ВВЕДЕНИЕ 21
В.1. СЕТЕВЫЕ ПРОТОКОЛЫ И МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ 22
В.2. МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ISO OSI 25
В.2.1. Физический уровень 25
В.2.2. Канальный уровень 27
В.2.3. Сетевой уровень 28
В.2.4. Транспортный уровень 30
В.2.5. Сеансовый уровень 32
В.2.6. Уровень представления 33
В.2.7. Прикладной уровень 33
В.3. СТЕК ПРОТОКОЛОВ TCP/IP 34
В.3.1. Протокол IP (Internet Protocol) 34
В.3.2. Протоколы TCP и UDP 35
В.3.3. Протоколы приложений 35
В.4. СПОСОБЫ ПЕРЕДАЧИ ИНФОРМАЦИИ 37
В.4.1. Синхронная передача данных 37
В.4.2. Пакетная передача данных 38
В.4.3. Асинхронная передача данных 39
В.5. ВИРТУАЛЬНАЯ ЦЕПЬ 39
В.5.1. Концепция виртуальной цепи 39
В.5.2. Постоянные и коммутируемые виртуальные цепи 42

ГЛАВА 1. МАРШРУТИЗАТОРЫ CISCO И СЕТЕВАЯ БЕЗОПАСНОСТЬ — КАК ЭТО ВЫГЛЯДИТ НА ПРАКТИКЕ 43

1.1. МАРШРУТИЗАТОРЫ CISCO: ВИД СПЕРЕДИ, СБОКУ, СВЕРХУ И... ИЗНУТРИ 44
1.2. ИДЕНТИФИКАЦИЯ ИНТЕРФЕЙСА 47
1.3. КАБЕЛИ 48
1.4. ПАМЯТЬ МАРШРУТИЗАТОРА: ТИПЫ, НАЗНАЧЕНИЕ, ОСОБЕННОСТИ ДОСТУПА 49
1.5. КОНСОЛЬ 50
1.6. КОМАНДЫ 53
1.6.1. Методика и синтаксис использования команд 53
1.6.2. Непривилегированный режим (режим пользователя) — стоит на страже правопорядка. Команды доступные в этом режиме 55
1.6.3. Привилегированный режим (режим администратора) 56
1.7. КОНФИГУРИРОВАНИЕ МАРШРУТИЗАТОРА. КАК ЭТО ДЕЛАЕТСЯ 56
Файл конфигурации 56
Защита конфигурационного файла CISCO 59
Возможность настройки маршрутизатора через Web и безопасность 60
Программа ConfigMaker 61
1.8. ОТЛАДКА. МОНИТОРИНГ ПРОИСХОДЯЩИХ СОБЫТИЙ 62

ГЛАВА 2. СЕТЕВЫЕ МОНИТОРЫ. АНАЛИЗ СТАБИЛЬНОСТИ И БЕЗОПАСНОСТИ СЕТИ. ПЕРЕХВАТ ДАННЫХ 64
2.1. СЕТЕВЫЕ МОНИТОРЫ — ОРУЖИЕ АДМИНИСТРАТОРА ИЛИ ВЗЛОМЩИКА? 65
2.2. ПАКЕТНЫЕ ДРАЙВЕРЫ, КОММУТАТОРЫ И КОНЦЕНТРАТОРЫ. ВОПРОСЫ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ ПО СЕТИ 66
2.3. MS NETWORK MONITOR — ПРОГРАММА ПЕРЕХВАТА ДЛЯ СЕРВЕРНЫХ ОПЕРАЦИОННЫХ СИСТЕМ 69
2.3.1. Перехват кадров с данными 69
2.3.2. Просмотр захваченных кадров 73
2.3.3. Фильтр захваченных кадров 75
2.4. ПРОГРАММА ETHEREAL — ПЕРЕХВАТ ДАННЫХ ПОД ПОЛЬЗОВАТЕЛЬСКИМИ ОПЕРАЦИОННЫМИ СИСТЕМАМИ (WINDOWS 2000/XP) 76

ГЛАВА 3. ФИЗИЧЕСКИЙ УРОВЕНЬ — КАНАЛ ПЕРЕДАЧИ ДАННЫХ, БЕЗОПАСНОСТЬ, СТАНДАРТЫ 79
Глобальные сети (WAN) 80
Локальные сети (LAN) 81
3.1. ПОСЛЕДОВАТЕЛЬНЫЕ ЛИНИИ 81
Последовательная и параллельная передача данных 82
Симметрический и асимметрический сигнал 82

Синхронная и асинхронная передача 82
Протоколы V.24, V.35 и X.21 85
Нуль-модемное соединение 88
3.2. МОДЕМЫ. АНАЛОГОВЫЕ ЛИНИИ 89
3.2.1. Назначение и принцип работы 89
3.2.2. Соединение модемов через провайдера 90
Dial-up-соединение 90
Выделенные линии 90
3.2.3. «Автоматические» модемы. Использование AT-команд для «прямого» управления модемом 91
3.2.4. Синхронная передача и асинхронная 93
3.2.5. Базовая полоса и голосовая полоса 93
3.2.6. Скорость передачи 95
3.2.7. Аппаратное сжатие данных. Особенности разных технологий 96
3.2.8. Обнаружение и коррекция ошибок 97
3.3. ЦИФРОВЫЕ ЛИНИИ 98
3.3.1. ISDN 98
Начальный интерфейс 99
Высокоуровневые протоколы и сигнализация 102
3.3.2. Линии E* 104
3.4. ЛОКАЛЬНЫЕ СЕТИ (LAN, LOCAL AREA NETWORK) 105
3.4.1. Кабели 105
Категории кабелей 105
Обжимка витой пары 107
Оптические кабели 108
3.4.2. Ethernet (10 Мбит/с) 112
3.4.3. Fast Ethernet (100 Мбит/с) 114
3.4.4. Gigabit Ethernet (1 Гбит/с) 114
3.4.5. FDDI (Fiber Distributed Data Interface) 115
3.5. БЕСПРОВОДНЫЕ ЛИНИИ GSM 115
Протоколы, стандарты, безопасность в сетях GSM 115
Подключение компьютера к Интернету через сеть GSM 120
GPRS (General Packet Radio Service) — не путать с глобальным позиционированием 122

ГЛАВА 4. КАНАЛЬНЫЙ УРОВЕНЬ. ПРОТОКОЛЫ, СТАНДАРТЫ, БЕЗОПАСНОСТЬ... 123
4.1. ПРОТОКОЛ SLIP 124
4.2. CSLIP — УСОВЕРШЕНСТВОВАННЫЙ SLIP 126
Появилось сжатие заголовков 126
Как происходит сжатие на практике 128
4.3. ПРОТОКОЛ HDLC — ОТЕЦ PPP 131
4.3.1. Описание и режимы работы протокола 131
4.3.2. Формат кадра HDLC 132
Поле Флаг 133
Поле адреса 133
Контрольная сумма (Checksum) 133
Поле данных и тип передаваемого протокола 134
Управляющее поле 134
4.3.3. Типы HDLC-кадров, их особенности и назначение 135
Информационный кадр (I-frame, I-кадр) 135
Суперкадр (S-frame, S-кадр) 136
Непронумерованный кадр (U-frame, U-кадр) 137
4.3.4. Обобщенная информация о протоколе HDLC 138
4.4. ПРОТОКОЛ PPP (POINT-TO-POINT PROTOCOL) — САМОЕ РАСПРОСТРАНЕННОЕ РЕШЕНИЕ 139
4.4.1. Общее описание 139
Основные функции PPP 139
Формат PPP-кадра 140
Протоколы — составляющие PPP 141
4.4.2. Набор номера по телефонной линии «изнутри» — с точки зрения PPP 142
4.4.3. Протокол LCP — ответственный за управление связью в PPP 143
Назначение протокола LCP. Выбор алгоритма аутентификации 143
Формат LCP-кадра 145
Разбираем пример кадра PPP-соединения 147
4.4.4. Управление доступом. PPP-Аутентификация 150
Протокол PAP 152
Протоколы типа CHAP 152
Расширяемый протокол аутентификации Extensible Authentication Protocol (EAP) 154
Протокол Radius решает проблемы аутентификации 156

4.4.5. Протокол управления обратным звонком — CBCP (Call-Back Control Protocol) 156

4.4.6. Дополнительные (вспомогательные) протоколы семейства PPP 159

Многоканальный протокол «точка-точка» — Multiline Protocol (MP) 159

Протоколы BAP (Bandwidth Allocation Protocol) и BACP (Bandwidth Allocation Control Protocol) 161

Протокол управления сжатием — Compression Control Protocol (CCP) 163

Протокол управления шифрованием — PPP Encryption Control Protocol (ECP) 164

4.4.7. IPCP. Протокол сетевого уровня, входящий в группу протоколов PPP 165

4.5. FRAME RELAY — ПРОТОКОЛ КАНАЛЬНОГО УРОВНЯ ДЛЯ ГЛОБАЛЬНЫХ СЕТЕЙ 167

Общее описание технологии 167

Кадр протокола Frame Relay 172

Перегруженная сеть. Переполнение канала 174

IP по Frame Relay 176

LMI 177

Конфигурация Frame Relay на маршрутизаторах CISCO 178

Резюме 178

4.6. ЛОКАЛЬНАЯ СЕТЬ (LOCAL AREA NETWORKS, LAN) И ПРОТОКОЛ ETHERNET 179

Обзор основных технологий локальных сетей 179

Технология Ethernet 181

4.7. БЕСПРОВОДНЫЕ ЛОКАЛЬНЫЕ СЕТИ (WIRELESS LOCAL AREA NETWORKS, WLAN) 191

4.7.1. Обзор технологий беспроводных локальных сетей 191

4.7.2. Типичная конфигурация WLAN 194

Access Point — AP 194

Магистральное соединение точка-точка 195

Одноранговые сети 194

Роуминг (несколько точек доступа) 195

4.7.3. Антенны 196

4.7.4. Безопасность WLAN 197

Wired Equivalent Privacy (WEP) 197

Служба Установки ID — Service Set ID (SSID) 197

IEEE 802.1X 198

4.7.5. Фиксированный беспроводный доступ (Fixed Wireless Access, FWA) 199

Обзор технологии 199
Отличия между FWA и WLAN 199
Основные преимущества FWA 200

ГЛАВА 5. ПРОТОКОЛ IP (INTERNET PROTOCOL) 201

5.1. НАЗНАЧЕНИЕ И ФУНКЦИИ ПРОТОКОЛА IP 202
Функции и особенности IP 202
Вспомогательные протоколы, входящие в состав IP 203
Маршрутизатор и обработка IP-дейтаграмм 204

5.2. УСТРОЙСТВО IP-ДЕЙТАГРАММЫ 208

5.3. ПРОТОКОЛ МЕЖСЕТЕВЫХ УПРАВЛЯЮЩИХ СООБЩЕНИЙ (INTERENT CONTROL MESSAGE PROTOCOL, ICMP) 214

5.3.1. Общая информация 214
Назначение протокола ICMP 214
Какие бывают ICMP-сообщения 215

5.3.2. Разбираем отдельные ICMP-сообщения 217
Сообщение Echo 217
Недоставляемая IP-дейтаграмма (Undeliverable IP datagram) 217
Подавление источником (Source Quench) 217
Перенаправление (Redirect) 218
Поиск маршрутизаторов с помощью ICMP 218
Время вышло (Time exceeded) 219
Запрос маски адреса подсети (Address mask request) 221
Синхронизация времени 221

5.4. ФРАГМЕНТАЦИЯ IP-ДЕЙТАГРАММ И УЯЗВИМОСТИ, ЕЮ ОБУСЛОВЛЕННЫЕ 222
Размер фрагментов 222
Фрагментирование дейтаграмм маршрутизаторами 223
Уязвимость механизма фрагментации 226

5.5. ДОПОЛНИТЕЛЬНЫЕ ЭЛЕМЕНТЫ IP-ЗАГОЛОВКА — ПОДВОДНЫЕ КАМНИ БЕЗОПАСНОСТИ 227

5.5.1. Какие они есть 227

5.5.2. Запись маршрута (Record Route) 228

5.5.3. Временная метка (Timestamp) 231

5.5.4. Маршрутизация от источника (Source Routing). Скрытые возможности атаки на сеть 233
Жесткая и свободная маршрутизации от источника 233
Атака на сеть 235

5.5.5. Опция IP Router Alert (опция тревоги) 236

5.6. ПРОТОКОЛЫ ARP И RARP 237
5.6.1. Общее описание стандартного ARP 237
Протокол ARP и устройство его заголовка 237
Схема работы ARP 238
5.6.2. Безопасность средствами ARP. Фильтр ARP 241
5.6.3. ARP-прокси 242
5.6.4. Протокол RARP (Reverse ARP) 243
5.7. ПРОТОКОЛ IGMP (INTERNET GROUP MANAGEMENT PROTOCOL) 244
5.8. МУЛЬТИКАСТИНГ И КАНАЛЬНЫЙ ПРОТОКОЛ 248

ГЛАВА 6. IP-АДРЕСА 251
6.1. ЧТО ТАКОЕ IP-АДРЕС И КАКОЙ У НЕГО ФОРМАТ 252
6.2. КЛАССЫ И СПЕЦИАЛЬНЫЕ АДРЕСА 253
Классы IP-адресов 253
Специальные IP-адреса 255
6.3. ПОДСЕТИ И МАСКИ СЕТИ 256
Почему стандартных механизмов IPv4 недостаточно для адресации 256
Подсети и маски 257
Использование постоянных и переменных сетевых масок 262
6.4. МЕХАНИЗМ БЕСКЛАССОВОЙ МЕЖДОМЕННОЙ МАРШРУТИЗАЦИИ CIDR 265
Бесклассовая адресация 265
Суперсети, автономные системы 266

ГЛАВА 7. МАРШРУТИЗАЦИЯ 275
7.1. ПРОДВИЖЕНИЕ (FORWARDING) И ЭКРАНИРОВАНИЕ (SCREENING) 276
7.2. МАРШРУТИЗАЦИЯ 278
7.2.1. Как это происходит 278
7.2.2. Обработка таблицы маршрутизации 281
7.3. РАБОТА С ТАБЛИЦАМИ МАРШРУТИЗАЦИИ 282
7.3.1. Таблицы маршрутизации в разных операционных системах и устройствах 283
Таблица маршрутизации в Windows NT 283
Таблица маршрутизации в Windows Server 2000/2003 284
Таблица маршрутизации в UNIX/Linux 284
Таблица маршрутизации на маршрутизаторах CISCO 285
7.3.2. Редактирование таблицы маршрутизации 286

Работа со статическими записями в таблице маршрутизации ... 287
Управление таблицей маршрутизации по протоколу SNMP ... 288
Объединение (aggregation) нескольких записей ... 289
7.4. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ ... 290
LSP и RVP ... 290
IPG (Interior Gateway Protocol) и EGP (Exterior Gateway Protocol) ... 292
Отметка протокола маршрутизации в таблице маршрутизации. Перераспределение ... 293
7.5. НЕЙТРАЛЬНЫЕ ТОЧКИ ОБМЕНА (NEUTRAL EXCHANGE POINT (NIX)) ... 293

ГЛАВА 8. ПРОТОКОЛ IP, ВЕРСИЯ 6 ... 295
8.1. ОСОБЕННОСТИ ПРОТОКОЛА IPv6 ... 296
Что нового появилось в протоколе IPv6 ... 296
Заголовок IPv6 ... 297
8.2. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ ЗАГОЛОВКОВ В IP-ДЕЙТАГРАММАХ ... 300
Опции перехода (Hop-by-Hop Options) ... 302
Заголовок маршрутизации ... 304
Фрагментация IPv6-дейтаграмм. Заголовки фрагментации ... 306
Заголовок аутентификации (протокол AH) ... 307
Заголовок безопасности (Протокол ESP) ... 307
8.3. ПРОТОКОЛ ICMPv6 ... 308
Отображение (mapping) IP-адреса в канальный адрес ... 310
Определение адреса маршрутизатора в локальной сети ... 314
Перенаправление (Redirect) ... 317
8.4. IPv6-АДРЕСА ... 318
Правила написания адресов ... 319
Групповые адреса (Multicasts) ... 320
Индивидуальные адреса ... 321
IPv6 и операционные системы семейства Windows ... 323

ГЛАВА 9. ПРОТОКОЛ УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ (TRANSMISSION CONTROL PROTOCOL, TCP) ... 325
9.1. TCP-СЕГМЕНТЫ ... 328
9.2. ДОПОЛНИТЕЛЬНЫЕ ЭЛЕМЕНТЫ TCP-ЗАГОЛОВКА ... 333
9.3. ПРИМЕР TCP-СЕГМЕНТА ИЗ СЕТИ (NETWORK MONITOR) ... 335
9.4. УСТАНОВКА И ЗАВЕРШЕНИЕ TCP-СОЕДИНЕНИЯ ... 336
9.4.1. Установка соединения ... 336

9.4.2. Завершение соединения 342
9.4.3. Разрыв соединения 344
9.5. ОПРЕДЕЛЕНИЕ СОСТОЯНИЯ СОЕДИНЕНИЯ 345
9.6. МЕТОДЫ ЗАДЕРЖКИ ОТВЕТА 347
9.7. ТЕХНИКА ОКНА 350
9.8. ПЕРЕГРУЗКА СЕТИ 353
9.8.1. Медленный старт 354
9.8.2. Предотвращение перегрузки 355
9.8.3. Потеря сегмента 356
9.9. ОПЦИЯ РАСШИРЕНИЯ ОКНА (INCREASE WINDOW OPTION) 358

ГЛАВА 10. ПРОТОКОЛ UDP (USER DATAGRAM PROTOCOL) 360
10.1. ПРОТОКОЛ UDP И ЕГО ОСОБЕННОСТИ 361
Общее описание протокола 361
Структура UDP-заголовка 362
Пример UDP-дейтаграммы 364
10.2. ФРАГМЕНТАЦИЯ 365
10.3. ШИРОКОВЕЩАНИЕ И ГРУППОВЫЕ РАССЫЛКИ — ОТЛИЧИТЕЛЬНАЯ ОСОБЕННОСТЬ ПРОТОКОЛА UDP 365
10.4. ЧЕГО НЕ «УМЕЕТ» UDP 366
10.5. СРАВНЕНИЕ UDP И TCP 366

ГЛАВА 11. СЛУЖБА ИМЕН DNS 368
11.1. ДОМЕНЫ И ПОДДОМЕНЫ 370
11.2. СИНТАКСИС ИМЕНИ 372
11.3. ОБРАТНЫЕ ДОМЕНЫ 373
11.4. ДОМЕН 0.0.127.IN-ADDR.ARPA 375
11.5. ДОМЕННЫЕ ЗОНЫ 375
Что такое зона 375
Специальные Зоны 376
11.6. ЗАРЕЗЕРВИРОВАННЫЕ ДОМЕНЫ И ПСЕВДОДОМЕНЫ 376
11.7. ЗАПРОСЫ DNS (РАЗРЕШЕНИЯ ИМЕНИ) 377
Запросы и их обработка 377
Как работают резолверы 378
Транспортные протоколы, используемые DNS. Особенности работы с перегруженными DNS-серверами 381
Технология Round Robin 382
11.8. ПРАКТИКА НАСТРОЙКИ РЕЗОЛВЕРОВ 383

Конфигурация резолвера в Unix 383
Конфигурация резолвера в Windows 384
11.9. СЕРВЕР ИМЕН 388
Типы серверов имен 388
Работа серверов имен 391
11.10. FORWARD-СЕРВЕРЫ 393

ГЛАВА 12. ПРОТОКОЛ DNS 395
12.1. ЗАПИСИ РЕСУРСОВ 396
12.2. ПРОТОКОЛ DNS 398
12.3. ОПЕРАЦИЯ DNS QUERY (ЗАПРОС) 399
12.3.1. Формат пакета DNS-запроса 399
12.3.2. Заголовок пакета запроса DNS query 400
12.3.3. Секция вопроса 402
12.3.4. Секция ответа, авторитетные серверы и дополнительная информация 405
12.3.5. Сжатие 406
12.3.6. Инверсный (обратный) запрос 409
12.3.7. Методы передачи ресурсных записей в DNS-пакете 409
12.4. ПРИМЕРЫ ОБЩЕНИЯ DNS-КЛИЕНТА И DNS-СЕРВЕРА 409
Практика использования программы NSLOOKUP для мониторинга DNS-серверов 422

ГЛАВА 13. РАСШИРЕННЫЕ ФУНКЦИИ ПРОТОКОЛА DNS 427
13.1. ОПЕРАЦИЯ DNS UPDATE 428
13.1.1. Общее описание 428
13.1.2. Формат DNS-пакета для операции UPDATE 430
Секция заголовка 431
Секция зоны 432
Секция условия (Prerequisite Section) 432
Секция обновления 433
Секция дополнительных данных 434
13.1.3. Файл журнала 434
13.1.4. Замечания 435
13.2. ОПЕРАЦИЯ DNS NOTIFY 435
Операция уведомления DNS Notify 435
Сообщение Notify 436

13.3. ВОЗРАСТАЮЩАЯ ПЕРЕДАЧА ЗОНЫ 439
Формат запроса 440
Формат ответа 441
Генеральная уборка 441
Примеры 441
13.4. ОТРИЦАТЕЛЬНОЕ КЭШИРОВАНИЕ (DNS NCACHE) 444
Какие отрицательные ответы будут храниться в памяти? 444
Сколько времени отрицательные ответы хранятся в памяти? 445
Поле MINIMUM (Минимум) в SOA-записи 445
Сохранение правил отрицательных ответов 446

ГЛАВА 14. РЕАЛИЗАЦИЯ СЕРВЕРА ИМЕН 447
14.1. НЕМНОГО ПРЕДЫСТОРИИ 448
14.2. БАЗА ДАННЫХ DNS И ЕЕ ЗАПИСИ 451
14.2.1. Синтаксис базы данных DNS 451
14.2.2. Формат записей в базе данных DNS 453
Запись SOA 453
Записи типа A 455
Записи типа CNAME 456
Записи типа HINFO и TXT 457
Записи типа NS 457
Записи типа MX 458
Записи типа PTR 459
Записи типа SRV 461
14.2.3. Специальные команды для работы с записями DNS 464
Команда $ORIGIN 464
Команда $INCLUDE 465
14.2.4. Реализация в Windows Server 2000/2003 465
14.3. BIND НОВОГО ПОКОЛЕНИЯ (ВЕРСИИ 8 И 9) 471
14.4. КОНФИГУРАЦИОННЫЙ ФАЙЛ BIND 473
14.4.1. Команды конфигурационного файла 474
14.4.2. Примеры конфигурирования name server 474
Кеширующий name server (Caching-only name server) 475
Авторитетный name server 475
14.4.3. Использование комментариев 477
14.4.4 Команда acl 478

14.4.5. Список IP-адресов 478
14.4.6. Команда controls 479
14.4.7. Команда include 480
14.4.8. Команда key 480
14.4.9. Команда logging — протоколирование нестандартных ситуаций 481
Описание команды logging 481
Создание канала протоколирования 483
14.4.10. Команда options — настройка глобальных опций DNS-сервера 485
14.4.11. Команда server 488
14.4.12. Команда trusted-keys 488
14.4.13. Команда view 489
14.4.14. Команда zone 493
Общее описание команды и ее назначения 493
14.5. ПАРАМЕТРЫ КОМАНДЫ OPTIONS 495
14.5.1. Спецификация файлов 495
Параметр directory 495
Параметр named-xfer 496
Параметр dump-file 496
Параметр pid-file 496
Параметр statistics-file 496
14.5.2. Параметры типа boolean 496
Параметр auth-nxdomain 496
Параметр fetch-glue 497
Параметр multiple-cnames 497
Параметр notify 497
Параметр recursion 497
14.5.3. Перенаправление Forwarding 498
Параметр forward 498
Параметр forwarders 498
14.5.4. Контроль имен (check-names) 498
14.5.5. Управление доступом (Access Control) 499
Параметр allow-query 499
Параметр allow transfer 499
14.5.6. Сетевые интерфейсы 500

Параметр listen-on 500
Параметр listen-on-verz.e6 500
14.5.7. Передача данных зоны 500
Параметр max-transfer-time-in 500
Параметр transfer-format 500
Параметр transfers-in 501
Параметр transfers-out 501
Параметр transfers-per-ns 501
14.5.8. Временные интервалы 501
Параметр clean-interval 501
Параметр statics-interval 501
14.6. КОМАНДЫ РЕДАКТИРОВАНИЯ ФАЙЛОВ ЗОНЫ. СПЕЦИАЛЬНЫЕ ВОЗМОЖНОСТИ BIND 9 502
14.6.1. Команда $TTL 502
14.6.2. Команда $GENERATE 502
14.6.3 Lightweight resolver 503
14.6.4. Команда lwres 504
14.7 ИНСТРУМЕНТЫ ДЛЯ ОТЛАДКИ И УПРАВЛЕНИЯ DNS 505
14.7.1. Способы контроля над конфигурированием 505
14.7.2. Проверка конфигурационных файлов 506
Программа named-checkconf 506
Программа named-checkzone 507
14.7.3. Программа nslookup — оптимальный выбор для тестирования DNS 507
Общее описание программы 507
Режим отладки 511
Уровень режима отладки debug 511
Уровень режима отладки d2 513
Замена сервера имен, используемого по умолчанию 516
Запись зоны 516
Имитация запросов от сервера имен 517
Наиболее часто встречаемые сообщения об ошибках программы nslookup 517
14.7.4. Прочие программы, предназначенные для проверки DNS 518
Программа Dnswalk 518
Программа Dig 519
14.8. ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ СЕРВЕРОМ ИМЕН. ПРОГРАММА RNDC 521

Общее описание и методика использования....521
Обзор команд программы rndc....523
14.9. СИГНАЛЫ....524
Методика использования сигналов....524
Сигнал HUP....524
Сигнал INT....524
Сигнал IOT....526
Сигнал KILL....527
Сигнал TERM....527
Сигналы USR1 и USR2....527
14.10. ДЕСЯТЬ НАИБОЛЕЕ ЧАСТО НАРУШАЕМЫХ ПРАВИЛ В КОНФИГУРАЦИИ DNS....528

ГЛАВА 15. РЕГИСТРАЦИЯ И ДЕЛЕГИРОВАНИЕ ДОМЕНОВ....530
15.1. МЕТОДИКА ДЕЛЕГИРОВАНИЯ ДОМЕНОВ....531
15.2. ПРИМЕР 1. ДЕЛЕГИРОВАНИЕ ДОМЕНА: СТАНДАРТНАЯ СИТУАЦИЯ....532
Сервер ns.company.tld....532
...Сервер ns.provider.net....533
Сервер ns.manager-tld.tld....534
15.3. ПРИМЕР 2. РАСШИРЕНИЕ КОМПАНИИ....534
Сервер ns.company.com....535
Сервер ns.branch.company.tld....535
15.4. РЕГИСТРАЦИЯ ДОМЕНА....536

ГЛАВА 16. ДЕЛЕГИРОВАНИЕ И РЕГИСТРАЦИЯ ОБРАТНЫХ ДОМЕНОВ....539
16.1. ВИДЫ И ТИПЫ ОБРАТНЫХ ДОМЕНОВ....540
16.2. ПРИМЕР ДЕЛЕГИРОВАНИЯ ОБРАТНОГО ДОМЕНА....541
16.2.1. Конфигурационные файлы....541
Сервер ns.firma.cz....542
Сервер ns.provider.net....543
Сервер ns.ripe.net (авторитетный сервер для вышестоящего домена)....543
16.2.2. Описание....543
16.2.3. Конфигурационные файлы (продолжение)....545
Сервер ns.firma.cz....545
Сервер ns.cbu.firma.cz....546
16.3. РЕГИСТРАЦИЯ ОБРАТНОГО ДОМЕНА....546

ГЛАВА 17. ИНТЕРНЕТ-РЕЕСТРЫ 549
17.1. МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ 550
17.2. РЕГИОНАЛЬНЫЕ ИНТЕРНЕТ-РЕЕСТРЫ (RIR) 552
17.3. КОДЫ СТРАН И RIR 553
17.4. IPv4-АДРЕСА И НОМЕРА АС 563
17.5. ИНТЕРНЕТ-РЕЕСТРЫ ИЛИ КАК ПОЛУЧИТЬ В УПРАВЛЕНИЕ ЧАСТЬ ИНТЕРНЕТА 564
17.5.1 Регистрация локального интернет-реестра (LIR) 564
17.5.2. Когда договор заключен 565
17.5.3. Базы данных RIPE 565
Объект Inetnum 566
Объект Domain (Домен) 567
Объекты Person (Персона) и Role(Роль) 567
Объект Aut-num 568
Объект маршрутизации 569
Объект Mntner 569
Просмотр содержимого базы данных 570
17.5.4. Связь с RIPE 571
Изменение базы данных 572
Как добавить объект в базу данных 572
Как модифицировать объект базы данных 574
Как удалить объект 575
17.5.5. Назначение IP-адресов и номеров автономных систем. Регистрация обратных доменов 575
17.5.6. Распределение адресного пространства 575
17.5.7. Защита и контроль над изменениями в базе RIPE. Уведомление и авторизация объектов 577
17.6. ДЕЛЕГИРОВАНИЕ ДОМЕНОВ ВТОРОГО УРОВНЯ 579

ГЛАВА 18. DNS В ЗАКРЫТЫХ КОРПОРАТИВНЫХ СЕТЯХ 580
18.1. ЗАКРЫТЫЕ КОРПОРАТИВНЫЕ СЕТИ И СВЯЗАННЫЕ С НИМИ DNS-ПРОБЛЕМЫ 581
18.2. КОРНЕВОЙ DNS-СЕРВЕР В WINDOWS SERVER 2000/2003 584

ГЛАВА 19. DNS И FIREWALL 585
19.1. ОБЩАЯ DNS: ДЛЯ ИНТЕРНЕТА И ЛОКАЛЬНОЙ СЕТИ 587
19.1.1. Трансляция всего Интернета по локальной сети 588
19.1.2. По локальной сети передаются только внутренние адреса 591
19.2. СЕРВЕР ИМЕН, ИНСТАЛЛИРОВАННЫЙ НА БРАНДМАУЭРЕ 593

19.2.1. Преобразование в локальной сети всего Интернета 593
19.2.2. Преобразование в локальной сети без преобразования в Интернете 594
19.3. ДУБЛИРОВАННЫЙ DNS 595

ГЛАВА 20. ЗАЩИТНЫЕ МЕХАНИЗМЫ И УЯЗВИМОСТИ TCP/IP И DNS 598
20.1. БЕЗОПАСНОСТЬ И УЯЗВИМОСТИ IP 599
Уязвимости IP 599
Методы атак на TCP/IP 600
Принципы IP-защиты 601
20.2. БЕЗОПАСНОСТЬ И УЯЗВИМОСТИ DNS 603
20.2.1. Уязвимости 603
20.2.2. Инструменты и механизмы защиты 604
Технология защиты TSIG 604
DNSSEC 605
СПИСОК ЛИТЕРАТУРЫ, ИСПОЛЬЗОВАННЫЙ ПРИ ПОДГОТОВКЕ РУССКОГО ИЗДАНИЯ КНИГИ 606