Глава 1. Основные принципы

В начале этой главы мы обсудили, как осуществляется обмен информацией во взаимосвязанном мире. Мы объяснили, что такое сеть и кому принадлежит Интернет, что такое данные и как они передаются по сети. Скорость, с которой данные передаются по сети, измеряется в пропускной способности (bandwidth) и производительности (throughput).

Все компьютеры, подключенные к сети и непосредственно участвующие в обмене данными, считаются хостами. Сетевая инфраструктура включает в себя три категории аппаратных компонентов:

- промежуточные устройства;
- оконечные устройства;
- сетевая среда передачи данных.

В небольших корпоративных и домашних сетях многие компьютеры работают и как серверы, и как клиенты. Такие сети называются одноранговыми. Каждое устройство, отправляющее сообщения через Интернет, должно иметь IP-адрес, идентифицирующий это устройство для других устройств в сети. Команда **ping** позволяет сетевому администратору проверить сквозное соединение между IP-адресом источника сообщения и IP-адресом получателя. Команда **traceroute** позволяет сетевому администратору выполнить трассировку маршрута сообщения от источника к получателю. Каждая отдельная сеть, по которой проходит сообщение, называется переходом. Команда traceroute отображает каждый переход на пути сообщения и время, которое требуется сообщению, чтобы достичь этой сети и вернуться обратно.

Глава 2. Сети в нашей повседневной жизни

В начале этой главы мы обсудили, что означает «быть на связи». В главе описаны различные типы сетей, включая сети сотовой связи, GPS, Wi-Fi, Bluetooth и NFC. Рассмотрены четыре основные категории компонентов сети: хосты, периферийные устройства, сетевые устройства и сетевая среда передачи данных. Чтобы устройство смогло обмениваться данными по сети, необходимо правильно настроить три элемента конфигурации IP:

• IP-адрес идентифицирует хост в сети;

• маска подсети идентифицирует сеть, к которой подключен хост;

• основной шлюз идентифицирует сетевое устройство, через которое хост подключается к Интернету или другой удаленной сети.

В данной главе подробно описано, как отслеживать все эти устройства, где они располагаются в сети и как подключены. Рассмотрены физическая и логическая топологии и значки, используемые в этих представлениях сети.

Наконец, мы обсудили кабели и среду передачи данных. Используются три типа сред, связывающих устройства и обеспечивающих путь, по которому передаются данные:

• медные жилы в кабелях;

• стеклянное или пластиковое волокно (волоконно-оптический кабель);

• беспроводная передача.

Наиболее распространенные типы кабелей — витая пара, коаксиальный и оптоволоконный. Четыре главных критерия для выбора сетевой среды передачи данных:

• расстояние, на которое среда способна передать сигнал;

• условия работы среды передачи данных;

• объем и необходимая скорость передачи данных;

• стоимость средств передачи данных и их установки.

Некоторые типы кабелей Ethernet, такие как неэкранированная витая пара (UTP) и коаксиальный кабель, более восприимчивы к ЭМП и РЧП. Экранированные витые пары менее подвержены воздействию ЭМП и РЧП. Волоконно-оптические кабели невосприимчивы к ЭМП и РЧП. У каждого типа кабеля есть свои достоинства и недостатки. Выбор оптимального типа кабеля зависит от требований конкретной сети.

Организация TIA/EIA определила две различных схемы проводки, которые называются T568A и T568B. Каждая предусматривает схему расположения выводов, или порядок подключения проводов на конце кабеля. Когда два устройства напрямую соединены Ethernet-кабелем UTP, важно, чтобы выводы для передачи и приема на каждом конце кабеля были расположены в обратном порядке. Одно устройство отправляет данные по определенному набору проводов, а устройство на другом конце кабеля по этим проводам принимает данные. Два устройства, использующие разные провода для приема и передачи, называются разнородными устройствами. Для обмена данными между ними нужен прямой кабель. Прямые кабели имеют одинаковые схемы распределения цветов на обоих концах.

Глава 3. Передача данных по локальной сети

В начале этой главы мы обсудили принципы связи по сети. У всех методов обмена данными есть три общих элемента:

- источник сообщения (отправитель);
- назначение (получатель);
- среда передачи (канал).

Сетевые протоколы определяют многие аспекты передачи информации по локальной сети, включая формат, размер и шаблоны сообщений, синхронизацию и кодирование. Стандарты сети и Интернета гарантируют, что один и тот же набор правил или протоколов одинаково реализован на всех устройствах, подключенных к сети. Многоуровневая модель описывает взаимодействие протоколов внутри каждого уровня, а также взаимодействие с верхними и нижними уровнями. Модель OSI используется для проектирования сетей передачи данных, технических требований к операциям, а также для поиска и устранения неполадок. TCP/IP — протокольная модель, поскольку в ней описываются функции, которые выполняются на каждом уровне протоколов, входящих в семейство протоколов TCP/IP.

Функции, которые выполняются на межсетевом уровне в модели TCP/IP, аналогичны функциям сетевого уровня в модели OSI. Функции транспортного уровня одинаковы в обеих моделях. Однако уровень сетевого доступа и уровень приложений модели TCP/IP разделены в модели OSI на дополнительные уровни, чтобы определить различные функции, которые должны выполняться на этих уровнях. Протоколы Ethernet определяют формат данных и способы их передачи по проводной сети. В стандартах Ethernet прописаны протоколы, использующиеся на уровнях 1 и 2 модели OSI. В процессе изготовления всем сетевым интерфейсам Ethernet даются физические адреса. Этот адрес называется MAC-адресом (Media Access Control — управление доступом к среде передачи данных). MAC-адрес идентифицирует каждый исходный и каждый конечный хосты в сети.

Для инкапсуляции каждого сообщения компьютера перед отправкой по сети используется особый формат, который называется кадром. В кадре указаны адреса исходного и конечного хостов. В иерархической архитектуре необходима схема логической адресации, которая позволяет определить местоположение хоста. Наиболее распространенная схема адресации для Интернета — протокол

IPv4. IPv6 — это протокол сетевого уровня, который в настоящее время реализуется в качестве замены IPv4. IP-адреса состоят из двух частей: одна идентифицирует локальную сеть, другая — отдельный хост. Для передачи данных по иерархической сети компьютеру требуются и физический MAC-адрес, и логический IP-адрес.

Управление IP-трафиком основано на характеристиках и устройствах, связанных с каждым из трех уровней иерархической модели проектирования сетей: доступа, распределения и ядра. Коммутатор Ethernet используется на уровне доступа. Когда хост отправляет сообщение другому хосту, подключенному к тому же коммутатору, коммутатор принимает и декодирует кадры, считывая физический (MAC) адрес сообщения. Когда хост отправляет широковещательное сообщение, коммутаторы пересылают его каждому подключенному хосту в той же локальной сети. Для определения MAC-адреса любого хоста, находящегося в той же локальной сети, хост-отправитель может использовать протокол IPv4, называемый протоколом разрешения адресов (ARP). IPv6 использует аналогичный метод, называемый поиском соседей. Уровень распределения связывает эти независимые локальные сети и управляет трафиком между ними. Наружу передается только трафик, направленный в другие сети. Сетевые устройства, составляющие уровень распределения, предназначены для соединения сетей, а не отдельных хостов. Отдельные хосты подключаются к сети с помощью устройств уровня доступа, таких как коммутаторы. Устройства уровня доступа связаны друг с другом посредством устройства уровня распределения, такого как маршрутизатор. Маршрутизатор — это сетевое устройство, связывающее несколько IP-сетей уровня 3. На сетевом уровне распределения маршрутизаторы перенаправляют трафик и выполняют другие функции, важные для эффективной работы сети.

Каждый порт (интерфейс) маршрутизатора связан со своей локальной сетью. У каждого маршрутизатора есть таблица локально подключенных сетей и их интерфейсов. Кроме того, в этих таблицах маршрутизации бывает информация о маршрутах, или путях для подключения к другим локально подключенным удаленным сетям. Термин «локальная сеть» (LAN) относится к группе взаимосвязанных локальных сетей, которыми управляет один и тот же администратор. Хотя LAN можно назвать и одну домашнюю или офисную локальную сеть, само определение расширилось и теперь предполагает наличие взаимосвязанных сетей, которые состоят из нескольких сотен хостов, установленных в разных зданиях. Если все хосты находятся в одной сети, они могут обмениваться данными. Дело в том, что они образуют один домен широковещательной рассылки, и хосты находят друг друга с использованием протокола ARP.

Обзор главы

В начале этой главы мы обсудили адресацию IPv4 и маски подсети. Хосту требуется адрес IPv4, чтобы участвовать в передаче данных через Интернет. У каждого пакета, передаваемого через Интернет, есть адрес IPv4 источника и назначения. Адрес IPv4 представляет собой серию из 32 двоичных битов (единиц и нулей). 32 бита группируются по четыре 8-битных байта в так называемые октеты. Логический 32-битный адрес IPv4 имеет иерархическую структуру и состоит из двух частей. Первая идентифицирует сеть, вторая - хост в сети. Обе части адреса IPv4 являются обязательными. При настройке хоста ему присваивается не только адрес IPv4, но и маска подсети. Аналогично адресу IPv4, длина маски подсети составляет 32 бита. Маска подсети показывает, какая часть адреса IPv4 относится к сети, а какая — к хосту.

Далее были рассмотрены различные типы адресов IPv4. В 1981 году адреса IPv4 Интернета назначались при помощи адресации с использованием классов. Эти диапазоны частных адресов состоят из одной сети класса A, 16 сетей класса B и 256 сетей класса C. Сегодня используется система, которая называется бесклассовой адресацией. Официальное название — бесклассовая междоменная маршрутизация (Classless Inter-Domain Routing, CIDR; произносится как «сайдр»). С помощью адресов IPv4 хосты могут обмениваться данными в режиме «один к одному» (одноадресная передача), «один ко многим» (многоадресная рассылка) или «один ко всем» (широковещательная рассылка).

В следующем разделе данной главы описан процесс получения адресов IPv4. Используя статический адрес, сетевой администратор может вручную настраивать сетевые данные хоста. Как минимум это будет адрес IPv4, маска подсети и основной шлюз для хоста. Вместо того чтобы сетевой администратор назначал адрес IPv4 каждой рабочей станции, проще использовать автоматическое

назначение адресов IPv4. Для этого используется протокол под названием Dynamic Host Configuration Protocol (DHCP). Когда вы подключаетесь к беспроводной сети в аэропорту или магазине, доступ в Интернет обеспечивает DHCP.

В следующем разделе данной главы обсуждалось управление адресами IPv4. Маршрутизатор создает шлюз, через который хосты одной сети могут обмениваться данными с хостами других сетей. Каждый интерфейс маршрутизатора подключается к отдельной сети. Адрес IPv4, назначенный интерфейсу, идентифицирует напрямую подключенную к нему локальную сеть. Каждый хост в сети обязательно использует маршрутизатор в качестве шлюза в другие сети. Процесс преобразования частных адресов в маршрутизируемые в Интернете адреса называется преобразованием сетевых адресов (NAT). NAT обеспечивает преобразование частного (локального) адреса IPv4 источника в публичный (глобальный) адрес. Входящие пакеты проходят обратный процесс.

В последнем разделе данной главы рассматривается адресация IPv6. Длина адреса IPv4 составляет 32 бита (4 байта). Длина адреса IPv6 увеличена до 128 бит (16 байт). При использовании IPv6 преобразование NAT не требуется, так как каждое устройство может иметь собственный, глобально маршрутизируемый адрес. Автоматическая настройка IPv6 упрощает администрирование адресов. Кроме того, разработчики IPv6 внесли усовершенствования в IP и связанные с ним протоколы, такие как ICMPv6. Были разработаны методы для сжатия адреса IPv6 в более удобный формат.

Глава 5. Предоставление сетевых сервисов

В начале этой главы мы обсудили, как взаимодействуют клиенты и серверы. Под термином «сервер» понимается хостовая машина, на которой выполняется прикладное программное обеспечение, предоставляющее информацию или службы для других хостов, подключенных к сети. Ключевой особенностью клиент-серверных систем является то, что клиент отправляет запрос серверу, а сервер в ответ выполняет функцию, например отправляет клиенту запрошенный документ. При обращении к веб-серверу для загрузки веб-страницы используется универсальный указатель ресурса (URL) для поиска сервера и определенного ресурса. Некоторые протоколы, используемые для сервисов Интернета:

- система доменных имен (Domain Name System, DNS);
- протокол Secure Shell (SSH);
- протокол простой передачи электронной почты (SMTP);
- почтовый протокол (POP);
- протокол доступа к сообщениям в Интернете (IMAP);
- протокол динамической конфигурации хоста сети (DHCP);
- веб-сервер;
- протокол передачи файлов (FTP).

В следующем разделе данной главы рассматриваются интернет-протоколы в действии. Далее перечислены различные протоколы, необходимые для обеспечения функций веб-страниц на четырех уровнях модели TCP/IP:

- **протокол уровня приложений** — протокол передачи гипертекста (HTTP);
- **протокол транспортного уровня** — протокол управления передачей (TCP) и протокол пользовательских датаграмм (UDP);
- **протокол межсетевого уровня** — интернет-протокол (IP);

- **уровень сетевого доступа** — конкретный протокол уровня сетевого доступа зависит от типа среды и способов передачи данных в физической сети.

TCP отслеживает количество сегментов, отправленных на тот или иной хост тем или иным приложением. Если отправитель не получает подтверждение в течение определенного периода времени, он предполагает, что эти сегменты потеряны, и заново передает их. Протокол UDP выполняет негарантированную доставку данных и не запрашивает подтверждения от получателя. При доставке сообщения по протоколу TCP или UDP запрашиваемые протоколы и службы распознаются по номеру порта. Порт — это числовой идентификатор в каждом сегменте, который позволяет отслеживать конкретные сеансы связи между клиентом и сервером.

В последнем разделе данной главы подробно рассмотрены прикладные протоколы и сервисы. DNS-имена регистрируются и организуются в Интернете в пределах определенных доменов. К числу наиболее популярных доменов сети Интернет относятся .com, .edu и .net. После получения IP-адреса веб-сервера веб-клиентом обозреватель на стороне клиента инициирует запрос веб-служб по этому IP-адресу и направит его через порт 80. Этот запрос отправляется на сервер по протоколу передачи гипертекстовых файлов (HTTP). При помощи HTML-кода браузер определяет формат веб-страницы и требуемые рисунки и шрифты. Протокол HTTP и стандарты HTML обеспечивают беспрепятственное взаимодействие серверов и клиентов от разных поставщиков.

Протокол передачи файлов (FTP) обеспечивает простой обмен файлами между компьютерами. Чтобы начать сеанс FTP, серверу отправляются управляющие запросы на подключение с использованием порта назначения TCP 21. Когда сеанс открыт, сервер изменяет порт TCP на порт 20 для передачи файлов данных. Когда появились сети, потребовался способ получать удаленный доступ к компьютерам, как если бы это были напрямую подключенные терминалы. Для решения этой задачи был разработан протокол Telnet. В сеансах Telnet все данные передаются по сети в виде открытого текста. Это означает, что данные могут быть перехвачены и легко прочитаны. В случае высоких требований к безопасности следует использовать протокол SSH для защищенного доступа к серверу. Протокол SSH обеспечивает защищенный удаленный вход в систему и другие защищенные сетевые сервисы.

Электронная почта — одно из наиболее популярных клиент-серверных приложений в сети Интернет. Каждый сервер электронной почты отвечает за прием и хранение почты пользователей в индивидуальных почтовых ящиках, созданных на сервере электронной почты. Прикладные протоколы, используемые для работы с электронной почтой, включают SMTP, POP3 и IMAP4. Система мгновенного обмена сообщениями (IM) позволяет пользователям общаться через Интернет в режиме реального времени. Для доступа к большинству сервисов мгновенного обмена сообщениями используется веб-клиент, встроенный в социальную сеть или сайт обмена информацией. IP-телефония использует технологию передачи голоса по протоколу IP (VoIP), которая преобразует аналоговые голосовые сигналы в цифровые данные.

Глава 6. Создание домашней сети

В начале этой главы мы обсудили, что собой представляет домашняя сеть. Домашняя сеть — это небольшая локальная сеть с устройствами, которые для обмена информацией обычно подключаются к интегрированному маршрутизатору и друг к другу. Маршрутизатор подключен к интернету. Как правило, домашний маршрутизатор обеспечивает и проводную, и беспроводную связь. Маршрутизаторы для домашних сетей и малых предприятий обычно оснащены Ethernet-портами и портом Интернета. Кроме проводных портов, многие домашние маршрутизаторы оснащены антенной беспроводной связи и встроенной точкой беспроводного доступа. В беспроводных технологиях для обмена информацией между устройствами используются электромагнитные волны. В спектр электромагнитных волн входят полосы частот радио- и телевизионных программ, видимый свет, рентгеновское излучение и гамма-излучение. В домашних сетях чаще всего используются технологии беспроводного доступа в нелицензируемых частотных диапазонах 2,4 ГГц и 5 ГГц. Наиболее часто реализуемый протокол проводной связи — Ethernet. Ethernet использует набор протоколов, которые позволяют сетевым устройствам взаимодействовать через подключение к проводной локальной сети.

В следующем разделе данной главы рассмотрены принципы работы Wi-Fi. Стандарты беспроводной связи для локальных сетей используют полосы частот 2,4 ГГц и 5 ГГц. В совокупности эти технологии

называются Wi-Fi. На беспроводных маршрутизаторах, использующих стандарты 802.11, нужно настроить несколько параметров. Среди них следующее:

- Network mode (Сетевой режим);
- Сетевое имя (Network Name, SSID);
- Standard Channel (стандартный канал);
- Широковещательная рассылка SSID.

Беспроводные устройства, работающие в одном и том же частотном диапазоне, создают помехи в сети Wi-Fi. Каналы создаются путем деления доступного радиочастотного спектра. Несколько точек доступа могут работать в непосредственной близости одна к другой, если они используют разные каналы связи. Чтобы избежать коллизий, технология беспроводной связи использует метод доступа, который называется множественным доступом с контролем несущей и предотвращением коллизий (CSMA/CA). CSMA/CA резервирует канал для определенного сеанса связи между устройствами. Если канал зарезервирован, никакое другое устройство не сможет передавать по нему данные, что позволит избежать возможных коллизий.

В следующем разделе данной главы описан процесс настройки беспроводной сети. Многие беспроводные маршрутизаторы, предназначенные для домашней сети, оснащены программой автоматической настройки, с помощью которой можно задать базовые параметры. Если включено вещание SSID, то имя SSID будет видимым для всех беспроводных клиентов в вашем диапазоне сигналов. Беспроводная сеть в смешанном режиме зависит от модели маршрутизатора, но может поддерживать комбинацию стандартов связи 802.11a, 802.11b, 802.11g, 802.11n и 802.11ac. На беспроводных маршрутизаторах применяются методы аутентификации, которые требуют ввести пароль или парольную фразу для подключения к сети с определенным SSID. Комбинация SSID без возможности широковещательной рассылки и парольной фразы гарантирует, что для доступа к вашей сети гостям потребуются данные от вас.

В следующем разделе данной главы обсуждаются сервисы интернет-провайдера. Интернет-провайдер обеспечивает связь между домашней сетью и Интернетом. Интернет-провайдером может быть местный поставщик услуг кабельного ТВ, поставщик услуг стационарной телефонии, оператор сотовой сети, обслуживающий ваш смартфон, или независимый поставщик, который арендует полосу пропускания на базе физической сетевой инфраструктуры другой компании. Два наиболее распространенных способа — это кабельное и DSL-подключение.

В следующем разделе данной главы рассматриваются вопросы безопасности домашней сети. Хакер может получить доступ к вашей сети из любой точки в зоне покрытия беспроводной связи. Получив доступ к вашей сети, хакер сможет бесплатно пользоваться интернет-сервисами, а также проникать на компьютеры в сети для повреждения файлов или кражи личной и конфиденциальной информации. Для устранения подобных уязвимостей в беспроводной сети требуются специальные меры безопасности и комбинация нескольких способов защиты беспроводной локальной сети. При использовании фильтрации по MAC-адресам решение о допуске конкретного устройства в беспроводную сеть принимается на основании MAC-адреса. Только тем устройствам, чьи MAC-адреса записаны в базу данных маршрутизатора, будет разрешено подключиться. Аутентификация — это предоставление разрешения на вход в сеть по результатам проверки подлинности набора учетных данных. Её цель — выяснить, является ли устройство, пытающееся установить соединение, доверенным устройством. Наиболее распространена аутентификация по имени пользователя и паролю. В беспроводной среде аутентификация позволяет выполнить проверку подлинности подключенного хоста, но процесс проверки выполняется несколько по-другому. Существует три типа методов беспроводной аутентификации: открытая аутентификация, Pre-Shared Key (PSK) и EAP. WPA2 использует также ключи шифрования от 64 до 256 бит. При этом WPA2, в отличие от WEP, генерирует новые динамические ключи каждый раз, когда клиент устанавливает соединение с точкой доступа.

В последнем разделе этой главы идет речь о мобильных устройствах в сети. Как и в случае других устройств с поддержкой Wi-Fi, важно принять меры безопасности при подключении мобильных устройств к сетям Wi-Fi. Никогда не передавайте информацию о логине и пароле, используя

незашифрованный текст (простой текст). При отправке конфиденциальных данных используйте VPN-соединение, когда это возможно. Включите функции безопасности в домашних сетях. В целях безопасности используйте шифрование WPA2.

Глава 7. Сетевая безопасность

В начале этой главы мы задали вопрос, угрожает ли атака среднестатистическому пользователю сети. Хакер, получивший доступ в сеть, становится источником четырех видов угроз: хищения информации, хищения персональных данных, потери данных или манипуляций с ними и прекращения обслуживания. Злоумышленники проникают в сеть извне, главным образом из Интернета или по беспроводным каналам. Внутренние угрозы возникают, когда некто получает санкционированный доступ к сети с помощью учетной записи пользователя или физический доступ к сетевому оборудованию. Социальная инженерия — это совокупность приемов, применяемых с целью заставить внутренних пользователей выполнить определенные действия или раскрыть конфиденциальную информацию обманным путем. Чаще всего для получения информации непосредственно у авторизованных пользователей хакеры применяют три метода: претекстинг, фишинг и вишинг. Другие типы атак, которые используют уязвимости компьютерного ПО: вирусы, интернет-черви и трояны. Их общим свойством является проникновение вредоносного ПО на хост. Вирус — это программа, которая распространяется, модифицируя другие программы или файлы. Интернет-червь аналогичен вирусу с тем отличием, что ему не требуется внедряться в существующую программу. Троян — программа, которая имитирует законную программу, но на самом деле служит инструментом атаки.

В следующем разделе рассмотрены различные методы совершения атак. Посредством DoS-атаки хакер создает лавинный трафик в системе или сети, чтобы помешать передаче нормального сетевого трафика, либо нарушает соединение между клиентом и сервером, чтобы блокировать доступ к сервису. Два распространенных вида DoS-атак: лавинная рассылка SYN-запросов и ping-запрос смерти. Цель DDoS-атаки — перенасыщение сетевых каналов бесполезными данными. Жертва DDoS-атаки обычно получает огромный поток трафика из сотен или тысяч источников атаки. В атаках методом грубой силы используется быстродействующий компьютер для подбора паролей или дешифровки. Злоумышленник активно перебирает большое число возможных вариантов для получения доступа или извлечения ключа шифрования. Многие угрозы связаны со сбором сведений о пользователях, которые в дальнейшем могут использоваться для рекламы, маркетинга и анализа. Источниками таких угроз являются шпионское ПО, отслеживание файлов cookie, рекламное ПО и всплывающие окна. Один из путей распространения спама — использование ботнета или бота. ПО бота может регистрировать нажатия клавиш, собирать пароли и финансовую информацию, перехватывать и анализировать пакеты, запускать DoS-атаки и распространять спам.

В следующем разделе данной главы рассказывается о том, как защитить сеть. Для обеспечения безопасности могут применяться как простые, недорогие способы, например регулярное обновление ПО, так и сложные реализации брандмауэров и систем обнаружения вторжений. Укрепление безопасности сети достигается, в частности, следующими способами: установкой исправлений и обновлений ПО, защитой от вирусов и шпионского ПО, блокированием спама и всплывающих окон и применением брандмауэров. Поддерживайте актуальное состояние программных приложений, устанавливая текущие исправления и обновления. Для обнаружения новых вирусов и предотвращения заражения компьютера антивирусное ПО использует известные сигнатуры вирусов. Антиспам защищает хосты, выявляя спам и принимая нужные меры, например помещая такие сообщения в папку нежелательной почты или удаляя их. Решения для обнаружения шпионских программ выявляют и удаляют шпионские приложения, а также предотвращают их установку в будущем. Многие приложения для обнаружения шпионских программ также находят и удаляют файлы cookie и рекламное ПО. Установив ПО для блокирования всплывающих окон, можно предотвратить появление всплывающих и фоновых окон. Многие веб-браузеры по умолчанию включают функцию блокирования всплывающих окон.

В последнем разделе данной главы рассказывается о том, как брандмауэры обеспечивают безопасность сетей. Брандмауэр предотвращает попадание нежелательного трафика в защищенные области сети. Обычно аппаратный брандмауэр пропускает в сеть два типа трафика: ответный трафик на запросы, отправленные из внутренней сети, и трафик на порты, которые намеренно оставлены открытыми. Переадресация (также перенаправление или проброс) портов (port forwarding) — это способ направления трафика между устройствами в различных сетях на основе правил.

Переключение портов позволяет маршрутизатору временно пересылать данные через входящие порты TCP и UDP к конкретному устройству.

Глава 8. Настройка устройств Cisco

В начале этой главы мы обсудили устройства Cisco для локальной сети. Коммутаторы Ethernet Cisco Catalyst серии 2960 подходят для сетей малого и среднего размера. Они предусматривают поддержку дополнительных портов для устройств с малым форм-фактором (SFP). Коммутатор оснащен консольным портом для управления устройствами. После запуска коммутатора начинается его самотестирование при включении питания (POST). В ходе POST проводится серия проверок функций коммутатора. Индикаторы мигают. Есть два способа подключить компьютер к сетевому устройству для настройки и мониторинга: внеполосное управление и внутриполосное управление. Во время загрузки устройство Cisco загружает в ОЗУ следующие два файла: файл образа IOS и файл загрузочной конфигурации.

Далее в главе рассмотрены устройства межсетевого взаимодействия. Как и компьютерам, маршрутизаторам требуются: операционная система (ОС), центральный процессор (CPU), оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ) и энергонезависимое оперативное запоминающее устройство (NVRAM). Маршрутизатор Cisco 1941 оснащен следующими разъемами: консольными портами, двумя интерфейсами локальной сети и разъемами для усовершенствованной интерфейсной платы для высокоскоростного WAN (EHWIC). Два наиболее распространенных способа доступа к интерфейсу командной строки на маршрутизаторе Cisco: консоль и SSH.

Следующий раздел данной главы содержит обзор Cisco IOS. Интерфейс командной строки (CLI) Cisco IOS — это текстовая программа, позволяющая вводить и исполнять команды Cisco IOS, и таким образом настраивать, отслеживать и обслуживать устройства Cisco. Режимы Cisco IOS используют иерархическую структуру и весьма похожи для коммутаторов и маршрутизаторов. В качестве меры безопасности программное обеспечение Cisco IOS отделяет доступ к средствам управления в следующих двух режимах команд: пользовательском режиме EXEC и привилегированном режиме EXEC. Чтобы настроить устройство, пользователь должен перейти в режим глобальной настройки. Режим глобальной конфигурации можно определить по командной строке с именем устройства, после которого следует (config)#, например Switch(config)#. Общий синтаксис команды — это команда, за которой следуют соответствующие ключевые слова и аргументы. Синтаксис обеспечивает шаблон или формат, который необходимо использовать при вводе команды. Полужирным шрифтом выделены команды и ключевые слова. Курсивом выделен аргумент, для которого пользователь определяет значение. Cisco IOS содержит контекстную справку и инструмент проверки синтаксиса команд. Команды и ключевые слова можно сократить до минимального количества символов, которые останутся уникальными.

В следующем разделе описаны команды show. С помощью команды show можно отобразить состояние практически любого процесса или функции маршрутизатора. Наиболее известные команды show:

• show running-config

• show interfaces

• show arp

• show ip route

• show protocols

• show version

В заключительном разделе данной главы рассказывается о том, как настроить сеть Cisco. Настройка коммутатора Cisco выполняется на заводе-изготовителе. Перед подключением к сети необходимо задать только основные параметры безопасности. Элементы, которые обычно настроены на коммутаторе локальной сети, включают имя хоста, информацию об IP-адресе управления, пароли и

описательную информацию. IP-адреса назначаются коммутаторам уровня 2, так что устройство может быть доступно через сеть для управления и настройки. Для обеспечения доступности маршрутизаторов необходимо настроить его внутриполосные интерфейсы. Маршрутизатор Cisco 1941 оснащен двумя интерфейсами Gigabit Ethernet и последовательной интерфейсной платой WAN (WIC), содержащей два интерфейса. Команда show ip interface brief применяется для проверки конфигурации интерфейса. Выходные данные показывают все интерфейсы, их адреса IPv4, а также их текущее состояние. Активные и действующие интерфейсы представлены значением «up» в столбцах «Status» и «Protocol».

И хотя вход в систему с несколькими различными паролями и парольными фразами неудобен, это необходимая мера предосторожности для защиты сетевой инфраструктуры от несанкционированного доступа. Установка пароля для доступа к консоли выполняется в режиме глобальной конфигурации. Указанные ниже команды предотвращают несанкционированный доступ к пользовательскому режиму с порта консоли. Перед настройкой протокола SSH на коммутаторе нужно настроить уникальное имя хоста и соответствующие параметры сетевого подключения. Для отображения используемой версии и конфигурации для протокола SSH на устройстве, который вы настроили в качестве сервера SSH, используйте команду show ip ssh. Адресом основного шлюза, как правило, является адрес интерфейса маршрутизатора, связанный с локальной сетью, в которой находится хост. IP-адрес хостового устройства и адрес интерфейса маршрутизатора должны находиться в одной сети. Чтобы настроить основной шлюз на коммутаторе, используйте команду глобального конфигурирования ip default-gateway. Настроенный IP-адрес — интерфейс маршрутизатора подключенного коммутатора.

Глава 9. Тестирование, поиск и устранение неполадок

В начале этой главы мы обсудили, что необходимо сделать, если ваша сеть не работает. Устранение проблем состоит в выявлении, локализации и исправлении возникающих проблем. Существует ряд структурированных методов поиска и устранения неполадок, в том числе «сверху вниз», «разделяй и властвуй» и «снизу вверх».

Далее в данной главе рассмотрены способы поиска и устранения неполадок в сетях. Есть множество служебных программ (обычно это команды CLI), которые помогают выявить неисправности в сети. Когда устройство не может получить IP-адрес или имеет неправильную настройку IP, оно не может обмениваться данными по сети, а также получить доступ к Интернету. На устройствах под управлением Windows можно вывести сведения об IP-конфигурации с помощью команды ipconfig в командной строке. Если в команде ping указан IP-адрес, на него по сети будет отправлен пакет эхо-запроса. Получив эхо-запрос, хост назначения возвращает пакет с откликом. Если источник получает отклик на эхо-запрос, наличие соединения подтверждается. Служебная программа tracert помогает установить, где пакеты могли быть потеряны или задержаны из-за узких мест или замедления трафика в сети.

Затем в данной главе было подробно рассмотрено, как выявлять и решать распространенные проблемы. При поиске и устранении неполадок в сети, в которой применяются и проводные, и беспроводные соединения, оптимальным чаще всего оказывается метод «разделяй и властвуй», позволяющий локализовать проблему на проводном или беспроводном участке. Погасшие светодиоды могут указывать на выход из строя устройства или порта либо на проблемы с кабелями. Если проводной клиент не может подключиться к беспроводному маршрутизатору, прежде всего необходимо проверить физическое подключение и кабельное соединение. Кабели — «нервная система» проводных сетей и наиболее частая причина их простоя. Если беспроводной клиент не может подключиться к точке доступа, могут иметь место проблемы с беспроводным каналом связи. В беспроводных сетях для передачи данных используются радиочастотные (РЧ) сигналы. Современные беспроводные сети включают в себя различные технологии, обеспечивающие безопасность передачи данных по беспроводной локальной сети: неправильная конфигурация любой из них может помешать обмену данными. Некоторые из параметров, которые чаще всего настраиваются неправильно: идентификатор SSID, аутентификация и шифрование. Если физическое соединение с проводным или беспроводным хостом исправно, следует проверить настройки IP со стороны клиента. Конфигурация IP существенным образом влияет на возможность подключения хоста к сети. Если хосты в проводной и беспроводной локальной сети могут подключиться к беспроводному маршрутизатору и к другим хостам в локальной сети, но не к Интернету, то проблема может быть в соединении между маршрутизатором и интернет-провайдером. Проверьте все настройки на маршрутизаторе, чтобы

убедиться, что никакие ограничения безопасности не могут быть причиной проблемы. Убедитесь в том, что локальные брандмауэры на клиентских устройствах не препятствуют функциональности сети.

Затем в данной главе обсуждались вопросы получения помощи и взаимодействия со службой поддержки заказчиков. Наиболее популярные источники помощи: документация, составленная ранее, сборники часто задаваемых вопросов (FAQ) в Интернете, советы коллег и других профессионалов в области сетей и источники в Интернете, включая форумы, статьи и блоги. Телефонная линия и служба поддержки заказчиков является первым местом, куда стоит обратиться конечному пользователю для получения помощи. Служба поддержки — это группа лиц, обладающих знаниями и инструментами, необходимыми, чтобы помочь диагностировать и исправить типичные проблемы. Когда специалисту службы поддержки 1-го уровня поступает звонок, начинается процесс сбора информации. Существуют также специальные системы для хранения и извлечения соответствующей информации. Крайне важно правильно собрать информацию на случай, если вызов будет передан специалисту 2-го уровня или потребуется выезд на объект.