

Урок 5 - Рекомендации по материалам сетевой академии Cisco

1. Базовые сведения о сетях

И Microsoft нет
необходимости
поддерживать TCP/IP.



Тейт
1994

Microsoft изобрела
новый протокол.
Мы называем его TCP/IP



Тейт
1995

Как вы уже догадались сегодня мы с вами, будем говорить о сетях, что это такое мы сейчас и попробуем разобраться ☺ На сегодняшний момент трудно переоценить важность сетей в современном мире, где изменения происходят настолько быстро что невозможно успеть все это осмыслить. Во многих компаниях одним из основных видов деятельности является работа в WWW и доступ к электронной почте. По оценкам специалистов на начало 2000г. В Internet работало более 300 миллионов пользователей, и этот показатель по прежнему растет экспоненциально.

Вопреки распространенному заблуждению, Internet – это не продукт Microsoft, появившийся в 1995 году. Прародителем Internet была сеть ARPANET, основанная в 1969г. Управлением по перспективным исследовательским программам при министерстве обороны США (Defense Advanced Research Project Agency, DARPA). Впоследствии ARPANET стала национальной магистралью сети NFSNET (National Science Foundation Network – сеть Национального научного фонда), которая связывала между собой большие ЭВМ машины и региональные сети США.

В конце 80-х сеть перестала быть научно – исследовательским проектом, переход на коммерческие рельсы занял около семи лет, сеть NFSNET была отключена в апреле 1994г. Сегодня основу глобальной сети составляет совокупность частных сетей, принадлежащих провайдером Internet.

Еще в середине 80-х сеть Internet состояла из первоначальных вычислительных центров ARPANET и группы университетов, в которых были установлены компьютеры DEC VAX с операционной системой семейства Berkeley UNIX. Университетские сети по большей части строились по технологии Ethernet и получали доступ в Internet по выделенной цифровой линии связи со скоростью 56 Kbit/s. Каждый сентябрь, когда студенты приступали к учебе, глобальная сеть испытывала существенные перегрузки. Ван Джейкобсон (Van Jacobson), научный сотрудник группы сетевых исследований при лаборатории Bell Labs при университете Лоренса, заинтересовался поведением существующих протоколов при повышенной нагрузке и нашел путь их оптимизации. Отсюда берут свое начало известные сегодня алгоритмы медленного старта, быстрой ретрансляции и быстрого восстановления.

Вступление в силу закона Мура (гласящего, что мощность вычислительных средств удваивается каждые 18 месяцев) и рыночный спрос существенно ускорили развитие глобальной сети. С конца 80-х когда были стандартизированы существующие на сегодняшний момент алгоритмы TCP, которые успешно функционируют уже десятки лет, и до сих пор живы и актуальны, можем только снять шляпу перед Бобом Каном (Bob Kahn), Винтом Церфом (Vint Cerf), Джоном Постелом (John Postel), Ван Джейкобсон (Van Jacobson) и другими людьми, которые стояли у истоков этого чуда.

Кто сегодня управляет Internet

Я думаю, вас интересует вопрос, кто же управляет Internet сейчас, так как разработка глобальной сети всегда осуществлялась на кооперативных и открытых началах. Сегодня, когда Internet важным фактором мировой экономики, многие обеспокоены тем, что руководство сетью сосредоточено в руках небольшой группы людей.

В процесс управления вовлечены следующие организации:

- ICANN (Internet Corporation for Assigned Names and Numbers – Организация по назначению имен и адресов в Internet) – именно про нее можно сказать, что она отвечает за работу глобальной сети (www.icann.org)
- IETF (Internet Engineering Task Force – проблемная группа проектирования сети) – эта организация отвечает за разработку и публикацию технических стандартов Internet, является открытым форумом, принять участие в котором может каждый желающий (www.ietf.org)
- ISOC (Internet Society – Общество Internet) – это членская организация которая объединяет в своих рядах пользователей Internet (www.isoc.org)

Среди перечисленных организаций наибольшая ответственность лежит на ICANN: она выступает в роли руководящего органа Internet. Исправляя ошибки прошлого и придумывая пути дальнейшего развития.

Сетевые стандарты и документация

Научно-техническая деятельность Сообщества пользователей Internet находит отражение в серии документов, известных как RFC (Requests For Comments – запросы на комментарии). Стандарты протоколов, предполагаемые технические изменения, а также информационные бюллетени в итоге находят свое отражение в документах RFC. Иногда они действительно имеют вид комментариев, но как правило выпускаются в виде пояснений к существующим методикам и технологиям.

Документы RFC имеют порядковые номера. На сегодняшний день их чуть более 3000. У них есть описательные названия (например Algorithm for Synchronizing Network Clocks – алгоритм синхронизации сетевых таймеров) но во избежание неоднозначности на документы RFC чаще всего ссылаются по номерам. Будучи опубликованными, документ RFC никогда не меняется. Изменения и дополнения выпускаются в виде нового документа со своим собственным номером. По соглашению, обновленные документы содержат всю информацию из предшествующих, которая остается актуальной, таким образом, происходит полная замена одного документа другим. Процесс публикации документов RFC, в свою очередь, описан в документе под названием Internet Official Protocol Standards (официальные стандарты протоколов Internet). В него также включены ссылки на большинство документов, содержащих описания протоколов. Поскольку эта информация часто меняется, данный документ повторно публикуется через каждые 100 номеров: если текущая версия имеет номер 2600, то следующей будет 2700 и т.д. Процесс публикации стандартов Internet описан в документе RFC2026. Другой полезный документ - RFC2555, 30 Years of RFCs C0 лет существования документов RFC). В нем рассмотрены культурные и технические аспекты публикации документов RFC.

Пусть вас не пугает обилие технических подробностей в документах RFC. В большинстве из них содержатся вводные описания и толкования, которые будут полезны системным администраторам. Некоторые документы специально написаны в виде обзора или общего введения. Чтение документов RFC — не самый простой способ разобраться в той или иной теме, но это авторитетный, лаконичный и бесплатный источник информации. Не все документы RFC написаны сухим техническим языком. Встречаются документы развлекательного содержания (некоторые опубликованы 1 -го апреля), среди которых нам особенно нравятся следующие:

- RFC1118 — The Hitchhikers Guide to the Internet (Руководство для путешественников по Internet автостопом);
- RFC 1149 — A Standard for the Transmission of IP Datagrams on Avian Carriers (Стандарт передачи дейтаграмм птичьей почтой);

- RFC2324 — Hyper Text Coffee Pot Control Protocol (HTCPCP/LO) (Гипертекстовый протокол управления кофеварками);
- RFC2795 — The Infinite Monkey Protocol Suite (IMPS) (Семейство протоколов для управления бесконечным числом обезьян).

Помимо последовательных номеров документам RFC могут назначаться номера серий FYI (For Your Information — к вашему сведению), BCP (Best Current Practice — лучший существующий подход) и STD (Standard — стандарт). Перечисленные серии являются подмножествами серии RFC, группирующими документы по важности или назначению. Документы FYI — это вводные или информационные материалы, предназначенные для широкой аудитории. Как правило, именно с них лучше всего начинать знакомство с исследуемой темой. Документы STD содержат описания протоколов Internet, которые прошли процедуру проверки и тестирования в IETF и были формально приняты в качестве стандартов. Документы BCP описывают рекомендуемые процедуры для администраторов Internet-серверов; с точки зрения системных администраторов, это наиболее ценные документы в серии RFC. Нумерация документов в рамках серий RFC, FYI, STD и BCP ведется раздельно, поэтому один документ может иметь несколько номеров. Например, документ RFC 1635, How to Use Anonymous FTP (как использовать анонимный протокол FTP) также известен как FYI0024.

Документы RFC доступны из самых разных источников. Список поддерживаемых зеркальных RFC-серверов можно получить на Web-узле www.rfceditor.org, который является центром сбора информации по документам RFC.

2. Основные принципы создания сетей

А теперь давайте перейдем непосредственно к материалам Cisco Network Academy и узнаем о сетях и принципах их организации более подробно. Начнем мы с вами с «**Основных сведений о сетях**» Глава 8.

В данной главе вы рассмотрите различные типы сетевых топологий, протоколов, логических моделей и аппаратного обеспечения, необходимые для создания сетей. А также узнаете об основных настройках, устранение неполадок и профилактическое обслуживание. Кроме того особое внимание будет уделено сетевому программному обеспечению, способами связи и взаимосвязями различных компонентов оборудования.

8.1 Объяснение принципов создания сетей

Компьютеры могут быть связаны в сети для коллективного использования данных и ресурсов. Сеть может быть очень простой и представлять собой два компьютера, соединенные одним кабелем, или сложной, в состав которой входят сотни компьютеров, подключенные к устройствам, которые регулируют поток информации. В состав сетей данных могут входить компьютеры общего назначения, такие как ПК и серверы, а также устройства с более специфическими функциями, такие как принтеры, телефоны, телевизоры и игровые приставки.

И по завершению данного раздела вы должны понять самое важное,

- Что такое компьютерная сеть.
- Основные преимущества организации сетей.

8.1.1 Определение компьютерных сетей

Компьютерная сеть, что это такое и для каких целей она используется, а также чем между собой они отличаются, и какие основные типы классификаций сетей используется.

8.1.2 Объяснение преимуществ организации сетей

Мы с вами знаем или догадываемся, что к преимуществам сетевых компьютеров и других устройств относится их низкая стоимость и высокая производительность. С помощью сетей можно совместно использовать ресурсы, что приводит к уменьшению дублирования и порчи данных.

Первые компьютеры были автономными устройствами. Другими словами, каждый компьютер работал отдельно, независимо от других. Очень скоро стала очевидной низкая эффективность такого подхода. Необходимо было найти решение, которое бы удовлетворяло трем перечисленным ниже требованиям, а именно:

- **устраняло дублирование оборудования и ресурсов;**
- **обеспечивало эффективный обмен данными между устройствами;**
- **сняло проблему управления сетью.**

Было найдено два решения, выполняющих поставленные условия. И это были локальные и глобальные сети.

8.2 Описание типов сетей

Организацией сети называется обеспечение взаимосвязи между рабочими станциями, периферийным оборудованием (принтерами, накопителями на жестких дисках, сканерами, приводами CD-ROM) и другими устройствами. При организации сети одной из задач является согласование различных типов компьютеров. Независимо от того, какие устройства используются в сети. Сложность, сферы применения и схемы сетей данных продолжают развиваться и сейчас. Для реализации связи между сетями различным типам сетей присваивают различные описательные имена. Наша с вами задача познакомиться с основными классификациями и типами сетей

8.2.1 Описание сети LAN

Локальные сети служат для объединения рабочих станций, периферии, терминалов и других устройств. Локальная сеть позволяет повысить эффективность работы компьютеров за счет совместного использования ими ресурсов, например файлов и принтеров. Как результат, это дает возможность предприятию использовать локальную сеть для связи воедино данных, функций обмена и вычислений, а также хранения информации на файл-серверах.

Характерными особенностями локальной сети являются:

- **ограниченные географические пределы;**
- **обеспечение многим пользователям доступа к среде с высокой пропускной способностью;**
- **постоянное подключение к локальным сервисам;**
- **физическое соединение рядом стоящих устройств.**

Более подробно с локальными сетями вы познакомитесь освоив данный раздел

8.2.2 Описание сети WAN

Быстрое распространение компьютеров привело к увеличению числа локальных сетей. Они появились в каждом отделе и учреждении. В то же время каждая локальная сеть — это отдельный электронный остров, не имеющий связи с другими себе подобными. Стало очевидным, что использования технологии локальных сетей уже недостаточно. Требовалось найти способ передачи информации от одной локальной сети к другой. Решить эту задачу помогло создание глобальных сетей. Глобальные сети служат для объединения локальных сетей и обеспечивают связь между компьютерами, находящимися в локальных сетях. Глобальные сети охватывают значительные географические пространства и дают возможность связать устройства, расположенные на большом удалении друг от друга

8.2.3 Описание сети WLAN

В традиционных локальных сетях устройства соединены друг с другом с помощью медных кабелей. В некоторых ситуациях установка медных кабелей может быть непрактичной, нежелательной или даже невозможной, что в этом случае делает вы можете ознакомиться в данной главе.

8.2.4 Описание одноранговых сетей

Существуют сети устройства в которых подключены непосредственно друг к другу, без каких-либо дополнительных сетевых устройств между ними. В сетях такого типа все устройства имеют равные возможности и ответственность. А также свои преимущества и недостатки.

8.2.5 Описание сетей с архитектурой "клиент/сервер"

В последнее время все большее распространение получила архитектура когда один компьютер запрашивает информацию или сервисы у другого. Другой компьютер именуемый "Сервер" предоставляет запрашиваемую информацию или сервис клиенту. Серверы в сети "клиент-сервер" часто выполняют операции по обработке для клиентских компьютеров, например, сортируют записи базы данных и отправляют только те записи, которые запрашивал клиент. В чем же преимущества такой организации сети вы как раз и сможете узнать из следующего раздела.

8.3 Описание базовых концепций и технологий создания сетей

В качестве IT специалиста от вас потребуются знания технология настройки сетевых компонентов и устранять проблемы, связанные с ними. Для эффективной настройки компьютера, подключаемого к сети, необходимо понимать принципы IP-адресации, протоколы и другие сетевые концепции. С чем вы и сможете познакомиться из данной главы.

8.3.1 Объяснение полосы пропускания и передачи данных

Данные, передаваемые по сети, могут двигаться в одном из трех режимов: симплексном, полудуплексном или полнодуплексном, при этом скорость передачи данных напрямую зависит от полосы пропускания и именно она определяет то количество информации, которое может быть передано.

8.3.2 Описание IP-адресации

Что такое IP адрес а что такое Маска подсети, для чего они используются, и так ли нам необходимы? И каждый ли узел подключенный к сети должен иметь IP адрес вы узнаете ознакомившись с материалами данного раздела.

8.3.3 Определение протокола DHCP

Использование DHCP-сервера упрощает администрирование сети, потому что отслеживание IP-адресов выполняется программным обеспечением. Автоматическая настройка стека TCP/IP также снижает вероятность назначения дублированных или недопустимых IP-адресов, при этом упрощая работу администратора и снижая вероятность ошибки.

8.3.4 Описание приложений и протоколов Интернета

Все в сети наверняка должны использовать для общения один и тот же язык, что бы понимать друг друга. Таким языком служит протокол, который является формальным описанием набора правил и соглашений, регламентирующих обмен информацией между устройствами в сети. Например, если группе людей поручают работу над общим проектом, то не имеет значения, кто эти люди по национальности — немцы, французы, итальянцы или американцы, — главное, чтобы они могли понять друг друга, т.е. разговаривали на одном языке. В современном мире такая группа людей, скорее всего, использовала бы английский язык. В сфере компьютерных технологий роль такого языка выполняют протоколы, которые понятны всем устройствам сети.

8.3.5 Определение протокола ICMP

Какой протокол используется устройствами сети для отправки управляющих сообщений и сообщений об ошибках на компьютеры и серверы. И каким образом он функционирует, узнайте из данного раздела.

8.4 Описание физических компонентов сети

Средой передачи данных называется физическая среда, пригодная для прохождения сигнала. Чтобы компьютеры могли обмениваться кодированной информацией, среда должна обеспечить их физическое соединение друг с другом. Их физическое объединение выполняется с помощью физических компонентов, а вот каких, нам и предстоит с вами узнать.

8.4.1 Знакомство с названиями, предназначением и характеристиками сетевых устройств

Сетевыми устройствами называются аппаратные средства, используемые для объединения сетей. По мере увеличения размеров и сложности компьютерных сетей усложняются и сетевые устройства, которые их соединяют. Однако, все сетевые устройства служат для решения одной или нескольких общих задач.

- Увеличивают число узлов, подключаемых к сети.
- Увеличивают расстояние, на которое может простираться сеть.
- Локализуют трафик в сети.
- Могут объединять существующие сети.
- Изолируют сетевые проблемы, делая их диагностику более простой.

8.4.2 Знакомство с названиями, предназначением и характеристиками наиболее распространенных сетевых кабелей

До недавнего времени кабели были единственной средой, использующейся для подключения устройств к сети. Существует огромное количество сетевых кабелей. В коаксиальных кабелях и витых парах для передачи данных используется медь. В волоконно-оптических кабелях для передачи данных используется стекло или пластик. Эти кабели имеют разную полосу пропускания, размеры и стоимость. Вам необходимо знать, какой тип кабеля лучше всего использовать в той или иной ситуации, чтобы вы могли использовать правильные кабели для выполнения определенных задач. Вам также понадобится уметь выявлять и устранять проблемы, с которыми придется сталкиваться.

8.5 Описание топологий и архитектур локальных сетей

Большинство компьютеров, с которыми вам придется работать, являются частью сети. Основополагающими блоками разработки компьютерных сетей являются топологии и архитектуры. Несмотря на то что вам, вероятно, не придется строить компьютерную сеть, вы должны понимать, как она спроектирована, для того чтобы работать с компьютерами, являющимися ее частью.

8.5.1 Описание топологий локальных сетей

Физическая топология определяет способ подключения компьютеров, принтеров и других устройств к сети. Логическая топология описывает способы получения доступа узлов к среде и их связывания в сети. Тип топологии определяет возможности сети, в том числе легкость настройки, скорость и длину кабелей.

8.5.2 Описание архитектур локальных сетей

Архитектура локальной сети описывает как физические, так и логические топологии, использующиеся в сети. А вот какие наиболее распространенные архитектуры локальных сетей существует вам и предстоит узнать.

8.6 Знакомство с организациями по стандартизации

Как мы с вами уже говорили установлением сетевых стандартов занимаются несколько всемирных организаций по стандартизации. Стандарты используются производителями в качестве основы при разработке технологий, особенно технологий связи и организации сетей, а вот какие все же организации занимаются стандартизацией мы с вами более подробно и узнаем из данной главы.

8.7 Знакомство со стандартами Ethernet

Протоколы Ethernet описывают правила, управляющие способом связи в сети Ethernet. Чтобы обеспечить совместимость всех устройств Ethernet друг с другом, Ethernet разработала стандарты для производителей и программистов, которые следует соблюдать при разработке устройств Ethernet.

8.7.1 Описание стандартов кабельных Ethernet

Данный раздел посвящен наиболее распространенным стандартам Ethernet с которыми вам и придется познакомиться.

8.7.2 Описание стандартов беспроводных Ethernet

Беспроводные технологии все больше и больше начинают повсеместно внедряться и вытеснять проводные технологии передачи данных, с основными стандартами беспроводных сетей вы как раз и сможете познакомиться.

8.8 Описание моделей данных OSI и TCP/IP

Для решения проблемы совместимости Международная организация по стандартизации (International Organization for Standardization, ISO) исследовала существующие схемы сетей. В результате исследования была признана необходимость в создании эталонной модели сети, которая смогла бы помочь поставщикам создавать совместимые сети. И в 1984 году ISO выпустила в свет эталонную модель взаимодействия открытых систем (OSI).

Эталонная модель OSI быстро стала основной архитектурной моделью взаимодействия между компьютерами. Несмотря на то, что были разработаны и другие архитектурные модели, большинство поставщиков сетей, желая сказать пользователям, что их продукты совместимы и способны работать с разными производимыми в мире сетевыми технологиями, ссылаются на их соответствие эталонной модели OSI. И действительно, эта модель является самым лучшим средством, имеющимся в распоряжении тех, кто надеется изучить технологию сетей.

8.8.1 Определение модели TCP/IP

Эталонная модель TCP/IP является общим базисом для разработки протоколов, использующихся в Интернет. Она состоит из уровней, выполняющих функции, необходимые для подготовки данных к передаче по сети. Сообщение начинается на верхнем, прикладном уровне и движется вниз по уровням TCP/IP к нижнему уровню, уровню сетевого доступа. По мере движения сообщения вниз, через каждый уровень, к сообщению добавляется заголовочная информация, после чего сообщение передается. По достижении места назначения сообщение движется обратно вверх через каждый уровень модели TCP/IP. По мере движения сообщения вверх по уровням к месту назначения информация о заголовке, добавленная к сообщению, отделяется.

8.8.2 Определение модели OSI

Эталонная модель OSI — это описательная схема сети; ее стандарты гарантируют высокую совместимость и способность к взаимодействию различных типов сетевых технологий. Кроме того, она иллюстрирует процесс перемещения информации по сетям. Это концептуальная структура, определяющая сетевые функции, реализуемые на каждом ее уровне. Модель OSI описывает, каким образом информация проделывает путь через сетевую среду (например, провода) от одной прикладной программы (например, программы обработки таблиц) к другой прикладной программе, находящейся в другом

подключенном к сети компьютере. По мере того, как подлежащая отсылке информация проходит вниз через уровни системы, она становится все меньше похожей на человеческий язык и все больше похожей на ту информацию, которую понимают компьютеры, а именно на "единицы" и "нули".

8.8.3 Сравнение OSI и TCP/IP

И модель OSI, и модель TCP/IP являются эталонными моделями, используемыми для описания процесса передачи данных. Модель TCP/IP используется именно для семейства протоколов TCP/IP, а модель OSI — для разработки стандартного взаимодействия для оборудования и приложений разных производителей. Эталонная модель OSI делит задачу перемещения информации между компьютерами через сетевую среду на семь менее крупных и, следовательно, более легко разрешимых подзадач. Каждая из этих семи подзадач выбрана потому, что она относительно автономна и, следовательно, ее легче решить без чрезмерной опоры на внешнюю информацию.

8.9 Описание настройки сетевого адаптера и модема

Сетевые адаптеры преобразуют пакеты данных в сигналы для передачи по сети. В ходе изготовления фирмой-производителем каждому сетевому адаптеру присваивается физический адрес, который заносится в специальную микросхему, устанавливаемую на плате адаптера. В большинстве сетевых адаптеров MAC-адрес зашивается в ПЗУ. Когда адаптер инициализируется, этот адрес копируется в оперативную память компьютера. Поскольку MAC-адрес определяется сетевым адаптером, то при замене адаптера изменится и физический адрес компьютера; он будет соответствовать MAC-адресу нового сетевого адаптера.

Для примера можно представить себе гостиницу. Предположим далее, что комната 207 имеет замок, открывающийся ключом А, а комната 410 — замок, открывающийся ключом F. Принято решение поменять замки в комнатах 207 и 410. После замены ключ А будет открывать комнату 410, а ключ F — комнату 207. В этом примере замки играют роль сетевых адаптеров, а ключи — роль MAC-адресов. Если адаптеры поменять местами, то изменятся и MAC-адреса.

8.9.1 Установка или обновление драйвера сетевого адаптера

Иногда производитель выпускает новые драйвера для сетевого адаптера. Новый драйвер может расширить функциональные возможности сетевого адаптера, либо он может требоваться для обеспечения совместимости операционной системы.

8.9.2 Подключение компьютера к существующей сети

Данный раздел рассматривает поледовательность действий которые необходимо совершить для подключения нового компьютера к сети.

8.9.3 Описание установки модема

Иногда, может возникнуть необходимость связи компьютеров с использованием телефонной системы общего пользования, как настроить подключение, вы и узнаете из данного раздела.

8.10 Знакомство с названиями, предназначением и характеристиками других технологий, используемых для установки соединения

Существует множество различных способов подключения к Интернету. Телефонные, кабельные, спутниковые и частные телекоммуникационные компании предлагают услуги подключения к Интернету для использования дома и в офисе. Для реализации связи между сайтами в Интернете существует несколько решений WAN. WAN-соединения работают на разных скоростях и предоставляют услуги различных уровней. Прежде чем реализовать какое-либо подключение к Интернету, найдите все имеющиеся ресурсы и определите наилучшее решение, удовлетворяющее потребностям вашего клиента, с возможными решениями вам и предстоит познакомиться в данном разделе.

8.11 Описание и применение стандартных процедур профилактического обслуживания, используемых для сетей

Для надежной работы сети необходимо регулярно выполнять ряд стандартных процедур профилактического обслуживания. Если один из компьютеров, подключенных к сети организации, не работает надлежащим образом, то, как правило, это затрагивает лишь одного пользователя. Но если вся сеть неисправна, то работать не сможет большое количество пользователей.

8.12 Устранение неполадок в сетях

Сетевые проблемы могут быть простыми или сложными. Чтобы оценить степень сложности проблемы, необходимо определить, сколько компьютеров в сети с ней столкнулись.

Если проблема возникает только на одном компьютере в сети, начните с поиска и устранения неполадок на этом компьютере. Если проблема затрагивает все компьютеры сети, начните процесс устранения неполадок в пункте сети, где подключены все компьютеры. Технический специалист должен разработать логический и целостный метод диагностики сетевых проблем, последовательно исключая по одной проблеме из списка.

Для точного определения, устранения и документирования проблемы выполните действия, описываемые в этом разделе.

Кроме того очень бы хотелось что бы вы не обделили своим вниманием и раздел 15 «Дополнительные сведения о сетях»

15.1 Знакомство с потенциальными угрозами безопасности и реализация надлежащих процедур защиты, связанных с сетями

Установка сетевых кабелей, как медных, так и волоконно-оптических, может быть опасной. Часто кабели приходится протягивать по потолкам и стенам, где могут быть препятствия и неожиданные или токсичные материалы. Необходимо надевать подходящую одежду и средства защиты от этих материалов. Например, надевайте длинные брюки, рубашку с длинными рукавами, прочную обувь, закрывающую стопы, и перчатки. И самое важное: надевайте защитные очки. Если возможно, выясните в домоуправлении или у ответственного за порядок в здании, есть ли опасные материалы или препятствия, о которых необходимо знать перед началом работ в области потолка.

По завершении данного раздела вы освоите:

- Описание правил техники безопасности при работе с оптоволокном.
- Описание угроз безопасности при работе с кабелями, резаками и резке кабелей.

15.2 Проектирование сети на основе потребностей клиента

Сеть работает лучше всего, если она спроектирована таким образом, чтобы удовлетворять потребностям клиента. Для создания сети требуется проанализировать окружающую обстановку и варианты ее создания. Необходимо поговорить с клиентом и другим людьми, участвующими в этом процессе. Важно иметь общую идею об аппаратном и программном обеспечении, которое будет использоваться в сети. Вы должны поинтересоваться будущим ростом компании и сети.

- Определение топологии.
- Определение протоколов и сетевых приложений.

Вот с чем вам придется познакомиться из данного раздела.

15.3 Описание компонентов сети клиента

Выбор сетевой топологии определяет типы устройств, кабелей и сетевых интерфейсов, которые будут требоваться для построения сети. Кроме того, необходимо настроить внешнее подключение к поставщику услуг Интернета. Один из шагов по организации сети заключается в определении подходящих сетевых компонентов, которые будут хорошо сочетаться с устройствами пользователя и сетевыми кабелями.

15.4 Реализация сети клиента

Установка и реализация сети может оказаться сложной задачей. Даже установка небольшой домашней сети может потребовать много сил и времени. Однако тщательное планирование поможет обеспечить более легкую и быструю установку.

Во время установки может возникнуть простой существующей сети. Например, при переделке зданий и установке сетевого кабеля могут возникать разрушения. Проект не является завершенным до тех пор, пока все устройства не будут установлены, настроены и протестированы.

15.5 Модернизация сети клиента

После определения местоположения всех сетевых устройств можно прокладывать сетевые кабели. Прокладка сетевых кабелей в некоторых новых или отреставрированных зданиях поможет избежать проблемы, связанной с прокладкой кабелей в отделанных стенах. Если кабель предварительно не проложен, это придется сделать вам. А как это сделать наилучшим образом, поможет освоить данный раздел.

15.6 Описание установки, настройки и управления простым почтовым сервером

Если клиент устанавливает в сеть дополнительные компьютеры или добавляет устройства беспроводного доступа, вы должны уметь правильно рекомендовать оборудование на основе потребностей клиента. Предложенное вами оборудование должно работать в сочетании с существующим оборудованием и кабельной проводкой, либо существующую инфраструктуру необходимо модернизировать.

По завершении данного раздела вы освоите:

- Установка и настройка беспроводного сетевого адаптера.
- Установка и настройка беспроводных маршрутизаторов.
- Тестирование соединения.

15.7 Описание процедур профилактического обслуживания сетей

Профилактическое обслуживание так же важно для сети, как и для подключенных к ней компьютеров. Необходимо проверить состояние кабелей, сетевых устройств, серверов и компьютеров и убедиться, что они содержатся в чистоте и рабочем состоянии. Необходимо разработать план для выполнения регулярного планового технического обслуживания и очистки. Это поможет избежать простоев сети и отказа оборудования.

15.8 Поиск и устранение неполадок в сети

Чтобы начать процесс поиска и устранения неполадок в сети, сначала необходимо найти источник проблемы. Выясните, сколько пользователей сети столкнулись с проблемой: один или целая группа. Если проблема касается одного пользователя, начните процесс ее устранения с компьютера этого пользователя, если большой группы пользователей обратите свое внимание на коммутационное оборудование.

В итоге можно сказать, что нами были рассмотрены вопросы планирования, реализации и модернизации сетей и сетевых компонентов. Всего того с чем вам придется столкнуться при работе с реальными сетями. Поскольку при объединении компьютеров в сеть число связей между машинами увеличивается, то при этом, как правило, усугубляются все имевшиеся ранее проблемы. Как говорят, "работа в сети — это когда вы не можете выполнить свое задание из-за отказа компьютера, о котором никогда не слышали".

Управление сетями — это, прежде всего, искусство и наука предотвращения их разрушения. Сюда обычно входят следующие задачи:

- поиск неисправностей в сетях, шлюзах и важных серверах;
- разработка схем уведомления администратора о наличии проблем;
- общий мониторинг сети с целью распределения нагрузки в ней и планирования ее дальнейшего расширения;
- документирование и визуализация работы сети;
- управление сетевыми устройствами с центральной станции.

С которыми мы с вами и познакомились.

3. Основы безопасности

Как вы заметили, организация сети это очень трудоемкий процесс требующий учета большого количества факторов однако организовать безопасность вашей сети еще труднее. И хотя присоединение к Интернету предоставляет огромные выгоды в виде доступа к колоссальному объему информации, оно не обязательно является хорошим решением для организаций с низким уровнем безопасности. Интернет страдает от серьезных проблем с безопасностью, которые, если их игнорировать, могут привести к ужасным последствиям для неподготовленных сетей. Ошибки при проектировании сервисов TCP/IP, сложность конфигурирования хостов, уязвимые места, появившиеся в ходе написания программ, и ряд других причин в совокупности делают неподготовленные сети открытыми для деятельности злоумышленников и уязвимыми к связанным с этим проблемам.

Данное положение дел сложилось по ряду причин. Одной из основных причин может быть то, что при разработке Интернет требования безопасности не учитывались, так как главным требованием при реализации Интернета было требование удобства при обмене информацией при проведении научных исследований. Тем не менее, феноменальный успех Интернета в сочетании с появлением большого числа категорий пользователей, включая пользователей, у которых отсутствует понятие этики, усугубило существующие недостатки в обеспечении безопасности до такой степени, что сети, открытые для доступа со стороны Интернета, стали подвергаться риску проникновений в них и нанесения им разрушений. Другими причинами являются следующие:

- уязвимость сервисов TCP/IP - ряд сервисов TCP/IP являются небезопасными и могут быть скомпрометированы умными злоумышленниками; сервисы, использующиеся в ЛВС для улучшения управления сетью, особенно уязвимы
- легкость наблюдения за каналами и маскарда - большинство трафика Интернета незашифровано; электронная почта, пароли и передаваемые файлы могут быть перехвачены, используя легкодоступные программы, затем злоумышленники могут использовать пароли для проникновения в системы
- отсутствие политики - многие сети могут быть сконфигурированы по незнанию таким образом, что будут позволять доступ к ним со стороны Интернета, не подозревая при этом о возможных злоупотреблениях этим; многие сети допускают использование большего числа сервисов TCP/IP, чем это требуется для деятельности их организации, и не пытаются ограничить доступ к информации об их компьютерах, которая может помочь злоумышленникам проникнуть в сеть
- сложность конфигурирования - средства управления доступом в хостах зачастую являются сложными в настройке и контроле за ними; неправильно сконфигурированные средства часто приводят к неавторизованному доступу.

К счастью, существуют простые и надежные решения, которые могут быть использованы для улучшения безопасности сети организации. С ними мы сейчас с вами и познакомимся, основываясь на материалы компании Cisco, Которая всегда очень серьезно относилась к вопросам безопасности сетей и пользовательских компьютеров.

Глава 9 «Основы безопасности»

9.1 Объяснение причин важности вопросов безопасности

Обеспечение безопасности компьютера и сети помогает сохранить данные и оборудование в рабочем состоянии и предоставить доступ только санкционированным пользователям. Все сотрудники организации должны уделять особенно высокое внимание безопасности, потому что бреши в системе безопасности могут привести к негативным последствиям для любого из них.

Кража, утрата, проникновение в сеть и физическое повреждение являются лишь некоторыми способами нанесения ущерба сети или компьютеру. Повреждение или утрата оборудования может означать потерю производительности. Ремонт и замена оборудования могут стоить компании времени и денег. Несанкционированное использование сети может привести к разглашению конфиденциальной информации и уменьшению количества сетевых ресурсов.

Атака, которая намеренно ухудшает производительность компьютера или сети, также может нанести ущерб производительности организации. Плохо реализованные меры безопасности для беспроводных сетевых устройств демонстрируют, что для несанкционированного доступа злоумышленников необязательно физическое подключение.

9.2 Описание угроз безопасности

Для успешной защиты компьютеров и сети технический специалист должен быть знаком с обоими типами угроз системе безопасности компьютера. Нужно помнить, угроза безопасности может исходить изнутри или извне организации, а уровень потенциальных повреждений может существенно варьироваться.

9.2.1 Определение вирусов, червей и Троянов

Компьютерные вирусы сознательно создаются и рассылаются атакующими. Вирус прикрепляется к небольшим элементам компьютерного кода, программного обеспечения или документам. Вирус выполняется при запуске программного обеспечения на компьютере. Если вирус распространяется на другие компьютеры, то они тоже могут стать переносчиками вируса, но это неединственная проблема безопасности, не нужно также забывать про сетевых червей и троянов.

9.2.2 Объяснение web-безопасности

Поскольку ежедневно всемирную паутину посещает огромное количество людей, веб-безопасность имеет большую важность. Некоторые функциональные возможности, делающие всемирную паутину полезной и занимательной, также могут нести в себе угрозу компьютеру. Атакующие могут использовать любой из этих инструментов для установки программы на компьютеры.

9.2.3 Определение рекламного, шпионского и нежелательного ПО

Рекламное, шпионское и нежелательное ПО обычно устанавливается на компьютере без ведома пользователя. Эти программы собирают информацию, хранящуюся на компьютере, изменяют конфигурацию компьютера или открывают на компьютере дополнительные окна без согласия пользователя.

9.2.4 Описание атаки "Отказ в обслуживании"

Отказ в обслуживании — это форма атаки, препятствующая доступу пользователя к обычным службам, таким как электронная почта и веб-сервер, поскольку система перегружена и не может откликаться на аномально большое количество запросов. При атаке типа "Отказ в обслуживании" производится рассылка запросов к системе, количества которых достаточно для того, чтобы запрашиваемая служба оказалась перегруженной и прекратила работу.

9.2.5 Описание спама и всплывающих окон

При использовании в качестве способа атаки спам может содержать ссылки на инфицированный веб-сайт или вложение, которое может инфицировать компьютер. В результате открытия таких ссылок или вложений на экране может появиться большое количество окон, которые будут отвлекать внимание пользователя и уводить его на рекламные сайты.

9.2.6 Описание атаки "социальная инженерия"

Социальный инженер — это человек, который умеет получить доступ к оборудованию или сети, обманом вынуждая людей предоставить необходимую для доступа информацию. Часто социальные инженеры завоевывают доверие сотрудника и убеждают его сообщить имя пользователя и пароль.

9.2.7 Описание атак ТСП/ІР

ТСП/ІР — это семейство протоколов, которое используется для управления всеми взаимодействиями в Интернете. К сожалению, ТСП/ІР также может делать сеть уязвимой для злоумышленников, в следствии своей не идеальности.

9.2.8 Описание разрушения и утилизации аппаратного обеспечения

Разрушение аппаратного обеспечения — это процесс удаления уязвимых данных из аппаратного и программного обеспечения перед их переработкой и утилизацией. Чтобы воспрепятствовать возможности восстановления данных с помощью специальных программ, данные на жестких дисках должны быть полностью стерты. Удаления файлов и даже форматирования диска будет недостаточно. С помощью сторонних инструментов можно переписать данные несколько раз, в результате чего не уничтоженные данные можно отобразить. Как этого избежать вы и узнаете из данного раздела.

9.2 Знакомство с процедурами обеспечения безопасности

Необходимо составить план обеспечения безопасности, с помощью которого можно было бы определить, как следует поступать в критической ситуации. План обеспечения безопасности необходимо постоянно обновлять, чтобы он отражал самые последние угрозы сети. В плане обеспечения безопасности необходимо указать процедуры, являющиеся основой действий технического специалиста. План обеспечения безопасности необходимо ежегодно пересматривать.

Частью процессов обеспечения безопасности является выполнение тестов, которые должны определить слабые места в системе безопасности. Тестирование необходимо выполнять регулярно. Ежедневно появляются все новые и новые угрозы. Регулярное тестирование покажет любые возможные слабые места текущего плана обеспечения безопасности, которые необходимо будет устранить. Как это сделать вы и узнаете из данного раздела.

9.4 Знакомство со стандартными процедурами профилактического обслуживания, направленными на обеспечение безопасности

Процесс и технологии обеспечения безопасности постоянно меняются. Ежедневно появляются новые разработки. Злоумышленники постоянно ищут новые способы для своих атак. Производители программного обеспечения должны регулярно создавать и выпускать новые исправления для устранения брешей и уязвимости своих продуктов. Если технический специалист оставит компьютер незащищенным, то злоумышленник может легко получить к нему доступ. Незащищенные компьютеры, подключенные к Интернету, могут быть заражены за несколько минут. В связи с постоянно меняющимися угрозами безопасности технический специалист должен понимать, как следует устанавливать исправления и обновления.

9.5 Устранение неполадок в системе обеспечения безопасности

Вирусы и черви всегда представляют собой угрозу безопасности. Злоумышленники постоянно ищут новые способы проникновения в компьютеры и сети. Поскольку новые вирусы создаются постоянно, защитную программу необходимо постоянно обновлять. Этот процесс может выполняться автоматически, но специалист по компьютерам должен знать, как вручную провести обновление программы защиты любого типа и всех прикладных программ пользователя.

Программы защиты от вирусов, шпионского и рекламного ПО ищут шаблоны кода программирования в программном обеспечении, установленном на компьютере. Эти шаблоны определяются путем анализа вирусов, которые перехватываются в Интернете и локальных сетях. Однако при загрузке файлов сигнатур с сайта-зеркала убедитесь в том,

что этот сайт является легальным. Всегда заходите на зеркальный сайт по ссылке с сайте производителя.

В данной главе мы рассмотрели вопросы компьютерной безопасности и причины, по которым так важно защищать компьютерное оборудование, сети и данные. Здесь были описывались угрозы, процедуры и операции профилактического обслуживания, связанные с обеспечением физической безопасности и защиты данных, которые помогут поддерживать безопасность компьютерного оборудования и данных. Системы безопасности защищает компьютеры, сетевое оборудование и данные от потери и физического повреждения.

Однако ознакомившись с главой 16, вы сможете почерпнуть дополнительные сведения о безопасности. Так как безопасность никогда не бывает излишней.

И помните ваш компьютер, на который беспрепятственно может заходить посторонний пользователь, в следствии того что вы не обеспечили надлежащим образом его безопасность, уже не может считаться ВАШИМ КОМПЬЮТЕРОМ.