

А. Ватаманюк

на 100%

# СОЗДАНИЕ, ОБСЛУЖИВАНИЕ И АДМИНИСТРИРОВАНИЕ СЕТЕЙ



Освойте на 100 %:

- основные подходы к проектированию и созданию сетей различных типов
- способы обслуживания сетей
- правила настройки и администрирования сетей

# **Александр Иванович Ватаманюк**

## **Создание, обслуживание и администрирование сетей на 100%**

*[http://www.litres.ru/pages/biblio\\_book/?art=425142](http://www.litres.ru/pages/biblio_book/?art=425142)*

*А. Ватаманюк. Создание, обслуживание и администрирование сетей на 100%: Питер; Санкт-Петербург; 2010  
ISBN 978-5-49807-702-4*

### **Аннотация**

Что такое компьютерные сети? Всего-навсего несколько компьютеров и соединяющие их провода? И да, и нет. Причем «нет» прежде всего потому, что устройство и механизм работы каждой сети уникальны и далеко не так просты, как может показаться рядовому пользователю. Данная книга содержит всю необходимую информацию о проектировании и создании сетей различных типов и режимах их работы, а также обо всех тонкостях обслуживания и администрирования сетей. Освойте организацию сетей на 100% с помощью этого максимально подробного и доступного практического руководства. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Информация, содержащаяся в данной книге, получена

из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

# Содержание

Введение	6
От издательства	8
Часть 1	9
Глава 1	10
Одноранговая сеть	11
Сеть на основе сервера	14
Глава 2	21
Топология «шина»	22
Топология «кольцо»	24
Топология «звезда»	26
Глава 3	29
Физический уровень	32
Канальный уровень	33
Сетевой уровень	35
Транспортный уровень	36
Сеансовый уровень	37
Уровень представления данных	38
Прикладной уровень	38
Глава 4	40
Понятие протокола	40
Основные протоколы	42
Стеки протоколов	43
Привязка	44

TCP/IP	45
IPX/SPX	47
NetBIOS/SMB	47
Конец ознакомительного фрагмента.	49

# **Ватаманюк Александр Иванович Создание, обслуживание и администрирование сетей на 100%**

## **Введение**

Компьютер уже давно стал неотъемлемой частью жизни людей. Он помогает решать множество вопросов. Практически в любой отрасли деятельности человека используются компьютеры. Образовательные программы, медицинское обслуживание, промышленные процессы – везде применяются компьютеры. На сегодня компьютеризация достигла такого уровня, что обойтись без них никак нельзя.

Отдельная эра в истории развития компьютеров началась с появлением локальных сетей, которые позволяют объединять компьютеры между собой. Именно локальная сеть подняла функциональность компьютера на невиданную до сих пор высоту. Даже один компьютер способен выполнять огромное количество операций, тем самым позволяя обра-

батывать большое количество данных и выдавать требуемый результат. А представьте себе, что можно сделать с помощью тысячи компьютеров, объединенных в одну сеть! Это дает возможности для выполнения таких заданий, на решение которых раньше уходили годы и были задействованы тысячи людей. Даже если не «копать» так глубоко, преимущества использования локальных сетей очевидны: общее использование ресурсов, баз данных, общение, Интернет и многое другое.

Сегодня существует большое количество способов объединения компьютеров в локальную сеть. Разного размера проводные и беспроводные локальные сети сотнями появляются каждый день. При этом если большие корпоративные сети требуют соответствующих знаний и уровня подготовки для их создания, то небольшие офисные и тем более домашние сети могут создавать простые пользователи. Главное при этом – достаточный уровень знаний и желание добиться результата.

Что касается желания, то это зависит только от вас. А вот в первом вопросе вам поможет книга, которую вы держите в руках. В ней собрано все необходимое для того, чтобы изучить принцип функционирования сетей и применить эти знания на практике. Дело остается только за малым: требуется ваше желание.

# От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу электронной почты [gromakovski@minsk.piter.com](mailto:gromakovski@minsk.piter.com) (издательство «Питер», компьютерная редакция).

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



# Часть 1

## Теоретические сведения о сетях

- Основные типы сетей
- Топология и режимы работы сети
- Модель ISO/OSI
- Протоколы передачи данных
- Среда передачи данных
- Методы доступа к передающей среде
- Понятие сетевого стандарта
- Особенности функционирования беспроводных сетей
- Стандарты IEEE 802.3
- Стандарты IEEE802.11
- Спецификации Bluetooth
- Спецификации HomePNA
- Спецификации HomePlug
- Механизмы и особенности управления сетью
- Сетевое оборудование

# Глава 1

## Основные типы сетей

- ☐ Одноранговая сеть
- ☐ Сеть на основе сервера

Появление компьютерных сетей было логичным шагом в истории компьютеризации общества. Благодаря этому шагу компьютеры получили еще большее распространение, а самое главное – практически в каждый дом пришел Интернет, предоставляющий доступ к практически неограниченным источникам информации.

Компьютерные сети прошли долгий этап развития. В результате на сегодня компьютеры можно объединить как в локальном, так и в глобальном масштабе.

Итак, существует два варианта сетей – локальные и глобальные. Принцип объединения в них компьютеров и работы в этих сетях практически идентичен, но масштабы сети накладывают свои ограничения и требования.

**Локальная сеть**, LAN (Local Area Networks) – сеть, с помощью которой компьютеры объединяются на ограниченной территории. Такой вариант сети встречается в офисах, на предприятиях, в залах ожидания аэропортов, вокзалов, в кафе, ресторанах и т. д. Главное ее предназначение – организация доступа к общим ресурсам внутри сети. При этом локальная сеть часто имеет подключение к Интернету, что

делает ее частью глобальной сети.

**Глобальная сеть**, WAN (Wide Area Networks) – разновидность сети, которая, согласно существующим легендам, образовалась из локальной сети достаточно больших масштабов. В результате появилась Всемирная паутина, она же Интернет.

Наиболее важным понятием, характеризующим сеть, является ее тип. Именно от типа сети зависят ее возможности, безопасность, управляемость и, самое главное, – доступ к важным данным.

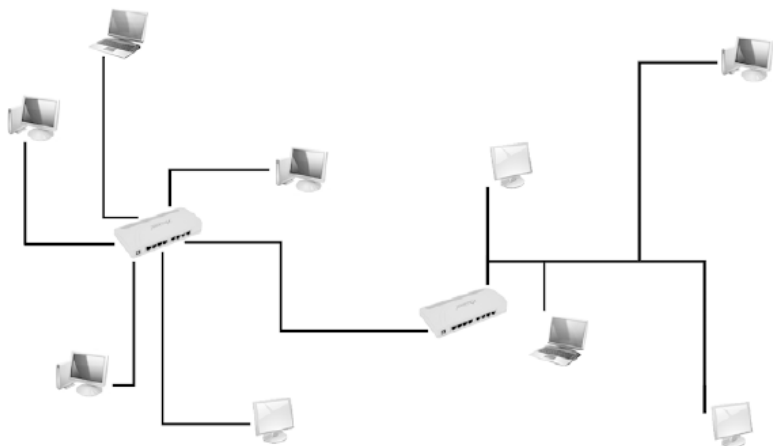
Различают два типа сетей – одноранговую и сеть на основе сервера. Сети обеих разновидностей выполняют поставленные перед ними задачи, но делают это по-разному, в чем вы сможете убедиться далее.

## **Одноранговая сеть**

Одноранговая сеть (рис. 1.1) является наиболее простой и дешевой в создании. Тем не менее она способна обеспечить своих пользователей всем необходимым для получения доступа к нужной информации, в том числе и к Интернету.

Главной особенностью такой сети является то, что каждый участник сети – рабочая станция – имеет одинаковые права и выступает в роли администратора своего компьютера. Это означает, что только он может контролировать доступ к своему компьютеру и только он может создавать об-

щие ресурсы и определять правила доступа к ним. С одной стороны, это делает сеть очень простой в создании, но с другой – администрирование такой сети вызывает достаточно много проблем, особенно если количество участников сети превышает 25–30.



**Рис. 1.1.** Пример одноранговой сети

Одноранговые сети находят свое применение в небольших офисах, ресторанах и кафе, залах ожидания, то есть в тех местах, которые позволяют поддерживать работу сети с небольшим количеством подключений. Однако, хотя это и противоречит всем принципам, одноранговые сети также используются в так называемых домашних сетях, количество

подключений к которым может быть очень большим, например 1000 и более компьютеров. Главное объяснение этому факту – хаотичный способ создания сети, который к тому же, как правило, не требует больших финансовых вложений.

Одноранговая сеть является крайне неуправляемой с точки зрения системного администратора, и чем больше участников сети, тем более этот факт заметен. Например, чтобы ограничить работу пользователя с теми или иными устройствами, потребуется выполнить определенные настройки операционной системы. Сделать это централизованно невозможно, поэтому требуется личное присутствие администратора возле каждого компьютера либо применение программ удаленного управления компьютером. Это же касается обновления антивирусных баз, установки обновлений операционной системы и офисных программ и т. д.

Учитывая изложенные факты, а также практику работы одноранговых сетей, ее использование можно считать оправданным только в случае, если количество узлов сети достаточно мало и все они расположены на небольшой территории, например в пределах одного или нескольких офисов.

Поддержка одноранговых сетей имеется в любой современной операционной системе семейства Microsoft Windows. По этой причине для организации такой сети никакого дополнительного программного обеспечения не требуется.

**Внимание**

В одноранговой сети доступ к общему ресурсу одновременно могут получить только 10 участников сети. Если для вас важен этот момент, то вам следует установить серверную операционную систему.

В табл. 1.1 приведены основные преимущества и недостатки одноранговой сети, на которые обязательно стоит обратить внимание, прежде чем выбрать тип будущей локальной сети.

**Таблица 1.1. Особенности одноранговых сетей**

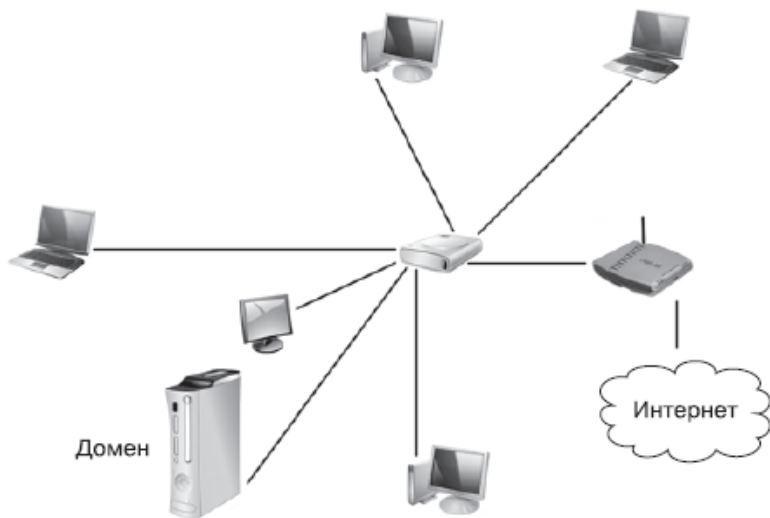
Преимущества сети	Недостатки сети
Простая и дешевая в создании	Отсутствует централизованное хранилище ресурсов
Не требует управляющих компьютеров	Отсутствует возможность административного управления пользователями и ресурсами
Работа сети не зависит от работоспособности отдельных узлов	Каждый пользователь должен самостоятельно следить за состоянием программного обеспечения
	За обновление антивирусных баз (и другого программного обеспечения) отвечает пользователь
	Низкий уровень защиты информации

## Сеть на основе сервера

Сеть на основе сервера (рис. 1.2), или, как ее еще часто называют, сеть типа «клиент – сервер», – наиболее востребованный тип сети, основными показателями которой являются высокие скорость передачи данных и уровень безопас-

ности.

Под словом «сервер» следует понимать выделенный компьютер, на котором установлена система управления пользователями и ресурсами сети. Данный компьютер в идеале должен отвечать только за обслуживание сети, и никакие другие задачи выполнять на нем не следует. Этот сервер называется *контроллер домена*. Он является наиболее важным объектом сети, поскольку от него зависит работоспособность всей сети. Именно поэтому данный сервер обязательно подключают к системе бесперебойного питания. Кроме того, в сети, как правило, присутствует дублирующий сервер, который называется вторичный контроллер домена.



## **Рис. 1.2.** Пример сети с управляющим сервером

Кроме контроллера домена в сети могут использоваться и другие серверы разного назначения, к числу которых относятся следующие.

□ **Файл-сервер.** Данный сервер представляет собой хранилище файлов разного типа. На нем, как правило, хранятся файлы пользователей, общие файловые ресурсы, аудио- и видеофайлы и многое другое. Главное требование к файловому серверу – надежная дисковая подсистема, которая может обеспечивать безопасное хранение файлов и доступ к ним в любое время суток. Часто на данном сервере устанавливается архивирующая система, например стример, с помощью которого осуществляется плановое создание архивных данных. Это обеспечивает гарантированное восстановление данных пользователей в случае непредвиденных сбоев оборудования.

□ **Сервер базы данных.** Серверы подобного типа наиболее востребованы, поскольку позволяют обеспечить доступ к единой базе данных. В качестве таковой могут выступать базы данных бухгалтерского и другого типа учета, юридическо-правовые базы данных и т. д. В качестве сервера базы данных используются мощные компьютеры с большим объемом оперативной памяти и RAID-массивом из быстрых жестких дисков. Очень важным является факт организации архивирования данных, поскольку от целостности базы дан-



ных и доступа к ней зависит работа всего предприятия.

□ **Сервер приложений.** Сервер приложений используется в качестве промежуточного звена между сервером базы данных и клиентским компьютером. Это позволяет организовать так называемую трехзвенную (или трехуровневую) архитектуру, с помощью которой выполнение программ, требующих обмен с базой данных, происходит максимально быстро и эффективно. Кроме того, за счет такой организации повышается безопасность доступа к данным и увеличивается управляемость процессом, поскольку легче контролировать работу одного компьютера, нежели сотни.

□ **Принт-сервер.** Специальный сервер, позволяющий сделать процесс печати более контролируемым и быстрым. Используется в сетях, которым необходим доступ к общему принтеру. Сервер подобного рода обеспечивает управление очередью печати и доступ к принтеру для клиентов любого типа: при проводном или беспроводном соединении, для переносного устройства или мобильного телефона.

□ **Интернет-шлюз.** Данный сервер позволяет предоставить пользователям локальной сети доступ в Интернет, а также организовать доступ к ресурсам по протоколам FTP и HTTP. Поскольку данный сервер является «окном» во внешнюю сеть, к нему предъявляются определенные требования, среди которых основными являются требования к безопасности локальных данных и защита от доступа к ним извне. Именно поэтому на таком сервере устанавливают различные

сетевые фильтры и брандмауэры, позволяющие эффективно фильтровать входящий и исходящий трафик, что делает использование Интернета более безопасным.

□ **Почтовый сервер.** Практически каждое серьезное предприятие, применяющее для организации обмена данными сеть на основе сервера, для общения с внешним миром пользуется корпоративными электронными ящиками. Этот подход вполне оправдан, поскольку позволяет контролировать входящий и исходящий трафик, тем самым блокируя возможность утечки информации. Подобную систему обмена информацией позволяет реализовать почтовый сервер с соответствующим программным обеспечением. На этот сервер дополнительно устанавливаются разнообразные антиспамовые фильтры, позволяющие бороться (насколько это возможно) со все возрастающим объемом рекламных писем, которые и называются *спамом*.

Кроме упомянутых выше, могут использоваться и другие типы серверов, что зависит только от потребностей сети. Подключение новых серверов не вызывает никаких трудностей, поскольку гибкость и возможности сети на основе сервера позволяют сделать это в любой момент.

С точки зрения системного администратора, сеть на основе сервера хотя и наиболее сложная в создании и обслуживании, но в то же время наиболее управляемая и контролируемая. Благодаря наличию главного компьютера управление учетными записями пользователей происходит очень легко

и, самое главное, – эффективно. Благодаря политикам безопасности также упрощается контроль над самими компьютерами, что делает сеть более управляемой, а данные в ней более защищенными.

На сервер устанавливается серверная операционная система, которая, в отличие от обычной операционной системы, обладает некоторыми преимуществами, например поддержкой нескольких процессоров, большего объема оперативной памяти, инструментами администрирования сети и т. д. К таким операционным системам относятся Windows Server 2003, Windows Server 2008 и т. д.

В табл. 1.2 показаны основные недостатки и преимущества сетей на основе выделенного сервера.

**Таблица 1.2.** Особенности сетей на основе выделенного сервера

Преимущества сети	Недостатки сети
Высокая скорость и производительность сети	Дорогая в создании и обслуживании
Использование выделенных серверов, что облегчает работу с ресурсами и упрощает контроль за их использованием	Постоянная необходимость в системном администраторе
Наличие дублирующих систем, позволяющих защитить данные и сделать доступ к ним бесперебойным	Зависимость сети от работоспособности контроллера домена
Централизованные обновления операционной системы и программного обеспечения	
Полный контроль над пользователями сети	
Высокий уровень безопасности данных	
Продвинутые средства мониторинга работоспособности сети	
Легкая расширяемость сети	

От выбора типа сети зависит ее будущее: расширяемость, возможность использования того или иного программного обеспечения и оборудования, надежность сети и многое другое. В этом плане сеть на основе сервера является наиболее предпочтительной и выгодной.

# Глава 2

## Топология и режимы работы сети

- ☐ Топология «шина»
- ☐ Топология «кольцо»
- ☐ Топология «звезда»

При проектировании и создании сети важное значение имеет способ объединения компьютеров и участников сети. От этого зависит скорость передачи данных, надежность сети, степень устойчивости к поломкам, возможности администрирования и многое другое. Поэтому первым и, пожалуй, самым важным правилом, от которого зависят упомянутые показатели, является топология сети.

Таким образом, *топология сети*, или *сетевая топология*, – это описание схемы сети, включающее в себя способ взаимного расположения компьютеров и их объединения. Кроме того, это описание содержит множество правил, связанных с прокладкой кабеля, подключением оборудования, взаимодействием управляющих устройств и т. д.

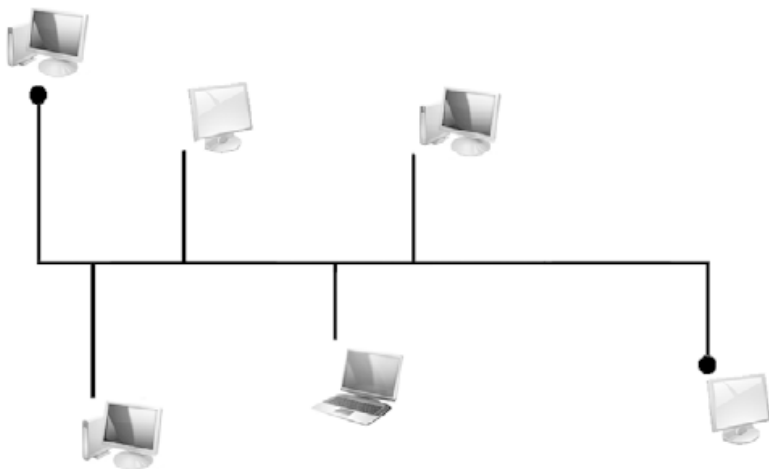
Различают сетевую топологию четырех видов: физическую, логическую, информационную и топологию управления обменом. Однако чаще всего понятие сетевой топологии ассоциируется именно с расположением компьютеров относительно друг друга, то есть с физической топологией.

Существует достаточно много способов объединения

компьютеров, то есть сетевых топологий. К их числу относятся топологии «шина», «звезда», «кольцо», «двойное кольцо», «дерево», «решетка» и др. Наибольшее распространение получили сетевые топологии «шина», «звезда» и «кольцо», поэтому рассмотрим их подробнее.

## Топология «шина»

Согласно топологии «шина», или, как ее еще часто называют, «общая шина», или «магистраль», все участники сети подключаются к центральному кабелю (рис. 2.1).



**Рис. 2.1.** Пример топологии «шина»

Для предотвращения дальнейшего распространения и возможного отражения сигнала на концах кабеля устанавливаются специальные заглушки – терминаторы, один из которых обязательно заземляется.

Данные в такой сети направляются сразу всем компьютерам, поэтому задача каждого компьютера – проверить, кому адресовано сообщение. Только компьютер, которому адресовано сообщение, может обработать его. При этом, пока данные не будут обработаны, никакие сообщения больше не отправляются. Как только данные обработаны, сигнал об этом поступает в сеть, и работа возобновляется.

Главное преимущество такой сети – простота и дешевизна создания. При ее построении используется минимальное количество кабеля и не требуется никакого управляющего оборудования: в обмене данными участвуют только сетевые адаптеры компьютеров. Если количество компьютеров уже достаточно велико, сеть часто разбивается на сегменты, для соединения которых используются повторители – концентраторы, коммутаторы, мосты и т. п.

Главный минус сети – сильная зависимость скорости передачи данных от количества подключенных компьютеров: чем больше компьютеров и других устройств, тем ниже скорость передачи данных. Кроме того, обрыв центрального кабеля парализует работу всей сети.

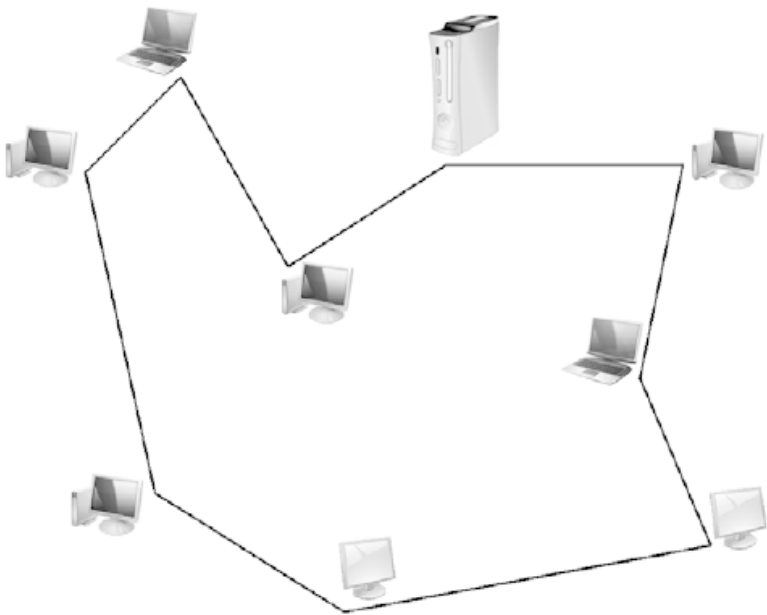
## Топология «кольцо»

Согласно топологии «кольцо» все компьютеры сети подключены последовательно и образуют своего рода замкнутую кольцевую систему (рис. 2.2).

Для передачи данных в сети используется маркерная система, то есть данные в конкретный момент может передавать только один компьютер. Причем данные передаются только следующему по кругу компьютеру (справа налево). Это позволяет избежать коллизий и увеличивает надежность сети в целом.

Когда компьютеру, обладающему маркером, необходимо передать данные, к маркеру добавляется адрес компьютера, которому эти данные предназначены, и маркерный блок отправляется в сеть по кругу. Таким образом, каждый компьютер, который лежит на пути следования маркерного блока, считывает из него адрес получателя и сравнивает его со своим адресом: если адреса не совпадают, они отправляются далее по кругу. Если адреса совпали, то есть отправитель найден, формируется подтверждающий блок и передается далее по кругу к отправителю. В дальнейшем данные уже передаются по найденному пути до тех пор, пока в этом есть необходимость. Как только передача данных заканчивается, маркер освобождается и идет далее по кругу до первого компьютера, которому необходимо передавать данные.





**Рис. 2.2.** Пример топологии «кольцо»

Использование топологии «кольцо» обладает некоторыми преимуществами. Например, каждый компьютер сети одновременно выступает повторителем, поэтому затухание сигнала возможно только между соседними компьютерами, что напрямую зависит от расстояния между ними. Кроме того, сеть способна справляться с очень большими объемами трафика за счет отсутствия коллизий и центрального управления

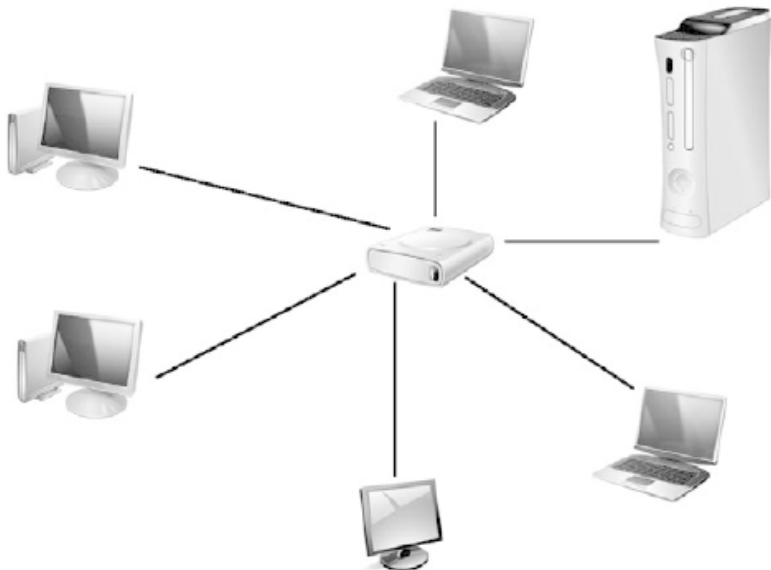
ющего узла.

У данного типа сети есть также и недостатки. Так, подключение нового компьютера требует остановки работы всей сети. Аналогичная ситуация происходит, если один из компьютеров выходит из строя: сеть становится неработоспособной. Кроме того, поиск неисправности в такой сети сопряжен со множеством сложностей.

## **Топология «звезда»**

Топология «звезда» на сегодня является наиболее распространенной. Согласно ей каждый компьютер или устройство сети подключается к центральному узлу, образуя подобным образом один сегмент сети (рис. 2.3).

Сегменты сети могут соединяться между собой одним из доступных способов, например посредством центрального либо промежуточного узла, образуя более сложную сеть или входя в состав комбинированной сети.



**Рис. 2.3.** Пример топологии «звезда»

В качестве центрального узла используется любое активное сетевое устройство с достаточным количеством портов. В самом простом случае в роли центрального узла выступает концентратор, который в силу своих ограничений позволяет передавать данные в конкретный момент только одному компьютеру. При этом поступившие на концентратор данные он сразу пересылает всем подключенным к нему устройствам. Если на концентратор в один момент поступают данные от двух разных отправителей, то оба пакета игнорируются.

В случае с более интеллектуальным узлом, например коммутатором, данные одновременно могут передаваться сразу несколькими компьютерами, что значительно увеличивает скорость обмена данными.

Несмотря на то что «звезда» наиболее дорогостоящая в использовании по сравнению с другими топологиями, благодаря своей надежности и высокой скорости передачи данных она уже практически стала стандартом. Большую роль играет также тот факт, что принятый уже достаточно давно стандарт АТХ подразумевает наличие на материнской плате персонального компьютера интегрированного сетевого адаптера, который изначально предназначен для работы с этой топологией.

# Глава 3

## Модель ISO/OSI

Функционирование сети подчиняется определенным теоретическим правилам. В качестве такой теоретической основы выступает свод правил и стандартов, которые описывают так называемую *модель взаимодействия открытых систем* (Open System Interconnection, OSI). Основным разработчиком модели является Международная организация по стандартизации (International Standards Organization, ISO), поэтому очень часто используется более короткое название – *модель ISO/OSI*.

Согласно модели ISO/OSI существует семь уровней, пройдя через которые, данные от одного компьютера могут быть переданы другому компьютеру, и абсолютно не важно, какая операционная система при этом используется и каким образом данные попадают от источника к адресату.

Уровни имеют названия и расположены в следующем порядке: физический канальный, сетевой, транспортный, сеансовый, уровень представления данных и прикладной уровень. Данные могут передаваться как в указанном, так и в обратном порядке. Так, при передаче данные начинают свое движение с прикладного уровня и доходят до физического уровня, который представляет собой среду передачи данных. Если же данные принимаются, то они проходят путь от фи-

зического до прикладного уровня (рис. 3.1).



**Рис. 3.1.** Схематическое отображение модели ISO/OSI

Описанная модель является стандартом для любой среды передачи данных, которых на сегодня используется три: кабель, радиоволны и инфракрасное излучение. Однако, в зависимости от среды передачи данных, имеются определенные различия в работе физического и канального уровней модели ISO/OSI, в чем вы сможете убедиться далее.

Каждый уровень отвечает только за свою часть подготовки данных к приему или передаче, что в результате позволяет сделать процесс передачи/приема максимально эффективным и, самое главное, независимым от среды передачи

данных, а также обойти вопрос совместимости оборудования, которое используется для этого.

Как уже было упомянуто выше, модель ISO/OSI состоит из семи уровней, а именно:

- *физический* – передача и прием электрических сигналов;

- *канальный* – управление каналом связи и доступом к среде передачи данных;

- *сетевой* – определение оптимальных маршрутов передачи данных;

- *транспортный* – контроль целостности и правильности данных в процессе передачи и приема данных;

- *сеансовый* – создание, сопровождение и поддержание сеанса связи;

- *уровень представления* – кодирование и шифрование данных с помощью требуемых алгоритмов;

- *прикладной* – взаимодействие с клиентскими программами.

Данные между разными уровнями модели передаются посредством стандартных интерфейсов и протоколов передачи данных, главная задача которых – обработка полученных данных и приведение их к тому виду, который необходим для работы следующего уровня. Более подробно о разных протоколах передачи данных вы сможете узнать далее.

# Физический уровень

Физический уровень (Physical Layer) является самым нижним в модели ISO/OSI. Он работает непосредственно с имеющимся каналом связи. Его главная задача – преобразование поступивших от вышестоящего уровня данных и передача соответствующих им электрических сигналов по существующему каналу связи получателю, а также прием данных от отправителя и их конвертация согласно существующим таблицам кодирования сигналов.

Прежде чем начать передачу электрических сигналов, алгоритмы физического уровня определяют тип канала связи и его свойства: электротехнические и механические характеристики, величину напряжений, расстояние между отправителем и получателем, скорость передачи данных и т. д., то есть все, что является критичным для передачи данных. Именно на этом этапе определяется, сеть какого типа используется (проводная или беспроводная), а также выясняется топология сети.

Функции физического уровня выполняют сетевые адаптеры на отправителе и получателе, а также повторители сигнала, например концентратор.

Стандартизация на уровне модели ISO/OSI позволяет использовать в сети оборудование разных производителей, не заботясь при этом об их совместимости, что позволяет со-



средоточиться только на процессе передачи и приема данных.

## Канальный уровень

Задача канального уровня (Data Link Layer) – обеспечение гарантированной передачи данных через физический канал, параметры и особенности которого уже установлены и «приняты во внимание» на физическом уровне. При этом решаются вопросы физической адресации, корректности отправленной и полученной информации, контроля возникающих ошибок, управления потоком информации и т. д.

Данные передаются блоками, которые называются кадрами. К каждому кадру добавляется несколько бит информации о типе кадра, а также контрольная сумма, которая сверяется при его получении адресатом. При несовпадении контрольных сумм запрашивается повторная передача кадра и данные синхронизируются.

Что касается локальных сетей, то за работу канального уровня отвечают два подуровня:

- MAC (Medium Access Control) – уровень доступа к разделяемой среде;
- LLC (Logical Link Control) – уровень управления логическим каналом.

Уровень MAC отвечает за получение доступа к общей среде передачи данных, в связи с чем каждый протокол пе-

редачи данных имеет соответствующую процедуру доступа. Кроме того, MAC отвечает за согласование режимов работы канального и физического уровней (дуплексный и полудуплексный режим соответственно), буферизацию фреймов и т. д.

Уровень LLC имеет три разные процедуры, отвечающие за качество доставки данных.

□ LLC1 – без установления соединения и без подтверждения доставки. Данная процедура управления каналом позволяет передавать данные с максимальной скоростью, для чего используются датаграммы.

□ LLC2 – с установлением соединения и подтверждением доставки. Этот вид управления каналом наиболее надежный. Он позволяет гарантированно доставлять данные и получать подтверждения о доставке. На этом уровне работает система контроля ошибок, которая дает возможность восстанавливать поврежденные блоки данных и упорядочивать их последовательность. Подобная система функционирует благодаря нумерации кадров, что позволяет запрашивать ошибочные кадры и упорядочивать их.

□ LLC3 – без установления соединения, но с подтверждением доставки. Данный тип управления каналом достаточно специфичен и часто используется в процессах, которые требуют быстрой передачи данных, но с подтверждением доставки. Как правило, это необходимо для разного рода процессов, происходящих в режиме реального времени, когда

временные затраты очень критичны. В этом случае передача следующего кадра осуществляется только после подтверждения доставки предыдущего.

Таким образом, LLC-уровень умеет передавать данные либо с помощью датаграмм, либо с использованием процедур с обеспечением качества передачи.

Канальный уровень может реализовываться как на аппаратном уровне (например, с помощью коммутаторов), так и с применением программного обеспечения (допустим, драйвера сетевого адаптера).

## **Сетевой уровень**

Сетевой (Network Layer) – один из важнейших уровней модели взаимодействия открытых систем. Поскольку для построения сети могут использоваться различные технологии и, а сеть может состоять из нескольких сегментов с абсолютно разными сетевыми топологиями, чтобы «подручить» эти сегменты, требуется соответствующий механизм. В качестве такого механизма и выступает сетевой уровень.

Кроме определения физических адресов всех участников сети, данный уровень отвечает за нахождение кратчайших путей доставки данных, то есть выполняет маршрутизацию пакетов. При этом постоянно отслеживается состояние сети и определяются новые маршруты, если возникают «заторы» на пути следования данных. Благодаря маршрутизации дан-

ные всегда доставляются с максимальной скоростью.

Сетевой уровень для доставки данных между разными сетевыми сегментами использует особую адресацию. Так, вместо MAC-адресов применяется пара чисел – номер сети и номер компьютера в этой сети. Использование нумерации позволяет составить точную карту сети независимо от топологии сегментов и определять альтернативные пути передачи данных.

На практике функции сетевого уровня выполняет маршрутизатор.

## **Транспортный уровень**

Транспортный уровень (Transport Layer) служит для организации гарантированной доставки данных, для чего используется подготовленный канал связи. При этом отслеживается правильная последовательность передачи и приема пакетов, восстанавливаются потерянные или отсеиваются дублирующие. При необходимости данные фрагментируются (разбиваются на более мелкие пакеты) или дефрагментируются (объединяются в большой пакет), что повышает надежность доставки данных и их целостность.

На транспортном уровне предусмотрено пять классов сервиса с различными уровнями надежности. Они различаются скоростью, возможностями восстановления данных и т. д. Например, некоторые классы работают без предварительной

установки связи и не гарантируют доставку пакетов в правильной последовательности. В этом случае за выбор маршрута отвечают промежуточные устройства, которые попадают на пути следования данных. Классы с установкой связи начинают свою работу с установки маршрута и только после того, как маршрут будет определен, начинают последовательную передачу данных.

Благодаря такому подходу всегда можно найти компромисс между скоростью и качеством доставки данных.

## **Сеансовый уровень**

Сеансовый уровень (Session Layer) используется для создания и управления сеансом связи на время, необходимое для передачи данных. Время сеанса зависит лишь от объема информации, которая должна быть передана. Поскольку этот объем может быть существенным, используются разные механизмы, контролирующие данный процесс.

Для управления сеансом применяется маркер, обладатель которого гарантирует себе право на связь. Кроме того, используются служебные сообщения, с помощью которых стороны могут, например, договариваться о способе передаче данных или сообщать о завершении передачи данных и освобождении маркера.

Чтобы передача данных была успешной, создаются специальные контрольные точки, которые позволяют начать по-

вторную передачу данных практически с того места, на котором произошел непредвиденный обрыв связи. В данном случае работают также механизмы синхронизации данных, определяются права на передачу данных, поддерживается связь в периоды неактивности и т. п.

## **Уровень представления данных**

Уровень представления данных, или представительский уровень (Representation Layer), является своего рода проходным уровнем, основная задача которого – кодирование и декодирование информации в представление, понятное вышестоящему или нижестоящему уровню. С его помощью обеспечивается совместимость компьютерных систем, использующих разные способы представления данных.

Этот уровень удобен тем, что именно здесь выгодно использовать разные алгоритмы сжатия и шифрования данных, преобразование форматов данных, обрабатывать структуры данных, преобразовывать их в битовые потоки и т. д.

## **Прикладной уровень**

Прикладной уровень (Application Layer) – последний «бастион» между пользователем и сетью. Он обеспечивает связь пользовательских приложений с сетевыми сервисами и службами на всех уровнях модели ISO/OSI, а также переда-

чу служебной информации, синхронизирует взаимодействие прикладных процессов и т. д.

# **Глава 4**

## **Протоколы передачи данных**

- ☐ Понятие протокола
- ☐ Основные протоколы

### **Понятие протокола**

В предыдущей главе мы познакомились с эталонной моделью, описывающей принцип подготовки, приема и передачи данных через любой имеющийся канал связи. Каждый из ее семи уровней решает поставленную перед ним задачу, выполняя свою функцию в подготовке или обработке данных. Для этого он использует стандартные процедуры межуровневого обмена информацией и протоколы передачи данных. Таким образом, получается, что модель ISO/OSI является теоретической основой функционирования сети, а сетевые протоколы – это то, что превращает теорию в практику.

Протокол передачи данных можно сравнить с набором правил и соглашений, которые описывают способ передачи данных между двумя и более объектами в сети.

Для обслуживания модели взаимодействия открытых систем используется достаточно большое количество сетевых протоколов. Многие из них вполне специфичны и часто выполняют только одно определенное действие, но делают это



быстро и, самое главное, правильно. Существуют также и более продвинутые и функциональные протоколы, которые могут выполнять определенные действия, захватывая сразу несколько уровней модели. Есть даже целые семейства (стеки) протоколов, которые являются составной частью протоколов с общим названием, например стеки протоколов TCP/IP или IPX/SPX.

### **Примечание**

Модель ISO/OSI разрабатывалась тогда, когда уже были разработаны многие протоколы, в частности TCP/IP. Ее главной задачей была стандартизация работы сетей. Однако когда модель была принята окончательно, оказалось, что она имеет довольно много недостатков. В частности, наиболее слабым звеном в модели стал транспортный уровень. По этой причине существует достаточно много протоколов, которые выполняют работу сразу нескольких уровней, что идет вразрез с самой моделью открытых систем.

Различают *низкоуровневые* и *высокоуровневые* протоколы.

Низкоуровневые работают на самых нижних уровнях модели ISO/OSI и, как правило, имеют аппаратную реализацию, что позволяет использовать их в таких сетевых устройствах, как концентраторы, мосты, коммутаторы и т. д.

Высокоуровневые протоколы работают на верхних уровнях модели ISO/OSI и обычно реализуются программным путем. Этот факт позволяет создавать любое количество протоколов разного применения, делая их настолько гибки-

ми, как того требует современная ситуация.

В табл. 4.1 приведены названия некоторых популярных протоколов и их положение в модели взаимодействия открытых систем.

**Таблица 4.1.** Популярные протоколы модели ISO/OSI

Уровни модели ISO/OSI	Протоколы передачи данных
Физический	X.25, RS-232, EIA-422, RS-485, V.21, ZyX, PEP
Канальный	Ethernet, ATM, PPP, PPTP, Frame Relay, FDDI, Token Ring
Сетевой	IPX, IP, ARP, ICMP, DDP
Транспортный	TCP, UDP, SPX, RTCP, RDP, RUDP
Сеансовый	RPC, SSL, WSP
Уровень представления данных	Telnet, FTP, SMTP, SNMP, TDI, XDR, NCP
Прикладной	HTTP, FTP, DHCP, DNS, POP3, SNMP, LDAP, Gopher

## Основные протоколы

Как вы уже могли заметить, количество протоколов, обслуживающих модель взаимодействия открытых систем, достаточно велико. Некоторые из этих протоколов, особенно низкоуровневые, не представляют особого интереса в плане знакомства с их принципом работы. Но принцип работы и возможности других протоколов все же стоит знать, особенно таких, как TCP/IP, UDP, POP3 и др.

# Стеки протоколов

Как уже упоминалось выше, часто за организацию работы всех уровней модели ISO/OSI отвечают стеки протоколов. Плюсом использования стеков протоколов является то, что все протоколы, входящие в стек, разработаны одним производителем, то есть они способны работать максимально быстро и эффективно.

За время существования сетей было разработано несколько различных стеков протоколов, среди которых наиболее популярными являются TCP/IP, IPX/SPX, NetBIOS/SMB, Novell NetWare, DECnet и др.

В составе стеков находятся протоколы, работающие на разных уровнях модели ISO/OSI, однако обычно выделяют только три типа протоколов: *транспортный, сетевой и прикладной*.

Плюсом использования стеков протоколов является то, что протоколы, работающие на нижних уровнях, применяют давно отлаженные и популярные сетевые протоколы, такие как Ethernet, FDDI и т. д. Благодаря аппаратной реализации этих протоколов становится возможным использовать одно и то же оборудование для разных типов сетей и тем самым достигать их совместимости на аппаратном уровне. Что касается высокоуровневых протоколов, то каждый из стеков имеет свои преимущества и недостатки, и очень часто слу-

чается так, что нет жесткой привязки «один протокол – один уровень», то есть один протокол может работать сразу на двух-трех уровнях.

## **Привязка**

Важным моментом в функционировании сетевого оборудования, в частности сетевого адаптера, является привязка протоколов. На практике она позволяет использовать разные стеки протоколов при обслуживании одного сетевого адаптера. Например, можно одновременно использовать стеки TCP/IP и IPX/SPX, и если при попытке установления связи с адресатом с помощью первого стека произошла ошибка, автоматически происходит переключение на использование протокола из следующего стека. В этом случае важным моментом является очередность привязки, поскольку она однозначно влияет на использование того или иного протокола из разных стеков.

Вне зависимости от того, какое количество сетевых адаптеров установлено в компьютере, привязка может осуществляться как «один к нескольким», так и «несколько к одному», то есть один стек протоколов можно привязать сразу к нескольким адаптерам или несколько стеков к одному адаптеру.

# ТСР/ІР

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol) на сегодня является наиболее распространенным и функциональным. Он работает в локальных сетях любых масштабов. Кроме того, это единственный из протоколов, который позволяет работать глобальной сети Интернет.

Протокол был создан в 70-х годах прошлого века управлением Министерства обороны США. Именно с его подачи началась разработка протокола, целью которого было соединение любых двух компьютеров, как бы далеко они ни находились. Конечно, они преследовали свою цель – обеспечить постоянную связь с центром управления, даже если все вокруг будет разрушено в результате военных действий. В итоге была образована глобальная сеть ARPAnet, которую министерство активно использовало в своих целях.

Толчком к дальнейшему усовершенствованию и широкому распространению стека TCP/IP стал тот факт, что его поддержка была реализована в компьютерах с операционной системой UNIX. В результате популярность протокола TCP/IP возросла.

В стек протоколов TCP/IP входит достаточно много протоколов, работающих на различных уровнях, но свое название он получил благодаря двум протоколам – TCP и IP.

TCP (Transmission Control Protocol) – транспортный протокол, предназначенный для управлением передачей данных в сетях, использующих стек протоколов TCP/ IP. IP (Internet Protocol) – протокол сетевого уровня, предназначенный для доставки данных в составной сети с использованием одного из транспортных протоколов, например TCP или UDP.

Нижний уровень стека TCP/IP использует стандартные протоколы передачи данных, что делает возможным его применение в сетях с использованием любых сетевых технологий и на компьютерах с любой операционной системой.

Изначально протокол TCP/IP разрабатывался для применения в глобальных сетях, именно поэтому он является максимально гибким. В частности, благодаря способности фрагментации пакетов данные, несмотря на качество канала связи, в любом случае доходят до адресата. Кроме того, благодаря наличию IP-протокола становится возможной передача данных между разнородными сегментами сети.

Недостатком TCP/IP-протокола является сложность администрирования сети. Так, для нормального функционирования сети требуется наличие дополнительных серверов, например DNS, DHCP и т. д., поддержание работы которых и занимает большую часть времени системного администратора.

## **IPX/SPX**

Стек протоколов IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) является разработкой и собственностью компании Novell. Он был разработан для нужд операционной системы Novell NetWare, которая еще до недавнего времени занимала одну из лидирующих позиций среди серверных операционных систем.

Протоколы IPX и SPX работают на сетевом и транспортном уровнях модели ISO/OSI соответственно, поэтому отлично дополняют друг друга. Протокол IPX может передавать данные с помощью датаграмм, используя для этого информацию о маршрутизации в сети. Однако для того, чтобы передать данные по найденному маршруту, необходимо сначала установить соединение между отправителем и получателем. Этим и занимается протокол SPX или любой другой транспортный протокол, работающий в паре с IPX.

К сожалению, стек протоколов IPX/SPX изначально ориентирован на обслуживание сетей небольшого размера, поэтому в больших сетях его использование малоэффективно: излишнее использование широковещательного вещания на низкоскоростных линиях связи недопустимо.

## **NetBIOS/SMB**

Достаточно популярный стек протоколов, разработкой ко-

торого занимались компании IBM и Microsoft, соответственно, ориентированный на использование в продуктах этих компаний. Как и у TCP/IP, на физическом и канальном уровне стека NetBIOS/SMB работают стандартные протоколы, такие как Ethernet, Token Ring и другие, что делает возможным его использование в паре с любым активным сетевым оборудованием. На верхних же уровнях работают протоколы NetBIOS (Network Basic Input/Output System) и SMB (Server Message Block).



# 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.