Компьютерные системы и сети

Выпуск 3

Компьютерные системы и сети

Серия основана в 2013 году

Ответственный редактор А.В. Пролетарский

РЕДАКЦИОННЫЙ СОВЕТ:

А.А. Александров (*председатель*), д-р техн. наук
М.А. Басараб, д-р физ.-мат. наук
В.В. Девятков, д-р техн. наук
И.П. Иванов, д-р техн. наук
А.П. Карпенко, д-р техн. наук
Е.А. Микрин, академик РАН
А.В. Пролетарский, д-р техн. наук
И.В. Рудаков, канд. техн. наук
В.В. Сюзев, д-р техн. наук
В.М. Черненький, д-р техн. наук
А.Б. Шаповалов, д-р техн. наук
В.А. Шахнов, член-корр. РАН

Компьютерные системы и сети

Выпуск 3

Е.В. Смирнова, А.В. Пролетарский, Е.А. Ромашкина

Технологии TCP/IP в современных компьютерных сетях

Допущено Федеральным учебно-методическим объединением в системе высшего образования по укрупненной группе специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника» в качестве учебного пособия для студентов (адъюнктов), обучающихся по основным образовательным программам высшего образования по направлениям подготовки бакалавриата/магистратуры укрупненной группы специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника»

2019

УДК 004.7
ББК 32.973.202
С50

Р е ц е н з е н т ы:
генеральный директор АО «РтСофт», д-р техн. наук *О.В. Синенко*;
директор фирмы «1С», канд. экон. наук *Б.Г. Нуралиев*

Смирнова, Е.В.

С50 Технологии TCP/IP в современных компьютерных сетях : учебное пособие / Е. В. Смирнова, А. В. Пролетарский, Е. А. Ромашкина. — Москва : Издательство МГТУ им. Н.Э. Баумана, 2019. — 638, [2] с. : ил. — (Компьютерные системы и сети).

ISBN 978-5-94627-179-0

Книга посвящена изучению стека протоколов TCP/IP — технологической основе сети Интернет. Описывается стек протоколов TCP/IP. Рассматривается протокол PPP и его основные компоненты, протоколы аутентификации, сжатия и шифрования данных PPP, протоколы туннелирования PPP, включая PPPoE, PPPoA, PPTP и L2TP, типы подключения к провайдерам.

Изучается протокол IP версии 4 и версии 6, технология NAT, архитектура безопасности IP. Рассматривается протокол разрешения адресов ARP, методы Gratuitous ARP и Proxy ARP. Описан протокол ICMP версии 4 и версии 6. Рассматривается разрешение адресов IPv6, определение недоступности соседа, дублирования адресов, обнаружение маршрутизатора с помощью протокола NDP.

Отдельная глава посвящена технологиям маршрутизации. Изучается архитектура протоколов маршрутизации, алгоритмы маршрутизации, подробно описан протокол OSPF, включая версию 3. Рассматриваются основополагающие протоколы транспортного уровня TCP и UDP. Приведено описание протоколов уровня приложений Telnet, SSH, SSL/TLS, DHCP, DHCPv6. Изложена методика поиска неисправностей в сетях TCP/IP.

Предлагаемые практические работы охватывают все рассмотренные темы. Издание содержит обширный глоссарий. Учебное пособие является результатом многолетнего сотрудничества МГТУ им. Н.Э. Баумана и компании D-Link по подготовке кадров для сферы информационно-коммуникационных технологий.

УДК 004.7
ББК 32.973.202

ISBN 978-5-94627-179-0

© Смирнова Е.В., Пролетарский А.В.,
Ромашкина Е.А., 2019
© Оформление. Издательство
МГТУ им. Н.Э. Баумана, 2019

Оглавление

Предисловие

Развитие технологий в сети Интернет определило бурную цифровизацию нашей жизни. Уже обыденностью стал Интернет вещей, нас окружают виртуальная и дополненная реальности. Через Интернет идет улучшение сферы здравоохранения и повышение качества повседневной жизни, доступнее становится образование, развиваются социальные сети. Все это и многое другое стало возможным благодаря технологической основе сети Интернет — стеку протоколов TCP/IP.

Эта книга посвящена подробному изучению протоколов TCP/IP — набору правил, определяющему, как доставить информацию в сети быстро и безопасно. Ее выпуск стал результатом многолетнего сотрудничества МГТУ им. Н.Э. Баумана и компании D-Link по подготовке кадров для сферы информационно-коммуникационных технологий. Это третья по счету книга в серии «Компьютерные системы и сети» после книг «Технологии коммутации и маршрутизации в локальных компьютерных сетях» и «Технологии современных беспроводных сетей Wi-Fi». Вместе с ранее изданными книгами по IP-телефонии, технологиям защиты информации в компьютерных сетях, управлению коммутируемой средой авторы предоставляют возможность специалистам изучить широкий спектр информационно-коммуникационных технологий, повысить квалификацию.

Учебное пособие состоит из 10 глав, 22 практических работ и обширного глоссария.

Глава 1 посвящена истории TCP/IP, в ней описываются стек протоколов TCP/IP.

В главе 2 рассматривается протокол PPP. Общий формат кадра PPP, функционирование канала PPP, LCP, NCP, протоколы аутентификации, сжатия данных, шифрования PPP, протоколы туннелирования, передача PPP через Ethernet и ATM, протоколы PPTP, L2TP, типы подключения к провайдерам.

Глава 3 посвящена протоколу IP версии 4 и версии 6, архитектуре безопасности.

В главе 4 рассматриваются протокол разрешения адресов ARP, методы Gratuitous ARP и Proxy ARP, разрешение адресов для IPv6.

В главе 5 представлен протокол ICMP, классы, типы и коды сообщений ICMP, правила генерации сообщений ICMP, утилита ping.

Глава 6 посвящена протоколу NDP, разрешению адресов IPv6 и определению недоступности соседа, определению дублирования адресов, обнаружению маршрутизатора.

В главе 7 вводится понятие маршрутизации; подробно представлены IP-интерфейсы маршрутизирующих коммутаторов, архитектура протоколов маршрутизации, алгоритмы маршрутизации, дистанционно-векторные протоколы маршрутизации, протокол OSPF, включая версию 3.

В главе 8 рассматриваются протоколы транспортного уровня TCP и UDP.

Глава 9 посвящена протоколам уровня приложений Telnet, SSH, SSL/TLS, DHCP, DHCPv6.

В главе 10 изложена методика поиска неисправностей в сетях TCP/IP.

Практическая часть содержит 22 лабораторные работы, охватывающие все теоретические вопросы. Теоретический материал и выполненные практические задания дают возможность получить полный объем знаний и компетенций по технологиям информационного обмена в сети.

Обозначения, используемые в книге

В тексте книги для обозначения сетевых устройств различных типов используются следующие пиктограммы:

Коммутатор

DSLAM

Маршрутизатор/
Коммутатор L3

Беспроводной
маршрутизатор

Рабочая
станция

Портативный
компьютер

Персональный
компьютер

Сервер

Сетевая
среда

Беспроводная
среда

Злонамеренный
пользователь

Шлюз
безопасности

1. Обзор TCP/IP

1.1. История TCP/IP

Термин TCP/IP, который относится к целому семейству протоколов, образован из названий двух из них: Transmission Control Protocol (TCP) и Internet Protocol (IP). Протоколы семейства TCP/IP начали разрабатывать как часть экспериментальной сети ARPAnet, созданной Агентством перспективных исследований Министерства обороны США (United States Defense Advanced Research Projects Agency, DARPA, или ARPA). Первоначально сеть ARPAnet использовала адаптированные к ее требованиям существующие на тот момент протоколы. Однако все они имели какие-либо недостатки или ограничения. Разработчики новой сети поняли, что использование имеющихся протоколов приведет к существенным проблемам по мере ее расширения.

В 1973 году началась разработка полноценной системы протоколов межсетевого обмена для сети ARPAnet. Самая ранняя ее версия, написанная в 1973 году, содержала описание только одного протокола: TCP. Эта аббревиатура означала «Transmission Control Program». Далее эта версия была доработана и в декабре 1974 года формально документирована в RFC 675 «Specification of Internet Transmission Control Program».

Тестирование и исследование TCP продолжались несколько лет. В марте 1977 года была документирована вторая версия TCP. В августе 1977 года произошел переломный момент в разработке TCP/IP. Джон Постел (Jon Postel), являющийся одним из разработчиков TCP/IP и Интернета, опубликовал в Internet Engineering Note number 2 ряд комментариев о состоянии TCP. В частности, он отметил, что новый протокол пытается выполнять слишком много функций и должен использовать принцип разбиения на уровни. Это замечание Постела привело к созданию архитектуры TCP/IP и разбиению первоначального TCP (Transmission Control Program) на два уровня: Transmission Control Protocol (TCP) на транспортном уровне и Internet Protocol (IP) на сетевом уровне. Процесс разбиения был описан в 1978 году в третьей версии TCP. Первая версия стандартов TCP и IP, используемая в современных сетях, была документирована в 1980 году как TCP version 4 и IP version 4. По этой причине у протокола IP первая версия 4, а не 1. TCP/IP быстро стал набором протоколов для ARPAnet, а позже, в 1983 году — для Интернета.

Успех стека протоколов TCP/IP определяется как историческими факторами (протоколы для Интернета), так и техническими характеристиками, включающими интегрированную адресную систему, возможность маршрутизации, независимость от нижележащих технологий LAN, WLAN и WAN, масштабируемость, использование открытых стандартов и универсальность.

2. Протокол PPP

Стек протоколов TCP/IP подразумевает, что функциональность второго уровня обеспечивается технологиями локальных и глобальных сетей. Технологии локальных сетей 802.11 были рассмотрены в книге «Технологии современных беспроводных сетей Wi-Fi». При подключении в Интернет зачастую используются двухточечные линии связи, т. е. линии связи, соединяющие устройство клиента с устройством провайдера услуг. Способы подключения локальных сетей к сетям провайдеров могут быть разными: через телефонную линию, по оптоволоконному кабелю, с использованием сотовой связи, кабельных модемов. Одним из протоколов для установления WAN-соединения является протокол PPP (Point-to-Point Protocol, протокол двухточечного соединения). Протокол PPP определяет метод транспортировки дейтаграмм различных протоколов сетевого уровня по последовательным каналам типа «точка-точка». Он описан в RFC 1661 и доработан в более поздних документах RFC 1662 и др. Для работы протокола PPP не требуются никакие дополнительные технологии канального уровня. Он функционирует непосредственно поверх физического соединения, которое использует одну из технологий доступа типа «точка-точка»: Dial-Up, ISDN, ADSL, GPON и т. п.

Существуют расширения протокола PPP, позволяющие передавать пакеты PPP через сети Ethernet (PPPoE) и ATM (PPPoA). Протокол PPP over Ethernet (PPPoE) описан в RFC 2516. Он служит для подключения множества устройств одной сети через единственное абонентское устройство к удаленному концентратору доступа, расположенному на стороне провайдера. Протокол PPPoE используется при подключении в Интернет по технологиям xDSL, ETTx и FTTx. Спецификация PPP over AAL5 (PPPoA) определена в RFC 2364 и описывает инкапсуляцию протокола PPP посредством ATM Adaptation Layer 5 (AAL5). Протокол PPPoA в основном применяется при подключении в Интернет с использованием кабельных модемов (стандарт DOCSIS) и технологий семейства xDSL.

PPP является протоколом с установлением соединения, который позволяет создавать L2-каналы поверх различных соединений физического уровня. Он поддерживает как синхронные, так и асинхронные каналы. Эти каналы, работающие в полнодуплексном режиме, подразумевают, что кадры отправляются и получаются в одном и том же порядке.

Несмотря на то что PPP расшифровывается как Point-to-Point Protocol, его правильнее рассматривать не как протокол, а как стек протоколов. PPP состоит из трех основных компонентов (рис. 2.1):

1) метода для инкапсуляции дейтаграмм множества протоколов. PPP определяет специальный формат кадра для инкапсуляции данных, основанный на кадре, используемом в протоколе HDLC (High-Level Data Link Control);

2) протокола управления каналом (Link Control Protocol, LCP), позволяющего автоматически устанавливать каналы связи, тестировать их,

3. Протокол IP

Протокол *IP* (Internet Protocol) является основным протоколом стека TCP/IP и *сетевого уровня* (network layer). Основная задача сетевого уровня — доставка данных между устройствами различных сетей, которые соединены произвольным образом, т. е. образуют *составную сеть* (internetwork) (рис. 3.1).

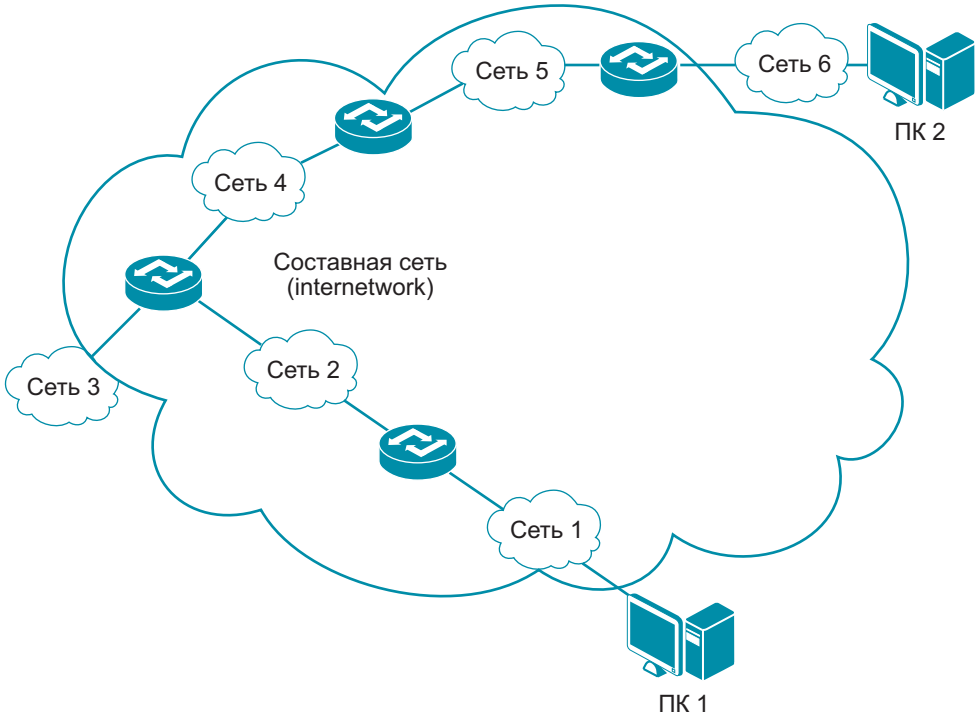

Рис. 3.1. Составная сеть

Сети могут быть построены с использованием различных протоколов канального и физического уровня. Таким образом, они используют различные форматы кадров, методы доступа к среде передачи, методы модуляции и кодирования. Для того чтобы соединить такие сети, нужен общий межсетевой уровень, использующий понятный всем нижележащим сетям протокол. Таким протоколом является протокол IP.

Успех протокола IP был обусловлен его характеристиками, несмотря на имеющиеся в нем ограничения. Он независим от протоколов нижележащих уровней и обеспечивает универсальную адресацию узлов, которая позволяет выполнять маршрутизацию пакетов данных в составных сетях. Протокол IP является протоколом без установления соединения (connectionless protocol). Это означает, что когда узел A хочет передать данные узлу B, им не надо

4. Протоколы разрешения адресов

Передача данных через составную сеть выполняется на сетевом уровне модели OSI с использованием IP-адреса, но фактическая передача выполняется на канальном уровне, который использует адреса канального уровня, например MAC-адреса.

В этой главе будет объяснено, каким образом по известному сетевому адресу (IP-адресу) можно узнать адрес канального уровня (MAC-адрес) устройства-получателя.

Два из семи уровней модели OSI ответственны за функции адресации. Это канальный и сетевой уровни. В модели TCP/IP это уровни доступа к сети и Интернет.

Рассмотрим пример: клиент локальный сети обращается к серверу www.dlink.ru (рис. 4.1).

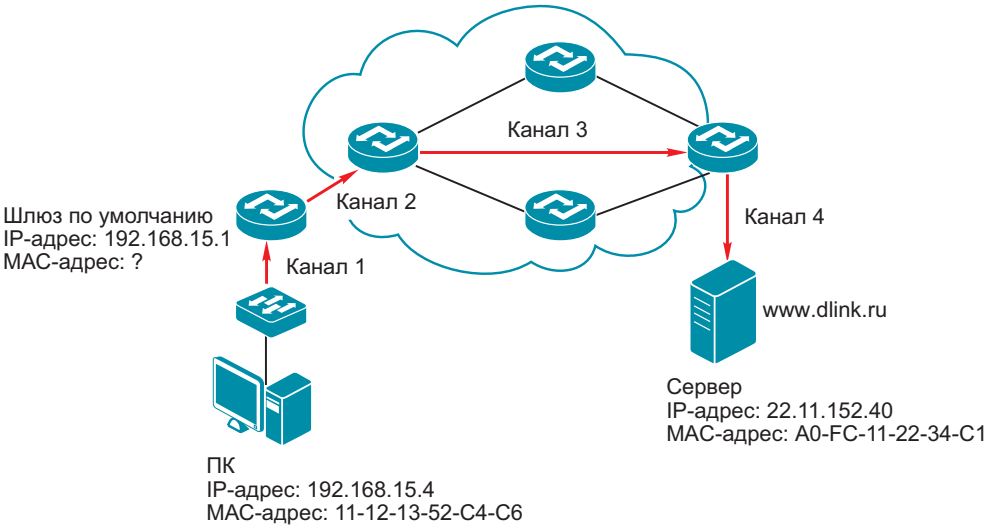

Рис. 4.1. Передача данных в составной сети

Логически соединение осуществляется между клиентом и сервером. Фактически клиент и сервер соединены последовательностью каналов связи, работающих по технологиям канального уровня. В примере таких каналов четыре. Они соединяют между собой маршрутизаторы, находящиеся между клиентом и сервером.

На каждом шаге на основе IP-адреса получателя принимается решение, куда отправить данные, но фактическая передача выполняется на втором уровне, с использованием адреса канального уровня следующего предполагаемого получателя кадра на маршруте.

5. Протокол ICMP

Основным протоколом сетевого уровня является протокол IP, который позволяет доставлять данные в сетях TCP/IP между узлами составной сети. Протокол IP не гарантирует надежной доставки пакета до адресата. Другими словами, отправитель передает пакеты через составную сеть и не получает подтверждение доставки.

Протокол IP не обладает механизмами отправки служебных сообщений, которые позволяли бы сообщать устройству-отправителю о проблемах, возникающих при передаче пакетов, или осуществлять тестирование соединения. Поэтому недостающие в протоколе IP функции выполняются с помощью протокола *Internet Control Message Protocol* (*ICMP*).

Протокол ICMP является неотъемлемой частью протокола IP и обеспечивает его поддержку в форме ICMP-сообщений, которые инкапсулируются в IP-пакеты. Первоначальный протокол ICMP был определен в RFC 792 одновременно с протоколом IP, описанным в RFC 791. В середине 1990-х годов появился протокол IPv6, для которого также надо было определить версию протокола ICMP. Таким образом, новую версию протокола ICMP назвали ICMPv6 (RFC 4443), а оригинальную версию ICMP стали называть ICMPv4.

Сообщения ICMPv4 и ICMPv6 имеют одинаковый базовый формат (рис. 5.1). Структура сообщения может быть разделена на две части — общую и уникальную. Общая часть состоит из трех полей, размер которых одинаков для всех типов сообщений:

- *Type* (*Tun*) — определяет тип сообщения ICMP;
- *Code* (*Kod*) — определяет подтип сообщения внутри ICMP-сообщения каждого типа;
- *Checksum* (*Контрольная сумма*) — вычисляется аналогично контрольной сумме заголовка IPv4.

Уникальная часть содержит поля, определенные для каждого типа сообщения.

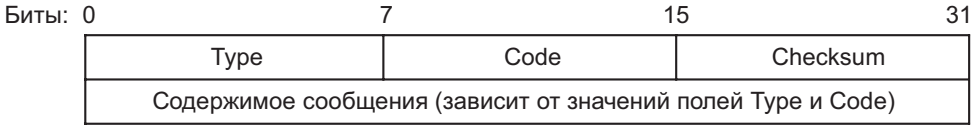

Рис. 5.1. Формат сообщения ICMPv4/v6

Обе версии протокола ICMPv4 и ICMPv6 определяют общую систему передачи сообщений. В дополнение к сообщениям, определенным протоколом ICMP, другие протоколы также могут определять свои типы сообщений ICMP. Некоторые самые важные из них приведены в табл. 5.1.

6. Протокол NDP

Изменения, которые были сделаны в IPv6, коснулись не только самого протокола IP, но и служебных протоколов сетевого уровня. В частности, в стеке TCP/IPv4 для разрешения адресов канального уровня используется протокол ARP. В стеке TCP/IPv6 функция разрешения адресов и ряд функций, относящихся к взаимодействию устройств в локальной сети, реализованы протоколом *NDP* (*Neighbor Discovery Protocol* — протокол обнаружения соседей). Протокол NDP, подобно протоколу ICMP, является протоколом обмена сообщениями, с помощью которых он выполняет ряд функций. В настоящее время он определен в RFC 4861.

Понятие «сосед» используется в различных сетевых протоколах и технологиях для обозначения устройств, способных отправлять сообщения непосредственно друг другу. В локальной сети имеются как компьютеры, так и маршрутизаторы (коммутаторы L3), поэтому термин «сосед» может применяться к любому из устройств. Поскольку компьютеры и маршрутизаторы играют разные роли в сети, в результате для этих устройств процесс обнаружения соседей будет различаться.

В RFC 4861 определены девять функций, выполняемых протоколом NDP. Для ясности эти функции можно разбить на три группы, как показано на рис. 6.1.

Рис. 6.1. Функции, выполняемые протоколом NDP

Задачу обнаружения в локальной сети маршрутизаторов и обмена данными между ними и узлами выполняют четыре функции.

- *Router Discovery* — позволяет узлам локальной сети обнаруживать маршрутизаторы и получать от них сетевые параметры, необходимые для автоконфигурации.
- *Parameter Discovery* — позволяет узлам получать параметры локальной сети и/или маршрутизаторов, например MTU локального канала связи.
- *Prefix Discovery* — используется для определения префикса сети.

7. Понятие маршрутизации

Протокол IP является *маршрутизируемым протоколом* (routable protocol), т. е. протоколом, формат пакета которого содержит адресную информацию, позволяющую определять маршрут и доставлять данные между устройствами различных физических сетей, соединенных произвольным образом. Процесс определения пути, по которому IP-пакет будет доставлен адресату, называется *маршрутизацией* (routing). Различные физические сети связаны между собой посредством специальных устройств, называемых *маршрутизаторами* (router). Каждый маршрутизатор напрямую подключается как минимум к двум сетям. Основным назначением маршрутизаторов является определение пути следования пакетов и принятие решения об их перенаправлении на одно из ближайших маршрутизирующих устройств.

Обычные компьютеры также участвуют в процессе доставки IP-пакетов. Прежде чем приложение на компьютере-отправителе начнет передачу данных приложению на узле-получателе, необходимо узнать IP-адрес получателя. IP-адрес назначения будет известен сетевому приложению, если его ввел пользователь или он получен в результате разрешения доменных имен с помощью протокола DNS (Domain Name System), например, когда в адресной строке браузера пользователь ввел доменное имя сайта. Далее компьютер должен определить начальный маршрут пакета и решить, какому из ближайших узлов он должен быть переправлен.

Существует два метода, с помощью которых IP-пакет может быть доставлен в пункт назначения (рис. 7.1): *прямая доставка* (*direct delivery*) и *непрямая доставка* (*indirect delivery*).

Прямая доставка выполняется между двумя узлами, находящимися в одной локальной сети (например, сети Ethernet или Wi-Fi). Узлы могут быть соединены друг с другом с помощью промежуточного устройства, такого как коммутатор или точка доступа. Локальные узлы также могут получать доступ друг к другу и обмениваться информацией без использования каких-либо дополнительных устройств. *Непрямая* доставка происходит в том случае, когда получатель пакета находится в другой локальной сети. При этом отправитель пересылает пакет ближайшему маршрутизирующему устройству, которое выполняет его дальнейшую доставку конечному получателю.

Подведя итог, можно сделать следующий вывод. Передача IP-пакетов между двумя устройствами, подключенными к одной локальной сети, происходит напрямую без использования маршрутизаторов. Отправитель сообщения помещает пакет в кадр канального уровня, пересылаемый физическим уровнем непосредственно получателю. Получатель принимает кадр, извлекает из него пакет и передает его на сетевой уровень. Если отправитель не знает MAC-адреса получателя, он может отправить, например, ARP-запрос и, получив ответ, сформировать кадр.

Как отправитель узнает, что он находится с получателем в одной локальной сети? Все просто. IP-адрес состоит из двух частей: номера (префикса)

8. Протоколы транспортного уровня

Основным протоколом сетевого уровня является протокол IP. Он передает сетевые пакеты *без установления соединения*, *без обеспечения надежности* и *без подтверждения доставки*. Получается, что при организации передачи данных на основе протокола IP, отправитель не будет знать, доставляются ли его IP-пакеты получателю или нет.

Во время передачи по сети IP-пакеты с определенной долей вероятности могут быть искажены или потеряны. Несмотря на то что некоторые сетевые приложения организуют собственную проверку доставки передаваемых данных, а также имеют собственные средства диагностики и обработки вероятных ошибок, существуют и такие приложения, которые перекладывают выполнение этих функций на стандартные сетевые протоколы. Обеспечить сетевым приложениям передачу данных с той степенью надежности, которая им требуется, способны протоколы *транспортного уровня*.

На транспортном уровне функционируют два основных протокола — TCP (Transmission Control Protocol, протокол управления передачей) и UDP (User Datagram Protocol, протокол дейтаграмм пользователей).

Протокол TCP обеспечивает установку соединения между отправителем и получателем, разбиение крупных информационных блоков на сегменты ограниченной длины, а также их гарантированную доставку получателю в заданном порядке и без ошибок. Функционирование протокола TCP предполагает его взаимодействие с протоколами уровня приложений, например, HTTP, FTP, SMTP и др.

Протокол UDP в отличие от TCP не устанавливает соединение перед передачей данных и не требует от получателя подтверждений о доставке, но за счет именно этих особенностей он работает быстрее, чем TCP. Протокол UDP используют в тех задачах, где в первую очередь необходимо обеспечить хорошую скорость передачи данных, а гарантия доставки и надежность имеют второстепенное значение. Примером такой задачи является передача потокового видео по технологии IPTV.

8.1. Адресация протоколов TCP и UDP

На сетевом уровне модели OSI для уникальной идентификации сетевого интерфейса используется сетевой адрес, например адрес IPv4. Сетевая адресация является механизмом, с помощью которого пакеты маршрутизируются в нужную сеть. На транспортном уровне существует еще один уровень адресации, который обеспечивает возможность приема/передачи данных несколькими сетевыми приложениями, одновременно работающими на одном IP-интерфейсе. Протоколы транспортного уровня TCP и UDP используют концепцию *порта* и *сокета*.

Большинство передач с использованием протоколов стека TCP/IP имеют форму обмена информацией между программой на одном устройстве с соответствующей программой на другом устройстве. Программа, которая

9. Протоколы уровня приложений

Уровень приложений (*Application layer*) находится на самом верху моделей OSI и TCP/IP. Он обеспечивает интерфейс между пользовательскими приложениями и нижележащей сетью, т. е. предоставляет приложениям возможность доступа к сервисам нижележащих уровней и определяет протоколы, с помощью которых они обмениваются данными. Существует множество протоколов уровня приложений. Рассмотрим некоторые из них, использующиеся при администрировании сетей.

9.1. Протокол Telnet

Telnet является старейшим среди протоколов TCP/IP. Он описан в RFC 854 и использует в качестве транспорта протокол TCP (порт 23). Telnet обеспечивает эмуляцию текстового терминала, позволяя терминалам или терминальным процессам взаимодействовать через сеть TCP/IP (рис. 9.1).

Протокол Telnet основан на трех основных идеях:

1) концепции сетевого виртуального терминала;
2) принципе согласования опций;
3) симметрии терминалов и процессов.

Каждый конец соединения Telnet играет роль *сетевого виртуального терминала* (*Network Virtual Terminal, NVT*). Сетевой виртуальный терминал — абстрактное устройство, которое представляет традиционный терминал. Это исключает необходимость запоминания клиентом и сервером информации о характеристиках терминалов друг друга. Таким образом, обеспечивается стандартный интерфейс при подключении к удаленному устройству. Виртуальный терминал имеет принтер, чтобы выводить на экран входящие данные, и клавиатуру, чтобы вводить данные, которые будут переданы удаленной стороне. Для того чтобы расширить минимальные возможности виртуального терминала, Telnet предоставляет сторонам соединения средства для согласования опций (например, локальный или удаленный эхо-контроль, страничный режим, высоту и ширину экрана и т. д.). При этом и сервер, и клиент могут предлагать свои опции независимо друг от друга. Одна сторона инициирует запрос, а другая сторона может либо принять, либо отвергнуть предложение. Если запрос принимается, то опция немедленно вступает в силу.

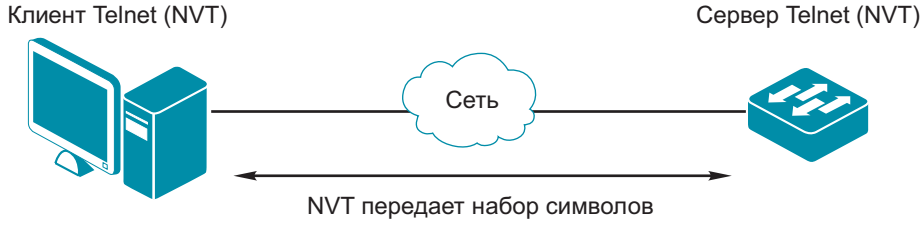

Рис. 9.1. Сервис Telnet

10. Поиск неисправностей в сетях TCP/IP

Поиск неисправностей в компьютерных сетях является одной из задач системных администраторов и сотрудников технической поддержки. Сети состоят из множества элементов: компьютеров, принтеров, IP-телефонов, серверов, систем хранения информации, сетевого оборудования, различного рода сетевого программного обеспечения и т. д. Устройства подключаются друг к другу с помощью кабелей или по беспроводной связи.

Из-за общего усложнения сетевой среды возрастает вероятность появления проблем со связью и снижения производительности. Администратор сети должен владеть методиками анализа сетевых проблем с точки зрения различных уровней модели TCP/IP или OSI и уметь использовать необходимые средства для эффективного выявления и устранения проблем со связью.

Первым шагом в решении сетевой проблемы является обнаружение ее источника. Сетевые проблемы могут произойти в той части сети, которую контролирует администратор, а могут быть частью внешней сети (сети провайдера). В этом разделе будут рассматриваться методики анализа сетевых проблем в локальных сетях.

10.1. Методика поиска неисправностей

Процесс поиска неисправностей в сетевой среде должен быть систематизирован. Необходимо определить конкретные признаки неисправности и выявить все потенциальные проблемы, которыми они могут быть вызваны. Затем устранить все возможные причины проблем и удостовериться, что все признаки неисправности исчезли.

Ниже приведены шаги процесса поиска неисправностей.

1. Получение подробной информации о возникшей проблеме. При диагностике любой проблемы полезно применять логический подход. Обычно при поиске неполадок следует искать ответы на такие вопросы:

- Что работает?
- Что не работает?
- Как между собой связаны вещи, которые работают и которые не работают?
- Работало ли когда-нибудь то, что сейчас не работает?
- Если да, то что изменилось с тех пор, когда оно работало?

Соберите все факты, которые позволят наиболее точно установить возможные причины проблемы.

2. Воспроизведение проблемы при возможности. При возможности самостоятельно воспроизведите проблему. Это позволит выяснить, правильно ли вы поняли ее причину.

3. Локализация и изоляция причины. Попытайтесь определить место, откуда начать поиск неполадок и изолировать ошибку в устройстве, программном обеспечении или конфигурации, которые вызывают проблему.

Лабораторные работы

Практическая часть состоит из 22 лабораторных работ. Каждая лабораторная работа содержит схему подключения с указанием количества рабочих мест, на которое она рассчитана.

Комплект оборудования на 1 рабочее место:

Маршрутизатор DIR-825/AC/G1 ..... 1 шт.
Коммутатор DES-1100-16 ..... 1 шт.
Коммутатор DGS-3120-24TC/*RI ..... 2 шт.
Консольный кабель ..... 2 шт.
Кабель Ethernet ..... 4 шт.
Кабель USB-COM (RS-232)[1] ..... 2 шт.
Рабочая станция с ОС Windows ..... 2 шт.
Рабочая станция с ОС Linux Ubuntu ..... 1 шт.

В лабораторных работах приведена настройка для устройств со следующими версиями программного обеспечения:

Маршрутизатор DIR-825/AC/G1 ..... v3.0.4
Коммутатор DES-1100-16 ..... v1.00.B29
Коммутатор DGS-3120-24TC/*RI v4.19.R005

Для лабораторных работ, в которых используется ОС Linux, подготовлен образ виртуальной машины DlinkLab_18.04LTS.ova для VirtualBox. В виртуальной машине установлены все необходимые пакеты и утилиты. Инструкция по установке образа виртуальной машины в VirtualBox описана в Приложении А.

Лабораторные работы можно выполнять на отдельной рабочей станции с ОС Linux Ubuntu. В этом случае должны быть установлены следующие пакеты и утилиты: pppoe, wireshark, vlan, xl2tpd, vsftpd, hping3, python 2.7, curl 7.58.0, minicom, telnet, openssh, openssl, tftpd-hpa, isc-dhcp-server.

Примечание

Пример установки пакета pppoe. В терминале введите команду:

```
$ sudo apt-get install pppoe
```

На рабочих станциях с ОС Windows должно быть установлено ПО:

Анализатор трафика Wireshark ..... https://goo.gl/JkpRMc
Программа эмуляции терминала PuTTY https://goo.gl/DHKV2m
TFTP-сервер Tftpd https://goo.gl/ziAPA3
FTP-сервер Golden FTP Server ..... https://goo.gl/jQBHKW
Утилита iPerf https://goo.gl/zsxR6T

[1] Кабель USB-COM (RS-232) нужен в том случае, если на рабочей станции отсутствует COM-порт для подключения консольного кабеля.

Лабораторная работа № 1. Подключение к сети провайдера с использованием метода доступа PPPoE

Протокол Point-to-Point Protocol over Ethernet (PPPoE) обеспечивает передачу пакетов PPP через сеть Ethernet и позволяет подключать сетевые узлы локальной сети через одно абонентское устройство к концентратору доступа (Access Concentrator, AC), расположенному на стороне провайдера.

Основную идею PPPoE можно объяснить следующим образом. Он моделирует телефонное соединение, в котором каждая сессия PPP трактуется как отдельная телефонная линия. Чтобы обеспечить соединение «точка-точка» через Ethernet, каждая сессия PPP должна знать MAC-адрес удаленного узла и установить уникальный идентификатор сессии. Эти задачи в PPPoE выполняет протокол обнаружения (Discovery). В то же время PPPoE не позволяет пользователю постоянно оставаться на связи. Он должен сообщать свое имя и пароль каждый раз, когда хочет подключиться к сети.

Протокол PPPoE использует клиент-серверную модель. Клиент PPPoE отправляет запрос на установление соединения PPPoE-серверу. После успешного завершения двумя сторонами переговоров PPP, функции управления доступом и аутентификации клиента PPPoE выполняет PPPoE-сервер.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Windows ..... 2 шт.
Рабочая станция с ОС Linux ..... 1 шт.
Коммутатор DES-1100-16 ..... 1 шт.
Маршрутизатор DIR-825 ..... 1 шт.
Кабель Ethernet ..... 3 шт.

Используемое ПО для ОС Linux:

- Анализатор трафика Wireshark
- Пакет PPPoE

Цель работы: смоделировать подключение к сети Интернет через PPPoE-соединение.

1.1. Настройка PPPoE-соединения между рабочими станциями и сервером

Смоделируем подключение нескольких пользователей к сети Интернет через PPPoE-соединение (рис. 1.1). В сети провайдера настроен PPPoE-сервер, через который пользователи получают доступ в Интернет, пройдя аутентификацию. Провайдер назначает каждому пользователю имя и пароль, на основе которых он будет управлять доступом и контролировать оплату предоставляемых услуг. На рабочей станции пользователя запущен PPPoE-клиент. PPP-соединение устанавливается напрямую с сервером без использования маршрутизатора.

Примечание
В лабораторной работе не рассматривается настройка перенаправления пакетов в сеть Интернет через PPPoE-сервер.

Проверка работоспособности

Установлено PPPoE-соединение с сервером? _____

1. На рабочей станции ПК 2 зайдите на Web-интерфейс маршрутизатора.
2. Настройте проброс PPPoE-трафика. Для этого выберите *Дополнительно → ALG/Passthrough* и установите переключатель *Проброс PPPoE*. Нажмите кнопку *Применить*.
3. Сохраните настройки. Выберите *Система → Конфигурация → Сохранить*.
4. Повторно подключитесь к PPPoE-серверу на рабочих станциях ПК 2 и ПК 3.

Установлено PPPoE-соединение с сервером? _____

Лабораторная работа № 2. Подключение к PPPoE-серверу из разных VLAN стандарта IEEE 802.1Q

Предположим, что сеть провайдера сегментирована с помощью VLAN на основе стандарта IEEE 802.1Q. В лабораторной работе рассмотрим, как организовать подключение к PPPoE-серверу пользователей из разных виртуальных локальных сетей (VLAN).

Виртуальной локальной сетью (Virtual Local Area Network, VLAN) называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, полностью изолирован от других узлов сети на канальном уровне. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса (индивидуального, группового или широковещательного). В то же время внутри виртуальной локальной сети кадры передаются по технологии коммутации, т. е. только на тот порт, который связан с адресом назначения кадра. С помощью виртуальных локальных сетей решается проблема распространения широковещательных кадров и вызываемых ими последствий, которые могут приводить к широковещательным штормам и существенно снижать производительность сети.

Основные определения IEEE 802.1Q:

- *VLAN ID* (VID) — идентификатор VLAN;
- *Tagging* (маркировка кадра) — процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра;
- *Untagging* (удаление тега из кадра) — процесс удаления информации о принадлежности к 802.1Q VLAN из заголовка кадра.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет соединять серверы с сетевыми интерфейсами, поддерживающими стандарт IEEE 802.1Q.

IP-адреса DNS-серверов _____

2. На рабочей станции ПК 1 посмотрите информацию о PPP-соединениях:

```
$ ifconfig
```

3. Посмотрите подробную информацию об виртуальном интерфейсе `enp0s3.10`. В терминале рабочей станции ПК 1 введите:

```
$ sudo cat /proc/net/vlan/enp0s3.10
```

4. Посмотрите подробную информацию об виртуальном интерфейсе `enp0s3.20`:

```
$ sudo cat /proc/net/vlan/enp0s3.20
```

Лабораторная работа № 3. Подключение к сети провайдера с использованием метода доступа L2TP

Протокол Layer Two Tunneling Protocol (L2TP) является комбинацией протоколов PPTP и Layer 2 Forwarding (L2F) — технологии, предложенной компанией Cisco Systems. IETF объединила в протоколе L2TP лучшие характеристики этих протоколов.

Протокол L2TP расширяет возможности протокола PPP. Он позволяет, чтобы конечные точки соединения канального уровня и PPP находились на разных устройствах, соединенных между собой IP-сетью.

Протокол L2TP определяет создание туннелей между LAC и LNS и последующую инкапсуляцию туннелируемых PPP-сессий.

Терминология L2TP:

- *L2TP Access Concentrator* (LAC, концентратор доступа L2TP) — это узел, который перенаправляет пакеты между LNS и удаленной системой (remote system). Пакеты, отправленные от LAC к LNS, туннелируются по протоколу L2TP. Соединение между LAC и удаленной системой либо является локальным (см. Client LAC), либо выполняется по протоколу PPP.
- *L2TP Network Server* (LNS, L2TP-сервер) — это узел, который действует как одна из конечных точек туннеля и является противоположной стороной LAC. LNS — логическая конечная точка PPP-сессии, которая туннелируется от удаленной системы с помощью LAC.
- *Client LAC* (клиент LAC) — это узел, на котором установлено программное обеспечение L2TP. Он может непосредственно участвовать в туннелировании и подключаться к LNS без использования отдельного LAC.
- *Remote System* (удаленная система) — это компьютер или маршрутизатор, который устанавливает соединение с LAC.

Лабораторная работа № 4. Планирование IP-подсетей

Для того чтобы устройство участвовало в сетевом взаимодействии с помощью протокола IP, его интерфейсу присваивается уникальный IP-адрес.

Адрес IPv4 представляет собой 32-разрядное (4 байта) двоичное поле. Для удобства восприятия и запоминания этот адрес разделяют на четыре части по 8 бит (октеты), каждый октет переводят в десятичное число и при записи разделяют точками. Это представление адреса называется *десятично-точечной нотацией*.

IP-адрес структурирован, он состоит из двух частей: из сетевой части адреса — идентификатора сети (Net ID) и из идентификатора узла (Host ID), который однозначно определяет устройство в сетевом сегменте. Идентификатор сети определяет конкретную сеть или сегмент сети, в которой находится узел, и используется для передачи данных на определенный сетевой интерфейс маршрутизатора. После того как данные достигают нужной сети, они, исходя из идентификатора узла, передаются уникальному узлу.

Формирование подсетей

Процедура разбиения сетей на подсети описана в RFC 950. Для этого в структуру IP-адреса был добавлен еще один уровень иерархии — подсеть (subnetwork). Таким образом, была создана трехуровневая иерархия в системе IP-адресации: сеть, содержащая подсети, каждая из которых включает определенное количество узлов.

С появлением трехуровневой иерархии IP-адреса потребовались дополнительные методы, которые позволяли бы определить, какая часть адреса указывает на идентификатор подсети, а какая — на идентификатор узла. Было предложено использовать битовую маску (bit mask), которая отделяла бы часть адресного пространства идентификаторов узлов от адресного пространства идентификаторов подсети. Такая битовая маска называется *маской подсети* (subnet mask).

Маска подсети — это 32-битное число, двоичная запись которого содержит непрерывную последовательность единиц в тех разрядах, которые определяют идентификатор подсети, и непрерывную последовательность нулей в тех разрядах, которые определяют идентификатор узла. Маска записывается в точечно-десятичном представлении аналогично IP-адресу.

При использовании масок можно разбивать сети на меньшие по размеру подсети путем расширения сетевой части адреса и уменьшения узловой части. Для вычисления количества подсетей используется формула 2^s, где s — количество бит, занятых под идентификатор сети из части, отведенной под идентификатор узла. Количество узлов в каждой подсети вычисляется по формуле $2^n - 2$, где n — количество бит, оставшихся в части, идентифицирующей узел, а два адреса — адрес подсети и широковещательный адрес — зарезервированы в каждой полученной подсети.

Задание 3. Посмотрите на рис. 4.3. Рабочая станция ПК 4 может обмениваться данными с рабочей станцией ПК 2, но при этом соединение с ПК 3 отсутствует. Укажите причину проблемы.

Лабораторная работа № 5. Настройка фильтрации трафика по IP-адресам

Маршрутизаторы D-Link поддерживают функцию фильтрации по IP-адресам (IP Filtering), которая разрешает или запрещает доступ в Интернет пользователям локальной сети на основе их IP-адресов. Администратор может настроить правила для обработки сетевых пакетов. При этом он может как полностью запретить доступ в Интернет для указанного IP-адреса, так и ограничить его определенными протоколами.

При попытке подключения пользователя в Интернет или к ресурсу, расположенному во внешней сети, маршрутизатор проверит правила фильтрации и определит, разрешен ли этому пользователю доступ или нет.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Windows ..... 3 шт.
Коммутатор DES-1100-16 ..... 1 шт.
Маршрутизатор DIR-825 ..... 1 шт.
Кабель Ethernet ..... 4 шт.

Цель работы: настроить правила фильтрации сетевых пакетов.

5.1. Фильтрация IPv4-адресов

Рассмотрим настройку IP-фильтрации для схемы сети, показанной на рис. 5.1. Требуется запретить рабочей станции ПК 2 доступ к рабочей станцией ПК 3 (серверу). Остальным рабочим станциям из локальной сети доступ к серверу разрешить.

Настройка рабочих станций и подключение устройств

1. Подключите рабочие станции ПК 1, ПК 2 и ПК 3 к коммутатору и маршрутизатору, как показано на рис. 5.1.

2. На рабочих станциях ПК 1, ПК 2 и ПК 3 настройте статические IP-адреса, как показано на рис. 5.1.

Лабораторная работа № 6. Изучение команд настройки коммутатора через CLI

В предыдущих лабораторных работах рассматривалась настройка коммутатора через Web-интерфейс. В дальнейшем для настройки некоторых функций коммутатора будет использоваться интерфейс командной строки (Command Line Interface, CLI). В связи с этим рассмотрим процесс подключения к интерфейсу командной строки через консольный порт и основные команды коммутатора.

Все команды CLI являются чувствительными к регистру, поэтому, прежде чем вводить команду, надо убедиться, что отключены все функции, которые могут привести к изменению регистра текста.

При работе в CLI можно вводить сокращенный вариант команды. Например, если ввести команду *sh sw*, то коммутатор интерпретирует эту команду как *show switch*.

Для описания ввода команд, ожидаемых значений и аргументов при настройке коммутатора через CLI используются приведенные ниже символы:

< угловые скобки >	
Назначение	Содержат ожидаемую переменную или значение, которое должно быть указано
Синтаксис	`config ipif <System> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable}] | bootp | dhcp]`
Описание	В приведенном примере синтаксиса пользователь должен указать имя IP-интерфейса, имя VLAN длиной до 32 символов и сетевой адрес. Угловые скобки вводить не надо
Пример	`config ipif System ipaddress 10.24.22.5/8 vlan default`
[квадратные скобки]	
Назначение	Содержат требуемое значение или набор аргументов. Может быть указано одно значение или аргумент
Синтаксис	`create account [admin | user] <username 15>`
Описание	В приведенном примере пользователь должен указать для учетной записи один из двух уровней привилегий (admin или user). Квадратные скобки вводить не надо.
Пример	`create account admin user1`

3. Если указано ключевое слово *system*, на коммутаторе восстановятся все заводские настройки по умолчанию в полном объеме. Коммутатор сохранит эти настройки в энергонезависимой памяти NVRAM и перезагрузится:

```
reset system
```

4. Перезагрузите коммутатор:

```
reboot
```

Лабораторная работа № 7. Настройка IPSec-туннеля между двумя сетями

Одним их недостатков первоначального протокола IP было отсутствие каких-либо механизмов, обеспечивающих аутентификацию и целостность данных, передаваемых через составную сеть. Для обеспечения различных сервисов безопасности на уровне IP для протоколов IPv4 и IPv6 был разработан набор протоколов IP Security, или IPSec.

В большинстве случаев IPSec используется для обеспечения сервисов виртуальных частных сетей (VPN). С помощью протоколов IPSec можно реализовать различные топологии VPN, основными из которых являются:
- шлюз безопасности–шлюз безопасности (Security gateway–Security gateway);
- узел–шлюз безопасности (Host–Security gateway);
- узел–узел (Host–Host).

Термин «шлюз безопасности» используется для обозначения устройства, которое реализует протоколы IPSec, например, маршрутизатор или межсетевой экран.

VPN на основе IPSec часто используется для безопасной передачи данных между двумя сетями, например для соединения главного офиса и филиала через Интернет. В этом случае в каждой из сетей устанавливается шлюз безопасности и между ними создается VPN-подключение. Шлюзом может быть как выделенное устройство, выполняющее только функции VPN, так и сетевое устройство — межсетевой экран или маршрутизатор.

В лабораторной работе рассмотрим настройку топологии «шлюз безопасности–шлюз безопасности».

В архитектуре IPSec можно выделить четыре основные части:
- безопасная ассоциация;
- протоколы IPSec;
- алгоритмы и методы шифрования/хеширования;
- безопасная ассоциация и управление ключами.

Безопасная ассоциация (Security Association, SA) — это набор алгоритмов и параметров безопасности, таких как ключи шифрования, который определяет, как шифровать и аутентифицировать поток данных между двумя

Какой протокол IPSec используется для защиты трафика? _____

В Wireshark установите фильтр для этого протокола. Зашифрованы данные, передаваемые по туннелю? _____

Объясните, будет ли шифроваться трафик, передаваемый между рабочей станцией ПК 1 и маршрутизатором R1._____

_____

_____

Лабораторная работа № 8. Изучение протоколов разрешения адресов

Процесс, который позволяет определить адрес канального уровня, используя известный адрес сетевого уровня, называется *разрешением адресов* (address resolution). В стеке TCP/IP для разрешения IPv4-адресов используется протокол ARP.

Процесс разрешения адресов в протоколе ARP выполняется путем обмена сообщениями типа «запрос–ответ»:

- *ARP Request* (ARP-запрос): устройство-источник, которому требуется отправить IP-пакет, посылает широковещательный запрос всем устройствам локальной сети, чтобы определить, кто является получателем пакета.
- *ARP Reply* (ARP-ответ): устройство-получатель отправляет назад источнику одноадресное сообщение, посылая в нем свой адрес канального уровня.

Поскольку ARP является протоколом динамического разрешения адресов, каждое разрешение адресов требует обмена сообщениями по сети. Всякий раз, когда устройство отправляет ARP-сообщение, оно использует полосу пропускания сети, а также загружает ЦПУ сетевых устройств на его обработку.

Решением данной проблемы является использование *кеширования* (caching). ARP-кеш представляет собой таблицу, связывающую между собой MAC- и IP-адреса узлов. По сути таблица — это просто разделы оперативной памяти устройства. Каждое устройство в сети создает и обслуживает свою собственную ARP-таблицу.

Существуют два способа создания записей в ARP-таблице:

- *статические записи* (Static ARP Entries), которые создают вручную и которые постоянно хранятся в ARP-таблице. Статические записи используются в том случае, если устройства взаимодействуют на постоянной основе;
- *динамические записи* (Dynamic ARP Entries) — связки физический адрес/IP-адрес создаются динамически в результате работы протокола ARP. Они хранятся в таблице только в течение определенного периода времени и затем удаляются. Это делается для того, чтобы не использовать много системной памяти и чтобы записи в таблице были актуальными.

В ARP-таблице могут храниться как статические, так и динамические записи.

Лабораторная работа № 9. Настройка протокола маршрутизации RIP с агрегированными каналами

Понятие маршрутизации

Процесс определения пути, по которому IP-пакет будет доставлен адресату, называется *маршрутизацией* (routing). Различные физические сети связаны между собой посредством специальных устройств, называемых *маршрутизаторами* (router). Каждый маршрутизатор напрямую подключается как минимум к двум сетям. Основное назначение маршрутизаторов — определение пути следования пакетов и принятие решения об их перенаправлении на одно из ближайших маршрутизирующих устройств.

Отправитель не всегда знает, где находится сеть, в которой расположен получатель. Отыскать ее помогают маршрутизирующие устройства. IP-пакет, предназначенный устройству из другой сети/подсети, пересылается локальному маршрутизатору (коммутатору L3), называемому *шлюзом по умолчанию* (default gateway). Для этого узел локальной сети должен знать IP-адрес шлюза по умолчанию — IP-адрес интерфейса маршрутизатора (коммутатора L3), на который перенаправляется весь трафик, не предназначенный для устройств данной локальной сети. Этот адрес указывается в настройках устройств. Его можно настроить на узле вручную либо получить динамически. Настройка шлюза по умолчанию не требуется, если передача данных будет выполняться только между устройствами одной локальной сети.

Как только одному компьютеру надо отправить пакет другому компьютеру, находящемуся в удаленной сети, он инкапсулирует его в кадр и передает по локальной сети шлюзу по умолчанию. Приняв пакет, маршрутизатор анализирует его IP-адрес назначения и определяет следующий шаг (hop) пакета, т. е. ближайший маршрутизатор, которому надо передать пакет, чтобы он был доставлен адресату. Таким образом, пакет передается от одного маршрутизирующего устройства другому, пока не достигнет маршрутизатора, находящегося с получателем в одной локальной сети.

Процесс маршрутизации пакетов в составных сетях выполняется на основе базы данных маршрутов, называемой *таблицей маршрутизации* (routing table). Она содержит записи, представляющие собой список наилучших маршрутов к определенным сетям и/или узлам. Записи в таблице маршрутизации может создавать вручную администратор сети в процессе конфигурации устройства или они могут создаваться автоматически в результате работы протоколов динамической маршрутизации.

В таблице маршрутизации возможны записи следующих типов.

- Маршрут к сети. Маршрут к сети с определенным идентификатором.
- Маршрут к узлу. Маршрут к узлу с определенным сетевым адресом.
- Маршрут по умолчанию (default route). Маршрут, который используется в том случае, если другой маршрут к пункту назначения неизвестен.

На коммутаторе SW3 введите:

```
create iproute default 192.168.30.2
```

16. Проверьте таблицу маршрутизации на всех коммутаторах:

```
show iproute
```

Коммутатор SW1:
Сколько записей в таблице маршрутизации? _____
Коммутатор SW2:
Сколько записей в таблице маршрутизации? _____
Коммутатор SW3:
Сколько записей в таблице маршрутизации? _____

17. Проверьте, по какому маршруту передаются данные от рабочей станции ПК 1 к рабочей станции ПК 2. В командной строке ПК 1 введите:

```
tracert 192.168.60.10
```

По какому маршруту передается трафик? Сколько на нем переходов? ____
_____

18. Проверьте, по какому маршруту передаются данные от рабочей станции ПК 2 к рабочей станции ПК 1. В командной строке ПК 2 введите:

```
tracert 192.168.50.10
```

По какому маршруту передается трафик? Сколько на нем переходов? ____
_____

Лабораторная работа № 10. Настройка протокола маршрутизации OSPF в широковещательной сети

Протокол OSPF (Open Shortest Path First) является протоколом динамической маршрутизации. Он способен быстро обнаруживать изменения топологии в автономной системе и вычислять новые маршруты после окончания периода сходимости. Период сходимости короткий, он включает минимальный обмен трафиком маршрутизации.

В протоколах с учетом состояния канала каждый маршрутизатор обслуживает базу данных, описывающую топологию автономной системы. Эта база данных называется *базой данных состояния канала* (Link State Database, LSDB). Она идентична на каждом маршрутизаторе. Каждая отдельная часть этой базы данных описывает локальное состояние определенного маршрутизатора, т. е. используемые им интерфейсы и его доступных соседей. Все

Лабораторная работа № 11. Настройка перераспределения маршрутов между RIP и OSPF

Перераспределение маршрутов (route redistribution) используется для передачи маршрутов, изученных с помощью одного протокола, в другой протокол маршрутизации. Для того чтобы выполнялось перераспределение маршрутов, должен быть хотя бы один маршрутизатор, на котором запущены одновременно два протокола маршрутизации и настроены правила передачи маршрутов. При перераспределении маршрутов из RIP в OSPF коммутатор SW2, показанный на рис. 11.1, будет выполнять роль граничного коммутатора автономной системы (AS boundary router, ASBR) и рассылать в сеть OSPF сообщения AS-external-LSA с описанием маршрутов к пунктам назначения за пределами автономной системы.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Windows ..... 2 шт.
Коммутатор DGS-3120-24TC ..... 3 шт.
Кабель Ethernet ..... 4 шт.
Консольный кабель ..... 2 шт.

Используемое ПО для ОС Windows:

- Программа эмуляции терминала PuTTY

Цель работы: настройки перераспределения маршрутов между RIPv2 и OSPFv2.

Настройка рабочих станций и подключение устройств

1. С помощью Ethernet-кабелей подключите рабочие станции ПК 1 и ПК 2 к портам коммутаторов, как показано на рис. 11.1.

2. На рабочих станциях ПК 1 и ПК 2 настройте статические IP-адреса, как показано на рис. 11.1.

3. Соедините коммутаторы SW1, SW2 и SW3 между собой с помощью Ethernet-кабелей, как показано на рис. 11.1

Настройка коммутатора SW1

1. Подключите рабочую станцию ПК 1 к консольному порту коммутатора с помощью кабеля RS-232. Запустите программу эмуляции терминала PuTTY.

2. Сбросьте настройки коммутатора к заводским настройкам по умолчанию:

```
reset config
```

3. Измените приглашение для ввода команд:

```
config command_prompt SW1
```

5. Убедитесь, что коммутатор SW2 является ASBR для area 0.0.0.0. В командной строке коммутатора SW2 введите:

```
show ospf
```

6. Посмотрите базу данных состояния канала (LSBD) на коммутаторе SW2:

```
show ospf lsdb
```

Что наблюдаете? Какие типы LSA находятся в таблице? _____
_____

7. Посмотрите таблицу маршрутизации на коммутаторе SW3:

```
show iproute
```

Сколько записей в таблице маршрутизации? _____
Информация о каких сетях содержится в таблице маршрутизации?_____
_____

Лабораторная работа № 12. Обнаружение и защита от атаки TCP SYN Flood

Протокол TCP (Transmission Control Protocol) выполняет установление TCP-соединения между отправителем и получателем, обеспечивает гарантированную доставку данных, обнаруживает ошибки и управляет потоком. Процесс установления TCP-соединения называется *трехсторонним рукопожатием* (three-way handshake). При установлении TCP-соединения клиент отправляет серверу TCP-сегмент с установленным битом SYN и ждет от него подтверждения. Сервер принимает соединение и в ответ отправляет сегмент с установленными битами SYN и ACK (SYN+ACK). Как только клиент получает сегмент SYN+ACK, он отправляет серверу сегмент с битом ACK. После этого TCP-соединение установлено и приложения могут обмениваться данными.

Схема трехстороннего рукопожатия подвержена атаке TCP SYN Flood, которая является разновидностью атак типа «отказ в обслуживании» (Denial-of-Service, DoS). Суть атаки в том, что злоумышленник посылает серверу множество TCP-сегментов с битом SYN, а затем игнорирует сегменты SYN+ACK от сервера. Злоумышленник будет блокировать ресурсы сервера, потому что сервер должен хранить информацию о каждом устанавливаемом соединении. В результате атаки происходит переполнение таблицы состояний, и сервер не сможет установить соединения с пользователями. Когда таблица состояний переполнена, неподтвержденные соединения отбрасываются, чтобы освободить место для новых соединений.

Проверка работоспособности

1. На рабочей станции ПК 2 запустите утилиту hping3:

```
$ sudo hping3 -c 300 -S -i u1 212.46.14.1
```

2. На рабочей станции ПК 1 зайдите на Web-интерфейс маршрутизатора. Выберите *Межсетевой экран → Защита от DoS*.
Что наблюдаете? Какой IP-адрес заблокировал маршрутизатор? _____
_____

Лабораторная работа № 13. Изучение механизма TCP Fast Open

Передача данных между клиентом и сервером начинается после завершения трехстороннего рукопожатия. Клиент может начать передачу данных сразу после отправки серверу TCP-сегмента с битом ACK, а сервер должен ожидать получение этого сегмента, прежде чем передавать данные. Процесс трехстороннего рукопожатия применяется при установке любого TCP-соединения и оказывает влияние на производительность всех сетевых приложений. Для повышения производительности был предложен механизм *TCP Fast Open* (TFO). Он предлагает способ безопасной передачи данных в сегментах с битом SYN в процессе трехстороннего рукопожатия.

Стандарт TCP позволяет передавать данные в сегментах с SYN, но запрещает получателю доставлять их приложению до окончания трехстороннего рукопожатия. Это делается с целью защиты от старых или повторяющихся сегментов. TFO удаляет это ограничение и позволяет доставлять приложению данные из сегментов SYN.

Изменение семантики TCP накладывает новые ограничения и делает TFO неподходящим для использования определенными приложениями. Существует ограничение на максимальный размер данных внутри сегмента с SYN — могут отправляться только определенные HTTP-запросы и приложения должны повторно использовать соединения. Для получения преимуществ от применения TFO он должен поддерживаться клиентом, сервером и приложением. В противном случае устанавливается стандартное TCP-соединение.

Основным компонентом TFO является *Fast Open Cookie* (cookie) — код аутентификации сообщения, генерируемый сервером. Клиент запрашивает cookie у сервера и использует их для ускоренного обмена данными в последующих запросах к тому же серверу. Для запроса или отправки cookie в TCP-сегменте используется опция *Fast Open Cookie*.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Linux ..... 2 шт.
Коммутатор DES-1100-16 ..... 1 шт.
Кабель Ethernet ..... 2 шт.

```
$ curl -s -w "%{time_connect}\n" 192.168.10.1:8000 --tcp-fastopen
```

Сравните время, затраченное на установление TCP-соединения с/без поддержки механизма TCP Fast Open. Какой можно сделать вывод? _____

_____

Лабораторная работа № 14. Настройка доступа к локальному FTP-серверу из внешней сети

Технология NAT преобразует адреса из частного адресного пространства сети в однозначное и зарегистрированное открытое адресное пространство IPv4. Существуют два варианта традиционного NAT — *базовый NAT* и *NAPT* (Network Address Port Translation). При базовом NAT в исходящих из частной сети пакетах NAT маршрутизатор заменяет локальный IP-адрес источника на глобальный IP-адрес из пула адресов и вносит запись в таблицу NAT, где фиксируется соответствие IP-адресов. Затем он рассчитывает новую контрольную сумму для заголовка IP, и измененный IP-пакет с новым заголовком передается адресату. Адрес получателя в пакете не изменяется.

NAPT (или Port Address Translation (PAT), или overloaded NAT) дополнительно преобразует номера портов TCP и UDP. NAPT позволяет большому числу узлов частной сети разделять единственный глобальный адрес. Чтобы можно было различать IP-пакеты различных отправителей, устройство NAPT заменяет номер порта TCP/UDP в заголовке TCP/UDP исходного IP-пакета на другой, уникальный номер порта TCP/UDP и вносит соответствующую запись в таблицу NAT. При таком преобразовании система должна заново рассчитать контрольную сумму не только заголовка IP, но и заголовка TCP/UDP. После этого она создает новые заголовки TCP/UDP и IP, затем передает IP-пакет соответствующему адресату. NAPT может быть скомбинирован с базовым NAT таким образом, чтобы использовался пул глобальных адресов совместно с преобразованием портов.

Рассмотрим ситуацию, когда во внутренней сети находится FTP-сервер и клиенту, находящемуся во внешней сети, необходимо получить к нему доступ. На границе внешней и внутренней сети находится маршрутизатор NAT. Он будет пропускать пакеты из внешней сети во внутреннюю только в том случае, если в таблице трансляции имеются соответствующие записи. Решением является использование функции *Virtual Server* (Виртуальные серверы). Функция позволяет создавать в таблице трансляции статические записи, обеспечивающие передачу пакетов из внешней сети на внутренние серверы. Обращение к серверу выполняется с использованием глобального IP-адреса маршрутизатора, который транслируется во внутренний IP-адрес. Отличить один запрашиваемый сервис от другого позволяет указание номеров портов TCP/UDP.

Проверка работоспособности

1. На рабочей станции ПК 2 подключитесь к FTP-серверу. Откройте браузер и введите:

```
ftp://212.46.14.1
```

2. Проверьте соединение между рабочими станциями ПК 1 и ПК 2 с помощью команды `ping`.
Объясните наличие/отсутствие связи между рабочими станциями_____
_____

3. На рабочей станции ПК 2 измените IP-адрес на 212.46.14.56. Маску подсети и основной шлюз оставьте без изменений.

4. Еще раз подключитесь к FTP-серверу.
Что наблюдаете? Почему так происходит? _____

Лабораторная работа № 15. Организация удаленного доступа к коммутатору по Telnet

Чтобы управлять коммутатором через интерфейс командной строки, сетевой администратор подключается к устройству консольным кабелем, открывает программу эмуляции терминала и вводит команды. Это удобно, если администратор рядом с устройством, но невозможно, когда он находится в другой комнате, здании или городе. Протокол *Telnet* помогает удаленно управлять коммутатором или другим устройством через виртуальный терминал, который запускается на рабочей станции.

В управляемых коммутаторах D-Link Telnet-сервер включен по умолчанию, поэтому для доступа к настройкам коммутатора администратор запускает на рабочей станции Telnet-клиент и вводит IP-адрес управления коммутатора. При этом рабочая станция должна находиться в той же подсети, что и коммутатор, если в сети не настроена маршрутизация.

Если на рабочей станции установлена ОС Windows, то в ней уже встроен Telnet-клиент, который нужно включить через *Программы и компоненты*, так как по умолчанию он выключен. Соединение Telnet запускается через командную строку Windows.

В ОС Linux для удаленного управления устройствами через Telnet используется установленная по умолчанию утилита *telnet*.

В обеих операционных системах получить доступ к коммутатору по Telnet можно с помощью программы эмуляции терминала PuTTY.

В лабораторной работе рассмотрено управление коммутатором по Telnet с рабочей станции ОС Linux и ОС Windows, поэтому используйте любую из этих операционных систем.

Лабораторная работа № 16. Организация удаленного доступа к коммутатору по SSH

Протокол SSH обеспечивает безопасное соединение благодаря шифрованию передаваемых данных, включая пароли.

Как и в протоколе Telnet, в SSH-соединении участвуют две стороны: клиент и сервер. Чтобы подключиться к интерфейсу командной строки коммутатора по протоколу SSH, администратор запускает на рабочей станции SSH-клиент и вводит IP-адрес управления коммутатора. При этом рабочая станция должна находиться в той же подсети, что и коммутатор, если в сети не настроена маршрутизация.

В управляемых коммутаторах D-Link по умолчанию активирован протокол Telnet. Для управления коммутатором через SSH администратор должен отключить Telnet и запустить SSH-сервер.

При подключении клиента SSH-сервер проверяет его подлинность с помощью одного из трех методов аутентификации.

- *Аутентификация по паролю*: клиент отправляет сообщение, в котором содержится пароль в открытом виде. Это сообщение передается по зашифрованному каналу.
- *Аутентификация узла*: выполняется аутентификация клиентского устройства, а не самого клиента. Этот метод работает, когда клиент отправляет подпись, созданную с помощью закрытого ключа узла. Таким образом, все пользователи, имеющие доступ к этому устройству, будут аутентифицированы.
- *Аутентификация с открытым ключом*: клиент отправляет серверу сообщение, в котором содержится открытый ключ клиента. Сообщение подписывается закрытым ключом. Когда сервер его получает, он проверяет ключ и подпись клиента. Если ключ и подпись верны, аутентификация успешна.

В лабораторной работе рассмотрим аутентификацию с открытым ключом. В ОС Linux для генерации ключей и удаленного управления устройствами через SSH используется установленная по умолчанию утилита OpenSSH.

В ОС Windows для генерации ключей и доступа к интерфейсу командной строки коммутатора по SSH используется программа PuTTY.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Linux или ОС Windows ..... 1 шт.
Коммутатор DGS-3120-24TC ..... 1 шт.
Кабель Ethernet ..... 1 шт.
Консольный кабель ..... 1 шт.

Используемое ПО для ОС Windows:

- Программа эмуляции терминала PuTTY
- Программа для генерации ключей PuTTYgen
- Программа для хранения пароля для закрытого ключа Pageant
- Анализатор трафика Wireshark
- TFTP-сервер Tftpd

Лабораторная работа № 17. Настройка безопасного доступа к Web-интерфейсу коммутатора

Web-интерфейс управления позволяет осуществлять настройку и мониторинг параметров коммутатора, используя любой компьютер, оснащенный стандартным Web-браузером. Браузер представляет собой универсальное средство доступа и может непосредственно подключаться к коммутатору по протоколу HTTP или HTTPS. Web-интерфейс обеспечивает графическое представление интерфейса управления коммутатора в режиме реального времени и предоставляет подробную информацию о состоянии портов, модулей, их типе и т. д.

Web-интерфейс управления коммутатора состоит из пользовательского графического интерфейса (GUI), запускающегося на клиенте, и HTTP/HTTPS-сервера, запускаемого на коммутаторе.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Linux ..... 1 шт.
Коммутатор DGS-3120-24TC ..... 1 шт.
Кабель Ethernet ..... 1 шт.
Консольный кабель ..... 1 шт.

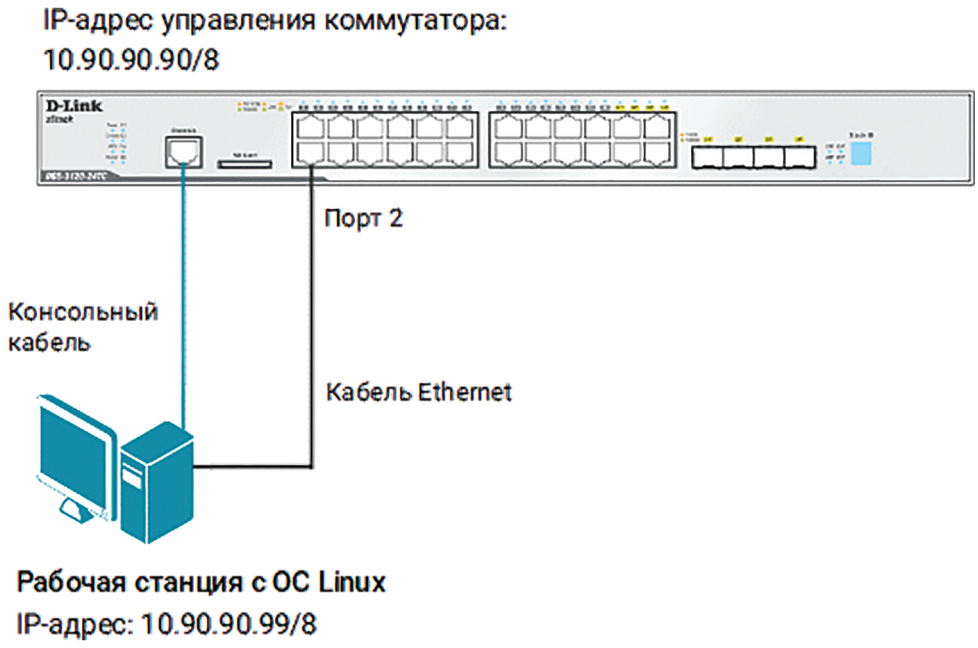

Рис. 17.1. Схема подключения

2. Запустите браузер, в адресной строке введите IP-адрес интерфейса управления коммутатора по умолчанию:

```
https://10.90.90.90
```

Примечание
Все браузеры считают самоподписанные сертификаты небезопасными и выдают ошибку с предупреждением, что соединение не защищено. В этом случае нажмите кнопку *Дополнительно → Добавить исключение → Подтвердите исключение безопасности*.

3. Остановите захват в Wireshark и проанализируйте захваченные пакеты. Зашифрован ли трафик, передаваемый между коммутатором и рабочей станцией?

_____

С помощью какого протокола установлено SSL-соединение?_____

Разверните пакет *Client Hello*. Какие алгоритмы шифрования поддерживает клиент?

_____

О каком алгоритме шифрования договорились сервер и клиент? _____

Лабораторная работа № 18. Изучение взаимодействия между клиентом и сервером DHCP

Dynamic Host Configuration Protocol (DHCP — протокол динамической конфигурации узла) — это сетевой протокол уровня приложений, позволяющий сетевым узлам автоматически получать IP-адреса и другие сетевые параметры, необходимые для работы в сети.

Основные компоненты DHCP:

- *Клиент DHCP* (DHCP client) — узел, использующий DHCP для получения конфигурационных параметров.
- *Сервер DHCP* (DHCP server) — узел, назначающий конфигурационные параметры клиентам DHCP.
- *Relay-агент DHCP* (DHCP Relay agent) — узел (маршрутизатор, коммутатор), который передает сообщения DHCP между клиентами и серверами, когда они находятся в разных подсетях.

Обычно DHCP-сервер не является выделенным компьютером, за исключением очень больших сетей. В большинстве случаев аппаратный сервер предоставляет сервисы DHCP наряду с выполнением других функций. Сервер не обязательно должен быть компьютером. Современные маршрутизаторы и коммутаторы L3 поддерживают функционал серверов DHCP.

Лабораторная работа № 19. Функционирование relay-агента DHCP

Сообщения DHCP передаются широковещательно. Чтобы клиент и сервер могли ими обмениваться, они должны находиться в одном широковещательном домене, т. е. в одной IP-сети или подсети. Это связано с тем, что маршрутизаторы не передают широковещательные пакеты на другие интерфейсы. Таким образом, если клиент и сервер DHCP находятся в разных сетях, для передачи сообщений между ними нужен посредник. Им является relay-агент DHCP.

Relay-агент DHCP — это любой узел, маршрутизатор или коммутатор, который настроен для передачи пакетов DHCP между клиентом и сервером, находящихся в разных сетях. Передача сообщений DHCP relay-агентом отличается от передачи IP-пакетов маршрутизатором. Маршрутизатор при передаче IP-пакета не изменяет в нем IP-адреса приемника и назначения. Relay-агент, получив сообщение DHCP, генерирует новое сообщение и отправляет его через соответствующий интерфейс.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Linux ..... 1 шт.
Рабочая станция с ОС Windows ..... 2 шт.
Коммутатор DGS-3120-24TC ..... 1 шт.
Кабель Ethernet ..... 3 шт.
Консольный кабель ..... 1 шт.

Используемое ПО для ОС Linux:

- Программа эмуляции терминала Minicom
- DHCP-сервер Isc-dhcp-server
- Анализатор трафика Wireshark

Цель работы: изучить настройку коммутатора в качестве relay-агента для перенаправления DHCP-сообщений между клиентом и сервером.

Настройка рабочей станции с ОС Linux

1. Подключите рабочую станцию ПК 1 к коммутатору, как показано на рис. 19.1. Запустите терминал. Настройте статический IP-адрес для сетевого интерфейса `enp0s3`:

```
$ sudo ifconfig enp0s3 192.168.1.1/24
```

2. Создайте маршрут по умолчанию:

```
$ sudo route add default gw 192.168.1.2
```

3. Посмотрите таблицу маршрутизации:

```
$ route
```

Какие изменения выполнил relay-агент? _____

_____

_____

_____

Примечание

DHCP-клиент, получивший предложение, широковещательно отправляет сообщение DHCPREQUEST с целью запроса предложенных конфигурационных параметров у выбранного сервера. Это сообщение получает relay-агент, который изменяет в нем адресную информацию в заголовках сетевого и канального уровня, а также добавляет свой IP-адрес в поле *Relay Agent IP address*. После всех изменений relay-агент отправляет одноадресное сообщение DHCPREQUEST серверу.

5. Выберите широковещательное сообщение DHCPACK, отправленное DHCP-сервером relay-агенту, и сравните его с одноадресным сообщением DHCPACK, которое relay-агент отправил рабочей станции ПК 2.

Какие изменения выполнил relay-агент? _____

_____

_____

_____

Примечание

Сервер, выбранный клиентом, отправляет ему одноадресное подтверждение DHCPACK, содержащее конфигурационные параметры, аналогичные ранее предложенным в сообщении DHCPOFFER. В сообщении DHCPACK в качестве MAC- и IP-адреса назначения указаны MAC- и IP-адрес соответствующего relay-агента. Прежде чем передать полученное сообщение клиенту, relay-агент выполняет в нем изменения, аналогичные изменениям, производимым с сообщением DHCPOFFER.

Лабораторная работа № 20. Настройка сети провайдера для подключения клиентов по IPoE

Рассмотрим пример настройки сети провайдера для подключения пользователей по технологии IPoE. Этот тип подключения удобен для пользователей — достаточно подключить маршрутизатор к сети провайдера с помощью Ethernet-кабеля. В настройках маршрутизатора по умолчанию уже установлен тип соединения *Динамический IPv4*. DHCP-сервер, настроенный в сети провайдера, автоматически назначит клиенту IP-адреса WAN-интерфейса, шлюза по умолчанию и DNS-серверов.

Как провайдер сможет контролировать доступ пользователей в сеть? Как правило, DHCP-сервер назначает IP-адреса случайным образом из

Лабораторная работа № 21. Настройка функции DHCP Local Relay

Из определения DHCP relay-агента следует, что это узел, который настроен для передачи пакетов DHCP между клиентом и сервером, находящихся в разных сетях. Relay-агент, помимо своего IP-адреса может добавлять в запрос клиента информацию опции 82. Предположим, что в пределах локальной сети или подсети администратору необходимо дифференцировать выдачу IP-адресов клиентам. Например, клиенту, подключенному к порту 6 коммутатора, всегда должен выдаваться строго определенный адрес, остальным клиентам — свободные адреса из какого-то диапазона. Данную задачу можно решить с помощью функции *DHCP Local Relay*, поддерживаемой коммутаторами D-Link. Она позволяет коммутатору добавлять опцию 82 в запросы клиентов, которые находятся с DHCP-сервером в одном широковещательном домене. При этом локальный relay-агент не изменяет IP- и MAC-адреса отправителя и получателя в DHCP-сообщении, а также не добавляет свой адрес в поле *Relay Agent IP address*. В DHCP-сообщение клиента будет автоматически добавляться опция 82. На основании информации из опции DHCP-сервер будет определять требуемые параметры, руководствуясь настроенной на нем политикой выдачи адресов. Опция 82 не будет удаляться локальным relay-агентом из ответов DHCP-сервера.

Оборудование на 1 рабочее место:

Рабочая станция с ОС Linux ..... 1 шт.
Рабочая станция с ОС Windows ..... 2 шт.
Коммутатор DGS-3120-24TC ..... 1 шт.
Кабель Ethernet ..... 3 шт.
Консольный кабель ..... 1 шт.

Используемое ПО для ОС Linux:

- Программа эмуляции терминала Minicom
- DHCP-сервер Isc-dhcp-server
- Анализатор трафика Wireshark

Цель работы: изучить функцию DHCP Local Relay.

Настройка рабочей станции с ОС Linux

1. Подключите рабочую станцию ПК 1 к коммутатору, как показано на рис. 21.1. Запустите терминал. Настройте статический IP-адрес для сетевого интерфейса `enp0s3`:

```
$ sudo ifconfig enp0s3 192.168.1.1/24
```

2. Запустите анализатор трафика Wireshark. Выберите интерфейс локальной сети `enp0s3` для захвата пакетов:

```
$ sudo wireshark
```

Лабораторная работа № 22.
Самостоятельная настройка сети и поиск неисправностей

Лабораторная работа предполагает самостоятельную настройку сети, которая показана на рис. 22.1.

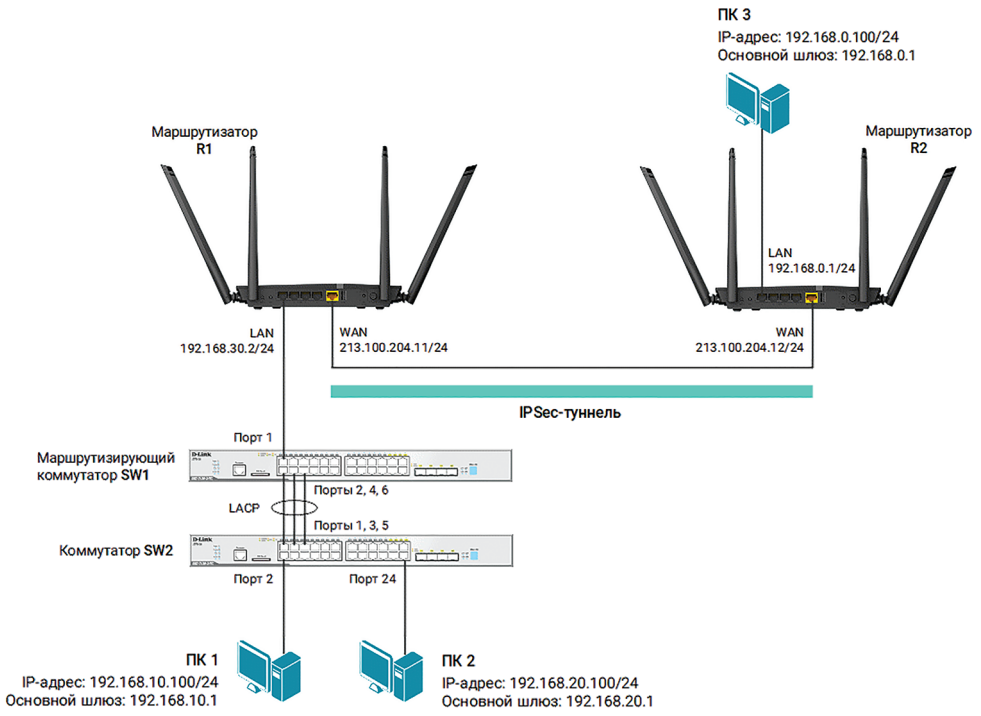

Рис. 22.1. Схема подключения

Порты и VLAN

Имя устройства	Порт	Имя VLAN	VID
SW1	1	default	1
	2, 4, 6	v10, v20	10, 20
SW2	1, 3, 5	v10, v20	10, 20
	2	v10	10
	24	v20	20

Приложение А. Инструкция по импорту и настройке образа виртуальной машины в VirtualBox

В виртуальной машине *DlinkLab_18.04LTS.ova* предустановлен пользователь:

Username: classroom

Password: classroom

1. Загрузите и установите VirtualBox — https://goo.gl/JBz4iB
2. Установите VirtualBox Extension Pack — https://goo.gl/JBz4iB
3. Загрузите образ DlinkLab_18.04LTS.ova — https://goo.gl/npW1Bm
4. Запустите VirtualBox и импортируйте образ DlinkLab_18.04LTS.ova. Выберите *Файл → Импорт конфигурации*. В открывшемся окне укажите путь к образу, затем нажмите кнопку *Далее*. Параметры импорта оставьте без изменений, нажмите кнопку *Импорт* (рис. А.1).

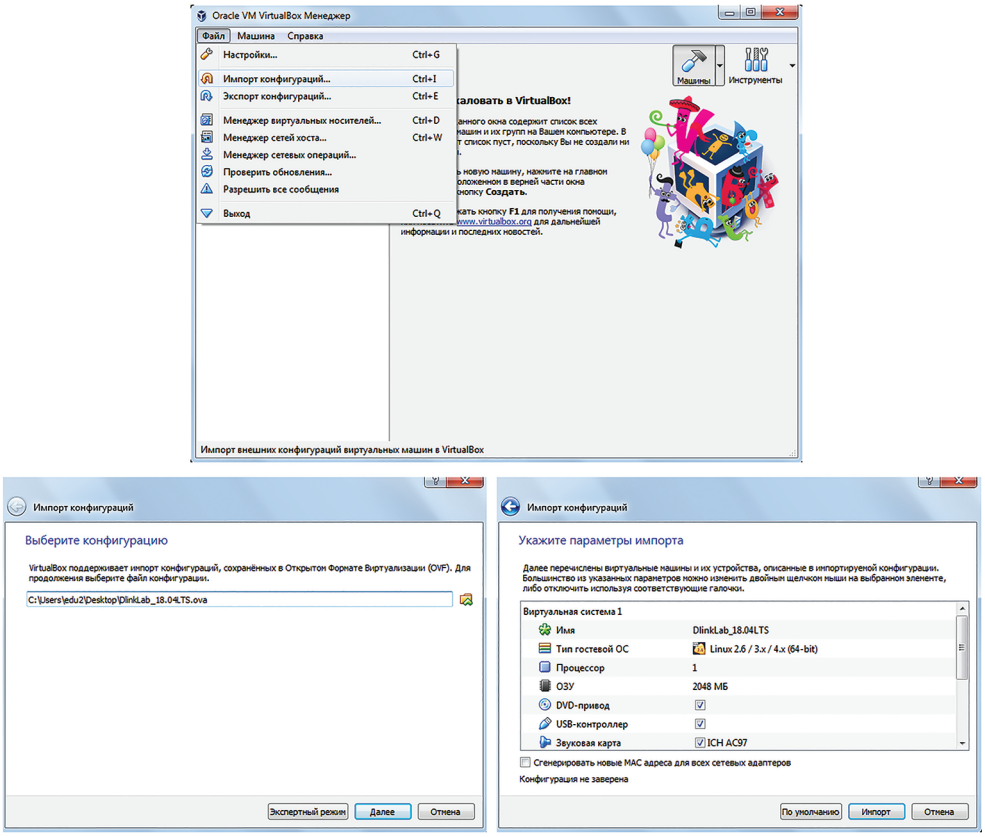

Рис. А.1. Импорт образа виртуальной машины

ЛИТЕРАТУРА

1. RFC 675. Specification of Internet Transmission Control Program. December 1974.
2. RFC 793. Transmission Control Protocol. September 1981.
3. RFC 1180. A TCP/IP Tutorial. January 1991.
4. Charles M. Kozierok. The TCP/IP Guide. http://www.tcpipguide.com
5. RFC 1661. The Point-to-Point Protocol (PPP). July 1994.
6. RFC 1332. The PPP Internet Protocol Control Protocol (IPCP). May 1992.
7. RFC 1994. PPP Challenge Handshake Authentication Protocol (CHAP). August 1996.
8. RFC 2433. Microsoft PPP CHAP Extensions. October 1998.
9. RFC 2759. Microsoft PPP CHAP Extensions, Version 2. January 2000.
10. RFC 3078. Microsoft Point-To-Point Encryption (MPPE) Protocol. March 2001.
11. Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны. М: ИНТУИТ, 2014.
12. Лапонина О.Р. Основы сетевой безопасности. Часть 2. Технологии туннелирования. М: ИНТУИТ, 2014.
13. Chris Le, Sanjeev Mervana. Design and Implementation of DSL-Based Access Solutions. Cisco Press, 2001.
14. RFC 2516. A Method for Transmitting PPP Over Ethernet (PPPoE). February 1999.
15. RFC 2364. PPP Over AAL5. July 1998.
16. RFC 2637. Point-to-Point Tunneling Protocol (PPTP). July 1999
17. RFC 2661. Layer Two Tunneling Protocol "L2TP". August 1999
18. RFC 791. Internet Protocol. September 1981
19. RFC 2474. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. December 1998.
20. Смирнова Е.В., Пролетарский А.В., Ромашкина Е.А., Суровов А.М., Федотов Р.А. Технологии коммутации и маршрутизации в локальных компьютерных сетях. М: Издательство МГТУ им. Н.Э. Баумана, 2013.
21. RFC 1517. Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR). September 1993.
22. RFC 1518. An Architecture for IP Address Allocation with CIDR. September 1993.
23. RFC 1519. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. September 1993.
24. RFC 3022. Traditional IP Network Address Translator (Traditional NAT). January 2001.
25. RFC 2640. Internet Protocol, Version 6 (IPv6) Specification. December 1998.
26. RFC 4291. IP Version 6 Addressing Architecture. February 2006.
27. RFC 3587. IPv6 Global Unicast Address Format. August 2003.
28. Sheila Frankel, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey, Steven R. Sharma. Guide to IPsec VPNs. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-77, 2005.
29. RFC 4301. Security Architecture for the Internet Protocol. December 2005.
30. RFC 4302. IP Authentication Header. December 2005.
31. RFC 4303. IP Encapsulating Security Payload (ESP). December 2005.
32. RFC 2408. Internet Security Association and Key Management Protocol (ISAKMP). November 1998.
33. RFC 2409. The Internet Key Exchange (IKE). November 1998.

ГЛОССАРИЙ

A

ACL (англ. Access Control List). Списки управления доступом. Списки управления доступом являются средством фильтрации потоков данных на аппаратном уровне. С помощью ACL можно ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS путем классификации трафика и переопределения его приоритета.

ADSL (англ. Asymmetric Digital Subscriber Loop). Асимметричный цифровой абонентский контур. Технология семейства xDSL, обеспечивающая передачу данных через тот же локальный телефонный контур, по которому предоставляются услуги обычной аналоговой телефонии.

AES (англ. Advanced Encryption Standard). Симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). Инициатива в разработке алгоритма AES принадлежит Национальному институту стандартов и технологий (NIST) США. В результате длительного процесса оценки предложенных алгоритмов в качестве алгоритма AES был выбран алгоритм Rijndael. Алгоритм AES определен в FIPS PUB 197-2001. Он был адаптирован под требования многих протоколов, включая протокол CCMP (CTR with CBC-MAC Protocol) для сетей 802.11.

AH (англ. Authentication Header). Один из протоколов IPSec, который обеспечивает целостность протоколов, расположенных выше в стеке протоколов, и целостность отдельных полей IP-заголовка, которые не изменяются при пересылке от отправителя к получателю, дополнительно может обеспечиваться анти-replay сервис, т. е. целостность некоторой последовательности дейтаграмм. В IPSecv3 реализация данного протокола не является обязательной.

ARP (англ. Address Resolution Protocol). Протокол разрешения адресов. Протокол, используемый для динамического преобразования IP-адресов в физические (аппаратные) MAC-адреса устройств локальной сети TCP/IP. В общем случае ARP требует передачи широковещательного сообщения всем узлам, на которое отвечает узел с соответствующим запросу IP-адресом.

Asymmetric chipper. Асимметричное шифрование. Криптосистема, в которой шифрование и расшифровывание выполняются с использованием двух разных ключей, один из которых называется открытым, а другой — закрытым. Важным свойством этой системы является то, что, зная открытый ключ, вычислительно невозможно определить закрытый ключ. Асимметричные криптосистемы могут использоваться для шифрования, подписи, а также для обмена ключа.

Authentication. Аутентификация. Сервис безопасности, который обеспечивает подтверждение того, что информация получена от законного источника и получатель является требуемым.

Учебное издание

Компьютерные системы и сети

Смирнова Елена Викторовна
Пролетарский Андрей Викторович
Ромашкина Екатерина Александровна

Технологии TCP/IP в современных компьютерных сетях

Оригинал-макет подготовлен
в Издательстве МГТУ им. Н.Э. Баумана.

В оформлении использованы шрифты
Студии Артемия Лебедева.

Подписано в печать 23.05.2019. Формат 70×100/16.
Усл. печ. л. 52,0. Тираж 550 экз. Заказ № 463.

Издательство МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5., стр.1.
press@bmstu.ru www.baumanpress.ru