Скачать Cisco Tracer – симулятор КС (как только попробуем статическую / динамическую модель. Посчитать общее количество оконечных узлов, которым мы располагаем)

Сеть – это совокупность устройств и систем, которые подключены друг к другу и общаются между собой (сервер, компьютеры, маршрутизаторы, телефоны и пр.). По размерам она достигает размера всеобщей паутины. Минимум может состоять из двух компов, где один из них является ведущим, а другой ведомый – сеть без выделенного сервера.

Из чего состоит сеть:

1. Оконечное устройство (узел, End-device) – устройства, которые передают или принимают какие-либо данные. (Компы, телефоны, сервера и пр.)
2. Промежуточные узлы (устройства) – устройства, которые соединяют оконечные узлы между собой (маршрутизаторы, коммутаторы, концентраторы, всевозможные модемы, точки доступа Wi-Fi и т.д.)
3. Сетевые среды – та область, где происходят непосредственно передача данных (кабели, сетевые карты, различного рода коннекторы, в т.ч воздушную среду передачи)

Основные средства, используемые для создания КС:

1. Приложения. При помощи приложения мы отправляем разные данные между устройств (открываем доступ, например). При этом приложения могут быть консольными и с графическим интерфейсом.

Приложения:

* Загрузчики – файловые менеджеры, работающие по протоколу FTP или TFTP (скачивание музыки, фильмов и пр.) – создается некий файлообменник между источником и потребителем. К этой категории можно отнести и резервное копирование, т.е. это встроенное или стороннее ПО или утилита, которая предназначена для копирования (скачивания)

FTP – это стандартный протокол передачи данных с установленным соединением и работает по протоколу TCP через порт 21

TFTP – это упрощенная версия протокола FTP и работает без установления соединения по протоколу UDP

Разница между FTP и TFTP – приложения по протоколу FTP могут догружать файлы при ошибке предыдущей разгрузке, а при TFTP – нет (придется всё заново качать).

* Интерактивное приложения (ISQ, например)
* Приложения в реальном времени (Zoom)

1. Сетевые ресурсы. (Сетевые принтеры, сетевые камеры)
2. Хранилища. Используя сервер или рабочую станцию, подключенную к сети, как место хранения данных (Гугл/Яндекс диск)
3. Резервное копирование
4. Отдельно стоящая IP-телефония. Работает она по протоколу IP, применяется повсеместно и традиционную телефонию вытесняет.

Топология КС

Топология КС делится на две большие категории:

1. Физическая – сеть, как выглядит на самом деле (коммутаторы, провода)
2. Логическая – каким путём будут идти пакеты в нашей физической топологии

Виды топологий:

1. Топология с общей шиной – одна из первых физических топологий. Суть в том, что к одному длинному кабелю подсоединили все устройства. Таким образом образовали локальную сеть. На концах кабеля установлены терминаторы (заглушка с R = 50 Ом).

Преимущества – очень простая, дешевая и длина с использованием репитеров может быть бесконечной.

Недостаток – если в кабеле происходит разрыв, то вся сеть парализуется до места замены кабеля

(картинка с прямой линией шины)

1. Кольцевая топология – в данной топологии каждое устройство подключено к двум соседним, таким образом образуется кольцо. Логика работы следующая: с одного конца компьютер только принимает, а с другого только отправляет. Т.е получается передача по кольцу, и следующий компьютер играет роль репитера, засчет этого отпадает нужда в терминаторах и репитерах. Для решения проблемы работоспособности сети применяется двойное кольцо, т.е. в каждое устройство входит два кабеля

(схема топологии)

1. Звезда
2. Полносвязная топология
3. Смешанная топология (древовидная)

Стандарты кабелей:

1. Американский стандарт EIA 568
2. Международный стандарт IDO 11801
3. Общий европейский EN 50173

Эти стандарты определены для 4-х типов кабелей:

1. Неэкранированная витая пара
2. Экранированная витая пара
3. Коаксиальный кабель
4. Волоконнооптический кабель

Характеристики кабелей:

1. Затухание [Дб/м] для определенной частоты
2. Перекрёстные наводки на ближнем конце [Дб/м] для определённой частоты
3. Импеданс – волновое сопротивление – полное сопротивление. Волновое сопротивление для коаксиального кабеля = 50 Ом, и 100-120 Ом для неэкранированной витой пары
4. Уровень защиты от внешнего электромагнитного излучения (электрический шум) [миллиВольт]. До 150 КГц источником фонового электрического шума являются линии электропередач, линии дневного света. От 150 КГц до 20 МГц источником шума является оргтехника. От 20 МГц до 1 ГГц телевизионные и радиопередатчики

Витая пара – одна или несколько пар изолированных проводников, скрученных между собой.

Витая пара имеет следующие разновидности:

1. Неэкранированная витая пара (UTP)
2. Экранированная витая пара (STP)
3. Фольгированная витая пара (FTP)
4. Фольгированная экранированная витая пара (SFTP)

Также может быть одно- и многожильные кабели, где одножильный кабель не предполагает прямых контактов с подключаемой периферией

Кабели на основе витой пары медные неэкранированные делятся на 5 категорий по своим электромеханическим свойствам:

1. Кабель категории один – применяется в случаях, где не требуется высокая скорость передачи данных для аналоговой и цифровой передачи голоса
2. Кабель категории два - используется для построения фирмы IBM для построения собственной сети. Основное требование – передача сигнала со спектром 1 МГц
3. Кабель категории три
4. Кабель категории четыре – улучшенный вариант кабеля категории три, способный выдерживать сигналы на частоте до 20 МГц
5. Кабель категории пять – кабель, разработанный для поддержки высокоскоростных протоколов (неэкранированный, 100Мб, 200 метров FastEthernet)

Вариант Ethernet на основе витой пары использует четырёхжильный кабель UTP. Кабели UTP выпускаются в двух- и четрырёхпарном исполнении. В последнем две пары предназначены для передачи данных, а две другие пары для передачи голоса. Для соединения используется разъём RJ45.

Отдельно в категории кабелей витой пары находятся кабели шестой и седьмой категории. 6-ая категории диапазоном 200 МГц, 7-ая – 600 МГц и обязательно экранируются. Причем каждая пара отдельно и провод в целом. Кабель категории 6 может как экранироваться, так и нет. – 10 ГБитов

1Е – это одна пара (лапша)

Cat1 – полоса частот 0.1 МГц (полоса пропускания), телефонный кабель 1 пара (лапша). Используется для передачи голоса или данных при помощи модема

Cat2 – 1 МГц, две пары проводников, поддерживает передачу данных до 4 Мбит/сек используется в телефонных сетях

Cat3 – 16МГц, двух парное исполнение, скорость передачи до 10Мбит/сек

Cat4 – 20Мгц, четыре скрученных пары, скорость передачи до 16 Мбит/сек

Cat5 – до 100МГц, четыре пары, скорость до 100Мбит/сек

Улучшенный кабель 5Е – 125 МГц, две пары, скорость до 100Мбит/сек, а в четырех парах до 1Гбит/сек на расстоянии 100 метров

Cat6E – 500 МГц, позволяет пропускать высокочастотные сигналы, скорость 100Мбит/сек

Cat7 – 600-700МГц, скорость до 100Гбит/сек

Протокол Token Ring – это протокол передачи данных с топологией кольца и маркерным доступом. Находится на канальном уровне модели OSI

Механизм работы передача данных в такой сети может осуществляться станцией владеющей маркером, маркер представляет собой 3-х байтный блок данных. Если узел, принимающий маркер, владеет информацией для ее передачи, то он его захватывает, а если станция не имеет информации передачи, то станция пересылает этот маркер следующей станции. При захвате маркера, станция меняет один бит и превращает маркер в блок начала передачи данных – добавляет к нему информацию, предназначенную для передачи, и отправляет эту посылку следующей станции. Станция, получив этот блок, проверяет, кому эта информация предназначена, так информационный блок проходит по кольцу, пока не достигнет получателя. Станция, получившая информацию, предназначенная для нее, копирует ее, ставит отметку о получении и отправляет дальше, по кольцу, следующей станции. Эта информация должна вернуться отправителю. После достижения этой информации до отправителя, отправитель анализирует ее, и при отсутствии ошибок, превращает эту последовательность в маркер и отправляет дальше по кольцу, следующей станции. Пока по кольцу двигается информационный блок, передача данных о других станциях невозможна. Каждая станция имеет право удерживать маркер определённое количество времени. По умолчанию – 10 мс. Такая технология передачи данных позволяет уйти от коллизий, главный недостаток любой Ethernet’овской сети. Сети с передачей маркера являются детерминистическими. То есть можно очень точно вычислить максимальное время, которое пройдет прежде чем любая конечная станция сможет передавать. Эта характеристика, а также характеристика надежности делает сеть Token Ring идеальной для применения, где задержка должна быть предсказуемой, и важна устойчивость функционирования сети. Максимум станций - 1024

Протокол FDDI – это протокол, основанный на оптоволоконно распределённом интерфейсе передачи данных до 200 км и в связи со специфической сферой применения сетей, построенных по этому протоколу, дальнейшее увеличение расстояния было нецелесообразно. Скорость передачи 100 Мбит/сек.

Технология:

Стандарт FDDI используется в сетях на основе топологии двойного кольца с передачей маркера. В качестве среды передачи используется оптоволоконный кабель. Стандарт определяет физический уровень и часть канального уровня. При этом передача данных по двум кольцам осуществляется противоположным направлением. Одно кольцо называется первичным, второе – вторичным. В физическом выражении кольцо состоит из двух или 2+ точечных соединений между смежными станциями.

Все станции делятся на две группы:

1. Станции класса Б – станции, подключенные к одному кольцу
2. Станции класса А – станции, подключенные к двум кольцам

Станции, подключенные к одному кольцу, подключены через концентратор (- отвечает за то, что в случае отказа или отключения питания любой станции Б, кольцо не прерывалось бы, когда как аналоговое устройство имеет питание, которое часто включается или выключается)

FDDI поддерживает полосу пропускания в масштабе реального времени. Этот протокол обеспечивает поддержку, путем использования двух типов трафика – синхронного ( - может потреблять часть общей полосы пропускания сети. Оставшаяся часть потребляется асинхронным трафиком. Синхронная полоса выделяется станциям А) и асинхронного (Распределение асинхронной полосы осуществляется с использованием 8-и уровневой схемой управления приоритетов. Каждой станции присваивается свой приоритет. Механизм приоритетов этого протокола может фактически блокировать станции, которые могут пользоваться синхронной полосой)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PA | SD | FC | DA | SA | UDP | FCS | ED |
| 16 | 16 | 8 | 32 | 32 | 4478 \* 8 | 32 | 16 |

PA – преамбула – заголовок. Подготавливает каждую станцию для приема прибывающих блоков данных

SD – ограничитель. Начало указывает на начало блоков данных

FC – поле управления блоков данных. Указывает на размер адресных полей ( ахахахахаххахахаххахаххахахаххахахааххахах – Руслан)

DA, SA – адреса. Поле назначения, оно может содержать одно-/много-составной широковещательный адрес

UDP – информационный блок, содержащий инфу, предназначенную для протоколов высшего уровня, либо управляющую информацию

FCS – поле, содержащее контрольную информацию о последовательности блоков данных, т.е. заполняется величиной избыточности

ED – ограничитель конца

Модель OSI

Была разработана в 1984г.

Модели OSI:

1. Физический уровень – определяет метод передачи данных, т.е. какая среда передачи используется, уровень напряжения, метод кодирования
2. Канальный уровень – берет на себя задачу адресации в пределах локальной сети, обнаруживает ошибки, проверяет целостность данных. На этом уровне включается мак адрес

На этом уровне данные называются кадрами, а на физическом уровне происходит преобразование в биты

1. Сетевой уровень – этот уровень объединяет участки сети и делает путь оптимальным, т.е. осуществляется маршрутизация. Каждое сетевое устройство должно иметь уникальный адрес, т.е. у нас начинает работать протокол IP-4 (двоичная система кодирования) или IP-6 (16-ричная система счисления)
2. Транспортный уровень – этот уровень берет на себя функцию транспорта (- файл в виде сегментов отправляется на компьютер. Здесь мы должны использовать порт. На этом уровне у нас включается уровень TCP (- с установлением соединения) и UDP (- без установления соединения))
3. Сеансовый уровень – этот уровень устанавливает, управляет и разрывает соединения между хостами
4. Уровень представления – на этом уровне происходит структуризация информации, т.е. привидение информации в читаемый вид
5. Прикладной уровень – это уровни, где работают наши привычные всевозможные приложения по протоколам FTP, HTTP и т.д.

Прохождение информации осуществляется строго с верхнего на нижний и с нижнего на верхний. Пропускать какой-либо уровень нельзя, такой режим называется инкапсуляцией (с верхнего на нижний) и деинкапсуляция (с нижнего на верхний). На прикладном уровне, на уровне представления и сеансовом уровне передаваемая информация обозначается как PDU и называется “данными” или “блоками данных”. Информация транспортного уровня называют сегментами.

Датаграмма – это блок данных на транспортном уровне

Процесс инкапсуляции

1. Набираем адрес нашей страницы, используя протокол HTTP. Данные упаковываются и спускаются на уровень ниже (представления).
2. На уровне представления эти данные появляются.
3. На третьем, сеансовом уровне у нас происходит установлении сессии между компьютером и сервером
4. На транспортном уровне должно быть установлено какое-то соединение с протоколом TCP
5. Сетевой уровень – указываем, на какой адрес отправлять пакет, соответственно мы указываем свой IP адрес и IP сервера
6. Тут у нас IP пакеты, где добавляется физический адрес. На канальном уровне мы делаем соответствие между физическим и IP
7. На физическом уровне происходит преобразование в электрический сигнал

На сегодняшний день модель OSI состоит из 4-х уровней: (лет 10 назад)

1. Прикладной – первые верхние три уровня
2. Транспортный – без изменений
3. Уровень интернета – переименованный сетевой уровень
4. Уровень сетевого доступа – два нижних уровня объединили и переименовали

IP адрес

IP-адрес – представляет собой 32-х битную последовательность, состоит из 4 октет. Принято записывать IP-адрес в виде десятичных цифр, причем каждая группа октетов отделяется точками (192.168.32.124). Для того, чтобы правильно отобразить IP-адрес устройства нужно знать его маску. Маска также состоит из 4-х октет, каждый октет отделен друг от друга точкой (225.225.225.0). Маска предназначена для определения номера сети, в которой работает заданный конечный узел. Если наложить маску на IP-адрес, то единицы маски превращает любое значение в IP-адресе в ноль. Оставшееся значение и есть номер узла. IP-адрес может быть записан двумя способами: 10-тичным и префиксным (192.168.32.124 / 22 – значение после “/” указывает, сколько первых бит отведено под адрес сети)

Порядок определения количества узлов в текущей сети:

1. 2^(32 - номер\_префикса) – 2
2. Два адреса в любой сети являются служебными, а именно нулевой нельзя использовать. Он относится под номер сети и последний адрес (- это 255) используется под широковещательную рассылку

IP-адреса имеют два цвета:

1. белый ( - публичные IP-адреса. Используется для выхода в интернет. Адреса, которые используются в локальных сетях, относятся к частным, к серым, и не маршрутизируются в интернете. Публичные IP-адреса назначаются публичным web-сервером для того чтобы любой пользователь мог попасть на этот сервер вне зависимости от местонахождения)
2. серый ( - частные IP-адреса)

Основное отличие частных и публичных адресов заключается в том, что используя частный мы можем назначить компьютеру любой номер, главное, чтобы не было совпадающих номеров. С публичными адресами всё значительно сложнее: выдача публичных номеров контролируется различными организациями

Мы – провайдер – LIR – RIR – IANA – ICAN

Нам нужно обратиться к своему интернет-провайдеру для получения публичного IP-адресу. Если у него есть свободный номер – он его выдает. Если нет: он обращается к локальному интернет-регистратору (LIR). Для города выделен свой LIR – стырить у кого-то конспект

LAN – обычная сеть, наиболее популярная

MAN – городская сеть, эта сеть чуть больше, чем LAN, и является чем-то связующим между LAN и WAN

Сетевые устройства и термины

Маршрутизаторы – используются для соединения различных сетей (2+). Он отвечает за определение пути, отправляемых данных. Маршрутизатор рассматривается как устройство третьего уровня, т.к. он работает на уровне 3 модели OSI и использует IP-адреса в своём интерфейсе.

Коммутатор – отвечает за соединение оконечных устройств, является основной магистралью ЛС (локальной сети). Предоставляет возможность для различных компьютеров соединиться между собой. Работает на уровне 2 стандарта модели OSI – устройство второго уровня

Беспроводной маршрутизатор – предназначен для распределения интернета на несколько устройств (WiFi)

Точка доступа – используется вместо коммутатора (в телефонах) в беспроводной сети

Хаб – очень упрощенный вариант коммутатора (набор диодов и сопротивления). Позволяет соединить несколько компьютеров, при этом передача данных осуществляется в широковещательном диапазоне

Репитер – устройство, у которого только один вход и выход. Он просто усиливает сигнал

Иерархическая трехуровневая модель построения КС:

1. уровень ядра (самый высокий)
2. уровень распределения
3. уровень доступа

Такая модель помогает планировать масштабируемую, надежную, доступную по цене объединенную сеть

Уровень ядра – основное назначение уровня ядра – организация связи между двумя локальными сетями. Для выполнения этой задачи устройство уровня ядра должны быть освобождены от всех задач, которые могут сказываться на уменьшении скорости и достоверности данных. Данные, пересылаемые на этом уровне предназначены для всех пользователей

Общие ресурсы сети

Функции:

1. Функции ввода и отображения информации на основании пользовательского интерфейса
2. Прикладные функции. Их назначение – решение задач в предметной области
3. Функции управления ресурсами

Для того, чтобы эти функции выполнялись есть три взаимосвязанных компонента:

1. Компоненты представления отвечают за пользовательский интерфейс
2. Прикладные компоненты реализуют алгоритм решения конкретной задачи
3. Компоненты управления ресурсами

Основой любой сети является модель “Клиент-сервер” (двухзвенная архитектура)

Первые ПК чуть-чуть видоизменили схему. На ПК была своя ОС

Многоуровневые модели:

1. Трехзвенная модель – клиент -> сервер\_приложений -> сервер\_БД -> БД. Эта схема позволяет уменьшить затраты клиента на содержание технических средств у себя в организации

Типы серверов:

1. Веб-сервер – предназначен для хранения гипертекстовой информации + работа с бинарными файлами
2. Серверы БД – предназначен для хранения пользовательских запросов
3. Серверы приложений – предназначены для централизованного решения прикладных задач прикладного характера
4. Файл-серверы – хранят информацию в виде файлов и предоставляют доступ к ней
5. Прокси сервер – предназначены для организации связей между клиентов и глобальной сетью, а также позволяет сохранять частозапрашиваемую информацию в кэш-памяти на жестком диске
6. Firewall (брандмауэр) – предназначен для анализа и фильтрации входных данных, поступающих из внешней сети
7. Удаленные БД – предназначены для организации связей между удалёнными пользователями и сетью организации

STP протокол

Основные характеристики для компьютерных сетей:

1. Масштабируемость
2. Избыточность (с помощью дополнительных коммутаторов и/или дополнительных связей – два порта в одном направлении)

Широковещательная петля образуется в сетях, в которых присутствуют 2+ коммутаторов или когда имеется 1+ соединения между двумя коммутаторами или 2+ порта в одном направлении. Широковещательные петли приводят к возникновению ситуации, когда широковещательные фреймы будут загружать сеть и это приведет к неработоспособности – широковещательный шторм.

Протокол STP предназначен для предотвращения образования широковещательных петель, STP программно выключает лишние (запасные) каналы связи и в итоге создает топологию дерева. STP постоянно отслеживает топологию сети и поэтому при падении основных каналов связи по возможности подключает запасные. Т.к. создается топология дерева, то в ней обязательно должен присутствовать корень, который называется рут коммутатор, а остальные коммутаторы из него произрастают.

Основные принципы работы STP:

1. Выбор коммутатора в роли рут
2. Все остальные коммутаторы выбирают единственный порт, направленных на рут
3. Блокировка лишних запасных каналов связи

Виды портов:

1. Рут порт – это порт на рут коммутаторе (кроме рут коммутатора), который имеет наилучший путь к рут коммутатору
2. DP – это порт, который находится в режиме передачи данных
3. NDP – заблокированный порт (запасной)

Сама технология выбора рут коммутатора. Все коммутаторы в топологии STP имеют идентификатор, который называется Bridge ID (BID)

BID состоит из двух параметров:

1. Приоритет
2. Мак адрес

Коммутатор с наименьшим битом берет на себя роль рута, если сравнение приоритетов не позволило выявить рут – сравниваются мак адреса. Коммутатор с наименьшим маком выигрывает

В момент включения или перезагрузки все коммутаторы считают себя рутами и рассылают helloBPDU STP, а дальше вступает алгоритм определения: Если BID коммутатора, получившего сообщения оказывается больше полученного, то этот коммутатор перестает рассылать свои hello и передает только все остальные. В итоге остается только один рут с наименьшим BID

После того, как был определён рут, нам надо определить порты. Рут имеет только порты с обозначением DP (то есть на прием-передачу), далее у коммутатора будет RP или NDP. Затем коммутаторы определяют, кто является лишней связью. В таком случае у одного из них порт будет DP, а примыкающий к нему NDP (т.е. он будет заблокирован). Каждые две секунды определяется состояние, в котором они находятся. Как только оборвется одна из связей меж ними, то они автоматически разблокируют порт. Потом один из коммутаторов должен определить, у кого порт будет RP

Когда STP топология выстроена (найден рут), она начинает рассылать BPDU-STP сообщение, содержащее следующую информацию:

1. RootBridgeID коммутатора в роли рута
2. BridgeID отправителя – BID коммутатора, который отправил это сообщение
3. RootPatchCost – стоимость пути до рут коммутатора. Стоимость пути определяется путем сложения стоимости всех путей между коммутатором и рутом
4. Таймеры, установленные на рут – таймер отправки BPDU, таймер ожидания

Коммутаторы в роли рута рассылает BPDU каждые 2 секунды. Выходит это сообщение со стоимостью пути = 0. Приходя в остальные коммутаторы в STP топологии, стоимость увеличивается.

1. Рут коммутатор отправляет BPDU во все порты сообщение со значением поля RootPatchCost = 0.
2. Switch1 принимает BPDU, изменяет поле BridgeID отправителя на свой BID, а также изменяет поле RootPatchCost и прибавляет к текущему сообщению 19. После этого отправляет BPDU дальше по всем DP портам.
3. Switch3 принимает BPDU и аналогично с Switch1 меняет два поля
4. И т.д.

Для выбора рут порта используется следующий алгоритм:

1. Наименьшее значение RootPatchCost
2. Наименьшее значение BridgeID отправителя
3. Наименьший приоритет порта (локальные значения)
4. Наименьший номер порта

Выбор кто будет DP и кто будет NDP:

1. Наименьшее значение RootPatchCost
2. Наименьшее значение BridgeID отправителя

Режим работы портов STP протокола:

1. Блокинг – порт не передает фреймы, не принимает, не изучает мак адреса. Он принимает и обрабатывает BPDU сообщения. Если BPDU сообщение не приходит в течении 20 сек (время по умолчанию), порт переходит в следующий режим, т.е в режим NDP
2. Листинг – в этом режиме порт принимает и отправляет BPDU и отбрасывает все остальные фреймы. В этом режиме он находится 15 секунд (тоже по умолчанию)
3. Лёнинг – в этом режиме порт уже определил свое состояние (DP или RP), он не передаёт приходящие фреймы, но изучает их и заполняет таблицы мак адресов. В этом режиме он находится 15 сек
4. Форвардинг – порт передает все приходящие фреймы, работает в штатном режиме
5. Enable – запускает режим редактирования (в самом начале. Один раз)

Switch# – допустили к режиму, а выход exit = -1, end = полностью

1. Config terminal или conf t – режим конфигурации

Switch-config# = все успешно

Switch-config# vlan 1..1005 – номер виртуальной сети

Switch-vlan# - успешно создал

Switch-vlan# name – имя сети

Switch# show vlan – выводит список виртуальных сетей, которые существуют в коммутаторе

Vlan может работать в режиме access или Trunk

Переход на порт:

Interface номер\_порта (например, fa0/6)

Switch-interface# - указывает на то, что мы в режиме редактирования определённого порта

Switch-interface#

Switchport mode имя\_режима – присваивание определённого режима для порта

Switch#IP address ip\_адрес маска\_подсети

Принцип работы протокола DHCP

Это протокол прикладного уровня TCP IP. Предназначен для выделения IP адреса оконечному узлу (протокол динамической конфигурации хоста [- узла сети])

Принцип работы DHCP: - процесс называется DORA

1. D - Discovery (поиск). Здесь клиент в самом первом состоянии находится в состоянии инициализации. Не имеет своего IP адреса. Его действия: он отправляет широковещательный (на все устройства локальной сети, где находится DHCP Server. Их может быть несколько) broadcast с сообщением “DHCPDISCOVER”.

Общий принцип: сервер всегда слушает 67 порт, т.е. находится в ожидании широковещательного сообщения от оконечного узла. И после его получения отправляет его ответное предложение “DHCPOFFER”. Клиент принимает это сообщение на 68 порту.

Шаг закончился ответом сервера;

1. O – Offer. Сервер отвечает на поиск предложением, предлагает IP-адрес в этом предложением, которое может подойти клиенту. Этот IP-адрес выделяется из области SCOPE (- область доступных адресов. Этот массив формируется администратором), которая задается администратором.

Если имеются адреса, которые не должны быть выделены для предложения оконечному узлу, то область может быть ограничена, указав только разрешенные адреса.

Например можно выделить 192.0.0.100 - 192.0.0.254 и сервер может ими оперировать.

Не все адреса могут быть назначены клиентом. Для этого можно создать диапазон адресов, которые называются EXCLUDE (Исключением)

DHCP выделяет доступные IP-адреса из области только на время. Провайдер, подключая нас к себе, он также выделяет IP-адреса, и шанс, за который он нас закрепит – минимален. При каждом подключении наш IP адрес поменяется, то есть не закрепится за нами. Но есть возможность назначить какому-либо клиенту назначить определённый IP адрес. Чаще всего такое делают по отношению к сетевому принтеру. Такое закрепление IP-адреса за конкретным оконечным узлом называется резервацией (RESERVATION).

Наше предложение содержит IP из доступной области и направляется оконечному узлу широковещательной (BROADCAST) или прямым (UNICAST). В этот момент оконечный узел не имеет IP-адреса (состоит из номера узла и номера сети) и передача прямого сообщения осуществляется по Mac-адресу (- физическому адресу устройства);

1. R - Request (запрос). Клиент получает DHCPOFFER сообщение и отправляет серверу сообщение DHCPREQUEST, уведомляя сервер, что он принимает предложенный ему IP-адрес. В сообщении также указывается IP-адрес сервера. “Ты мне предоставил этот IP-адрес, и я принимаю его. Теперь ты знаешь об этом.”

Оконечное устройство этим сообщением говорит другим серверам, что конкретно этот IP-адрес занят.

1. A - Acknowledgement (подтверждение). Сообщение отправляет сервер. Получив от оконечного узла сообщение DHCPREQUEST, он окончательно подтверждает передачу IP-адреса клиенту. Для этого он высылает сообщение “DHCPACK”. Это может быть широковещательным или прямым сообщением, которое подтверждает владельца IP-адреса и период (срок аренды), на которое ему выделен этот адрес.

Срок аренды при динамическом распределении – DHCP сервер выделяет из области и оставляет там запись резервирования конкретного IP-адреса за определённым оконечным устройством и здесь же указывается срок действия (срок аренды / LEASE TIME). Этот срок может быть от 24 часов до нескольких месяцев. Этот параметр указывается в настройках сервер.

В чем необходимость предоставления адреса в аренду:

1. Отключение или выход из строя оконечного узла, обеспечивает возможность использования предоставленного IP-адреса другим устройствам;
2. Есть возможность при необходимости предоставить оконечному узлу уникальный адрес;

После получения адреса оконечное устройство берёт его в аренду на конкретное время, что будет зафиксировано переходом в состояние BOUND. После достижения половины срока аренды клиент активизирует процедуру получения нового IP-адреса и обновления адреса (RENEWING). Процесс повторного получения проходит по упрощённой схеме. Формируется прямой запрос DHCPREQUEST от оконечного узла, начиная с третьего шага, а сервер подтверждает запрос DHCPACK. После время аренды начинает новый отсчет (если сервер подтвердил). Если подтверждение не поступает, то оконечное устройство запрашивает адрес по истечению первой половины, делая новый запрос, т.е. это тогда, когда наступит 25%. Следующий запрос будет отправлен по истечению еще одной половины оставшегося времени и т.д., пока не наступит 7/8 от всего времени аренды. После этого все запросы на аренду IP-адреса будут широковещательными. (сервер может не отвечать и устройство начинает решать проблему самостоятельно)

Три подхода для распределения IP-адресов:

1. Статическое распределение – когда на компе делаем вручную
2. Динамическое распределение – назначение на определенное время
3. Автоматическое распределение – сервер закрепляет адреса из области НАВСЕГДА. Т.е. срок аренды не ограничен

Опции DHCP

Для работы в сети оконечному узлу требуется не только IP, но и маска сети, шлюз по умолчанию и адрес сервера. Опции представляют собой пронумерованные пункты – строки данных, которые содержат необходимые клиенту параметры конфигурации (опции / Option)

Опции (основные):

1. Маска подсети IP
2. –
3. Основной шлюз
4. –
5. –
6. Адрес севера DNS (основной и резервный)

…

51. Определяет, на какой срок IP-адрес предоставляется в аренду

55. Список запрашиваемых опций, т.е., отправляя сообщение с опцией 55, оконечное устройство выставляет список запрашиваемых числовых кодов опций в порядке предпочтения.

82. Ретрансляция DHCP сервера. Благодаря этой опции оконечное устройство и сервер могут общаться, находясь в разных подсетях. Ретранслятор получает сообщение клиентов в своей подсети, отправляет сообщение серверу, за счет этого и происходит связь между оконечным устройством одной подсети.

Протокол DHCP позволяет загрузку компьютера без использования носителей данных. Такая загрузка происходит сетевой картой и обозначается “PXE”. Для конфигурации сетевой загрузки используются опции 43, 60, 66 и 67

Службы сетевой безопасности и сетевые службы ОС.

Система безопасности – комплекс мер, направленных на поддержание удобства использования и защиты целостности сети и данных. Средства сетевой безопасности используют программные и аппаратные технологии. Система сетевой безопасности борется с различными угрозами. Средства сетевой безопасности предназначены для борьбы с сетевыми угрозами. Они блокируют проникновение и распространение угроз в сети. Эффективная система сетевой безопасности управляет доступом к сети. Для реализации своих задач система сетевой безопасности может использовать основные службы и сетевые функции ОС, которые используются любой ОС для подключения к интернету с целью предоставления или получения расширенных функций и дополнительных возможностей. При использовании сетевых функций данные отправляются разработчику ПО, которые им обрабатываются. Эти данные позволяют предоставить облачные сетевые функции. Они называются обязательными данными службы. Они могут содержать сведения, относящиеся к работе сетевой функции, которые требуются для защиты обновления и работы базовой службы. Обязательные данные службы могут включать сведения, необходимые сетевой функции для выполнения задач. Например, сведения о конфигурации ОС. Сетевые функции влияют на тип обязательных данных служб, а также данных основных служб. Основные службы используются для своевременного обновления программного продукта. Администраторы могут отключить большинство основных служб. Но желательно предусмотреть возможность размещения служб локально, оценить последствия отключения служб.

Аутентификация предназначена для проверки подлинности входа в рабочие или учебные учетные записи. Проверяется паспорт пользователя и предоставляет доступ к нескольким приложениям и системным компонентам. При отключении этой службы нужные компоненты могут потерять функциональность, а пользователь не сможет войти. Цифровые файлы хранятся на клиентских устройствах, используются для шифрования данных и проверки. Доверенные корневые сертификаты выдаются центром сертификации, хранятся в списке доверия сертификата. Автоматический механизм обновления корневых сертификатов связывается с центром обновления и таким образом корректируется список. Недоверенные сертификаты – мошеннические. Недоверенные сертификаты также хранятся в списке на локальном устройстве и обновляются автоматически. Если автоматическое обновление отключено, приложения и веб-сайты могут перестать работать, так как они не получили обновленный корневой сертификат, который использует приложение. Кроме того, не будет обновляться и список (надежных)? сертификатов. Конфигурация служб используется компонентами и приложениями операционной системы. Такие как служба телеметрии для динамического обновления их конфигурации. Служба лицензирования используется для активации операционной системы и приложений

Межсетевой экран

Межсетевой экран - устройство контроля доступа в сеть, предназначенное для блокировки всего трафика за исключением разрешённых данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в максимально короткие сроки. Существуют маршрутизаторы, которым можно предоставить возможность анализа входных пакетов, чтобы они могли выполнять две функции: функцию маршрутизатора и функцию межсетевого экрана, однако скорость обработки пакетов уменьшается в десятки раз, поэтому применяются отдельно маршрутизаторы, отдельно межсетевые экраны. Последние наделены большим набором настроек:

1. Прохождение трафика на межсетевом экране должно быть выполнено по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих служб.
2. Межсетевые экраны позволяют осуществлять централизованное управление безопасность, а именно: в одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребности в обновлении систем, но позволяет снизить вероятность возникновения ошибки при ее конфигурировании, в результате чего эти системы могут быть подвергнуты атакам.

Существуют 3 типа:

- Межсетевые экраны прикладного уровня

- Межсетевые экраны с пакетной фильтрацией.

Межсетевые экраны прикладного уровня (proxy-сервер или прокси-экран) представляют собой программные пакеты. На основе операционных систем общего назначения или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами - по одному на каждую сеть, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствуют явные разрешения на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты. Правила политики безопасности усиливаются при использовании модулей доступа.

В межсетевом экране прикладного уровня каждому разрешенному протоколу должен соответствовать свой собственный модуль доступа. Лучшими считаются те, которые построены специально для разрешенного протокола. При использовании межсетевого экрана прикладного уровня все соединения проходят через него. Соединения начинаются на системе-клиенте и поступают на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол. На основании этого он определяет, соответствует ли пакет политике безопасности. При несоответствии отклоняя его. Если полученные данные соответствуют правилам безопасности, то межсетевой экран создает новое соединение между своим внешним интерфейсом и системой-сервером.