Ответы на вопросы и задания

Глава 1

1. Централизованное сетевое приложение.
2. Ячеистая, звезда.
3. Кольцевая.
4. Иерархическая звезда.
5. Адрес назначения, адрес отправителя, идентификатор входного интерфейса.
6. Утверждения (б) и (г) не всегда верны:
7. Утверждения (а), (б), (в) могут быть верными в некоторых случаях, а утверждение (г) верно всегда.
8. Все перечисленные устройства можно назвать коммутаторами.
9. Не может.
10. Невозможность динамического перераспределения пропускной способности физического канала между абонентами, возможность отказа в соединении, необходимость предварительного установления соединения, неэффективность использования пропускной способности при передаче пульсирующего трафика.
11. Наличие очередей и связанный с этим случайный характер задержек.
12. Нет.
13. Все коммутаторы, а также конечный узел-получатель, лежащие на пути устанавливаемого соединения.
14. Практически нельзя.
15. То, в котором фиксируется маршрут.
16. Во второй половине 60-х годов.
17. ARPANET — одна из первых глобальных сетей, ставшая прародительницей Интернета.
18. Работы по созданию LAN активизировались в результате появления недорогих мини-компьютеров и персональных компьютеров.
19. Массовые индивидуальные клиенты (запрашиваемые услуги — телефонная связь, телевидение, радио, доступ в Интернет) и корпоративные

клиенты (запрашиваемые услуги — все те услуги, которые запрашивают индивидуальные клиенты, а кроме этого, услуги по созданию виртуальных частных сетей, хостинг баз данных и веб-сайтов).

20. С одной стороны, нет, поскольку существует традиционное деление сетей на эти два типа. С другой стороны, да, так как эта сеть может выполнять внутрикорпоративные функции и принадлежит корпорации, которая занимается предоставлением телекоммуникационных услуг.
21. Модель OSI стандартизует, во-первых, семиуровневое представление средств взаимодействия систем в сетях с коммутацией пакетов, во-вторых, перечень функций, которые должен выполнять каждый уровень, в-третьих, названия всех уровней.
22. Да, семиуровневая декомпозиция задачи сетевого взаимодействия является одним из возможных вариантов. В частности, в существовавшей еще до появления модели OSI модели сетевого взаимодействия TCP/IP определены только 4 уровня.
23. Не соответствуют стандарту название séances layer, правильное название — session layer.
24. Все утверждения верны.
25. Как правило, протоколы транспортного уровня устанавливаются на конечных узлах, для того чтобы обеспечить требуемое качество передачи данных «из конца в конец». На промежуточных узлах сети, например, на маршрутизаторах, транспортный протокол не является обязательным, но он может быть там установлен для поддержки дополнительных функций, например, удаленного управления промежуточным узлом, так как при этом промежуточный узел является конечным узлом по отношению к управляющему узлу, или для вмешательства промежуточного узла в управление качеством передачи данных между конечными узлами. Так, маршрутизатор может использовать транспортный протокол для замедления передачи данных узлом, создающим перегрузку в сети.
26. Сетевые службы работают на прикладном уровне модели OSI.
27. Не существует строгого закрепления за каждым уровнем стека протоколов названия для единицы передаваемых данных (PDU). Во-первых, количество уровней может различаться (7 в модели OSI и 4 в стеке TCP/IP), во-вторых, названия могут различаться от технологии к технологии. Однако существует некоторое традиционное закрепление названий за тем или иным уровнем, например:
    - «кадр», или «фрейм», — это название протокольной единицы данных канального уровня модели OSI, а также уровня межсетевых интерфейсов стека TCP/IP;
    - «пакет» — название единицы данных сетевого уровня модели OSI, а также сетевого уровня стека TCP/IP (наряду с другим названием «дейтаграмма», используемым для единицы данных протокола IP);

- «сегмент» — название единицы данных транспортного уровня стека TCP/IP (PDU протокола TCP);
- «дейтаграмма» — используется на транспортном (PDU протокола UDP), а также сетевом (PDU протокола IP) уровнях стека TCP/IP, этот термин связан не столько с уровнем протокола, сколько со способом передачи данных;
- «сообщение» — этот термин используется для обозначения PDU прикладного, представительного и сеансового уровней модели OSI;
- «поток» — в стеке TCP/IP служит для обозначения данных, поступающих с прикладного на транспортный уровень.

28. В некоторых случаях да, а в некоторых — нет, так как RFC — это более узкое понятие, принятое в технологии TCP/IP.

Глава 2

1. По оплетке коаксиального кабеля передаются информационные сигналы, и она является экраном, защищающим внутреннюю жилу от внешних электромагнитных полей.
2. Коллизия — это одновременная передача данных по разделяемой среде более чем одной станцией.
3. Логическая единица при манчестерском кодировании кодируется перепадом электрического сигнала от низкого потенциала к высокому.
4. Синхронизация достигается изменением состояния сигналов, предаваемых передатчиком приемнику.
5. Для предотвращения монополизации разделяемой среды одним узлом.
6. Преимущество заключается в повышении реальной скорости передачи пользовательских данных (при той же скорости передачи битов) благодаря тому, что увеличивается доля пользовательских данных по отношению к общей длине кадра, включающей также длину заголовка неизменной длины. Недостаток — увеличение времени ожидания доступа к среде (разделяемой или индивидуальной).
7. Максимальная скорость 14 880 кадров в секунду.
8. Максимальная скорость 9,76 Мбит/с.
9. Благодаря лучшим эксплуатационным свойствам.
10. По значению второго бита старшего байта адреса.
11. По значению первого (младшего) бита старшего байта адреса.
12. Потому что метод доступа, применяемый в сетях этого типа, позволяет в каждый момент времени передавать по кольцу данные только одной станции.

13. За счет обязательной передачи токена другой станции после истечения времени удержания токена.
14. Для передачи данных при отказе первичного кольца.
15. При превышении коэффициента использования порога 30–50%.
16. Разделение единой среды передачи данных на несколько отдельных сред (сегментов). Объединение сегментов в единую сеть.
17. Потому что конечные узлы сети «не видят» мост, то есть его присутствие в сети для конечных узлов незаметно.
18. Большим количеством портов и высокой скоростью продвижения кадров.
19. MAC-адрес источника.
20. Нет.
21. Для удаленного управления портом.
22. Он «затапливает» сеть, передавая кадр на все выходные порты кроме того, на который кадр получен.
23. Порт с наименьшей метрикой пути до корневого моста.
24. Надежность (отказоустойчивость).
25. Наименьшее значение расстояния до корневого моста среди всех портов одного коммутатора. Наименьшее расстояние до корневого моста для двух портов разных коммутаторов, соединенных линией связи.
26. Назначить приоритеты коммутаторам и портам.
27. За счет одновременного выбора альтернативных портов в процессе выбора корневых и назначенных портов.
28. Для повышения помехоустойчивости кабеля.
29. Одномодовый (SMF) кабель.
30. Вдоль оптической оси волокна.
31. Полоса пропускания линии.
32. Затухание линии связи зависит от длины кабеля.
33. Волоконно-оптические кабели.
34. Три.
35. Сократить спектр сигналов и обеспечить самосинхронизацию кода.
36. Процедура автопереговоров используется для согласования скорости передачи данных между двумя непосредственно связанными портами.
37. За счет введения избыточного бита и запрета на использование комбинаций битов с большим количеством нулей.
38. Фильтрация нежелательного трафика.

39. Список доступа коммутатора не может ограничить широковещательный трафик. Часто списки доступа коммутаторов не могут использовать в своих условиях информацию верхних уровней, например, IP-адреса.
40. Нет.
41. Порт, подключенный к линии доступа, может быть связан только с одной виртуальной сетью, в то время как транк — с несколькими.
42. Максимальное количество виртуальных локальных сетей составляет 4096.
43. Метод CSMA/CA предотвращает возникновение коллизий, в то время как метод CSMA/CD нет.
44. До 10 м.
45. Максимальная скорость передачи данных составляет 723 Кбит/с.

Глава 3

1. Утверждения (а), (д) и (е) верны всегда, а (б) и (в) — нет, так как для выполнения своих основных функций, относящихся к физическому и канальному уровням, сетевые адреса не требуются. Однако в некоторых случаях, например, если устройство имеет блок управления по протоколу сетевого уровня SNMP, ему должен быть назначен сетевой адрес. Утверждение (г) не верно, так как сетевые адреса присваиваются каждому интерфейсу, а не целиком маршрутизатору. Отдельный адрес может быть присвоен только блоку управления маршрутизатора.
2.
   - 127.0.0.1 — адрес зарезервирован в качестве адреса обратной связи и не может быть использован для идентификации сетевого интерфейса.
   - 201.13.123.245 — адрес класса C может быть использован для идентификации сетевого интерфейса.
   - 226.4.37.105 — адрес класса D не может быть использован для идентификации сетевого интерфейса.
   - 103.24.254.0 — адрес класса A может быть использован для идентификации сетевого интерфейса.
   - 10.234.17.25 — адрес сети 10.0.0.0 класса A. Эти адреса зарезервированы для использования в автономных сетях, не являющихся частью Интернета.
   - 154.12.255.255 — широковещательный адрес для сети 154.12.0.0 класса B, он не может быть использован для идентификации сетевого интерфейса.

- 13.13.13.13 — адрес класса A может быть использован для идентификации сетевого интерфейса.
- 204.0.3.1 — адрес класса C может быть использован для идентификации сетевого интерфейса.
- 193.256.1.16 — синтаксически неверный адрес, максимальное значение байта — 255.
- 194.87.45.0 — адрес класса C может быть использован для идентификации сетевого интерфейса.
- 195.34.116.255 — широковещательный адрес для сети 195.34.116.0 класса C, он не может быть использован для идентификации сетевого интерфейса.
- 161.23.45.305 — синтаксически неверный адрес, превышено максимальное значение байта.

3. Номер подсети 198.65.12.64. Для нумерации узлов в данной сети может быть использовано 4 бита, то есть 16 значений. Так как двоичные значения 0000 и 1111 зарезервированы, то максимальное число узлов — 14.
4. В общем случае нет, так как не существует глобальной зависимости между сетевыми адресами и доменными именами. Но если администратор при назначении доменных имен для узлов использовал некий алгоритм, учитывающий IP-адреса (например, узлу с IP-адресом 195.50.60.1 давалось имя WS1.star.com, узлу 195.50.60.2 — WS2.star.com, а узлу 195.50.60.3 — WS3.star.com и т. д.), то в таком частном случае по доменному имени можно определить соответствующий IP-адрес.
5. Поскольку ARP-таблица строится для каждого интерфейса, то их число для каждого из перечисленных устройств равно количеству их сетевых интерфейсов.
6. В общем случае это определить невозможно (см. ответ на вопрос 4).
7. Для задания 254 адресов достаточно одного байта. В сети класса B для адресации узлов отведено 2 байта. Таким образом, один из них, а именно старший байт, может быть использован для нумерации подсетей, максимально возможное число которых в таком случае равно 256. Одна из них будет выбрана провайдером для собственных нужд, а 255 предоставлено клиентам. На маршрутизаторе поставщика услуг, соединяющем его сеть с сетями абонентов, должна быть установлена маска 255.255.255.0.
8. Если по каким-то причинам (адрес получателя указан неверно, промежуточный узел потерпел крах, размер пакета слишком большой, буфер промежуточного узла переполнен и т. д.) пакет не дошел до адресата, протокол IP не предпринимает никаких мер по повторной его передаче, оставляя эту работу протоколам вышележащих уровней.
9. Вариант (в).

10. Нет. Для правильной маршрутизации пакетов в сети с использованием масок достаточно того, что маски передаются протоколами маршрутизации RIP-2, OSPF или устанавливаются вручную для каждой записи таблицы маршрутизации.
11. К преимуществам относится сокращение числа записей в таблицах маршрутизации, а значит, ускорение процесса маршрутизации и повышение пропускной способности Интернета. Кроме того, CIDR позволяет более эффективно распределять адреса — число выделяемых адресов не должно жестко соответствовать классам A, B или C. Для повсеместного внедрения CIDR может потребоваться изменение адресов в уже существующих сетях, что является трудоемкой процедурой и требует согласования с провайдером.
12. Да, если длина префикса *n* двоичных разрядов, то количество адресов равно 2 32 – *n*. Чем короче префикс, тем большее количество IP-адресов может входить в этот пул, и наоборот.
13. Вариант (г).
14. Вариант (в).
15. Объем данных составляет 1 795 638 байт.
16. Верным является вариант (б). Ответ (в) некорректный, так как маршрут по умолчанию — это частный (вырожденный) случай таблицы маршрутизации.
17. Вариант (а).
18. Внешний шлюзовой протокол отвечает за выбор маршрута между автономными системами. Внутренние шлюзовые протоколы отвечают за маршрут внутри автономной системы.
19. Вариант (б).
20. OSPF-маршрутизаторы используют метрику, учитывающую пропускную способность составных сетей.
21. ICMP-сообщение всегда направляется узлу-источнику пакета, вызвавшего ошибку. Оно обрабатывается либо ядром операционной системы, либо протоколами транспортного и прикладного уровней, либо приложениями, либо просто игнорируется. Важно, что обработка ICMP-сообщений не входит в обязанности протоколов IP и ICMP.
22. Протокол ICMP служит дополнением протокола IP несколько другого рода. Он не предназначен для исправления возникших при передаче пакета проблем: если пакет потерян, ICMP не может послать его заново. ICMP является средством оповещения отправителя об ошибках, возникших при передаче его пакетов. Таким образом обеспечивается обратная связь между посланным пакетом и отправителем.
23. Варианты (б) и (в).

24. В качестве номера назначенного порта может выступать произвольное число, уникальное в пределах данного глобального IP-адреса, например:

Частный адрес	Порт отправителя	Глобальный адрес	Назначенный порт
10.0.25.1	1035	193.55.13.79	5700
10.0.25.2	1035	193.55.13.79	5701
10.0.25.3	1035	193.55.13.79	5702
10.0.25.2	1047	193.55.13.79	5703
10.0.25.1	1047	193.55.13.79	5704

Глава 4

1. Образовывать гибкую среду для создания физических каналов, которые затем используются телекоммуникационными сетями другого типа, например, компьютерными или телефонными.
2. Нет, и это является недостатком сетей PDH.
3. Защита сетевого соединения SDH работает в сетях любой топологии, а защита на основе разделения кольца — только в кольцевых топологиях. Защита на основе разделения кольца более экономично использует пропускную способность сети.
4. Три: OTU1, OTU2 и OTU3.
5. Появление высокоскоростных и надежных цифровых каналов технологий PDH и SDH.
6. Сети Frame Relay используют технику виртуальных каналов.
7. Комбинации «метка-порт» должны быть *уникальными* в пределах одного коммутатора.
8. Постоянные виртуальные каналы (PVC).
9. CIR определяет гарантированную пропускную способность соединения, то есть сеть гарантирует передачу данных пользователя со скоростью предложенной нагрузки, если эта скорость не превосходит CIR.
10. Параметр Be служит для того, чтобы оператор сети мог дифференцированно обрабатывать кадры, которые не укладываются в профиль CIR.
11. Для улучшения качества обслуживания чувствительного к задержкам голосового трафика.
12. Качество обслуживания в сети определяют следующие параметры:
    - задержка доставки пакета;
    - вариация задержки доставки пакета;
    - доля потерь пакетов в очередях.
13. Частота замеров составляет 8000 Гц.

14. Задержка пакетизации составляет 187 мс.
15. Постоянные (PVC) и коммутируемые (SVC) виртуальные каналы.
16. Масштабируемость маршрутизации, так как достаточно определить маршрут для пути, и все соединения, которые находятся внутри этого пути, будут ему следовать.
17. Трафик с постоянной битовой скоростью.
18. Трафик с переменной битовой скоростью, требующий соблюдения средней скорости передачи данных и синхронизации источника и приемника.
19. Разработчики технологии IP switching преследовали следующие цели:
    - ускорить продвижение IP-пакетов через сеть совместными усилиями протоколов стеков IP и ATM;
    - устранить дублирование протоколов маршрутизации.
20. В соответствии с замыслом разработчиков технология MPLS должна была поддерживать различные протоколы маршрутизации, например, IP и IPX, но на практике она работает только с IP, так как остальные протоколы маршрутизации перестали применяться. Тем не менее в широком смысле MPLS и сегодня является многопротокольной технологией, так как она может переносить данные протоколов канального уровня, например, Ethernet (что не входило в первоначальные планы разработчиков).
21. Протоколы маршрутизации.
22. Число уровней иерархии стандартами MPLS не ограничивается.
23. LER является пограничным устройством LSR.
24. Отображение IP-адресов (или другой адресной информации, например, номеров VLAN) на определенный путь LSP.
25. Это однонаправленный канал.
26. Ethernet, ATM, Frame Relay, PPP.
27. Защита линии, узла и пути.
28. Технология MPLS применяется:
    - для ускорения продвижения пакетов (MPLS IGP);
    - решения задач инжиниринга трафика;
    - предоставления услуг виртуальных частных сетей (MPLS VPN).
29. Стремление расширить область применения знакомой и успешной технологии.
30. В семейство Carrier Ethernet входят следующие технологии:
    - Ethernet на основе MPLS;
    - Ethernet на основе Ethernet (Carrier Ethernet Transport).
31. Использование псевдоканалов внутри туннелей MPLS обеспечивает масштабируемость услуги Carrier Ethernet, так как все требуемые свойства

услуг сетей операторского класса — детерминированность маршрута, гарантии пропускной способности, отказоустойчивость — обеспечиваются туннелями MPLS, так что оператору не требуется поддерживать эти свойства для каждого отдельного пользовательского соединения, представляемого псевдоканалом.

32. Нет.
33. Потому что эта технология основана на инкапсулировании пользовательского кадра Ethernet с MAC-адресами, принадлежащими сетям пользователя, в такой кадр Ethernet провайдера, в котором применяются MAC-адреса коммутаторов сети провайдера.
34. Сегодня применяются:
    - коммутируемый доступ через телефонную сеть;
    - ADSL-доступ через абонентское окончание телефонной сети;
    - доступ через сеть кабельного телевидения;
    - беспроводной доступ.

Глава 5

1. Протокол SMTP ориентирован на передачу (pull protocol), то есть SMTP-клиент является инициатором передачи данных, а протокол POP3 ориентирован на прием данных (push protocol), соответственно, POP3-клиент является инициатором получения данных от сервера.
2. Получая доступ к почтовому серверу по протоколу POP3, вы «перекачиваете» адресованные вам сообщения в память своего компьютера, при этом на сервере не остается никакого следа от считанной вами почты. Если же доступ осуществляется по протоколу IMAP, то в память вашего компьютера передаются только копии сообщений, хранящихся на почтовом сервере.
3. В почтовой службе используются как SMTP-, так и TCP-соединения.
4. Почтовый клиент пользователя обращается к системе DNS, которая хранит данные об IP-адресе почтового сервера, обслуживающего домен пользователя.
5. Теги — это служебные пометки, помещаемые в начале и конце фрагмента текста и определяющие, в каком формате данная часть текста должна быть выведена на экран (курсивным или полужирным начертанием, крупным или мелким шрифтом и т. п.). Гиперссылка — особый тип тега, содержащий информацию о веб-странице или объекте, который может находиться как на том же компьютере, так и на других компьютерах Интернета. Отличие гиперссылки от других тегов состоит в том, что элемент, описываемый ею, не появляется автоматически на экране, вместо этого

на месте тега (гиперссылки) на экран выводится некоторое условное изображение или особым образом выделенный текст — имя гиперссылки. URL — это адрес специального формата, используемый браузером для нахождения веб-страницы. URL содержит указания на тип протокола доступа, DNS-имя сервера, на котором хранится нужная страница, и путь к объекту, обычно представляющий собой составное имя файла относительно главного каталога веб-сервера, предлагаемого по умолчанию.

6. Одной из важнейших функций веб-клиента является поддержание графического пользовательского интерфейса при выполнении поиска и просмотра веб-страниц. HTTP-клиент, работая в связке с HTTP-сервером, обеспечивает передачу данных между клиентом и сервером веб-службы.
7. Веб-сервер сообщает об ошибках на стороне клиента, таких как указание адреса несуществующей страницы или необходимости выполнить процедуру авторизации, а также о неуспешном выполнения операции по вине сервера, например, когда сервер не поддерживает версию HTTP, предложенную клиентом.
8. FTP особенно удобно использовать для доступа к тем файлам, данные которых нет смысла просматривать удаленно, а гораздо эффективней целиком переместить на клиентский компьютер (например, файлы исполняемых модулей приложений).
9. Нет, FTP обладает примитивными средствами защиты.
10. Модуль User Interface.
11. Два порта TCP требуются для поддержки протекающих параллельно управляющего сеанса и сеанса передачи данных.
12. Модель управляемого объекта содержит характеристики объекта, которые нужны для автоматизированного управления этим объектом. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблица маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.
13. Протокол UDP не обеспечивает надежной доставки сообщений, однако он менее загружает управляемые устройства, чем более надежный протокол TCP.
14. Протокол telnet может использоваться для управления коммуникационными устройствами — маршрутизаторами, коммутаторами и хабами.
15. Асимметричная схема шифрования (с открытым ключом) является более масштабируемой.
16. Нет, открытый ключ необходимо защищать от подлогов.
17. Сертификат содержит различную информацию о владельце сертификата, в том числе его открытый ключ.