Резервирование сетевых соединений в критически важных приложениях

Живучесть сетевых соединений, способность системы к самовосстановлению в случае отказа каналов связи и к оптимизации при наличии нескольких работающих каналов — критически важные характеристики связи для бесперебойной работы удалённого терминального оборудования. Особую важность эта задача приобретает, когда речь идёт о необслуживаемых устройствах, таких как банкоматы и киоски самообслуживания. В этих случаях терминал должен работать многие сутки, а иногда и месяцы, без какого-либо, даже минимального (на уровне "нажать аварийную кнопочку"), вмешательства человека. Соответственно, и оборудование связи, обслуживающее его, должно уметь автоматически выходить из любых, самых запутанных ситуаций, в которые её могут завести реалии отечественной телекоммуникационной среды — и, по возможности, делать это минимально заметным образом с точки зрения прикладных программ и устройств.

Например, наземный канал связи (Ethernet, *x*DSL и др.) практически всегда приходится подстраховывать сотовым каналом GPRS или CDMA. Более того, специфика банковских транзакций требует, чтобы даже при многократных переходах с основного канала на резервный(-е) и обратно была гарантирована доставка данных и поддерживался непрерывный сеанс работы прикладного программного обеспечения. Оборудование NSG предлагает богатый набор аппаратных и программных механизмов для этой цели — как стандартных, совместимых с оборудованием других производителей, так и фирменных, разработанных с учётом особенностей данного круга задач. Это обеспечивается модульной конструкцией, высокой аппаратной и программной гибкостью, присущими устройствам NSG.

Устройство NSG–700/4AU может оснащаться двумя сменными интерфейсами

Очевидное и необходимое условие для резервирования каналов связи, которое сразу ставит аппаратуру NSG на корпус впереди других аналогичных устройств — наличие не менее чем 3 сетевых интерфейсов. Это относится, за единичными исключениями, ко всей продуктовой линейке NSG, в том числе к устройствам доступа младшего класса, предназначенным для подключения одиночных банкоматов и POS-терминалов. Так, наиболее массовое устройство NSG–700/4AU имеет 3 порта Fast Ethernet, 3 порта RS–232 и 2 разъёма расширения, в которые может устанавливаться десяток различных типов интерфейсных модулей. Современные модули NSG для сетей GSM и 3G оснащаются двумя SIM-картами и могут работать через двух операторов.

Кроме того, модули GSM и 3G[1] поддерживают два режима передачи данных — пакетный (GPRS/EDGE/HSDPA) и канальный (CSD, или GSM data). Например, при нормальной работе сотовой сети можно использовать модуль в режиме GPRS, а при высокой нагрузке, когда реальная пропускная способность GPRS падает вплоть до нуля — переключать его в режим GSM data и устанавливать соединения по требованию. При соединениях по коммутируемым телефонным линиям могут использоваться несколько альтернативных телефонных номеров.

Рынок аппаратуры и услуг для бесперебойного подключения по нескольким каналам связи является узкоспециализированным и едва ли может похвастаться большим разнообразием предложений. С технической точки зрения и с точки зрения организации услуг, все решения NSG существенно отличаются от других продуктов, представленных на этом рынке, по следующим основным пунктам:

- Устройства доступа NSG позволяют резервировать соединения по нескольким каналам связи различного типа (Ethernet, GPRS, CDMA[2], dial-up[3] и др.), в то время как конкурирующие продукты рассчитаны, как правило, исключительно на работу через двух операторов GPRS.
- Встроенные средства мониторинга работоспособности каналов и интегрированная конструкция (модемный модуль является составной частью устройства доступа) гарантируют восстановление работоспособности в любых ситуациях — в том числе и при некорректной работе сети GPRS, которая может наблюдаться в периоды пиковых нагрузок.
- Компания NSG является исключительно производителем оборудования. Это означает, что заказчик разово приобретает оборудование в собственность и в дальнейшем не несёт бремени ежемесячных абонентских платежей оператору-посреднику (за исключением расходов на собственно услуги операторов связи по каждому из используемых каналов). Кроме того, уменьшается число сторонних организаций и их сотрудников, причастных к передаче конфиденциальной банковской информации, что положительно сказывается на общей безопасности системы.

Модули GPRS/EDGE и 3G для маршрутизаторов NSG оснащены двумя SIM-картами

[1] Модули (U)IM–EDGE всех модификаций обратно совместимы с услугой GPRS. Модуль UIM–3G обратно совместим с услугами EDGE и GPRS.

[2] Модуль UM–EVDO/A *h/w ver*.5 поддерживает услуги CDMA 1x, EV-DO rev.0 и rev.A.

[3] Модули IM–V34, IM–V92.

Физическое резервирование подключений GPRS, CDMA и dial-up

В важном частном случае, когда речь идёт о подключении терминального устройства через двух операторов GPRS, пользователь имеет выбор: использовать один модуль GSM/EDGE или 3G с двумя SIM-картами, либо установить в одно шасси два раздельных модуля. Оба варианта имеют свои достоинства и недостатки, и оба заслуживают рассмотрения применительно к конкретным техническим требованиям и бюджету проекта.

Решение с одним 2-симчатым модулем имеет меньшую стоимость — не только из-за отсутствия второго модуля, но и благодаря использованию более дешёвого шасси NSG–700/4AU *h/w ver.5*. Но такой модуль работает с операторами только попеременно. Переустановление соединения и, в том числе, переход на другого оператора выполняется через аппаратный рестарт модуля — это единственный способ гарантировать вывод сотового интерфейса из любых нештатных состояний. Однако после рестарта требуется некоторое время для загрузки внутреннего программного обеспечения, регистрации в сети и собственно подключения. В зависимости от типа модуля и скорости реакции сети, оно может составлять от 15 до 50 сек. В течение этого времени передача данных невозможна.

Решение с двумя модулями обходится дороже, поскольку для него настоятельно рекомендуется использовать шасси NSG–700/4AU *h/w ver.6*, обеспечивающее аппаратный рестарт модуля в обоих разъёмах расширения. Модули работают независимо друг от друга и могут быть постоянно подключены каждый к своей сети. Поскольку услуга GPRS оплачивается по объёму данных, а не по времени, это не влечёт никаких затрат, зато при отказе одного канала другой готов к работе немедленно.

Аналогичным образом, шасси NSG–700/4AU *h/w ver.6* рекомендуется использовать, если один из модулей — GPRS/EDGE или 3G, а другой — CDMA или модем для коммутируемых телефонных линий.

Стандартные средства IP-маршрутизации

Процедура альтернативной маршрутизации пакетов предусмотрена самой технологией IP, равно как и её предшественницей — технологией X.25. Однако в простейшем варианте, доступном конечному пользователю, суть её оказывается выхолощенной. Камень преткновения состоит в том, что в существующей модели предоставления услуг Интернет пользователь всегда имеет IP-адрес в пределах блока адресов, принадлежащих данному оператору. При переключении на другого оператора, абонентский терминал неизбежно будет использовать другой IP-адрес, соответствующий новой сети. То же самое происходит, как правило, при переподключении к одному и тому же оператору (если в контракте не предусмотрена отдельная услуга статического IP-адреса). Это может быть приемлемо, в лучшем случае, для POS-терминалов, работающих в сеансовом режиме. Для банкоматов, предполагающих непрерывное взаимодействие с процессингом, смена IP-адреса "на лету" недопустима ни технически, ни с точки зрения безопасности. В такой ситуации прикладное программное обеспечение обязано прервать текущий сеанс работы и начать новый сеанс по полной процедуре: взаимная аутентификация обеих сторон, инициализация сессии и т.д. Для некоторых типов банковского ПО такая ситуация крайне нежелательна даже во время холостой работы банкомата — не говоря уже о том, что любая транзакция, выполняемая в момент переключения, неизбежно будет сброшена.

Безусловно, технология IP предусматривает механизмы, позволяющие использовать постоянный IP-адрес при подключении через нескольких операторов. Однако для конечного пользователя они, по существу, недоступны. Во-первых, для этого потребовалось бы выделить каждому пользователю (в данном случае, банкомату) статический глобальный IP-адрес, не зависящий от используемого канала связи — что уже само по себе требует дополнительных затрат. Во-вторых, один и тот же IP-адрес не может одновременно принадлежать к адресному пространству двух или более операторов, поскольку это в корне противоречит иерархической схеме IP-адресации. Как следствие, абонентская площадка должна взаимодействовать с операторами уже не как часть их сетей, а как самостоятельный, равный им, субъект Интернет, имеющий собственное пространство IP-адресов (т.н. *автономная система*). В частности, если говорить о динамической маршрутизации, то для такого взаимодействия требуются уже не относительно простые протоколы маршрутизации между узлами (RIP, OSFP), а значительно более сложные протоколы межсетевой маршрутизации (BGP и т.п.), требующие бóльших вычислительных ресурсов и более сложные в настройке.

Наконец, такое подключение выглядит достаточно проблематично с организационной точки зрения. Если пользователь подключён одновременно к двум операторам и взаимодействует с ними как равный, то образуется лишняя связь между сетями этих операторов. Это факт они должны учитывать в своих схемах маршрутизации, безопасности и т.п. Сложно представить себе двух или более операторов, согласованно настраивающих свои подключения для такого общего абонента. Если же учесть, что число абонентов на многие порядки превосходит число операторов, то задача управления такой многосвязной совокупностью сетей становится совершенно неподъёмной.

Таким образом, на практике альтернативная маршрутизация, организованная исключительно классическими средствами IP, почти нереализуема. О ней имеет смысл говорить только в отдельных частных случаях, когда речь идёт о двух каналах связи и двух подсетях в пределах сети одного и того же оператора. Но такое решение представляет, в основном, академический интерес.

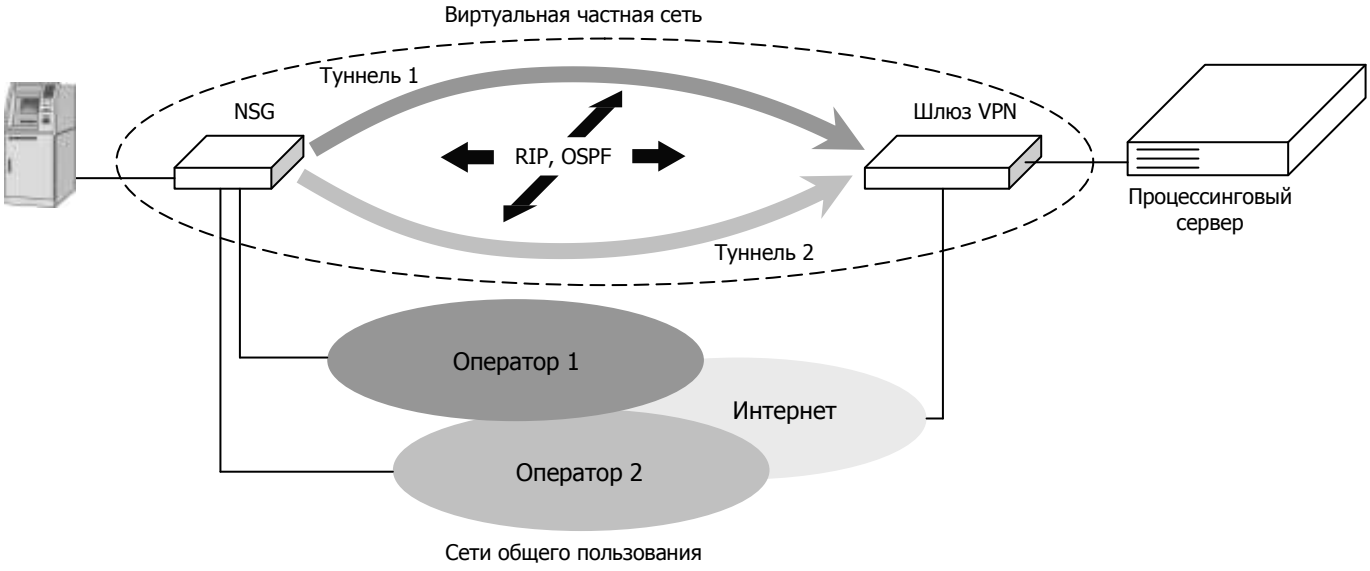
Современная практика построения IP-сетей предлагает корпоративному пользователю другой путь: организацию собственной наложенной виртуальной сети поверх сетей общего пользования. Для этого предназначены механизмы туннелирования и VPN — но тут есть свои подводные камни, о которых речь пойдёт ниже.

Виртуальные частные сети

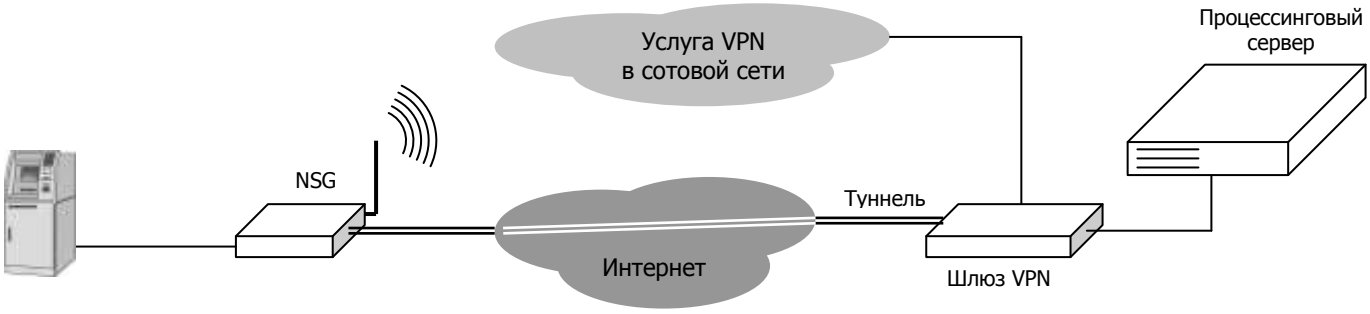
Виртуальная частная сеть (VPN) может быть построена на основе туннелей 2–3 уровней (PPTP, IPsec) и/или одноимённой услуги, предлагаемой сотовыми операторами. Основной и наиболее очевидной функцией VPN обычно является защита данных, но эта задача выходит за рамки данной статьи. Применительно к вопросу резервирования соединений, VPN позволяет решить две частные задачи:

— Внутри сети можно назначить постоянные IP-адреса (из приватного диапазона, например, 10.*x.x.x* или 192.168.*x.x*) банкомату и сетевым устройствам. Благодаря этому, банкомат всегда виден процессингу под одним и тем же адресом, независимо от того, по какому маршруту был доставлен конкретный пакет.

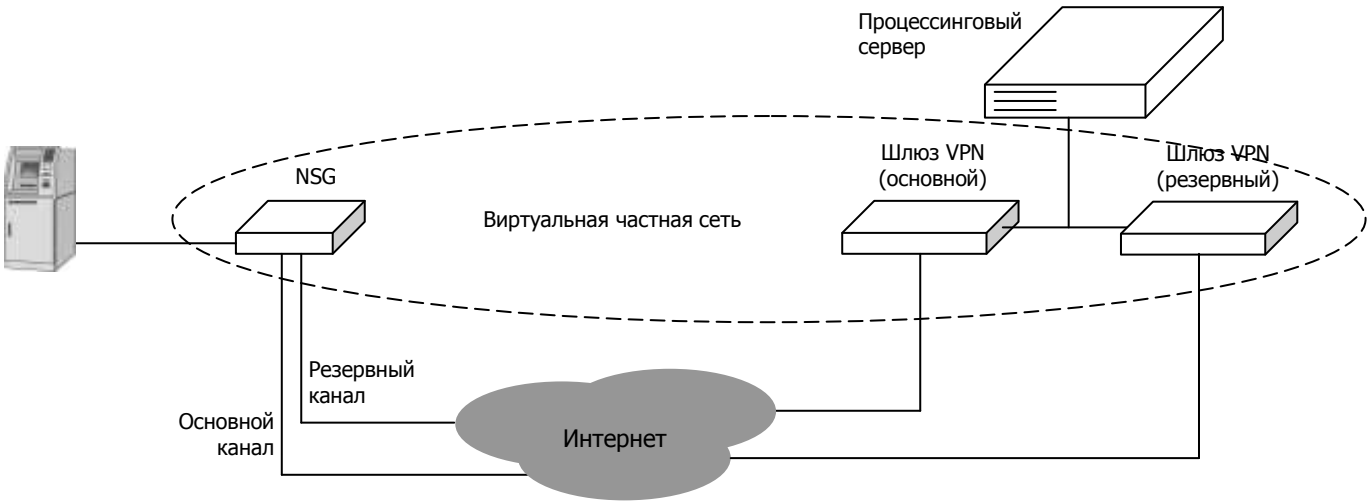
— В пределах приватной сети, имеющей единое адресное пространство, могут применяться протоколы динамической маршрутизации между отдельными узлами сети — RIP или OSPF.



Как частные случаи, туннели VPN могут быть построены не к одному и тому же публичному интерфейсу центрального VPN-шлюза, а к разным интерфейсам, подключенным к разным сетям. Такая конфигурация применяется, например, когда один из туннелей строится через сети общего пользования (наземные или беспроводные), а вместо второго используется услуга VPN сотового оператора.



Устройства NSG также предусматривают установление резервных туннелей к физически раздельным резервным шлюзам на центральном узле — как по раздельным каналам связи, так и при работе через одни и те же каналы.



Работа протоколов динамической маршрутизации опирается на частый обмен служебными сообщениями. Из двух вышеупомянутых протоколов OSPF создаёт значительно меньший объём служебного трафика, поэтому он является, как правило, предпочтительным. Это особенно существенно при подключениях по GPRS и CDMA, услуги которых оплачиваются именно по объёму данных.

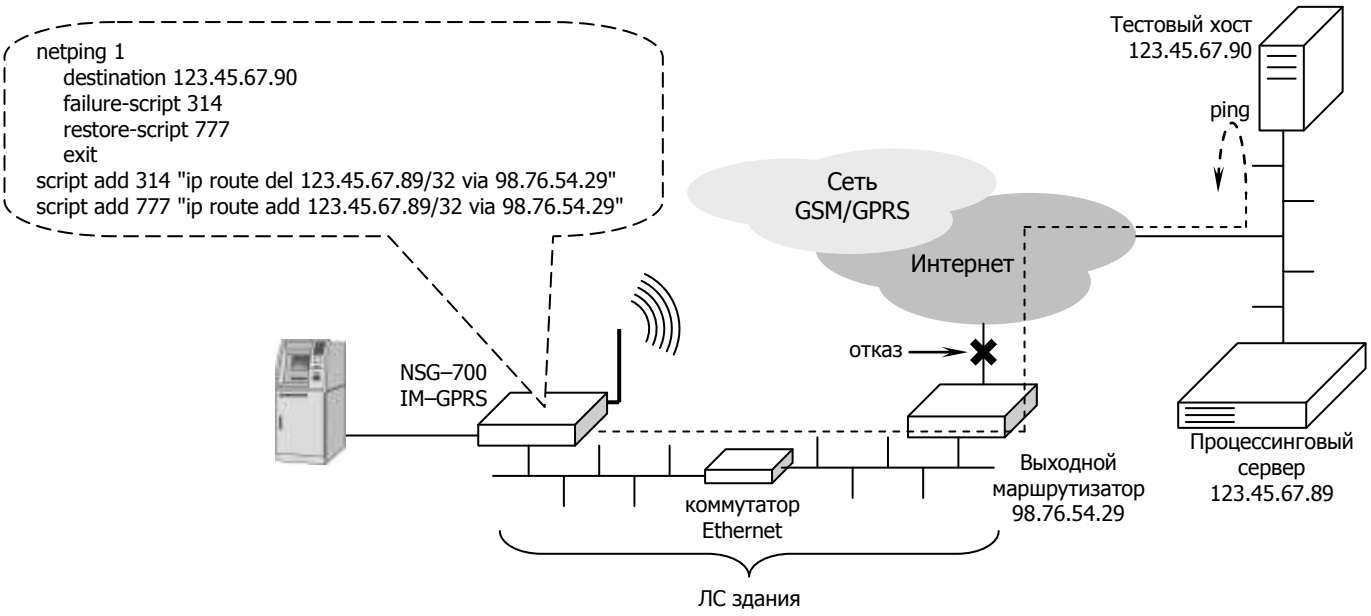
Однако в этом месте в оптимистичной картине, нарисованной выше, есть один маленький изъян. Реализация OSPF в оборудовании одного из ведущих производителей, которое повсеместно применяется на центральных узлах, имеет одну официально признанную особенность[1], не позволяющую использовать этот протокол на туннелях VPN. Тем не менее, дополнительные механизмы NSG Linux, такие как функциональность *netping* и скрипты, позволяют обойти эту проблему и успешно обеспечить динамическую маршрутизацию в виртуальной частной сети при падении и восстановлении туннелей.

В отдельных случаях может использоваться также комбинация RIP и OSPF. Такое решение целесообразно, если основным является VPN-туннель через наземное подключение Ethernet, *x*DSL и т.п. (с фиксированной оплатой), а резервным — услуга VPN сотового оператора.

Контроль состояния каналов связи и туннелей VPN

Для конечного пользователя, подключённого к двум каналам связи, выбор работающего маршрута содержит в себе ещё одну задачу. Основным критерием для этого выбора является факт отказа физического интерфейса или протокола канального уровня — а это недостаточно надёжный критерий, поскольку он отражает состояние только *непосредственно подключённого* сегмента сети. Например, если банкомат включён через локальную сеть здания, а авария происходит на участке от здания к поставщику услуг, то детектировать её средствами 1–2 уровней принципиально невозможно, поскольку порт Ethernet остаётся в нормальном состоянии.

Программное обеспечение NSG решает эту проблему с помощью встроенного механизма *netping*. Устройство периодически посылает пакеты на некоторый адрес в сети банка и, таким образом, контролирует работу каналов связи на всём протяжении от банкомата до процессингового центра. Далее, в зависимости от результатов, могут быть выполнены заданные действия, например, внесены изменения в таблицу маршрутизации.



Стоит заметить, что в сетях X.25 процедура альтернативной маршрутизации также опирается на факт доступности или недоступности *конечного* хоста и, таким образом, в процессе установления соединения тестируется полностью весь маршрут от начальной точки до конечной. Это один из механизмов, обеспечивающих высокую устойчивость таких сетей.

Аналогичный контроль состояния туннелей необходим для обеспечения отказоустойчивости сетей VPN. Все современные технологии VPN включают в себя встроенные механизмы для этой цели. В разных технологиях они, в силу сложившейся терминологии, называются по-разному: *keepalive, echo, Dead Peer Detection* — но суть их остаётся неизменной: устройства периодически обмениваются пакетами "запрос-ответ", чтобы убедиться в работоспособности соединения. Программное обеспечение NSG Linux предусматривает использование таких механизмов как для туннелей VPN, так и для физических соединений. Кроме того, оно обеспечивает принудительную взаимосвязь между состояниями каждого физического интерфейса и туннелей, выходящих через него.

[1] Вне всякого сомнения, если бы такая особенность имела место в продукте какого-нибудь другого производителя, то её следовало бы расценивать как ошибку. Однако великие не ошибаются — они просто делают вещи, не до конца понятные современникам…

Бесперебойные соединения

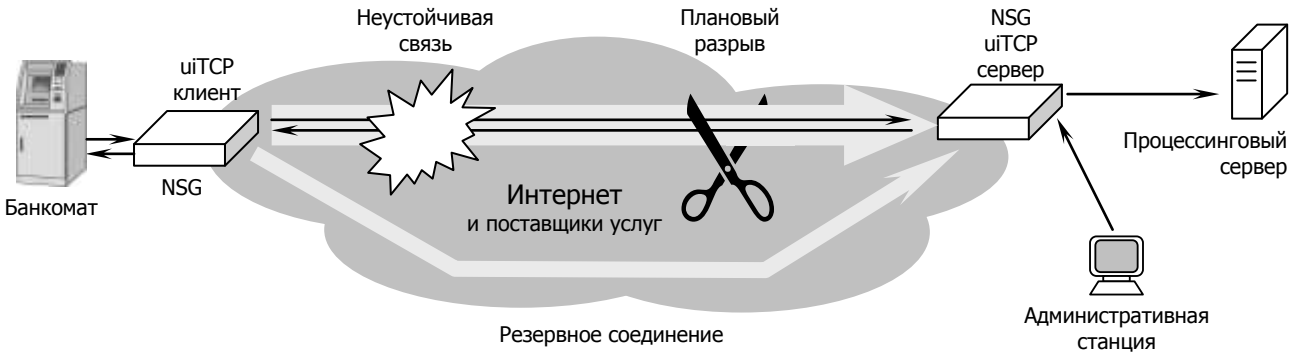
Стандартные механизмы IP и VPN, описанные выше, предназначены для решения только одной части задачи. Они позволяют находить маршрут между двумя узлами сети, если таковой вообще существует. Однако ни один из них не гарантирует доставку пакетов, если время обнаружения отказа и поиска нового маршрута оказывается больше, чем обычный таймаут протокола TCP (несколько десятков секунд) — что, вообще говоря, случается достаточно часто, особенно при работе через сотовые сети. Предполагается, что дальнейший контроль осуществляется протоколом прикладного уровня или непосредственно пользователем. Однако если обычный пользователь Интернет, например, может просто повторно нажать на ссылку нужного Web-сайта, то в банковских приложениях потеря пакета или даже одного байта данных — это нештатная ситуация. Чтобы обеспечить гарантированную доставку пакетов при переключениях между несколькими каналами и операторами связи, компанией NSG разработана фирменная система бесперебойных соединений ***ui*TCP**® (Un-Interruptible TCP).

***ui*TCP** — наиболее сложное и комплексное решение, воплощающее в себе многолетний опыт работы специалистов NSG в области сетей X.25, Frame Relay, IP и VPN. В нём аккумулированы многие фирменные наработки, накопленные ранее при создании систем X.25-over-X.25 (задолго до того, как появился термин "туннелирование"), X.25-over-TCP/IP, IP-over-X.25, X.25-over-Ethernet и др., а также современные методы построения сетей и защиты данных. При этом собственно факт бесперебойности — это только верхушка айсберга. За кулисами ***ui*TCP** работает целый набор разнообразных механизмов и протоколов. Не будь ***ui*TCP**, каждый из них нужно было бы (и можно было бы, благодаря гибкости ПО NSG Linux) настраивать вручную; однако здесь все они собраны в единую систему и работают прозрачно для пользователя.

Технология ***ui*TCP** обеспечивает:

— Поддержание постоянного сеанса обмена прикладными данными независимо от состояния каналов связи и переключений между ними.
— Неограниченное число каналов связи произвольных типов, выбираемых в порядке их приоритета или по кругу.
— Постоянный мониторинг наличия связи между устройствами.
— Переключение с основного канала на резервный(-е), с GPRS на GSM data и с основного GSM-оператора на резервного, с сохранением прежнего IP-адреса или его изменением.
— Автоматическое возвращение на основной (или более приоритетный) канал при восстановлении его работоспособности, выполняемое в периоды отсутствия полезного трафика.
— Передачу различных типов IP-трафика, в том числе:
  — Данных из прикладных TCP-соединений пользователя с заданным номером порта
  — Данных из прикладных UDP-потоков пользователя с заданным номером порта
  — Пакетов заданных датаграммных протоколов (UDP, IPsec и др.)
  — Произвольных IP-пакетов
— Доступ к терминальному оборудованию, находящемуся в любых типах сетей (Интернет, внутренние сети поставщиков услуг Интернет, сети сторонних организаций) с любыми IP-адресами (глобальными или приватными через NAT, динамическими или статическими).
— Установление прикладных сеансов обмена данными (как TCP, так и датаграммных) по инициативе любой из сторон.

Применительно к банковским решениям, поскольку все прикладные протоколы (NDC, DDC) работают поверх TCP, естественной архитектурой для решения поставленной задачи является TCP-прокси, или, иначе говоря, подставной хост. Банкомат устанавливает TCP-сессию, вместо реального процессингового сервера, к устройству NSG, расположенному в непосредственной близости от него (как правило, в самом банкомате). Это устройство играет роль *клиента ui*TCP и оснащается фиксированными и сменными интерфейсами в зависимости от используемых каналов связи.



Программное обеспечение клиентской части отвечает за выбор работоспособного канала (из нескольких возможных) и устанавливает следующую TCP-сессию с *сервером ui*TCP. Сервер ***ui*TCP** устанавливается непосредственно в процессинговом центре или в головном офисе банка — там, откуда уже можно гарантировать 100% доступ к процессинговому хосту. Он принимает входящие TCP-сессии от клиентов и устанавливает

заключительную сессию к хосту. Таким образом, данные прикладных протоколов передаются по эстафете из трёх TCP-сессий, где первая и третья проходят по гарантированно надёжной среде (например, по локальной сети), а бесперебойная работа второй обеспечивается собственно средствами ***ui*TCP**.

Помимо TCP-соединений, с которыми связано исторически сложившееся название технологии, ***ui*TCP** обеспечивает также бесперебойную передачу датаграммных протоколов 4 уровня, либо произвольных IP-пакетов. В частности, внутри туннеля ***ui*TCP** может находиться вложенный туннель, например, IPsec.

Механизм ***ui*TCP** способен работать через любые сети и каналы связи, с любыми IP-адресами клиента (статическими или динамическими, глобальными или приватными). Он универсально применим ко всем типам сетей, со всеми типами среды передачи и скоростями, которые поддерживаются маршрутизаторами NSG: ЛС Ethernet сторонних организаций, городские сети Fiber Ethernet, сотовые сети всех существующих в России стандартов (GSM, CDMA, 3G), коммутируемые телефонные линии, *x*DSL, E1 и др.

Дополнительные возможности ***ui*TCP** предусматривают:

— Прохождение любых типов и реализаций NAT как на выходе из сети поставщика услуг Интернет, так и на входе в сеть процессингового центра. Протокол TCP передаётся через NAT всегда (в отличие от, например, GRE или IPsec). Если поставщик услуг фильтрует трафик по определённым протоколам и портам TCP, то для работы ***ui*TCP** могут быть намеренно назначены как общеупотребительные номера портов TCP для стандартных служб (25, 80 и т.п.), так и уникальные специфические номера портов.

— NAT для локальных адресов на обеих сторонах. Принимая входящий сеанс обмена данными, отвечающая сторона ***ui*TCP** может инициировать следующую в цепочке сессию как с исходными IP-адресами и номерами портов, так и с изменёнными. На практике это означает, например, что при массовой инсталляции все банкоматы могут быть настроены совершенно одинаково, равно как и локальная сторона устройств NSG. Различение будет производиться уже на стороне сервера, где эти соединения сходятся в одну точку. Сервер различает входящие пакеты по уникальному имени клиента и может подставлять в них заданные IP-адрес источника, IP-адрес назначения и порт TCP назначения.

— Систему безопасности на основе SSL, функционально эквивалентную STunnel, HTTPS и другим методам защиты данных на 4 уровне, включающую в себя:
  — Асимметричное шифрование с длиной ключа до 2048 бит.
  — Взаимную аутентификацию сторон с использованием сертификатов X.509.

  Таким образом, ***ui*TCP** представляет собой полноценную фирменную VPN транспортного уровня, отличающуюся от других аналогичных решений (OpenVPN, KerioNet и т.п.) гарантированной доставкой пакетов.

— Горячее резервирование сервера. Клиентам могут быть указаны не только резервные каналы связи, но и резервные сервера, которые могут располагаться совершенно в других сетях и помещениях, нежели основной. Более того, система предусматривает механизм принудительного "мягкого" перевода клиентов на другой сервер по мере завершения текущих транзакций. После того, как все клиенты ушли с сервера, он может быть безопасно остановлен.

— Агрегирование нескольких каналов связи в одно соединение с увеличенной пропускной способностью.

— Централизованный мониторинг и управление клиентскими устройствами ***ui*TCP**, в т.ч. автоматизированный сбор статистики, обновление программного обеспечения, обновление сертификатов.

— Web-управление (HTTP или HTTPS) и мониторинг текущего состояния каналов. Сервер системы оснащён Web-интерфейсом, с помощью которого дежурный оператор в банке или процессинговом центре имеет возможность наблюдать текущее состояние клиентов, статистику их работы, распределение активности между основным и резервным(и) каналами связи, установленные TCP-сессии и т.п. Он также может рестартовать отдельные интерфейсы или клиентское устройство целиком, обновлять их программное обеспечение и т.п.

— Web-интерфейс для настройки ***ui*TCP**. При наличии установленного туннеля через Web-интерфейс сервера может осуществляться также настройка клиента.

— Вывод журнала с различной степенью детализации в локальный файл или в SQL-совместимую базу данных.

— Встроенное управление клиентами посредством SMS при отсутствии других каналов связи.

— Интеграцию с технологическим окружением банкомата: датчиками охраны, системами электропитания, сигнализации, климат-контроля и т.п.

Программный комплекс ***ui*TCP** работает на всех продуктах NSG под управлением NSG Linux. В качестве клиентского устройства, а также в качестве сервера в небольших системах и опытных инсталляциях (до 30 клиентов) рекомендуется использовать, как правило, устройства NSG–700. Для построения крупномасштабных систем применяются высокопроизводительные коммуникационные шлюзы NSG–1000/GW.

ООО "Эн-Эс-Джи"
Россия 105187 Москва
ул. Кирпичная, д.39, офис 1302
Тел.: (+7–495) 918–32–11
Факс: (+7–495) 918–27–39

http://www.nsg.ru/
mailto:info@nsg.net.ru
mailto:sales@nsg.net.ru
mailto:support@nsg.net.ru