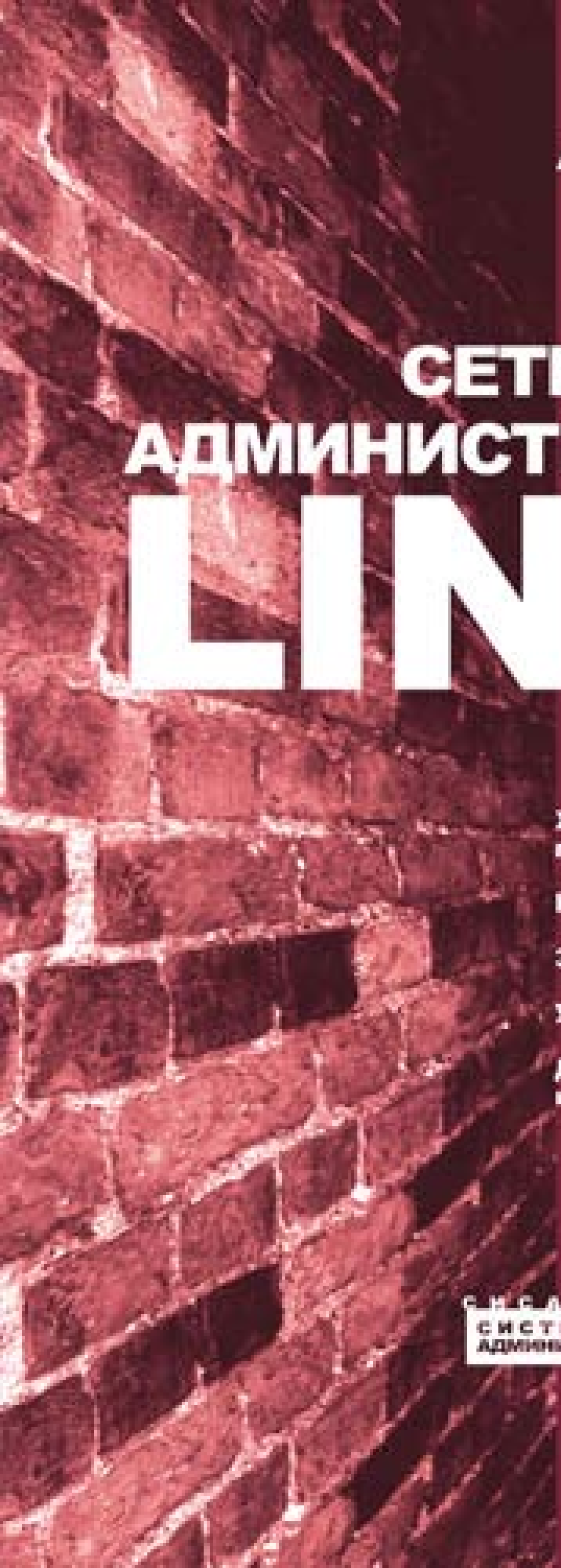


bhv

АЛЕКСЕЙ СТАХНОВ

СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ LINUX

- Характеристики и возможности протоколов семейства TCP/IP
- Настройка сервисов и служб
- Защищенный удаленный доступ
- Управление сетевым трафиком
- Диагностика и аудит сети и служб

СИСТЕМНЫЙ АДМИНИСТРАТОР

+CD

Алексей Стахнов

СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ LINUX

Санкт-Петербург
«БХВ-Петербург»
2004

УДК 681.3.06
ББК 32.973-018.2
С78

Стахнов А. А.

С78 Сетевое администрирование Linux. — СПб.: БХВ-Петербург, 2004. — 480 с.: ил.

ISBN 5-94157-277-8

В книге представлены теоретические и практические знания, позволяющие хорошо понимать процессы, происходящие в сети. Рассматриваются сетевые модели, протоколы, адреса, службы, конфигурирование сетевых интерфейсов, настройка серверов FTP, Proxy, INN, Apache, Samba, Mars, обсуждается сетевая файловая система, взаимодействие Linux с другими операционными системами. Описывается конфигурирование локальной сети: сетевые принтеры, шлюз в Интернет, настройка Firewall, учет трафика и т. п. Приведено множество программ, помогающих обслуживать сеть и заботиться о ее безопасности. Рассказано, как создать, настроить и обеспечить надежное функционирование сервера небольшой локальной сети, способного выполнять большинство типовых задач. На прилагаемом компакт-диске находятся последние версии программного обеспечения, рассмотренного в книге.

Для системных администраторов

УДК 681.3.06
ББК 32.973-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Екатерина Капалыгина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Оформление серии	*Via Design*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 27.02.04.
Формат $70\times100^{1}/_{16}$. Печать офсетная. Усл. печ. л. 38,7.
Тираж 4000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953.Д.001537.03.02
от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в Академической типографии "Наука" РАН
199034, Санкт-Петербург, 9 линия, 12.

ISBN 5-94157-277-8

Содержание

Введение

Традиционным элементом практически любой книги является введение. Любой человек, взяв незнакомую книгу в руки, первым делом интересуется тремя вещами: аннотацией, введением и оглавлением книги. Позвольте представить вам введение моей книги.

Благодарности

Хотелось бы сказать о людях, благодаря которым эта книга в конце концов была создана.

Огромное спасибо моей жене Светлане и дочке Наталье за проявленное терпение, поддержку и понимание — мало людей согласятся видеть мужа и отца на протяжении многих месяцев спиной к окружающей действительности и лицом к монитору. Спасибо всем остальным членам моей семьи — без их чуткости и поддержки мне было бы намного тяжелее работать.

Отдельное спасибо Юрию Осьмеркину — это он меня привел в мир Linux и консультировал по множеству вопросов, связанных с материалом книги.

Я благодарен коллективу издательства "БХВ-Петербург" за веру в молодых авторов и терпение в работе с ними. Особо хочется отметить следующих людей: Екатерину Капалыгину, моего редактора, благодаря ее стараниям книга приобрела единый стиль подачи материала; Евгения Рыбакова — за решение общих проблем; и других специалистов, создавших книгу в том виде, в котором читатель увидит ее в магазинах.

Я благодарен сотням и тысячам энтузиастов, плодами работы которых я воспользовался при написании книги, — составителям и переводчикам разнообразной документации, FAQ, How To и различных статей, авторам программ и просто их пользователям.

Почему написана эта книга

Достаточно сложный вопрос. Здесь переплелись и меркантильный интерес, и честолюбие, желание попробовать себя в другой области, попытка побороть свою неуверенность и лень, и не в последнюю очередь — хотелось сделать книгу для наших реалий и нашей специфики. Не секрет, что большинство переводной литературы неадекватно для нашей полунищей действительности. Часто можно встретить несколько "раздражающие" для глаза администратора бюджетной организации советы типа "в качестве маршрутизатора мы рекомендуем использовать устройство фирмы Cisco со следующими параметрами...". Конечно, с точки зрения надежности, простоты в обслуживании и тому подобных вещей такой совет верен. А с точки зрения банального бюджета какой-нибудь государственной конторы — заплатить 4—5 тысяч американских долларов за "железку" размером с кирпич — полный абсурд. Поэтому для наших реалий нужна книга, описывающая построение сетевой и программной инфраструктуры, позволяющей решать большинство типовых задач. Помимо этого, одной из причин для создания книги явилось желание систематизировать и углубить свои собственные знания об операционной системе Linux и ее приложениях.

Для кого написана эта книга

Прежде чем создавать какое-то произведение, автор всегда должен определить своего потенциального читателя. Каким же я его вижу? Это должен быть человек, увлекающийся информационными технологиями, который обладает достаточно приличным багажом знаний в области программного обеспечения (как правило, операционная система Windows), почти наверняка тем или иным образом связанный с администрированием (по крайней мере, как администратор своего собственного персонального компьютера), которому интересно возиться с программным обеспечением и который собирается перейти, или недавно это сделал, к использованию операционной среды Linux. При этом уровень книг серии "для чайников" или "сделай все за 21 день" его заведомо не устраивает, поскольку ему необходимо четко представлять себе возможности операционной системы, ее структуру, решаемые с ее помощью прикладные задачи, наиболее популярное программное обеспечение, его установка, настройка и использование.

Вот так я представляю себе читателя книги.

Структура книги

Книга разбита на пять частей плюс приложения. Рассмотрим, что в них описывается и для кого они предназначены.

Часть I представляет интерес для новичков в мире Linux. В ней содержится обзор протоколов семейства TCP/IP, процесс настройки и отладки сетевых интерфейсов, а также настройка модемного соединения. Этот раздел является вводным (базисным), поскольку дальнейшее изложение материала подразумевает знание специфики протоколов TCP/IP и настроенной сети. Он будет интересен в первую очередь новичкам и "продвинутым" пользователям, поскольку администраторы со стажем должны знать данную тему "на зубок".

Часть II представляет интерес как для новичков, так и для опытных пользователей операционной системы Linux, поскольку именно здесь рассматриваются вопросы конфигурирования сетевых служб. В этой части описывается конфигурирование DHCP, DNS, почтового сервера, службы LDAP, FTP, NNTP, Apache, Proxy-сервера и NTP-сервера. Именно эта часть позволит вам создать полнофункциональный сервер, способный выполнить около 90% задач типичного сервера небольшой организации. Вторую часть я старался сделать доступной для понимания начинающему пользователю. Она содержит большой объем информации в достаточно сжатом виде и требует размышлений и экспериментов от читателя.

В *части III* я опять возвращаюсь к настройке сетевых сервисов. Поскольку мы за плюрализм и демократию, наша сеть не является гомогенной средой и волей-неволей приходится взаимодействовать с различными операционными системами. В этой части мы ознакомимся с NFS (сетевой файловой системой UNIX), научимся предоставлять и получать доступ к каталогам операционных систем Windows и Novell.

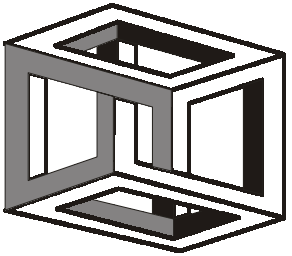
Предыдущие части книги были подготовительным этапом для *части IV*. Она предназначена больше для опытных пользователей, т. к. я хотел, чтобы моя книга служила вам верой и правдой в качестве справочного пособия долгое время, и вы периодически возвращались к ней для решения специфических задач, возникающих в вашей работе. Здесь вы найдете описание основных приложений, используемых для организации НОРМАЛЬНОГО функционирования сети организации, подключенной к Интернету. В этой части рассмотрена защита сети от нежелательного воздействия, организация виртуальных частных сетей, учета сетевого трафика, настройка сетевых принтеров, изготовление бездисковых компьютеров и организация шлюза в Интернете.

Часть V посвящена администрированию системы. Здесь рассмотрен удаленный безопасный доступ к хостам, а также утилиты для администрирования и мониторинга сети.

В *приложениях* находится список рекомендуемой литературы, небольшая коллекция ссылок, тем или иным образом касающихся Linux и программ для этой операционной системы, а также список наиболее часто применяемых сетевых портов и программ, их использующих.

Как со мной связаться

Те читатели, которые хотят внести свои предложения или уточнения по содержанию данной книги, поделиться интересными идеями, темами и т. п., могут воспользоваться электронным адресом **alst@farlep.net**. Я постараюсь ответить на все письма. Также можно воспользоваться моим сайтом **www.alst.od.ua**.



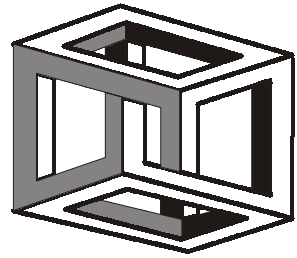
ЧАСТЬ I

Сетевые протоколы и конфигурирование

Эта часть является вводной. Как в хорошем детективе, прежде чем приступать к поиску преступника, нужно осмотреть место происшествия. Продолжая аналогию — прежде чем углубляться в дебри специфического программного обеспечения, необходимо узнать фундамент, на котором оно стоит, те общие моменты, которые используются большинством программ.

Данная часть интересна в первую очередь новичкам и опытным пользователям, поскольку администраторы со стажем должны хорошо знать эту тему. В ней содержится обзор протоколов семейства TCP/IP, процесс настройки и отладки сетевых интерфейсов, настройка модемного соединения, поскольку дальнейшее изложение материала подразумевает знание специфики протоколов TCP/IP и настроенной сети.

ГЛАВА 1



Сетевые протоколы

В данной главе будут рассмотрены базовые понятия, сетевые модели и протоколы, используемые в сетях. На фундаменте, заложенном этой главой, выстроена вся книга, поэтому рекомендую начинающим ознакомиться с ней, а более опытным полистать, освежить свои знания.

Модели сетевых взаимодействий

Как и любая сложная система, сеть опирается на стандарты, без которых невозможно ее нормальное функционирование. За последние двадцать лет было создано множество концепций сетевых взаимодействий, однако наибольшее распространение получили всего две:

- модель взаимодействия открытых систем (OSI);
- модель сетевого взаимодействия TCP/IP.

Терминология

Для облегчения понимания содержимого этой главы, приведем основные термины (табл. 1.1).

Таблица 1.1. *Базовые сетевые термины*

Термин	Определение
Датаграмма	Пакет данных. Обозначает единицу информации при сетевом обмене
DNS (Domain Name Service, служба доменных имен)	Специально выделенные компьютеры, которые производят поиск соответствия символического имени хоста и цифрового адреса хоста

Таблица 1.1 *(продолжение)*

Термин	Определение
Интернет	Глобальная компьютерная сеть, основанная на семействе протоколов TCP/IP
FTP (File Transfer Protocol, протокол передачи файлов)	Протокол используется для приема и передачи файлов между двумя компьютерами
IP (Internet Protocol, протокол Интернет)	Основа семейства протоколов TCP/IP. Практически любой протокол из этого семейства базируется на протоколе IP
ICMP (Internet Control Message Protocol, протокол управляющих сообщений в стеке протоколов IP)	Используется для передачи управляющих сообщений протокола IP
NFS (Network File System, сетевая файловая система)	Система виртуальных дисков, позволяющая клиентским компьютерам использовать каталоги сервера в качестве диска
NIC (Network Information Center, сетевой информационный центр)	Организация, которая отвечает за администрирование и раздачу сетевых адресов и имен
Узел (Node, Host)	Компьютер в сети. Название применимо как к клиенту, так и к серверу
OSI (Open System Interconnection, взаимодействие открытых систем)	Модель взаимодействия открытых систем
RFC (Request For Comments, запрос для пояснений)	Стандарты протоколов Интернета и их взаимодействия
RIP (Routing Information Protocol, протокол маршрутизации информации)	Протокол, используемый для обмена информацией между маршрутизаторами
SMTP (Simple Mail Transfer Protocol, простой протокол передачи электронной почты)	Используется для обмена электронной почтой
SNMP (Simple Network Management Protocol, простой протокол управления сетью)	Используется для управления сетевыми устройствами
TCP (Transmission Control Protocol, протокол управления передачей)	Используется для надежной передачи данных
Telnet	Протокол, осуществляющий удаленное сетевое подключение к компьютеру, эмулирующее терминал

Таблица 1.1 *(окончание)*

Термин	Определение
UDP (User Datagram Protocol, протокол пользовательских датаграмм)	Используется для обмена блоками информации без установки соединения

Модель взаимодействия открытых систем (OSI)

Еще в 1983 году Международная организация по стандартизации (International Organization for Standardization, ISO) разработала стандарт взаимодействия открытых систем (Open System Interconnection, OSI). В результате получилась семиуровневая модель:

1. Физический уровень (Physical Level).
2. Уровень данных (Data Link Level).
3. Сетевой уровень (Network Level).
4. Транспортный уровень (Transport Level).
5. Уровень сессии (Session Level).
6. Уровень представления (Presentation Level).
7. Уровень приложения (Application Level).

Первый уровень самый "приземленный", последующие — все более и более абстрагируются от особенностей физической среды передачи информации.

Каждый уровень модели OSI решает свои задачи, использует сервисы, предоставляемые предыдущим уровнем и, в свою очередь, предоставляет сервисы следующему уровню. Согласно этой модели, уровни не могут "перескакивать" через соседей, например, транспортный уровень не может непосредственно пользоваться сервисом физического уровня, он обязан пройти по цепочке: Сетевой уровень → Уровень данных → Физический уровень. В табл. 1.2 приведено описание уровней сетевой модели OSI.

Таблица 1.2. *Уровни сетевой модели OSI*

Уровень	Название	Описание
1	Физический уровень	Отвечает за физическое подключение компьютера к сети. Определяет уровни напряжения, параметры кабеля, разъемы, распайку проводов и т. п.
2	Уровень данных	Физически подготавливает данные для передачи (разбивая их на кадры определенной структуры) и преобразует обратно во время приема (восстанавливая из кадров)

Таблица 1.2 *(окончание)*

Уровень	Название	Описание
3	Сетевой уровень	Маршрутизирует данные в сети
4	Транспортный уровень	Обеспечивает последовательность и целостность передачи данных
5	Уровень сессии	Устанавливает и завершает коммуникационные сессии
6	Уровень представления	Выполняет преобразование данных и обеспечивает передачу данных в универсальном формате
7	Уровень приложения	Осуществляет интерфейс между приложением и процессом сетевого взаимодействия

На каждом уровне блоки информации имеют собственное название (табл. 1.3).

Таблица 1.3. *Название блока информации в модели*

Уровень	Название уровня	Название блока информации
1	Физический уровень	Бит
2	Уровень данных	Кадр (пакет)
3	Сетевой уровень	Датаграмма
4	Транспортный уровень	Сегмент
5, 6, 7	Уровень приложения	Сообщение

Несмотря на то, что OSI является международным стандартом и на его основе правительство США выпустило спецификации GOSIP (Government Open Systems Interconnection Profile, Государственный регламент взаимодействия открытых систем), у производителей программного обеспечения стандарт OSI широкой поддержки не получил. Это объясняется несколькими причинами:

- волокита в принятии стандарта;
- его "оторванность" от реалий;
- наличие большого числа уровней трудно для реализации и приводит к потере производительности;
- широчайшее распространение протокола TCP/IP, и нежелание потребителей отказываться от него.

В результате, спецификации OSI сегодня — это, в основном, страницы в учебнике, в реальной жизни они не применяются.

Модель сетевого взаимодействия TCP/IP

Архитектура семейства протоколов TCP/IP (Transmission Control Protocol/ Internet Protocol, протокол управления передачей/интернет-протокол) основана на представлении, что коммуникационная инфраструктура содержит три вида объектов: процессы, хосты и сети.

Основываясь на этих трех объектах, разработчики выбрали четырехуровневую модель:

1. Уровень сетевого интерфейса (Network Interface Layer).
2. Уровень межсетевого интерфейса — Интернета (Internet Layer).
3. Транспортный уровень (Host-to-Host Layer).
4. Уровень приложений/процессов (Application/Process Layer).

Сопоставление сетевых моделей OSI и TCP/IP

Нетрудно заметить, что модель TCP/IP отличается от модели OSI. В табл. 1.4 показано соответствие модели TCP/IP и модели OSI.

Таблица 1.4. *Соответствие модели TCP/IP и модели OSI*

TCP/IP	OSI
Уровень приложений	Уровень приложений
	Уровень представления
	Уровень сеанса
Транспортный уровень	Транспортный уровень
Межсетевой уровень (Интернет)	Сетевой уровень
Уровень сетевого интерфейса	Уровень канала данных
	Физический уровень

Как видно из таблицы, уровень сетевого интерфейса модели TCP/IP соответствует сразу двум уровням модели OSI, а уровень приложений модели TCP/IP — трем уровням модели OSI.

Сетевые протоколы

В данном разделе мы рассмотрим различные сетевые протоколы, используемые в современной компьютерной индустрии. Пожалуй, это основная часть сетевых моделей (аппаратная часть все-таки не настолько важна для функционирования сети). Также здесь будут рассмотрены протоколы транспортного уровня, на которые опираются протоколы уровня приложений.