Мультипротокольные маршрутизаторы NSG

Программное обеспечение NSG Linux

Руководство пользователя

Часть 3

Протоколы канального уровня
Коммутация пакетов

Версия программного обеспечения 1.0 build 3

Обновлено 09.11.2008

Москва 2008

АННОТАЦИЯ

Данный документ содержит руководство по настройке и применению мультипротокольных маршрутизаторов NSG, оснащенных программным обеспечением NSG Linux. Руководства по применению других продуктов NSG, а также базового программного обеспечения NSG для серий NPS–7e, NSG–500, NX–300 и NSG–800 содержатся в отдельных документах.

Документ состоит из следующих разделов:

В третьей части данного документа рассмотрена настройка протоколов канального уровня (Ethernet и VLAN, SLIP, Cisco-HDLC, Frame Relay), организация сеансового доступа средствами протоколов PPP и PAD, доступа к асинхронным портам средствами Telnet и Reverse Telnet, и коммутация пакетов на втором уровне (Ethernet bridging, аппаратный коммутатор Ethernet, постоянные виртуальные соединения Frame Relay и Raw HDLC). Упрощённым случаем протокольной обработки являются порты с прозрачной инкапсуляцией — Telnet и Reverse Telnet. Полностью рассмотрен также стек X.25, включая настройку канального, пакетного уровней и коммутацию пакетов X.25.

Общее описание системы, описание общесистемных параметров и командного языка системы приведены в Части 1. Настройка физических интерфейсов различного типа представлена в Части 2. Настройка IP-маршрутизации и связанных с ней служб, а также механизмов управления IP-трафиком и обеспечения QoS, описана в Части 4. Часть 5 посвящена построению туннелей и виртуальных частных сетей различных типов. В Части 6 изложены начала работы с ОС Linux в объёме, желательном для администрирования и отладки сетей на основе оборудования NSG с использованием расширенных возможностей системы.

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. Кирпичная, д.39, офис 1302
Тел.: (+7–495) 918–32–11
Факс: (+7–495) 918–27–39

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

§ СОДЕРЖАНИЕ §

Часть 3. Протоколы канального уровня. Коммутация пакетов.

§3.1. Архитектура объектов физического и канального уровней

Инкапсуляция и коммутация пакетов на физическом и канальном уровнях устройств NSG–900 осуществляется при помощи портов. В терминах программного обеспечения NSG Linux, *порт* представляет собой комплексный объект, который может включать драйвер физического интерфейса, обработчик протоколов канального уровня и интерфейс сетевого либо прикладного уровня для подключения к IP-маршрутизатору либо определенному приложению, соответственно. Эти компоненты автоматически создаются, связываются друг с другом и согласованно конфигурируются по мере настройки порта — в тех пределах, пока конфигурация определена однозначно и не требует дополнительных указаний от пользователя.

С точки зрения протоколов канального уровня, каждый порт относится к одной из следующих категорий, каждой из которых соответствуют определенные типы физической среды и режим передачи:

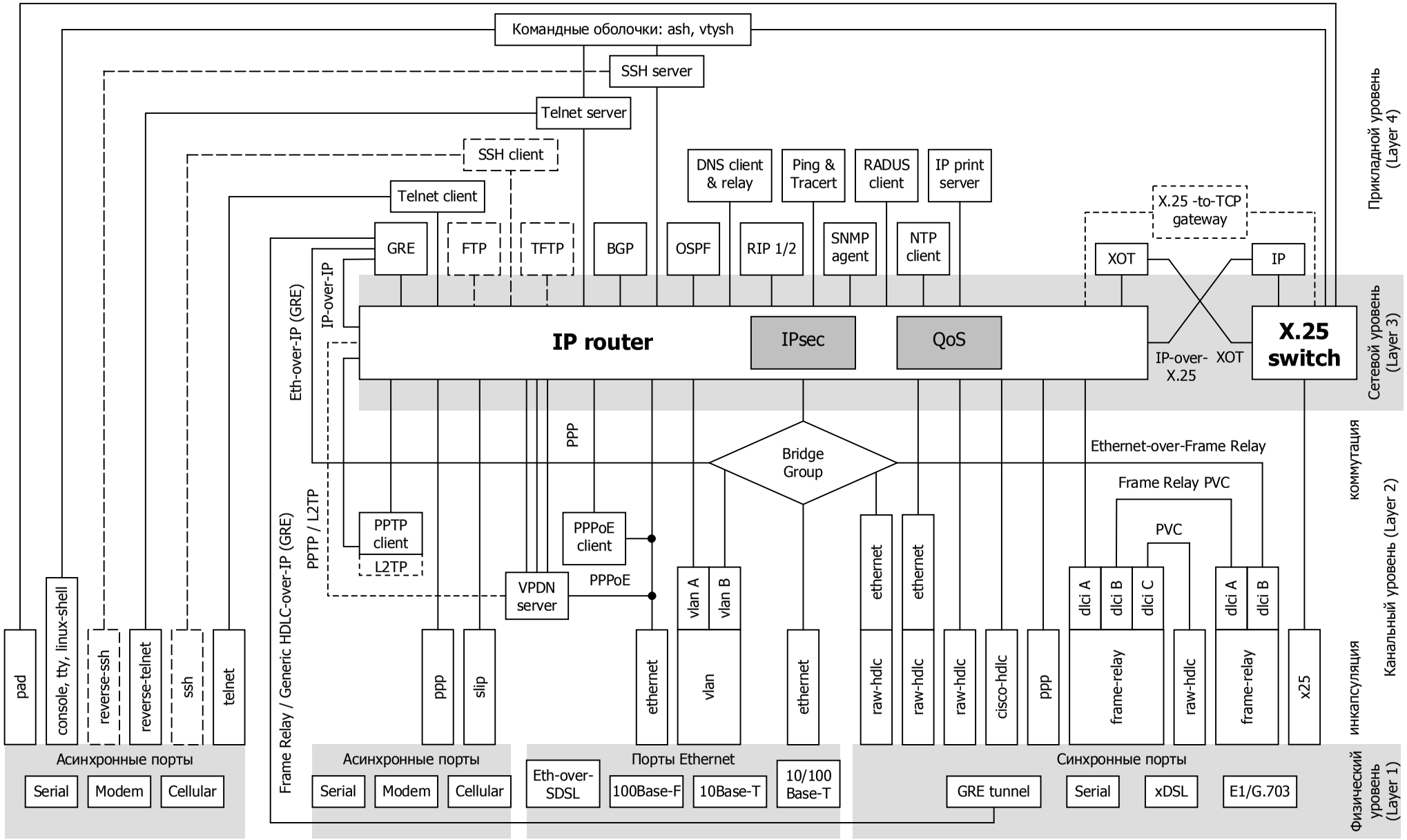
Категория портов	**Протоколы канального уровня** (encapsulation)	**Имена и конфигурация**	**Физические и виртуальные интерфейсы**
Ethernet	ethernet (IEEE 802.3) vlan (IEEE 802.1Q)	eth0	Встроенный Fast Ethernet
		sN при card sN {im-et10 | um-et100}	Сменные Ethernet 10Base–T
Синхронные	cisco-hdlc frame relay ppp x25 raw-hdlc	xN	Группы на многоканальных интерфейсах E1
		tN	Туннели HDLC-over-IP (GRE)
		sN при card sN { im-e1 | im-2e1 }	Группа 1 или режим unframed на одноканальных интерфейсах E1
		sN, кроме указанных исключений	Сменные V.24, V.24/V.35, RS–530, X.21, *x*DSL, G.703, G.703.1
Асинхронные	ppp slip tty — подключение к основной командной оболочке linux-shell — подключение к командной оболочке Linux console — подключение к одной из двух командных оболочек в зависимости от имени пользователя reverse-telnet — подключение к локальному серверу Telnet telnet — подключение посредством клиента Telnet к удаленному серверу pad — PAD для доступа в сеть X.25	aN	Встроенные асинхронные
		sN	Сменные RS–485
		sN при card sN { im-v24 | im-v35 } port sN physical-layer async либо card sN uim-cdma card sN uim-3g	Сменные V.24 и V.24/V.35, сотовые модемы, модемы ТФОП
	one-wire — интерфейс 1-Wire для технологического управления	aN sN при card sN { im-v24 | im-v35 } port sN physical-layer async	Встроенные и сменные асинхронные порты + внешний адаптер 1–Wire
		sN при card sN im-1w	Контроллер 1–Wire
Discrete I/O	нет	sN при card sN im-dio	Контроллер дискретного ввода-вывода
USB	printer — для подключения принтера в режиме печати через сетевой порт TCP/IP	sN при card sN um-usb	Сменный USB

Порты для передачи данных могут иметь следующие системные имена:

eth0 — Встроенный порт Fast Ethernet.

s1, s2, ... — Универсальные порты (разъемы расширения). Доступны только в случае, если в системе имеются разъемы расширения, для которых известен тип установленного интерфейсного модуля. Количество таких имен равно количеству сконфигурированных универсальных портов; порты, для которых тип интерфейсного модуля равен empty, недоступны для дальнейшего конфигурирования. Номера портов соответствуют номерам разъемов расширения, указанным на корпусе.

ПРИМЕЧАНИЕ Набор доступных команд и параметров конфигурации для портов sN зависит от типа установленного физического интерфейса и/или его настроек.



Иерархическая архитектура протоколов в NSG Linux

(компоненты, показанные длинным пунктиром, доступны только средствами командной оболочки Linux, коротким пунктиром — находятся в разработке)

a1, a2, … Встроенные асинхронные порты. Количество таких имен равно количеству обнаруженных в устройстве асинхронных портов. Номера портов соответствуют номерам, указанным на корпусе.

x1, x2, … Виртуальные порты для многоканальных физических интерфейсов E1 (в данной версии не поддерживаются). Каждому порту данного типа соответствует одна группа канальных интервалов (таймслотов) в потоке E1.

t1, t2, … Виртуальные синхронные порты, представляющие собой окончания туннелей HDLC-over-IP (GRE).

Более подробно эти взаимосвязи будут рассмотрены ниже.

ВНИМАНИЕ Категория порта однозначно связана с его символическим именем только для фиксированных портов (Ethernet или асинхронных). Большинство портов в устройствах NSG являются *универсальными*, т.е. представляют собой разъемы расширения, которые оборудуются сменными интерфейсными модулями. Такие порты могут относиться к любой из трех категорий в зависимости от типа и конфигурации интерфейсного модуля.

На вершине иерархической структуры порта находится системный *интерфейс*, через который непосредственно происходит обмен данными с объектами вышестоящего уровня (IP-маршрутизатором, прикладными программами) или с другими портами. В простейшем случае порт представляет собой полностью *одноканальный* объект, т.е. имеет внутри себя только один канал данных, на всех уровнях сетевой иерархии. Примерами таких портов являются синхронные порты с инкапсуляцией PPP, Cisco-HDLC, с прозрачным протоколом (кроме портов с физическими интерфейсами E1), Ethernet, все типы асинхронных портов.

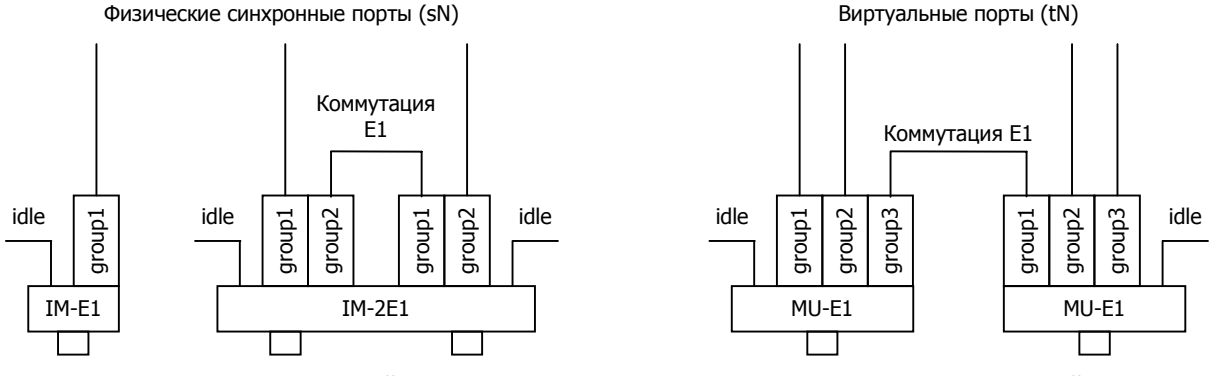
Порты с инкапсуляцией Frame Relay, X.25 и VLAN являются *многоканальными*. Эти протоколы предусматривают эмуляцию нескольких виртуальных сред передачи (каналов или локальных сетей) на канальном уровне. Для каждого из таких портов создаются дочерние объекты — DCLI, логические каналы X.25 или VLAN, соответственно — имеющие уникальные номера в пределах данного порта. Объектам DLCI и VLAN соответствуют свои *суб-порты*, через которые осуществляется обмен данными; сам порт при этом лишь отрабатывает процедуры протокола.

В частности, для обработки пакетов IP необходимо назначить соответствующему порту или суб-порту так называемый *IP-префикс* (совокупность IP-адреса и длины маски, например, 10.0.0.1/8). Интерфейс, которому не присвоен никакой IP-префикс, может:

— участвовать в коммутации на канальном уровне (*Ethernet bridging, Frame Relay switching, raw sync switching*) или коммутации X.25
— использоваться для мультипротокольной инкапсуляции трафика (например, PPP-over-Ethernet)
— автоматически подключаться к одному из прикладных процессов (командная оболочка, Telnet-сервер или клиент)
— использоваться для технологического мониторинга и управления физическими параметрами (Discrete I/O, 1–Wire)

ПРИМЕЧАНИЕ Фактически при назначении IP-префикса происходит создание IP-интерфейса (или суб-интерфейса), который связывает порт (или его дочерний объект) с IP-маршрутизатором. IP-интерфейс относится к третьему (сетевому) уровню протокольной иерархии.

Физические интерфейсы E1, работающие в структурированном (*framed*) режиме G.704, также являются многоканальными, но эта многоканальность реализована на первом уровне сетевой иерархии. Такие интерфейсы выделяют из потока E1 одну или несколько *групп* канальных интервалов (таймслотов) для передачи данных. В зависимости от типа интерфейса E1 (одно- или многоканальный, соответственно), выбранные группы служат в качестве физической среды передачи либо для порта sN, либо для виртуальных портов tN, присоединенных к данному физическому интерфейсу sN. Кроме того, группы могут коммутироваться между собой на физическом уровне, минуя протокольную обработку на канальном и вышестоящих уровнях. Организация групп и их коммутация с портами или друг с другом — дополнительные задачи, которые являются специфическими для настройки интерфейсов E1.



Одноканальные интерфейсы E1 Многоканальные интерфейсы E1

§3.2. Настройка синхронных портов

§3.2.1. Синхронные протоколы

Команды в меню портов, описываемые ниже, определяют параметры протоколов второго и третьего уровней. Эти команды относятся к настройке как физических синхронных портов, так и виртуальных портов, представляющих собой окончания туннелей HDLC-over-GRE. (Подробнее о туннелировании см. Часть 5.)

Общей и ключевой для всех типов синхронных портов является следующая команда:

encapsulation { cisco-hdlc | frame-relay | ppp | x25 | raw-hdlc }
Тип протокола канального уровня.

Первые четыре типа портов не требуют комментариев. Порты с инкапсуляцией raw-hdlc предназначены для прозрачной передачи синхронного трафика, представленного в виде кадров формата HDLC общего вида (к таковым, в частности, относятся кадры Cisco-HDLC, PPP, Frame Relay, X.25). Этот формат подразумевает:

— флаг — 0x7E (01111110 в двоичном представлении);
— контрольная последовательность кадра — ITU–T FCS–16;
— порядок приема/передачи байтов данных — младшим битом вперед;
— прием/передача данных — без побитной инверсии (NRZ).

Длина кадра HDLC не должна превышать 1600 байт (это ограничение обусловлено особенностями реализации устройств NSG).

Такие порты могут коммутироваться (с помощью PVC) друг на друга или на виртуальные каналы Frame Relay, а также использоваться для передачи пакетов IP, Ethernet и IP-over-Ethernet.

Если для порта задана инкапсуляция cisco-hdlc, ppp или raw-hdlc, то в системе появляются суб-интерфейсы с именами вида sN.0. Примеры: s1.0, s2.0, и т.д. Если для порта задана инкапсуляция frame-relay, то при создании каждого виртуального канала (DLC) в системе появляется суб-интерфейс с именами вида sN.<dlci>, где sN — имя физического порта, <dlci> — номер виртуального канала (DLCI). Примеры: s2.16, s2.100, и т.д. Именно эти объекты используются для маршрутизации и коммутации пакетов.

Дальнейшая настройка порта зависит от выбранной инкапсуляции.

§3.2.2. Параметры портов Cisco-HDLC, Sync PPP и Raw HDLC

Порты данных синхронных типов позволяют передавать IP-трафик, т.е. могут служить IP-интерфейсами. Общим для всех IP-интерфейсов является параметр

ip address <ip-префикс> [peer <ip-адрес>] [broadcast <ip-адрес>] [anycast <ip-адрес>]
no ip address <ip-префикс>
Установка и удаление IP-адресов. Обязательным параметром данной команды является IP-префикс (адрес и длина маски, например, 123.134.145.156/24). При необходимости можно отдельно назначить адреса удаленной стороны (peer) в соединении "точка-точка", широковещательной (broadcast) и групповой (anycast) рассылки.

а также группа других параметров, относящихся к протоколу IP. Настройка этих параметров подробно рассмотрена в Части 4.

Порты Cisco-HDLC и Sync PPP предназначены только для передачи IP-трафика. Порт Raw HDLC, как правило, используется для коммутации с другим аналогичным портом или каналом Frame Relay; если он не является IP-интерфейсом, то настройка параметров IP для него не требуется.

ПРИМЕЧАНИЕ В данной версии NSG Linux для порта Sync PPP значение IP-адреса является фиктивным и не используется. В ходе процедуры установления PPP-соединения устройство NSG Linux посылает удаленной стороне пакет IPCP со значением адреса 0.0.0.0. Если на удаленной стороне установлено также устройство NSG Linux, оно соглашается на работу с таким адресом, и процедура идет дальше своим чередом. Однако другие устройства (например, под управлением базового ПО NSG) обычно интерпретируют такой пакет как запрос на присвоение динамического IP-адреса. В этом случае на удаленной стороне необходимо сконфигурировать IP-адрес, который она должна назначать устройству NSG Linux.

cisco-hdlc { keepalive | timeout } <1...100>
Значения параметров протокола Cisco-HDLC. Команда доступна только при инкапсуляции cisco-hdlc.
keepalive — Интервал времени(в секундах), через который будут посылаться пакеты *keepalive*.
timeout — Время ожидания (в секундах). Если за этот период не придет пакет *keepalive*, то интерфейс перейдет в состояние DOWN.

raw-hdlc type { ip | ethernet | loopback }

Только для портов с инкапсуляцией raw-hdlc: инкапсуляция внутри пакетов HDLC.

- ip — Порт может использоваться в качестве IP-интерфейса (т.е. иметь IP-адрес и другие параметры IP), а также коммутироваться с другим аналогичным портом или с виртуальным каналом Frame Relay (см. п.3.6). Значение по умолчанию.
- ethernet — Порт работает в режиме Ethernet-over-HDLC, т.е. кадры Ethernet инкапсулируются в кадры HDLC. Для такого порта в системе создаётся широковещательный интерфейс, как и для физического порта Ethernet.
- loopback — Порт работает в режиме программного шлейфа, т.е. коммутируется сам с собой. В этом режиме он может быть использован только для кольцевого теста, инициируемого удалённой стороной.

В случае инкапсуляции Ethernet-over-HDLC на удалённой стороне линии может быть установлен либо другой маршрутизатор с таким же физическим интерфейсом и аналогичными настройками, либо мост Ethernet-over-HDLC с таким же физическим интерфейсом. Кроме того, порт такого типа может быть включён в состав программного моста Ethernet (см. п.3.5). Данная инкапсуляция не зависит от конкретного типа физической среды передачи и совместима с аналогичными программными и аппаратными продуктами других производителей, в первую очередь, с мостами Ethernet-over-*x*DSL, Ethernet-over-E1 и др.

Если в маршрутизаторе NSG установлен интерфейс WAN с инкапсуляцией Ethernet-over-HDLC, а на другой стороне линии NSG–50 или мост стороннего производителя, то вместе они образуют "удаленный" порт Ethernet. С точки зрения как программных компонент IP-маршрутизатора, так и подключенной локальной сети он выглядит как порт Ethernet.

ПРИМЕЧАНИЕ Протокольную настройку raw-hdlc type ethernet необходимо отличать от фирменной инкапсуляции NSG Ethernet-over-SDSL (см. Часть 2). Последняя реализована на физическом уровне, используется только в модулях NSG IM–SDSL *h/w ver.2* и мосте NSG–50 SDSL, и не совместима ни с какими другими продуктами.

Пример. Настроить порт 1 для работы с внешней синхронизацией, интерфейс V.35, протокол Cisco-HDLC.

```
card s1 im-v35
port s1 ip address 192.168.1.1/24
```

При этом следующие значения будут установлены по умолчанию:

```
adm-state up
physical-layer sync
mode external
baudrate 64000
encapsulation cisco-hdlc
cisco-hdlc keepalive 10
cisco-hdlc timeout 25
ip address 192.168.1.1/24 peer 0.0.0.0 broadcast 0.0.0.0 anycast 0.0.0.0
```

§3.2.3. Параметры портов Frame Relay

Если порту назначена инкапсуляция frame-relay, то в меню порта доступны следующие команды:

frame-relay lmi { none | ansi | ccitt }

Тип управления в протоколе Frame Relay.

frame-relay intf-type { dte | dce }

Логический тип порта Frame Relay:
dte — "user" (по умолчанию)
dce — "network"

frame-relay t391 <0...255>
frame-relay t392 <0...255>
frame-relay n391 <0...255>
frame-relay n392 <0...255>
frame-relay n393 <0...255>

Значения параметров протокола Frame Relay.

frame-relay dlci <16...1022>
no frame-relay dlci <16...1022>

Создание/настройка и удаление виртуального канала (DLC) с указанным идентификатором (DLCI). Первая команда создает канал с указанным номером, если он не существует, и осуществляет вход в меню настройки DLC (см. следующий параграф).

ПРИМЕЧАНИЕ Для специалистов, знакомых с базовым программным обеспечением маршрутизаторов NSG, следует заметить, что используемое в нем понятие *станции Frame Relay* аналогично понятию суб-интерфейса Frame Relay.

§3.2.4. Настройка виртуальных каналов Frame Relay

Для использования виртуального канала Frame Relay необходимо создать его в меню (config-port-sN)# и перейти в подменю (config-dlci-NN)# для его настройки:

```
(config-port-s1)# frame-relay dlci 17
(config-dlci-17)#
```

Номер виртуального канала (DLCI) должен быть уникальным в пределах одного порта. Два DLC, принадлежащие к разным портам, могут иметь одинаковые DLCI. В меню (config-dlci-NN)# доступны следующие основные команды:

description — Административное описание данного DCL — текстовая строка длиной до 255 знаков. Если строка содержит пробелы, ее необходимо заключить в кавычки.

cir <бит/с> — Установка значения параметра CIR.

bc <бит> — Установка значения параметра BC.

be <бит> — Установка значения параметра BE.

ПРИМЕЧАНИЕ Параметры CIR, BC, BE относятся только к исходящему трафику, т.е. к пакетам, отправляемым в линию. Входящий трафик принимается весь, независимо от данных параметров.

route port <имя-порта> <dlci>
route port <имя-порта> no
route port no no

Установить постоянное виртуальное соединение (PVC) для пересылки пакетов из данного DLC в указанный DLC указанного порта Frame Relay, либо в указанный порт с инкапсуляцией RAW (см. п.3.6), либо удалить существующий PVC.

encapsulation { ip | ethernet }

Выбор инкапсуляции трафика внутри виртуального соединения:

- ip — Через DLC передаются непосредственно пакеты IP. На удалённой стороне DLC (через один или несколько промежуточных коммутаторов Frame Relay) должен быть сконфигурирован аналогичный IP-интерфейс с инкапсуляцией во Frame Relay.
- ethernet — DLC эмулирует порт Ethernet, при этом:
  - — IP-пакеты, передаваемые в него из маршрутизатора, предварительно инкапсулируются в кадры Ethernet.
  - — DLC может быть включён в состав программного моста Ethernet на локальном и/или удалённом устройстве (см. п.3.5).

Выбор инкапсуляции IP либо Ethernet относится только к трафику, терминируемому на локальном устройстве NSG. Для пакетов Frame Relay, коммутируемых в другой DLC или в порт raw-hdlc, эта инкапсуляция не имеет значения, поэтому команда route доступна в обоих случаях.

В обоих случаях DLC могут служить IP-интерфейсами. Общим для всех IP-интерфейсов является параметр

ip address <ip-префикс> [peer <ip-адрес>] [broadcast <ip-адрес>] [anycast <ip-адрес>]
no ip address <ip-префикс>

Установка и удаление IP-адресов. Обязательным параметром данной команды является IP-префикс (адрес и длина маски, например, 123.134.145.156/24). При необходимости можно отдельно назначить адреса удаленной стороны (peer) в соединении "точка-точка", широковещательной (broadcast) и групповой (anycast) рассылки.

а также группа других параметров, относящихся к протоколу IP. Настройка этих параметров подробно рассмотрена в Части 4.

Если DLC предполагается использовать только для прозрачной коммутации пакетов Frame Relay, то параметры IP-интерфейса для него не требуются и, как правило, их следует устанавливать равными нулю (за исключением некоторых экзотических случаев).

Особенности реализации протокола Frame Relay в устройствах NSG. Гарантии качества услуг (QoS) для виртуального соединения Frame Relay определяются в терминах следующих пяти параметров:

- CIR — *Committed Information Rate* — согласованная информационная скорость канала (бит/с).
- EIR — *Exceeded Information Rate* — допустимое превышение информационной скорости канала (бит/с).
- T_C — *Commited Rate Measuremet Interval* — период времени, на котором производится регулировка потока трафика.
- BC — *Committed Burst Size* — количество бит, которое может быть передано по логическому каналу за интервал времени T_C.
- BE — *Exceeded Burst Size* — количество бит, на которое может быть превышено значение BC за интервал времени T_C.

Эти параметры связаны друг с другом соотношениями:

$$BC=T_C \times CIR; \qquad BE=T_C \times EIR$$

Таким образом, независимыми из них являются любые три, а оставшиеся два в этом случае определяются однозначно. В устройствах NSG пользователем устанавливаются значения CIR, BC и BE. Параметры T_C (в секундах) и EIR (в битах) вычисляются, если не вдаваться в подробности, по формулам $T_C=BC/CIR$ и $EIR=BE/T_C$.

По данному DLC в каждый интервал T_C передается BC бит и, если канал загружен не полностью, то еще BE бит сверх того. Например:

CIR=256000 BC=128000 BE=128000

Тогда T_C = BC/CIR = 0,5 сек, т.е. в каждые полсекунды будет гарантированно передаваться 128000 бит. Если другие DLC неактивны и физическая скорость на канале достаточно велика, то в эти же полсекунды будет передано еще 128000 бит. Максимальная информационная скорость, таким образом, может достигать 512000 бит/с.

Меньшие значения T_C обеспечивают более равномерный поток трафика, но увеличивают нагрузку на процессор.

ПРИМЕЧАНИЕ Строго говоря, параметры Frame Relay вычисляются в устройствах NSG несколько более сложным образом из-за того, что системный таймер работает с дискретностью 0,01 с. Таким образом, время T_C, вычисленное по вышеприведенной формуле, должно быть округлено до десятков миллисекунд; интервалы менее 10 мс не допускаются. Обозначим эту величину T_C^*. После этого значения BE и BC пересчитываются по следующим формулам:

$$BC^*=T_C^* \times CIR; \qquad BE^*=T_C^* \times EIR$$

Именно эти значения используются при формировании трафика Frame Relay. Как видно, они могут немного отличаться от значений, заданных пользователем. Фактически из пяти параметров DLCI неизменными остаются следующие три: CIR, EIR и $T_C^*=0{,}01 \times round(100 \times BC/CIR)$, а BC и BE подгоняются под эти значения.

Если CIR:0, то T_C принимается равным 1 сек., BC независимо от установки обнуляется (т.е. не гарантируется никакая передача), а возможное количество передаваемых бит в секунду (при отсутствии нагрузки по другим DLC) определяется параметром BE.

ВНИМАНИЕ Если установить CIR:0 BC:x BE:0, то информация вообще передаваться не будет!

Все вышеописанные параметры относятся только к формированию исходящего трафика. Ограничение входящего трафика (полисинг) в сетях Frame Relay не предусмотрено. Для того, что, чтобы регулировать поток трафика в обратном направлении, необходимо соответствующим образом настроить параметры DLCI на другой стороне соединения. В частности, стандарты Frame Relay допускают создание несимметричных DLCI, т.е. скорости передачи и параметры качества услуги в противоположных направлениях могут быть различными.

Пример. Настроить порт 2 для работы с модулем SDSL, скорость 2048000 бит/с, протокол Frame Relay, LMI CCITT. Два DLC с номерами 16 и 17 делят общую полосу пропускания пополам.

```
port s2
    physical sdsl
    mode master
    baudrate 2048000
    encapsulation frame-relay
    frame-relay lmi ccitt
    frame-relay dlci 16
        ip address 12.0.0.1/8
        cir 1024000
        bc 1024000
        bc 1024000
        exit
    frame-relay dlci 17
        ip address 12.0.1.1/8
        cir 1024000
        bc 1024000
        bc 1024000
        exit
    exit
```

§3.2.5. Общие параметры портов X.25

Для синхронного порта с инкапсуляцией X.25 доступны следующие специфические команды:

lapb ... Настройка параметров канального уровня.

x25 ... Настройка параметров пакетного уровня.

connections Вывод номеров логических каналов, адресов источника и назначения, и текущего состояния соединений. Это разовая команда, не записываемая в конфигурацию.

§3.2.6. Параметры канального уровня X.25

Настройка параметров канального уровня (Layer 2) X.25 производится в подменю (config-lapb)# для выбранного физического порта. Подменю содержит следующие команды:

mode { dte | dce }

Логический тип порта (на канальном уровне). Для двух портов, соединенных друг с другом, должны быть установлены противоположные типы — один DTE, другой DCE.
Значение по умолчанию — dte.

Следует отметить, что логический тип порта, в общем случае, никак не связан с его аппаратным типом. Кроме того, логический тип для канального и пакетного уровней устанавливается в NSG Linux раздельно (в отличие от базового программного обеспечения NSG, где параметр TE относится одновременно к обоим уровням). Однако на практике такие сложные конфигурации требуются нечасто, в большинстве случаев логический тип обоих уровней совпадает с аппаратным типом.

modulo { 8 | 128 }

Формат поля номера пакета в заголовке канального уровня:
- 8 длина поля 3 бита, т.е. пакеты могут нумероваться от 0 до 7 (значение по умолчанию)
- 128 длина поля 7 бит, т.е. пакеты могут нумероваться от 0 до 127

k <1 ... modulo-1>

Размер окна канального уровня, т.е. максимальное число пакетов, которые могут быть переданы, не дожидаясь подтверждения о приеме предыдущего пакета. Минимальное значение 1 означает, что порт должен ждать подтверждения для каждого пакета, прежде чем отправить следующий пакет. Максимальное значение равно количеству неповторяющихся номеров кадров, которые возможны при данном значении параметра modulo: 7 либо 127, соответственно.
По умолчанию устанавливается максимальное значение.
Аналогом данного параметра в базовом ПО NSG для устройств младших серий является FW.

t1 <1...64>

Время ожидания подтверждения от удаленной стороны, в секундах. Если подтверждение не получено, пакет посылается повторно. Значение по умолчанию — 3 сек. Аналог в базовом ПО NSG — параметр T1.

t2 <1...32>

Время, в течение которого должно быть отправлено подтверждение на принятый пакет. Значение по умолчанию — 2 сек. В базовом ПО NSG аналогичный параметр не настраивается, а де-факто время ответа автоматически минимизируется: если в выходной очереди есть данные на передачу, то ответ посылается в первом же пакете данных, если нет — немедленно.

n2 <1...255>

Максимальное число повторных попыток передачи пакета, если за время t1 не получено подтверждение о приеме. Значение по умолчанию — 9. Аналог в базовом ПО NSG — параметр N2.

§3.2.7. Параметры пакетного уровня X.25

Настройка параметров пакетного уровня (Layer 3) X.25 производится в подменю (config-x25)# для выбранного физического порта. Подменю содержит следующие команды:

mode { dte | dce }
: Логический тип порта (на пакетном уровне). Для двух портов, соединенных друг с другом, должны быть установлены противоположные типы — один DTE, другой DCE.
Значение по умолчанию — dte.

Следует отметить, что логический тип порта, в общем случае, никак не связан с его аппаратным типом. Кроме того, логический тип для канального и пакетного уровней устанавливается в NSG Linux раздельно (в отличие от базового программного обеспечения NSG, где параметр TE относится одновременно к обоим уровням). Однако на практике такие сложные конфигурации требуются нечасто, в большинстве случаев логический тип обоих уровней совпадает с аппаратным типом.

Значение по умолчанию для обоих параметров — 128 байт. В базовом ПО NSG размер пакета в обоих направлениях устанавливается одним параметром LG.

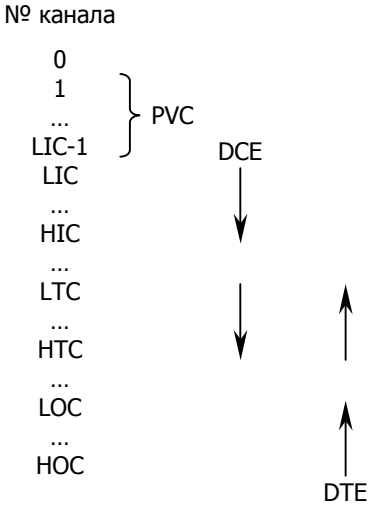
Следующая группа параметров позволяет регулировать распределение номеров логических каналов:

lic <1...4095>
hic <1...4095>
: Диапазон номеров логических каналов, которые могут использоваться только устройством DCE (*lowest/highest incoming channel*).

ltc <1...4095>
htc <1...4095>
: Диапазон номеров логических каналов, которые могут использоваться как устройством DCE, так и устройством DTE (*lowest/highest two-way channel*).

loc <1...4095>
hoc <1...4095>
: Диапазон номеров логических каналов, которые могут использоваться только устройством DTE (*lowest/highest outgoing channel*).

Понятия *incoming* и *outgoing* здесь используются применительно к устройству DTE. Выбор номера канала при установлении логического соединения происходит следующим образом (см. рисунок):



— Нулевой логический канал в большинстве реализаций X.25 не используется.

— Диапазон номеров от 1 до LIC-1 зарезервирован для PVC (в данной реализации NSG Linux не поддерживаются).

— Если соединение устанавливается по инициативе устройства DCE, оно ищет свободный канал с наименьшим номером, двигаясь последовательно в порядке возрастания номеров от LIC к HIC и затем от LTC к HTC.

— Если соединение устанавливается по инициативе устройства DTE, оно ищет свободный канал с наибольшим номером, двигаясь последовательно в порядке убывания номеров от HOC к LOC и затем от HTC к LTC.

Распределение номеров должно быть задано одинаковым образом на обеих сторонах соединения. При этом выполнение условий LTC=HIC+1 и LOC=HTC+1, вообще говоря, не требуется, т.е. между диапазонами могут быть пропущенные номера, не используемые ни в каком случае.

Такой алгоритм позволяет избежать ситуации, когда оба устройства DCE и DTE одновременно пытаются установить соединение по одному и тому же логическому каналу (за исключением случая, когда этот канал — последний свободный). Наличие раздельных диапазонов для входящих и исходящих соединений оставляет каждому из устройств некоторый запас логических каналов, находящихся в его монопольном распоряжении. Это гарантирует, что каждое из устройств будет в состоянии инициировать соединение даже в том случае, если все каналы, выделенные для двусторонних соединений, заняты по инициативе удаленной стороны.

По умолчанию lic=hic=loc=hoc=0, ltc=1, htc=1024, т.е. зарезервированные диапазоны отсутствуют, а каналы с номерами от 1 до 1024 могут использоваться для установления SVC по инициативе любой из сторон. Подобная же упрощенная схема используется в базовом ПО NSG, с той разницей, что параметр, определяющий верхнюю границу диапазона номеров, именуется LC; номера каналов при установлении PVC задаются явным образом и автоматически исключаются из рассмотрения при установлении SVC.

modulo { 8 | 128 }
Формат поля номера пакета в заголовке пакетного уровня:
8 длина поля 3 бита, т.е. пакеты могут нумероваться от 0 до 7 (значение по умолчанию)
128 длина поля 7 бит, т.е. пакеты могут нумероваться от 0 до 127

win <1 ... modulo-1>
Размер окна пакетного уровня для входящих соединений. Данный размер используется по умолчанию, если иное не указано в пакете CALL.

wout <1 ... modulo-1>
Размер окна пакетного уровня для исходящих соединений.

Максимальное значение обоих параметров win и wout равно количеству неповторяющихся номеров кадров, которые возможны при данном значении параметра modulo: 7 либо 127, соответственно. По умолчанию оба параметра имеют значение 2. В базовом ПО NSG вместо двух этих параметров используется один параметр PW.

Максимальный размер пакета (точнее, поля данных пакетного уровня) также устанавливается отдельно для входящих и исходящих пакетов:

x25 ips { 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4098 }
Максимальный размер входящих (*incoming*) пакетов, в байтах.

x25 ops { 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4098 }
Максимальный размер исходящих (*outgoing*) пакетов, в байтах.

Последние четыре параметра относятся к порту, работающему в режиме Layer 3 DTE, и определяют максимальное время ожидания подтверждения (в секундах) для различных типов пакетов. Если за указанное время подтверждение от удаленной стороны не получено, производится повторная передача. Названия таймаутов приведены в соответствии с терминологией стандарта X.21:

t20 <1...1000>
DTE Restart Request retransmission timer. Значение по умолчанию — 180 сек.

t21 <1...1000>
DTE Call Request retransmission timer. Значение по умолчанию — 200 сек.

t22 <1...1000>
DTE Reset Request retransmission timer. Значение по умолчанию — 180 сек.

t23 <1...1000>
DTE Clear Request retransmission timer. Значение по умолчанию — 180 сек.

В базовом ПО NSG аналогом параметра t21 является T2, остальные таймауты не настраиваются.

§3.3. Настройка асинхронных портов

§3.3.1. Асинхронные протоколы

Протокол, используемый асинхронным портом, устанавливается следующей командой в меню порта:

encapsulation { ppp | slip | tty | linux-shell | reverse-telnet | telnet | console | pad | sms-handler | one-wire | unused }

Тип протокола канального уровня:

ppp — протокол PPP
slip — протокол SLIP
tty — вход в основную командную оболочку (vtysh)
linux-shell — вход в командную оболочку ОС Linux (ash)
telnet — прозрачное подключение к серверу Telnet
reverse-telnet — прозрачное подключение удаленного клиента Telnet к данному порту
console — специальный тип для разделяемого консольного порта в отдельных типах шасси
pad — сборщик-разборщик пакетов (PAD) X.3/X.28/X.29
sms-handler — обработчик команд SMS-управления (монопольно, или совместно с PPP)
one-wire — интерфейс технологического управления, никакие протоколы высших уровней не предусмотрены.
unused — формальное значение, используемое по умолчанию.

Порты TTY, Linux-Shell и Console не имеют дополнительных параметров. Дальнейшая настройка портов остальных типов зависит от выбранной инкапсуляции.

§3.3.2. Параметры портов PAD

При выборе инкапсуляции PAD в меню порта имеется следующий дополнительный параметр:

pad — Вход в узел меню, позволяющий определить группу специфических параметров для этого протокола.

Дополнительный узел меню pad содержит следующие команды:

dtr-control <0 ... 60>

Управление сигналом DTR интерфейса RS–232 при разрыве сетевого соединения: сигнал опускается на указанное число секунд (по умолчанию — 2 сек.), затем поднимается снова. Это позволяет разорвать физическое соединение, реинициализировать модем и т.п. Если установлено значение 0, то сигнал DTR поднят постоянно.

prompt <строка>

Строка приглашения, которая будет выводиться подключённому пользователю при работе в командном режиме PAD. Значение по умолчанию — звёздочка (*).

local-x121-address <X.121 адрес>

X.121 адрес, который будет подставляться в пакеты CALL, отправляемые с данного порта, в качестве вызывающего адреса (Calling Address). Адрес может содержать до 15 десятичных цифр. Если адрес не установлен (в качестве значения при этом выводится $), то вызывающий адрес в пакетах CALL отсутствует.

remote-x121-address <X.121 адрес>

X.121 адрес, который будет использоваться для автоматического установления соединения по поднятию сигнала DCD (в текущей версии не реализовано) или при инициализации порта, если DCD в этот момент уже поднят. Данный адрес будет подставляться в пакеты CALL, отправляемые с данного порта, в качестве вызываемого адреса (Called Address). Адрес может содержать до 15 десятичных цифр.
Если адрес не установлен (в качестве значения при этом выводится $), то никакое соединение автоматически не устанавливается.

packet-size { 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 }

Максимальная длина собираемого пакета (в байтах). Это один из критериев, по которым может производиться отправка пакета. Значение по умолчанию — 128.

window <1 ... 7>

Размер окна пакетного уровня для соединений, устанавливаемых с данного порта. Передаётся в поле Facilities пакета CALL. Значение по умолчанию — 2.

par-<номер> <значение>

Параметры профиля PAD. В данной версии NSG Linux поддерживаются следующие параметры:

Параметры согласно ITU–T X.3		Значение для профилей	
Номер	**Назначение**	**прозрачный**	**построчный**
1	Сигнал ВНИМАНИЕ (Recall character)	0	1
2	ЭХО (Echo)	0	1
3	Сигнал отправки пакета (Forwarding characters)	0	2
4	Тайм-аут отправки пакета (Idle timer delay)	0	0
5	Подчиненное устройство (Ancillary Device Control)	0	0
12	Управление потоком (Flow Control)	0	1
13	Вставка символа перевода строки (Linefeed Insertion)	0	6

По умолчанию установлен прозрачный профиль.

timeout <1 ... 2147483647 >

Максимальное время неактивности, по истечении которого соединение X.25 разрывается. Данный параметр является единым для командного режима и режима данных, на приём и на передачу. Значение по умолчанию — 300 сек.

При подключении к порту типа PAD выводится приглашение PAD, после чего можно ввести адрес X.121 и установить коммутируемое логическое соединение с удалённым узлом сети. (При условии, что в устройстве определён маршрут к вызываемому узлу, см. п.3.7.) Если удалённый хост назначает при этом определённый профиль PAD (например, прозрачный), этот профиль будет принят и установлен на порту устройства NSG.

ПРИМЕЧАНИЕ Реализация PAD в данной версии NSG Linux является ограниченной. Пользователь может ввести вызываемый адрес (без фасилит) и установить соединение к удалённому хосту X.25. Другие возможности PAD планируется реализовать по мере потребности в них.

§3.3.3. Параметры портов Telnet

При выборе инкапсуляции Telnet в меню порта имеются следующие дополнительные параметры:

remote-address <ip-адрес>

IP-адрес удаленного сервера Telnet, к которому автоматически устанавливается соединение. Если адрес не указан (установлен в 0.0.0.0), то при подключении к данному порту пользователь попадает в командный режим клиента Telnet и устанавливает соединение вручную при помощи команды open.

remote-port <tcp-порт>

Номер порта TCP удаленного сервера Telnet, к которому автоматически устанавливается соединение. По умолчанию устанавливается порт 10023.

transparent { yes | no }

Включение/выключение прозрачного режима Telnet. В непрозрачном режиме клиент перехватывает и обрабатывает escape-последовательности, в прозрачном — пропускает все символы без изменения. По умолчанию устанавливается непрозрачный режим.

§3.3.4. Параметры портов Reverse Telnet

При выборе инкапсуляции Reverse Telnet в меню порта имеются следующие дополнительные параметры:

reverse-telnet

Вход в узел меню, позволяющий определить группу специфических параметров для этого протокола.

Дополнительный узел меню reverse-telnet содержит следующие команды:

tcp-port <номер>

Номер порта TCP, по которому осуществляется доступ удаленного клиента Telnet к данному физическому порту. Рекомендуется использовать номера портов TCP старше 3000 во избежание конфликтов с портами стандартных служб и протоколов.

authentication { local | tac_plus | no }

Использовать аутентификацию. Если аутентификация включена, то при обращении к данному порту TCP пользователь должен будет ввести имя и пароль, прежде чем получит доступ в физический порт. В данной версии NSG Linux аутентификация может производиться по локальному списку, который составляется командой users, либо с помощью удалённых серверов TACACS+. Подробно о локальном списке пользователей см. §3.8.1, о клиенте TACACS+ — §3.8.4.

group-name <имя>

Установить группу пользователей, которые будут иметь доступ к данному порту. Данный параметр имеет смысл только при включённой аутентификации. Если аутентифицированный пользователь не является членом указанной группы, его обращение будет отвергнуто.
Если указанная группа не существует, то доступ к данному порту запрещён для всех пользователей.
Для удаления привязки к группе следует ввести пустое имя группы: group-name "" (либо назначить новую группу).
Если аутентификация включена, но группа не указана, то доступ к данному порту разрешён для всех аутентифицированных пользователей.

escape-break <символ>
escape-terminate <символ>
escape-char <символ>

Установить спецсимволы, которые будут использоваться в ходе сеанса Telnet с данным физическим портом для посылки специального сигнала BREAK, для завершения сеанса и в качестве ESCAPE-символа, соответственно. В качестве спец-символа может использоваться любой печатаемый символ, либо спецсимволы CTRL–@, CTRL–A, CTRL–B, ... CTRL–Z, ... <CTRL–_, которые вводятся в данной команде парами символов из следующего набора:

^@ ^A ... ^Z ^[^/ ^] ^^ ^_

По умолчанию, в качестве ESCAPE-символа установлена тильда (~), символы для посылки BREAK и TERMINATE не установлены.

Символы escape-break и escape-terminate используются сами по себе. После символа, определённого как escape-char, может быть введён один из следующих символов для непосредственного управления физическим интерфейсом:

.	Завершить Telnet-соединение.
,	Опустить сигнал DTR на 2 сек., чтобы принудить подключённый модем разорвать соединение.
#	Послать сигнал BREAK.
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.

§3.3.5. Параметры портов SLIP

При выборе инкапсуляции PPP в меню порта имеются следующие дополнительные параметры:

virtual-template <1...25>

Номер шаблона IP-интерфейса. Шаблон содержит совокупность параметров, относящихся к работе протокола IP, аутентификации по PAP/CHAP и т.п. Если номер равен 0, все параметры устанавливаются по умолчанию. Подробно об использовании шаблонов см. п.3.3.11.

При создании IP-интерфейса с инкапсуляцией SLIP воспринимаются только следующие параметры, описанные в шаблоне virtual-template:

ip address
peer ip address
ip mtu
keepalive

Остальные параметры, входящие в состав шаблона, относятся только к интерфейсу PPP и в данном случае игнорируются.

Особо следует остановиться на параметре keepalive, поскольку в самом протоколе SLIP механизм посылки контрольных пакетов не предусмотрен. Вместо него используется так называемый механизм *outfill* (термин из SLIP в Linux). В случае отсутствия входящего трафика через заданный интервал времени посылается пакет-пустышка (байт 0xC0), который воспринимается удаленной стороной как подтверждение работоспособности. Если в течение времени 3×keepalive не принят ни один пакет, SLIP-соединение разрывается, физические сигналы порта (DTR, RTS) опускаются, и через 1 сек. порт рестартует и пытается установить соединение заново.

§3.3.6. Параметры портов PPP

При выборе инкапсуляции PPP в меню порта имеются следующие дополнительные параметры:

virtual-template <1...25> [aux <1...25>]

Номер шаблона IP-интерфейса. Шаблон содержит совокупность параметров, относящихся к работе протокола IP, аутентификации по PAP/CHAP и т.п. Если номер равен 0, все параметры устанавливаются по умолчанию. Подробно об использовании шаблонов см. п.3.3.11.
Опционально: если используется модуль GPRS или 3G с двумя SIM-картами, то после необязательного ключевого слова aux указывается номер шаблона для резервного оператора.

chat-script <имя> [aux <имя>]

Только при использовании инкапсуляции ppp: имя сценария, который будет использован для установки физического соединения. Имя может вводиться в кавычках или без них. Пустая строка ("") означает, что для данного интерфейса никакой сценарий не используется.
Опционально: если используется модуль GPRS или 3G с двумя SIM-картами, то после необязательного ключевого слова aux указывается имя сценария для резервного оператора.

ПРИМЕЧАНИЕ Если в шаблоне для данного виртуального интерфейса указан режим установления соединения по требованию (ppp connection on-demand), то для нормальной работы интерфейса необходимо указать какой-либо сценарий, хотя бы пустой:

```
chat-script DUMMY "'' ''"
```

(Первая пара апострофов означает "ничего не ждать", вторая — "ничего не посылать"; все тело сценария взято в двойные кавычки.)

chat-log { previous | current }

Только при использовании инкапсуляции ppp: просмотр журнала выполнения сценария физического соединения. Ключевое слово previuos выводит журнал последней завершенной попытки, current — текущей попытки. Во втором случае, повторяя ввод команды, можно проследить ход работы сценария по мере его выполнения.

ppp-log { previous | current }

Только при использовании инкапсуляции ppp: просмотр журнала сеанса PPP. Ключевое слово previuos выводит журнал последней завершенной попытки, current — текущей попытки. Во втором случае, повторяя ввод команды, можно проследить ход сеанса по мере его выполнения.

prio main <0...10> [aux <0...10>]

При использовании модуля GPRS или 3G с двумя SIM-картами: максимальное число попыток соединения с основным и с резервным оператором, соответственно. После исчерпания этого числа интерфейс переключается на другую SIM-карту. Подробнее о работе с 2 SIM-картами см. п.3.3.7.
Значения по умолчанию — prio main 1 aux 0, т.е. резервное соединение не используется.

§3.3.7. Особенности использования сотовых модемных модулей с двумя SIM-картами

Модули IM–GPRS *h/w ver.3*, UIM–3G оснащены двумя гнёздами для SIM-карт и позволяют динамически переключаться между двумя сотовыми операторами. Основной считается SIM-карта, установленная в в гнездо на верхней стороне модуля. Режим работы (с обеими картами или только с основной) устанавливается аппаратно при помощи перемычки на модуле.

Если перемычка установлена в режим работы с двумя SIM-картами, то для этого режима требуются следующие специфические программные настройки:

— Два шаблона виртуальных интерфейсов и два сценария соединения (для основного и резервного операторов, соответственно).
— В меню асинхронного порта параметры chat-script и virtual-template содержат ключевое слово aux и указание на сценарий и шаблон для резервного оператора, соответственно.
— В меню этого же порта используется параметр prio, определяющий, в некотором смысле, "относительные веса" основного и резервного операторов. Значение 0 указывает, что данный оператор не используется никогда.

Переключение SIM-карты на модуле, сценария физического соединения и протокольных параметров сеанса PPP производится синхронно. При изменении *virtual-template* или любого из параметров в меню порта интерфейс рестартует немедленно и безусловно.

Если для порта указано prio main M aux N, то в данной бета-версии интерфейс всегда делает M попыток соединиться с основным оператором, затем N попыток с резервным, затем цикл начинается снова. В частности, если услуга одного оператора недоступна (по любой причине), то интерфейс быстро исчерпает разрешенное число попыток и переключится на альтернативного оператора. В последующих версиях планируется реализовать более интеллектуальный алгоритм переключения с раздельным подсчётом успешных и неудачных попыток.

Набор параметров (MAIN/AUX), используемый в текущей попытке, и число оставшихся попыток для этого оператора можно просмотреть при помощи команды show в меню порта.

§3.3.8. Особенности использования проводных и сотовых модемных модулей

Интерфейсные модули IM–V34 и IM–V92 — аналоговые модемы тональной частоты, предназначенные для передачи данных по коммутируемым телефонным линиям.

Модули IM–GPRS и IM–EDGE предназначены для подключения к сотовым сетям GSM/GPRS/EDGE, при этом они могут работать как в режиме канальной передачи данных (*Channel Separated Data*, CSD), так и в пакетных режимах GPRS (*General Radio Packet Service*) и EDGE (*Enhanced Data rates for Global Evolution*).

Модуль UIM–3G предназначен для подключения к сотовым сетям UMTS третьего поколения и поддерживает высокоскоростной пакетный режим HSDPA (*High-Speed Downlink Packet Access*), а также технологии 2 и 2+ поколений GSM, GPRS, EDGE.

Модули IM–CDMA, UIM–CDMA и UIM–EVDO предназначены для подключения к сотовым сетям CDMA 2000 1x/EV-DO (CDMA Evolution, Data Only).

Особенности работы данных модулей на физическом уровне подробно рассмотрены в Части 2. Применительно к выбору протокола второго уровня, имеются следующие зависимости от используемого модуля и режима подключения:

— В канальном режиме (CSD) сети GSM и при проводном соединении устанавливается соединение физического уровня между двумя модемами. Поверх этого соединения может работать любой асинхронный протокол (ppp, slip, reverse-telnet, telnet и др.), однако следует заметить, что из всего этого списка только протокол PPP обеспечивает достаточно развитые механизмы для управления установлением и разрывом соединения.

— В пакетном режиме всех сотовых сетей устанавливается соединение на 1–3 уровнях протокольного стека между абонентским терминалом (модемом) и сетью оператора, которая одновременно является и физической средой передачи, и поставщиком сетевых услуг. Соединение осуществляется по тому протоколу, который предлагается сетью. В реальности это исключительно IP-over-PPP (другие протоколы, предусмотренные стандартами, на практике не поддерживаются). Поэтому для всех пакетных режимов единственная допустимая инкапсуляция — ppp.

Для непосредственного доступа к модему и управления им при помощи AT-команд (снятия PIN-кода, проверки работоспособности, проверки доступности сети, установления пробного соединения и т.п.) следует, как правило, назначить порту инкапсуляцию Reverse Telnet, например (шасси NSG–700/4AU):

```
!
nsg
    card s2 uim-cdma
    port s2
        encapsulation reverse-telnet
        reverse-telnet
            tcp-port 8023
            exit
    exit port eth0 ip address 192.168.0.1/24
    exit
!
```

В этом случае, установив со своего компьютера Telnet-соединение

```
telnet 192.168.0.1 8023
```

пользователь оказывается прозрачно подключён к модему и может вводить AT-команды.

Чтобы гарантировать восстановление работоспособности модуля из любого состояния, рекомендуется установить перемычку аппаратного рестарта по падению сигнала DTR порта. Однако в этом случае после рестарта модулю требуется некоторое время для загрузки внутреннего программного обеспечения и регистрации в сети. В течение этого времени модуль может быть не готов обрабатывать AT-команды, поэтому необходима принудительная задержка в начале сценария. Задержка легко реализуется следующим образом:

```
chat-script DIALUP "TIMEOUT n XXX-\rAT-OK AT TIMEOUT 45 OK ..."
```

При исполнении сценария PPP-интерфейс сначала ждет строку XXX в течение n секунд, затем, не получив ее, посылает пустую строку, затем AT и получает OK. Посылка пустой строки здесь рекомендуется для того, чтобы дополнительно очистить буфер, в котором могли остаться какие-то символы от предыдущего сеанса. (Иногда наблюдается на некоторых типах сотовых модулей.) Следующая пара AT OK восстанавливает таймаут по умолчанию — 45 сек (можно вместо этого вставить TIMEOUT 45 непосредственно перед следующим ожидаемым ответом).

Рекомендуемая задержка для модулей IM–V34, IM–V92 — 3 сек. Для сотовых модулей задержка варьируется в пределах от 10 до 25 сек и подбирается экспериментально в зависимости от типа модуля и конкретной сети.

Подробное описание настройки сотовых модулей приведено в документах NSG:

Использование модулей GSM/GPRS, EDGE и 3G в сетевом оборудовании NSG
Управление модулями UIM–CDMA и UIM–EVDO с помощью AT-команд

§3.3.9. Особенности использования консольного порта в устройствах NSG–700

Консольный порт устройств NSG–700 может также использоваться для передачи данных наравне с другими асинхронными портами. Для работы в режиме консольного ему назначается специальный тип протокола encapsulation console, предусмотренный только для данного порта. Никакие настройки, производимые средствами основного программного обеспечения, в этом режиме не действуют. Интерфейс всегда работает с аппаратным управлением потоком, в формате 8N1, скорость устанавливается в загрузчике U-Boot переменной окружения baudrate.

В заводской конфигурации порт настроен как консольный. Изменить тип console на любой другой протокол, доступный для асинхронного порта, возможно только при управлении устройством по сети (посредством Telnet, SSH или X.25).

Если порт используется для передачи данных, то установить ему режим console можно в любое время. По этой причине не рекомендуется использовать его для подключения к вышестоящей сети, чтобы избежать ошибок, приводящих к потере удаленного управления устройством.

ПРИМЕЧАНИЕ В процессе загрузки программного обеспечения данный порт функционирует как консольный, в частности, выводит сообщения и приглашения U-Boot. Может возникнуть ситуация, когда подключенное оборудование (например, консоль другого сетевого устройства) пытается интерпретировать эти сообщения как команды, отвечает на них (например, ERROR), устройство NSG–700 также воспринимает эти ответы как команды U–Boot, и т.п. В результате устройство бесконечно перезагружается или впадает в иное неработоспособное состояние.
Для устранения подобной ситуации необходимо использовать загрузчик U-Boot версии *NSG build 2* или старше с установленной переменной окружения silent=yes.

§3.3.10. Сценарии соединения для асинхронных портов

Сценарии соединения предназначены для инициализации оборудования, подключенного к асинхронным портам устройства NSG, и установления соединений на физическом уровне. В данной версии NSG Linux сценарии используются только для асинхронных портов с инкапсуляцией ppp. Для управления сценариями используются следующие команды в меню (config-nsg)#:

chat-script <имя> "<строка сценария>"
no chat-script <имя>

Создание/изменение и удаление сценария. Имя сценария представляет собой текстовый идентификатор, по которому асинхронный порт может ссылаться на данный сценарий (параметр chat-script в конфигурации порта). Остальная часть команды рассматривается как единая строка, являющаяся собственно сценарием. Максимальная длина сценария — 255 символов.

Просмотреть существующие сценарии можно с помощью команды display all или display config в меню (config-nsg)#.

Сценарий представляет собой последовательность записей "жду" — "посылаю", разделенных пробелами. Нечетные члены последовательности представляют собой сообщения, ожидаемые от модема или удаленной системы, а следующие за ними четные — команды, выдаваемые интерфейсом в линию. Пример ввода сценария:

```
(config-nsg)# chat-script logging_on "ogin: vasya.pupkin assword: qwerty"
```

Поскольку тело сценария содержит пробелы, оно, как строковый параметр, должно быть заключено в кавычки ("). Для ввода кавычек, пробелов и других спецсимволов в текст записей сценария используются особые правила, описанные ниже.

Приведенный выше пример означает, что интерфейс PPP будет ожидать от удаленной системы приглашения, оканчивающегося на ogin: (без пробела). Когда эта последовательность символов будет получена, в линию будет послана строка vasya.pupkin. Затем клиент будет ждать, пока из линии будет получено приглашение assword:, и в ответ пошлет строку qwerty — и так далее до конца сценария. Каждая посылаемая последовательность символов дополняется символом <CR>.

ВНИМАНИЕ Пароль для входа в удаленную систему представляет собой, с точки зрения сценария, обычную запись, не выделяющуюся среди остальных, и хранится в конфигурации устройства в открытом виде.

Любая запись сценария (ожидание или посылка) может быть заключена в апострофы, или одинарные прямые кавычки ('). Апостроф необходим, если запись сама по себе должна содержать пробелы, например:

```
(config-nsg)# chat-script logging_on "'ogin: ' vasya.pupkin 'assword: ' qwerty"
```

Здесь, в отличие от предыдущего примера, записи 'ogin: ' и 'assword: ' означают, что устройство будет ждать от удаленной системы подсказок, оканчивающихся пробелами после двоеточия.

Кроме пробела, в апострофы следует заключать записи, содержащие спецсимволы: & @ и др.

Два апострофа означают пустую запись ('' — не путать с одиночной двойной кавычкой!). Если такая запись стоит в качестве записи ожидания, то клиент PPP ничего не ждет и сразу переходит к посылке следующей команды. В частности, чтобы начать выполнение сценария не с ожидания, а с выдачи команды модему, следует указать пустой первый член последовательности:

```
'' ATZ OK ATDP1234567 CONNECT ...
```

Если пустая запись стоит на месте записи, посылаемой в модем, то посылается символ <CR>, т.е. пустая строка. В частности, если сценарий должен завершиться получением сообщения CONNECT, то для соблюдения четности записей следует указать:

```
"... CONNECT ''"
```

Внутри апострофов не могут использоваться спецсимволы, перечисленные в конце данного параграфа. Однако допускается брать в апострофы не всю запись а только ее фрагмент; в этом случае запись рассматривается как единое целое. Например, следующие две записи эквивалентны:

```
'ABC '123
'ABC 123'
```

а следующая запись может быть сделана только с двумя парами апострофов, чтобы спецсимвол \N оказался вне их:

```
'sending NULL '\N' sent NULL'
```

Если в течение некоторого времени (по умолчанию 45 секунд) ожидаемая последовательность не будет получена, то выполнение сценария заканчивается неудачей и интерфейс PPP переходит в исходное состояние. Продолжительность тайм-аута может быть изменена включением параметра TIMEOUT в сценарий перед строкой ожидания. Например, в сценарии

```
"'' ATZ OK ATDT5551212 CONNECT '' TIMEOUT 10 'ogin:' sidorov"
```

тайм-аут перед ожиданием строки ogin: будет уменьшен до 10 секунд. Нулевое значение TIMEOUT указывает, что время ожидания не ограничено.

В качестве записи ожидания может быть указана последовательность записей "ожидание"–"посылка"–…–"ожидание", разделенных дефисами. Например, сценарий

```
"'' ATD1234 CONNECT-ATD1256-CONNECT-ATD1278-CONNECT ''"
```

означает, что если после набора номера 1234 в течение 45 секунд не получен ответ CONNECT, то модем должен набрать номер 1256; если по этому номеру тоже не удается соединиться (нет ответа, получен BUSY, NO CARRIER, NO DIALTONE и т.п.) — набрать 1278. Как только получен ответ CONNECT, выполнение альтернативной ветви завершается и исполняется следующий шаг основного сценария — в данном случае, посылка пустой строки и нормальное завершение сценария. Если все варианты альтернативных посылок испробованы и ни на одну из них не получен ожидаемый ответ (в общем случае он может быть свой для каждой из посылок), выполнение сценария завершается аварийно.

Аналогичный пример для команд и ответов, содержащих спецсимволы:

```
"'' 'AT+CPIN?' '+CPIN: READY-AT+CPIN=9876-+CPIN: READY' ATD1234 CONNECT ''"
```

В этом случае сначала проверяется регистрация модуля IM–GPRS (или внешнего модема) в сети GSM. Если получен ответ +CPIN: READY (с пробелом!), то интерфейс приступает к набору номера; если нет — вводит PIN-код (AT+CPIN=9876) и снова ждет ответа +CPIN: READY.

ПРИМЕЧАНИЕ Основные команды для подключения к сотовым сетям см. в документах NSG:
Управление модулем IM–GPRS с помощью AT-команд.
Управление модулем IM–EDGE с помощью AT-команд.
Управление модулями CDMA и EVDO с помощью AT-команд.

Специальным образом вводятся символы, перечисленные ниже.

\? Вопросительный знак. При последовательным нажатии клавиш \ и ? обратный слэш преобразуется в вопросительный знак "на лету"

\" Двойная кавычка ("), например:

```
... OK AT+CGDCONT=1,\"IP\",\"internet.cellprovider.ru\" OK ATD*99# CONNECT ...
```

В этом случае в модуль IM–GPRS будет послан следующий GPRS-контекст:

```
+CGDCONT=1,"IP","internet.cellprovider.ru"
```

\\ Обратный слэш (\) — например, для некоторых фирменных команд у отдельных типов модемов.

Три вышеприведенные escape-последовательности являются общими для всех строковых параметров, к которым относится сценарий соединения. Помимо этого, в сценариях предусмотрены дополнительные спецсимволы и инструкции:

\-	Дефис (-) как текстовый символ в записи ожидания — чтобы отличать его от дефиса, разделяющего альтернативные варианты посылок/ответов. Для команд, посылаемых PPP-интерфейсом, допускается вводить дефис обычным образом.
\b	Символ <BS> (0x08)
\c	Подавить символ <CR> в конце строки. Данный спецсимвол может использоваться только в конце строки и только для команд, посылаемых PPP-интерфейсом. По умолчанию, в конце каждой посылаемой строки вставляется символ <CR>.
\d	Задержка на 1 сек (только для команд, посылаемых PPP-интерфейсом)
\K	Послать сигнал BREAK (только для команд, посылаемых PPP-интерфейсом)
\n	Символ <LF> (0x0A)
\N	Послать символ NULL (0x00; только для команд, посылаемых PPP-интерфейсом)
\p	Задержка на 1/10 сек (только для команд, посылаемых PPP-интерфейсом)
\r	Символ <CR> (0x0D)
\s	Пробел (символ 0x20). Это альтернативный способ ввода пробела, не разрывающий целостность отдельной записи. Его можно использовать вместо апострофов, чтобы ввести пробел в тело посылки/ответа, например: AT+CGREG? +CGREG:\s1,1
\t	Символ горизонтальной табуляции (0x09)
^A … ^Z	Непечатаемые управляющие символы с кодами от 0x01 до 0x1A
^[, ^], ^^,^_	Непечатаемые управляющие символы с кодами от 0x1B, 0x1D, 0x1E, 0x1F, соответственно
\^	Символ ^
\'	Апостроф

Пример. Для IP-интерфейса типа PPP, работающего в режиме сервера, сценарий обычно содержит команды инициализации модема и перевода его в режим ожидания входящих звонков:

```
chat-script wait4call "'' ATZ OK ATS0=1"
```

§3.3.11. Шаблон IP-интерфейса для портов PPP

Для настройки IP-интерфейсов, которые предполагается использовать с асинхронными портами PPP или с протоколами на основе PPP (PPPoE, PPTP), предназначены *шаблоны (virtual templates)*. Шаблон представляет собой совокупность дополнительных параметров, связанных с установкой физического соединения, аутентификацией, согласованием параметров IP и другими функциями. Эти параметры могут относиться к режиму клиента (т.е. для подключения устройства NSG к удаленной системе), к режиму сервера (т.е. для подключения удаленных пользователей к устройству NSG), или к обоим режимам.

Создание/редактирование и удаление шаблонов производится в меню команд NSG (config-nsg)# при помощи команд:

```
virtual-template <1...25>
no virtual-template <1...25>
```

При этом первая команда создает шаблон с указанным номером, если он не существует, и осуществляет вход в меню редактирования шаблона. Ссылка на номер используемого шаблона входит в конфигурацию асинхронного порта с инкапсуляцией PPP (см. п.3.3.1), клиента и сервера PPPoE, туннеля PPTP (см. Часть 5).

В меню настройки шаблона (config-virtual-template-N)# (где N — номер шаблона) содержатся следующие основные команды:

description <комментарий>
: Текстовое описание данного шаблона для удобства администрирования. Если строка содержит пробелы, она должна быть заключена в кавычки. Максимальная длина описания — 255 символов.

ip address <ip-адрес>
: Установка IP-адреса для создаваемого IP-интерфейса. (Фактический адрес может отличаться от установленного, если использована опция ppp ipcp accept-address yes.) Если IP-адрес должен быть получен от удаленной стороны, то значение данного параметра следует установить равным 0.0.0.0.

ip mtu <100...1500>
: Размер MTU создаваемого интерфейса. По умолчанию для асинхронного порта MTU = 1500. Для интерфейса PPPoE значение данного параметра игнорируется и принудительно устанавливается MTU = 1492, для интерфейса PPTP MTU = 1480.

keepalive { no | <0…100> [retry {<1…100> | no }] }

Проверка целостности соединения. Для порта с инкапсуляцией PPP, а также для протокольных объектов на основе PPP (PPPoE, PPTP и т.п.) используется механизм LCP Echo. Для порта с инкапсуляцией SLIP посылаются пустые пакеты; подробнее об этом механизме см. п.3.3.5.
Первый параметр определяет интервал (в секундах) между посылкой контрольных пакетов; если значение параметра равно нулю или no, запросы не посылаются. При этом ответы на приходящие запросы отсылаются в любом случае (в т.ч. и при keepalive 0).
Второй параметр устанавливает максимальное количество запросов. Если на указанное число запросов подряд не получено ни одного ответа, соединение разрывается. Суммарное время, по истечении которого интерфейс сочтет соединение неработающим и рестартует, равно произведению этих двух параметров. Значение retry no показывает, что разрыв соединения не производится, независимо от отсутствия ответов на запросы; такая установка целесообразна, например, если пакеты *keepalive* посылаются с единственной целью предотвратить разрыв соединения на физическом уровне из-за отсутствия трафика (переход сотовых модемов в "спящий" режим и т.п.)
При изменении параметра keepalive параметр retry автоматически принимает значение no. Таким образом, чтобы использовать механизм зондирования и разрыва соединения, данную команду необходимо вводить полностью.
По умолчанию установлены следующие значения параметров: keepalive 10 retry no.

peer ip address <ip-адрес>

IP-адрес удаленной стороны. При установлении соединения автоматически создается соответствующая запись в маршрутной таблице.
Этот же адрес используется в случае, если удаленный клиент PPP требует назначить ему динамический IP-адрес, а требуемое значение не определено никакими другими средствами (например, сервером RADIUS в результате аутентификации). Если устройство NSG не должно назначать IP-адрес удаленной стороне, то данный параметр следует установить равным 0.0.0.0.
Если шаблон используется для создания интерфейсов PPPoE сервера, то удаленным клиентам назначаются последовательные IP-адреса, начиная с заданного; максимальное число используемых адресов определяется параметром pppoe limit в настройках VPDN-группы (см. Часть 5).

ppp connection { permament | on-demand | passive }

Режим работы PPP-интерфейса:

permament	Интерфейс стремится поддерживать сеанс PPP постоянно. При разрыве соединения — рестартует и пытается установить его заново. Этот режим установлен по умолчанию.
on-demand	Интерфейс устанавливает физическое соединение и сеанс PPP только при наличии пакетов в выходной очереди данного интерфейса.
passive	Интерфейс не пытается инициировать сеанс PPP. После рестарта интерфейс отрабатывает сценарий физического соединения (он должен быть задан обязательно) и затем не посылает LCP-запросы, а только ждет запросы от удаленной стороны. Этот режим типичен для сервера PPP-доступа.

ВНИМАНИЕ При установленной опции ppp connection on-demand для соответствующего физического порта обязательно должен быть указан какой-либо сценарий установления физического соединения, хотя бы формальный:

```
chat-script dummy "'' ''"
```

В противном случае маршрут на данный интерфейс не будет создан.

ppp authentication { pap | chap | ms-chap | ms-chap-v2 | noauth } { local | radius }

При работе в режиме сервера: режим аутентификации удаленного клиента при открытии сеанса.
Первый параметр определяет протокол аутентификации или отсутствие таковой. Второй параметр определяет способ аутентификации:

local	локальный список пользователей (см. п.3.8.1)
radius	удаленный сервер RADIUS

ppp refuse-auth { [pap] [chap] [ms-chap] [ms-chap-v2] [eap] | no }

При работе в режиме клиента: отказываться от выполнения аутентификации по специфическим протоколам, если она запрашивается удаленной стороной. По умолчанию параметр имеет значение no, т.е. устройство NSG согласно аутентифицировать себя по любому из перечисленных протоколов. Чтобы сузить этот список, следует запретить конкретные протоколы; в этом случае аутентификация будет производиться только по оставшимся.

ppp sent-username <имя_пользователя>

При работе в режиме клиента: в ответ на запрос аутентификации отсылать указанное имя и соответствующий ему пароль из локального списка пользователей (см. п.3.8.1). Данные имя и пароль используются при аутентификации по всем протоколам, не запрещенным командой ppp refuse-auth. Если строки с указанным именем пользователя не оказывается в локальном списке пользователей, то запрос на аутентификацию отвергается.

ppp idle-time {<30…86400> | no }

Тайм-аут неактивности, в секундах. Если в течение указанного времени через интерфейс не передаются данные, соединение разрывается. При значении no (установлено по умолчанию) разрыв соединения по отсутствию активности не производится.

ppp session-time {<60…86400> | no }

Максимальная продолжительность сеанса PPP, в секундах. По истечении указанного времени сеанс принудительно разрывается. Опция доступна только при работе в режиме сервера (connection passive) или в режиме соединения по требованию (connection on-demand). При значении no (установлено по умолчанию) время соединения не ограничено.

ppp ipcp accept-address { yes | no } [remote { yes | no }

При работе в режиме клиента: разрешить использование адреса, присылаемого удаленной стороной, в качестве своего локального адреса. По умолчанию установлено значение no. Опциональный параметр remote указывает, следует ли соглашаться на использование адреса удалённой стороны, который она сама себе назначает:

- no — Использовать только адрес, заданный параметром peer ip address (при условии, что он не равен 0.0.0.0). Этот режим используется по умолчанию.
- yes — Принимать IP-адрес, назначаемый удалённой стороной. Значение peer ip address игнорируется. Этот режим позволяет разрешить конфликтную ситуацию, которая может возникнуть в случае установления соединения по требованию (см. ниже).

ppp ipcp accept-dns { yes | no }

При работе в режиме клиента: запросить адреса серверов DNS у удаленной стороны. В ответ удаленная сторона может прислать адреса одного или двух серверов. Назначенные адреса можно использовать в клиенте и ретрансляторе DNS (см. Часть 4). По умолчанию установлено значение yes.

ВНИМАНИЕ Для того, чтобы клиент DNS получал и использовал адреса серверов, назначенные в ходе установления сеанса PPP, необходимо указать в его настройках update-from <имя_интерфейса>.

ppp ipcp dns <ip-адрес>

При работе в режиме сервера: передавать удаленной стороне указанный адрес DNS. Если значение параметра равно 0.0.0.0, адрес DNS не передается.

ppp set-default-route { yes | no } [metric <1…255>]

Установка данного интерфейса в качестве маршрута по умолчанию. Значение по умолчанию no. Опциональный параметр metric позволяет принудительно установить метрику маршрута, определяющую его порядок в списке других маршрутов по умолчанию. По умолчанию маршруты создаются с метрикой 1.

ВНИМАНИЕ Указание метрики необходимо, если в системе имеются другие маршруты по умолчанию (как созданные на других PPP-интерфейсах командой set-defaultroute, так и созданные статически командой ip route ...). В частности, если интерфейс планируется использовать в качестве резервного, его метрика должна быть больше, чем метрика основного маршрута. Если это правило не соблюдено, то вероятен конфликт, в результате которого не будет создан ни один маршрут, или они будут созданы в неправильном порядке, или все они окажутся неработоспособными.

ПРИМЕЧАНИЕ Если PPP-интерфейс используется в режиме *dial-up* клиента со следующими настройками:
— Соединение устанавливается по требованию (connection on-demand)
— Адреса назначаются удаленной стороной (ipcp accept-address yes)
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:

```
ppp ipcp accept-address yes remote yes
```

ppp encrypt-mppe {no | auto | 40 | 128} [mode { stateless | stateful }]

Согласие и требование шифрования MPPE (Microsoft Point-to-Point Encryption):

- 40 или 128 — Использовать шифрование с указанной длиной ключа.
- no — Не использовать шифрование. (Значение по умолчанию.)
- auto — Автоматическое согласование факта шифрования и длины ключа. в процессе согласования параметров соединения.
- mode — Режим шифрования MPPE (необязательный параметр). Значение по умолчанию — stateless.

ppp data-compression { enable | disable }

Согласование сжатия данных:

disable — Запретить сжатие данных (установка по умолчанию). Может быть полезно, в частности, при работе в некоторых сотовых сетях, поскольку наблюдались ситуации, когда на стороне оператора алгоритм согласования сжатия отрабатывался некорректно и приводил к разрыву соединения на этапе CCP.

enable — Разрешить согласование сжатия по алгоритму BSD Compression. Для начала предлагается максимальная степень сжатия (15:15). Данная установка имеет смысл только в том случае, если удалённая сторона также поддерживает BSD Compression.

При настройке MPPE следует учитывать следующие особенности реализации данного механизма:

1. 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.
2. В режиме auto выбирается максимально безопасный режим передачи, т.е. шифрование включается всегда, если оно допускается противоположной стороной, и длина ключа устанавливается максимальной разрешённой для обеих сторон. В реализациях MPPE других производителей есть различия, приводящие к тому, что в некоторых случаях эти продукты при соединении друг с другом выбирают режим без шифрования или с минимальной длиной ключа. Во избежание проблем, рекомендуется всегда указывать режим шифрования явным образом на обеих сторонах.
3. Параметр stateful/stateless определяет только очерёдность посылки того и другого предложения. Будут ли эти предложения приняты удалённой стороной, зависит от реализации MPPE у конкретного производителя. В частности, продукты компании Microsoft всегда используют режим stateful; если они получают встречное предложение stateless, то немедленно разрывают соединение, не давая шанса предложить альтернативный вариант. Продукты Cisco Systems при несовпадающих настройках посылают встречное предложение и успешно согласовывают шифрование в больше числе случаев. Во избежание проблем, рекомендуется всегда указывать режим stateful/stateless явным образом на обеих сторонах.

ppp debug { on | off }

Включение расширенного режима отладки PPP. По умолчанию установлено значение off, т.е. вывод краткого набора сообщений об основных событиях PPP-сеанса.

ppp options "<строка>"

Ввод дополнительных опций PPP, для установки которых в данной версии NSG Linux не предусмотрены отдельные команды. В строку могут быть включены (через пробел) любые опции, предусмотренные для службы PPP (pppd) в Linux.
Подробно обо всех возможных опциях см. *man-pages* по pppd.

ПРИМЕЧАНИЕ Параметры PPP, для которых предусмотрены отдельные команды в настройках шаблона, рекомендуется вводить именно с помощью этих команд.

Созданные шаблоны интерфейсов PPP используются в конфигурации физических асинхронных портов (см. п.3.3.1) и служб PPPoE, PPTP. Для выбора шаблона используется соответствующие команды в меню настройки портов и VPDN-групп, например:

```
(config-nsg)# virtual-template 1
.....
(config-nsg)# port a1
(config-a1)# encapsulation ppp
(config-a1)# virtual-template  1
.....
(config-nsg)# vpdn-group 1
(config-vpdn-group)# virtual-template 1
```

Если шаблон интерфейса не задан (значение 0), или указанный шаблон не существует, то PPP-соединение будет устанавливаться, по умолчанию, следующим образом:
— локальный и удаленный адреса назначаются удаленной стороной
— аутентификация не производится

§3.3.12. Параметры порта для SMS-управления

Инкапсуляция sms-handler может быть установлена на портах, к которым подключены модули IM–GPRS, IM–EDGE или IM–3G. Она служит для обработки SMS-сообщений, приходящих на данный модуль. SMS-сообщения могут быть посланы с мобильного телефона GSM или UMTS, на котором установлено приложение MoNsTer (MObile NSg TERminal). С помощью SMS удалённый пользователь может выполнять различные операции, определенные в файле конфигурации nsgsms.conf (см. следующий параграф).

При выборе инкапсуляции SMS-handler в меню порта имеется следующий дополнительный параметр:

sms-handler Вход в узел меню, позволяющий определить группу специфических параметров для этого протокола.

Дополнительный узел меню sms-handler содержит следующие команды:

debug-level <0...4>

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 6).

number-of-sms <1...8>

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.

user-phone <номер> [user-name <имя>] [group-name <группа>]
no user-phone <номер>

Включение указанного номера телефона в "белый список" и исключение из него. Любые SMS-команды принимаются к исполнению только в том случае, если номер отправителя определился и входит в этот список; все другие SMS игнорируются.

Для управления может быть задано до 32 номеров (см. также описание файла конфигурации /etc/nsgsms.conf).

Номер может содержать до 31 знака.

Необязательные поля user-name и group-name могут использоваться для определения прав пользователя при выполнении некоторых операций.

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.

Помимо вышеперечисленных, в узле sms-handler имеется ещё одна группа параметров, используемых при совместном использовании SMS-управления и передачи данных, а также при обращении к сотовому модему утилитой at (см. следующие два параграфа).

Пример конфигурации:

```
!
nsg
    port s1
        encapsulation sms-handler
        baudrate 115200
        sms-handler debug-level 2
        sms-handler number-of-sms 3
        sms-handler user-phone "1239876543" user-name "vova" group-name "admins"
        sms-handler user-phone "9871234567" user-name "masha" group-name "blondes"
        exit
```

§3.3.13. SMS-управление при передаче данных

SMS-управление может осуществляться одновременно с передачй данных по протоколу PPP (как в режиме пакетном, так и в канальном режиме). В этом случае обработчик SMS включается между модемом и PPP-интерфейсом. Если модем находится в режиме передаче данных, то обработчик SMS периодически приостанавливает передачу, переводит модем в командный режим (без разрыва PPP-соединения), проверяет наличие входящих SMS, обрабатывает их, отправляет ответ и по завершении работы возвращает модем в режим данных.

Сигнал DCD в ходе этой процедуры сохраняется поднятым, поэтому PPP-соединение формально не разрывается. Однако следует соразмерять возможное время выполнения длительных команд (например, *ping* с большим временем ожидания и большим числом пакетов одновременно) и время срабатывания механизмов *keepalive*, контролирующих фактическую работу данного интерфейса.

Для настройки одновременной работы PPP и SMS-управления узел меню sms-handler доступен также при установленной encapsulation ppp. При этом, помимо общих параметров SMS, перечисленных в предыдущем параграфе, используются следующие два:

sms-handler ppp-cooperation { yes | no }

Включение/выключение режима совместной работы:

- yes — Разрешить работу с SMS на интерфейсе, настроенном как encapsulation ppp.
- no — Запретить работу с SMS, если интерфейс настроен как encapsulation ppp. Запрет действует независимо от наличия PPP-соединения. (Установка по умолчанию.)

sms-handler inquiry-time { 10...84600 | no }

Периодичность проверки входящих SMS, в секундах. Следует выбирать его не кратным периоду посылки контрольных пакетов (*keepalive*, *ping* и т.п.), чтобы не возникла ситация, когда подряд несколько пакетов попадают в моменты обработки SMS и не возвращаются вовремя.
Значение no указывает, что прерывать сеанс обмена запрещено. В этом случае обработчик SMS будет проверять наличие входящих SMS только в периоды отсутствия PPP-соединения (при установке ppp connection on-demand или passive) или разово в момент рестарта интерфейса.

Использовать механизм прерывания PPP-сеанса не рекомендуется для модулей IM–GPRS *h/w ver.3* на чипсетах PIML и FLYFOT. Ввиду ошибки в их внутреннем программном обеспечении, если команда +++ поступает на модем в момент приёма данных из эфира, они впадают в полностью неработоспособное состояние. Через положенное время это приводит к рестарту интерфейса (по неактивности, по непрохождению пакетов *keepalive* и т.п.), работоспособность модуля восстанавливается и соединение устанавливается заново. Вероятность возникновения такой ситуации и её допустимость зависят от типа приложения и характера трафика. Например, при подключении POS-терминала, который производит эпизодические кратковременные транзакции, эта вероятность весьма мала. Однако если такая потеря связи недопустима в принципе, то следует установить режим inquiry-time no. При этом, чтобы гарантировать обработку SMS за конечное время, можно ограничить время неактивности (ppp idle-time) и/или максимальную предолжительность сеанса (ppp session-time), чтобы стимулировать завершение сеансов PPP. Эти параметры доступны во всех режимах, включая ppp connection permanent.

После разрыва соединения интерфейс рестартует, обработчик SMS первым получает доступ к модулю, выполняет свои задачи, и только после этого начинает пропускать команды сценария PPP-соединения. Соответственно, в сценарии соединения должна быть предусмотрен увеличенный таймаут до получения первого OK в начале работы (см. п.3.3.8):

```
TIMEOUT n  XXX-\rAT-OK
```

В противном случае, если OK не получено за время 2n, порт рестартует, сорвёт работу обработчика SMS, и всё начнётся заново.

§3.3.14. Передача SMS и исполнение других AT-команд

Для передачи SMS-оповещений из скриптов Linux, например, регулярно по времени, или в случае наступления какого-либо события (изменения состояния интерфейсов, срабатывания датчиков технологического контроля и т.п.), используется утилита at. Эта же утилита может использоваться для исполнения любых AT-команд, например, для проверки уровня сигнала.

Для работы at устанавливает служебное TCP-соединение с обработчиком SMS. Номер порта определяется командой:

sms-handler control-tcp-port <1024...65535>

Номер порта TCP, на котором обработчик SMS ожидает соединения от утилиты at. Значение по умолчанию — 50000.

§3.3.15. SMS-управление: формат файла nsgsms.conf

Файл конфигурации /etc/nsgsms.conf определяет закрытый перечень операций, которые могут быть выполнены через SMS-запрос. В данном файле также описываются вид и параметры меню, которое будет загружаться в мобильный телефон, и, при необходимости, права пользователей и групп.

Как правило, файл конфигурации формируется производителем и входит в состав ПО устройства для конкретных заказных поставок. Однако квалифицированные пользователи могут создавать и редактировать его под свою ответственность.

Файл конфигурации составляется в простом текстовом формате и может быть просмотрен или изменён с помощью любого текстового редактора. В командной оболочке Linux устройств NSG для этой цели имеется редактор nano. Во многих случаях пользователю может быть удобно выгрузить файл на свой компьютер, отредактировать привычными ему средствами, и затем загрузить обратно по tftp или любому другому протоколу передачи файлов.

Файл содержит меню операций (по постановке задачи, непустое), 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.

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

Если значение опции короче, чем строка, выводимая АОН, 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.

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.

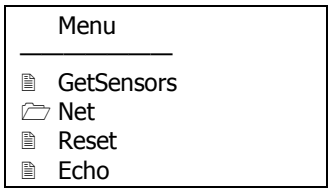
ПРИМЕЧАНИЕ Параметры типа set и choice передаются в виде текстовой строки, состоящей из нулей и единиц. Нули соответствуют не выбранным значениям, единицы — выбраннным, общее число символов равно числу предлагаемых вариантов. Дальнейший разбор этой строки производится в вызываемом скрипте.

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 6 данного руководства и соответствующую документацию по Linux.

Пример файла конфигурации:

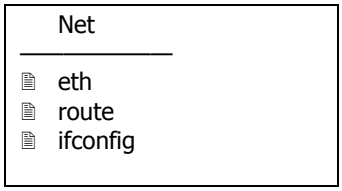
```
USER 79031111111;
USER 79262222222 Vasya root;
MENU {
GetSensors() nsgow /dev/nsg/a1;
Net{
    eth(AdmState:choice:up:down) ifconfig eth0 $1;
    route() ip route show;
    ifconfig(interface:string) ifconfig $1;
    }
Reset(password:password tmo:number) nsgreset $U $G $1 $2;
Echo(str) echo $1;
}
```

При такой конфигурации пользователь MoNsTer увидит на мобильном телефоне список:

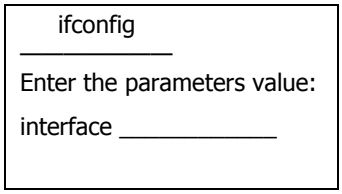


где второй пункт (Net) является подменю, а три остальные — командами.

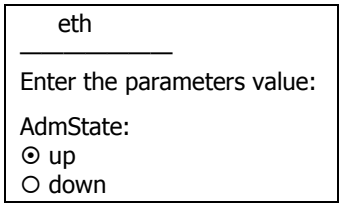
При выборе пункта Net он увидит следующий экран:



При выборе пункта ifconfig:



При выборе пункта eth:



§3.4. Настройка портов Ethernet

Для настройки портов Ethernet, привязанных к реальным физическим интерфейсам, на канальном уровне используются команды:

mac-address XX:XX:XX:XX:XX:XX
Назначение MAC-адреса порту.

Для встроенных портов Ethernet уникальный MAC-адрес устанавливается при изготовлении, но в случае необходимости может быть изменён пользователем. Сменные модули IM–ET10, IM–ET10F, UM–ET100, IM–SDSL не имеют собственных MAC-адресов, и для них устанавливается адрес, равный MAC-адресу встроенного порта. Поскольку два порта Ethernet одного устройства не подключаются к одной локальной сети, это, в общем случае, не вызывает затруднений. Для полностью корректной конфигурации сети можно также назначить модулям уникальные MAC-адреса, но при этом рекомендуется ограничиться изменением только двух младших байт.

encapsulation { ethernet | vlan }
Тип пакетов Ethernet:
ethernet — обычная физическая ЛС Ethernet
vlan — VLAN (IEEE 802.1Q)

vlan <1...4094>
no vlan <1...4094>
Создание/настройка и удаление виртуальной локальной сети. Первая команда создает VLAN с указанным номером, если она не существует, и осуществляет вход в меню настройки VLAN. Внутри меню доступны все те же пункты, что и для физического порта Ethernet, за очевидным исключением adm-state, mac-address и encapsulation.
Команда доступна только при инкапсуляции vlan.

ПРИМЕЧАНИЕ Идентификатор VLAN 1, как правило, используется многими VLAN-устройствами для особой цели: если пакет, полученный без тега VLAN, должен быть отправлен в сегмент с поддержкой VLAN, то ему принудительно присваивается тег с этим номером. Использовать VLAN 1 для других целей без настоятельной на то необходимости не рекомендуется.

Если для порта задана инкапсуляция vlan, то при создании каждой VLAN в системе появляется суб-интерфейс с именем вида sN.<vlan> или eth0.<vlan>, где sN, eth0 — имя физического порта, <vlan> — номер VLAN. Примеры: s1.2, eth0.6, и т.д.

В расширенном смысле, под портами Ethernet в устройствах NSG могут подразумеваться различные типы объектов, предназначенных для передачи пакетов Ethernet, а именно:

а) порты, привязанные к физическим интерфейсам Ethernet и Ethernet-over-SDSL (см. Часть 2)

б) виртуальные порты:

Ethernet-over-HDLC (см. п.3.2.2):

```
port sN
    encapsulation raw-hdlc
    raw-hdlc type ethernet
```

Ethernet-over-Frame Relay (см. п.3.2.4):

```
port sN
    encapsulation frame-relay
    frame-relay dlci 17
        encapsulation ethernet
```

Ethernet-over-IP (GRE) (см. Часть 5):

```
tunnel ip N
    encapsulation eth-br-over-ip
```

в) интерфейсы виртуальных сетей (VLAN), организованные на физических интерфейсах (см. выше)

г) программные мосты как целое (см. след. параграф)

Данные объекты могут:

— Являться IP-интерфейсами, т.е. инкапсулировать и передавать пакеты IP-over-Ethernet, поступающие непосредственно от маршрутизатора.
— Входить в состав программных мостов (*bridge groups*), подробнее см. п.3.5.
— Содержать в себе клиента или сервер PPPoE.

Возможности, предусмотренные в данной версии NSG Linux, указаны в таблице.

Привязка порта	**Инкапсуляция**	**Дочерние VLAN**	**MAC-адрес**	**IP интерфейс**	***bridge groups***	**PPPoE**	
						server	**client**
Физический Ethernet и Ethernet-over-SDSL	encapsulation ethernet	+	настраиваемый	+	+	+	+
	encapsulation vlan		настраиваемый		+		
VLAN			от родительского физ. интерфейса	+	+	+	+
Ethernet-over-HDLC			не настаиваемый	+	+	+	
Ethernet-over-Frame Relay				+	+	+	
Ethernet-over-IP (GRE)					+		
Bridge			нет	+		+	

IP-интерфейсом может быть любой порт Ethernet, кроме порта с encapsulation vlan (в последнем случае интерфейсами маршрутизатора служат индивидуальные VLAN) и туннеля GRE. Для настройки IP-интерфейса используется команда:

ip address <ip-префикс> [peer <ip-адрес>] [broadcast <ip-адрес>] [anycast <ip-адрес>]
no ip address <ip-префикс>

Установка и удаление IP-адресов. Обязательным параметром является IP-префикс (адрес и длина маски, например, 123.134.145.156/24). При необходимости можно отдельно назначить адреса удаленной стороны (peer) в соединении "точка-точка", широковещательной (broadcast) и групповой (anycast) рассылки.

а также группа других параметров, относящихся к протоколу IP. Настройка этих параметров подробно рассмотрена в Части 4.

ПРИМЕЧАНИЕ Встроенный порт Fast Ethernet устройств NSG–900 и модуль UM–ET100 автоматически определяют состояние линии, т.е. при отсутствии физического соединения с сетью соответствующий IP-интерфейс ставится в состояние DOWN, а соответствующие ему маршруты удаляются из таблицы маршрутизации.
Для встроенных интерфейсов Fast Ethernet устройства NSG–700, модулей IM–ET10, IM–ET10F, а также интерфейсов *x*DSL, настроенных в режиме моста, состояние IP-интерфейса не зависит от наличия физического соединения.

В состав программного моста Ethernet может входить любой из вышеперечисленных объектов Ethernet, в т.ч. порты с encapsulation vlan (коммутация "порт-на-порт") и порты с encapsulation ethernet (коммутация "сеть-на-сеть). Подробно об организации мостов см. п.3.5.

Клиент и сервер PPPoE могут функционировать только на физических портах с encapsulation ethernet и на индивидуальных VLAN в случае encapsulation vlan. Подробно о службах PPPoE см. Часть 5.

§3.5. Коммутация пакетов Ethernet

§3.5.1. Bridge Groups

Устройства под управлением NSG Linux могут работать в режиме прозрачного моста Ethernet между двумя или более физическими локальными сетями Ethernet, виртуальными сетями (VLAN), а также синхронными каналами WAN, каналами Frame Relay и туннелями GRE, на другой стороне которых также установлены аналогичные мосты. Создание/настройка и удаление мостов производится в меню команд NSG (config-nsg)# при помощи команд:

```
bridge <1...255>
no bridge <1...255>
```

При этом первая команда создает мост с указанным номером, если он не существует, и осуществляет вход в меню настройки моста.

Дальнейшая настройка моста производится в меню (config-bridge-NN)#, содержащем следующие специфические команды:

description Административное описание данного моста — текстовая строка длиной до 255 знаков. Если строка содержит пробелы, ее необходимо заключить в кавычки.

aging-time <10...1000000>
Время жизни MAC-адресов (в секундах) в адресных таблицах моста.

forward-time <4...200>
Задержка перехода, в секундах. (Задержка, которую необходимо выждать перед переходом в новое состояние после изменений сетевой топологии.)

hello-time <1...10>
Интервал между рассылками сообщений Hello (в секундах).

max-age <6...200>
Максимальное время жизни записей в таблицах MAC-адресов.

priority <0...65535>
Приоритет моста в рамках протокола Spanning Tree. Меньшее значение соответствует более высокому приоритету. Мост с наименьшим приоритетом будет выбираться в качестве корневого.

stp { on | off }
Включить/выключить Spanning Tree Protocol. По умолчанию протокол включён.

show-macs Вывести таблицу MAC-адресов.

show Вывести статус и статистику данного моста.

После того, как мост создан, к нему должны быть подключены два или более порта Ethernet (и/или эквивалентных им объектов). Мост будет запоминать MAC-адреса, находящиеся за каждым из этих портов, и перераспределять пакеты Ethernet согласно их MAC-адресам назначения. Подключение и отключение производится следующей командой:

```
bridge-group { <номер> | no }
```

Данная команда используется в меню настройки следующих объектов:

— портов Ethernet с физической средой Ethernet или SDSL (config-eth0)#, (config-sN)#
— индивидуальных VLAN на портах Ethernet (config-vlan-N)#
— виртуальных каналов Frame Relay (config-dlci-N)#, если для данного DLC установлено encapsulation ethernet
— портов Raw-HDLC (config-port-N)#, если для порта установлено raw-hdlc type ethernet
— туннелей GRE с инкапсуляцией IP (config-tunnel-N)#

При подключении данных объектов к мосту они безусловно отключаются от IP-интерфейса маршрутизатора. При этом все связанные с ними параметры IP обнуляются и становятся недоступными для конфигурирования. Вместо это сам мост, как единое целое, всегда имеет IP-интерфейс, подключенный к маршрутизатору. Для этого интерфейса настраивается полный набор параметров IP для этого интерфейса (см. Часть 4). На нём также может использоваться сервер PPPoE (см. Часть 5).

§3.5.2. Коммутация VLAN

При использовании VLAN коммутация пакетов Ethernet может осуществляться двумя способами:

а) Коммутация "сеть-на-сеть"

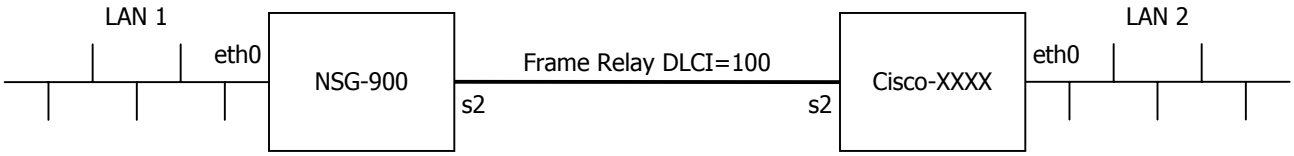
При таком способе коммутации в состав моста могут входить:

— Физические порты Ethernet с инкапсуляцией ethernet
— Индивидуальные VLAN (в т.ч. и расположенные на одном и том же физическом порту)
— Виртуальные каналы Frame Relay, порты Raw-HDLC и туннели GRE, если их удаленные стороны входят в состав аналогичных мостов (на устройствах NSG, Cisco Systems, или совместимых с ними).

Коммутация осуществляется между индивидуальными физическими или виртуальными сетями Ethernet, непосредственно или через транспорт Frame Relay, GRE. Используемые VLAN могут иметь различные номера, поскольку теги 802.1q через мост не передаются. Во входящем пакете, если он получен из VLAN, тег анализируется (именно по нему определяется принадлежность пакета данному мосту) и затем удаляется. Далее пакеты передаются через мост в обычном формате Ethernet, т.е. без тегов. Если выходная сеть является виртуальной, то при передаче в нее к пакету добавляется тег с номером этой VLAN.

Таким образом, данный способ коммутации обеспечивает обмен данными между любыми двумя хостами, находящимися в физических или виртуальных сетях, подключенных к мосту.

Пример. На одной стороне канала Frame Relay установлено устройство NSG, на другой стороне Cisco. Простая коммутация между двумя физическими сетями Ethernet.




```
bridge 1

port eth0
    bridge-group 1
    exit

port s2
    baudrate 2048000
    encapsulation frame-relay
    frame-relay lmi ansi
    frame-relay dlci 100
        cir 2048000
        bridge-group 1
        exit
    exit
```

```
bridge irb

interface FastEthernet0/0
    ip address 10.0.0.31 255.0.0.0
    no ip mroute-cache
    duplex auto
    speed auto
    bridge-group 1
    exit

interface Serial0/1
    no ip address
    encapsulation frame-relay IETF
    clockrate 2048000
    frame-relay map bridge 100 broadcast
    frame-relay interface-dlci 100
    frame-relay lmi-type ansi
    frame-relay intf-type dce
    bridge-group 1
    exit

bridge 1 protocol ieee
no bridge 1 route ip
```

Если на обеих сторонах канала Frame Relay используются устройства NSG, второе устройство настраивается аналогично первому.

б) Коммутация "порт-на-порт"

При таком способе коммутации в состав моста могут входить только физические порты Ethernet с инкапсуляцией vlan, а также виртуальные каналы Frame Relay, порты Raw-HDLC и туннели GRE — при условии, что на удаленной стороне канала имеется аналогичный мост. Пакеты передаются через мост в неизменном виде, вместе с тегами 802.1q. Таким образом, адресат может получить пакет только в том случае, если он находится в VLAN с тем же номером, что и отправитель.

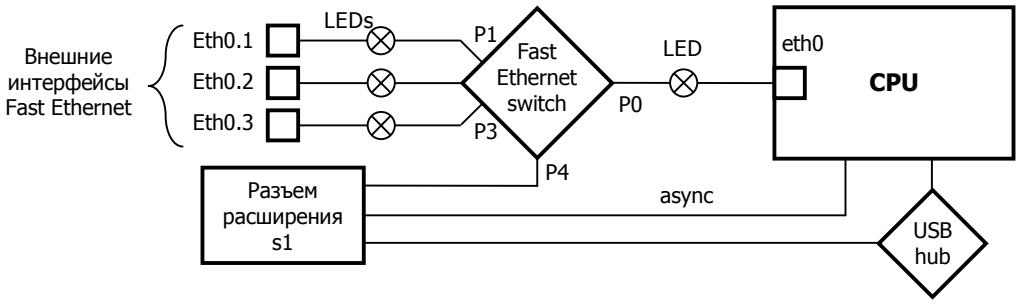
Bridge Group в данном случае удобнее рассматривать не как один мост, а как совокупность нескольких мостов — по одному на каждый используемый идентификатор VLAN. Пересылка пакетов осуществляется независимо в рамках каждой VLAN, заданной одинаковым номером на нескольких портах Ethernet. Как следствие, необходимо, чтобы VLAN с одним и тем же номером была определена, как минимум, на двух физических портах Ethernet; эти порты могут находиться как на одном устройстве, так и на разных устройствах, соединенных через сеть Frame Relay.

§3.5.3. Использование аппаратного коммутатора Ethernet в устройствах NSG–700

Устройства NSG–700 оснащены встроенным коммутатором Fast Ethernet с поддержкой VLAN. Коммутатор имеет 5 физических интерфейсов:

— phy 0 — подключён к внутреннему порту eth0, находящемуся на процессоре
— phy 1 ... phy 3 — подключены к разъёмам Eth0.1 ... Eth0.3 на корпусе устройства, соответственно
— phy 4 — подключён к разъему расширения s1, если в него установлен модуль IM–SDSL *h/w ver.2*.

Внутренняя архитектура устройств в части Ethernet показана на рисунке.



Для настройки коммутатора используются следующие команды в меню (config-nsg)#:

ethernet-switch
Вход в меню коммутатора. Дальнейшая настройка выполняется в меню (config-ethernet-switch)#:

mode { normal | vlan }
Режим работы коммутатора:
normal Обычная коммутация между всеми портами без учёта тегов VLAN.
vlan Передача пакетов на основе тегов VLAN и заданной таблицы коммутации.

show В режиме VLAN: показать текущую таблицу коммутации. Примеры таблиц коммутации см. ниже.

Если коммутатор работает в режиме VLAN, то для каждого идентификатора VLAN, указанного в настройках хотя бы одного порта, создаётся так называемая VLAN-группа. Каждую такую группу можно рассматривать как отдельный коммутатор с собственным набором физических интерфейсов phy 0 ... phy 4, работающий независимо от остальных. Максимальное число VLAN-групп — 15, т.е. число идентификаторов VLAN, обрабатываемых индивидуально, для всей совокупности интерфейсов не может превышать 15. Помимо этого, всегда существует одна специальная группа other, в которую каждый интерфейс также может включаться или не включаться.

phy <0...4> norm vlan-group { no | <vid> }
phy <0...4> vlan vlan-groups { no | <vid_list> } { deny-other | permit-other }
Только в режиме VLAN: режим работы для указанного физического интерфейса коммутатора и его принадлежность к VLAN-группам. Данная команда относится как к внешним физическим интерфейсам, так и к внутреннему, подключённому к порту Ethernet процессора.
norm Предполагается, что к интерфейсу подключён сегмент обычной сети Ethernet, т.е. входящие и исходящие пакеты не имеют тегов VLAN. Интерфейс включается в единственную VLAN-группу с указанным идентификатором <vid>. Если вместо этого указано значение vlan-group no, то интерфейс не включён ни в одну VLAN-группу, т.е. работа через него запрещена.
vlan Предполагается, что к интерфейсу подключён физический сегмент с одной или более VLAN, т.е. входящие и исходящие пакеты имеют теги VLAN. Список VLAN, поддерживаемых на данном интерфейсе, может содержать одиночные идентификаторы VLAN и диапазоны из двух идентификаторов, разделенных знаком "-"; элементы списка разделяются запятыми. Интерфейс включается во все VLAN-группы с перечисленными идентификаторами. Дополнительный параметр определяет принадлежность интерфейса к специальной группе other:
deny-other Включить интерфейс в VLAN-группу other.
permit-other Исключить интерфейс из VLAN-группы other.
В частности, если для интерфейса типа vlan установлено vlan-groups no deny-other, то интерфейс не включён ни в одну VLAN-группу, т.е. работа через него запрещена.

ВНИМАНИЕ Параметры deny-other и permit-other относятся не к идентификаторам VLAN, определённым на данном физическом интерфейсе, а ко всей совокупности VLAN, определённых на всех пяти интерфейсах коммутатора.

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. Если такой группы нет, то пакет приписывается к группе other.
   — входящий пакет, не имеющий тега VLAN и пришедший на физический интерфейс типа norm, приписывается к группе с номером, равным значению <vid> для этого порта. Если для интерфейса установлено <vid>=no, то пакет приписывается к группе other, но на следующем этапе он будет уничтожен.
   — входящий пакет, не имеющий тега VLAN и пришедший на физический интерфейс типа vlan, приписывается к группе other.

   При этом сам пакет не изменяется.
2) Если группа, к которой приписан входящий пакет, не содержит в своём списке номер физического интерфейса, с которого пришел этот пакет, то пакет уничтожается. В частности, это относится:
   — ко всем пакетам, поступившим через интерфейс типа norm с настройкой vlan-group no
   — к пакетам без тегов VLAN, поступившим через интерфейс типа vlan с настройкой deny-other
   — к пакетам с тегами VLAN, поступившим через интерфейс типа vlan с настройкой deny-other, если идентификатор VLAN, указанный в теге, не относится ни к одной из явно определённых VLAN-групп.

   Остальные пакеты передаются во все физические интерфейсы, указанные в списке данной группы.
3) На выходе из коммутатора каждый исходящий пакет может быть изменен по следующим правилам:
   — если пакет отправляется в физический интерфейс типа norm и имеет тег VLAN, то тег будет удален.
   — если пакет отправляется в физический интерфейс типа vlan 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 физические интерфейсы типа norm будут уходить только пакеты без тегов VLAN, а в физические интерфейсы типа vlan 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. В частности, рекомендуется обратить внимание на согласованную настройку физического интерфейса phy 0 коммутатора и порта eth0 процессора.
Рекомендуется также указывать списки используемых VLAN явным образом на каждом интерфейсе.

ВНИМАНИЕ На устройствах NSG–700 с версией материнской платы ранее ATM5 или версией NSG Linux ранее 1.0 *build 3* отработка сложных конфигураций может происходить с ошибками, в зависимости от предыдущей истории перенастройки коммутатора. В этом случае необходимо сохранить конфигурацию и рестартовать всё устройство по питанию (при нажатии кнопки Reset или программной перезагрузке коммутатор не рестартует).
В ныне выпускаемых версиях рестарт коммутатора при каждом изменении его конфигурации выполняется автоматически, поэтому накопление ошибок не происходит.

Примеры конфигурирования.

а) Коммутатор и внутренний порт в нормальном режиме Ethernet:

```
ethernet-switch normal
port eth0 encapsulation ethernet
```

Это обычный режим работы единой физической сети Ethernet без VLAN.

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

```
ethernet-switch normal
port eth0 encapsulation vlan
```

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 соединён с определённой VLAN на внутреннем порту eth0. Данная конфигурация устанавливается командой ethernet-switch mode vlan по умолчанию.

```
!
    nsg
        ethernet-switch
            mode vlan
            phy 0 vlan vlan-groups "101-103" deny-other
            phy 1 norm vlan-group 101
            phy 2 norm vlan-group 102
            phy 3 norm vlan-group 103
            phy 4 norm vlan-group no
            exit
        port eth0
            encapsulation vlan
            vlan 101
                ip address 10.0.0.1/8
                exit
            vlan 102
                ip address 20.0.0.1/8
                exit
            vlan 103
                ip address 30.0.0.1/8
                exit
            exit
```

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:

```
ethernet-switch show

Ethernet switch is in VLAN mode
VLAN memberships:
                P0   P1   P2   P3   P4
————   ————————————————
 VLAN 101    X    X    .    .    .
 VLAN 102    X    .    X    .    .
 VLAN 103    X    .    .    X    .
     others    .    .    .    .    .
```

г) Подключение к VLAN сегменту простых (не VLAN) сегментов.

```
!
    nsg
        ethernet-switch
            mode vlan
            phy 0 vlan vlan-groups "55,77" permit-other
            phy 1 norm vlan-group 55
            phy 2 norm vlan-group 77
            phy 3 vlan vlan-groups "55,77" permit-other
            phy 4 norm vlan-group no
            exit
        port eth0
            encapsulation vlan
            vlan 101
                ip address 10.0.0.1/8
                exit
            vlan 102
                ip address 20.0.0.1/8
                exit
            vlan 103
                ip address 30.0.0.1/8
                exit
            vlan 55
                ip address 50.0.0.1/8
                exit
            vlan 77
                ip address 70.0.0.1/8
                exit
            exit
```

Результат выполнения данной настройки:

```
ethernet-switch show

Ethernet switch is in VLAN mode
VLAN memberships:
             P0   P1   P2   P3   P4
———— ———————————————————
  VLAN 55    X    X    .    X    .
  VLAN 77    X    .    X    X    .
    others   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. Пакеты всех остальных VLAN из третьего сегмента будут переданы только на интерфейс eth0 процессора. Однако из их числа устройство обработает только пакеты с тегами VLAN 101, 102, 103, 55 и 77; остальные будут уничтожены драйвером порта Ethernet.

д) VLAN сеть с ограничением доступа.

```
!
    nsg
        ethernet-switch
            mode vlan
            phy 0 vlan vlan-groups "101,102" permit-other
            phy 1 vlan vlan-groups "101,102" deny-other
            phy 2 vlan vlan-groups "101" permit-other
            phy 3 norm vlan-group no
            phy 4 norm vlan-group no
            exit
```

Результат выполнения данной настройки:

```
ethernet-switch show

Ethernet switch is in VLAN mode
VLAN memberships:
             P0   P1   P2   P3   P4
———— ———————————————————
 VLAN 101    X    X    X    .    .
 VLAN 102    X    X    .    .    .
    others   X    .    X    .    .
```

Здесь коммутатор пропустит из первого сегмента только пакеты с тегами VLAN 101 и 102, все остальные будут уничтожены.

Необходимо обратить внимание, однако, что и из второго сегмента не все пакеты пройдут через коммутатор, несмотря на то, что для него сконфигурировано permit-other. Если через физический интерфейс 2 поступит пакет с тегом VLAN 102, то он будет приписан к VLAN группе 102. Но, согласно таблице, эта группа содержит только физические интерфейсы 0 и 1, поэтому пакет будет уничтожен. Чтобы все пакеты сегмента 2 были пропущены, необходимо настроить интерфейс следующим образом:

```
phy 2 vlan vlan-groups "101,102" permit-other
```

е) Объединение двух сегментов без доступа к процессору устройства NSG–700.

```
!
    nsg
        ethernet-switch
            mode vlan
            phy 0 norm vlan-group 700
            phy 1 norm vlan-group 666
            phy 2 norm vlan-group 666
            phy 3 vlan vlan-groups "700" deny-other
            phy 4 norm vlan-group no
            exit
        port eth0
            ip address 10.0.0.7/8
            exit
```

Результат выполнения данной настройки:

```
ethernet-switch show

Ethernet switch is in VLAN mode
VLAN memberships:
             P0  P1  P2  P3  P4
———— ———————————————————
VLAN 666      .   X   X   .   .
VLAN 700      X   .   .   X   .
  others      .   .   .   .   .
```

Здесь первый и второй физические сегменты соединены друг с другом, но не имеют доступа ни в третий сегмент, ни к интерфейсу eth0. Физический интерфейс 0 имеет тип norm, поэтому и для внутреннего порта eth0 необходимо использовать encapsulation ethernet (это настройка по умолчанию). 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.

§3.6. Коммутация пакетов Frame Relay и синхронного трафика

§3.6.1. Коммутация Frame Relay

Для установления постоянного виртуального соединения (PVC) между двумя виртуальными каналами (DLC) сети Frame Relay используется следующая команда в меню настройки DLC:

```
(config-dlci-NN)# route port <имя> <dlci>
```

где NN — номер текущего DLC, <имя> — символическое имя выходного порта (например, s3), <dlci> — номер выходного DLC на этом порту.

Команда является односторонней, т.е. устанавливает только пересылку пакетов из данного DLC в указанный выходной DLC. (Иначе говоря, полученное PVC будет симплексным.) Для того, чтобы установить полноценное двустороннее (дуплексное) PVC, необходимо использовать эту команду два раза — в меню настройки каждого из двух DLC. Пример:

```
(config-nsg)# port s1 frame-relay dlci 17 route port s3 81
(config-nsg)# port s3 frame-relay dlci 81 route port s1 17
```

В частности, постоянное виртуальное соединение может быть асимметричным, т.е. иметь различную скорость передачи в одну и в другую сторону. Чтобы получить такое соединение, нужно установить для двух DLC различные значения CIR/BC/BE.

Для просмотра имеющихся правил коммутации Frame Relay можно использовать команду display в меню портов, параметров Frame Relay или DLC.

Для удаления правил коммутации используется команда

```
(config-dlci-NN)# route no no
```

Разрыв PVC, как и его установление, должен быть выполнен с обеих сторон.

§3.6.2. Коммутация синхронного трафика

Синхронные порты с инкапсуляцией raw-hdlc предназначены для приема/передачи произвольного трафика, представленного пакетами HDLC общего вида (точное определение таких пакетов см. в п.3.2.1). Несколько потоков такого трафика могут быть мультиплексированы в один канал Frame Relay; для этого следует установить PVC между каждым из входных физических портов и соответствующим DLC, например:

```
port s1 encapsulation frame-relay
port s2 encapsulation raw_hdlc
port s1 frame-relay dlci 17 route port s2 no
port s2 route port s1 17
```

Как можно видеть, отличие от коммутации Frame Relay состоит в том, что в команде route вместо номера виртуального канала указывается no. Аналогичным образом производится удаление PVC:

```
port s1 frame-relay dlci 17 route port no no
port s2 route port no no
```

Два порта с инкапсуляцией raw-hdlc могут быть скоммутированы друг на друга:

```
port s1 encapsulation raw_hdlc
port s2 encapsulation raw_hdlc
port s1 route port s2 no
port s2 route port s1 no
```

Устройство с такой конфигурацией де-факто будет работать как преобразователь интерфейсов, синхронный модем, повторитель или устройство доступа к каналу E1 — в зависимости от используемых интерфейсных модулей на обоих портах. Безусловно, такое употребление является не самым целесообразным для маршрутизаторов, однако этот режим может быть полезен для целей тестирования и диагностики. В частности, синхронный порт может быть замкнут сам на себя, т.е. работать в качестве программного шлейфа:

```
port s1 encapsulation raw_hdlc
port s1 route port s1 no
```

Все данные, получаемые из линии, отправляются в этом случае обратно в ту же линию. Тот же результат можно получить с помощью настройки port s1 raw-hdlc type loopback.

§3.7. Маршрутизация и фильтрация вызовов X.25

Создание маршрутов и фильтров для пакетов X.25 CALL производится в меню (config-nsg)# при помощи команды следующего вида:

x25 route add [prio <1...512>] <критерии> <назначение>

Создание маршрута X.25. Команда содержит три группы параметров:

prio <1...512> Приоритет, он же порядковый номер записи в таблице маршрутизации (1 — наивысший). Параметр необязательный. Записи в таблице всегда имеют сплошную нумерацию. Если параметр отсутствует или превосходит число существующих записей более чем на единицу, то создаваемому маршруту присваивается номер, следующий за последним существующим. Если заданный номер меньше числа существующих записей, то новая запись вставляется в указанную позицию, а все последующие сдвигаются вниз.

<критерии> Маршрутизация или сброс пакета CALL может производиться на основании следующих критериев:

- destination <шаблон> — Шаблон вызываемого адреса (*called address*) X.121. Подробно о формате шаблона см. ниже.
- source <шаблон> — Шаблон вызывающего адреса (*calling address*) X.121.
- input-port {порт|служба} — Имя порта или службы (например, s1 или xot), через который получен данный пакет. Данный критерий равносилен фиксированной маршрутизации в базовом ПО NSG.
- cud <строка> — Значение поля данных (*call user data*) в пакете CALL — символьная строка. Если строка содержит пробелы или дефисы, ее необходимо заключить в кавычки, в остальных случаях кавычки необязательны. Максимальная длина поля — 124 символа при использовании *facility* Fast Select, 12 символов в остальных случаях.

Обязательным является указание хотя бы одного из вышеперечисленных критериев маршрутизации. В отличие от базового ПО NSG, допускается также маршрутизация по совокупности критериев, например, по вызываемому и вызывающему адресам одновременно.

<назначение> В качестве выходного объекта должно быть указано одно и только одно из следующих ключевых слов и имен:

- clear — Уничтожить данный пакет, т.е. отвергнуть вызов.
- contunue — Продолжить поиск в таблице маршрутизации. В данной версии NSG Linux параметр является формальным (т.е. строка с таким значением ничего не делает) и просто зарезервирован для последующих версий.
- local — Вызов должен направлен на одну из локальных служб X.25 на устройстве NSG. В данной версии NSG Linux единственной такой службой является *X.25 daemon*. Обратившись к нему с удаленного PAD, можно получить доступ к управлению устройством в режиме командной строки.
- port <порт> — Направить вызов в указанный физический порт X.25.
- xot <ip-адрес> [xot-source <ip-адрес>] — Направить вызов через службу XOT на указанный удаленный IP-хост. Дополнительно можно указать IP-адрес, который будет подставляться в пакеты XOT в качестве IP-адреса источника. Если этот адрес не указан, в качестве *source address* указывается адрес IP-интерфейса, через который отправляются пакеты.

Примеры создания маршрутов X.25:

```
(config-nsg)# x25 route add prio 1 destination 1234567 port s2
(config-nsg)# x25 route add prio 2 destination 987654 xot 123.145.167.189
```

При обработке пакета CALL записи в таблице маршрутизации рассматриваются последовательно в порядке убывания приоритета (возрастания порядкового номера). Как только найдена первая запись, под которую подпадает данный пакет, он отправляется по указанному маршруту (за исключением маршрута continue, означающего продолжение поиска в таблице маршрутизации). Все последующие записи игнорируются;

никакого сравнения записей на предмет соответствия большему или меньшему числу критериев, большего или меньшего соответствия шаблонам не производится.

Если соединение по указанному маршруту не может быть установлено, стороне-инициатору соединения посылается пакет CLEAR, и на этом обработка вызова заканчивается. Альтернативная маршрутизация в данной версии NSG не предусмотрена. Также не предусмотрена трансляция сетевых адресов X.25.

Для вывода таблицы маршрутизации X.25 используется команда display all или display config в меню (config-x25-route)# или любом вышестоящем меню. Для удаления маршрута используется команда:

x25 route del <номер>

Удаление маршрута производится только по его порядковому номеру. После удаления записи из середины таблицы все последующие сдвигаются на одну строку вверх, поэтому удалять несколько записей подряд следует в порядке убывания номеров, либо проверять текущий вид таблицы маршрутизации после каждого удаления.

В качестве критерия для маршрутизации пакета CALL может использоваться как точный вызываемый или вызывающий адрес X.121, так и шаблон адреса. Шаблон может содержать, помимо десятичных цифр, следующие подстановочные символы:

*	Любое число любых цифр, в том числе и их отсутствие
?	Любая одна цифра
[...]	Любая одна цифра из перечисленных в квадратных скобках

Подстановочные символы могут располагаться в шаблоне в любой позиции, любое число раз. Примеры шаблонов:

123	Подходят все адреса, содержащие фрагмент "123" в начале, середине или конце.
?123*	Подходит адрес 7123345, не подходят 12378 и 56123
123[45]678	Подходят адреса 1234678 и 1235678, не подходит 12345678

§3.8. Аутентификация пользователей

§3.8.1. Настройка локального списка пользователей

Список имен и паролей пользователей для аутентификации редактируется из меню (config-nsg)# с помощью следующих команд:

users user-name <имя> { open | xor | sha1 | md5 | exor | esha1 | emd5 } <пароль>

Создать пользователя и установить пароль для него. Пароль может вводиться и храниться в устройстве как в открытом, так и в зашифрованном виде:

- open — Пароль вводится и хранится в открытом виде.
- xor — Пароль вводится в открытом виде и шифруется с помощью алгоритма XOR. Данный метод не является стойким и позволяет однозначно восстановить пароль; он предназначен, в основном, для сокрытия пароля от просто любопытствующих глаз, которые могли бы подсмотреть конфигурацию "через плечо".
- sha1, md5 — Пароль вводится в открытом виде, но в устройстве сохраняется только его хэш, полученный по алгориму SHA–1 либо MD5, соответственно. Таким образом, восстановить пароль невозможно.
- exor — Далее вводится пароль, уже зашифрованный по алгоритму XOR.
- esha1, emd5 — Далее вводится не пароль, а его хэш по SHA–1 либо MD5, соответственно.

Последние три варианта предназначены для переноса существующей конфигурации на другое устройство. При выводе конфигурации командой write terminal пароли выводятся именно в таком виде, что позволяет без проблем загрузить сценарий конфигурации на новое устройство.

users user-name <имя> { open | xor | sha1 | md5 | exor | esha1 | emd5 } ""

Установить пустой пароль для данного пользователя. Способ ввода пароля в данном случае не имеет значения.

users no user-name <имя>

Удалить пользователя.

Пары "имя–пароль" создаются и уничтожаются одновременно для всех способов аутентификации. Список пользователей используется в следующих ситуациях:

— При аутентификации устройства NSG как клиента PPP, PPPoE, PPTP на удаленной системе.
— При аутентификации удаленных клиентов PPP, PPPoE, подключающихся к устройству NSG, если в шаблоне PPP-интерфейса указан способ аутентификации local.
— При аутентификации устройства NSG как клиента Dynamic DNS на удалённом сервере Dynamic DNS.
— При аутентификации пользователей, подключающихся к устройству NSG по Telnet, SSH, X.25 или через физический асинхронный порт, если для них включена аутентификация и указан способ local.

ВНИМАНИЕ Пароли, хранящиеся в формате sha1 или md5 возможно использовать только в последнем случае. Для аутентификации в сеансах PPP, PPPoE, PPTP и Dynamic DNS пароль должен храниться либо в открытом виде, либо в XOR.

ПРИМЕЧАНИЕ Для совместимости с предыдущими версиями допускается синтаксис, использованный в версиях NSG Linux 1.0 *build 1.1* и ранее:

```
username <имя> password <пароль>
no username <имя>
```

При вводе конфигурации эти строки автоматически преобразуются в новый синтакис.

Пароли для системных пользователей *root* и *nsg* устанавливаются таким же образом, однако имеют две особенности:

— Оба пароля хранятся в системе только в виде хэша по алгоритму MD5, т.е. в команде user-name допустимы только ключи md5 и emd5.

— Оба пароля хранятся отдельно от паролей остальных пользователей, поэтому после установки или изменения пароля можно удалить их из общего списка:

```
users no user-name nsg
users no user-name root
```

В этом случае пользователи *nsg* и *root* будут не видны в конфигурации, но они останутся в системе с паролями, установленными на этот момент.

§3.8.2. Группы пользователей

Для удобства администрирования пользователи могут быть объединены в группы. Например, все пользователи, входящие в определённую группу, могут иметь право доступа по Reverse Telnet к определённому физическому порту. Управление группами производится при помощи команд:

users user-group <имя>
users no user-group <имя>
Создание/настройка и удаление группы, соответственно.

Дальнейшая настройка производится в меню выбранной группы:

add-user <имя>
del-user <имя>
Включение указанного пользователя в текущую группу и его исключение, соответственно. Один и тот же пользователь может входить одновременно в несколько групп.
Если пользователь с указанным именем не существует, то он будет формально включён в группу, однако войти в систему с этим именем будет невозможно до тех пор, пока такой пользователь не будет создан.

§3.8.3. Настройка клиента RADIUS

Клиент RADIUS в данной версии NSG Linux позволяет производить аутентификацию, авторизацию и учет работы пользователей с помощью централизованного сервера при доступе по протоколу PPP и его производным (PPTP, PPPoE, PPTP). Управление клиентом RADIUS производится в меню (config-nsg)#.

radius Включение клиента RADIUS и переход в меню его настройки.

no radius Выключение клиента RADIUS. (Эквивалентно radius host 0.0.0.0 и установке остальных параметров в значения по умолчанию.)

Дальнейшая настройка производится в меню (confg-radius)#:

host <ip-адрес>
Определение IP-адреса удаленного сервера RADIUS.

auth-port <udp-port>
Номер порта UDP, используемого для аутентификации на сервере. Значение по умолчанию — 1812.

acct-port <udp-port>
Номер порта UDP, используемого для отсылки статистики на сервер. Значение по умолчанию — 1813.

key <строка>
Ключ для шифрования аутентификационной информации, используемый сервером и клиентом RADIUS. Значение параметра — строка символов, используемая для шифрования. Эта же строка должна быть задана в конфигурации сервера RADIUS для данного клиента. Строка не может содержать пробелы.

timeout <1...86400>
Время ожидания (в секундах) перед повторной передачей пакета, если на предыдущую посылку не получен ответ от сервера. Значение по умолчанию — 60.

retry <1...1000>
Количество повторных попыток аутентификации (в случае отсутствия ответов). Десятичное значение. Значение по умолчанию — 10. Если за указанное число попыток ответ от сервера не получен, клиенту будет отказано в подключении к устройству NSG.

ВНИМАНИЕ При аутентификации через RADIUS, если пользователь определил имя устройства (командой hostname), следует вручную установить соответствие указанного имени и одного из IP-адресов устройства. Для этого нужно добавить соответствующую строку в файл /etc/hosts.

§3.8.4. Настройка клиента TACACS+

Клиент TACACS+ в данной версии NSG Linux позволяет производить аутентификацию и авторизацию пользователей с помощью централизованного сервера при доступе к асинхронному порту по Reverse Telnet. Управление клиентом TACACS+ производится в меню (config-nsg)# с помощью команд:

authentication tacacs-server

Вход в меню настройки клиента TACACS+. Меню (config-authentication)# в данной версии NSG Linux содержит только его; клиент RADIUS будет перенесён в него в последующих версиях.

Меню (config-tacacs-server)# содержит следующие команды:

add <1...8> server <имя> key <ключ> port <0...65535> timeout <0...65535>

Добавление новых серверов для аутентификации. Всего клиент может использовать до 8 серверов. Первым параметром является порядковый номер сервера. Остальные имеют следующий смысл:

server <имя>	IP-адрес сервера или его имя (если включена служба DNS)
key <ключ>	Ключ для шифрования пакетов TACACS+
port <0...65535>	Номер порта TCP сервера; значение по умолчанию — 49
timeout <0...65535>	Время ожидания ответа от сервера, в секундах; значение по умолчанию — 5 сек.

Максимальная длина имени и ключа — по 127 символов.

delete <1...8>

Удаление существующего сервера из списка. При удалении сервера из середины списка нумерация оставшихся серверов сдвигается на единицу, так что они всегда будут пронумерованы подряд, начиная с единицы. При попытке создать сервер с номером, большим чем число существующих серверов плюс единица, он также получит следующий порядковый номер.

retry <1...16>

Число попыток обращения к каждому серверу.

Клиент TACACS+ последовательно посылает по одному запросу к каждому серверу, в порядке их нумерации. Если список исчерпан, а ответ не получен, то посылка запросов начинается снова с первого сервера, и повторится, в общей сложности, retry раз к каждому серверу. После первого ответа (положительного или отрицательного) от какого-либо сервера посылка запросов прекращается.

Пример:

```
authentication
    tacacs-server
        add 1 server "tac_plus_main_server" key "tackey" timeout 7
        add 2 server "tac_plus_reserv" key "xxx" port 3076 timeout 10
        retry 2
```

В данном случае сначала будет выдан запрос на сервер tac_plus_main_server. Если сервер не ответит в течении 7 секунд, запрос будет направлен на сервер tac_plus_reserv. Если он также не ответит в течение 10 секунд, процедура повторится ещё один раз.

ВНИМАНИЕ При аутентификации через TACACS+, если пользователь определил имя устройства (командой hostname), следует вручную установить соответствие указанного имени и одного из IP-адресов устройства. Для этого нужно добавить соответствующую строку в файл /etc/hosts.

ПРИМЕЧАНИЕ Меню tacacs-server описывает только параметры серверов. Собственно реквизиты для аутентификации (имена, пароли, группы) задаются в меню соответствующих служб или вводятся пользователем вручную.

§3.9. Просмотр состояния и статистики портов

Команда отображения статистики имеется в меню большинства сетевых устройств (в терминах Linux), присутствующих в системе, включая:

— физические порты
— виртуальные каналы Frame Relay
— виртуальные сети VLAN
— туннели IP-over-IP (GRE), IP-in-IP (Linux), IP-over-X.25, PPTP
— мосты Ethernet
— интерфейсы клиента PPPoE

Исключением в данной версии являются динамически создаваемые интерфейсы сервера PPPoE.

Формат команды:

show
show statistics checkpoint 0
: Вывод состояния, числа изменений состояния UP/DOWN, и текущей статистики объекта, начиная от момента старта устройства или данного объекта. Две вышеуказанные команды являются синонимами. Формат вывода частично варьируется в зависимости от типа объекта.
Для объектов, представляющих собой IP-интерфейсы, в статистике учитывается только IP-трафик. Для портов учитывается трафик канального уровня (в т.ч. заголовки канального уровня, пакеты *keepalive*, пакеты LCP и др.). Дополнительные байты физического уровня (бит-стаффинг и др.) в статистике не учитываются.

show statistics checkpoint <1..15> [set | unset]
: Вывод статистики относительно указанной контрольной точки. Опциональные команды set и unset устанавливают и удаляют контрольную точку, соответственно.
Нулевой точкой для сбора статистики, которая присутствует всегда, является момент старта устройства (или объекта). Помимо нее, для каждого объекта может быть установлено до 15 дополнительных контрольных точек.

show statistics checkpoint all unset
: Удаление всех установленных контрольных точек.