Министерство сельского хозяйства Республики Узбекистан
Ташкентский государственный аграрный университет

КУРСОВЯ РАБОТА

Кафедра Информационные системы и технологии

На тему: Виртуальные компьютерные сети: организация и функционирование..

Приниял:

_____

Выполнил: _____

Тошкент 2023 г

СОДЕРЖАНИЕ

ВВЕДЕНИК

Возрастание мощностей вычислительной техники и общий уровень прогресса информационной науки стали главными факторами в процессе разработки и внедрения интегрированных вычислительных сетей. Набор отдельных вычислительных сетей, которые связаны между собой в общую сеть при помощи каналов связи и специальных сопрягающих устройств представляет собой интерсеть.

Естественно, основной целью создания сетей является обеспечение информационного обмена между двумя вычислительными машинами, которые входят в сеть. Самой крупной по своим объемам и количеству подсоединенного компьютерного оборудования считается «глобальная

паутина», то есть, сеть Интернет. Сегодня практически все крупные, да и мелкие компании, а также некоторые опытные пользователи имеют в сети Интернет свои сайты. Сайты позволяют хранить информацию в интернете в удобном и доступном виде.

Возникшая сравнительно недавно технология виртуальных локальных сетей (Virtual LAN, VLAN) позволила преодолеть многие из существовавших ограничений. Виртуальной сетью

является группа узлов сети, трафик которой, включая широковещательный, на канальном уровне является полностью изолированным от других узлов.

Технология VLAN способна облегчить процесс формирования изолированных сетей, связь между которыми реализуется при помощи маршрутизаторов с поддержкой протокола сетевогоуровня, к примеру, IP. Данное решение способно создать существенно более

мощные ограничения на пути ошибочного трафика из одной сети в другую.

.

1.1 “Организация и функционирование виртуальных компьютерных сетей”

В границах виртуальной компьютерной сети реализуется логическое объединение группы пользователей компьютерной сети в противоположность их физическому объединению,

которое основано на территориальных признаках и сетевой топологии. Подобные сети способны полностью ликвидировать физические барьеры на пути создания рабочих групп «по интересам» в масштабах сети более высокого уровня, но особенно это является актуальным для корпоративных компьютерных сетей, так как появляется возможность объединить физически разрозненных работников компании в группы пользователей при сохранении целостности связей внутри групп.

При этом может быть обеспечена повышенная организационная гибкость в процессах управления компанией. Технология виртуальных компьютерных сетей дает возможность сетевым администраторам сгруппировать различных пользователей корпоративной сети,

которые совместно пользуются одним и теми же сетевыми ресурсами. Подразделение корпоративной сети на логические сегменты, каждый из которых является виртуальной

компьютерной сетью, способно предоставить совокупность значительных преимуществ в администрировании сети, обеспечении безопасности информации, в управлении

широковещательными передачами из виртуальной сети по магистрали корпоративной сети.

Использование виртуальной компьютерной сети в корпоративной среде обладает рядом

преимуществ перед другими методами объединения сегментов сети. К ним в первую очередь

следует отнести:

1. Возможность формирования функциональных рабочих групп.

2. Возможность контроля широковещательного трафика.

3. Повышенный уровень безопасности информации, исключающий несанкционированный

доступ.

В виртуальных компьютерных сетях можно относительно несложно решать проблемы, которые связаны с перемещениями, добавлениями и изменениями. Организация таких сетей предоставляет возможность сокращения административных издержек, в случае смены

пользователями своих рабочих мест, а, помимо этого, технология виртуальных сетей способна предоставить очень много преимуществ для межсетевых взаимодействий.

Формирование рабочих групп по физическому расположению сетевого компьютерного оборудования, как это реализуется в сетях с разделяемой средой, очень часто может создать

трудноразрешимые проблемы. Это может стать причиной переноса рабочих мест пользователей или передачи больших информационных объемов через сильно загруженные

маршрутизаторы. Помимо этого, трудоемкость настройки маршрутизаторов превращает практически в нереальную задачу формирования временных рабочих групп из числа

удаленных друг от друга сотрудников.

Коммутация компьютерных сетей способна обеспечить реализацию создания виртуальных сетей из групп пользователей, опираясь на стоящие перед ними задачи, а не по физическому местоположению в сети. Пользователи,

которые остаются в своей рабочей группе, имеют

возможность свободного перемещения по сети. Возможность простого перемещения и добавления узлов виртуальной сети, а также других изменений в сети совместно с возможностью эффективной интеграцией традиционных локальных компьютерных сетей, способны повысить уровень гибкости в корпоративной сети.

Виртуальные компьютерные сети, по сути, могут считаться составной частью ATM-архитектур (Asynchonous Transfer Mode, то есть, асинхронной передачи данных), поэтому сама концепция и некоторые технологические принципы

виртуальных сетей уже осуществлены в коммутаторах

локальных сетей, предлагающих аналогичные преимущества при коммуникациях через разделяемые магистрали локальных компьютерных сетей.

Для конечного пользователя виртуальная компьютерная сеть, как часть коммутируемой архитектуры, может быть невидимой. Создание виртуальной компьютерной сети можно

рассматривать не только в качестве решения по эффективному применению разделяемых концентраторов, маршрутизации, коммутации или сетевого управления. Она является сочетанием всех этих элементов, которое обеспечивает гибкую сегментацию и высокоэффективное администрирование всей сети.

В связи с этой тенденции, актуальность данной темы весьма открыта. И нет сомнений того, что компьютерная сеть является неотъемлемой частью информационных технологий для передачи, хранения и использования информации. Выбранная автором тема по назначению и использованию локальных сетей является актуальной в настоящее время, так как в любой организации, фирме, предприятии, учебном заведении, где стоят персональные компьютеры, наличие LAN LAN (Local Area Network) - Сокращённое обозначение локальной компьютерной сети присутствует всегда.

Самая крупная по своей объёмности и наличию подключённых компьютеров является "Глобальная паутина" - Internet. В настоящее время довольно много людей знает про существование Интернета. Все крупные и мелкие предприятия, организации и даже опытные пользователи имеют в Интернете свой сайт Сайт - Документ в формате htm или php где хранится информация любого содержания, имеющая свой индивидуальный адрес в сети Интернет. . Благодаря сайтам информация в интернете хранится в удобном и доступном виде. Все достоинства и недостатки локальных сетей их назначение, использование, настройка, протяжка и использование будет рассмотрено в данной курсовой по дисциплине "Сети ЭВМ и телекоммуникации”.

Предметом исследования в курсовой работе является виртуальная, локальная компьютерная сеть о которой слышал практически каждый человек так или иначе связанный с компьютером.

Появившаяся несколько лет тому назад, технология виртуальных локальных сетей (Virtual LAN, VLAN) позволяет преодолеть указанное ограничение. Виртуальной сетью называется группа узлов

сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов.

Технология VLAN облегчает процесс создания изолированных сетей, связь между которыми осуществляется с помощью маршрутизаторов с поддержкой протокола сетевого уровня, например IP. Такое решение создает гораздо более мощные барьеры на пути ошибочного трафика из одной сети в другую.

Технология виртуальных сетей предоставляет гибкую основу для построения крупной сети, соединенной маршрутизаторами, так как коммутаторы позволяют создавать полностью изолированные сегменты программным путем, не прибегая к физической коммутации.

1.2 Способы построения виртуальных сетей

Все способы построения виртуальных сетей можно разбить на несколько основных схем:

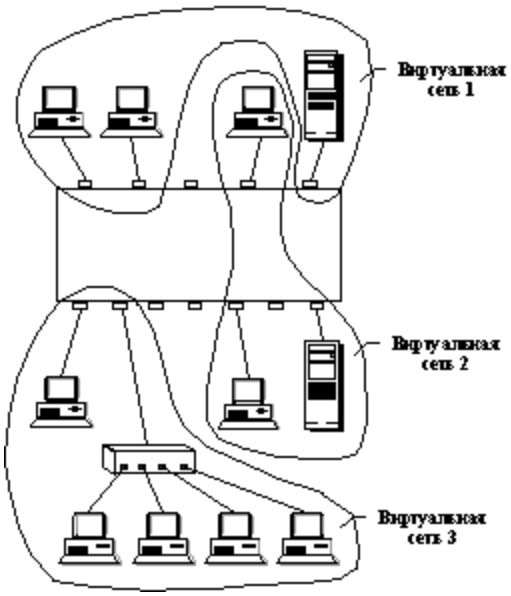
- группировка портов;
- группировка MAC-адресов;
- добавление к кадрам меток номеров виртуальных сетей;
- использование стандарта LANE для образования виртуальных сетей в сетях, построенных на коммутаторах ATM;
- использование сетевого уровня.

Все способы за исключением последнего решают проблему создания виртуальных сетей на канальном уровне и поэтому не зависят от протоколов, работающих в сети на верхних уровнях. Последний способ требует, чтобы во всех узлах сети работал какой-либо протокол сетевого уровня - IP, IPX, AppleTalk и т.п. В этом случае концепция виртуальной сети совпадает с пониманием этого

термина на сетевом уровне, то есть виртуальная сеть IP является подсетью IP, а виртуальная сеть IPX является сетью IPX. [3]

• Группировка портов является самым простым способом разделения VLAN. Суть этого способа состоит в том, что каждый порт коммутатора помечается номером VLAN, к которой относится этот порт. Тогда при передаче каждого кадра коммутатор проверяет, принадлежит ли получатель той же VLAN, что и отправитель. Если да, то кадр направляется по указанному MAC-адресу, иначе кадр выбрасывается. (рисунок 5)

Этот способ прост и удобен для сетевого администратора. Но этот способ обладает одним серьезным недостатком. Он вызван тем, что при передаче кадра от одного коммутатора к другому (а получатель кадра может быть подключен не к тому же коммутатору, что и отправитель) информация о принадлежности источника к определенной VLAN никак не передается. Поэтому для корректного разделения VLAN необходимо связать “фрагменты” VLAN, расположенные на каждой паре соседних коммутаторов отдельным каналом, не используемым другими VLAN. При сколь либо большом количестве VLAN (а в большой сети их могут быть сотни) возникает проблема нехватки числа портов коммутатора. Поэтому на практике этот способ используется в сочетании с третьим из указанных выше способов. [4]



Виртуальные сети, построенные на одном коммутаторе

• Группировка MAC-адресов. При использовании этого способа все MAC-адреса одной сети канального уровня помечаются номерами включающих их VLAN. Этот способ свободен от недостатков предыдущего. Но он требует большого объема кропотливой работы сетевого администратора, как при проведении начальной разметки, так и при ее изменениях, выполняемых при замене, добавлению и удалению компьютеров (их сетевых карт) размечаемой сети.

Описанные два подхода основаны только на добавлении дополнительной информации к адресным таблицам моста и не используют возможности встраивания информации о принадлежности кадра к виртуальной сети в передаваемый кадр. Остальные подходы используют имеющиеся или дополнительные поля кадра для сохранения информации и принадлежности кадра при его перемещениях между коммутаторами сети. При этом нет необходимости запоминать в каждом коммутаторе принадлежность всех MAC-адресов интерсети виртуальным сетям.

• Добавление к кадрам меток номеров виртуальных сетей. В этом способе к обычному кадру локальной сети формата Ethernet, TokenRing или FDDI добавляется специальное поле для хранения номера виртуальной сети. Оно используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно удаляется. При этом модифицируется протокол взаимодействия "коммутатор-коммутатор", а программное и аппаратное обеспечение конечных узлов остается неизменным. Примеров таких фирменных протоколов много, но общий недостаток у них один - они не поддерживаются другими производителями. Компания Cisco предложила использовать в качестве стандартной добавки к кадрам любых протоколов локальных сетей заголовок протокола 802.10, предназначенного для поддержки функций безопасности вычислительных сетей. Сама компания использует этот метод в тех случаях, когда коммутаторы объединяются между собой по протоколу FDDI. Однако, эта инициатива не была поддержана другими ведущими производителями коммутаторов. [4]

Новый стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети.

Стандарт IEEE 802.1p специфицирует метод указания приоритета кадра, основанный на использовании новых полей, определенных в стандарте IEEE 802.1Q.

Спецификация IEEE 802.1p, создаваемая в рамках процесса стандартизации 802.1Q, определяет метод передачи информации о приоритете сетевого трафика. Стандарт 802.1p специфицирует алгоритм изменения порядка расположения пакетов в очередях, с помощью которого обеспечивается своевременная доставка чувствительного к временным задержкам трафика.

Существует два способа построения виртуальных сетей, которые использует уже имеющиеся поля для маркировки принадлежности кадра виртуальной сети, однако эти поля принадлежат не кадрам канальных протоколов, а пакетам сетевого уровня или ячейкам технологии ATM.

- использование стандарта LANE для образования виртуальных сетей в сетях, построенных на коммутаторах ATM. (рисунок 6)

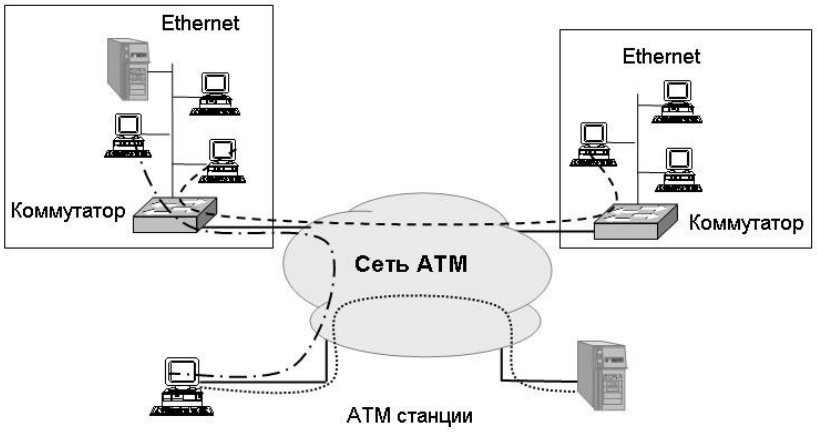
Технология ATM (Asynchronous Transfer Mode — режим асинхронной передачи) является одной из самых перспективных технологий построения высокоскоростных сетей. Она обеспечивает максимально эффективное использование полосы пропускания каналов связи при передаче различного рода информации: голоса, видеоинформации, данных от самых разных типов устройств — асинхронных терминалов, узлов сетей передачи данных, локальных сетей и т.д. (к таким сетям относятся практически все ведомственные сети). Сети, в которых используется ATM-технология, называются ATM-сетями**.** Эффективность ATM-технологии заключается в возможности применения различных интерфейсов для подключения пользователей к сетям ATM.

Спецификация LANE вводит такое понятие как эмулируемая локальная сеть - ELAN. Это понятие имеет много общего с понятием виртуальной сети:

- ELAN строится в сети, состоящей из коммутаторов (коммутаторов ATM);
- связь между узлами одной и той же ELAN осуществляется на основе MAC-адресов без привлечения сетевого протокола;
- трафик, генерируемый каким-либо узлом определенной ELAN, даже широковещательный, не выходит за пределы данной ELAN.

Кадры различных ELAN не свешиваются друг с другом внутри сети коммутаторов ATM, так как они передаются по различным виртуальным соединениям и номер виртуального соединения VPI/VCI является тем же ярлыком, который помечает кадр определенной VLAN в стандарте 802.1Q и аналогичных фирменных решениях.

Если VLAN строятся в смешанной сети, где имеются не только коммутаторы ATM, то "чистые" коммутаторы локальных сетей, не имеющие ATM-интерфейсов, должны использовать для создания виртуальной сети один из выше перечисленных методов, а пограничные коммутаторы, имеющие наряду с традиционными еще и ATM-интерфейсы, должны отображать номера VLAN на номера ELAN при передаче кадров через сеть ATM.



Использование технологи LANE

- использование сетевого уровня

При использовании этого подхода коммутаторы должны для образования виртуальной сети понимать какой-либо сетевой протокол. Такие коммутаторы называют коммутаторами 3-го уровня, так как они совмещают функции коммутации и маршрутизации.

Каждая виртуальная сеть получает определенный сетевой адрес - как правило, IP или IPX.

Тесная интеграция коммутации и маршрутизации очень удобна для построения виртуальных сетей, так как в этом случае не требуется введения дополнительных полей в кадры, к тому же администратор только однократно определяет сети, а не повторяет эту работу на канальном и сетевом уровнях. Принадлежность конечного узла к той или иной виртуальной сети в этом случае задается традиционным способом - с помощью задания сетевого адреса. Порты коммутатора также получают сетевые адреса, причем могут поддерживаться нестандартные для классических маршрутизаторов ситуации, когда один порт может иметь несколько сетевых адресов, если через него проходит трафик нескольких виртуальных сетей, либо несколько портов имеют один и тот же адрес сети, если они обслуживают одну и ту же виртуальную сеть. [5]

При передаче кадров в пределах одной и той же виртуальной сети коммутаторы 3-го уровня работают как классические коммутаторы 2-го уровня, а при необходимости передачи кадра из одной виртуальной сети в другую - как маршрутизаторы. Решение о маршрутизации обычно принимается традиционным способом - его делает конечный узел, когда видит на основании сетевых адресов источника и назначения, что кадр нужно отослать в другую сеть.

Однако, использование сетевого протокола для построения виртуальных сетей ограничивает область их применения только коммутаторами 3-го уровня и узлами, поддерживающими сетевой протокол. Обычные коммутаторы не смогут поддерживать такие виртуальные сети, и это является большим недостатком.

По этим причинам наиболее гибким подходом является комбинирование виртуальных сетей на основе стандартов 802.1 Q/p с

последующим их отображением на "традиционные сети" в коммутаторах 3-го уровня или маршрутизаторах. Для этого коммутаторы третьего уровня и маршрутизаторы должны понимать метки стандарта 802.1 Q.

1.3 Оборудование для построения виртуальных сетей

*поддержка интерфейсов и протоколов только локальных сетей;

*усеченные функции маршрутизации;

*поддержка механизма виртуальных сетей;

Коммутатор 3 уровня и маршрутизатор: сходства и различия

Сходства:

Коммутатор 3 уровня является как коммутатором, так и маршрутизатором: его можно рассматривать как маршрутизатор с несколькими портами Ethernet и с функцией коммутации. Коммутатор 3 уровня включает коммутацию пакетов, проверяя их IP-адреса и MAC-адреса. Таким образом, коммутаторы уровня 3 могут разделить порты на отдельные VLAN и выполнять маршрутизацию между ними. Как и традиционный маршрутизатор, коммутатор 3 уровня также

можно настроить для поддержки протоколов маршрутизации, таких как RIP, OSPF и EIGRP.

Различия:

- Аппаратное обеспечение - основное различие между коммутатором L3 и маршрутизатором. Аппаратное обеспечение внутри коммутатора 3 уровня сочетает его с традиционными коммутаторами и маршрутизаторами, обеспечивая более высокую производительность для локальных сетей. Кроме того, коммутатор 3 уровня, разработанный специально для использования в интрасетях, обычно не имеет портов WAN и обладает функциями, которыми обычно обладает традиционный маршрутизатор. Таким образом, коммутатор 3 уровня часто используется для поддержки маршрутизации между VLAN.
- Интерфейсы - еще одно различие между коммутатором L3 и маршрутизатором. коммутатор 3 уровня ограничен в поддерживаемых им интерфейсах. В то время, как у маршрутизатора есть больше опций, таких как SDH, SONET, E1/T1 и т.д. Кроме того,

маршрутизаторы были устройствами, которые подключали LAN к WAN, а коммутаторы были просто устройствами LAN.

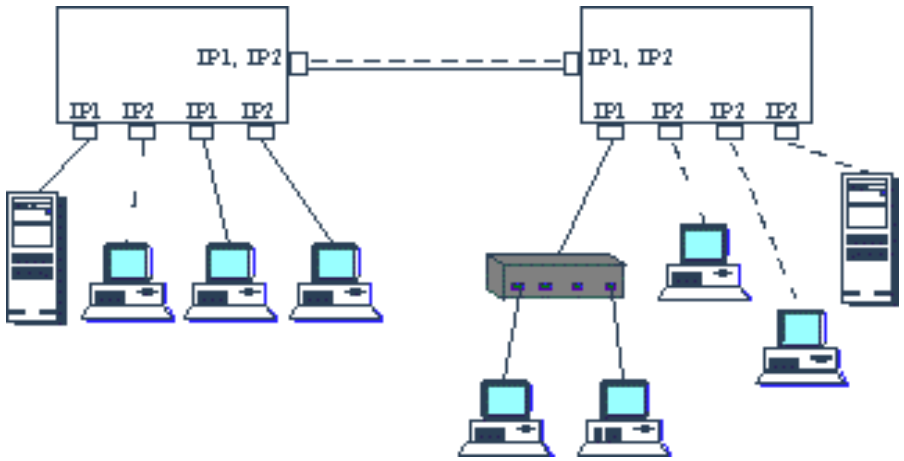
- Принцип работы – коммутатор 3 уровня просматривает MAC-адрес хоста назначения и отправляет кадр только этому получателю. Маршрутизатор ссылается на целевой IP-адрес, а не на его MAC-адрес, поэтому он обеспечивает больше функциональных возможностей, чем простая маршрутизация пакетов, например назначение IP-адресов (DHCP) и фильтрация брандмауэра. [6]

Усеченные функции маршрутизации выражаются у разных производителей по разному. Часто коммутаторы не поддерживают функции автоматического построения таблиц маршрутизации, которые поддерживаются протоколами маршрутизации, такими как

RIP или OSPF. Такие коммутаторы должны работать в паре с маршрутизатором и получать от него готовые таблицы маршрутизации. По такой схеме взаимодействует коммутатор Catalist 5000 компании Cisco с маршрутизаторами этой же компании.

Если же коммутатор третьего уровня поддерживает протоколы RIP и OSPF (последний в силу своей сложности реализуется в коммутаторах третьего уровня реже), то его ограниченность часто проявляется в поддержке только протокола IP, или же IP и IPX.

Тесная интеграция коммутации и маршрутизации удобна для администратора и часто повышает производительность. Во первых потому, что можно определить сначала виртуальные сети на основании информации только второго уровня, например, с помощью группировки портов, а затем, при необходимости объявить эти виртуальные сети подсетями IP и организовать в этом же устройстве их связь за счет маршрутизации



Объединение виртуальных сетей с помощью коммутатора 3-го уровня

Если же коммутатор не поддерживает функций сетевого уровня, то его виртуальные сети могут быть объединены только с помощью внешнего маршрутизатора. Некоторые компании выпускают специальные маршрутизаторы для применения совместно с

коммутаторами. Примером такого маршрутизатора служит маршрутизатор Vgate компании RND, изображенный на рисунке 8.

Этот маршрутизатор имеет один физический порт для связи с портом коммутатора, но этот порт может поддерживать до 64 MAC-адресов, что позволяет маршрутизатору объединять до 64 виртуальных сетей. [3]

1.4 Что такое VPN?

Сервисы VPN предназначены для людей чтоб они безопасно пользовались и интернетом.

Это технология обеспечивает сохранность корпоративных и правительственных сетей. В наши дни она доступна каждому.

Преимущества и недостатки

Рассмотрим преимущества и недостатки использования VPN-сервисов. К плюсам относят следующее: Возможность скрыть личность в интернете. Маскировка IP-адреса и шифровка интернет-трафика гарантирует, что никто не сможет следить за вами в интернете. Обход геоблокировки. Иногда на сайт нельзя войти, поскольку он заблокирован в той или иной стране. Это и есть геоблокировка. При помощи VPN-сервиса можно выбрать ту страну или тот регион, в котором сайт не заблокирован. Это позволит

беспрепятственно открыть интернет-страницу. Защита сетевого подключения. Рекомендуется использовать VPN при подключении к бесплатному общественному Wi-Fi. По этой сети киберпреступники могут украсть данные кредитной карты, банковские реквизиты, логин и пароль от электронной почты или социальных сетей. VPN шифрует все онлайн-коммуникации и гарантирует, что никто не сможет отследить деятельность в интернете. Обход файрвола. Находясь на работе, в университете, в аэропорту или даже отеле, можно столкнуться с применением файрволов, настройки которых блокируют некоторые сайты. VPN позволяет легко обойти файрвол в такой ситуации. К минусам стоит отнести: замедление интернет-скорости; неправильный выбор VPN может поставить под угрозу конфиденциальность; качественные VPN-сервисы платные; не все устройства поддерживают VPN по умолчанию. Специалист по интернет-безопасности Макс Эдди пишет, что самая большая проблема с VPN связана не с технологиями, а с доверием, поскольку весь трафик проходит через системы VPN-компаний. При желании они могут видеть все, что пользователи делают в интернете, а затем продавать эти данные. Они могут размещать рекламу на просматриваемых веб-сайтах.

Как выбрать VPN.

Многие VPN-компании стараются получить доверие пользователей, но это сделать крайне сложно. Перед выбором VPN-сервиса обязательно изучайте политику конфиденциальности, чтобы понять, какие усилия компания прилагает для ее защиты. Еще придерживайтесь таких советов по выбору VPN: изучите характеристики (скорость интернета, тип шифрования, анонимность

и прочее); проверьте совместимые устройства; найдите сервис с

дружественным пользовательским интерфейсом, чтобы проще было установить и настроить VPN; убедитесь, что сможете работать с серверами тех регионов, которые необходимы (у каждой компании ограниченный список серверов в разных уголках мира); определитесь, подходит ли тарифный план; убедитесь, что сервис предоставляет гарантию на возврат денег за услуги. Как подключить VPN? Сначала выберите VPN-сервис, а затем перейдите на официальный компании. Возможно, придется зарегистрироваться на портале. Дальше скачайте программное обеспечение на компьютер или телефон, выполните установку. Запустите приложение, активируйте тарифный план и запустите VPN. Не верьте тому, что все VPN-провайдеры предоставляют абсолютно одинаковые услуги. Сначала решите, что нужно от VPN, а затем выберите правильный сервис, основываясь на собственных требованиях и предпочтениях.

Топология локальной сети

Первое к чему нужно приступать при изучении основ функционирования компьютерных сетей, это топология (структура) локальной сети. Существует три основных вида топологии: шина, кольцо и звезда.

Линейная шина

Все компьютеры подключены к единому кабелю с заглушками по краям (терминаторами). Заглушки необходимы для предотвращения отражения сигнала. Принцип работы шины заключается в следующем: один из компьютеров посылает сигнал всем участникам локальной сети, а другие анализируют сигнал и если он предназначен им, то обрабатывают его. При таком взаимодействии, каждый из компьютеров проверяет наличие сигнала в шине перед отправкой данных, что исключает возникновения коллизий. Минус данной топологии — низкая производительность, к тому же, при повреждении шины нарушается нормальное функционирование локальной сети и часть компьютеров не в состоянии обрабатывать либо посылать сигналы.

Кольцо

В данной топологии каждый из компьютеров соединен только с двумя участниками сети. Принцип функционирования такой ЛВС заключается в том, что один из компьютеров принимает информацию от предыдущего и отправляет её следующему выступая в роли повторителя сигнала, либо обрабатывает данные если они предназначались ему. Локальная сеть, построенная по кольцевому принципу более производительна в сравнении с линейной шиной и может объединять до 1000 компьютеров, но, если где-то возникает обрыв сеть полностью перестает функционировать.

Звезда

Топология звезда, является оптимальной структурой для построения ЛВС. Принцип работы такой сети заключается во взаимодействии нескольких компьютеров между собой по средствам центрального коммутирующего устройства (коммутатор или свитч). Топология звезда позволяет создавать высоконагруженные

масштабируемые сети, в которых центральное устройство может выступать, как отдельная единица в составе многоуровневой ЛВС. Единственный минус в том, что при выходе из строя центрального коммутирующего устройства рушится вся сеть или её часть. Плюсом является то, что, если один из компьютеров перестаёт функционировать это никак не сказывается на работоспособности всей локальной сети.

Что такое MAC-адрес, IP-адрес и Маска подсети?

Прежде чем познакомиться с основными принципами взаимодействия сетевых устройств, необходимо подробно разобрать, что такое IP-адрес, MAC-адрес и Маска подсети. MAC-адрес, IP-адрес и Маска подсети.

MAC-адрес — это уникальный идентификатор сетевого оборудования, который необходим для взаимодействия устройств в локальной сети на физическом уровне. MAC-адрес «вшивается» в сетевую карту заводом изготовителем и не подлежит изменению, хотя при необходимости это можно сделать на программном уровне. Пример записи MAC-адреса: 00:30:48:5a:58:65.

IP-адрес – это уникальный сетевой адрес узла (хоста, компьютера) в локальной сети, к примеру: 192.168.1.16. Первые три группы цифр IP-адреса используется для идентификации сети, а последняя группа для определения «порядкового номера» компьютера в этой сети. Если провести аналогию, то IP-адрес можно сравнить с почтовым адресом, тогда запись будет выглядеть так: регион.город.улица.дом. Изначально, использовались IP-адреса 4-ой версии (IPv4), но когда количество устройств глобальной сети возросло до максимума, то данного диапазона стало не хватать, в следствии чего был разработан протокол TCP/IP 6-ой версии — IPv6. Для локальных сетей достаточно 4-ой версии TCP/IP протокола.

Маска подсети – специальная запись, которая позволяет по IP-адресу вычислять адрес подсети и IP-адрес компьютера в данной сети. Пример записи маски подсети: 255.255.255.0. О том, как происходит вычисление IP-адресов мы рассмотрим чуть позже.

Что такое ARP протокол или как происходит взаимодействие устройств ЛВС?

ARP — это протокол по которому определяется MAC-адрес узла по его IP-адресу. Например, в нашей локальной сети есть несколько компьютеров. Один должен отправить информацию другому, но при этом знает только его IP-адрес, а для взаимодействия на физическом уровне нужен MAC-адрес. Что происходит? Один из компьютеров отправляет широковещательный запрос всем участникам локальной сети. Сам запрос, содержит IP-адрес требуемого компьютера и собственный MAC-адрес. Другой компьютер с данным IP-адресом, понимает, что запрос пришел к нему и в ответ высылает свой MAC-адрес на тот, который пришел в запросе. После чего собственно и инициализируется процесс передачи информационных пакетов.

Сетевой коммутатор и маршрутизатор (роутер)

Для согласования работы сетевых устройств используется специальное сетевое оборудование — коммутаторы и маршрутизаторы. Исходя из рассмотренного выше, важно понять простую истину — коммутаторы работают с MAC-адресами, а маршрутизаторы (или роутеры) с IP-адресами.

Коммутатор содержит таблицу MAC-адресов устройств локальной сети непосредственно подключенных к его портам. Изначально таблица пуста и начинает заполняться при старте работы коммутатора, происходит сопоставление MAC-адресов устройств и портов, к которым они подключены. Это необходимо для того, чтобы коммутатор напрямую пересылал информационные пакеты тем

участникам локальной сени, которым они предназначены, а не опрашивал все устройства ЛВС.

Маршрутизатор также имеет таблицу, в которую заносит IP-адреса устройств на основе анализа локальной сети. Роутер может самостоятельно раздавать IP-адреса устройствам ЛВС благодаря протоколу динамического конфигурирования узла сети (DHCP). Таблица маршрутизации позволяет роутеру вычислять наикратчайшие маршруты для отправки информационных пакетов между различными узлами ЛВС. Данные узлы (компьютеры) могут находиться в любом сегменте многоуровневой сети невзирая на архитектуру той или иной подсети. К примеру, маршрутизатор связывает локальную сеть с глобальной (интернет) через сеть провайдера.

Что такое NAT?

В последнем пункте данной статьи, рассмотрим, что такое NAT. Как уже упоминалось ранее, маршрутизатор связывает между собой сети не только на локальном уровне, но и взаимодействует с сетью провайдера с целью получения доступа к сети интернет. Для пересылки пакетов во внешнюю сеть, роутер не может использовать IP-адреса компьютеров из локальной сети, так как данные IP-адреса являются «частными» и предназначены только для организации взаимодействия устройств внутри ЛВС. Маршрутизатор имеет два IP-адреса (внутренний и внешний), один в локальной сети (192.168.1.0), другой (к примеру 95.153.133.97) ему присваивает сеть провайдера при динамическом распределении IP-адресов. Именно второй IP-адрес роутер будет использовать для отправки и получения пакетов по сети интернет. Для реализации такой подмены и был разработан NAT.

NAT (Network Address Translation) — механизм преобразование сетевых адресов, является частью TCP/IP-протокола.

ЛИТЕРАТУРЫ

1. Астахова, И.Ф. Компьютерные науки. Деревья, операционные системы, сети / И.Ф. Астахова и др. - М.: Физматлит, 2013. - 88 с.

2. Астахова, И.Ф. Компьютерные науки. Деревья, операционные системы, сети / И.Ф. Астахова, И.К. Астанин и др. - М.: Физматлит, 2013. - 88 с.

3. Баринов, В.В. Компьютерные сети: Учебник / В.В. Баринов, И.В. Баринов, А.В. Пролетарский. - М.: Academia, 2018. - 192 с.

4. Баринов, В.В. Компьютерные сети: Учебник / В.В. Баринов. - М.: Академия, 2015. - 256 с.

5. Кузин, А.В. Компьютерные сети: Учебное пособие / А.В. Кузин.. - М.: Форум, НИЦ Инфра-М, 2013. - 192 с.

6. Кузин, А.В. Компьютерные сети: Учебное пособие / А.В. Кузин, Д.А. Кузин. - М.: Форум, 2018. - 704 с.

7. Кузьменко, Н.Г. Компьютерные сети и сетевые технологии / Н.Г. Кузьменко. - СПб.: Наука и техника, 2013. - 368 с.

8. Куроуз, Д. Компьютерные сети. Нисходящий подход / Д. Куроуз, К. Росс. - М.: Эксмо, 2016. - 912 с.

9. Куроуз, Дж. Компьютерные сети: Нисходящий подход / Дж. Куроуз. - М.: Эксмо, 2018. - 800 с.

10. Луганцев, Л.Д. Компьютерные сети / Л.Д. Луганцев. - М.: МГУИЭ, 2001. - 452 с.

11. Максимов, Н.В. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - М.: Форум, 2017. - 320 с.

12. Максимов, Н.В. Компьютерные сети: Учебное пособие для студентов учреждений среднего профессионального образования / Н.В. Максимов, И.И. Попов. - М.: Форум, НИЦ Инфра-М, 2013. - 464 с.

13. Новожилов, Е.О. Компьютерные сети: Учебное пособие / Е.О. Новожилов.

- M.: Academia, 2017. - 288 с.
14. Новожилов, Е.О. Компьютерные сети / Е.О. Новожилов. - М.: Academia,