

Оглавление

Введение	16
Как организована книга	16
Дополнительные ресурсы	19
Обозначения, принятые в книге	19
Часть I	
Беспроводные сетевые технологии и их компоненты	21
Глава 1. Введение в IEEE 802.11	22
Стандарты IEEE 802.11	23
Уровень MAC 802.11	24
Подуровень PHY 802.11	25
IEEE 802.11	25
802.11b	26
802.11a	26
802.11g	26
Компоненты беспроводной сети 802.11	27
Станции	27
Беспроводные точки доступа	27
Порты	28
Режимы IEEE 802.11	28
Режим инфраструктуры	29
Специализированный режим	30
Заключение	31
Глава 2. Безопасность беспроводных сетей	32
Безопасность беспроводных сетей в стандарте 802.11	33
Аутентификация	33
Открытая аутентификация	33
Аутентификация с общим ключом	34
Шифрование и целостность данных	35
WEP	35
Процесс шифрования WEP	36
Процесс дешифрования WEP	36
Слабые места стандарта IEEE 802.11	37
Аутентификация в стандарте IEEE 802.1X	38
Основные элементы стандарта 802.1X	38
Контролируемые и неконтролируемые порты	40
EAP поверх LAN	41
Об исправлении уязвимостей стандарта 802.11 в стандарте 802.1X ..	41
Защищенный доступ Wi-Fi	42
Безопасность в WPA	43
Аутентификация	43
Шифрование	43
Целостность данных	44

Что нужно изменить в программном обеспечении для поддержки WPA	44
Беспроводные точки доступа	45
Беспроводные сетевые адаптеры	45
Беспроводные клиенты	46
Поддержка смешанной среды	46
Рекомендуемые конфигурации безопасности	46
Атаки на беспроводные сети	47
Заключение	48
Глава 3. Поддержка беспроводных клиентов в Windows	49
Windows XP (до SP1)	49
Поддержка беспроводных сетевых адаптеров	49
Поддержка роуминга	50
Служба беспроводной настройки	50
Принцип работы службы беспроводной настройки	50
Аутентификация IEEE 802.1X	52
Пользовательский интерфейс программ настройки беспроводных сетей	53
Область уведомлений рабочего стола	53
Диалоговое окно подключения к беспроводной сети	53
Вкладка Wireless Networks (Беспроводные сети)	55
Диалоговое окно Advanced вкладки Wireless Networks	56
Диалоговое окно свойств беспроводной сети	56
Вкладка Authentication (Проверка подлинности) в окне свойств беспроводного соединения	58
Windows XP (с SP1 и выше) и Windows Server 2003	59
Изменения в пользовательском интерфейсе конфигурации беспроводных сетей	59
Диалоговое окно Connect To Wireless Networks	59
Окно свойств беспроводного соединения	60
Изменения в обновлении беспроводной безопасности WPA	62
Windows 2000	64
Конфигурирование беспроводных клиентов Windows	66
Конфигурирование беспроводных клиентов вручную	66
Конфигурирование с помощью групповых политик	66
Заключение	72
Глава 4. RADIUS, IAS и Active Directory	73
RADIUS	73
Компоненты инфраструктуры RADIUS	73
Клиенты, запрашивающие доступ к ресурсам	74
Серверы, предоставляющие доступ к ресурсам	74
RADIUS-серверы	75
Базы данных учетных записей	75
RADIUS-прокси	76
Сообщения RADIUS	76
Процессы аутентификации, авторизации и учета в RADIUS	77
Способы защиты трафика RADIUS	78

Использование сильных общих секретов	78
Использование атрибута Message-Authenticator	79
Использование IPSec	80
IAS	80
Настройка IAS под Windows 2000	81
Настройка сервера IAS	81
Ведение журнала удаленного доступа – свойства локального файла	84
Настройка IAS в Windows Server 2003	86
Настройки сервера IAS	86
Ведение журналов удаленного доступа	87
IAS в качестве RADIUS-сервера	90
Конфигурирование клиентов RADIUS	91
Обзор политики удаленного доступа	93
Условия и ограничения политики удаленного доступа	93
Конфигурация политик удаленного доступа	94
Условия политики удаленного доступа	94
Разрешение удаленного доступа	95
Настройка профиля политики удаленного доступа	96
Авторизация соединения с помощью политики удаленного доступа	101
Авторизация по пользователю	101
Авторизация по группе	102
IAS в роли RADIUS-прокси	102
Обработка запросов на соединение	105
Политики обработки запросов на соединение	105
Группы удаленных RADIUS-серверов	110
Active Directory	113
Учетные записи	114
Входящие свойства учетных записей	115
Группы	117
Заключение	118
Глава 5. EAP	119
Типы EAP в Windows	120
EAP-MD5 CHAP	121
EAP-TLS	122
Конфигурирование EAP-TLS на беспроводном клиенте	123
Конфигурирование EAP-TLS на сервере IAS	125
Protected EAP (PEAP)	126
EAP поверх RADIUS	127
EAP-TLS и процесс аутентификации IEEE 802.1X	128
PEAP	130
Конфигурирование PEAP на беспроводном клиенте	131
Конфигурирование PEAP на сервере IAS	132
PEAP-MS-CHAP v2	134
Конфигурирование PEAP-MS-CHAP v2 на беспроводных клиентах	134

Конфигурирование PEAP-MS-CHAP v2 на сервере IAS	135
Взаимодействие PEAP и MS-CHAP v2	135
PEAP-TLS	137
Взаимодействие PEAP и TLS	137
Быстрое переподключение в PEAP	138
Заключение	139
Глава 6. Сертификаты и инфраструктура открытых ключей	140
Сертификаты	140
Поля сертификата	141
Инфраструктура открытых ключей	142
Центры сертификации	142
Иерархии сертификатов	144
Аннулирование сертификатов	146
Аннулирование сертификатов и IAS	147
Проверка сертификатов	149
Проверка сертификатов сервером IAS	149
Проверка сертификатов беспроводным клиентом Windows	151
Поддержка сертификатов в Windows	152
Управление сертификатами с помощью оснастки Certificates	152
Службы сертификатов	155
Получение сертификата для аутентификации IEEE 802.1X	156
Автоматическая подача заявок	156
Автоматическая подача заявки на сертификат компьютера	156
Автоматическая подача заявки на сертификат пользователя	158
Запрос сертификата через веб-страницу	158
Запрос сертификата с помощью оснастки Certificates	159
Импорт сертификата с помощью оснастки Certificates	159
Создание программы или сценария с использованием CAPICOM	161
Аутентификация компьютеров и пользователей	161
Аутентификация компьютеров и пользователей с помощью EAP-TLS	162
Аутентификация компьютеров и пользователей с помощью PEAP-MS-CHAP v2	162
Управление аутентификацией компьютеров и пользователей с помощью настройки параметра реестра AuthMode	163
Групповые политики и аутентификация IEEE 802.1X	164
EAP-TLS и групповая политика для компьютеров	164
EAP-TLS и групповая политика для пользователей	164
Использование сторонних СА для беспроводной аутентификации	165
Сертификаты на сервере IAS	165
Сертификаты на беспроводных клиентах	166
Заклучение	166

Часть II

Создание беспроводных сетей	167
Глава 7. Расположение точек доступа	168
Проектирование беспроводных сетей	168
Требования к беспроводным точкам доступа	168
Разделение каналов	170
Модификаторы распространения сигнала	171
Источники интерференции	172
Количество беспроводных точек доступа	172
Развертывание беспроводных точек доступа	173
Анализ расположения беспроводных точек доступа	174
Временная установка беспроводных точек доступа	175
Замер мощности сигнала	175
Перемещение беспроводных AP, источников затухания и интерференции	175
Проверка объема покрытия	175
Обновление плана	176
Заключение	176
Глава 8. Развертывание беспроводной локальной сети с использованием EAP-TLS	177
Необходимые компоненты	177
Конфигурирование инфраструктуры сертификатов	178
Установка инфраструктуры сертификатов	181
Настройка автоматической подачи заявок на сертификат компьютера	182
Настройка автоматической подачи заявок на сертификат пользователей	183
Настройка учетных записей и групп Active Directory для беспроводного доступа	186
Конфигурирование сервера IAS	186
Конфигурирование основного сервера IAS	187
Получение и установка сертификата компьютера	187
Установка IAS и его настройка	189
Настройка IAS для работы с клиентами RADIUS	193
Использование IPSec для защиты трафика RADIUS	194
Настройка политики удаленного доступа для беспроводных соединений	194
Конфигурирование IAS из Windows 2000	194
Конфигурирование IAS Windows Server 2003	196
Конфигурирование дополнительного сервера IAS	199
Получение и установка сертификата компьютера	199
Копирование конфигурации основного сервера IAS на дополнительный	200
Конфигурирование настроек групповой политики Wireless Network (IEEE 802.11)	200
Конфигурирование беспроводных точек доступа	202

Конфигурирование компьютеров беспроводных клиентов	202
Установка сертификата компьютера	202
Установка сертификата пользователя	203
Установка сертификата через веб-страницу	204
Запрос сертификата	204
Установка сертификата из файла сертификата	205
Конфигурирование аутентификации 802.1X для EAP-TLS	206
Заключение	207
Глава 9. Пример из практики: беспроводная сеть Microsoft	209
История беспроводной локальной сети Microsoft	209
Беспроводные сетевые технологии Microsoft	211
Размышления о проектировании и развертывании сети	211
Производительность	211
Масштабируемость	212
Роуминг и мобильность	212
Безопасность	212
Аутентификация	212
Подслушивание	213
Ложные беспроводные точки доступа	213
Развертывание беспроводной сети	214
Первый этап: предварительная установка	214
Второй этап: установка	214
Третий этап: доставка	215
Четвертый этап: подготовка к началу использования сети пользователями	215
Текущее состояние и инфраструктура	215
Контроллеры доменов Active Directory	216
Windows Server 2003 CA	217
Беспроводные клиенты, работающие под управлением Windows XP	218
Точки доступа Cisco Aironet серий 340 и 350	219
RADIUS-серверы и RADIUS-прокси, работающие под управлением Windows Server 2003	220
Дочерний домен North America	220
Другие дочерние домены	223
Леса NT.Dev, Win.SE и Win.Deploy	223
Настройки политики удаленного доступа для беспроводных соединений	224
Централизованная запись журнала в базу данных SQL	224
Заключение	224
Глава 10. Развертывание беспроводной локальной сети с использованием PEAP-MS-CHAP v2	226
Необходимые компоненты	226
Конфигурирование учетных записей и групп Active Directory для беспроводного доступа	227
Конфигурирование сервера IAS	229

Конфигурирование основного сервера IAS	229
Получение и установка сертификата компьютера	229
Установка IAS и его настройка	230
Настройка IAS для работы с клиентами RADIUS	235
Использование IPSec для защиты трафика RADIUS	236
Конфигурирование политики удаленного доступа для беспроводных соединений	236
Конфигурирование IAS из Windows 2000	236
Конфигурирование IAS из Windows Server 2003	238
Конфигурирование дополнительного сервера IAS	240
Получение и установка сертификата компьютера	241
Установка IAS и настройка компьютера дополнительного сервера на чтение свойств записей домена	241
Копирование конфигурации основного сервера IAS на дополнительный сервер	241
Конфигурирование настроек групповой политики беспроводной сети	242
Конфигурирование беспроводных точек доступа	243
Конфигурирование компьютеров беспроводных клиентов	244
Установка сертификата корневого CA	244
Конфигурирование аутентификации 802.1X для PEAP-MS-CHAP v2	247
Заключение	249
Глава 11. Дополнительное конфигурирование беспроводной локальной сети	250
Доступ в интернет для бизнес-партнеров	250
Использование гостевого доступа	251
Конфигурирование групп беспроводных гостей, содержащих гостевую учетную запись	252
Конфигурирование беспроводных точек доступа на использование VLAN, присоединенного к интернету	253
Конфигурирование политики удаленного доступа для гостевых беспроводных соединений	253
Конфигурирование беспроводных клиентов Windows для неаутентифицированного доступа	254
Использование ратифицированного доступа	256
Межлесная аутентификация	257
Конфигурирование инфраструктуры сертификатов	260
Конфигурирование лесов Active Directory для учетных записей и групп	260
Конфигурирование основного сервера IAS на компьютере из первого леса	260
Конфигурирование дополнительного сервера IAS на другом компьютере из первого леса	261
Конфигурирование основного сервера IAS на компьютере из второго леса	261

Конфигурирование дополнительного сервера IAS на другом компьютере из второго леса	261
Конфигурирование IAS как основного RADIUS-прокси	262
Конфигурирование IAS в качестве дополнительного RADIUS-прокси	264
Конфигурирование аутентификации RADIUS на беспроводных точках доступа	265
Конфигурирование компьютеров беспроводных клиентов	265
Использование RADIUS-прокси	
для масштабирования аутентификаций	266
Конфигурирование инфраструктуры сертификатов	267
Конфигурирование учетных записей и групп Active Directory	267
Конфигурирование IAS в качестве RADIUS-сервера на нескольких компьютерах	268
Конфигурирование IAS в качестве основного RADIUS-прокси	268
Конфигурирование IAS в качестве дополнительного RADIUS-прокси	270
Конфигурирование аутентификации RADIUS на беспроводных точках доступа	270
Конфигурирование компьютеров беспроводных клиентов	271
Одновременное использование	
аутентификаций EAP-TLS и PEAP-MS-CHAP v2	271
Конфигурирование IAS из Windows 2000 для одновременной поддержки EAP-TLS и PEAP-MS-CHAP v2	271
Windows 2000 и типы EAP	272
Конфигурирование IAS из Windows Server 2003 для одновременной поддержки EAP-TLS и PEAP-MS-CHAP v2	273
Заключение	274
Глава 12. Защищенные беспроводные сети	
для дома и малого бизнеса	275
Настройка безопасности беспроводной сети	276
Безопасность беспроводной сети	277
Шифрование	277
Шифрование WEP	277
Выбор ключа WEP	278
Шифрование WPA	278
Аутентификация	279
Аутентификация открытых систем	279
Аутентификация с общим ключом	279
Аутентификация IEEE 802.1X	279
Аутентификация WPA с предварительным ключом	280
Рекомендуемый метод аутентификации: WPA-PSK или аутентификация открытых систем	281
Использование службы WZC в Windows XP	282
Настройка беспроводной сети, использующей беспроводные точки доступа	282

Конфигурирование беспроводных точек доступа	282
Конфигурирование беспроводных клиентов Windows	284
Конфигурирование беспроводных клиентов на использование WEP	284
Конфигурирование беспроводных клиентов для использования WPA	288
Настройка беспроводной сети без беспроводных точек доступа	289
Конфигурирование основного беспроводного клиента	290
Конфигурирование дополнительных беспроводных клиентов Windows XP	293
Заключение	295
Глава 13. Инфраструктура RADIUS для предоставления общего доступа	297
Компоненты инфраструктуры RADIUS для беспроводного доступа в общественных местах	299
Конфигурирование беспроводного ISP	301
Конфигурирование беспроводных точек доступа	301
Конфигурирование IAS, работающего в качестве основного RADIUS-прокси	301
Установка IAS и его настройка	302
Конфигурирование основного IAS RADIUS-прокси для работы с RADIUS-клиентами	304
Конфигурирование политики обработки запросов на соединение для основного RADIUS-прокси	305
Конфигурирование IAS в качестве дополнительного RADIUS-прокси	309
Настройка поставщика услуг	309
Настройка частных организаций	310
Использование IAS в качестве RADIUS-сервера	310
Конфигурирование основного и дополнительного серверов IAS во внешней сети	312
Конфигурирование фильтров пакетов на межсетевом экране ...	312
Использование IAS в качестве RADIUS-прокси	313
Конфигурирование основного IAS RADIUS-прокси в наружной сети	314
Конфигурирование дополнительного IAS RADIUS-прокси в наружной сети	316
Конфигурирование основного и дополнительного серверов IAS в локальной сети	316
Заключение	320
Часть III	
Поиск и устранение неисправностей в беспроводных сетях ...	321
Глава 14. Проблемы с беспроводными клиентами Windows	322
Инструменты для поиска неисправностей	322
Папка Network Connections	323
Трассировка	324

Сетевой монитор Microsoft	325
Оснастка Wireless Monitor	326
Распространенные проблемы с соединением и аутентификацией	327
Заключение	329
Глава 15. Проблемы с беспроводными точками доступа	330
Инструменты обнаружения неисправности беспроводной точки доступа	330
Индикаторы на панели	330
Программы обследования местности	331
Поддержка SMNP	331
Диагностика	332
Распространенные проблемы беспроводных точек доступа	332
Невозможно увидеть беспроводную точку доступа	332
Невозможно аутентифицироваться на беспроводной точке доступа	333
Параметры 802.1X	334
Параметры RADIUS	334
Конфигурация WPA	336
Можно связаться только с беспроводной точкой доступа	336
Заклучение	337
Глава 16. Решение проблем аутентификационной инфраструктуры	338
Инструменты обнаружения неисправностей в IAS	338
Запись в журнал событий IAS	338
Сетевой монитор	339
Запись в журнал событий SChannel	339
Трассировка	340
Агент SMNP	341
Оснастка Performance Logs and Alerts	341
Решение проблем аутентификации и авторизации IAS	341
Решение проблем проверки сертификатов	343
Проверка сертификатов, установленных на беспроводном клиенте	343
Проверка сертификата сервера IAS	347
Решение проблем с проверкой паролей	347
Проверка учетных данных беспроводного клиента	348
Проверка сертификата сервера IAS	348
Общие проблемы аутентификации	349
Заклучение	351
Часть IV	
Приложения	353
Приложение А. Оптимальные способы развертывания беспроводных сетей	354
Безопасность	354
PKI	355

Беспроводные точки доступа	357
Беспроводные сетевые адаптеры	357
Active Directory	357
RADIUS	358
Работа	360
Масштабируемость	360
Приложение В. Беспроводные ISP	
и службы Windows Provisioning Services	361
Служба Wireless Provisioning Services в Windows XP	362
Приложение С. Настройка защищенного беспроводного доступа	
в тестовой лаборатории	363
Аутентификация PEAP-MS-CHAP v2	363
DC1	365
IAS1	374
PIS1	380
Беспроводная точка доступа	381
CLIENT1	381
Аутентификация EAP-TLS	383
DC1	383
IAS1	389
CLIENT1	392
Заключение	393
Алфавитный указатель	394