ADSL маршрутизатор / мост с интерфейсом 10/100Base-TX Ethernet NSG –200/A

Руководство пользователя

Версия программного обеспечения 1.38

Обновлено 21.01.2004

Москва 2004

СОДЕРЖАНИЕ

ВНИМАНИЕ При получении устройства необходимо проверить комплектацию и наличие заполненного гарантий-ного талона. Отсутствие гарантийного талона с отметкой организации-продавца является основанием для отказа в гарантийном обслуживании и технической поддержке со стороны ООО «NSGate».

1. Введение

1.1. Назначение и область применения устройства

NSG–200/A - абонентский маршрутизатор / мост для линий ADSL. Устройство предназначено для обеспечения корпоративным и индивидуальным пользователям доступа в Интернет и корпоративные сети.

NSG–200/A обеспечивает передачу данных по существующей кабельной сети ТФОП с сохранением имеющегося у абонента канала тональной частоты (ТЧ). При использования телефонной линии одновременно с передачей данных необходима установка внешнего частотного разделителя (сплиттера) для разделения телефонного трафики и данных; телефонный аппарат подключается к низкочастотному выходу сплиттера, устройство ADSL — к высокочастотному. Для подключения к ПК пользователя или локальной сети офиса устройство имеет один порт Ethernet 10/100Base-TX и может исполнять функции IP-маршрутизатора либо прозрачного моста.

На стороне оператора услуг используется ADSL коммутатор (ADSL DSLAM), например NSG-800/maxA, или коммутатор любых других производителей.

Программное обеспечение и конфигурация хранятся во внутренней флэш-памяти устройства и не требуют загрузки при включении питания Простая система управления на основе Web-интерфейса позволяет легко настроить устройство даже пользователю, не обладающему специальными знаниями в области сетевого администрирования..

1.2. Технические характеристики

ADSL

- Поддержка ADSL G.DMT (8,0/1,0 Мбит/с) согласно ITU-T G.992.1
- Поддержка ADSL G.Lite (1,5/0,5 Мбит/с) согласно ITU-T G.992.2

ATM

- Multi-protocol over AAL5 (RFC 1483)
- Classic IP-over-ATM (RFC 1577, RFC 1483)
- PPPoA (RFC 2364)
- PPPoE (RFC 2516)
- Формат ячеек ATM ITU–T I.361
- ATM Forum UNI 3.1/4.0
- Поддержка до 8 ATM VCC (Virtual Circuit Connection) на каждом порту
- Поддержка UBR

Сетевые протоколы

- RIP1 (RFC 1058), RIP2 (RFC 1389),
- Статическая маршрутизация
- TFTP клиент и сервер
- HTTP
- DHCP сервер и ретранслятор
- NAT (RFC 1631)
- Фильтрация IP-пакетов
- Режим прозрачного моста

Общесистемные характеристики

- Автоматическая перезагрузка после сбоя питания
- Автоматическое установление соединений после сбоя питания
- Управление и мониторинг с помощью Web-интерфейса
- Удаленное обновление встроенного программного обеспечения по HTTP

Аппаратные характеристики

- Один порт ADSL (RJ–11)

- Один порт Ethernet 10/ 100 BaseT (RJ–45)
- Светодиодные индикаторы состояния устройства
- Габариты: 129×146×29 мм (ш×г×в)
- Вес: 0,270 кг
- Энергопитание: —7,5 В
- Макс. потребляемая мощность: 5 Вт

Условия эксплуатации

- Температура 5…50°C
- Влажность не более 95% без конденсации

1.3. Внешний вид устройства

Передняя панель

На передней панели устройства NSG–200/A расположены 4 светодиодных индикатора:

PWR зеленый светодиод, светится непрерывно при наличии питания;
LAN зеленый светодиод, светится при наличии соединения с сетью Ethernet, мигает при приеме/передаче данных через порт Ethernet;
WAN зеленый светодиод, светится непрерывно при наличии соединения с удаленным узлом доступа;
DIAG желтый светодиод, мигает в процессе загрузки устройства и установления соединения. После выключения светодиода устройство готово к работе.

Задняя панель

На задней панели устройства расположены три разъема:

LAN порт Ethernet 10/100Base-TX (RJ–45) для подключения локальной сети или ПК пользователя.
PWR разъем питания постоянного тока (7,5 В, 1000 мА)
ADSL разъем RJ–11 для подключения к линии ADSL

Кроме того, на задней панели расположена защищенная кнопка Reset, которую следует использовать лишь в исключительных случаях. При нажатии этой кнопки происходит удаление всех настроек, выполненных пользователем, и перезагрузка устройства с заводской конфигурацией.

2. Включение и подготовка к работе

2.1. Системные требования

Для использования NSG–200/A необходимы следующие аппаратные, программные средства и установочные параметры:

- Линия ADSL (обычная телефонная линия, подключенная к мультиплексору доступа ADSL на стороне оператора)
- Локальная сеть Ethernet, либо персональный компьютер с сетевым адаптером Ethernet 10/100Base-TX
- Поддержка протокола TCP/IP на пользовательском компьютере (компьютерах)
- Обязательные параметры, предоставляемые поставщиком услуг Интернет:
  IP-адрес
  Маска подсети
  Адрес шлюза по умолчанию
- Дополнительные параметры, предоставляемые поставщиком услуг Интернет в случае необходимости:
  Идентификатор VPI/VCI
  Имя и пароль пользователя PPP
  Адрес DNS
- Web-броузер (рекомендуется MSIE 5.0 и старше)

ВНИМАНИЕ При непосредственном подключении к ПК через порт Ethernet IP-адрес ПК должен находиться в диапазоне, определенном адресом NSG–200/A и маской подсети. При подключении через локальную сеть Ethernet IP-адрес и маска должны быть предварительно установлены на NSG–200/A в соответствии с фактической конфигурацией сети.

По умолчанию NSG–200/A имеет IP-адрес 192.168.1.1 и маску 255.255.255.0. Кроме того, устройство поставляется с включенным сервером DHCP, поэтому при непосредственном подключении ПК к устройству вместо ручной конфигурации IP-адреса и маски на ПК можно включить на нем клиента DHCP. (Опция "IP-адреса назначаются сервером" в конфигурации протокола TCP/IP для Windows.)

2.2. Подключение устройства

1. Подключить порт Ethernet к коммутатору или концентратору локальной сети при помощи кабеля “Straight RJ–45“, либо непосредственно к абонентскому ПК при помощи кабеля “Crossover RJ–45“.
2. При использовании линии ADSL для одновременной передачи голоса и данных подключить разъем LINE частотного разделителя (сплиттера) к линии и подключить телефонный аппарат к гнезду PHONE сплиттера.
3. Подключить порт ADSL к абонентской линии (без использования телефона), либо к гнезду DSL сплиттера (при одновременной передаче голоса и данных).
4. Включить устройство и дождаться окончания загрузки. Убедиться в наличии соединения с NSG–200/A при помощи команды *ping*.

2.3. Вход в систему

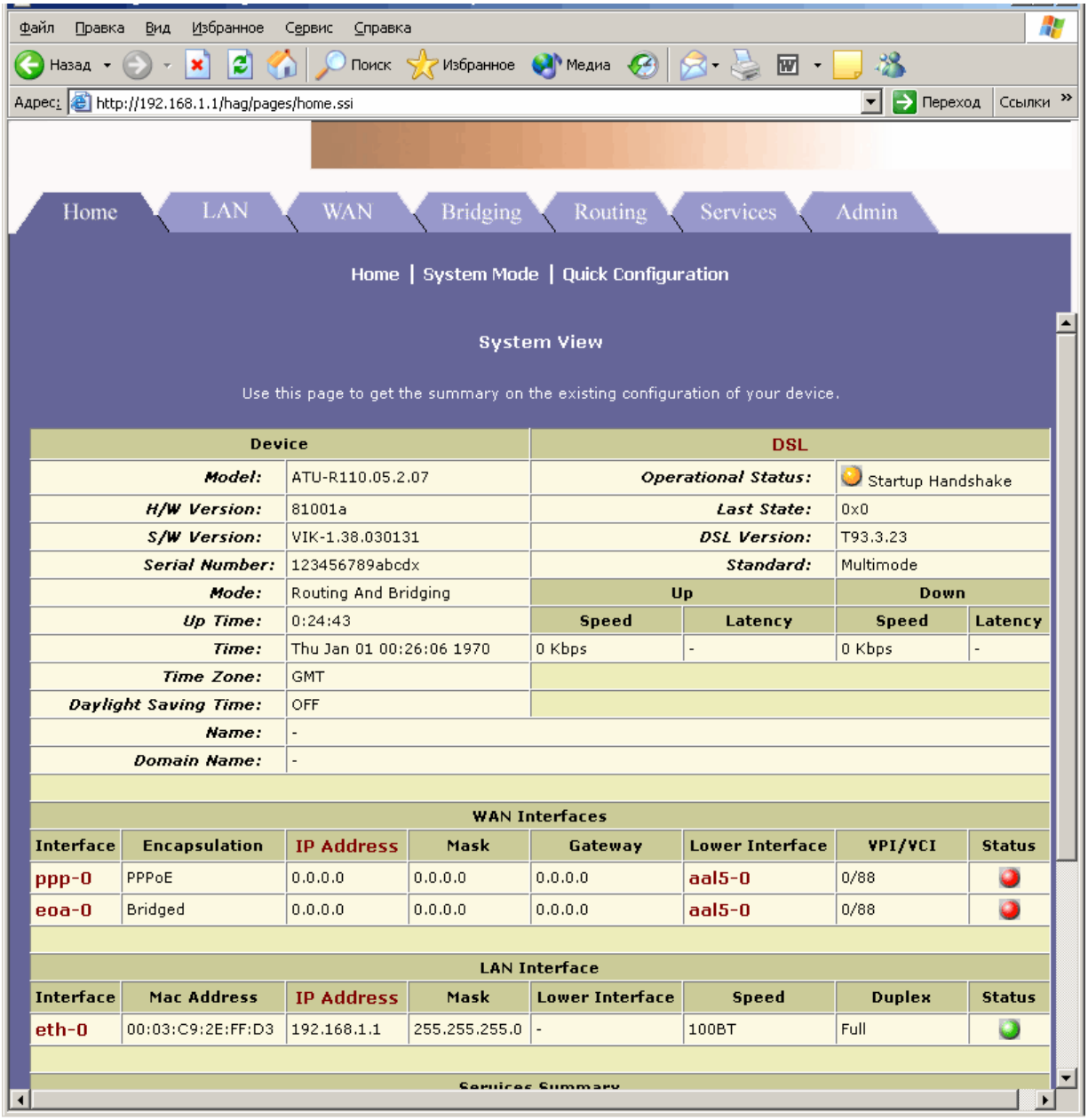
Ввести в адресной строке Web-броузера IP-адрес устройства NSG–200/A. По умолчанию устройство имеет адрес 192.168.1.1.

После этого появится окно входа в систему.

При первом входе в систему следует ввести имя пользователя **root** и пароль **root**, установленные по умолчанию, и нажать на кнопку OK. Впоследствии можно устанавливать и изменять пароль.

Если аутентификация прошла успешно, на экране появится основное управляющее окно.

3. Общие параметры системы — панель Home



3.1. Web-интерфейс устройства

Web-интерфейс устройства NSG–200/A оформлен в виде семи панелей, представляющих различные категории параметров. Все панели, кроме Home, содержат по несколько страниц, относящихся к более частным разделам конфигурации. Некоторые параметры представлены одновременно на нескольких панелях, например, IP-адрес интерфейса Ethernet содержится как на панели LAN (конфигурация локальной сети), так и на панели Routing (настройка таблиц маршрутизации).

На всех панелях Web-интерфейса используются следующие единообразные кнопки:

Submit	Передать в устройство все параметры, введенные пользователем на данной странице. Переданные параметры вступают в силу и действуют временно, до следующей перезагрузки устройства. Подробнее о процедуре сохранения конфигурации см. п.3.3.
Refresh	Перезагрузить текущую страницу с обновленными значениями статистики.
Clear	Обнулить счетчики статистики
Help	Вывести справку об использовании Web-интерфейса

3.2. Просмотр параметров системы

Заглавная страница Web-интерфейса System View содержит сводную информацию о состоянии различных компонент системы. Страница состоит из четырех разделов:

Device	Информация о версиях программной и аппаратной частей устройства, системном времени и другие общесистемные параметры.
DSL	Информация о состоянии физического соединения ADSL.
WAN Interfaces	Конфигурация виртуальных интерфейсов WAN. Поскольку все данные в линии инкапсулируются в ячейки ATM, в одной физической линии может быть образовано несколько виртуальных соединений (до 8), каждое из которых связано с определенным виртуальным интерфейсом. В частности, различные ATM-соединения могут использоваться для подключения к различным поставщикам услуг Интернет через одного оператора DSL, для передачи разнородного трафика (пакетного голоса и данных) и т.п.
LAN interface	Конфигурация интерфейса Ethernet для локальной сети.
Services Summary	Конфигурация различных дополнительных сервисов, предоставляемых устройством: NAT, фильтрации пакетов, RIP, DHCP, IGMP.

Ссылки, расположенные в этих разделах, приводят на страницы настройки соответствующих параметров, расположенные в разделах LAN, WAN, Routing, Bridging, Services. Сама по себе данная страница не предусматривает никаких изменений конфигурации.

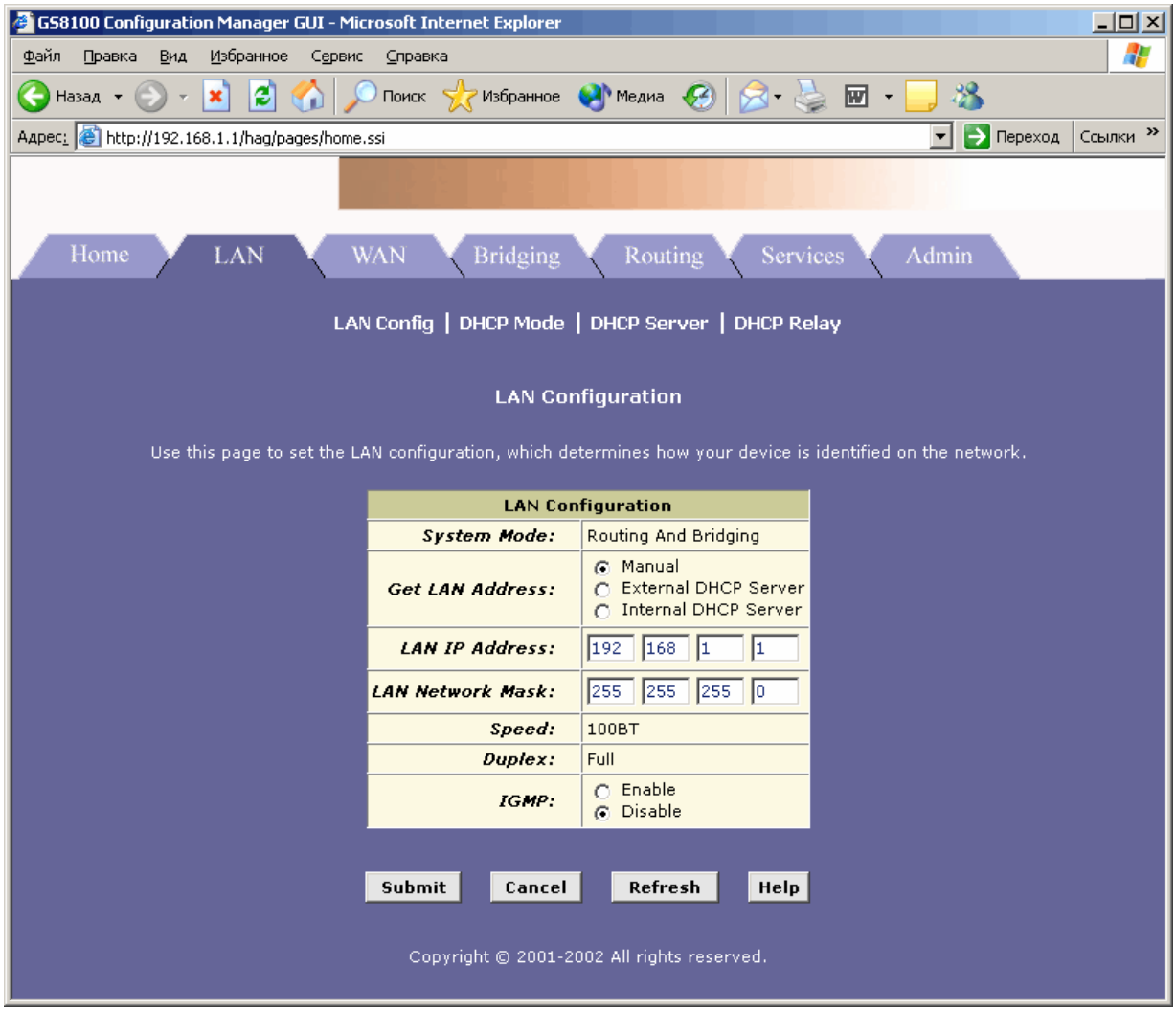
Кнопка Modify предназначена для изменения общесистемных параметров: даты и времени, часового пояса, перехода на летнее время (DST), имени узла и домена. Настройки производятся в отдельном окне. После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

ВНИМАНИЕ	После завершения настройки необходимо сохранить полученную конфигурацию в энергонезависимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

3.3. Быстрая настройка системы

Для быстрого доступа к ключевым параметрам конфигурации системы предназначена страница Quick Configuration. На данной странице можно настроить параметры ATM-интерфейсов WAN, службу DNS и реквизиты пользователя для подключения по протоколам PPP-over-something.

4. Параметры локальной сети — панель LAN



4.1. Настройка интерфейса LAN

Настройка интерфейса LAN производится на странице LAN Configuration и состоит в назначении ему IP-адреса и маски подсети и/или выборе способа их назначения. IP-адрес и маска являются обязательными для работы в режиме маршрутизатора; при работе всех ATM-интерфейсов в режиме моста они требуются только для доступа к конфигурации самого устройства и не влияют на передачу данных. Подробнее см. разделы Routing, Bridging. Текущий режим работы устройства показывается в первой строке таблицы.

Назначение IP-адреса и маски порту LAN может производиться одним из трех способов:

- Вручную — адрес и маска устройства вводятся пользователем в соответствующих полях данного окна и являются фиксированными.
- От внешнего сервера DHCP, расположенного в глобальной сети (например, в сети поставщика услуг Интернет).
- От внутреннего сервера DHCP, расположенного в локальной сети.

В двух последних случаях устройство NSG–200/A является клиентом внешнего или внутреннего сервера DHCP. При этом поле маски подсети становится недоступным, но в поле IP-адреса по-прежнему может быть введен адрес, который в данном случае является желательным. Устройство запрашивает этот адрес у сервера, и если он входит в пул адресов данного сервера и свободен, то получает именно этот адрес. В противном случае сервер назначает иной адрес, который, однако, не будет показан на данной странице.

Статический IP-адрес необходимо использовать практически всегда, когда устройство NSG–200 является маршрутизатором для выхода из локальной сети в глобальную, поскольку его адрес должен быть указан в конфигурации всех локальных компьютеров в качестве шлюза по умолчанию. Исключением является только ситуация, когда шлюзом по умолчанию является другой маршрутизатор с фиксированным IP-адресом, использующий протокол RIP для динамического формирования таблицы маршрутизации.

Статический IP-адрес необходим также, если устройство NSG–200/A само является сервером DHCP для локальной сети, либо осуществляет трансляцию сетевых адресов (NAT). Установленные адрес и маска должны быть учтены при настройке этих служб.

После ввода требуемых параметров следует нажать кнопку Submit.

После изменения статического IP-адреса устройство разрывает текущее соединение с управляющим ПК. Если был выбран режим клиента DHCP, то устройство запрашивает новый адрес и если он отличается от прежнего, также разрывает соединение. Необходимо изменить IP-адрес и маску ПК соответствующим образом и восстановить подключение к устройству.

ВНИМАНИЕ До повторного входа в систему устройство NSG–200/A не должно отключаться от источника питания или перезагружаться. После входа в систему необходимо сохранить полученную конфигурацию в энергонезависимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

4.2. Выбор служб DHCP

Устройство NSG–200/A может само являться сервером или ретранслятором DHCP для компьютеров локальной сети. В первом случае оно назначает локальным компьютерам IP-адреса и другие параметры согласно заданной конфигурации. Во втором случае оно передает запросы клиентов DHCP на указанный сервер во внешней сети (например, в сети поставщика услуг Интернет) и возвращает клиентам ответы сервера.

Настройка служб DHCP производится на странице DHCP Mode панели LAN. После выбора режима работы службы DHCP необходимо нажать кнопку Submit.

ПРИМЕЧАНИЕ Службы DHCP Server и DHCP Relay позволяют назначать IP-адреса и другие параметры компьютерам в локальной сети, однако никак не влияют на IP-адрес порта Ethernet самого устройства NSG–200/A. Параметры сервера и ретранслятора DHCP сохраняются при отключении этих служб. Будучи единожды настроенными, эти службы могут быть в любой момент выключены и позже активированы снова с прежними параметрами.

4.3. Настройка сервера DHCP

Настройка сервера DHCP производится на странице DHCP Server панели LAN. По умолчанию, в для сервера определен один пул адресов с минимальным набором параметров. Три иконки в правой части таблицы позволяют изменять основные параметры пула (в данном случае — исключать некоторые адреса и устанавливать имя домена), просматривать список всех его параметров, или удалять пул. Устройство NSG–200/A поддерживает до двух пулов IP-адресов.

Для создания нового пула адресов используется кнопка Add. Она открывает окно, в котором следует ввести параметры пула. Обязательными являются поля Start IP Address, End IP Address, Netmask и Gateway Address. Имя домена (пула) вводится для удобства администрирования и не влияет на работу сервера. Поле MAC Address используется для того, чтобы всегда назначать компьютеру с данным MAC-адресом сетевого адаптера фиксированный IP-адрес. В этом случае значения полей Start IP Address и End IP Address должны совпадать, т.е. пул состоит из одного адреса. Остальные поля (адреса различных серверов) являются необязательными. После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

Для просмотра текущего списка используемых адресов необходимо нажать кнопку Address Table.

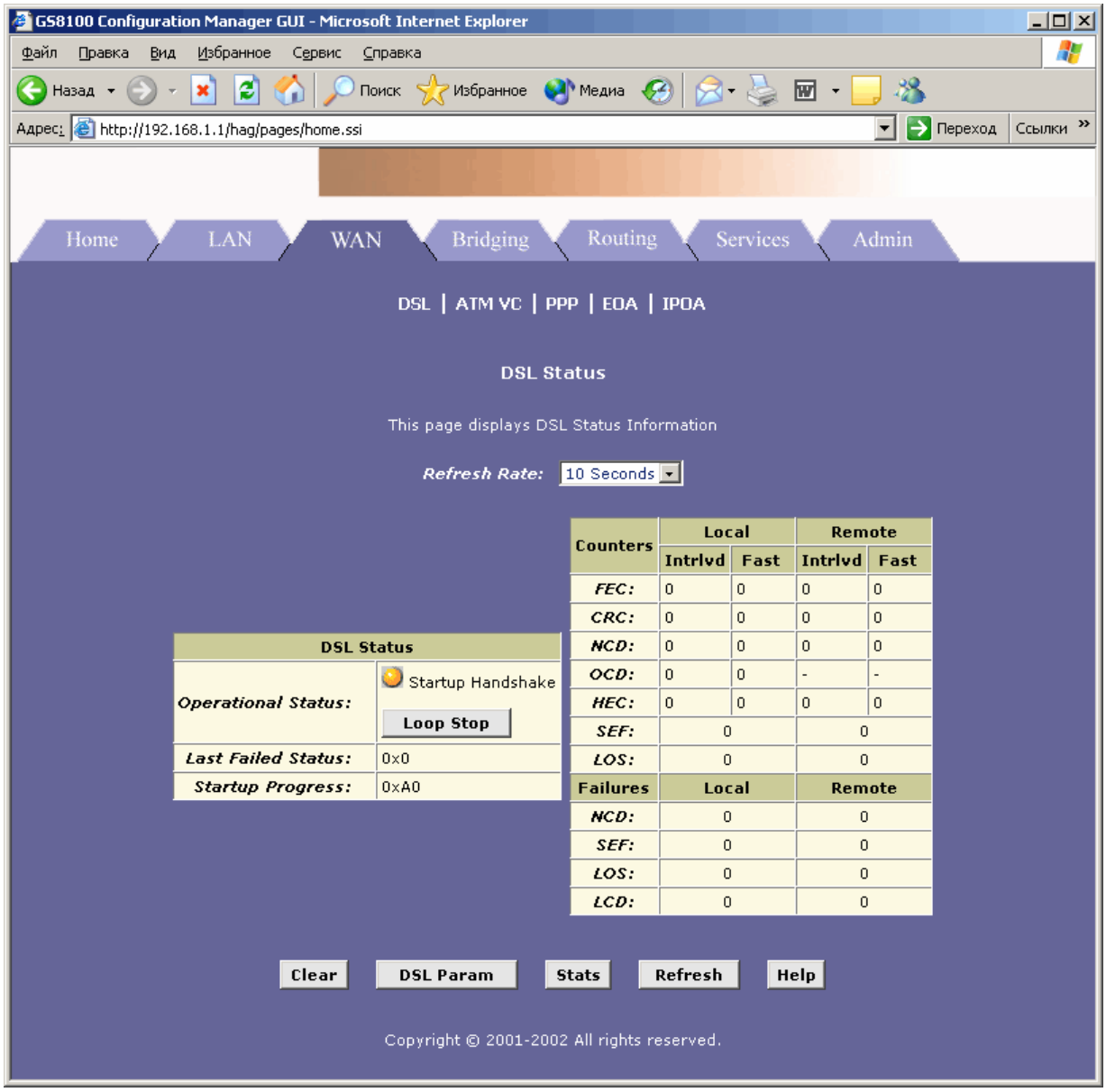
4.4. Настройка ретранслятора DHCP

Настройка ретранслятора DHCP производится на странице DHCP Relay панели LAN. Необходимо ввести адрес сервера DHCP, к которому будут направляться запросы, и выбрать интерфейсы, на которых будет работать ретранслятор. (После выбора интерфейса из списка необходимо нажать кнопку Add.) Запросы клиентов DHCP, поступающие со стороны этого интерфейса (-ов), будут передаваться на указанный сервер, а ответы сервера — возвращаться на исходный интерфейс. Как правило, ретранслятор DHCP обслуживает локальную сеть, т.е. интерфейс eth-0, а сервер DHCP предоставляется поставщиком услуг Интернет и расположен во внешней сети.

После ввода требуемых параметров следует нажать кнопку Submit.

ВНИМАНИЕ После завершения настройки необходимо сохранить полученную конфигурацию в энергонезависимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

5. Транспорт и интерфейсы глобальной сети — панель WAN



Для передачи по любой сети пакеты IP должны быть упакованы (инкапсулированы) в пакеты какого-нибудь протокола канального, а затем физического уровня. Со стороны локальной сети эту роль выполняет протокол Ethernet.

Все данные, передаваемые по линии ADSL, помещаются в ячейки ATM, которые образуют несколько независимых потоков — виртуальных каналов. Достоинство такого метода состоит в том, что в одной физической линии может существовать несколько виртуальных каналов. Например, они могут соединять пользователя с несколькими различными поставщиками услуг Интернет через одного оператора DSL и сеть ATM. Или же один канал может использоваться для передачи данных, а другой — для пакетов IP-телефонии, с разными показателями времени задержки, гарантиями доставки пакетов и т.п. Сложность же, помимо самой процедуры инкапсуляции, состоит в том, что протокол ATM не является "родным" для IP и требует специальных преобразований, которые описаны спецификацией AAL5 (ATM Adaptation Level 5).

Кроме того, оператору ADSL может быть желательно получить на своей стороне пользовательский IP-трафик уже упакованным в некоторый протокол канального уровня, соответствующий архитектуре его сети. Например, для передачи IP-пакетов по локальной сети оператора они должны быть упакованы в пакеты Ethernet, для надежной аутентификации пользователя — предпочтителен протокол PPP, причем не исключено, что одновременно требуется то и другое. По этой причине в системах ADSL используется целый набор различных способов инкапсуляции, включая:

- IP-over-ATM (RFC 1577) -over-ADSL
- IP-over- Ethernet-over-ATM (RFC 1483) -over-ADSL

- IP-over-PPP-over-ATM-over-ADSL
- IP-over-PPP-over-Ethernet-over-ATM-over-ADSL

Устройство NSG–200/A поддерживает все четыре способа. Назначение параметров виртуальных соединений ATM, выбор требуемого режима инкапсуляции и его параметров определяется исключительно оператором сети ADSL и должно производиться согласованным образом на обеих сторонах соединения. На абонентской стороне следует установить конфигурацию, предписанную оператором.

5.1. Физический уровень соединений ADSL

Статистика работы физического уровня ADSL представлена на странице DSL Status панели WAN. Никаких дополнительных настроек на данном уровне не предусмотрено, приемник и передатчик устройства работают в автоматическом режиме и самостоятельно согласуют параметры передачи со станционной стороной. Пользователь может только изменить период обновления статистики.

Счетчики ошибок, представленные на данной странице, позволяют судить об устойчивости работы соединения, но не предназначены для непосредственного реагирования со стороны пользователя. Они могут представлять интерес для оператора в случае возникновения проблем с качеством приема-передачи на физическом уровне.

Более подробную информацию о настройках соединения ADSL можно получить при помощи кнопки DSL Param. Полную статистику можно получить при помощи кнопки Stats. В окне статистики выводятся данные за текущий 15-минутный интервал. Кроме того, устройство хранит статистику за последние 24 часа разбитую на страницы по 4 часа (16 интервалов). Эти страницы доступны по ссылкам в нижней части страницы статистики.

5.2. Виртуальные соединения ATM

Настройка виртуальных соединений ATM производится на странице ATM VC Configuration панели WAN. Устройство поддерживает до восьми виртуальных соединений, определяемых номерами VPI/VCI и оканчивающихся интерфейсами aal5–0...aal5–7. Именно на эти интерфейсы должен направляться трафик вышестоящих протоколов — IP, PPP или Ethernet. Кроме того, каждое соединение характеризуется способом мультиплексирования различных протоколов, которые могут по нему передаваться: LLC (несколько различных протоколов в одном соединении) или MUX (отдельное соединение для каждого протокола).

Иконки в правой части таблицы позволяют изменять и удалять существующие соединения, а кнопка Add — добавлять новые. Номера VPI/VCI, тип мультиплексирования LLC/MUX и максимальное число протоколов в соединениях типа LLC должны быть установлены согласно указаниям оператора.

После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

ПРИМЕЧАНИЕ Тип мультиплексирования не может быть изменен, если через данный интерфейс установлено виртуальное соединение с оператором. В этом случае необходимо удалить интерфейс и создать его заново с требуемым типом.

5.3. Интерфейсы IP-over-ATM

Если оператор ADSL использует инкапсуляцию IP-over-ATM (IPoA), то настойка соответствующих интерфейсов производится на странице IPoA Configuration панели WAN. Для изменения параметров и удаления существующих интерфейсов используются иконки в правой части таблицы, для добавления новых — кнопка Add. Интерфейс IPoA характеризуется следующими параметрами:

Interface — Имя интерфейса (ipoa-0...ipoa-7)

Lower interface — Интерфейс AAL5, обслуживающий данный IP-интерфейс типа IPoA. При создании нового интерфейса IPoA следует в первую очередь выбрать имя одного из существующих интерфейсов AAL5 и нажать кнопку Add, и только затем конфигурировать другие параметры.

Configured IP address
Netmask — IP-адрес и маска подсети для данного интерфейса (по указанию оператора).

IPF Type — Классификация интерфейса с точки зрения применения к нему правил фильтрации пакетов и защиты от сетевых атак:

- public — интерфейс подключен к сети общего пользования и требует наиболее жестких правил фильтрации;
- private — интерфейс подключен к корпоративной сети, к нему применяются наименее жесткие правила
- DMZ (Demilitarized Zone) — интерфейс подключен к сегменту корпоративной сети, открытому для доступа из сети общего пользования (например, в нем установлены Web- и FTP-сервер компании. К пакетам, поступающим на

данный интерфейс — как со стороны LAN, так и из Интернет — применяется промежуточный набор правил.

Подробнее о средствах защиты сети см. раздел "Настройка брандмауэра".

IPoA Type — Соответствие стандарту RFC 1577 (по указанию оператора).

Default Route — Следует ли определить данный интерфейс в качестве маршрута по умолчанию. Подробнее о конфигурации маршрутов см. раздел "Таблица маршрутизации".

Gateway IP Address — IP-адрес шлюза по умолчанию для данного интерфейса (по указанию оператора), если он определен в качестве маршрута по умолчанию.

После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

5.4. Интерфейсы Ethernet-over-ATM

Если оператор ADSL использует инкапсуляцию Ethernet-over-ATM (EoA), то настойка соответствующих интерфейсов производится на странице RFC1483/Ethernet over ATM (EoA) Configuration панели WAN. Для изменения параметров и удаления существующих интерфейсов используются иконки в правой части таблицы, для добавления новых — кнопка Add. Интерфейс EoA характеризуется следующими параметрами:

Interface — Имя интерфейса (eoa-0...eoa-7)

Lower interface — Интерфейс AAL5, обслуживающий данный интерфейс Ethernet-over-ATM.

Configured IP address
Netmask — IP-адрес и маска подсети для данного интерфейса (по указанию оператора).

IPF Type — Классификация интерфейса с точки зрения применения к нему правил фильтрации пакетов и защиты от сетевых атак:

- public — интерфейс подключен к сети общего пользования и требует наиболее жестких правил фильтрации;
- private — интерфейс подключен к корпоративной сети, к нему применяются наименее жесткие правила
- DMZ (Demilitarized Zone) — интерфейс подключен к сегменту корпоративной сети, открытому для доступа из сети общего пользования (например, в нем установлены Web- и FTP-сервер компании. К пакетам, поступающим на данный интерфейс — как со стороны LAN, так и из Интернет — применяется промежуточный набор правил.

Подробнее о средствах защиты сети см. раздел "Настройка брандмауэра".

Use DHCP — Использование клиента DHCP для данного интерфейса. Если клиент включен, то IP-адрес, маска подсети и шлюз по умолчанию для данного интерфейса назначаются сервером оператора.

Default Route — Следует ли определить данный интерфейс в качестве маршрута по умолчанию. Подробнее о конфигурации маршрутов см. раздел "Таблица маршрутизации".

Gateway IP Address — IP-адрес шлюза по умолчанию для данного интерфейса (по указанию оператора), если он определен в качестве маршрута по умолчанию.

После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

Интерфейс Ethernet-over-ATM может использоваться как для передачи маршрутизируемого IP-трафика, так и для работы в режиме моста, в зависимости от конфигурации сети оператора.

ПРИМЕЧАНИЕ — Если подключение к оператору осуществляется по протоколу PPP-over-Ethernet (PPPoE), отдельная конфигурация интерфейса EoA не требуется. Вместо него используется интерфейс PPPoE.

5.5. Интерфейсы PPP-over-ATM

Многие операторы ADSL используют инкапсуляцию PPP-over-ATM (PPPoA) либо PPP-over-Ethernet (PPPoE) - over-ATM для решения целого ряда задач, а именно:

- Аутентификации пользователя с помощью имени и пароля
- Авторизации пользователя, т.е. определения круга предоставляемых ему услуг
- Передачи пользователю параметров и настроек IP-сети

Если оператор использует инкапсуляцию PPPoE или PPPoA, то настойка соответствующих интерфейсов производится на странице PPP Configuration панели WAN. Для просмотра, изменения параметров и удаления

существующих интерфейсов используются иконки в правой части таблицы, для добавления новых — кнопка Add. Интерфейсы PPP характеризуются следующими параметрами:

Interface — Имя интерфейса (ppp-0...ppp-23). Использовать несколько интерфейсов PPP для соединения с одним поставщиком услуг Internet возможно только в случае, если это интерфейс типа PPPoA. Соединения PPPoE допускают только один интерфейс.

ATM VCC — Интерфейс AAL5, обслуживающий данный интерфейс PPP-over-ATM.

IPF Type — Классификация интерфейса с точки зрения применения к нему правил фильтрации пакетов и защиты от сетевых атак:
- public — интерфейс подключен к сети общего пользования и требует наиболее жестких правил фильтрации;
- private — интерфейс подключен к корпоративной сети, к нему применяются наименее жесткие правила
- DMZ (Demilitarized Zone) — интерфейс подключен к сегменту корпоративной сети, открытому для доступа из сети общего пользования (например, в нем установлены Web- и FTP-сервер компании. К пакетам, поступающим на данный интерфейс — как со стороны LAN, так и из Интернет — применяется промежуточный набор правил.

Подробнее о средствах защиты сети см. раздел "Настройка брандмауэра".

Status — Административный статус интерфейса:
- Start — интерфейс начинает работу при включении питания устройства
- Stop — интерфейс существует, но не активен
- StartOnData — интерфейс начинает работу при появлении данных для передачи.

Protocol — PPPoA либо PPPoE.

Service Name — Название услуги оператора (для удобства пользователя). Например, один оператор может предоставлять разные услуги для обычного просмотра Web-страниц и для деловых коммуникаций, доступ к которым предоставляется с разными именами и паролями.

Use DHCP — Использование клиента DHCP для данного интерфейса. Протокол PPP сам по себе предусматривает получение IP-адреса, маски подсети, адресов шлюза по умолчанию и сервера DNS от оператора. Клиент DHCP в данном случае позволяет дополнительно получить адреса ряда дополнительных прикладных серверов.

Use DNS — Выбор адресов DNS, распространяемых встроенным сервером DHCP для компьютеров локальной сети. Если данная опция включена, используются адреса DNS, полученные от оператора в ходе установления PPP-соединения; если выключена — адреса, заданные в настройках сервера DHCP. При выключенном сервере DHCP опция игнорируется. Подробнее о настройке сервера DHCP см. раздел "Параметры локальной сети".

Default Route — Следует ли определить данный интерфейс в качестве маршрута по умолчанию. Подробнее о конфигурации маршрутов см. раздел "Таблица маршрутизации".

Security Protocol — Протокол аутентификации: PAP либо CHAP.

Login Name
Password — Имя пользователя и пароль для доступа в сеть оператора.

После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

Текущие параметры интерфейсов PPP, в том числе адреса и другие параметры, динамически назначаемые операторами, можно просмотреть на странице PPP Configuration панели WAN. Помимо этого, на данной странице можно установить тайм-аут для разрыва соединения при длительной неактивности соединения (в минутах). Если при этом включена опция Ignore WAN to LAN traffic, активность соединения определяется только по передаче данных от пользователя в глобальную сеть; это позволяет игнорировать случайный нисходящий трафик (широковещательные пакеты, запросы ICMP, попытки сканирования портов блуждающими хакерами и т.п.), способный поддерживать видимую активность неограниченно долгое время. После ввода требуемых параметров следует нажать кнопку Submit.

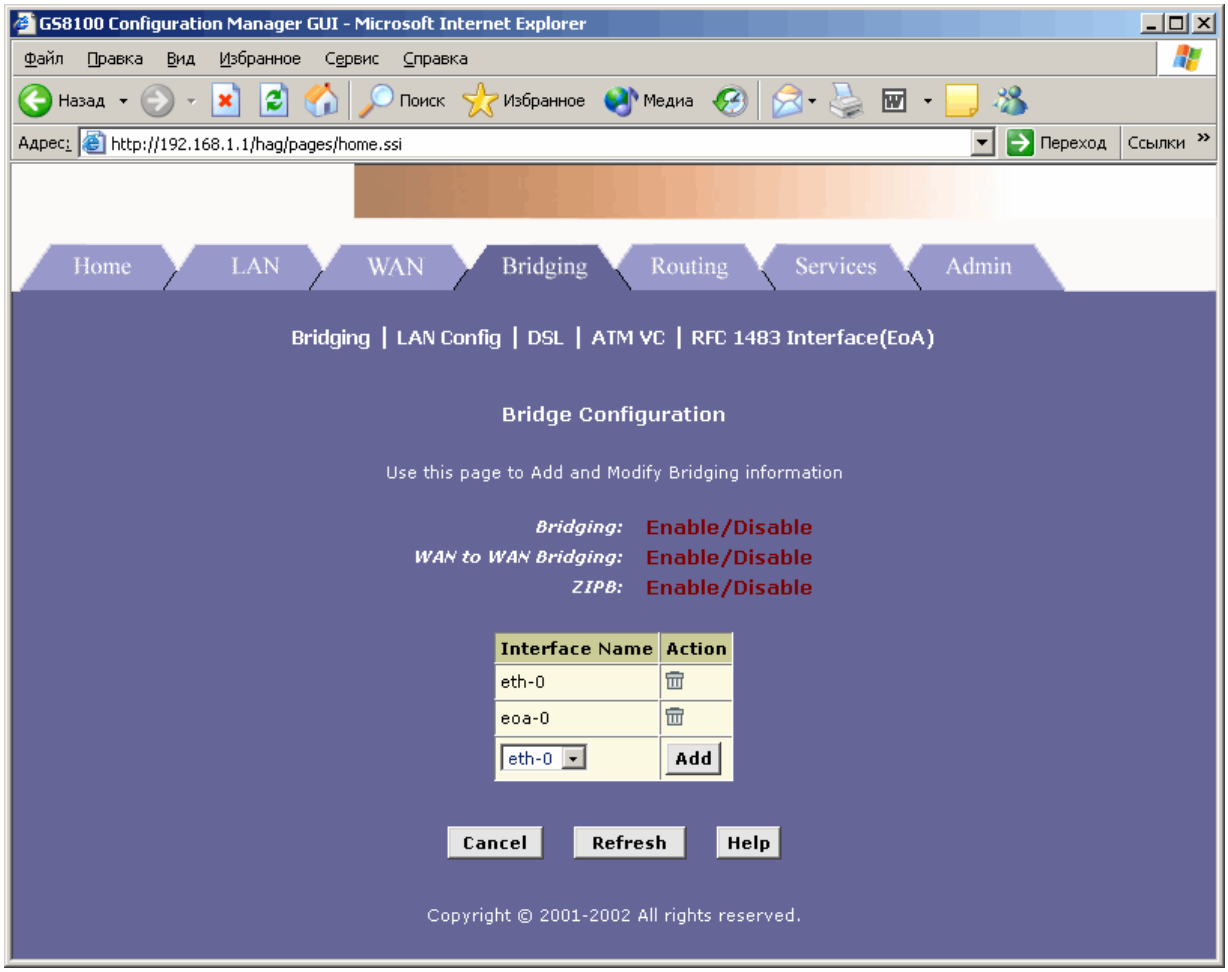
Полный перечень параметров интерфейса можно просмотреть, если нажать на иконку "Свойства" (в виде указующего перста). Помимо вышеперечисленных параметров и за исключением пароля, в этом окне выводится текущее состояние PPP-соединения (Oper. Status) и причина последнего разъединения:

- VC down — отсутствие ATM-соединения. Рекомендуется проверить конфигурацию на страницах PPP и ATM VC, а также выполнить тестирование соединения на странице Diagnostics панели Admin.
- No Valid PADO Recvd — устройство инициировало установление PPP-соединения, но не получило ответа от оператора. Рекомендуется проверить статистику ошибок на странице DSL. При необычно большом числе ошибок проверить целостность линии или обратиться к оператору.

- No Valid PADS Recvd — после начального согласования пареметров PPP-соединения устройство не получило подтверждения от оператора. Рекомендуется проверить статистику ошибок на странице DSL. При необычно большом числе ошибок проверить целостность линии или обратиться к оператору.
- Auth Failure — ошибка аутентификации пользователя. Рекомендуется проверить, в первую очередь, соблюдение регистра и положение клавиатуры РУС/ЛАТ при вводе пароля.
- No Activity — соединение разорвано по тайм-ауту из-за неактивности пользователя.
- Stopped by User — соединение разорвано по инициативе пользователя (например, путем установки статуса интерфейса в значение Stop).
- PATD Received — от оператора получен специальный пакет, требующий разорвать соединение. Если восстановить соединение не удается, рекомендуется проверить, в первую очередь, баланс личного счета у оператора и соблюдение правил пользования услугами. (Участие в спаме, хакерской деятельности и т.п. легко отслеживается и блокируется штатными средствами оператора, что и проявляется указанным образом).
- Intrenal Failure — сбой в работе программного обеспечения NSG–200/A.

ВНИМАНИЕ После завершения настройки необходимо сохранить полученную конфигурацию в энерго-независимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

6. Работа в режиме моста — панель Bridging



Устройство NSG–200/A может использоваться в качестве моста и в качестве маршрутизатора, а также в обоих режимах одновременно. Как правило, применяется режим маршрутизатора, однако возможны ситуации, в которых требуется именно режим моста:

- Если сеть оператора построена таким образом, что предполагает рассматривать интерфейс его IP-маршрутизатора и все компьютеры локальной сети абонента как одну подсеть IP.
- Если в сети используются иные протоколы третьего уровня, помимо IP — например, IPX или AppleTalk.

Для работы в режиме моста необходимы, как минимум, два интерфейса Ethernet . Как правило, это интерфейс eth–0 локальной сети и один из интерфейсов eoa–N глобальной сети, привязанный к некоторому виртуальному соединению ATM. Если интерфейсу моста (например, eth–0) назначен IP-адрес, то считается, что на нем следует использовать маршрутизацию пакетов IP. При этом, однако, интерфейс работает как мост для остальных протоколов.

Настройка режима моста производится на странице Bridging панели Bridging и состоит в выборе интерфейсов, для которых он будет применяться. Интерфейсы Ethernet-over-ATM должны быть предварительно созданы и сконфигурированы на странице EoA. Для добавления интерфейсов в список необходимо выбрать их из выпадающего меню и нажать кнопку Add. Для удаления интерфейсов из состава моста следует нажать иконку в виде мусорной корзины.

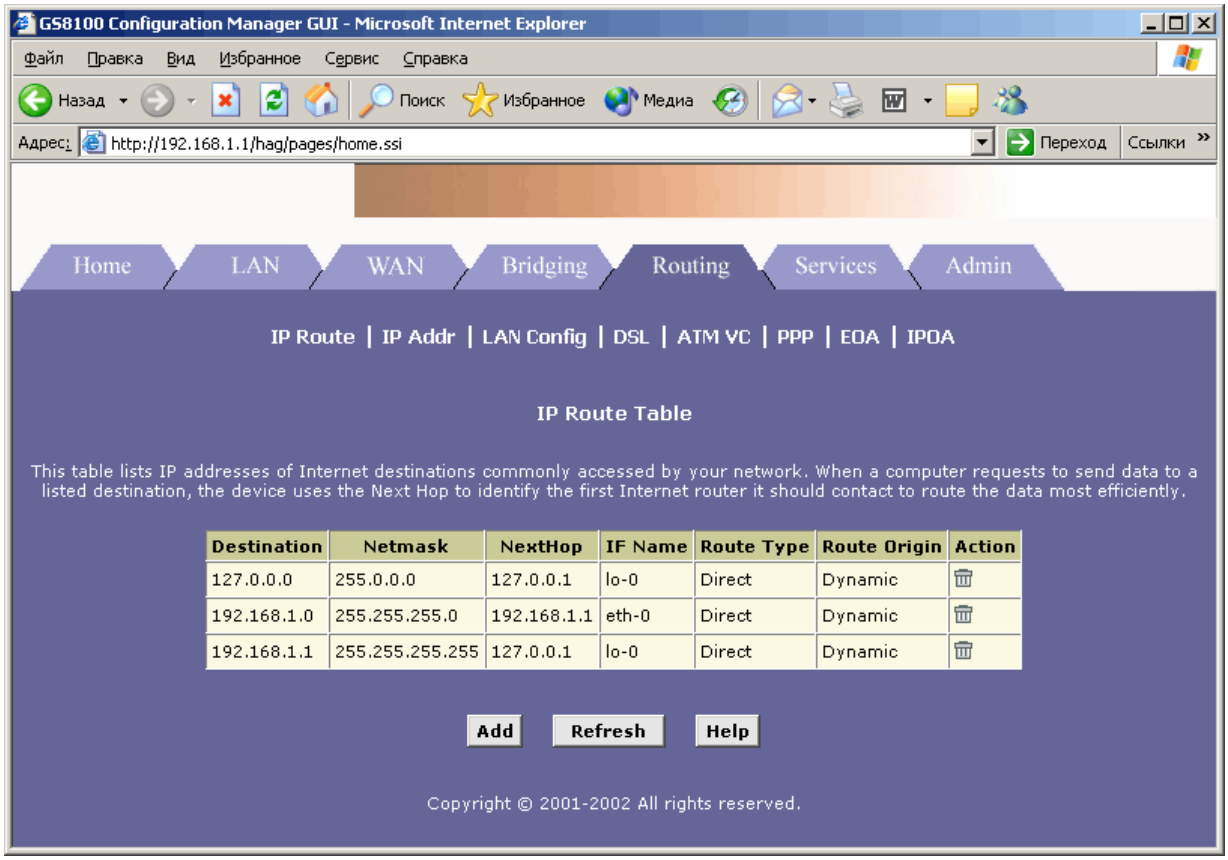
Опция Bridging позволяет разрешить или запретить работу всего моста. Опция ZIPB включает или выключает сжатие пакетов при передаче через глобальную сеть. (Использовать сжатие можно только в том случае, если оно поддерживается на обеих сторонах соединения.)

После ввода требуемых параметров следует нажать кнопку Submit.

Остальные ссылки на данной панели приводят на страницы конфигурации соответствующих интерфейсов и используемого ими транспорта глобальной сети. В частности, с их помощью удобно проверять назначение интерфейсам IP-адресов.

ВНИМАНИЕ После завершения настройки необходимо сохранить полученную конфигурацию в энергонезависимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

7. IP-маршрутизация



7.1. Просмотр параметров и статистики IP-интерфейсов

Список всех IP-адресов и масок, назначенных интерфейсам устройства NSG–200/A, представлен на странице IP Address Table панели Routing. Какие-либо изменения конфигурации на данной странице не предусмотрены.

Суммарная статистика работы устройства по всем IP-интерфейсам выводится в отдельном окне по нажатию кнопки Global Stats.

Ручная настройка таблицы маршрутизации производится на странице IP Route Table. Остальные ссылки на данной панели приводят на страницы конфигурации соответствующих интерфейсов и используемого ими транспорта глобальной сети.

7.2. Настройка таблицы маршрутизации

Ручная настройка таблицы маршрутизации требуется от пользователя лишь в сложных случаях, например, когда трафик различных приложений следует направлять по различным виртуальным соединениям ATM-over-ADSL, которые имеют различные характеристики (голосовые пакеты и данные) или ведут к различным провайдерам (один — в корпоративную сеть, другой — к сайтам непотребного содержания). В большинстве случаев достаточно тех маршрутов, которые устанавливаются по умолчанию при установлении соединений в глобальной сети.

Все маршруты, действующие на данный момент, представлены на странице IP Route Table панели Routing. Статические маршруты, установленные пользователем, имеют атрибут Local; маршруты, сформированные автоматически (при установлении соединений, или в результате работы протокола RIP), обозначаются как Dynamic. В остальном таблица маршрутизации выглядит стандартным образом.

Для добавления нового статического маршрута используется кнопка Add. В открывающемся окне следует ввести адрес и маску сети назначения и адрес шлюза или следующего маршрутизатора. Остальные параметры маршрута устанавливаются автоматически. После ввода требуемых параметров следует нажать кнопку Submit, затем Close.

Для удаления маршрута используется иконка в виде мусорной корзины.

7.3. Использование протокола RIP

Устройство NSG–200/A поддерживает протоколы динамической маршрутизации RIP 1 и RIP 2. Включение и настройка этих протоколов производится на странице RIP панели Services, причем конфигурация может различаться для различных интерфейсов, на прием и на передачу.

Для службы RIP необходимо установить статус (включена/выключена) и, если она включена, то период рассылки сообщений RIP, срок жизни динамических записей в таблице маршрутизации и список интерфейсов, на которых будут рассылаться и/или приниматься сообщения RIP. Для каждого используемого интерфейса необходимо установить метрику, формат сообщений, рассылаемых данным устройством, и формат сообщений, которые оно должно принимать; после этого следует нажать кнопку Add. По возможности рекомендуется использовать протокол RIP 2 (если он поддерживается соседними маршрутизаторами). После ввода требуемых параметров следует нажать кнопку Submit.

В большинстве случаев подключения одиночного пользователя или небольшой сети использование RIP не является необходимым, поскольку используется только два маршрута: из локальной сети в сеть поставщика услуг Интернет, либо из глобальной сети в локальную. Включать протокол RIP следует обычно, если в локальной сети установлено более одного маршрутизатора, либо в глобальной сети установлено более одного соединения, либо это явно предписано оператором.

Для просмотра статистики работы RIP следует нажать кнопку Global Stats.

ВНИМАНИЕ После завершения настройки необходимо сохранить полученную конфигурацию в энергонезависимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

8. Трансляция сетевых адресов (NAT)

Механизм трансляции сетевых адресов (NAT) выполняет двоякую функцию. С одной стороны, он позволяет многим компьютерам локальной сети, в том числе с "приватными" адресами (10.0.0.0/24, 192.168.0.0./16 и др.) получать доступ в Интернет под одним или несколькими "глобальными" адресами, выделенными данной сети вышестоящим поставщиком услуг. С другой стороны, он скрывает структуру внутренней сети и тем самым делает ее компьютеры недоступными для внешнего мира.

NAT может работать в нескольких режимах (в Web-интерфейсе — *flavours*), различающихся правилами преобразования адресов и портов. По умолчанию, механизм NAT включен и настроен для работы в режиме NAPT (преобразование адресов и портов) следующим образом: внутренние адреса 192.168.1.2...192.168.1.13 (наиболее употребительные для небольших приватных сетей) преобразуются во внешние адреса, динамически назначенные поставщиком услуг Интернет или указанные в конфигурации интерфейсов WAN, а внутренние номера портов последовательно заменяются на номера в диапазоне 50000...51024. Подробное описание этого и других режимов NAT см. в разделе "Добавление правил NAT". Если данное правило не соответствует требованиям пользователя, его необходимо удалить и создать новое.

Управление правилами трансляции адресов осуществляется на страница NAT панели Services. Данный раздел состоит из трех страниц: NAT Global Configuration, NAT Rule Configuration и NAT Translations, переход между которыми осуществляется при помощи выпадающего меню.

8.1. Общие параметры и статистика NAT

На странице NAT Global Configuration представлены общие параметры механизма NAT — переключатель Enable/Disable и набор таймеров (в секундах):

TCP Idle Timeout	Максимальное время неактивности для установленного соединения TCP.
TCP Close Wait	Максимальное время неактивности для соединения TCP, находящегося в стадии разрыва.
TCP Def Timeout	Максимальное время неактивности для соединения TCP, находящегося в стадии установления.
UDP Timeout	Максимальное время неактивности для протокола на основе UDP.
ICMP Timeout	Максимальное время неактивности для протокола на основе ICMP.
GRE Timeout	Максимальное время неактивности для протокола на основе GRE.
Default Nat Age	Время жизни для всех остальных сеансов NAT.

По истечении указанных тайм-аутов установленные соответствия между внутренними и внешними портами данной категории удаляются из таблицы NAT. После ввода требуемых параметров следует нажать кнопку Submit.

Параметры NAPT Port Start и NAPT Port End определяют диапазон портов, используемых правилами типа NAPT во внешней сети. Данные параметры не могут быть изменены пользователем.

Для просмотра общей статистики работы NAT необходимо нажать кнопку Global Stats.

Для просмотра статистики по отдельным правилам NAT используются кнопки Stats на странице NAT Rule Configuration.

Список текущих сеансов NAT представлен на странице NAT Translations. Для получения более подробных сведений о каком-либо сеансе следует нажать иконку в виде указующего перста.

8.2. Добавление правил NAT

Список правил NAT представлен на странице NAT Translations панели Services. Для добавления нового правила следует нажать кнопку Add. Вид окна для составления нового правила зависит от выбранного типа преобразования. После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

ВНИМАНИЕ	После завершения настройки необходимо сохранить полученную конфигурацию в энергонезависимой памяти при помощи кнопки Commit (панель Admin, страница Commit & Reboot).

Для удаления правила и получения подробных сведений используются две иконки в правой части таблицы. Однажды созданное правило не может быть изменено; единственный способ внести изменения — это удалить правило и создать новое.

8.2.1. Правило типа NAPT

Правило типа NAPT преобразует IP-адреса и номера портов в пакетах, исходящих из внутренней сети, в IP-адреса и номера портов внешнего интерфейса. Ответы, приходящие из внешней сети, передаются на исходный адрес и порт во внутренней сети. Для правил этого типа устанавливаются следующие параметры:

Rule ID	Порядковый номер (приоритет) правила. Для одних и тех же интерфейсов и IP-адресов может быть определено по несколько правил, которые проверяются в порядке возрастания номеров. В результате из них применяется правило с наименьшим приоритетом, остальные игнорируются. Необходимо внимательно расставлять номера правил, чтобы частные правила стояли в таблице раньше, чем более общие. Рекомендуется нумеровать правила не подряд, а, например, с шагом 5 или 10, чтобы можно было впоследствии вставить между ними новые.
IF Name	Имя интерфейса, к которому применяется правило, или All, если ко всем. Обычно в этом поле указывается интерфейс WAN, используемый для соединения с глобальной сетью.
Local Address From Local Address To	Начало и конец диапазона внутренних IP-адресов. Чтобы определить правило только для одного компьютера, следует ввести одинаковые значения в обоих полях. Чтобы исключить из рассмотрения некоторый поддиапазон адресов, следует создать два правила. Чтобы задать правило для всех адресов локальной сети, следует определить диапазон от 0.0.0.0 до 255.255.255.255.
Global Address	Внешний IP-адрес, назначенный поставщиком услуг Интернет. Если для соединения с глобальной сетью используется несколько интерфейсов, то в правило, относящееся к некоторому интерфейсу, следует ввести адрес этого интерфейса. Такое правило не будет действовать на пакеты, проходящие через остальные интерфейсы.

После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

8.2.2. Правило типа BASIC

Правило типа BASIC, как и NAPT, используется для доступа внутренних компьютеров во внешнюю сеть, Однако оно преобразует только IP-адреса по принципу 1:1, не затрагивая номера портов. Оно позволяет отображать адрес на адрес, или пул внутренних адресов на пул внешних адресов. Размер пулов может не совпадать — как правило, внешний пул меньше внешнего, или состоит только из одного адреса. В этом случае внешние адреса выделяются внутренним компьютерам по принципу "кто первый встал — того и тапочки". Если все внешние адреса исчерпаны, то больше ни один компьютер из локальной сети не сможет получить доступ в Интернет, пока один из уже работающих компьютеров не разорвет все соединения и не освободит адрес. Для правил этого типа устанавливаются следующие параметры:

Rule ID — Порядковый номер (приоритет) правила. Для одних и тех же интерфейсов и IP-адресов может быть определено по несколько правил, которые проверяются в порядке возрастания номеров. В результате из них применяется правило с наименьшим приоритетом, остальные игнорируются. Необходимо внимательно расставлять номера правил, чтобы частные правила стояли в таблице раньше, чем более общие. Рекомендуется нумеровать правила не подряд, а, например, с шагом 5 или 10, чтобы можно было впоследствии вставить между ними новые.

IF Name — Имя интерфейса, к которому применяется правило, или All, если ко всем. Обычно в этом поле указывается интерфейс WAN, используемый для соединения с глобальной сетью.

Protocol — Протокол, к которому применяется данное правило: любые прикладные протоколы на основе TCP, UDP, ICMP, конкретные протоколы в диапазоне 1...255 (по номеру), или Any.

Local Address From
Local Address To — Начало и конец диапазона внутренних IP-адресов. Чтобы определить один адрес, следует ввести одинаковые значения в обоих полях.

Global Address From
Global Address To — IP-адреса интерфейсов глобальной сети. Чтобы определить один адрес, следует ввести одинаковые значения в обоих полях.

После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

8.2.3. Правило типа FILTER

Правило типа FILTER представляет собой расширенный вариант BASIC, который может применяться избирательно к определенным IP-адресам и/или номерам портов во внешней сети. Для правил этого типа устанавливаются следующие параметры:

Rule ID — Порядковый номер (приоритет) правила. Для одних и тех же интерфейсов и IP-адресов может быть определено по несколько правил, которые проверяются в порядке возрастания номеров. В результате из них применяется правило с наименьшим приоритетом, остальные игнорируются. Необходимо внимательно расставлять номера правил, чтобы частные правила стояли в таблице раньше, чем более общие. Рекомендуется нумеровать правила не подряд, а, например, с шагом 5 или 10, чтобы можно было впоследствии вставить между ними новые.

IF Name — Имя интерфейса, к которому применяется правило, или All, если ко всем. Обычно в этом поле указывается интерфейс WAN, используемый для соединения с глобальной сетью.

Protocol — Протокол, к которому применяется данное правило: любые прикладные протоколы на основе TCP, UDP, ICMP, конкретные протоколы в диапазоне 1...255 (по номеру), или Any.

Local Address From
Local Address To — Начало и конец диапазона внутренних IP-адресов. Чтобы определить один адрес, следует ввести одинаковые значения в обоих полях.

Global Address From
Global Address To — IP-адреса интерфейсов глобальной сети. Чтобы определить один адрес, следует ввести одинаковые значения в обоих полях.

Destination Address From
Destination Address To
Destination Port From
Destination Port To — Адрес(а) и порт(ы), к которым будет применяться данное правило. Например, если не указать диапазон адресов, но установить оба значения портов равными 21, то при обращении к любому внешнему FTP серверу внутренний адрес компьютера будет заменяться на адрес внешнего интерфейса, а при обращении к серверу HTTP — передаваться без изменений.

Если в качестве адреса указан адрес подсети, то правило будет применяться ко всем адресам в этой подсети (при обращении по указанным портам).

После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

8.2.4. Правило типа BITMAP

Правило типа BITMAP обеспечивает двустороннее преобразование IP-адресов по принципу 1:1 без учета и изменения номеров портов. Для правил этого типа устанавливаются следующие параметры:

Rule ID — Порядковый номер (приоритет) правила. Для одних и тех же интерфейсов и IP-адресов может быть определено по несколько правил, которые проверяются в порядке возрастания номеров. В результате из них применяется правило с наименьшим приоритетом, остальные игнорируются. Необходимо внимательно расставлять номера правил, чтобы частные правила стояли в таблице раньше, чем более общие. Рекомендуется нумеровать правила не подряд, а, например, с шагом 5 или 10, чтобы можно было впоследствии вставить между ними новые.

IF Name — Имя интерфейса, к которому применяется правило, или All, если ко всем. Обычно в этом поле указывается интерфейс WAN, используемый для соединения с глобальной сетью.

Local Address — Внутренний IP-адрес.

Global Address — Внешний IP-адрес.

После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

8.2.5. Правило типа RDR

Правило типа RDR создает виртуальный сервер: если из внешней сети поступает пакет с определенным адресом и портом назначения, то он передается на некоторый адрес и порт во внутренней сети. Например, пакеты, адресованные на порт 80 (HTTP), передаются реальному Web-серверу, расположенному во внутренней сети. В ответах, отправляемых во внешнюю сеть, внутренние IP-адрес и номер порта заменяются на исходные. Для правил этого типа устанавливаются следующие параметры:

Rule ID — Порядковый номер (приоритет) правила. Для одних и тех же интерфейсов и IP-адресов может быть определено по несколько правил, которые проверяются в порядке возрастания номеров. В результате из них применяется правило с наименьшим приоритетом, остальные игнорируются. Необходимо внимательно расставлять номера правил, чтобы частные правила стояли в таблице раньше, чем более общие. Рекомендуется нумеровать правила не подряд, а, например, с шагом 5 или 10, чтобы можно было впоследствии вставить между ними новые.

IF Name — Имя интерфейса, к которому применяется правило, или All, если ко всем. Обычно в этом поле указывается интерфейс WAN, используемый для соединения с глобальной сетью.

Protocol — Протокол, к которому применяется данное правило: любые прикладные протоколы на основе TCP, UDP, ICMP, конкретные протоколы в диапазоне 1...255 (по номеру), или Any.

Local Address From
Local Address To — Начало и конец диапазона внутренних IP-адресов. Если в обоих полях введены одинаковые значения, то все пакеты, подпадающие под данное правило, будут направляться на этот адрес. Если введен некоторый диапазон, то пакеты будут направляться на первый доступный сервер, адрес которого находится в данном диапазоне. Такой вариант обычно используется для балансировки нагрузки и резервирования серверов.

Global Address From
Global Address To — IP-адреса интерфейсов глобальной сети. Правило будет действовать на все интерфейсы, адреса которых попадают в указанный диапазон.

Destination Port From
Destination Port To — Порт или диапазон портов, которые будут прослушиваться данным виртуальным сервером. Эти параметры служат в качестве фильтра: если в пакете, поступившем из глобальной сети, адрес назначения не попадает в указанный диапазон, пакет уничтожается. Например, для виртуального Web-сервера следует указать номер порта 80.

Local Port — Номер порта сервера во внутренней сети, если он отличается от стандартного. Например, если реальный Web-сервер использует нестандартный порт 2080, а приходящие запросы HTTP, как ожидается, будут адресованы на порт 80, то следует ввести:

Destination Port From	80
Destination Port To	80
Local Port:	2080

После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

8.2.6. Правило типа PASS

Правило типа PASS представляет собой исключение из какого-либо другого правила или правил и позволяет пакетам, исходящим от определенной группы внутренних адресов, проходить во внешнюю сеть без преобразования. Для правил этого типа устанавливаются следующие параметры:

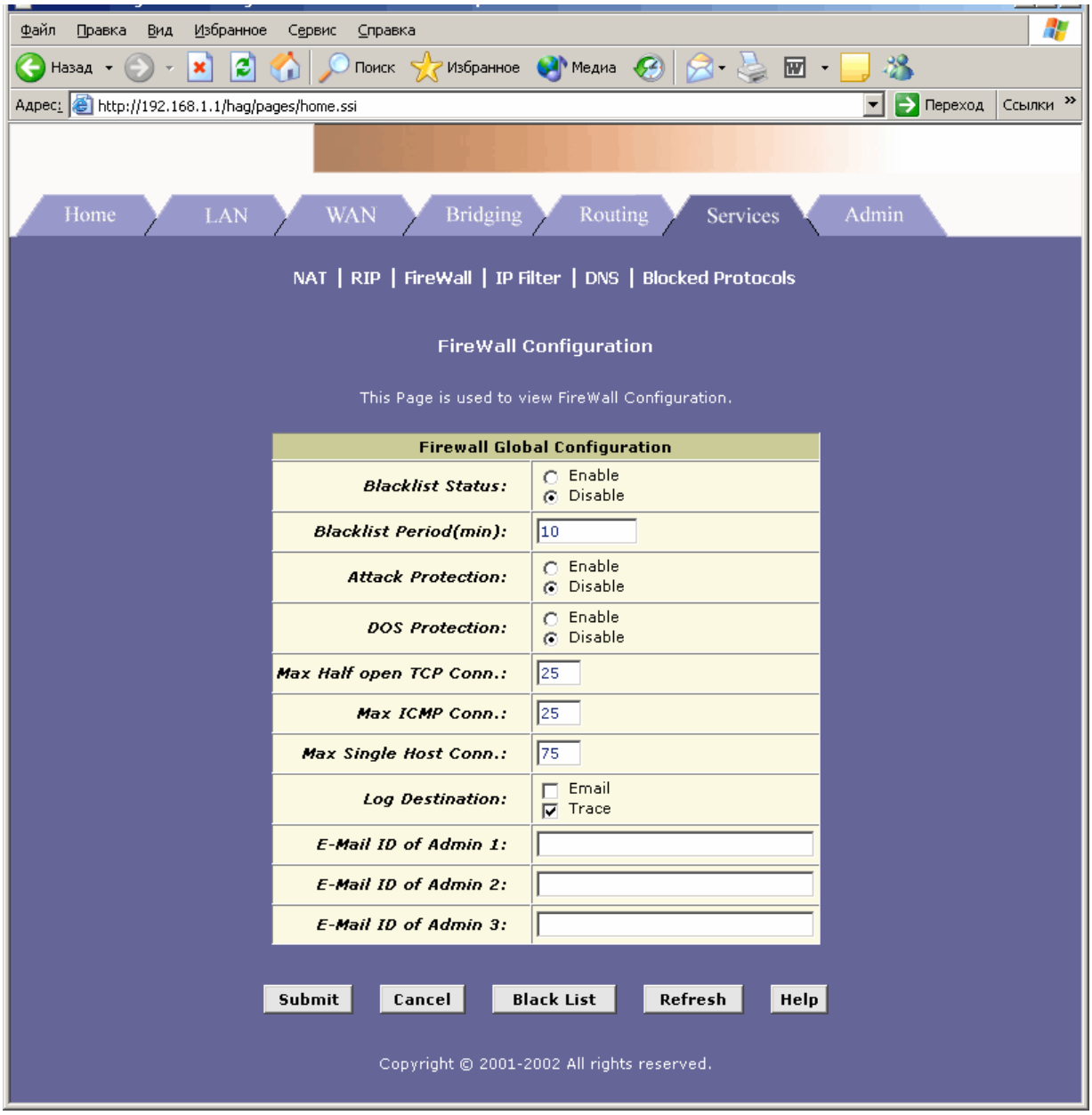
Rule ID — Порядковый номер (приоритет) правила. В данном случае этот параметр особенно важен: правило PASS должно иметь меньший номер, чем правило, из которого требуется сделать исключение. Тогда оно будет применено первым и достигнет поставленной цели.

IF Name — Имя интерфейса, к которому применяется правило, или All, если ко всем. Обычно в этом поле указывается интерфейс WAN, используемый для соединения с глобальной сетью.

Local Address From
Local Address To — Начало и конец диапазона внутренних IP-адресов. Чтобы определить один адрес, следует ввести одинаковые значения в обоих полях.

После ввода требуемых параметров в каждом окне следует нажать кнопку Submit, затем Close.

9. Обеспечение безопасности



Средства обеспечения безопасности сети в NSG–200/A включают как пассивные инструменты — развитый набор фильтров для проходящих пакетов — так и активный брандмауэр, способный идентифицировать сетевые атаки, предпринимать превентивные действия против них и уведомлять администратора о таких событиях.

9.1. Брандмауэр

Настройка брандмауэра производится на странице FireWall Configuration панели Services. Страница содержит следующие параметры:

Blacklist Status
Blacklist Period

Блокировка адресов, с которых предпринимаются действия, квалифицируемые как попытка атаки. Если блокировка включена, то после обнаружения атаки NSG–200/A уничтожает все пакеты с этих адресов в течение указанного времени.

Attack Protection

Включение защиты от следующих типов атак:

- IP Spoofing — посылка на интерфейс WAN пакетов, в которых в качестве источника указан IP-адрес локальной сети, расположенной за устройством NSG–200/A;
- Tear Drop — посылка пакетов, содержащих перекрывающиеся фрагменты;
- Smurf and Fraggle — посылка пакетов, в которых в качестве источника указан широковещательный IP-адрес локальной или глобальной сети;

	• Land Attack — посылка пакетов, в которых адрес источника совпадает с адресом назначения; • Ping of Death — посылка пакетов некорректной длины.
DoS Protection	Включение защиты от атак типа Denial of Service. Превышение любого из следующих трех параметров квалифицируется как атака.
Max Half open TCP Conn.	Максимальный процент соединений TCP, находящихся в стадии установления. При превышении данного предела все "полуоткрытые" соединения TCP разрываются, после чего процедура установления соединений начинается снова. Защита от атак типа SYN DoS.
Max ICMP Conn.	Максимальный процент соединений ICMP. При достижении данного предела старые соединения ICMP разрываются по мере поступления запросов на установление новых, так что общее число сеансов остается постоянным. Защита от атак типа ICMP DoS.
Max Single Host Conn.	Максимальный процент одновременных соединений, инициированных одним удаленным хостом. Защита от произвольных DoS-атак, исходящих с одного хоста. При выборе данного параметра следует учитывать число и назначение хостов, находящихся в локальной сети.
Log Destination	Способ регистрации событий брандмауэра: трасса (ведется на сервере в локальной сети) либо уведомление администраторов по электронной почте.
E-Mail ID of Admin 1/2/3	Почтовые адреса, по которым следует рассылать уведомления об обнаруженных атаках и предпринятых мерах.

После ввода требуемых параметров следует нажать кнопку Submit.

Список адресов, заблокированных на данный момент, можно просмотреть при помощи кнопки Black List. Список содержит как адреса, автоматически заблокированные брандмауэром на указанное время, так и адреса, на которые установлены постоянные фильтры. Чтобы немедленно удалить адрес из "черного списка" (например, в случае ошибочного срабатывания брандмауэра), следует нажать иконку в виде мусорной корзины.

9.2. Фильтрация IP-пакетов

Настройка фильтрации производится на странице IP Filter Configuration панели Services. Страница содержит список фильтров, заданных пользователем, и некоторые глобальные настройки.

Параметр Security Level позволяет быстро изменять набор фильтров, действующих на данный момент. Каждый создаваемый фильтр относится к степеням безопасности High (высокая), Medium (средняя) или Low (низкая). При выборе одного из этих трех значений активируются только те фильтры, которые отнесены к данной категории. При выборе None фильтрация не производится.

Параметры Private/Public/DMZ Deafult Action позволяют выбрать действие по умолчанию для интерфейсов, подключенных к частной сети, сети общего пользования и "демилитаризованной зоне". Категория каждого интерфейса с точки зрения фильтрации указывается при его создании (см. раздел "Транспорт и интерфейсы глобальной сети"). Выбранное действие (принять либо уничтожить пакет) применяется к пакетам, не подпадающим явным образом ни под одно из установленных правил.

Категория Public, как правило, устанавливается для интерфейсов глобальной сети (типов EoA, IPoA, PPP), соединяющих устройство с сетями общего пользования. Для этих интерфейсов обычно выбирается наиболее жесткие ограничения: "всё, что не разрешено — то запрещено". По умолчанию устанавливается значение Deny; пропускаются только те пакеты, которые явно разрешены каким-либо правилом.

Категория Private, как правило, устанавливается для интерфейсов корпоративной сети. Это всегда интерфейс LAN, а также, возможно, какие-либо из интерфейсов EoA, IPoA, PPP, соединяющие устройство с удаленными сегментами корпоративной сети. Для этих интерфейсов обычно выбирается наименее жесткие ограничения: "всё, что не запрещено— то разрешено ". По умолчанию устанавливается значение Accept; блокируются только те пакеты, которые явно запрещены каким-либо правилом.

Категория DMZ (De-Militarized Zone) предназначена для интерфейсов, подключенных к открытому сегменту частной сети — например, к открытым Web- и FTP-серверам. Для этих интерфейсов обычно выбирается промежуточная степень ограничений. Как правило, по умолчанию устанавливается значение Deny, а затем определяется набор фильтров, разрешающих доступ по определенным протоколам (например, http и ftp).

В таблице фильтров указываются основные параметры и административный статус каждого фильтра. Три иконки в правой части таблицы позволяют просматривать все параметры, редактировать и удалять фильтр; кнопка Stats выводит окно с подробной статистикой работы фильтра.

После внесения изменений на данной странице следует нажать кнопку Submit.

9.3. Создание фильтров для IP-пакетов

Для создания нового фильтра следует нажать кнопку Add на странице IP Filter Configuration панели Services. Предварительно необходимо сформулировать критерии фильтрации, требуемое действие (разрешить/запретить) и административные характеристики создаваемого фильтра. Настройки фильтра включают следующие параметры:

Rule ID — Номер (приоритет) фильтра. Правила применяются к каждому пакету последовательно, в порядке возрастания номеров (от меньшего к большему). Таким образом, правила с меньшими номерами имеют более высокий приоритет. Рекомендуется нумеровать создаваемые правила не подряд, а с шагом 5 или 10, чтобы впоследствии можно было вставить между ними новые правила.

Action — Действие, которое должно быть выполнено, если пакет удовлетворяем условиям фильтра:
- Accept — передать по назначению
- Deny — уничтожить пакет

Direction — Направление передачи, к которому относится данный фильтр:
- Incoming — пакет поступает из локальной сети
- Outgoing — пакет адресован в глобальную сеть

Interface — Название или категория интерфейса, к которому применяется фильтр.

In Interface — Название или категория интерфейса, на котором был принят пакет (только для исходящих пакетов).

Log Option — Регистрация срабатываний фильтра в системном журнале.

Security Level — Уровень защиты, при котором данный фильтр будет активен. Сам уровень устанавливается опцией Security Level на странице IP Filter. Если, например, выбран уровень защиты Medium, то будут включены те и только те фильтры, для которых установлен этот уровень, но не High и не Low. Чтобы фильтр был активен, как это обычно требуется, при "некотором и меньших" уровнях защиты, следует отметить в данной секции несколько полей.

Blacklist Status — Если данная опция включена, то адреса нарушителей будут автоматически вноситься в "черный список". Подробнее о "черном списке" см. раздел "Брандмауэр".

Log Tag — Произвольный текст (до 16 символов), который будет добавлен к записи о срабатывании данного фильтра в системном журнале. Имеет смысл только при включенной опции Log Option.

Start/End Time — Время действия/бездействия фильтра, от 00:00:00 до 23:59:59.

TOD Rule Status — (Time of Day) Активность фильтра в указанное время суток:
- Enable — только в указанный интервал (по умолчанию)
- Disable — только вне указанного интервала

Src IP Address — IP-адрес источника пакета. Адрес может подпадать под действие фильтра в следующих случаях:
- any — любой адрес
- eq — точно равен адресу, указанному в следующих 4 полях
- neq — не равен адресу, указанному в следующих 4 полях
- lt, lteq, gt, gteq — арифметически меньше, меньше или равен, больше, больше или равен указанному
- range — находится в указанном диапазоне
- out of range — находится вне указанного диапазона
- self — совпадает с IP-адресом интерфейса NSG–200/A, к которому относится данное правило

Dest IP Address — IP-адрес назначения пакета. Возможны все те же критерии, что и для Src IP Address, плюс следующий:
- bcast — любой пакет, посланный по широковещательному адресу на принимающем интерфейсе. Ввод конкретного адреса в данном случае не требуется.

Protocol — Протокол транспортного (TCP, UDP, ICMP) или прикладного (по номерам портов 1…255) уровня. Возможные условия фильтрации:
- any — любой протокол
- eq — только выбранный протокол
- neq — любой протокол, кроме выбранного

Store State — Если данная опция включена, правило применяется также и к пакетам, передаваемым через данный интерфейс в противоположном направлении в ходе IP-сеанса.

Source/Dest Port — Номера портов источника и назначения (только для случая, когда в поле Protocol выбран TCP или UDP). Возможны все те же критерии фильтрации, что и для Src IP Address.

TCP Flag — Специфический тип пакетов TCP:
- SYN — только с установленным флагом SYN
- NOT-SYN — только без флага SYN
- ANY — любые пакеты TCP

ICMP Type — Специфическое значение в поле типа пакета ICMP (Один из четырех наиболее употребительных, или по номеру 1…255). Возможные условия фильтрации:
- any — любой тип
- eq — только выбранный тип
- neq — любой тип, кроме выбранного

ICMP Code — Специфическое значение в поле кода пакета ICMP (1…255). Возможные условия фильтрации:
- any — любой код
- eq — только выбранный код
- neq — любой код, кроме выбранного

IP Frag Pkt — Учет фрагментации пакетов. Возможные значения:
- Yes — применять правило только к фрагментированным пакетам
- No — применять правило только к нефрагментированным пакетам
- Ignore — применять правило к любым пакетам (по умолчанию)

IP Option Pkt — Учет поля ToS заголовков IP-пакетов. Возможные значения:
- Yes — применять правило только к пакетам с установленными флагами ToS
- No — применять правило только к пакетам с нулевым полем ToS
- Ignore — применять правило к любым пакетам (по умолчанию)

Packet Size — Размер пакета. Арифметические операторы для сравнения размера пакета с заданной величиной — те же, что и для Src IP Address.

После ввода всех требуемых параметров следует нажать кнопку Submit, затем Close.

9.4. Управление работой IP-фильтров

Для просмотра статистики работы некоторого фильтра следует нажать соответствующую ему кнопку Stats на странице IP Filter Configuration панели Services.

Для просмотра информации об установленных соединениях следует нажать кнопку Session. В открывающемся окне представлен полный список существующих соединений и правил фильтрации, применяемых к ним, со следующими параметрами:

Session Index — Номер сеанса, присвоенный системой.

Time to expire — Время, оставшееся до разрыва соединения по тайм-ауту.

Protocol — Протокол транспортного уровня.

I/F — Интерфейс, на котором применяется правило.

IP Address — Адреса взаимодействующих хостов. Инициатор соединения указан первым.

Port — Номера портов на обеих сторонах соединения.

In/Out Rule Index — Номера правил, применяемых для входящих и исходящих пакетов данного соединения.

In/Out Action — Действие, предпринимаемое согласно данным правилам (Accept, Deny, или Unknown, если никакие фильтры не применяются).

Action(s) — Иконка в виде мусорной корзины позволяет принудительно разорвать соединение.

9.5. Запрет определенных протоколов

Страница Blocked Protocols панели Services позволяет устанавливать упрощенные правила, блокирующие передачу пакетов некоторых протоколов через NSG–200/A независимо от остальных возможных критериев. После внесения изменений на данной странице следует нажать кнопку Submit.

10. Служба DNS

Устройство NSG–200/A может выступать в качестве ретранслятора DNS для хостов локальной сети. Настройка службы DNS производится на странице DNS Configuration панели Services. Для работы в качестве ретранслятора необходимо включить эту службу на NSG–200/A. После этого устройство должно получить адрес реального сервера DNS, расположенного, как правило, в сети поставщика услуг Интернет или в центральном сегменте корпоративной сети. Этот адрес (или несколько) может быть получен следующими способами:

- Введен статически на странице DNS Configuration панели Services. После ввода адреса необходимо нажать кнопку Add. После внесения изменений на данной странице следует нажать кнопку Submit.
- Получен динамически в ходе установления PPP-соединения с соответствующим сервером доступа. При создании интерфейса должна быть включена опция "Use DNS".

Оба типа адресов могут использоваться совместно. После внесения изменений на данной странице следует нажать кнопку Submit.

На клиентских компьютерах установить IP-адрес NSG–200/A в качестве сервера DNS (как правило — основного). Если используется динамическая конфигурация клиентских компьютеров от встроенного сервера DHCP устройства NSG–200/A, то в параметрах сервера DHCP следует указать собственный адрес NSG–200/A в локальной сети, а на клиентах DHCP — включить опцию "Адреса DNS назначаются автоматически".

11. Администрирование устройства

11.1. Изменение пароля пользователя

Изменение пароля пользователя производится на странице User Password Configuration панели Admin. Необходимо ввести старый пароль и дважды — новый пароль, затем нажать кнопку Submit.

Имя пользователя всегда root. Изменение его, или заведение новых пользователей, не предусмотрено.

11.2. Сохранение конфигурации и перезагрузка устройства

Изменения, переданные в устройство при нажатии кнопки Submit, относятся к текущей конфигурации и остаются в силе до следующей перезагрузки устройства. Для сохранения сделанных изменений они должны быть записаны в энергонезависимую память устройства.

Сохранение текущей конфигурации осуществляется на панели Admin, страница Commit & Reboot. Для записи конфигурации в энергонезависимую память необходимо нажать кнопку Commit.

Перезагрузка устройства осуществляется по нажатию кнопки Reboot. Выпадающее меню Reboot Mode позволяет выбрать одну из трех возможных конфигураций:

- Reboot from Last Configuration — Последняя конфигурация, записанная в энергонезависимую память кнопкой Commit
- Reboot from Backup Configuration — Предыдущая конфигурация (используется в случае, если последняя конфигурация оказалась неработоспособной)
- Reboot from Default Configuration — Заводская конфигурация устройства

11.3. Модернизация программного обеспечения

Модернизация программного обеспечения NSG–200/A производится на странице Image Upgrade панели Admin при помощи протокола HTTP. Файл с новой версией программного обеспечения должен быть сохранен на компьютере, с которого осуществляется модернизация, или доступен по сети. На данной странице необходимо ввести путь к файлу, либо выбрать его при помощи кнопки Browse. После этого следует нажать кнопку Upgrade.

11.4. Просмотр системных сообщений

Для просмотра системных сообщений используется страница Alarm панели Admin. Каждому системному событию соответствует одна строка на этой странице. Периодичность автоматического обновления информации в этом окне можно установить при помощи меню Refresh Rate. Для ручного обновления используется кнопка Refresh. Для очистки системного журнала используется кнопка Clear.

11.5. Диагностика виртуальных соединений

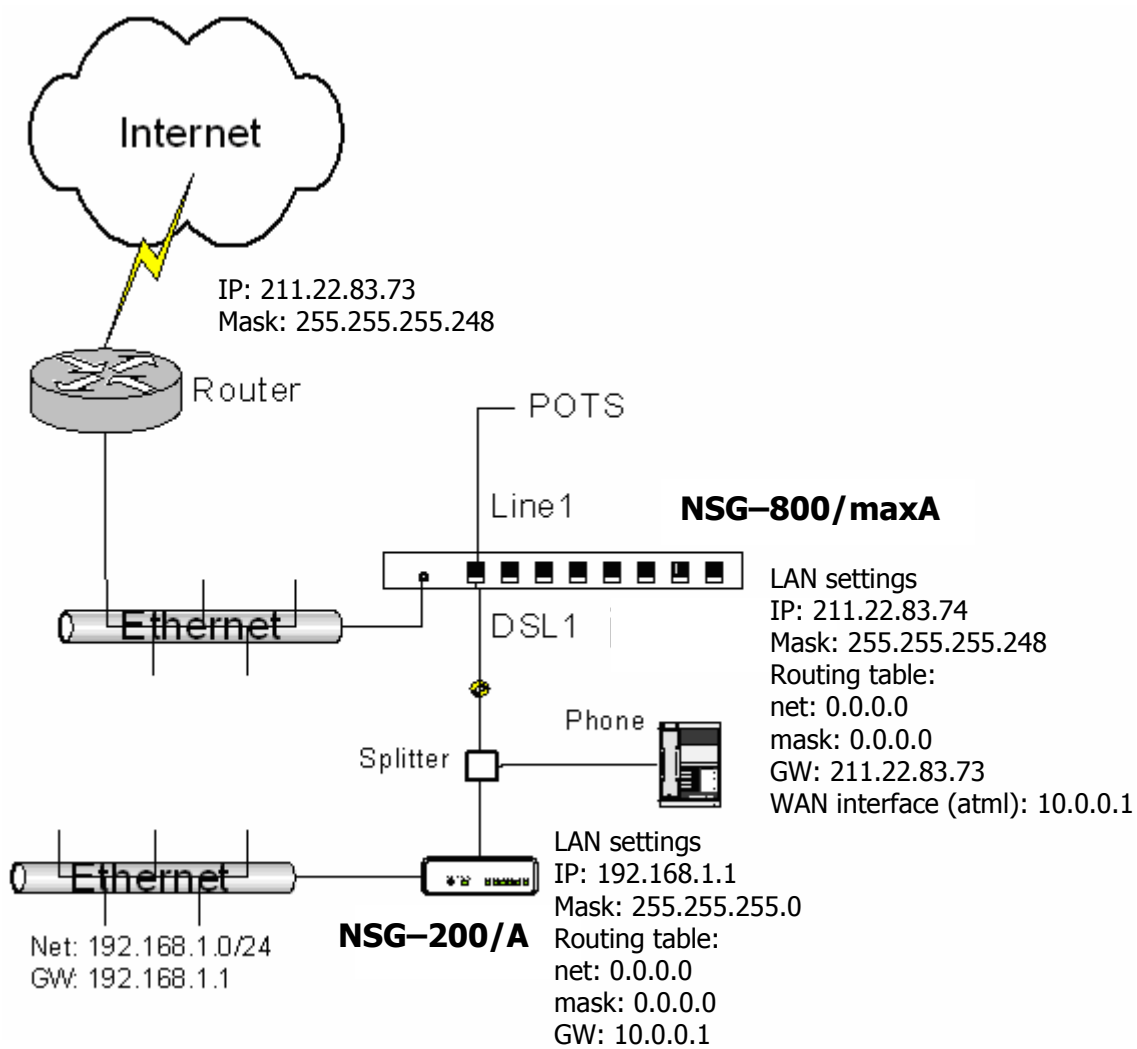
Для проверки работы виртуальных соединений ATM-over-ADSL можно использовать страницу Diagnostics панели Admin. Следует выбрать один из существующих интерфейсов ATM и нажать кнопку Submit. Устройство последовательно выполняет набор тестов от физического до прикладного уровня. Первый неудачный тест в списке, как правило, указывает на источник проблемы.

11.6. Настройка портов для управления устройством

По умолчанию, для управления NSG–200/A используются стандартные порты HTTP — 80 и Telnet — 23. При необходимости эти номера портов могут быть изменены на любые другие в диапазоне 61000…62000. Изменения производятся на странице Port Settings панели Admin. После внесения изменений следует нажать кнопку Submit.

12. Базовая конфигурация

Типовая конфигурация системы ADSL-доступа, состоящей из сервера доступа NSG–800/maxA и абонентского устройства NSG–200 представлена на рисунке. Для подключения одиночного компьютера к представленной системе необходимо соединить ПК и устройство NSG–200/A кабелем "Crossover RJ–45" и установить на устройстве следующие параметры:



- Панель LAN, страница LAN Configuration:
  LAN IP Address 192.168.*n*.1
  Subnet mask 255.255.255.0
  Get LAN Address Manual
  Нажать кнопку Submit.
- Панель LAN, страница DHCP Configuration:
  DHCP Mode None
  Нажать кнопку Submit.
- Панель WAN, страница ATM VC:
  Открыть окно редактирования существующего соединения aal5–0 (щелкнуть мышью на значке карандаша).
  Изменить номер VCI с 35 на 32.
  Нажать кнопку Submit, затем Close.
  Нажать кнопку Submit на панели WAN.
- Панель WAN, страница PPP:
  Удалить существующий интерфейс ppp–0 (щелкнуть мышью на значке мусорной корзины).
  Нажать кнопку Submit.
- Панель WAN, страница Bridging:
  Установить опцию Disable.
  Нажать кнопку Submit.
- Панель WAN, страница IPoA:
  Нажать кнопку Add. Открывается страница добавления интерфейса типа IPoA. Установить следующие значения

параметров:

IPoA interface	ipoa–0
Conf. IP Address	10.0.0.*n+1*
Net Mask	255.255.255.0
IPF	Public
IPoA Type	RFC 1577
Default Route	Enable
Gateway IP Address	10.0.0.1
Lower Interface	aal5–0 и нажать кнопку Add

Нажать кнопку Submit, затем Close.

Нажать кнопку Submit на панели WAN.

Здесь *n+1* — номера, указанные оператором (фактически в данной конфигурации *n* — это номер порта на устройстве NSG–800/maxA). В зависимости от конфигурации конкретной системы доступа, оператором могут быть указаны иные IP-адреса и маски, а также ряд дополнительных настроек; некоторые из вышеприведенных настроек, наоборот, могут не потребоваться. Инструкция о настройке специфических параметров для данной системы доступа предоставляется оператором.

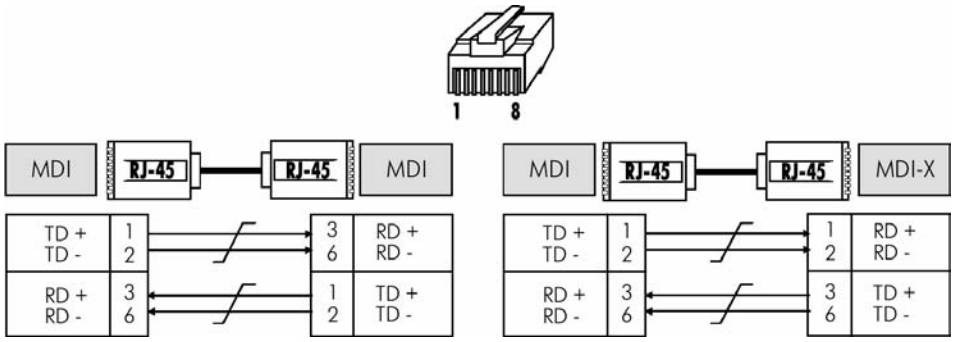
После изменения IP-адреса NSG–200/A соединение будет разорвано. Необходимо изменить параметры стека TCP/IP на ПК (для этого, возможно, потребуется перезагрузить ПК) и восстановить соединение с NSG–200/A. После этого можно продолжить настройку NSG–200/A.

ВНИМАНИЕ До повторного входа в систему устройство NSG–200/A не должно отключаться от источника питания или перезагружаться. После входа в систему необходимо сохранить полученную конфигурацию в энергонезависимой памяти.

ВНИМАНИЕ**:** Изменения, переданные в устройство при нажатии кнопки Submit, относятся к текущей конфигурации и остаются в силе до следующей перезагрузки устройства. Для сохранения сделанных изменений они должны быть записаны в энергонезависимую память устройства.

Сохранение текущей конфигурации осуществляется на панели Admin, страница Commit & Reboot. Для записи конфигурации в энергонезависимую память необходимо нажать кнопку Commit.

Приложение A. Описание кабелей



Кабель “Crossover RJ–45“ Кабель “Straight RJ–45 “

Приложение B. Комплект поставки

Устройство NSG–200/A	1
Гарантийный талон	1
Руководство по эксплуатации	1
Адаптер питания 7,5 V 1A	1
Кабель “Straight RJ–45”	1
Кабель телефонный RJ–11	1
Частотный разделитель (сплиттер)	1

ООО «НСГейт»
Россия 105187, Москва
ул. Кирпичная, д.39, офис 1318
Тел.: (+7–095) 918–27–00

http://www.nsg2u.ru/
mailto:nsg2u@nsg.ru