

Администрирование сетей Cisco: освоение за месяц

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
	1 Before you begin	2 What is a Cisco network?	3 Cisco's internetwork operating system (IOS)	4 Managing switch ports
	✓	✓ <i>immense</i>	✓ <i>class act</i>	✓
7 Securing ports	8 Managing virtual LANs (VLANs)	9 Breaking the VLAN barrier	10 IP address assignment	11 Securing the network
✓ <i>masterful</i>	✓ <i>brilliant</i>	✓	✓	
14 Connecting switches using trunk links	15 Automatically configuring VLANs	16 Protecting against bridging loops	17 Optimizing network performance	18 Making the network scalable
				19
21 Manually directing traffic	22 A dynamic routing protocols crash course	23 Tracking down devices	24 Securing Cisco devices	25 Facilitating trouble shooting
				26
28 Recovering from disaster	29 Next steps	30 More on Next Steps	31	

Бен Пайпер

УДК 004.71
ББК 32.972.5
П12

Пайпер Б.

П12 Администрирование сетей Cisco: освоение за месяц / пер. с англ. М. А. Райтмана. – М.: ДМК Пресс, 2018. – 316 с.: ил.

ISBN 978-5-94074-519-6

Эта книга в доступной форме рассказывает об администрировании сетей с применением оборудования Cisco. С помощью практических заданий вы сможете за месяц получить полное представление о том, как работают сети, и получите знания, которые сможете использовать уже сегодня. Вы сможете не только усовершенствовать свои навыки, но так же будете в состоянии объяснить, почему сети работают так, а не иначе.

Издание будет полезно начинающим администраторам сетей.

УДК 004.71
ББК 32.972.5

Authorized Russian translation of the English edition of Learn Cisco Network Administration in a Month of Lunches ISBN 9781617293634 © 2017 by Manning Publications Co.

This translation is published and sold by permission of Manning Publications Co., which owns or controls all rights to publish and sell the same.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-617-29363-4 (анг.)
ISBN 978-5-94074-519-6 (рус.)

Copyright © 2017 by Manning Publications Co.
© Оформление, издание, перевод, ДМК Пресс, 2018

Содержание

Предисловие	12
Благодарности	13
Об этой книге	14
Об авторе	16
Глава 1. Прежде чем начать	17
1.1. Для вас ли эта книга?.....	17
1.2. Как пользоваться этой книгой.....	18
1.2.1. Основные главы.....	19
1.2.2. Практические занятия.....	19
1.2.3. Углубленное изучение.....	19
1.2.4. Дополнительно.....	19
1.3. Практические соображения.....	19
1.3.1. Выбор тестового оборудования.....	20
1.3.2. Рассмотрим виртуальную лабораторию.....	21
1.3.3. Практика в условиях реальной сети.....	21
1.3.4. Мои рекомендации для вашей тестовой среды.....	22
1.3.5. Версии операционной системы Cisco IOS.....	22
1.4. Онлайн-ресурсы.....	23
1.5. Замечание по моим рекомендациям.....	23
1.6. Немедленно стать эффективным администратором сетей.....	24
Глава 2. Что такое сети Cisco?	25
2.1. Правда о коммутаторах и маршрутизаторах.....	26
2.2. MAC-адрес.....	27
2.3. Ethernet-кадр: большой конверт.....	29
2.3.1. Когда все говорят, никто не слушает.....	30
2.4. Широковещательные домены.....	31
2.4.1. Избавление от лавинной передачи: таблица MAC-адресов.....	32
2.4.2. Разделение широковещательного домена.....	33
2.4.3. Соединение широковещательных доменов.....	34
2.4.4. Адресация устройств из разных широковещательных доменов.....	35
2.5. Адреса протокола Интернета.....	35
2.5.1. Где ты?.....	36
2.5.2. Дилемма: IP- или MAC-адрес.....	37
2.5.3. ARP: протокол определения адреса.....	37

2.6. Связь широковещательных доменов с помощью маршрутизатора.....	39
2.6.1. Где ты? И где я?	39
2.6.2. Определение подсети.....	39
2.7. Пересылка между доменами с использованием шлюза по умолчанию.....	42
2.8. Управление маршрутизаторами и коммутаторами	46
2.9. Практическое задание	46
Глава 3. Краткий курс по операционной системе Cisco IOS	47
3.1. Что такое IOS?.....	47
3.2. Авторизация на устройствах Cisco	48
3.3. Команда show	50
3.3.1. Фильтрация вывода.....	53
3.4. Идентификация версии и пакета IOS.....	56
3.4.1. Номера версий	56
3.4.2. Пакеты	57
3.5. Просмотр рабочей конфигурации	57
3.6. Изменение рабочей конфигурации	59
3.7. Сохранение конфигурации запуска	61
3.8. Команда по	62
3.9. Команды, использованные в этой главе.....	64
3.10. Практическое задание	64
Глава 4. Управление портами коммутатора	65
4.1. Просмотр состояния порта.....	66
4.2. Включение портов	68
4.2.1. Команда interface range	70
4.3. Отключение портов	71
4.3.1. Поиск неиспользуемых интерфейсов	72
4.4. Изменение скорости порта и дуплекса	73
4.4.1. Скорость	73
4.4.2. Дуплекс.....	74
4.4.3. Автосогласование	74
4.4.4. Изменение скорости порта	75
4.4.5. Изменение дуплексного режима.....	76
4.5. Команды, использованные в этой главе.....	77
4.6. Практическое задание	78
Глава 5. Защита портов с помощью технологии Port Security.....	79
5.1. Конфигурация минимального уровня функции Port Security	80
5.1.1. Предотвращение атаки по MAC-адресу	80
5.1.2. Режим нарушения.....	84
5.2. Проверка функции Port Security	85
5.3. Перемещение устройств.....	86
5.3.1. Port Security помнит все!.....	87

5.3.2. Время старения	88
5.4. Запрещение доступа неавторизованных устройств	90
5.4.1. Обеспечение максимальной защиты с помощью функции Port Security	91
5.4.2. «Липкие» MAC-адреса	91
5.4.3. Предостережение о «липких» MAC-адресах	94
5.5. Команды, использованные в этой главе	94
5.6. Практическое задание	95
Глава 6. Управление виртуальными локальными сетями	96
6.1. Что такое виртуальная локальная сеть?	96
6.2. Инвентаризация виртуальных локальных сетей	97
6.2.1. База данных виртуальной сети	97
6.2.2. Виртуальная сеть по умолчанию	99
6.2.3. Сколько виртуальных сетей создавать?	99
6.2.4. Планирование новой виртуальной сети	99
6.3. Создание виртуальных локальных сетей	100
6.4. Назначение виртуальных локальных сетей	102
6.4.1. Проверка конфигурации порта	102
6.4.2. Настройка доступа к виртуальной сети	103
6.4.3. Настройка режима доступа	104
6.5. Виртуальная сеть для пропуска голосового трафика	105
6.6. Работа в созданных виртуальных сетях	107
6.7. Команды, использованные в этой главе	108
6.8. Практическое задание	108
Глава 7. Преодоление барьера виртуальной сети с помощью коммутируемых виртуальных интерфейсов	109
7.1. Соединение «виртуальная сеть – подсеть»	110
7.2. Коммутаторы или маршрутизаторы?	114
7.2.1. Включение IP-маршрутизации	115
7.3. Что такое коммутируемые виртуальные интерфейсы?	116
7.3.1. Создание и конфигурирование SVI-интерфейсов	117
7.4. Шлюзы по умолчанию	119
7.4.1. Тестирование соединения между виртуальными сетями	120
7.5. Команды, использованные в этой главе	121
7.6. Практическое задание	121
Глава 8. Назначение IP-адресов с использованием протокола DHCP	123
8.1. Коммутатор или не коммутатор?	124
8.2. Конфигурирование DHCP-сервера Cisco	124
8.2.1. Области адресов	125
8.2.2. Опции	126
8.2.3. Время аренды	126
8.2.4. Подсети и виртуальные локальные сети	127

8.3. Настройка пула DHCP	127
8.4. Исключение адреса из списка выдаваемых адресов	129
8.5. Настройка устройств для запроса адресов у DHCP-сервера	130
8.6. Ассоциирование пулов DHCP с виртуальными сетями	132
8.7. Создание второго пула DHCP	134
8.8. Просмотр аренды DHCP	136
8.9. Использование DHCP-серверов других компаний	136
8.9.1. Решение проблемы передачи DHCP Discover с помощью команды ip helper-address	138
8.10. Команды, использованные в этой главе	139
8.11. Практическое задание	139
Глава 9. Обеспечение безопасности сети с помощью списков контроля доступа.....	140
9.1. Блокирование трафика «IP–IP»	141
9.1.1. Создание списка контроля доступа	142
9.2. Применение списка контроля доступа к интерфейсу	146
9.3. Блокировка трафика «IP-подсеть»	148
9.3.1. Подстановочные маски	149
9.3.2. Замена списка ACL	150
9.3.3. Применение списка управления доступом к коммутируемому виртуальному интерфейсу	152
9.4. Блокирование трафика «подсеть–подсеть»	153
9.5. Команды, использованные в этой главе	157
9.6. Практическое задание	157
Глава 10. Подключение коммутаторов с использованием транков	158
10.1. Подключение дополнительного коммутатора	159
10.2. Принципы транков виртуальной сети	160
10.2.1. Настройка транка виртуальной сети	161
10.2.2. Настройка протокола DTP для автоматического согласования транка	162
10.3. Настройка Коммутатора 2	164
10.3.1. Настройка виртуальных сетей на дополнительном коммутаторе	166
10.4. Перемещение устройств на другой коммутатор	167
10.5. Изменение инкапсуляции транка	169
10.6. Команды, использованные в этой главе	171
10.7. Практическое задание	171
Глава 11. Автоматическая настройка виртуальных сетей с помощью протокола VTP	173
11.1. Пара слов в предостережение	174
11.2. Настройка Коммутатора 1 в качестве VTP-сервера	175
11.3. Настройка Коммутатора 2 в качестве VTP-клиента	176
11.4. Создание виртуальных сетей на Коммутаторе 1	178

11.5. Включение VTP-отсечения	180
11.6. Команды, использованные в этой главе	185
11.7. Практическое задание.....	185
Глава 12. Защита от петель коммутации с помощью протокола STP	186
12.1. Как работает протокол STP.....	188
12.1.1. Как протокол STP действует в случае потери соединения	190
12.2. Протокол RSTP.....	193
12.3. Режим PortFast.....	195
12.4. Команды, использованные в этой главе.....	197
12.5. Практическое задание	198
Глава 13. Оптимизация сети с использованием каналов порта	199
13.1. Статический или динамический агрегированный канал?.....	200
13.1.1. Статический агрегированный канал.....	200
13.1.2. Динамический агрегированный канал	201
13.2. Настройка динамического агрегированного канала с помощью протокола LACP.....	201
13.3. Создание статического агрегированного канала	205
13.4. Методы балансировки нагрузки	207
13.5. Команды в этой главе.....	211
13.6. Практическое задание	211
Глава 14. Обеспечение масштабируемости сети путем совместного использования маршрутизаторов и коммутаторов.....	212
14.1. Конфигурация «маршрутизатор-на-палочке»	213
14.2. Подключение Маршрутизатора 1	215
14.3. Настройка субинтерфейсов	216
14.4. Таблица IP-маршрутизации	221
14.5. Применение списка доступа на субинтерфейсе	223
14.6. Команды в этой главе.....	224
14.7. Практическое задание.....	225
Глава 15. Направление трафика вручную с использованием таблицы IP-маршрутизации.....	226
15.1. Подключение Маршрутизатора 1 к Коммутатору 2.....	228
15.2. Настройка транзитных подсетей	229
15.2.1. Назначение транзитных IP-адресов непосредственно физическим интерфейсам	230
15.2.2. Назначение транзитных IP-адресов субинтерфейсам и SVI-интерфейсам	231
15.3. Удаление транка между коммутаторами	233
15.4. Настройка шлюзов по умолчанию	233
15.5. Создание пула DHCP для подсети Executives	235

15.6. Команды, использованные в этой главе	242
15.7. Практическое задание.....	242

Глава 16. Интенсивный курс по протоколам динамической маршрутизации.....

16.1. Идентификаторы маршрутизаторов	245
16.1.1. Настройка loopback-интерфейсов	245
16.2. Настройка протокола EIGRP.....	246
16.2.1. Выбор наилучшего маршрута	252
16.2.2. Маршрутизация при сбоях.....	255
16.2.3. Выводы по протоколу EIGRP.....	255
16.3. Протокол OSPF.....	256
16.4. Команды, использованные в этой главе.....	261
16.5. Практическое задание	262

Глава 17. Обнаружение устройств.....

17.1. Сценарии обнаружения устройств	263
17.2. Этапы обнаружения устройства	264
17.2.1. Получение IP-адреса.....	264
17.2.2. Обнаружение устройства до последнего перехода.....	264
17.2.3. Получение MAC-адреса.....	264
17.3. Пример 1 – обнаружение сетевого принтера	265
17.3.1. Обнаружение последнего перехода с помощью команды traceroute.....	265
17.3.2. Протокол CDP	266
17.3.3. Получение MAC-адреса устройства	267
17.3.4. Просмотр таблицы MAC-адресов	268
17.4. Обнаружение сервера.....	269
17.4.1. Обнаружение последнего перехода с помощью команды traceroute.....	269
17.4.2. Получение MAC-адреса устройства	270
17.4.3. Просмотр таблицы MAC-адресов	271
17.5. Команды, использованные в этой главе	273
17.6. Практическое задание.....	274

Глава 18. Защита устройств Cisco

18.1. Создание привилегированной учетной записи пользователя	276
18.1.1. Проверка учетной записи	276
18.2. Реконфигурация линий VTY.....	278
18.2.1. Включение доступа по SSH и запрет доступа по Telnet	279
18.2.2. Ограничение доступа по протоколу SSH с использованием списков доступа.....	280
18.3. Защищаем консольный порт.....	282
18.4. Команды, использованные в этой главе.....	283
18.5. Практическое задание	284

Глава 19. Содействие устранению неполадок с помощью журналирования и отладки	285
19.1. Настройка журналирования	286
19.2. Инструменты отладки	287
19.2.1. Отладка функции Port Security	288
19.2.2. Отладка DHCP-сервера	289
19.2.3. Отладка протокола VTP	290
19.2.4. Отладка IP-маршрутизации	291
19.3. Уровни важности событий	292
19.4. Настройка syslog-сервера	294
19.5. Команды, использованные в этой главе	295
19.6. Практическое задание	296
Глава 20. Восстановление после сбоя	297
20.1. Ограничьте область поиска подмножеством устройств	298
20.2. Перезагрузка устройства	298
20.2.1. Перезагрузка по расписанию	299
20.3. Удаление конфигурации запуска	301
20.4. Сброс пароля	302
20.4.1. Сброс пароля на маршрутизаторе	303
20.4.2. Сброс пароля на коммутаторе	305
20.5. Команды, использованные в этой главе	305
Глава 21. Контрольный список производительности и работоспособности	307
21.1. Перегружен ли процессор?	308
21.2. Каково время непрерывной работы системы?	309
21.3. Поврежден ли сетевой кабель или разъем?	309
21.4. Пинг необычно велик или сбоит?	310
21.5. Нестабильны ли маршруты?	311
21.6. Команды, использованные в этой главе	313
21.7. Практическое задание	313
Глава 22. Следующие шаги	314
22.1. Сертификационные ресурсы	314
22.2. Лаборатория виртуальной интернет-маршрутизации Cisco	315
22.3. Устранение неполадок с позиции конечного пользователя	315
22.4. Никогда не останавливайтесь	316
Предметный указатель	317

Глава 2

Что такое сети Cisco?

Любая организация проводит основные объемы трафика через устройства двух типов: коммутаторы и маршрутизаторы. Cisco – наиболее популярный бренд, производящий надежные коммутаторы и маршрутизаторы, поэтому многие компании приняли его как стандарт для подобного рода устройств. Для прочего сетевого оборудования, например брандмауэра или точки беспроводного доступа, кто-то предпочитает Cisco, кто-то выбирает что-нибудь другое или использует бренды совместно. Но если сеть построена с использованием маршрутизаторов и коммутаторов Cisco, то это сеть Cisco.

Нет никаких обязательных требований к тому, чтобы использовать исключительно этот бренд. Вы можете использовать коммутаторы Cisco с маршрутизаторами Juniper, и они будут прекрасно работать вместе. Можно использовать маршрутизатор Cisco с коммутатором Juniper, и они тоже прекрасно уживутся. Но есть парочка возражений против подобных тандемов.

Во-первых, последовательность конфигурирования устройств Cisco в корне отлична от настройки оборудования Juniper. Синтаксис команд и терминология совершенно различны. Администрирование смешанных сетей требует знаний обеих платформ и принципов их взаимодействия, а эта книга посвящена только оборудованию компании Cisco.

Во-вторых, если у вас возникают проблемы и вы не уверены, связаны они с маршрутизатором или коммутатором, вам придется обращаться за техподдержкой сразу к обеим компаниям. В худшем случае каждая компания начнет тыкать пальцем в конкурента. В лучшем случае это чревато задержками, пока они придут к соглашению.

Использование в одной сети коммутаторов и маршрутизаторов разных брендов – это плохая идея. Вот почему большинство компаний использует и маршрутизаторы, и коммутаторы только компании Cisco. Так проще. И даже если у вас смешанная сетевая среда, эта книга все равно будет вам полезна, чтобы научиться администрировать коммутаторы и маршрутизаторы Cisco. Просто напомню, что в этой книге описывается сеть Cisco, и это *всегда* маршрутизаторы и коммутаторы компании Cisco.

На рис. 2.1 показано, как мой компьютер пересылает «конверт», содержащий некоторые данные, на сервер базы данных. В этой главе вы узнаете, как коммутаторы и маршрутизаторы определяют наилучший путь для передачи данных.

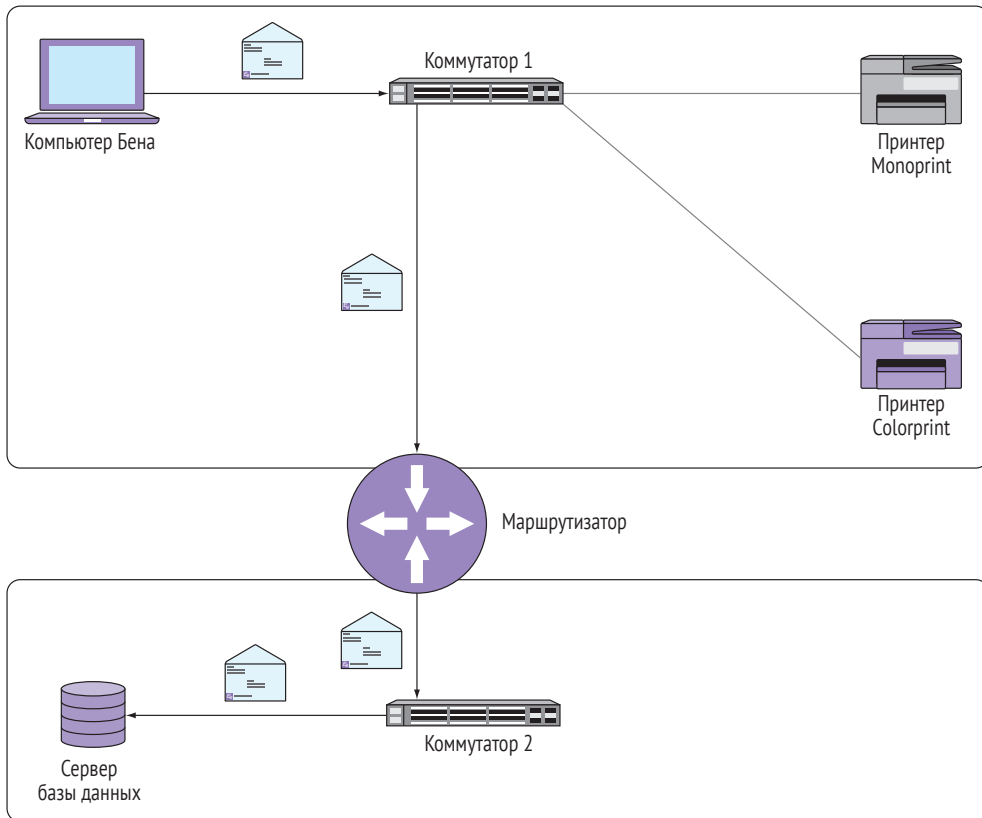


Рис. 2.1 ❖ Коммутаторы и маршрутизатор в сети

2.1. ПРАВДА О КОММУТАТОРАХ И МАРШРУТИЗАТОРАХ

Новички часто задают два вопроса:

- что на самом деле делают коммутаторы и маршрутизаторы?
- почему эти устройства имеют и MAC- и IP-адреса?

Эти, казалось бы, простые вопросы не имеют простых ответов. Я неоднократно наблюдал попытки дать ответ на эти вопросы в нескольких предложениях, но все эти попытки вносили лишь больше сумятицы и еще больше запутывали.

Истина в том, что и коммутаторы, и маршрутизаторы – это порождение конкретной технологической необходимости, а не каких-либо общих практических надобностей. В принципе, ни один из этих приборов не наделен какой-то особенной интеллектуальностью, хотя Cisco и снабжает их некоторым количеством «мозгов», чтобы улучшить их функциональность. Как и большинство

технологий, коммутаторы и маршрутизаторы появились как результат сомнительных решений, принятых десятилетия назад.

Новые технологии обычно строятся на более ранних. Например, электронные книги позаимствовали концепции *страниц* и *закладок* у традиционных печатных книг. Попробуйте объяснить, что такое страница, кому-нибудь, кто знаком с прокруткой, но никогда не видел традиционных печатных книг. Как вы это сделаете? Прежде чем объяснять, что такое страница, надо объяснить, зачем они существуют.

Поэтому, прежде чем объяснять, что такое маршрутизатор или коммутатор, я должен коротко пояснить, для решения каких проблем они служат. После того как вы это поймете, все встанет на свои места, и вы сразу же сможете администрировать собственную сеть Cisco.

2.2. MAC-АДРЕС

Много лет назад кто-то решил, что все сетевые приборы должны иметь определенный идентификатор, чтобы идентифицировать друг друга в сетевом пространстве, и назвал этот идентификатор MAC-адресом (от англ. Media Access Control – управление доступом к среде). MAC-адрес – это строка длиной 48 бит, содержащая шестнадцатеричное число, примерно вот так: 0800.2700.EC26. Вероятно, вы уже встречались с чем-то подобным.

Что интересно: производители сетевых устройств присваивают им MAC-адреса еще на стадии изготовления. Целесообразность этого состоит в том, что можно просто включить устройства в сеть и коммутировать их между собой, не имея никакого руководства по конфигурации. Звучит достойно, но есть одна проблема: производитель присваивает MAC-адрес в отсутствие связи с тем, куда именно будет помещено устройство в конечном итоге. То есть это не совсем адрес, поскольку он совершенно не помогает в определении месторасположения устройства.

Практикум

Запустите оболочку командной строки Windows и введите команду `ipconfig /all`. В появившемся списке MAC-адрес сетевой карты вашего компьютера будет указан в строке **Физический адрес** (Physical Address). Если установлено несколько сетевых карт, вы увидите несколько MAC-адресов.

MAC-адрес сродни полному имени человека. Его присваивают при рождении для простой идентификации, чтобы выделить человека из толпы или послать сообщение на его имя. Если мы с вами находимся в толпе людей и вы хотите послать мне сообщение, но понятия не имеете, где я, вы можете, набрав побольше воздуха, крикнуть: «Бен Пайпер, где ты?» И если я в той толпе, то получу ваше сообщение.

Сетевые устройства общаются друг с другом таким же образом, но вместо полного имени используют MAC-адреса. Предположим, мой компьютер имеет MAC-адрес 0800.2700.EC26, и его надо напечатать на сетевом принтере с именем Monoprint и MAC-адресом 0020.3500.CE26. Мой компьютер физически соединен с принтером через устройство, называемое коммутатором, как показано на рис. 2.2. Точнее, мой компьютер и принтер *физически* присоединены к отдельным Ethernet-портам коммутатора. Отметим, что, в отличие от беспроводной точки доступа, подключение к коммутатору *всегда* производится с помощью кабеля. Таким образом, коммутатор – это место сбора всех сетевых устройств. Подобно тому, как я с вами и с другими могу собраться на переполненном рынке, сетевые устройства собираются вместе в коммутаторе. Такой набор соединенных между собой устройств называется локальной вычислительной сетью (ЛВС, от англ. Local area network, LAN).

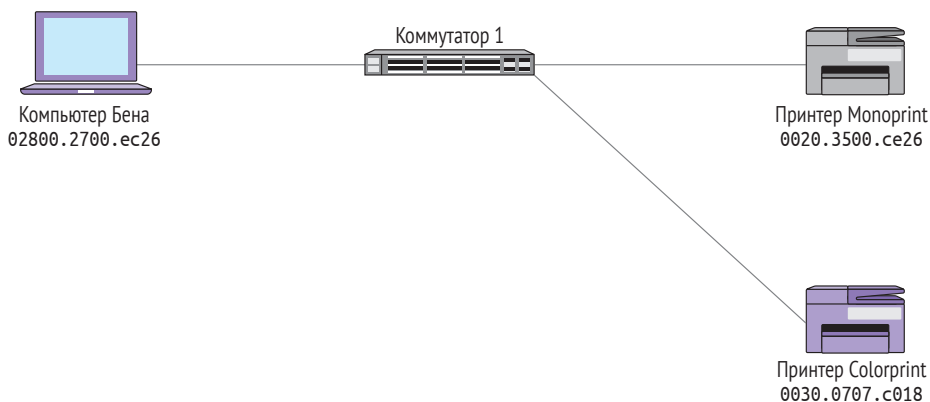


Рис. 2.2 ❖ Два принтера соединены с компьютером через коммутатор

Но здесь возникает проблема: мой компьютер не знает, где расположен принтер Monoprint, не знает даже, является ли он частью локальной сети – частью «толпы», подключенной к коммутатору. *MAC-адрес, подобно полному имени, может служить хорошим идентификатором, но он не может указать точного месторасположения устройства.* Именно поэтому мой компьютер вынужден просто «кричать в рупор», вызывая Monoprint по его MAC-адресу.

Дополнительно

Каждое устройство в процессе изготовления получает заводской уникальный идентификатор (organizationally unique identifier, OUI) в виде строки, содержащей шестнадцатеричное число. Идентификатор OUI образует левую часть MAC-адреса,

присваиваемого при изготовлении. Его можно рассматривать как «фамилию» прибора. Хотя они и присваиваются при «рождении», устройства одной серии имеют идентичный номер QUI. Остальная часть MAC-адреса – это просто следующий член возрастающей последовательности. Таким образом, производитель достигает уникальности MAC-адреса каждого устройства.

2.3. ETHERNET-КАДР: БОЛЬШОЙ КОНВЕРТ

Мой компьютер создает *Ethernet-кадр*, содержащий указания на источник – его собственный MAC-адрес – и конечный адресат – MAC-адрес принтера. Рисунок 2.3 демонстрирует Ethernet-кадр в виде большого конверта с адресами отправителя и получателя.

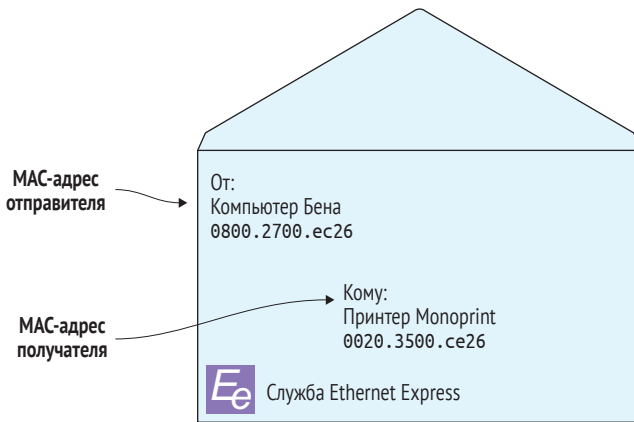


Рис. 2.3 ❖ Ethernet-кадр
содержит MAC-адреса отправителя и получателя

Мой компьютер собирает данные, которые хочет обработать на принтере, помещает их в «большой конверт» и отправляет на коммутатор. Коммутатор получает кадр и обращается к MAC-адресу удаленного принтера. Изначально коммутатор не знает, подключен к нему принтер или нет, поэтому он рассылает кадр всем остальным подключенным сетевым устройствам для определения, есть ли среди них принтер. Это называется *лавинной передачей*.

На шаге 1, на рис. 2.4, мой компьютер отправляет Ethernet-кадр, адресованный принтеру Monoprint, со своим MAC-адресом (0020.3500.ce26). На шаге 2 коммутатор рассылает этот кадр всем подключенным устройствам.

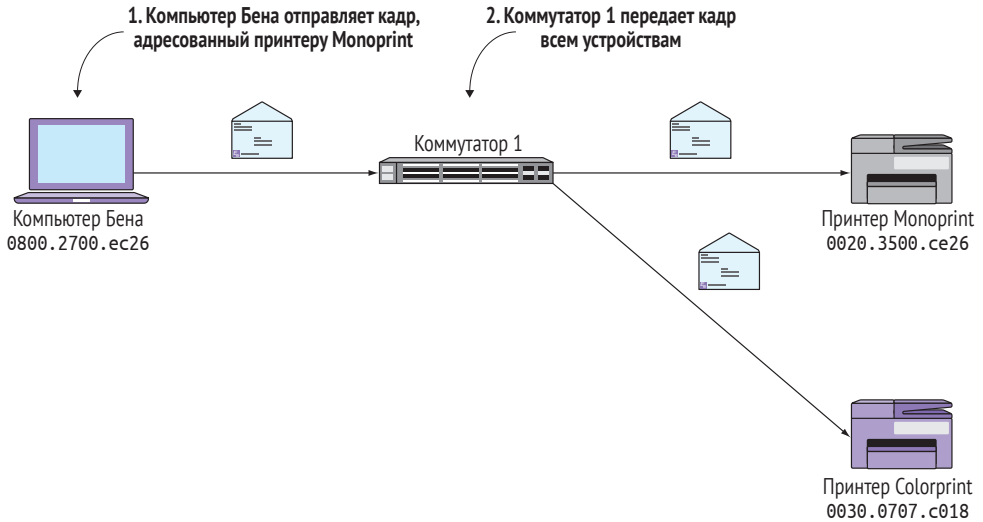


Рис. 2.4 ❖ Лавинная передача Ethernet-кадра

2.3.1. Когда все говорят, никто не слушает

Лавинная передача имеет тот же эффект, что и крик в рупор в большой толпе. Все слышат вас, но в то же время в толпе люди не могут расслышать друг друга. Для увеличения эффективности вы временно прекращаете их общение. Но даже после того, как вы прокричали в рупор, пройдет какое-то время, после того как люди получают ваше сообщение и поймут, что оно адресовано не им. То же самое происходит, когда коммутатор рассылает сообщение всем устройствам. Все они не в состоянии слышать друг друга, пока идет лавинная передача. А затем они должны обработать сообщение, чтобы понять – должны ли они что-то сделать в соответствии с ним. Это явление называется *прерыванием*.

Хотя несколько рассылок кадров и прерываний и не представляется чем-то значительным, представьте, что произойдет в толпе, скажем человек на 1000, в которой у каждого есть рупор. Как раз в тот момент, как вы собрались отправить мне сообщение через свой рупор, кто-то прямо рядом с вами кричит что-нибудь еще через свой. После того как у вас утихнет звон в ушах, вы поднимаете свой рупор только для того, чтобы опять быть прерванным кем-нибудь еще. Пока, наконец, не произойдет пауза, достаточная для пересылки сообщения. Да, это проблема. Вы действуете со всеми остальными в одной среде – в воздухе. При таком методе коммуникации «один – многим» трудно ожидать, что конкретная персона получит сообщение вовремя. И чем больше толпа, тем больше проблем.

В сети с несколькими устройствами лавинная передача не представляет проблем. А если в локальной сети сотни или тысячи устройств, то это проблематично. И это порождает другую проблему. Сеть, которая не может связать тысячи устройств, практически бесполезна.

2.4. ШИРОКОВЕЩАТЕЛЬНЫЕ ДОМЕНЫ

Предположим, что вы добавили в топологию сети еще один коммутатор, назвали его Коммутатор 2 и присоединили к нему сервер базы данных, как показано на рис. 2.5. Когда мой компьютер отправляет кадр на MAC-адрес сервера, Коммутатор 1 начинает лавинную передачу (и прерывание) на все устройства, присоединенные к его портам, включая и Коммутатор 2! Коммутатор 2, в свою очередь, тоже передает кадр всем устройствам. В этом случае сервер базы данных – всего лишь рядовое устройство, присоединенное к Коммутатору 2.

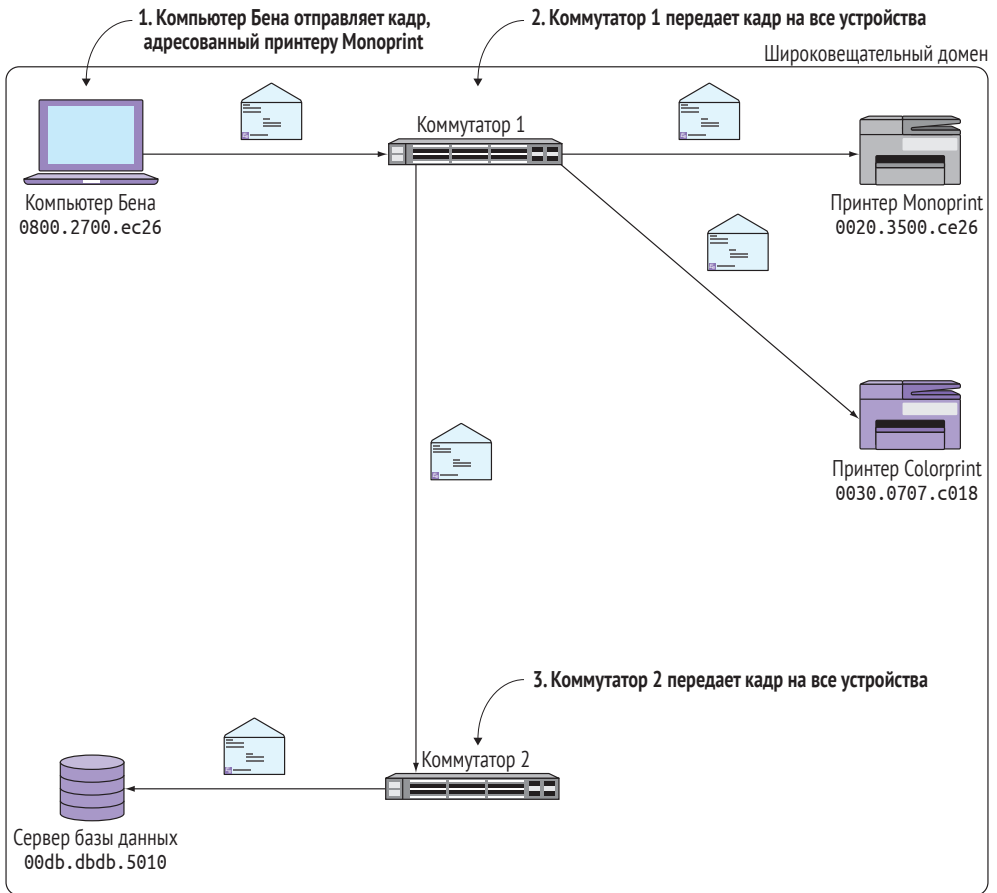


Рис. 2.5 ❖ Коммутатор 2 расширяет широковещательный домен

В шаге 1 мой компьютер пересылает кадр на MAC-адрес сервера базы данных (00db.dbdb.5010). В шаге 2 Коммутатор 1 рассылает кадр всем устройствам. И наконец, в шаге 3 Коммутатор 2 передает кадр на сервер базы данных.

Все эти устройства, которые получили кадр, – члены одного *широковещательного домена*. Широковещательный домен – это не устройство и даже не настраиваемый параметр, а скорее неотъемлемый атрибут сети. Для лучшего понимания представлю следующую аналогию.

Когда вы стоите один в центре улицы, вы – не толпа. Но если несколько человек собирается вокруг вас, вы становитесь частью толпы. И вы становитесь частью еще большей толпы, когда вокруг вас собирается больше людей. Вы не меняетесь, но меняется ваше виртуальное свойство – часть толпы, – в зависимости от того, сколько людей собралось вокруг вас. Точно так же и устройство становится частью широковещательного домена тех устройств, которые получили кадр при лавинной передаче.

2.4.1. Избавление от лавинной передачи: таблица MAC-адресов

Лавинная передача – неизбежная операция при использовании MAC-адресов. К счастью, коммутаторы используют ловкий трюк, чтобы уменьшить необходимость лавинной передачи. Каждый раз, когда коммутатор получает кадр, он изучает MAC-адрес источника и порт, к которому присоединен источник кадра. Эта информация используется для построения *таблицы MAC-адресов*.

Дополнительно

В документации Cisco таблица MAC-адресов иногда называется ассоциативной памятью (content addressable memory, CAM), но это одно и то же.

Когда Коммутатор 1 получает кадр от моего компьютера, он записывает его MAC-адрес 0800.2700.ac26, а также порт, к которому компьютер подключен, – FastEthernet0/1. Эта информация добавляется в таблицу MAC-адресов, как показано в табл. 2.1.

Таблица 2.1. Таблица MAC-адресов Коммутатора 1

Устройство	MAC-адрес	Порт коммутатора
Компьютер Бена	0800.2700.ec26	FastEthernet0/1

Теперь предположим, сервер базы данных отправляет кадр с MAC-адресом моего компьютера. Кадр попадает на Коммутатор 2, который отправляет его напрямиком на Коммутатор 1. Но вместо слепого забрасывания кадром всех устройств Коммутатор 1 проверяет таблицу MAC-адресов.

Он видит, что MAC-адрес 0800.2700.ec26 соответствует устройству, подключенному к порту FastEthernet0/1, и отправляет кадр *только* на этот порт, как показано на рис. 2.6. Это работает по принципу старого телефонного коммутатора, откуда и происходит термин *коммутатор*.

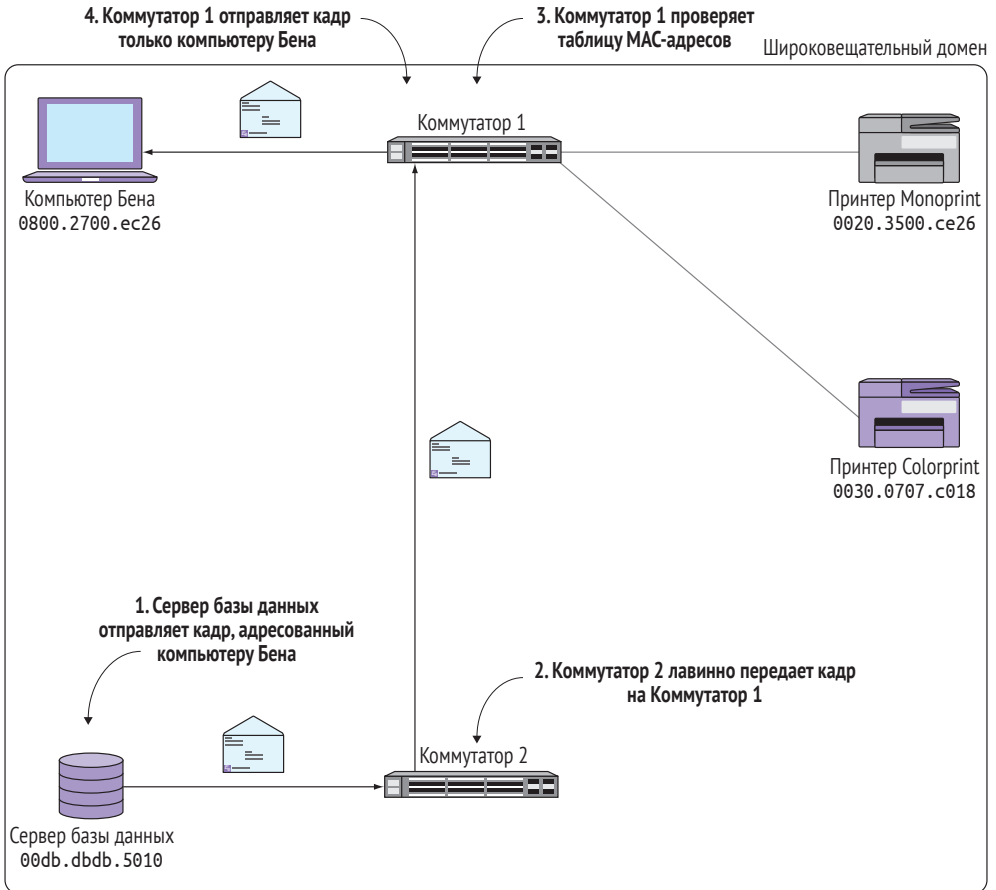


Рис. 2.6 ❖ Как таблица MAC-адресов позволяет избавиться от лавинной передачи

На шаге 1 сервер базы данных отправляет кадр на MAC-адрес моего компьютера (0800.2700.ec26). На шаге 2 Коммутатор 2 (лавинно) отправляет кадр на Коммутатор 1. На шаге 3 Коммутатор 1 сверяется с таблицей MAC-адресов и находит порт запрашиваемого адреса. На шаге 4 Коммутатор 1 отправляет кадр только на порт моего компьютера, а не лавинно передает кадр на все остальные устройства.

2.4.2. Разделение широковещательного домена

С ростом размера широковещательного домена коммуникации становятся все более затруднительными. И как следствие, широковещательный домен, состоящий из сотен устройств, начинает работать неудовлетворительно. Но современной компании требуется сеть, соединяющая тысячи устройств. И просто наличия связи недостаточно. Сеть должна быть быстрой и надежной.

Решение заключается в ограничении размера широковещательного домена. Это значит, что его нужно разбить на части таким образом, чтобы отдельные части имели связь друг с другом.

Возвращаясь к нашему примеру, мы видим, что простейший путь разбить широковещательный домен – это отключить Ethernet-кабель, соединяющий Коммутаторы 1 и 2, как показано на рис. 2.7. Отмечу, что коммутаторы не соединяются каким-либо иным способом. Это простая часть. А теперь сложная: мой компьютер и сервер базы данных размещены на разных широковещательных доменах. Не существует путей для их связи друг с другом. Что вы натворили? Вы не можете просто заново соединить коммутаторы, потому что воссоздадите то, что было, – единый широковещательный домен.

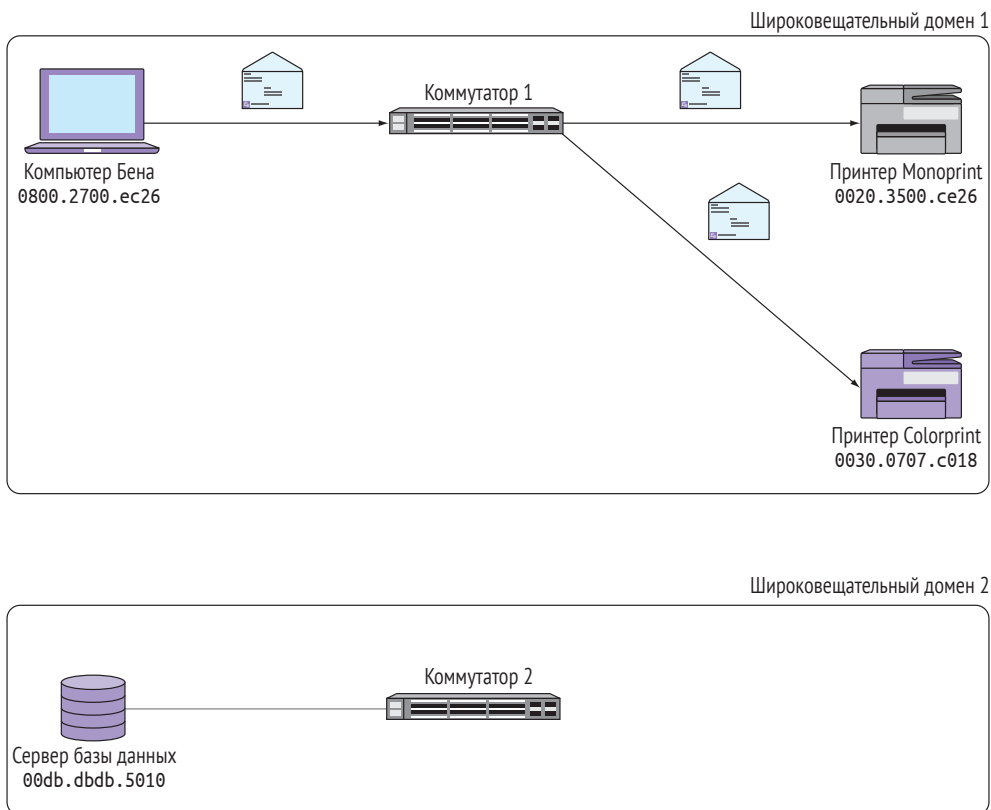


Рис. 2.7 ❖ Два широковещательных домена

2.4.3. Соединение широковещательных доменов

Для соединения двух широковещательных доменов без повторения этой ужасной проблемы лавинной передачи необходимо сделать две вещи.

Во-первых, так как два широковещательных домена не имеют связи, вам нужно специальное устройство, физически соединяющее их, но таким образом, чтобы рассылка кадров не выходила за границы широковещательного домена. Так как кадр содержит MAC-адреса и отправителя, и адресата, это устройство будет эффективно скрывать MAC-адреса одного широковещательного домена от другого.

Во-вторых, так как MAC-адреса одного широковещательного домена скрыты от другого, вам нужна другая схема адресации устройств для обращения к оборудованию в разделенных доменах. Новая адресная схема, в отличие от MAC-адресов, должна не только идентифицировать прибор, но и предоставлять какие-то указания на то, в каком домене прибор размещен. Давайте начнем с последнего.

2.4.4. Адресация устройств из разных широковещательных доменов

Схема адресации должна удовлетворять следующим требованиям:

- во-первых, адрес должен быть уникальным для всех широковещательных доменов. Два устройства из одного домена не могут иметь одинаковый адрес;
- во-вторых, адрес должен сообщать, какому домену он принадлежит. *Адрес должен быть не только уникальным идентификатором прибора, но также и сообщать другим устройствам, к какому домену он принадлежит.* Все это для того, чтобы избежать этих ужасных проблем лавинной передачи;
- в-третьих, адреса не могут присваиваться «при рождении», подобно MAC-адресу. Они должны конфигурироваться вами как сетевым администратором.

К счастью, вам нет необходимости ломать над этим голову. Такая адресная схема существует, и вы уже пользовались ею.

2.5. АДРЕСА ПРОТОКОЛА ИНТЕРНЕТА

Вы уже знаете, как выглядят IP-адреса. Один из самых распространенных IP-адресов – 192.168.1.1. Это последовательность четырех восьмеричных чисел (*октетов*), разделенных точкой, каждое число может располагаться в диапазоне от 0 до 255.

Вы, вероятно, видели адреса типа 192.168.х.х, всплывающие в различных местах. Это связано с тем, что адреса 192.168.х.х зарезервированы для использования в частных сетях, используемых у вас дома или на работе. Они глобально не уникальны, так как не доступны в общем пространстве Интернета. Но вы можете их использовать для адресации устройств в своей собственной внутренней сети.

В отличие от MAC-адресов, вы можете присваивать IP-адрес любому устройству, какому захотите. Вы можете создать собственную схему адресации, основанную на месторасположении прибора, а не просто на том, что они есть. Давайте рассмотрим пример.