Решения для поставщиков услуг Интернет на основе продуктов NSG

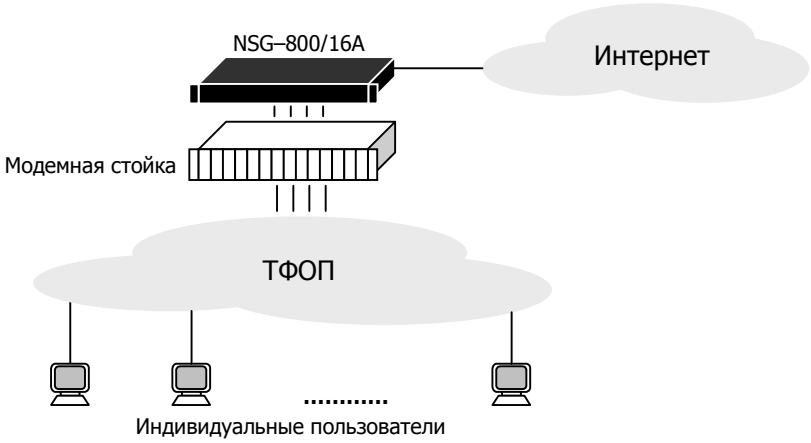
Компания NSG является крупнейшим российским производителем оборудования для сетей IP, Frame Relay и X.25. Модульные мультипротокольные маршрутизаторы NSG могут эффективно использоваться в сетях различного типа и назначения, в том числе для предоставления услуг Интернет и удаленного доступа в корпоративные сети. Следует сразу оговориться, что данная статья посвящена исключительно услугам сеансового доступа для индивидуальных пользователей на основе коммутируемых телефонных линий или PPPoE. Применение аппаратуры NSG для высокоскоростного доступа в Интернет и предоставления услуг корпоративным пользователям будет рассмотрено в отдельной статье.

Модемный доступ

Классический доступ в Интернет по коммутируемым телефонным линиям — технология устоявшаяся и хорошо известная, поэтому здесь трудно предложить что-либо существенно новое. Основные продукты NSG для таких применений — серверы асинхронного доступа NSG–800/16A и NSG–900/16A, выпускаемые в 16- и 8-портовых конфигурациях. Помимо асинхронных портов RS–232, эти модели имеют также встроенный порт Fast Ethernet и два разъема расширения; сменные интерфейсные модули позволяют подключать их к глобальным сетям с различной средой передачи.

Сервер асинхронного доступа NSG–800/16A (внизу) и универсальный маршрутизатор NSG–800/4WL

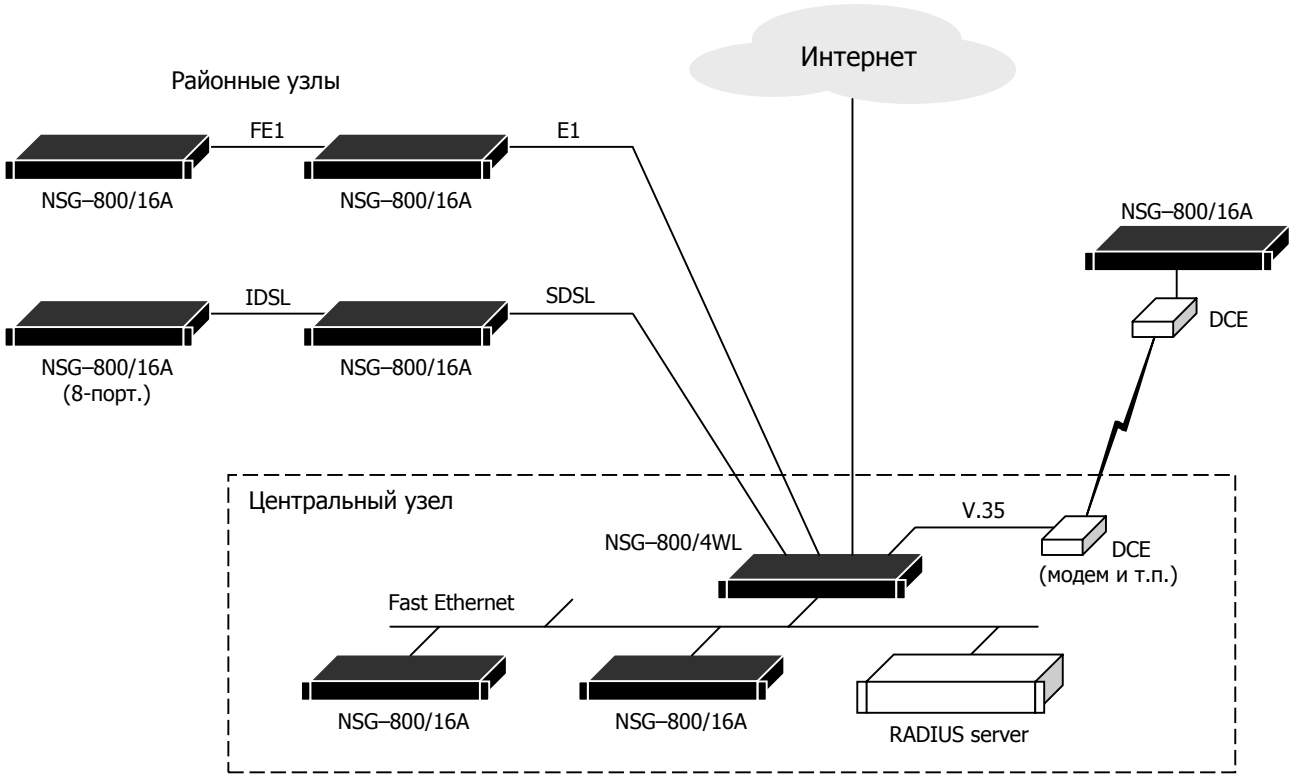
Одна из особенностей национальных коммуникаций в России и странах СНГ состоит в том, что модемный доступ по протоколам V.34 и даже ниже будет, по всей вероятности, оставаться наиболее реалистичным вариантом для большинства пользователей в сколько-либо обозримом будущем. Большие расстояния, дефицитные и низкокачественные линии связи, архаичное оборудование АТС, низкая плотность пользователей и их еще более низкая платежеспособность, инертность местных телефонных сетей в сочетании с их фактической монополией — неотъемлемые черты евразийской телекоммуникационной среды.



Классическая система модемного доступа на основе NSG–800/16A

Именно этим особенностям вполне отвечают NSG–800/16A и NSG–900/16A. На основе этих устройств — как и все продукты NSG, весьма недорогих по сравнению с именитыми зарубежными аналогами — можно эффективно строить небольшие удаленные узлы доступа в районных городах и в сельской местности. Следует отметить также, что программные возможности устройств NSG–800, NX–300, NSG–500 и NPS–7e полностью совпадают, и при необходимости можно достичь еще более значительной экономии, используя устройства младших серий с меньшим числом портов и меньшей производительностью.

Устройство NSG может подключаться как непосредственно к локальной сети поставщика услуг, так и к глобальным сетям с использованием различных технологий и протоколов. Широкий выбор интерфейсов WAN и гибкое программное обеспечение предоставляют большую свободу в выборе магистрального подключения: по физическим линиям xDSL, каналам E1 (в режимах *framed* и *unframed*, NTU и *drop-and-insert*), или с помощью разнообразной аппаратуры физического уровня со стандартными последовательными интерфейсами (V.35 и др.) — в зависимости от того, какой из способов доступен в данной местности.



Территориально-распределенная система доступа

Немаловажно и то, что устройства NSG представляют собой, по существу, единый продукт, эволюционно развивавшийся на протяжении многих лет. Благодаря этому они уже переболели всеми "детскими болезнями", неизбежными для любого нового продукта, и обладают высокой надежностью и устойчивостью работы. В сочетании со средствами удаленного управления — Telnet или SNMP (а для NSG–800/16A — также Web в сети IP или удаленная консоль в сети Frame Relay) — это позволяет эффективно использовать устройства NSG на удаленных необслуживаемых площадках. Таким образом, модемные серверы NSG идеально подходит для построения распределенных систем доступа в Интернет, охватывающих обширные территории с низкой плотностью абонентов.

Что касается пользовательской стороны узла доступа, то устройства NSG–800/16A и NSG–900/16A оснащены стандартными портами RS–232 (число которых может быть доведено до 18 за счет разъемов расширения) и могут работать в сочетании с любыми типами модемов и модемных стоек. Последнее существенно для российских условий, поскольку каждая телефонная линия плоха по-своему: в одной большое затухание, в другой — уровень шумов, в третьей — нестабильность параметров, и т.п. Поставщик услуг Интернет может самостоятельно выбирать тот тип модемов, который наиболее надежно работает на линиях, данных ему богом и местной телефонной сетью. Свободные порты WAN и Ethernet могут быть использованы для подключения удаленных узлов "цепочкой", построения резервных периферийных каналов связи между узлами, или постоянного подключения привелигированных пользователей (местных организаций и учреждений, пунктов коллективного доступа, Интернет-кафе и т.п.)

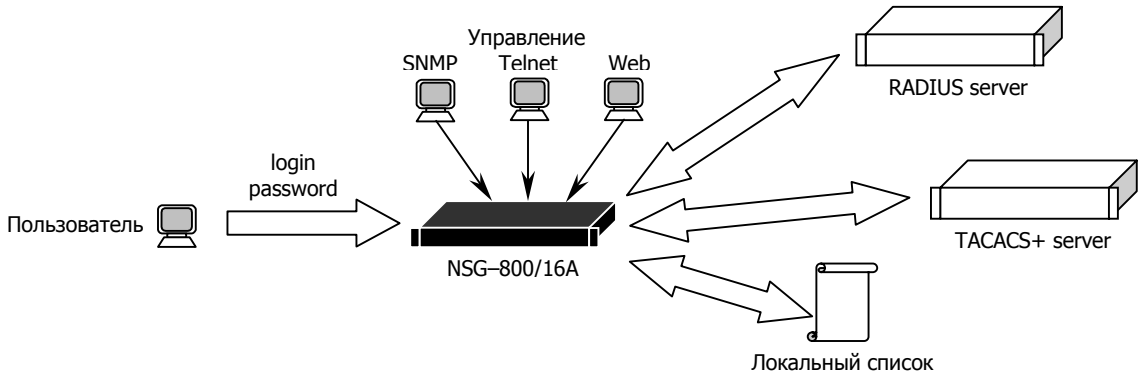
Устройство NSG–900/16A, по сравнению со своим аналогом из 800-й серии, представляет собой новое поколение продуктов NSG, работающее под управлением программного обеспечения NSG Linux. Оно предоставляет дополнительные возможности для построения современных IP-сетей, такие как VPN, QoS, расширенный набор протоколов динамической маршрутизации. Кроме того, Cisco-подобный командный интерфейс, привычный многим системным администраторам, делает работу с ним более комфортной.

Аутентификация пользователей

Функции AAA (аутентификация, авторизация пользователей и учет потребляемых услуг) — принципиально важные аспекты работы сервис-провайдера, поскольку служат основой для расчетов за услуги. В устройствах NSG они могут производиться различными способами, в зависимости от предпочтений и потребностей оператора.

Простейший способ аутентификации пользователя — терминальный режим, при котором пользователь должен ввести имя и пароль непосредственно после установления модемного соединения. Более современный и безопасный способ — аутентификация на этапе установления PPP-соединения при помощи протоколов PAP и/или CHAP. При необходимости можно использовать и оба способа одновременно.

Источником аутентификации и авторизации пользователей может быть как локальный список, так и удаленные сервера RADIUS или TACACS+[1]. При работе с централизованными серверами AAA устройство NSG посылает им также статистику работы пользователей. Централизованная служба AAA совершенно необходима в распределенных системах доступа, описанных выше.



Средства аутентификации и управления работой пользователей

Одновременно с аутентификацией пользователя сервер может установить для него дополнительные атрибуты, такие как IP-адрес, максимальная продолжительность сеанса, набор фильтров и т.п. В ходе установления PPP-соединения устройство NSG может назначать пользователю параметры IP, такие как динамический IP-адрес (полученный от сервера или заданный локально для данного пользователя или интерфейса) и адреса серверов DNS.

Аутентификация с использованием PAP/CHAP работает одинаковым образом для всех способов сеансового доступа — как модемного, так и на основе PPPoE. Аутентификация в терминальном режиме[1] возможна, по определению, только при модемном подключении, и предоставляет дополнительные возможности. Пользователю может быть предоставлен как сервис PPP, так и сервис X.25 PAD. При локальной аутентификации выбор сервиса осуществляется по суффиксу в имени пользователя, при централизованной — согласно настройкам, указанным в учетной записи пользователя на сервере RADIUS/TACACS+. Такая динамическая авторизация может быть использована для предоставления дополнительных услуг, рассмотренных ниже.

Для учета работы пользователей можно использовать различные приложения, например, биллинговую систему UTM 4.0 и старше компании NetUP (http://www.netup.ru/) Сеанс работы пользователя может быть принудительно разорван администратором или управляющим приложением при помощи Telnet, SNMP или Web-интерфейса[1].

Динамические фильтры и гостевой вход

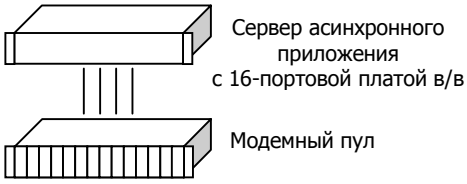
В серверах доступа NSG реализована поддержка IP-фильтров, включаемых индивидуально для каждого пользовательского сеанса[1]. Если в ответе сервера авторизации содержатся атрибуты *Filter-Id* (RADIUS) либо *inacl, outacl* (TACACS+), то для данного пользователя будет активирована указанный фильтр или группа фильтров. После завершения сеанса эти фильтры удаляются.

Механизм динамически включаемых фильтров позволяет ограничить права заданной категории пользователей, например, возможность доступа к платному контенту. Одна из наиболее повсеместных задач подобного рода — это организация гостевого входа, позволяющего анонимному пользователю зайти на сервер регистрации (и никуда более!), чтобы зарегистрироваться и активировать платежную карту.

Реализация динамических фильтров в устройствах NSG в высокой степени совместима с реализациями других производителей. Это позволяет, в частности, устанавливать серверы NSG в существующие системы доступа, никак не изменяя при этом настройки серверов авторизации и имеющихся серверов доступа.

[1] В настоящее время поддерживается только в NSG–800 и младших сериях.

Доступ к Интернет и архаичным приложениям

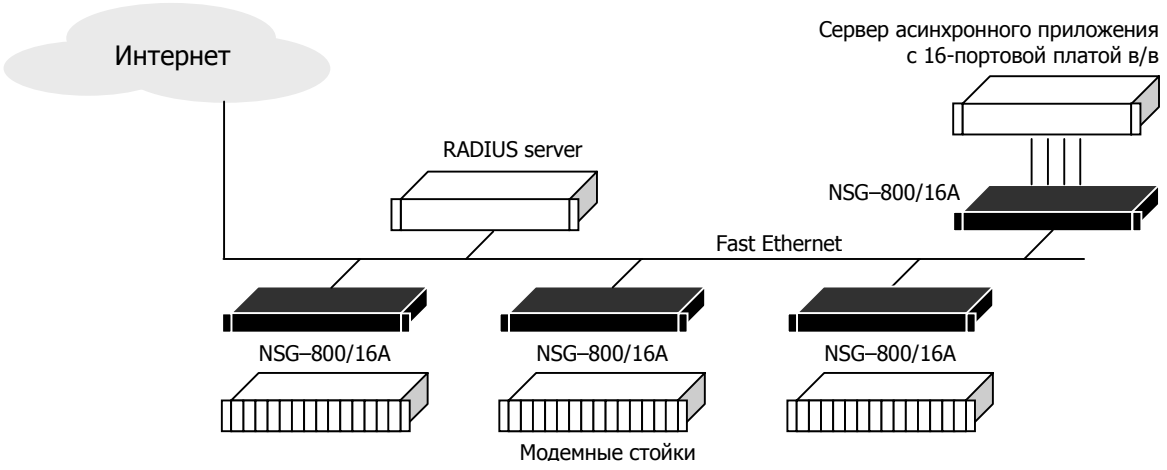


Исходная конфигурация
унаследованного приложения

Функция динамической конфигурации портов в режиме PPP либо PAD, поддерживаемая устройствами NSG–800 и младших серий, предназначена отнюдь не только для доступа в публичные сети X.25. Конфигурация в режиме PAD придает порту определенный "интеллект". Простой асинхронный порт является "тупым", т.е. прозрачно пропускает через себя весь трафик; понятие *сеанса* для него принципиально не определено. Порт типа PAD, напротив, работает в сеансовом режиме и позволяет устанавливать и разрывать сетевые соединения как в ручном, так и в автоматическом режиме. Эта возможность может быть использована для подключения к приложениям, ориентированным на работу через физический последовательный порт или Telnet. Примерами таких приложений являются услуги UUCP, FIDO, BBS, некоторые корпоративные системы.

Пусть пользователю с именем *pppupkin* необходимо предоставить доступ к Интернет, а пользователю с именем *uuurupin* — например, к UUCP-почте. Будем считать, что исходная конфигурация архаичной системы — это сервер с мультипортовой платой ввода-вывода. Чтобы обеспечить доступ через один и тот же модемный пул как к услугам Интернет, так и к этому серверу, порты модемных серверов конфигурируются для аутентификации в терминальном режиме. Сервер приложения подключается к аналогичному устройству NSG–800/16A, работающему в режиме PAD-концентратора.

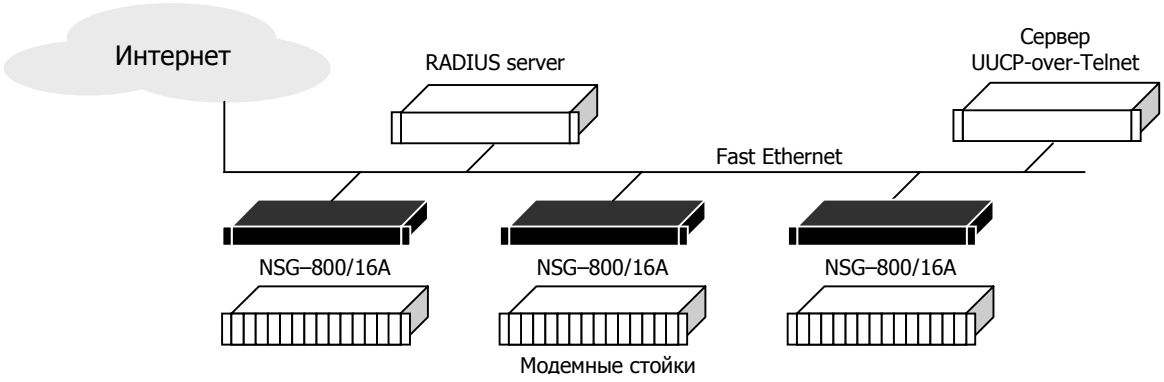
Если очередному пользователю назначена услуга PPP, то порт принимает тип PPP и пользователь получает доступ к Интернет (или корпоративной интрасети) обычным образом. Если же ему назначена услуга PAD, то порт принимает тип PAD и автоматически устанавливает соединение X.25 со свободным портом PAD-концентратора; обоим PAD-ам назначается прозрачный профиль. Таким образом, пользователь оказывается прозрачно подключен к порту сервера. Соединение может устанавливаться через синхронные порты, глобальную сеть X.25 (в т.ч. наложенной на ту же транспортную инфраструктуру Frame Relay или TCP/IP), или локальную сеть Ethernet при помощи фирменной технологии X.25-over-Ethernet.



Система с доступом к Интернет либо к унаследованному приложению
(в зависимости от имени пользователя)

Другая протокольная реализация (с такой же аппаратной конфигурацией) состоит в том, что порт PAD автоматически устанавливает соединение с локальным Telnet-клиентом на этом же устройстве. Клиент Telnet так же автоматически устанавливает соединение с устройством NSG–800/16A, подключенным к прикладному серверу. Это устройство сконфигурировано в качестве сервера Reverse Telnet и обеспечивает проключение трафика на асинхронные порты. Как клиент, так и сервер Telnet работают в прозрачном режиме. Таким образом, пользователь *uuurupin* снова оказывается прозрачно подключен к одному из портов архаичного сервера. В отличие от предыдущего решения, данный вариант реализован почти полностью на основе IP-транспорта — сеть X.25 оказывается ограничена рамками одного модемного сервера. Такое решение более удобно для WAN-систем, построенных без использования других протоколов.

Наконец, если архаичное приложение позволяет использовать транспорт Telnet вместо физических портов, т.е. может быть сконфигурировано для работы в качестве Telnet-сервера, то выделенный сервер Reverse Telnet в последней конфигурации оказывается излишним. Клиенты Telnet с модемных серверов могут устанавливать соединения непосредственно с прикладным сервером. Такое решение возможно, в частности, для одного из самых распространенных архаичных приложений — UUCP-почты.



Система с доступом к Интернет либо к UUCP-почте через Telnet

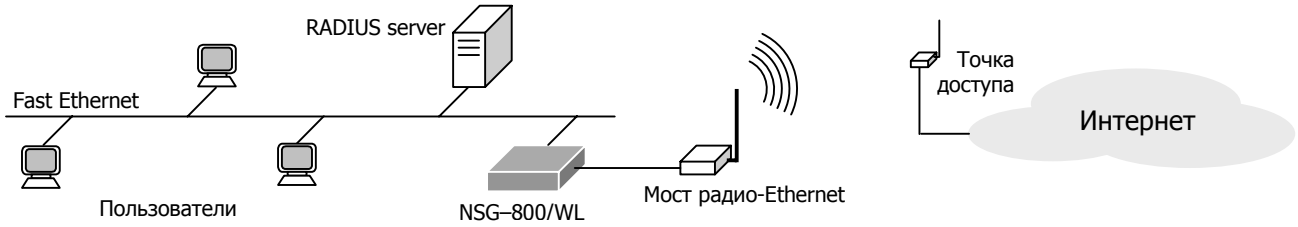
Если пользователю, подключенному в режиме PAD, следует предоставить несколько архаичных услуг по его выбору, то порт конфигурируется без автоматического установления соединения X.25. Пользователь должен ввести номер одного из пунктов меню (1, 2, ...) который одновременно является адресом X.121. Фактически он отправляет вызов по этому адресу, который маршрутизируется на соответствующий прикладной сервер или сервер Telnet.

Сеансовый доступ в локальных сетях

Системы индивидуального доступа на основе технологии PPP-over-Ethernet (PPPoE) позволяют организовать сеансовое подключение пользователей в локальных сетях жилых домов, гостиниц, офисных центров для мелких арендаторов, и т.п. Аутентификация пользователей обеспечивает индивидуальный учет и оплату потребляемых услуг для каждого пользователя.

Оптимальную аппаратную конфигурацию для такого применения имеют маршрутизаторы NSG–800/WL и NSG–900/2WL, оснащенные одним портом Fast Ethernet и одним или двумя разъемами расширения. Как и остальные продукты NSG, при помощи сменных интерфейсных модулей они могут подключаться к вышестоящему оператору по различным типам транспортной среды, включая аппаратуру DCE со стандартными последовательными интерфейсами, физические линии, каналы E1 (структурированные и неструктурированные), а также широкополосные системы местного доступа, построенные на основе технологии Ethernet или оснащенные интерфейсами Ethernet. В частности, это могут быть радиомосты для подключения к городским сетям Ethernet, внешние модемы xDSL, кабельные модемы, волоконно-оптические системы, оптические мосты прямой видимости и т.п.

Устройство NSG–800/WL — оптимальная модель для сервера PPPoE



Система доступа на основе PPPoE с широкополосным подключением к вышестоящему оператору

Возможна также конфигурация, при которой устройство NSG подключено только единственным портом к локальной сети Fast Ethernet и служит для аутентификации пользователей и учета потребляемых услуг. Пользовательский трафик направляется обратно через эту же сеть на другой маршрутизатор, служащий шлюзом в глобальную сеть. (При этом непосредственная работа пользователей через выходной маршрутизатор запрещена на уровне IP- или MAC-адресов.) Такая конфигурация представляет, в основном, академический интерес, но может быть востребована в некоторых ситуациях.

Устройство конфигурируется для работы в режиме сервера PPPoE и обслуживает клиентов, находящихся в той же локальной сети. Аутентификация пользователей выполняется на этапе установления PPP-соединения при помощи протоколов PAP и/или CHAP, локально или на удаленном сервере RADIUS, TACACS+. Эти же удаленные сервера назначают атрибуты сеанса PPP и осуществляют учет услуг. Таким образом, работа клиента в этой сети происходит в основном аналогично модемному подключению; такой тип сетей называется виртуальными сетями коммутируемого доступа (*virtual private dial-up networks*, VPDN).

ООО "Эн-Эс-Джи"
Россия 105187 Москва
ул. Кирпичная, д.39, офис 1302
Тел.: (+7–095) 918–32–11
Факс: (+7–095) 918–27–39

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