



**Эд Уилсон**

# Мониторинг и анализ сетей

**Реальные сценарии,  
простые примеры,  
множество иллюстраций**

**Улучшение производительности  
и поддержка новых приложений**

**Профессиональные приемы  
мониторинга безопасности  
и защита**

# **Мониторинг и анализ сетей**

---

Эд Уилсон

**Издательство “Лори”**

# **Network Monitoring and Analysis**

---

A Protocol Approach to Troubleshooting

Ed Wilson

**Prentice Hall PRT**

---

Upper Saddle River, New Jersey 07458

**Network Monitoring and Analysis**  
**A Protocol Approach to Troubleshooting**  
Ed Wilson

Copyright ©by Prentice Hall PRT  
All rights reserved  
ISBN 0-13-026495-4

**Мониторинг и анализ сетей**  
Эд Уилсон

Переводчик *О. Труфанов*  
Корректор *И. Гришина*  
Верстка *Л. Федякина*

© Издательство "ЛОРИ", 2021  
Изд. № : ОАІ (03)  
ЛР № : 07612 30.09.97 г.  
ISBN 978-5-85582-437-7

Подписано в печать 04.05.2021 Формат 70 × 100/16  
Бумага газетная, Гарнитура Баскервиль, Печать офсетная  
Печ. л. 23, Ти раж 100

# Содержание

<b>ЧАСТЬ I Анализ протоколов: участники взаимодействия</b>	<b>1</b>
<b>Глава 1 Базовые сетевые модели</b>	<b>3</b>
Модель OSI	3
Уровень приложений	6
Уровень представлений	7
Сеансовый уровень	8
Транспортный уровень	9
Сетевой уровень	10
Канальный уровень	11
Физический уровень	12
Проект IEEE 802	13
Усовершенствования, сделанные в модели OSI	13
Подуровень управления логическим каналом (LLC)	13
Подуровень управления доступом к среде передачи (MAC)	15
Как данные перемещаются по проводам	15
Процесс создания пакета	16
Особенности коммуникации в сетях Ethernet	18
Какова во всем этом роль протоколов?	21
Стек протоколов	21
Иерархический подход	22
Как все это объединяется?	24
Прикладные протоколы	26
Транспортные протоколы	26
Сетевые протоколы	27
Сетевая служба с поддержкой соединения	27
Сетевая служба без поддержки соединения	28
Адресация на канальном уровне	29
Адресация на сетевом уровне	29
Инкапсуляция данных	30
Реализация IP поверх различных стандартов LAN	31
Управление потоком	35
Функции межсетевого обмена сетевого уровня OSI	36
Службы WAN	36
Обзор главы	41
В следующей главе	42
<b>Глава 2 Стек протоколов TCP/IP</b>	<b>43</b>
Протокол TCP	46
Заголовок TCP	47
Трехходовое квитирование	50
Концепция времени молчания TCP	52
Полуоткрытые соединения и другие аномалии	53
Генерация команды сброса	54
Обработка команды сброса	55
Сценарий 1: локальный пользователь инициирует закрытие	56
Сценарий 2: TCP получает FIN из сети	56

Сценарий 3: оба пользователя закрывают соединение одновременно	57
Обмен срочной информацией	57
Управление окном	57
Интерфейс пользователь/TCP	59
Команды пользователя TCP	59
Send (Послать)	60
Receive (Получить)	62
Close (Закреть)	62
Status Abort (Прервать)	63
TCP/Низкоуровневый интерфейс	63
Происходящие события: пользовательские вызовы	64
Состояние прослушивания	65
Вызов SEND (Послать)	65
Протокол IP	67
Заголовок IP	71
Обзор главы	84
В следующей главе	84
<b>Глава 3 Стек протоколов SPX/IPX</b>	<b>85</b>
Протокол SPX	85
Заголовок SPX	85
Протокол IPX	91
Протокол без соединения	91
Работа на сетевом уровне модели OSI	91
Структура пакета	92
Адресация IPX	95
Сетевой номер	95
Зарезервированные сетевые номера	96
Внутренний сетевой номер	96
Номер узла	96
Номер сокета	97
Как работает маршрутизация IPX	98
Интерфейсы сеансов и дейтаграмм	100
Структуры заголовка сообщений	101
Обзор главы	103
В следующей главе	103
<b>Глава 4 Блоки сообщений сервера</b>	<b>104</b>
Обзор работы SMB	105
Определение имени сервера	105
Разрешение имени сервера	106
Транспорт сообщения	106
Пример потока сообщений	106
Согласование диалекта	108
Создание соединения	108
Обратная совместимость	109
Настройка сеанса	109
Управление соединением	109
Подпись SMB	110
Оппортунистические блокировки	110
Исключающая oplock	111
Пакетная блокировка oplock	112
Level II Oplocks	114

Модель безопасности	115
Пример доступа/общего ресурса	116
Аутентификация	117
Поддержка распределенной файловой системы (DFS)	118
Заголовок SMB	119
Поле TID	120
Поле UID	120
Поле PID	120
Поле MID	121
Поле флагов	121
Поле Flags2	123
Поле состояния	123
Задержки	124
Буфер данных (BUFFER) и форматы строк	124
Кодирование режима доступа	125
Кодирование функции открытия (Open)	126
Кодирование действия открытия (Open)	126
Кодирование атрибутов файла	127
Кодирование расширенных атрибутов файла	127
Пакетные запросы (Сообщения "AndX")	128
Обзор главы	130
В следующей главе	130

## ЧАСТЬ II Сетевой трафик

### Анализ и оптимизация: взгляд на проблемы . . . . . 131

#### Глава 5 Клиентский трафик . . . . . 133

Инициализация клиента	133
Трафик DHCP	134
Трафик клиента WINS	142
Регистрация имен и обновление	142
Трафик регистрации в системе	147
Поиск сервера регистрации	148
Оптимизация регистрации в сети	156
Просмотр	159
Объявления хостов броузеров	161
Где находятся резервные броузеры?	163
Оптимизация трафика броузера	165
Обзор главы	166
В следующей главе	166

#### Глава 6 Серверный трафик . . . . . 167

DNS	167
Разрешение адреса	167
Рекурсивный поиск	169
Объединение с WINS	170
Оптимизация DNS	170
Инициализация BDC	170
Где находится PDC?	171
Обновления в базе данных	184
Оптимизация трафика синхронизации учетных записей	186
Служба NetLogon	186

Обзор главы . . . . .	190
В следующей главе . . . . .	190
<b>Глава 7 Трафик приложений . . . . .</b>	<b>191</b>
Работа с файлами и печать . . . . .	191
Запрос WINS . . . . .	191
Широковещание . . . . .	192
ARP . . . . .	193
Трехходовое квитиование . . . . .	194
Сеанс NetBIOS . . . . .	195
Согласование диалекта SMB . . . . .	196
Просмотр Интернета . . . . .	201
Страницы Web . . . . .	201
Secure Sockets Layer . . . . .	207
Оптимизация трафика броузера в интрасети . . . . .	208
Обзор главы . . . . .	209
В следующей главе . . . . .	209
<b>Глава 8 Exchange и почта Интернета . . . . .</b>	<b>210</b>
Exchange . . . . .	210
Открытие и закрытие сеанса . . . . .	213
Сервер Exchange в действии . . . . .	214
Протокол POP3 . . . . .	216
Общение Exchange с другим сервером . . . . .	226
Обзор главы . . . . .	229
В следующей главе . . . . .	229
<b>ЧАСТЬ III Сетевые мониторы: инструментальные средства работы . . . . .</b>	<b>231</b>
<b>Глава 9 Семейство сетевых мониторов компании Microsoft . . . . .</b>	<b>233</b>
Сетевой монитор . . . . .	233
Создание перехвата . . . . .	234
Перехват трафика вручную . . . . .	236
Просмотр перехваченных данных . . . . .	238
Сохранение перехваченных данных . . . . .	239
Фильтрация данных перехвата . . . . .	240
Анализ перехваченных данных . . . . .	242
Система безопасности сетевого монитора . . . . .	245
Защита с помощью пароля . . . . .	246
Установка сетевого монитора: обнаружение других мониторов . . . . .	247
Сетевой монитор Systems Management Server 1.2 . . . . .	249
Дополнительные свойства . . . . .	249
Соединение с удаленными агентами . . . . .	251
Мастера-помощники . . . . .	252
Конфигурирование триггеров . . . . .	254
Network Monitor 2.0 . . . . .	256
Новые свойства . . . . .	256
А вот это не работает . . . . .	259
Дополнительные свойства безопасности . . . . .	259
Обзор главы . . . . .	263
В следующей главе . . . . .	264



<b>ЧАСТЬ IV Сценарии поиска неисправностей:</b>	
<b>распространенные проблемы</b>	<b>265</b>
<b>Глава 10 Вопросы поиска неисправностей</b>	<b>267</b>
Рабочая станция не может зарегистрироваться	267
Можно ли сделать ring сервера?	267
Рассмотрим случай с портативным компьютером	272
Рабочая станция не может получить выделяемый DHCP адрес	272
Взгляд на диалог	273
Проанализируйте, что пропущено	273
Рабочая станция работает медленно	275
Можно ли точно определить понятие "медленная"?	275
Что является источником недовольства?	275
Проблемы с регистрацией	276
Я пытаюсь аутентифицироваться, но где?	277
Странные ошибки журнала событий	281
Метод поиска серверных проблем	281
Выполнение без сопровождения	283
Избыточное ширококовещание	285
Кто это делает?	285
Почему они это делают?	287
Обзор главы	288
В следующей главе	288
<b>Глава 11 Вопросы безопасности</b>	<b>289</b>
Нелегальные серверы DHCP	289
Есть ли у меня для вас адрес?	289
Итак, где вы?	294
Нелегальный анализ сети ("вынюхивание")	294
Прежде всего необходимо их найти	295
Как отбить нюх чужим ищейкам	295
Обзор главы	296
<b>Приложение А Список общеизвестных номеров портов TCP и UDP</b>	<b>297</b>
<b>Приложение В Утилиты командной строки</b>	<b>310</b>
<b>Приложение С Общие NCP</b>	<b>312</b>
<b>Приложение D Поиск обычных сетевых ошибок</b>	<b>321</b>
<b>Приложение E Суффиксы NetBIOS</b>	<b>323</b>
<b>Приложение F Запуск контроллера домена</b>	<b>325</b>
<b>Приложение G Открытие страницы Web</b>	<b>336</b>
<b>Глоссарий</b>	<b>347</b>