Бесперебойный TCP-канал: универсальное решение

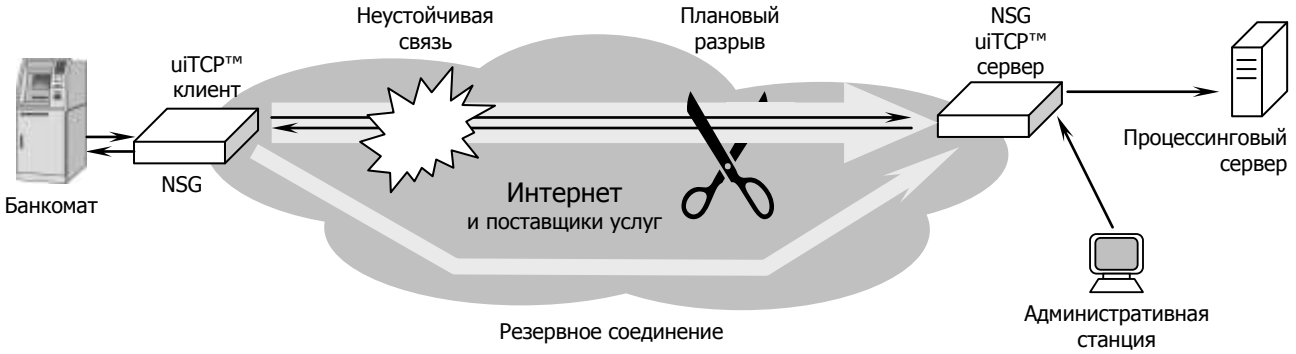
Надёжные каналы связи — обязательная компонента для системы автоматизации банковских услуг. Увы, с информационными магистралями в XXI веке дела в России обстоят немногим лучше, чем с проезжими дорогами во времена Гоголя — и уже едва ли когда-либо в этой жизни будет по-другому. Поэтому для выживания в этой стране нужны особые подходы и особые инструменты. Вместо того, чтобы асфальтировать автодороги, в России сконструировали автомобиль "Нива"; для езды по информационному бездорожью — системы резервирования каналов связи, позволяющие выбрать из нескольких доступных каналов один, наименее плохой в данный момент времени, и переключаться между ними таким образом, чтобы это не сказывалось на работе пользователя.

Компания NSG, будучи старейшим российским разработчиком сетевого оборудования (корни этих разработок уходят ещё во времена СССР и СЭВ), по логике самой жизни не могла игнорировать насущное требование российской действительности — идти своим путём, непохожим на мировой. Новая разработка NSG — фирменная технология бесперебойных соединений, *uiTCP*™ (Un-Interruptible TCP), предназначена для прозрачного резервирования каналов связи в банковских (и не только) системах.

Специфическая особенность банковских сетевых решений состоит в необходимости бесперебойного функционирования протоколов прикладного уровня (как специфических — NDC, DDC, так и общеупотребительных — HTTPS, MS RDP, Citrix ISA). Все они работают, в свою очередь, поверх протокола TCP. Таким образом, естественная архитектура для решения поставленной задачи — это 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 может оснащаться широким ассортиментом фиксированных и сменных портов для различной среды передачи. Более того, резервирование может осуществляться в рамках одного интерфейсного модуля GSM или 3G с двумя SIM-картами различных операторов, или путём выбора между пакетным (GPRS) или канальным (CSD, он же GSM data) режимом передачи данных.

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.



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 стандартов (GSM, CDMA, 3G), коммутируемые модемные линии , *x*DSL, E1 и др.

Столь же всеяден *ui*TCP и по отношению к клиентской стороне. Он одинаково пригоден для подключения банкоматов IP-over-Ethernet и X.25, киосков самообслуживания с протоколом IP-over-PPP, POS-терминалов без встроенных сетевых протоколов, пользовательских ПК и т.п. При этом на удалённой площадке может располагаться как одно устройство, так и целый офис, батарея POS-терминалов, или локальный модемный пул.

Помимо TCP-соединений, с которыми связано исторически сложившееся название технологии, *ui*TCP обеспечивает также бесперебойную передачу датаграммных протоколов 4 уровня, либо произвольных IP-пакетов.

Однако 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 теперь все они собраны в единое решение и работают прозрачно для пользователя.

Основные функции и механизмы *ui*TCP включают:

— 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 CSD 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 неактивности пользователя.

— 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

— Доступность терминального оборудования, находящегося 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.

Дополнительные возможности, предоставляемые ***ui*TCP**, включают:

— 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 назначать им заданные IP-адрес источника, IP-адрес назначения и порт TCP назначения.

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

— 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 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.

Программный комплекс *ui*TCP работает на всех продуктах NSG под управлением NSG Linux. В частности, для построения крупномасштабных систем используются 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