



ВИДЕОСАМОУЧИТЕЛЬ

2в1: книга+видеокурс

Александр Ватаманюк

Создание и обслуживание локальных сетей



ПИТЕР

Видеосамоучитель

Александр Ватаманюк

**Создание и обслуживание
локальных сетей**

«Питер»

2008

Ватаманюк А. И.

Создание и обслуживание локальных сетей / А. И. Ватаманюк — «Питер», 2008 — (Видеосамоучитель)

Данная книга поможет вам получить базовые теоретические знания и практические навыки по планированию, проектированию, монтажу и настройке компьютерных сетей, а также по обеспечению их безопасности и поиску неисправностей. Изложенный материал будет интересен как начинающим сетевым администраторам, так и специалистам смежных областей, которые делают первые шаги в изучении компьютерных сетей. Рассматривается настройка сетей в Windows XP и Windows Vista. Видеокурс прилагается только к печатному изданию книги.

© Ватаманюк А. И., 2008

© Питер, 2008

Содержание

Введение	5
От издательства	6
Часть 1	7
Глава 1	7
1.1. Причины появления сети и перспективы ее развития	7
1.2. Как создаются сети и кто это может сделать	8
Глава 2	9
2.1. Одноранговая сеть	9
2.2. Сеть на основе сервера	11
Глава 3	15
3.1. Модель ISO/OSI	15
3.2. Сетевой протокол	19
3.3. Протоколы работы с электронной почтой	24
Конец ознакомительного фрагмента.	25

Александр Иванович Ватаманюк

Создание и обслуживание локальных сетей

Введение

Компьютерные сети оплели весь земной шар, и вы, хотите того или нет, увязли в них так же прочно, как муха в паутине. Теперь попробуйте ответить на вопрос: нужно ли пытаться разобраться с этой ситуацией или пустить все на самотек?

Принимая решение, имейте в виду: уровень компьютеризации вырос настолько, что лишь безнадежно отсталый человек может оказаться незатронутым ею, даже если техника заполняет его быт и работу.

Книга, которую вы держите в руках, приобщит вас к научно-техническому прогрессу и научит жить в современном компьютерном обществе. Из нее вы узнаете много интересной и полезной информации о том, что такое компьютерная сеть и как с ней «общаться». Люди же более любознательные получают неоценимый опыт и смогут использовать его на практике.

Книга содержит большое количество текстовой и графической информации, которая облегчит понимание самой сущности локальной сети. Мало того, к изданию прилагается диск с видеоуроками, которые в режиме реального времени познакомят вас со всем процессом, начиная с создания сети и заканчивая ее настройкой и обслуживанием. На компакт-диске вы также найдете краткое описание программного обеспечения для контроля сетевого трафика, работы в Интернете, антивирусной защиты и многие из рассмотренных программ. Коммерческие продукты представлены ознакомительными и демонстрационными версиями. Как правило, в демонстрационных версиях недоступны некоторые инструменты и функции, но пользоваться ими можно сколь угодно долго. Ознакомительные версии обычно полнофункциональны, но действуют в течение ограниченного времени (30 дней или меньше). Некоторые из рассмотренных в книге программ являются бесплатными, их возможности и срок действия неограниченны.

Только ленивый не познает и не оценит возможности компьютерных сетей! Не становитесь им!

Книга ориентирована на определенную категорию читателей, однако это совсем не означает, что любой человек не сможет разобраться с ее материалом. По подобному принципу создавался и этот видеосамоучитель. Конечно, основная его аудитория – читатели, которые хотят больше узнать о локальных сетях и способах их создания. Тем не менее осилить и понять ее сможет даже малоопытный компьютерный пользователь.

В любом случае, даже если вас не очень интересуют разные компьютерные штучки и тем более сети, прочитав книгу, вы ими заинтересуетесь. Это гарантировано. Поэтому просто расслабьтесь и просвещайтесь, и будьте уверены в том, что вы с легкостью овладеете изложенным материалом!

От издательства

Ваши замечания, предложения и вопросы отправляйте по следующему адресу электронной почты: dgurski@minsk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства <http://www.piter.com> вы найдете подробную информацию о наших книгах.

Часть 1

Компьютерная сеть. Общие понятия

Глава 1

Сеть? Это что еще такое?

- Причины появления сети и перспективы ее развития
- Как создаются сети и кто это может сделать

1.1. Причины появления сети и перспективы ее развития

Когда компьютер только задумывали, главной его задачей предполагалось облегчение труда человека и автоматизация и ускорение выполнения некоторых арифметических операций. Никто тогда даже думать не мог, что компьютеров через несколько десятков лет будет настолько много, что рано или поздно они будут объединены в один громадный «организм», удовлетворяющий практически все потребности человека. Тем не менее так оно и произошло, по крайней мере очень близко к этому.

Каковы же причины появления сети? Как минимум можно выделить несколько:

- несовершенство существующих компьютеров и компьютерной техники;
- недостаток мощности отдельного компьютера для выполнения сложной задачи;
- слишком большое количество людей, задействованных в достижении поставленной цели;
- новые направления в науке, требующие все больших человеческих и компьютерных ресурсов.

Этот список можно продолжать очень долго, но факт остается фактом: рано или поздно сеть должна была возникнуть и она возникла.

Таким образом, сеть – не что иное, как некоторое количество компьютеров, определенным способом подключенных друг к другу. Однако это только часть понятия. На самом деле сюда еще нужно включить сетевые операционные системы, прикладные программы, специальные программные механизмы обмена информацией и многое другое.

Можно сказать однозначно, что появление сети изменило жизнь всего человечества. Преимуществ у сети много, больше, чем можно было бы себе представить. Вот только некоторые из них:

- организация одновременной работы многих пользователей с одним источником, будь то распределенная база данных или обычный офисный документ;
- использование всех компьютеров сети для выполнения одной работы с целью осуществления сложного, требующего много ресурсов проекта;
- обмен информацией любого характера, будь то рабочие данные или фильмы и музыка;
- получение данных из любой точки земного шара с использованием для этого сети спутников;
- общение (устное, письменное, визуальное) на расстоянии;
- использование компьютерных сетей для обучения и любого другого типа образования.

Преимуществ сети много, а недостатков практически нет. Ну разве что возможность тотального наблюдения за любым подключенным к сети пользователем...

Каковы перспективы дальнейшего развития сети? Все очень просто: глобальная компьютеризация и возможность мгновенного получения любой информации с использованием для

этого любого устройства с коммуникационными способностями. После этого, наверное, жизнь станет гораздо скучнее.

1.2. Как создаются сети и кто это может сделать

Сети возникают с пугающей скоростью. Порой приходишь в знакомый офис через неделю, а в нем уже функционирует современная сеть с высокой пропускной способностью. Но самое главное, что организовать сеть может практически любой человек, более или менее знакомый с принципом и правилами ее создания. Так почему бы вам не стать этим «любим»?

Конечно, сразу создать сеть с большим количеством компьютеров будет достаточно трудно, даже если вы прочтете гору книг по теме. Самый простой способ научиться – познакомиться с теорией и попроситься к кому-нибудь в ученики. И будет большим плюсом, если вы попытаетесь сами соединить хотя бы два рядом стоящих компьютера в домашних условиях. Это и станет началом вашей сетевой практики.

Однако, как обычно, все нужно начинать с теории. Необходимо познакомиться с существующими стандартами и топологиями, увидеть сетевое оборудование, пощупать кабель, коннекторы и т. д.

Данная книга призвана облегчить процесс освоения принципов сети и дать основные практические советы. Как говорится, не святые горшки лепят, все в ваших руках. Поэтому учите теорию и осваивайте практику!

Глава 2

Типы сетей

- Одноранговая сеть
- Сеть на основе сервера

Сегодня, как и 10 лет назад, существует два типа сетей: одноранговая сеть и сеть на основе сервера (выделенного компьютера). Каждая из них имеет как преимущества, так и недостатки.

Одноранговая сеть, скорее всего, придется по душе пользователям, которые хотят сначала попробовать сеть в деле или ограничены в средствах. Сеть на основе сервера организуют там, где важен полный контроль над всеми рабочими местами. Это может быть и небольшая домашняя сеть, и объемная корпоративная система сетей, объединенных в одну общую.

Эти два разных типа имеют общие корни и принципы функционирования, что в случае необходимой модернизации позволяет перейти от более простого варианта (одноранговой сети) к более сложному (сети на основе сервера).

2.1. Одноранговая сеть

Одноранговую сеть построить достаточно просто. Особенность такой сети в том, что все входящие в ее состав компьютеры работают сами по себе, то есть ими никто не управляет.

Одноранговая сеть выглядит как некоторое количество компьютеров, объединенных определенным образом в одну рабочую группу (рис. 2.1). Именно отсутствие управляющей машины (сервера) делает ее построение дешевым и эффективным мероприятием.

Любой компьютер в такой сети можно назвать как рабочим, так и сервером, поскольку нет какой-либо конкретной выделенной машины, которая осуществляла бы административный или другой контроль. За компьютером такой сети следит сам пользователь (или пользователи), который работает на нем. В этом кроется главный недостаток одноранговой сети – ее пользователь должен не просто уметь работать на компьютере, но и иметь представление об администрировании. Кроме того, ему в большинстве случаев приходится самому справляться с возникающими внештатными ситуациями и защищать себя от разнообразных неприятностей, начиная с вирусов и заканчивая программными и аппаратными неполадками.

Как и полагается, одноранговая сеть позволяет использовать общие файлы, принтеры, модемы и т. п. Однако из-за отсутствия управляющего компьютера каждый пользователь разделяемого ресурса должен самостоятельно устанавливать права доступа к нему.

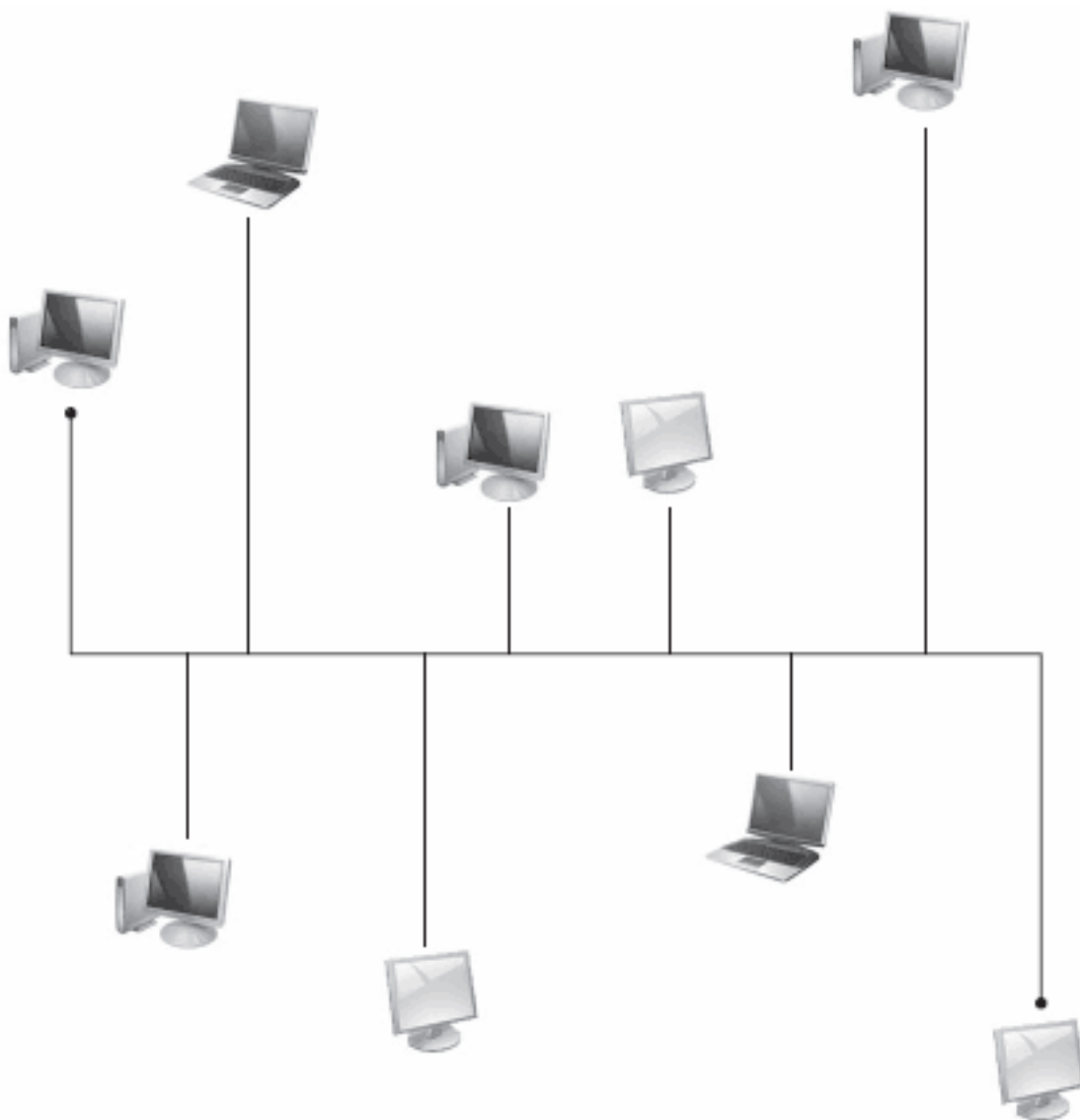


Рис. 2.1. Пример одноранговой сети

Для работы с одноранговыми сетями можно использовать любую операционную систему. Ее поддержка реализована в Windows, начиная с Windows 95, поэтому никакого дополнительного программного обеспечения для работы в локальной сети не требуется. Однако если вы хотите обезопасить себя от разных программных проблем, лучше использовать операционную систему достаточно высокого класса, например Windows XP.

Одноранговую сеть обычно применяют тогда, когда нужно связать несколько (как правило, до десяти) компьютеров и не нужно использовать строгую защиту данных. Большое количество компьютеров подключать не рекомендуется, так как отсутствие «контролирующих органов» рано или поздно приводит к возникновению различных проблем. Ведь из-за одного необразованного или ленивого пользователя под угрозу ставится безопасность и работоспособность всей сети.

Если вы заинтересованы в более защищенной и контролируемой «организации», то создавайте сеть на основе сервера.

В табл. 2.1 перечислены основные преимущества и недостатки одноранговой сети.

Таблица 2.1. Преимущества и недостатки одноранговой сети

Преимущества	Недостатки
Дешевая в создании	Недостаточный контроль над клиентскими местами
Не нужен выделенный сервер (или серверы)	Отсутствие механизма настраиваемого доступа нескольких пользователей к разным ресурсам на одном компьютере
Не требуется специальное программное обеспечение	Низкая безопасность и защищенность сети от вирусных атак
Не нужен человек, который будет поддерживать сеть и клиентские места	Отсутствие нормального механизма резервного копирования данных
	Необходимость подготовленности пользователя к разным административным мерам — обновлению антивирусной базы, архивированию данных, определению механизмов доступа к раздаваемым ресурсам и т. д.
	Для предоставления пользователям общего ресурса, который будет интенсивно использоваться, требуется достаточно мощный компьютер
	Ограниченная расширяемость сети

2.2. Сеть на основе сервера

Сеть на основе сервера – наиболее часто встречающийся тип, который используют как в полноценных домашних сетях и в офисах, так и на крупных предприятиях (рис. 2.2).

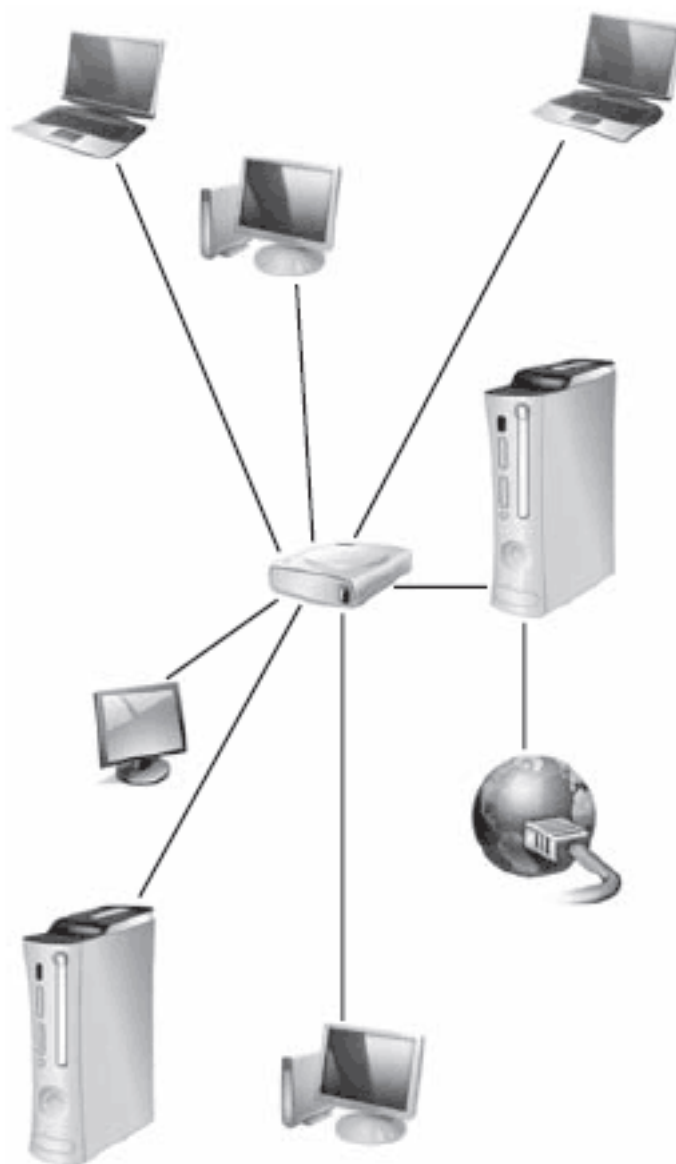


Рис. 2.2. Пример сети на основе сервера

Как ясно из названия, данная сеть использует сервер, контролирующий работу всех подключенных клиентских компьютеров. Главная его задача – создание, настройка и обслуживание учетных записей пользователей, настройка прав доступа к общим ресурсам, механизма авторизации и смены паролей доступа и многое другое.

Как правило, сервер характеризуется большой мощностью и быстродействием, необходимым для выполнения поставленных задач: будь то работа с базой данных или обслуживание других запросов пользователей. Сервер оптимизирован для быстрой обработки запросов пользователей, обладает специальными механизмами программной защиты и контроля. Достаточная мощность сервера позволяет снизить требования к мощности клиентской машины.

За работой сети на основе сервера обычно следит специалист – системный администратор. Он отвечает за регулярное обновление антивирусных баз, устраняет возникшие неполадки, разделяет общие ресурсы и т. п.

Количество рабочих мест в такой сети может быть разным – от нескольких до сотен или тысяч компьютеров. С целью поддержки производительности сети на необходимом уровне при возрастании количества подключенных пользователей устанавливают дополнительное или более скоростное сетевое оборудование, серверы и т. д.

Не все серверы выполняют одинаковую работу. Существуют следующие специализированные машины, позволяющие автоматизировать или просто облегчить выполнение тех или иных задач.

- **Файл-сервер.** Используется в основном для хранения разнообразных данных, начиная с офисных документов и заканчивая музыкой и видео. Обычно на таком сервере создаются личные папки пользователей, обращаться к которым могут только они (или другие пользователи, получившие право доступа). Для управления таким сервером используют любую сетевую операционную систему, например Windows 2000 или Windows 2003. Благодаря кэшированию файлов доступ к ним значительно ускоряется.

- **Принт-сервер.** Главная его задача – обслуживание очереди печати сетевых принтеров и обеспечение доступа к ним. Очень часто с целью экономии средств файл-сервер и принт-сервер совмещают.

- **Сервер базы данных.** Основная его задача – обеспечить максимальную скорость поиска и записи нужных данных в базу данных или получения информации из нее с последующей передачей конечному пользователю сети. Это самые мощные из всех серверов. Они обладают максимальной производительностью, так как от этого зависит комфортность работы всех пользователей.

- **Сервер приложений.** Промежуточный сервер между пользователем и сервером базы данных. Как правило, на нем выполняются те из запросов, которые требуют максимальной производительности и должны быть переданы пользователю, не затрагивая ни сервер базы данных, ни пользовательский компьютер. Это могут быть как часто запрашиваемые из базы данные, так и любые программные модули.

Кроме перечисленных выше, существуют другие серверы, например почтовые, коммуникационные, серверы-шлюзы и т. д.

Достаточно часто в целях экономии средств на один из серверов «вешают» обслуживание нехарактерных для него заданий. В этом случае следует понимать, что скорость выполнения им тех или иных задач может значительно понижаться.

Сеть на основе сервера предоставляет широкий спектр услуг и возможностей, которых трудно или невозможно добиться от одноранговой сети. Кроме того, последняя уступает в плане защищенности и администрирования. Имея выделенный сервер или серверы, легко обеспечить резервное копирование, что является первоочередной задачей, если в сети присутствует сервер базы данных.

В табл. 2.2 перечислены основные преимущества и недостатки сети на основе сервера.

Таблица 2.2. Преимущества и недостатки сети на основе сервера

Преимущества	Недостатки
Практически неограниченная расширяемость	Достаточно дорогая в создании и обслуживании
Контроль над клиентскими местами	Необходимо специальное программное обеспечение, способное работать в сети
Наличие четкого механизма доступа к общим ресурсам	Нужен постоянный системный администратор, который будет поддерживать сеть и клиентские места
Единая антивирусная база	Сложный процесс расширения сети (прокладка кабеля)
Высокая производительность	
Централизованное резервное копирование всей информации	
Низкие требования к мощности клиентских машин	

Глава 3

Модель сети и сетевые протоколы

- Модель ISO/OSI
- Сетевой протокол
- Протоколы работы с электронной почтой
- Другие протоколы

Какой бы ни была сеть, она должна подчиняться определенным законам. Не забывайте, что сеть – это не только кусок провода, но и все устройства, которые в нее входят, в том числе и компьютеры. Представьте себе на минуту, что нет никаких правил работы сети. Какие функции должны выполнять сетевая карта или маршрутизатор, как должен реагировать на это компьютер?

Чтобы избежать хаоса и упорядочить «взаимоотношения» в сети, используется специальная система правил и стандартов. Их представителями являются сетевая модель взаимодействий ISO/OSI и протоколы передачи данных.

3.1. Модель ISO/OSI

Пожалуй, ключевым понятием в стандартизации сетей и всего, что к ним относится, является *модель взаимодействия открытых систем* (Open System Interconnection, OSI), разработанная Международной организацией по стандартизации (International Standards Organization, ISO). На практике применяется короткое название «модель ISO/OSI».

Описываемая модель состоит из семи уровней (рис. 3.1), каждый из которых отвечает за определенный круг задач, осуществляя их с помощью заложенных в этот уровень алгоритмов – стандартов и протоколов. Для связи между уровнями используются процедуры взаимодействия. Таким образом, выполнив свою часть задачи, нижестоящий уровень передает готовые данные вышестоящему. Вот и получается, что, пройдя всю цепочку из семи уровней, на выходе получают готовые к «употреблению» данные. При этом они успевают должным образом закодироваться или декодироваться, пройти проверку целостности и многое другое.



Рис. 3.1. Уровни модели ISO/OSI

Основное различие между проводными (Ethernet 802.3) и беспроводными (IEEE 802.11) сетями кроется только в двух крайних уровнях – физическом и канальном. Остальные же работают абсолютно одинаково и не имеют никаких различий.

Рассмотрим все уровни модели ISO/OSI подробнее.

Физический уровень

Физический уровень – самый первый, «нижний» уровень. Фактически он представляет собой аппаратную часть сети и описывает способ передачи данных, используя для этого любой имеющийся канал – проводной или беспроводной. Исходя из выбранного канала передачи данных должно использоваться соответствующее сетевое оборудование с определенными параметрами передачи данных, учитывающими всевозможные особенности канала, такие как полосы пропускания, защита от помех, уровень сигнала, кодирование, скорость передачи данных в физической среде и т. п.

Таким образом, всю описанную работу вынуждено выполнять сетевое оборудование: сетевая карта, мост, маршрутизатор и т. д.

Физический уровень – один из уровней, который отличает беспроводные сети от их «собратьев» – проводных сетей. Разница между ними заключается в канале передачи данных: в первом случае это радиоволны определенной частоты или инфракрасное излучение, в другом – любая физическая линия, например коаксиал, витая пара или оптоволокно.

Канальный уровень

Главная его задача – удостовериться, что канал свободен и ничто не станет угрожать надежности передачи и целостности пакетов. В идеале протоколы канального уровня в паре с сетевым оборудованием должны проверить, является ли канал свободным для передачи данных, не имеется ли коллизий и т. п.

Такую проверку необходимо проводить каждый раз, поскольку локальная сеть редко состоит всего из двух компьютеров, хотя даже в этом случае канал может быть занят. Обнаружив, что канал свободен, данные, которые необходимо передать другому компьютеру, делятся на более мелкие части – кадры. Каждый такой кадр снабжается контрольной суммой и отправляется. Приняв этот кадр, получатель проверяет контрольные суммы и, если они совпадают, принимает его и отправляет подтверждение о доставке. В противном случае кадр игнорируется, фиксируется ошибка, которая отправляется получателю, и кадр передается заново. Так, кадр за кадром, происходит передача всего объема данных.

Канальный уровень также описывает алгоритмы работы в конкретной физической среде, например при использовании витой пары или оптоволокна. Сюда же включаются и правила прокладки кабеля.

Как и в случае с физическим уровнем, канальный также имеет различия для проводных и беспроводных сетей. Связано это со спецификой сетевого оборудования. Так, беспроводное оборудование на данный момент работает только в полудуплексном режиме, а это означает, что одновременно может вестись только прием или только передача. Этот факт резко снижает эффективность обнаружения коллизий и, соответственно, скорость передачи данных в беспроводных сетях.

Поскольку модель ISO/OSI жестко регламентирует действия каждого уровня, то разработчикам пришлось немного модернизировать протоколы канального уровня для работы в беспроводных сетях. В частности, в случае беспроводной передачи данных используются протоколы CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) или DCF (Distributed Coordination Function).

Протокол CSMA/CA характеризуется тем, что избегает коллизий при передаче данных, используя явное подтверждение доставки, которое говорит о том, что пакет доставлен и он не поврежден.

Работает это следующим образом. Когда один компьютер собирается передать данные другому, то всем станциям сети посылается короткое сообщение (ready to send, RTS), содержащее в себе информацию о получателе и времени, необходимом для передачи данных. Получив такой пакет, все компьютеры прекращают передачу данных на указанное время. Получатель отправляет отправителю сообщение о готовности приема данных (clear to send, CTS). Получив его, компьютер-отправитель высылает первую порцию данных и ждет подтверждения доставки пакета. После подтверждения доставки передача данных продолжается. Если же подтверждение не пришло, компьютер-отправитель повторно передает конкретный пакет.

Это гарантирует доставку пакетов данных, но в то же время заметно снижает скорость передачи данных. Именно поэтому беспроводные сети всегда были медленнее проводных и таковыми останутся надолго, если не навсегда. Чтобы хоть как-то повысить скорость, один из протоколов канального уровня производит фрагментацию (разделение на фрагменты) пакетов, что увеличивает шанс их передачи с удачным исходом, исключая повторную пересылку.

Сетевой уровень

Как и канальный, сетевой уровень занимается передачей информации. Однако между ними есть существенная разница: канальный уровень может передавать данные между компьютерами, которые подключены с использованием одной топологии. Если сеть является комбинированной, за работу принимается сетевой уровень.

Данные в сетевом уровне делятся на порции, которые называются пакетами. Перед тем как начать передачу данных другому компьютеру, происходит преждевременная настройка связи, заключающаяся в выборе пути, по которому будут передаваться данные. Этот процесс называется *маршрутизацией*. Выбор нужного маршрута – одна из основных функций сетевого

уровня. Невозможно выбрать идеальный путь, поскольку рано или поздно на одном из отрезков может повыситься трафик, что приведет к увеличению времени передачи пакетов. Поэтому нужный путь выбирается по среднему значению всех необходимых параметров: пропускной способности, интенсивности трафика, дальности и скорости передачи, ее надежности и т. п.

Как правило, при выборе маршрута используются маршрутизаторы. В их таблицах хранится информация о скорости передачи между отдельными отрезками сети, трафике, среднем времени передачи и т. д., основываясь на которой протоколы сетевого уровня могут выбрать оптимальный путь прохождения данных.

Организация сетевого уровня может осуществляться как программно, так и аппаратно.

Транспортный уровень

Идеальную сеть создать невозможно – хоть где-то, но произойдет отклонение от требований ее построения. Если сеть достаточно большая и включает несколько маршрутизаторов, то это не только усложняет ее, но и приводит к ее ненадежности.

Основная задача транспортного уровня – обеспечить требуемую степень надежности при передаче информации между выбранными компьютерами. Транспортный уровень может делать это пятью способами. Каждый из них отличается не только защищенностью данных при пересылке, но и временем их доставки или возможностью исправления возникающих ошибок. Поэтому, начиная с данного уровня, выбор варианта доставки может производить программа, то есть непосредственно пользователь. Зачем назначать максимальные предосторожности перед отправкой и во время передачи данных, если сеть характеризуется хорошим качеством и низкой вероятностью появления ошибок? Логично выбрать наиболее простой способ из пяти существующих. И наоборот, если в сети часто происходят коллизии, которые приводят к потере информации, следует использовать способ, который гарантирует вам доставку данных в любом случае.

Транспортным уровнем можно управлять программно, а не только аппаратными средствами.

Сеансовый уровень

Сеансовый уровень контролирует передачу пакетов между компьютерами. Осуществляя синхронизацию принятых и отправленных пакетов, протоколы сеансового уровня отслеживают недостающие и передают их заново. За счет того что передаются только недостающие пакеты, достигается повышение скорости.

Уровень представления данных

Чтобы урегулировать процессы отправки и получения информации между двумя компьютерами, существует уровень представления, который приводит ее к единому синтаксическому стандарту, поэтому именно здесь эффективно использовать разнообразные методы шифрования данных, чем и занимаются многие протоколы.

Прикладной уровень

Этот уровень отвечает за связь с прикладными программами. Он представляет собой обычный набор протоколов, с помощью которых можно осуществлять доступ к любым ресурсам сети.

Таким образом, пройдя все семь уровней, сообщение пользователя пополняется служебной информацией (заголовками) каждого из них. Аналогично, попав к нужному получателю и опять пройдя все семь уровней, информация очищается от всей служебной информации.

3.2. Сетевой протокол

В предыдущем разделе была кратко рассмотрена модель ISO/OSI, которая описывает работу любого сетевого оборудования и сети в целом. Однако это всего лишь модель, рисунок на бумаге. Чтобы все это начало работать, необходим механизм, ее реализующий. Таким механизмом является протокол передачи данных, а если точнее, множество протоколов.

Таким образом, *протокол* – набор правил, использование которых делает возможной передачу данных между компьютерами. Все эти правила работают в рамках модели ISO/OSI и не могут отступать от нее ни на шаг, поскольку это может повлечь за собой несовместимость оборудования и программного обеспечения.

Поскольку каждый из уровней модели ISO/OSI обладает своими особенностями, то реализация всех этих особенностей невозможна в рамках одного протокола. Мало того, она даже невыгодна, поскольку значительную часть логики можно разрабатывать на уровне аппаратного обеспечения, что приводит к максимально быстрой обработке данных. Исходя из этих соображений было разработано множество узконаправленных протоколов, каждый из которых выполняет свою задачу и делает это с максимальной отдачей и быстродействием.

Все протоколы можно разделить на низкоуровневые и высокоуровневые.

Низкоуровневые реализованы давно, и никаких кардинальных изменений в них не вносятся, что за длительное время их использования позволило найти и устранить все возможные дыры и ошибки в их работе.

Примечание

Низкоуровневые протоколы реализуются на аппаратном уровне, что позволяет добиться максимального быстродействия и безошибочности.

Что касается *высокоуровневых* протоколов, то их разрабатывают и совершенствуют постоянно. В этом нет ничего плохого, даже наоборот: всегда существует возможность придумать новый, более эффективный способ передачи данных.

Примечание

Как правило, высокоуровневые протоколы реализуются в виде драйверов к сетевому оборудованию для разных операционных систем.

Существует множество разных протоколов, каждый из которых имеет свои особенности. Одни из них узконаправленные, другие имеют более широкое применение. Разрабатываются несколькими фирмами, поэтому неудивительно, что каждая из них создает свой собственный стек (набор) протоколов. Хотя эти стеки по умолчанию между собой несовместимы, существуют дополнительные протоколы, являющиеся мостами между ними, что позволяет использовать в одной операционной системе несколько несовместимых между собой протоколов.

Следует также упомянуть тот факт, что не все протоколы могут применяться в одинаковых условиях. Бывает, применение одного из них выгодно для небольшой группы компьютеров одноранговой сети и крайне невыгодно для большого количества машин сети на основе сервера с несколькими маршрутизаторами и общим выходом в Интернет.

Наибольшую популярность приобрели такие стеки протоколов, как NetBIOS/ NetBEUI, IPX/SPX, TCP/IP и др. Более подробно познакомиться с их возможностями вы сможете ниже.

Протокол NetBIOS

NetBIOS (Network Basic Input/Output System) – один из первых сетевых протоколов, разработанный в 1984 году с целью создания интерфейса передачи сообщений по локальной сети, как одноранговой, так и на основе сервера.

Для передачи сообщений по сети NetBIOS используются логические имена компьютеров. Когда компьютер заходит в сеть, он не только сообщает об этом всем остальным, но и заносит имена всех подключенных к сети компьютеров в свою динамическую таблицу.

В силу своей простоты NetBIOS является одним из самых быстрых протоколов, и это его сильная сторона.

На самом деле NetBIOS не является полноценным протоколом, поскольку описывает только программную часть передачи данных – набор сетевых API-функций. Это означает, что, используя его, можно только подготовить данные для передачи. Физическая же передача осуществляется только с помощью любого транспортного протокола. В частности, обычно в паре с протоколом NetBIOS используется транспортный протокол NetBEUI.

Плюсом этой технологии является непривязанность к транспортному протоколу, что позволяет использовать любой другой подходящий для этих целей протокол. Кроме того, неоспоримым достоинством является его быстрое действие.

Недостаток же заключается в том, что для полноценной работы NetBIOS требуется, чтобы на всех компьютерах сети стоял одинаковый транспортный протокол, иначе машины не смогут синхронизироваться. Еще один минус протокола – отсутствие поддержки маршрутизации, без которой не обходится любая сеть сложной топологии. Именно поэтому протокол NetBIOS, как правило, находит свое применение только в сетях малого размера, обычно в одноранговых.

Протокол NetBEUI

NetBEUI (NetBIOS Extended User Interface) – транспортный протокол, «брат» NetBIOS, его расширение. Однако он обладает большей надежностью доставки сообщений и устойчивостью к ошибкам. Достигается все это путем подтверждающих пакетов, каждый раз присылаемых в ответ на полученное сообщение. Кроме того, до начала передачи устанавливается логическая связь между компьютером-отправителем и компьютером-получателем, что уже гарантирует доставку пакетов.

Еще один механизм, обеспечивающий надежность передачи данных, – механизм, отслеживающий время «жизни» пакета (TTL). Если по истечении этого времени компьютер-получатель не пришлет подтверждение о доставке очередного пакета данных, компьютер-отправитель отправляет порцию данных повторно. Аналогично повторная передача происходит и в случае, если пакет оказался поврежденным и компьютер-получатель его отклоняет, о чем и сообщает компьютеру-отправителю.

Так же как и NetBIOS, NetBEUI не поддерживает маршрутизацию в сети, что не позволяет эффективно использовать его скорость и применять в глобальных сетях. Тем не менее этот протокол является одним из основных компонентов NT-систем и его установка происходит автоматически.

Протокол IPX/SPX

IPX и SPX являются представителями стека протоколов, разработанных компанией Novell, которая в свое время являлась прямым конкурентом Microsoft. Конкуренция велась в области сетевых операционных систем: с одной стороны стояла операционная система Novell Netware, с другой – Windows NT. Соответственно каждая из этих систем использовала свой набор протоколов.

К сожалению, со временем Novell сдала свои позиции и первенство завоевали сетевые версии операционных систем Windows NT. Тем не менее разработанные Novell протоколы используются до сих пор и будут использоваться еще очень долго.

IPX/SPX представляет собой набор подпротоколов, каждый из которых может выполнять возложенную на него задачу на высоком уровне (рис. 3.2). Два нижних уровня (физический и сетевой) реализуют стандартные протоколы Ethernet.

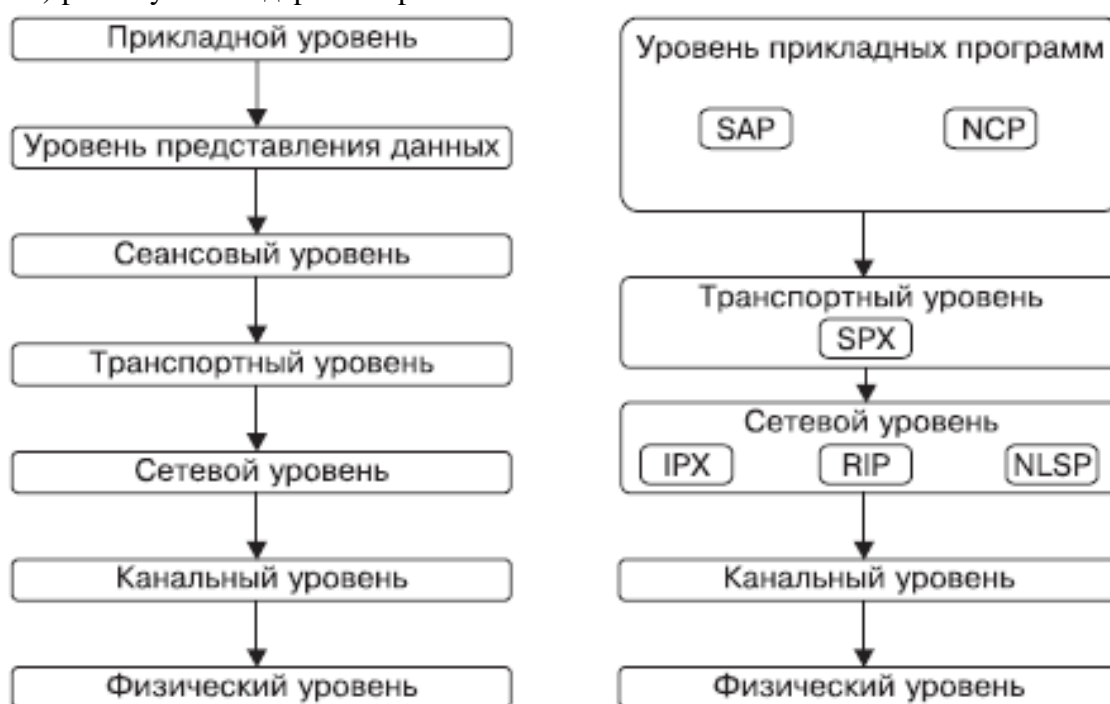


Рис. 3.2. Распределение протоколов стека IPX/SPX по уровням модели ISO/OSI

Ниже описаны только некоторые из протоколов, входящих в состав стека протоколов IPX/SPX.

IPX (Internetwork Packet Exchange) – отвечает за работу сетевого уровня. Его основные функции – вычисление адресов компьютеров сети и организация маршрутизации между двумя wybranнми машинами. Анализируя данные других протоколов, IPX составляет наиболее эффективный путь маршрутизации. После этого пакет данных (датаграмма¹) с добавленной информацией об адресе получателя и отправителя идет по выбранному маршруту. К сожалению, этот протокол самостоятельно работать не может, поскольку не устанавливает соединение между компьютерами. Без этого нельзя ожидать от него надежной доставки пакетов.

SPX (Sequenced Packet Exchange) – протокол транспортного уровня. Он отвечает за установку соединения между wybranнми компьютерами и передает сообщения – датаграммы.

¹ В работе протокол использует понятие «датаграмма» – пакет данных, снабженный служебной информацией о получателе и отправителе.

SAP (Service Advertising Protocol) – отвечает за работу сразу трех уровней: прикладного, представления и сеансового. Однако одна из основных его функций – рассылка сообщений о доступных сервисах. Благодаря этому все сетевые устройства знают об имеющихся сетевых сервисах. SAP – очень мощное средство организации службы поддержки, однако это и является его основным недостатком. Поскольку любое сетевое устройство постоянно посылает о себе информацию, это приводит к повышению трафика сети и соответственно снижению ее эффективности. Для уменьшения засорения сети используют возможности маршрутизаторов, которые позволяют фильтровать «чужие» SAP-сообщения.

NCP (NetWare Core Protocol) – протокол верхнего (прикладного) уровня. Он отвечает за взаимодействие сервера операционной системы Novell NetWare и рабочей станции. С его помощью пользователь видит любую нужную информацию о ресурсах сети, открывает, изменяет и сохраняет файлы, меняет их атрибуты, удаляет, копирует и т. д.

Протокол TCP/IP

TCP/IP – самый распространенный протокол транспортного уровня как в локальных, так и в глобальных сетях. В свое время он был разработан Министерством обороны США, что уже говорит о его надежности.

Протокол TCP/IP имеет открытый интерфейс. Это означает, что вся информация об этом протоколе открыта и любой может использовать ее по своему желанию и назначению.

На самом деле TCP/IP состоит из нескольких протоколов.

Как вы уже заметили, в его названии есть разделитель, то есть он состоит из названий двух протоколов. Первый из них – TCP (Transmission Control Protocol), второй – IP (Internet Protocol). Это говорит о том, что в нем участвует по меньшей мере два протокола (рис. 3.3).



Рис. 3.3. Распределение протоколов стека TCP/IP по уровням модели ISO/OSI

На самом деле в стеке TCP/IP участвует намного больше протоколов. Это связано с тем, что каждый из них предназначен для выполнения определенных задач. Как известно, лучше иметь несколько механизмов, работа которых отлажена до мелочей, нежели один большой, но вызывающий неполадки.

Ниже описаны некоторые протоколы, входящие в стек TCP/IP.

TCP (Transmission Control Protocol) осуществляет обмен данными между двумя компьютерами с предварительно установленной логической связью. Он постоянно используется в Интернете, поскольку надежность соединения и универсальность в этом случае играют очень большую роль. Кроме того, TCP обеспечивает надежность доставки сообщений, принимая подтверждение доставки каждой его порции путем подтверждающих пакетов, каждый раз присылаемых в ответ на полученное сообщение. При этом в самом начале устанавливается логическая связь между компьютером-отправителем и компьютером-получателем, что уже гарантирует доставку пакетов.

UDP (User Datagram Protocol) – при использовании этого протокола не нужно иметь установленное логическое соединение двух компьютеров. Когда передаются данные другому компьютеру, предполагается, что он где-то есть, то есть подключен к сети. В этом случае нет никакой гарантии, что обмен данными произойдет. При этом к отсылаемому пакету просто добавляется IP-адрес машины, которой нужно отослать сообщение. Если сообщение принято, присылается подтверждение об этом, иначе отсылка данных повторяется через некоторый промежуток времени. Как ни странно, протокол UDP применяется в сети достаточно часто. Благодарить за это нужно скорость его работы, которая достигается за счет того, что не устанавливаются соединения с другими компьютерами, а это позволяет использовать трафик в нужном направлении. Так, данный протокол часто используют в сетевых играх, для передачи звуковых данных интернет-радио и в других случаях, где надежность доставки пакетов не играет большой роли.

IP (Internet Protocol) – протокол более высокого уровня, чем TCP и UDP. Он используется непосредственно для передачи данных по ранее установленному (или не установленному) соединению и имеет механизмы маршрутизации. Пользуясь информацией о маршрутизации между выбранными компьютерами, он просто добавляет адрес отправителя и получателя к пакету и отправляет его дальше. Наиболее востребованной функцией протокола является разбивка большого пакета на более мелкие на одном компьютере и соответственно соединение всех частей на другом. Это значит, что IP не контролирует доставку сообщений конечному адресату. IP-адреса машины-отправителя и машины-получателя включаются в заголовок датаграммы и используются для ее передачи между шлюзами. При этом информация о маршрутизации, находящаяся на шлюзе, указывает, куда передавать датаграмму на каждом этапе.

ICMP (Internet Control Message Protocol) контролирует протокол IP, отслеживает любые изменения, влияющие на процесс маршрутизации. При возникновении каких-либо ошибок об этом узнают и отправитель, и получатель. При этом в сообщении указывается причина сбоя.

RIP (Routing Information Protocol) – «родной брат» протокола IP. Они оба связаны с маршрутизацией. Тем не менее протокол RIP отвечает за выбор наилучшего маршрута доставки данных.

ARP (Address Resolution Protocol) – работает с адресами компьютеров, то есть определяет фактический адрес машины, расположенной в той или иной ветке сети. Например, если нужно узнать физический адрес в сети Ethernet, имея при этом IP-адрес, ARP конвертирует 32-битный IP-адрес в 48-битный Ethernet-адрес.

DNS (Domain Name System) – важнейший протокол, который позволяет определять адрес компьютера, ориентируясь на его логическое имя.

RARP (Reverse Address Resolution Protocol) – протокол, определяющий адрес компьютера в сети. Работает аналогично протоколу ARP, однако конвертирование происходит в обратном порядке, то есть 48-битный Ethernet-адрес конвертируется в 32-битный IP-адрес.

BOOTP (Boot Protocol) – относится к прикладному уровню. С его помощью можно запустить сетевой компьютер, используя данные о загрузке с сервера.

FTP (File Transfer Protocol) – протокол, который позволяет загружать файлы с одного компьютера на другой. Именно его вы используете каждый раз, когда пытаетесь выгрузить или загрузить файл с FTP-сервера в Интернет.

TELNET – используется для связи между двумя компьютерами с целью управления одним из них. Протокол очень эффективен в действии и позволяет связывать любые два компьютера, где бы они ни находились.

Кроме описанных, существует набор протоколов, отвечающих за разные аспекты функционирования сети, в частности администрирование, работу с электронной почтой и т. п.

Имея в составе мощный набор вспомогательных протоколов, TCP/IP не зря так популярен. К тому же сегодня это единственный эффективный протокол, который используется для работы в Интернете.

3.3. Протоколы работы с электронной почтой

Без этих протоколов невозможна работа электронной почты. Что такое электронная почта и как без нее плохо, объяснять, пожалуй, не нужно.

Особенностью этих протоколов является их узкая направленность – использование для других целей принципиально невозможно, да и не имеет смысла. Их задача – организация обмена электронными сообщениями.

Еще одной особенностью почтовых протоколов является однозадачность: например, протокол, умеющий отсылать сообщения, не умеет их принимать, и наоборот. Именно поэтому такие протоколы работают парами.

SMTP (Simple Message Transfer Protocol) – почтовый протокол для передачи электронных сообщений. Он накапливает письма и рассылает их по тем адресам, которые указаны в заголовках.

Благодаря своей простоте² и возможностям, SMTP завоевал достойное место под солнцем. Есть, конечно, и недостатки, основной из которых – отсутствие механизма аутентификации входящих соединений и шифрования передачи данных между серверами.

SMTP рассчитан на передачу только текстовой информации, поэтому для отсылки файлов разработан стандарт UUENCODE. Благодаря этому дополнению также появляется возможность использовать разную кодировку писем. Однако и UUENCODE не является полноценным дополнением, поскольку при кодировании файла в текстовый формат теряется информативность, то есть его эмоциональный характер, формат и т. п.

Поэтому вместе с SMTP работает еще одно расширение почты – MIME (Multipurpose Internet Mail Extension), выполняющее больше функций.

Достоинством протокола SMTP является возможность отправлять сообщения с любым форматом вложения, будь то простой текстовый файл или файл с любимой песней. Однако у всего есть свои недостатки – сообщение, прошедшее через кодировку UUENCODE, увеличивается в размере в среднем на 30 %.

² Именно так переводится с английского полное название протокола – «простой протокол передачи сообщений».

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.