Рисунок 6-9: Альтернативная конфигурация

Эта конфигурация с одним файрволом иногда считается менее защищенный, чем использование двух файрволов. Есть вероятность, что файрвол может быть перегружен в момент пиковой нагрузки. Есть также более прямой канал между внутренней сетью и Интернетом, по которому намного проще атаковать вашу подсеть.

Прокси-сервер

Прокси-серверы (прокси) помогают управлять доступом к сети. Согласно определению, прокси это любой сервер, который ведет себя как посредник между хостом и другим компьютером, чаще всего другим сервером. На практике, прокси-сервера наиболее часто используются для предоставления клиентского доступа в Интернет. Прокси-сервер часто реализуется на той же аппаратной платформе, что и обращенный к Интернет файрвол в периметр-сети в маленьких сетях. Он может быть развернут как отдельное устройство.

Основные прокси операции

Теперь, мы изучим базовые прокси операции (рисунок 6-10). В сети с прокси-сервером, клиент хочет получить информацию с сервера в Интернете. Он посылает запрос прокси-серверу. Прокси фильтрует запрос, основываясь на правилах настроенных на сервере, и посылает его в Интернет если запрос удовлетворяет правилам.

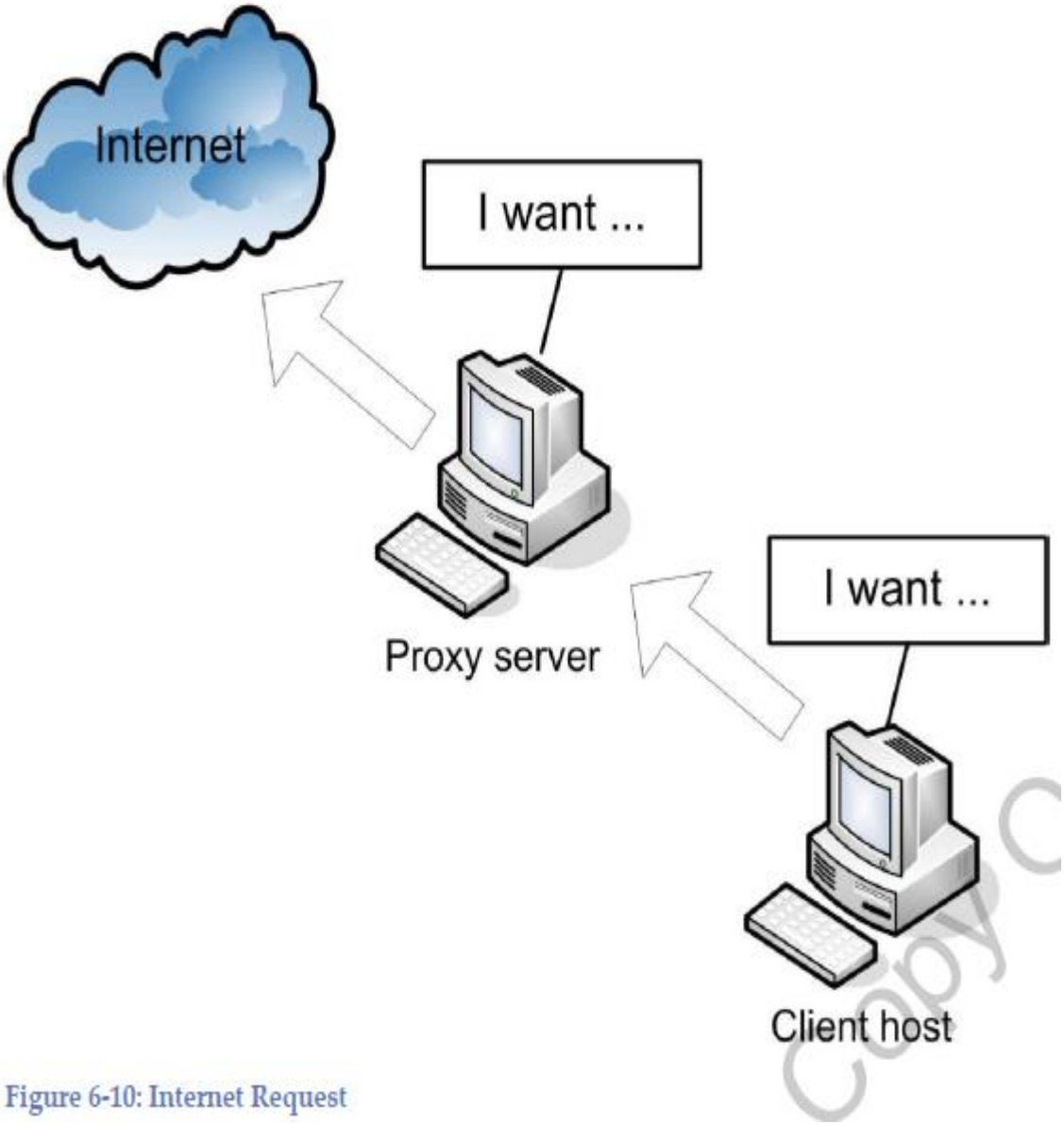


Figure 6-10: Internet Request

Рисунок 6-10: Интернет запрос

Фильтрация часто проводится по серверу, который является местом назначения, таким образом, ограничивая Интернет доступ по URL. Тем не менее, могут использоваться и другие методы, такие как фильтрация контента.

Фильтрация контента

Процесс фильтрации запросов основанный на информации содержащейся в пакете.

Процесс ответа аналогичен. Интернет сервер посылает ответ (рисунок 6-11). Еще раз, он проходит через фильтр прокси-серверы, перед тем как быть доставленным клиенту.

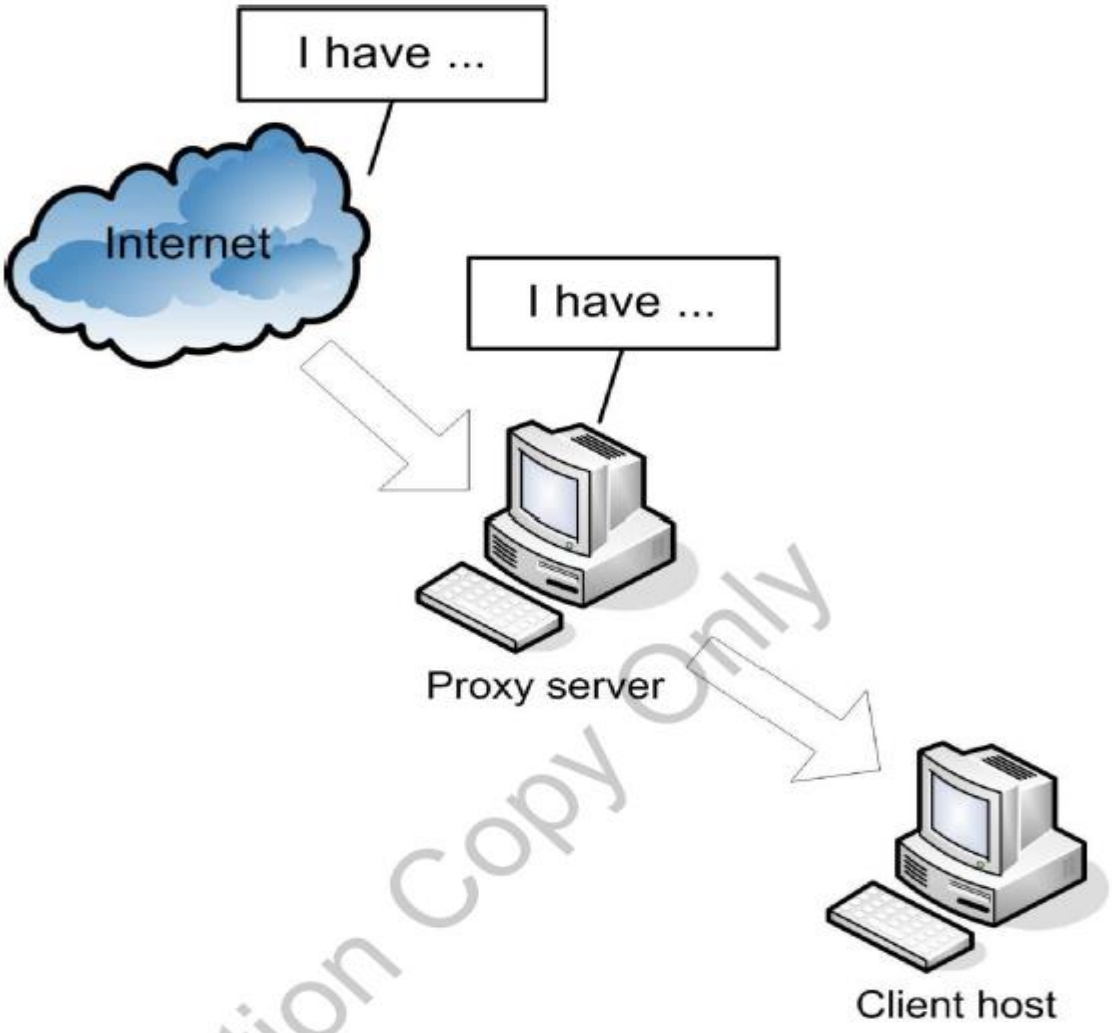


Рисунок 6-11:

Вдобавок, ответ обычно кэшируется на прокси-сервере. Если другой клиент (или тот же), посылает тот же запрос, прокси отвечает ему из своего кэша вместо того чтобы еще раз обращаться к Интернету. Это помогает уменьшить трафик между вами и Интернетом.

Типы прокси-серверов

Типы базовых прокси

- Пересылающий прокси (forwarding proxy)
  Клиент называет специфические серверы, к которым он хочет иметь доступ. Прокси берет запросы из внутренней сети и пересылает их в Интернет.
- DNS прокси

Специализированный пересылающий прокси, который пересылает DNS запросы к внешнему DNS серверу и возвращает результат клиенту.

- Открытый прокси (open proxy)
  Может пересылать пакеты из внутренней сети в Интернет и наоборот.

- Обратный прокси (Reverse proxy)
  Получает запросы из Интернета и направляет их во внутреннюю сеть

Когда используется обратный прокси, внешний клиент может даже не знать о существовании внутренней сети.

Обратный прокси дает дополнительный уровень безопасности для вашей сети. Вы можете как обычно настроить обратный прокси для работы с кодированием/декодированием для серверов, которые это поддерживают. Обратный прокси может так же обеспечивать балансировку нагрузки, когда поддерживается множество веб-сервисов.

NAT

Ранее в курсе мы рассматривали NAT. Функциональность NAT обычно реализуется на роутере в периметр-сети, особенно в маленьких сетях.

Мы быстро вспомним необходимость использования NAT. Так как доступные публичные IPV4 адреса становятся дефицитными, стало привычным использование приватных адресов внутри локальных сетей. Тем не менее, они не могут быть использованы в Интернете, поэтому частные адреса должны быть переведены в публичные адреса для интернет-трафика.

Рассмотрим базовый функционал NAT (рисунок 6-12).

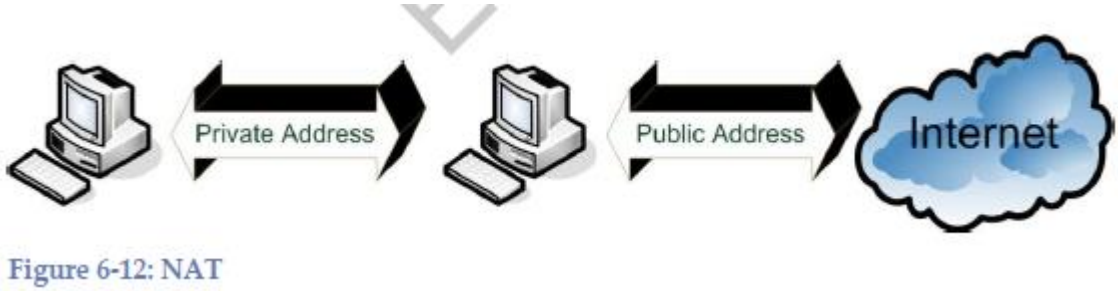


Figure 6-12: NAT

Рисунок 6-12: NAT

Пакеты, поступающие с транспортного уровня TCP\IP, для передачи содержат адрес источника и места назначения. Многие сети используют приватные адреса внутри сетей, но это может вызвать большие проблемы. Приватные адреса не могут быть использованы в Интернете.

Чтобы обойти это, пакеты посылаться через NAT сервер. NAT заменяет IP адрес источника публичным адресом и посылает его в Интернет. Когда ответ (или подтверждение) возвращается назад, NAT совершает обратный процесс. Публичный адрес заменяется оригинальным приватным адресом, и пакет посылается оригинальному источнику.

VPN

Мы рассматривали VPN ранее в курсе. Но они заслуживают дополнительного рассмотра, так как роутеры используют как конечные VPN точки когда VPN кончается LAN-ом. VPN могут быть использованы в LAN-to-LAN конфигурациях как защищенные каналы между сетями (рисунок 6-13).

В этом случае, роутеры используются как конечные точки на обоих концах.

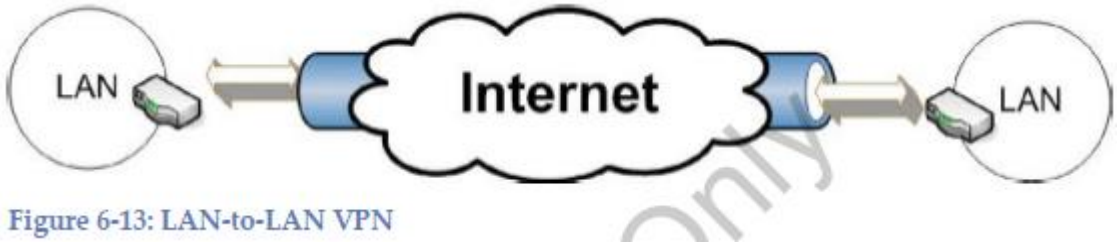


Figure 6-13: LAN-to-LAN VPN

Рисунок 6-13: LAN-to-LAN VPN

Другая возможность использования VPN как поддержки удаленного защищенного доступа в PC -LAN конфигурации (рисунок 6-14). Роутер ведет себя как конечная точка на конце LAN к VPN-у. PC настроен как конечная VPN точка на другом конце. Конечные LAN точки могут быть настроены так, чтобы поддерживать множественные одновременные удаленные соединения. Вы можете сконфигурировать конечную точку в центральном офисе, чтобы обеспечить удаленный доступ и к PC, и к LAN.

Figure 6-14: PC-to-LAN VPN

Рисунок 6-14: PC-to-LAN VPN

В защищенных VPN, конечные точки аутентифицируются перед тем как туннели развертываются. Защищенное соединение, в большинстве ситуаций, обеспечивается через кодирования информации. Обычно, VPN соединение прозрачно для конечного пользователя.

Наиболее распространенным туннельным протоколом является L2TP. Он имеет схожую функциональность с более старым протоколом PPTP, который до сих пор используется некоторыми программами.

L2TP (Туннельный протокол 2-го уровня, Layer 2 Tunneling Protocol)

Популярный VPN туннельный протокол.

PPTP (Туннельный протокол точка-точка, Point-to-Point Tunneling Protocol)

Старый туннельный протокол, который все еще используется.

L2TP популярный выбор для реализации VPN-ов. Тем не менее, присутствует потенциальная проблема, так как L2TP сам по себе не предоставляет поддержки для сильной аутентификации или защиты информации. Вы можете добавить эти необходимые приложения, используя IPsec вместе с L2TP.

IPsec (Интернет протокол Безопасности, Internet Protocol Security)

Набор протоколов предоставляющих аутентификацию и шифрование.

IPsec реализован на Интернет уровне в TCP/IP модели. Плюсы этого приложения заключаются в том, что приложения не должны специально разрабатываться для использования IPsec. Безопасность применяется к данным на выход и удаляется на обратном пути.

Преимущество использования L2TP с IPsec заключается в обеспечении безопасности между хостом-источником и хостом-местом назначения. PPTP обеспечивает безопасность только между двумя конечными VPN точками.

Выводы:

В этой главе вы выучили:

- Основную функциональность роутеров и их использование.
- Software против hardware роутеров.
- Назначение и цель таблиц маршрутизации и информации о маршруте.
- Протоколы маршрутизации и их использование.
- Специализированные роутеры и их использование.

Заключение

Благодаря возникновению и развитию сетей передачи данных появился новый, высокоэффективный способ взаимодействия между людьми. Компьютерные сети стали проникать буквально во все области человеческой деятельности. При этом большинство сетей существуют независимо друг от друга, решая конкретные задачи для конкретных групп пользователей. В соответствии с этими задачами выбираются те или иные сетевые технологии и аппаратное обеспечение.

Построить универсальную физическую сеть мирового масштаба из однотипной аппаратуры просто невозможно, поскольку такая сеть не может удовлетворять потребности всех ее потенциальных пользователей. Одним нужна высокоскоростная сеть для соединения машин в пределах здания, а другим - надежные коммуникации между компьютерами, разнесенными на сотни километров.

Чтобы обеспечить эффективную работу компании в условиях экономики идей, отдел ИТ должен превратиться из центра затрат в отдел, создающий добавленную стоимость. Создание и воплощение новых идей, бизнес-моделей, решений и методов потребует использования новых видов программного обеспечения или приложений, учета новых рисков, реализации новых способов создания, эксплуатации и использования технологии, которая теперь не просто поддерживает бизнес, но САМА ЕСТЬ бизнес.

Hewlett Packard Enterprise помогает заказчикам в построении эффективной, продуктивной и безопасной ИТ-среды посредством соединения традиционных подходов с новыми, что позволяет компаниям быстро реагировать на идеи создавая, используя и развивая новые решения на основе лучшего опыта и лучших бизнес-моделей.

Hewlett Packard Enterprise помогает выбрать и внедрить вычислительные мощности, которые могут оказать значительное влияние на результаты и эффективность бизнеса, построить хранилище, способное «думать» в не меньшей степени, чем хранить, использовать сети, осуществляющие обмен данными быстрее и безопаснее, чем когда либо.

Литература

1. FRANK MILLER. Designing & Deploying Network Solutions for Small and Medium Business. Instructor Textbook Rev. 1.0. – 2014. – 602 p.

2. Designing & Deploying Network Solutions for Small and Medium Business. Student Lab Guide Rev. 1.0. – 2014. – 125 p.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 4-ое издание. Издательство: Питер – 2010 – 944 с.