Часть X. Приложения (на веб-сайте)

Приложение В. “Ответы на контрольные вопросы”
Приложение Г. “Практические задания главы 12. Анализ классовых сетей IPv4”
Приложение Д. “Практические задания главы 13. Анализ существующих масок подсети”
Приложение Е. “Практические задания главы 14. Анализ существующих подсетей”
Приложение Ж. “Практические задания главы 19. Проект подсети”
Приложение З. “Практические задания главы 20. Маски подсети переменной длины”
Приложение И. “Практические задания главы 21. Суммирование маршрутов”
Приложение К. “Практические задания главы 22. Простые списки управления доступом IPv4”
Приложение Л. “Практические задания главы 25. Основы протокола IP версии 6”
Приложение М. “Практические задания главы 27. Реализация IPv6-адресации на маршрутизаторах”
Приложение Н. “Таблицы для запоминания материала”
Приложение О. “Таблицы для запоминания материала с ответами”
Приложение П. “Решения для диаграмм связей”
Приложение Р. “План изучения”

Приложение В

Ответы на контрольные вопросы

Глава 1

1. Г и Е. Ethernet определяет и физические протоколы, и протоколы канала связи, а PPP — протокол канала связи, IP — протокол сетевого уровня, SMTP и HTTP — протоколы уровня приложений.
2. А и Ж. IP — протокол сетевого уровня, TCP и UDP — протоколы транспортного уровня, SMTP и HTTP — протоколы уровня приложений.
3. Б. Взаимодействие на смежных уровнях происходит в одном компьютере, когда два расположенных рядом уровня чем-либо обмениваются. Обычно верхний уровень запрашивает какую-либо службу у нижнего, а нижний предоставляет какие-то услуги верхнему.
4. Б. Взаимодействие на одинаковых уровнях происходит между разными компьютерами, поскольку выполняемая функция требует наличия более чем одного участника. Например, передающий узел устанавливает порядковый номер сегмента, а принимающий генерирует для него соответствующий номер подтверждения. Функции и процессы выполняются на том же уровне в рамках какой-либо модели, но реализация такого уровня должна быть одинакова в разных устройствах.
5. А. Инкапсуляция — это процесс добавления заголовка в начале блока данных, полученных от вышестоящего уровня (и, возможно, концевика).
6. Г. В соответствии с соглашением, термин *фрейм* относится к части сетевого сообщения, включающей заголовок и концевик канала связи, со скрытыми данными. Термин *пакет* не включает заголовок и концевик канала связи, оставляя заголовок сетевого уровня с его скрытыми данными. Термин *сегмент* не включает заголовок сетевого уровня, оставляя заголовок транспортного уровня и его скрытые данные.
7. В. Сетевой уровень отвечает за передачу данных по всему пути от пункта к пункту. Ему требуется способ идентификации каждого устройства с использованием адресов, и эти адреса должны быть логическими адресами, не привязанными к физическим деталям сети.
8. А. Физический уровень модели OSI включает все стандарты, определяющие форму разъемов, соединительные кабели, электронные устройства и кодировку электрических сигналов для передачи битов по кабелю.
9. В и Д. Названия уровней сверху вниз: прикладной, представления, сеанса, транспортный, сетевой, канала связи и физический.

Глава 2

1. А. Стандарт IEEE определяет стандарты Ethernet LAN со стандартными названиями, начинающимися на 802.3, все они используют кабельную проводку. Стандарт IEEE определяет также беспроводные стандарты LAN со стандартными названиями, начинающимися на 802.11 и являющимися стандартами, отдельными от Ethernet.
2. В. Число перед словом “BASE” определяет скорость в мегабитах в секунду (Мбит/с). 1000 Мбит/с равно 1 Гигабиту в секунду (1 Гбит/с). “T” в суффиксе подразумевает витую пару (twisted-pair) или кабель UTP. Таким образом, 1000BASE-T — это название стандарта Ethernet для кабеля UTP со скоростью 1 Гбит.
3. Б. У перекрещенных кабелей провода перекрестно соединяют пары контактов, чтобы передающий контакт на одном устройстве соединялся с получающим контактом на другом. У перекрещенных кабелей Ethernet на 10 и 100 Мбит/с пара контактов 1 и 2 на одном конце кабеля соединена с контактами 3 и 6 на другом конце соответственно.
4. Б, Г и Д. В маршрутизаторах, беспроводных точках доступа и сетевых картах персональных компьютеров контакты 1 и 2 портов Ethernet используются для передачи данных, а в коммутаторах — контакты 3 и 6. Прямыми кабелями соединяют устройства, использующие противоположные пары контактов, поскольку кабель уже не должен перекрещивать пары.
5. Б. Сетевые платы (и порты коммутатора) используют алгоритм множественного доступа с контролем несущей и обнаружением конфликтов (CSMA/CD) для реализации полудуплексной логики. Хотя алгоритм CSMA/CD пытается избежать коллизий, он также отмечает случаи, когда коллизии действительно происходят, и устанавливает правила, согласно которым узлы Ethernet должны прекратить передачу, подождать и попытаться передать снова позже.
6. В. Находящееся в концевике Ethernet 4-байтовое поле FCS позволяет получающему узлу удостовериться в правильности полученной информации. Для этого используется математическая формула, являющаяся ключевой частью процесса обнаружения ошибок. Обратите внимание, что стандарт Ethernet определяет процесс обнаружения ошибок, но не восстановления после ошибок.
7. Б, В и Д. Встроенный универсальный MAC-адрес, присвоенный каждому порту Ethernet изготовителем и разделенный на две 3-байтовые половины. Первая половина называется уникальным идентификатором организации (OUI), присвоенным компании производителя. Это уникальное шестнадцатеричное число, используемое только этой компанией.
8. В и Г. Стандарт Ethernet поддерживает одноадресатные адреса, идентифицирующие одиночный узел Ethernet и групповые адреса, применяющиеся для передачи одного фрейма на несколько узлов Ethernet. Двумя типами групповых адресов являются *широковещательный* и *многоадресатный адреса*.

Глава 3

1. Б. Уровень 1 модели OSI, физический уровень, определяет физическую передачу битов по такой физической передающей среде, как кабель или радиоволны. Уровень 2 модели OSI, канальный уровень, определяет протоколы, контролирующие и управляющие передачей, включая определение фреймов канала связи, включая адреса и поля, позволяющие осуществлять обнаружение ошибок.
2. Б. Четырехжильный кабель, предоставляемый телефонной компанией, подключается к устройству, выступающему в роли модуля CSU/DSU. Это может быть внешний модуль CSU/DSU или интегрированный в плату последовательного интерфейса маршрутизатора. У коммутатора LAN нет последовательных интерфейсов, а у последовательных интерфейсов маршрутизатора нет трансиверов.
3. В. Выделенные линии способны работать на разных предустановленных скоростях, кратных 64 Кбайт/с. Скорости могут быть также кратны скорости T1 (1,544 Мбит/с).
4. В. Стандартный заголовок HDLC не включает поле Type, идентифицирующее тип пакета, инкапсулируемого во фрейме HDLC.
5. Б и Г. Физическая инсталляция использует модель, при которой каждый маршрутизатор использует физический канал связи Ethernet для подключения к некоему устройству провайдера SP. Канал связи Ethernet не распространяется на клиентские устройства. С точки зрения канала связи оба маршрутизатора используют тот же заголовок и концевик стандарта Ethernet, используемый в локальных сетях; HDLC не имеет значения на каналах связи Ethernet WAN.
6. Б и В. Выделенные линии передают данные на той же скорости в обоих направлениях, обеспечивая симметричные услуги. Модем DSL и кабельный модем предоставляют асимметричные скорости, с более быстрой скоростью приема. BGP — это протокол маршрутизации, а не технологий доступа к Интернету.
7. В. При технологии DSL требования к телефонным проводам не изменяются. Телефон может быть подключен к любой телефонной розетке, как будто модем DSL и маршрутизатор не существуют.

Глава 4

1. А и В. Сетевой уровень задает структуру логической адресации, которая является иерархической, в отличие от физической. Логическое упорядоченное построение адресной схемы позволяет легко группировать адреса в блоки и таким образом оптимизировать адресацию. Выбором пути называется процесс поиска оптимального маршрута в сети.
2. В и Д. Поскольку компьютеры PC1 и PC2 разделены маршрутизаторами, они должны полагаться на них, чтобы использовать логику маршрутизации. При маршрутизации маршрутизатор отбрасывает заголовок канала связи входящего фрейма и принимает решение о перенаправлении пакета, извлеченного из фрейма. В результате наибольшим элементом, передаваемым с компьютера

PC1 на компьютер PC2, является пакет IPv4 (или пакет IPv6), известный под более общим названием L3PDU.

3. Б. 224.1.1.1 — это адрес сети класса D, адрес 223.223.223.255 — широковещательный для подсети класса C с адресом 223.223.223.0, поэтому они не могут быть назначены хостам.
4. Г. Первый октет адреса сети класса A находится в диапазоне от 1 до 126 включительно; класса B — 128–191 включительно; и класса C — 192–223 включительно. Технически значение 127 принадлежит диапазону класса A, но это зарезервированный адрес, используемый для обратной связи.
5. Г и Е. Если не используются подсети, все адреса относятся к сети класса A, 10.0.0.0. Если в сети есть маршрутизатор и хосты находятся в другом сегменте (подключены к другому его порту), они не могут иметь адреса из сети 10.0.0.0.
6. А. Компьютер PC1 посылает фрейм Ethernet на маршрутизатор Router1 с MAC-адресом компьютера PC1 как адресом отправителя и MAC-адресом маршрутизатора Router1 как адресом получателя. Маршрутизатор Router1 извлечет встроенный пакет IP из фрейма Ethernet, отбросит заголовок и концевик фрейма. Маршрутизатор Router1 перенаправит пакет IP, упаковав его во фрейм HDLC, причем инкапсулирован будет не фрейм Ethernet, а именно пакет IP. Маршрутизатор Router2 извлечет пакет IP из фрейма HDLC и перенаправит его в LAN Ethernet, добавив новый заголовок и концевик Ethernet, но этот заголовок будет отличаться от прежнего. Адресом отправителя будет MAC-адрес маршрутизатора Router2, а адресом получателя — MAC-адрес компьютера PC2.
7. В. Маршрутизаторы сравнивают IP-адрес получателя пакета с таблицей маршрутизации IP, находят соответствие и, используя инструкции, перенаправляют пакет IP по соответствующему маршруту.
8. Б и В. Хосты IPv4 обычно используют простую логику с двумя ветвями. Чтобы передать пакет IP на другой хост в той же сети или подсети IP, находящейся в той же сети LAN, отправитель посылает пакет IP непосредственно на этот хост. В противном случае отправитель посылает пакет на свой стандартный маршрутизатор (стандартный шлюз).
9. А и В. Маршрутизаторы осуществляют все действия, перечисленные во всех четырех ответах. Но протокол маршрутизации выполняет функции, перечисленные только в двух ответах. Независимо от протокола маршрутизации, маршрутизатор изучает маршруты для подсетей и сетей IP, непосредственно соединенных с его интерфейсами. Маршрутизаторы также перенаправляют (маршрутизируют) пакеты IP, и этот процесс называется маршрутизацией IP, или перенаправлением IP; он не зависит от работы протокола маршрутизации.
10. Протокол преобразования адресов (ARP) действительно позволяет компьютеру PC1 изучать информацию, но эта информация не хранится на сервере. Команда ping действительно позволяет пользователю PC1 выяснить, могут ли пакеты передаваться по сети, но она тоже не использует сервер. Система доменных имен (DNS) позволяет компьютеру PC1 действовать как клиенту DNS, причем сервер DNS предоставляет информацию об IP-адресах, соответствующих указанному имени хоста.

Глава 5

1. Г. Три ответа определяют функции TCP: восстановление после ошибок, управление потоком и сегментация. Правильный ответ определяет функцию, не осуществляемую ни протоколом TCP, ни UDP, а протоколами прикладного уровня.
2. Г и Д. Большинство заголовков включают поле, идентифицирующее следующий заголовок в сообщении. Протокол Ethernet использует поле Type Ethernet и заголовок IP, использующий поле Protocol. Используя поле номера порта, заголовки TCP и UDP идентифицируют приложение, которое должно получить данные, следующие за заголовком TCP или UDP соответственно.
3. А, Б, В и Е. Маршрутизацию определяет протокол IP, а не TCP. Шифрование определяет множество протоколов, но не TCP. В правильных ответах просто перечислены различные средства протокола TCP.
4. В. Протокол TCP, а не UDP использует механизм скользящего окна, восстановление после ошибок и упорядоченную передачу сегментов. Шифрование или маршрутизацию оба протокола транспортного уровня не выполняют.
5. В и Е. Термины *пакет* и *L3PDU* описывают заголовок и данные, инкапсулируемые уровнем 3. Термины *фрейм* и *L2PDU* относятся к заголовку (и концевику), а также к данным, инкапсулируемым уровнем 2. Термины *сегмент* и *L4PDU* относятся к заголовку и данным, инкапсулируемым в соответствии с протоколом транспортного уровня.
6. Б. Имя хоста — это текст между косыми черточками (// и /). Текст перед символами // описывает используемый протокол уровня приложений, а текст после символа / — название веб-страницы.
7. А и Г. Потоки данных технологии VoIP наиболее чувствительны к задержкам, их флуктуации и потерям пакетов; чем меньше задержки, флуктуации и потери, тем лучше. Тем не менее потоки VoIP обычно требуют меньшей полосы пропускания, чем потоки обычных данных.

Глава 6

1. А. Коммутатор сравнивает адрес получателя со своей таблицей MAC-адресов. Если найдена совпадающая запись, коммутатор знает, через какой интерфейс отправить фрейм дальше, если не найдена — лавинно рассылает через все порты, кроме того, откуда он пришел.
2. В. Коммутатор рассылает лавинно широковещательные, многоадресатные (если не используется оптимизация многоадресатных потоков) и фреймы с адресом получателя, который устройству неизвестен (т.е. адрес получателя фрейма отсутствует в таблице MAC-адресов коммутатора).
3. А. Коммутатор рассылает лавинно широковещательные, многоадресатные (если не используется оптимизация многоадресатных потоков) и фреймы с адресом получателя, который устройству неизвестен (т.е. адрес получателя фрейма отсутствует в таблице MAC-адресов коммутатора).

4. Б. Коммутатор должен изучить расположение каждого MAC-адреса, используемого в сети LAN, относительно локального коммутатора. Когда коммутатор посылает фрейм, исходный MAC-адрес идентифицирует отправителя. Интерфейс, на который поступает фрейм, идентифицирует локальный интерфейс коммутатора, ближайший к этому узлу в топологии LAN.
5. А и Б. Когда фрейм, отправленный устройством PC3, попадает в коммутатор, у последнего есть в таблице только адрес 1111.1111.1111, MAC-адрес PC1. Фрейм от PC3 адресован устройству с MAC-адресом 2222.2222.2222, поэтому он рассылается лавинным образом, т.е. пересылается через все интерфейсы, кроме того, откуда пришел фрейм.
6. А. Домен коллизий представляет собой совокупность устройств, фреймы которых могут сталкиваться. Мосты, коммутаторы и маршрутизаторы разделяют, или сегментируют, локальную сеть на меньшие по размеру домены коллизий, а концентраторы и повторители — нет.
7. А, Б и В. Широковещательный домен состоит из устройств, широковещательные фреймы которых могут достигать друг друга. Концентраторы, повторители, мосты и коммутаторы не разделяют (сегментируют) локальную сеть на отдельные широковещательные домены, а маршрутизаторы разделяют.
8. Б и Г. Стандарты IEEE Ethernet поддерживают 100-метровые каналы связи по кабелям UTP. Большинство стандартов для оптоволоконных кабелей, как в двух правильных ответах, допускают длину больше 100 метров.
9. Г. Дуплексный режим применяется на любом канале связи Ethernet между коммутатором и компьютером. Автопереговоры IEEE устанавливают состояние, при котором две конечные точки на канале связи выбирают наилучшую скорость и наилучший дуплекс, поддерживаемый обеими точками, причем дуплекс предпочтительней, чем полудуплекс.

Глава 7

1. А и Б. Команда в вопросе пользовательская, ей достаточно пользовательского режима доступа. Поскольку команда пользовательская, ее нельзя использовать в режиме конфигурации, если не предварить ее ключевым словом do (например, do show mac address-table). Таким образом, эту команду можно использовать и в пользовательском, и в привилегированном режиме.
2. Б. Упомянутая в вопросе команда перезагрузки является пользовательской, ей требуется привилегированный режим, известный также как режим enable. Поскольку команда пользовательская, ее нельзя использовать в режиме конфигурации, если не предварить ее ключевым словом do (например, do reload). В пользовательском режиме эта команда недоступна.
3. Б. Протокол SSH обеспечивает возможность защищенной удаленной регистрации (входа в систему), шифруя все потоки данных, включая обмен паролями. Telnet передает все данные (включая пароли) как открытый текст.

4. А. Коммутаторы (и маршрутизаторы) хранят текущую конфигурацию в оперативной памяти, используя NVRAM для хранения файла конфигурации, загруженного на коммутатор (или маршрутизатор) при загрузке операционной системы IOS.
5. Е. Файл конфигурации startup-config находится в памяти NVRAM, а файл конфигурации running-config — в оперативной памяти.
6. Б и В. Команда exit переводит пользователя из режим конфигурации назад, в режим глобальной конфигурации, или, если пользователь уже в режиме глобальной конфигурации, назад в привилегированный режим. Из консольного режима она возвращает пользователя в глобальный режим конфигурации. Команда end или комбинация клавиш <Ctrl+Z> возвращают пользователя в привилегированный режим независимо от текущего подрежима конфигурации.

Глава 8

1. Б. Если указаны обе команды, операционная система Cisco IOS использует пароль, указанный в команде enable secret.
2. Б и В. Протокол SSH требует кроме имени пользователя использования пароля. Имена пользователя (и пароли), поддерживаемые протоколом SSH, можно задать глобальной командой username. Линии vty также следует настроить подкомандой vty login local, чтобы они требовали использования имен пользователя. Команда transport input ssh могла бы быть частью конфигурации, но это не глобальная команда конфигурации (как указано в одном неправильном ответе). Аналогично в одном ответе упоминается команда username как команда режима конфигурации vty, что также является неправильным.
3. Б. Первый символ, не являющийся пробелом, после команды banner login будет интерпретирован как символ-разделитель. В данном случае это будет буква “t” в слове “this”, а вторая буква “t” встречается в слове “the” и будет интерпретирована как конец сообщения. В результате при подключении к устройству будет выводиться текст, находящийся между двумя буквами “t”, а именно “his is”.
4. Б. Стандартная настройка максимального количества MAC-адресов в режиме безопасности — 1, следовательно, команду switchport port-security maximum вводить не нужно. При автоматическом обнаружении предопределять конкретные MAC-адреса также не нужно. Тем не менее нужно разрешить защиту порта, что требует подкоманды интерфейса switchport port-security.
5. А, Г, и Е. Чтобы разрешить доступ к устройству через протокол Telnet, в коммутаторе должны быть установлены пароли. Минимальное требование — должен быть установлен пароль на линии vty с помощью команды _password. Кроме того, следует настроить IP-адрес в устройстве (на одном интерфейсе VLAN) и указать стандартный шлюз, чтобы коммутатор мог обмениваться пакетами с хостами из других подсетей.
6. Е. У коммутатора Cisco нет команды для отключения автопереговоров о скорости и дуплексе. Но если на порте коммутатора настроены команды speed и duplex, то автопереговоры отключаются.

7. Д. В режиме конфигурации интерфейса на коммутаторах Cisco может быть задана скорость (командой speed) и дуплекс (командой duplex).

Глава 9

1. Б. Сеть VLAN — это набор устройств на том же уровне 2 широковещательного домена. Подсеть зачастую включает тот же набор устройств, но это концепция уровня 3. Термин *домен коллизий* относится к набору устройств Ethernet, но с другими правилами, отличными от правил VLAN, определяющих устройства, входящие в тот же домен коллизий.
2. Г. *Подсеть* и *сеть VLAN* — это не эквивалентные термины, тем не менее устройства в одной сети VLAN обычно принадлежат одной и той же подсети IP, и наоборот.
3. Б. Стандарт 802.1Q определяет 4-байтовый заголовок, добавляемый после полей адреса получателя фрейма и MAC-адреса отправителя. Добавление этого заголовка не изменяет ни адрес первоначального отправителя фрейма, ни адрес получателя. Сам заголовок содержит 12-битовое поле идентификатора VLAN, связанное с фреймом.
4. А. Стандарт 802.1Q определяет собственную сеть VLAN как отдельную сеть VLAN на магистральном канале, для которого устройства не будут добавлять заголовок 802.1Q для фреймов в этой сети VLAN. Коммутаторы могут установить собственную сеть VLAN с любым идентификатором VLAN, но коммутаторы требуют согласования. Стандартная собственная сеть VLAN — это VLAN 1. Обратите внимание, что только одна такая собственная сеть VLAN разрешена на любом магистральном канале; в противном случае эта VLAN, ассоциируемая с неотмеченными фреймами, не будет распознана получающим коммутатором.
5. А и В. Если в конфигурации указан ключ dynamic auto, то коммутатор может автоматически согласовывать магистральный канал, однако при этом он только отвечает на соответствующие служебные сообщения, но не инициирует процесс согласования магистрали. Следовательно, коммутатор на другом конце канала должен быть настроен так, чтобы он инициировал процесс автосогласования, т.е. у него должен быть указан в конфигурации ключ dynamic desirable.
6. А и Б. Стандартное состояние VTP — прозрачного режима VTP — означает, что коммутатор может настроить сети VLAN, поэтому VLAN настраиваются. Кроме того, подробности конфигурации VLAN, включая ее имя, отображаются в составе текущего конфигурационного файла.
7. Б и В. Команда show interfaces switchport выводит и административное, и оперативное состояние каждого порта. Когда коммутатор полагает, что порт подключен к магистрали, эта команда выводит оперативное состояние магистрального канала “trunk”. Команда show interfaces trunk выводит набор интерфейсов, включая интерфейсы, работающие в настоящее время как магистральные каналы. Таким образом, обе эти команды идентифицируют интерфейсы, работающие с магистральными каналами.

Глава 10

1. Д и Е. Протокол CDP собирает информацию о смежных устройствах, а с помощью команды show cdp с разными опциональными параметрами можно увидеть более или менее подробную информацию.
2. Д и Е. Команда show cdp neighbors выводит по одной строке на каждого соседа. Она выводит информацию о платформе соседа, как правило, включающую номер устройства. Команда show cdp entry Hannah выводит группу сообщений о соседнем маршрутизаторе, включая подробности о модели устройства и версии IOS.
3. А, Б и Г. Если в выводе команды show interfaces status указано отключенное состояние интерфейса (disabled), то это свидетельствует о том, что порт административно отключен и в выводе команды show interfaces будет отображаться строка "administratively down/down". Интерфейс должен быть в подключенном состоянии (connect), чтобы устройство могло пересылать через него фреймы.
4. А и Г. В коммутаторе SW2 была отключена система автоматического согласования параметров интерфейса стандарта IEEE, когда были вручную установлены скорость и дуплексность. Тем не менее коммутаторы компании Cisco могут определить скорость и режим работы дистанционного порта даже при отключенном автосогласовании. Кроме того, согласно стандарту IEEE для скорости передачи 1 Гбит/с используется дуплексный режим, если режим дуплексности не может быть согласован, поэтому соединение в любом случае будет нормально функционировать, поскольку на обоих концах канала используются скорость 1 Гбит/с и дуплексный режим.
5. Б и Г. С помощью команды show interfaces можно просмотреть текущую скорость работы и режим дуплексности интерфейса, но нельзя сказать, какая скорость была согласована или указана в конфигурации. В выводе команды show interfaces status может быть показан префикс a- перед значением скорости и режимом дуплексности; он означает, что скорость и режим были автоматически согласованы. В противном случае параметры были заданы вручную в конфигурации.
6. Б и В. Операционная система IOS добавляет MAC-адреса в безопасном режиме порта в виде статических записей, поэтому они не отображаются в выводе команды show mac address-table dynamic. Команда show mac address-table port-security — неправильная.
7. А и В. Команда show mac address-table выводит все записи таблицы MAC-адресов коммутатора, включая динамически изученные и статически определенные адреса. Вывод перечисляет (слева направо) идентификатор VLAN, MAC-адрес, тип (статический или динамический) и соответствующие порты, через которые посланные на указанный адрес фреймы покидают данный коммутатор.
8. Г. Команда show interface switchport выводит значения, заданные на коммутаторе командой switchport mode в административном режиме, указывая, что коммутатор SW1 использует команду конфигурации switchport mode trunk. Демонстрируется текущее рабочее состояние (trunk). Один из четырех неправильных ответов утверждает, что рабочее состояние коммутатора SW2 также должно

быть trunk; тем не менее один коммутатор может использовать магистральное соединение, а другой нет. Другой ответ утверждает, что административным режимом должен быть trunk, обязывающий использовать команду switchport mode trunk. Но у коммутатора SW2 есть несколько других параметров конфигурации, заданных командами switchport mode dynamic desirable и switchport mode dynamic auto. Правильный ответ относится к одной из этих команд, которые должны работать правильно.

Глава 11

1. Б и Г. Общее правило, чтобы определить, должны ли интерфейсы двух устройств быть в той же подсети или нет, — это выяснить, отделяются ли два интерфейса друг от друга маршрутизатором. Чтобы предоставить хостам в одной сети VLAN путь для отправки данных хостам вне этой VLAN, интерфейс LAN локального маршрутизатора должен быть подключен к той же сети VLAN, что и хост, а также иметь адрес в той же подсети, что и хосты. Все хосты в той же сети VLAN на том же коммутаторе не будут отделены друг от друга маршрутизатором, поэтому все эти хосты также будут в той же подсети. Однако другой компьютер, подключенный к тому же коммутатору, но находящийся в другой сети VLAN, потребует прохождения своих пакетов через маршрутизатор, чтобы они достигли хоста А. Таким образом, IP-адрес хоста А должен находиться в подсети, отличной от подсети этого нового хоста.
2. Г. По определению два адреса в каждой подсети IPv4 не могут использоваться как адреса хостов: первое (самое низкое) числовое значение в подсети — это идентификатор подсети и последнее (самое высокое) числовое значение в подсети — это широковещательный адрес подсети.
3. Б и В. Необходимо по крайней мере 7 битов подсети, поскольку $2^6 = 64$; всего 6 битов подсети не обеспечит 100 различных подсетей, а 7 битов — вполне, так как $2^7 = 128 => 100$. Аналогично 6 битов хоста недостаточно, поскольку $2^6 – 2 = 62$, но 7 битов хоста вполне достаточно, так как $2^7 – 2 = 126 => 100$. Общее количество битов сети, подсети и хоста должно составлять 32 бита, поэтому один из ответов неправильный. Ответ с 8 битами сети не может быть правильным, поскольку вопрос утверждает, что используется сеть класса B, поэтому количеством битов сети всегда должно быть 16. У двух правильных ответов 16 битов сети (так как в вопросе указана сеть класса B) и по крайней мере 7 битов для подсетей и хостов в каждом.
4. А и В. Документом RFC 1918 определены следующие частные сети IPv4: сеть класса А 10.0.0.0, 16 сетей класса В (от 172.16.0.0 до 172.31.0.0) и 256 сетей класса С, начинающиеся с 192.168.
5. А, Г и Д. Документом RFC 1918 определены следующие частные сети IPv4: сеть класса А 10.0.0.0, 16 сетей класса В (от 172.16.0.0 до 172.31.0.0) и 256 сетей класса С, начинающиеся с 192.168. Три правильных ответа относятся к диапазону открытых сетей IP и не к зарезервированным значениям.
6. А и В. У сетей класса А, В и С без подсетей есть две части: сети и хоста.

7. Б. У сетей класса A, B и C без подсетей есть две части: сети и хоста. Для создания подсетей инженер создает новую часть подсети, заимствуя биты хоста и сокращая их количество. Часть подсети в структуре адреса появляется только после того, как инженер выберет нестандартную маску. Размер части сети останется прежним.
8. В и Г. *Идентификатор подсети* (Subnet ID — сокращение от subnet identifier), *адрес подсети* (subnet address) и *номер подсети* (subnet number) — это синонимы, относящиеся к числу, которое идентифицирует подсеть. Фактическое значение — это разделенное точками десятичное число, поэтому термин *имя подсети* (subnet name) неприменим. Термин *широковещательный адрес подсети* (subnet broadcast) — это синоним термина *широковещательный адрес подсети* (subnet broadcast address). Он относится к последнему (самому высокому) числовому значению в адресе подсети.

Глава 12

1. Б и В. Сетевые идентификаторы сети класса A имеют первый октет в диапазоне 1–126 и нули в последних трех октетах. Адрес 130.0.0.0 — это фактически сеть класса B (диапазон первого октета от 128 до 191 включительно). Все адреса, которые начинаются с 127, зарезервированы, поэтому адрес 127.0.0.0 — это не сеть класса A.
2. Д. Все адреса сети класса B начинаются со значения в диапазоне от 128 до 191 включительно в первом октете. В первом октете идентификатора сети может быть любое значение в диапазоне 128–191 и любое значение в диапазоне от 0 до 255 включительно во втором октете, с десятичными нулями в последних двух октетах. Во втором октете двух из ответов находится 255, что вполне приемлемо. Во втором октете двух из ответов находится 0, что также приемлемо.
3. Б и Г. Первый октет (172) находится в диапазоне адресов (128–191) сети класса B. В результате идентификатор сети может быть сформирован при копировании первых двух октетов (172.16) и заполнен нулями последних двух октетов (172.16.0.0). Для всех сетей класса B по умолчанию задана маска 255.255.0.0, а количество битов хоста во всех не разделенных на подсети сетях класса B составляет 16.
4. А и В. Первый октет (192) находится в диапазоне адресов (192–223) сети класса C. В результате идентификатор сети может быть сформирован при копировании первых трех октетов (192.168.6) и заполнен нулями последнего октета (192.168.6.0). Для всех сетей класса C по умолчанию задана маска 255.255.255.0, а количество битов хоста во всех не разделенных на подсети сетях класса C составляет 8.
5. Г. Для поиска широковещательного адреса сети выясните сначала ее класс, а затем определите количество октетов хоста. Затем преобразуйте октеты хоста в 255, чтобы получить широковещательный адрес сети. В данном случае адрес 10.1.255.255 находится в сети класса A с тремя последними октетами хоста для широковещательного адреса сети 10.255.255.255. Адрес 192.168.255.1 — это адрес

сети класса C с последним октетом как часть хоста для широковещательного адреса сети 192.168.255.255. Адрес 224.1.1.255 принадлежит сети класса D, а следовательно, не находится ни в какой одноадресатной сети IP, поэтому вопрос к нему неприменим. Адрес 172.30.255.255 — это адрес сети класс B с последними двумя октетами хоста. Таким образом, широковещательный адрес этой сети — 172.30.255.255.

6. Б. Для поиска идентификатора сети выясните сначала ее класс, а затем определите количество октетов хоста. Затем преобразуйте октеты хоста в нули, чтобы получить идентификатор сети. В данном случае адрес 10.1.0.0 находится в сети класса A, с тремя последними октетами хоста для идентификатора сети 10.0.0.0. Адрес 192.168.1.0 — это адрес сети класса C с последним октетом как часть хоста для идентификатора сети 192.168.1.0. Адрес 127.0.0.0 выглядит как идентификатор сети, но начинается с зарезервированного значения (127), поэтому он не находится ни в какой сети класса A, B, или C. Адрес 172.20.0.1 — это адрес сети класса B с последними двумя октетами хоста, таким образом, идентификатор этой сети — 172.20.0.0.

Глава 13

1. В. Рассмотрим преобразование по одному октету за раз. Каждый из первых двух октетов преобразуется в 8 двоичных единиц. Число 254 преобразуется в 8-битовое двоичное значение 11111110, а десятичное число 0 преобразуется в 8-битовое двоичное число 00000000. В результате полное количество двоичных единиц, определяющих длину префикса, составляет 8+8+7+0 =/23.
2. Б. Рассмотрим преобразование по одному октету за раз. Каждый из первых трех октетов преобразуется в 8 двоичных единиц. Число 240 преобразуется в 8-битовое двоичное значение 11110000. В результате полное количество двоичных единиц, определяющих длину префикса, составляет 8+8+8+4 =/28.
3. В. Значение /24 — это эквивалент маски, содержащей 24 двоичные единицы. Чтобы преобразовать маску в формат DDN, напишите все двоичные единицы (в данном случае 24), а остаток до 32-го разряда дополните двоичным нулями. Затем берите по 8 битов за раз и пересчитайте их из двоичной системы в десятичную (либо запомните девять возможных значений октета маски DDN и их двоичные эквиваленты). Значение маски /24 в двоичном виде составит 11111111 11111111 11111111 00000000. Поскольку каждый из первых трех октетов состоит целиком из двоичных единиц, они преобразуются в 255. Последний октет состоит целиком из двоичных нулей, он преобразуется в десятичное число 0. В результате получится маска DDN 255.255.255.0. Таблица десятично-двоичных преобразований приведена в приложении **A**.
4. Б. Значение /30 — это эквивалент маски, содержащей 30 двоичных единиц. Чтобы преобразовать маску в формат DDN, напишите все двоичное единицы (в данном случае 30), а остаток до 32-го разряда дополните двоичным нулями. Затем берите по 8 битов за раз и пересчитайте их из двоичной системы в десятичную (либо запомните девять возможных значений октета маски DDN и их двоичные эквиваленты). Значение маски /30 в двоичном виде составит 11111111

11111111 11111111 11111100. Поскольку каждый из первых трех октетов состоит целиком из двоичных единиц, они преобразуются в 255. Последний октет, 11111100, преобразуется в десятичное число 252. В результате получится маска DDN 255.255.255.252. Таблица десятично-двоичных преобразований приведена в приложении **A**.

5. В. Размер части сети всегда составляет 8, 16 бит или 24 бита, в зависимости от класса сети A, B или C соответственно. Поскольку адрес из сети класса A — N=8. Маска 255.255.255.0 преобразуется в префикс /24. Количество битов подсети — разница между длиной префикса (24) и N, поэтому в данном случае S=16. Размер части хоста — это число, которое, будучи добавлено к длине префикса (24), даст 32, таким образом, H=8 в данном случае.
6. А. Размер части сети всегда составляет 8, 16 бит или 24 бита, в зависимости от класса сети A, B или C соответственно. Поскольку адрес из сети класса C — N=24. Количество битов подсети — разница между длиной префикса (27) и N, поэтому в данном случае S=3. Размер части хоста — это число, которое, будучи добавлено к длине префикса (27), даст 32, таким образом, H=5 в данном случае.
7. Б и Г. Правила бесклассовой адресации определяют структуру IP-адреса с двумя частями: префикса и хоста. Часть хоста определяется так же, как и при классовой IP-адресации. Длина префикса по правилам бесклассовой адресации — это совместная длина частей сети и подсети при использовании концепции классовой IP-адресации. Математически длина префикса равна количеству двоичных единиц в маске. В данном случае при маске 255.255.255.0 длина префикса составит 24 бита. Длина части хоста — это количество битов, добавленных к 24, чтобы получилось 32, т.е. 8 битов.
8. Г. Правила бесклассовой адресации определяют структуру IP-адреса с двумя частями: префикса и хоста. Эта логика игнорирует правила классов A, B и C, она может быть применена к 32-разрядным IPv4-адресам от любого класса. При игнорировании правил класса A, B и C бесклассовая адресация игнорирует любые различия между частями сети IPv4-адреса.
9. А и Б. Маски в двоичном представлении определяют количество двоичных единиц, выделяющих длину части префикса (сеть + подсеть). В сети класса B часть сети составляет 16 битов. Для поддержки 100 подсетей часть подсети должна быть по крайней мере 7 битов длиной. Шесть битов подсети составили бы только $2^6 = 64$ подсетей, а 7 битов подсети составят $2^7 = 128$ подсетей. Ответ: префикс /24 предоставит 8 битов подсети, маска 255.255.255.252 — 14 битов подсети.

Глава 14

1. Г. При использовании классовых концепций IP-адресации, описанных в главе 13, у адресов есть три части: сети, подсети и хоста. Для адресов в одной классовой сети часть сети должна быть идентична у всех адресов в той же сети. Для адресов в той же подсети части сети и подсети должны иметь идентичные значения. Часть хоста различных адресов в той же подсети является индивидуальной.

2. Б и Г. Идентификатор подсети в любой подсети — это наименьшее число в диапазоне, широковещательный адрес подсети — наибольшее, а пригодные для использования IP-адреса находятся между ними. У всех адресов в подсети идентичные двоичные значения в части префикса (бесклассовое представление), а также в частях сети и подсети (классовое представление). Чтобы быть самым младшим номером, у идентификатора подсети должно быть самое низкое возможное двоичное значение (все нули) в части хоста. Чтобы быть самым старшим номером, у широковещательного адреса должно быть максимально возможное двоичное значение (все единицы) в части хоста. Ни идентификатор подсети, ни широковещательный адрес подсети к пригодным для использования адресам не относится, поэтому у адресов в диапазоне, пригодных для использования IP-адресов, никак не могут быть все нули или единицы в части хоста.
3. В. Маска преобразуется в 255.255.255.0. При поиске идентификатора подсети для каждого октета маски со значением 255 можно просто скопировать соответствующие значения IP-адреса. Для октетов маски с десятичным числом 0 можно сразу записать нули в соответствующем октете идентификатора подсети. Таким образом, для нахождения идентификатора подсети 10.7.99.0 скопируйте числа 10.7.99, а для 4-го октета напишите 0.
4. В первую очередь, резидентская подсеть (идентификатор той подсети, в которой располагается адрес) в цифровой форме должна быть меньше IP-адреса, что исключает один из ответов. Маска преобразуется в 255.255.255.252. Поскольку первые три октета маски имеют значения 255, можно скопировать первые три октета IP-адреса. Для четвертого октета значение идентификатора подсети должно быть кратно 4, поскольку 256 – 252 (маска) = 4. К кратным числам относятся 96 и 100, а правильный выбор — это самое близкое кратное к значению IP-адреса в этом октете (97) без превышения. Таким образом, правильный идентификатор подсети 192.168.44.96.
5. В. Резидентский идентификатор подсети в данном случае 172.31.77.192. Широковещательный адрес подсети можно найти на основании идентификатора подсети и маски несколькими методами. Маска преобразуется в 255.255.255.224, таким образом, интересен октет 4 с магическим значением 256 – 224 = 32. Для трех октетов, где маска = 255, скопируйте идентификатор подсети (172.31.77). Для интересующего октета возьмите значение идентификатора подсети (192), добавьте магическое значение (32), вычтите 1, получится 223. Это даст широковещательный адрес подсети 172.31.77.223.
6. В. Чтобы ответить на этот вопрос, необходимо выяснить диапазон адресов в подсети, что, как правило, означает необходимость вычислить идентификатор и широковещательный адрес подсети. При идентификаторе/маске подсети 10.1.4.0/23 маска преобразуется в 255.255.254.0. Для поиска широковещательного адреса после процесса, описанного в данной главе, можно скопировать первые два октета идентификатора подсети, поскольку маска имеет в них значение 255. В четвертом октете запишете 255, поскольку у маски в четвертом октете 0. В интересующем октете 3 добавьте магическое значение (2) к значению идентификатора подсети (4), вычтите 1, чтобы получить значение 2 + 4 – 1 = 5.

(Магическое значение в данном случае вычисляется как 256 – 254 = 2.) Это дает широковещательный адрес 10.1.5.255. Последний пригодный для использования адрес на единицу меньше: 10.1.5.254. Диапазон, который включает последние 100 адресов, — 10.1.5.155–10.1.5.254.

7. Б. Чтобы ответить на этот вопрос, необходимо вычислить широковещательный адрес подсети, поскольку следует знать нижний конец диапазона адресов в подсети. Первый IP-адрес в подсети на единицу больше идентификатора подсети, или 192.168.9.97. Первые 20 адресов составляют диапазон 192.168.9.97–192.168.9.116.

Глава 15

1. Б и Д. В маршрутизаторах компании Cisco есть выключатель питания, в коммутаторах — обычно нет.
2. А. И в маршрутизаторах, и в коммутаторах используются IP-адреса, поэтому обе команды, ip address *адрес маска* и ip address dhcp, могут использоваться в коммутаторах и маршрутизаторах. Команда interface vlan 1 встречается только в коммутаторах.
3. Б и Г. Чтобы маршрутизировать пакеты, у интерфейса маршрутизатора должен быть IP-адрес и его состояние должно быть “up” и “up”. В последовательных каналах в лабораторном стенде, когда не используются модули CSU/DSU, на одном конце канала в интерфейсе должна стоять команда clock rate, которая в данном случае будет задавать скорость линии. Команды bandwidth и description не влияют на работоспособность канала.
4. В. Если первый код состояния интерфейса равен “down”, значит, есть проблема на уровне 1 (например, кабель не подключен к интерфейсу).
5. В и Д. Команда show ip interface brief выводит все IPv4-адреса интерфейса, но не маски. Команда show version не выводит ни IP-адресов, ни масок. Остальные три команды выводят и адреса, и маски.
6. Б. У маршрутизатора есть по одному IPv4-адресу для каждого используемого интерфейса, а у коммутатора LAN только один IPv4-адрес, используемый для обращения к коммутатору. В остальных ответах перечислены параметры конфигурации, использующие те же соглашения и для маршрутизаторов, и для коммутаторов.

Глава 16

1. Б. Компьютеры используют логику с двумя возможностями: передать локальные пакеты (предназначенные для хостов в той же подсети) непосредственно или передать дистанционные пакеты (предназначенные для хостов в других подсетях) на стандартный шлюз/маршрутизатор. В данном случае компьютер имеет IP-адрес 192.168.5.77 с маской 255.255.224.0, поэтому он находится в подсети 192.168.4.64/27. Диапазон адресов этой подсети от 192.168.4.64 до 192.168.4.95, включая адрес подсети и широковещательный адрес. В результате

компьютер передаст пакет на свой стандартный шлюз. Что касается других неправильных ответов, то если бы команда ping использовала имя хоста, то она сначала запросила бы у сервера DNS имя. Кроме того, у компьютера уже есть IP-адрес, поэтому в сервере DHCP нет необходимости.

2. А и В. Используя идентификатор подсети и маску, маршрут определяет группу адресов, представленных в соответствии с маршрутом. Маршрутизатор может использовать эти номера для поиска диапазона адресов, соответствующего этому маршруту. В двух других ответах названы факты, полезные при перенаправлении пакетов по соответствующему маршруту.
3. А и Е. Из всех перечисленных команд только две синтаксически правильные команды настройки маршрутизатора. Командой, разрешающей магистральное соединение 802.1Q, является encapsulation dot1q *vlan_id*.
4. В. Если в конфигурации устройства указана команда no ip subnet-zero, маршрутизатор не позволит настроить на интерфейсах IP-адреса из нулевой подсети. В указанных ответах подсеть 10.0.0.0 255.254.0.0 является нулевой, ее диапазон — 10.0.0.1–10.1.255.254. Команда ip address 10.1.2.2 255.254.0.0 не будет принята устройством.
5. В. Конфигурация средств маршрутизации коммутатора уровня 3 использует интерфейсы VLAN с номером интерфейса, соответствующим идентификатору VLAN. Соответствующие подключенные маршруты, как все связанные маршруты IP, перечисляют интерфейсы, но не IP-адрес следующей транзитной точки перехода. Эти три подключенных маршрута перечислят интерфейсы VLAN 1, 2 и 3 соответственно.
6. В. Команда ip route может ссылаться на IP-адрес следующего транзитного маршрутизатора или на интерфейс локального маршрутизатора. Она также может ссылаться на соответствующий идентификатор и маску подсети, определяя диапазон адресов в соответствии с маршрутом.
7. А. В правильном синтаксисе команды должен быть сначала указан адрес подсети, затем маска подсети в десятично-точечном формате и в конце команды — выходной интерфейс или IP-адрес следующего транзитного узла на маршруте.

Глава 17

1. Г и Д. Обе версии протокола RIP используют дистанционно-векторную логику, а протокол EIGRP использует другой вид логики, улучшенный дистанционно-векторный или сбалансированный гибридный.
2. В и Г. Обе версии протокола RIP используют ту же метрику счетчика переходов.
3. Б, В, Г, и Д. Только прежняя версия протокола RIP (RIP-1) не поддерживает маски подсети переменной длины (VLSM).
4. Б. Протоколы состояния канала не обмениваются информацией о маршрутах. Они передают информацию о метриках, но это информация интерфейсов, она не привязана к подсети. Протоколы состояния канала требуют, чтобы алгоритм SPF получал различные элементы информации и создавал маршруты на их основе.

5. А и Г. Протокол OSPF использует алгоритм SPF, разработанный на базе математического алгоритма Дейкстры.
6. Б. Команда network 10.0.0.0 0.255.255.255 area 0 работает потому, что она соответствует всем интерфейсам с первым октетом 10. Остальная часть команд соответствует следующему: всем адресам, завершающимся на 0.0.0 (шаблон маски 255.0.0.0); всем адресам, начинающимся на 10.0.0 (шаблон маски 0.0.0.255); и всем адресам, начинающимся на 10.0 (шаблон маски 0.0.255.255).
7. А. Команда network 0.0.0.0 255.255.255.255 area 0 соответствует всем IP-адресам из-за шаблона маски 255.255.255.255, поэтому она разрешает протокол OSPF в области 0 на всех интерфейсах. Ответ с шаблоном маски 0.255.255.0 некорректен, поскольку он содержит несколько последовательностей двоичных 0, разделенных двоичными 1. Ответ с символами x синтаксически некорректен. Ответ с шаблоном маски 255.0.0.0 означает “соответствует всем адресам, последние три октета которых равны 0.0.0”, поэтому ни один из трех интерфейсов этому не соответствует.
8. А и Д. Из трех неправильных ответов два — реальные команды, которые просто не перечисляют соседей OSPF. Команда show ip ospf interface brief выводит список интерфейсов, на которых разрешен протокол OSPF, но не соседей. Команда show ip interface выводит подробности IPv4 об интерфейсах, но не имеет никакого отношения к OSPF. Один из неправильных ответов — show ip neighbor — недопустимая команда IOS.

Глава 18

1. Б и Г. Клиент передает сообщение Discover, а сервер возвращает сообщение Offer. Затем клиент посылает сообщение Request, в ответ на которое сервер возвращает IP-адрес в сообщении Acknowledgment.
2. Д. Из команд в ответах три синтаксически корректны, а одна нет: ip dhcp-server 10.1.10.1. Ответ с этой командой неправильный. Команда ip helper-address 10.1.10.1 действительно необходима как подкоманда интерфейса, но только на дистанционных маршрутизаторах, таких как Boston. Эта команда не нужна серверу DNS, поскольку после приема команды ip helper-address 10.1.10.2 она не поможет работе DHCP или DNS. И наконец, команда ip name-server 10.1.10.2 на маршрутизаторе Atlanta сработает, но она просто позволит пользователям CLI маршрутизатора Atlanta использовать сервер DNS и никак не влияет на пользовательский трафик DNS.
3. Б. Конфигурация помещает в пул DHCP параметры каждого клиента: IP-адрес клиента, маску, IP-адреса стандартного маршрутизатора и сервера DNS. Пул также содержит отрезок времени, на протяжении которого клиент резервирует адрес. Вне пула DHCP находится только список исключенных (ip dhcp exclude-address).
4. Б и Г. Компьютер должен знать собственный IP-адрес, маску, IP-адрес стандартного маршрутизатора и IP-адреса серверов DNS.
5. А. Проверка с помощью команды ping собственного адреса не покажет, работает ли локальная сеть, поскольку пакет через сеть не передается. Необходимо

пересылать пакеты эхо-запросов от устройства PC1 через стандартный шлюз (R1), чтобы проверить работоспособность сети, по крайней мере, на участке от хоста до шлюза. Единственный ответ, в котором указано, что пакеты будут проходить искомый участок сети (между PC1 и R1), — ping 10.1.1.1, даже несмотря на то, что такая проверка дает отрицательный результат.

6. А, В и Д. Команда tracert в операционных системах компании Microsoft и команда traceroute в операционной системе Cisco IOS выводит список IP-адресов промежуточных маршрутизаторов и адрес хоста-получателя. Первой записью в выводе команды будет адрес ближайшего маршрутизатора к хосту — шлюза.
7. В. Символ звездочки (*) около соединения с номером 2 указывает на последнее активное соединение, в которое команда resume переключит пользователя, если в ней не указать параметров.

Глава 19

1. А. При 50-процентном росте маска должна определить достаточно битов подсети, чтобы создать 150 подсетей. В результате маска должна иметь по крайней мере 8 битов подсети (7 битов подсети составят 2^7, или 128 подсетей, а 8 битов подсети составляют 2^8, или 256 подсетей). Точно так же потребность в 50-процентном росте для наибольшей подсети означает, что часть хоста нуждается в достаточном количестве битов для 750 номеров хостов в подсети. Девяти битов хоста недостаточно ($2^9 - 2 = 510$), но 10 битов хоста поставляют 1022 хоста/подсети ($2^{10} - 2 = 1022$). При 16 битах сети, обусловленных выбором сети класса В, проект нуждается в общей сложности в 34 битах (по крайней мере) маски (16 сетей, 8 подсетей, 10 хостов), но есть только 32 бита, поэтому требованиям не соответствует ни одна из масок.
2. Б. При 20-процентном росте проект должен поддерживать 240 подсетей. 7 битов подсети не удовлетворят эту потребность ($2^7 = 128$), необходимо 8 битов подсети ($2^8 = 256$). Аналогично минимальное количество битов хоста также составляет 8, поскольку 20-процентный рост потребует наличия 144 хостов на подсеть. Это количество требует 8 битов хоста ($2^8 - 2 = 254$). Это минимальные количества битов хоста и подсети.У правильного ответа, 10.0.0.0/22, есть 8 битов сети, так как выбрана сеть класса А, 14 битов подсети (/22 – 8 = 14) и 10 битов хоста (32 – 22 = 10). Эта маска обеспечивает по крайней мере 8 битов подсети и 8 битов хоста. Маски в других ответах либо не обеспечивают 8 битов хоста, либо 8 битов подсети.
3. Б. Для обеспечения 1000 подсетей необходимо 10 битов подсети ($2^{10} = 1024$). Проект использует сеть класса В, а значит, уже существует 16 битов сети. Самой короткой соответствующей требованиям маской будет 255.255.255.192 или /26, она состоит из 16 битов сетей плюс 10 битов подсети. Ответ /28 также предоставляет достаточно подсетей, но по сравнению с /26 маска /28 оставляет меньше битов для хоста, а следовательно, обеспечивает меньше хостов на подсеть.
4. Г. Для выбора маски с максимальным количеством подсетей следует выбрать маску с минимальным количеством битов хоста, что в свою очередь максими-

зирует количество битов подсети. В данном случае проект требует 200 хостов на подсеть. Семь битов хоста не обеспечивают достаточно хостов в подсети ($2^7 - 2 = 126$), а 8 битов хоста вполне ($2^8 - 2 = 254$). Проект использует сеть класса А с 8 битами сети. Префиксная маска /24 (маска с 8 битами хоста — это минимум для обеспечения достаточного количества хостов на подсеть) максимизирует размер части подсети, предоставляя в данном случае 16 битов подсети.

5. В и Г. Маска преобразуется в 255.255.252.0, таким образом, разница между идентификатором подсети и 256 (называемая в этой книге магическим числом) составляет 256 – 252 = 4. Поэтому идентификаторы подсети начинаются с 172.30.0.0, потом 172.30.4.0, затем 172.30.8.0 и т.д., каждый на 4 больше в третьем октете. Маска, используемая с сетью класса В, подразумевает 6 битов подсети для 64 полных идентификаторов подсети. Последний из них, 172.30.252.0, может быть использован частично, поскольку у третьего октета, где находятся биты подсети, то же значение, что и у маски в третьем октете.
6. А. Первый (наименьший в цифровой форме) идентификатор подсети совпадает с номером классовой сети, или 192.168.9.0. Каждый остальной идентификатор подсети на 8 больше предыдущего и создает последовательность 192.168.9.8, 192.168.9.16, 192.168.9.24, 192.168.9.32 и т.д. до 192.168.9.248.
7. Г. При использовании маски /24 (255.255.255.0) идентификаторы подсети увеличиваются на 1 в третьем октете. При сети класса В есть 16 битов сети, и следующие 8 битов с маской /24 — биты подсети, таким образом, весь третий октет содержит биты подсети. У всех идентификаторов подсети в последнем октете будет 0, поскольку весь четвертый октет состоит из битов хоста. Обратите внимание, что 172.19.0.0 (нулевая подсеть) и 172.19.255.0 (широковещательная подсеть), как ни странно, являются вполне допустимыми идентификаторами подсети.
8. Г. Согласно описанному в этой главе процессу, при сети класса А и маске /25 получается 8 битов сети (по классу) и 17 битов подсети (октеты 2 и 3 полностью, а также 1 бит подсети в октете 4). Магическое число применяется в четвертом октете для поиска значения, добавляемого к предыдущему идентификатору подсети при поиске следующего идентификатора подсети. Магическое число в данном случае 256 – 128 = 128.В результате четвертый октет будет или 0 или 128. Октеты 2 и 3 могли быть любым значением от 0 до 255 включительно. Только один ответ (10.1.1.192) нарушает значение этого диапазона.

Глава 20

1. Б, В, и Г. Бесклассовые протоколы маршрутизации по определению поддерживают маски VLSM, поскольку бесклассовые протоколы маршрутизации передают маску подсети в своих анонсах маршрутизации. Из всех ответов только протокол RIP версии 1 (RIP-1) не является бесклассовым протоколом маршрутизации.
2. А. Под аббревиатурой “VLSM” понимают как маски переменной длины, так и процесс разделения сети на подсети с разными масками.

3. А. Подсеть 10.5.0.0 255.255.240.0 предполагает использование диапазона 10.5.0.0–10.5.15.255, который не пересекается с условием. Подсеть 10.4.0.0 255.254.0.0 предполагает использование диапазона 10.4.0.0–10.5.255.255, который пересекается с сетью в условии. Подсеть 10.5.32.0 255.255.224.0 предполагает использование диапазона 10.5.32.0–10.5.63.255, который пересекается с сетью в условии. Подсеть 10.5.0.0 255.255.128.0 предполагает использование диапазона 10.5.0.0–10.5.127.255, который пересекается с сетью в условии.
4. Г. В ответах предлагаются четыре следующих диапазона: 172.16.0.0/21: 172.16.0.0–172.16.7.255, 172.16.6.0/23: 172.16.6.0–172.16.7.255, 172.16.16.0/20: 172.16.16.0–172.16.31.255, 172.16.11.0/25: 172.16.11.0–172.16.11.255. Подсеть 172.16.8.0/22 в вопросе подразумевает диапазон 172.16.8.0–172.16.11.255, включающий диапазон адресов подсети 172.16.11.0/25.
5. В. В вопросе перечислены три существующих подсети, которые вместе используют часть сети класса С 192.168.1.0. Эти подсети используют в последнем октете значения 0–63, 128–131 и 160–167. Новая подсеть с маской /28 нуждается в 16 последовательных номерах подсетей, и все они будут кратны 16 в последнем октете (0, 16, 32 и т.д.). Взглянув на используемые номера снова, можно заметить, что они начинаются с 64 и продолжаются до 127, следовательно, здесь есть более чем достаточное пространство для 16 адресов. Таким образом, самый низкий в цифровой форме номер подсети — 192.168.1.64/28 с диапазоном 192.168.1.64–192.168.1.79.

Глава 21

1. В. Диапазон всех трех сетей присутствует во всех ответах, за исключением подсети 10.3.64.0 255.255.224.0, которая предполагает использование диапазона адресов 10.3.64.0–10.3.95.255. В остальных ответах для подсети 10.3.64.0 255.255.192.0 характерен наименьший диапазон адресов (10.3.64.0–10.3.127.255).
2. В и Г. Сеть с адресом 10.0.0.0 и маской 255.0.0.0 включает в себя все подсети, начинающиеся со значения 10 в первом октете; сеть 10.1.0.0 с маской 255.255.0.0 включает в себя подсети, начинающиеся с 10.1, поэтому эти два ответа включают диапазоны сетей, перечисленные в вопросе. Подсеть 10.1.32.0 255.255.224.0 предполагает использование диапазона 10.1.32.0–10.1.63.255, который не включает в себя все необходимые адреса. Подсеть 10.1.48.0 255.255.248.0 представляет собой диапазон адресов 10.1.48.0–10.1.55.255, в который не входят две из сетей, перечисленных в вопросе.
3. Г. Согласно описанному в книге процессу, диапазоны адресов в подсетях таковы: 10.1.12.0–10.1.12.255, 10.1.14.0–10.1.14.255 и 10.1.15.0–10.1.15.255. Таким образом, весь диапазон составляет 10.1.12.0–10.1.15.255. Наименьшим идентификатором подсети является 10.1.12.0, а исходным значением /P должно быть /23. Вычисление идентификатора подсети и широковещательного адреса для этих двух номеров дает 10.1.12.0/23 и широковещательный адрес 10.1.13.255. Этот диапазон не включает все адреса первоначальной подсети, поэтому повторите процесс со значениями 10.1.12.0 и /22. Эта комбинация дает подсеть 10.1.12.0 и широковеща-

тельный адрес 10.1.15.255, который действительно включает все адреса. Получаем наилучшую подсеть и маску 10.1.12.0/22.

4. Б. Согласно описанному в книге процессу, диапазоны адресов в подсетях таковы: 192.168.1.64–192.168.1.79, 192.168.1.80–192.168.1.95 и 192.168.1.96–192.168.1.111. Таким образом, весь диапазон составляет 192.168.1.64–192.168.1.111. Наименьшим идентификатором подсети является 192.168.1.64, а исходным значением /P должно быть /27.Вычисление идентификатора подсети и широковещательного адреса для этих двух номеров дает 192.168.1.64/27 и широковещательный адрес 192.168.1.95. Этот диапазон не включает все адреса первоначальной подсети, поэтому повторите процесс со значениями 192.168.1.64 и /26. Эта комбинация дает подсеть 192.168.1.64 и широковещательный адрес 192.168.1.127, который действительно включает все адреса. Получаем наилучшую подсеть и маску 192.168.1.64 /26.

Глава 22

1. А и В. В стандартных списках ACL проверяется IP-адрес отправителя. Диапазон адресов 10.1.1.1–10.1.1.4 может быть проверен с помощью стандартного списка, но придется настроить несколько команд access-list. Чтобы выделить списком все хосты в подсети Барни, можно указать команду access-list 1 permit 10.1.1.0 0.0.0.255.
2. А и Г. Диапазон допустимых номеров ACL для стандарта нумерации списков ACL IP — это 1–99 и 1300–1999 включительно.
3. Г. Шаблон маски 0.0.0.255 позволяет проверить все пакеты, первые 3 октета которых совпадают с указанными в правиле. Такая маска понадобится, если нужно выделить подсеть, сетевая часть и часть подсети которой занимают первые три октета.
4. Д. Шаблон маски 0.0.15.255 позволяет проверить пакеты на основании первых 20 бит IP-адреса. Такая маска понадобится, если нужно выделить подсеть, сетевая часть и часть подсети которой занимает 20 бит.
5. А. Маршрутизатор всегда осуществляет поиск в операторах ACL по порядку и прекращает поиск после обнаружения первого соответствия. Другими словами, используется логика первого соответствия. Пакет с IP-адресом отправителя 1.1.1.1 соответствовал бы любой из трех заданных явно команд, описанных в вопросе. В результате будет использоваться первый оператор.
6. Б. В одном неправильном ответе с шаблоном маски 0.0.255.0 будет соответствие всем пакетам, адреса которых начинаются с 172.16 и содержат 5 в последнем октете. Другой неправильный ответ соответствует только одному IP-адресу 172.16.5.0. Еще один неправильный ответ использует шаблон маски 0.0.0.128, который содержит только один двоичный бит шаблона и обеспечивает соответствие только адресам 172.16.5.0 и 172.16.5.128. Правильный ответ соответствует диапазону адресов 172.16.4.0–172.16.5.255, который включает все адреса подсети, указанной в вопросе (172.16.5.0–172.16.5.127).

Глава 23

1. Д и Е. Расширенные списки управления доступом позволяют проверять параметры уровня 3 (IP) и уровня 4 (TCP, UDP) в заголовках пакетов, а также некоторую другую информацию, но не позволяют проверять информацию уровня приложений. Именованные расширенные списки ACL позволяют проверять те же параметры, что и нумерованные.
2. А и Д. Правильный диапазон номеров расширенных списков ACL — 100–199 и 2000–2999. Ответы, в которых указаны параметры eq www после адреса 10.1.1.1, предполагают проверку номера порта отправителя, а пакеты передаются веб-серверу, но не в обратном направлении.
3. Д. Поскольку пакет передается веб-клиенту, следует проверять в правилах номер порта веб-сервера в качестве параметра порта отправителя. Диапазон IP-адресов клиента не указан в вопросе, а адреса серверов — указаны. Поэтому адрес отправителя, начинающийся с октетов 172.16.5, должен присутствовать в правильном ответе.
4. Д. Именованный список управления доступом позволяет проверять те же параметры в пакете, что и нумерованный.
5. А и В. В операционных системах IOS до версии 12.3 нумерованные списки управления доступом при перенастройке необходимо было полностью удалять и переконфигурировать, даже если нужно всего лишь изменить в нем одну строку. Начиная с версии 12.3 в правилах списка управления доступом можно нумеровать строки с правилами и добавлять или удалять нужную строку при переконфигурировании.
6. В. Согласно рекомендациям компании Cisco, стандартные списки управления доступом нужно размещать как можно ближе к получателю.
7. А. Протокол NTP используют сообщения, передаваемые между клиентами и серверами, чтобы они могли согласовать свое время с сервером. Протокол NTP совершенно не связан с синхронизацией последовательного канала. Он не подсчитывает также циклы процессора, а полагается на сообщения сервера NTP. Кроме того, поскольку клиент определяет IP-адрес сервера, они не обязаны находиться в той же подсети.

Глава 24

1. Е. Термин *бесклассовое* (classless) свидетельствует о том факте, что маршруты анонсируют блок адресов с маской, позволяя, по существу, игнорировать ограничения класса A, B и C и задавать используемый блок адресов. Кроме того, поскольку необходимо описать маршруты между различными компаниями (разными доменами маршрутизации), используется термин *междоменная* (interdomain).
2. Г. Изначально технология CIDR была предназначена для суммирования нескольких сетей класса A, B или C, чтобы уменьшить размер таблиц маршрутизации в Интернете. В представленных ответах только запись 200.1.0.0 255.255.0.0 описывает суммарную сеть.

3. Б и Д. В документе RFC 1918 описаны частные сети. В нем указаны сеть класса A 10.0.0.0, сети класса B 172.16.0.0–172.31.0.0, а также сети класса C 192.168.0.0–192.168.255.0.
4. В. При использовании статической трансляции NAT все правила задаются вручную. Поскольку в вопросе указано, что должны быть преобразованы внутренние адреса, следует указать параметр inside.
5. А. При использовании динамической трансляции NAT все записи трансляции пакетов создаются, когда первый пакет проходит из внутренней сети через устройство.
6. А. Параметр list 1 задает список управления доступом IP, который используется для проверки пакетов и идентификации внутренних локальных адресов.
7. А и В. В конфигурации пропущен параметр overload в команде ip nat inside source, а также отсутствует команда ip nat outside в конфигурации последовательного интерфейса.
8. Б. В последней строке указано, что в пуле есть семь адресов и все они использованы, а значение счетчика приблизительно равно 1000. Следовательно, около 1000 новых потоков было отброшено, поскольку в пуле трансляции NAT нет свободных адресов.

Глава 25

1. В. Трансляция NAT, а именно ее разновидность PAT, позволяет многим хостам использовать частные IPv4-адреса, обладая одним открытым IPv4-адресом, но это было одним из краткосрочных решений проблемы исчерпания IPv4-адресов. Протокол IP версии 5 существовал недолго и как сугубо экспериментальный протокол, не имеющий никакого отношения к исчерпанию IPv4-адресов. Протокол IPv6 предназначен для решения проблемы исчерпания IPv4-адреса, и это долгосрочное решение. Протокол ARP не влияет на количество используемых IPv4-адресов.
2. А. При маршрутизации пакетов IPv6 маршрутизаторы используют те же этапы процесса, что и при маршрутизации пакетов IPv4. Маршрутизаторы перенаправляют пакеты IPv6 на основании IPv6-адреса получателя, указанного в заголовке пакета IPv6. В результате маршрутизатор отбрасывает заголовок и концевик канала связи входящего фрейма, оставляя пакет IPv6. Маршрутизатор сравнивает IPv6-адрес получателя (не отправителя) в заголовке с адресами IPv6 (не IPv4) в таблице маршрутизации, а затем перенаправляет пакет на основании найденного маршрута.
3. Г. Если следовать описанному здесь процессу, то на первом этапе удаляется до трех предваряющих нулей в каждом квартете, — остается FE80:0:0:100:0:0:0:123. Остаются две последовательности нулевых квартетов (все-0); после замены самой длинной строки нулей на :: получаем адрес FE80:0:0:100::123.
4. Б. В этом вопросе много квартетов, позволяющих сделать ошибку: удаление замыкающих нулей в квартете шестнадцатеричных цифр. При сокращении IPv6-

адреса удаляются только предваряющие нули в квартете. У большинства квартетов есть замыкающие нули (в правой стороне квартета), так что не удаляйте их.

5. А. У несокращенной версии IPv6-адреса должно быть 32 цифры, и только у одного ответа есть 32 шестнадцатеричных цифры. В данном случае исходное число демонстрируют четыре квартета и ::. Таким образом, :: заменяет четыре квартета 0000, чтобы в общем имелось восемь квартетов. Затем для каждого квартета с менее чем четырьмя цифрами добавляются предваряющие нули, чтобы у каждого квартета было по четыре шестнадцатеричных цифры.
6. В. Длина префикса /64 означает, что последние 64 бита, или последние 16 цифр, адреса должны быть заменены на нули. Этот процесс создает несокращенный префикс 2000:0000:0000:0005:0000:0000:0000:0000. Последние четыре квартета полностью заполнены нулями, что делает эту строку лучшим кандидатом на замену::. После удаления предваряющих нулей в других квартетах получаем ответ 2000:0:0:5::/64.

Глава 26

1. В. Уникальные локальные адреса начинаются с части FD в первых двух цифрах.
2. А. Глобальные одноадресатные адреса могут начинаться со многих разных значений, но чаще всего они начинаются с шестнадцатеричной 2 или 3.
3. Г. Глобальный префикс маршрутизации — это блок адресов, представленный как префиксное значение и длина префикса, предоставленная некой уполномоченной организацией. У всех IPv6-адресов компании одинаковое значение в начальных битах IPv6-адресов. Аналогично, когда компания использует блок открытых IPv4-адресов, у них будет то же значение в части сети.
4. Б. Создание блока глобальных одноадресатных адресов подсетей с использованием единой длины префикса для всех подсетей подразумевает разделение адреса на три части. Частями являются глобальный префикс маршрутизации, подсеть и идентификатор интерфейса.
5. Г. Уникальные локальные адреса начинаются с 2-х шестнадцатеричных цифр (префикса FD), сопровождаемых 10-ю шестнадцатеричными цифрами глобального идентификатора.

Глава 27

1. А. В единственно правильном ответе указан тот же IPv6-адрес, что и в вопросе, — с длиной префикса /64, причем без пробела в синтаксисе. Еще один (неправильный) ответ идентичен ему, но между адресом и длиной префикса оставлен пробел, что синтаксически неправильно. Оба ответа с параметром eui-64 используют и не используют префикс; префикс должен быть указан, хотя ни один из этих ответов не дал бы IPv6-адрес, указанный в вопросе.
2. Б. При параметре eui-64 маршрутизатор вычислит часть идентификатора IPv6-адреса интерфейса на основании его MAC-адреса. Начав с адреса 5055.4444.3333, маршрутизатор вставляет в его среднюю часть FF FE (5055.44FF.FE44.3333). Затем

маршрутизатор инвертирует седьмой бит в первом байте. Мысленно преобразуйте шестнадцатеричное значение 50 в двоичное 01010000, инвертируйте седьмой бит, чтобы получить строку 01010010, и преобразуйте ее обратно в шестнадцатеричное 52. Окончательное значение идентификатора интерфейса — 5255:44FF:FE44:3333. В неправильных ответах приведены иные значения.

3. А и В. Два правильных ответа из этих четырех демонстрируют минимально необходимую конфигурацию для поддержки протокола IPv6 на маршрутизаторе Cisco: разрешение маршрутизации IPv6 вообще (ipv6 unicastrouting) и разрешение протокола IPv6 на каждом интерфейсе в частности, при добавлении одноадресатного адреса к каждому интерфейсу (ipv6 address...). В двух неправильных ответах приведены несуществующие команды.
4. А. При команде ipv6 address, отданной для глобального одноадресатного адреса, но без адреса, локальный в пределах канала связи маршрутизатор вычислит свой локальный в пределах канала связи адрес интерфейса на основании его MAC-адрес и правил EUI-64. Первая половина локального в пределах канала связи адреса начинается с FE80:0000:0000:0000. Затем маршрутизатор вычисляет вторую половину значения локального в пределах канала связи адреса, добавляя в середину MAC-адреса (0200.0001.000A) части FF FE (0200.00FF.FE01.000A) и инверсии седьмого бита (0000.00FF.FE01.000A).
5. Б. Адрес FF02::1 используется всеми хостами IPv6 на канале связи, адрес FF02::5 — всеми маршрутизаторами OSPFv3, а адрес FF02::A — всеми маршрутизаторами EIGRPv6. Адрес FF02::2 используется для передачи пакетов на все маршрутизаторы IPv6 канала связи.
6. В. Маршрутизатор R1 формирует требуемый многоадресатный адрес узла, используя формат FF02::1:FF*xx*:*xxxx*, где *xx*:*xxxx* заменяется последними шестью шестнадцатеричными цифрами одноадресатного адреса. Если у локального в пределах канала связи адреса и одноадресатного адреса разные значения в последних шести шестнадцатеричных цифрах, то маршрутизатор создаст многоадресатный адрес опрашиваемого узла для обоих. Для формирования многоадресатного адреса опрашиваемого узла FF02::1:FF00:A последними шестью шестнадцатеричными цифрами адреса должно быть шестнадцатеричное 00:000A. Из трех ответов с одноадресатными адресами IPv6 только один представляет значение, последние шесть шестнадцатеричных цифр которого 00:000A. Кроме того, в данном случае локальным в пределах канала связи адресом будет FE80::FF:FE01:A, что приведет к многоадресатному адресу опрашиваемого узла FF02::1:FF01:A, который не является адресом, указанным в вопросе.

Глава 28

1. Б. Компьютер PC1 должен обнаружить MAC-адрес компьютера PC2. В отличие от протокола IPv4, IPv6 не использует протокол ARP, вместо него он использует протокол NDP. А именно: компьютер PC1 использует сообщение запроса соседа NDP (NS), а компьютер PC2 отвечает сообщением анонса соседа NDP (NA). SLAAC имеет отношение к присвоению адреса, а не к обнаружению MAC-адреса соседа.

2. Г. Хосты могут опросить все маршрутизаторы, оповещая о себе в сообщении NDP Router Solicitation (RS), а маршрутизаторы отвечают сообщением NDP Router Advertisement (RA). Запрос соседа NDP (NS) также может использоваться компьютером PC1, но не с целью изучения IPv6-адреса своего стандартного маршрутизатора. DAD — функция, использующая сообщения NS и NA протокола NDP, но она не осуществляет поиск адреса стандартного маршрутизатора. И наконец, правила EUI-64 не определяют ни протокол, ни сообщения.
3. А и В. Сообщение NDP RA содержит IPv6-адрес маршрутизатора, известные на канале связи префиксы IPv6 и соответствующие длины префикса. При использовании протокола DHCPv6 хост изучает IPv6-адрес сервера DNS по сообщениям DHCPv6. Для MAC-адресов соседей по каналу связи хосты используют сообщения NDP NA и NS.
4. В. Хосты используют сообщения NDP, а именно: Router Solicitation (RS) и Router Advertisement (RA) для изучения IPv6-адресов потенциальных стандартных маршрутизаторов. Другие параметры обычно получают от сервера DHCPv6 с фиксацией состояния.
5. Г. SLAAC позволяет хосту выбрать свой одноадресатный адрес. Хост также использует протокол NDP, чтобы изучить длину префикса и адреса любых стандартных маршрутизаторов. Затем он использует сервер DHCP без фиксации состояния для изучения адресов серверов DNS.
6. Б и Г. При SLAAC хост узнает префикс от маршрутизатора, используя сообщения NDP RS/RA, а остальную часть адреса (идентификатор интерфейса) хост вычисляет сам. Хост может использовать правила EUI-64 или определенный процесс для выбора случайного значения идентификатора интерфейса. Хост не узнает идентификатор интерфейса от любого другого устройства, позволяя избавить процесс от фиксации состояния, поскольку никакое другое устройство не должно присваивать хосту его полный адрес.
7. А. Команда show ipv6 neighbors выводит все IPv6-адреса соседей (как маршрутизаторов, так и хостов) и соответствующие им их MAC-адреса. Она не учитывает маршрутизаторы, оставляя эту информацию для команды show ipv6 routers.

Глава 29

1. А и В. При наличии IPv6-адреса на рабочем интерфейсе маршрутизатор добавляет подключенный маршрут для префикса (подсети), используемого командой ipv6 address. Он также добавляет локальный маршрут хоста (с длиной префикса /128) на основании одноадресатного адреса. Маршрутизатор не добавляет маршрут на основании адреса, локального в пределах канала связи.
2. А. Все четыре ответа представляют примеры команд, использующих исходящий интерфейс. Две команды, начинающиеся с ip route, определяют только маршруты IPv4; они были бы отклонены из-за префиксов IPv6, использованных в командах. Две команды, начинающиеся с ipv6 route, синтаксически правильны, но они должны содержать интерфейс локального маршрутизатора (интерфейс

маршрутизатора, на котором применяется команда). Маршрутизатор R5 должен использовать свой локальный интерфейс S0/1/1 как исходящий.

3. Б. Все четыре ответа приводят примеры команд, использующих IPv6-адрес следующего транзитного маршрутизатора. В двух ответах упоминаются собственные IPv6-адреса маршрутизатора R5 (одноадресатный и локальный для канала связи), что неправильно; адрес должен принадлежать соседнему маршрутизатору, в данном случае R6. Для двух ответов, в которых упоминаются адреса на маршрутизаторе R6, правильным будет использующий глобальный одноадресатный адрес маршрутизатора R6. Ответ, использующий локальный в пределах канала связи адрес маршрутизатора R6, требовал бы также исходящего интерфейса R5, поэтому ответ, использующий адрес FE80::FF:FE00:6, также будут отброшен.
4. А и Г. Поскольку у маршрутизатора уже есть конфигурация IPv4, новый процесс OSPFv3 IPv6 будет в состоянии автоматически выбрать собственный идентификатор маршрутизатора. Таким образом, команда router-id для OSPFv3 (один из ответов) хоть и допустима, но не обязательна. Протокол OSPFv3 не использует команду network *префикс/длина*, поэтому данный ответ неправильный. В двух других ответах перечислены команды, необходимые для конфигурации.
5. Б и Г. Команда show ipv6 ospf interface brief выводит по одной строке для каждого интерфейса, на котором разрешен протокол OSPV3. Команда show ipv6 protocols выводит информацию обо всех источниках информации о маршрутизации IPv6; выводятся также сообщения об интерфейсах, на которых разрешен протокол OSPFv3.

Б и В. Протокол OSPFv2 поддерживает маршруты IPv4, в то время как протокол OSPFv3 поддерживает маршруты IPv6. Протокол EIGRP для IPv6 обычно называют EIGRPv6.