МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и компьютерных наук
кафедра информационной безопасности

Захаров А.А.

«СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

по направлению подготовки
10.03.01 «Информационная безопасность» профиль
«Безопасность компьютерных систем»
для обучающихся по специальности
10.05.03 «Информационная безопасность автоматизированных систем (специалитет)»
специализация «Безопасность открытых информационных систем»
10.05.01 «Компьютерная безопасность (специалитет)» специализация
«Безопасность компьютерных систем и сетей»
форма обучения очная

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью дисциплины «Сети и системы передачи данных» является изучение методов и средств построения и эксплуатации программно-аппаратных технологий, изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий передачи информации.

Задачей курса является:

- Изучение принципов построения, функционирования и применения аппаратных средств современной вычислительной техники;
- Изучение основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций.

Изучение курса основано на следующих дисциплинах: «Информатика», «Операционные системы».

В результате изучения дисциплины студенты должны знать:

- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности.
- основные подсистемы современных ОС и их назначение; механизм функционирования основных подсистем администрирования объектов защиты на уровне администратора безопасности; методы программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.

уметь:

- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения.
- администрировать подсистемы информационной безопасности в телекоммуникационных сетях и системах, администрировать современные программные средства на объектах защиты на уровне администратора безопасности.

Тема 1. ВВЕДЕНИЕ

Интернет — глобальная сеть, объединяющая множество сетей, построенных по совершенно разным принципам. Это компьютерная система общения мирового масштаба, расстояние в ней не является препятствием. При ее создании необходимо было решить две основные проблемы. Во-первых, надо было осуществить такое соединение компьютеров, чтобы их удаленность друг от друга и разные принципы организации локальных сетей не имели никакого значения. Эта задача была решена путем разработки специальных устройств (мостов, шлюзов, маршрутизаторов). Во-вторых, надо было научить компьютеры «понимать» друг друга и «договариваться» между собой. Это было осуществлено путем разработки соглашений (договоренностей), определяющих правила передачи данных, — протоколов.

Сегодня везде можно услышать о Всемирной паутине — World Wide Web (WWW), которую образуют компьютеры-серверы Интернета. Каждый Web - сервер является как бы узелком этой информационной паутины. Web-серверы хранят всевозможные информационные ресурсы (изображения, документы, программы, таблицы, справочную информацию), к которым можно получить доступ из любой точки нашей Земли. Доступ является интерактивным и позволяет пользователю самому решать, по каким адресам обращаться, что выбирать, как передвигаться в сети. Важной особенностью работы в Интернете является наличие гиперссылок, с помощью которых, переходя от одной к другой, вы можете найти любую интересующую вас информацию.

Вопросы для подготовки

1. Коммуникации в мире с развитыми сетевыми технологиями.
2. Современное состояние и перспективы коммуникаций.
3. Компьютерные сеть как платформа Архитектура Интернет.
4. Направления в развитии сетей.

Тема 2. КОММУНИКАЦИИ С ПОМОЩЬЮ СЕТЕЙ

В наши дни компьютерные сети обретают все более важное значение в жизни человечества, их развитие весьма перспективно. Сети могут объединять и делать доступными информационные ресурсы как небольших предприятий, так и крупных организаций, занимающих удаленные друг от друга помещения, подчас даже в разных странах. Компьютеры объединяют в сеть всегда с определенной целью, и, в зависимости от нее, определяются и виды сетей: локальную, региональную, корпоративную, глобальную.

Компьютерные сети – система компьютеров, связанных каналами передачи информации

В компьютерной сети - любое из подключенных устройств можно использовать для передачи, хранения и обработки информации.

Сети **по размерности** делятся на **локальные, региональные, корпоративные, глобальные**.

- **локальная сеть** (LAN — Local Area Network) – соединение компьютеров, расположенных на небольших расстояниях друг от друга (от нескольких метров до нескольких км)

ПК в таких сетях расположены в одном помещении, на одном предприятии, в близко расположенных зданиях.

Локальные сети не позволяют обеспечить совместный доступ к информации пользователям, находящимся, например, в различных частях города. На помощь приходят **региональные сети**, объединяющие компьютеры в пределах одного региона (города, страны, континента).

- **региональная сеть** (MAN — Metropolitan Area Network) – объединение ПК и локальных сетей для решения общей проблемы регионального масштаба

Региональная вычислительная сеть связывает компьютеры, расположенные на значительном расстоянии друг от друга. Она может включать компьютеры внутри большого города, экономического региона,

отдельной страны. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки — сотни километров.

Многие организации, заинтересованные в защите информации от несанкционированного доступа (например, военные, банковские и пр.) создают, так называемые **корпоративные сети**. Корпоративная сеть может объединять тысячи и десятки тысяч компьютеров, размещенных в различных странах и городах (в качестве примера можно привести сеть корпорации Microsoft)

- **корпоративные сети -** объединение локальных сетей в пределах одной корпорации

Потребности формирования единого мирового информационного пространства привели к созданию глобальной компьютерной сети Интернет.

- **глобальные сети** (WAN — Wide Area Network) **–** система связанных между собой локальных сетей и ПК пользователей, расположенных на удаленных расстояниях, для общего использования мировых информационных ресурсов**.**

Различные виды каналов

Некоторые из них являются взаимоисключающими, некоторые могут описывать один канал с разных сторон.

Каналы бывают **цифровые и аналоговые.**

К **аналоговым** каналам можно отнести обыкновенный телефонный канал. Для его использования необходимо специальное устройство — модем, преобразующее цифровую информацию в аналоговую. Аналоговые каналы сильно подвержены влиянию помех и обладают малой пропускной способностью (несколько десятков килобайт в секунду). Сейчас наблюдается тенденция по замене всех аналоговых каналов на цифровые, причем не только в компьютерных сетях, но и в телефонных.

Каналы делятся также на **выделенные** и **коммутируемые.**

При использовании **коммутируемой** линии соединение формируется на время передачи данных, а по окончании этой передачи — разъединяется. Коммутируемой является связь по обычной телефонной линии.

Выделенная линия работает по-другому:

соединение является постоянным, всегда позволяет передать данные от одного компьютера к другому. Выделенные линии отличаются от коммутируемых высокой скоростью (до десятков Мегабит в секунду) и высокой ценой аренды.

По физическому устройству каналы подразделяются на электрические **проводные, оптические и радиоканалы.**

Проводные каналы представляют собой соединение электрическим кабелем, возможно сложно устроенным. Во всех таких каналах применяется передача данных при помощи электрических импульсов.

Оптические каналы связи базируются на световодах. Сигнал же передается при помощи лазеров.

Радиоканалы действуют по тому же принципу, что радио и телевидение.

Для передачи информации по каналам связи необходимо преобразовывать компьютерные сигналы в сигналы физических сред.

Например, при передаче информации по оптоволоконному кабелю представленные в компьютере данные будут преобразованы в оптические сигналы, для чего используются специальные технические устройства – сетевые адаптеры.

- **Сетевые адаптеры (сетевые карты)-** технические устройства, выполняющие функции сопряжения компьютеров с каналами связи.

Если канал связи – телефонная линия, то при приеме – передачи информации используется модем.

- **Модем** – (модулятор – демодулятор) – устройство для преобразования цифровых сигналов ПК в звуковые (аналоговые) сигналы телефонной линии и наоборот.

Для того, чтобы информацию, переданную одним ПК, понял другой ПК, необходимо было разработать единые правила, называемые протоколами**.**

Протокол – набор соглашений о правилах формирования и передачи сообщений, о способах обмена информацией между ПК, о правилах работы различного оборудования в сети

Вопросы для подготовки

1. Платформа для коммуникаций.
2. LAN, WAN и Интернет.
3. Протоколы.
4. Использование уровневых моделей.
5. Сетевая адресация.

Лабораторная работа №1 "Конфигурация маршрутизатора"

Изучение базовых возможностей программы Cisco Packet Tracer**.**

Создать простую топологию сети, состоящей из одного маршрутизатора и одного хостового устройства, в программе Cisco Packet Tracer.

Произвести базовую настройку маршрутизатора с использованием интерфейса командной строки (CLI):

1. задать имя устройства;
2. поднять сетевые интерфейсы;
3. выполнить минимальную конфигурацию безопасности.

Тема 3. МОДЕЛЬ OSI. УРОВЕНЬ ПРИЛОЖЕНИЙ И ТРАНСПОРТНЫЙ УРОВЕНЬ

В модели TCP/IP и в модели OSI самый верхний уровень носит название Application layer — то есть уровень приложений или прикладной уровень. Большая часть полезных данных, передаваемых по сети, создаются на этом уровне и именно с этим уровнем взаимодействует человек посредством прикладного ПО. Все остальные уровни, по сути, выполняют задачу обслуживания передачи данных с уровня приложений на одном компьютере уровню приложений на другом компьютере.

Пример инкапсуляции данных

Рассмотрим типичный пример передачи. Клиент, пользуясь веб-браузером обращается к веб-серверу за страничкой какого-то сайта. Уровень приложений — это браузер и веб сервер. Обе этих программы «знают» один и тот же протокол уровня приложений — HTTP благодаря чему и «понимают» друг друга.

Клиент создаёт HTTP запрос. Этот запрос попадает на транспортный уровень. Он небольшой, поэтому он не разбивается на сегменты, а попадает в один TCP сегмент, в котором ставится порт получателя — 80 — стандартный порт, на котором обычно работает HTTP сервер.

Далее операционная система клиента делает DNS запрос, чтобы узнать какой IP адрес соответствует имени ciscotips.ru и формирует IP пакет, заворачивая в него сегмент, поля IP адрес отправителя и получателя заполняются соответственно адресами клиента и сервера.

Пакет на уровне Network Access заворачивается, например, в Ethernet или wifi кадр и уходит в локальную сеть — к шлюзу. Шлюз разворачивает кадр, смотрит на адрес получателя пакета, формирует новый кадр и передаёт следующему маршрутизатору. Цепочка повторяется пока пакет не дойдёт до маршрутизатора, который является шлюзом целевого сервера. Этот маршрутизатор передаёт пакет серверу.

Сервер получает пакет, достаёт из него сегмент. Операционная система видит, что порт получателя 80 и сверяется со своей таблицей, чтобы понять какой приложение у неё слушает какой порт. Выясняется, что это, например, веб-сервер Apache. Ему и передаётся содержимое сегмента, то есть, собственно, HTTP запрос. И в данном примере из всей цепочи передающих программ и устройств только браузер и веб-сервер «понимают» смысл того, что находится в пакете, для остальных устройств — это просто черный ящик. Поле с данными. Сервер понимает, что надо дать клиенту содержимое странички index.html и в соответствии с протоколом HTTP формирует ответ.

Аналогичным образом данные эти заворачиваются в один или несколько сегментов, сегменты в пакеты, пакеты во фреймы и уходят обратно клиенту. Браузер получает ответ и отображает страничку.

Соответствие между уровнем приложений в OSI и TCP/IP

В модели OSI есть три уровня (7,6 и 5), которые соответствуют одному уровню приложений в модели TCP/IP:

- Приложений;
- Представлений;
- Сессий.

По сути дела, это означает, что в TCP/IP работа программиста не определена так строго — он может реализовывать соответствующий, например, уровню сессий, функционал в своём приложении, а может и нет. Рассмотрим назначение этих уровней подробнее.

Уровень приложений в OSI — занимается собственно отправкой и получением полезных данных. Как видно в примере с HTTP, именно здесь обитает ПО, которое знает в каком байте запроса или ответа что должно находиться.

Уровень представлений занимается преобразованием данных, чтобы снять эту задачу с программиста конечного продукта. Например, на этом уровне может происходить смена кодировки текста, преобразование картинок из одного формата в другой, сжатие данных, шифрование данных. В модели

TCP/IP всё это тоже может присутствовать и присутствует, но программист сам решает, как ему в рамках своего единственного уровня запрограммировать тот или иной функционал.

Уровень сессий занимается отслеживанием сессий в рамках приложений. Надо понимать, что это не те сессии, которые имеются в TCP, а это именно сессии с точки зрения логики конкретного приложения. Например, человек зашёл в скайп — с точки зрения скайпа для человека открылась сессия. Или человек зашёл в онлайн игру — тоже сессия. То есть всё это в любом случае есть в реальной жизни, но в OSI явно выделяется в отдельный уровень.

Протоколы уровня приложений

На уровне приложений существует бесчисленное множество протоколов, так как разработчик ПО в праве создать свой собственный протокол, когда ему это нужно. Тем не менее, администратору надо свободно понимать принципы функционирования основных наиболее часто использующихся протоколов, чтобы грамотно организовать сеть. Наиболее распространённые протоколы уровня приложений, с которыми мы работаем каждый день — это HTTP, POP, SMTP, IMAP, DNS, DHCP, FTP, Telnet.

Вопросы для подготовки

1. Функции уровня приложений модели OSI.
2. Обеспечение приложений и служб.
3. Примеры протоколов и служб уровня приложения.
4. Транспортный уровень модели OSI.
5. Функции транспортного уровня.
6. TCP протокол – надежное соединение.
7. Управление сессиями TCP.
8. Протокол UDP – соединение с низкими накладными расходами.

Тема 4. СЕТЕВОЙ УРОВЕНЬ МОДЕЛИ OSI

Основная задача сетевого уровня модели OSI (или уровня сетевого взаимодействия протокола TCP/IP) — доставка пакетов от одного узла-отправителя к узлу-получателю не зависимо от того к какой локальной сети принадлежат узлы. Если на канальном уровне передача информации между узлами сети возможна только в пределах одной логической сети, то сетевой уровень определяет правила доставки данных между логическими сетями, формирование логических адресов сетевых устройств, определение, выбор и поддержание маршрутной информации.

Если на канальном уровне адресация узлов осуществлялась при помощи физического MAC-адреса сетевого устройства, то на сетевом уровне появляются логические адреса — IP адреса сетевого устройства (интерфейса). IP-адреса интерфейсов одной IP-сети имеют общую часть, которая называется адресом или номером IP-сети и специфическую для каждого интерфейса часть, называемую адресом, или номером, данного интерфейса в данной IP-сети.

Соответственно, IP-сетью называется множество компьютеров (IP-интерфейсов), часто, но не всегда подсоединенных к одному физическому каналу связи, способных пересылать IP-дейтаграммы друг другу непосредственно (то есть без ретрансляции через промежуточные компьютеры, считая, что маршрутизатор, в принципе то-же является компьютером).

IP-адрес обычно записывается в форме 4-х трехразрядных десятичных чисел, называемых октетами, разделенных точкой — например 192.168.100.100. Каждое из этих десятичных чисел соответствует одному байту двоичного представления адреса.

Так как IP-адрес содержит в себе как адрес узла (точнее, интерфейса, так как в общем случай узел может иметь более одного интерфейса — например компьютер с двумя сетевыми платами) так и адрес сети, то необходим

механизм для «вычленения» из IP-адреса интерфейса адреса сети, к которой принадлежит интерфейс и номера интерфейса в данной сети.

Для этого служит **маска сети**. Маска сети используется для определения того, какие биты являются частью номера сети, а какие – частью идентификатора хоста (для этого применяется логическая операция конъюнкции – “И”).

Таким образом адресное пространство любой сети состоит из:

- Адреса сети — это адрес, который используется для организации маршрутизации между несколькими сетями. При получении IP-адреса хоста маршрутизатор накладывает на него маску и определяет адрес сети, затем по этому адресу определяется адрес шлюза, на который нужно отправить пакет.
- Адреса хостов в сети — это набор IP-адресов, которые могут быть выданы хостам. Чтобы подсчитать количество адресов, нужно от общего количества адресов сети отнять два адреса: 1 — адрес самой сети и 2 — широковещательный адрес. При обмене пакетами между хостами в одной сети маршрутизатор и шлюз не нужны.
- Широковещательный адрес (Broadcast) — это адрес, который не присвоен ни одному хосту в сети. Данный адрес используется для отправки широковещательных пакетов, которые предназначены каждому хосту сети.

На сетевом уровне функционируют протоколы: IP, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPSec, ARP, RARP, DHCP, BootP, SKIP, RIP

Вопросы для подготовки

1. IPv4.
2. Деление устройств на группы.
3. Маршрутизация – как управляются пакеты данных.
4. Процесс маршрутизации.

Лабораторная работа №2 "Конфигурирование статических маршрутов"

Изучение методов настройки статической маршрутизации.

Создать топологию сети, состоящей из трех последовательно соединенных маршрутизаторов, в программе Cisco Packet Tracer.

- Произвести базовую настройку каждого маршрутизатора с использованием интерфейса командной строки (CLI):
    1. задать имя устройства;
    2. поднять сетевые интерфейсы;
    3. выполнить минимальную конфигурацию безопасности.
- На каждом маршрутизаторе вручную настроить статические маршруты.
- Выполнить работу с использованием лабораторного оборудования.

Тема 5. АДРЕСАЦИЯ В СЕТИ – IPV4

IPv4 поддерживает три различных типа режимов адресации.

Режим одноадресной адресации:

В этом режиме данные отправляются только на один конечный хост. Поле Адрес назначения содержит 32-битный IP-адрес хоста назначения. Здесь клиент отправляет данные на целевой сервер:

Режим широковещательной адресации:

В этом режиме пакет адресован всем хостам в сегменте сети. Поле Адрес назначения содержит специальный широковещательный адрес, то есть **255.255.255.255**. Когда хост видит этот пакет в сети, он обязан его обработать. Здесь клиент отправляет пакет, который развлекается всеми серверами:

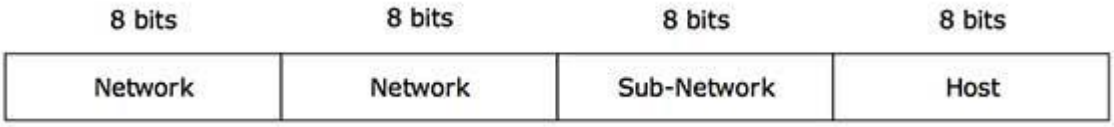
Режим многоадресной адресации:

Этот режим представляет собой сочетание двух предыдущих режимов, то есть отправленный пакет не предназначен ни одному хосту, ни всем хостам в сегменте. В этом пакете адрес назначения содержит специальный адрес, который начинается с 224.xxx и может использоваться несколькими хостами.

Здесь сервер отправляет пакеты, которые принимаются более чем одним сервером. Каждая сеть имеет один IP-адрес, зарезервированный для номера сети, который представляет сеть, и один IP-адрес, зарезервированный для широковещательного адреса, который представляет все хосты в этой сети.

Схема иерархической адресации

IPv4 использует иерархическую схему адресации. IP-адрес длиной 32 бита разделен на две или три части, как показано на рисунке:

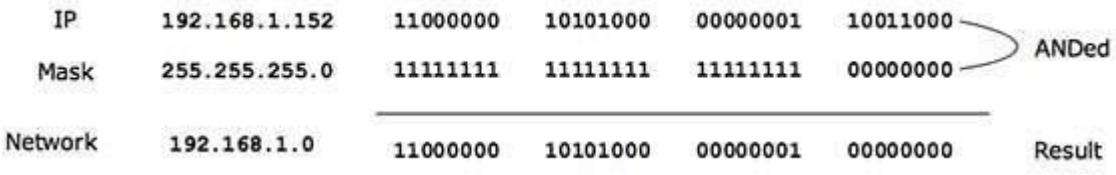


Один IP-адрес может содержать информацию о сети, ее подсети и, в конечном счете, хосте. Эта схема позволяет IP-адресу быть иерархическим,

когда сеть может иметь много подсетей, которые, в свою очередь, могут иметь много хостов.

Маска подсети

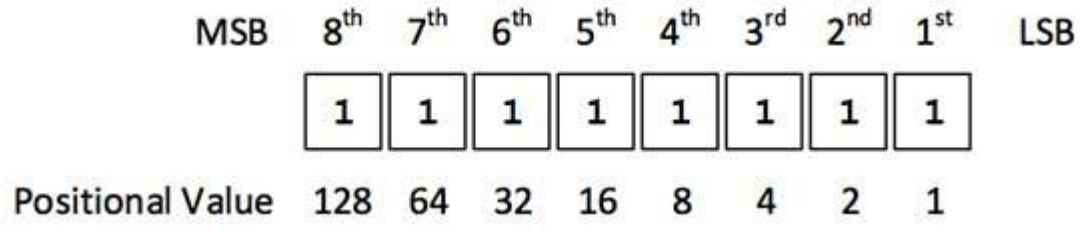
32-битный IP-адрес содержит информацию о хосте и его сети. Очень необходимо различать оба. Для этого маршрутизаторы используют маску подсети, которая равна размеру сетевого адреса в IP-адресе. Маска подсети также имеет длину 32 бита. Если в двоичном IP-адресе указано AND и его маска подсети, то в результате вы получите сетевой адрес. Например, скажем, IP-адрес — 192.168.1.152, а Маска подсети — 255.255.255.0, тогда:



Таким образом, маска подсети помогает извлечь идентификатор сети и хост из IP-адреса. Теперь можно определить, что 192.168.1.0 — это номер сети, а 192.168.1.152 — это хост в этой сети.

Бинарное Представление

Метод позиционного значения — это самая простая форма преобразования двоичного значения из десятичного. IP-адрес является 32-битным значением, которое делится на 4 октета. Бинарный октет содержит 8 битов, и значение каждого бита может быть определено положением значения бита ‘1’ в октете.



Позиционное значение битов определяется как 2, возведенное в степень (позиция — 1), то есть значение бита 1 в позиции 6 равно 2 ^ (6-1), то есть 2 ^ 5, что составляет 32. Общее значение Октет определяется суммированием позиционного значения битов. Значение 11000000 составляет 128 + 64 = 192.

Вопросы для подготовки

1. IPv4 адреса.
2. Адреса различного назначения.
3. Назначение адресов.
4. Идентификация сети.
5. Вычисление адресов.
6. Тестирование сетевого уровня.

Тема 6. КАНАЛЬНЫЙ И ФИЗИЧЕСКИЙ УРОВНИ МОДЕЛИ OSI

Канальный уровень предназначен для передачи данных между двумя узлами, находящихся в одной локальной сети. Роль PDU исполняют фреймы. Фреймы канального уровня не пересекают границ локальной сети, что позволяет данному уровню сосредоточиться на локальной доставке (фактически межсетевой доставкой занимаются более высокие уровни).

Заголовок фрейма формируется из аппаратных адресов отправителя и получателя, что позволяет однозначно определить устройство, которое отправило данный фрейм и устройство, которому он предназначен. При этом никакая часть адреса не может быть использована, чтобы определить некую логическую/физическую группу, к которой принадлежит устройство.

Канальный уровень состоит из двух подуровней: LLC и MAC.

Канальный уровень выполняет функции:

- LLC Multiplexing: Интерфейс между сетевым уровнем и MAC, чтобы несколько различных протоколов сетевого уровня могли сосуществовать.
- LLC Flow control: Механизм ограничении скорости передачи данных при медленном приёмнике
- LLC Error control: Определение (и иногда исправление) ошибок с помощью чексумм
- MAC Adressing mechanism: Адрессация на основе уникальных MAC-адресов
- MAC Channel access control mechanism: предоставляет протокол множественного доступа

Наиболее часто на канальной уровне используются протоколы:

- PPP (Point-To-Point Protocol, протокол прямого соединения между двумя узлами)
- SLIP (Serial Line Internet Protocol, предшественник PPP, который всё ещё используется в микроконтроллерах)

- Ethernet II framing

Физический уровень (Physical layer)

Физический, — самый нижний в модели OSI. Этот уровень осуществляет передачу неструктурированного, «сырого» потока битов по физической среде (например, по сетевому кабелю). Здесь реализуются электрический, оптический, механический и функциональный интерфейсы с кабелем. Физический уровень также формирует сигналы, которые переносят данные, поступившие от всех вышележащих уровней. На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера, в частности, количество контактов в разъемах и их функции. Кроме того, здесь определяется способ передачи данных по сетевому кабелю. Физический (Physical) уровень предназначен для передачи битов (нулей и единиц) от одного компьютера к другому. Содержание самих битов на данном уровне значения не имеет. Этот уровень отвечает за кодирование данных и синхронизацию битов, гарантируя, что переданная единица будет воспринята именно как единица, а не как ноль. Наконец, Физический уровень устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы, передаваемые по сетевому кабелю.

Физический уровень выполняет функции:

- Побитовая доставка
- Физическое кодирование (способ представления данных в виде импульсов)
- LLC Error control: Определение (и иногда исправление) ошибок с помощью чексумм
- MAC Adressing mechanism: Адрессация на основе уникальных MAC-адресов
- MAC Channel access control mechanism: предоставляет протокол множественного доступа

Наиболее часто на физическом уровне используются протоколы:

- Ethernet physical layer (семейство стандартов с оптическими или электрическими свойствами соединений между устройствами)
- USB

Вопросы для подготовки

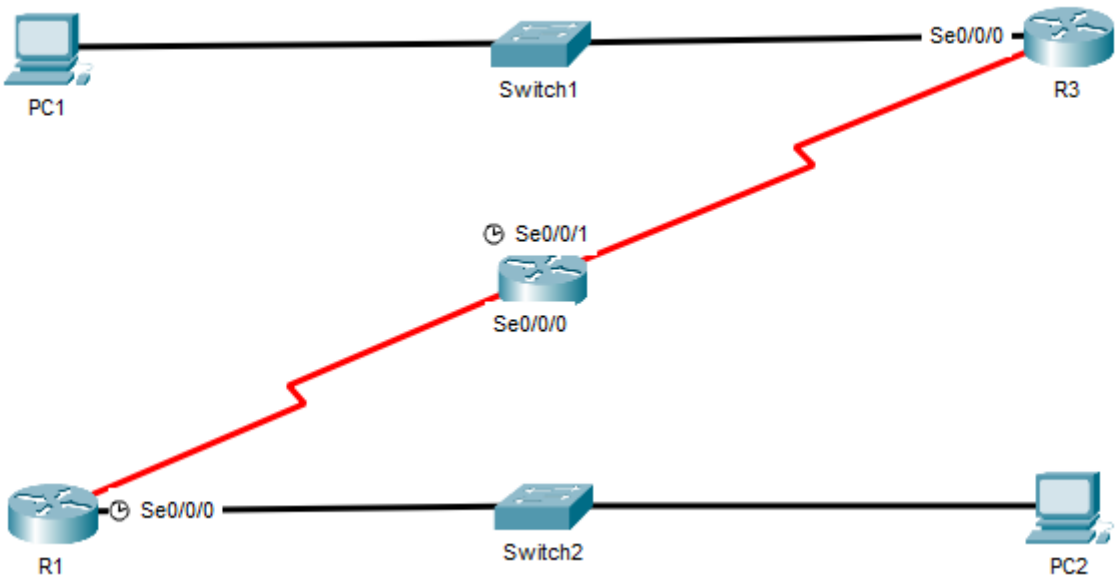
1. Канальный уровень.
2. Методы доступа к среде.
3. Адресация и деление данных на кадры в подуровне доступа к среде.
4. Физический уровень модели OSI.
5. Коммуникационные сигналы.
6. Физическая передача сигналов и кодирование: представление данных.
7. Среда передачи данных.

Лабораторная работа №3 "Конфигурирование RIPv2"

Изучение настройки и принципов работы сетевого протокола динамической маршрутизации RIPv2.

- Создать топологию сети в программе Cisco Packet Tracer;
- Произвести базовую настройку каждого маршрутизатора с использованием интерфейса командной строки (CLI):
    1. задать имя устройства;
    2. поднять сетевые интерфейсы;
    3. выполнить минимальную конфигурацию безопасности.
- Выполнить настройку протокола RIP на маршрутизаторах R1, R2 и R3;
- Активировать протокол RIPv2 на маршрутизаторах R1, R2 и R3;
- Выполнить работу с использованием лабораторного оборудования.

Используемая топология:



План адресации:

Устройство	Интерфейс	IP адрес	Маска подсети	Шлюз по умолчанию
R1	S0/0	192.168.1.1	255.255.255.252	N/A
	Fa0/0	172.16.100.1	255.255.255.128	N/A
R2	S0/0	192.168.1.2	255.255.255.252	N/A
	S0/1	192.168.0.2	255.255.255.252	N/A
R3	S0/0	192.168.0.1	255.255.255.252	N/A
	Fa0/0	172.16.200.1	255.255.255.128	N/A
PC1	NIC	172.16.200.10	255.255.255.128	172.16.200.1
PC2	NIC	172.16.100.10	255.255.255.128	172.16.100.1

Тема 7. ETHERNET

Ethernet это стандарт, который относится только к построению локальных сетей LAN (Local Area Network). Локальная сеть мала, в отличие от старшего брата WAN (Wide Area Network), которую еще называют **глобальной сетью**. Локальная сеть у вас дома, в офисе, то есть на любой небольшой территории. Именно локальная сеть - один из основных идентификаторов наличия **Ethernet.**

В терминах семиуровневой модели OSI (если не знаете про нее, почитайте, это интересно!), стандарт Ethernet живет на первом и на втором уровнях. На первом уровне описаны способы передачи электрических, оптических и беспроводных (радио, например) сигналов, а на втором формирование кадров (фреймов). И тут мы делаем вывод:

Ethernet — это набор описаний способов физической передачи сигналов (электричество) на первом уровне модели OSI и формирования кадров (фреймов) на втором уровне модели OSI внутри локальных сетей LAN.

Есть 2 технологии Ethernet:

1. Классический Ethernet
    1. Разделяемая среда
    2. Ethernet - Gigabit Ethernet
2. Коммутируемый Ethernet
    1. Точка-точка
    2. Появился в Fast Ethernet
    3. Единственный вариант в 10G Ethernet

В качестве общей шины использовался коаксиальный кабель. В дальнешем такая схема была заменена на концентраторы Ethernet (hub).

Физическая топология – звезда

Логическая топология – общая шина

Компьютеры подключаются к концентратору с помощью витых пар, но внутри – общая шина, то есть все данные, которые приходят на один порт, передаются на все остальные порты.

Для идентификации сетевых интерфейсов узлов внутри сети Ethernet используются MAC-адреса. Очевидно, что они должны быть уникальны в одном сегменте сети. Если несколько имеют один и тот же MAC, то один из них работать не будет и какой именно не регламентировано

Коммутируемый Ethernet

Это новая технология, появилась в 1995году, спецификация IEEE 802.3u. В ней нет разделяемой среды и используется топология “точка-точка”. Для этого придумали новый тип сетевых устройств – коммутаторы. Внешне концентратор (для классического Ethernet) и коммутатор почти не отличаются, но внутреннее отличие очень большое: концентратор использует топологию “общая шина”, коммутатор же – полносвязную топологию. Концентратор работает на физическом уровне, он передает электрические сигналы, которые поступают на один порт, на все порты. Коммутатор работает на канальном уровне: он анализирует заголовок канального уровня, извлекает адрес получателя и передает данные только на тот порт, к которому подключен получатель.

Особенности работы коммутаторов

В нем хранится таблица коммутации: соответствие порта и MAC-адреса. Для ее заполнения используется алгоритм обратного обучения. Коммутатор анализирует заголовки канального уровня, извлекает адрес отправителя и заполняет таблицу.

В реальности в этой таблице может храниться еще другая метаинформация (например, состояние порта, номер vlan и т.п.) Для передачи кадров внутри коммутатора используется **алгоритм прозрачного моста.**

Использовались они в классическом Ethernet-е для уменьшения числа коллизий для больших сетей. Принцип был таков: мост подключается к двум

сегментам сети и пропускает данные через себя, только если они передаются из одного сегмента сети в другой.

Вопросы для подготовки

1. Ethernet – соединение через LAN 3.
2. Кадр Ethernet.
3. Контроль доступа к среде в Ethernet.
4. Физический уровень Ethernet.
5. Концентраторы и коммутаторы.
6. Протокол разрешения адресов (ARP).

Тема 8. ПЛАНИРОВАНИЕ И МОНТАЖ СЕТИ

Планирование сети.

Несмотря на то, что планированием и монтажом больших сетей обычно занимаются специализированные компании-интеграторы, сетевому администратору часто приходится планировать определенные изменения в структуре сети — добавление новых рабочих мест, добавление или удаление сетевых протоколов, добавление или удаление сетевых служб, установка серверов, разбиение сети на сегменты и т.д. Данные работы должны быть тщательно спланированы, чтобы новые устройства, узлы или протоколы включались в сеть или исключались из нее без нарушения целостности сети, без снижения производительности, без нарушения инфраструктуры сетевых протоколов, служб и приложений.

Установка и настройка сетевых узлов (устройств активного сетевого оборудования, персональных компьютеров, серверов, средств коммуникаций).

Данные работы могут включать в себя — замену сетевого адаптера в ПК с соответствующими настройками компьютера, перенос сетевого узла (ПК, сервера, активного оборудования) в другую подсеть с соответствующим изменениями сетевых параметров узла, добавление или замена сетевого принтера с соответствующей настройкой рабочих мест.

Установка и настройка сетевых протоколов.

Данная задача включает в себя выполнение таких работ — планирование и настройка базовых сетевых протоколов корпоративной сети, тестирование работы сетевых протоколов, определение оптимальных конфигураций протоколов.

Установка и настройка сетевых служб.

Корпоративная сеть может содержать большой набор сетевых служб. Кратко перечислим основные задачи администрирования сетевых служб:

- установка и настройка служб сетевой инфраструктуры (службы DNS, DHCP, WINS, службы маршрутизации, удаленного доступа и виртуальных частных сетей);
- установка и настройка служб файлов и печати, которые в настоящее время составляют значительную часть всех сетевых служб;
- администрирование служб каталогов (Novell *NDS*, Microsoft Active Directory), составляющих основу корпоративной системы безопасности и управления доступом к сетевым ресурсам;
- администрирование служб обмена сообщениями (системы электронной почты);
- администрирование служб доступа к базам данных.

Поиск неисправностей.

Сетевой администратор должен уметь обнаруживать широкий спектр неисправностей — от неисправного сетевого адаптера на рабочей станции пользователя до сбоев отдельных портов коммутаторов и маршрутизаторов, а также неправильные настройки сетевых протоколов и служб.

Поиск узких мест сети и повышения эффективности работы сети.

В задачу сетевого администрирования входит анализ работы сети и определение наиболее узких мест, требующих либо замены сетевого оборудования, либо модернизации рабочих мест, либо изменения конфигурации отдельных сегментов сети.

Мониторинг сетевых узлов.

Мониторинг сетевых узлов включает в себя наблюдение за функционированием сетевых узлов и корректностью выполнения возложенных на данные узлы функций.

Мониторинг сетевого трафика.

Мониторинг сетевого трафика позволяет обнаружить и ликвидировать различные виды проблем: высокую загруженность отдельных сетевых

сегментов, чрезмерную загруженность отдельных сетевых устройств, сбои в работе сетевых адаптеров или портов сетевых устройств, нежелательную активность или атаки злоумышленников (распространение вирусов, атаки хакеров и др.).

Обеспечение защиты данных.

Защита данных включает в себя большой набор различных задач: резервное копирование и восстановление данных, разработка и осуществление политик безопасности учетных записей пользователей и сетевых служб (требования к сложности паролей, частота смены паролей), построение защищенных коммуникаций (применение протокола IPSec, построение виртуальных частных сетей, защита беспроводных сетей), планирование, внедрение и обслуживание инфраструктуры открытых ключей (PKI).

Вопросы для подготовки

1. LAN – физическое соединение.
2. Соединение устройств.
3. Разработка адресной схемы.
4. Расчет подсетей.

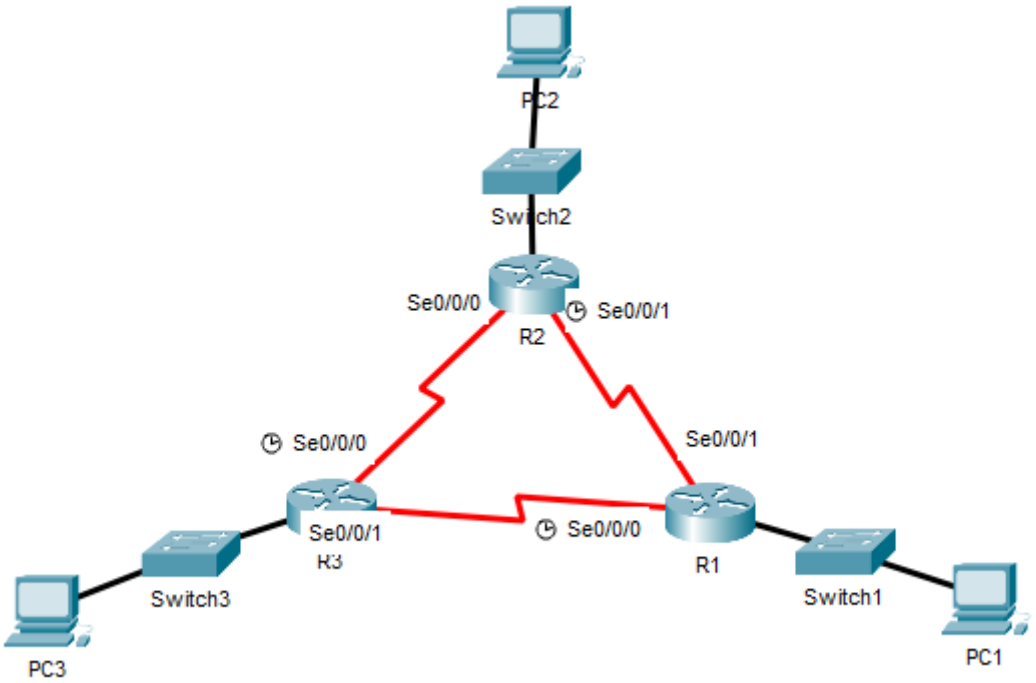
Лабораторная работа №4 "Конфигурирование EIGRP"

Изучение настройки и принципов работы сетевого протокола динамической маршрутизации EIGRP.

- Создать топологию сети в программе Cisco Packet Tracer;
- Произвести базовую настройку каждого маршрутизатора с использованием интерфейса командной строки (CLI):
    1. задать имя устройства,
    2. поднять сетевые интерфейсы,
    3. выполнить минимальную конфигурацию безопасности;
- Выполнить настройку протокола динамической маршрутизации EIGRP на маршрутизаторах R1, R2 и R3;

- Проанализировать маршруты EIGRP;
- Отключить автоматическую суммаризацию маршрутов EIGRP;
- Выполнить работу с использованием лабораторного оборудования.

Используемая топология:



План адресации:

Устройство	Интерфейс	IP адрес	Маска подсети	Шлюз по умолчанию
R1	Fa0/0	172.17.1.1	255.255.255.0	N/A
	S0/0	172.17.3.1	255.255.255.252	N/A
	S0/1	192.168.1.5	255.255.255.252	N/A
R2	Fa0/0	172.17.2.1	255.255.255.0	N/A
	S0/0	172.17.3.2	255.255.255.252	N/A
	S0/1	192.168.1.9	255.255.255.252	N/A
	Lo1	203.0.113.1	255.255.255.252	N/A
R3	Fa0/0	192.168.10.1	255.255.255.0	N/A
	S0/0	192.168.1.6	255.255.255.252	N/A
	S0/1	192.168.1.10	255.255.255.252	N/A
PC1	NIC	172.17.1.10	255.255.255.0	172.17.1.1
PC2	NIC	172.17.2.10	255.255.255.0	172.17.2.1
PC3	NIC	192.168.10.10	255.255.255.0	192.168.10.1

Тема 9. КОНФИГУРИРОВАНИЕ И ТЕСТИРОВАНИЕ СЕТИ

Подобно персональному компьютеру, маршрутизатор или коммутатор не могут функционировать без операционной системы. Без операционной системы у аппаратных средств нет никаких возможностей. Cisco Internetwork Operating System (IOS) является системным программным обеспечением в устройствах Cisco.

Cisco IOS предоставляет устройствам следующие сетевые службы:

- Базовые функции маршрутизации и коммутации
- Надежный и безопасный доступ к сетевым ресурсам
- Сетевая масштабируемость

Детали работы IOS варьируются в различных устройствах межсетевого взаимодействия, в зависимости от назначения устройства и набора функций.

К службам, предоставленным Cisco IOS, обычно получают доступ, используя интерфейс командной строки (CLI). Функции, доступные через CLI, варьируются в зависимости от версии IOS и типа устройства.

Файл самой IOS составляет несколько мегабайтов в размере и хранится в области памяти с возможностью перезаписи информации, называемой флэш-памятью. Флэш-память обеспечивает энергонезависимую память. Это означает, что содержимое памяти не теряется, если отключить питание устройства. Даже при том, что содержимое не теряется, оно может быть изменено или перезаписано при необходимости.

Использование флэш-памяти позволяет IOS обновляться до более новых версий или добавлять новые функции. Во многих архитектурах маршрутизаторов IOS копируется в RAM, когда устройство включается, и IOS выполняется из RAM во время работы устройства. Эта возможность увеличивает производительность устройства.

Вопросы для подготовки

1. Конфигурирование устройств Cisco – основы IOS.
2. Применение базовой конфигурации с помощью Cisco IOS.

3. Проверка соединения.
4. Отслеживание и документирование сетей.

Тема 10. СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Статические маршруты используются по ряду причин, часто в тех случаях, когда не существует динамического маршрута к IP-адресу назначения или необходимо заменить маршрут, полученный динамически.

По умолчанию административное расстояние статического маршрута равно единице, что обеспечивает им приоритет по сравнению с маршрутами, полученными из любого протокола динамической маршрутизации. Если сделать значение административного расстояния больше значения для протокола динамической маршрутизации, статический маршрут может превратиться в запасную сеть на случай отказа динамической маршрутизации. Например, для маршрутов, полученных с помощью протокола EIGRP, административное расстояние по умолчанию равно 90 для внутренних маршрутов и 170 для внешних. Для настройки статического маршрута, который заменяется маршрутом EIGRP, задайте административное расстояние больше 170.

Статический маршрут такого вида с большим административным расстоянием называется плавающим статическим маршрутом. Он устанавливается в таблице маршрутизации только в том случае, если исчезает маршрут, полученный динамически. Примером плавающего статического маршрута является ip route 172.31.10.0 255.255.255.0 10.10.10.2 101.

Статический маршрут для взаимодействия через интерфейс без IP-адреса следующего перехода

Если вы указываете статический маршрут к интерфейсу и не задаете IP-адрес следующего перехода, маршрут вставлен в таблицу маршрутизации только, когда интерфейс активен. Эта конфигурация не рекомендуется, потому что, когда точки статического маршрута к интерфейсу и не имеет никакой информации о следующем переходе, маршрутизатор полагает, что каждый из хостов в диапазоне маршрута напрямую подключается через тот

интерфейс. Примером такого статического маршрута является ip route 0.0.0.0 0.0.0.0 Ethernet0.

При использовании конфигурации этого типа маршрутизатор выполняет протокол ARP по Ethernet для каждой точки назначения, которую находит в маршруте по умолчанию, поскольку считает все эти точки непосредственно связанными с Ethernet 0. Использование статического маршрута этого вида, особенно если он используется множеством пакетов, направленных в несколько разных подсетей назначения, может привести к высокой загрузке процессора и образованию очень большого ARP-кеша (наряду с ошибками выделения памяти). Поэтому этот вид статического маршрута не рекомендуется.

При определении адреса следующего узла на непосредственно связанный интерфейс маршрутизатор не выполняет ARP для каждого адреса назначения (DA). Примером является маршрут ip route 0.0.0.0 0.0.0.0 Ethernet0 192.168.1.1. Можно указать только адрес напрямую подключенного следующего узла, но делать это не рекомендуется по причинам, которые описаны в этом документе. Указывать адрес напрямую подключенного следующего перехода не обязательно. Можно задать адрес удаленного следующего перехода и интерфейс, к которому удаленный следующий переход делает рекурсивный вызов.

Если существует возможность, что интерфейс со следующим переходом выключается, и следующий переход стал бы достижимым через рекурсивный маршрут, то необходимо задать и IP-адрес следующего перехода и альтернативный интерфейс, через который должен быть найден следующий переход. Например, ip route 10.0.0.1 255.255.255.255 Последовательных 3/3 192.168.20.1. Добавление альтернативного интерфейса позволяет установке статического маршрута стать более детерминированной.

Вопросы для подготовки

1. Протоколы маршрутизации и перенаправление пакетов.

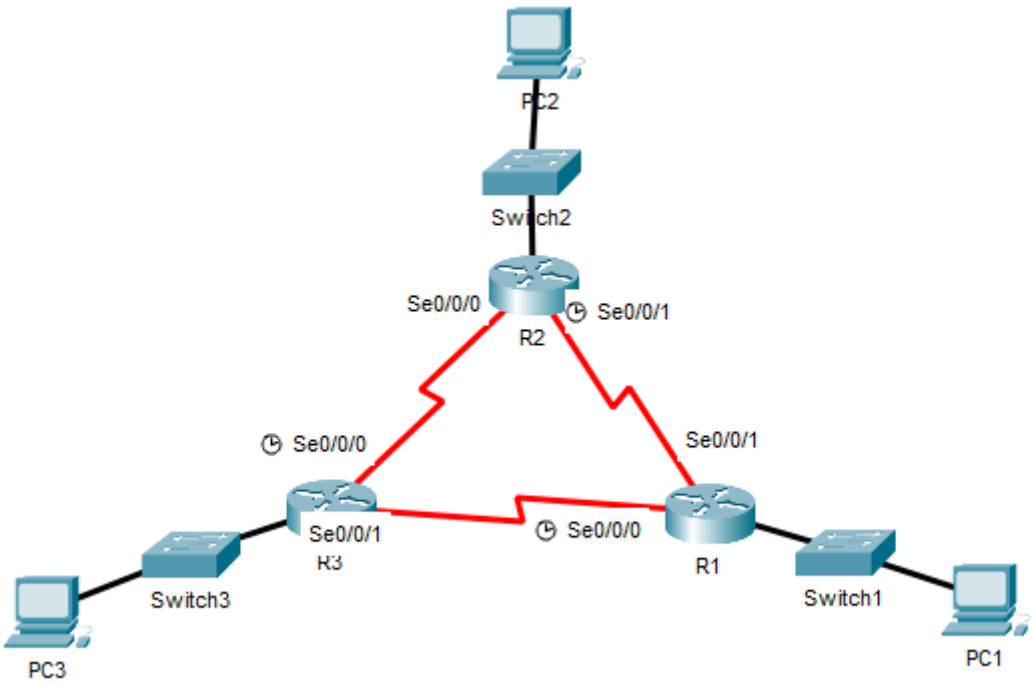
2. CLI конфигурация и адресация.
3. Построение таблицы маршрутизации.
4. Функции определения пути и коммутации.
5. Статическая маршрутизация.
6. Маршрутизаторы в сетях.
7. Обзор конфигурации маршрутизатора.
8. Обнаружение подключенных сетей.
9. Статические маршруты с «NextHop» адресами.
10. Статические маршруты с выходными интерфейсами.
11. Суммарный маршрут и маршрут по умолчанию.
12. Поддержка и исправления статических маршрутов.

Лабораторная работа №5 "Конфигурирование OSPF"

Изучение настройки и принципов работы сетевого протокола динамической маршрутизации OSPF.

- Создать топологию сети в программе Cisco Packet Tracer;
- Произвести базовую настройку каждого маршрутизатора с использованием интерфейса командной строки (CLI):
    1. задать имя устройства;
    2. поднять сетевые интерфейсы;
    3. выполнить минимальную конфигурацию безопасности.
- Выполнить настройку протокола динамической маршрутизации OSPF на маршрутизаторах R1, R2 и R3;
- Настроить OSPF Router ID на маршрутизаторах R1, R2 и R3;
- Проанализировать маршруты OSPF;
- Выполнить работу с использованием лабораторного оборудования.

Используемая топология:



План адресации:

Устройство	Интерфейс	IP адрес	Маска подсети	Шлюз по умолчанию
R1	Fa0/0	172.16.0.17	255.255.255.240	N/A
	S0/0	192.168.0.1	255.255.255.252	N/A
	S0/1	192.168.0.5	255.255.255.252	N/A
R2	Fa0/0	10.1.1.1	255.255.255.0	N/A
	S0/0	192.168.0.2	255.255.255.252	N/A
	S0/1	192.168.0.9	255.255.255.252	N/A
R3	Fa0/0	172.16.0.33	255.255.255.248	N/A
	S0/0	192.168.0.6	255.255.255.252	N/A
	S0/1	192.168.0.10	255.255.255.252	N/A
PC1	NIC	172.16.0.20	255.255.255.240	172.16.0.17
PC2	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC3	NIC	172.16.0.35	255.255.255.248	172.16.0.33

Тема 11. ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется программно. В случае UNIX-систем демонами маршрутизации; в других системах — служебными программами, которые называются иначе, но фактически играют ту же роль.

Демоны маршрутизации обмениваются между собой информацией, которая позволяет им заполнить таблицу маршрутизации оптимальными маршрутами. Протоколы, с помощью которых производится обмен информацией между демонами, называется протоколами динамической маршрутизации.

Демоны динамической маршрутизации:

- Quagga
- GNU Zebra
- XORP
- Bird

Как правило, демоны динамической маршрутизации поддерживают множество протоколов и используют информацию, полученную по одним протоколам для работы других.

Протоколы динамической маршрутизации:

- RIP
- OSPF
- EIGRP
- BGP
- IS-IS

Сами протоколы динамической маршрутизации можно классифицировать по нескольким критериям.

По алгоритмам:

- Дистанционно-векторные протоколы (Distance-vector Routing Protocols);

- RIP
- Протоколы состояния каналов связи (Link-state Routing Protocols).
- OSPF
- IS-IS

Иногда выделяют третий класс, усовершенствованные дистанционно-векторные протоколы (advanced distance-vector), для того чтобы подчеркнуть существенные отличия протоколов от классических дистанционно-векторных.

EIGRP

По области применения разделяют на:

1. Протоколы междоменной маршрутизации (EGP):
    1. BGP
2. Протоколы внутридоменной маршрутизации (IGP):
    1. OSPF
    2. RIP
    3. EIGRP
    4. IS-IS
    5. IGP (Interior Gateway Protocol)
    6. IGP-протоколы используются для передачи информации о маршрутах в пределах автономной системы (AS).

К современным IGP-протоколам, как правило, такие требования:

- Быстрая сходимость
- Выбор маршрутов в зависимости от физических характеристик сети (bandwidth, delay)
- Поддержка VLSM
- Возможность суммировать маршруты

Если говорить об использовании IGP-протоколов в провайдерской среде, то также могут добавиться такие требования:

- Поддержка большого количества маршрутов

- Совместимость и поддержка других технологий. Например, MPLS-TE
- EGP-протоколы используются для передачи информации между автономными системами (AS).

На текущий момент представитель этого класса протоколов один: BGP.

Хотя, чаще всего, BGP используется для передачи маршрутов между разными AS, он может также использоваться и внутри корпоративной сети. Особенно, когда сеть большая.

К EGP-протоколам, как правило, такие требования:

- Возможность настройки протокола с помощью политик, в которых выбор маршрута выполняется не столько и не столько на основании физических характеристик сети, а на основании правил компании
- Способность переносить большое количество маршрутов (порядок размера текущей IPv4 таблицы 500 000 маршрутов)

Вопросы для подготовки

1. Классификация динамических протоколов маршрутизации.
2. Метрики.
3. Административные дистанции.
4. Сабнеттинг.

Тема 12. ДИСТАНЦИОННО-ВЕКТОРНЫЕ ПРОТОКОЛЫ МАРШРУТИЗАЦИИ

Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюзов) является внутренним протоколом шлюзов и пригоден для использования в различных топологиях и средах. В хорошо спроектированной сети EIGRP хорошо масштабируется и позволяет обеспечить малое время конвергенции при минимальном сетевом трафике.

Принцип работы EIGRP

Основными преимуществами EIGRP являются:

- низкое потребление сетевых ресурсов в режиме нормальной эксплуатации (в условиях стабильной сети передаются только пакеты "hello")
- при возникновении изменений по сети передаются только изменения, произошедшие в маршрутной таблице, а не вся таблица целиком; это позволяет уменьшить нагрузку на сеть, создаваемую протоколом маршрутизации
- малое время конвергенции в случае изменения в топологии сети (в отдельных случаях сходимость обеспечивается почти мгновенно)
- протокол EIGRP является усовершенствованным протоколом дистанционной-векторной маршрутизации, в котором для расчета кратчайшего пути к конечному адресу используется алгоритм диффузного обновления (Diffused Update Algorithm – DUAL).

Основные версии протокола

Существуют две основные версии протокола EIGRP – версия 0 и 1. В ранних версиях программного обеспечения Cisco IOS (вплоть до версий 10.3(11), 11.0(8) и 11.1(3)) используется более ранняя версия протокола EIGRP (по этой причине некоторые объяснения, содержащиеся в настоящем документе, могут быть не действительны для этих версий). Мы настоятельно рекомендуем использовать последнюю версию EIGRP, поскольку эта версия

содержит множество улучшений, связанных со стабильностью и производительностью.

Основные принципы

При расчете наилучшего пути к конечному адресу типичный дистанционно-векторный протокол сохраняет следующую информацию: расстояние (distance) (суммарная метрика или расстояние, например счетчик переходов) и вектор (следующий переход).

Вместо того, чтобы рассчитывать на полные регулярные обновления для выполнения повторной сходимости, EIGRP (вместо отбрасывания данных) строит таблицу топологии используя для этого все объявления своих соседей и выполняет сходимость либо посредством поиска подходящего беспетлевого маршрута в таблице топологии, либо (если о таком маршруте ничего не известно) посредством опроса своих соседей. Второй маршрутизатор сохраняет информацию, полученную от первого и третьего маршрутизаторов.

Из этих кратких пояснений очевидно, что EIGRP должен обеспечить следующее:

- систему, при которой EIGRP пересылает обновления, необходимые в данный момент (это достигается посредством обнаружения и обслуживания соседей)
- способ, позволяющий определить, какой из маршрутов, полученный маршрутизатором, является беспетлевым
- процедуру, позволяющую удалять нерабочие маршруты из таблиц топологии на всех маршрутизаторах, находящихся в сети
- процедуру опроса соседей, которая позволит найти новые маршруты к конечному адресу взамен утраченных старых маршрутов

Обнаружение и обслуживание соседей

Для распространения маршрутной информации по сети в EIGRP используется непериодическое инкрементное обновление маршрутов. Это

означает, что EIGRP пересылает обновления только для изменяющихся маршрутов и только в тот момент, когда такие маршруты изменяются.

Основной недостаток таких обновлений заключается в том, что вы можете не узнать, в какое время маршрут, проходящий через соседний маршрутизатор, стал недоступным. Нельзя блокировать по времени маршруты, ожидающие получение новой таблицы маршрутизации от соседа. Для надежной пересылки изменений в маршрутной таблице в EIGRP используется механизм взаимодействия между соседними маршрутизаторами (два маршрутизатора становятся "соседями" в том случае, если каждый из них получает пакеты "hello" от своего соседа).

EIGRP посылает пакеты "hello" каждые 5 секунд (для каналов с высокой пропускной способностью) и каждые 60 секунд (для многоточечных каналов с низкой пропускной способностью).

Пятисекундный пакет "hello" используется:

- в сетевых средах (например, Ethernet, Token Ring и FDDI)
- в последовательных каналах "точка-точка" (например, выделенные линии, использующие протоколы PPP или HDLC; подчиненные интерфейсы Frame Relay типа "точка-точка" и подчиненный интерфейс ATM
- многоточечные линии с высокой пропускной способностью (выше, чем у линии T1) (например, ISDN PRI и Frame Relay)

Шестидесятисекундный пакет "hello":

- многоточечные линии с пропускной способностью как у T1 или ниже – как у многоточечных интерфейсов Frame Relay, многоточечных интерфейсов ATM, коммутируемых виртуальных каналов ATM и базовых интерфейсов обмена ISDN

Частота, с которой EIGRP отправляет пакеты "hello", называется hello-интервалом; этот параметр можно настраивать для каждого интерфейса в отдельности при помощи команды **ip hello-interval eigrp**. Время удержания –

время, в течение которого маршрутизатор будет считать соседнее устройство действующим, не получая при этом от него пакет "hello". Время удержания обычно равняется трем hello-интервалам (15 и 180 секунд по умолчанию). Время удержания настраивается при помощи команды **ip hold-time eigrp**.

Вопросы для подготовки

1. Обнаружение сетей.
2. Поддержка таблицы маршрутизации.
3. Маршрутные петли.
4. Дистанционно-векторные протоколы маршрутизации в настоящее время.

Тема 13. RIP, VLSM И CIDR

Начальное развитие классовой адресации решило проблему ограничения на 256 сетей - на какое-то время. Десятилетие спустя стало ясно, что пространство IP-адресов истощается весьма быстро. В ответ на это Инженерная группа по развитию интернета (IETF) представила Бесклассовую Междоменную маршрутизацию (CIDR), которая использует Подсети с Маской Переменной длины (VLSM), чтобы помочь сохранить адресное пространство.

С **введением CIDR и VLSM**, ISP могли теперь назначать одну часть классовый сети одному клиенту и другую часть - другому клиенту. Это присвоение несмежных адресов ISP шло параллельно с разработкой бесклассовых протоколов маршрутизации. Для сравнения: классовые протоколы маршрутизации всегда суммируют на классовой границе и не включают маску подсети в маршрутные обновления. Бесклассовые протоколы маршрутизации в действительности включают маску подсети в маршрутные обновления и не обязаны выполнять суммирование. Бесклассовые протоколы маршрутизации, которую будут обсуждаться в последующих публикациях, — это RIPv2, EIGRP и OSPF.

С введением VLSM и CIDR, администраторы сети вынуждены были использовать дополнительные навыки разделения на подсети. VLSM просто разделяет подсеть на подсети. Подсети могут быть далее разделены на подсети на нескольких уровнях, как Вы узнаете в этой рубрике. В дополнение к разделению на подсети стало возможно суммировать большое количество классовых сетей в совокупный маршрут, или суперсеть. В этой рубрике также будут представлено суммирование маршрутов.

Вопросы для подготовки

1. RIP версии 1: дистанционно векторный, классовый протокол маршрутизации.
2. Основы конфигурирования RIPv1.

3. Обнаружение и исправление ошибок.
4. Автоматическая суммаризация.
5. Маршрут по умолчанию и RIPv1. VLSM и CIDR.
6. Классовая и бесклассовая адресация.
7. VLSM и суммаризация маршрутов.

Тема 14. RIPv2

Поскольку бесклассовые протоколы маршрутизации, как RIPv2, могут перенести и сетевой адрес, и маску подсети, они не обязаны суммировать эти сети к своим классовым адресам на главных сетевых границах. Поэтому, бесклассовые протоколы маршрутизации, такие как **RIPv2, поддерживают VLSM**.

Маршрутизаторы, использующие RIPv2, больше не должны применять маску входящего интерфейса, чтобы определить маску подсети в распространяемом маршруте. Сеть и маска явно включаются в каждое маршрутное обновление.

В сетях, которые используют схему адресации VLSM, бесклассовый протокол маршрутизации важен, чтобы распространять все сети наряду с их корректными масками подсетей. Глядя на вывод debug ip rip для R3 на рисунке, мы можем видеть, что RIPv2 включают сети и их маски подсетей в свои маршрутные обновления.

Также заметьте на рисунке, что мы еще раз добавили маршрутизатор R4 в топологию. Помните с RIPv1, R3 отправлял бы R4 только маршрут 172.30.0.0, у которого была та же самая маска, как у интерфейса выхода FastEthernet 0/0. Поскольку интерфейс 172.30.100.1 имеет маску /24, RIPv1 включал бы только подсети 172.30.0.0 с маской /24. Единственный маршрут, который удовлетворял этому условию, был 172.30.110.0.

Однако, с RIPv2, R3 может теперь включать все подсети 172.30.0.0 в свои маршрутные обновления к R4, как показано в выводе отладки на рисунке. Это потому, что RIPv2 может включать надлежащую маску подсети с сетевым адресом в обновлении.

Вопросы для подготовки

1. Ограничения RIPv1.
2. Конфигурирование RIPv2.
3. VLSM и CIDR.

4. Обнаружение и исправление ошибок в RIPv2.

Тема 15. ТАБЛИЦЫ МАРШРУТИЗАЦИИ

В создание и поддержку таблицы маршрутизации в маршрутизаторе Cisco вовлечены три процесса:

- Различные процессы маршрутизации, которые фактически запускают сетевой протокол или протокол маршрутизации, такой как улучшенный протокол маршрутизации внутреннего шлюза (EIGRP), связь между промежуточными системами (IS-IS), первоочередное открытие кратчайших маршрутов (OSPF).
- Сама таблица маршрутизации, которая получает сведения от процессов маршрутизации и отвечает на запросы данных от процесса переадресации.
- Процесс переадресации, который запрашивает информацию из таблицы маршрутизации, чтобы принять решение о переадресации пакета.

Чтобы понять, как происходит построение таблицы маршрутизации, рассмотрим взаимодействие между протоколами маршрутизации и таблицей маршрутизации.

Построение таблицы маршрутизации

Основные вопроси при построении маршрутной таблицы:

- Административное расстояние – Это мера надежности источника маршрута. Если маршрутизатор узнает о получателе из нескольких протоколов маршрутизации, то сравниваются административные расстояния и преимущество получают маршруты с меньшим административным расстоянием. Другими словами, это степень доверия источнику маршрута.
- Метрики – это мера, используемая протоколом маршрутизации для вычисления лучшего пути к данному месту назначения, если известно множество путей к нему. Каждый протокол маршрутизации использует свою метрику.
- Длина префикса

Поскольку каждый процесс маршрутизации получает обновления и иную информацию, он выбирает наилучший путь к указанному пункту назначения и предпринимает попытку внедрить данный путь в таблицу маршрутизации. Например, если протокол EIGRP определяет наилучший путь к адресу 10.1.1.0/24, выполняется попытка установки данного пути в таблицу маршрутизации.

Маршрутизатор решает, устанавливать ли маршруты, представленные процессом маршрутизации, основанном на административном расстоянии маршрута. Если данный маршрут имеет наименьшую административную длину до цели (по сравнению с другими маршрутами таблицы), он будет прописан в таблице маршрутизации. Если этот маршрут не является маршрутом с лучшим административным расстоянием, он отклоняется.

Для лучшего понимания давайте обратимся к примеру. Предположим, что в маршрутизаторе работает 4 процесса маршрутизации —: EIGRP, OSPF, RIP и IGRP. Все 4 процесса получили данные о различных маршрутах к сети 192.168.24.0/24, и каждый выбрал наилучший путь к этой сети, используя внутренние метрики и процессы.

Каждый из четырех процессов пытается установить свой маршрут к сети 192.168.24.0/24 в таблицу маршрутизации. Каждый из процессов маршрутизации назначил административное расстояние, которое используется для определения маршрута, который следует установить.

Резервные маршруты

Что другие протоколы, RIP, IGRP и OSPF, делают с неустановленными маршрутами? Что делать, если оптимальный маршрут, полученный от EIGRP, недоступен? ПО Cisco IOS® использует два похода к решению этой проблемы: Сначала каждый процесс маршрутизации должен периодически пытаться установить свои лучшие маршруты. Если наиболее предпочтительный маршрут недоступен, то на следующей попытке будет выбран следующий по приоритету маршрут (в соответствие с административным расстоянием). Другим решением для протокола маршрутизации, которому не удалось

установить маршрут в таблице, является использование маршрута и передача процессу таблицы маршрутизации команды послать отчет, если лучший маршрут даст сбой.

Для протоколов, не имеющих своей информации таблиц маршрутизации, например IGRP, используется первый метод. Каждый раз, когда протокол IGRP получает обновление маршрута, он пытается установить обновленные данные в таблицу маршрутизации. Если в таблице маршрутизации на это направление уже назначен маршрут, попытка установки закончится неудачей.

Для протоколов, не имеющих БД маршрутной информации, например EIGRP, IS-IS, OSPF, BGP и RIP, резервный маршрут регистрируется при сбое первоначальной попытки установить маршрут. Если маршрут, установленный в таблице маршрутизации, отказывает по тем или иным причинам, процесс обслуживания таблицы маршрутизации вызывает процессы всех протоколов маршрутизации, которые зарегистрировали резервный маршрут, и просит установить этот маршрут в таблицу. Если резервный маршрут зарегистрировали несколько протоколов, предпочтительный маршрут выбирается на основе административного расстояния.

Настройка административного расстояния

Административное расстояние по умолчанию не всегда подходит для вашей сети; можно внести изменение, чтобы маршруты RIP были предпочтительны, например, по сравнению с маршрутами IGRP. Перед тем как объяснить, как регулировать административные расстояния, необходимо посмотреть на последствия изменения административного расстояния.

Опасно изменять административное расстояние в протоколах маршрутизации! Изменение расстояний по умолчанию может привести к образованию петель маршрутизации. Рекомендуется изменять административное расстояние с осторожностью и с полным представлением о том, что требуется получить, и всех последствиях своих действий.

Для полных протоколов изменение расстояния относительно просто. Для этого необходимо ввести команду distance в режиме субконфигурации процесса маршрутизации.

Вопросы для подготовки

1. Структура таблицы маршрутизации.
2. Процесс просмотра таблицы маршрутизации.
3. Процесс маршрутизации.

Тема 16. EIGRP

Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюзов) является внутренним протоколом шлюзов, пригодным для различных топологий и сред. В хорошо спроектированной сети EIGRP хорошо масштабируется и обеспечивает чрезвычайно короткое время согласования с минимальным сетевым трафиком.

Принцип работы EIGRP

Основными преимуществами EIGRP являются:

- очень низкое использование сетевых ресурсов во время нормальной работы; только пакеты приветствия передаются в стабильной сети
- когда происходит изменение, распространяются только изменения таблицы маршрутизации, не вся таблица маршрутизации; это уменьшает нагрузку, которую сам протокол маршрутизации оказывает на сеть
- малое время конвергенции для изменений в топологии сети (в некоторых ситуациях конвергенция может быть почти мгновенной),

EIGRP – это улучшенный дистанционно-векторный протокол, который вычисляет кратчайший путь к назначению в рамках сети с помощью алгоритма диффузионного обновления (DUAL).

Основные версии протокола

Существует две основных редакции EIGRP, версии 0 и 1. Версии Cisco IOS, предшествующие 10.3 (11), 11.0 (8) и 11.1 (3), функционируют с более ранней версией EIGRP; некоторые пояснения в данной статье неприменимы к этой более ранней версии. Мы настоятельно рекомендуем пользоваться последней версией EIGRP, поскольку она отличается повышенными параметрами производительности и усовершенствованиями надежности.

EIGRP использует минимальную пропускную способность на пути к сети назначения и общую задержку для вычисления показателей маршрутизации. Можно также настроить и другие метрики. Однако мы не рекомендуем делать этого, поскольку в этом случае в вашей сети могут

появиться петли по маршрутизации. Метрики пропускной способности и задержки определяются из значений, настраиваемых в интерфейсах маршрутизаторов на пути к сети назначения.

Вопросы для подготовки

1. Основы конфигурации EIGRP.
2. Подсчет метрики EIGRP.
3. DUAL.
4. Расширенная конфигурация EIGRP.

Тема 17. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ ПО СОСТОЯНИЮ КАНАЛА

Протоколы маршрутизации можно классифицировать по различным группам в соответствии с их характеристиками. В частности, протоколы маршрутизации можно классифицировать по следующим признакам:

- **Назначение** — протокол внутренней маршрутизации (IGP) или протокол внешней маршрутизации (EGP)
- **Принцип работы** — дистанционно-векторный протокол, по состоянию канала или векторов маршрутов
- **Поведение** — протоколы классовой маршрутизации (устаревший метод) или бесклассовой маршрутизации

Например, протоколы маршрутизации IPv4 можно классифицировать следующим образом:

- **RIPv1 (устаревший)** — дистанционно-векторный классовый протокол внутренней маршрутизации;
- **IGRP (устаревший)** — дистанционно-векторный классовый протокол внутренней маршрутизации, разработанный компанией Cisco (не используется после выхода IOS 12.2 и более поздних версий);
- **RIPv2** — дистанционно-векторный бесклассовый протокол внутренней маршрутизации;
- **EIGRP** — дистанционно-векторный бесклассовый протокол внутренней маршрутизации, разработанный компанией Cisco;
- **OSPF** — бесклассовый протокол внутренней маршрутизации, по состоянию канала;
- **IS-IS** — бесклассовый протокол внутренней маршрутизации, по состоянию канала;
- **BGP** — бесклассовый протокол внешней маршрутизации, по вектору маршрута.

Протоколы классовой маршрутизации RIPv1 и IGRP являются устаревшими протоколами и используются только в старых сетевых

топологиях. Позднее эти протоколы были усовершенствованы в протоколы бесклассовой маршрутизации — RIPv2 и EIGRP. По своей природе протоколы маршрутизации по состоянию канала относятся к протоколам бесклассовой маршрутизации.

Вопросы для подготовки

1. Внедрение протоколов маршрутизации по состоянию канала.

Тема 18. OSPF

Протокол OSPF (Open Shortest Path First), описанный в стандарте RFC 2328, — это внутренний шлюзовый протокол, используемый для распространения данных маршрутизации внутри одной автономной системы. В этом документе описана работа протокола OSPF и его использование для проектирования и построения современных крупных и сложных сетей.

Общие сведения

Протокол OSPF был разработан, чтобы удовлетворить потребность интернет-сообщества в функциональном, непроприетарном протоколе внутреннего шлюза (IGP) для семейства протоколов TCP/IP. Обсуждение создания общего и совместимого протокола IGP для Интернета началось в 1988 году, но не было формализовано до 1991 года. В это время рабочая группа OSPF предложила утвердить OSPF в качестве чернового стандарта Интернета.

Протокол OSPF основан на технологии отслеживания состояния канала, которая является отступлением от векторных алгоритмов Беллмана-Форда, используемых в традиционных протоколах маршрутизации Интернета, таких как RIP. В стандарте OSPF были представлены новые концепции, такие как аутентификация обновлений маршрутизации, маски подсети переменной длины (VLSM), суммирование маршрутов и т. п.

В следующих главах мы рассмотрим терминологию и алгоритм OSPF, а также доводы за и против использования протокола в современных сложных и крупных сетях.

Сравнение OSPF и RIP

Быстрый рост и расширение современных сетей привели к тому, что протокол RIP достиг пределов своих возможностей. Протокол RIP имеет определенные ограничения, которые могут привести к возникновению проблем в крупных сетях:

- Протокол RIP поддерживает максимум 15 переходов. Сеть RIP, включающая более 15 переходов (15 маршрутизаторов) рассматривается как недоступная.
- Протокол RIP не может обрабатывать маски подсети переменной длины (VLSM). В условиях нехватки IP-адресов отсутствие гибкости и эффективности, которые предлагает назначение IP-адресов с использованием VLSM, является серьезным недостатком.
- Периодические широковещательные рассылки полной таблицы маршрутизации потребляют значительную долю пропускной способности. Это основная проблема крупных сетей, особенно на медленных каналах и облаках WAN.
- Конвергенция протокола RIP происходит медленнее, чем конвергенция OSPF. В крупных сетях конвергенция занимает около минуты. По истечению периода времени захвата и сбора мусора маршрутизаторы RIP начнут постепенно объявлять об истечение времени ожидания данных, которые не были получены в последнее время. Это неприемлемо в крупных средах, так как может привести к несогласованности маршрутизации.
- В RIP отсутствуют концепции задержки сети и стоимости канала. Решения о маршрутизации основываются на числе переходов. Путь с наименьшим числом переходов до места назначения всегда более предпочтителен, даже если более длинный путь обладает большей совокупной пропускной способностью канала и меньшими задержками.
- Сети RIP являются однородными. Понятие областей или границ отсутствует. С появлением бесклассовой маршрутизации и интеллектуального использования агрегирования и суммирования, сети RIP морально устарели.

В новой версии протокола RIP, которая называется RIP2, было представлено несколько усовершенствований. RIP2 решает задачи VLSM, аутентификации и многоадресных обновлений маршрутизации. Протокол RIP2 — это незначительное улучшение по сравнению с протоколом RIP (теперь он называется RIP1), так как в нем сохраняются ограничения на число

переходов и медленная конвергенция. Эти возможности критически важны для современных крупных сетей.

OSPF, в свою очередь, решает большую часть задач, описанных выше:

- В OSPF число переходов не ограничено.
- Интеллектуальное использование VLSM очень удобно при назначении IP-адресов.
- OSPF использует мультиадресную рассылку IP для отправки обновлений состояния канала. Это уменьшает объем обработки на маршрутизаторах, которые не прослушивают пакеты OSPF. Кроме того, обновления отправляются только при изменениях маршрутизации, а не периодически. Это обеспечивает более эффективное использование пропускной способности.
- OSPF предлагает более совершенную конвергенцию, RIP. Это связано с тем, что изменения маршрутизации распространяются мгновенно, а не периодически.
- OSPF предлагает более эффективное выравнивание нагрузки.
- OSPF предлагает логическое определение сетей, подразумевающее разделение маршрутизаторов на области. Это позволяет ограничить распространение обновлений по сети. Кроме того, эта возможность предоставляет механизм агрегирования маршрутов и сокращение ненужного распространения данных подсети.
- OSPF поддерживает аутентификацию маршрутизации с использованием различных методов аутентификации на основе пароля.
- Протокол OSPF обеспечивает передачу и маркировку внешних маршрутов, введенные в автономную систему. При этом отслеживаются внешние маршруты, введенные внешними протоколами, такими как BGP.

Безусловно, это приводит к усложнению настройки и устранения неполадок сетей OSPF. Администраторы, привыкшие к простоте RIP, столкнутся с большим объемом новой информации, который необходимо усвоить, чтобы управлять сетями OSPF на должном уровне. Кроме того,

увеличится объем служебных данных для выделения памяти и загрузки ЦП. Некоторые из маршрутизаторов под управлением RIP могут потребовать модернизации для обработки служебных данных OSPF.

Вопросы для подготовки

1. Основы конфигурации OSPF.
2. Метрика OSPF.
3. OSPF и сети со множественным доступом.
4. Расширенное конфигурирование OSPF.

СПИСОК ЛИТЕРАТУРЫ

1. **Паринов А.В. Сети связи и системы коммутации:** Учебное пособие / Паринов А.В., Ролдугин С.В., Мельник В.А. - Воронеж:Научная книга, 2016. - 178 с. ISBN 978-5-4446-0906-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/923309 (дата обращения: 15.05.2020). – Режим доступа: по подписке.
2. **Нужнов Е.В. Компьютерные сети. Часть 2. Технологии локальных и глобальных сетей:** учебное пособие / Нужнов Е.В. — Таганрог: Издательство Южного федерального университета, 2015. — 176 с. — ISBN 978-5-9275-1691-9. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/78675.html (дата обращения: 15.05.2020). — Режим доступа: для авторизированных пользователей.
3. **Чернецова Е.А. Системы и сети передачи информации. Часть 1. Системы передачи информации** / Чернецова Е.А. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2008. — 203 с. — ISBN 978-5-86813-204-9. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/17966.html (дата обращения: 15.05.2020). — Режим доступа: для авторизированных пользователей.
4. **Чернецова Е.А. Системы и сети передачи информации. Часть 2. Сети передачи информации** / Чернецова Е.А. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2008. — 199 с. — ISBN 978-5-86813-207-0. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/17967.html (дата обращения: 15.05.2020). — Режим доступа: для авторизированных пользователей.

Интернет-ресурсы

1. Учебный центр cisco.netocad.com для проведения тестов и проверки знаний.

2. Авторизованные курсы по сетевым технологиям:

1. CCNA Exploration 1: Network Fundamentals Tyumen State University. Режим доступа: https://1404116.netacad.com/courses/78983/assignments/1567605
2. CCNA R&S: Routing Protocols Tyumen State University. Режим доступа: https://1404116.netacad.com/courses/98158