Маршрутизаторы NSG

Программное обеспечение NSG Linux 2.0

Руководство пользователя

Часть 2

Настройка физических интерфейсов, портов и сетевых интерфейсов

Обработка трафика Ethernet

Версия программного обеспечения 2.0 build 7

Обновлено 18.04.2017

Москва 2017

АННОТАЦИЯ

Данный документ содержит руководство по настройке и применению маршрутизаторов NSG, оснащенных программным обеспечением NSG Linux 2.0. Документ имеет следующую структуру:

Руководства по применению маршрутизаторов под управлением NSG Linux 1.0 и базового программного обеспечения NSG, а также других продуктов NSG (модемов, мостов и т.п.), содержатся в отдельных документах.

ВНИМАНИЕ

Данное Руководство пользователя предназначено для лучшего понимания процедуры настройки в целом и описывает сущность выполняемых действий — а именно, *что* необходимо настраивать. Рассматриваемые вопросы относятся, как правило, к сущности используемой технологии и являются общими для любых её реализаций, независимо от конкретного производителя и устройства. (Исключением являются вопросы, специфичные для оборудования NSG — таких, как организация пользовательского интерфейса или настройка системы бесперебойных соединений ***ui*TCP**.)

Основной документацией по NSG Linux 2.0 является встроенная справка на борту устройства. Она описывает конкретные команды и параметры настройки — т.е. *как* настраивать функции и возможности, описанные в данном Руководстве. Для просмотра справки по каждому из параметров следует использовать кнопку в Web-интерфейсе или команду _manual (_m) в консольном интерфейсе. Если справка на вашем языке отсутствует, следует установить на устройстве русскую локаль.

ВНИМАНИЕ Продукция компании непрерывно совершенствуется, в связи с чем возможны изменения отдельных аппаратных и программных характеристик по сравнению с настоящим описанием. Сведения о последних изменениях приведены в файлах README.TXT, CHANGES, а также в документации на отдельные устройства.

Замечания и комментарии по документации NSG принимаются по адресу: doc@nsg.net.ru.

ООО «Эн–Эс–Джи»
Россия 105187 Москва
ул. Вольная, д.35
Тел./факс: (+7–495) 727–19–59 (многоканальный)

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

§ СОДЕРЖАНИЕ §

Часть 2. Настройка физических интерфейсов, портов и сетевых интерфейсов

§2.1. Общие сведения о физических интерфейсах, портах и сетевых интерфейсах

§2.1.1. Архитектура объектов 1–3 уровней

В программном обеспечении NSG Linux 2.0 принята следующая терминология и обозначения:

Портом называется программный объект, осуществляющий обработку протоколов младших уровней протокольного стека, в большинстве случаев — физического уровня (Ethernet PHY, RS–232 и т.п.), канального уровня (PPP, Ethernet и др.) и уровня межсетевого взаимодействия (IP). Отдельные типы портов осуществляют обработку неструктурированного трафика вплоть до прикладного уровня (инкапсуляция reverse-telnet, raw-tcp) или работают вообще вне сетевого стека (sms-handler, one-wire). Настройка всех портов производится в узле .port и далее по имени порта.

По существу, порт включает в себя компоненты нескольких протокольных уровней, от физического и выше — до того уровня, который подразумевает обработку пакетов между несколькими портами. Настройки всех этих компонент внесены в состав порта, чтобы не плодить в системе лишние объекты. По этой причине термины "интерфейс" и "порт" в NSG Linux 2.0 можно считать равнозначными.

Физическим интерфейсом называется объект первого уровня модели OSI, непосредственно взаимодействующий с аппаратным приёмопередатчиком. В NSG Linux 2.0 поддерживаются только простые физические интерфейсы, не предусматривающие разделение данных на физическом уровне. Каждому из таких интерфейсов соответствует один и только один протокольный порт. Физические интерфейсы могут быть встроены в шасси или реализованы в виде сменных модулей и карт. На шасси или карте может быть один или несколько физических интерфейсов. Имена интерфейсов на шасси фиксированы, на сменных картах совпадают с именем разъёма расширения (например, s1) или формируются автоматически из имени карты и номера интерфейса на ней (например, для 2-портовой карты — c1-1 и c1-2).

Инкапсуляция определяет протокол передачи данных канального уровня. В зависимости от выбранной инкапсуляции в меню порта появляются узлы и параметры, специфичные для выбранного протокола.

Если протокол канального уровня предусматривает разделение на виртуальные дочерние объекты, то они обозначаются по схеме имя_порта.номер_суб-порта, например, vlan eth0.101; порты с другими типами инкапсуляции не предполагают разделения на дочерние объекты. На практике это относится только к портам Ethernet, а также другим Ethernet-подобным объектам. Для каждой VLAN создаётся свой IP-интерфейс, настраиваемый и функционирующий независимо от остальных.

Сетевым интерфейсом называется объект, осуществляющий обработку протокола IP. В командном дереве NSG Linux 2.0 сетевые интерфейсы являются составной частью портов. Соответственно, в меню каждого порта, предназначенного для передачи данных по сети, имеются настройки сетевого интерфейса, т.е. IP и вышестоящих протокольных уровней. Если выбранный тип инкапсуляции на порту не предусматривает передачу IP-трафика, то сетевой интерфейс над ним не создаётся и параметры IP в его меню отсутствуют.

Основная задача NSG Linux 2.0 состоит в обработке пакетов на 3 уровне, т.е. уровне межсетевого взаимодействия. На этом уровне осуществляется обычная IP-маршрутизация пакетов по адресу назначения, маршрутизация по расширенному набору параметров (адресу источника, протоколам, номерам портов и т.п.), фильтрация, преобразование сетевых адресов и портов (NAT), большинство функций туннелирования и т.п. Как частный случай, устройство NSG может выступать в отдельных задачах в качестве конечного хоста и терминировать трафик прикладного уровня (например, Telnet) на себя. Настройка IP-маршрутизации, служб IP и VPN описана в Частях 3–6 данного документа.

Имена портов и интерфейсов. Поскольку вся совокупность настроек 1–3 (а для определённых типов портов и более высоких) уровней рассматривается в NSG Linux 2.0 как один цельный объект, то имя сетевого интерфейса, как правило, совпадает с именем порта и физического интерфейса. Однако в отдельных случаях имя IP-интерфейса, назначаемое системой, может не совпадать с именем порта, и переделывать эти правила именования нецелесообразно — например, сетевой интерфейс ppp1 и порт 3g. В пределах командных оболочек NSG Linux 2.0 (nsgsh, Web) такие имена являются синонимами и разрешаются друг в друга автоматически, поэтому при необходимости (например, в настройках фильтров) можно указывать любое из них.

Явным образом определить имя сетевого интерфейса, динамически назначенного системой заданному порту, можно при помощи команды .system.get-iface-name.*имя_порта* . Это может потребоваться, например, для использования в скриптах ОС Linux вне командных оболочек NSG, например:

```
ip route add 1.2.3.4/32 dev ${nsgsh -q .system.get-iface-name.m1}
```

Данная специальная команда не предназначена для работы в интерактивном режиме и по этой причине не вынесена в меню командных оболочек NSG. В интерактивном режиме выяснить имя интерфейса можно с помощью команды show в меню порта.

§2.1.2. Идентификация сменных интерфейсных карт, опций и USB-устройств

Если в устройстве имеются разъёмы расширения для сменных интерфейсных модулей, то в меню им соответствуют узлы с именами вида .port.s1 и т.п. Для фиксированных опций, устанавливаемых в заводских условиях, используются обозначения вида .port.m1 и т.п. Указать тип модуля или опции, установленного в данный разъём, можно двумя способами:

— Выбрать тип вручную из списка type .
— Выполнить автоматическое определение с помощью разовой команды update , если оно возможно для данного типа модуля.

Аналогичным образом устанавливается тип внешнего устройства USB, подключённого к фиксированному порту USB (.port.usb*N*) или к разъёму расширения, в который вставлен адаптер UM–USB.

В данной версии NSG Linux 2.0 поддерживаются следующие типы интерфейсных модулей и внешних устройств:

Модуль или устройство	Обозначение	Автоопределение	Примечание
UM–LTE/3G opt18xx.LTE/3G	lte	да	Sierra Wireless MC7710
UM–EVDO/A *v7* opt18xx.CDMA	cdma	да	ATEL EP45
UM–EVDO/A *v5*	cdma	да	CMOTech CNE–680
UIM–CDMA *v2*, UIM–EVDO *v2*	cdma	да	CMOTech CNE–510/550
UM–3G *v6* opt18xx.3G	3g	да	Fibocom H330
UIM–3G *v1*, UM–3G *v2, v3, v5, v6*	3g	да	SimCom SIM5210, 5216, 5320
UIM–EDGE *v3a*	edge-3a	да	SimCom SIM700, в зависимости от прошивки
UIM–EDGE *v3*	edge	да	
UM–WiFi *v1, v2* opt18xx.WiFi *v1, v2*	wifi	да	
UM–2V24A	2com	да	Создаются 2 порта
UM–ET100 *v1, 3*, ME–Eth	eth	да	
UM–ETH703, ME–2M	eth-703	да	
IM–GPRS (все версии) IM–CDMA *v1,3* IM–EDGE *v1,2* IM–V35–2 (только асинхр. режим) IM–V24A IM–V34, IM–V92	rs-232	нет	Wavecom/PIML/FLYFOT AnyDATA.NET SimCom SIM600
USB Flash, HDD	storage	да	
Принтеры с поддержкой HP JetDirect	printer	да	
Сенсорный блок NSG MS–6	multisensor	да	
Адаптеры USB/RS–232	rs-232	да	Любые на чипах Prolific и FTDI
Адаптеры USB/Ethernet 10/100	eth	да	По заказу
Адаптер USB/RS–485 "Меркурий 230"	mercury	да	
Адаптер USB/RS–485 "Болид"	bolid	да	

Для двухпортовых карт серии ME–*xxx* (устройство NSG–1000e) каждый порт настраивается отдельно.

В зависимости от типа установленного модуля, в этом же узле появляются параметры, специфичные для данного модуля. Для модуля UM–2V24A (2 порта RS–232 async) создаются два дочерних узла с именами вида s1.0 и s1.1, настраиваемые независимо друг от друга.

ВНИМАНИЕ Сотовые модули устаревших модификаций, а также модемы для коммутируемых телефонных линий и другие модули, работающие только через асинхронный внутренний интерфейс (обозначения вида IM–*xxx*), необходимо определять только как rs-232 .

§2.1.3. Коммутаторы, мосты и туннели

Помимо поэтапной инкапсуляции и трансляции данных с верхних уровней протокольного стека в физическую среду передачи и обратно, на 1–2 уровнях может выполняться коммутация пакетов Ethernet между физическими портами, равнозначными им объектами (например, туннелями GRE с инкапсуляцией Ethernet), и/или отдельными VLAN на них. Коммутация Ethernet может производиться программно с помощью *bridge groups* или, на некоторых типах устройств (NSG–605, NSG–700, NSG–1800), с помощью встроенного управляемого коммутатора. *bridge group* подключается к вышестоящим уровням протокольного стека как один объект, содержащий внутри себя IP-интерфейс; аппаратный коммутатор — как один или несколько, в зависимости от настроек. Аналогичным образом функционирует *bond group* — объединение нескольких каналов Ethernet в одно соединение.

С точки зрения описанной выше архитектуры, *bridge group* и *bond group* работают как составные объекты 2 и 3 уровней, включающие в себя с верхней стороны IP-интерфейс. Снизу под ними, в отличие от простых портов, находятся одновременно несколько портов, от которых остаётся, по существу, только компонента 1 уровня — физический интерфейс.

Туннели 2 и 3 уровней (PPPoE, PPTP, GRE, IPsec, Open VPN, а также NSG *ui*TCP в определённых конфигурациях) функционируют аналогично физическим портам, но вместо физического уровня в них используется несущее соединение через публичную сеть. Сверху туннель заканчивается, в зависимости от типа и конфигурации, псевдо-портом 2 уровня (Ethernet) либо интерфейсом 3 уровня (IP) для передачи приватного трафика.

Названия туннелей, *bridge group* и *bond group* в NSG Linux 2.0 строятся по определённым шаблонам, например, br*N* или pppoe*N*. При создании нового объекта этих типов достаточно ввести его номер, нужный префикс будет добавлен автоматически. Имя интерфейса IP или Ethernet во всех случаях совпадает с именем объекта.

§2.1.4. Горячая замена USB-устройств

Для внешних устройств USB, а также для сменных интерфейсных карт серии ME–*xxx* (устройство NSG–1000e), допускается горячая замена (подключение и отключение "на ходу" без выключения устройства) в полуавтоматическом режиме. При этом:

— Если устройство отключается или карта извлекается из шасси, то связанные с ней порты и другие программные объекты автоматически переходят в DOWN. Существующая конфигурация при этом не изменяется.

— Если устройство подключается или карта вставляется в шасси, то для него может иметься сохранённая ранее конфигурация. Однако она не вступает в действие автоматически. Чтобы задействовать эту ветвь конфигурации, необходимо выполнить команду _apply или ▷ (либо перезагрузить устройство).

§2.2. Настройка портов Ethernet и Eth-over-something

§2.2.1. Идентификация портов, параметры физического и канального уровня

Порты Ethernet и Ethernet-over-something в устройствах NSG могут быть фиксированными (на шасси) или сменными на следующих интерфейсных модулях и картах NSG:

type = "eth"	Модуль UM–ET100 (*h/w ver.1* или *ver.3*) или одиночный порт на карте ME–Eth.
type = "eth-703"	Модуль UM–ETH703 или одиночный порт на карте ME–2M с аппаратной инкапсуляцией Ethernet-over-E12 (G.703.6).

Фиксированные порты (в т.ч. порты на PCI-картах) имеют имена eth0, eth1 и т.д. в зависимости от их числа на шасси. Одиночные сменные порты — s1, s2 и т.д. в зависимости от номера разъёма расширения. Порты на двухпортовых картах серии ME–*xxx* для устройства NSG–1000e имеют имена вида cX-Y, где X — номер слота расширения на шасси (от 1 до 8), Y — номер порта на карте (1 или 2), и настраиваются независимо друг от друга.

MAC-адрес фиксированного порта, по умолчанию, формируется автоматически из заводского номера устройства и номера порта. Модули UM–ET100 *h/w ver.3*, UM–ETH703 и карты ME–Eth также имеют собственный MAC-адрес.

В случае необходимости порту может быть принудительно назначен произвольный MAC-адрес в узле link. В большинстве случаев это не требуется и не рекомендуется, чтобы в одной сети случайно не оказалось двух устройств с одинаковыми адресами. Однако иногда это бывает необходимо, например, если устройство NSG устанавливается взамен какого-либо другого, и MAC-адрес старого устройства занесён в настройки сервера DHCP, систем контроля пользовательского доступа, фильтров и т.п.; таким образом, замена происходит прозрачно и не требует перенастройки других компонент системы.

ПРИМЕЧАНИЕ Модули UM–ET100 *h/w ver.1* не имеют собственного MAC-адреса. Необходимо назначить им уникальный MAC-адрес программно из диапазона 00:09:56:*xx*:*xx*:*xx* . Без этого модуль не перейдёт в состояние UP.

Для интерфейсов Ethernet ручная настройка скорости порта и режима Full/Half duplex в данной версии NSG Linux не предусмотрена по причине неактуальности; эти параметры успешно согласовываются автоматически встроенными средствами Ethernet-контроллера.

Для интерфейсов Ethernet-over-E12 (G.703.6) в меню порта присутствует специфический узел phy, предназначенный для настройки физического уровня G.703.6. В нём следует выбрать требуемый режим синхронизации (от внешнего сигнала или от внутреннего генератора), а также можно установить аппаратный шлейф для тестирования линии с удалённой стороны. Как правило, интерфейс устройства NSG является оконечным оборудованием сети PDH оператора связи и его передатчик синхронизируется от приёмника; приёмник во всех случаях синхронизируется от сети. Только если два устройства испытываются "на столе" и соединяются физическим кабелем, на одном из них (не важно, каком именно) необходимо установить режим синхронизации от внутреннего генератора (и не забыть вернуть его в исходное состояние перед установкой в реальную сеть).

§2.2.2. Параметры IP

Ключевым параметром для порта Ethernet является его IP-префикс, т.е. совокупность адреса данного порта и маски подсети. Вместе они определяют адресное пространство сети, в которую включён данный порт. Префикс записывается в формате A.B.C.D/M, где A.B.C.D — IP-адрес, а M — длина маски (количество бит, равных единице). Подробнее о структуре IP-адресов см. Часть 3. В частности, для наиболее часто используемых масок длина составляет:

255.0.0.0 — /8
255.255.255.0 — /24
255.255.255.252 — /30 (допустимо только для соединений "точка-точка")
255.255.255.255 — /32 (для интерфейсов Ethernet недопустимо)

Префикс настраивается в узле ifAddress.prefix внутри меню порта. При необходимости возможно присвоить порту вторичные IP-префиксы (*aliases*); чтобы создать новый префикс, нужно нажать на кнопку + или ввести команду _new в данном узле.

Специфическим для портов Ethernet в NSG Linux 2.0 является параметр configurable. Если он имеет значение no, то никакие изменения настроек данного порта не применяются и не сохраняются в конфигурации. Это специальный режим, используемый для технологических и отладочных целей; пользователям устанавливать его не следует, за исключением тех интерфейсов, на которых он установлен по умолчанию.

Другие адреса (peer, broadcast, anycast) используются только в отдельных специфических случаях и для большинства практических задач не требуются.

Если IP-адрес и другие параметры данному сетевому интерфейсу должны быть назначены по DCHP, то следует установить:

```
ifAddress.configurable = "dhcp"
```

Подробнее о настройке клиента DHCP см. Часть 4.

Другие параметры физического и канального уровней Ethernet содержатся в узле link; настройка этих параметров также требуется только в редких случаях. Чтобы просмотреть текущее состояние и статистику порта, следует выполнить команду show.

ПРИМЕЧАНИЕ Порты Ethernet на устройствах NSG–6*xx* и порты Ethernet, соединённые с встроенными коммутаторами устройств NSG–700, NSG–1800, всегда находятся в состоянии UP, вне зависимости от состояния подключённого кабеля. Это их конструктивная особенность, и ключевое слово UP в статусе порта в данном случае не имеет значения.

§2.2.3. Настройка VLAN

На портах Ethernet, а также на программных объектах, эквивалентных им, могут образовываться виртуальные сети — VLAN — согласно спецификации IEEE 802.1q. Каждая VLAN может являться сетевым интерфейсом маршрутизатора и иметь все атрибуты, присущие IP-интерфейсу (IP-адрес и т.п.), либо коммутироваться с другими Ethernet-обектами (портами, VLAN, туннелями GRE) посредством *bridge groups*. Имя VLAN образуется из номера родительского объекта и номера VLAN, например, eth0.101.

VLAN могут иметь номера от 1 до 4095. Номер VLAN 1 в программном обеспечении NSG Linux не является особым и может использоваться наравне с другими. Наряду с пакетами VLAN, на порту могут присутствовать обычные пакеты Ethernet без тегов VLAN; к этим пакетам применяются параметры IP, установленные в корневом узле меню порта. Автоматическое преобразование нетегированных пакетов во VLAN 1 не производится.

VLAN могут быть вложенными, т.е. внутри одной VLAN также могут создаваться VLAN следующего уровня, и т.п. — так называемые *cascaded* VLAN, или Q-in-Q. В этом случае они именуются последовательно через точку, например, eth0.101.203.16. Это означает, что в заголовок Ethernet пакета последовательно добавляются теги 16, 203 и 101. С точки зрения простого VLAN-коммутатора, не поддерживающего Q-in-Q, такой пакет принадлежит к VLAN 101.

Число уровней вложенности VLAN программно не ограничено, но необходимо учитывать, что каждый следующий тег увеличивает длину пакета на 4 байта. Стандартные электронные компоненты Ethernet обрабатывают пакеты длиной до 1518 байт. Большинство современного оборудования гарантирует поддержку одноуровневых VLAN — с длиной пакета до 1522 байт. Более длинные пакеты могут не проходить через отдельные порты отдельных экземпляров оборудования, имеющегося в сети (как NSG, так и других производителей); в случае крайней необходимости, использование вложенных VLAN на таких портах возможно, но требует уменьшения длины пакета (параметры MTU, MSS и т.п.)

§2.2.4. Настройка приоритетов IEEE 802.1p

Тег VLAN, помимо идентификатора, может содержать значение приоритета пакета. Функционально данное поле аналогично полю ToS/DiffServ в заголовке IP, но применяется на втором уровне в пределах данной сети Ethernet. При обработке пакета в маршрутизаторе заголовок Ethernet отбрасывается на входе и заново составляется на выходе; приоритет 802.1p при этом сохраняется отдельно в виде внутреннего атрибута, действительного в пределах данного маршрутизатора.

ПРИМЕЧАНИЕ В данной версии NSG Linux внутренний приоритет не учитывается при обработке пакета с помощью *iptables*. Он может либо передаваться прозрачно с входа на выход, либо устанавливаться принудительно в соответствии с какими-либо другими критериями.

Приоритет 802.1p может принимать значения от 0 до 7 (0 — наивысший). Внутренний приоритет может задаваться в формате 4-байтового числа (от 0 до 4294967295), или пары 2-байтовых (от 0 до 65535), где первое число означает номер очереди, второе — номер класса в этой очереди. Соответственно, на входе и на выходе может производиться преобразование одного приоритета в другой по заданным правилам. Правила устанавливаются в узлах in-CoS2Class-map, out-Class2CoS-map, соответственно.

Для входящих пакетов в узле in-CoS2Class-map можно создать до 8 элементов с именами 0…7, соответствующих приоритетам 802.1p на входе. Значением каждого параметра является внутренний приоритет, который должен быть установлен данному пакету (в любом из двух форматов).

Для исходящих пакетов в узле out-Class2CoS-map можно создавать записи с именами, соответствующими внутренним приоритетам пакетов (как в формате одиночного числа, так и в формате очередь:класс). Значением каждого параметра является приоритет 802.1p, который должен быть установлен в заголовке исходящего пакета Ethernet.

ПРИМЕЧАНИЕ Записи в обоих форматах эквивалентны, т.е., например, 1:2 означает то же самое, что 65537 (1×65535+2). Следует обращать внимание на то, чтобы один и тот же внутренний приоритет не оказался описан в этом списке дважды. Для этого проще всего использовать для всех записей один и тот же формат.

В обоих случаях, если для имеющегося значения исходного приоритета не найдено соответствующего элемента списка, то значение нового приоритета устанавливается в 0.

§2.2.5. Настройка MAC VLAN

NSG Linux 2.0 поддерживает механизм клонирования интерфейсов Ethernet, позволяющий организовать на одном физическом порту несколько дополнительных интерфейсов, каждый со своим MAC-адресом — так называемые MAC VLAN. В отличие от пакетов IEEE 802.1q, пакеты, посылаемые и принимаемые таким интерфейсом, являются обычными пакетами Ethernet и не содержат каких-либо специфических тегов. Таким образом, в одном физическом сегменте Ethernet возможно организовать несколько раздельных виртуальных сетей, каждая со своим MAC-адресом сетеобразующего порта NSG, своим пространством IP-адресов и своим набором хостов-участников.

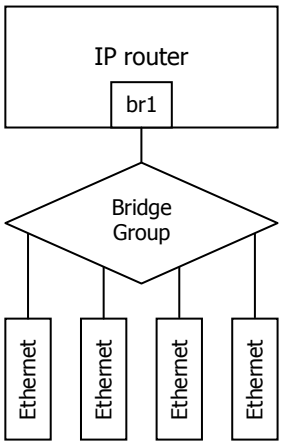
Интерфейсы MAC VLAN могут создаваться как на физических портах Ethernet, так и на отдельных VLAN и других эквивалентных им объектах. Создание MAC VLAN производится в узле macvlan, который содержится во всех портах Ethernet, VLAN и т.п. Создаваемые клоны получают имена вида родительскийПорт.m*N*. Дальнейшая настройка полностью аналогична настройке физического порта Ethernet; в первую очередь, для MAC VLAN необходимо, по существу этого объекта, установить уникальный MAC-адрес, отличный от адреса родительского порта.

В частности, интерфейс MAC VLAN может сам содержать внутри себя не только простые нетегрированные сети, но и VLAN IEEE 802.1q. Запрещается только создавать одну MAC VLAN внутри другой.

Механизм MAC VLAN особенно актуален для создания виртуальных маршрутизаторов (см. Часть 1). С его помощью можно, например, подключить несколько виртуальных маршрутизаторов, каждый из которых имеет свои выделенные физические порты для локальных сетей, к одному общему каналу связи с вышестоящим поставщиком услуг.

§2.3. Обработка трафика Ethernet на общесистемном уровне

§2.3.1. Программные коммутаторы (*bridge groups*)



Для прозрачного обмена пакетами Ethernet (без анализа IP и вышестоящих уровней) между портами Ethernet используются программные коммутаторы Ethernet, называемые также *bridge groups* или "подключения типа мост". Каждый программный коммутатор эквивалентен физическому коммутатору Ethernet, к которому могут подключаться физические порты Ethernet целиком, отдельные VLAN на них, а также виртуальные объекты (туннели GRE и т.п.) с инкапсуляцией Ethernet.

Если в состав *bridge group* включается порт Ethernet, на котором определены VLAN, то весь трафик этого порта коммутируется на остальные порты данной группы как есть, включая как пакеты с тегами VLAN, так и пакеты без тегов. Если в состав группы включена индивидуальная VLAN, то во входящих из неё пакетах тег отбрасывается и после этого пакет коммутируется на остальные порты. В пакеты, которые поступают из других портов данной группы и должны быть отправлены в данную VLAN, добавляется тег этой VLAN.

Коммутатор как единое целое соединяется с маршрутизатором через виртуальный интерфейс с именем вида brN, имеющий все атрибуты сетевого интерфейса (IP-адрес и т.п.). В этом случае его следует рассматривать как виртуальный порт маршрутизатора, подключённый через виртуальный же коммутатор к нескольким физическим (или также виртуальным — VLAN, GRE и т.п.) портам. Объекты, включённые в состав коммутатора, непосредственно к маршрутизатору не подключены и никаких параметров, присущих IP-интерфейсу, не имеют.

В частности, если коммутатор предназначен только для передачи пакетов между портами, то IP-адрес для него не требуется; этот адрес только позволяет сделать само устройство NSG доступным, как IP-хост, в объединённой сети Ethernet.

Создание и настройка программных коммутаторов производится в узле .ethernet.bridge . Параметры собственно коммутатора определяют работу с таблицей MAC-адресов и поведение коммутатора с точки зрения протокола Spanning Tree. Включение и исключение портов Ethernet (или эквивалентных им объектов) в состав *bridge group* производится в меню этих портов.

ПРИМЕЧАНИЕ В устройствах NSG–605 в состав *bridge group* может входить не более одного физического порта Ethernet. Для объединения двух или более физических портов в этих устройствах следует использовать настраиваемый аппаратный коммутатор (узел .ethernet-switch, специфический для данной модели).

ПРИМЕЧАНИЕ Настройку *bridge groups* и *bond groups* не следует производить через порты, входящие в эти группы, поскольку после применения конфигурации доступ к устройству будет утерян. Рекомендуется предварительно настроить управление через любой другой порт (сетевой или консольный) и производить конфигурацию через него. При отсутствии такой возможности следует выполнить конфигурацию полностью, но не применять; затем сохранить её и перезагрузить устройство.

§2.3.2. Многоканальные соединения Ethernet (*bond groups*)

Механизм многоканальных соединений позволяет объединить несколько физических портов Ethernet (или эквивалентных им объектов — VLAN, туннелей и т.п.) в одну физическую сущность с увеличенной пропускной способностью, балансировкой нагрузки и резервированием. В терминах различных реализаций и разных производителей, такое объединение называется *aggregation*, *bonding*, *grouping*, *teaming*, *trunking* и т.п. Существует несколько различных алгоритмов объединения, предназначенных для разных целей; наиболее современным вариантом является спецификация IEEE 802.3ad, впоследствии перенесённая, по формальным соображениям, в 802.1AX.

Архитектурно многоканальные соединения в NSG Linux 2.0 представлены в виде *bond groups*, аналогичных *bridge groups*. Настройка соединений как целого производится в узле .ethernet.bond , порт или иной Ethernet-подобный объект включается в состав соединения с помощью команды bond-group в своём меню. Многоканальное соединение, как целое, представляет собой виртуальный интерфейс маршрутизатора с именем вида bnN. Объекты, включённые в состав соединения, непосредственно к маршрутизатору не подключены и никаких параметров, присущих IP-интерфейсу, не имеют.

Основными параметрами для работы многоканального соединения являются:

Режим работы соединения (mode) — алгоритм, управляющий распределением пакетов между каналами, входящими в его состав. Возможны следующие алгоритмы (иначе называемые политиками):

active-backup Горячее резервирование без увеличения пропускной способности. В каждый момент работает только один из каналов, остальные находятся в резерве и один из них включается в работу только в том случае, если активный канал выходит из строя. Основной канал устанавливается параметром primary .
MAC-адрес многоканального соединения виден извне только на одном порту, чтобы не вызывать проблем для смежного коммутатора.
Если соединение переключается на другой канал, то в этом канале рассылаются контрольные ARP-запросы в самом порту Ethernet и в каждой из VLAN, сконфигурированных на нём.

balance-rr Балансировка нагрузки и резервирование каналов на уровне отдельных пакетов. Пакеты передаются по очереди в каждый из работоспособных каналов (по кругу, *round robin*).

balance-xor Балансировка нагрузки и резервирование каналов на уровне парных взаимодействий. Пакеты, принадлежащие каждой паре MAC-адресов (источник, назначение) передаются в определённый канал, таким образом, все парные взаимодействия распределяются равномерно между действующими каналами. Более сложные алгоритмы распределения взаимодействий между каналами могут быть установлены параметром xmit-hash-policy .

broadcast Резервирование с помощью широковещательной рассылки: каждый пакет передаётся одновременно во все действующие каналы.

802.3ad Динамическая агрегация каналов согласно стандарту IEEE 802.3ad. Каналы с одинаковой скоростью и режимом Full/Half Duplex объединяются в группы (*aggregation groups*). В каждом агрегаторе используются одновременно все каналы в соответствии с 802.3ad. Алгоритм распределения пакетов между каналами устанавливается параметром xmit-hash-policy .

ВНИМАНИЕ Не все возможные политики совместимы со стандартом 802.3ad, особенно в части обработки пакетов с нарушенной последовательностью. При использовании таких политик на оборудовании различных производителей возможны проблемы с совместимостью.

Для работы данного алгоритма требуется, чтобы коммутаторы поддерживали механизм IEEE 802.3ad Dynamic link aggregation. Как правило, режим 802.3ad на них не включён по умолчанию, поэтому требуется настройка коммутаторов.

balance-tlb Адаптивная балансировка нагрузки на передачу (*transmit load balancing*). Не требует специальной поддержки агрегации на промежуточных коммутаторах. Исходящие пакеты распределяются между активными каналами таким образом, чтобы обеспечить им равномерную загрузку относительно номинальной скорости каждого канала. Все входящие пакеты принимаются одним активным каналом; если он выходит из строя, то другой канал становится активным и принимает его MAC-адрес.

balance-alb Адаптивная балансировка нагрузки (*adaptive load balancing*). Включает в себя balance-tlb плюс балансировку нагрузки на приёме (*rlb*) для пакетов IPv4. Не требует специальной поддержки агрегации на промежуточных коммутаторах; балансировка на приёме производится с помощью манипулирования пакетами ARP. В исходящие ответы ARP вместо системного MAC-адреса подставляется адрес конкретного порта в нём, с тем, чтобы каждый из удалённых хостов присылал пакеты на определённый порт устройства NSG.

По умолчанию используется самый простой алгоритм агрегирования — balance-rr. Для политик balance-xor и 802.3ad возможные алгоритмы распределения пакетов по портам устанавливаются параметром xmit-hash-policy :

layer2 Канал для отправки пакета однозначно определяется комбинацией MAC-адресов источника и назначения по следующей формуле:

(source_MAC XOR destination_MAC) modulo slave_count

т.е. над MAC-адресами источника и назначения выполняется битовая операция XOR (исключающее ИЛИ), и результат в виде числа делится на число каналов в соединении. Остаток от деления и будет номером канала, в который отправится пакет. Как можно видеть, результат не зависит от перестановки источника и назначения; весь трафик между определённой парой узлов всегда идёт по определённому каналу.
Алгоритм совместим с IEEE 802.3ad.

layer2+3 Канал для отправки пакета определяется по совокупности MAC- и IP-адресов источника и назначения по следующей формуле:

(((source_IP XOR dest_IP) AND 0xffff) XOR (source_MAC XOR destination_MAC)) modulo slave_count

Трафик между определённой парой хостов IP всегда идёт по определённому каналу. Благодаря этому обеспечивается более равномерная балансировка трафика, особенно в случае, когда бóльшая его часть передаётся через промежуточные маршрутизаторы.
Для протоколов 3 уровня, отличных от IP, данный алгоритм равносилен layer2 .
Алгоритм совместим с IEEE 802.3ad.

layer3+4 Канал для отправки пакета определяется по совокупности IP-адресов и номеров портов источника и назначения:

((source_port XOR dest_port) XOR ((source_IP XOR dest_IP) AND 0xffff) modulo slave_count

Благодаря этому трафик определённого узла может распределяться между несколькими каналами, хотя пакеты одного и того же TCP-соединения или UDP-потока всегда передаются по одному и тому же каналу.
Для фрагментированных пакетов TCP и UDP, а также для всех прочих протоколов 4 уровня, учитываются только IP-адреса. Для протоколов 3 уровня, отличных от IP, данный алгоритм равносилен layer2 .
Алгоритм не полностью совместим с IEEE 802.3ad. Если в одном TCP-соединении или UDP-потоке присутствуют одновременно фрагментированные и нефрагментированные пакеты, то они могут быть разбросаны по разным каналам и в результате получены с нарушением исходной последовательности. Это достаточно редкая ситуация, но при работе с некоторыми иными реализациями 802.3ad она принципиально может приводить к несовместимости.

Важнейшим элементом многоканальных соединений является механизм контроля состояния отдельных физических каналов. Контроль может производиться двумя способами: либо по состоянию Link канала (MII-монитор), либо с помощью обмена пакетами ARP с некоторыми контрольными хостами (ARP-монитор). Данные ARP-запросы называются "непрошеными" или "дармовыми" (*gratuitous*), поскольку не вызваны необходимостью передачи IP-трафика. ARP-монитор и MII-монитор являются взаимоисключающими механизмами и не могут использоваться одновременно; для нормальной работы соединения всегда должен быть включён один и только один из них.

Настройка MII-монитора состоит в задании интервала опроса состояния порта (miimon). Работа ARP-монитора управляется параметрами arp-interval, arp-ip-target и arp-validate .

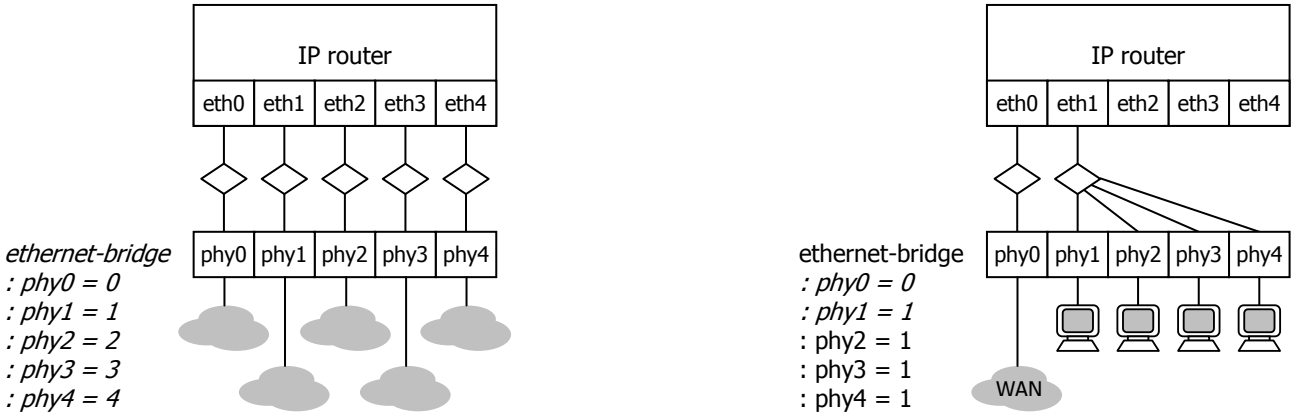
Остальные параметры относятся к второстепенным деталям и в большинстве случаев могут быть установлены в значения по умолчанию.

§2.3.3. Настройка аппаратного коммутатора в устройстве NSG–605

Устройство NSG–605 и его модификации имеют 5 портов Ethernet и встроенный аппаратный коммутатор. В данном случае необходимо различать сетевые интерфейсы IP-маршрутизатора (объекты 2–3 уровней) и физические интерфейсы Ethernet (объекты 1 уровня). Эти объекты соединяются друг с другом при помощи аппаратного коммутатора. Настройка коммутатора производится в узле .ethernet-switch . Посмотреть текущую таблицу коммутации можно командой .ethernet-switch.show .

Стандартные имена eth0 ... eth4 в данном случае относятся к сетевым интерфейсам маршрутизатора. Это программные (виртуальные) объекты, которые участвуют в передаче IP-трафика, а также могут включаться в состав *bridge groups* (но не более одного в каждую группу).

Физические интерфейсы имеют имена phy0 ... phy1, соответственно. В заводской конфигурации каждый из них скоммутирован с соответствующим сетевым интерфейсом и может рассматриваться вместе с ним как единое целое — маршрутизируемый порт Ethernet (на рисунке слева).

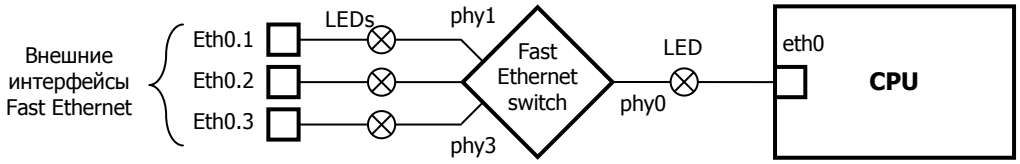


Если требуется иная конфигурация, то для каждого физического интерфейса можно указать номер сетевого интерфейса, к которому он должен быть подключён. Каждый физический интерфейс может подключаться только к одному сетевому интерфейсу. К одному интерфейсу маршрутизатора могут быть подключены несколько физических интерфейсов, скоммутированных также и друг с другом. На рисунке справа показана часто используемая конфигурация, когда один из портов используется для подключения к вышестоящей сети, а остальные четыре — в качестве коммутатора для локальной сети. (Курсивом приведены настройки по умолчанию, в конфигурации не показываемые.)

Если к сетевому интерфейсу не подключено ни одного физического интерфейса, то он не может использоваться для передачи данных. Однако такой интерфейс может использоваться для протокольных целей, например, от его адреса могут строиться туннели, посылаться *ping* и т.п.

§2.3.4. Настройка аппаратного коммутатора в устройствах NSG–700, NSG–1800

Устройства NSG–700 и NSG–1800 имеют встроенный коммутатор с поддержкой VLAN. Он представляет собой самостоятельное аппаратное устройство с 5 физическими портами, обозначаемыми phy0 ... phy4. Внутренняя архитектура устройств в части Ethernet показана на рисунке.



В устройствах NSG–700 порт phy0 коммутатора подключён к порту eth0 процессора, внешних портов три. (4-й порт подключён к разъёму расширения s1 и может использоваться только в режиме Ethernet-over-SDSL; в NSG Linux 2.0 модуль IM–SDSL не поддерживается, и поэтому порт заблокирован.) В устройстве NSG–1800 порт phy0 коммутатора подключён к порту eth1 процессора, внешних портов четыре.

Коммутатор может транслировать пакеты Ethernet либо прозрачно, без учёта их тегов VLAN и без модификации, либо избирательно на основе тегов VLAN. В сочетании с настройками VLAN на порту Ethernet процессора это позволяет логически разделить внешние порты коммутатора. Настройка коммутатора производится в узле .ethernet.switch .

Параметр vlan-mode определяет режим работы коммутатора по существу:

false — Обычная коммутация между всеми портами без учёта тегов VLAN.

true — Передача пакетов на основе тегов VLAN и заданной таблицы коммутации.

Если коммутатор работает в режиме VLAN, то каждый его порт далее настраивается индивидуально. В настройках порта указывается один или несколько (см. ниже) идентификаторов VLAN, которые он обрабатывает. Для каждого идентификатора VLAN, указанного хотя бы в одном порту, создаётся так называемая *VLAN-группа*. Группу можно рассматривать как отдельный коммутатор с собственным набором физических интерфейсов phy0 ... phy4, работающий независимо от остальных. Максимальное число VLAN-групп — 15, т.е. число идентификаторов VLAN, обрабатываемых индивидуально, для всей совокупности интерфейсов не может превышать 15.

ПРИМЕЧАНИЕ Порт процессора может обрабатывать пакеты как с тегами VLAN (если на нём настроены соответствующие VLAN), так и без них. Однако коммутатор работает либо в режиме без учёта VLAN (пропускает любые пакеты без разделения по портам), либо в режиме разделения портов по VLAN. Смешанный режим также возможен, но сложен в настройке и неактуален на практике, поэтому в NSG Linux 2.0 не предусмотрен.

В меню каждого порта коммутатора параметр vlan-tagged определяет режим работы порта:

false — Нетегированный: предполагается, что к порту подключён сегмент обычной сети Ethernet, т.е. входящие и исходящие пакеты не имеют тегов VLAN. Порт включается в единственную VLAN-группу с идентификатором, указанным параметром vlan-group. Если для данного параметра указано значение 4095, то работа через него запрещена.

true — Тегированный: предполагается, что к порту подключён физический сегмент с одной или более VLAN, т.е. входящие и исходящие пакеты имеют теги VLAN. СписокVLAN, поддерживаемых на данном порту, составляется в узле vlan-groups. Порт включается во все VLAN-группы с перечисленными идентификаторами. Пакеты, принадлежащие к одной из этих VLAN, транслируются в другие порты — члены данной группы. Пакеты с любыми другими тегами, или без тегов вообще, игнорируются. Если список пустой, то порт не включён ни в одну VLAN-группу, т.е. работа через него запрещена.

Обработка пакетов производится следующим образом:

1) Каждый входящий пакет приписывается к одной из групп по следующим правилам:
   — входящий пакет, имеющий тег VLAN, приписывается к группе с номером равным номеру тега. При этом сам пакет не изменяется.
   — входящий пакет, не имеющий тега VLAN и пришедший на нетегированный порт, приписывается к группе с номером, равным значению vlan-group для этого порта.
   — входящий пакет, не имеющий тега VLAN и пришедший на тегированный порт, уничтожается.
2) Если группа, к которой приписан входящий пакет, не содержит в своём списке номер порта, с которого пришел этот пакет, то пакет уничтожается. В частности, это относится:
   — ко всем пакетам, поступившим через нетегированный порт, если для него не указана корректная vlan-group (от 2 до 4094).
   — к пакетам без тегов VLAN, поступившим через тегированный порт.
   — к пакетам с тегами VLAN, поступившим через тегированный порт, если идентификатор VLAN, указанный в теге пакета, не относится ни к одной из явно определённых VLAN-групп на данном порту.

   Остальные пакеты передаются во все порты, включённые в данную группу.
3) На выходе из коммутатора каждый исходящий пакет может быть изменен по следующим правилам:
   — если пакет отправляется в нетегированный порт и имеет тег VLAN, то тег будет удален.
   — если пакет отправляется в тегированный порт и не имеет тега VLAN, то в этот пакет будет добавлен тег с номером группы, которой принадлежит пакет.
   — во всех остальных случаях пакет не изменяется.

   Таким образом, в нетегированные порты будут уходить только пакеты без тегов VLAN, а в тегированные порты будут уходить только пакеты с тегами.

ПРИМЕЧАНИЕ Как можно видеть, конфигурация интерфейсов коммутатора может, в общем случае, не соответствовать природе физических сегментов сети, подключенных к ним. На практике, однако, рекомендуется следить за наличием такого соответствия, чтобы исключить вероятность ошибочной настройки. Рекомендуется также указывать списки используемых VLAN явным образом на каждом интерфейсе.

Просмотреть результаты коммутации можно командой .ethernet-switch.show . Команда выводит таблицу, показывающую, какие VLAN-группы определены в коммутаторе и какие физические порты в них включены. Примеры вывода см. ниже.

Примеры конфигурирования (устройство NSG–700).

Курсивом указаны значения, установленные по умолчанию.

а) Коммутатор и внутренний порт в нормальном режиме Ethernet:

```
ethernet
: switch
: : vlan-mode              = false
port
: eth0
: : ifAddress
: : : prefix               = "192.168.0.1/24"
```

Это обычный режим работы единой физической сети Ethernet без VLAN.

б) Коммутатор в нормальном режиме Ethernet, внутренний порт в режиме VLAN:

```
ethernet
: switch
: : vlan-mode              = false
port
: eth0
: : vlan
: : : eth0.2
: : : : ifAddress
: : : : : prefix           = "192.168.2.1/24"
: : : eth0.3
: : : : ifAddress
: : : : : prefix           = "192.168.3.1/24"
.....................................
```

Данный режим работы соответствует одной физической сети Ethernet, в которой определено несколько VLAN. Количество и номера VLAN могут быть произвольными.

в) Коммутация на основе VLAN — подключение 3 изолированных физических сегментов.

Обмен пакетами напрямую между интерфейсами коммутатора запрещён, каждый из физических интерфейсов phy1 ... phy3 соединён с определённой VLAN на внутреннем порту eth0. Данная конфигурация аналогична той, которая устанавливалась в NSG Linux 1.0 командой ethernet-switch mode vlan по умолчанию.

```
ethernet
: switch
: : phy0
: : : vlan-groups
: : : : 1                       = 101
: : : : 2                       = 102
: : : : 3                       = 103
: : : vlan-tagged               = true
: : phy1
: : : vlan-group                = 101
: : phy2
: : : vlan-group                = 102
: : phy3
: : : vlan-group                = 103
: : vlan-mode                   = true
port
: eth0
: : vlan
: : : eth0.101
: : : : ifAddress
: : : : : prefix                = "10.0.0.1/8"
: : : eth0.102
: : : : ifAddress
: : : : : prefix                = "20.0.0.1/8"
: : : eth0.103
: : : : ifAddress
: : : : : prefix                = "30.0.0.1/8"
```

Здесь на порту eth0 определены три IP-интерфейса eth0.101, eth0.102, eth0.103, каждый из которых соединён с соответствующим физическим сегментом сети. Результат выполнения данной настройки:

```
nsg:ethernet.switch>show

Ethernet switch is in VLAN mode
VLAN memberships:
             P0   P1   P2   P3
————————————————————————————
 VLAN 101    X    X    .    .
 VLAN 102    X    .    X    .
 VLAN 103    X    .    .    X
```

г) Объединение двух сегментов без доступа к процессору.

```
ethernet
: switch
: : phy0
: : : vlan-group                = 700
: : phy1
: : : vlan-group                = 666
: : phy2
: : : vlan-group                = 666
: : phy3
: : : vlan-groups
: : : : 1                       = 700
: : : vlan-tagged               = true
: : vlan-mode                   = true
port
: eth0
: : ifAddress
: : : prefix                    = "10.0.0.7/8"
```

Результат выполнения данной настройки:

```
nsg:ethernet.switch>show

Ethernet switch is in VLAN mode
VLAN memberships:
             P0   P1   P2   P3
————   ————————
 VLAN 666     .    X    X    .
 VLAN 700     X    .    .    X
```

Здесь первый и второй физические сегменты соединены друг с другом, но не имеют доступа ни в третий сегмент, ни к порту eth0 процессора. Физический интерфейс phy0 нетегированный, поэтому и порт процессора настраивается без использования VLAN. Порт eth0 будет принадлежать VLAN 700 в третьем сегменте, причём присвоение и удаление тегов VLAN в данном случае производится на интерфейсе коммутатора. Никакие другие пакеты через коммутатор пропущены не будут.

д) Подключение физических сегментов к сегменту VLAN.

```
ethernet
: switch
: : phy0
: : : vlan-groups
: : : : 1                       = 55
: : : : 2                       = 77
: : : vlan-tagged               = true
: : phy1
: : : vlan-group                = 55
: : phy2
: : : vlan-group                = 77
: : phy3
: : : vlan-groups
: : : : 1                       = 55
: : : : 2                       = 77
: : : vlan-tagged               = true
: : vlan-mode                   = true
port
: eth0
: : vlan
: : : eth0.55
: : : : ifAddress
: : : : : prefix                = "55.0.0.1/8"
: : : eth0.77
: : : : ifAddress
: : : : : prefix                = "77.0.0.1/8"
```

Результат выполнения данной настройки:

```
nsg:ethernet.switch>show

Ethernet switch is in VLAN mode
VLAN memberships:
             P0   P1   P2   P3
————   ————————
  VLAN 55    X    X    .    X
  VLAN 77    X    .    X    X
```

Здесь все узлы первого сегмента будут частью VLAN 55 из третьего сегмента; также к ней относится субинтерфейс eth0.55 процессора. Аналогично с VLAN 77.

§2.4. Настройка асинхронных портов RS–232 и RS–485

§2.4.1. Идентификация портов и параметры физического уровня

Порты RS–232 и RS–485 в устройствах NSG могут быть фиксированными (на шасси) или сменными на следующих интерфейсных модулях и картах NSG:

type = "2com"	Модуль UM–2V24A, 2 порта
type = "rs-232"	Модули IM–V24A, IM–V35–2 (только асинхронный режим); внешний адаптер USB/RS–232 на порту USB; опция opt1820.Eth-async для устройства NSG–1820
type = "rs-485"	Модуль IM–485–2 (*в данной версии не поддерживается*)

Фиксированные порты имеют имена rs-232, rs-485 или a1, a2 и т.д. в зависимости от их числа на шасси. Сменные порты — s1, s2 и т.д. в зависимости от номера разъёма расширения (для UM–2V24A — s*N*.0 и s*N*.1). Опции — m1, m2 и т.д.

В общем случае, вне зависимости от выбранной инкапсуляции, для асинхронного порта необходимо установить параметры физического уровня — скорость и формат асинхронной посылки. (Исключением является инкапсуляция PPP, которая однозначно требует 8n1.) По умолчанию, порты работают с настройками 9600 бит/с, 8n1.

Управление потоком для порта RS–232 настраивается отдельным параметром. Если он отсутствует в меню порта, это означает, что либо данный порт работает всегда с аппаратным управлением потоком, либо без него (в зависимости от конкретного порта и модели устройства), и отключить/включить его нельзя в силу конструктивных ограничений. В частности:

— На устройствах NSG–1800, NSG–1810, NSG–1820 порт a1 всегда работает без управления потоком, выходные сигналы DTR и RTS всегда подняты, входные сигналы DCD и CTS игнорируются.

Для непосредственного доступа в порт (например, для ручной настройки подключённого модема с помощью AT-команд) предусмотрена команда raw-access . Команда доступна в том случае, если на порту не включён никакой протокольный обработчик, т.е. установлено encapsulation = "none" или adm-state = "down" . В режиме ручного управления весь ввод и вывод прозрачно передаётся в порт и обратно, за исключением следующих *escape*-последовательностей:

~.	Завершить соединение.
~,	Опустить сигнал DTR на 2 сек., чтобы принудить подключённый модем разорвать соединение.
~#	Послать сигнал BREAK в асинхронную линию. Это специфический код, который не может быть передан по Telnet и может быть сгенерирован только локально на физическом порту. Он требуется для некоторых специальных целей, в частности, для входа в меню загрузчика на устройствах некоторых производителей.
~D	Поднять сигнал DTR.
~d	Опустить сигнал DTR.
~R	Поднять сигнал RTS.
~r	Опустить сигнал RTS.
~M	Вывести состояние сигналов DCD и CTS.
~?	Вывести список возможных *escape*-последовательностей на экран.

Например, для завершения сеанса работы необходимо нажать последовательно две клавиши "~" и ".".

Для порта RS–485 управление потоком не используется. Режим работы линии (шина/отвод, Full/Half Duplex) выбирается аппаратно с помощью перемычек в кабеле (для модуля IM–485) или микропереключателей (для встроенных портов); подробнее см. документацию по аппаратной части.

Другие параметры в меню порта зависят от выбранной инкапсуляции 2 уровня. При смене инкапсуляции в меню появляются и удаляются соответствующие узлы.

§2.4.2. Инкапсуляция reverse-telnet

Инкапсуляция reverse-telnet предназначена для доступа по сети в данный физический порт. Как правило, такой порт используется для удалённого управления каким-либо другим оборудованием через консольный порт. При выборе данного режима на устройстве открывается некоторый TCP-порт и данные из него транслируются в физический порт и обратно. Зайдя на устройство NSG, например, по Telnet:

```
telnet A.B.C.D  P
```

(где A.B.C.D — любой из IP-адресов устройства NSG, а P — номер порта TCP), пользователь попадает в асинхронный кабель и может передавать по нему данные в целом так же, как если бы он был подключён к этому кабелю непосредственно COM-портом своего компьютера. При этом, правда, есть некоторые ограничения, часть из которых преодолевается с помощью параметров, описанных ниже, а часть — с помощью инкапсуляции raw-tcp.

Основным и обязательным параметром для работы Reverse-Telnet является номер порта TCP, на котором устройство ожидает входящие соединения. По умолчанию, используется порт 50010. В частности, зайти в порт Reverse Telnet можно непосредственно с самого устройства NSG с помощью команды:

```
telnet 127.0.0.1  50010
```

(из командной оболочки Linux), или аналогично из консольного или Web-интерфейса (узел .tools.telnet).

Остальные параметры опциональны и относятся к двум важным механизмам, связанным с Reverse Telnet.

Управляющие последовательности. Для управления сеансом работы Telnet и самого асинхронного порта используются *escape*-последовательности из 2 символов. Чтобы использовать их, необходимо назначить *escape*-символ, означающий начало последовательности; этот символ не должен использоваться при нормальном обмене данными через порт. По умолчанию, это символ "~" (тильда). Обрабатываемые *escape*-последовательности перечислены в предыдущем параграфе.

Кроме того, можно определить отдельные символы для посылки BREAK и для завершения сеанса одной клавишей вместо двух. Символы завершения сеанса особенно актуальны при заходе с одного устройства на соседнее, с него — на следующее и так далее "по цепочке", что часто приходится делать при нарушении маршрутизации в сети. В этом случае важно иметь на разных устройствах разные символы завершения (или, в общем случае, вообще разные *escape*-символы), чтобы можно было выйти точно с заданного устройства, сохраняя всю предыдущую цепочку сеансов.

Аутентификация пользователей. Прежде чем дать удалённому пользователю выход в физический порт, устройство NSG может потребовать от него аутентификации. Аутентификация выполняется по локальному списку, по централизованному серверу RADIUS или TACACS+. Например, если устройство NSG используется на удалённом узле для консольного доступа к оборудованию, принадлежащего различным владельцам, то каждый из пользователей должен иметь доступ только к тем портам, к которым подключено его оборудование.

Аутентификация настраивается в узле .system.aaa.reverse-telnet . В данном узле следует составить список, каждый элемент которого описывает некоторый способ аутентификации. Обязательным параметром для каждого способа является его тип: локальная, RADIUS или TACACS+. Для централизованных серверов необходимо указать также IP-адрес (server) и ключ для доступа к серверу (secret). Для локальной аутентификации необходимо создать соответствующих пользователей в узле .system.users , назначив каждому имя и пароль.

ПРИМЕЧАНИЕ С созданным именем и паролем пользователя возможно также войти на само устройство NSG, однако при этом, по умолчанию, не будет доступно ни одной команды. Таким образом, это не угрожает безопасности устройства.

Если в списке содержится более одного элемента, то они рассматриваются последовательно в порядке нумерации. При этом, если очередной способ дал положительный результат, то аутентификация считается успешной и завершается. Если получен отрицательный ответ или он не получен вообще за установленный таймаут, то делается попытка аутентифицироваться по следующему способу. Если список способов исчерпан и ни по одному из них не получено положительного ответа, то аутентификация считается неудачной. Подробнее о системном механизме аутентификации см. Часть 1.

Помимо реквизитов пользователя, на сервер TACACS+ передаётся имя порта, к которому он пытается подключиться; это имя также может учитываться сервером. Пример конфигурации:

```
user = basile {
  pap = cleartext poUpkInE
  service = raccess {
  port = a1, a7
  }
}
```

Здесь пользователю разрешен доступ к портам a1 и a7. Если атрибут port не указан, то доступ разрешен ко всем портам.

§2.4.3. Инкапсуляция raw-tcp

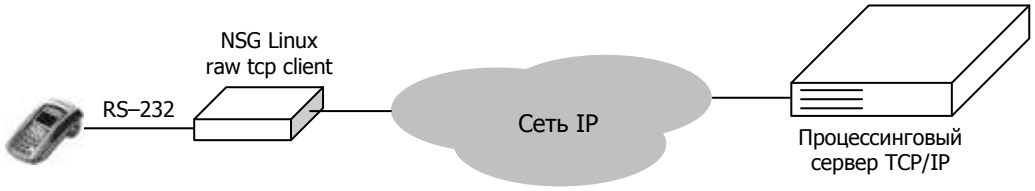
Инкапсуляция reverse-telnet предназначена для обмена данными в текстовом режиме и имеет свои ограничения. Во-первых, протокол Telnet сам по себе использует некоторую процедуру установления соединения (*handshake*) на прикладном уровне, в ходе которой пересылаются несколько служебных пакетов между клиентом и сервером. Во-вторых, определённые спецсимволы могут не передаваться, а использоваться клиентом или сервером Telnet для особых целей, например, символ CTRL–] в Telnet-клиентах означает, как правило, выход из режима обмена данными в командный режим. Таким образом, передача по Telnet не является полностью прозрачной и непригодна для задач, где стороны могут обмениваться произвольными бинарными данными строго один-в-один, не допуская ни единого потерянного, изменённого или добавленного бита. Эта типичная ситуация для подключения POS-терминалов без встроенного сетевого протокола, а также некоторых моделей оборудования, управляемого через COM-порт фирменными утилитами в бинарном режиме.

Для таких задач вместо reverse-telnet следует использовать инкапсуляцию raw-tcp. В этом случае только устанавливается TCP-соединение на транспортном уровне и произвольные бинарные данные копируются из него в физический порт и обратно. Порт raw-tcp в устройствах NSG может работать в 2 режимах: клиента и сервера. Клиентом всегда должен быть порт на той стороне, откуда инициируется соединение.

ПРИМЕЧАНИЕ Инкапсуляция raw-tcp предполагает передачу данных с относительно высокой скоростью и по этой причине требует аппаратного управления потоком. По этой причине она отключена на портах, где это управление не поддерживается (a1, модуль IM–V24A на всех NSG–18*xx*.)

Ключевые и обязательные параметры для клиента raw-tcp — это IP-адрес и TCP-порт сервера, к которому он должен обращаться. Для сервера — TCP-порт, на котором он ожидает соединения. IP-адрес для сервера является необязательным, по умолчанию, он принимает соединения на всех адресах, назначенных устройству; этот параметр можно использовать, чтобы разрешить входящие соединения только по какому-то определённому адресу.

Для подключения асинхронного POS-терминала к процессинговому серверу, работающему по TCP/IP, требуется одиночный порт-клиент raw-tcp. Два порта raw-tcp (на одном или разных устройствах), клиент и сервер, соединённые по сети друг с другом, образуют прозрачную "трубу" для передачи произвольного асинхронного трафика из одного физического интерфейса RS–232 в другой.



Подключение асинхронного POS-терминала к процессингу TCP/IP

Прозрачная передача асинхронных данных между COM-портами двух ПК

Опциональные параметры регулируют процедуру установления TCP-соединения и взаимодействие между ним и сигналами интерфейса RS–232. Таким образом, подключённое оборудование может управлять соединением и контролировать его состояние:

— TCP-соединение может поддерживаться по возможности постоянно, либо устанавливаться по поднятию входящего сигнала DCD и разрываться при падении этого сигнала. Например, подключённый POS-терминал начинает транзакцию с поднятия своего сигнала DTR (поскольку подключение производится кросс-кабелем, то на устройство NSG он приходит как DCD), а завершает опусканием.

— Наоборот, исходящий сигнал DTR может быть постоянно поднят, постоянно опущен или опускаться на заданное время при разрыве соединения. Например, для подключённого модема падение DTR на 2 сек. приводит, при обычных настройках, к разрыву физического соединения.

— При неудачной попытке соединения с сервером следующая попытка может предприниматься немедленно, либо после заданной паузы.

§2.4.4. Инкапсуляция ppp — краткие сведения о протоколе

PPP (Point-to-Point Protocol) — сложный и гибкий протокол, имеющий большое число параметров и применений. Это основной протокол 2 уровня для передачи пакетов IP через асинхронные среды передачи WAN "точка-точка", к которым относятся коммутируемые модемные линии, коммутируемые соединения GSM в канальном режиме (CSD, или GSM data), все пакетные технологии сотовых сетей 2 и 3 поколений (GPRS/EDGE/HxDPA, CDMA), а также нуль-модемные соединения и мультипротокольные инкапсуляции PPP-over-Ethernet (PPPoE), PPP-over-ATM (PPPoA), Point-to-Point Tunneling Protocol (PPTP), PPP-over-X.25. Базовым вариантом, наиболее простым, является асинхронная линия; все остальные варианты применения по существу используют ту же самую процедуру.

Процедура работы PPP разделяется на несколько этапов, каждый из которых обрабатывается отдельным протоколом. Их понимание необходимо для корректной настройки PPP и поиска возможных нестыковок.

1 этап — соединение на физическом уровне. Обработчик протокола PPP (pppd), как правило, должен отработать некоторый скрипт на подключённом модеме: послать строку инициализации, команду дозвона с номером телефона, и, в конечном счёте, получить от модема ответ CONNECT и поднятие сигнала DCD на физическом интерфейсе (или его аналога в соединениях PPPoE, PPTP).

Если после установления физического соединения вызываемая сторона (сервер) требует ввода имени и пароля пользователя в терминальном режиме, то это также должно делаться посредством модемного скрипта.

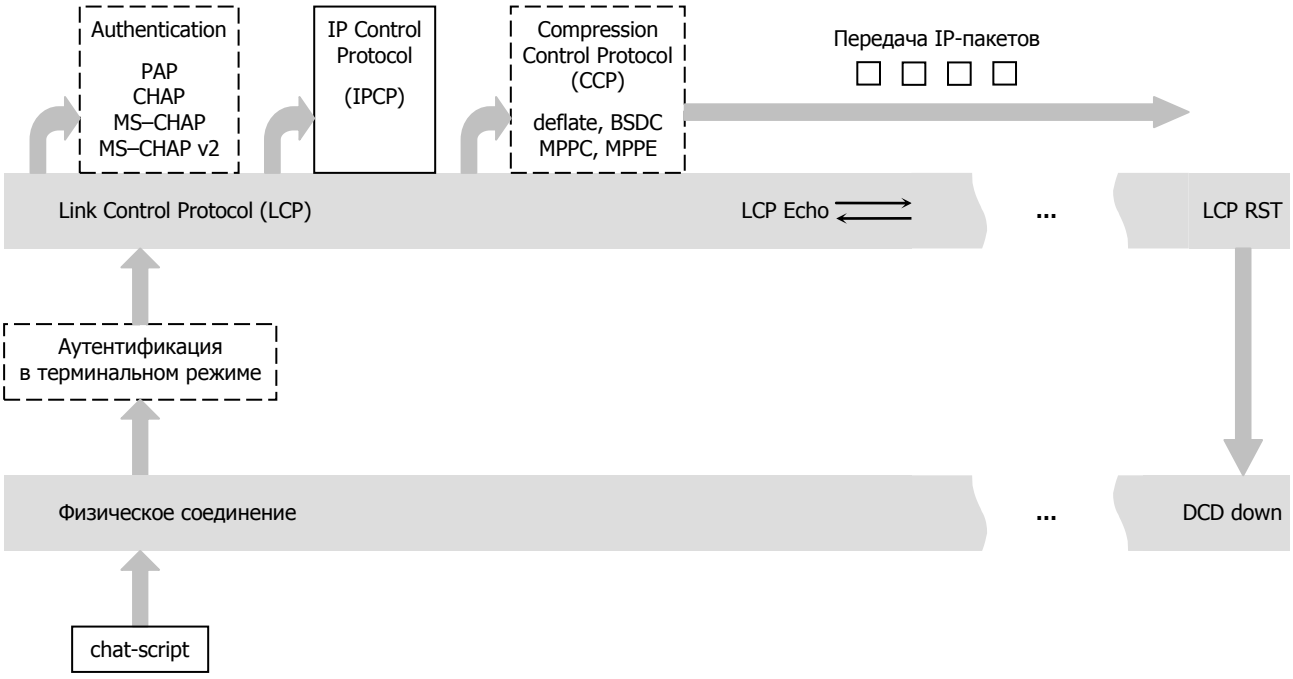
2 этап — по поднятию DCD запускается протокол LCP (Link Control Protocol), базовый компонент стека PPP. С его помощью согласовываются последующие процедуры, например, будет ли выполняться аутентификация и какой из встроенных протоколов (PAP, CHAP и т.п.) будет использоваться для этой цели.

3 этап — после поднятия LCP запускаются три процедуры, которые могут исполняться последовательно или одновременно:

3.1 — аутентификация. Каждая из сторон может потребовать от другой стороны аутентифицировать себя с помощью имени и пароля. Используются протоколы PAP, CHAP, MS-CHAP или MS-CHAPv2. Протокол PAP является небезопасным, поскольку при этом передаётся сам пароль в зашифрованном виде; он может быть перехвачен и расшифрован, поскольку способ шифрования общеизвестен. Протокол CHAP и его модификации передают только хэш от совокупности пароля клиента и имени сервера, поэтому в части сохранности пароля они являются безопасными.

Очевидно, что если аутентификация не завершается успехом, то сторона, запросившая её, разрывает соединение.

Дополнительно в аутентификации может участвовать третья сторона — сервер аутентификации, авторизации и учёта (Authentication, Authorization and Accounting — AAA), на котором централизованно хранятся имена и пароли. Сторона, запрашивающая аутентификацию (сервер доступа) пересылает ему по протоколу RADIUS или TACACS+ то, что получила от клиента, а в ответ сервер присылает свой вердикт: разрешить подключение этого клиента или нет. Кроме того, сервер может прислать дополнительные настройки для работы клиента: IP-адрес, который следует ему назначить, фильтры и т.п. Далее, в процессе работы, сервер доступа может периодически отсылать серверу AAA статистику работы клиента. Если централизованный сервер AAA не используется, то имена и пароли клиентов хранятся в локальной таблице на сервере доступа.



3.2 — согласование параметров IP. Каждая из сторон может иметь заранее установленные (статические) IP-адреса для себя и для партнёра, или одна сторона может запрашивать их у другой. Каждая сторона может соглашаться с адресами, предлагаемыми другой стороной, или не соглашаться. Используется протокол IPCP.

Взаимное знание IP-адресов в PPP-соединении является, по существу, формальным требованием, но оно должно быть выполнено для работы протокола. Эти адреса нужны только для пакетов, передаваемых или принимаемых непосредственно одним из устройств. Допустима даже такая ситуация, когда одна сторон использует одну пару адресов для себя и для партнёра, а другая — другие адреса (один или оба). При этом транзитный трафик, тем не менее, будет передаваться. В частности, в некоторых современных сетях 3G сервер назначает IP-адрес клиенту, но не сообщает свой собственный; в этом случае NSG Linux автоматически выбирает для сервера некоторый случайный адрес вида 10.*x.x.x*, хотя никакого практического смысла он не имеет.

В любом случае, обе стороны должны иметь для работы PPP какие-либо IP-адреса для себя и для партнёра, хотя бы формальные. Если согласовать их не удаётся, например, сторона А пытается назначить адрес стороне Б, а на стороне Б согласование адресов запрещено, то процедура аварийно завершается и соединение разрывается.

Помимо адресов, на этапе IPCP могут передаваться другие параметры, существенные для работы стека IP. В первую очередь, это адреса серверов DNS.

3.3. Согласование параметров сжатия. Используется протокол CCP. При передаче трафик может сжиматься "на лету", а также защищаться с помощью алгоритма MPPE (Microsoft Point-to-Point Encryption). По умолчанию, все алгоритмы сжатия являются опциональными, поэтому процедура может считаться успешно завершенной, если стороны договорились работать без сжатия. Однако если на разных сторонах принудительно установлены несовпадающие алгоритмы или параметры (особенно для MPPE) и запрещёна прозрачная передача, то процедура завершится аварийно и соединение будет разорвано.

4. После успешного завершения этих 3 процедур соединение готово к передаче пакетов IP поверх PPP. Но чтобы пакеты пошли в это соединение, должна быть настроена IP-маршрутизация. Специфический приём маршрутизации именно для сеансовых PPP-соединений состоит в том, что данное соединение, если оно успешно установлено, объявляется маршрутом по умолчанию (и удаляется из маршрутной таблицы после разъединения). Можно также сделать это заранее (статическими маршрутами), можно — динамически (если партнёр поддерживает протоколы динамической маршрутизации).

ВНИМАНИЕ Если для задания маршрутов используются одновременно несколько способов, то между ними может возникнуть конфликт, и в результате будет действовать только один из маршрутов. Например, если в устройстве определён некоторый маршрут по умолчанию и, кроме того, устанавливается второй маршрут по умолчанию через PPP-соединение, то необходимо установить приоритет между ними с помощью метрик.

Кроме того, в большинстве случаев на интерфейсе IP-over-PPP требуется использовать NAT. Это необходимо, если устройство работает в качестве клиента и получает от оператора единственный IP-адрес для самого себя, а за ним стоит локальная сеть из одного или нескольких хостов. NAT не требуется в следующих случаях:

— Удалённая сторона знает, что маршруты в сеть, расположенную за данным устройством, проходят через это PPP-соединение.
— Данное устройство является единственным пользователем PPP-соединения (например, одиночный ПК на *dial-up* доступе).
— Весь трафик из/в локальную сеть передаётся внутри какого-либо туннеля (PPTP, IPsec, STunnel etc.). В этом случае все пакеты туннеля посылаются и принимаются только данным устройством. С точки зрения публичной сети, оно является единственным пользователем PPP-соединения.

Во всё время существования соединения в рамках PPP продолжает работать протокол LCP. В частности, любая из сторон может затребовать повторную аутентификацию, согласование адресов или параметров сжатия. Если одна из сторон решает штатно завершить соединение по какой-либо причине (например, по достижении максимального времени неактивности или максимальной продолжительности сеанса), она присылает пакет LCP Reset и следом разрывает физическое соединение.

Очевидно, что существование PPP-соединения на 2 и вышележащих уровнях имеет смысл только при условии, что под ним имеется физическое соединение. По этой причине pppd следит за состоянием сигнала DCD на порту. Если модемы разъединяются по какой-либо причине, немедленно удаляются соответствующие соединения, установленные процедурами PPP.

Возможны, однако, ситуации, когда физическое соединение становится де-факто неработоспособным, но это не приводит к падению DCD — из-за неисправности модема, его аппаратных особенностей, настройки (AT&C0) и т.п.. Например, в сетях GPRS нередка ситуация, когда соединение номинально существует, но его пропускная способность падает до нуля из-за высокой загруженности сети. Чтобы своевременно обнаруживать такие ситуации, в LCP предусмотрен механизм Echo: стороны PPP-соединения при отсутствии полезного трафика обмениваются пакетами LCP Echo Request/Echo Reply. Если ответы не возвращаются, то соединение считается умершим и принудительно уничтожается. Каждая из сторон может посылать или не посылать свои пакеты Echo Request, но обязана отвечать на запросы партнёра.

Протокол PPP по сути своей является симметричным, т.е. обе стороны в нём имеют одинаковые права. (Это, однако, не относится к надстройкам над ним — PPTP, PPPoE, PPPoA). Однако по функциональной роли две стороны, в большинстве практических задач, весьма чётко дифференцируются на клиент и сервер. Как правило, клиент инициирует физическое соединение и процедуру LCP, должен аутентифицировать себя серверу, получает от сервера IP-адреса и другие настройки IP. Сервер находится в режиме ожидания, запрашивает у клиента аутентификацию по тому или иному протоколу, назначает ему IP-адреса и передаёт дополнительные параметры. Однако в отдельных задачах любое из этих различий может быть перевёрнуто, IP-адреса могут назначаться статически, а аутентификация может быть обоюдной (причём по разным протоколам).

Для работы в качестве клиента или сервера PPP необходимо установить на порту инкапсуляцию ppp. После этого в меню порта появляются параметры, специфические для PPP.

§2.4.5. Инкапсуляция ppp — настройка порта для исходящих соединений

Если устройство NSG работает в качестве клиента PPP, то на нём необходимо выполнить, в большинстве случаев, следующие основные настройки:

Сценарий дозвона, состоящий из пар "жду" — "посылаю" … В простейшем случае он может выглядеть так:

chat.script = "'' ATD*номер* CONNECT ''"

На практике, однако, рекомендуется добавить несколько операций. Во-первых, обменяться с модемом сообщениями AT OK, чтобы убедиться, что он жив. Во-вторых, программно инициализировать модем (ATZ). В-третьих, поскольку большинство телефонных сетей СССР использует импульсный набор номера (P), то указать это явно в команде ATD:

chat.script = "'' AT OK ATZ OK ATDP*номер* CONNECT ''"

Чередовать два или более вызываемых номера, если первый не отвечает, можно с помощью конструкции:

chat.script = "'' AT OK ATZ OK ATDP*номер1* CONNECT-ATDP*номер2*-CONNECT-ATDP*номер3*-CONNECT ''"

Если модем выключается по падению сигнала DTR (например, некоторые модемы IDC, или встроенные модемные модули NSG IM–V34, IM–V92), то после начала работы, т.е. поднятия DTR, необходимо дать ему некоторое время (2–3 сек) для включения и загрузки встроенного программного обеспечения. Попутно рекомендуется прочистить буфер порта. Это делается следующей конструкцией:

chat.script = "TIMEOUT 3 XXX-\rAT-OK ATDP*номер* TIMEOUT 45 CONNECT ''"

В данном случае pppd сначала ждёт, что к нему из модема придёт строка "XXX". Этого заведомо не произойдёт, поэтому получается просто пауза в 3 сек. Далее посылается пустая строка (\r) для очистки буфера и "AT", ожидается ответ "OK". После этого начинается собственно дозвон и восстанавливается стандартное время ожидания 45 сек.

Наконец, если сервер требует аутентификации в терминальном режиме (что ныне используется крайне редко, поскольку все современные устройства поддерживают протоколы аутентификации, встроенные непосредственно в PPP), то заключительная часть скрипта принимает примерно следующий вид:

chat.script = " ... ATDP*номер* ogin: *имя* assword: *пароль* ''"

ВНИМАНИЕ Категорически важно соблюдать чётность и порядок следования элементов скрипта дозвона. Скрипт всегда начинается ожиданием и завершается посылкой. Чтобы пропустить очередной элемент, используется элемент из двух одинарных апострофов подряд (''', не путать с двойной кавычкой "), означающий пустую строку.

Сценарий не требуется, если устройство NSG соединяется с PPP-сервером напрямую нуль-модемным кабелем или по выделенной модемной линии.

Если используемый порт не имеет сигнала DCD и/или не поддерживает управление потоком (RTS/CTS), то следует установить дополнительные опции, соответственно:

options = "local nocrtscts"

Режим установления и разрыва соединения. Соединение может устанавливаться по требованию или поддерживаться, по возможности, постоянно; это определяется параметром connection. Критериями для его разрыва может быть отсутствие полезного трафика в течение некоторого времени, или достижение максимальной продолжительности сеанса (idle-time, session-time) или отсутствие связи де-факто (параметры lcp-echo-*). Очевидно, что первые два критерия имеют смысл только при connection = "on-demand".

Имя и пароль для аутентификации устройства NSG по протоколам PAP/CHAP на удалённом сервере. Строго говоря, аутентификация выполняется по совокупности 3 параметров: имя клиента, имя сервера и пароль. В данной версии NSG Linux они могут быть указаны двумя способами:

— В общесистемной таблице паролей — в узле .system.ppp-secrets.pap или .system.ppp-secrets.chap (в зависимости от того, какой из протоколов аутентификации используется). Обязательными являются только имя клиента и пароль. Имя сервера используется редко, поэтому обычно вместо него ставится просто звёздочка (*), означающая любое имя. В меню порта указывается только имя клиента (sent-username), которое служит ключом для поиска в таблице паролей.

— Индивидуально для данного порта в параметре sent-password . Если данный параметр присутствует, то он имеет приоритет; в противном случае производится поиск по значению sent-username в общесистемной таблице. Имя сервера и IP-адрес в данном случае не указываются, если они необходимы — следует пользоваться системной таблицей паролей. Для 2-симчатых сотовых модулей допускается ситуация, когда для одного оператора пароль указывается в порту, а для другого — ищется в системной таблице. Данный способ задания пароля применим только для *клиентов* PPP (и производных от него протоколов).

Пароль может содержать в т.ч. спецсимволы, имеющие особое значение в файлах pap-secrets/chap-secrets: @, #, *, *пробел*. Для хранения внутри устройства эти символы преобразуются в соответствующие *esc*-последовательности автоматически. Особыми являются символы " и \ — их необходимо вручную вводить в виде *esc*-последовательностей \" и \\, соответственно.

ВНИМАНИЕ Параметр authentication определяет протокол, по которому устройство NSG будет *требовать* аутентификацию *от удалённой стороны*, и используется, как правило, на стороне сервера. Список протоколов, по которым устройство NSG — как правило, в качестве клиента — согласно (или, строго говоря, *не* согласно) аутентифицировать *себя на удалённой стороне*, определяется параметром refuse-auth . По умолчанию, принимаются любые протоколы аутентификации, запрошенные удалённой стороной, за исключением EAP.

ВНИМАНИЕ Если устройство NSG (или иная *NIX-система) служит одновременно и в качестве клиента, и в качестве сервера по PPP или производным от него протоколам, настоятельно рекомендуется задавать имена и пароли раздельно: для клиентов — непосредственно в меню соответствующих портов, для серверов — в узле system.ppp-secrets .
Возможно также использовать секрет, состоящий не из 2, а из 3 компонент: имени клиента, имени сервера и пароля. Имя сервера в данном случае позволяет использовать каждый пароль только для той или иной задачи.
В частности, данные меры предосторожности абсолютно необходимы, если устройство подключается в качестве клиента к сотовым сетям GPRS, 3G или CDMA с общеизвестными именем и паролем, и одновременно служит сервером для доступа по PPP или PPTP.

IP-адреса. Как правило, в современных сетевых решениях сервер назначает клиентам IP-адреса, а также адреса DNS. Поэтому достаточно использовать настройки по умолчанию:

```
ipcp.accept-address = "true"
ipcp.accept-dns = "true"
ipcp.accept-peer-address = "true"
```

Если адреса не назначаются автоматически, то нужно задать их вручную в параметрах ppp.main.ip-address, ppp.main.peer-ip-address.

Сжатие и защита трафика. Данная версия NSG Linux поддерживает алгоритмы сжатия *deflate*, BSD Compression (BSDC) и защиту трафика с помощью MPPE. Каждый из этих алгоритмов имеет свой набор параметров. Поскольку в корпоративных сетевых решениях программные возможности сторон, как правило, заранее известны, то рекомендуется сразу установить требуемые значения параметров вручную, одинаковым образом на обеих сторонах, чтобы исключить возможные нестыковки. При несогласованных значениях параметров (например, одна сторона требует обязательного использования MPPE, а другая задаёт аутентификацию PAP) PPP-соединение установлено не будет.

При настройке MPPE следует учитывать следующие особенности данного механизма:

1. С точки зрения протокола PPP, MPPE есть частный случай сжатия данных, поэтому для его работы необходимо, в первую очередь, установить data-compression=true .
2. Возможности использования MPPE связаны с выбранным протоколом аутентификации:
   — MPPE–128 может быть осуществлено при MS–CHAP или MS–CHAP v2
   — MPPE–40 может быть осуществлено только при MS–CHAP v2.
   Инициатором аутентификации при этом может быть любая сторона.
3. Если противоположной стороной соединения является компьютер под управлением продуктов компании Microsoft, то необходимо установить режим stateful. В этих продуктах он является единственно возможным для PPP и PPPoE и предпочтительным для PPTP.

Маршрутизация и NAT. Чтобы установить данное PPP-соединение в качестве маршрута по умолчанию, используется параметр default-route. Если в системе существует другой маршрут по умолчанию, например, заданный статически, то необходимо задать им различные метрики.

Что касается маршрутизации в обратную сторону, то в большинстве случаев удалённый сервер назначает клиенту единственный IP-адрес и ничего не знает о сетях, расположенных за этим клиентом. Поэтому на PPP-интерфейсе клиента необходимо включить *NAT masquerading*. В NSG Linux 2.0 правила NAT устанавливаются, как это принято в *NIX-системах, централизованно для всего устройства, в данном случае — в узле ip.nat.POSTROUTING. Однако для удобства пользователя в узле ppp предусмотрена команда add-nat/del-nat, которая автоматически генерирует (и, соответственно, удаляет) соответствующее правило NAT.

ВНИМАНИЕ Команда add-nat/del-nat только создаёт правила NAT, но не применяет их. После включения/выключения NAT необходимо отдельно применить изменения в узле .ip.nat.POSTROUTING.

ПРИМЕЧАНИЕ Если PPP-интерфейс используется в режиме клиента *dial-up* со следующими настройками:
— Соединение устанавливается по требованию (connection = "on-demand")
— Адреса назначаются удаленной стороной (ipcp.accept-address = "true")
то для него в таблице маршрутизации создается запись с некоторыми фиктивными IP-адресами. Это необходимо для того, чтобы направить пакеты на интерфейс в то время, когда соединение отсутствует. После установления PPP-соединения она заменяется записью с фактическими адресами.
Фиктивные адреса в данном случае выбираются случайным образом из приватных диапазонов. Гипотетически может возникнуть ситуация, когда они конфликтуют с существующей схемой распределения адресов в сети. В этом случае следует назначить их явным образом при помощи параметров ip-address, peer-ip-address и разрешить удалённой стороне переопределять оба адреса при установлении соединения:

```
ipcp.accept-address = "true"
ipcp.accept-peer-address = "true"
```

§2.4.6. Инкапсуляция ppp — настройка порта для входящих соединений

Если устройство NSG работает в качестве сервера PPP-доступа, то на нём необходимо выполнить, в большинстве случаев, следующие основные настройки:

Сценарий дозвона, который будет инициализировать модем и ставить его в режим автоответа, например:

```
chat.script = "'' ATZ OK ATS0=1 OK ''"
```

Рекомендуется добавить в скрипт также начальную паузу для старта и инициализации модема. Это требуется не только тогда, когда модем выключается по падению сигнала DTR, но и в общем случае. Дело в том, что современные скоростные устройства могут начать отрабатывать скрипт быстрее, чем модем придёт в исходное состояние после предыдущего соединения. Поэтому рекомендуется следующий скрипт:

```
chat.script = "TIMEOUT 3 XXX-\rAT-OK ATS0=1 OK ''"
```

Если режим автоответа на модеме по каким-либо причинам использовать нельзя, то можно установить в скрипте неограниченное время ожидания и "ручной" ответ на входящий звонок:

```
chat.script = "TIMEOUT 3 XXX-\rAT-OK AT TIMEOUT 0 RING ATA TIMEOUT 45 CONNECT ''"
```

ВНИМАНИЕ Категорически важно соблюдать чётность и порядок следования элементов скрипта дозвона. Скрипт всегда начинается ожиданием и завершается посылкой. Чтобы пропустить очередной элемент, используется элемент из двух одинарных апострофов подряд (''', не путать с двойной кавычкой "), означающий пустую строку.

Сценарий не требуется, если устройство NSG соединяется с клиентом (например, с POS-терминалом) напрямую нуль-модемным кабелем или по выделенной модемной линии.

Если используемый порт не имеет сигнала DCD и/или не поддерживает управление потоком (RTS/CTS), то следует установить дополнительные опции, соответственно:

```
options = "local nocrtscts"
```

Режим установления и разрыва соединения. Соединение устанавливается, как правило, по требованию клиента. Для параметра connection применительно к серверу имеют смысл значения permanent и passive. Рекомендуется использовать режим passive — в этом случае устройство NSG не посылает запросов LCP, а только ждёт, пока они поступят от клиента. Исключением является соединение с клиентом, работающим под управлением продуктов корпорации Microsoft по нуль-модемному кабелю или выделенной линии. Ввиду особенностей архитектуры драйверов в этих продуктах, их PPP-клиент в такой ситуации не может начать работу первым и должен сначала получить что-либо от сервера, поэтому на сервере необходимо установить режим permanent. (Кроме того, необходимо установить специальный драйвер NSG для асинхронной нуль-модемной линии, или аналогичный драйвер от другого производителя; встроенный нуль-модемный драйвер Microsoft предназначен только для эмуляции локальной сети и непригоден для PPP-соединений.)

Критериями для разрыва соединения, как и в случае клиента, может быть отсутствие полезного трафика в течение некоторого времени, достижение максимальной продолжительности сеанса (idle-time, session-time) или отсутствие связи де-факто (параметры lcp-echo-*).

Аутентификация удалённых клиентов на устройстве NSG производится только встроенными средствами протокола PPP. Необходимо выбрать протокол аутентификации (ppp.main.authentication) и источник аутентификации (ppp.main.authentication-scheme): локальная таблица пользователей PPP (local) или системный механизм аутентификации (system-aaa), позволяющий задействовать централизованные серверы RADIUS или TACACS+.

Локальная таблица пользователей для *сервера* PPP (и производных от него протоколов) всегда хранится в узле .system.ppp-secrets.pap или .system.ppp-secrets.chap. Каждая запись таблицы содержит 3 параметра: имя клиента, имя сервера и пароль. В качестве имени сервера может быть указана просто звёздочка (*), означающая любое имя; по существу же это должно быть имя устройства NSG, заданное параметром system.hostname (или специальное имя, заданное дополнительными опциями pppd).

ВНИМАНИЕ Если устройство NSG (или иная *NIX-система) служит одновременно и в качестве клиента, и в качестве сервера по PPP или производным от него протоколам, настоятельно рекомендуется задавать имена и пароли раздельно: для клиентов — непосредственно в меню соответствующих портов, для серверов — в узле system.ppp-secrets .
Возможно также использовать секрет, состоящий не из 2, а из 3 компонент: имени клиента, имени сервера и пароля. Имя сервера в данном случае позволяет использовать каждый пароль только для той или иной задачи.
В частности, данные меры предосторожности абсолютно необходимы, если устройство подключается в качестве клиента к сотовым сетям GPRS, 3G или CDMA с общеизвестными именем и паролем, и одновременно служит сервером для доступа по PPP или PPTP.

Дополнительно в таблице может быть указан список IP-адресов, с которых разрешено работать данному клиенту. Если клиент при установлении PPP-соединения не имеет собственного адреса и просит назначить ему адрес, то сервер NSG посылает ему первый адрес из этого же списка.

Если используется централизованная аутентификация, то она настраивается в узле .system.aaa.ppp . В данном узле следует составить список, каждый элемент которого описывает некоторый сервер аутентификации. Обязательными параметрами для каждого сервера являются его тип (RADIUS или TACACS+), IP-адрес (server) и ключ для доступа к серверу (secret). Если в списке содержится более одного элемента (сервера), то они рассматриваются последовательно в порядке нумерации; при этом, если получен положительный ответ от очередного сервера, то аутентификация считается успешной и завершается, если получен отрицательный ответ или он не получен вообще за установленный таймаут, то делается попытка аутентифицироваться на следующем сервере. Если список серверов исчерпан и ни от одного из них не получено положительного ответа, то аутентификация считается неудачной. Подробнее о системном механизме аутентификации см. Часть 1.

IP-адреса. Как правило, сервер PPP-доступа знает собственный IP-адрес и назначает IP-адреса клиентам. При этом PPP-интерфейсы сервера часто делаются ненумерованными и все используют один и тот же адрес, "позаимствованный у" ("*borrowed from*") какого-либо другого интерфейса, чаще всего, Ethernet. Этот адрес указывается в параметре ppp.main.ip-address .

Адреса для клиентов должны быть разными для разных портов и могут устанавливаться двумя способами. Один вариант — адреса указываются в параметре ppp.main.peer-ip-address каждого порта; в этом случае все клиенты, подключающиеся к данному порту сервера, будут использовать этот адрес. Другой вариант — адреса указываются индивидуально для каждого клиента в локальной таблице пользователей или на централизованном сервере аутентификации RADIUS/TACACS+; в этом случае каждый клиент будет иметь один и тот же адрес независимо от того, к какому порту он подключён. Если настроены и те, и другие адреса, то приоритет имеют адреса, привязанные индивидуально к клиентам — как более специфичные.

ПРИМЕЧАНИЕ В данной версии NSG Linux 2.0 обработка IP-адресов, назначаемых клиентам централизованно сервером RADIUS/TACACS+, не поддерживается. Устройство NSG назначает клиентам IP-адреса, определяемые локальной настройкой peer-ip-address, и игнорирует адреса, присылаемые сервером аутентификации.

В любом случае, адреса сторон в PPP-соединении никак не связаны друг с другом. Ясности ради, можно выбрать адреса традиционным образом — из одной сети с маской /30, но настоятельной необходимости в этом нет. Адреса могут быть произвольными, понятия сети и маски для PPP-соединений не имеют смысла.

Помимо адресов, в большинстве задач клиентам требуется передать один или несколько адресов DNS, которые указываются в узле ppp.main.ipcp .

Сжатие и защита трафика. К сжатию трафика "на лету" и его защите в PPP-соединениях относится всё сказанное в предыдущем параграфе для клиента PPP.

Маршрутизация и фильтрация. Очевидно, что PPP-интерфейс для сервера, как правило, не является маршрутом по умолчанию, поэтому следует установить ppp.main.default-route = "false".

При установлении соединения создаётся маршрут к удалённому клиенту через данный сетевой интерфейс. Про сети, расположенные за клиентом, сервер ничего не знает. В большинстве случаев ему незачем это знать, поскольку все эти сети скрыты за *NAT masquerading* на клиенте; с точки зрения сервера, все они вместе с клиентом составляют единый, непосредственно подключённый, хост.

Если NAT не используется и необходимо указать маршруты в сети, расположенные за PPP-клиентом, то проблема, как правило, состоит в том, что заранее неизвестно, к какому из портов сервера подключится данный клиент в очередной раз и какой IP-адрес он при этом получит. Для этой задачи возможны два решения:

— Каждому клиенту назначается специфический IP-адрес при аутентификации по локальной таблице пользователей или от централизованного сервера RADIUS/TACACS+, и задаются статические маршруты в удалённые сети через этот адрес как gateway.

— Используется динамическая маршрутизация (RIP, OSPF).

Дополнительно на сервере PPP-доступа рекомендуется создать в узле .ip.filter.FORWARD фильтр, который будет запрещать отправку пакетов, адресованных PPP-клиентам, через интерфейс, служащий маршрутом по умолчанию. Дело в том, что если клиент разорвал соединение, а для него продолжают поступать пакеты, то, поскольку маршрута к клиенту уже нет, эти пакеты будут отправляться по умолчанию на вышестоящий хост, оттуда снова возвращаться на PPP-сервер и так далее до тех пор, пока у них не истечёт TTL. В принципе, эта ситуация не грозит никакими катастрофическими последствиями, но создаёт бесполезную нагрузку на сеть; в некоторых случаях она может быть существенной — например, когда к клиенту продолжает идти недосмотренный видеопоток или большой недозакачанный файл. Подробно о настройке IP-фильтров и NAT см. Часть 3.

§2.4.7. Инкапсуляция ppp — отладка и тонкая настройка

Поскольку процедура PPP-соединения очень сложная и многоступенчатая, в ней всегда есть много потенциальных мест для возникновения ошибок. Поэтому для PPP-соединений особенно важно иметь отладочные инструменты и уметь пользоваться ими.

Лог работы порта PPP можно просмотреть командой log или ppp.log . В логе отражается исполнение как скрипта дозвона, так и процедуры LCP. При возникновении проблем следует в первую очередь определить, на каком из этих двух этапов происходит сбой. Далее, если дозвон происходит нормально, а проблема связана с LCP, нужно включить отладку командой ppp.main.debug-level = 1, повторить попытку и изучить лог в соответствии с принципами, описанными в п.§2.4.4. Если самостоятельно разрешить проблему не представляется возможным, лог следует передать в службу технической поддержки NSG по электронной почте.

Состояние порта можно просмотреть командой ppp.show . Если порт находится в состоянии UP, но пакеты через него не отправляются, следует проверить текущую таблицу IP-маршрутизации — ip.route.show .

В дополнение к параметрам, явно перечисленным в узле ppp.main, пользователь может задавать большинство других настроек, предусмотренных для pppd. (Исключением являются отдельные функции, не включённые при генерации NSG Linux — например, *multilink*.) Список дополнительных опций (через пробел) указывается в поле ppp.main.options . Такие опции могут потребоваться для тонкой настройки PPP в некоторых сложных случаях. Полный список опций pppd содержится в соответствующих *man pages*.

§2.4.8. Инкапсуляция login

Инкапсуляция login для порта RS–232 означает, что данный порт будет использоваться для входа в систему в консольном режиме. В отличие от выделенного консольного порта, настройка которого возможна только за пределами данной операционной среды (т.е. только в сервисном режиме, см. Часть 1), настройка порта в данном случае производится внутри основной операционной среды. В частности, его инкапсуляция может быть изменена на любую другую в любое время.

Следует подчеркнуть, что такой порт не является, однако, системной консолью в буквальном смысле. Понятие "системная консоль" играет особую роль в конфигурации системы (строго говоря, прописывается особым образом в строке запуска ядра Linux и/или основных конфигурационных файлах) и включает в себя две функции, в общем случае, никак не связанные друг с другом: вывод отладочных сообщений ядра Linux и возможность интерактивного входа в систему. В данном случае порт не является особым и выполняет только вторую из этих функций. Основные различия между выделенным консольным портом и портом с инкапсуляцией login приведены в таблице.

	Выделенный консольный порт	**Порт RS–232 с инкапсуляцией** login
Вывод диагностических сообщений ядра	Да	Нет
Вход в систему	Да	Да
Настройка	Только из сервисного режима (если предусмотрено для данной модели и для данной версии ПО сервисного режима)	Только из основного режима работы
Возможность переконфигурации для передачи пользовательских данных с иной инкапсуляцией		Да

§2.4.9. Инкапсуляция one-wire

Инкапсуляция one-wire для порта RS–232 означает, что данный порт используется для работы с датчиками и контроллерами технологического управления на основе шины 1–Wire. К порту должен быть подключён адаптер RS–232/1–Wire (Элин ML97U или аналогичный). В этом случае порт RS–232 становится равнозначен порту 1–Wire, и в меню порта появляется узел 1–Wire со специфическими параметрами и командами. Дальнейшая настройка производится аналогично настройке порта 1–Wire (см.§2.9).

§2.4.10. Инкапсуляция reverse-ssh

Инкапсуляция reverse-ssh предназначена для безопасного доступа по сети к физическому порту устройства NSG. В отличие от reverse-telnet, выбор порта определяется не номером порта TCP, а именем и паролем пользователя; подключаться во всех случаях следует по номеру порта TCP, назначенному для службы SSH.

ВНИМАНИЕ При изменении имени пользователя необходимо сначала применить данное изменение, и только затем устанавливать пароль для него.

Зайдя на устройство NSG с указанным именем и паролем, пользователь попадает не в одну из командных оболочек системы, а прозрачным образом в асинхронный кабель, и может передавать по нему данные в целом так же, как если бы он был подключён к этому кабелю непосредственно COM-портом своего компьютера. Служба Reverse SSH принимает входящее зашифрованное соединение, расшифровывает данные из него и транслирует эти данные в физический порт и обратно.

В отличие от Telnet, сервер SSH работает в прозрачном режиме. Но к нему подключаются, с одной стороны, клиент SSH, а с другой — утилита nsgcu для работы с асинхронным портом. И тот, и другая могут истолковывать определённые символы и последовательности как управляющие, и в этом случае передача будет не полностью прозрачной. Для передачи бинарных потоков необходимо установить пустые значения *escape*-символов как на стороне клиента (например, вызовом ssh -e none ...), так и на стороне устройства NSG (фактически они относятся не к серверу SSH, а к nsgcu).

§2.5. Настройка модемов для коммутируемых линий

§2.5.1. Типы и идентификация модемов для коммутируемых телефонных линий

Для передачи данных по коммутируемым линиям телефонных сетей общего пользования (ТФОП) в устройствах NSG используются сменные модули:

type = "rs-232" Модули IM–V92 (снят с производства), IM–V34

Оба типа модулей представляют собой встраиваемые модемы, работающие через внутренний асинхронный интерфейс. По этой причине они идентифицируются как rs-232 и настраиваются так же, как порт RS–232 с подключённым к нему внешним модемом. Для управления используется стандартный набор основных AT-команд. Модемы поддерживают протоколы ITU–T V.92, V.34 соответственно, а также младшие модемные протоколы.

§2.5.2. Аппаратное управление модемом

Перемычка J1 на модуле определяет его поведение при падении сигнала DTR внутреннего асинхронного интерфейса. Если она установлена, электропитание модуля выключается при падении DTR; таким образом, модуль аппаратно рестартует при каждом рестарте порта. Это позволяет гарантированно вывести его из любого нештатного состояния, но требует некоторого времени (2–3 сек.) для старта модуля и загрузки его встроенного программного обеспечения. В большинстве задач рекомендуется использовать эту возможность.

§2.5.3. Настройка асинхронного интерфейса

Модемные модули работают с устройством через внутренний асинхронный интерфейс. Параметры этого интерфейса со стороны шасси могут быть любыми; модуль, по умолчанию, настроен в режиме автоматического определения скорости и режима передачи в порту (если иное не установлено намеренно с помощью соответствующих AT-команд). Рекомендуется использовать настройки по умолчанию: 8n1 и аппаратное управление потоком.

Выбор оптимальной скорости в порту зависит от характера задачи. Для передачи относительно больших объёмов трафика (резервное подключение офисов, сбор статистики с удалённых объектов) следует установить в порту максимальную скорость — 115200 или 230400 бит/с, особенно если передаются данные с высокой степенью сжимаемости (несжатая статистика).

ВНИМАНИЕ Необходимо различать скорость в асинхронном порту между шасси и модемом и скорость в модемной линии. Скорость в линии не может быть выше, чем скорость в порту. Поскольку модем может выполнять сжатие данных, обычно рекомендуется устанавливать скорость в порту в 2–4 раза выше максимально возможной для данной линии.

С другой стороны, для применений, заведомо не требующих высокой скорости, рекомендуется ограничить скорость в порту; при этом автоматически будет ограничена скорость в линии, согласование между модемами начнётся с меньших скоростей, завершится быстрее, а полученное низкоскоростное соединение будет более надёжным. Типичный пример такой задачи — подключение банкомата или POS-терминала; в этом случае рекомендуется ограничиться значением по умолчанию 9600 бит/с, а на заведомо низкокачественных линиях уменьшить его до 2400 бит/с.

§2.5.4. Инкапсуляция reverse-telnet — прямой доступ к модему

Инкапсуляция reverse-telnet для модемного модуля обеспечивает прямой доступ к модему. Пользователь может подключиться к устройству по Telnet по выбранному порту TCP и в результате попадает непосредственно во внутренний асинхронный порт, к которому подключён модем. В результате он может управлять модемом вручную с помощью AT-команд, в частности, удостовериться в работоспособности модема, установить какие-либо специфические режимы работы, установить вручную требуемый протокол и скорость в линии, выполнить исходящее соединение с удалённым модемом или ответить на входящее. Обычно такие операции требуются только для отладки работы модема.

ПРИМЕЧАНИЕ Протокол Telnet предназначен для передачи текстовых символов и не является полностью прозрачным, поскольку некоторые бинарные символы в нём могут иметь специальное значение и не передаваться на удалённую сторону (например, CTRL-]). Для передачи произвольного бинарного трафика следует использовать инкапсуляцию raw-tcp.

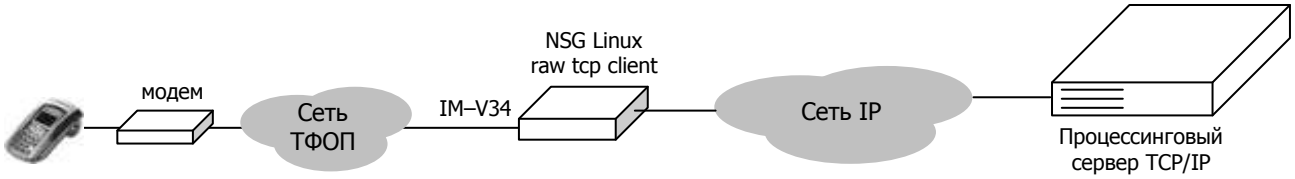
§2.5.5. Инкапсуляция raw-tcp

Инкапсуляция raw-tcp настраивается аналогично таковой в порту RS–232. Подробно о настройке данной инкапсуляции см.§2.4.3. Поскольку она не предусматривает управления модемом, возможности её применения в данном случае ограничены; тем не менее, она решает ряд практических задач.

Важнейшая из таких задач — это построение сервера *dial-up* доступа для POS-терминалов, не имеющих встроенного сетевого протокола. В этом случае модем устанавливает физическое соединение самостоятельно в режиме автоответа на входящие звонки. Порт настраивается в режиме клиента raw-tcp и транслирует это соединение далее по сети TCP/IP к заданному серверу. На модеме рекомендуется выполнить (в режиме прямого доступа, см. след. параграф) следующие предварительные настройки:

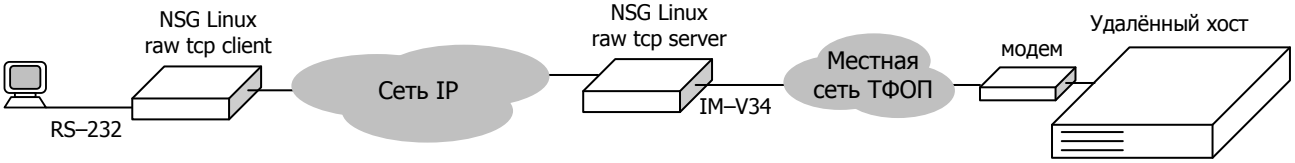
ATE0	Отключить эхо
ATQ1	Отключить сообщения модема
ATS0=1	Автоответ после 1 звонка
AT&W	Сохранение настроек

Первые две из этих команд позволяют избежать отправки на сервер сообщений модема типа OK, ERROR, CONNECT. Поскольку эти сообщения не предусмотрены протоколом обмена между POS и сервером, реакция сервера на них может быть неадекватной.



Подключение POS-терминала к процессинговому серверу по модемной линии и сети TCP/IP

Другой возможный сценарий для применения инкапсуляции raw-tcp — это использование устройства NSG в качестве удалённого модема. Модемный порт настраивается в качестве сервера Raw TCP; пользователь, зайдя на этот порт с удалённого клиента, может выполнить исходящее соединение в местной телефонной сети. Поскольку соединение Raw TCP между устройствами NSG прозрачное для любых бинарных данных, поверх него и последующего модемного соединения могут работать любые протоколы, например, PPP или X/Y/Zmodem.



Удалённый доступ к модему на устройстве NSG

§2.5.6. Инкапсуляция ppp

Инкапсуляция ppp для модемного модуля настраивается аналогично таковой в порту RS–232, см.§2.4.4–§2.4.7. Модемный порт NSG может использоваться как в режиме клиента для подключения к удалённому серверу PPP, так и в режиме сервера для подключения удалённых клиентов PPP (в частности, POS-терминалов с встроенным стеком TCP/IP и *dial-up* модемом).

Применительно к модемным модулям NSG для телефонных линий, настройка PPP не имеет особенностей, за исключением того, что рекомендуется во всех случаях использовать аппаратный рестарт (установить перемычку J1 на модуле) и включить в скрипт дозвона начальную задержку, чтобы дать модулю время на инициализацию:

```
chat.script = "TIMEOUT 3 XXX-\rAT-OK ... "
```

§2.6. Настройка сотовых интерфейсов GSM/UMTS и CDMA

§2.6.1. Типы и идентификация интерфейсов Wireless WAN (WWAN)

Для передачи данных по сотовым сетям GSM, GSM/UMTS* и CDMA в устройствах NSG используются встроенные интерфейсы (NSG–600, NSG–1800, NSG–1820), сменные модули и опции. Все современные модули WWAN, выпускаемые компанией NSG, используют для соединения с шасси внутренний интерфейс USB; к ним относятся:

type = "3g"	Модуль UM–3G *h/v ver.6*, опция opt18xx.3G.6 (чипсет Fibocom H330)
type = "3g"	Модуль UM–3G *h/v ver.3, 4* (чипсет SimCom SIM5320, *снят с производства*)
type = "3g"	Модуль UM–3G *h/v ver.2* (чипсет SimCom SIM5216, *снят с производства*)
type = "3g"	Модуль UIM–3G *h/v ver.1* (чипсет SimCom SIM5210, *снят с производства*)
type = "edge-3a"	Модуль UIM–EDGE *h/v ver.3a* (чипсет SimCom SIM700, *снят с производства*)
type = "edge"	Модуль UIM–EDGE *h/v ver.3* (чипсет SimCom SIM700, *снят с производства*)
type = "cdma"	Модуль UM–EVDO/A *h/v ver.7*, опция opt18xx.CDMA.7 (чипсет ATEL EP45)
type = "cdma"	Модуль UM–EVDO/A *h/v ver.5* (чипсет CMOTech CNE–680, *снят с производства*)
type = "cdma"	Модуль UIM–EVDO *h/v ver.2* (чипсет CMOTech CNE–550, *снят с производства*)
type = "cdma"	Модуль UIM–CDMA *h/v ver.2* (чипсет CMOTech CNE–510, *снят с производства*)

Фиксированные порты WWAN в устройствах серий NSG–600 и NSG–1820 (обр. 2012 г.) называются 3g, edge, edge-3a или cdma, соответственно; опции в NSG–1800 и NSG–1820MC — m1, m2, m3 в зависимости от того, в какой позиции они установлены. Сменные модули в NSG–1800 и NSG–700 получают имена s1, s2 в зависимости от номера разъёма расширения. Идентификация USB-модулей в NSG Linux 2.0 может выполняться автоматически командой update. Особенности работы разных модификаций одного типа модулей учитываются автоматически и не требуют внимания пользователя (в отличие от NSG Linux 1.0).

Внутренний интерфейс USB не предусматривает никаких настроек физического уровня. Меню порта содержит только протокольные параметры, которые зависят от выбранной инкапсуляции 2 уровня. При смене инкапсуляции в меню появляются и удаляются соответствующие узлы.

Помимо перечисленных выше сотовых модулей, в устройствах NSG–700 (но не NSG–1800) могут использоваться также модули ранних модификаций, выпущенные в 2004–2009 гг. и работающие через внутренний асинхронный порт. Особенности настройки таких модулей приведены в §2.6.10.

§2.6.2. Аппаратное управление сотовым модемом

Перемычка J1 на модуле определяет его поведение при падении сигнала DTR внутреннего асинхронного интерфейса. Если она установлена, электропитание модуля выключается при падении DTR; таким образом, модуль аппаратно рестартует при каждом рестарте порта. Это позволяет гарантированно вывести его из любого нештатного состояния, но требует некоторого времени (в среднем, 30–35 сек.) на старт модуля, загрузку его встроенного программного обеспечения и регистрацию в сети оператора. В большинстве задач настоятельно рекомендуется использовать эту возможность.

ПРИМЕЧАНИЕ Для модулей UIM–EVDO *h/v ver.2*, UIM–CDMA *h/v ver.2*, используемых на шасси NSG–700 под управлением NSG Linux 1.0, ранее рекомендовалось отключить аппаратный рестарт (снять перемычку), поскольку он происходил некорректно. В NSG Linux 2.0 эта проблема решена и аппаратный рестарт следует использовать так же, как и на других модулях.

Модули для сетей GSM и GSM/UMTS поддерживают 2 SIM-карты и позволяют подключаться к одному либо к другому оператору. Верхняя SIM-карта всегда считается основной (main), нижняя — вспомогательной (aux). Выбор SIM-карты происходит в момент рестарта модуля, т.е. рестарт является обязательным условием для этого. Перемычка J2 на этих модулях устанавливает режим выбора SIM-карты:

Установлена	Всегда используется верхняя SIM-карта.
Снята	Используемая SIM-карта выбирается программно.

ВНИМАНИЕ Аппаратное управление сотовым модемом не может использоваться в разъёме расширения s2 на устройствах NSG–700/4AU модификации *h/w ver.5* и более ранних. В случае категорической необходимости установить сотовый модуль именно в этот разъём — обязательно следует: перемычку аппаратного рестарта снять, перемычку выбора SIM-карты установить. Модуль всегда будет работать с основной SIM-картой и без рестарта.

Для фиксированных сотовых интерфейсов в устройствах серий NSG–600 и NSG–18*xx* аппаратный рестарт и программный выбор SIM-карты включены конструктивно и не выключаются.

* В просторечии именно эти сети называются 3G. Это не вполне верно, поскольку понятие 3G включает в себя целый ряд различных технологий и услуг, в т.ч. UMTS, CDMA 2000 и другие.

§2.6.3. Прозрачный доступ к модулю и ручной рестарт модуля

Если порт не находится в работе, т.е. имеет encapsulation = "none" или adm-state = "down", то в меню порта доступна команда raw-access . Она позволяет зайти на модем в терминальном режиме и управлять им вручную с помощью AT-команд. Таким образом можно убедиться в работоспособности модема, проверить установление входящих и исходящих соединений, установить и сохранить параметры конфигурации самого модема. Наиболее важные AT-команды для управления сотовыми интерфейсами приведены в Приложении 2–A.

Ручной рестарт модуля производится командой restart.

Дополнительное поле ввода в обеих командах позволяет явно выбрать нужную SIM-карту для 2-симчатых модулей: main либо aux. Если параметр не указан, модуль стартует с главной SIM-картой (если для неё не установлено число попыток 0) и отсчёт числа попыток для программного выбора SIM-карты начинается заново. Подробно о работе с 2 SIM-картами см. §2.6.5.

При выполнении рестарта в качестве скрипта nsgsh указание SIM-карты является обязательным, например:

```
nsgsh -q .port.edge.restart.main
```

Чтобы выполнить рестарт без принудительного выбора SIM-карты, в данном случае следует ввести после последней точки любое продолжение, отличное от main и aux.

ВНИМАНИЕ Команда restart с явно указанным параметром main или aux изменяет текущую конфигурацию устройства, устанавливая число попыток для одной и для другой SIM-карты 0 и 1, соответственно. Если после этого выполнить команду "сохранить", то эти значения так и останутся в конфигурации навсегда. Поэтому после применения команды необходимо восстановить прежние значения вручную, либо рестартовать устройство без сохранения.

Режим ручной настройки модема применяется, как правило, на этапе первоначальной установки устройства. В этом режиме следует проверить:

— Наличие SIM-карты и отключение PIN-кода (и отключить его, если он не отключён) — команды AT+CPIN, AT+CLCK или AT$$CHV1, AT$$DISCHV1/AT$$ENACGV1 или AT+RLOCK в зависимости от типа модуля (подробнее см. Приложение 2–A).

— Уровень сигнала сотовой сети (при необходимости, оптимизировать его за счёт перемещения антенны) — AT+CSQ или AT+CSQ?

— Имя сотового оператора GSM/UMTS — AT+COPS?

— Регистрацию в сети и доступность услуг — AT+CREG?, AT+CGREG?, AT$$CURRSTATE, AT$$NLOC, AT+STATE .

— Возможность соединения на физическом уровне с помощью команды ATD... При успешном соединении будет получен ответ CONNECT и далее, с небольшим интервалом, LCP-запросы (короткие бинарные пакеты, начинающиеся и кончающиеся знаком ~). Если физическое соединение устанавливается, то вручную больше делать нечего, следует приступать к отладке PPP-соединения.

ВНИМАНИЕ Вопреки распространённому мнению, уровень сигнала сотовой сети является, в большинстве случаев, далеко не определяющим параметром для успешной работы модема. Чаще всего он является достаточно высоким (>10 условных единиц) и относительно постоянным. Поэтому в постоянном мониторинге этого параметра нет никакой необходимости (по крайней мере, на стационарных объектах). Более существенную роль играет целый ряд других обстоятельств, таких как загруженность соты, канала от базовой станции в вышестоящую сеть, вышестоящих каналов связи и узлов сети.

Для модемов GSM и UMTS перемещение антенны в разумных пределах (± длина антенного кабеля), а также её ориентация в пространстве, чаще всего не играет существенной роли. (Кроме очевидных случаев, например, перемещения из внутреннего угла железобетонных стен на окно.) Технология CDMA, напротив, очень чувствительна к положению антенны: даже небольшое перемещение, в пределах 30–50 см, может сильно изменить уровень принимаемого сигнала. Антенна CDMA всегда должна располагаться вертикально.

В отдельных сложных случаях следует обратить внимание также на следующие параметры:

— Выбранный тип услуги (GPRS/EDGE/WCDMA/HSDPA или CDMA 1x/EV-DO).

— Выбранный оператор. В зависимости от типа модема и прошивки, имели место случаи, когда при большой разнице уровня сигнала "своего" и "чужого" оператора модем пытался зарегистрироваться в сети "чужого" оператора. При этом команда AT+CSQ показывала вполне нормальный уровень сигнала (чужого), но никакие услуги, естественно, не предоставлялись.

— Устойчивость выбора соты. Если модем часто переключается из одной соты в другую, то это может означать, что сигнал от обеих базовых станций примерно одинаково слаб. Следует подобрать положение антенны так, чтобы улучшить приём хотя бы одного из сигналов (не важно, какого именно).

§2.6.4. Инкапсуляция ppp

Настройка инкапсуляции PPP для сотовых интерфейсов производится в основном так же, как для портов RS–232 и модемных модулей IM–V34 (см. §2.4.4–§2.4.7, §2.1.2).

ВНИМАНИЕ Услуги пакетной передачи данных в сетях 2G и 3G всегда подразумевают PPP-соединение между пользователем и сетью. (Теоретически предусмотрены также некоторые другие протоколы, например, X.28 PAD, но на практике они не реализуются.) Соединения "точка-точка" между двумя клиентами напрямую не предусмотрены и могут быть реализованы только как IP-соединения между двумя узлами, подключёнными к общей IP-сети (см. §2.6.7**).**

Использование протокола PPP для пакетных услуг сотовых сетей имеет следующие особенности:

1. **Разблокировка SIM-карты.** В большинстве случаев каждая попытка соединения начинается с аппаратного рестарта модема и его регистрации в сети. Это требовало бы, по аналогии с обычным сотовым телефоном, ввода PIN-кода. Теоретически его можно ввести в скрипте дозвона, но на практике это весьма рискованно: при неправильно введённом PIN-коде скрипт отработается 3 раза и SIM-карта будет заблокирована, прежде чем пользователь заподозрит неладное. Предполагается, что в устройствах NSG SIM-карта недоступна для посторонних лиц и используется только для работы в этом устройстве. Поэтому при настройке можно исходить из того, что PIN-код на ней заранее отключён. Для этого нужно либо вставить SIM/R–UIM карту в сотовый телефон, либо подключиться к модулю напрямую (см. выше) и использовать соответствующие AT-команды в зависимости от типа модуля.

2. **Точка доступа** (Access Point Node, APN) — специфический параметр для сетей GSM и UMTS. Определяет сервер доступа, с которым будет работать данный клиент, и фактически заменяет собой номер телефона для *dial-up* доступа. APN назначается оператором и является критически важным параметром, поскольку услуга в сети оператора устанавливается на конкретном APN для каждого клиента. Если APN указан неправильно, то PPP-соединение с сетью устанавливаться не будет или будет работать с неправильными настройками (например, с динамическим IP-адресом из общего пула вместо заданного статического адреса).

   APN устанавливается в модеме в составе так называемого GPRS-контекста — совокупности параметров, описывающих модемное соединение. По существу, это основной и единственный значимый параметр в нём. Контекст устанавливается командой AT+CGDCONT=номер_контекста,тело_контекста. В некоторых моделях сотовых модулей он сохраняется в энергонезависимой памяти, в других — нет; для единообразия рекомендуется всегда использовать данную команду в составе скрипта.

ВНИМАНИЕ Операторы GSM/UMTS могут предлагать услуги типа "доступ в Интернет без настроек", для которых не требуется устанавливать ни имя APN, ни имя/пароль пользователя. Эта же услуга может предоставляться автоматически, если указанные параметры введены неверно. Однако следует иметь в виду, что услуга в этом случае может тарифицироваться по максимальной ставке (как WAP). Для операторов это удобный и технически безупречный способ получения максимальной прибыли от некомпетентных пользователей. В целях экономии средств настоятельно рекомендуется задавать APN, имя и пароль в явном виде, а также обращать внимание на то, по какому классу тарифицируется ваш трафик в выставляемых счетах.

3. **Модемный скрипт.** По существу, подключение к сотовой сети в пакетном режиме есть отдельная операция, имеющая мало общего с телефонным звонком, и она осуществляется специальной AT-командой. Однако для удобства записи модемных команд в клиентах, изначально ориентированных на обычные *dial-up* модемы, она имеет синоним: ATD#777 для модемов CDMA и ATD*99****номер_контекста#* для сетей GSM и GPRS.

   Настройка скрипта производится в узле chat. Для большинства случаев подходят типовые скрипты, выработанные в ходе эксплуатации устройств с сотовыми модулями. Поэтому в NSG Linux 2.0 предусмотрен упрощённый набор параметров: пользователю нужно ввести только начальный таймаут, необходимый для инициализации модуля, и для сетей GSM/UMTS — имя APN. После этого автоматически генерируется скрипт следующего вида, соответственно:

   ```
   TIMEOUT таймаут XXX-\rAT-OK ATD#777 CONNECT ''          или
   TIMEOUT таймаут XXX-\rAT-OK AT+CGDCONT=1,"IP","apn" OK ATD*99***1# CONNECT ''
   ```

   Величина начального таймаута по умолчанию — 30 секунд. Это средняя величина, подходящая для большинства случаев. Иногда она может быть уменьшена или, наоборот, должна быть увеличена в зависимости от типа модуля, особенностей конкретной сети и т.п. Следует заметить, что по мере усложнения и совершенствования технологий это время, как правило, увеличивается: от 10–15 сек. для первых модулей IM–GPRS *h/w ver.1* до, иногда, 35–40 сек в сетях CDMA EV-DO и UMTS HSDPA.

   Автоматически созданный скрипт можно просмотреть командой show.

   Если автоматический скрипт недостаточен, то пользователь может ввести скрипт целиком в поле script. Явно заданный скрипт имеет приоритет перед всеми параметрами, заданными отдельно. В большинстве таких случаев достаточно скопировать автоматически построенный скрипт из команды show и вставить в него нужную пару AT... OK .

4. **Режим соединения.** Услуга пакетного подключения по сути своей предназначена для постоянного соединения и тарифицируется по объёму переданных/принятых данных. В то время, когда обмена данными нет, она ничего не стоит и не препятствует работе других услуг. Поэтому для пакетных соединений рекомендуется использовать режим connection="permanent"; режим on-demand для них нецелесообразен. Режим passive в данном случае не имеет смысла.

5. **Контроль соединения.** Для пакетных сотовых соединений, особенно для соединений GPRS/EDGE, абсолютно необходим механизм LCP Echo, следящий за их фактической работоспособностью. Во всех практических реализациях гарантированная минимальная скорость передачи не устанавливается, и де-факто скорость может падать до нуля (в GPRS/EDGE — строго до нуля), при том, что соединение номинально существует и никаких явных сигналов о его разрыве (NO CARRIER, LCP Reset, падение DCD) на физическом уровне не поступает. Достоверно обнаружить такую ситуация возможно только средствами LCP Echo или аналогичных механизмов (*ping*, DPD и т.п.) вышележащих уровней. Для уверенного обнаружения рекомендуется, исходя из практического опыта, устанавливать суммарное время 30–45 сек (3 попытки по 10–15 сек); при уменьшении этого параметра возможны ложные срабатывания.

   По стандарту, каждая сторона PPP-соединения обязана отвечать на входящие пакеты LCP Echo Request даже в том случае, если не посылает свои. К сожалению, в некоторых сетях сотовых операторов могут встречаться нарушения стандарта. В этом случае вместо LCP Echo следует использовать *ping* или другие механизмы 3 и более высоких уровней в сочетании со скриптами, рестартующими сотовый интерфейс. В устройствах NSG для этой цели имеется сервис *netping*, позволяющий быстро настроить необходимые процедуры даже пользователям без специального знания ОС Linux (см. Часть 4).

   Пакеты LCP Echo выполняют ещё одну важную функцию: они поддерживают более или менее постоянный поток данных и предотвращают переход модуля в "спящий" режим.

6. **Имя и пароль пользователя.** Поскольку в сотовой сети устройство NSG является всегда клиентом, то пароль для него можно и нужно указывать непосредственно в настройках порта, в узле sent-password . Использовать для этой цели общесистемные таблицы паролей PAP и CHAP (.system.aaa.ppp-secrets) нецелесообразно, а в некоторых случаях может быть даже небезопасно для системы в целом.
   Как правило, в сетях GSM/UMTS используется протокол аутентификации PAP, в сетях CDMA — CHAP. В любом случае, аутентификация производится только средствами PPP, а не в терминальном режиме.

7. **IP-адреса.** В подавляющем большинстве случаев IP-адреса в сотовых сетях назначаются оператором. Это относится и к услуге "статических адресов" — под этим термином сотовые операторы понимают совсем не то, что сетевые инженеры. В сотовых сетях он обычно означает только то, что IP-адрес для данной SIM-карты назначается заранее известный — один из пула, состоящего только из этого единственного адреса (вместо случайного адреса из большого общего пула). Но, тем не менее, он назначается именно оператором, и на клиентском устройстве должна быть включена установка accept-address="true" . Прописывать этот адрес статически на клиентском устройстве не требуется.

   Как правило, базовая услуга доступа в Интернет, предоставляемая сотовыми операторами, подразумевает динамический приватный адрес в сети оператора. Выход из сети оператора в Интернет производится через NAT оператора, что накладывает ряд ограничений — например, хосты из внешнего мира не могут инициировать обращения к сотовому клиенту. Преодолеть это ограничение без подписки на дополнительные услуги возможно, если сотовый клиент после соединения инициирует установление любого туннеля (PPTP, IPsec, STunnel, etc.) на центральный сервер корпоративной сети. Когда такой туннель установлен, хосты из центрального офиса могут обращаться к сотовому клиенту в удалённом офисе и к устройствам в локальной сети удалённого офиса, расположенным за ним, так же, как и по физическому каналу WAN "точка-точка".

   Для использования дополнительных услуг (VPN, статические и/или реальные IP-адреса) в сетях GSM/UMTS организуется специальная точка доступа. В сетях CDMA для этой цели требуется аутентификация пользователя по существу — с уникальными именем и паролем, в соответствии с которыми выбирается IP-адрес или другая специфическая услуга.

ПРИМЕЧАНИЕ Термин "VPN" в сотовых сетях также обычно имеет иное значение, нежели в других отраслях IP-технологий. Как правило, под ним подразумевается закрытая сеть, изолированная от Интернета и доступная только для абонентов с SIM-картами данного корпоративного пользователя. Она же соединяется с фиксированной IP-сетью пользователя (центральным офисом и т.п.) безопасным туннелем (L2TP, IPsec и т.п.), образуя единую IP-сеть между центральным офисом и удалёнными клиентами.

   Адрес удалённой стороны (сервера) также назначается оператором. Однако по существу он не требуется ни для каких практических целей и нужен только формально для соблюдения требований протокола. Иногда в современных сетях он даже не сообщается клиенту, это можно легко видеть из трассы PPP-соединения при включённом отладчике. В этом случае устройство NSG самостоятельно выбирает некоторый случайный фиктивный адрес, который будет считаться адресом удалённой стороны.

8. **Сжатие и шифрование** трафика в сотовых сетях обычно не используются.

9. **Маршрутизация и NAT.** Удалённый клиент, с точки зрения сотового оператора, всегда представляет собой ровно 1 устройство — для него нет разницы, будет ли это одиночный компьютер с модемом или маршрутизатор, за которым стоит целая локальная сеть. Соответственно, он всегда обеспечивает только один маршрут на единственный IP-адрес сотового клиента. Чтобы хосты в локальной сети, расположенной за устройством NSG, могли общаться с внешним миром, необходимо либо включить NAT на внешнем (сотовом) интерфейсе, либо установить какой-либо туннель к центральному офису и прописать маршруты в обе стороны через этот туннель. Возможно использование обоих способов одновременно: пакеты, адресованные в сеть центрального офиса, маршрутизируются в туннель, а все остальные — по умолчанию напрямую в PPP-соединение и при этом проходят через NAT.

   Настройка NAT производится в узле .ip.nat и включает в себя очень широкий набор возможностей. Для удобства пользователя, в узле ppp имеются команды add-nat/del-nat, которые автоматически выполняют минимальный набор настроек для простейшего варианта NAT — маскарадинга, т.е. подстановки IP-адресов источника в исходящих пакетах. Просмотреть эту настройку можно командой .ip.nat.show .

10. **Настройка компьютеров в локальной сети.** Как правило, устройство NSG используется в качестве маршрутизатора для выхода из локальной сети (даже если это вырожденная сеть из 1 банкомата или ПК) во внешний мир. Для этого на хостах локальной сети должны быть сделаны следующие настройки:
    - — IP-адрес и маска подсети — совместимые с настройками локального интерфейса Ethernet устройства NSG.
    - — Адрес шлюза по умолчанию — адрес локального интерфейса Ethernet устройства NSG.
    - — Адреса DNS — могут использоваться любые известные DNS, доступные для пользователей данного сотового оператора (некоторые операторы ограничивают услуги DNS для чужих пользователей или, наоборот, доступ своих клиентов к чужим DNS). Наиболее логично использовать DNS своего же оператора. Узнать их можно, например, из журнала PPP-соединения (по умолчанию они запрашиваются, accept-dns="true"). Если адреса DNS получены, они автоматически добавляются в начало списка известных серверов для работы как локального клиента DNS на устройстве NSG, так и DNS-прокси для обслуживания третьих хостов.

      Вместо сервера DNS рекомендуется использовать само устройство NSG в режиме DNS-прокси. Оно принимает запросы от локальных хостов и ретранслирует их на внешний сервер DNS. Удобство такого метода в том, что он не требует заранее знать адреса DNS оператора (которые, к тому же, могут изменяться по его усмотрению). Для локальных хостов указывается адрес устройства NSG, который находится в полной власти пользователя, а оно получает адреса DNS оператора каждый раз при установлении PPP-соединения.

    Автоматическая настройка локальных хостов может выполняться при помощи встроенного сервера DHCP на устройстве NSG. В настройках сервера DHCP указываются все вышеперечисленные параметры, передаваемые клиентам. Пример комплексной настройки PPP, DNS-прокси и сервера DHCP приведён в Приложении 2–A.

Особенности взаимодействия "система-модем-оператор". При отладке сотовых соединений, особенно при анализе трасс PPP в проблемных случаях, необходимо иметь в виду, что пакетное сотовое соединение, хотя и сделано внешне максимально похожим на традиционное соединение по коммутируемой линии, **принципиально** отличается от него по существу. Это достаточно сложная последовательность встроенных прокси-сервисов и инкапсуляций, обеспечиваемых сотовым модемом и сетью оператора и невидимых для PPP-демона на пользовательском устройстве.

В частности, дозвон, соединение с сетью, а в сетях GSM/UMTS также и аутентификация — это чисто формальные операции, которые выполняются между клиентом PPP и модемом и не требуют взаимодействия с сетью. Поэтому в трассе они могут завершаться успешно, а проблема начинается позже, на этапе IPCP — когда впервые требуется взаимодействие с сетью по существу, чтобы получить IP-адреса. Если на этом этапе наблюдается только регулярная отправка запросов ICMP без получения ответов на них, или циклический обмен пакетами IPCP с формальными адресами вида 10.11.12.13 и т.д. (в зависимости от типа сотового модема), это означает, что система работает только с модемом, а модем дальше с сетью — не работает. В этом случае следует проверить исправность антенны, уровень радиосигнала (AT+CSQ) и доступность услуги пакетной передачи данных (AT+CGREG?). В некоторых случаях целесообразно принудительно зафиксировать выбор услуги GSM либо UMTS.

§2.6.5. Работа с двумя сотовыми операторами

Устройства NSG поддерживают подключение через двух или даже нескольких сотовых операторов. Для этого имеются два принципиально различных решения.

Сотовые модули и встроенные интерфейсы для сетей GSM и UMTS имеют 2 гнезда для SIM-карт разных операторов. Однако физически они имеют только один приёмопередатчик и могут работать с двумя операторами только попеременно. Считается, без ограничения общности, что SIM-карта предпочтительного оператора вставлена всегда в верхнее гнездо, резервного оператора — в нижнее. Выбор оператора осуществляется программно (или может быть аппаратно зафиксирован на верхнюю SIM-карту.) Независимо от выбранного оператора, такой интерфейс всегда имеет одно и то же имя, и маршрут в вышестоящую сеть будет одним и тем же через этот интерфейс. С точки зрения вышестоящих протокольных уровней, это в любом случае один и тот же объект 2 уровня.

Настройки PPP-соединения для одного и для другого операторов производятся в узлах ppp.main и ppp.aux , соответственно. Выбор SIM-карты производится после разрыва предыдущего соединения в момент аппаратного рестарта модуля. Рестарт является в данном случае обязательным. При этом синхронно устанавливаются активная SIM-карта, скрипт дозвона (критически важный элемент, поскольку содержит имя APN), имя/пароль пользователя и набор параметров собственно PPP.

Выбор регулируется двумя параметрами ppp.main.attempts и ppp.aux.attempts . Эти параметры определяют число попыток соединения через того и другого оператора. Каждая попытка может засчитываться как удачная или неудачная, в зависимости от причины разъединения. Если попытка была удачной (например, завершена по инициативе устройства NSG), то следующая предпринимается через того же оператора. Если попытка была неудачной (например, не удалось получить CONNECT), то счётчик оставшихся попыток уменьшается на единицу и, если он доходит до нуля, то модуль переключается на другого оператора. Например, установка

```
ppp.main.attempts  = 5
ppp.aux.attempts   = 3
```

означает, что модуль будет предпринимать сначала 5 попыток соединения через основного оператора, затем 3 через резервного. Таким образом, это в некотором смысле "относительные веса" того и другого операторов. Если один из параметров равен нулю, то соединения через этого оператора производиться не будут. (Значение другого параметра в этом случае может быть любым, но для однозначности рекомендуется устанавливать в такие случаях 0 и 1. В частности, именно такие параметры устанавливает команда restart с явно указанным параметром main либо aux.)

ПРИМЕЧАНИЕ На некоторых типах устройств (NSG–1820MC) два сотовых интерфейса могут иметь одновременный доступ к пулу из двух SIM-карт. В этом случае распределение SIM-карт между ними производится также с помощью параметров main.attempts и aux.attempts . Для одного из интерфейсов должна быть запрещена работа с одной SIM-картой (attempts=0), для другого — с другой.

На практике по истечении некоторого времени работы соединение можно считать успешным в любом случае, независимо от причины завершения. Более того, этот критерий использовать необходимо, поскольку все сотовые операторы ограничивают максимальную продолжительность сеанса (обычно 24 или 8 часами); если он отсутствует, то, например, соединение, продержавшееся максимально разрешённое время и прерванное по инициативе оператора, будет считаться неудачным — вопреки здравому смыслу. Минимальное время, после которого попытка безусловно объявляется успешной, устанавливается параметром min-success-time (отдельно для каждого оператора).

Дополнительный параметр ppp.priority определяет, является ли оператор main абсолютно приоритетным. Если значение параметра равно true и модуль работает через резервного оператора, то после разрыва он безусловно возвращается на основного оператора и начинает цикл с начала. Такая установка рекомендуется, если основной оператор предпочтителен по существу, т.е. имеет значительно лучшее качество или меньшую стоимость услуг. Если параметр имеет значение false, то цикл продолжается и модуль пытается восстановить связь с резервным оператором, до тех пор, пока не будет достигнуто предельное число неудачных попыток ppp.aux.attempts .

В большинстве практических ситуаций оба доступных сотовых оператора работают приблизительно одинаково плохо и стоят примерно одинаково дорого, поэтому отдавать кому-либо из них особое предпочтение нет смысла и рекомендуется использовать установки:

```
ppp
: main
: : attempts        = 1
: aux
: : attempts        = 1
: prio              = false
```

Устройство будет поочерёдно обращаться к одному и к другому оператору.

При потере связи время восстановления будет складываться, в наихудшем случае (если разрыв не происходит явно) из времени срабатывания LCP Echo (30–45 сек), времени рестарта модуля (30–35 сек), нескольких секунд на отработку процедуры нового соединения и на промежуточные паузы — итого 60–75 сек. Это время необходимо учитывать при настройке прикладного программного обеспечения, например, *keepalive* в банкомате должен иметь порог срабатывания не меньше этого времени.

ПРИМЕЧАНИЕ Практическое правило "большого пальца" подсказывает, что при использовании процедур *keepalive* на нескольких последовательных уровнях (LCP Echo в PPP, LCP Echo во вложенном PPTP или DPD в IPsec, *ping*, *keepalive* прикладного ПО) время его срабатывания на каждом вышестоящем уровне следует выбирать, как минимум, в 3 раза больше нижележащего.

Принципиально другое решение — это установка двух или более сотовых модулей на одно шасси серий NSG–700, NSG–1800. Оно объективно дороже, поскольку означает наличие в устройстве 2 приёмопередатчиков, но зато обеспечивает более оперативное реагирование. Оба сотовых интерфейса подключены одновременно, каждый к своей сети, и при потере связи время переключения на другого оператора ограничено снизу только временем, необходимым для обнаружения этого факта — 30–45 сек. Кроме того, такое решение более гибкое: можно использовать интерфейсы разных стандартов (например, UMTS и CDMA) или комбинировать их с интерфейсами иных типов.

При таком подходе каждый из интерфейсных модулей работает независимо от другого и поддерживает связь, по возможности, постоянно. С точки зрения 3 уровня протокольного стека, в устройстве имеются 2 (или более) сетевых интерфейсов с разными именами, выбор между которыми производится средствами IP-маршрутизации: метриками маршрутов, динамической маршрутизацией и т.п. В простейшем случае, для резервного интерфейса следует принудительно назначить метрику больше 1; тогда при наличии основного соединения (метрика по умолчанию — 1) пакеты пойдут в него, и только при его отсутствии — в резервное. Подробно об IP-маршрутизации см. Часть 3.

Оба варианта резервирования могут использоваться и совместно, поскольку ни в коей степени не противоречат друг другу. Например, можно установить в одно шасси два 2-симчатых модуля и работать, в общем случае, через 4 операторов, причём постоянно поддерживать связь с двумя из них.

§2.6.6. Мониторинг и выбор сотовой услуги

Мониторинг работы сотового модема производится только с помощью AT-команд. Однако эти команды передаются, в общем случае, через тот же самый внутренний интерфейс между устройством NSG и модемом, через который идут данные. Таким образом, мониторинг принципиально возможен только в следующих случаях:

— Модем не используется для передачи данных (encapsulation = "none" или adm-state = "down"). В этом случае к нему можно подключится с помощью команды raw-access (см. §2.6.3) и вводить нужные AT-команды в ручном режиме.

— Модем поддерживает команды временного выхода в командный режим (+++) и возвращения в режим передачи данных (ATO). Чтобы выполнять такое переключение, необходимо задействовать обработчик SMS (см. §2.6.12, §2.6.17).

— USB-модем имеет независимый второй интерфейс для управления.

Некоторые типы модемов поддерживают второй способ, некоторые — третий, некоторые — не поддерживают ни одного. В частности, для отдельных типов сменных и встроенных сотовых интерфейсов:

Модули UIM–3G, UM–3G всех версий, UIM–EVDO *ver.3a*, UM–EVDO/A *ver.7*, опции opt18xx.3G, opt18xx.CDMA Устройства NSG–18*xx*H, NSG–6*xx*H, частично NSG–6*xx*G	Имеют дополнительный порт для управления
Модули UM–EVDO/A Устройства NSG–6*xx*D, NSG–18*xx*D, (чипсет CMOTech CNE–680)	Имеют дополнительный порт для управления, требуют отдельной настройки для автоматического мониторинга из *ui*TCP.
Модули UIM–EDGE *ver.3* (чипсет SimCom SIM700, без наклейки) Все унаследованные типы модулей с внутренним асинхронным интерфейсом: IM–GPRS, IM–EDGE, IM–CDMA (чипсеты Wavecom, PIML, FlyFot, AnyDATA.NET)	Имеют единственный порт и управляются только через обработчик SMS
в т.ч. модули IM–GPRS *ver.2* и *3* (чипсеты FlyFot и PIML)	Управление возможно, но не рекомендуется, поскольку команда +++ может приводить к зависанию модема (далее он штатно рестартует средствами PPP, но на это время связь теряется).
Модули UIM–CDMA *ver.2*, UIM–EVDO *ver.2* (чипсеты CMOTech CNE–550, CNE–510)	Мониторинг в режиме передачи данных не предусмотрен

Если используемый модем допускает мониторинг в рабочем режиме, то в меню порта доступна команда radio-info, разово запрашивающая уровень сигнала, регистрацию на услуги, имя оператора и некоторые другие параметры в зависимости от типа модуля. Уровень сигнала выводится 3 способами: в децибелах, в условных единицах (от 0 до максимального значения 31, 99 — сигнал отсутствует) и в "палках" (от 1 до 4). Имеется также устаревшая команда csq-check, запрашивающая только уровень сигнала в условных единицах.

Возможно также подключиться непосредственно к модему из командной оболочки Linux с помощью утилиты nsgcu (см. Часть 7), но для этого необходимо знать внутреннее имя сетевого устройства, которое зависит от типа шасси, номера разъёма расширения и типа модуля.

Выбор предоставляемой услуги производится модемом, как правило, автоматически. Встроенное программное обеспечение модема имеет собственный алгоритм выбора по совокупности многих критериев, который его разработчики сочли оптимальным для большинства случаев. Если полученный результат не соответствует желаемому, или приводит к неустойчивой работе модуля, то в некоторых случаях можно попытаться выбрать услугу принудительно (GPRS/EDGE либо 3G, CDMA 1x либо EV-DO) в узле ppp...chat.mode . Выбор между услугами GPRS и EDGE, а также между EV-DO rev.0 и rev.A, производится всегда автоматически и пользователю неподконтролен.

Следует, однако, иметь в виду, что принудительный выбор услуги имеет и свою обратную сторону. Как минимум, необходимо удостовериться, что выбранная услуга доступна на данной площадке. Жесткий выбор высокоскоростной услуги может приводить к более частым разрывам и переустановлениям соединения, или к более или менее продолжительным периодам отсутствия связи (хотя де-факто низкоскоростная услуга в это время доступна). Его можно рекомендовать для приложений, которые в любом случае не могут работать по низкоскоростным соединениям — например, для передачи видео.

Наоборот, выбор низкоскоростной услуги иногда делает связь более устойчивой. Его можно рекомендовать, в некоторых случаях, для подключения банкоматов, технологических датчиков и другого оборудования, не создающего большого трафика. Следует, однако, иметь в виду, что разные услуги отличаются, помимо скорости, ещё рядом качественных показателей — временем обращения пакетов (*ping*), гарантиями минимальной скорости и др. Особенно велики в этом смысле различия между услугами GPRS/EDGE и WCDMA/HSDPA: в сетях 2G при перегрузке пакетные данные сбрасываются полностью и фактическая скорость соединения падает строго до нуля, в сетях 3G управление трафиком более гибкое. Поэтому жёсткий выбор низкоскоростного режима в них не всегда бывает оправданным.

В сетях CDMA, наоборот, обе услуги 1x и EV-DO относятся к 3G, поэтому также обеспечивают эффективное управление трафиком в условиях перегрузок. В этих сетях низкоскоростной режим 1x качественно уступает высокоскоростному только по времени *ping*; если оно не является критическим параметром, то выбор 1x ради большей устойчивости связи будет вполне оправданным.

Косвенно судить о выбранной услуге, не прерывая передачу данных, можно по времени прохождения *ping*, поскольку оно сильно различается для разных услуг. Для чистоты эксперимента лучше посылать *ping* на какой-либо недалёкий хост, например, на DNS сервер данного оператора. Характерные времена *ping* (короткими пакетами) для разных сотовых технологий:

Услуги GSM/UMTS	*ping*, мс	Услуги CDMA	*ping*, мс
HSDPA	80–120	EV-DO rev.A	80–120
WCDMA	180–250	EV-DO rev.0	~250
EDGE	~350	1X	~450
GPRS	~550 и более (в некоторых старых сетях до 2000)		

ПРИМЕЧАНИЕ В общем случае, предпочтительно пользоваться современными высокоскоростными услугами даже для задач, не требующих больших объёмов данных. Дело, помимо скорости, именно в других показателях качества. Короткое время *ping* делает работу пользователей (например, в Telnet) более комфортной, а работу приложений — более устойчивой, поскольку позволяет чётко различить ситуации с задержкой пакетов (в среднем, она пропорциональна времени *ping*) и их безвозвратной потерей. Например, если прикладное ПО банкомата имеет короткий таймаут (5–10 сек) для подтверждения транзакции, то в старых сетях GPRS оно может работать крайне неустойчиво из-за того, что к чистому времени ответа сервера добавляется ещё 30–50% на передачу пакетов по сети.
Другой критически важный критерий выбора услуги — это бесперебойная доставка данных, хотя бы на минимальной скорости. Преимущества современных сетей 3G (UMTS и CDMA) и 4G перед традиционными сетями GSM в этом смысле вполне очевидны.

Автоматизация мониторинга радиоинтерфейса. Для автоматического анализа уровня сигнала и других параметров сотовый интерфейс может рассматриваться как датчик с аналоговым выходом, работающий в рамках общего обработчика событий (см. Часть 4). В порту предусмотрен узел event-generator, в котором можно определить интересующие состояния уровня сигнала (например, нормальный, неустойчивый и недопустимо низкий). Переходы из одного состояния в другое считаются событиями и вызывают ответное

действие, указанное в обработчике. В частности, это может быть переход на другой канал связи, отправка уведомлений по SMS и электронной почте, включение индикации, отправка TCP-уведомлений на сервер мониторинга NSG, и т.п. В частности, TCP-уведомления могут, помимо сервера, учитываться системой *ui*TCP и выводиться в окне мониторинга клиента.

Пример. Устройство NSG–1800. Светодиодный индикатор будет включаться следующим образом в зависимости от уровня сигнала на интерфейсе `s1` :

16…31	Зелёный
8…15	Жёлтый
4…7	Красный
0…3	Погашен
99 (сеть не найдена)	Погашен

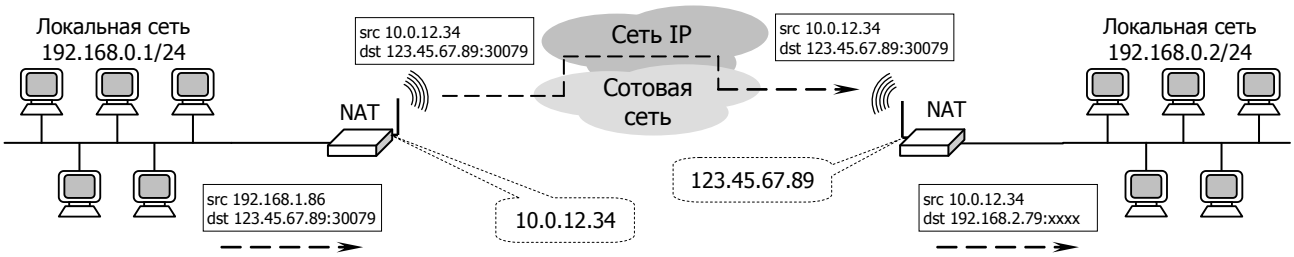
```
port
: s1
: type                  = "3g"
: enable                = true
: : CSQ
: : : 1
: : : : from            = 16
: : : : to              = 31
: : : : event-name      = "HIGH"
: : : 2
: : : : from            = 8
: : : : to              = 15
: : : : event-name      = "MEDIUM"
: : : 3
: : : : from            = 4
: : : : to              = 7
: : : : event-name      = "LOW"
: : : 4
: : : : to              = 3
: : : : event-name      = "ZERO"
: : : 5
: : : : from            = 99
: : : : event-name      = "NONE"
services
: event-handler
: : 1
: : : virt-sensor       = "s1.CSQ"
: : : prev-state        = "other"
: : : state             = "HIGH"
: : : action            = ".tools.led(red=off;green=on)"
: : 2
: : : virt-sensor       = "s1.CSQ"
: : : prev-state        = "other"
: : : state             = "MEDIUM"
: : : action            = ".tools.led(red=on;green=on)"
: : 3
: : : virt-sensor       = "s1.CSQ"
: : : prev-state        = "other"
: : : state             = "LOW"
: : : action            = ".tools.led(red=on;green=off)"
: : 4
: : : virt-sensor       = "s1.CSQ"
: : : prev-state        = "other"
: : : state             = "ZERO"
: : : action            = ".tools.led(red=off;green=off)"
: : 5
: : : virt-sensor       = "s1.CSQ"
: : : prev-state        = "other"
: : : state             = "NONE"
: : : action            = ".tools.led(red=off;green=off)"
```

§2.6.7. Соединения "точка-точка" в режиме пакетной передачи данных

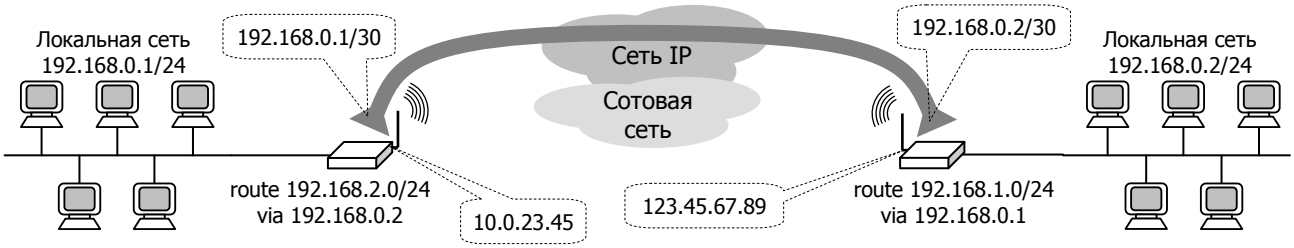
Технологии пакетной передачи данных в сотовых сетях принципиально ориентирована на соединение пользователя с сетью, как с поставщиком доступа в Интернет (или в корпоративную сеть) и не предусматривает, в отличие от канального режима GSM, непосредственного соединения между двумя абонентами на физическом уровне. Если требуется соединить два офиса через сотовую сеть, то эту задачу следует решать как передачу данных между ними через абстрактную промежуточную сеть IP. Фактически это общая задача построения корпоративной интрасети поверх сети общего пользования, а вся специфика сотовой сети состоит только в подключении того и другого офиса к оператору.

Для решения задачи необходимо, чтобы хотя бы один из двух офисов имел статический IP-адрес. (Как правило, это головной офис компании, в этом случае он может быть один, а филиалов с динамическими адресами — несколько.) Если всё происходит внутри сети одного оператора, то этот статический адрес может быть из приватного диапазона (10.x.x.x, 192.168.x.x и др.), если нет — то обязательно глобальным. Далее возможны 2 варианта:

Соединение через NAT. На обоих устройствах доступа, в филиале и в центральном офисе, настраивается NAT, причём по-разному. В филиале для исходящих пакетов выполняется *masquerading*, т.е. подмена внутреннего IP-адреса источника на адрес, назначенный оператором. В головном офисе настраивается *Destination NAT*, т.е. во входящем пакете, адресованном на каждый конкретный TCP или UDP порт, подменяются адрес (на адрес из внутренней сети) и порт назначения. С такими настройками клиенты из сети филиала могут инициировать соединения с серверами, находящимися в головном офисе. Если филиал также имеет статический адрес, то аналогичным образом можно настроить доступ в обратном направлении — из головного офиса в филиал.



Туннелирование — более современный подход. Туннель, строящийся в данном случае поверх IP, играет роль виртуального канала WAN "точка-точка", а совокупность этих туннелей и составляет сущность понятия "виртуальная частная сеть". Туннель может быть незащищённым (GRE, PPTP без MPPE) или защищённым (PPTP+MPPE, IPsec, STunnel, OpenVPN, NSG ***ui*TCP** и др.). Технология GRE требует статических адресов для обеих сторон, остальные — только для сервера (головного офиса). В любом случае, пакеты из одной внутренней сети в другую маршрутизируются в этот туннель, как когда-то — в физический канал "точка-точка". Поскольку пользовательские пакеты упаковываются внутрь туннельных пакетов целиком и заголовки тех и других пакетов нигде не пересекаются, то адресное пространство виртуальной сети полностью изолировано от адресного пространства оператора и находится в полном распоряжении пользователя.



Помимо туннелирования пакетов IP через сеть оператора, возможен и другой вариант — объединение сетей на втором уровне. При этом в туннель GRE (или GRE поверх какого-либо из безопасных туннелей) упаковываются пакеты Ethernet целиком, вместе с заголовками второго уровня. В сотовых сетях такой подход, как правило, нецелесообразен, поскольку в туннель попадает весь обильный широковещательный трафик обеих сетей: запросы и оповещения клиентов локальной сети, пакеты ARP и др. Он легко может загрузить относительно узкий сотовый канал на все 100%, и обойдётся при этом в немалую сумму. Однако в отдельных случаях (подключение банкомата, видеокамеры, технологического датчика со строго определённой функциональностью) такое решение бывает вполне оправданно.

Подробно о различных видах туннелирования и VPN см. Часть 5.

§2.6.8. Особенности использования интерфейсов EV-DO rev.A *ver.5*

Сотовые интерфейсы NSG, построенные на основе чипсета CMOTech CNE–680 (модуль UM–EVDO/A *ver.5* и устройства NSG–600D, NSG–605D, NSG–1820D, NSG–1820HD), имеют следующую особенность. По умолчанию, данный чипсет работает в режиме acm-modem для совместимости с имеющимися инсталляциями на базе NSG Linux 1.0. Однако режим usb-serial имеет два важных преимущества:

— Возможен мониторинг работы модема (контроль уровня сигнала и т.п.) во время передачи данных.
— Отсутствует конфликт с внешними USB-накопителями (Flash, HDD).

Смена режима выполняется один раз командой switch-to-usb-serial-mode . Команда доступна, как и raw-access, при установке adm-state = "down" или encapsulation = "none" . Подробнее см. §2.10.3. Если данная команда недоступна, значит, модем уже находится в режиме usb-serial .

Применительно к NSG Linux 2.0 и современным модификациям устройств, данная операция не имеет каких-либо негативных последствий и рекомендуется к выполнению при первоначальной настройке устройства, чтобы не заниматься этим впоследствии.

ПРИМЕЧАНИЕ Для работы под управлением NSG Linux 1.0, а также при установке в разъём s2 устройств NSG–700 *h/w ver.5* и ранее, необходимо всегда использовать модуль в режиме acm-modem.

§2.6.9. Особенности использования интерфейсов и опций EV-DO rev.A *ver.7*

Сотовые интерфейсы на основе чипсета ATEL EP45 (модуль UM–EVDO/A *ver.*7 и опция opt18xx.CDMA.7 для устройств NSG–1800, NSG–1820) могут использоваться с одной или двумя антеннами. Если антенна единственная, то её необходимо подключать к разъёму main. Для улучшения работы интерфейса, особенно на площадках со слабым или неустойчивым сигналом, рекомендуется использовать две антенны.

Данные модули и опции реализованы на унифицированной подложке, используемой для модулей и опций как CDMA, так и LTE/UMTS/GSM. По этой причине они имеют 2 гнезда для карт SIM/R–UIM. Для модулей CDMA используется только главная (main, в большинстве устройств — верхняя) карта и, соответственно, настраивается только узел ppp.main . В случае необходимости возможно использование и двух карт R–UIM, используемых попеременно (например, для оптимизации расходов на трафик, в зависимости от особенностей тарифной политики оператора).

§2.6.10. Использование устаревших типов сотовых модулей NSG

Помимо ныне выпускаемых сотовых модулей, NSG Linux 2.0 поддерживает работу со следующими типами сотовых модулей 2003–2009 годов выпуска:

IM–EDGE *h/w ver.2*	Чипсет SimCom SIM600, 2 SIM-карты
IM–EDGE *h/w ver.1*	Чипсет SimCom SIM600, 1 SIM-карта
IM–GPRS *h/w ver.3*	Чипсет FLYFOT M260 или PIML 900/1800 Plus, 2 SIM-карты
IM–GPRS *h/w ver.2*	Чипсет FLYFOT M260 или PIML 900/1800 Plus, 1 SIM-карта
IM–GPRS *h/w ver.1*	Чипсет Wavecom 2406B или Q24Plus, 1 SIM-карта
IM–CDMA *h/w ver.3*	Чипсет AnyDATA.NET DTU–450X
IM–CDMA *h/w ver.1*	Чипсет AnyDATA.NET DTG–450

Все перечисленные модули взаимодействуют с устройством только через внутренний асинхронный интерфейс и настраиваются вручную как type = "gsm-2sim" . Соответственно, настройки порта для них содержат параметры асинхронного интерфейса:

```
port s1
: baudrate          = 115200
: data-bits         = 8
: flowcontrol       = "hardware"    (если настраивается для данного порта)
: parity            = "none"
: stop-bits         = 1
```

Наиболее существенным из них является скорость, поскольку она должна быть согласована в порту шасси и во внутреннем порту модема. Из всех перечисленных модулей, только модем Wavecom 2406B поддерживает автоматическое определение скорости, и для него скорость в порту шасси может быть любой. Для остальных модулей она должна быть установлена вручную одинаковой с обеих сторон.

Чтобы настроить скорость во внутреннем порту модема, нужно соединиться с ним (команда raw-access) на той скорости, которая установлена в данный момент. По умолчанию, модули поставлялись настроенными на скорость 115200 бит/с. Изменять её особого смысла нет, поскольку она не влияет, в отличие от канального режима CSD и от проводных *dial-up* модемов, ни на скорость установления соединения, ни на его устойчивость. Только иногда, если сеть реально обеспечивает скорость на радиоинтерфейсе выше 115200 бит/с, целесообразно увеличить скорость в порту до 230400 бит/с. Это бывает в сетях CDMA и крайне редко в сетях EDGE.

Если на скорости 115200 бит/с соединиться с модулем не удаётся, то, вероятно, она была изменена в процессе эксплуатации; наиболее вероятные значения — 230400 и 9600. Если они также не подходят, то следует перепробовать все остальные. Если соединиться с модулем не удаётся ни на какой скорости, то данный экземпляр неисправен и, за давностью лет, не подлежит ремонту.

Устанавливать скорость в порту модема и сохранять её в энергонезависимой памяти модема необходимо одной командой, поскольку иначе ввести команду сохранения будет невозможно. Синтаксис команды:

для модулей IM–EDGE обеих модификаций: AT+IPR=115200&W
для модулей IM–GPRS и IM–CDMA всех модификаций: AT+IPR=115200;&W

После этого необходимо отключиться от модуля, изменить скорость в порту шасси, и соединиться с модулем заново.

ВНИМАНИЕ Модули IM–*xxx* не могут использоваться в разъёме расширения s2 шасси NSG–700/4AU *h/w ver.5* и более ранних.

Аппаратный рестарт модема производится с помощью перемычки J1 так же, как и для USB-модулей (см. §2.6.2). Модули с 1 и с 2 SIM-картами программно не различаются; для модулей с одной SIM-картой следует использовать узел ppp.main и игнорировать узел aux .

Скрипты для устаревших сотовых модулей не могут быть сгенерированы автоматически, поскольку точный тип модуля (GSM, CDMA) неизвестен. Их необходимо ввести вручную по образцу, приведённому в §2.6.4.

Другие особенности настройки отдельных типов модулей:

— В модулях IM–EDGE обеих модификаций при сбросе настроек командой AT&F устанавливается скорость 230400 бит/с. Для остальных — 115200 бит/с.

— Для модулей IM–GPRS *h/w ver.2,3* во всех режимах, а также для модулей IM–EDGE обеих модификаций при работе в режиме CSD в качестве отвечающего, необходимо установить дополнительную опцию

```
ppp.{main|aux}.options = "local"
```

Данная опция отключает контроль за состоянием сигнала DCD модема, поэтому, как следствие, для контроля за состоянием соединения абсолютно необходимо использовать LCP echo или *netping*.

— Для модулей IM–GPRS *h/w ver.1* можно уменьшить начальный таймаут до 10–15 сек.

— Модули IM–GPRS *h/w ver.1* для работы в пакетном режиме требуют явной установки AT+CGCLASS="CG". Для работы в канальном режиме — класс "B" (установлен по умолчанию) или "CC". Данная установка выполняется один раз при настройке модуля и запоминается автоматически.

— Для модулей IM–GPRS *h/w ver.2, 3* не рекомендуется использовать SMS-управление. Если попытка переключения в командный режим попадает в момент обмена данными, то эти модули "зависают". (Далее они штатно рестартуются средствами PPP-интерфейса, но это в любом случае приводит к временному отсутствию связи.)

— Модули IM–GPRS, за исключением крайне редких *h/w ver.1* на чипсете Wavecom Q24Plus, при снятой перемычке J1 не разрывают физическое соединение при падении DTR. В пакетном режиме GPRS это ещё одно обстоятельство, в силу которого следует всегда устанавливать эту перемычку. В канальном режиме CSD удалённая сторона должна корректно разрывать физическое соединение после завершения сеанса.

§2.6.11. Услуга канальной передачи данных

Классическая услуга CSD (Channel Separated Data, передача данных в канальном режиме) на скоростях 2400–9600 бит/с является "родной" услугой сетей GSM поколения 2G. Преимущество данной услуги в том, что она имеет равный приоритет с передачей голоса, и в случае перегрузки сети связь не теряется — в отличие от GPRS/EDGE. Кроме того, она обеспечивает относительно небольшое время *ping*. Недостатки — низкая скорость и высокая стоимость, поскольку услуга оплачивается по времени соединения. Как следствие, соединения устанавливаются обычно только при наличии данных на передачу (connection = "on-demand") и принудительно разрываются через небольшое время (параметры idle-time, session-time). Это, в свою очередь, приводит к достаточно длинной (20–40 сек.) процедуре установления связи на физическом уровне всякий раз, когда клиенту необходимо что-то передать в сеть.

В части физического соединения, настройка заключается в написании модемного скрипта. Скрипт во всех случаях аналогичен таковому для *dial-up* модема и асинхронного порта с внешним модемом (см. §2.4.5, §2.4.6). Особенность скрипта для CSD состоит в том, что желательно, по возможности, использовать протокол V.110 — если он поддерживается обеими сторонами. Он обеспечивает ускоренную процедуру соединения: при удачном выборе других параметров, в пределах 6–8 сек. Такое время важно, поскольку позволяет уложиться в рамки психологического порога, например, при снятии денег в банкомате или при обслуживании покупателя в магазине, когда за ним стоит длинная очередь. Выбор модемного протокола производится хорошо стандартизованной командой AT+CBST .

Примеры скриптов для настройки вызывающего и отвечающего модемов в режиме V.110:

```
chat.script = "'' AT OK ATZ OK AT+CBST=71,0,1 OK ATDномер CONNECT ''"
chat.script = "'' ATZ OK AT+CBST=71,0,1 OK ATS0=1 OK ''"
```

Аппаратный рестарт модема при работе в режиме CSD, как правило, не требуется, поскольку модем и сеть отрабатывают разрыв связи надёжно и корректно. Более того, он нежелателен, поскольку значительно увеличивает время соединения. Поэтому целесообразно снять перемычку J1 и исключить начальный таймаут.

В отличие от пакетных услуг, де-факто жёстко привязанных к услуге доступа в сеть IP сотового оператора, услуга CSD есть только передача данных на физическом уровне в режиме "точка-точка" между двумя модемами. На вышестоящих уровнях протокольного стека она может быть использована по-разному:

1. **Подключение к поставщику услуг Интернет общего пользования** (самому сотовому оператору, обычно по "короткому" номеру, или к наземному оператору *dial-up* доступа). В этом случае имеем ту же ситуацию, что и при использовании пакетных услуг (см. предыдущие параграфы).
2. **Подключение к собственному GSM или проводному модему на другой площадке.** В этом случае оператор обеспечивает только физический уровень. Вышестоящие протокольные уровни теоретически могут быть произвольными: это не только PPP, но и SLIP, X.28, или неструктурированные асинхронные данные. Однако, в связи с низкой востребованностью ныне и в перспективе, иные протоколы реализованы в NSG Linux 2.0 лишь частично.

Наиболее предпочтительным можно считать вариант, когда CSD-клиент подключается к собственному пулу сотовых модемов, работающих в сети того же оператора, по следующим причинам:

— При соединениях "точка-точка" внутри сотовой сети возможно использовать протокол V.110.

— Стоимость вызовов внутри сети оператора ниже, чем вызовов на городскую телефонную сеть.

— В соединении могут быть использованы иные протоколы, помимо PPP. Например, сотовый модем может быть настроен в качестве отвечающего и передавать асинхронный поток от удалённого POS-терминала, не имеющего встроенного сетевого протокола, в сеть TCP/IP (encapsulation = "raw-tcp") аналогично §2.5.5.

— Пользовательский трафик изолирован от Интернет, защищён встроенными средствами сети GSM и может быть дополнительно защищён с помощью MPPE. Хотя оба эти способа на сегодняшний день не считаются абсолютно надёжными, в совокупности это можно считать приемлемой степенью защиты для многих некритических применений.

§2.6.12. Инкапсуляция sms-handler — общие сведения

Услуга SMS-управления устройством NSG и подключённым к нему оборудованием — фирменная разработка компании NSG. Для управления используется исключительно услуга SMS сетей GSM и UMTS, без использования сетевых протоколов передачи данных. Управление производится на основе меню, которое хранится на устройстве NSG. Выбор пунктов меню приводит к исполнению заданных сценариев (скриптов) для управления как самим устройством NSG, так и подключённым к нему оборудованием.

SMS-управление может осуществляться через сотовый модем как в монопольном режиме, так и совместно с передачей данных по протоколу PPP.

ПРИМЕЧАНИЕ Технология SMS в сетях CDMA отличается от таковой в GSM/UMTS, причём ряд её ключевых компонент являются закрытыми. По этой причине SMS-управление в сетях CDMA не поддерживается.

После обработки команды устройство NSG отправляет пользователю SMS с результатом её выполнения. Если команда выводит большое количество текста (например, состояние и статистику интерфейса), то ответ разбивается на несколько SMS. Максимальное число SMS, которое может быть послано в ответ на одну команду, ограничивается в настройках порта.

Статус и результаты выполнения команд сохраняются в журнале приложения на мобильном телефоне.

ПРИМЕЧАНИЕ Отдельные модели телефонов могут иметь свои собственные особенности работы с SMS, например, запрос дополнительного подтверждения перед отправкой сообщения, безусловное сохранение всех принятых SMS на SIM-карте (что приводит к её переполнению), и т.п. Как правило, такие особенности носят системный характер и не могут быть изменены средствами прикладных программ.

В состав NSG Linux 2.0 входят две реализации SMS-управления: на основе Java Mobile Edition (старая, разработка 2008 г.) и на основе простых текстовых сообщений (новая). Для обоих реализаций предлагаются фирменные приложения NSG для сотовых телефонов с поддержкой Java и для платформы Android, соответственно. Они предоставляют удобное меню для выбора команд, ввода или выбора параметров, отправки и приёма SMS, просмотра журнала команд и т.п. Основные различия между этими реализациями приведены ниже.

ПРИМЕЧАНИЕ Рекомендуется использовать управление на основе простых текстовых SMS. Реализация на основе Java является устаревшей и не поддерживается сотовыми модулями и опциями 3G *ver.6* и выше. В связи с выходом из употребления телефонов на основе платформы Symbian, дальнейшая поддержка и развитие данной реализации не поддерживается, и она может быть окончательно удалена в одной из ближайших версий NSG Linux.

	Java ME	**текст**
Формат SMS	Фирменный бинарный	Простой текстовый
Режим использования сети	Специфические нетривиальные номера SMS-портов источника и назначения. При обмене SMS между сетями различных операторов номера портов могут не передаваться, поэтому *a priori* работоспособность системы гарантируется только в пределах одной сети.	Только тривиальный SMS-порт 0 (*plain text*). Передаётся прозрачно между всеми операторами GSM/UMTS.
Приложение NSG для сотового телефона	MoNsTer (Mobile NSG Terminal)	NSG SMS Shell
Платформа приложения	Java Mobile	Android
Платформы сотовых телефонов	Symbian S40, S60, ^3/Anna/Belle Windows (не проверено)	Android 2.1 и выше SDK ver.7 и выше
Средства конфигурации	отдельный файл (создаётся вручную)	настройка средствами nsgsh/Web
Возможность построения иерархического меню	Да	Нет
Возможность работы без использования приложения на сотовом телефоне	Нет	Да
Число записей в журнале	До 16 последних команд	Программно не ограничено, старые записи удаляются вручную

Безопасность управления обеспечивается самой его организацией, а также рядом дополнительных механизмов. Администратор составляет меню SMS-управления по своему усмотрению и включает в него те и только те команды, которые он считает целесообразным сделать доступными для удалённого управления, исходя из баланса между соображениями производственной необходимости и безопасности. Таким образом, меню представляет собой "песочницу" (*sandbox*): SMS обрабатываются в изолированной командной среде внутри основной операционной среды устройства, и никакие другие команды для них недоступны в принципе.

В Java-реализации присутствует дополнительная степень защиты: SMS передаются в фирменном двоичном формате, непригодном для прочтения человеком. Формат сообщений является закрытой разработкой NSG. Кроме того, концепция SMS-портов и работа с ними мало известны даже специалистам самих сотовых сетей.

Следующий уровень защиты от несанкционированного доступа обеспечивается "белым списком" телефонных номеров. Служба SMS-управления обрабатывает те и только те SMS-команды, которые поступают с заранее заданных номеров. Всю другие сообщения (как с иными телефонными номерами, так и с не определившимися) игнорируются.

В текстовой/Android реализации предусмотрено управление правами пользователей (доступным набором команд) на уровне индивидуальных пользователей и групп.

В последующих версиях NSG Linux дополнительно могут быть реализованы, по мере потребности, следующие механизмы защиты:

— "белый список" на основе кодов IMEI (уникальных заводских номеров сотовых приёмопередатчиков) или заводских кодов устройства Android.
— парольная защита для критически важных команд (например, для получения меню, без которого невозможна дальнейшая работа, или для перезагрузки устройства).

ПРИМЕЧАНИЕ В текстовой/Android реализации команды и ответы на них передаются в SMS открытым текстом. Если считается, что для данной системы это не безопасно и перехват SMS может привести к утечке чувствительной конфиденциальной информации, то следует принять меры к её сокрытию. Например, безобидный запрос состояния порта `ifconfig eth0` показывает, в частности, его IP-адрес и, таким образом, гипотетически может помочь злоумышленнику раскрыть структуру сети; конструкция `ifconfg eth0 | grep -v inet` удалит из вывода строку с IP-адресом, который администратору, надо полагать, и так известен.

§2.6.13. Инкапсуляция sms-handler — общая настройка порта

Если для порта установлена инкапсуляция sms-handler, то порт используется для SMS-управления в монопольном режиме и не может быть использован для передачи данных. При выборе инкапсуляции SMS-handler в меню порта имеется узел sms-handler, содержащий настройки обработчика SMS. Одновременная работа SMS и PPP на одном порту возможна, но для этого порт должен иметь инкапсуляцию PPP, а SMS-управление будет в этом случае вспомогательной функцией (см. §2.6.17).

С помощью SMS удалённый пользователь может выполнять различные операции, определенные в файле конфигурации nsgsms.conf либо в узле macros, в зависимости от выбранной реализации. Общими для обеих реализаций SMS-управления являются следующие параметры:

mode — Режим работы SMS-управления:
- MoNsTer — Реализация на базе Java Mobile (старая)
- text — Реализация на базе текстовых сообщений (новая)

Это ключевой параметр, определяющий выбор одного из двух режимов.

sim — SIM-карта, используемая для отправки в 2-симчатых модулях и интерфейсах: main или aux. Параметр действует только при отправке SMS в монопольном режиме; при работе службы SMS совместно с PPP он игнорируется, выбор SIM-карты определяется PPP-демоном.

number-of-sms — Максимальное количество SMS, которое может быть послано в ответ на одну команду. Если команда приводит к выводу большого объёма данных (например, команда show), то устройство посылает их в нескольких последовательных SMS (1 SMS = 160 знаков). Если длина ответа на конкретный запрос будет больше, то ответ будет обрезан до текста, помещающегося в заданное число SMS-сообщений.

control-tcp-port
inquiry-time

Параметры, специфичные для работы нескольких механизмов (передача данных, SMS-управление, исполнение AT-команд) через один и тот же порт. Подробнее о данных параметрах см. §2.6.17).

§2.6.14. Инкапсуляция sms-handler — настройка порта для MoNsTer

Параметры порта. Для Java-реализации в меню порта предусмотрены, наряду с описанными выше параметрами, также следующие:

debug-level — Уровень детализации отладочных сообщений:
- 0 Нет вывода.
- 1 Выводятся только важные сообщения (в основном, системные ошибки).
- 2 Дополнительно к 1, выводятся сообщения о пришедших SMS и результаты их обработки.
- 3 Дополнительно к 2, выводятся принятые и отправленные сообщения в том виде, как они появляются на линии (т.е. AT команды модема и ответы на них).
- 4 Дополнительно к 3, выводится дамп всего трафика на линии.

По умолчанию установлено значение 0. Для целей отслеживания активности пользователей рекомендуется установить 2. Сообщения выводятся в файл /var/log/sms.log, который можно просмотреть средствами командной оболочки Linux (см. Часть 7).

user-phones — "Белый список" телефонных номеров, с которых разрешён приём управляющих SMS. Все SMS, приходящие с любых других номеров, игнорируются. Для управления может быть задано до 32 номеров (см. также описание файла конфигурации /etc/nsgsms.conf).
Номер может содержать до 31 знака. Рекомендуется вводить номер полностью в том виде, в каком он определяется сетью, например, 79876543210.

ВНИМАНИЕ Если введена только часть номера (например, 9 цифр при 10-значном номерном плане), то система будет принимать SMS-сообщения от любых отправителей, у которых конец номера совпадает с введённой строкой. Пользоваться этой возможностью следует с крайней осторожностью, в основном, в демонстрационных инсталляциях.

Аналогичные параметры имеются также в текстовой/Android реализации, но там они имеют несколько иной смысл формат ввода. По этой причине они описаны отдельно в следующем параграфе.

Приложение MoNsTer может исполняться на сотовых телефонах и смартфонах с поддержкой Java Mobile Edition. Системные требования для работы приложения:

— MIDP 2.0 (JSR 118)
— CLDC 1.0/1.1 (JSR 30/139)
— Wireless Messaging API (JSR 120/205)
— поддержка многозадачного исполнения мидлетов (рекомендуется)

Приложение может быть установлено на мобильный телефон одним из следующих способов:

— Штатным Web-броузером мобильного телефона загрузить с сайта NSG описательный файл monster.jad, затем следовать штатной автоматизированной процедуре установки Java-приложений из Интернет. При заходе на корень сайта http://www.nsg.ru большинство мобильных телефонов корректно определяются Web-сервером, и для них автоматически генерируется упрощённая заглавная страница со ссылками на загружаемые файлы. Объём основного файла приложения monster.jar — около 30 Кбайт.

— Загрузить файл monster.jar на мобильный телефон с Web-сайта NSG или с прилагаемого CD-ROM любыми доступными средствами (через USB, Bluetooth, Wi-Fi, ИК-порт, флэш-карту и т.п.) и установить его с помощью штатного менеджера приложений.

В процессе установки будет выведено предупреждение об установке программного обеспечения без цифровой подписи. Следует подтвердить установку.

Для первоначальной настройки программы необходимо выбрать пункт Конфигурация и ввести телефонный номер SIM-карты, установленной в устройство NSG. Затем выбрать пункт Выполнить — Get Menu для загрузки меню команд с устройства NSG. После обмена SMS внутри пункта Выполнить появится пункт Menu, в котором содержатся все команды, определённые администратором устройства NSG.

Для выполнения команды следует выбрать её в меню и нажать кнопку OK (на большинстве моделей расположена в центре джойстика). Если команда требует параметры, то будет предложено соответствующее меню или текстовое поле ввода. Выбор пунктов меню осуществляется клавишей OK, ввод текста и чисел (например, IP-адресов) — обычным образом с помощью алфавитно-цифровых клавиш, перемещение по окну — как правило, с помощью джойстика. После ввода параметров следует нажать программируемую клавишу Выполнить и подтвердить отправку SMS.

Меню SMS-управления. Собственно список команд, доступных через SMS, оформляется в виде меню, которое хранится на устройстве в виде текстового файла /etc/nsgsms.conf или /etc/private/nsgsms.conf. Файл создаётся, редактируется или загружается готовый с другой машины средствами ОС Linux (см. Часть 7).

Файл содержит меню операций (по смыслу задачи, оно должно содержать хотя бы одну команду), а также может содержать описания пользователей.

Описание пользователя начинается со слова USER, за которым следует номер телефона (в том формате, в котором он определяется сотовой сетью). Затем опционально имя пользователя, и если оно есть, то за ним опционально имя группы (в данной версии NSG Linux не используются).

```
USER <phone> [<user_name> [<group_name>]];
```

Если значение опции короче, чем строка, выводимая AOH, то SMS-управление доступно для любых клиентов, у которых конечная часть номера совпадает с заданным значением.

Меню операций начинается со слова MENU, за которым в фигурных скобках следует описание меню. Синтаксис меню описан ниже; фигурные и круглые скобки — это не метасимволы, а обычные символы.

```
MENU {<menu_description>}
```

Описание меню состоит из последовательности субменю и команд

```
<menu_description> := <submenu>|<command> ...
```

Субменю начинается с имени, за которым в фигурных скобках следует описание субменю

```
<submenu> := <submenu_name> {<submenu_description>};
```

В свою очередь, <submenu_description> также может содержать субменю и /или команды.

Описание команды имеет следующий синтаксис

<command> := <command_name> (<parameter>, ...) <script>;

<parameter> := <name>[:<modificator>[:<modificator>]...]

Все <submenu_name> и <command_name> одного уровня будут появляться в виде списка на экране мобильного телефона. При выборе <submenu_name> будет произведён переход к следующему списку, а при выборе <command_name> на экране телефона появится форма с параметрами для ввода.

Круглые скобки после имени команды обязательны, даже если команда не имеет параметров. Имя параметра может содержать модификаторы, которые определяют тип значения параметра. Модификаторы указываются после имени параметра, через двоеточие. Первый модификатор может быть одним из следующих:

string	Текстовая строка
number	Целое число
decimal	Десятичное число
phone	Телефонный номер
password	Пароль (при вводе заменяется звёздочками)
choice	Выбор одного и только одного значения из нескольких (*radio button*)
set	Выбор нескольких из возможных значений (*checkboxes*)

Если модификатор не указан, то по умолчанию параметр имеет тип string.

За модификаторами string, number, decimal, phone, password может следовать (через двоеточие) целое число, которое определяет максимальное число символов в параметре (по умолчанию 16).

За модификаторами choice и set должны следовать (через двоеточие) имена, которые будут появляться на экране телефона в соответствующих списках выбора. По умолчанию, в случае choice выбрано первое из предлагаемых имён; в случае set не выбрано ни одно из полей.

Последнее поле команды <script> определяет операцию, которая должна быть выполнена при получении SMS с соответствующей командой. <script> — это произвольная строка, которая передается на выполнение в командную оболочку Linux. Строка может содержать следующие подстановочные символы:

$0	Заменяется на <command_name>
$1, $2, $3, ...	Заменяются на значения переданных параметров в порядке их следования в описании команды
$U, $G	Заменяются на имя пользователя и имя группы, соответственно, для определившегося телефонного номера отправителя SMS.

Параметры типа set и choice передаются скрипту-обработчику в виде текстовой строки, состоящей из нулей и единиц. Нули соответствуют не выбранным значениям, единицы — выбранным, общее число символов равно числу предлагаемых вариантов. Дальнейший разбор этой строки следует производить в вызываемом скрипте.

Результат выполнения скрипта (а именно, то, что он выводит в стандартный выходной поток) будет отправлен на телефон пользователя в виде одной или нескольких SMS. Подробно о скриптах Linux см. Часть 7 данного руководства и соответствующую документацию по Linux.

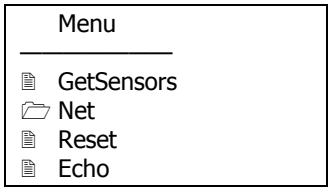
Пример. Удалённый рестарт банкомата. В цепь электропитания банкомата включён силовой контроллер NSG SPC–2i, подключённый к порту 1–Wire. Предполагается, что контроллер имеет аппаратный идентификатор 3A6E0E0100000062. Продолжительность прерывания питания устанавливается в настройках данной цепи данного контроллера на данном порту (по умолчанию — 1 сек.)

```
MENU {
ResetATM() nsgsh .port.1-wire.device.swt2-3A6E0E0100000062.circuit.1.drop;
}
```

Пример более сложного файла конфигурации. К порту a1 подключён внешний адаптер RS–232/1–Wire, за которым находится шина 1–Wire с набором датчиков.

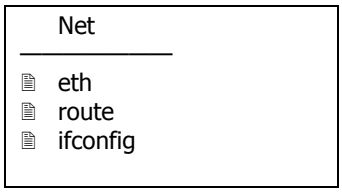
```
USER 79031111111;
USER 79262222222 Vasya root;
MENU {
GetSensors() nsgow .port.a1.1-Wire;
Net{
    eth(AdmState:choice:up:down) /etc/eth0config $1;
    route() ip route show;
    ifconfig(interface:string) ifconfig $1;
    }
Reset(password:password tmo:number) nsgreset $U $G $1 $2;
Echo(str) echo $1;
}
```

При такой конфигурации пользователь MoNsTer увидит на мобильном телефоне список:

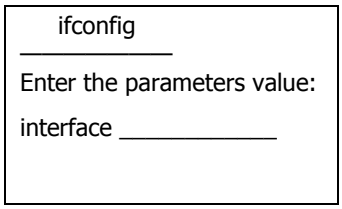


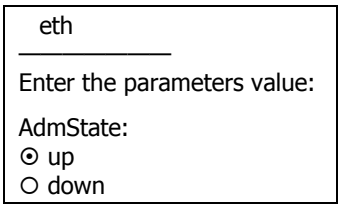
где второй пункт (Net) является подменю, а три остальные — командами.

При выборе пункта Net он увидит следующий экран:



При выборе пунктов ifconfig и eth, соответственно:





При выполнении команды eth будет вызван пользовательский скрипт /etc/eth0config, которому в качестве параметра будет передана строка 10 либо 01, соответственно. Нижеприведённый пример скрипта ставит интерфейс eth0 в состояние, соответственно, up либо down :

```
#!/bin/sh
case $1 in
10)
ifconfig eth0 up
;;
01)
ifconfig eth0 down
;;
*)
ifconfig eth0 up
;;
esac
```

Данный скрипт следует создать на борту вручную с помощью редактора nano, ручного ввода с консоли (cat >/etc/eth0config, по окончании нажать CTRL–D и Enter), или создать на ПК и перенести на устройство любыми доступными средствами (SSH, TFTP и т.п.). Скрипту необходимо дать права на исполнение:

```
chmod +x /etc/eth0config
```

§2.6.15. Инкапсуляция sms-handler — настройка порта для текстового управления

Параметры порта. Для текстовой/Android реализации в меню порта предусмотрены, наряду с общими параметрами, также следующие (специфичные по форме, но не по смыслу):

log-level Уровень детализации отладочных сообщений: от одних только фатальных ошибок (fatal) до всех сообщений без исключения (debug). Для эксплуатационного режима работы рекомендуется уровень info. Журнал обработчика SMS можно просмотреть командой log.

users "Белый список" телефонных номеров, с которых разрешён приём управляющих SMS. Все SMS, приходящие с любых других номеров, игнорируются. В отличие от Java-реализации, номер необходимо вводить полностью в том виде, в каком он определяется сетью, например, +79876543210.

ВНИМАНИЕ Знак "+" в начале имени пользователя является опциональным. При проверке имени пользователя он игнорируется. Однако при отправке SMS используется строго имя пользователя — так, как оно записано в конфигурации. Некоторые сотовые сети понимают ввод номера без "+", другие — нет. По этой причине рекомендуется писать имя пользователя всегда с "+", за исключением специальных номеров (коротких и т.п.).

Меню и права доступа. В отличие от Java-реализации, список SMS-команд и права для их исполнения в данном случае описываются непосредственно в дереве конфигурации. Кроме того, в SMS могут быть переданы любые другие команды и скрипты ОС Linux, но они доступны для исполнения только пользователю с правами root (см. ниже).

macros Список макрокоманд, принимаемых для исполнения по SMS. Имена макрокоманд могут быть любыми, но желательно сокращать их для удобства дальнейшего набора вручную на телефоне.

macros.*имя*.script
Единственным параметром макрокоманды в данной версии NSG Linux является скрипт, выполняемый при получении данной команды по SMS. Скрипт может содержать произвольные команды ОС Linux (оболочка ash), а также вызов командной оболочки nsgsh в пакетном режиме. (В качестве примера, по умолчанию установлен запрос конфигурации — nsgsh -q _print.) Макрокоманда может содержать до 9 подстановочных символов $1, $2, ..., $9, вводимых пользователем при отправке SMS. Например, следующая макрокоманда

```
macros
: s
: : script = "ifconfig eth$1"
```

при получении SMS с текстом "s 0", "s 1" и т.п. будет выводить состояние интерфейсов eth0, eth1 и т.п. соответственно.

Если макрокоманда содержит аргументы, то для неё автоматически формируется список args по числу этих аргументов. Для каждого аргумента указываются:

description Текстовое описание макрокоманды. Включается в ответ команды getm (см. ниже) и служит подсказкой при вводе параметра в приложении NSG SMS Shell.

type Тип параметра:
- string Произвольная символьная строка
- number Целое число

Учитывается при вводе параметров в приложении NSG SMS Shell — в зависимости от выбранного значения, пользователю предлагается алфавитно-цифровая или цифровая клавиатура, соответственно. При вводе булевских (true/false) и перечислимых значений, а также строк специфического формата (IP-адрес, префикс и т.п.) пользователю необходимо самостоятельно следить за их корректностью.

Эти параметры не обязательны и непосредственно на исполнение макрокоманды не влияют.

ПРИМЕЧАНИЕ При использовании nsgsh в скриптах следует обратить внимание на права, требуемые для исполнения выбранных команд, поскольку в момент их исполнения на устройстве может быть уже открыта административная сессия, и в этом случае nsgsh запустится с правами read-only. Подробнее см. Часть 1.

users.*имя*.rights
Права доступа для данного пользователя. Допустимые значения и форматы ввода:
- root Выполняется любой скрипт ОС Linux и любая макрокоманда из списка macros. При этом, если строка начинается с символа $, то вся последующая её часть рассматривается как скрипт Linux; любая другая — как макрокоманда.
- user Выполняется любая макрокоманда из списка macros.
- macro1,macro2,macro3,... (Список имен макрокоманд через запятую) — выполняются только перечисленные макрокоманды

users.*имя*.emulate-sms

Тестовая команда для проверки работы полученной конфигурации. Показывает результат, который получится при обработке SMS с указанным текстом от данного пользователя.

Ручное управление по SMS. В качестве команды на устройство отправляется текстовая SMS. Она может содержать макрокоманду, определённую на устройстве, команду или скрипт ОС Linux. В частности, пользователь с правами root может отправить скрипт из нескольких команд ОС Linux (хотя это, как правило, нецелесообразно). Пользователь с правами user может задать в одном SMS только одну макрокоманду.

Чтобы получить список доступных макрокоманд, следует отправить на устройство SMS с текстом getm .

Результат исполнения команды отправляется в одном или нескольких ответных SMS. Если ответных СМС несколько, то они будут пронумерованы, начиная с 0 (для автоматической обработки). Номер сообщения отделяется от текста символом #, в нулевом сообщении указывается также общее количество сообщений. Например ответ из трёх СМС выглядит так:

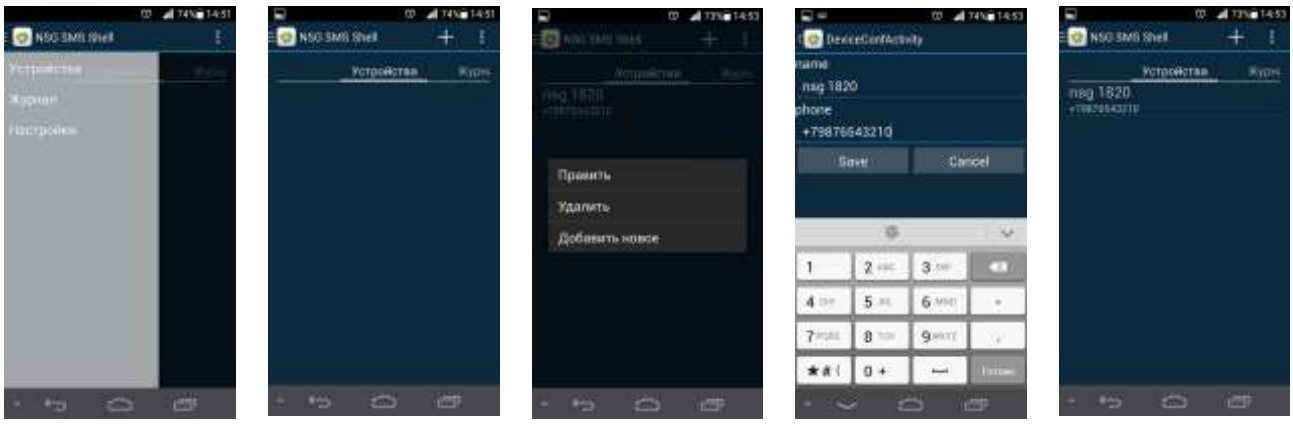
```
0#3#начало текста...
1#продолжение текста...
2#окончание текста.
```

Приложение NSG SMS Shell предназначено для смартфонов и планшетов на платформе Android 2.1 и выше. Для установки приложения следует загрузить файл SmsSh.apk с Web-сайта NSG и разрешить на устройстве установку несертифицированных приложений из сторонних источников.

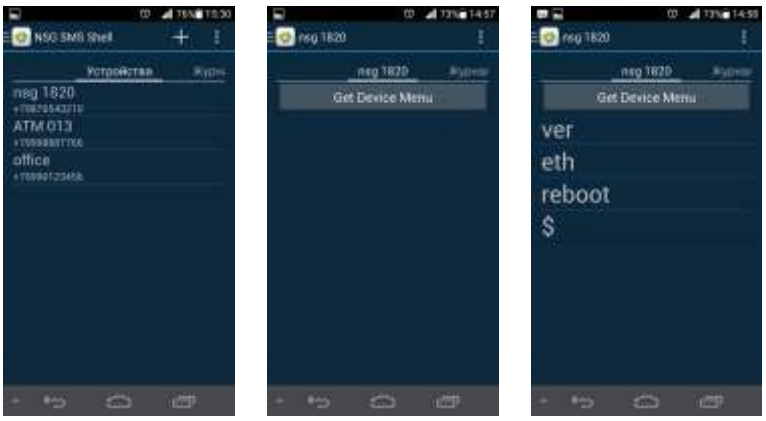
Пример. Конфигурация порта для SMS-управления:

```
macros
: eth
: : script         = "nsgsh -q .port.eth$1.show"
: : args
: : : arg1
: : : : description = "eth port number"
: : : : type        = "number"
: reboot
: : script         = "echo OK; nohup reboot -d20 >/dev/null 2>&1"
: ver
: : script         = "nsgsh -q .system.show.version"
users
: "79990001122"
: : rights         = "root"
```

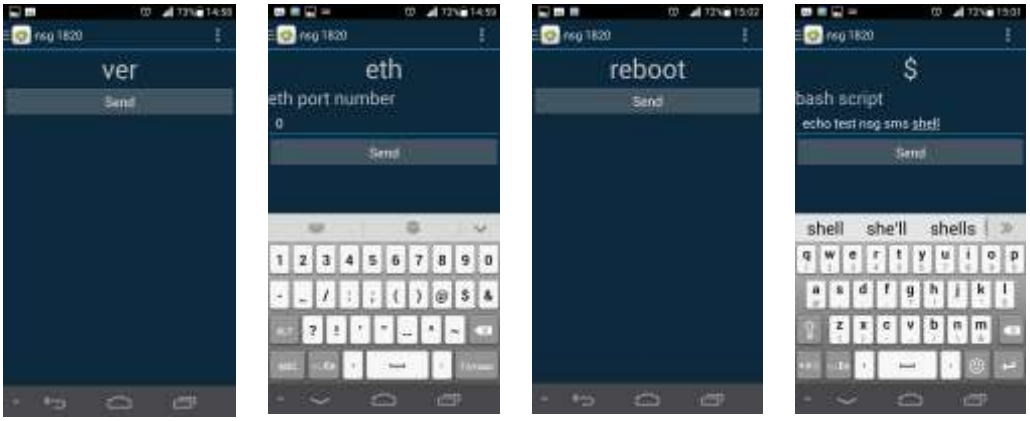
Для первоначальной настройки необходимо выбрать в меню программы пункт "Устройства" и нажать + для добавления нового управляемого устройства NSG. Для каждого устройства требуется ввести его текстовое описание и телефонный номер.



С одного телефона можно управлять несколькими устройствами. При выборе одного из устройств открывается его меню. Для вновь созданного устройства меню содержит единственную команду "Get Device Menu". После этого в меню появляется список макрокоманд, доступных данному пользователю. Пользователю с правами root, как в данном примере, дополнительно предлагается пункт $ для ввода произвольных скриптов и команд ОС Linux:



При выборе какой-либо из доступных команд открывается окно для ввода её аргументов, если таковые имеются. При выборе пункта $, аналогично, открывается окно для ввода команды ОС Linux (вводить первый символ $ при этом не требуется):



Результаты выполнения команд, полученные в ответных SMS, можно просмотреть в журнале приложения:

§2.6.16. Отправка текстовых SMS

В состав NSG Linux 2.0 входит утилита at2 для работы с модулями GSM/UMTS/LTE посредством AT-команд, в частности, для отправки текстовых SMS. Узел sms-send в меню порта GSM/UMTS/LTE представляет удобный интерфейс к этой команде для отправки SMS непосредственно из пользовательских оболочек NSG Linux 2.0. В качестве параметров в нём необходимо указать только телефонный номер адресата и текст сообщения.

Отправка SMS может быть также задана в качестве реакции на заданные события в системе, например, изменение состояния интерфейсов, срабатывание датчиков и т.п. Подробнее о механизмах генерации и обработки событий см. Часть 4. Для отправки сообщений можно как вызывать непосредственно утилиту at2 скриптами ОС Linux (см. Часть 7), так и обращаться к узлу меню send-sms с помощью пакетного режима nsgsh (см. Часть 1) или внутренних скриптов nsgconfd (см. Часть 4).

§2.6.17. Совместное использование SMS-управления и PPP

Обработчик SMS-сообщений, помимо своей основной функции, решает задачу управления модемами устаревших типов (IM–*xxx*, а также UIM–EDGE *h/w ver.3*) в процессе передачи данных. Режим совместной работы устанавливается для порта с инкапсуляцией PPP параметром

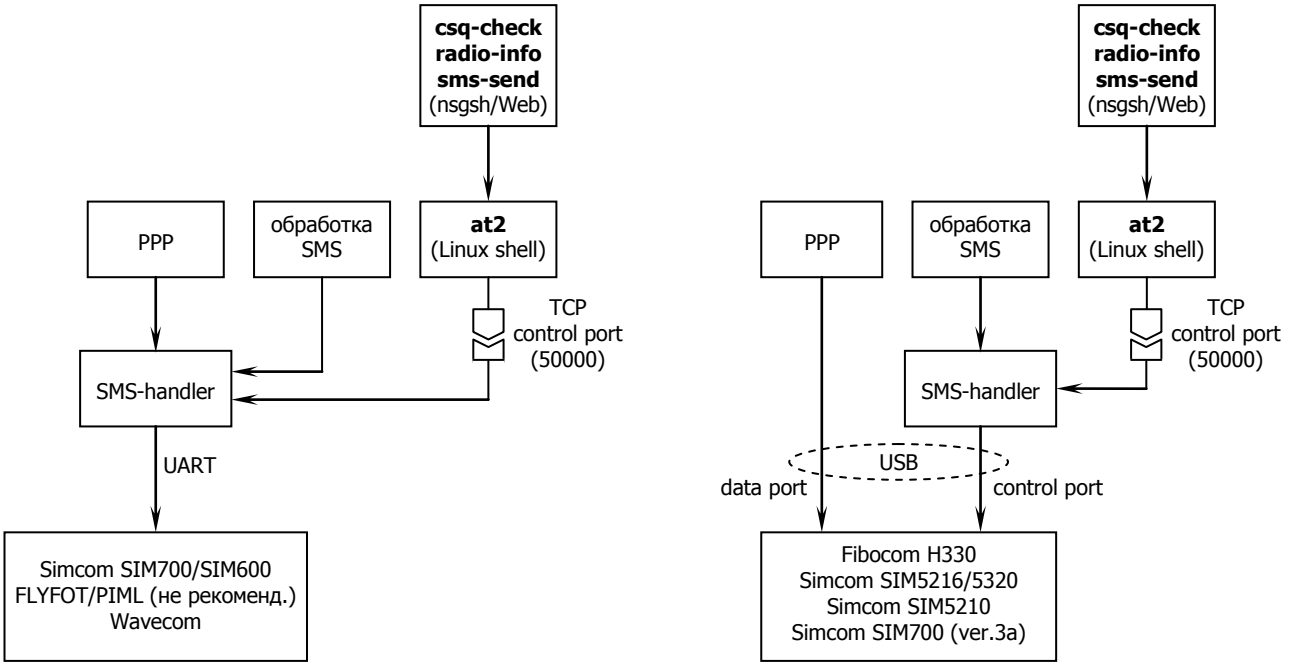
```
ppp.sms-cooperation = true
```

Проблема состоит в том, что перечисленные модули имеют единственный порт для взаимодействия с шасси. Если через этот порт передаются данные, то одновременно исполнять через него AT-команды невозможно. Поэтому обработчик встраивается между модемом и PPP-демоном, контролирует поток данных между ними, периодически переводит модем в командный режим и выполняет AT-команды: считывание входящих SMS, проверку уровня сигнала, отправку SMS и т.п. Период опроса (в Java-реализации) устанавливается параметром sms-handler.inquiry-time .

Для современных типов модемов GSM/UMTS (UIM–EDGE *h/w ver.3a*, UM–3G всех модификаций) на внутреннем интерфейсе USB эмулируются несколько последовательных портов. Обработчик определяет имя вспомогательного порта модема, следит за его созданием в системе после рестарта модема и подключается к нему. Таким образом, работа с SMS происходит без вмешательства в передачу данных, через отдельный порт, и параметр не имеет смысла. По этой причине в новой реализации SMS-управления (текстовой/Android) он не предусмотрен.

Пользователю ни в коем смысле не требуется выполнять эти операции вручную, но желательно, тем не менее, понимать, как происходит работа с модемом и почему, например, не всегда возможно узнать у него текущий уровень сигнала сети или выбранный тип услуги.

Помимо этого, в системе имеется ещё и третий претендент на доступ к модему — утилита at2, с помощью которой выполняется проверка уровня сигнала (csq-check, at2 csq) и отправка текстовых SMS (at2 sms), не имеющая отношения к SMS-управлению. Подробно об at2 см. Часть 7. Если модуль имеет вспомогательный порт и этот порт свободен, то at2 может обращаться к нему непосредственно. Если же единственный, или вспомогательный порт уже занят обработчиком SMS, то обработчик способен принимать AT-команды от других приложений, исполнять их на модеме и возвращать ответы модема. Для этой цели он открывает в системе служебный TCP порт (параметр sms-handler.control-tcp-port, по умолчанию — 50000). Через этот порт к нему обращаются другие команды и утилиты.



ПРИМЕЧАНИЕ Если обработчики SMS-сообщений включены на двух или более портах одновременно, то необходимо назначить им разные номера портов TCP. В противном случае все операции, производимые через них другими программными компонентами (контроль уровня сигнала, опрос информации о состоянии сети, отправка текстовых SMS) будут обращаться только к одному сотовому интерфейсу (определяемому случайным образом в зависимости от порядка их поднятия).

§2.7. Настройка сотовых интерфейсов HSPA+ и LTE

§2.7.1. Особенности интерфейсов Wireless MAN (WMAN)

Сотовые интерфейсы нового поколения, предназначенные для передачи данных по сетям LTE (4G) и UMTS (в режимах вплоть до HSPA+, 3,75G), имеют следующее архитектурное отличие от более ранних модулей. В соответствии с современной концепцией "Ethernet-поверх-всего-что-шевелится", они эмулируют не асинхронный интерфейс "точка-точка" с коммутируемыми соединениями и протоколом PPP, а Ethernet-подобный сетевой интерфейс с формально широковещательной средой передачи и с полным набором сопутствующих протоколов и сервисов для передачи IP (ARP, DHCP и т.п.). Таким образом, с точки зрения сетевой архитектуры, их уместнее именовать уже не модемами, а мостами, а данный тип подключений — Wireless MAN (WMAN), по аналогии с различием между проводными сетями MAN и WAN.

Такой подход обеспечивает более высокую пропускную способность внутреннего интерфейса между модемом и хостом, при одновременном уменьшении вычислительной нагрузки на обе эти стороны. Это весьма существенная деталь для высокоскоростных подключений 3,75G и 4G. Он также позволяет использовать для настройки интерфейса, вместо сложного и многообразного протокола PPP, более простые механизмы IP-over-Ethernet. Значительная часть параметров устанавливается автоматически или единственным возможным образом. При этом протокол PPP, а вместе с ним и последние из интерфейсов "точка-точка", окончательно переходит в разряд "унаследованных", что качественно сокращает зоопарк сетевых технологий и, что самое важное, объём знаний, необходимых современному эффективному сетевому администратору.

ПРИМЕЧАНИЕ С точки зрения технологий сотовых сетей, данное различие в представлении модема по отношению к хосту не играет существенной роли; в любом случае, для передачи данных в эфир используются собственные специфические протоколы и инкапсуляции сотовой сети. Современные модули пока ещё поддерживают работу как в режиме эмуляции Ethernet, так и в режиме эмуляции PPP, для совместимости с унаследованными системами.

Технология LTE предусматривает работу в различных частотных диапазонах и с использованием различных технологий дуплексирования (FDD, TDD). Разные операторы используют разные диапазоны и технологии. В зависимости от конкретного чипсета, сотовые модули могут поддерживать работу в единственной или в разных сетях LTE, а также поддерживать или не поддерживать откат на режимы 3G и 2G.

§2.7.2. Типы и идентификация интерфейсов Wireless MAN

Для передачи данных по сотовым сетям 3,75G и 4G в устройствах NSG используются фиксированные опции (NSG–1800, NSG–1820) и сменные модули (NSG–1800, NSG–700). К ним относятся:

type = "lte"	Модуль UM–LTE/3G, опция opt18xx.LTE/3G (чипсет Sierra Wireless MC7710)
type = "hspap"	*зарезервировано*

Опции WMAN в устройствах NSG–18*xx* и NSG–1820MC называются m1, m2, m3 в зависимости от того, в какой позиции они установлены. Сменные модули в NSG–1800 и NSG–700 получают имена s1, s2 в зависимости от номера разъёма расширения. Идентификацию USB-модулей в NSG Linux 2.0 рекомендуется выполнять автоматически командой update ; в отличие от ручного выбора, она сразу выявляет ситуации, когда модуль неисправен или неправильно установлен.

Особенности работы разных модификаций одного типа модулей учитываются автоматически и не требуют внимания пользователя. Более того, типы lte и hspap по существу являются синонимами и продублированы только для удобства интерпретации пользователем.

ПРИМЕЧАНИЕ Использование модулей LTE на шасси NSG–700 не всегда целесообразно в связи с ограничением пропускной способности на внутреннем интерфейсе USB 1.1 (макс. около 5 Мбит/с).

§2.7.3. Аппаратное управление сотовым модулем

Перемычка J1 на модуле определяет его поведение при рестарте внутреннего порта устройства. Если она установлена, электропитание модуля выключается и модуль аппаратно рестартует каждый раз вместе с портом. Это позволяет гарантированно вывести его из любого нештатного состояния, но требует некоторого времени на инициализацию модуля, загрузку его встроенного программного обеспечения и регистрацию в сети оператора. В большинстве задач настоятельно рекомендуется использовать эту возможность.

Модули данной группы поддерживают 2 SIM-карты и позволяют подключаться к одному либо к другому оператору. Верхняя SIM-карта всегда считается основной (main), нижняя — вспомогательной (aux). Выбор SIM-карты происходит в момент рестарта модуля, т.е. рестарт является обязательным условием для этого. Перемычка J2 устанавливает режим выбора SIM-карты:

Установлена	Всегда используется верхняя SIM-карта.
Снята	Используемая SIM-карта выбирается программно.

Для фиксированных сотовых интерфейсов в устройствах NSG–18*xx* аппаратный рестарт и программный выбор SIM-карты включены конструктивно и не выключаются.

§2.7.4. Прозрачный доступ к модулю и ручной рестарт модуля

Если порт не находится в работе, т.е. имеет adm-state = "down", то в меню порта доступна команда raw-access . Она позволяет зайти на модем в терминальном режиме и управлять им вручную с помощью AT-команд. Таким образом можно убедиться в работоспособности модема, проверить регистрацию в сети оператора и т.п. В отличие от унаследованных модулей Wireless WAN, данная возможность, как правило, не предназначена для конечного пользователя и применяется только для отладки работы модуля в сложных случаях, по указанию службы технической поддержки NSG. При этом основная часть отладочной информации снимается автоматически с помощью команд show (см. след. параграф).

Ручной рестарт модуля производится командой restart.

Дополнительное поле ввода в обеих командах позволяет явно выбрать нужную SIM-карту для 2-симчатых модулей: main либо aux. Если параметр не указан, модуль стартует с главной SIM-картой (если для неё не установлено число попыток 0) и отсчёт числа попыток для программного выбора SIM-карты начинается заново. Подробно о работе с 2 SIM-картами см. §2.6.5.

При выполнении рестарта в качестве скрипта nsgsh указание SIM-карты является обязательным, например:

```
nsgsh -q .port.m1.restart.main
```

Чтобы выполнить рестарт без принудительного выбора SIM-карты, в данном случае следует ввести после последней точки любое продолжение, отличное от main и aux.

ВНИМАНИЕ Команда restart с явно указанным параметром main или aux изменяет текущую конфигурацию устройства, устанавливая число попыток для одной и для другой SIM-карты 0 и 1, соответственно. Если после этого выполнить команду "сохранить", то эти значения так и останутся в конфигурации навсегда. Поэтому после применения команды необходимо восстановить прежние значения вручную, либо рестартовать устройство без сохранения.

§2.7.5. Выбор режима и контроль работы радиоинтерфейса

Наиболее вероятным источником потенциальных проблем, судя по имеющемуся на данный момент опыту, является регистрация модуля в должной сети и на должные услуги. Для контроля выполнения этих процедур предназначены команды узла show :

module-info Вывод информации о модуле: тип, версия прошивки, поддерживаемые режимы и т.п., а также о SIM-карте. Позволяет убедиться, как минимум, в их работоспособности, за исключением физического приёмопередатчика и антенн.

progress Выводит поэтапно ход подключения и регистрации в сети. Конечным результатом должно быть состояние RUNNING. Если оно не достигнуто, то следует включить максимальный уровень отладки для вывода более полной информации.

ПРИМЕЧАНИЕ Регистрация модуля в сети может занимать длительное время, особенно при первом включении в сети данного оператора — до нескольких минут. Вопрос о том, являются ли тому причиной особенности данной технологии как таковой, или медленная работа баз данных у конкретного оператора, или проверки модуля по IMEI в АНБ, ФСБ, таможне и других компетентных органах, не входит в сферу деятельности компании NSG.

Пример вывода:

```
[Fri Jan 1 00:16:54 UTC 2010]: ---- DAEMON READY ----
[Fri Jan 1 00:16:55 UTC 2010]: INITIALIZE
[Fri Jan 1 00:16:58 UTC 2010]: SIM_CHECKING
[Fri Jan 1 00:17:01 UTC 2010]: CLEAR UP
[Fri Jan 1 00:17:03 UTC 2010]: SET RADIO ACCESS MODE
[Fri Jan 1 00:17:06 UTC 2010]: CONNECT BS
[Fri Jan 1 00:17:09 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:11 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:13 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:16 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:18 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:20 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:22 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:25 UTC 2010]: - waiting the connection....
[Fri Jan 1 00:17:27 UTC 2010]: RUNNING
```

Длительная пауза перед RUNNING является в данном случае типичной для первого выхода в эфир.

radio-info — Вывод текущей информации о текущем состоянии модуля, уровне сигнала, режиме работы и т.п.

log — Вывод общего журнала работы порта. При выполнении команды _apply журнал обнуляется.

interface — Вывод состояния сетевого интерфейса.

Уровень детализации вывода для вышеперечисленных команд устанавливается параметром debug-level (0 — минимальный, 2 — максимальный).

Список режимов (Radio Access Technologies, RAT), поддерживаемых конкретным модулем, можно проверить командой show.module-info, а выбрать из них конкретный режим или более ограниченный перечень (например, только 2G/3G, но не LTE) — параметром mode. По умолчанию, режим выбирается автоматически. Содержание меню для данного параметра составляется автоматически в зависимости от модуля.

Помимо режимов реальной передачи данных, в меню mode имеется дополнительный пункт TESTING. В нём выполняются все операции инициализации модуля, за исключением регистрации в сети и получения IP-адреса. Этот режим предназначен для ручной диагностики и отладки возможных проблем. При выборе этого режима в узле show доступна дополнительная команда:

show.networks

Поиск всех доступных сетей и режимов работы. Операция длительная (десятки секунд), предельное время ожидания задается параметром в данной команде (30 … 180). Рекомендуется выполнять данную команду перед ручной установкой режима и в других проблемных ситуациях. Актуальность её связана, в первую очередь, с тем, что покрытие сетей LTE далеко от сплошного и, вероятно, ещё не скоро станет таковым.

ПРИМЕЧАНИЕ При обращении в службу технической поддержки по поводу работы модулей LTE/HSPA+ настоятельно рекомендуется сразу присылать вывод команд module-info, progress и networks при установленном debug-level=2, чтобы сократить лишний этап переписки.

§2.7.6. Настройка сетевых протоколов

После того, как соединение с оператором установлено на уровне сотовой сети (с точки зрения стека TCP/IP, он является физическим), интерфейс WMAN рассматривается, применительно к протоколам и процедурам вышестоящих уровней, как аналог интерфейса Ethernet. В частности, интерфейс может быть включён в состав программного моста Ethernet. Но некоторые параметры и механизмы в данном случае не имеют смысла ввиду специфики интерфейса и отношений "абонент-оператор" (например, построение VLAN), поэтому соответствующие узлы исключены из меню.

Настройка параметров IP на интерфейсе и в связанных с ним службах выполняется, по умолчанию, автоматически — посредством DHCP. При этом от оператора принимаются IP-адреса и маска для данного интерфейса и для удалённой (операторской) стороны, адрес шлюза по умолчанию, адреса DNS. Соответствующие изменения вносятся в текущую таблицу маршрутизации и в список DNS-серверов.

Если от оператора требуется получить только адреса, но не маршрут по умолчанию, или принять маршрут, но с заданной метрикой, чтобы не конфликтовать с другими имеющимися маршрутами, то следует установить параметр ifAddress.configurable="dhcp" явным образом. В этом случае становится доступным подузел dhcp-options, в котором можно управлять получением, интерпретацией и применением параметров DHCP.

IP-адреса и маски могут быть также назначены статически, если это не противоречит настройкам операторской стороны.

Заключительным этапом является настройка NAT в случае, если устройство NSG должно выпускать через данный интерфейс транзитный трафик из внутренней локальной сети в сеть оператора. Для упрощения настройки в порту данного типа предусмотрен параметр

service.add-nat/del-nat

позволяющий автоматически сгенерировать в узле .ip.nat.POSTROUTING простейшее правило маскарадинга для данного интерфейса (или, соответственно, удалить его). В соответствии с общей политикой построения интерфейса NSG Linux 2.0, данные изменения не вступают в силу автоматически, их необходимо применить вручную в указанном узле.

Пример. Минимальная конфигурация устройства в качестве шлюза для доступа из локальной сети в Интернет через сеть LTE:

```
ip
: nat
: : POSTROUTING
: : : 1
: : : : out-interface   = "m1"
: : : : target          = "MASQUERADE"
port
: eth0
: : ifAddress
: : : prefix            = "192.168.1.1/24"
: m1
: : type                = "lte"
```

§2.8. Настройка портов Wi-Fi (IEEE 802.11)

§2.8.1. Архитектура протоколов и структура сетей Wi-Fi

Сеть Wi-Fi, в предельно упрощённом понимании, можно рассматривать как локальную сеть Ethernet, в которой подменён физический уровень и среда передачи: вместо электрических сигналов в медной паре используются радиосигналы в эфире. Поверх этого физического носителя и связанных с ним протоколов используются, в конечном счёте, пакеты 2 уровня в формате, аналогичном Ethernet (так называемый уровень *псевдо-Ethernet*). Внутри этих пакетов могут передаваться уже пакеты любого типа, предусмотренного в качестве полезной нагрузки для Ethernet: IP, NetBIOS, PPPoE и т.п.

Сети Wi-Fi, как правило, строятся по топологии "звезда", аналогично проводным сетям Ethernet. Роль коммутатора Ethernet в них выполняет *точка доступа* (*Access Point, AP*). Она выполняет несколько функций:

— Коммутацию пакетов псевдо-Ethernet между виртуальными портами, к которым подключены клиенты. Клиенты в сетях Wi-Fi называются *станциями* (*Station*); этот режим является парным к Access Point и называется также *Infrastructure*, чтобы отличать его от режима *Ad-Hoc* (см. ниже). На одну точку доступа может приходиться произвольное число станций, ограниченное только её аппаратными ресурсами. При этом каждая станция обменивается данными только с точкой доступа и не взаимодействует напрямую с другими станциями. Обмен данными между двумя станциями также происходит через точку доступа, как через коммутатор.

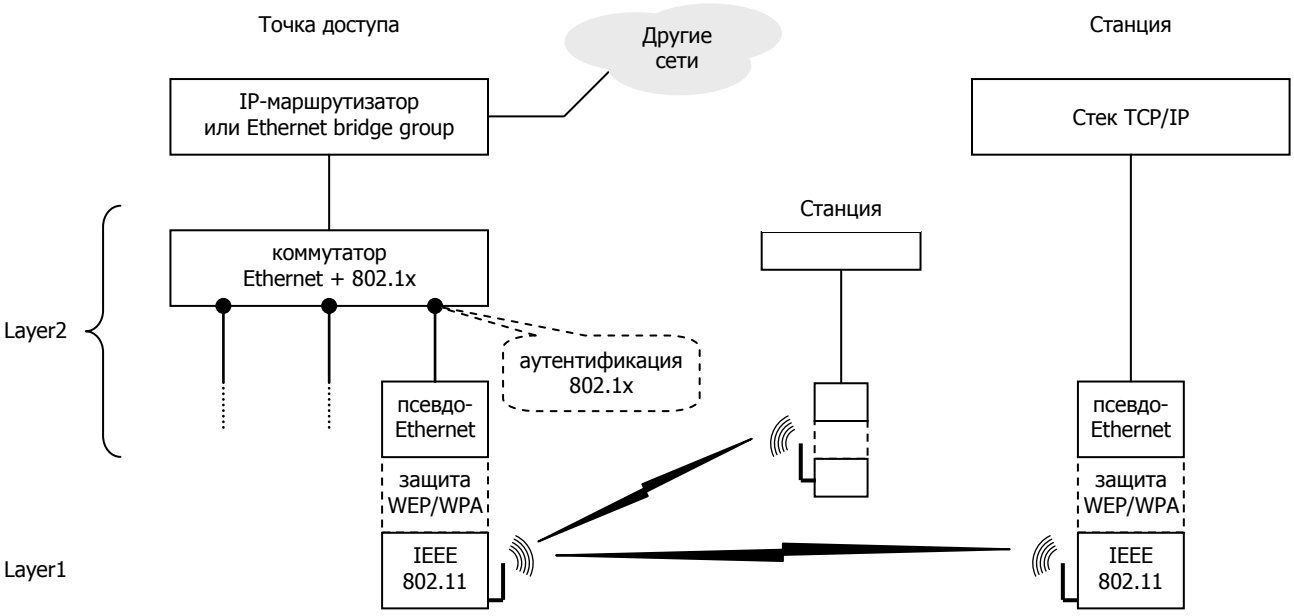
— Опционально: аутентификацию клиентов при подключении к виртуальному порту коммутатора. Аутентификация основана на протоколе IEEE 802.1x и, по существу, технически никак не связана с проводной или беспроводной природой сети. В беспроводных сетях она актуальна только по той причине, что физически проконтролировать розетки на коммутационной панели несложно, но отловить несанкционированного пользователя в радиоэфире — значительно труднее.

— Опционально: защиту трафика, передаваемого между устройствами. Ключ, используемый для защиты, одновременно может служить общим паролем для всех клиентов сети: если он хранится надлежащим образом, то посторонние пользователи подключиться к сети не могут. Именно такая конфигурация сегодня является наиболее распространённой.

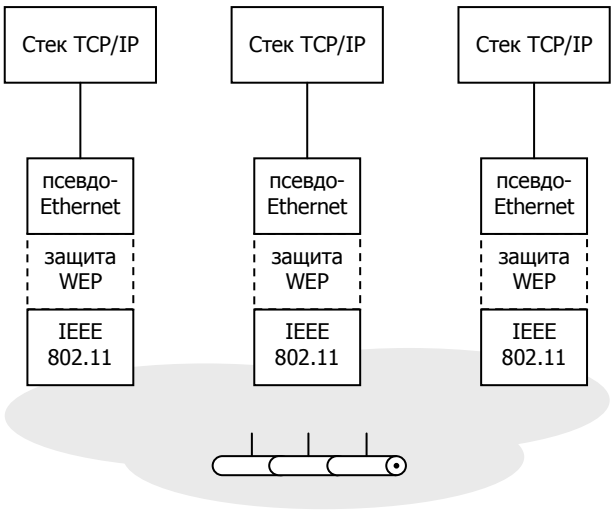
— Взаимодействие между данной беспроводной сетью и другими сетями. Как правило, это делается в режиме маршрутизации пакетов IP из беспроводной сети в вышестоящие сети. Однако в отдельных задачах точка доступа может настраиваться и в качестве коммутатора 2 уровня между проводным и беспроводным сегментами сети.

— Опционально: точка доступа, если она единственная, может выполнять по отношению к клиентам функции сервера DHCP и сервера или прокси-сервера DNS (подробнее об этих службах см. Часть 4).

Точек доступа в одной сети может быть несколько, чтобы охватить радиопокрытием бóльшую территорию и обеспечить свободное перемещение клиентов (роуминг) в пределах этой территории. В этом случае естественно использовать централизованную аутентификацию, чтобы не настраивать список пользователей на каждой точке.



Помимо сетей с топологией "звезда", в которых каждое устройство является либо точкой доступа, либо клиентской станцией, возможен третий режим — *одноранговой сети* (*Ad-Hoc*). Он предполагает установление соединения между устройствами напрямую, без использования выделенной точки доступа. При этом он вовсе не подразумевает, что в одной сети всегда находятся ровно 2 устройства; устройств может быть несколько, и они взаимодействуют по принципу "каждый-с-каждым" в единой радиосреде передачи. В качестве аналогии с проводными сетями, его можно уподобить общему коаксиальному кабелю.



ВНИМАНИЕ Режим Ad-Hoc отнюдь не означает взаимодействие двух и только двух устройств; он вполне допускает существование и третьих устройств, в том числе — несанкционированных, установленных злоумышленниками в зоне радиовидимости. Более того, он не предусматривает аутентификации 802.1x и использует только весьма слабый алгоритм WEP (см. след. параграф) для защиты трафика. По этим причинам он принципиально является слабо защищённым, и сегодня используется крайне редко.

Таким образом, настройка сети Wi-Fi в любом случае разбивается на две последовательные задачи:

— Физическое и логическое подключение через радиоинтерфейс, обеспечивающее обмен пакетами псевдо-Ethernet. Эта процедура заменяет собой физическое подключение порта Ethernet к коммутатору.

— Настройка вышележащих уровней (в большинстве задач — IP). Эта часть полностью аналогична настройкам, которые требуются в проводной сети Ethernet: назначение IP-адресов, маршрутов, DNS и т.п.

§2.8.2. Защита трафика в сетях Wi-Fi

Сети Wi-Fi, как уже говорилось выше, принципиально более небезопасны, чем проводные сети, поскольку сложно гарантировать, что злоумышленник с достаточно хорошей антенной не расположился где-либо в пределах радиовидимости. Поэтому для всех корпоративных сетей Wi-Fi, как правило, используется защита трафика. Для этой цели, по мере развития данной технологии, были предложены следующие механизмы:

— WEP (Wired Equivalent Privacy). Основан на алгоритме RC4 с длиной ключа 64 бит (пользовательский ключ 40 бит, или 10 шестнадцатеричных символов, или 5 ASCII символов + вектор инициализации 24 бита) и 3-шаговой процедуре инициализации (*handshake*). Иногда называется также WEP64 или WEP40, чтобы отличить от модификации с большей длиной ключа.

— WEP2, он же WEP104 или WEP128. То же самое, но с увеличенной длиной ключа — 128 бит (в т.ч. пользовательский ключ 104 бита, или 13 ASCII-символов).

— WPA (Wi-Fi Protected Access) — более сложный алгоритм, предусмотренный стандартом IEEE 802.11i. Основан на том же самом алгоритме RC4, но включает в себя 4 основные компоненты:
  — Временный протокол управления ключами TKIP, закрывающий наиболее уязвимые места WEP.
  — Механизм контроля целостности сообщений (MIC).
  — Использование совместно с механизмом аутентификации IEEE 802.1x.
  — Использование протокола EAP и его модификаций (PEAP и др.) для передачи идентификатора и пароля клиента в процессе аутентификации.

  Иногда в настройках беспроводных устройств обозначается как TKIP, чтобы подчеркнуть отличие от WPA2.

— WPA2 — вместо RC4 и TKIP использует новый алгоритм CCMP, включающий в себя более безопасную 4-шаговую процедуру инициализации, защиту трафика с помощью AES и интегрированный механизм управления ключами. Иногда в настройках беспроводных устройств обозначается как AES или CCMP. В любом случае, если одно из двух взаимодействующих устройств не поддерживает его, то допускается откат на WPA (TKIP).

На сегодняшний день WEP представляет собой чисто символическую защиту, поскольку взламывается за небольшое время общедоступными программными и аппаратными средствами. По этой причине его использование не рекомендуется. Он может иметь смысл только для очень старого оборудования (ранее 2004 г. выпуска), и только в случае, если это оборудование не допускает обновления своего программного обеспечения хотя бы до поддержки TKIP. Как следствие, не рекомендуется использование режима Ad-Hoc.

Алгоритм WPA (TKIP) также нельзя считать безопасным. Существуют конструктивные методы для его взлома за короткое время, хотя они и требуют существенно бóльшей компетенции.

Наконец, в 2010 г. была выявлена уязвимость и в алгоритме WPA2, причём не методом подбора паролей (*brute force attack*) и не методом взлома ключей. Тем не менее, этот алгоритм остаётся относительно наименее уязвимым, по крайней мере, при достаточной длине секрета (рекомендуется не менее 13 случайных ASCII-символов).

Принципиально другой подход к безопасности состоит в том, чтобы отказаться от неё на уровне беспроводной сети вообще и использовать безопасные туннели 2–4 уровней. В частности, PPPoE и PPTP иногда используются в домовых сетях (в основном, для аутентификации клиента и учёта потребляемых услуг), хотя также не являются достаточно безопасными. Для корпоративных применений следует использовать только IPsec или технологии на основе SSL (STunnel, OpenVPN и т.п.). При таком решении, однако, следует уделить особое внимание тому, чтобы несанкционированный клиент не смог никак воспользоваться услугами сети в обход этих туннелей: отказаться от назначения адресов по DHCP, исключить выход в Интернет через маршрут по умолчанию, заблокировать фильтрами все излишние протоколы и порты, и т.п.

§2.8.3. Аутентификация 802.1x

Аутентификация является обязательной составной частью алгоритмов WPA и WPA. Стандарт IEEE 802.1x предусматривает следующую процедуру аутентификации:

1. Клиент физически подключается к порту коммутатора, поддерживающего 802.1x, и получает режим ограниченного доступа. В этом режиме он может только передать свои реквизиты (идентификатор станции, пароль, сертификат) централизованному серверу RADIUS через этот коммутатор.
2. Коммутатор запрашивает реквизиты клиента и проверяет их либо по своему локальному списку пользователей, либо по централизованному серверу RADIUS.
3. При успешной аутентификации пользователю открывается режим полного доступа, в котором он может обмениваться пакетами Ethernet с любыми другими узлами в данной сети 2 уровня. При этом особую роль на следующем этапе играют широковещательные пакеты: запросы и ответы DHCP, ARP, PPPoE discovery.
4. Клиент может в любой момент запросить деаутентификацию и перейти в ограниченный режим. В частности, чтобы физически отключиться от коммутатора, корректная последовательность действий — это сначала деаутентифицироваться, а затем физически отключить кабель от порта коммутатора. Некорректная последовательность — кабель просто выдёргивается из работающего порта — также приводит к тому, что по переходу в состояние DOWN порт автоматически теряет аутентификацию и переходит в ограниченный режим.

В случае беспроводных сетей эта процедура полностью остаётся в силе, с тем только отличием, что вместо физического порта коммутатора она применяется к виртуальному порту точки доступа.

Для выполнения аутентификации в сетях с WPA/WPA2 NSG Linux 2.0 предусматривает два наиболее употребительных метода:

— На основе разделяемого секрета — *private mode*, он же WPA–PSK или WPA2–PSK, соответственно. Предназначен, в основном, для сетей, имеющих единственную точку доступа: домашних сетей, малых офисов. В этом случае для всех устройств используется общий секрет (Pre-Shared Key), который вводится в их конфигурации вручную.
  При необходимости, конечно, можно настроить таким образом и несколько точек доступа, но очевидно, что с ростом их числа работа по настройке и эксплуатации такой сети (смена секретов и т.п.) становится всё более трудоёмкой и чреватой ошибками.

— На основе модели Open System Authentication — *enterprise mode*, иногда обозначаемый как просто WPA или WPA2. Использует аутентификацию на централизованном сервере RADIUS и предназначен для корпоративных сетей, состоящих из большого числа точек доступа. Каждому клиенту назначается уникальный набор сетевых реквизитов (идентификатор станции, пароль и т.п.).

§2.8.4. Настройка точки доступа

При построении собственной беспроводной сети необходимо, в первую очередь, установить на беспроводном устройстве режим точки доступа и включить его:

```
port.имя.mode = "access-point"
port.имя.adm-state = "up"
```

ПРИМЕЧАНИЕ Если пункт access-point в меню отсутствует, это значит, что установленный модуль или опция Wi-Fi поддерживает работу только в режиме станции.

Далее на точке доступа необходимо настроить следующий набор параметров, согласованный с настройками клиентских станций (см. след. параграф).

1. Физическое определение сети

Каждая из сетей, доступных в некоторой географической точке, должна иметь уникальный идентификатор — SSID. Если идентификаторы двух или более сетей, видимых одновременно, совпадают, то ни одна из них не сможет функционировать нормально. Кроме того, SSID также используется при генерации PSK. По этим причинам не рекомендуется использовать очевидные типовые идентификаторы, такие как *default, office54g* и т.п.

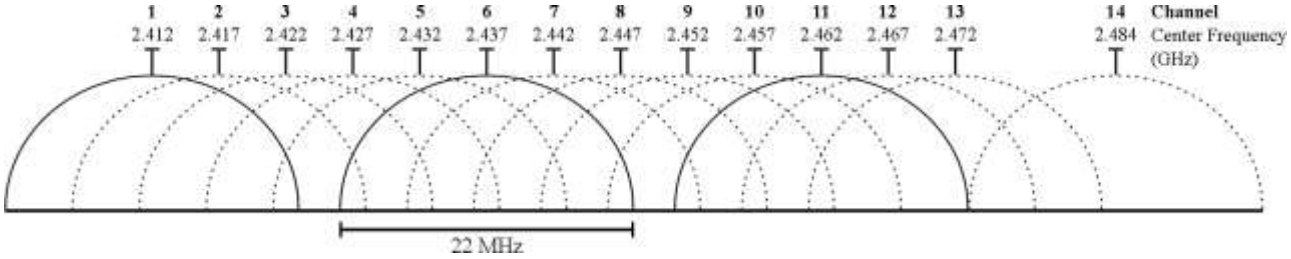
Другие параметры сети настраиваются в узле details. Как правило, в большинстве случаев для них подходят значения по умолчанию, изменять их рекомендуется только в случае явной необходимости.

— Режим (скорость) работы сети. В зависимости от используемой аппаратной части, это может быть IEEE 802.11b,11g, 11n (т.н. *greenfield mode*) или 11bgn — смешанный режим (*mixed mode*).

— Максимально разрешённое число клиентов, работающих в сети одновременно.

— Частотный канал, на котором работает данная сеть. Всего в диапазоне 2,4 ГГц определено 14 каналов, но разрешённый набор каналов различается для разных стран и регионов. Устройства NSG поставляются настроенными на российский набор каналов — с 1 по 13.
Если в одной системе работает несколько точек доступа, то каждая из них должна работать на своём частотном канале (как минимум, каждая из видимых в данной географической точке).

ПРИМЕЧАНИЕ Частотные каналы, определённые стандартом, имеют ширину 22 МГц, а разнесены всего на 5 МГц, поэтому частично пересекаются. По этой причине следует использовать только каналы 1, 6 или 11. Предварительно рекомендуется просканировать эфир (в режиме клиентской станции, см. след. параграф) и выбрать для работы наименее загруженный (по числу сетей и мощности их сигналов) диапазон.



Частотные диапазоны Wi-Fi в диапазоне 2,4 ГГц
Источник: en.wikipedia.org, автор Michael Gauthier

Точки доступа периодически посылают в эфир сообщения о своём присутствии (*beacons*); интервал рассылки сообщений настраивается параметров beacon_int (в миллисекундах). Дополнительно, сеть может быть *видимой* или *скрытой*. Если сеть скрытая, то из этих сообщений исключается SSID, причём это может быть сделано двумя способами: в поле SSID передаётся либо пустая строка, либо последовательность из нулей такой же длины, как и реальный SSID. Второй способ совместим с более широким кругом устройств, но в некоторой степени раскрывает информацию о SSID. Кроме того, в обоих скрытых режимах точка доступа не отвечает станциям, посылающим широковещательный запрос.

Не следует рассматривать сокрытие сети как меру безопасности. В лучшем случае, оно защищает от случайного некомпетентного соглядатая, но никак не от целеустремлённого хакера. При обмене пакетами в сети SSID, по определению, передаётся в открытом виде, поэтому злоумышленник всегда может перехватить его и использовать для дальнейшего взлома. Таким образом, сокрытие сети создаёт лишь ложную иллюзию безопасности, и в то же время затрудняет настройку клиентов.

2. Безопасность сети

Если в сети предполагается использовать аутентификацию и/или защиту данных, то их настройка производится в узле .port.wlan0.security .

Для алгоритмов WEP/WEP2 необходимо назначить, как минимум, один ключ. Ключ должен состоять ровно из 10 либо 26 шестнадцатеричных символов, или 5 либо 13 ASCII символов; формат ввода и выбор между WEP и WEP2 распознаются автоматически. Всего ключей может быть до 4 шт., но действующим из них всегда является только один. Автоматический перебор ключей в WEP не предусмотрен, т.е. если действующие ключи на двух устройствах не совпадают, то соединение не будет установлено, даже если действующий ключ одного устройства находится в списке запасных для другого. Запасные ключи предназначены исключительно для удобства их быстрой одновременной смены, но сама эта смена в любом случае производится вручную. Номер действующего ключа в указывается в поле wep_default_key .

Для алгоритма WPA необходимо включить либо выключить поддержку WPA2 (напомним, что WPA2 всегда допускает откат на WPA) и выбрать режим аутентификации: personal либо enterprise. В зависимости от этого режима, изменяется набор других параметров. Для режима personal необходимо ввести разделяемый секрет — текстовую строку. Это ещё не собственно ключ, а одна из компонент для его создания, поэтому длина секрета может быть произвольной. Относительно надёжным считается секрет, состоящий из не менее чем 13 символов. Символы, как и в любом пароле, должны быть случайными, чтобы исключить подбор по словарю.

Для аутентификации WPA/WPA2 в режиме enterprise необходимо ввести параметры сервера RADIUS: IP-адрес, ключ для доступа к серверу. Опционально — номер порта UDP, на котором работает сервер (если отличается от стандартного) и IP-адрес, который будет указываться в запросах как адрес источника (по умолчанию, указывается адрес интерфейса, с которого отправляются запросы RADIUS; данный параметр позволяет принудительно установить любой другой IP-адрес, принадлежащий данному устройству). Далее, для установления безопасных туннелей PEAP/TLS/TTLS точка доступа должна иметь свой сертификат X.509.

Опционально может быть задан фильтр клиентских MAC-адресов (security.mac-address-list) . Фильтр создаётся в виде именного списка, в котором именем элемента является MAC-адрес станции, а значением — ключевое слово accept (принять) либо deny (отвергнуть). Для станций, не найденных в этом списке, применяется политика по умолчанию mac-address-list.policy .

ПРИМЕЧАНИЕ Не следует переоценивать фильтры как меру безопасности, поскольку серьёзный злоумышленник может перехватить MAC-адреса работающих станций и назначить их своему адаптеру. Скорее, это удобный инструмент для того, чтобы временно разрешить или запретить работу каких-то из своих же, заранее известных, станций.

3. Протоколы выше уровня псевдо-Ethernet

После того, как клиент успешно прошёл аутентификацию, обмен ключами и зарегистрировался на точке доступа, вступают в действие механизмы согласования параметров для протоколов вышележащих уровней. Данные процедуры уже ни в коей мере не являются специфическими для беспроводных сетей, а относятся к любым сетевым интерфейсам независимо от физической среды под ними.

Если точка доступа является исключительно мостом 2 уровня между данным беспроводным сегментом и другими сегментами (проводными или беспроводными) сети, то необходимо организовать соединение в режиме моста. Применительно к устройствам NSG, для этого нужно создать bridge-group и включить в неё данный порт WLAN и один или несколько других портов Ethernet (или равносильных им объектов). Возможно даже организовать агрегацию нескольких каналов WLAN между двумя устройствами в одно логическое соединение (bond-group). Подробно о программной коммутации Ethernet см. §2.3.1.

Наиболее распространённой можно считать конфигурацию, когда беспроводной сегмент одновременно является выделенной IP-подсетью, а единственная точка доступа использует стек протоколов IP-over-[pseudoEthernet-over-]802.11 и является для своих клиентов одновременно сервером DHCP, шлюзом по умолчанию и DNS-прокси. В этом случае необходимо, в первую очередь, сконфигурировать точку доступа как IP-маршрутизатор: назначить IP-адрес беспроводному интерфейсу (по постановке задачи — статически, см. §2.2.2), IP-адреса интерфейсам, соединённым с вышестоящими сетями, маршруты по умолчанию и/или в требуемые удалённые сети. Далее, необходимо настроить сервер DHCP для автоматической настройки стека IP на клиентах. (В противном случае потребуется вручную настраивать каждого клиента в отдельности.) Использование этой же точки доступа в качестве DNS-прокси (вместо настоящего сервера DNS в вышестоящей сети) также целесообразно в многих задачах, например, если соединение с вышестоящим оператором динамическое и само настраивается средствами DHCP или PPP. Подробно о настройке IP-маршрутизации см. Часть 3, сервера DHCP и DNS-прокси см. Часть 4, там же приведён законченный пример конфигурации.

Если на данной точке доступа вместо IP-over-pseudoEthernet используется IP-over-PPPoE (с целью аутентификации клиентов и учёта потребляемых ими услуг), то необходимо настроить сервер PPPoE и привязать его к данному беспроводному интерфейсу. Подробно о настройке сервера PPPoE см. Часть 5.

§2.8.5. Настройка клиентской станции

Режим клиентской станции является парным к режиму точки доступа и должен настраиваться совместно с ней (см. пред. параграф), независимо от того, являются ли оба устройства продуктами одного или разных производителей. Обычная постановка задачи состоит в том, что точка доступа уже имеется, и необходимо настроить клиентов для соединения с нею.

Чтобы установить режим клиентской станции и включить его, на устройстве под управлением NSG Linux 2.0 необходимо выполнить настройки:

```
port.wlan0.mode = "station"
port.wlan0.adm-state = "up"
```

В меню станции имеются два ключевых узла — команда scan для просмотра списка доступных сетей и список connections для настройки соединений с каждой сетью. Каждый элемент списка содержит набор специфических параметров, относящихся к той или иной сети; имя элемента может быть произвольным. В аппаратных и программных продуктах других производителей аналогичный набор часто называется *профилем* (*profile*) сети.

Для того, чтобы станция могла работать с некоторой сетью, необходимо создать для этой сети соединение в узле connections и указать в нём идентификатор (SSID) данной сети. Список сетей, доступных в данной точке, можно просмотреть командой scan. Если сеть скрытая, т.е. не передаёт в эфир свой SSID, то его необходимо знать заранее и специально разрешить подключение к таким сетям.

Параметр mode выбирает режим клиентской станции в сети либо однорангового соединения. Для клиентской станции он должен быть установлен в значение infrastructure.

Параметр security выбирает режим безопасности: WEP/WEP2, WPA/WPA2 или открытая передача. Другие параметры безопасности зависят от этого выбора.

Если выбран режим wep, то в настройках станции появляется узел security.wep, в котором необходимо ввести хотя бы один ключ и сделать его активным. Для этого необходимо заранее знать ключ, используемый точкой доступа. Подробно о настройке ключей WEP см. предыдущий параграф. Различение между WEP и WEP2 производится по длине ключа.

Если выбран режим wpa, то в настройках станции появляется узел security.wpa со своими дочерними узлами. Выбор WPA (TKIP) либо WPA2 (AES, CCMP, с возможным откатом на TKIP) производится параметром wpa2. Выбор режима WPA Personal либо Enterprise — в узле method.

Если выбран метод Personal, то дополнительно появляется один параметр — разделяемый секрет (PSK), или passphrase. Он должен быть известен заранее.

Если выбран метод Enterprise, т.е. модель Open System Authentication, то требуется ввести более обширный набор реквизитов, требуемых для аутентификации EAP на централизованном сервере RADIUS. Значения этих параметров должны быть согласованы с настройками сервера:

identity	Уникальный идентификатор станции в системе.
open.password	Пароль доступа для данной станции.
open.eap	Протокол, из числа расширений EAP, используемый для аутентификации. В данной версии NSG Linux поддерживаются PEAP, EAP-TLS и EAP-TTLS.
open.ca_cert	Путь и имя файла, содержащего сертификат клиента.
open.phase2	Дополнительные параметры для второй фазы аутентификации (внутри защищённого туннеля).

Наконец, подключение к сети (точнее говоря, попытка подключения) и отключение от неё производятся с помощью параметра active. Устройство последовательно пытается соединиться со всеми известными ему сетями, имеющими флаг active = true. Порядок следования сетей при этом определяется параметрами priority в каждом из известных соединений.

Далее необходимо настроить вручную параметры IP на беспроводном интерфейсе. Простейший вариант — если в сети (непосредственно на точке доступа, либо где-либо в сети за ней) настроен сервер DHCP. В этом случае достаточно включить клиента DHCP:

```
port.wlan0.ifAddress.configurable = "dhcp"
```

Если данное сетевое решение не предусматривает автоматической настройки клиентов, то необходимо настроить вручную IP-адрес и маску на интерфейсе, IP-маршрутизацию (как минимум, маршрут по умолчанию в данный интерфейс) и, при необходимости, клиента DNS.

Если вышестоящая сеть выделяет для клиентской станции только один адрес и ничего не знает о сетях, расположенных за этой станцией, то дополнительно необходимо настроить на интерфейсе NAT, а именно, IP-маскарадинг (или Source NAT, если IP-адрес интерфейса заранее известен). Это обычная ситуация при подключении к сетям общего пользования. Пример минимальной настройки (она же выполняется разовой командой add-nat/del-nat):

```
ip
: nat
: : POSTROUTING
: : : 1
: : : : out-interface  = "wlan0"
: : : : target         = "MASQUERADE"
```

Подробно о настройке IP-маршрутизации и NAT см. Часть 3, клиентов DHCP и DNS — Часть 4.

Если вместо IP-over-pseudoEthernet используется IP-over-PPPoE, то необходимо настроить клиента PPPoE и привязать его к данному беспроводному интерфейсу. Подробно о настройке клиента PPPoE см. Часть 5.

Автоматизация мониторинга радиоинтерфейса. Для автоматического анализа уровня сигнала и других параметров сотовый интерфейс может рассматриваться как датчик с аналоговым выходом, работающий в рамках общего обработчика событий (см. Часть 4). В порту предусмотрен узел event-generator, в котором можно определить интересующие состояния уровня сигнала (например, нормальный, неустойчивый и недопустимо низкий). Переходы из одного состояния в другое считаются событиями и вызывают ответное действие, указанное в обработчике. В частности, это может быть переход на другой канал связи, отправка уведомлений по SMS и электронной почте, включение индикации, отправка TCP-уведомлений на сервер мониторинга NSG, и т.п. В частности, TCP-уведомления могут, помимо сервера, учитываться системой *ui*TCP и выводиться в окне мониторинга клиента.

§2.8.6. Настройка соединений Ad-Hoc

Режим соединения Ad-Hoc, по существу, есть урезанный вариант клиентской станции. Ключевое отличие заключается в параметре mode. Из всех средств безопасности доступно только WEP/WEP2. Минимальный вариант настроек с включенным WEP/WEP2:

```
port
: wlan0
: : mode                = "station"
: : adm-state           = "up"
: : connection
: : : имя_соединения
: : : : ssid            = "сеть"
: : : : active          = true
: : : : mode            = "ad-hoc"
: : : : security        = "wep"
: : : : wep
: : : : : key0          = "ключ"
: : : : : wep_default_key = 0
```

Далее необходимо настроить IP-адреса, маршрутизацию, DNS и т.п. на всех узлах данной сети. Как правило, это относительно небольшие системы с простейшей статической конфигурацией, выполняемой вручную.

§2.9. Настройка портов технологического управления 1–Wire

§2.9.1. Типы и идентификация интерфейсов 1–Wire

1–Wire — низкоскоростная последовательная шина, удобная для задач технологического мониторинга и управления. Устройства под управлением NSG Linux 2.0 поддерживают, помимо своей основной функции передачи данных, вспомогательную функцию мониторинга и управления разнообразным оборудованием на этой же площадке. Они выполняют роль ведущего устройства шины 1–Wire и могут управлять различными типами датчиков (для мониторинга) и контроллеров (для управления) для различных физических параметров.

В устройствах NSG предусмотрены следующие типы портов 1–Wire:

— Встроенный порт на устройствах NSG–700/4AU *h/w ver.6* и выше, NSG–600 и NSG–605 с индексом *i* (*industrial control*), NSG–1820MC.

— Внешний адаптер RS–232/1–Wire стороннего производителя (например, Элин ML97U). Для порта в этом случае следует установить инкапсуляцию 1-wire.

Вся настройка, мониторинг и управление устройствами 1–Wire производятся в меню соответствующего порта. На шине, подключённой к этому порту, может находиться практически неограниченное число устройств. Каждое устройство содержит, как правило, несколько входных/выходных объектов (электрических цепей и т.п.). Наконец, в узле каждого объекта имеется свой набор команд, которые выполняются независимо от других объектов на этом и других устройствах.

Управление устройствами 1–Wire во многих задачах удобно сочетается с возможностью создавать в системе новых пользователей и индивидуальные меню для них. Это позволяет предоставить доступ в систему низкоквалифицированному техническому персоналу — например, дежурным операторам, имеющим инструкцию в определённых ситуация рестартовать определённые устройства по питанию — без опасений, что они повредят что-либо за пределами их компетенции.

Аппаратные вопросы подключения датчиков и контроллеров 1–Wire подробно описаны в документе NSG:

Маршрутизаторы NSG. Модули и аксессуары 1-Wire для технологического управления и мониторинга. Руководство пользователя.

ПРИМЕЧАНИЕ Программное обеспечение NSG Linux содержит закрытый список поддерживаемых устройств 1–Wire. Другие устройства, выполненные на тех же микросхемах, как правило, могут быть представлены как устройства одного из известных типов. Для поддержки устройств, выполненных на иных типах микросхем 1–Wire, следует обращаться в службу технической поддержки NSG.

§2.9.2. Идентификация устройств 1–Wire

Каждая микросхема 1–Wire имеет собственный аппаратный идентификатор, содержащий её тип и уникальный заводской номер. Устройства, подключённые к одной шине, различаются по этому идентификатору. Идентификатор, как правило, указывается на корпусе изделия 1–Wire.

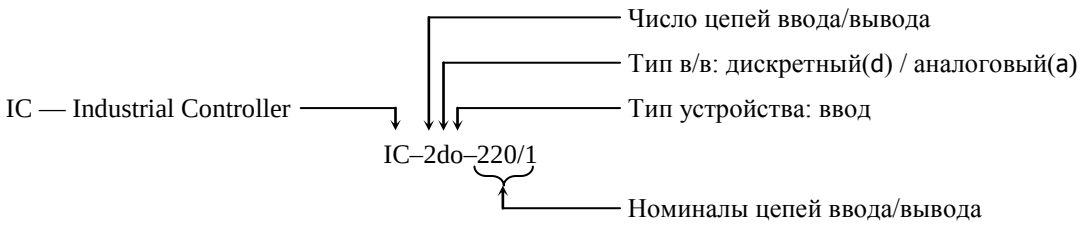
Список устройств, подключённых к шине, находится в узле devices. Каждое устройство обозначается префиксом и заводским идентификатором, например, swt2-3A6E0E0100000062 — переключатель на 2 электрические цепи. Префикс — вспомогательная часть, нужная исключительно для удобства администрирования, и может быть произвольным. Список можно составлять и изменять вручную, но эффективнее выполнить эту процедуру автоматически с помощью команды autoconfig.

Аппаратный идентификатор устройства позволяет судить о типе микросхемы, но этого не всегда достаточно для того, чтобы исчерпывающе определить тип устройства. Поэтому в меню большинства устройств имеется параметр type, позволяющий выбрать один из нескольких продуктов NSG, построенных на данной микросхеме и известных системе. Основной вопрос, применительно к построению системы управления — это является ли данное устройство датчиком (т.е. работает только на считывание состояния входов, *read-only*) или контроллером (работает на чтение и запись в выходные цепи, *read-write*).

В некоторых устройствах параметр type может иметь иной смысл. Например, для термодатчиков на основе микросхемы DS18S20 (Элин ML20S) он определяет единицы изменения: градусы Цельсия или Фаренгейта.

Контроллеры NSG SPC–8, SPC–2 и др. являются, по определению, устройствами вывода. Устройства 1–Wire сторонних производителей добавляются в NSG Linux индивидуально по мере необходимости.

Номенклатура большинства устройств NSG для шины 1–Wire построена по следующей схеме:



§2.9.3. Ручной мониторинг и управление входными/выходными цепями

Мониторинг и управление производятся в меню каждого из устройств 1–Wire, присутствующих на шине. Для большинства устройств в нём содержится узел circuits, содержащий цепи ввода-вывода (в зависимости от их числа и типа на данном устройстве). Команды show в меню порта, устройства и отдельно взятой цепи показывают состояние всех входов/выходов в пределах данного узла.

Если рассматриваемое устройство является контроллером *read-write*, то в меню каждой его выходной цепи добавляются команды и параметры для управления ею. Для двоичных электрических цепей это команды short и open (замкнуть/разомкнуть постоянно), pulse и drop (замкнуть/разомкнуть на короткое время), toggle (изменить состояние на противоположное). Время замыкания/размыкания цепи для команд pulse/drop устанавливается параметром reset-delay.

ВНИМАНИЕ Начальное состояние для контроллеров 1–Wire не определено по самой постановке задачи. Предполагается, что управление есть разовое действие. После него, до следующего акта управления, цепи контроллера должны находиться в установленном состоянии неограниченно долго, вне зависимости от программной среды управляющего устройства. Иначе говоря, устройство NSG может рестартовать (программно) целиком, может рестартовать отдельно его порт 1–Wire — состояние контроллеров при этом не изменяется.
Если шина 1–Wire, или отдельные контроллеры на ней, имеют автономное электропитание, то они независимы от устройства NSG и аппаратно, т.е. при отключении питания устройства NSG их состояние сохраняется неопределённо долго (пока сами они имеют питание).

§2.9.4. Автоматизация мониторинга и управления

Командная оболочка и Web-интерфейс являются только пользовательским интерфейсом для работы с устройствами 1–Wire. Реально они вызывают утилиту nsgow, исполняемую в командной среде ОС Linux. Подробное описание этой утилиты и её опций см. в Части 7. На её основе пользователь может писать разнообразные скрипты для опроса датчиков и управления контроллерами, вызывать её автоматически через telnet, ssh, cgi и другие инструменты автоматизации.

Пример 1. Нижеприведённый скрипт раз в час опрашивает датчик температуры, анализирует вывод, и если ответ находится вне диапазона 20.0 … 29.9°C, отправляет SMS администратору:

```
#!/bin/sh
(
while [ 1 -ne 0 ]; do
    TEMP=$(nsgow .port.1-wire -d 1046FE6201080072)
    if echo $TEMP | grep -v "t =  2"; then
        at2 sms .port.edge +79012345678 "$(hostname) $TEMP"
    fi
    sleep 3600
done >/dev/null 2>&1
)&
```

Пример 2. Нижеприведённая конфигурация проверяет доступность заданного хоста и, если он становится недоступен, передёргивает питание в розетке A:

```
services
: netping
: : reset_my_buggy_host
: : : destination      = "123.45.67.89"
: : : failure-script   = "nsgow .port.1-wire -d 3A6E0E0100000062:b -A drop"
```

Возможно также вызывать nsgow опосредованно, через вызов nsgsh в режиме скрипта. Эквиваленты для вышеприведённых примеров (во втором случае устройству необходимо заранее присвоить один из типов *read-write* и сохранить конфигурацию):

```
nsgsh -q .port.1-wire.device.1046FE6201080072.show
nsgsh -q .port.1-wire.device.3A6E0E0100000062.circuit.A.drop
```

§2.10. Настройка других типов портов

§2.10.1. Принтеры

В состав NSG Linux 2.0 входит принт-сервер для работы с локальными принтерами, подключенными через порты USB (встроенные либо сменный адаптер UM–USB). Поддержка сетевой печати реализована на основе технологии HP JetDirect (другое название — Raw Socket Printing). Таким образом, попутно со своей основной функцией передачи данных, устройство NSG позволяет превратить принтер, не оснащённый сетевым интерфейсом, в сетевое устройство.

ПРИМЕЧАНИЕ Перед приобретением устройства и принтера для совместной эксплуатации следует уточнить, поддерживает ли данная модель принтера технологию JetDirect. Информацию о совместимости можно получить на специализированных Web-ресурсах и, в отдельных случаях, в службах технической поддержки фирм-производителей.
Список проверенных моделей принтеров, а также адаптеров USB–LPT, доступен на Web-сайте NSG (http://www.nsg.ru) в разделах FAQ, Форум и Документация/Справочные материалы. Компания NSG будет признательна пользователям за любую (положительную или отрицательную) информацию о совместимости других моделей принтеров.

Для порта, к которому подключён принтер, необходимо установить тип

```
type = "printer"
```

Основным параметром порта этого типа является номер порта TCP, который обслуживается принт-сервером. По умолчанию, используется порт 9100. Если к устройству подключено два или три принтера, то для них можно использовать порты 9101 и 9102; каждый принтер должен иметь уникальный номер порта.

Дополнительными параметрами являются привязка к определённому IP-адресу (если нет, то он доступен по всем IP-адресам, присвоенным данному устройству NSG), и режим одно/двустороннего обмена. Большинство современных моделей принтеров работает в двустороннем режиме, обеспечивающем расширенный обмен диагностической информацией с соответствующими драйверами и утилитами.

Для работы с принт-сервером на клиентских ПК должен быть установлен драйвер принтера и сделана привязка этого драйвера не к локальному физическому порту, а к виртуальному порту TCP/IP.

ПРИМЕЧАНИЕ Сетевой принтер, работающий на основе Raw Socket Printing, не имеет ничего общего с понятием "общего доступа к принтерам и файлам" в сети Майкрософт. В сети Майкрософт такой принтер настраивается как локальный, подключённый к виртуальному порту TCP/IP.

Примеры настройки клиентских ПК в ОС Windows и Linux приведены в документе NSG:

Настройка клиентов сетевой печати TCP/IP

§2.10.2. Устройства хранения данных

В NSG Linux 2.0 предусмотрена поддержка различных типов накопителей, в зависимости от типа устройства:

— USB Flash и USB HDD, подключаемых к фиксированному порту USB или через сменный адаптер UM–USB.

— Карт памяти формата MicroSD (SDHC до 32 ГБ, или SDSC до 2ГБ, в зависимости от модели устройства), устанавливаемых во встроенное гнездо на некоторых моделях и модификациях.

В первом случае для порта должен быть установлен тип устройства

```
type = "storage"
```

Для дальнейшей работы накопитель необходимо смонтировать в файловую систему устройства командой mount . Команда требует подтверждения (в консольном интерфейсе) или выбора yes (в Web-интерфейсе). Обратная операция — unmount — выполняется перед физическим извлечением накопителя; в частности, она обязательна, если накопитель использовался для записи, например, для хранения журналов.

Если подключённый накопитель корректно отформатирован и не вызывает системных конфликтов (см. след. параграф), то в данном узле дерева появляется список файлов, имеющихся на накопителе, и возможных операций с ними. Корневая директория накопителя обозначается в данном случае как //, в связи с особенностями работы Web-интерфейса.

Файлы могут быть скопированы, перемещены или удалены, поодиночке или целыми директориями. Для копирования и перемещения предлагаются некоторые стандартные директории на устройстве (например, используемые по умолчанию для хранения сертификатов) или свободное указание пути по усмотрению пользователя. Следует помнить, однако, что копировать и перемещать файлы можно только в директории, запись в которые разрешена; на большинстве устройств, за исключением серии NSG–1000, это только /etc и её

поддиректории. Чтобы переименовать файл, оставляя его в прежней директории, следует использовать ту же операцию перемещения и указать путь ./новое_имя .

Информацию о каждом файле можно получить с помощью команды info в меню этого файла. Эта же команда в меню накопителя показывает сведения о системном имени накопителя, точке его монтирования и т.п., а также дополнительные указания в некоторых особых случаях.

ПРИМЕЧАНИЕ Предполагается, что внешний накопитель используется в устройствах NSG, в основном, для простых операций переноса и хранения небольшого числа файлов, лежащих в его корневой директории. Например, это может быть хранение журналов различных служб или перенос сертификатов и ключей на устройство.
Не рекомендуется использовать для этой цели накопители с большим числом файлов и сложной структурой директорий, поскольку её анализ и построение соответствующего командного дерева может занять неоправданно длительное время.
Также предполагается, что на накопителе имеется только один раздел, отформатированный в одной из наиболее распространённых файловых систем: FAT16, FAT32 (все устройства), EXT2 (кроме NSG–600), NTFS (кроме NSG–600 и NSG–700). Работа с накопителями, содержащими несколько разделов, в данной версии NSG Linux не предусмотрена.

§2.10.3. Особенности использования USB-накопителей совместно с модулями EVDO/A

При использовании внешних накопителей USB Storage (Flash, HDD) на устройстве, в котором имеется сотовый интерфейс на основе чипсета CMOTech CNE–680 (NSG–600D, NSG–605D, сменный модуль UM–EVDO/A *ver.5*) имеется следующая проблема, связанная с особенностями его конструкции и настройки.

USB-модемы в ОС Linux могут работать в двух режимах: ACM Modem (прямая интеграция в систему) и USB Serial (эмуляция одного или нескольких COM-портов поверх USB). Исторически сложилось так, что модули NSG CDMA/EV-DO работают в режиме acm-modem . Однако CNE–680 — это составное устройство, содержащее в себе собственно модем и встроенную флэш-память, которая должна эмулировать CD-ROM с драйверами для Windows. В Linux она вполне бесполезна и, хуже того, при выборе режима acm-modem некорректно работает с драйвером usb-storage . (В Windows подобная проблема отсутствует по той причине, что там всегда используется только usb-serial и, видимо, производитель не уделил достаточного внимания альтернативному режиму.) В NSG Linux, чтобы разрешить этот конфликт, при обнаружении CNE–680 драйвер usb-storage отключается и, следовательно, никакие другие USB-накопители не могут быть использованы. Следовательно, для работы с USB-накопителями необходимо сначала перенастроить CNE–680 в режим usb-serial . Эта процедура требуется только один раз и выполняется следующим образом:

1. Если в устройстве имеется интерфейс CNE–680, то драйвер usb-serial, как уже сказано, отключается. Если при этом подключить к устройству USB-накопитель, то он будет обнаружен системой, но не будет смонтирован, с сообщением No partitions found . Подробности выводятся в окно команды info: в данном случае дело не в том, что на накопителе нет разделов или они не отформатированы, а в отсутствии нужного драйвера для него.
2. Следует перейти в меню порта CDMA и отключить его командой adm-state = "down" или encapsulation = "none". При этом в меню порта становится доступна разовая команда switch-to-usb-serial-mode . Данная команда перенастраивает CNE–680 и пытается рестартовать его. Поведение модема после перенастройки может быть не вполне предсказуемым, поэтому команду, возможно, потребуется повторить. Критерием успешной перенастройки является исчезновение команды switch-to-usb-serial-mode из меню.
3. Рестартовать устройство. После перезагрузки сотовый модуль работает в режиме usb-serial и не конфликтует с usb-storage, поэтому можно использовать USB-накопители, как описано в предыдущем параграфе. Конфигурация порта остаётся неизменной, поскольку она относится к самому шасси NSG и не связана напрямую с режимом работы модема; необходимый драйвер для модема выбирается и подключается автоматически.

После того, как сотовый модем единожды переведён в режим usb-serial, дальнейшая работа с ним производится обычным образом, никаких специальных настроек не требуется и подключение USB-накопителей возможно в любой момент. Более того, режим usb-serial имеет ещё одно существенное преимущество: он позволяет контролировать состояние радиоинтерфейса (уровень сигнала и т.п.) параллельно с передачей данных. По этой причине целесообразно при первоначальной настройке устройства сразу перевести модем в режим usb-serial, независимо от перспектив использования USB–накопителей.

Вернуть модем в режим acm-modem возможно; для этого следует подключиться к модулю в режиме raw-access и ввести команды

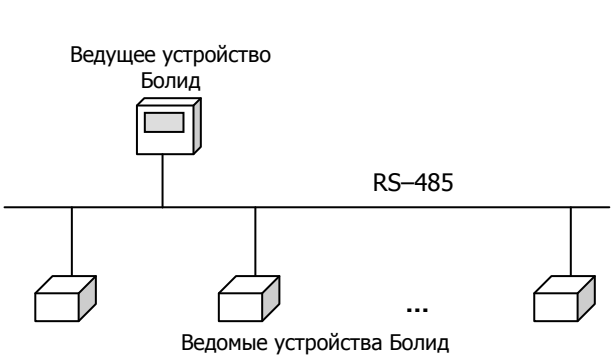
```
AT$$UMSD_RUN_MODE=5
AT$$RESET
```

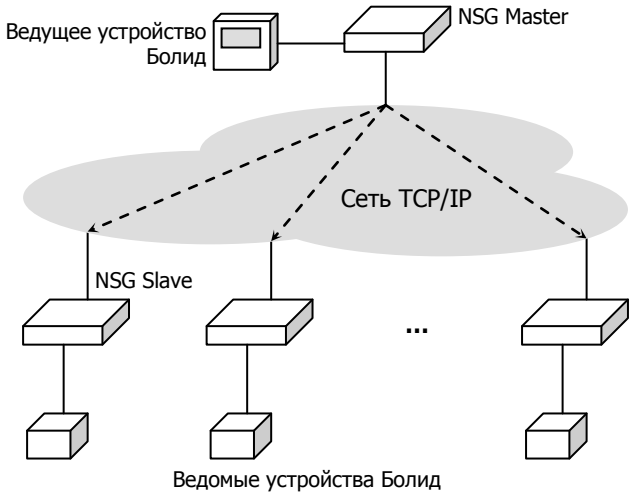
однако практическая необходимость в этом может возникнуть крайне редко: когда модуль, единожды переключённый в режим usb-serial, требуется снова использовать под управлением NSG Linux 1.0, или на шасси NSG–700/4AU *h/w ver.5* и ранее в разъёме s2. Именно для совместимости с ними модуль изначально поставляется настроенным в режиме acm-modem, несмотря на его изъяны.

Текущий режим работы модема можно определить, не прибегая к ручному вводу команд, по его внутреннему имени, которое фигурирует в выводе команд log и show порта: /dev/ttyACM*n* либо /dev/ttyUSB*n*, соответственно.

§2.10.4. Охранная система "Болид"

Данная версия NSG Linux 2.0 поддерживает работу совместно с системой охранной и противопожарной сигнализации "Болид" и позволяет использовать произвольную сеть TCP/IP для обмена данными между ведущим и ведомыми устройствами этой системы. Базовая архитектура системы "Болид" на основе физической шины RS–485 и сетецентрическая архитектура на основе виртуальной шины TCP/IP показаны на рисунках.





Ведущее (*master*) и ведомые (*slave*) устройства Болид подключаются к аппаратуре NSG посредством адаптеров Болид USB/RS–485. Устройство NSG, работающее на стороне *master*, устанавливает TCP-соединения с заданными устройствами NSG *slave*. Данные, поступающие от ведущего устройства Болид, транслируются на все ведомые устройства; данные, поступающие от каждого из ведомых устройств, транслируются на ведущее. Таким образом, сеть IP между устройствами NSG образует виртуальную шину для передачи данных по схеме "точка-многоточка", которая заменяет собой физическую шину RS–485.

ВНИМАНИЕ При настройке таймаутов на оборудовании "Болид" необходимо учитывать время передачи пакетов по сети, особенно в системах с большими задержками (спутниковых, сотовых). По умолчанию, система настроена на работу по физической шине, на которой время задержки не превосходит нескольких миллисекунд.

Для настройки работы с системой "Болид" необходимо установить в порту USB (встроенном или сменном)

```
type = "bolid"
```

и указать, в первую очередь, режим работы данного устройства (строго говоря, данного порта USB) — *master* или *slave*. Далее **для ведомого порта** устанавливается номер порта TCP, на котором он ждёт соединения от ведущего устройства.

Для ведущего устройства (порта) NSG необходимо создать список ведомых устройств (портов), каждое из которых определяется сочетанием IP-адреса и номера порта TCP. Уникальным для каждого ведомого порта должно быть только это сочетание, т.е. разные физические устройства NSG (с заведомо разными IP-адресами) могут использовать один и тот же номер порта TCP, а несколько портов USB на одном устройстве должны использовать разные порты TCP. Дополнительно можно указать текстовое описание ведомого устройства (для удобства администрирования) и параметры отправки пакетов TCP *keepalive* (интервал отправки и допустимое число потерянных пакетов). Если подтверждения о получении пакетов *keepalive* не приходят указанное число раз подряд, TCP-соединение с данным клиентом считается разорванным.

Для контроля работы системы ведётся журнал на ведущем устройстве NSG. При необходимости в более детальной отладке можно включить трассировщик, записывающий в журнал, наряду с событиями порта, передаваемые данные в 16-ричном виде.

При необходимости любое из устройств системы может быть административно выключено, или любой из клиентов может быть административно отключён со стороны сервера.

Пример. Тривиальный стенд системы "Болид" на одном устройстве NSG–700/4AU h/w *ver.6u*. Ведущее устройство системы подключено к порту usb1 на передней панели, два ведомых — к модулям UM–USB в разъёмах s1 и s2. Курсивом отмечены существенные настройки, установленные по умолчанию.

```
port
: s1
: : type     = "bolid"
: : : master          = false
: : : tcp-port        = 50016
: s2
: : type     = "bolid"
: : : master          = false
: : : tcp-port        = 50017
: usb1
: : type     = "bolid"
: : : master          = true
: : : slaves
: : : : 1
: : : : : destination  = "127.0.0.1:50016"
: : : : 2
: : : : : destination  = "127.0.0.1:50017"
```

§2.10.5. Датчики MS–6 и Меркурий 230

Данная версия NSG Linux 2.0 поддерживает следующие типы внешних датчиков, подключаемых к порту USB (фиксированному или сменному):

— Мультидатчик NSG MS–6.

— Электросчётчик Меркурий 230. Подключается через фирменный адаптер USB–RS485 и рассматривается вместе с ним, с точки зрения NSG Linix, как единое USB-устройство.

В настройках порта USB для данных устройств следует указать тип multisensor либо mercury, соответственно. Встроенная в NSG Linux 2.0 система обработки событий позволяет контролировать показания данных датчиков и реагировать заданным образом в случае, если они выходят за пределы заданных диапазонов. Настройка диапазонов по каждой из измеряемых величин производится с помощью механизма генератора событий в узле event-generator данного порта, аналогично датчикам 1–Wire. Подробно о генераторе событий и обработчике событий см. Часть 4.

§2.11. Псевдо-интерфейсы IP

Локальные псевдо-интерфейсы — это виртуальные объекты, не имеющие под собой физического носителя. Через них не может физически передаваться трафик, однако им могут назначаться IP-адреса, как и реальным физическим и туннельным интерфейсам устройства. Такие объекты могут быть полезны для некоторых специфических задач, например, для построения туннелей.

В заводской конфигурации устройства определены два псевдо-интерфейса: lo и dummy0. В отличие от физических интерфейсов, эти псевдо-интерфейсы всегда находятся в состоянии UP.

Другое частое использование псевдо-интерфейсов — в качестве заготовок для будущих туннельных интерфейсов *ui*TCP. При создании датаграммного соединения (*socket*) типа net, именуемого также "виртуальным интерфейсом", ему назначаются только основные параметры — IP-адреса и маска. Для всех остальных параметров, таких как, например, NAT и QoS, можно создать псевдо-интерфейс с таким же именем и описать все нужные параметры в этом узле. При создании туннеля и соединения в нём виртуальный интерфейс *ui*TCP автоматически ассоциируется с имеющимся псведо-интерфейсом и принимает все его характеристики.

§2.12. Настраиваемая светодиодная индикация

Устройства, работающие под управлением NSG Linux 2.0, могут быть оснащены настраиваемыми светодиодными индикаторами. Основное назначение этих индикаторов — отображение различных состояний устройства под управлением системного обработчика событий (*event handler*, см. Часть 4). В частности, индикаторы могут отображать состояние заданных интерфейсов, прохождение тестовых *ping*-ов, показания подключённых датчиков и др.

Для ручного управления светодиодами имеется узел меню .tools.led . Структура данного узла зависит от числа индикаторов и их типа (одно- или двухсегментные) на конкретном шасси. Для каждого сегмента каждого индикатора можно индивидуально установить состояние "включён" или "выключен".

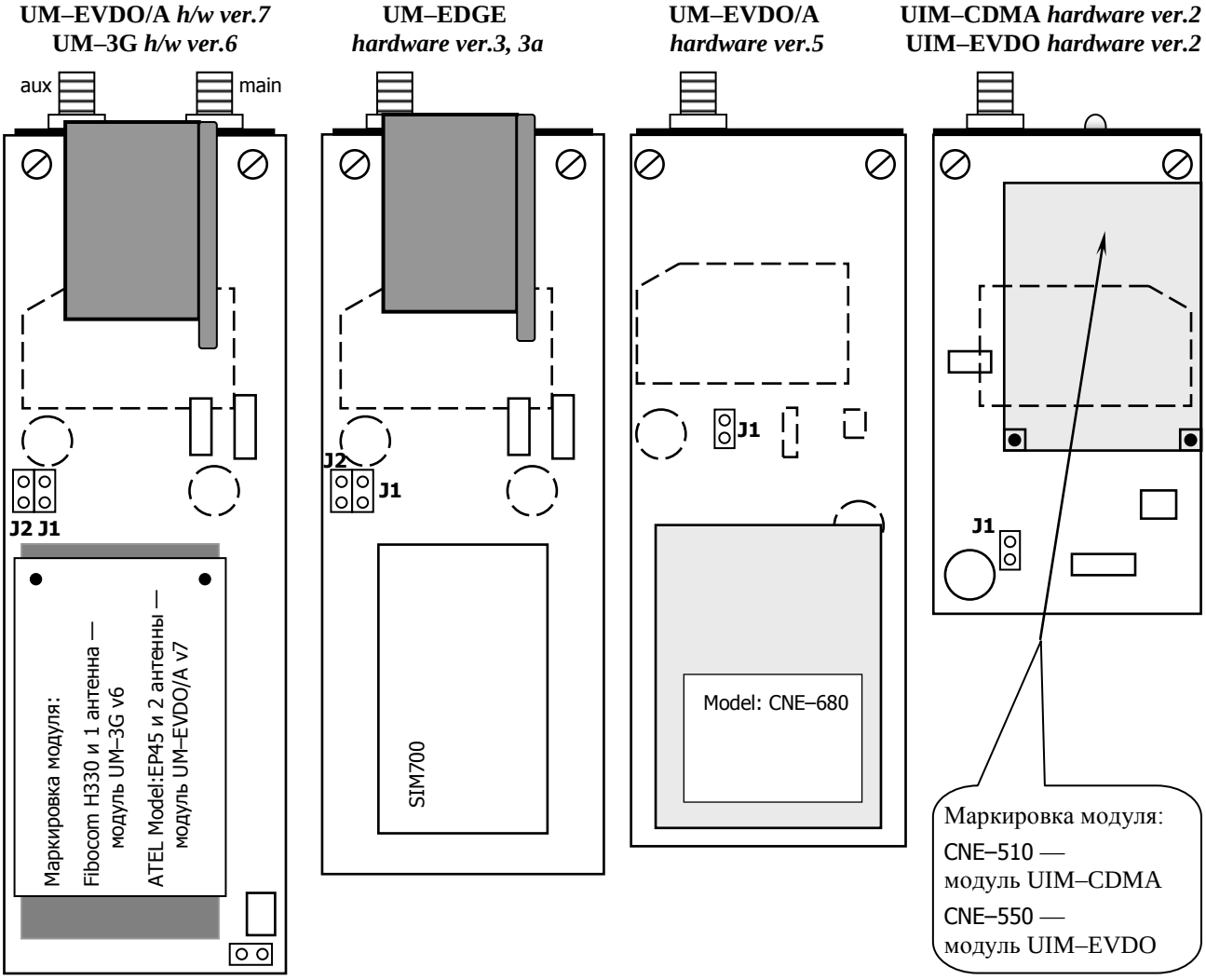
ПРИМЕЧАНИЕ Одновременное включение зелёного и красного сегмента светодиода даёт жёлтый или оранжевый цвет, но использовать его следует с осторожностью, поскольку его часто легко спутать с чисто красным.

ПРИМЕЧАНИЕ В отдельных партиях устройств NSG–700 ранних выпусков светодиоды отсутствуют, нефункциональные, одноцветные или с перевёрнутыми сегментами. Эти особенности аппаратно не распознаются, поэтому команды данного узла строятся и исполняются вслепую, без учёта их фактического результата.

Приложение 2–A. Особенности настройки сотовых интерфейсов 2G и 3G

§2–A.1. Сменные сотовые модули с внутренним интерфейсом USB

Следующие типы сотовых модулей NSG работают через внутренний интерфейс USB и могут автоматически идентифицироваться NSG Linux 2.0:



Версии модуля UIM–EDGE аппаратно имеют одинаковый чип SIM700D, но радикально различаются его внутренней прошивкой. Версию можно определить по серийному номеру чипа (вторая строчка):

ver.3 MP061044*xxxxxxx* и ранее, MP061139*xxxxxxx*
ver.3a MP061047*xxxxxxx*, MP061105*xxxxxxx* и выше

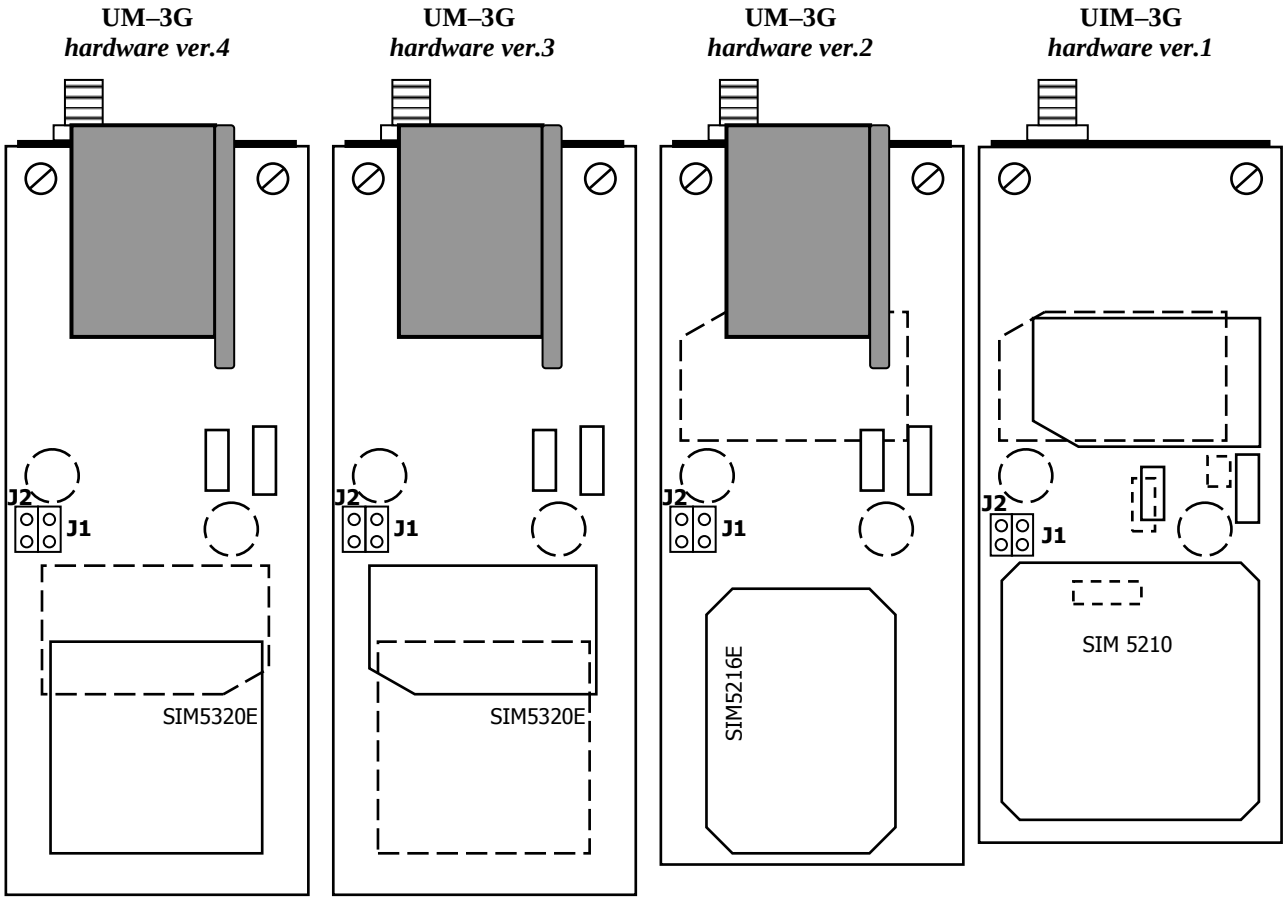
Назначение перемычек J1, J2 для всех типов модулей

J1 — управление дополнительной реакцией на падение сигнала DTR в порту (разъеме расширения) устройства NSG

1–2 (положение по умолчанию)	При падении DTR происходит аппаратный рестарт модема (равносильно выключению/включению питания)
2–3 (только IM–GPRS *h/w ver.1*)	При падении DTR модем переходит в режим Low Functionality (равносильно AT+CFUN=0, AT+CPOF)
все разомкнуты	Дополнительная реакция отсутствует

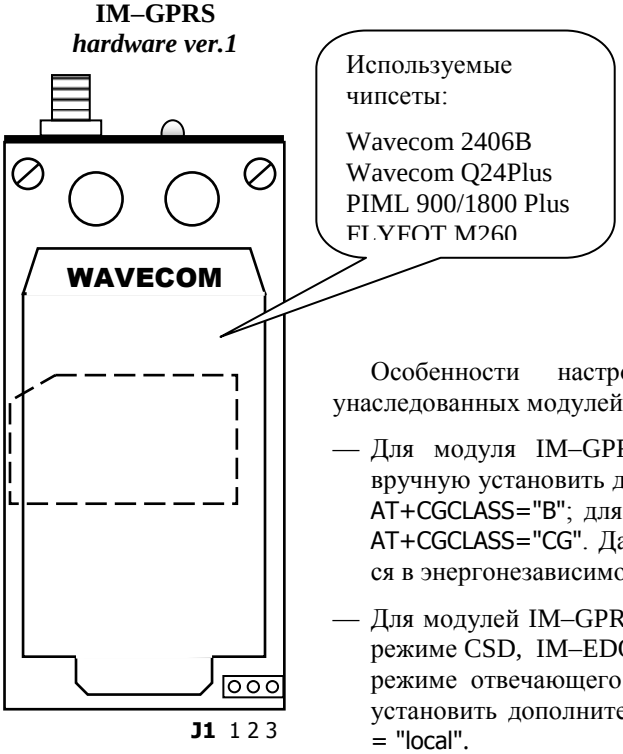
J2 — выбор SIM-карты (для модулей GSM/UMTS с 2 SIM-картами)

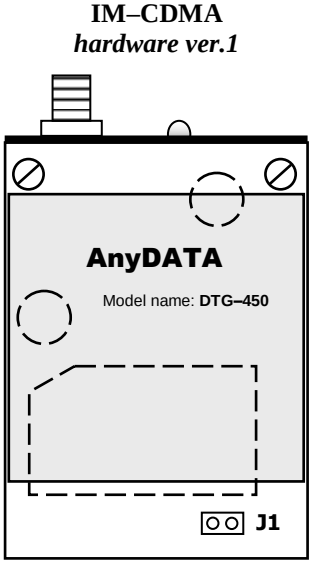
замкнуто	Всегда используется основная SIM-карта MAIN (верхняя, внешняя)
разомкнуто	Используемая SIM-карта выбирается программно, синхронно с выбором *chat-script* и *virtual-template*



§2–A.2. Сменные сотовые модули с внутренним интерфейсом UART

Следующие типы унаследованных сотовых модулей NSG работают через внутренний асинхронный интерфейс и идентифицируются в NSG Linux 2.0 как тип порта rs-232:



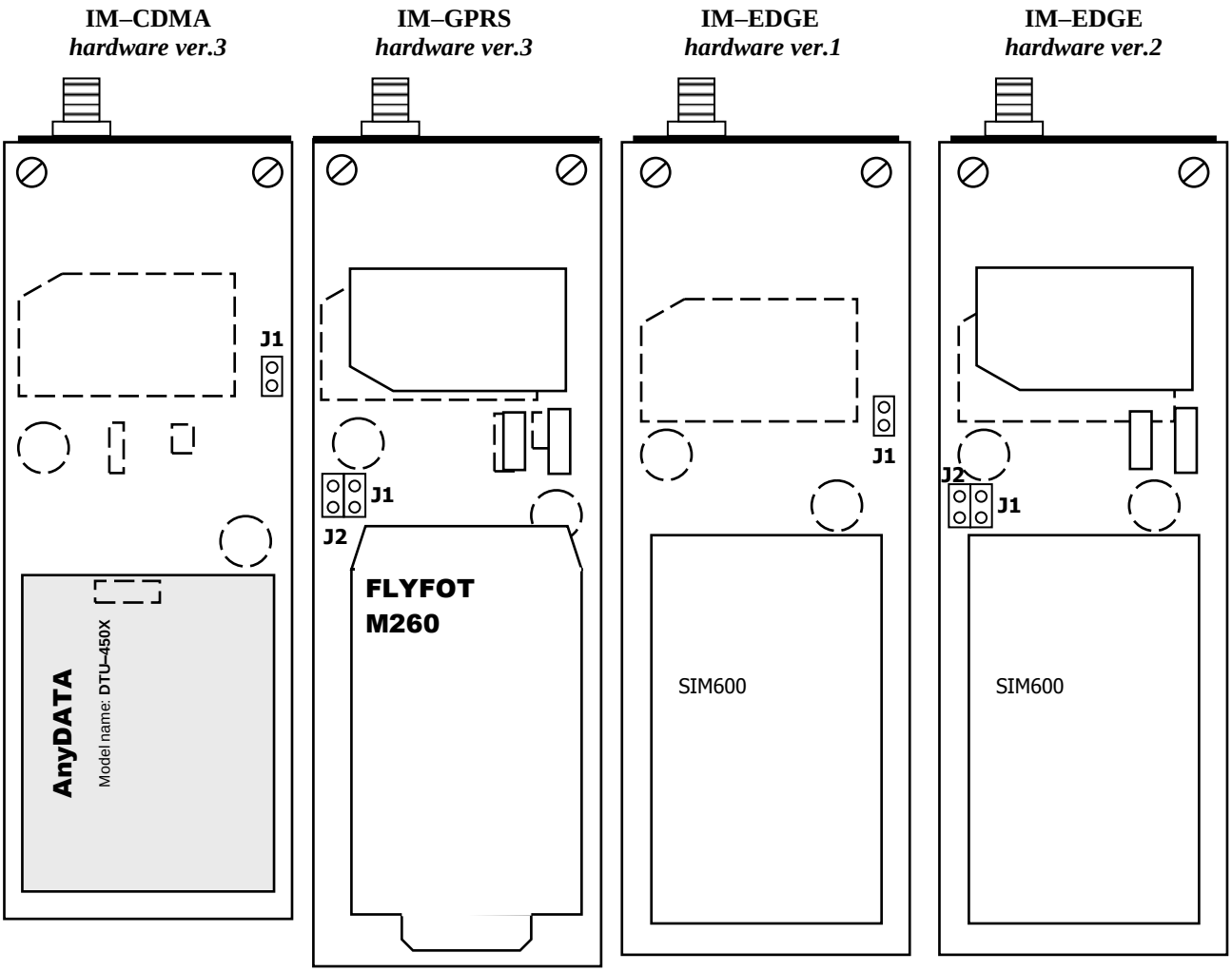


Особенности настройки отдельных типов унаследованных модулей:

— Для модуля IM–GPRS *h/w ver.1* необходимо вручную установить для работы в режиме GPRS: AT+CGCLASS="B"; для работы в режиме CSD — AT+CGCLASS="CG". Данная установка сохраняется в энергонезависимой памяти.

— Для модулей IM–GPRS *h/w ver.2, 3* при работе в режиме CSD, IM–EDGE *h/w ver.1, 2* при работе в режиме отвечающего модема CSD необходимо установить дополнительную опцию PPP: options = "local".

— В модулях IM–EDGE *h/w ver.1, 2* при сбросе конфигурации командой AT&F устанавливается скорость в порту модуля 230400 бит/с.



§2–A.3. AT-команды для разблокировки SIM- и R-UIM карт

Для ручного ввода AT-команд используется режим raw-access, доступный при adm-state="down" или encapsulation="none".

Для всех сотовых модемов 3G/EDGE/GPRS:

+CPIN? Проверка состояния PIN-кода. Основные ответы:

+CPIN: READY	Ввод PIN не требуется (PIN-код отключен на данной SIM-карте, либо уже введен)
+CPIN: SIM PIN	Требуется ввод кода PIN
+CME ERROR nn	Ошибка

+CPIN="nnnn" Ввод PIN-кода. Ответы:

OK	Код правильный
+CME ERROR nn	Ошибка

Отдельные типы модулей допускают ввод как в кавычках, так и без них. Для единообразия, значение PIN рекомендуется всегда вводить как текстовую строку — в кавычках. Это же относится ко всем остальным командам, связанным с PIN-кодом.

+CLCK=<facility>,<mode>[,<password>[,<class>]]

Блокировка SIM-карты или отдельных услуг. Команда доступна только после правильного ввода PIN-кода (или при отключенном PIN-коде). Наиболее актуальны следующие значения:

+CLCK="SC",0,"nnnn"	Отключить запрос PIN-кода
+CLCK="SC",1,"nnnn"	Включить запрос PIN-кода
+CLCK="SC",2	Просмотр текущего статуса блокировки SIM-карты и отдельных услуг.

Команда доступна только после правильного ввода PIN-кода (или при отключенном PIN-коде). В первом и втором случаях третьим аргументом команды должен быть правильный PIN-код. Название услуги "SC" всегда должно вводиться в верхнем регистре, в кавычках.

+CLCK?	Просмотр текущего статуса блокировки SIM-карты и отдельных услуг. Команда доступна только после правильного ввода PIN-кода (или при отключенном PIN-коде). **ВНИМАНИЕ:** Данная команда не поддерживается в модулях IM–EDGE *h/w ver.1* ранних выпусков с версией прошивки N60_V7.4.4_B103 и UIM–EDGE *h/w ver.3*.

Для сотовых модемов EVDO/A *ver.7* (ATEL)

+CPIN?	Проверка состояния PIN-кода. Основные ответы:	
	+CPIN: READY	Ввод PIN не требуется (PIN-код отключен на данной SIM-карте, либо уже введен)
	+CPIN: SIM PIN	Требуется ввод кода PIN
	+CME ERROR nn	Ошибка
+CPIN="nnnn"	Ввод PIN-кода. Ответы:	
	OK	Код правильный
	+CME ERROR nn	Ошибка
+CPINE="nnnn",0	Отключение проверки PIN-кода.	
+CPINE="nnnn",1	Включение проверки PIN-кода.	

Для сотовых модемов CDMA/EVDO *ver.2* и *ver.5* (CMOTech)

$$CHV1?	Запрос статуса модуля R–UIM и PIN-кода. Возможные ответы:	
	$$CHV1: 0,0,0,0	Карта R–UIM отсутствует.
	$$CHV1: 1,1,1,1	Карта R–UIM заблокирована после 3 неправильных попыток ввести код. Для разблокировки карты требуется ввод PUK-кода.
	$$CHV1: 1,0,1,1	Запрос PIN-кода включен, PIN-код еще не введен. Требуется ввести PIN-код.
	$$CHV1: 1,0,1,0	Запрос PIN-кода включен, PIN-код введен верно. Модуль готов к работе.
	$$CHV1: 1,0,0,0	Запрос PIN-кода отключен. Модуль готов к работе.
$$CHV1=<pin-код>	Ввод PIN-кода (без кавычек).	
$$DISCHV1=<pin-код>	Отключение проверки PIN-кода.	
$$ENACHV1=<pin-код>	Включение проверки PIN-кода.	

Для сотовых модемов CDMA *ver.1* и *ver.3* (AnyDATA)

В модуле IM–CDMA *h/w ver.1* (чипсет AnyDATA.NET DTG–450), если на используемой карте R–UIM не отключен запрос PIN-кода, то при первом включении будет выдано диагностическое сообщение:

```
+RUIMPIN, RUIM has locked. Input 4-digit PIN using 'at+rlock=1,xxxx'
```

Для ввода PIN-кода используется команда, указанная выше. Пример неправильного ввода PIN:

```
AT+RLOCK=1,1234
+RLOCK: 1,FAIL,0x9804
```

Пример правильного ввода PIN:

```
AT+RLOCK=1,9876
+RLOCK: 1,PASS,0x9000

+RUIMREADY, PIN verification had finished successfully.
```

Введенный PIN-код запоминается в энергонезависимой памяти модуля. При последующих включениях с той же картой R–UIM он вводится автоматически, при этом выдается сообщение:

```
+RUIMREADY, PIN verification had finished successfully.
```

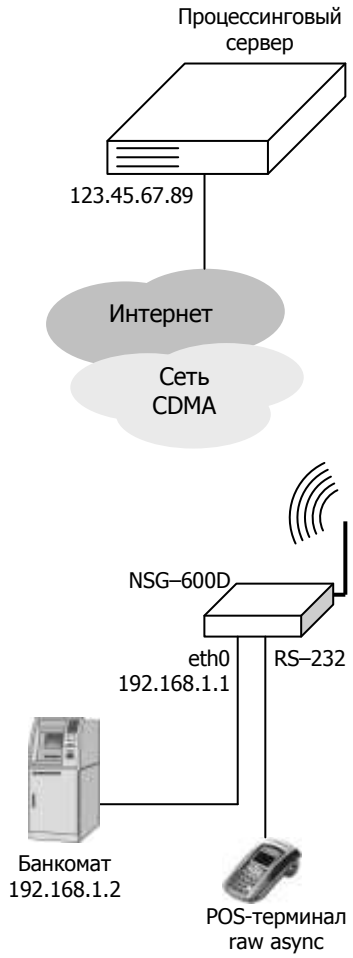
Если запрос PIN-кода отключен, то никакие сообщения не выдаются.

В модуле IM–CDMA *h/w ver.3* (чипсет AnyDATA.NET DTU–450X) диагностические сообщения по сути те же, но менее развёрнутые: +RUIMPIN либо +RUIMREADY. Для ввода PIN-кода используется та же самая команда AT+RLOCK. Однако введённый PIN-код запоминается только на время текущего сеанса; после рестарта модуля он запрашивается снова. Команда для отключения запроса PIN-кода производителем не документирована, хотя, вероятно, имеется. Для отключения запроса следует вставить карту в мобильный телефон CDMA и воспользоваться его меню настроек.

§2–A.4. Примеры конфигурации

Пример 1. Требуется подключить банкомат с портом Ethernet и POS-терминал с портом RS–232 без встроенного протокольного стека к процессинговому серверу TCP/IP через сеть CDMA. Порт терминала работает с типовыми настройками 9600 8n1. Используется устройство NSG–1820MC с опцией opt18xx.CDMA. Запрос PIN-кода на R–UIM карте отключён. Курсивом показаны существенные элементы конфигурации, установленные по умолчанию.

```
ip
: nat
: : POSTROUTING
: : : 1
: : : : out-interface          = "m1"
: : : : target                 = "MASQUERADE"
port
: m1
: : type                       = "cdma"
: : adm-state                  = "up"
: : ppp
: : : main
: : : : chat
: : : : : timeout              = 30
: : : : debug-level            = 1
: : : : default-route          = true
: : : : ipcp
: : : : : accept-address       = true
: : : : : accept-peer-address  = true
: : : : lcp-echo-failure       = 3
: : : : lcp-echo-interval      = 10
: : : : sent-username          = "mobile"
: : : : sent-password          = "internet"
: eth0
: : ifAddress
: : : prefix                   = "192.168.1.1/24"
: : : configurable             = true
: : link
: : : adm-state                = "up"
: rs-232
: : encapsulation              = "raw-tcp"
: : raw-tcp
: : : ip-address               = "123.45.67.89"
: : : tcp-port                 = 9876
```



Примечание. Для упрощённой настройки NAT достаточно выполнить *команду* add-nat/del-nat в узле .port.cdma.ppp .

Пример 2. Требуется подключить офис к Интернет по сети 3G (оператор — Мегафон) и обеспечить автоматическую настройку клиентских компьютеров. Предполагается, что услуга 3G в данной точке доступна и её можно выбрать принудительно, чтобы исключить откат на 2G в случаях временного ухудшения радиосигнала. Используется устройство NSG–700/4AU с модулем UM–3G. Подробно о настройке служб DNS и DHCP см. Часть 4.

```
ip
: nat
: : POSTROUTING
: : : 1
: : : : out-interface       = "s1"
: : : : target              = "MASQUERADE"
port
: s1
: : type                    = "3g"
: : encapsulation           = "ppp"
: : ppp
: : : adm-state             = "up"
: : : main
: : : : chat
: : : : : APN               = "internet"
: : : : : mode              = "UMTS"
: : : : default-route       = true
: : : : ipcp
: : : : : accept-address    = true
: : : : : accept-dns        = true
: : : : : accept-peer-address = true
: : : : sent-password       = "gdata"
: : : : sent-username       = "gdata"
: eth0
: : ifAddress
: : : prefix                = "192.168.1.1/24"
: : : configurable          = true
services
: dhcp
: : eth0
: : : adm-state             = "up"
: : : dns1                  = "192.168.1.1"
: : : gateway               = "192.168.1.1"
: : : ip-address-pool
: : : : from                = "192.168.1.2"
: : : : to                  = "192.168.1.255"
: : : mask                  = "255.255.255.0"
: dns
: : eth0
: : : adm-state             = "up"
```