

Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного бюджетного образовательного
учреждения высшего образования
**«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»**
(КФ МГТУ им. Н.Э. Баумана)

Ю.С. Белов, Е.А. Черепков

ПРОТОКОЛЫ МАРШРУТИЗАЦИИ В IP-СЕТЯХ

Методические указания к лабораторной работе
по дисциплине «Компьютерные сети»

Калуга – 2018


УДК 004.62
ББК 32.972.1
Б435

Методические указания составлены в соответствии с учебным планом КФ МГТУ им. Н.Э. Баумана по направлению подготовки 09.03.04 «Программная инженерия» кафедры «Программного обеспечения ЭВМ, информационных технологий».

Методические указания рассмотрены и одобрены:


- Кафедрой «Программного обеспечения ЭВМ, информационных технологий» (ИУ4-КФ) протокол № 3 от «21» ноября 2018 г.

Зав. кафедрой ИУ4-КФ

 к.т.н., доцент Ю.Е. Гагарин


- Методической комиссией факультета ИУ-КФ протокол № 4 от «26» ноября 2018 г.

Председатель методической
комиссии факультета ИУ-КФ

 к.т.н., доцент М.Ю. Адкин

- Методической комиссией
КФ МГТУ им.Н.Э. Баумана протокол № 3 от «4» декабря 2018 г.

Председатель методической комиссии
КФ МГТУ им.Н.Э. Баумана

 д.э.н., профессор О.Л. Перерва



Рецензент:

к.т.н., доцент кафедры ИУ6-КФ

 А.Б. Лачихина

Авторы

к.ф.-м.н., доцент кафедры ИУ4-КФ
ассистент кафедры ИУ4-КФ

 Ю.С. Белов
 Е.А. Черепков

Аннотация

Методические указания к выполнению лабораторной работы по курсу «Компьютерные сети» содержат общие сведения о различных протоколах, используемых в IP сетях и базовых принципах их функционирования.

Предназначены для студентов 4-го курса бакалавриата КФ МГТУ им. Н.Э. Баумана, обучающихся по направлению подготовки 09.03.04 «Программная инженерия».

© Калужский филиал МГТУ им. Н.Э. Баумана, 2018 г.
© Ю.С. Белов, Е.А. Черепков, 2018 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
ЦЕЛЬ И ЗАДАЧИ РАБОТЫ, ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ЕЕ ВЫПОЛНЕНИЯ.....	5
КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА ИЗУЧЕНИЯ, ИССЛЕДОВАНИЯ	6
ПОСТРОЕНИЕ ТАБЛИЦЫ МАРШРУТИЗАЦИИ	9
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ	30
КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ	31
ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ	32
ОСНОВНАЯ ЛИТЕРАТУРА.....	33
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА	33

ВВЕДЕНИЕ

Настоящие методические указания составлены в соответствии с программой проведения лабораторных работ по курсу «Компьютерные сети» на кафедре «Программное обеспечение ЭВМ, информационные технологии» факультета «Информатика и управление» Калужского филиала МГТУ им. Н.Э. Баумана.

Методические указания, ориентированные на студентов 4-го курса направления подготовки 09.03.04 «Программная инженерия», содержат базовые сведения об основных протоколах в IP сетях.

Методические указания составлены для ознакомления студентов с протоколами, применяемые в IP сетях и особенностях их использования. Для выполнения лабораторной работы студенту необходимы минимальные знания семиуровневой модели OSI.

ЦЕЛЬ И ЗАДАЧИ РАБОТЫ, ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ЕЕ ВЫПОЛНЕНИЯ

Целью выполнения лабораторной работы является формирование практических навыков по настройке маршрутизации.

Основными задачами выполнения лабораторной работы являются:

1. Ознакомиться с реализацией функций маршрутизатора в системах на базе ОС Windows Server.
2. Изучить функционирование протоколов маршрутизации и средств диагностики.

Результатами работы являются:

1. Правильно составленная таблица маршрутизации.
2. Работающая сеть.
3. Подготовленный отчет.

КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА ИЗУЧЕНИЯ, ИССЛЕДОВАНИЯ

Большинство протоколов маршрутизации, применяемых в современных сетях с коммутацией пакетов, ведут свое происхождение от сети Internet и ее предшественницы — сети ARPANET. Для того чтобы понять их назначение и особенности, полезно сначала познакомиться со структурой сети Internet, которая наложила отпечаток на терминологию и типы протоколов.

Internet изначально строилась как сеть, объединяющая большое количество существующих систем. С самого начала в ее структуре выделяли магистральную сеть (core backbone network): а сети, присоединенные к магистрали, рассматривались как автономные системы (autonomous systems, AS). Магистральная сеть и каждая из автономных систем имели свое собственное административное управление и собственные протоколы маршрутизации. Необходимо подчеркнуть, что автономная система и домен имен Internet — это разные понятия, которые служат разным целям. Автономная система объединяет сети, в которых под общим административным руководством одной организации осуществляется маршрутизация, а домен объединяет компьютеры (возможно, принадлежащие разным сетям), в которых под общим административным руководством одной организации осуществляется назначение уникальных символьных имен. Естественно, области действия автономной системы и домена имен могут в частном случае совпадать, если одна организация выполняет обе указанные функции.

Общая схема архитектуры сети Internet показана на рис. 1. Далее маршрутизаторы мы будем называть шлюзами, чтобы оставаться в русле традиционной терминологии Internet.

Шлюзы, которые используются для образования сетей и подсетей внутри автономной системы, называются внутренними шлюзами (interior gateways), а шлюзы, с помощью которых автономные системы присоединяются к магистрали сети, называются внешними шлюзами (exterior gateways). Магистраль сети также является автономной

системой. Все автономные системы имеют уникальный 16-разрядный номер, который выделяется организацией, учредившей новую автономную систему, InterNIC.

Соответственно протоколы маршрутизации внутри автономных систем называются протоколами внутренних шлюзов (interior gateway protocol, IGP), а протоколы, определяющие обмен маршрутной информацией между внешними шлюзами и шлюзами магистральной сети — протоколами внешних шлюзов (exterior gateway protocol, EGP). Внутри магистральной сети также допустим любой собственный внутренний протокол IGP.

Смысл разделения всей сети Internet на автономные системы — в ее многоуровневом модульном представлении, что необходимо для любой крупной системы, способной к расширению в больших масштабах. Изменение протоколов маршрутизации внутри какой-либо автономной системы никак не должно влиять на работу остальных автономных систем. Кроме того, деление Internet на автономные системы должно способствовать агрегированию информации в магистральных и внешних шлюзах. Внутренние шлюзы могут использовать для внутренней маршрутизации достаточно подробные графы связей между собой, чтобы выбрать наиболее рациональный маршрут. Однако если информация такой степени детализации будет храниться во всех маршрутизаторах сети, то топологические базы данных так разрастутся, что потребуют наличия памяти гигантских размеров, а время принятия решений о маршрутизации станет неприемлемо большим.

Поэтому детальная топологическая информация остается внутри автономной системы, а автономную систему как единое целое для остальной части Internet представляют внешние шлюзы, которые сообщают о внутреннем составе автономной системы минимально необходимые сведения — количество IP-сетей, их адреса и внутреннее расстояние до этих сетей от данного внешнего шлюза.

Приведенная на рис. 1 структура Internet с единственной магистралью достаточно долго соответствовала действительности,

поэтому специально для нее был разработан протокол обмена маршрутной информацией между автономными системами, названный EGP. Однако по мере развития сетей поставщиков услуг структура Internet стала гораздо более сложной, с произвольным характером связей между автономными системами. Поэтому протокол EGP уступил место протоколу BGP, который позволяет распознать наличие петель между автономными системами и исключить их из межсистемных маршрутов. Протоколы EGP и BGP используются только во внешних шлюзах автономных систем, которые чаще всего организуются поставщиками услуг Internet. В маршрутизаторах корпоративных сетей работают внутренние протоколы маршрутизации, такие как [RIP](#) и [OSPF](#).

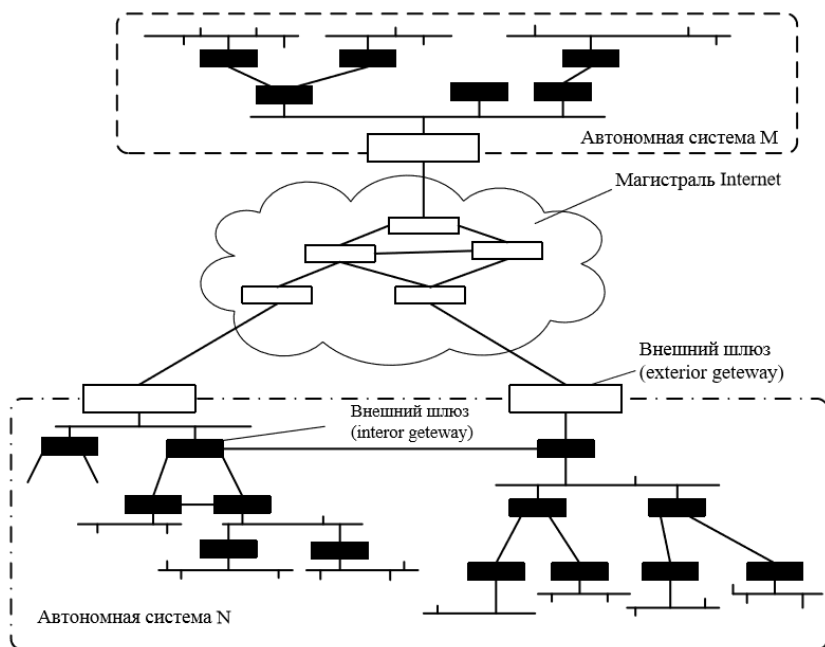


Рис. 1. Магистраль и автономные системы Internet

ПОСТРОЕНИЕ ТАБЛИЦЫ МАРШРУТИЗАЦИИ

Протокол RIP (Routing Information Protocol)

Протокол RIP является внутренним протоколом маршрутизации дистанционно-векторного типа, он представляет собой один из наиболее ранних протоколов обмена маршрутной информацией и до сих пор чрезвычайно распространен в вычислительных сетях ввиду простоты реализации.

Для IP имеются две версии протокола RIP: первая и вторая. Протокол RIPv1 не поддерживает масок, то есть он распространяет между маршрутизаторами только информацию о номерах сетей и расстояниях до них, а информацию о масках этих сетей не распространяет, считая, что все адреса принадлежат к стандартным классам А, В или С. Протокол RIPv2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня. Так как при построении таблиц маршрутизации работа версии 2 принципиально не отличается от версии 1, то в дальнейшем для упрощения записей будет описываться работа первой версии.

В качестве расстояния до сети стандарты протокола RIP допускают различные виды метрик: хопы, метрики, учитывающие пропускную способность, вносимые задержки и надежность сетей, а также любые комбинации этих метрик. Метрика должна обладать свойством аддитивности — метрика составного пути должна быть равна сумме метрик составляющих этого пути. В большинстве реализации RIP используется простейшая метрика — количество хопов, то есть количество промежуточных маршрутизаторов, которые нужно преодолеть пакету до сети назначения.

Рассмотрим процесс построения таблицы маршрутизации с помощью протокола RIP на примере составной сети, изображенной на рис. 2.

Этап 1 — создание минимальных таблиц В этой сети имеется восемь IP-сетей, связанных четырьмя маршрутизаторами с

идентификаторами: M1, M2, M3 и M4. Маршрутизаторы, работающие по протоколу RIP, могут иметь идентификаторы, однако для работы протокола они не являются необходимыми. В RIP-сообщениях эти идентификаторы не передаются.

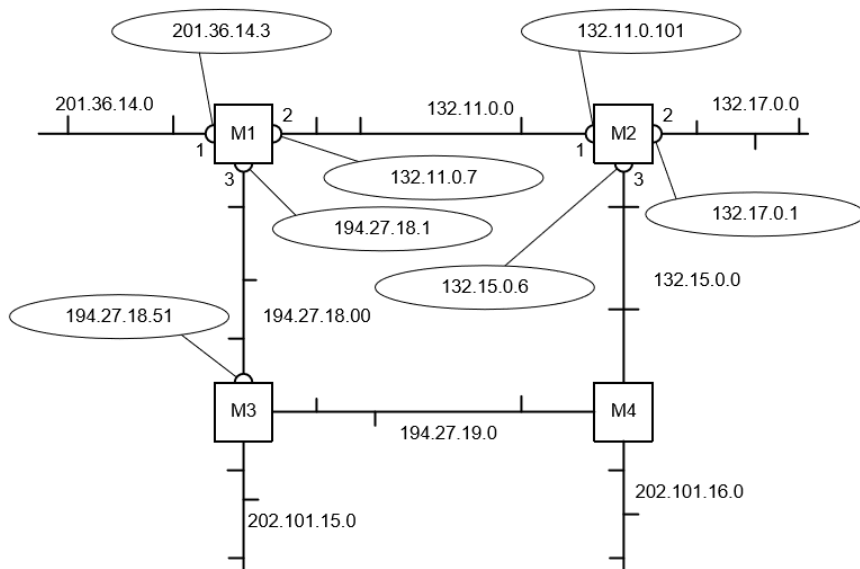


Рис. 2. Сеть, объединенная RIP-маршрутизаторами

В исходном состоянии в каждом маршрутизаторе программным обеспечением стека TCP/IP автоматически создается минимальная таблица маршрутизации, в которой учитываются только непосредственно подсоединенные сети. На рисунке адреса портов маршрутизаторов в отличие от адресов сетей помещены в овалы.

Этап 2 — рассылка минимальных таблиц соседям. После инициализации каждого маршрутизатора он начинает посылать своим соседям сообщения протокола RIP, в которых содержится его минимальная таблица.

RIP-сообщения передаются в пакетах протокола UDP и включают два параметра для каждой сети: ее IP-адрес и расстояние до нее от передающего сообщение маршрутизатора.

Соседями являются те маршрутизаторы, которым данный маршрутизатор непосредственно может передать IP-пакет по какой-либо своей сети, не пользуясь услугами промежуточных маршрутизаторов. Например, для маршрутизатора М1 соседями являются маршрутизаторы М2 и М3, а для маршрутизатора М4 — маршрутизаторы М2 и М3.

Таким образом, маршрутизатор М1 передает маршрутизатору М2 и М3 следующее сообщение:

сеть 201.36.14.0, расстояние 1;
сеть 132.11.0.0, расстояние 1;
сеть 194.27.18.0, расстояние 1.

Этап 3 — получение RIP-сообщений от соседей и обработка полученной информации. После получения аналогичных сообщений от маршрутизаторов М2 и М3 маршрутизатор М1 наращивает каждое полученное поле метрики на единицу и запоминает, через какой порт и от какого маршрутизатора получена новая информация (адрес этого маршрутизатора будет адресом следующего маршрутизатора, если эта запись будет внесена в таблицу маршрутизации). Затем маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации.

Протокол RIP замещает запись о какой-либо сети только в том случае, если новая информация имеет лучшую метрику (расстояние в [хопах](#) меньше), чем имеющаяся. В результате в таблице маршрутизации о каждой сети остается только одна запись; если же имеется несколько равнозначных в отношении расстояния путей к одной и той же сети, то все равно в таблице остается одна запись, которая пришла в маршрутизатор первая по времени. Для этого правила существует исключение — если худшая информация о какой-

либо сети пришла от того же маршрутизатора, на основании сообщения которого была создана данная запись, то худшая информация замещает лучшую.

Аналогичные операции с новой информацией выполняют и остальные маршрутизаторы сети.

Этап 4 — рассылка новой, уже не минимальной, таблицы соседям. Каждый маршрутизатор отправляет новое RIP-сообщение всем своим соседям. В этом сообщении он помещает данные о всех известных ему сетях — как непосредственно подключенных, так и удаленных, о которых маршрутизатор узнал из RIP-сообщений.

Этап 5 - получение RIP-сообщений от соседей и обработка полученной информации. Этап 5 повторяет этап 3 — маршрутизаторы принимают RIP-сообщения, обрабатывают содержащуюся в них информацию и на ее основании корректируют свои таблицы маршрутизации.

На этом этапе маршрутизатор M1 получил от маршрутизатора M3 информацию о сети 132.15.0.0, которую тот в свою очередь на предыдущем цикле работы получил от маршрутизатора M4. Маршрутизатор уже знает о сети 132.15.0.0, причем старая информация имеет лучшую метрику, чем новая, поэтому новая информация об этой сети отбрасывается.

О сети 202.101.16.0 маршрутизатор M1 узнает на этом этапе впервые, причем данные о ней приходят от двух соседей — от M3 и M4. Поскольку метрики в этих сообщениях указаны одинаковые, то в таблицу попадают данные, которые пришли первыми. В нашем примере считается, что маршрутизатор M2 опередил маршрутизатор M3 и первым переслал свое RIP-сообщение маршрутизатору M1.

Если маршрутизаторы периодически повторяют этапы рассылки и обработки RIP-сообщений, то за конечное время в сети установится корректный режим маршрутизации. Под корректным режимом маршрутизации здесь понимается такое состояние таблиц маршрутизации, когда все сети будут достижимы из любой сети с помощью некоторого рационального маршрута. Пакеты будут

доходить до адресатов и не заикливаться в деталях, подобных той, которая образуется на рис. 2, маршрутизаторами М1-М2-М3-М4.

Очевидно, если в сети все маршрутизаторы, их интерфейсы и соединяющие их каналы связи постоянно работоспособны, то объявления по протоколу RIP можно делать достаточно редко, например, один раз в день. Однако в сетях постоянно происходят изменения — изменяется как работоспособность маршрутизаторов и каналов, так и сами маршрутизаторы, и каналы могут добавляться в существующую сеть или же выводиться из ее состава.

Для адаптации к изменениям в сети протокол RIP использует [ряд механизмов](#).

Адаптация RIP-маршрутизаторов к изменениям состояния сети

К новым маршрутам RIP-маршрутизаторы приспосабливаются просто — они передают новую информацию в очередном сообщении своим соседям и постепенно эта информация становится известна всем маршрутизаторам сети. А вот к отрицательным изменениям, связанным с потерей какого-либо маршрута, RIP-маршрутизаторы приспосабливаются сложнее. Это связано с тем, что в формате сообщений протокола RIP нет поля, которое бы указывало на то, что путь к данной сети больше не существует.

Вместо этого используются два механизма уведомления о том, что некоторый маршрут более недействителен:

- истечение времени жизни маршрута;
- указание специального расстояния (бесконечности) до сети, ставшей недоступной.

Для отработки первого механизма каждая запись таблицы маршрутизации (как и записи таблицы продвижения моста/коммутатора), полученная по протоколу RIP, имеет время жизни (TTL). При поступлении очередного RIP-сообщения, которое подтверждает справедливость данной записи, таймер TTL устанавливается в исходное состояние, а затем из него каждую секунду вычитается единица. Если за время тайм-аута не придет новое

маршрутное сообщение об этом маршруте, то он помечается как недействительный.

Время тайм-аута связано с периодом рассылки векторов по сети. В RIP IP период рассылки выбран равным 30 секундам, а в качестве тайм-аута выбрано шестикратное значение периода рассылки, то есть 180 секунд. Выбор достаточно малого времени периода рассылки объясняется несколькими причинами, которые станут понятны из дальнейшего изложения. Шестикратный запас времени нужен для уверенности в том, что сеть действительно стала недоступна, а не просто произошли потери RIP сообщений (а это возможно, так как RIP использует транспортный протокол UDP, который не обеспечивает надежной доставки сообщений).

Если какой-либо маршрутизатор отказывает и перестает слать своим соседям сообщения о сетях, которые можно достичь через него, то через 180 секунд все записи, которые породил этот маршрутизатор, станут недействительными у его ближайших соседей. После этого процесс повторится уже для соседей ближайших соседей — они вычеркнут подобные записи уже через 360 секунд, так как первые 180 секунд ближайшие соседи еще передавали сообщения об этих записях.

Как видно из объяснения, сведения о недоступных через отказавший маршрутизатор сетях распространяются по сети не очень быстро, время распространения кратно времени жизни записи, а коэффициент кратности равен количеству [хопов](#) между самыми дальними маршрутизаторами сети. В этом заключается одна из причин выбора в качестве периода рассылки небольшой величины в 30 секунд.

Если отказывает не маршрутизатор, а интерфейс или сеть, связывающие его с каким-либо соседом, то ситуация сводится к только что описанной — снова начинает работать механизм тайм-аута и ставшие недействительными маршруты постепенно будут вычеркнуты из таблиц всех маршрутизаторов сети.

Тайм-аут работает в тех случаях, когда маршрутизатор не может послать соседям сообщение об отказавшем маршруте, так как-либо он

сам неработоспособен, либо неработоспособна линия связи, по которой можно было бы передать сообщение.

Когда же сообщение послать можно, RIP-маршрутизаторы не используют специальный признак в сообщении, а указывают бесконечное расстояние до сети, причем в протоколе RIP оно выбрано равным 16 хопам (при другой метрике необходимо указать маршрутизатору ее значение, считающееся бесконечностью). Получив сообщение, в котором некоторая сеть сопровождается расстоянием 16 (или 15, что приводит к тому же результату, так как маршрутизатор наращивает полученное значение на 1), маршрутизатор должен проверить, исходит ли эта «плохая» информация о сети от того же маршрутизатора, сообщение которого послужило в свое время основанием для записи о данной сети в таблице маршрутизации. Если это тот же маршрутизатор, то информация считается достоверной и маршрут помечается как недоступный.

Такое небольшое значение «бесконечного» расстояния вызвано тем, что в некоторых случаях отказы связей в сети вызывают длительные периоды некорректной работы RIP-маршрутизаторов, выражающейся в заиклиивании пакетов в петлях сети. И чем меньше расстояние, используемое в качестве «бесконечного», тем такие периоды становятся короче.

Рассмотрим случай заиклиивания пакетов на примере сети, изображенной на рис. 2.

Пусть маршрутизатор M1 обнаружил, что его связь с непосредственно подключенной сетью 201.36.14.0 потеряна (например, по причине отказа интерфейса 201.36.14.3). M1 отметил в своей таблице маршрутизации, что сеть 201.36.14.0 недоступна. В худшем случае он обнаружил это сразу же после отправки очередных RIP-сообщений, так что до начала нового цикла его объявлений, в котором он должен сообщить соседям, что расстояние до сети 201.36.14.0 стало равным 16, остается почти 30 секунд.

Каждый маршрутизатор работает на основании своего внутреннего таймера, не синхронизируя работу по рассылке объявлений с другими

маршрутизаторами. Поэтому весьма вероятно, маршрутизатор M2 опередил маршрутизатор M1 и передал ему свое сообщение раньше, чем M1 успел передать новость о недостижимости сети 201.36.14.0. А в этом сообщении имеются данные, порожденные следующей записью в таблице маршрутизации M2.

Эта запись была получена от маршрутизатора M1 и корректна до отказа интерфейса 201.36.14.3, а теперь она устарела, но маршрутизатор M2 об этом не узнал.

Теперь маршрутизатор M1 получил новую информацию о сети 201.36.14.0 — эта сеть достижима через маршрутизатор M2 с метрикой 2. Раньше M1 также получал эту информацию от M2. Но игнорировал ее, так как его собственная метрика для 201.36.14.0 была лучше. Теперь M1 должен принять данные о сети 201.36.14.0, полученные от M2, и заменить запись в таблице маршрутизации о недостижимости этой сети.

В результате в сети образовалась маршрутная петля: пакеты, направляемые узлам сети 201.36.14.0, будут передаваться маршрутизатором M2 маршрутизатору M1, а маршрутизатор M1 будет возвращать их маршрутизатору M2. IP-пакеты будут циркулировать по этой петле до тех пор, пока не истечет время жизни каждого пакета.

Маршрутная петля будет существовать в сети достаточно долго. Рассмотрим периоды времени, кратные времени жизни записей в таблицах маршрутизаторов.

- Время 0-180 с. После отказа интерфейса в маршрутизаторах M1 и M2 будут сохраняться некорректные записи, приведенные выше. Маршрутизатор M2 по-прежнему снабжает маршрутизатор M1 своей записью о сети 201.36.14.0 с метрикой 2, так как ее время жизни не истекло. Пакеты зацикливаются.
- Время 180-360 с. В начале этого периода у маршрутизатора M2 истекает время жизни записи о сети 201.36.14.0 с метрикой 2, так как маршрутизатор M1 в предыдущий период посылал ему сообщения о сети 201.36.14.0 с худшей метрикой, чем у M2, и они не могли подтверждать эту запись. Теперь маршрутизатор

M2 принимает от маршрутизатора M1 запись о сети 201.36.14.0 с метрикой 3 и трансформирует ее в запись с метрикой 4. Маршрутизатор M1 не получает новых сообщений от маршрутизатора M2 о сети 201.36.14.0 с метрикой 2, поэтому время жизни его записи начинает уменьшаться. Пакеты продолжают заикливаться.

- Время 360-540 с. Теперь у маршрутизатора M1 истекает время жизни записи о сети 201.36.14.0 с метрикой 3. Маршрутизаторы M1 и M2 опять меняются ролями — M2 снабжает M1 устаревшей информацией о пути к сети 201.36.14.0, уже с метрикой 4, которую M1 преобразует в метрику 5. Пакеты продолжают заикливаться.

Если бы в протоколе RIP не было выбрано расстояние 16 в качестве недостижимого, то описанный процесс длился бы до бесконечности (вернее, пока не была бы исчерпана разрядная сетка поля расстояния и не было бы зафиксировано переполнения при очередном наращивании расстояния).

В результате маршрутизатор M2 на очередном этапе описанного процесса получает от маршрутизатора M1 метрику 15, которая после наращивания, превращаясь в метрику 16, фиксирует недостижимость сети. Период нестабильной работы сети длился 36 минут!

Ограничение в 15 хопов сужает область применения протокола RIP до сетей, в которых число промежуточных маршрутизаторов не может быть больше 15. Для более масштабных сетей нужно применять другие протоколы маршрутизации, например, OSPF, или разбивать сеть на автономные области.

Приведенный пример хорошо иллюстрирует главную причину нестабильной работы маршрутизаторов, работающих по протоколу RIP. Эта причина коренится в самом принципе работы дистанционно-векторных протоколов — использовании информации, полученной из вторых рук. Действительно, маршрутизатор M2 передал маршрутизатору M1 информацию о достижимости сети 201.36.14.0, за достоверность которой он сам не отвечает. Искоренить эту причину

полностью нельзя, ведь сам способ построения таблиц маршрутизации связан с передачей чужой информации без указания источника ее происхождения.

Не следует думать, что при любых отказах интерфейсов и маршрутизаторов в сетях возникают маршрутные петли. Если бы маршрутизатор M1 успел передать сообщение о недостижимости сети 201.36.14.0 раньше ложной информации маршрутизатора M2, то маршрутная петля не образовалась бы. Так что маршрутные петли даже без дополнительных методов борьбы с ними, описанными в следующем разделе, возникают в среднем не более чем в половине потенциально возможных случаев.

Методы борьбы с ложными маршрутами в протоколе RIP.

Несмотря на то, что протокол RIP не в состоянии полностью исключить переходные состояния в сети, когда некоторые маршрутизаторы пользуются устаревшей информацией об уже несуществующих маршрутах, имеется несколько методов, которые во многих случаях решают подобные проблемы.

Ситуация с петлей, образующейся между соседними маршрутизаторами, описанная в предыдущем разделе, надежно решается с помощью метода, получившем название расщепления горизонта (split horizon). Метод заключается в том, что маршрутная информация о некоторой сети, хранящаяся в таблице маршрутизации, никогда не передается тому маршрутизатору, от которого она получена (это следующий маршрутизатор в данном маршруте). Если маршрутизатор M2 в рассмотренном выше примере поддерживает технику расщепления горизонта, то он не передаст маршрутизатору M1 устаревшую информацию о сети 201.36.14.0, так как получил ее именно от маршрутизатора M1.

Практически все сегодняшние маршрутизаторы, работающие по протоколу RIP, используют технику расщепления горизонта.

Однако расщепление горизонта не помогает в тех случаях, когда петли образуются не двумя, а несколькими маршрутизаторами.

Рассмотрим более детально ситуацию, которая возникнет в сети, приведенной на рис. 2, в случае потери связи маршрутизатора 2 с сетью А. Пусть все маршрутизаторы этой сети поддерживают технику расщепления горизонта. Маршрутизаторы М2 и М3 не будут возвращать маршрутизатору в этой ситуации данные о сети 201.36.14.0 с метрикой 2, так как они получили эту информацию от маршрутизатора М1. Однако они будут передавать маршрутизатору информацию о достижимости сети 201.36.14.0 с метрикой 4 через себя, так как получили эту информацию по сложному маршруту, а не от маршрутизатора М1 непосредственно. Например, маршрутизатор М2 получил эту информацию по цепочке М4-М3-М1. Поэтому маршрутизатор М1 снова может быть обманут, пока каждый из маршрутизаторов в цепочке М3-М4-М2 не вычеркнет запись о достижимости сети 1 (а это произойдет через период 3×180 секунд).

Для предотвращения заикливания пакетов по составным петлям при отказах связей применяются два других приема, называемые триггерными обновлениями (*triggered updates*) и замораживанием изменений (*hold down*).

Способ триггерных обновлений состоит в том, что маршрутизатор, получив данные об изменении метрики до какой-либо сети, не ждет истечения периода передачи таблицы маршрутизации, а передает данные об изменившемся маршруте немедленно. Этот прием может во многих случаях предотвратить передачу устаревших сведений об отказавшем маршруте, но он перегружает сеть служебными сообщениями, поэтому триггерные объявления также делаются с некоторой задержкой. Поэтому возможна ситуация, когда регулярное обновление в каком-либо маршрутизаторе чуть опередит по времени приход триггерного обновления от предыдущего в цепочке маршрутизатора и данный маршрутизатор успеет передать по сети устаревшую информацию о несуществующем маршруте.

Второй прием позволяет исключить подобные ситуации. Он связан с введением тайм-аута на принятие новых данных о сети, которая только что стала недоступной. Этот тайм-аут предотвращает принятие

устаревших сведений о некотором маршруте от тех маршрутизаторов, которые находятся на некотором расстоянии от отказавшей связи и передают устаревшие сведения о ее работоспособности. Предполагается, что в течение тайм-аута «замораживания изменений» эти маршрутизаторы вычеркнут данный маршрут из своих таблиц, так как не получают о нем новых записей и не будут распространять устаревшие сведения по сети.

Протокол «состояния связей» OSPF

Протокол OSPF (Open Shortest Path First, открытый протокол «кратчайший путь первым») является реализацией алгоритма состояния связей (он принят в 1991 году) и обладает многими особенностями, ориентированными на применение в больших гетерогенных сетях.

В OSPF процесс построения таблицы маршрутизации разбивается на два крупных этапа. На первом этапе каждый маршрутизатор строит граф связей сети, в котором вершинами графа являются маршрутизаторы и IP-сети, а ребрами — интерфейсы маршрутизаторов. Все маршрутизаторы для этого обмениваются со своими соседями той информацией о графе сети, которой они располагают к данному моменту времени. Этот процесс похож на процесс распространения векторов расстояний до сетей в протоколе RIP, однако сама информация качественно другая — это информация о топологии сети. Эти сообщения называются router links advertisement — объявление о связях маршрутизатора. Кроме того, при передаче топологической информации маршрутизаторы ее не модифицируют, как это делают RIP маршрутизаторы, а передают в неизменном виде. В результате распространения топологической информации все маршрутизаторы сети располагают идентичными сведениями о графе сети, которые хранятся в топологической базе данных маршрутизатора.

Второй этап состоит в нахождении оптимальных маршрутов с помощью полученного графа. Каждый маршрутизатор считает себя центром сети и ищет оптимальный маршрут до каждой известной ему

сети. В каждом найденном таким образом маршруте запоминается только один шаг — до следующего маршрутизатора, в соответствии с принципом одношаговой маршрутизации. Данные об этом шаге и попадают в таблицу маршрутизации.

После первоначального построения таблицы маршрутизации необходимо отслеживать изменения состояния сети и вносить коррективы в таблицу маршрутизации. Для контроля состояния связей и соседних маршрутизаторов OSPF-маршрутизаторы передают специальные короткие сообщения HELLO. Если состояние сети не меняется, то OSPF маршрутизаторы корректировкой своих таблиц маршрутизации не занимаются и не посылают соседям объявления о связях. Если же состояние связи изменилось, то ближайшим соседям посылается новое объявление, касающееся только данной связи, что, конечно, экономит пропускную способность сети. Получив новое объявление об изменении состояния связи, маршрутизатор перестраивает граф сети, заново ищет оптимальные маршруты (не обязательно все, а только те, на которых отразилось данное изменение) и корректирует свою таблицу маршрутизации. Одновременно маршрутизатор ретранслирует объявление каждому из своих ближайших соседей (кроме того, от которого он получил это объявление).

При появлении новой связи или нового соседа маршрутизатор узнает об этом из новых сообщений HELLO. В сообщениях HELLO указывается достаточно детальная информация о том маршрутизаторе, который послал это сообщение, а также о его ближайших соседях, чтобы данный маршрутизатор можно было однозначно идентифицировать. Сообщения HELLO отправляются через каждые 10 секунд, чтобы повысить скорость адаптации маршрутизаторов к изменениям, происходящим в сети. Небольшой объем этих сообщений делает возможной такое частое тестирование состояния соседей и связей с ними.

Так как маршрутизаторы являются одними из вершин графа, то они обязательно должны иметь идентификаторы.

Протокол OSPF обычно использует метрику, учитывающую пропускную способность сетей. Кроме того, возможно использование двух других метрик, учитывающих требования к качеству обслуживания в IP пакете, — задержки передачи пакетов и надежности передачи пакетов сетью. Для каждой из метрик протокол OSPF строит отдельную таблицу маршрутизации. Выбор нужной таблицы происходит в зависимости от требований к качеству обслуживания пришедшего пакета (см. рис. 3).

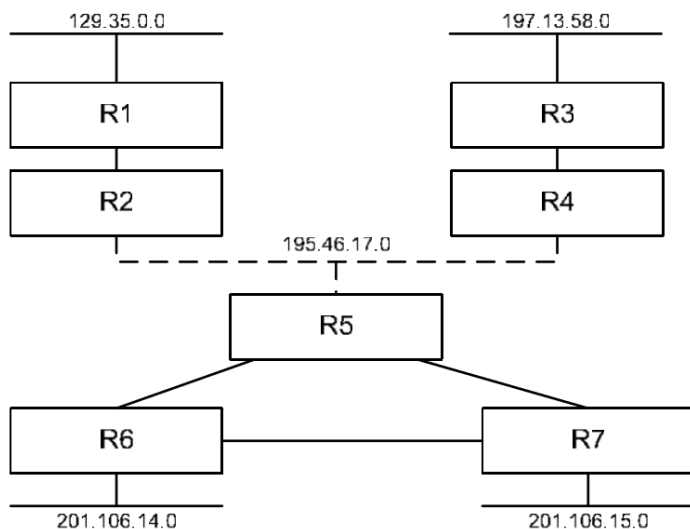


Рис. 3. Построение таблицы маршрутизации по протоколу OSPF

Маршрутизаторы соединены как с локальными сетями, так и непосредственно между собой глобальными каналами типа «точка-точка». Данной сети соответствует граф, приведенный на рис. 4.

Протокол OSPF в своих объявлениях распространяет информацию о связях двух типов: маршрутизатор - маршрутизатор и маршрутизатор - сеть. Примером связи первого типа служит связь «R3 - R4», а второго — связь «R4 - 195.46.17.0». Если каналам «точка-точка» дать IP-адреса, то они станут дополнительными вершинами графа, как и локальные

сети. Вместе с IP-адресом сети передается также информация о маске сети.

После инициализации OSPF-маршрутизаторы знают только о связях с непосредственно подключенными сетями, как и RIP-маршрутизаторы. Они начинают распространять эту информацию своим соседям. Одновременно они посылают сообщения HELLO по всем своим интерфейсам, так что почти сразу же маршрутизатор узнает идентификаторы своих ближайших соседей, что пополняет его топологическую базу новой информацией, которую он узнал непосредственно. Далее топологическая информация начинает распространяться по сети от соседа к соседу и через некоторое время достигает самых удаленных маршрутизаторов.

Каждая связь характеризуется метрикой. Протокол OSPF поддерживает стандартные для многих протоколов (например, для протокола Spanning Tree) значения расстояний для метрики, отражающей производительность сетей: Ethernet — 10 единиц, Fast Ethernet — 1 единица, канал T1 — 65 единиц, канал 56 Кбит/с — 1785 единиц и т. д.

При выборе оптимального пути на графе с каждым ребром графа связана метрика, которая добавляется к пути, если данное ребро в него входит. Пусть на приведенном примере маршрутизатор R5 связан с R6 и R7 каналами T1, а R6 и R7 связаны между собой каналом 56 Кбит/с. Тогда R7 определит оптимальный маршрут до сети 201.106.14.0 как составной, проходящий сначала через маршрутизатор R5, а затем через R6, поскольку у этого маршрута метрика будет равна $65 + 65 = 130$ единиц. Непосредственный маршрут через R6 не будет оптимальным, так как его метрика равна 1785. При использовании хопов был бы выбран маршрут через R6, что не было бы оптимальным.

Протокол OSPF разрешает хранить в таблице маршрутизации несколько маршрутов к одной сети, если они обладают равными метриками. Если такие записи образуются в таблице маршрутизации, то маршрутизатор реализует режим баланса загрузки маршрутов (load balancing), отправляя пакеты попеременно по каждому из маршрутов.

При инициализации маршрутизаторов, а также для более надежной синхронизации топологических баз маршрутизаторы периодически обмениваются всеми записями базы, но этот период существенно больше, чем у RIP-маршрутизаторов.

Так как информация о некоторой связи изначально генерируется только тем маршрутизатором, который выяснил фактическое состояние этой связи путем тестирования с помощью сообщений HELLO, а остальные маршрутизаторы только ретранслируют эту информацию без преобразования, то недостоверная информация о достижимости сетей, которая может появляться в RIP-маршрутизаторах, в OSPF-маршрутизаторах появиться не может, а устаревшая информация быстро заменяется новой, так как при изменении состояния связи новое сообщение генерируется сразу же.

Периоды нестабильной работы в OSPF-сетях могут возникать. Например, при отказе связи, когда информация об этом не дошла до какого-либо маршрутизатора и он отправляет пакеты сети назначения, считая эту связь работоспособной. Однако эти периоды продолжаются недолго, причем пакеты не закливаются в маршрутных петлях, а просто отбрасываются при невозможности их передать через неработоспособную связь.

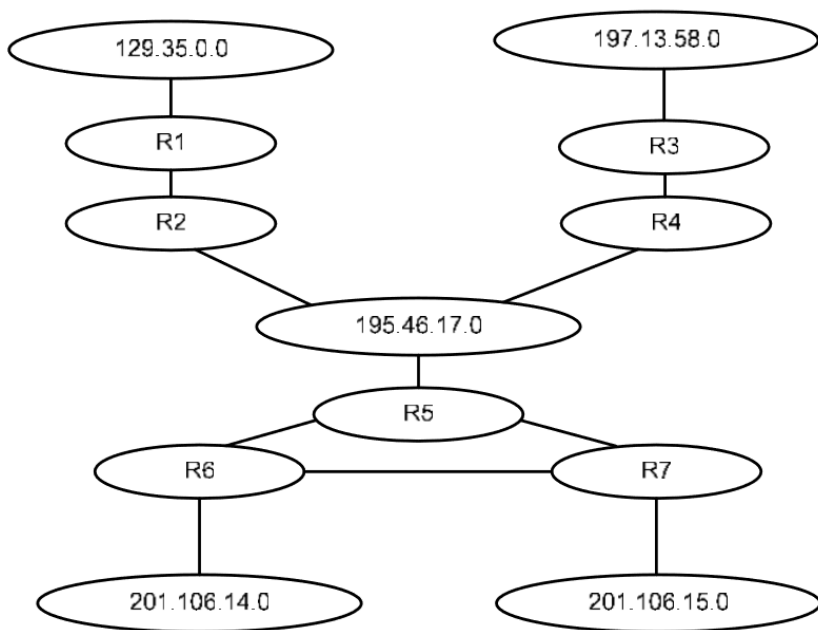


Рис. 4. Граф сети, построенный протоколом OSPF

К недостаткам протокола OSPF следует отнести его вычислительную сложность, которая быстро растет с увеличением размерности сети, то есть количества сетей, маршрутизаторов и связей между ними. Для преодоления этого недостатка в протоколе OSPF вводится понятие области сети (area) (не нужно путать с автономной системой Internet). Маршрутизаторы, принадлежащие некоторой области, строят граф связей только для этой области, что сокращает размерность сети. Между областями информация о связях не передается, а пограничные для областей маршрутизаторы обмениваются только информацией об адресах сетей, имеющих в каждой из областей, и расстоянием от пограничного маршрутизатора до каждой сети. При передаче пакетов между областями выбирается один из пограничных маршрутизаторов области, а именно тот, у которого расстояние до нужной сети меньше. Этот стиль напоминает стиль работы протокола RIP, но нестабильность здесь устраняется тем,

что петлевидные связи между областями запрещены. При передаче адресов в другую область OSPF маршрутизаторы агрегируют несколько адресов в один, если обнаруживают у них общий префикс.

OSPF-маршрутизаторы могут принимать адресную информацию от других протоколов маршрутизации, например, от протокола RIP, что полезно для работы в гетерогенных сетях. Такая адресная информация обрабатывается так же, как и внешняя информация между разными областями.

Команда route и таблица маршрутизации в Windows Server

Создание статических маршрутов выполняется с помощью специальных программ из комплекта TCP/IP. В Windows 2000 утилита для создания (или удаления) элементов таблицы маршрутизации называется Route.exe и запускается из командной строки со следующими параметрами и переключателями:

ROUTE [-f] [-p] [command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]]

-f — удаляет все элементы в таблице маршрутизации. При использовании этого переключателя с командой ADD сначала удаляются старые элементы, а затем добавляется новый.

-p — при использовании с командой ADD создает в таблице постоянный элемент маршрута, который сохраняется даже после перезапуска системы. При использовании с командой PRINT отображает на экране только постоянные маршруты.

[command](#) — ключевое слово, которое конкретизирует выполняемое действие.

destination — адрес сети или хоста в строке таблицы, на которую направлено действие команды.

MASK netmask — маска подсети, которую следует применять к адресу, заданному в переменной destination.

gateway — адрес маршрутизатора, на который должны отправляться пакеты, адресованные хосту или сети, заданным в переменной destination.

METRIC metric — значение метрики, характеризующее относительную эффективность данного маршрута.

IF interface — адрес платы сетевого адаптера, которой система должна пользоваться для передачи данных маршрутизатору, адрес которого задан в переменной gateway.

Переменная command принимает одно из четырех значений:

- PRINT — отобразить содержимое таблицы маршрутизации (при использовании с параметром p отображаются только неудаляемые маршруты);
- ADD — создать новый маршрут;
- DELETE — удалить существующий маршрут;
- CHANGE — изменить параметры существующего маршрута.

Команда **ROUTE PRINT** отображает текущее содержимое таблицы маршрутизации. Для удаления маршрута воспользуйтесь командой **ROUTE DELETE**, указав с помощью переменной destination, какой маршрут нужно удалить. Чтобы создать новый маршрут, введите команду **ROUTE ADD** с параметрами маршрута, заданными в соответствующих переменных. Подобным образом работает и команда **ROUTE CHANGE**, за исключением того, что указанные в ней параметры присваиваются существующему маршруту, заданному с помощью переменной destination. Переменная destination содержит адрес сети или хоста, информацию о маршруте, к которым вы вводите. Другими переменными задаются маска подсети, адрес шлюза, адрес интерфейса и эффективность маршрута.

Таблица 1. Структура таблицы маршрутизации в Windows Server

Network Address	Netmask	Gateway Address	Interface	Metri c
0.0.0.0	0.0.0.0	192.168.2.100	192.168.2.5	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.2.0	255.255.255.0	192.168.2.5	192.168.2.5	1
192.168.2.5	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.2.255	255.255.255.255	192.168.2.5	192.168.2.5	1
224.0.0.0	224.0.0.0	192.168.2.5	192.168.2.5	1
255.255.255.255	255.255.255.255	192.168.2.5	0.0.0.0	1

Записи в таблице расположены горизонтально. Назначение информации в каждом из столбцов приведено ниже.

- Сетевой адрес (Network Address). Содержит адрес сети, для которой приведена информация маршрутизации. В общем случае для большинства записей в этом поле размещается адрес сети, но оно также может содержать информацию маршрутизации для определенного узла. Последняя называется маршрутом узла (host route).
- Маска подсети (Netmask). Задаёт так называемую маску подсети, используемую для определения, какие из битов в сетевом адресе являются идентификатором сети.

- Адрес шлюза (Gateway Address). Указывает IP-адрес шлюза (маршрутизатора), который система должна использовать для отправки пакетов по заданному сетевому адресу. Если это запись для сети, к которой система подключена непосредственно, тогда поле содержит адрес сетевого интерфейса системы.
- Интерфейс (Interface). В этом столбце сохраняется IP-адрес сетевого интерфейса системы, служащий для отправки трафика по адресу шлюза.
- Метрика маршрута (Metric). Указывает расстояние между системой и сетью назначения, обычно выражается в количестве транзитов, необходимых для того, чтобы трафик достиг целевого адреса.

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Составить таблицу маршрутизации и проверить работоспособность сети. Для этого нужно:

1. Войдя в систему с правами администратора на компьютере 224u7 посмотреть таблицу маршрутизации. Убедиться в недоступности сетей аудиторий 158, 161, 219, 226, 231.
2. Изучив схему имеющейся сети добавить в таблицу маршрутизации компьютера 224u7 5 записей, позволяющих работать с компьютерами аудиторий, указанных в пункте 1, в течении неограниченного по времени периода. Проверить работоспособность при помощи утилит ping и tracert.
3. Используя подход, применяемый в технологии CIDR, проанализировать добавленные в таблицу маршрутизации 5 записей и заменить их одной. Проверить работоспособность.
4. С компьютера 224u7 выполнить трассировку маршрута до сервера yandex.ru, изобразить упрощенную схему сети прохождения пакетов до данного ресурса (без использования масок).
5. С компьютера 224u7 выполнить трассировку маршрута до телефона или планшета одного из учащихся, находящегося в этой аудитории (предварительно выяснив IP адрес устройства). Сделать выводы. Предложить пути решения выявленной проблемы.
6. Ответить на контрольные вопросы и оформить отчет.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

1. Дайте определение понятиям «магистральная сеть» и «автономные системы».
2. Раскройте различие внутренних и внешних шлюзов.
3. Раскройте различие протоколов внутренних и внешних шлюзов.
4. Раскройте различие протоколов EGP и BGP.
5. Приведите примеры внутренних протоколов IGP.
6. Опишите назначение протокола RIP.
7. Назовите метрики, предусмотренные стандартом протокола RIP для определения расстояния до сети.
8. Приведите этапы построения таблиц маршрутизации с помощью протокола RIP.
9. Назовите механизмы уведомления о недействительных маршрутах в протоколе RIP.
10. Перечислите методы борьбы с ложными маршрутами в протоколе RIP.
11. Раскройте сущность метода расщепления горизонта.
12. Раскройте сущность метода триггерных обновлений.
13. Раскройте сущность метода замораживания изменений.
14. Раскройте назначение протокола OSPF.
15. Приведите этапы построения таблиц маршрутизации с помощью протокола OSPF.
16. Перечислите недостатки протокола OSPF.

ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

На выполнение лабораторной работы отводится 2 занятия (4 академических часа: 3 часа на выполнение и сдачу лабораторной работы и 1 час на подготовку отчета).

Отчет на защиту предоставляется в печатном виде.

Структура отчета (на отдельном листе(-ах)): титульный лист, формулировка задания, ответы на контрольные вопросы, описание процесса выполнения лабораторной работы, выводы.

ОСНОВНАЯ ЛИТЕРАТУРА

1. Смелянский, Р.Л. Компьютерные сети. В 2 т. Т. 1. Системы передачи данных: учебник для вузов /Р.Л. Смелянский М.: Изд. центр «Академия». 2011. -304 с.
2. Смелянский, Р.Л. Компьютерные сети. В 2 т. Т. 2. Сети ЭВМ: учебник для вузов /Р.Л. Смелянский М.: Изд. центр «Академия». 2011 -240 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

3. Технологии коммутации и маршрутизации в локальных компьютерных сетях: учеб пособие для вузов / А.В. Пролетарский, Е.В. Смирнова [и др.]. под ред. А.В. Пролетарского.- М.: Изд-во МГТУ им. Н.Э. Баумана 2013. -389 с.ил.
4. Дейтел, Х.М. Как программировать на С++/ Х.М. Дейтел, Дж. Дейтел: пер. с англ. – М.: Бином-Пресс, 2011. -800 с.:тл

Электронные ресурсы:

5. Научная электронная библиотека <http://eLIBRARY.RU>
6. Электронно-библиотечная система <http://e.lanbook.com>
7. Компьютерные сети и технологии <http://www.xnets.ru>