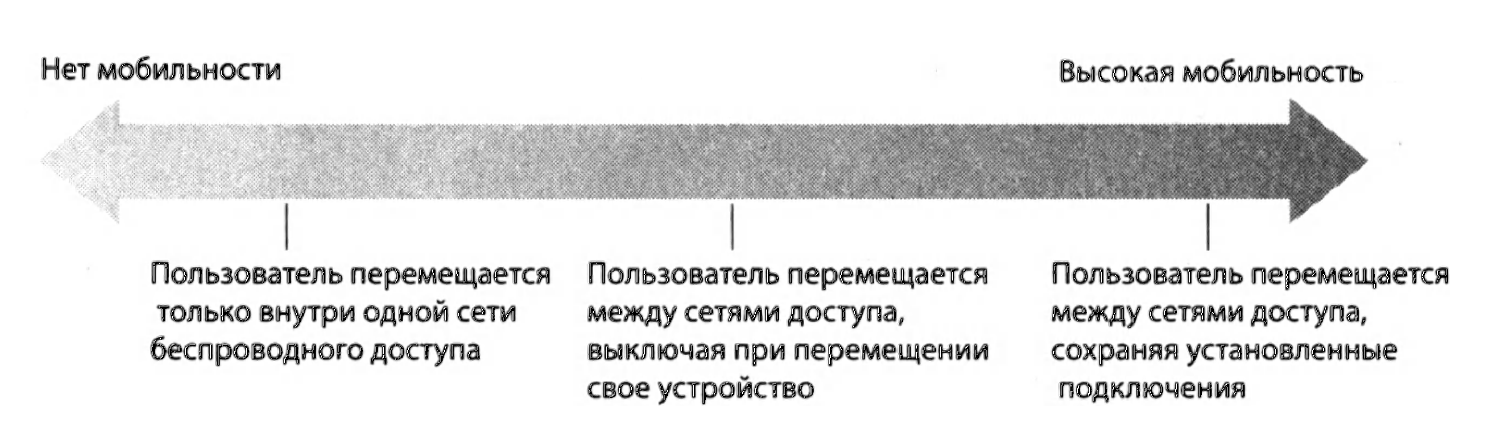
**Управление мобильностью: Принципы**

Теперь, когда мы уже обсудили *беспроводную* природу каналов свя­зи беспроводных сетей, настало время переключить наше внимание на *мобильность,* открываемую беспроводными каналами связи. В самом широком смысле, мобильный узел — это узел, меняющий точку под­ключения к сети с течением времени. По причине того, что сам термин «мобильность» приобрел большое количество значений, как в мире компьютерных, так и сетевых технологий, сначала нам следует обсудить более подробно несколько категорий мобильности.

• *С точки зрения оборудования сетевого уровня насколько мобилен тот или иной пользователь?* Физически мобильный пользователь, в зависимости от того, как он или она перемещается между точками подключения, представляет собой целый набор различных задач для сетевого уровня. На одном конце спектра на рис. 6.21 пользователь может перемещаться по зданию с ноутбуком, оборудованным интер­фейсом для подключения к беспроводной сети. Как мы уже видели ранее, с точки зрения сетевого уровня этот пользователь *не* является мобильным. Более того, если пользователь остается ассо­циированным с одной и той же точкой доступа вне зависимости от местоположения, такой пользователь не является мобильным даже на канальном уровне.

Представим, что на противоположном конце спектра находится пользователь, несущийся на скорости 150 километров час по автома­гистрали на своем спортивном BMW, при этом он проезжает мимо большого количества беспроводных точек доступа и хочет сохранить установленное TCP подключение к удаленному приложению на протяжении всей поездки. Этот пользователь *однозначно* является мобильным! Однако между этими крайностями есть пользователь, переносящий портативный компьютер с одного местоположения (например, рабочего кабинета или общежития) в другое (напри­мер, кофейня или учебная аудитория) и желающий подключиться к сети в новом местоположении. Этот пользователь также является мобильным (хотя, конечно, гораздо менее мобильный, чем водитель BMW!), однако он не нуждается в сохранении текущих подключе­ний во время перемещения между точками подключения к сети. На рис. 6.21 изображен спектр категорий мобильности пользователей с точки зрения сетевого уровня.

**Рис. 6.21**. Различные категории мобильности с точки зрения уровня сети

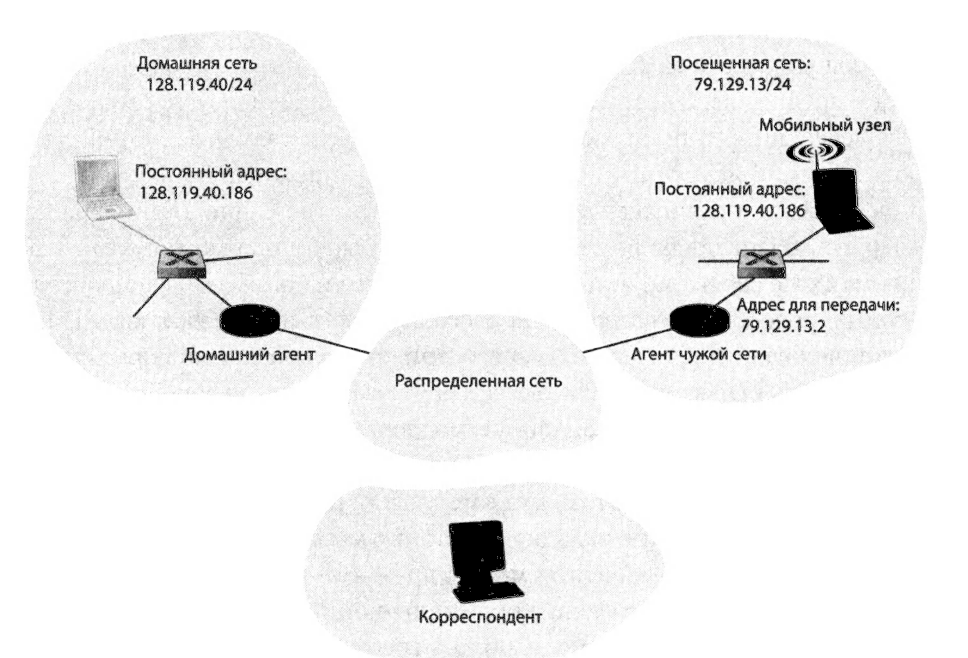
*Насколько важно для мобильного узла сохранять свой адрес неиз­менным?* Когда вы имеете дело с мобильной телефонией, ваш номер телефона, а по сути это является адресом сетевого уровня вашего мо­бильного телефона, остается неизменным при перемещении из сети одного оператора в сеть другого. Должен ли ноутбук сохранять тот же IP-адрес при перемещении между IP-сетями?

Ответ на этот вопрос во многом зависит от запущенных в момент вре­мени приложений. Так, для водителя спортивного BMW, желающего сохранять текущее TCP-подключение к удаленному приложению во время скоростной поездки по автобану, было бы гораздо удобнее иметь неизменный IP-адрес. Вспомним, что Интернет-приложению требуется знать IP-адрес и номер порта устройства, с ко­торым установлено подключение. Если мобильному устройству уда­ется при перемещении сохранять IP-адрес, то мобильность становится невидимой с точки зрения удаленного приложения. Такая невидимость несет большую пользу, ведь приложению не нужно более заботиться о том, что IP-адрес может поменяться в любой момент, таким обра­зом, единый программный код приложения может быть использован для обслуживания как мобильных, так и немобильных подключений. В следующем разделе мы убедимся, что мобильный IP предоставляет необходимую прозрачность, что позволяет мобильному узлу сохра­нять фиксированный IP-адрес при перемещении между сетями.

*Какая доступна вспомогательная проводная инфраструктура?* Во всех вышеописанных ситуациях мы всегда отталкивались от того, что существует некая постоянная инфраструктура, к которой может подключиться мобильный пользователь, например, это может быть домашняя ISP сеть, сеть беспроводного доступа в офисе, а также сети беспроводного доступа, развернутые вдоль автобана. Но что если нет ни одной из перечисленных инфраструктур? Если два пользо­вателя находятся в достаточной близости друг к другу для установ­ления соединения, могут ли они установить сетевое подключение в отсутствие всякой инфраструктуры сетевого уровня? Децентрали­зованные (ad hoc) сети обеспечивают как раз нужные возможности. Эта быстроразвивающаяся сфера в данный момент представляет со­бой передовой край исследования мобильных сетей, но находится вне поля нашего зрения. Однако книга Перкинса и веб-сайт рабочей группы IETF Mobile Ad Hoc Network содержат наиболее деталь­ное описание данной проблемы.

Для иллюстрации проблем, возникающих в связи с разрешением мобильным пользователям сохранять установленные подключения при перемещении между сетями, давайте проведем аналогию с примером из человеческий жизни. Молодой человек двадцати с чем-то лет, покидая родительский дом, становится «мобильным», проживая в общежитиях и на съемных квартирах, часто меняя при этом свой адрес. Если давняя подруга желает пообщаться с ним, каким образом она может получить новый адрес своего мобильного друга? Одним из наиболее распростра­ненных способов является связь с его семьей, так как мобильный мо­лодой человек, скорее всего, «зарегистрирует» свой новый адрес среди членов семьи (как минимум, для того, чтобы родители смогли при не­обходимости оказать материальную поддержку в выплате квартплаты). Таким образом, родительский дом с неизменившемся адресом стано­вится единственным местом, куда могут в первую очередь обратиться другие люди, желающие наладить контакт с мобильным молодым чело­веком. Впоследствии общение между друзьями может быть либо опо­средованное (например, если корреспонденция сначала отправляется на адрес родительского дома, а затем пересылается по адресу мобиль­ного молодого человека), либо прямое (например, если подруга будет пользоваться адресом, полученным от родителей своего друга для непо­средственной отправки писем).

В сетевых технологиях постоянный дом мобильного узла (например, ноутбука или смартфона) называется **домашней сетью,** а мобильное устройство, входящее в состав домашней сети и выполняющее задачи по управлению мобильностью (о нем речь пойдет ниже), называется **домашним агентом.** Сеть, в которой находится мобильный узел в настоя­щий момент времени, носит название **чужой** (или **посещенной) сети,** а устройство-элемент чужой сети, помогающее мобильному узлу с за­дачами управления мобильностью, называется **агентом чужой сети.** Так для мобильных специалистов домашней, скорее всего, будет являться сеть компании, в которой они работают, тогда как посещенной — сеть на рабочем месте коллеги, которого они посещают. **Корреспондент** — это устройство, желающее установить связь с мобильным узлом. Выше­перечисленные концепции отражены на рис. 6.22 вместе с понятиями адресации, обсуждаемыми ниже. Обратите внимание, что на рис. 6.22 агенты изображены в сочетании с маршрутизаторами (т. к. процессы обрабатываются маршрутизаторами), однако в качестве альтернативы, процессы могут также выполняться на других хостах или серверах, при­сутствующих в сети.

**Рис. 6.22. Первичные элементы архитектуры мобильной сети**

**Адресация**

Как уже отмечалось выше, чтобы мобильность была прозрачной для сетевых приложений, мобильному узлу желательно сохранять свой адрес в ходе перемещения из одной сети в другую. Когда мобильный узел находится в чужой сети, в нее должен быть маршрутизирован весь поток данных, посылаемый на постоянный адрес узла. Каким образом это осуществить? Первый вариант — это когда чужая сеть должна со­общать всем остальным сетям, что к ней подключился данный узел. Это можно осуществить путем обычного обмена внутридоменной и междоменной маршрутной информацией, что не потребует значи­тельных изменений в имеющейся инфраструктуре маршрутизации. Чужая сеть может просто оповестить соседние сети о наличии у нее высокоспецифичного маршрута к постоянному адресу мобильного узла (что, по сути, является оповещением других сетей о наличии кор­ректного пути для маршрутизации дейтаграмм на постоянный адрес мобильного узла). После этого соседние сети распро­странят эту маршрутную информацию как часть обычной процедуры обновления маршрутной информации и таблиц переадресации. Когда мобильный узел покинет одну чужую сеть и подключится к другой, эта новая чужая сеть распространит новый высокоспецифичный маршрут к мобильному узлу, а старая чужая сеть удалит маршрутную информа­цию, касающуюся данного узла.

Такой подход позволяет решить сразу две проблемы, при этом от­сутствует какая-либо необходимость во внесении сколько-нибудь зна­чительных изменений в инфраструктуру сетевого уровня. Другие сети знают местоположение мобильного узла и, благодаря тому, что таблицы перенаправления отсылают дейтаграммы в чужую сеть, маршрутиза­ция дейтаграмм на мобильный узел значительно облегчается. Однако значительным недостатком этого подхода является ограниченная мас­штабируемость. Если бы ответственность за управление мобильностью лежала на сетевых маршрутизаторах, то им пришлось бы обрабатывать таблицы перенаправления, содержащие записи о, возможно, миллионах мобильных узлов и обновлять эти записи при перемещении этих узлов.

Альтернативный подход (применяемый на практике) состоит в вы­талкивании обработки мобильности из ядра сети на периферию — сквоз­ная тема в нашем изучении архитектуры Интернета. Вполне естественно было бы осуществить это посредством домашней сети мобильного узла. Аналогично тому, как родители отслеживают местоположение своего двадцатилетнего чада, домашний агент из домашней сети мобильного узла может заниматься отслеживанием того, к какой чужой сети подключается мобильный узел. Для обновления местоположения мобиль­ного узла потребуется некий протокол взаимодействия мобильного узла (или агента чужой сети, представляющего интересы мобильного узла) и домашнего агента.

Сейчас давайте более подробно обсудим агент чужой сети. Концеп­туально наиболее простой подход, изображенный на рис. 6.22, заклю­чается в расположении агентов сети на пограничных маршрутизаторах чужой сети. Одной из задач агента чужой сети является создание для мобильного узла так называемого **адреса для передачи** (Care-of address, СОА). Таким образом, один мобильный узел ассоциируется сразу с дву­мя адресами: **постоянным адресом** (аналогичен адресу родительско­го дома мобильного молодого человека из нашего примера) и адресом для передачи, иногда называемым **адресом в чужой сети** (аналогичен адресу дома, в котором временно проживает наш мобильный молодой человек). В примере на рис. 6.22 постоянный адрес мобильного узла 128.119.40.186. При посещении сети 79.129.13/24 мобильному узлу присваивается адрес для передачи 79.129.13.2. Вторая задача агента чу­жой сети заключается в информировании домашнего агента о том, что данный мобильный узел находится в его (агента чужой сети) сети и ему присвоен адрес для передачи. Вскоре мы увидим, что адрес для переда­чи будет использован для перенаправления дейтаграмм на мобильный узел через агент чужой сети.

Несмотря на то, что мы разделили функциональность мобильного узла и агента чужой сети, мобильному узлу ничего не будет стоить пере­нять ответственность последнего. Например, при регистрации в чужой сети мобильный узел может самостоятельно получить адрес для передачи (например, с помощью такого протокола как DHCP) и самостоятельно проинформировать домашний агент о полученном адресе для передачи.

**Перенаправление на мобильный узел**

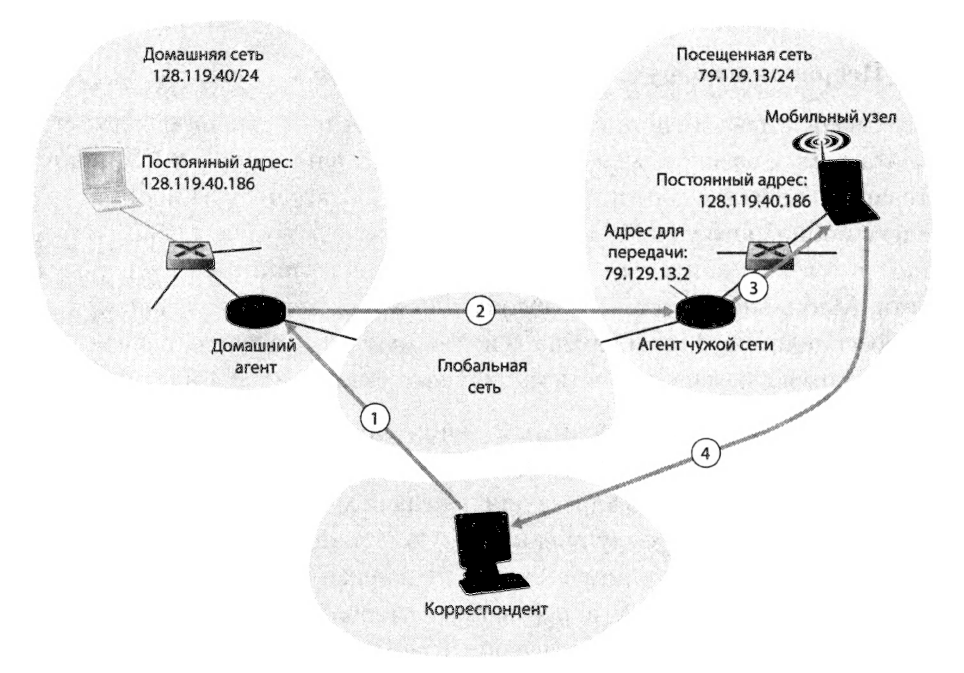
К настоящему моменту мы уже изучили механизмы получения мо­бильным узлом адреса для передачи (СОА), а также способы инфор­мирования домашнего агента о полученном мобильным узлом адресе. Однако оповещение домашнего агента об адресе для передачи решает только часть проблемы. Каким образом необходимо производить адре­сацию и пересылку дейтаграмм на этот мобильный узел? Так как только домашний агент (но не маршрутизаторы, подключенные к сети) знает местоположение мобильного узла, простой адресации дейтаграммы по постоянному адресу мобильного узла с последующей отправкой в ин­фраструктуру уровня сети будет недостаточно. Нужно сделать что-то еще. Для решения этой проблемы можно выделить два подхода, кото­рые мы будем называть прямой и непрямой маршрутизацией.

**Непрямая маршрутизация на мобильный узел**

Сначала давайте поговорим о корреспонденте, желающем отправить дейтаграмму на мобильный узел. При применении **непрямой маршру­тизации** корреспондент просто отправляет дейтаграмму на постоянный адрес мобильного узла, будучи при этом в счастливом неведении о том, находится ли мобильный узел в домашней сети или посещает чужую сеть. Мобильность остается абсолютно невидимой (прозрачной) для корреспондента. В этом случае дейтаграммы, как правило, сначала на­правляются в домашнюю сеть мобильного узла (см. шаг 1 на рис. 6.23).

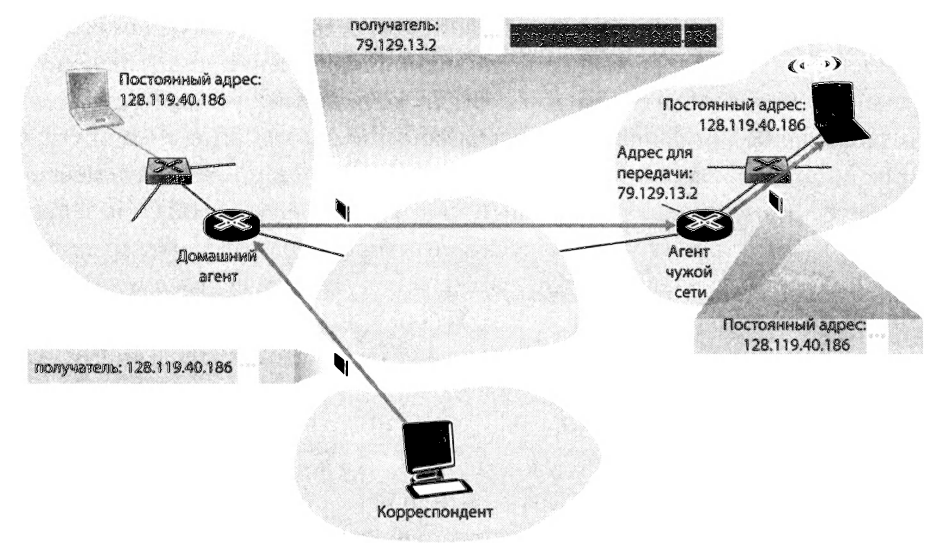
Теперь давайте переключим свое внимание на домашний агент. В до­бавок к ответственности за взаимодействие с агентом чужой сети, по­зволяющее отслеживать адреса для передачи мобильных узлов, домаш­ний агент имеет еще одну очень важную функцию. Его вторая работа заключается в том, что домашний агент должен быть «начеку» и пере­хватывать дейтаграммы, адресованные мобильным узлам-элементам домашней сети, находящимся в данный момент времени в других сетях. Домашний агент получает эти дейтаграммы, а затем пересылает их аген­ту чужой сети в два этапа. Сначала дейтаграмма пересылается агенту чу­жой сети с помощью адреса для передачи (СОА) мобильного узла (шаг 2 на рис. 6.23), а затем переадресуется агентом чужой сети мобильному узлу (шаг 3 на рис. 6.23).

Будет полезно рассмотреть такое перенаправление более детально. Домашнему агенту понадобится отправить дейтаграмму с помощью адре­са для передачи, полученного мобильным узлом, таким образом, оборудо­вание сетевого уровня перенаправит дейтаграмму в чужую сеть. С другой стороны, желательно, чтобы отправляемая дейтаграмма осталась неиз­менной, так как приложению-получателю нет необходимости знать о том, что она была переадресована домашним агентом. Обе цели достигаются в случае, если исходная дейтаграмма, отправляемая корреспондентом, подвергается полной **инкапсуляции** со стороны домашнего агента, то есть передается как часть новой (более крупной) дейтаграммы. Эта большая дейтаграмма адресуется и доставляется на адрес для передачи мобильно­го узла. Агент чужой сети, которому «принадлежит» адрес для передачи, полученный мобильным узлом, получит и декапсулирует дейтаграмму, иначе говоря, извлечет исходную дейтаграмму, отправленную корреспон­дентом из более крупной инкапсулирующей и переадресует извлеченную исходную дейтаграмму (шаг 3 на рис. 6.23) мобильному узлу.

**Рис. 6.23. Непрямая маршрутизация на мобильный узел**

На рис. 6.24 изображена отправка корреспондентом исходной дей­таграммы в домашнюю сеть, передача инкапсулированной дейтаграммы чужому агенту и доставка исходной дейтаграммы на мобильный узел. Внимательный читатель заметит, что процессы инкапсуляции и декап-суляции, описываемые здесь, идентичны понятию туннелирования, об­суждаемого ранее в контексте многоадресной передачи данных по IP и протокола IPv6.

Теперь давайте обсудим то, каким образом мобильный узел осущест­вляет отправку дейтаграмм корреспонденту. На самом деле все очень просто, так как мобильный узел может адресовать дейтаграммы корре­спонденту *напрямую* (используя свой собственный постоянный адрес как адрес отправителя и адрес корреспондента — в качестве адреса по­лучателя). Так как мобильный узел знает адрес корреспондента, в об­ратной маршрутизации дейтаграмм через домашнего агента нет необхо­димости. Это также отражено на рис. 6.24.

**Рис. 6.24. Инкапсуляция и декапсуляция**

Давайте подведем итог нашей беседе о непрямой маршрутизации, перечислив функциональность сетевого уровня, необходимую для под­держки мобильности.

* *Протокол связи мобильный узел — агент чужой сети.* Мобильный узел будет зарегистрирован агентом чужой сети при подключении к ней. Точно так же регистрация мобильного узла будет отменена, когда он покинет чужую сеть.
* *Протокол регистрации агент чужой сети — домашний агент.* Агент чужой сети произведет регистрацию адреса для передачи мобильного узла у домашнего агента. Агенту чужой сети не нужно явно отменять регистрацию у домашнего агента, когда мобильный узел покидает сеть, так как регистрация нового адреса для пере­дачи при регистрации мобильного узла в новой сети выполнит эту задачу
* *Протокол инкапсуляции дейтаграммы домашним агентом.* Инкапсу­ляция и переадресация исходной дейтаграммы корреспондента вме­сте с дейтаграммой, отправляемой по адресу для передачи мобиль­ного узла.
* *Протокол декапсуляции дейтаграммы чужим агентом.* Извлечение исходной дейтаграммы корреспондента из инкапсулирующей и пе­ресылка извлеченной дейтаграммы мобильному узлу.

Предыдущее обсуждение позволяет получить представление обо всех элементах — агентах чужой сети, домашнем агенте и непрямой переадре­сации, — необходимых для того, чтобы мобильный узел мог сохранять установленные соединения при перемещении из одной сети в другую. Для примера совместного использования вышеупомянутых элементов давайте представим, что мобильный узел подключен к чужой сети А, про­изведена регистрация у домашнего агента полученного узлом адреса для передачи, и поступающие дейтаграммы подвергаются непрямой маршру­тизации через агент домашней сети. Теперь мобильный узел перемещает­ся в чужую сеть Б и регистрируется в ней с помощью агента этой сети, со­общающего агенту домашней сети полученный узлом адрес для передачи (СОА). Начиная с этого момента домашний агент будет перенаправлять получаемые дейтаграммы в чужую сеть Б. С точки зрения корреспонден­та мобильность является прозрачной, или невидимой, так как дейтаграм­мы подвергаются маршрутизации с помощью одного и того же домашнего агента: как до перемещения в другую сеть, так и после. С точки зрения домашнего агента поток дейтаграмм остается непрерывным: изначально входящие дейтаграммы пересылались в чужую сеть А, после изменения адреса для передачи — стали переадресовываться в чужую сеть Б. Однако будет ли поток дейтаграмм оставаться непрерывным с точки зрения мо­бильного узла при перемещении из одной сети в другую? Так как отрезок времени между отключением мобильного узла от сети А (с этого момента он больше не сможет получать дейтаграммы по сети А) и подключением в сети Б (момент регистрации мобильным узлом нового СОА у домашне­го агента) невелик, будет потеряно только небольшое количество дейта­грамм. Вспомните из материала, изученного ранее, что одной из проблем сквозных соединений является потеря большого количества дейтаграмм в связи с перегрузкой сети. Таким образом, случайная потеря нескольких дейтаграмм при пере­мещении мобильного узла из одной сети в другую ни коим образом не влечет катастрофических последствий. Если есть необходимость в под­ключении без потерь, то целостность данных будет восстановлена с помо­щью механизмов верхнего уровня, независимо от того, в чем причина по­тери данных, будь то перегрузка сети или же мобильность пользователя. Подход с непрямой маршрутизацией применяется в стандарте мобильно­го IP, речь о котором пойдет позднее.

**Прямая маршрутизация на мобильный узел**

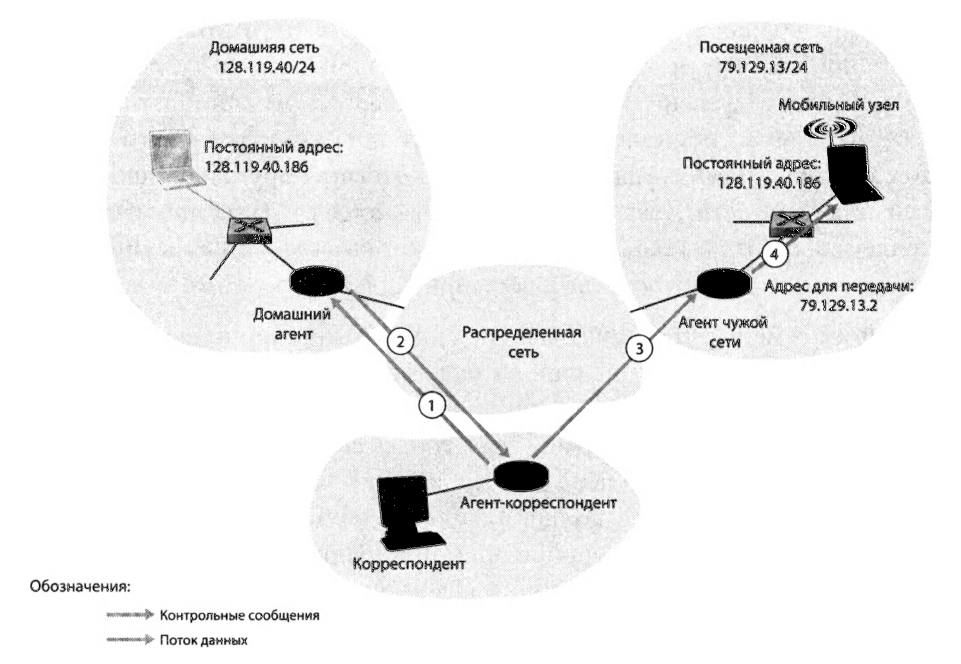
Подход с применением непрямой маршрутизации имеет один серьез­ный недостаток, называемый **проблемой треугольной маршрутизации:**

дейтаграммы, адресованные мобильному узлу, должны сначала быть отправлены (маршрутизированы) на домашний агент, а затем на чужой агент притом, что между корреспондентом и мобильным узлом суще­ствует более эффективный маршрут. В худшей из ситуаций представьте себе мобильного пользователя, решившего подключиться к сети своего коллеги. Оба сидят за одним столом напротив друг друга и обменивают­ся данными по сети. Дейтаграммы от корреспондента (в данном случае — коллеги посетителя) маршрутизируются на домашний агент мобильного пользователя, а затем обратно в сеть, принадлежащую его коллеге!

**Прямая маршрутизация** позволяет побороть неэффективность «тре­угольной» маршрутизации, однако делает это за счет увеличения слож­ности структуры. При применении подхода с прямой маршрутизацией **агент-корреспондент,** находящийся в той же сети, что и корреспондент, сначала узнает адрес для передачи мобильного узла. Это можно осуще­ствить, если агент-корреспондент опросит домашний агент, при этом предполагается, что (как и при непрямой маршрутизации) была произ­ведена своевременная регистрация и домашний агент обладает самой последней информацией об адресе для передачи мобильного узла. Кор­респондент также может выполнять функции агента-корреспондента точно также как мобильный узел может выполнять функции агента чу­жой сети. Вышеуказанное отражено в шагах 1 и 2 на рис. 6.25. В этом случае агент-корреспондент отсылает дейтаграммы напрямую по адресу для передачи мобильного узла аналогично тому, как направляет данные домашний агент (шаги 3 и 4 на рис. 6.25).

Несмотря на то, что прямая маршрутизация позволяет справиться с проблемой «треугольной» маршрутизации, эта технология ставит пе­ред нами две новые важные задачи:

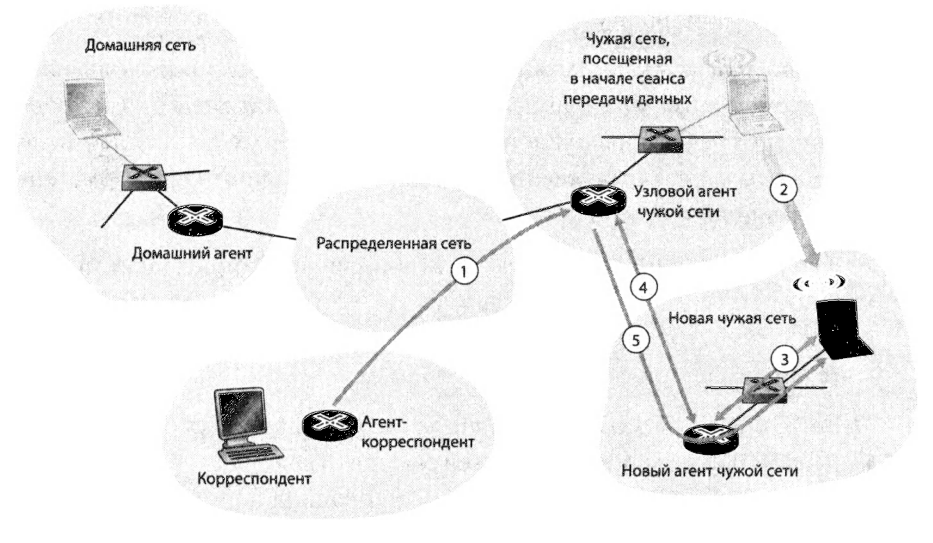
* **Протокол локализации мобильного пользователя** необходим аген­ту-корреспонденту для опроса домашнего агента с целью получения адреса для передачи мобильного узла (шаги 1 и 2 на рис. 6.25).
* **Каким образом будет осуществляться пересылка данных** в слу­чае перемещения мобильного узла из одной чужой сети в другую? В случае непрямой маршрутизации эта проблема легко решалась обновлением адреса для передачи, регистрируемого домашним агентом. Однако при прямой маршрутизации агент-корреспондент опрашивает домашний агент только один раз: в самом начале сеанса передачи данных. Поэтому обновление адреса для передачи, храня­щегося в памяти домашнего агента по мере необходимости будет не­достаточно для решения проблемы маршрутизации данных на мо­бильный узел, перешедший в новую чужую сеть.

**Рис. 6.25. Прямая маршрутизация данных для мобильного пользователя**

Одним из возможных решений задачи было бы создание нового про­токола, информирующего агент-корреспондент об изменившемся адре­се для передачи. Альтернативное решение, применяемое, как вы убеди­тесь, на практике в сетях стандарта GSM, работает следующим образом. Предположим, что в данный момент происходит передача данных мо­бильному узлу через чужую сеть, в которой он был локализован в на­чале сеанса передачи данных (шаг 1 на рис. 6.26).

Мы будем называть агент чужой сети, в которой был впервые найден мобильный узел, **узловым агентом чужой сети.** Когда мобильный узел переходит в новую чужую сеть (шаг 2 на рис. 6.26), он регистрируется с помощью нового агента чужой сети (шаг 3), после чего тот предостав­ляет узловому агенту чужой сети новый адрес для передачи мобильного узла (шаг 4). Узловой агент чужой сети по получении инкапсулирован­ной дейтаграммы для уже вышедшего из его сети мобильного узла, мо­жет совершить ре-инкапсуляцию этой дейтаграммы и переадресовать ее мобильному узлу (шаг 5) с помощью нового адреса для передачи.

Если мобильный узел с течением времени перейдет уже в третью чу­жую сеть, ее агент свяжется с узловым агентом чужой сети для настрой­ки переадресации данных в новую сеть.

**Рис. 6.26. Мобильный трансфер между сетями с помощью прямой**

**маршрутизации**

**Мобильный протокол Интернета**

Интернет-архитектура и протоколы для поддержки мобильности, известные как мобильный IP, определены, в первую очередь в RFC 5944 для IPv4. Мобильный IP представляет собой гибкий стандарт, поддерживающий несколько режимов работы (например, с агентом чу­жой сети или без него), несколько способов, используя которые, аген­ты и мобильные узлы могут обнаруживать друг друга, использование одного или нескольких адресов для передачи (СОА), а также несколь­ко форм инкапсуляции. По своей сути мобильный IP — достаточно сложный стандарт и его детальное описание потребовало бы отдельной книги, кстати, такая книга существует — ее написал Чарльз Перкинс. Наша скромная цель здесь — дать краткое описание наиболее важных аспектов мобильного IP и проиллюстрировать его применение на не­скольких общих примерах.

Архитектура мобильного IP включает большое количество элемен­тов, которые мы уже обсудили ранее, в том числе концепции домашнего агента, агентов чужих сетей, адресов для передачи, а также инкапсуля­ции и декапсуляции. Использующийся в настоящий момент стандарт RFC 5944 предписывает применение непрямой маршрутизации на мобильный узел.

Стандарт мобильного IP содержит три важных составляющих:

* *Обнаружение агента.* Мобильный IP определяет протоколы, ис­пользуемые домашним агентом и агентом чужой сети для инфор­мирования мобильных узлов о предоставляемых сервисах, а также протоколы для востребования мобильными узлами сервисов аген­тов домашней и чужой сети.
* ***Регистрация у домашнего агента****.* Мобильный IP определяет прото­колы, используемые мобильным узлом и/или агентом чужой сети с целью регистрации или отмены регистрации адреса для передачи у агента домашней сети мобильного узла.
* ***Непрямая маршрутизация дейтаграмм.*** Стандарт также определяетто, каким образом домашний агент осуществляет пересылку дейта­грамм на мобильные узлы, в том числе правила переадресации дей­таграмм, правила обработки ошибок и несколько форм инкапсуля­ции.

Для стандарта мобильного IP вопросы обеспечения безопасности особенно важны. Например, аутентификация мобильного узла абсолют­но необходима для гарантии того, что злоумышленник не зарегистрирует у домашнего агента подложный адрес для передачи, что вызвало бы пе­реадресацию всех дейтаграмм, предназначенных для данного IP-адреса, на устройство злоумышленника. Безопасность мобильного IP достига­ется с использованием большого количества механизмов, которые мы изучим позднее, поэтому мы не будем отдельно обращать внимание на вопросы безопасности в тексте нашего обсуждения.

**Обнаружение агента**

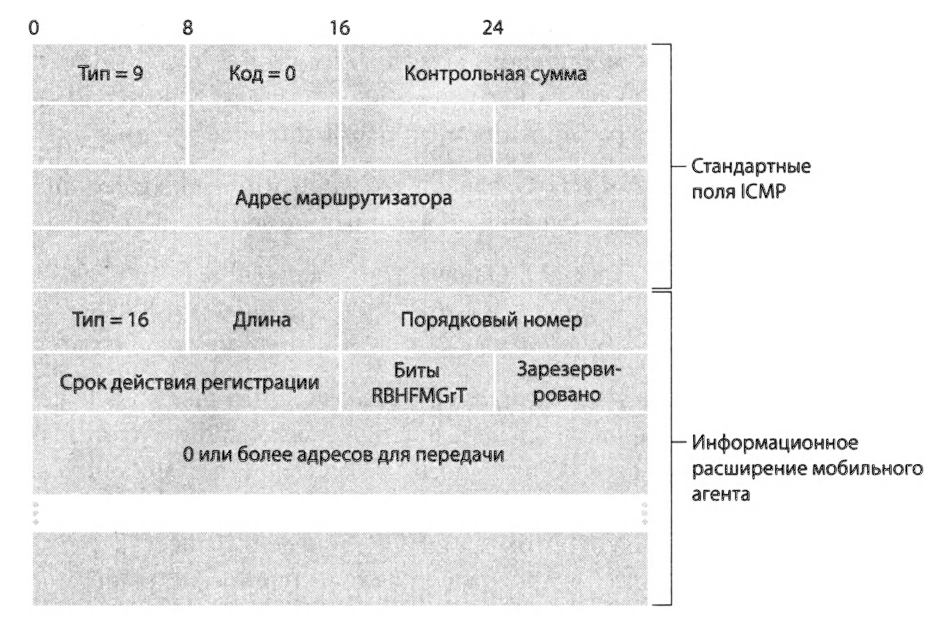
По переходе в новую сеть, будь то подключение к чужой сети или возвращение в домашнюю, узел с мобильным IP должен «идентифици­ровать личность» соответствующего агента чужой или домашней сети. На самом деле это есть обнаружение нового агента чужой сети, обладаю­щего новым сетевым адресом, позволяющим оборудованию уровня сети мобильного узла понять, что узел переместился в новую чужую сеть. Этот процесс называется **обнаружением агента.** Обнаружение агента происходит одним из двух способов: с помощью информационных со­общений агента, либо через затребование у него информации.

В случае с **информационными сообщениями** агент чужой или до­машней сети распространяет («рекламирует») информацию о предоставляемых им услугах, расширяя соответствующий протокол обнару­жения маршрутизатора. Агент периодически транслирует сообщение ICMP со значением поля типа 9 (обнаружение маршрутизатора) по всем подключенным к нему каналам связи. Это сообщение обнаруже­ния маршрутизатора содержит IP-адрес маршрутизатора (то есть аген­та), позволяя, таким образом мобильному узлу узнать IP-адрес агента сети. Сообщение обнаружения маршрутизатора также содержит инфор­мационное расширение мобильного агента, включающее в себя допол­нительную информацию, необходимую мобильному узлу. Среди наибо­лее важных полей этого расширения можно выделить следующие:

* *Бит домашнего агента (Н).* Означает, что данный агент является до­машним агентом сети, в которой он в данный момент находится.
* *Бит агента чужой сети (F).* Означает, что данный агент является агентом чужой сети для сети, в которой он в данный момент нахо­дится.
* *Бит необходимости регистрации (R).* Означает, что при подключе­нии к данной сети мобильный пользователь *обязан* пройти регистра­цию у агента этой сети. В частности это означает, что мобильный пользователь не может получить адрес для передачи в чужой сети (например, с помощью протокола DHCP) и перенять на себя функ­ции агента чужой сети без прохождения процедуры регистрации у ее агента.
* *Биты инкапсуляции* М, *G.* Обозначают, будет ли использована фор­ма инкапсуляции, отличная от инкапсуляции IP-b-IP.
* *Поля адреса для передачи (СОА).* Перечень из одного или несколь­ких адресов для передачи, предоставляемый агентом чужой сети. В нашем примере, приводимом ниже, адрес для передачи будет ас­социирован с агентом чужой сети, который станет получать дейта­граммы, отправляемые по этому адресу для передачи и пересылать их нужному мобильному узлу. При регистрации у домашнего агента мобильный пользователь выберет один из этих адресов в качестве своего адреса для передачи.

На рис. 6.27 приведены некоторые ключевые поля информационно­го сообщения агента.

В случае с **запросом информации об агенте** мобильный узел, же­лающий получить сведения об агенте, не дожидаясь информационного сообщения, может передать сообщение с требованием информации об агенте, представляющее собой обычное сообщение ICMP со значением поля типа 10. Агент, получивший сообщение с требованием передачи информации о себе, направит его напрямую мобильному узлу, который сможет продолжить выполнять необходимые действия так, будто бы по­лучил информационное сообщение без дополнительных требований.

Рис. 6.27. Сообщение обнаружения маршрутизатора ICMP с расширением

мобильного агента

**Регистрация у домашнего агента**

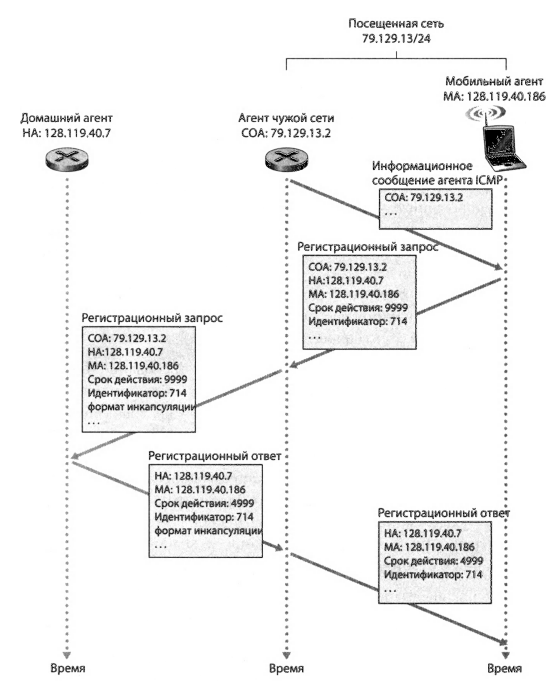
Как только мобильный узел получил адрес для передачи (СОА), он должен зарегистрировать этот адрес у агента домашней сети. Это мо­жет быть осуществлено либо через агента чужой сети (который и про­изведет регистрацию СОА у домашнего агента), либо непосредственно узлом с мобильным IP. Далее мы рассмотрим первый из двух вариантов. Для его осуществления потребуется пройти четыре шага.

1. Следуя инструкциям в информационном сообщении агента чужой сети, мобильный узел направляет ему регистрационное сообщение IP-адреса. Регистрационное сообщение передается внутри дейта­граммы UDP, направляемой на порт 434. Оно содержит адрес для пе­редачи, предложенный агентом чужой сети, адрес домашнего агента (НА), постоянный адрес мобильного узла (МА) желаемый срок действия регистрации, 64-битный регистрационный идентификатор. Желаемый срок регистрации — это значение времени в секундах, на протяжении которой регистрация в сети будет оставаться дей­ствительной. Если регистрация не обновляется на домашнем агенте в указанный период времени, она перестает быть действительной. Регистрационный идентификатор играет роль порядкового номера, используемого для соотнесения полученного регистрационного от­вета с регистрационным требованием (см. ниже).

1. Агент чужой сети получает регистрационное сообщение и записы­вает постоянный IP-адрес мобильного узла. Теперь агент этой сети знает, что он должен выполнять поиск дейтаграмм, содержащих ин­капсулированные дейтаграммы, адрес назначения которых совпада­ет с постоянным адресом мобильного узла. После этого агент чужой сети направляет регистрационное сообщение мобильного IP-адреса (опять же внутри дейтаграммы UDP) на порт 434 домашнего агента. Это сообщение содержит адрес для передачи, НА, МА, требуемый формат инкапсуляции, требуемый срок действия регистрации и ре­гистрационный идентификатор.
2. Домашний агент получает регистрационное требование и проверя­ет его аутентичность и правильность. После этого домашний агент связывает постоянный IP-адрес мобильного узла с адресом для пе­редачи. В будущем дейтаграммы, поступающие на домашний агент и адресованные мобильному узлу, будут инкапсулированы и от­правлены посредством туннелирования на адрес для передачи. До­машний агент также отсылает ответ о регистрации мобильного IP-адреса, содержащий НА, МА, реальный срок действия регистрации, регистрационный идентификатор запроса, который был подтверж­ден данным ответом.
3. Агент чужой сети получает регистрационный ответ и пересылает его мобильному узлу.

На данном этапе регистрация завершена и мобильный узел может получать дейтаграммы, отправленные на его постоянный адрес. Выше­описанные шаги проиллюстрированы на рис. 6.28. Обратите внимание, что домашний агент указывает срок действия регистрации меньший, чем был запрошен мобильным узлом.

Агент чужой сети не должен явно отменять регистрацию адреса для передачи, когда мобильный узел покидает его сеть. Отмена регистрации произойдет автоматически, когда мобильный узел перейдет в новую сеть (независимо от того, будет ли это еще одна чужая сеть либо домаш­няя) и зарегистрирует новый адрес для передачи.

****

**Рис. 6.28. Информационное сообщение агента и регистрация мобильного IP**

Стандарт мобильного IP допускает наличие множества дополни­тельных алгоритмов и возможностей вдобавок к описанным выше. За­интересованный читатель может получить информацию в книге Пер-кинса спецификации RFC 5944.