GABD-000082
Ed. 01

OfficeServ 7200

# Руководство пользователя сервера Data Server

## АВТОРСКОЕ ПРАВО



## ТОВАРНЫЕ ЗНАКИ

Enterprise IP Solutions
OfficeServ™ является товарным знаком SAMSUNG Electronics Co., Ltd.
Имена продуктов, упоминающиеся в данном руководстве, могут быть товарными знаками и/или зарегистрированными товарными знаками соответствующих компаний.

**Данное руководство необходимо прочитать и использовать его в качестве инструкции для правильной установки и эксплуатации продукта.**

Содержание руководства может быть изменено без предварительного уведомления в целях улучшения системы, стандартизации и по другим техническим причинам.

При необходимости получения обновленных руководств или при возникновении вопросов относительно их содержания обратитесь в **Центр документации** по указанному адресу или посетите веб-узел:

**Адрес: Document Center 2nd Floor IT Center. Dong-Suwon P.O. Box 105, 416, Maetan-3dong Yeongtong-gu, Suwon-si, Gyeonggi-do, Korea 442-600**

**Веб-узел: http://www.samsungdocs.com**

# ВВЕДЕНИЕ

## Назначение

В данном документе описывается сервер OfficeServ 7200 Data Server, являющийся приложением для OfficeServ 7200, а также процедуры установки и использования программного обеспечения.

## Содержание и структура документа

В документе содержится 3 главы, 1 приложение и список сокращений.

### Глава 1. Обзор сервера OfficeServ 7200 Data Server

В данной главе приведено краткое описание сервера OfficeServ 7200 Data Server.

### Глава 2. Установка сервера OfficeServ 7200 Data Server

В данной главе приведено описание процедур установки и входа в систему.

### Глава 3. Использование сервера OfficeServ 7200 Data Server

В данной главе описан процесс использование меню сервера OfficeServ 7200 Data Server.

### Приложение A. Настройка VPN в Windows XP/2000

В данной главе описан процесс настройки VPN в Windows XP/2000.

### СОКРАЩЕНИЯ

Описание сокращений, часто используемых в документе.

# Условные обозначения

Для обозначения особо важной информации в документе используются следующие специальные обозначения для соответствующих параграфов. Эти сведения могут располагаться отдельно от основного текста. Они всегда сопровождаются заголовком, выделенным заглавными буквами в полужирном начертании.


**ПРЕДУПРЕЖДЕНИЕ**

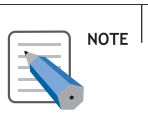
Информация или инструкции, которым необходимо следовать для предотвращения травматизма и несчастных случаев с летальным исходом.


**ОСТОРОЖНО**

Информация или инструкции, которым необходимо следовать для предотвращения сбоя в работе или повреждения системы.


**КОНТРОЛЬНАЯ ТОЧКА**

Контрольные точки для оператора, использующиеся для проверки стабильности работы системы.




**ПРИМЕЧАНИЕ**

Дополнительная информация для справки.

# Отображение информации на экране консоли

- Поля, написанные шрифтом `'Courier New'`, будут использоваться для различения основного текста и текста, отображающегося на экране консоли.
- Полужирный шрифт `'Bold Courier New'` используется для отображения на экране консоли значений, вводимых оператором.

# Справочные материалы

### Общее описание OfficeServ 7200

В общем руководстве OfficeServ 7200 приведено описание OfficeServ 7200 и информация о системе, включая конфигурацию оборудования, технические характеристики и функции.

### Руководство по установке OfficeServ 7200

В руководстве по установке OfficeServ 7200 приведены условия, необходимые для установки, процедура установки, а также процедуры осмотра и запуска системы.

### Руководство по техническому обслуживанию OfficeServ 7200

В руководстве по техническому обслуживанию OfficeServ 7200 приведено краткое описание системы, технические характеристики аппаратного обеспечения, информация по поиску и устранению неисправностей, которые могут возникнуть во время работы, а также процедура программирования для технического обслуживания.

### Справочник по установке OfficeServ 7200

В справочнике по установке OfficeServ 7200 кратко изложена информация из общего описания OfficeServ 7200 и руководства по установке OfficeServ 7200, а также сведения, необходимые для установки системы.

### Руководство пользователя сервера OfficeServ 7200 Feature Server

В руководстве пользователя сервера услуг OfficeServ 7200 Feature Server описывается сервер Feature Server, являющийся приложением для OfficeServ 7200, а также процедуры установки и использования Feature Server.

### Руководство по программированию OfficeServ 7200

В руководстве по программированию сервера телефонии OfficeServ 7200 Call Server содержится описание процедур программирования (MMC) телефонной системы с помощью телефона.

### Руководство по использованию сервера OfficeServ 7200 Data Server

В руководстве по использованию сервера OfficeServ 7200 Data Server приводится функциональное описание режима настройки, процедура установки приложения сервера Data Server.

# Журнал редактирования

| № редакции | Дата выпуска | Примечания |
|---|---|---|
| 00 | 04. 2004. | Первая редакция |
| 01 | 04. 2005. | - Добавлены предупреждения, элементы Port Forward (Переадресация портов), Static NAPT (Статический NAPT), Network DB list (Список сетевых баз данных), Filtering Service (Служба фильтрации).<br>- Изменены названия и описания некоторых функций. |

# ВОПРОСЫ БЕЗОПАСНОСТИ

Для безопасной и правильной работы системы перед ее установкой и эксплуатацией оператор/пользователь должен ознакомиться со следующей информацией.

## Символы

**Осторожно**

Общий предупредительный сигнал

**Ограничение**

Указание на запрещенное для продукта действие

**Указание**

Указание на выполнение специально предусмотренного действия

# ОСТРОЖНО

**Предупреждение системы безопасности**

Обратите внимание, что доступ через сетевой экран разрешен для всех внешних пользователей, если для параметра Remote IP (Удаленный IP-адрес) установлено значение ‘0.0.0.0’, а для параметра Port (Порт) - значение ‘0:’.

**Задание диапазона IP-адресов**

Количество IP-адресов, заданное для параметров ‘Local IP range’ (Диапазон локальных IP-адресов) и ‘Remote IP range’ (Диапазон удаленных IP-адресов), должно быть одинаковым. Если, например, количество IP-адресов для параметра ‘Local IP range’ (Диапазон локальных IP-адресов) равно 10, а для параметра ‘Remote IP range’ (Диапазон удаленных IP-адресов) - 20, будут установлены только первые 10.

**Настройка PPTP в Windows XP/2000**

В Windows XP/2000 пользователь может использовать службу клиента DHCP. При подключении клиентом VPN PPTP во время работы клиента DHCP будут обнаружены ошибки. Для предотвращения ошибок отключите клиент DHCP. Для этого выберите [Пуск] → [Программы] → [Администрирование] → [Службы] и выберите установку клиента PPTP.

**Предупреждение об изменении сетевых интерфейсов**

В случае изменения параметров сетевого интерфейса (например, IP-адреса, шлюза и маски подсети) во время работы маршрутизатора, используемые им IP-сеансы будут на время приостановлены.

**Изменение базы данных**

Базы данных модулей WIM и LIM встроены в сервер OfficeServ 7200 Data Server. При изменении базы данных происходит перезапуск системы.

**Переменный IP для DHCP, PPPoE и VDSL**

При использовании нескольких IP-адресов, информация об общих IP-адресах (например, в меню ‘Port Forward’ (Переадресация портов) и ‘Static NAPT’ (Статический NAPT)) не изменяется автоматически. Для служб VoIP, требующих настройки меню ‘Port Forward’ (Переадресация портов) и ‘Static NAPT’ (Статический NAPT), и служб VPN, требующих настройки IP-адреса WAN, необходимо использовать параметр ‘Fixed IP’ (Фиксированный IP-адрес).

**Использование WEB-обозревателя**

Для работы с сервером OfficeServ 7200 Data Server в качестве веб-браузера необходимо использовать Microsoft Internet Explorer 6.0 или более поздней версии.

**Закрытый ключ**

Закрытый ключ поставляется в комплекте. Закрытый ключ позволяет получать доступ к SSH из внешней сети. Пльзваться этим ключом должен только администратор.

**Удалить временные файлы Интернета**

Удалите временные файлы Интернета после обновления пакета Data Server. Выберите [Internet Explorer] → [Сервис] → [Свойства обозревателя], и в меню [Временные файлы Интернета] нажмите кнопки [Удалить "Cookie"] и [Удалить файлы]. Если временные файлы Интернета не удалены, модуль управление сервером Data Server через WEB-интерфейс отображается неправильно.

**Эта страница оставлена пустой преднамеренно.**

# СОДЕРЖАНИЕ

**Эта страница оставлена пустой преднамеренно.**

# ГЛАВА 1. Обзор сервера OfficeServ 7200 Data Server

В данной главе приводится описание системы OfficeServ 7200 и сервера OfficeServ 7200 Data Server.

## Знакомство с OfficeServ 7200

OfficeServ 7200 - это идеальная телефонная система для небольших компаний, поддерживающая до 120 внутренних абонентов. Система обеспечивает поддержку не только голосовых вызовов, но и передачу данных по вычислительным сетям. Пользователям компьютеров, серверов, цифровых, IP и мобильных телефонов легко могут воспользоваться разнообразными функциями системы.
The OfficeServ 7200 is configured with a cabinet mounted on a 19-inch rack, internal station, wireless LAN device, and application software.
Having a conventional server on a Linux platform outside of the cabinet, the OfficeServ 7200 provides the following application software:

- OfficeServ 7200 Feature Server(UMS, Mail Server, SIP Server)
- OfficeServ Admin(OfficeServ Operator, CTI)
- OfficeServ Solution(System Manager, Web Management, PCMMC, OfficeServ EasySet)

OfficeServ 7200 обеспечивает такие сетевые функции, как IP коммутатор, маршрутизатор, межсетевой экран сервера данных, который работает совместно с сервером телефонии или сервером приложений. В данном документе описывается сервер данных OfficeServ 7200 Data Server.


**Конфигурация OfficeServ 7200**

Информацию о конфигурации, функциях и технических характеристиках OfficeServ 7200 см. в общем описании OfficeServ 7200.

# Знакомство с сервером данных OfficeServ 7200 Data Server

Комплекс системы OfficeServ 7200 состоит из телефонной системы OfficeServ 7200 Call Server, сервера приложений Feature Server и сервера данных OfficeServ 7200 Data Server функции, которого приведенные ниже.

## Коммутатор

- Функции коммутатора Dummy L2 Switch.
- Функции управляемого LAN коммутатора при подключении платы к плате WIM (гнездо 2 основного устройства).
- Функции адаптивного моста с использованием алгоритма Spanning tree.
- Функции приоритета фреймов на уровне 2 протокола 802.1p.
- Управление потоком 802.3x на уровне 2.
- Функции виртуальной локальной сети (VLAN), которая функционируети на основе отслеживания IP порта, MAC-адреса и тегов 802.1 Q.
- Поддержка IP многоадресной рассылки (наблюдение по протоколу IGMP).

## Маршрутизатор

- Управление путями и создание очередей для пакетов данных как во внешней глобальной, так и во внутренней локальной сетях.
- Статическая и динамическая маршрутизация.
- Поддержка протоколов маршрутизации RIPv1, RIPv2 и OSPFv2.
- Маршрутизация между VLAN виртуальными сетями.
- Функции клиента при использовании протоколов DHCP, PPP и PPPoE для интерфейсов Ethernet WAN.
- Поддержка протоколов HDLC, PPP и инкапсуляции по технологии Frame Relay через последовательный V.35 интерфейс WAN.
- Поддержка многоадресной рассылки IP-адресов.
- Поддержка протоколов групповой трансляции IGMPv1 или IGMPv2.

- Назначение интерфейсов платы WIM.
  - 2 порта WAN Ethernet: один порт используется в качестве резервного (10 Мбит/с).
  - 1 порт LAN Ethernet: установка соединения с коммутатором для подключения к локальной сети.
  - 1 последовательный порт V.35: поддержка выделенного канала путем подключения к DSU или CSU.
  - 1 порт DMZ Ethernet: организация зоны DMZ.
- Плата локальной сети LIM
  - Плата LIM предназначена для организации локальной сети и содержит 16 портовый коммутатор уровня 2.
  - Установка модуля LIM в слот 2 рядом с модулем WIM обеспечивает полную управляемость данного LIM модуля.
- Интерфейса DMZ
  - Для защиты внутренней сети от внешних проникновений используется порт DMZ. Это отдельный порт LAN для подключения различных устройств, которым требуется свободный доступ извне, например, почтовый или веб-сервер.

## Безопасность сети передачи данных

- Входящая и исходящая NAT/PT трансляция
  - Управление доступом к внутренним ресурсам путем переключения между глобальным IP-адресом и локальнымIP-адресом.
- Сетевой экран
  - Управление доступом извне с использованием списка расширенного доступа.
- Система обнаружения проникновения (IDS)
  - Обнаружение и оповещение о доступе в неавторизованные области с использованием списка доступа.
  - Опознавание и оповещение о неавторизованных пакетах путем применения основного правила проникновения для пакетов.
  - Обнаружение и блокировка атак с целью отключения (DoS), например синхронных лавин пакетов.
- Виртуальная частная сеть (VPN)
  - Функции шлюза VPN на основе PPTP и IPSec.
  - Сохранение конфиденциальности и целостности системы с использованием туннельных протоколов VPN и шифрования данных.

## Приложения сети передачи данных

- Функциями приложений сети передачи данных называются службы NAT/PT, сетевой экран, VPN, DHCP и шлюз уровня приложений Application Level Gateway (ALG).
- Службы выполняется как приложения, запущенные на модуле WIM.
- Шлюз уровня приложений Application Level Gateway (ALG)
  - Поддержка ALG для неблокируемой передачи VoIP сигналов и данных, при включенной функции безопасности.
- Сервер DHCP
  - Автоматическая установка сетевой среды для оборудования IP или других функциональных элементов системы OfficeServ 7200.

## QoS

- Назначение приоритета для фреймов уровня 2 на основе стандарта 802.1p (функция коммутатора).
- Назначение приоритета очередности для пакетов уровня 3 и выбранных IP-адресов.
- Назначение приоритета очередности для пакетов уровня 4 и пакетов RTP (порт UDP/TCP).

## Управление

- Поддержка функции отладки через соединение Telnet для специалистов.
- Настройки и проверки работы функционального блока сервера данных с помощью WEB-обозревателя.
- Обмен данными IDS и данными аварийной сигнализации с системным администратором.
- Обновление ПО
  - Обновление по протоколу TFTP
  - Обновление по протоколу HTTP

# Глава 2. Установка сервера OfficeServ 7200 Data Server

В данной главе описываются процедуры установки и входа в систему сервера OfficeServ 7200 Data Server.

## Процедура установки

Пакет программного обеспечения включен в сервер OfficeServ 7200 Data Server, поэтому дополнительная установка программного обеспечения не требуется. В пакет программного обеспечения включены следующие компоненты:

| Пакет | Файл | Описание |
|---|---|---|
| Пакет для загрузки ПЗУ | bootldr.img-vx.xx<br>bootldr.img-vx.xx.sum | Программа для загрузки ПЗУ |
| Основой пакет | ds-pkg-vx.xx.tar.gz | Пакет обновления для HTTP при управлении через веб-интерфейс |
| | app.img-vx.xx<br>app.img-vx.xx.sum | Пакет обновления раздела ‘app’ для TFTP |
| | config.img-vx.xx<br>config.img-vx.xx.sum | Пакет обновления раздела ‘config’ для TFTP |
| | kernel.img-vx.xx<br>kernel.img-vx.xx.sum | Пакет обновления раздела ‘kernel’ для TFTP |
| | log.img-vx.xx<br>log.img-vx.xx.sum | Пакет обновления раздела ‘log’ для TFTP |
| | ramdisk.img-vx.xx<br>ramdisk.img-vx.xx.sum | Пакет обновления раздела ‘ramdisk’ для TFTP |
| | flash1.img-vx.xx<br>flash1.img-vx.xx.sum | Первый файл для работы с флэш-памятью |
| | flash2.img-vx.xx<br>flash2.img-vx.xx.sum | Второй файл для работы с флэш-памятью |


**Конфигурация пакета программного обеспечения**

В каждом пакете имеется отдельный файл для проверки контрольной суммы, а x.xx обозначает версию.

Для доступа к серверу Data Server настройте среду следующим образом.

1. Установите плату WIM в слот 1, а плату LIM слот 2.
   - Для подключения платы WIM к плате LIM через заднюю панель проверьте положение перемычек JP1, 2, 3, 4 При внутреннем (перемычки переставлены к задней части платы LIM) соединении плат WIM и LIM, порт LAN на плате WIM будет отключен.
   - Если перемычка JP1, 2, 3, 4 направлена к передней части платы WIM, необходимо подключить порт LAN платы WIM к порту платы LIM с помощью кабеля LAN.
2. Подключите компьютер к порту платы LIM.
3. Запустите на компьютереобозреватель Internet Explorer и установите соединение с IP-адресом (10.0.0.1) локальной сети. По умолчанию для платы WIM назначен IP-адрес 10.0.0.1.

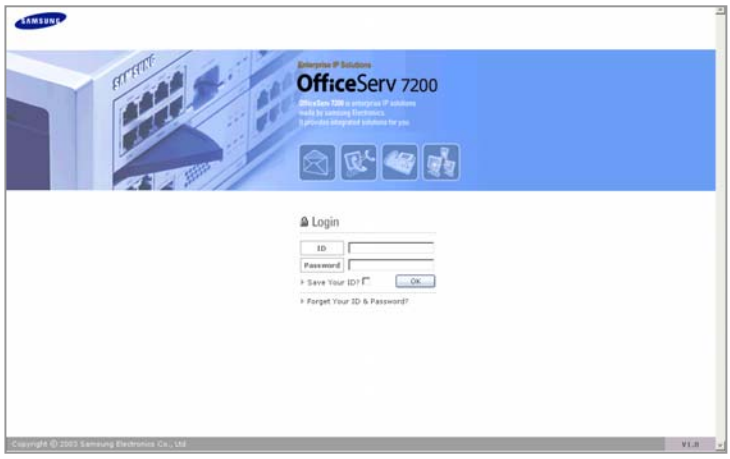

**Использование WEB--обозревателя**

Для работы с сервером OfficeServ 7200 Data Server в качестве веб-браузера необходимо использовать Microsoft Internet Explorer 6.0 или более поздней версии.

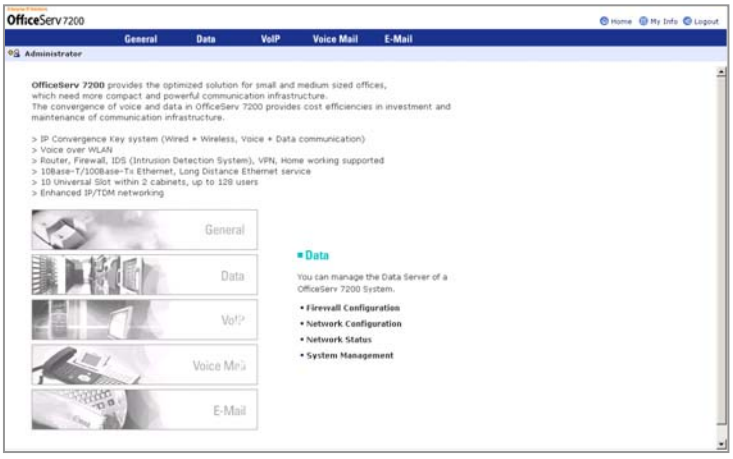
# Запуск сервера OfficeServ 7200 Data Server

Для запуска сервера OfficeServ 7200 Data Server выполните следующую процедуру.

1. Запустите Internet Explorer и введите IP-адрес сервера Data Server в строку адреса. Отобразится окно входа в систему, изображенное ниже.




2. Войдите в систему с использованием учетной записи и пароля администратора. Отобразится следующее окно.



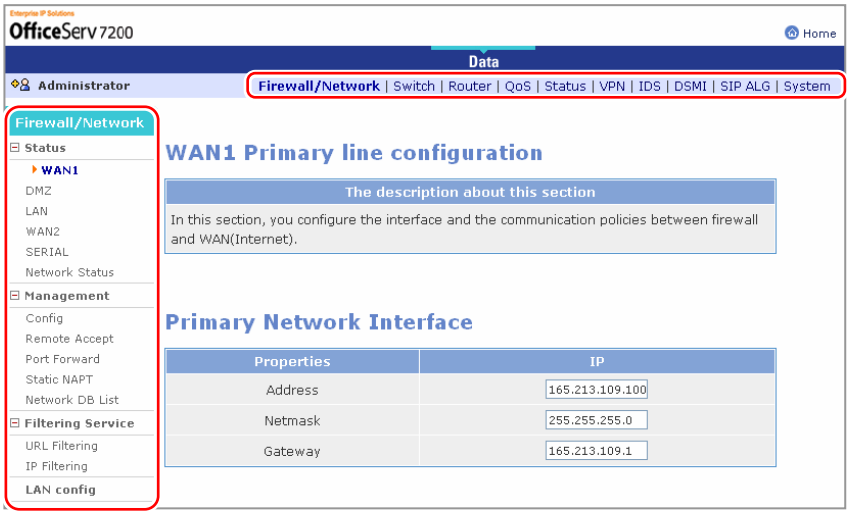
Нажмите кнопку [Logout] (Выход) в верхней части окна, чтобы завершить соединение с сервером Data Server.

NOTE

**Сервер OfficeServ 7200 Feature Server**

Меню VoIP, Voice Mail (Голосовая почта) и E-Mail (Электронная почта) относятся к серверу OfficeServ 7200 Feature Server. Подробную информацию об этих меню см. в руководстве пользователя сервера OfficeServ 7200 Feature Server.

*3.* Щелкните [Data] (Данные) для использования меню для сервера Data Server, изображенных в следующем окне.

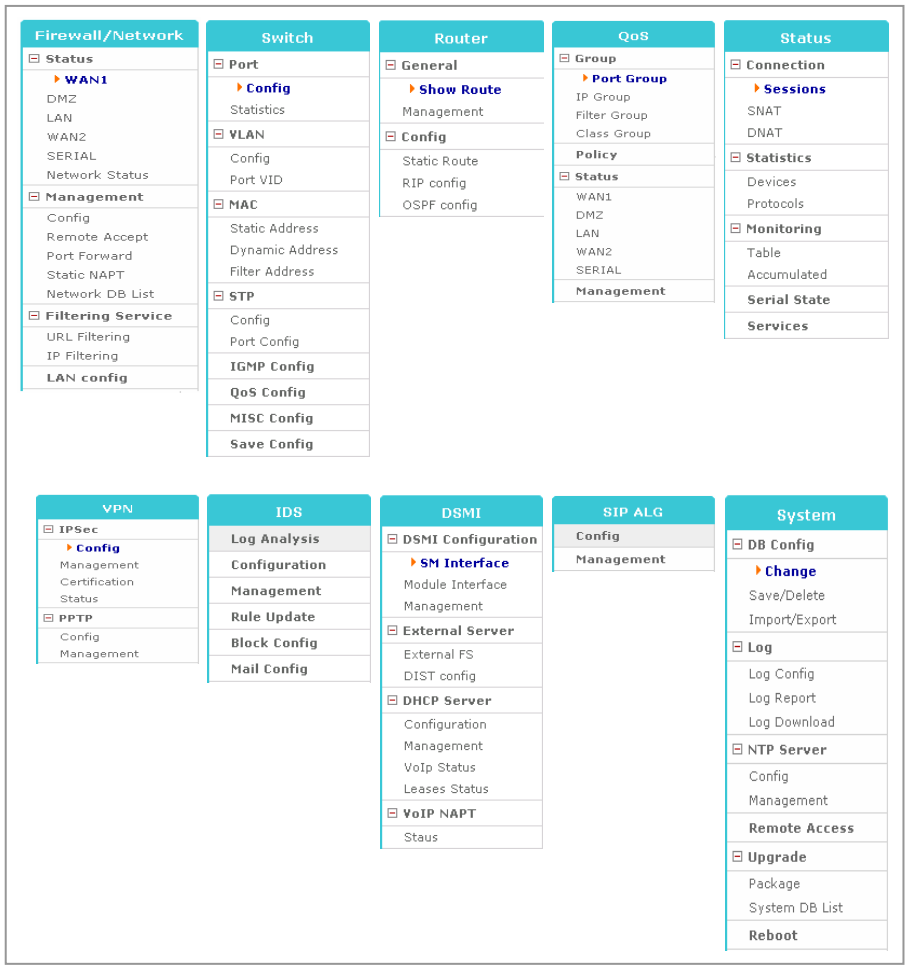



При выборе меню ‘Data’ (Данные) подменю сервера Data Server отображаются в левой части окна. Описания каждого подменю приведены в главе 3. Использование сервера OfficeServ 7200 Data Server.

# Глава 3. Использование сервера OfficeServ 7200 Data Server

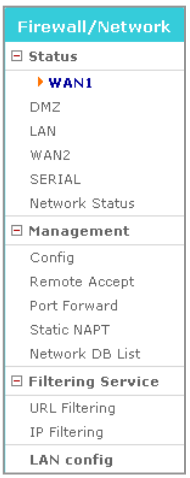
В данной главе описан процесс использование меню сервера OfficeServ 7200 Data Server.

Меню сервера OfficeServ 7200 Data Server выглядят следующим образом.



# Меню Firewall/Network (Сетевой экран/Сеть)

Чтобы отобразить подменю Firewall/Network (Сетевой экран/Сеть) выберите [Firewall/Network] (Сетевой экран/Сеть).




| Меню | Подменю | Описание |
|---|---|---|
| Status (Состояние) | WAN1 | Отображение пользовательских настроек порта WAN1, который является внешним портом. |
| | DMZ | Отображение пользовательских настроек порта DMZ, который является внутренним портом. |
| | LAN | Отображение пользовательских настроек порта LAN, который является внутренним портом. |
| | WAN2 | Отображение пользовательских настроек порта WAN2, который является внешним портом. |
| | SERIAL) | Отображение пользовательских настроек порта SERIAL (Последовательный v/35), который является внешним портом. |
| | Network status (Состояние сети) | Отображение состояния всех портов. |
| Management (Управление) | Config (Настройка) | Настройка сети и сетевого экрана. |
| | Remote Accept (Разрешение удаленного доступа) | Разрешение доступа к сетевому экрану. |

| | | |
|---|---|---|
| | Port Forward (Переадресация портов) | Установка переадресации портов |
| | Static NAPT (Статический NAPT) | Установка 1:1 NAT. |
| | Network DB List (Список сетевых баз данных) | Удаление баз данных, в которых хранятся настройки. |
| Filtering Service (Служба фильтрации) | URL Filtering (Фильтрация URL-адресов) | Блокировка доступа к домену из Интернета. |
| | IP Filtering (Фильтрация IP-адресов) | Блокировка доступа к IP-адресу из Интернета. |
| LAN config (Настройка локальной сети) | - | Установка скорости передачи данных и системы передачи данных. |

# Status (Состояние)

В меню [Status] (Состояние) отображаются настройки параметров WAN1, DMZ, LAN, WAN2 и SERIAL (Последовательный).

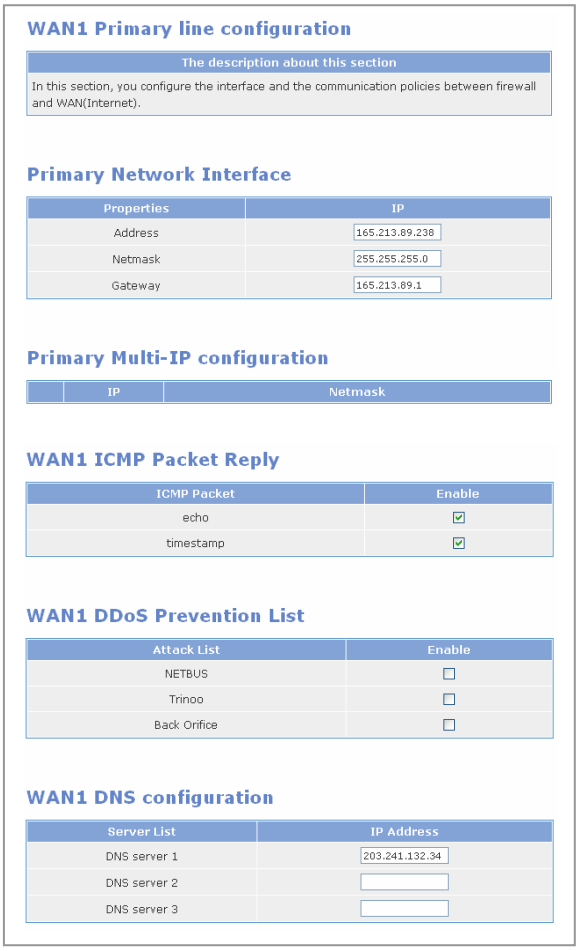
NOTE

**Процедура настройки порта**

Для настройки портов WAN1, LAN, DMZ, WAN2 и SERIAL (Последовательный) используется меню [Firewall/Network] (Сетевой экран/Сеть)→ - [Management] (Управление)→ - [Config] (Настройка). Процедуру настройки см. в описании меню.

## WAN1

В меню [Status] (Состояние)→ [WAN1] отображается настройка порта WAN1, который является внешним портом, использующим публичный IP-адрес.




**Настройки порта**

Подробные описания элементов для настройки портов см. в меню [Firewall/Network] (Сетевой экран/Сеть) → [Management] (Управление) → [Config] (Настройка).

## DMZ

В меню [Status] (Состояние)→ [DMZ] отображается настройка порта DMZ, который является внутренним портом, использующим локальный IP-адрес.

## LAN

В меню [Status] (Состояние) → [LAN] отображается настройка порта LAN, который является внутренним портом, использующим локальный IP-адрес.

## WAN2

В меню [Status] (Состояние) → [WAN2] отображается настройка порта WAN2, который является внешним портом, использующим публичный IP-адрес.

## SERIAL (ПОСЛЕДОВАТЕЛЬНЫЙ)

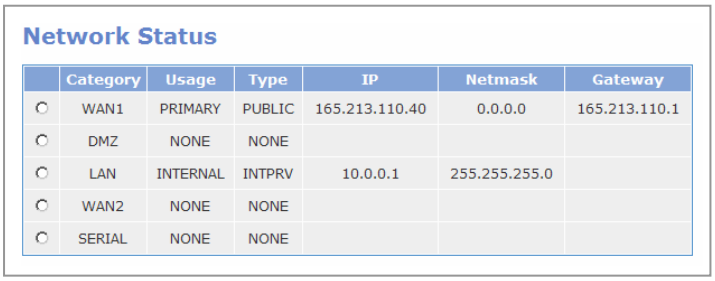
В меню [Status] (Состояние) → [SERIAL] (Последовательный) отображается настройка порта SERIAL (Последовательный), который является внешним портом, использующим публичный IP-адрес.


**Настройки портов DMZ, LAN, WAN2 и SERIAL (Последовательный)**

- Настройки портов DMZ, LAN, WAN2 и SERIAL (Последовательный) отображаются в окне, аналогичном окну [Status] (Состояние) → [WAN1].
- Если к порту не подключено ни одной линии (в меню [Management] (Управление)→ [Config] (Настройка) для него отображается значение ‘Not Used’ (Не используется)), в поле его настроек отображается сообщение ‘No line’s connected to this port’ (Линя к порту не подключена).

# Network Status (Состояние сети)

В меню [Status] (Состояние)→ [Network Status] (Состояние сети) отображаются настройки для портов WAN1, DMZ, LAN, WAN2 и SERIAL (Последовательный).




| Элемент | Описание |
|---|---|
| Category (Категория) | Порты WAN1, DMZ, LAN, WAN2 и SERIAL (Последовательный) |
| Usage (Использование) | - NONE (HET): линия не используется<br>- PRIMARY (Основной): основная используемая линия<br>- INTERNAL (Внутренний): локальная сеть |
| Type (Тип) | - NONE (HET): линия не используется<br>- PUBLIC (Общий): порт, использующий общий IP-адрес<br>- INTPRV (Внутренний, частный): внутренний порт, использующий локальный IP-адрес |

# Management (Управление)

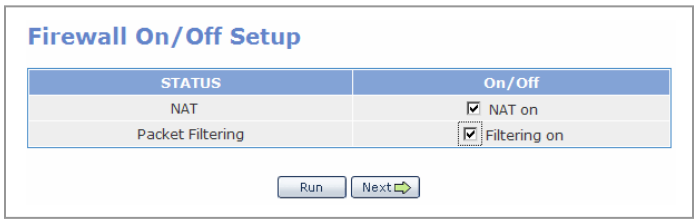
Меню [Management] (Управление) используется для настройки портов, относящихся к сетевому экрану и сети.

## Config

Меню [Config] (Настройка) используется для настройки портов WAN1, LAN, DMZ, WAN2 и SERIAL (Последовательный). Для настройки элементов в каждом окне выберите [Management] (Управление)→ [Config] (Настройка). Нажмите кнопку [Next] (Далее) и используйте следующую процедуру для настройки сетевого экрана и сети.

## Первоначальная настройка

*1.* Выберите [Management] (Управление)→ [Config] (Настройка), чтобы отобразить окно, изображенное ниже. По умолчанию отображаются элементы ‘NAT’ и ‘Packet Filtering’ (Фильтрация пакетов). Установите флажки, чтобы поменять состояние на ‘On’ (Вкл.) и нажмите кнопку [Run] (Запустить).
Если флажки уже установлены, нажмите кнопку [Next] (Далее).

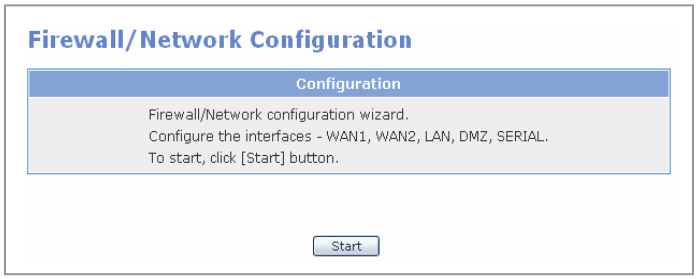



NOTE

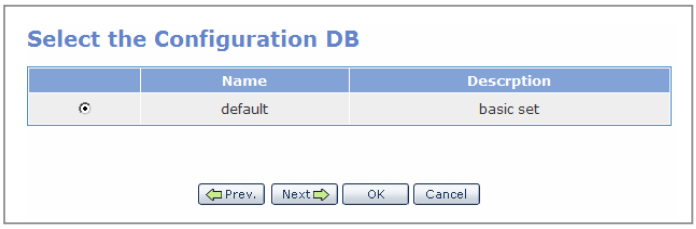
**Network Address Translation(NAT)**

NAT используется для переадресации пакетов, направленных из локальной сети во внешнюю сеть через сетевой экран.

*2.* Для начала настройки сетевого экрана и сети нажмите кнопку [Start] (Запуск).

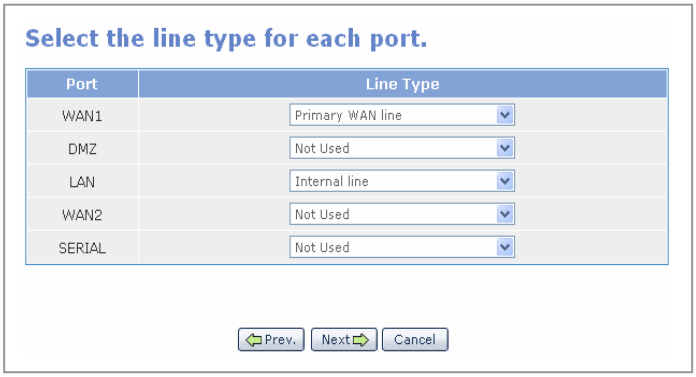



*3.* Задать новые настройки, а также запустить или изменить заранее созданные файлы настроек можно с помощью следующего окна. По умолчанию для порта LAN назначен IP-адрес 10.0.0.1. Выберите элемент ‘default’ (по умолчанию) и нажмите кнопку [Next] (Далее).



## Установка типа линии для каждого порта

Внешние порты (WAN1, WAN2, SERIAL (Последовательный)) используют общие IP-адреса, а внутренние (например, DMZ, LAN) - личные IP-адреса. Выберите тип линии для каждого порта, как показано ниже.




Внешний порт (WAN1,WAN2, SERIAL (Последовательный))

- Primary WAN line (Первичная линия WAN): основная используемая линия
- Secondary WAN line (Вторичная линия WAN): дополнительная линия
- Third WAN line (Третичная линия WAN): дополнительная линия
- Not Used (Не используется): не используется ни одна линия WAN

• Внутренний порт (DMZ, LAN)

- Internal line (Внутренняя линия): используется внутренняя линия
- Not Used (Не используется): внутренняя линия не используется

Настройте сеть следующим образом: для порта WAN1 выберите основную линию (Primary WAN line (Первичная линия WAN)), для порта LAN выберите внутреннюю линию (Internal line (Внутренняя линия)), а для портов WAN2, SERIAL (Последовательный) и DMZ укажите Not Used (Не используется).

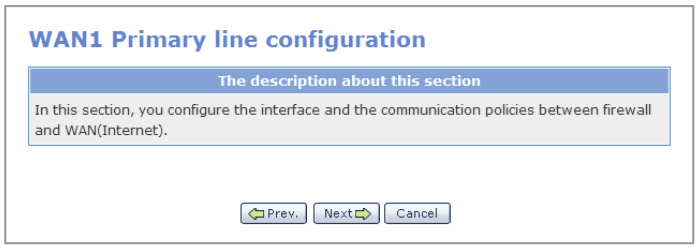
CAUTION

**Переменный IP для DHCP, PPPoE и VDSL**

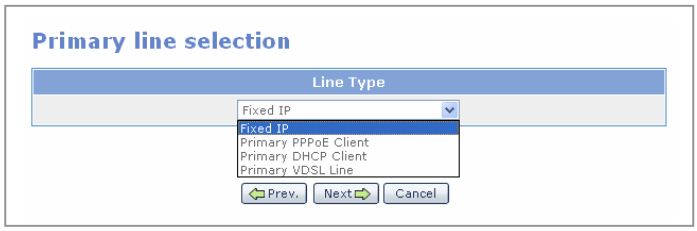
При использовании переменного IP-адреса информация об общих IP-адресах (например, в меню ‘Port Forward’ (Переадресация портов) и ‘Static NAPT’ (Статический NAPT)) не изменяется автоматически. Для служб VoIP, требующих настройки меню ‘Port Forward’ (Переадресация портов) и ‘Static NAPT’ (Статический NAPT), и служб VPN, требующих настройки IP-адреса WAN, необходимо использовать параметр ‘Fixed IP’ (Фиксированный IP-адрес).

## Настройка WAN1

*1.* Первое окно для настройки порта WAN1 с использованием параметра ‘Primary WAN line’ (Первичная линия WAN) выглядит следующим образом. Для начала настройки порта WAN1 нажмите кнопку [Next] (Далее).

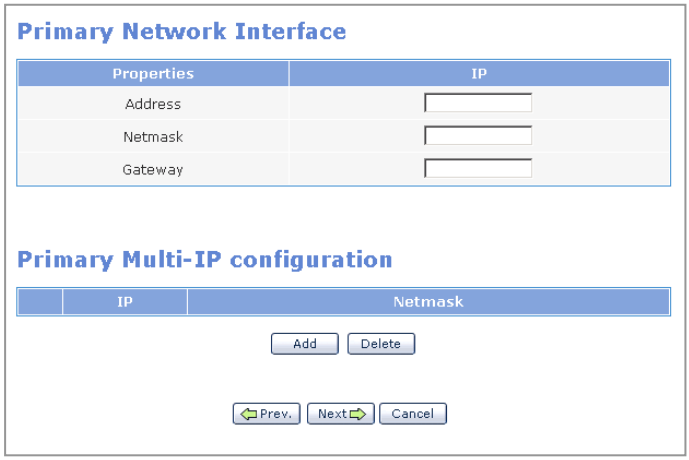



*2.* Выберите тип линии для первичной линии WAN. Выберите для внешней сети один из четырех параметров, показанных ниже.




Четыре параметра для первичной линии WAN описаны ниже.

- Fixed IP (Фиксированный IP-адрес): введите значения в поля Address (Адрес), Netmask (Маска сети) и Gateway (Шлюз) для настройки порта WAN1 во внешней сети, где используется статический IP-адрес, и нажмите кнопку [Next] (Далее). Для добавления еще одного IP-адреса нажмите кнопку [Add] (Добавить) и добавьте его

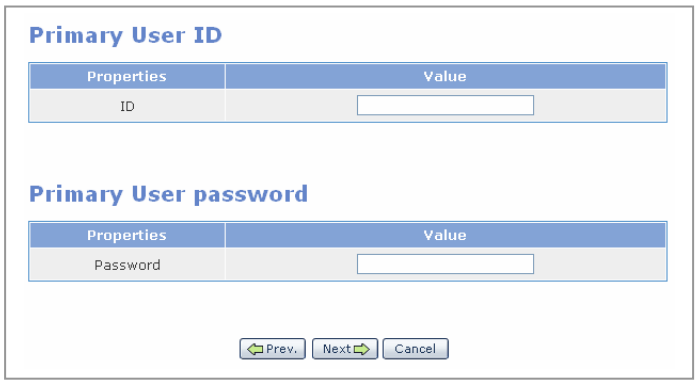



CAUTION

**Предупреждение об изменении сетевых интерфейсов**

В случае изменения параметров сетевого интерфейса (например, IP-адреса, шлюза и маски подсети) во время работы маршрутизатора используемые им IP-сеансы будут на время приостановлены.

- Primary PPPoE Client (Первичный клиент PPPoE): введите имя пользователя и пароль для подключения к внешней сети, в которой используется переменный IP-адрес через PPPoE, а затем нажмите кнопку [Next] (Далее).

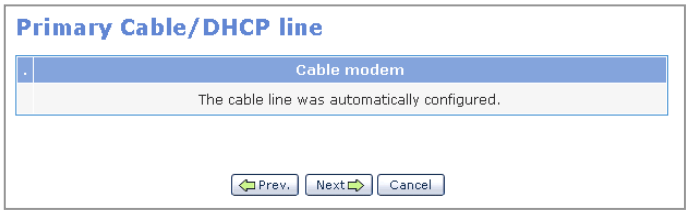


CAUTION

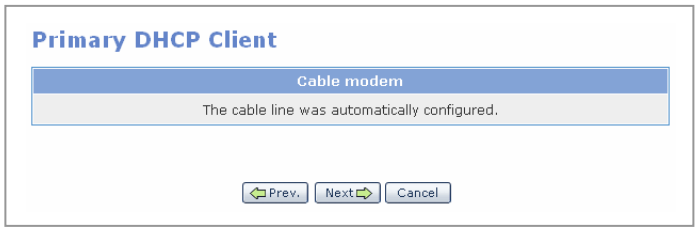
**Удалить временные файлы Интернета**

Удалите временные файлы Интернета после обновления пакета Data Server. Выберите [Internet Explorer] → [Сервис] → [Свойства обозревателя] и в меню [Временные файлы Интернета] нажмите кнопки [Удалить "Cookie"] и [Удалить файлы].
Если временные файлы Интернета не удалены, настройки управление Data Server через WEB-интерфейс отобразятся не правильно.

- Primary Cable line (Первичная кабельная линия): внешняя сеть, использующая кабельный модем
  Поскольку кабельные модемы устанавливаются автоматически, нажмите кнопку [Next] (Далее) и перейдите к следующему окну.




- Primary DHCP Client (Первичный клиент DHCP): информация о порте WAN1 автоматически настроится на внешнюю сеть, в которой используется переменный IP-адрес, назначаемый с помощью DHCP сервера внешней сети. Для перехода к следующему окну нажмите кнопку [Next] (Далее).

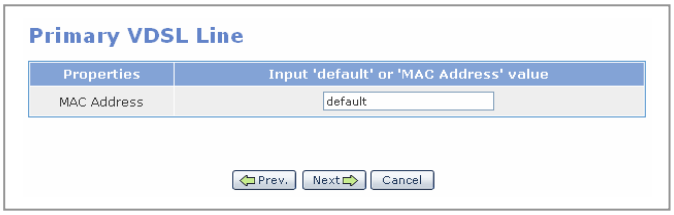



NOTE

**Настройки PPPoE/DHCP/VDSL**

Производительность при выгрузке и загрузке данных может ухудшаться в зависимости от возможностей модема.

- Primary VDSL line (Первичная линия VDSL): внешняя сеть, использующая модем VDSL.
  Введите в поле ‘Mac address’ (MAC-адрес) значение ‘default’ (по умолчанию), чтобы отключить проверку подлинности MAC-адресов, и нажмите кнопку [Next] (Далее). Введите MAC-адрес в поле ‘Mac address’ (‘Mac-адрес) для использования функции копирования MAC-адресов.



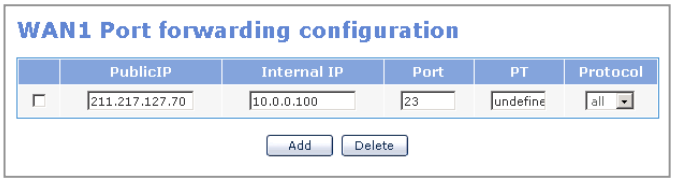

NOTE

**Функция копирования MAC-адресов**

При выполнении проверки подлинности в исходящих пакетах MAC-адресов компьютеров, подключенных к плате, эти MAC-адреса заменяются на MAC-адрес интерфейса WAN1.

*3.* Настройте элементы, указанные ниже, и нажмите кнопку [Next] (Далее).

- WAN1 Port forwarding configuration (Настройка переадресации для порта WAN1)
  Этот параметр используется для поддержки внешними серверами служб внутренних серверов, расположенных за сетевым экраном.




Предположим, что публичный IP-адрес порта WAN1 - ‘211.217.127.70’, а локальный IP-адрес внутреннего сервера - ‘10.0.0.100’. Внешний компьютер перед сетевым экраном получит доступ на службу Telnet внутреннего сервера после настройки переадресации для порта Telnet.
Нажмите кнопку [Add] (Добавить) и введите значения для параметров, описанных ниже. После ввода данных, приведенных

в окне, внешняя сеть может установить соединение через адрес ‘211.217.127.70’ с адресом внутренней сети (10.0.0.100) для службы Telnet.

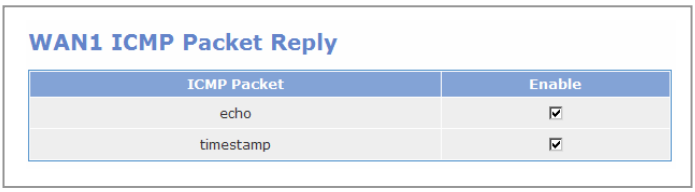
- PublicIP (Общий IP-адрес): публичный IP-адрес сетевого экрана
- InternalIP (Внутренний IP-адрес): локальный IP-адрес внутреннего сервера, подключенного к сетевому экрану
- Port (Порт): порт сетевого экрана (например, порт сервера Telnet)
- Зкщещсщд (Протокол)Ж протокол (фддб есзб гвз)

NOTE

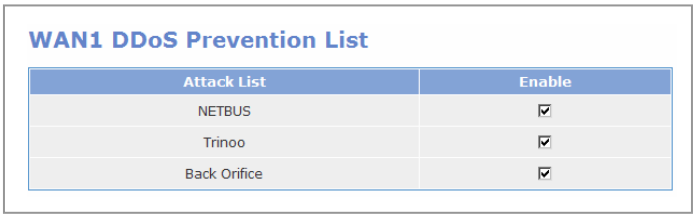
**Настройка диапазона портов**

- При использовании диапазона портов от 0 до 100 введите ‘0:100’.
- ‘0:’ обозначает все порты.

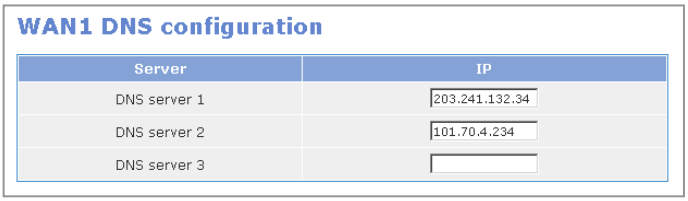
- WAN1 ICMP Packet Reply (Ответ на пакеты ICMP WAN1)
  По умолчанию сетевой экран не отвечает на эхо запрос ICMP и запрос временной метки ICMP. Однако если флажки ‘echo’ (эхо) и ‘timestamp’ (штамп времени) установлены, то ответ на внешнюю команду ping будет производиться. Если флажки не установлены, происходит отключение запроса по истечении времени ожидания ответа.




- Предотвращение атак DDoS на порту WAN1
  Установите изображенные ниже флажки для предотвращения атак DDoS с использованием соответствующего шпионского программного обеспечения.

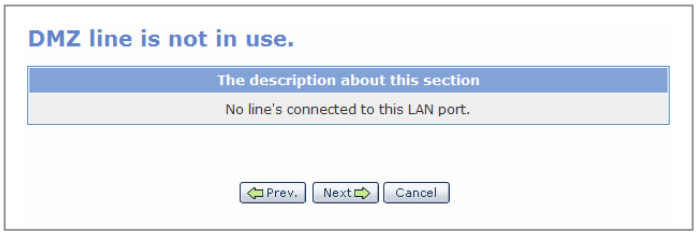


- WAN1 DNS configuration (Настройка DNS для порта WAN1)
  Введите IP-адрес сервера DNS. При использовании PPPoE/DHCP адрес DNS не вводится. Проверка доменных имен будет выполняться внешним сервером.




## Настройка DMZ

В приведенном ниже окне для параметров DMZ установлено значение ‘No line’ (Нет линии). Это значение было установлено в окне <Select the line type for each port> (Установка типа линии для каждого порта) (см. раздел ‘Установка типа линии для каждого порта’).
Нажмите кнопку [Next] (Далее) и перейдите к следующему окну.




NOTE

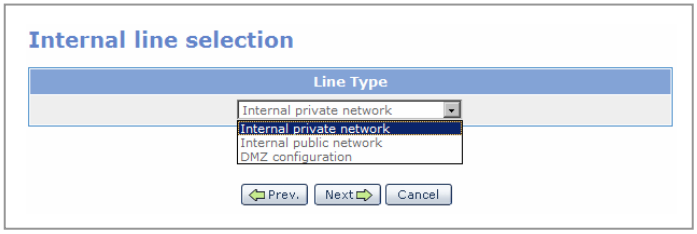
**При использовании параметра ‘Internal line (Внутренняя линия)’**

Если в окне <Select the line type for each port> (Установка типа линии для каждого порта) для порта DMZ было установлено значение ‘Internal line’ (Внутренняя линия) (см. раздел ‘Установка типа линии для каждого порта’), выполните процедуру установки, описанную в разделе "Настройка LAN".

## Настройка LAN

1. В приведенном ниже окне для параметра LAN установлено значение ‘Internal line’ (Внутренняя линия). Это значение было установлено в окне <Select the line type for each port> (Установка типа линии для каждого порта) (см. раздел ‘Установка типа линии для каждого порта’). Для начала настройки порта LAN нажмите кнопку [Next] (Далее).

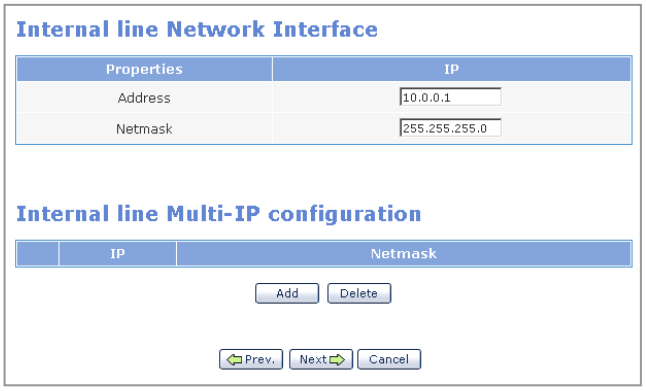

2. Выберите тип внутренней линии.



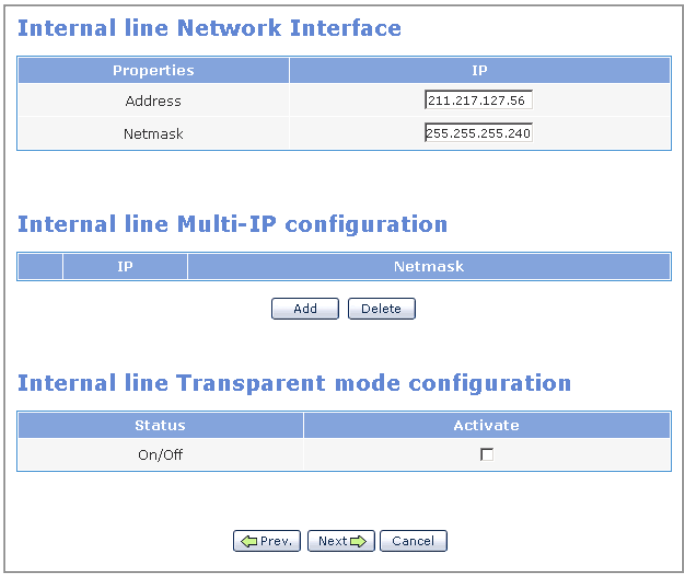

Ниже описываются типы внутренних линий.

- Internal private network (Внутренняя частная сеть): выберите этот параметр для настройки внутренней сети с использованием локальных IP-адреса.

  Введите значения для параметров IP address (IP-адрес), Netmask (Маска сети) и укажите шлюз для использования порта LAN в качестве внутренней локальной сети, а затем нажмите кнопку [Next] (Далее). Для добавления еще одного IP-адреса, нажмите кнопку [Add] (Добавить) и добавьте элемент.

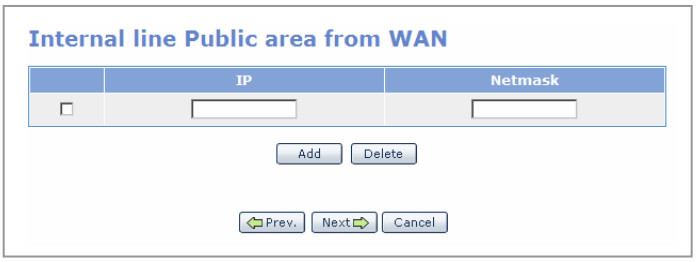



- Internal public network (Внутренняя общая сеть): выберите этот параметр для настройки внутренней сети с использованием публичного IP-адреса.

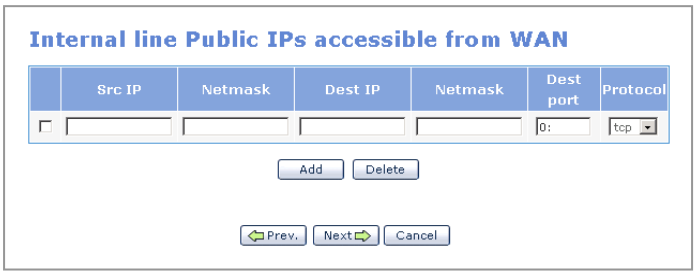



Для добавления IP-адреса, нажмите кнопку [Add] (Добавить). Если установлен флажок ‘Internal line Transparent mode configuration’ (Настройка прозрачного режима внутренней линии), будет включена функция Proxy ARP. Если флажок не установлен, функция отключена.

Введите значения для параметров IP address (IP-адрес) и Netmask (Маска сети) для использования локальной сети в качестве внутренней общей сети, а затем нажмите кнопку [Next] (Далее).




- Если хост, на котором используется публичный IP-адрес, находится не во внутренней, а во внешней сети, настройте параметры, описанные выше.
- IP (IP-адрес): введите IP-адрес хоста. Если имеется возможность настроить каждую сеть, используйте соответствующий сетевой адрес.
- Netmask (Маска сети): Введите ‘255.255.255.255’. Если имеется возможность настроить каждую сеть, используйте соответствующий адрес подсети.
  Введите значения для параметров IP address (IP-адрес) и Netmask (Маска сети), а затем нажмите кнопку [Next] (Далее). Отобразится окно, изображенное ниже.

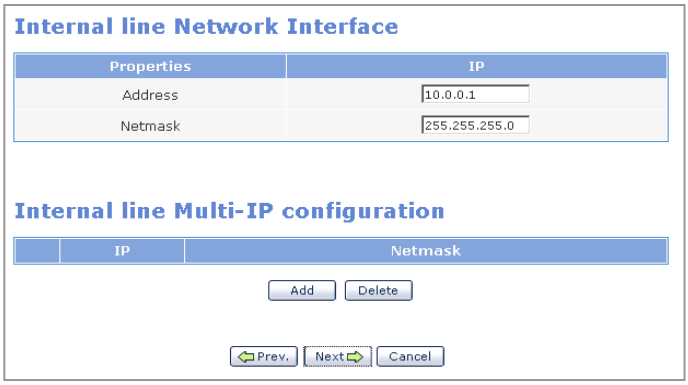



Для добавления еще одного IP-адреса, отличного от IP-адреса внешней линии, используемого в настоящее время, нажмите кнопку [Add] (Добавить) и добавьте элемент.
Для использования функции Proxy ARP установите флажок ‘Internal line Transparent mode configuration’ (Настройка прозрачного режима внутренней линии).

Настройте параметры ‘Src IP’ (Исходный IP-адрес) и ‘Netmask’ (Маска сети), чтобы разрешить доступ из внешней сети к указанному серверу с публичным IP-адресом расположенным за сетевым экраном. Установите для параметров ‘Src IP’ (Исходный

IP-адрес) и ‘Netmask’ (Маска сети) значение ‘0.0.0.0’, чтобы разрешить доступ из всех внешних сетей.

- DMZ configuration (Настройка DMZ): выберите этот параметр для настройки зоны DMZ.



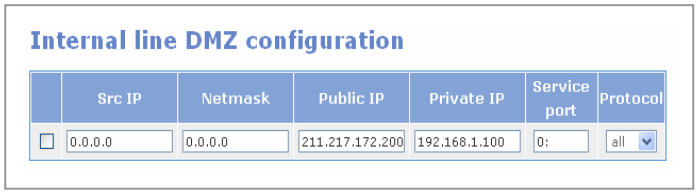

Введите значения для параметров IP address (IP-адрес), Netmask (Маска сети) и укажите шлюз для использования локальной сети в качестве сети DMZ, а затем нажмите кнопку [Next] (Далее). Для добавления еще одного IP-адреса, нажмите кнопку [Add] (Добавить) и добавьте элемент.


Настройте параметры ‘Src IP’ (Исходный IP-адрес) и ‘Netmask’ (Маска сети), чтобы разрешить внешним сетям доступ к указанному серверу с общим IP-адресом внутри сетевого экрана. Установите для параметров ‘Src IP’ (Исходный IP-адрес) и ‘Netmask’ (Маска сети) значение ‘0.0.0.0’, чтобы разрешить доступ из всех внешних сетей.

*3.* Включите порта для переадресации пакетов, полученных через сеть WAN, к хосту, расположенного в DMZ.

- Src IP (Исходный IP-адрес): введите исходный IP-адрес пакета, который необходимо переадресовать на порт.
- Netmask (Маска сети): введите маску сети пакета, который необходимо переадресовать на порт.
- Public IP (Публичный IP-адрес): введите IP-адрес WAN.
- Private IP (Локальный IP-адрес): введите IP-адрес хоста, расположенного в DMZ.
- Service Port (Служебный порт): введите номер порта, на который выполняется переадресация пакета.
- Protocol (Протокол): выберите тип протокола для переадресации.

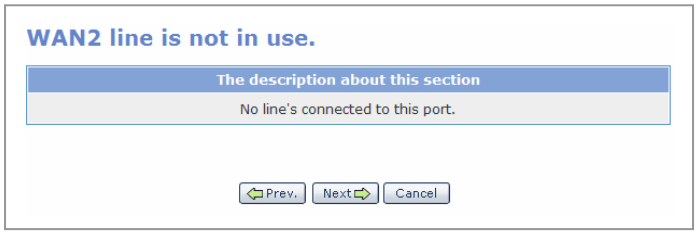
В следующем окне представлен пример переадресации всех пакетов (Src IP (Исходный IP-адрес): 0.0.0.0, Network (Сеть): 0.0.0.0, Service Port (Служебный порт): 0, Protocol (Протокол): all (все)), проходящих через IP-адрес интерфейса (211.217.172.200) к хосту (192.168.1.100), расположенному в DMZ.




*4.* Если порты LAN и DMZ настраивались с использованием внутренней локальной сети, разрешите серверу внутри зоны DMZ доступ к серверу локальной сети LAN. Нажмите кнопку [Add] (Добавить), чтобы настроить IP-адрес, а зачем нажмите кнопку [Next] (Далее).

## Настройка WAN2

В приведенном ниже окне для порта WAN2 установлено значение ‘No line’ (Нет линии). Это значение было установлено в окне <Select the line type for each port> (Установка типа линии для каждого порта) (см. раздел ‘Установка типа линии для каждого порта’).
Нажмите кнопку [Next] (Далее) и перейдите к следующему окну.



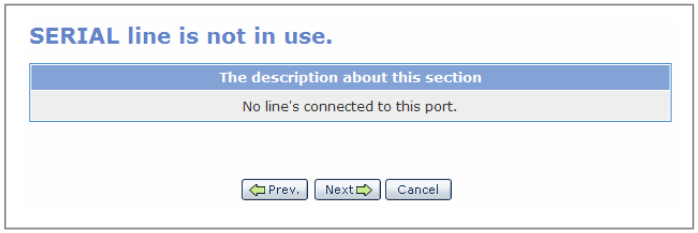

NOTE

**Настройка WAN2**

Если в окне <Select the line type for each port> (Установка типа линии для каждого порта) для порта WAN2 было установлено значение Primary WAN line (Первичная линия WAN), Secondary WAN line (Вторичная линия WAN) или Third WAN line (Третичная линия WAN) (см. раздел ‘Установка типа линии для каждого порта’), выполните процедуру установки, описанную в разделе "Настройка ‘WAN1".

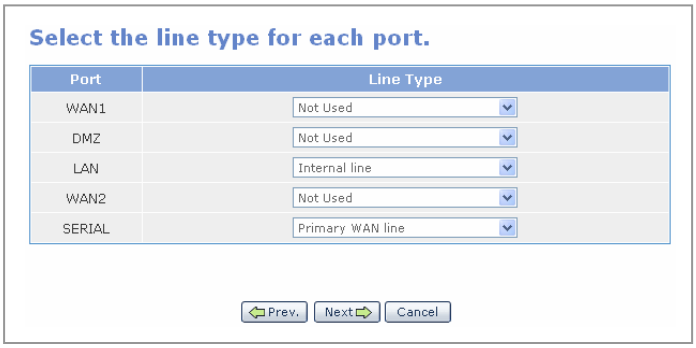
## Настройка SERIAL (Последовательного порта)

В приведенном ниже окне для параметра SERIAL (Последовательный) установлено значение ‘No line’ (Нет линии). Это значение было установлено в окне <Select the line type for each port> (Установка типа линии для каждого порта) (см. раздел ‘Установка типа линии для каждого порта’).
Нажмите кнопку [Next] (Далее) и перейдите к следующему окну.

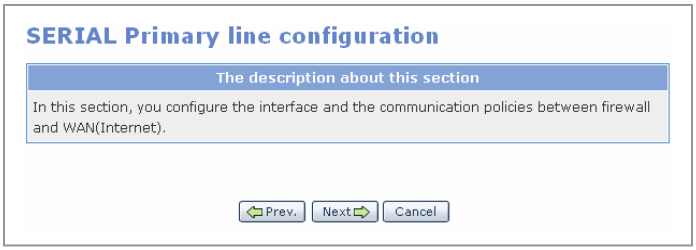



Для использования порта SERIAL (Последовательный) в качестве первичной линии WAN используйте следующую процедуру.

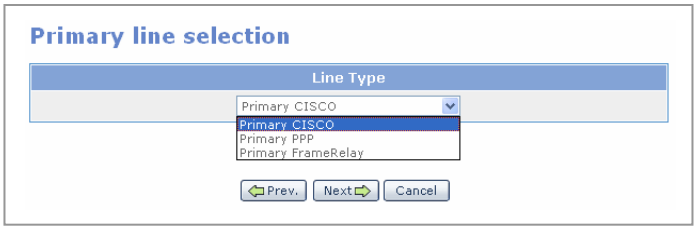
1. В окне <Select the line type for each port> (Установка типа линии для каждого порта) установите для порта SERIAL значение ‘Primary WAN line’ (Первичная линия WAN) (см. раздел ‘Установка типа линии для каждого порта’) и нажмите кнопку [Next] (Далее).



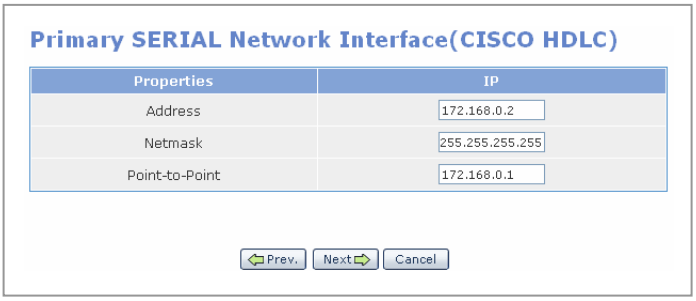

2. Для начала настройки порта SERIAL (Последовательный) нажмите кнопку [Next] (Далее).



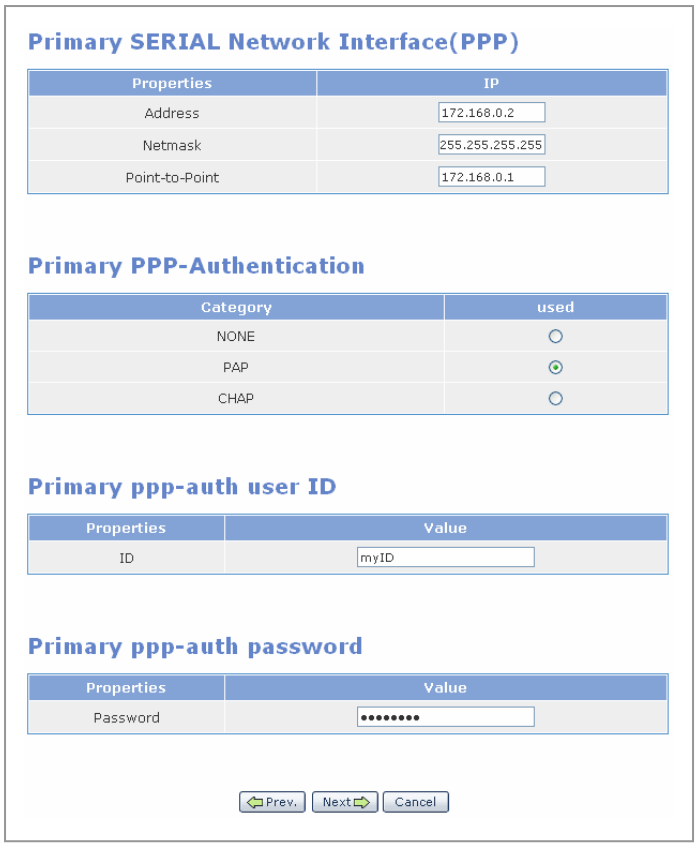
*3.* Выберите тип первичной линии.




- Primary CISCO (Первичная CISCO)
  В окне <Primary line selection> (Выбор первичной линии) выберите ‘Primary CISCO’ (Первичная CISCO) и нажмите кнопку [Next] (Далее), после чего отобразится окно, изображенное ниже. Введите значения параметров и нажмите кнопку [Next] (Далее). Метод CISCO относится к технологии HDLC, разработанной компанией Cisco.

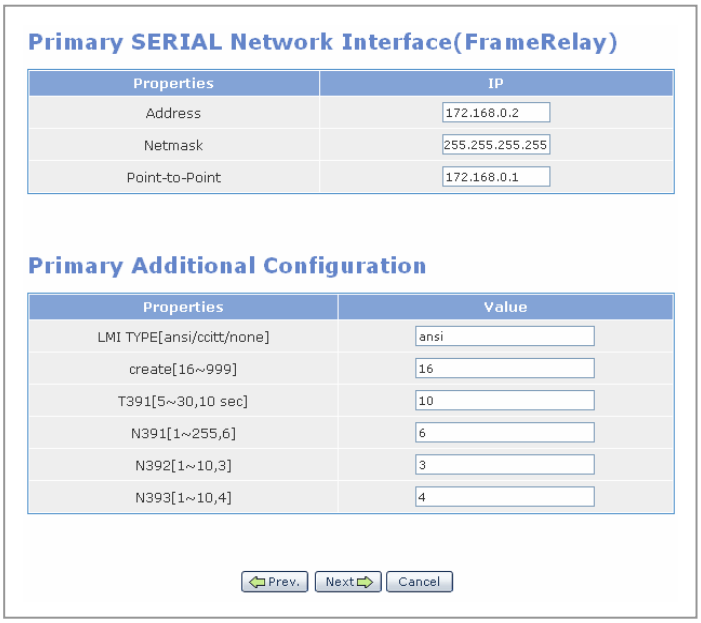


- Primary PPP (Первичная PPP)
  В окне <Primary line selection> (Выбор первичной линии) выберите ‘Primary PPP’ (Первичная PPP) и нажмите кнопку [Next] (Далее), после чего отобразится окно, изображенное ниже. Введите значения для параметров IP address (IP-адрес), Netmask (Маска сети) и элементов точка-точка, а затем нажмите кнопку [Next] (Далее).




Если для параметра Primary PPP-Authentication (Первичная PPP - проверка подлинности) установлено значение ‘NONE’ (Нет), вводить имя пользователя и пароль не требуется.

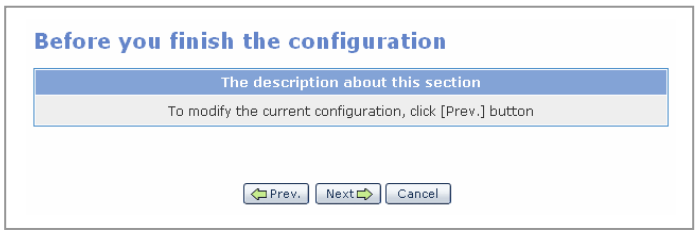
- Primary FrameRelay (Первичный FrameRelay)
  В окне <Primary line selection> (Выбор первичной линии) выберите ‘Primary FrameRelay’ (Первичный FrameRelay) и нажмите кнопку [Next] (Далее), после чего отобразится окно, изображенное ниже. Введите значения следующих параметров и нажмите кнопку [Next] (Далее):



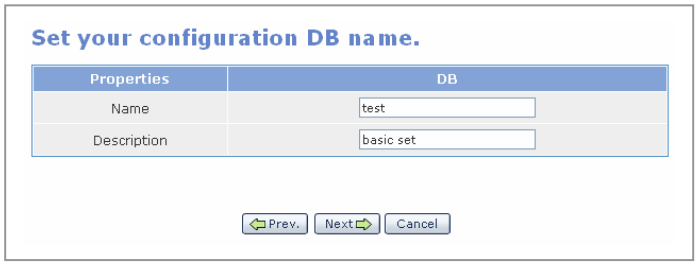

| Элемент | Описание |
|---|---|
| LMI TYPE [ansi, ccitt, none] (Тип LMI [ansi, ccitt, нет]) | Тип сигнала |
| create[16~999] (создать [16~999]) | Номер канала сигнала. Постоянная виртуальная цепь (PVC). |
| T391[5 - 30,10 sec] (T391[5 - 30,10 сек]) | Временной интервал DTE для отправки сигнала проверки активности |
| N391[1 - 255,6] | Интервал полного опроса состояния, означающий цикл запроса полной информации о состоянии на основе количества раз отправки сигнала проверки активности. |
| N392[1 - 10,3] | Счетчик порога ошибок, учитывающий количество повторов ошибок перед деактивацией ссылки. |
| N393[1 - 10,4] | N393 всегда выше или ниже значения N392, поскольку число указывает, сколько событий будет сохранено. |

## Сохранение настроек

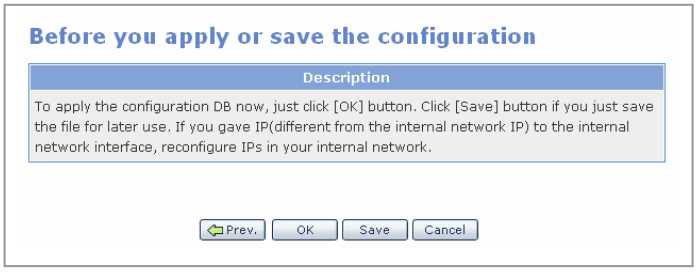
1. Ниже изображено окно, в котором отображается завершающий этап настройки сетевого экрана и сети. Нажмите кнопку [Next] (Далее) и перейдите к следующему окну.




2. Введите значения в поля Name (Имя) и Description (Описание) и нажмите кнопку [Next] (Далее), чтобы сохранить настройки в базе данных. В поле ‘Name’ (Имя) можно вводить только текст в верхнем и нижнем регистрах и цифры. Специальные символы вводить нельзя, а значение ‘default’ (По умолчанию) недоступно.

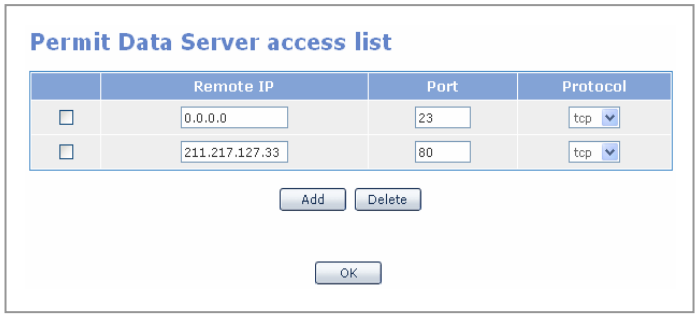



3. Для сохранения настроек в файл под именем, заданным выше, нажмите кнопку [Save] (Сохранить). Нажмите кнопку [OK] для применения настроек после сохранения или нажмите кнопку [Cancel] (Отмена) для отмены.



# Remote Accept (Разрешение удаленного доступа)

Меню [Remote Accept] (Разрешение удаленного доступа) используется для разрешения доступа для указанного IP-адреса к сетевому экрану. Если в меню [Management] (Управление) '→ [Config] (Настройка) - Firewall On/Off Setup' (Сетевой экран вкл/выкл) для параметра 'Packet Filtering' (Фильтрация IP-адресов) установлено значение 'Filtering on' (Фильтрация вкл), доступ к сетевому экрану извне запрещен. Для внешних серверов доступ к сетевому экрану закрыт. При необходимости, однако, некоторые серверы могут получить доступ.
Выберите [Management] (Управление)→ [Remote Accept] (Разрешение удаленного доступа), установите значения для IP-адреса, порта и протокола, как показано ниже, а затем нажмите кнопку [OK].




При использовании значений параметров, указанных выше, сервер с IP-адресом '211.217.127.33' может получить доступ к сетевому экрану через Интернет. Кроме того, другие внешние серверы могут получить доступ к сетевому экрану с использованием таких программ, как Telnet и SSH.

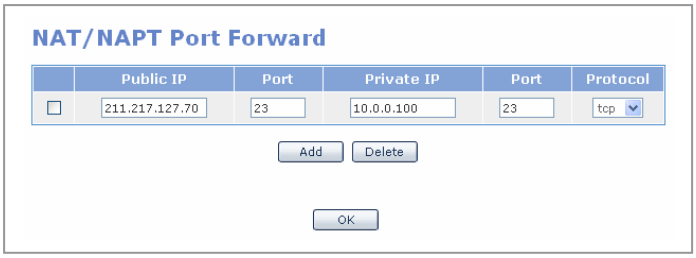
CAUTION

**Предупреждение системы безопасности**

Обратите внимание, что доступ к сетевому экрану разрешен для всех внешних пользователей, если для параметра Remote IP (Удаленный IP-адрес) установлено значение '0.0.0.0', а для параметра Port (Порт) - значение '0:'.

# Port Forward (Переадресация портов)

Меню [Port Forward] (Переадресация портов) используется для переадресации пакетов, что обеспечивает возможность использовать извне службы внутренних серверов, расположенных за сетевым экраном.




Предположим, что внутренний сервер использует публичный IP-адрес сетевого экрана ‘211.217.127.70’ и локальный IP-адрес ‘10.0.0.100’. Показанная конфигурация дает возможность доступа извне по адресу ‘211.217.127.70’ на локальный сервер с адресом ‘10.0.0.100’ службы telnet.

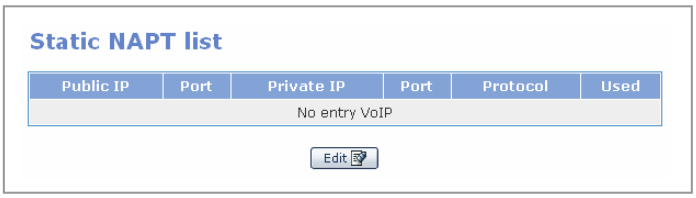
- Public IP (Общий IP-адрес): публичный IP-адрес сетевого экрана
- Internal IP (Внутренний IP-адрес): локальный IP-адрес внутреннего сервера, подключенного к сетевому экрану
- Port (Порт): номер порта службы (например, порт сервера telnet)
- Protocol (Протокол): выбор протокола (all, tcp, udp)

NOTE

**Задание порта**

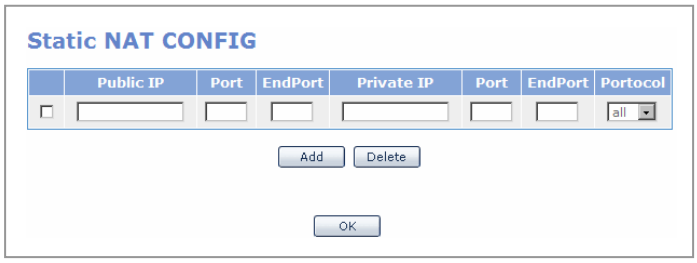
Пользователи не могут указать диапазон портов. При необходимости используйте меню Static NAPT (Статический NAPT).

## Static NAPT (Статический NAPT)



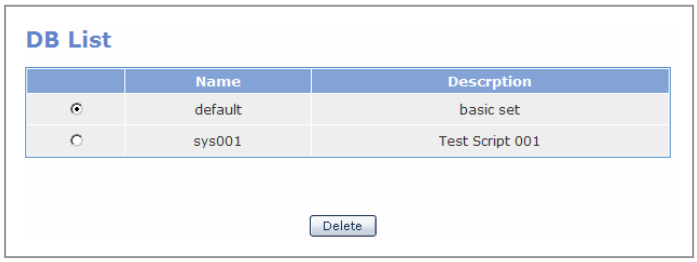

В окне ‘Static NAPT list’ (Список статического NAPT) отображаются настройки меню [Static NAPT] (Статический NAPT).
В общем, в этом окне отображается также значение параметра ‘VoIP NAPT’ в меню DSMI, а также пользовательская настройка меню ‘Static NAPT’ (Статический NAPT).

Для перехода к окну, в котором можно ввести значения для параметра Static NAPT (Статический NAPT), нажмите кнопку [Edit] (Редактировать).




## Network DB List (Список сетевых баз данных)

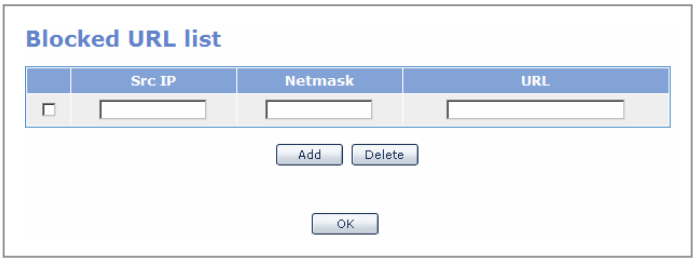
Меню [DB List] (Список баз данных) используется для удаления файла настроек, сохраненного с помощью меню [Management] (Управление) → [Config] (Настройка).



# Filtering Service (Служба фильтрации)

Меню [Filtering Service] (Служба фильтрации) используется для блокировки указанных URL- и IP-адресов.

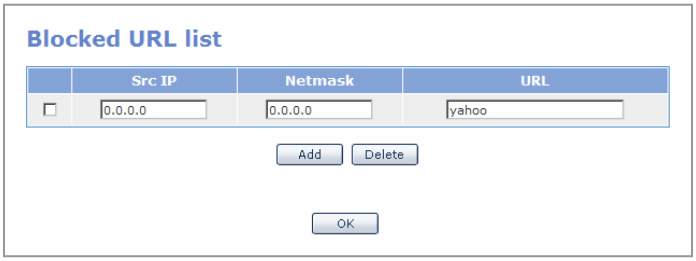
## URL Filtering (Фильтрация URL-адресов)



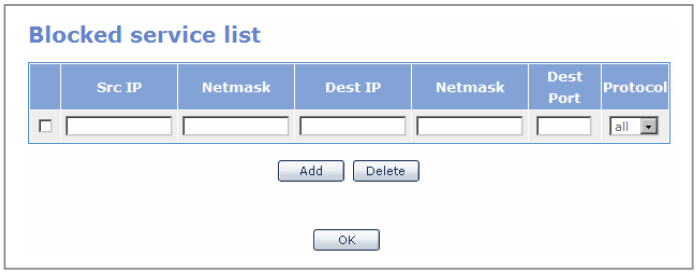

Меню [URL Filtering] (Фильтрация URL-адресов) используется для запрета доступа к указанному URL-адресу с удаленного хоста или сети.

- SrcIP (Исходный IP-адрес): внутренний хост или сеть, в которой будет производиться фильтрация. Введите IP-адрес для фильтрации URL-адресов от каждого хоста и сетевые адреса для фильтрации URL-адресов из каждой сети.
- Netmask (Маска сети): установите для параметра Netmask (Маска сети) значение ‘255.255.255.255’ для фильтрации URL-адресов от каждого хоста. Укажите подсеть сети для фильтрации URL-адресов из каждой сети.
- URL (URL-адрес): имя сайта (домен), которое необходимо заблокировать

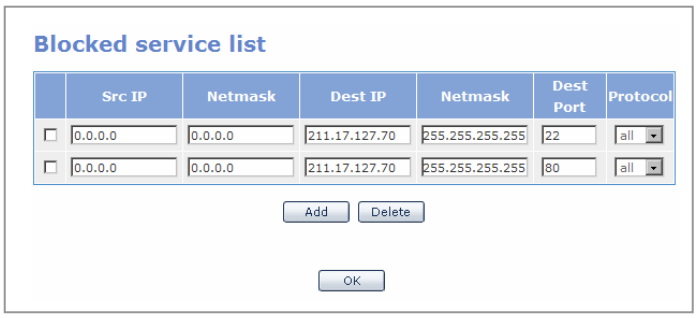
На рисунке ниже приведен пример блокировки доступа на сайт ‘yahoo’ для всех внутренних пользователей. Введите значения, показанные на рисунке, и нажмите кнопку [OK] для завершения настройки.



## IP Filtering (Фильтрация IP-адресов)



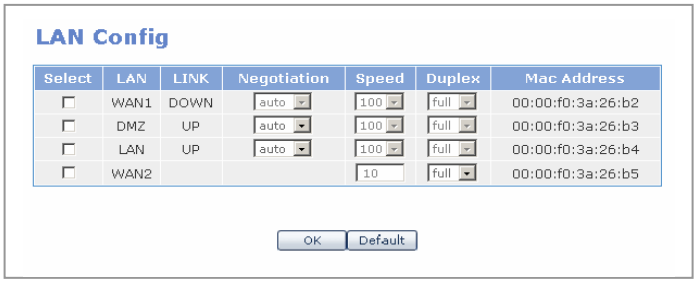

Меню [IP Filtering] (Фильтрация IP-адресов) используется для запрета доступа к указанной службе внешнего IP-адреса для внутренних пользователей. Введите соответствующие значения для параметров ‘Src IP’ (Исходный IP-адрес) и ‘Netmask’ (Маска сети), а также укажите информацию о службе внешней сети, к которой необходимо запретить доступ. Для этого укажите значения параметров ‘Dest IP’ (IP-адрес назначения), ‘Netmask’ (Маска сети), ‘Dest Port’ (Порт назначения) и ‘Protocol’ (Протокол).
При вводе IP-адреса сети и подсети в поля Src IP (Исходный IP-адрес) и Netmask (Сеть) пользователь может включить фильтрацию для всей сети.




Нажмите кнопку [Add] (Добавить) и введите значения, как показано на рисунке, приведенном выше. Нажмите кнопку [OK]. После этого получить доступ к портам 80 (HTTP) и 22 (FTP), IP-адрес назначения которых - ‘211.17.127.70’, будет невозможно с любого терминала.

# LAN Config (Настройка локальной сети)

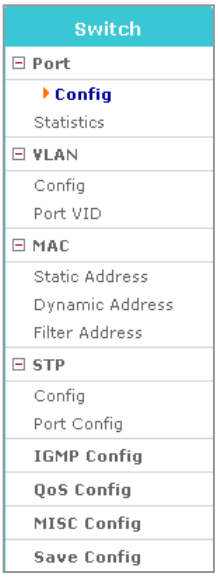
Меню [LAN Config] (Настройка локальной сети) используется для настройки согласования, скорости передачи и системы передачи данных для каждого порта.
Установите флажок для порта, который требуется настроить, и нажмите кнопку [OK].
Для установки для параметров значений по умолчанию нажмите кнопку [Reset] (Сброс).




| Элемент | Описание |
|---|---|
| Negotiation (Согласование) | - auto (авто): управление скоростью с помощью согласования.<br>- force (усилие): управление скоростью с помощью форсирования.<br>Установите для этого элемента значение ‘force’ (Усилие) при установке для параметра Duplex (Дуплекс) значения ‘Full’ (Полный). |
| Speed (Скорость), Мбит/с | Скорость передачи данных через порт |
| Duplex (Дуплекс) | - full (полный): двунаправленный (полнодуплексная система)<br>- half (полудуплекс): однонаправленный (полудуплексная система)<br>Настройка интерфейса WAN2 10 M зависит от настройки его соответствующего<br>модема. |

# Меню Switch (Коммутатор)

Чтобы отобразить подменю [Switch] (Коммутатор) в левой верхней части окна, выберите [Switch] (Коммутатор).




| Меню | Подменю | Описание |
|---|---|---|
| Port (Порт) | Config (Настройка) | Настройка среды порта коммутатора. |
| | Statistics (Статистика) | Отображение состояния соединения, скорости, системы передачи данных и статистики порта коммутатора. |
| VLAN (Виртуальная локальная сеть) | Config (Настройка) | Настройка виртуальной локальной сети (VLAN). |
| | Port VID (Идентификатор VID порта) | Установка метода обработки непомеченных пакетов, если для режима VLAN установлено значение ‘Tag-based VLAN’ (Виртуальная локальная сеть на основе тегов). |
| MAC (MAC-адреса) | Static Address (Статический адрес) | Сохранение MAC-адреса в таблицу статических адресов коммутатора. |
| | Dynamic Address (Динамический адрес) | Извлечение таблицы динамических адресов или удаление MAC-адреса. |

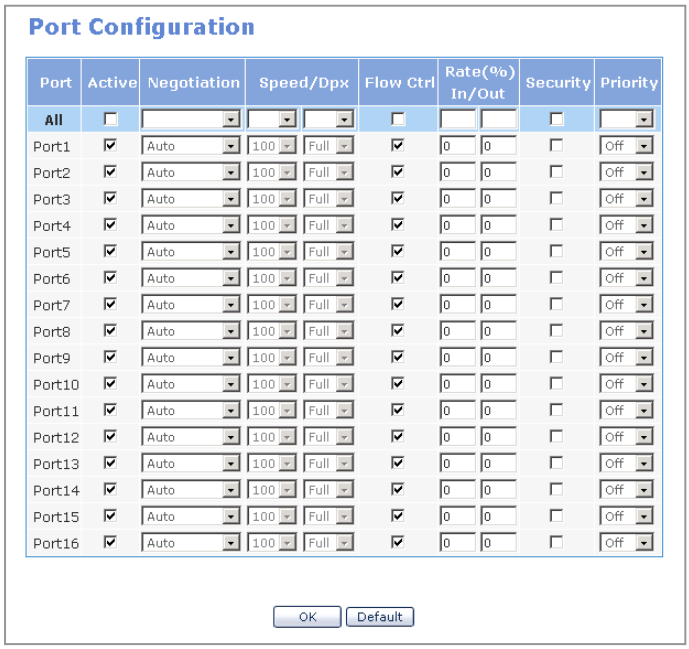
| | | |
|---|---|---|
| | Filter Address (Фильтрация адреса) | Ввод MAC-адреса для блокировки данных фреймов, которые содержат информацию о MAC-адресе, идентичную введенному с коммутатора значению. |
| STP (Протокол STP) | Config (Настройка) | Предотвращение "лавины" широковещательной передачи благодаря обратной связи коммутатора с помощью функции STP. |
| | Port Config (Настройка порта) | Настройка состояния STP. |
| IGMP Config (Настройка IGMP) | - | Эффективная обработка многоадресных пакетов с помощью наблюдения по протоколу IGMP. |
| QoS Config (Настр. QoS) | - | Обработка QoS путем последовательного назначения приоритета пакетам, поступающим на коммутатор, или повышения приоритета определенного порта. |
| MISC Config (Настройка MISC) | - | Настройка зеркалирования и других функций коммутатора. |
| Save Config (Настройка сохранения) | - | Сохранение параметров на флэш-диск или инициализация всех значений параметров. |

# Port (Порт)

Меню [Port] (Порт) используется для настройки и просмотра функций, связанных с портом.

## Config (Настройка)

Выберите [Port] (Порт) → [Config] (Настройка) для настройки среды порта коммутатора.

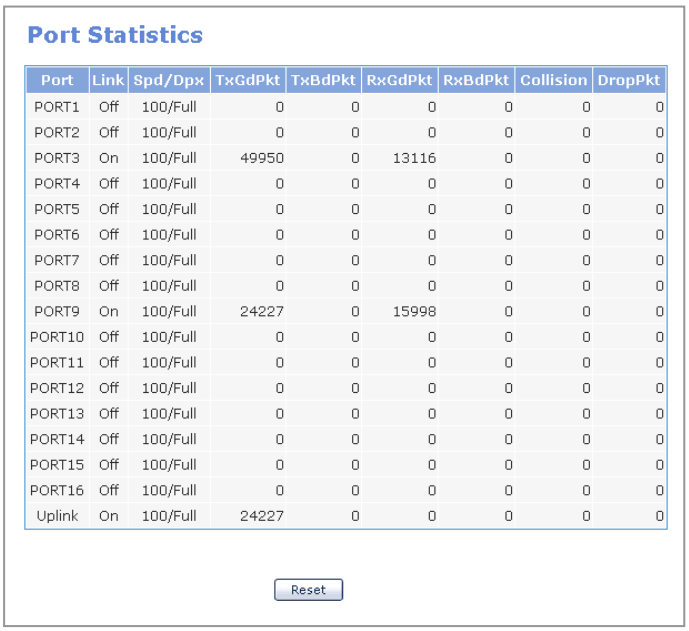



| Элемент | Описание |
|---|---|
| Port (Порт) | Коммутатор оборудован 16 портами.<br>Выберите All (Все) для работы со всеми портами одновременно. |
| Active (Активный) | Настройка использования порта. |
| Negotiation (Согласование) | - Auto (Авто): настройка скорости с помощью автосогласования.<br>- Force (Усилие): настройка скорости принудительно.<br>Установите для значение ‘force’ (принудительго) если параметр Duplex (Дуплекс) имеет значение ‘Full’ (Полный). |

| | |
|---|---|
| Speed/Dpx (Скорость/Дуплекс) | - Speed (Скорость): автоматическая настройка в соответствии со значением, установленным для параметра ‘Path Cost’ (Стоимость пути) в меню [Switch] (Коммутатор) → [STP] → [Port Config] (Настройка порта) (10 Мбит/с, если для параметра ‘Path Cost’ (Стоимость пути) установлено значение ‘100’, и 100 Мбит/с, если ‘19’.)<br>- Dpx (Дуплекс): выберите значение Full (Полный) (двунаправленный) или Half (Полудуплекс) (однонаправленный). |
| Flow Ctl (Управление потоком) | Настройка использования управления потоком. Управление потоком выполняется в соответствии со значением, установленным для параметра Rate(%) In/Out (Скорость получения/отправки данных). |
| Rate(%) In/Out (Скорость получения/отправки данных) | Потоком можно управлять, установив значение параметра Rate(%) In/Out (Скорость получения/отправки данных) для каждого порта. Единица измерения представляет собой коэффициент скорости порта. Установите для этого параметра значение ‘0’, если управление потоком не используется (элемент управления потоком не выбран). |
| Security (Безопасность) | Настройка разрешения обновления таблицы MAC-адресов. Исходный MAC-адрес не обновляется для порта коммутатора, для которого установлен параметр ‘Security’ (Безопасность). Таким образом, подключение другого терминала к данному порту невозможно. Таким образом, терминалу, которому запрещен доступ (с неуказанным статическим MAC-адресом), доступ в сеть будет запрещен. |
| Priority (Приоритет) | Если для этого параметра установлено значение ‘Low’ (Низкий) или ‘High’ (Высокий), приоритету присваивается соответствующее значение независимо от настроек битов QoS, получаемых этим портом пакетов.<br>Этот параметр можно настроить, если в качестве режима QoS в меню [Switch] (Коммутатор) → [QoS Config] (Настр. QoS) → [QoS Configuration] (Настройка QoS) не установлен параметр FCFS (First Come First Service). |

## Statistics (Статистика)

Меню [Port] (Порт) → [Statistics] (Статистика) используется для просмотра состояния соединения, скорости, системы и статистики передачи данных. Числа представляют собой накопленные значения за период с момента загрузки системы до текущей даты. Окно автоматически обновляется каждые пять секунд. Нажмите кнопку [Reset] (Сброс), чтобы сбросить все значения на ‘0’.



**Port Statistics**

| Port | Link | Spd/Dpx | TxGdPkt | TxBdPkt | RxGdPkt | RxBdPkt | Collision | DropPkt |
|---|---|---|---|---|---|---|---|---|
| PORT1 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT2 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT3 | On | 100/Full | 49950 | 0 | 13116 | 0 | 0 | 0 |
| PORT4 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT5 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT6 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT7 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT8 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT9 | On | 100/Full | 24227 | 0 | 15998 | 0 | 0 | 0 |
| PORT10 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT11 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT12 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT13 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT14 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT15 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| PORT16 | Off | 100/Full | 0 | 0 | 0 | 0 | 0 | 0 |
| Uplink | On | 100/Full | 24227 | 0 | 0 | 0 | 0 | 0 |

Reset

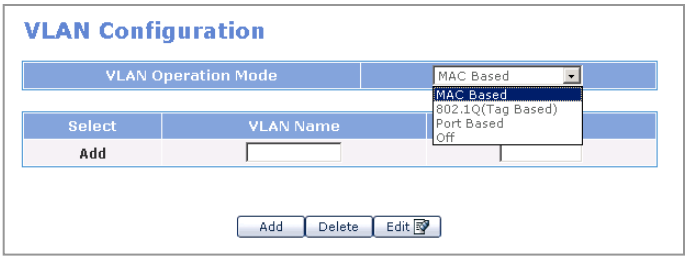
- TxGdPkt: количество пакетов, успешно отправленных на порт.
- TxBdPkt: количество пакетов, для которых выполнена коммутация, но их передача на порт выполнена неуспешно.
- RxGdPkt: количество пакетов, успешно полученных портом.
- RxBdPkt: количество пакетов, успешно полученных портом, для которых не была выполнена коммутация.
- Collision (Конфликт): количество конфликтов, которые произошли между пакетами, полученными от порта, и пакетами, для которых была выполнена коммутация.
- DropPkt: количество пакетов, для которых выполнена коммутация на порт, но которые были сброшены в буфер.

# VLAN (Виртуальная локальная сеть)

Меню [VLAN] (Виртуальная локальная сеть) используется для настройки виртуальной локальной сети (VLAN).

## Config (Настройка)

Выберите [VLAN] (Виртуальная локальная сеть) → [Config] (Настройка), чтобы отобразить окно настройки виртуальной локальной сети.




Выберите режим виртуальной локальной сети в списке ‘VLAN Operation Mode’ (Режим работы виртуальной локальной сети) и нажмите кнопку [OK]. Затем введите имя и идентификатор виртуальной локальной сети и нажмите кнопку [Add] (Добавить), чтобы добавить виртуальную сеть. Чтобы удалить виртуальную локальную сеть, выберите ее и нажмите кнопку [Delete] (Удалить).

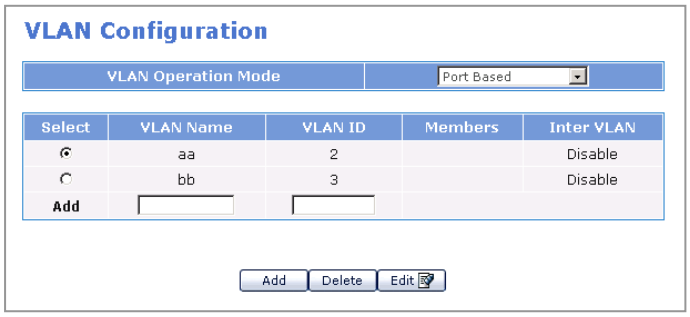
Настройка виртуальной локальной сети определяется по трем указанным ниже режимам работы.

- Виртуальная локальная сеть на основе портов
- Виртуальная локальная сеть на основе тегов (802.1 Q)
- Виртуальная локальная сеть на основе MAC-адресов

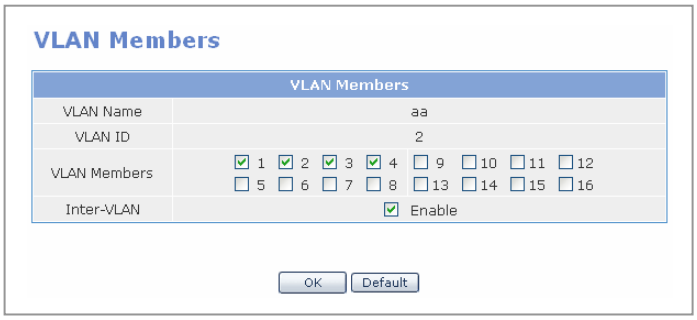
### Виртуальная локальная сеть на основе портов

Этот параметр используется для настройки виртуальной локальной сети на основе портов. Один порт можно назначить нескольким виртуальным локальным сетям. В этих случаях, широковещательные пакеты, переданные портом, передаются во все виртуальные локальные сети, содержащие этот порт. Порты, не назначенные ни одной виртуальной локальной сети, используются как отдельная виртуальная сеть.

В качестве режима работы виртуальной локальной сети выберите ‘Port Based’ (На основе порта) в окне <VLAN Configuration> (Настройка виртуальной локальной сети).




Выберите виртуальную локальную сеть и нажмите кнопку [Edit] (Редактировать), после чего отобразится окно, изображенное ниже. Выберите целевой порт для параметра VLAN Members (Члены виртуальной локальной сети) и нажмите кнопку [Save] (Сохранить).

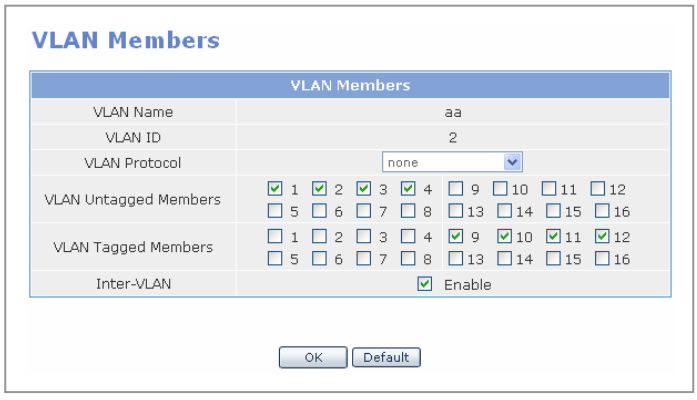



Для установки соединения между виртуальными локальными сетями используйте службу Inter-VLAN (Соединение между виртуальными сетями).
Элемент ‘Inter-VLAN’ (Соединение между виртуальными сетями), упомянутый выше, используется для подключения физического порта через магистраль между WIM и LIM.
Для настройки соединения между виртуальными локальными сетями необходим общий порт групп VLAN. При установке флажка ‘Enable’ (Включено) для параметра ‘Inter-VLAN’ (Соединение между виртуальными сетями) модуль WIM и LIM будет использовать физический порт, подключенный через магистраль, в качестве общего порта. В этом случае установите перемычку на плате WIM ближе к магистрали.
При установке перемычки на плате WIM ближе к ее передней части выберите один из портов (1 - 16) платы LIM, чтобы установить

соединение с портом LAN платы WIM. Для использования службы соединения между виртуальными локальными сетями настройте порт как член VLAN. Службу Inter-VLAN (Соединение между виртуальными сетями) можно использовать, предоставив общий доступ к порту для всех виртуальных локальных сетей.

## Виртуальная локальная сеть на основе тегов (802.1 Q)

Если в виртуальной локальной сети необходимо принять решение относительно пакета, поступающего на определенный порт (если порт назначен нескольким виртуальным сетям), его можно принять, исходя из информации о теге, которая содержится в пакете.
Пакеты, которые не содержат теги, доставляются только в одну виртуальную локальную сеть в соответствии со значением параметра PVID [Port VID(VLAN ID)] (Идентификатор VID порта (Идентификатор виртуальной локальной сети)).
Определите виртуальную локальную сеть с помощью информации об управлении тегами (TCI) в протоколе уровня 2.
Виртуальная локальная сеть на основе тегов состоит из членов с тегами или без тегов и обрабатывается соответствующим образом. Поскольку сетевое оборудование, поддерживающее стандарт 802.1 Q, в большинстве случаев не используется для обработки пакетов с тегами, поступающих на порт коммутатора, то перед передачей полученных пакетов с тегами их рекомендуется преобразовывать.
В окне <VLAN Configuration> (Настройка виртуальной локальной сети) в качестве рабочего режима виртуальной сети укажите ‘Tag Based’ (На основе тегов) и нажмите кнопку [Edit] (Редактировать), после чего отобразится окно, изображенное ниже. Выберите порты для параметра VLAN Untagged Members (Члены виртуальной локальной сети без тегов) и VLAN Tagged Members (Члены виртуальной локальной сети с тегами) и нажмите кнопку [Save] (Сохранить).

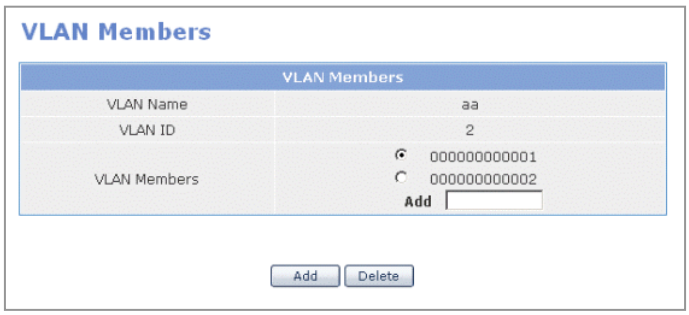


- VLAN Untagged Members (Члены виртуальной локальной сети без тегов): если один из портов (1 - 16) установлен для коммутации и передачи, выберите порт для доставки фреймов Ethernet, из которых будет удалена информация TCI. Подключите терминал (без поддержки IEEE 802.1Q) к выбранному порту и настройте виртуальную локальную сеть с тегами.
- VLAN Tagged Members (Члены виртуальной локальной сети с тегами): если один из портов (1 - 16) установлен для коммутации и передачи, выберите порт для хранения и отправки информации TCI. Подключите терминал, поддерживающий IEEE 802.1Q, к выбранному порту.

## Виртуальная локальная сеть на основе MAC-адресов

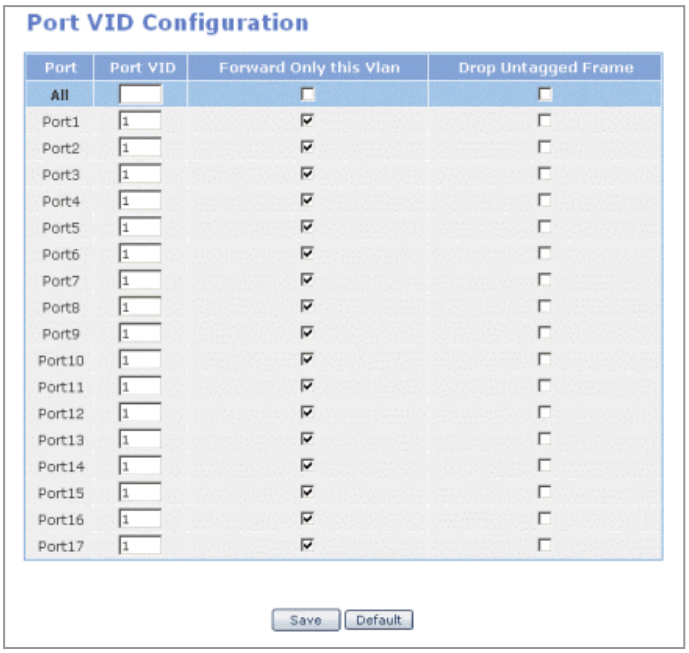
Виртуальная локальная сеть настраивается для каждого MAC-адреса. Если виртуальная локальная сеть настраивается без информации о порте, номер члена виртуальной сети может измениться. В одной или нескольких виртуальных локальных сетях можно сохранить до 1024 MAC-адресов.
Поскольку виртуальная локальная сеть на основе MAC-адресов в основном не содержит информацию о порте, порт используется как член виртуальной сети, получая данные по протоколу ARP (Address Resolution Protocol). Таким образом, пакет ARP необходимо передать на коммутатор, чтобы члены виртуальной локальной сети могли обмениваться пакетами.

В окне <VLAN Configuration> (Настройка виртуальной локальной сети) в качестве рабочего режима виртуальной сети укажите ‘MAC Based VLAN’ (Виртуальная локальная сеть на основе MAC-адресов), выберите целевую виртуальную сеть и нажмите кнопку [Edit] (Редактировать), после чего отобразится окно, изображенное ниже. Введите MAC-адрес члена в поле ‘Add’ (Добавить) и нажмите кнопку [Add] (Добавить), чтобы добавить члена, или [Delete] (Удалить), чтобы удалить его.



# Port VID (Идентификатор VID порта)

Если в качестве режима работы виртуальной локальной сети указан ‘Tag-based VLAN’ (Виртуальная локальная сеть на основе тегов), необходимо установить параметр Port VID (Идентификатор VID порта) в меню [VLAN] (Виртуальная локальная сеть) → [Port VID] (Идентификатор VID порта) для определения системы обработки пакетов без тегов.




| Элемент | Описание |
|---|---|
| Port VID (Идентификатор VID порта) | Идентификатор виртуальной локальной сети для пакетов без тегов.<br>Если порт получает пакет без тега, пакет коммутируется в виртуальную локальную сеть, идентичную идентификатору VID порта. |
| Forward Only this Vlan (Переадресация только этой виртуальной сети) | Если этот флажок установлен, включите функцию отбрасывания пакета, тег полученного пакета с тегом отличается идентификатора VID порта.<br>Если этот флажок не установлен, пакет будет ретранслирован в соответствии с полученной информацией о теге. |

| | |
|---|---|
| Drop Untagged Frame (Отбрасывание фрейма без тега) | Установите флажок для этого параметра, чтобы отбрасывать пакеты без тегов, или снимите флажок, чтобы ретранслировать пакеты без тегов только в виртуальную локальную сеть, соответствующую назначенному идентификатору VID порта. |

NOTE

**Значение параметра Port VID (Идентификатор VID порта)**

Для параметра Port VID (Идентификатор VID порта) введите значение, не превышающее 255.

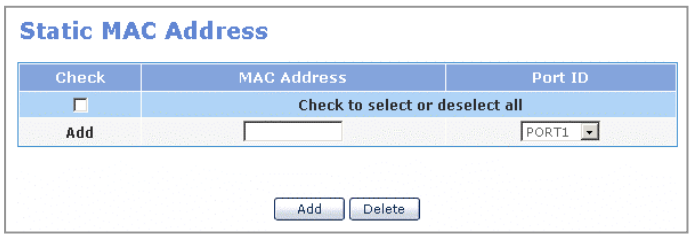
# MAC (MAC-адреса)

Меню [MAC] (MAC-адреса) используется для просмотра таблицы соответствия MAC-адресов и портов коммутатора или для настройки фильтрации MAC-адресов.

## Static Address (Статический адрес)

Выберите [MAC] (MAC-адреса) → [Static Address] (Статический адрес) для сохранения MAC-адреса в таблицу адресов в зависимости от физического соединения номера порта коммутатора между и заносимого компьютера.

То есть MAC-адрес можно хранить в таблице адресов коммутатора без использования обновление таблицы MAC-адресов, в которой он будет храниться даже в том случае, если устройство не подключено к коммутатору, а также по истечении максимального срока хранения (интервал обновления таблицы MAC-адресов).




Введите MAC-адрес и номер порта, а затем нажмите кнопку [Add] (Добавить). Выберите MAC-адрес и нажмите кнопку [Delete] (Удалить), чтобы удалить адрес.

Если в меню [Port] (Порт) → [Config] (Настройка) для порта установлен параметр Security (Безопасность), то поиск исходного MAC-адреса не выполняется. В этом случае со статической MAC адресацией функцию

безопасности базируется на физической привязке MAC-адресов компьютеров и портов коммутатора.

NOTE

**Количество статических MAC-адресов**

Независимо от порта можно ввести до 50 статичных MAC-адресов.

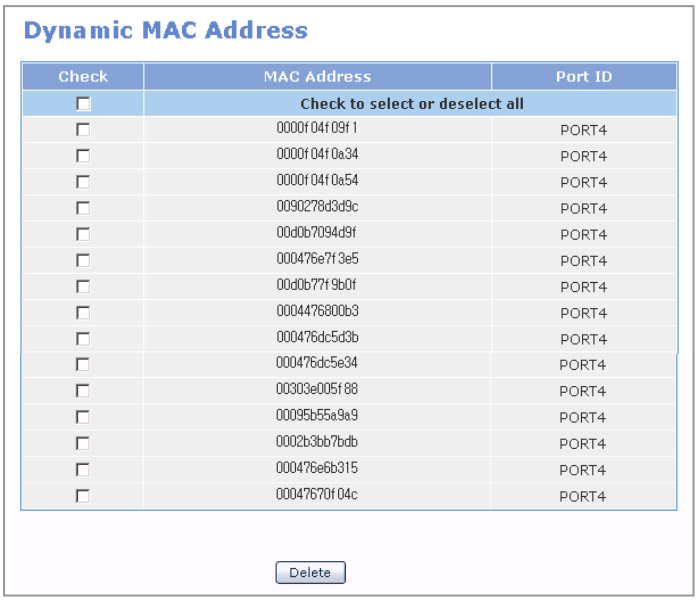
NOTE

**Настройка VID**

В режиме виртуальной локальной сети 802.1Q, при настройке в меню ‘Static Address’ (Статический адрес) и ‘Filter Address’, задайте ‘VLAN ID’ (Идентификатор виртуальной локальной сети). Если значение не введено, будет установлено значение ‘0’..

## Dynamic Address (Динамический адрес)

Выберите [MAC] (MAC-адреса) → [Dynamic Address] (Динамический адрес) для просмотра таблицы динамических адресов.

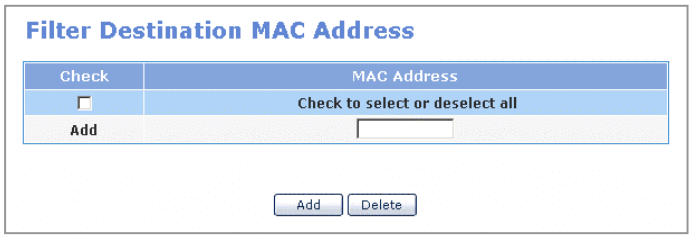



Выберите MAC-адрес и нажмите кнопку [Delete] (Удалить), чтобы удалить адрес.

## Filter Address (Фильтрация адреса)

Фильтрация MAC-адресов используется для блокировки нежелательного трафика. Выберите меню [Filter Address] (Фильтрация адреса) и введите

MAC-адрес для блокировки пакетов, поступающих от коммутатора. MAC-адрес - это адрес места назначения пакетов, поступающих на порт коммутатора.



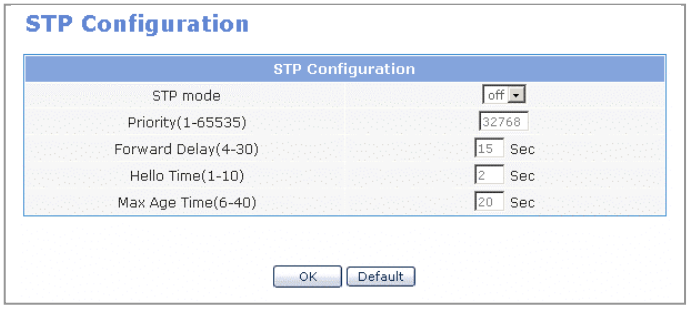

Введите MAC-адрес и номер порта, а затем нажмите кнопку [Add] (Добавить).
Выберите MAC-адрес и нажмите кнопку [Delete] (Удалить), чтобы удалить адрес.

# STP (Протокол STP)

Меню [STP] (Протокол STP) используется для настройки функции протокола STP (Spanning Tree Protocol) предотвращения зацикливания пакетов или для получения информации о состоянии STP.

## Config (Настройка)

Выберите [STP] (Протокол STP) → [Config] (Настройка) для включения протокола STP и предотвращения обратной связи коммутатора.

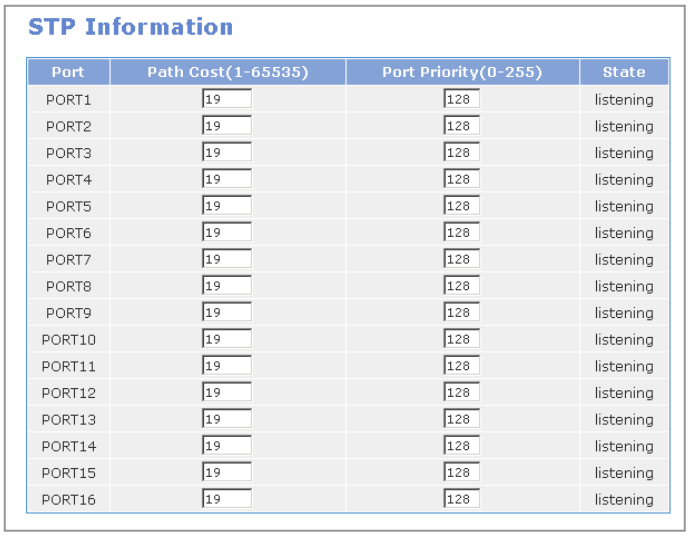



| Элемент | Описание |
|---|---|
| STP Mode (Режим STP) | Настройка использования протокола STP. |
| Priority (Приоритет) | Установка приоритета для отключения портов в случае возникновения обратной связи коммутатора. |

| | |
|---|---|
| Forward Delay (Задержка переадресации) | Если протокол STP находится в состоянии обучения или запоминания, по истечении времени ожидания, заданного для этого параметра, состояние изменяется на переадресацию. (Подробные сведения см. в меню [STP] (Протокол STP) → [Port Config] (Настройка порта)) |
| Hello Time (Время приветствия) | Установка интервала передачи сообщений об установке соединения STP. |
| Max Age Time (Максимальный срок хранения) | Задание времени ожидания для попытки установки нового соединения, если сообщение об установке соединения STP не получено. |

## Port Config (Настройка порта)

Выберите [STP] (Протокол STP) → [Port Config] (Настройка порта) для настройки или просмотра информации о состоянии STP.

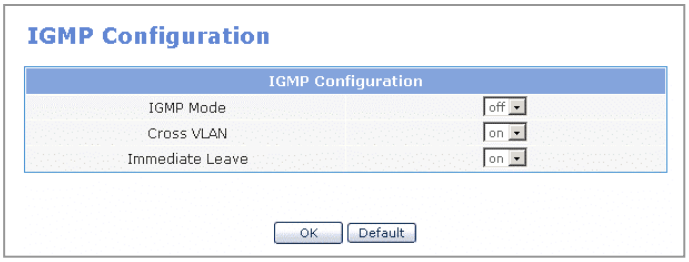



| Элемент | Описание |
|---|---|
| Port (Порт) | Коммутатор оборудован 16 портами.<br>Выберите All (Все) для работы со всеми портами одновременно. |
| Path Cost (Стоимость пути) | Установка скорости в соответствии со скоростью каждого порта коммутатора. Установите значение ‘100’ для скорости 10 Мбит/с и ‘19’ - для 100 Мбит/с. Значение ‘Speed’ (Скорость) параметра ‘Speed/Dpx’ (Скорость/Дуплекс) в меню [Switch] (Коммутатор) → [Port] (Порт) → [Config] (Настройка) устанавливается автоматически в соответствии с настройкой этого параметра. |

| | |
|---|---|
| Port Priority (Приоритет порта) | Установка приоритета для отключения портов в случае возникновения обратной связи коммутатора. |
| State (Состояние) | Состояние каждого порта.<br>- blocking (блокировка): если на коммутаторе возникает обратная связь, блокируется соответствующий порт и данные на него не отправляются.<br>- listening (прослушивание): порт запоминает путь к корневому мосту и может передавать/получать BPDU (данные фреймов для обмена данными между коммутаторами). Тем не менее, порт не может обновлять данные и обновлять таблицу MAC-адресов. Это состояние сохраняется в течение времени, заданного для параметра ‘Forward Delay’ (Задержка переадресации) в окне <STP Configuration> (Настройка STP).<br>- learning (запоминание): похоже на состояние ‘listening’ (прослушивание), но при этом может осуществляться обмен BPDU и обновление таблицы MAC-адресов. Тем не менее, данные отправить невозможно. Это состояние сохраняется в течение времени, заданного для параметра ‘Forward Delay’ (Задержка переадресации) в окне <STP Configuration> (Настройка STP).<br>- forwarding (переадресация): включение нормального соединения. |

# IGMP Config (Настройка IGMP)

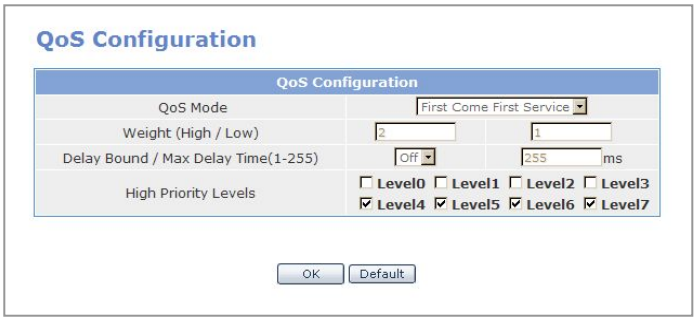
Меню [IGMP Config] (Настройка IGMP) используется для эффективной обработки многоадресных пакетов с помощью наблюдения по протоколу IGMP (Internet Group Management Protocol).




| Элемент | Описание |
|---|---|
| IGMP Mode (Режим IGMP) | Настройка выполнения многоадресной передачи данных с помощью наблюдения по протоколу IGMP. Если наблюдение по протоколу IGMP не используется, выполняется вещание полученного многоадресного пакета. |
| Cross VLAN (Передача данных между виртуальными локальными сетями) | Если этот параметр установлен, пакет можно передавать между разными виртуальными локальными сетями при получении многоадресного пакета коммутатором. |
| Immediate Leave (Немедленное удаление) | Установите этот параметр для удаления члена таблицы многоадресных сообщений при получении сообщения IGMPv2. Этот параметр также позволяет быстро вносить информацию в таблицу многоадресных сообщений, если хосты подключены непосредственно к портам коммутатора. |

# QoS Config (Настр. QoS)

Меню [QoS Config] (Настр. QoS) используется для обработки QoS путем назначения приоритета пакетам, последовательно поступающих на коммутатор, или повышения приоритета определенного порта.

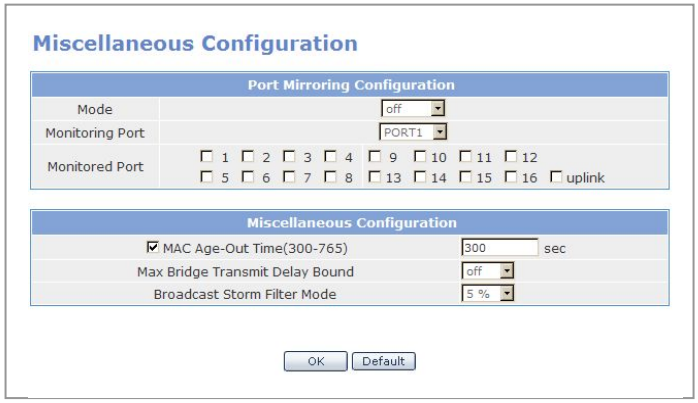



| Элемент | Описание |
|---|---|
| QoS Mode (Режим QoS) | Выбор режима QoS.<br>- First Come First Service (Обслуживание в порядке поступления): Отправка пакетов осуществляется в порядке их поступления (QoS не используется).<br>- All High before Low (Все пакеты с высоким приоритетом перед пакетами с низким): сначала выполняется отправка пакетов с высоким приоритетом, а затем с низким. Передача пакетов с низким приоритетом не выполняется до тех пор, пока не будут переданы пакеты с высоким приоритетом.<br>- Weighted Round Robin (Взвешенное циклическое обслуживание): пакеты с высоким и низким приоритетами передаются в соответствии с фиксированным весом. Например, при установке для параметра High weight (Высокий вес) значения ‘5’, а для параметра Low weight (Низкий вес) - ‘2’ перед отправкой 2 пакетов с низким приоритетом будет отправлено 5 пакетов с высоким приоритетом. |
| Weight (Вес) | Если необходимо использовать метод ‘Weighted Round Robin’ (Взвешенное циклическое обслуживание), установите соотношение высокого и низкого весов. |

| | |
|---|---|
| Delay Bound/ Max Delay Time (Предельное значение задержки/ максимальное время задержки) | Ограничение времени выполняется для предотвращения чрезмерной задержки пакетов с низким приоритетом, если в качестве режима QoS установлен ‘All High before Low’ (Все пакеты с высоким приоритетом перед пакетами с низким) или ‘Weighted Round Robin’ (Взвешенное циклическое обслуживание). Значение параметра ‘Max Delay Time’ (Максимальное время задержки) указывается в миллисекундах (1/1000 сек). Исходное значение - 255 мс. Этот параметр обрабатывается, если пакеты с низким приоритетом не коммутируются, что приводит к превышению значения времени, заданного для этого параметра. |
| High Priority Levels (Уровни высокого приоритета) | Существует 8 тегов для обозначения приоритета. Другими словами, параметры Level 0 (Уровень 0) - Level 7 (Уровень 7) не обозначают приоритет. Приоритет устанавливается по порядку уровня с высоким приоритетом.<br>Поскольку LIM обрабатывает приоритет с двумя очередями (High (Высокий) и Low (Низкий)), выбранный уровень является уровнем с высоким приоритетом. |

# MISC Config (Настройка MISC)

Меню [MISC Config] (Настройка MISC) используется для настройки функции зеркальности и других функций коммутатора.

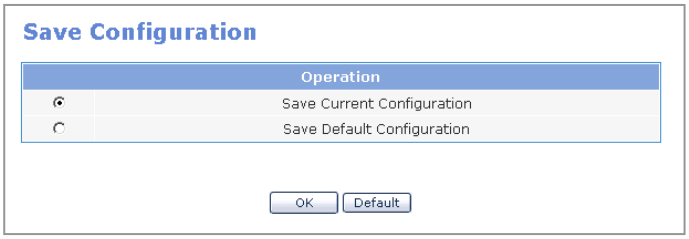



| Элемент | Описание |
|---|---|
| Mode (Режим) | Настройка использования зеркальности.<br>- Не горит: зеркальность не используется.<br>- Tx: зеркальность используется для пакетов Tx.<br>- Rx: зеркальность используется для пакетов Rx.<br>- Both (Оба): зеркальность используется для пакетов Tx и Rx. |

| | |
|---|---|
| Monitoring Port (Контролирующий порт) | Установка порта, выполняющего контроль. Как правило, это означает порт подключения компьютера для контроля. |
| Monitored Port (Контролируемый порт) | Установка целевого порта контроля. Другими словами, установка порта, к которому подключен контролируемый терминал. Контролируемый порт может быть не указан. |
| MAC Age-Out Delay Bound (Предельное значение задержки хранения MAC-адресов) | Установка времени, в течение которого обновленный MAC-адрес (запоминание) может храниться в таблице адресов. Значение по умолчанию 300 сек.<br>Если LIM не управляется с помощью WIM и порт LAN отключен, обновленный MAC-адрес будет автоматически удален через 300 секунд. Поэтому новый MAC-адрес не обновляется мгновенно при повторном подключении порта LAN.<br>Если контроль управляемым модулем LIM (установлен в слот 2) осуществляется с помощью WIM, а порт LAN отключен, обновленный MAC-адрес будет немедленно удален автоматически. При повторном подключении порта LAN новый MAC-адрес и таблица MAC-адресов обновляются мгновенно. |
| Max Bridge Transmit Delay Bound (Максимальное предельное значение задержки передачи данных по мосту) | Установка для параметра максимального времени ожидания пакета Off (Выкл.), 1 sec (1 сек), 2 sec (2 сек) или 4 sec (4 сек). |
| Broadcast Storm Filter Mode (Режим фильтра "лавины" широковещательной передачи) | Выберите значение 5, 10, 15, 20, 25 % от общего размера буфера. Широковещательные пакеты, превышающие это значение, будут утеряны. |

# Save Config

Меню [Save Config] (Настройка сохранения) используется для сохранения параметров на флэш-память. Поскольку параметры в основном сохраняются в ОЗУ, при выключении системы они будут утеряны. Параметры сохраняются на флэш-память для предотвращения удаления данных при перезагрузке.




| Элемент | Описание |
|---|---|
| Save Current Configuration (Сохранить текущую настройку) | Сохранение текущих параметров на флэш-память. При выполнении перезагрузки системы без сохранения параметров они будут утеряны и не будут применены к системе. |
| Save Default Configuration (Сохранить настройку по умолчанию) | Изменение параметров на флэш-памяти на значения по умолчанию. Значения по умолчанию используются после перезагрузки системы. |

NOTE

**Сохранение или импорт базы данных коммутатора**

Выберите [System] (Система) → [DB Config] (Настройка базы данных) → [Save/Delete] (Сохранить/Удалить) для сохранения базы данных коммутатора.
Выберите [System] (Система) → [DB Config] (Настройка базы данных) → [Import/Export] (Импорт/Экспорт) для импорта сохраненной базы данных. Постле импорта базы данных выполните перезагрузку WIM.

# Меню Router (Маршрутизатор)

Чтобы отобразить подменю Router (Маршрутизатор) в левой верхней части окна, выберите [Router] (Маршрутизатор).

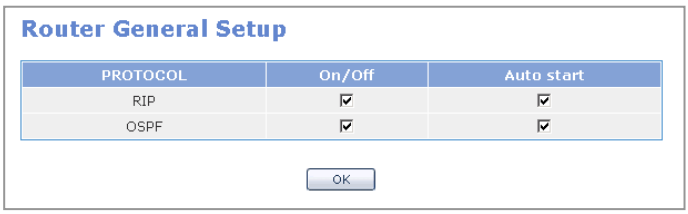

| Меню | Подменю | Описание |
|---|---|---|
| General (Общие) | Show Route (Показать маршрут) | Отображение таблицы маршрутизации сервера Data Server. |
| | Management (Управление) | Запуск и остановка служб RIP и OSPF и настройка выполнения служб при перезагрузке системы. |
| Config (Настройка) | Static Route (Статический маршрут) | Настройка статического маршрута. |
| | RIP config (Настройка RIP) | Настройка RIP. |
| | OSPF config (Настройка OSPF) | Настройка OSPF. |

# General (Общие)

Меню [General] (Общие) используется для запуска и остановки служб RIP и OSPF, а также для просмотра таблицы маршрутизации сервера Data Server.

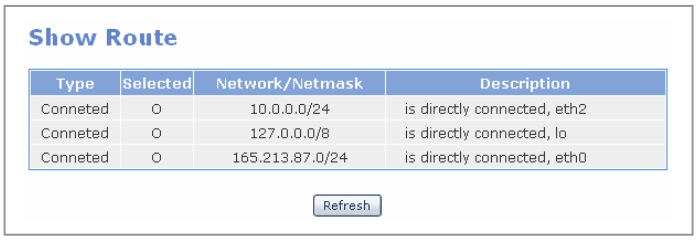
## Management (Управление)

Выберите [General] (Общие) → [Management] (Управление) для запуска или остановки служб RIP и OSPF. Установите флажок ‘Auto Start’ (Автостарт) для автоматического запуска службы после перезагрузки системы.




## Show Route (Показать маршрут)

Выберите [General] (Общие) → [Show Route] (Показать маршрут) для извлечения таблицы маршрутизации сервера Data Server.




| Элемент | Описание |
|---|---|
| Type (Тип) | - Connected (Подключено): сеть подключена непосредственно к сетевому интерфейсу сервера Data Server.<br>- RIP: данные о маршруте, полученные от других маршрутизаторов по протоколу RIP.<br>- OSPF: данные о маршруте, полученные от других маршрутизаторов с помощью OSPF. |
| Selected (Выбрано) | Обозначение активности маршрутизации. |
| Network/Netmask (Сеть/Маска сети) | Информация о сети в маршруте. |
| Description (Описание) | Описание маршрута. |

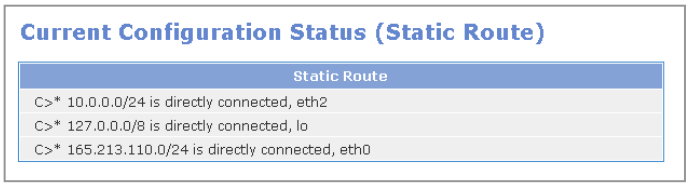
# Config (Настройка)

Меню [Config] (Настройка) используется для настройки статического маршрута, RIP и OSPF.

## Static Route (Статический маршрут)

Выберите [Config] (Настройка) → [Static Route] (Статический маршрут) для настройки статического маршрута. Настройте следующие параметры и нажмите кнопку [Save] (Сохранить).

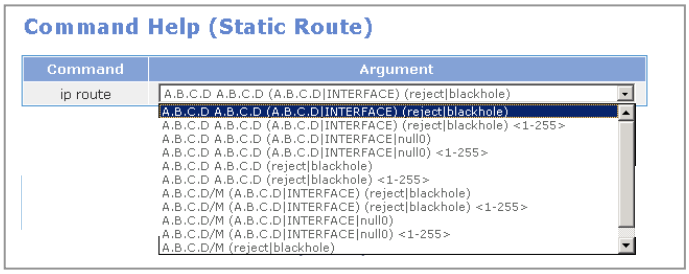
- Current Configuration Status (Текущее состояние настройки)




В этом окне отображается таблица маршрутизации сервера Data Server, которая совпадает с таблицей, отображающейся в окне меню [Router] (Маршрутизатор) ( [General] (Общие) ( [Show Route] (Показать маршрут). Тем не менее, в указанном выше окне отображаются следующие типы маршрутов.

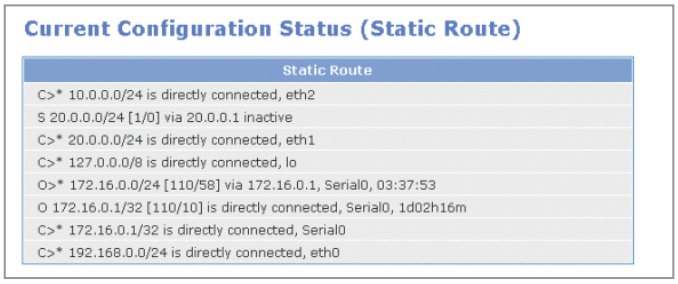
| Элемент | Описание |
|---|---|
| C>* | Сетевой маршрут подключен непосредственно к сетевому интерфейсу сервера Data Server. |
| O | Данные о маршруте, полученные от других маршрутизаторов с помощью OSPF. |
| R | Данные о маршруте, полученные от других маршрутизаторов по протоколу RIP. |
| S | Статический маршрут, установленный администратором. |

- Input Configuration Command (Ввод команды настройки)
  Выберите аргумент, соответствующий команде ‘ip route’.
  При выборе параметра ‘Argument’ (Аргумент) будут отображены все аргументы, соответствующие команде. Выберите аргумент из списка.




- Input Configuration Command (Ввод команды настройки)
  Выберите команду, как показано выше, или введите команду настройки статического маршрута, как показано ниже.


Результат выполнения команды применяется в окне <Current Configuration Status> (Текущее состояние настройки) меню [Router] (Маршрутизатор) ( [Config] (Настройка) ( [RIP Config] (Настройка RIP). Например, результат ввода команды статического маршрута, приведенной выше, отображается в окне <Current Configuration Status> (Текущее состояние настройки), изображенном ниже.




NOTE

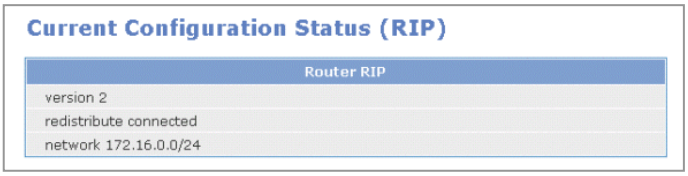
**Удаление статического маршрута**

Чтобы удалить заданную информацию о статическом маршруте, перед маршрутом IP-адреса укажите ‘no’. Другими словами, при вводе команды ‘no ip route 20.0.0.0/24 20.0.0.1’ заданная информация о статическом маршруте будет удалена.

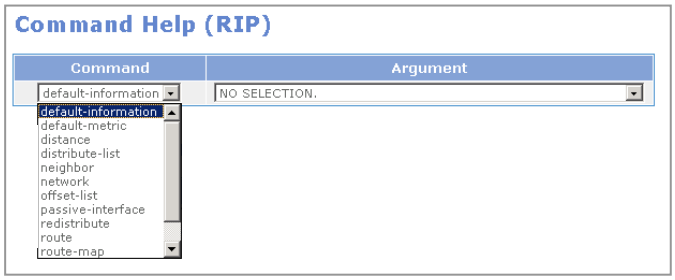
## RIP Config (Настройка RIP)

Выберите [Config] (Настройка) → [RIP Config] (Настройка RIP) для настройки протокола RIP. Настройте следующие параметры и нажмите кнопку [Save] (Сохранить).

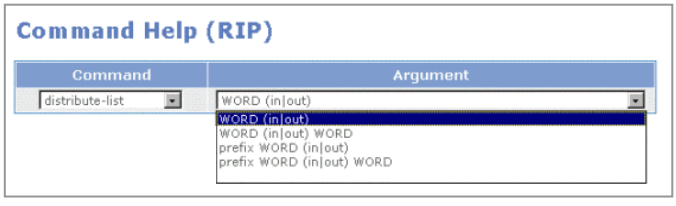
- Current Configuration Status (Текущее состояние настройки)
  Этот элемент отображает текущее состояние протокола RIP. Состояние обновляется при выполнении команды RIP, введенной в окно <Input Configuration Command> (Ввод команды настройки) меню [Router] (Маршрутизатор) → [Config] (Настройка) → [Static Route] (Статический маршрут).



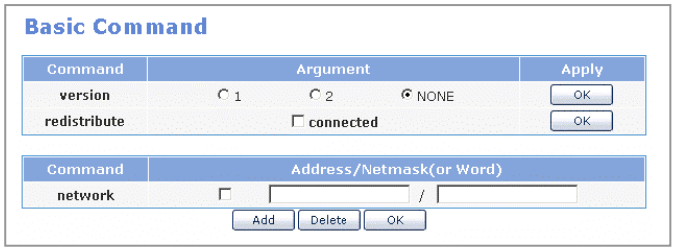

- Command Help (Справка по команде)
  Выберите команду RIP в списке ‘Command’ (Команда) и выберите аргумент для этой команды в списке ‘Argument’ (Аргумент).




Например, команде ‘distribute-list’ соответствуют следующие аргументы.



- Basic Command (Основная команда)
  После ввода параметров нажмите кнопку [OK] для отображения примененного значения в окне <Current Configuration Status> (Текущее состояние настройки).

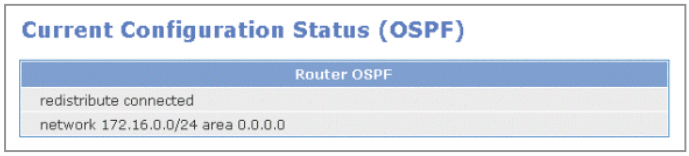



- Input Configuration Command (Ввод команды настройки)
  Выберите команду таком же образом как в окне <Command Help(RIP)> (Справка по команде (RIP)) или напрямую введите команду RIP и нажмите кнопку [OK].

# OSPF Config

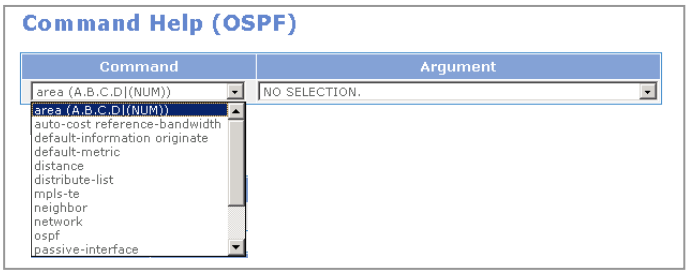
Select [Config] → [OSPF Config] to set OSPF. Set the following items and click the [Save] button.

- Current Configuration Status
  This item displays the current OSPF status. The status is updated when the OSPF command entered into the <Input Configuration Command> window of the [Router] → [Config] → [Static Route] menu is executed.

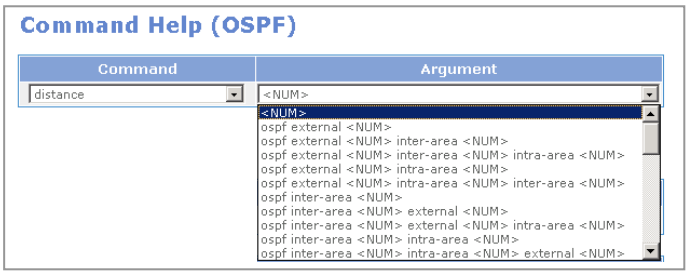



If set as 'area 0.0.0.0' as shown above, the information on the route directly connected to the network interface of the Data Server is delivered through 'network 172.16.0.0'.

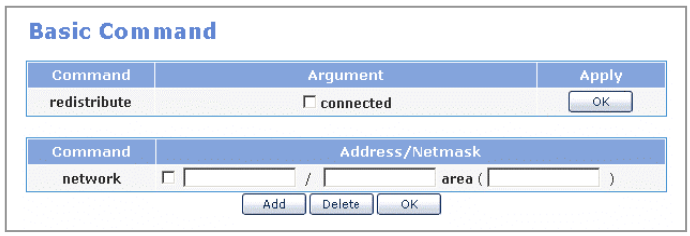
- Command Help (Справка по команде)
  Выберите команду OSPF в списке 'Command' (Команда) и выберите аргумент для этой команды в списке 'Argument' (Аргумент).




Например, команде 'distance' соответствуют следующие аргументы.



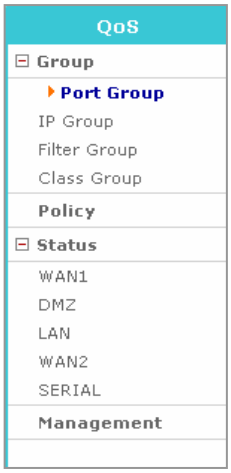
- Basic Command (Основная команда)
  После ввода параметров нажмите кнопку [OK] для отображения примененного значения в окне <Current Configuration Status> (Текущее состояние настройки).




- Input Configuration Command (Ввод команды настройки)
  Выберите команду таком же образом как в окне <Command Help(RIP)> (Справка по команде (RIP)) или напрямую введите команду OSPF и нажмите кнопку [OK].

# Меню QoS

Чтобы отобразить подменю QoS в левой верхней части окна, выберите [QoS].



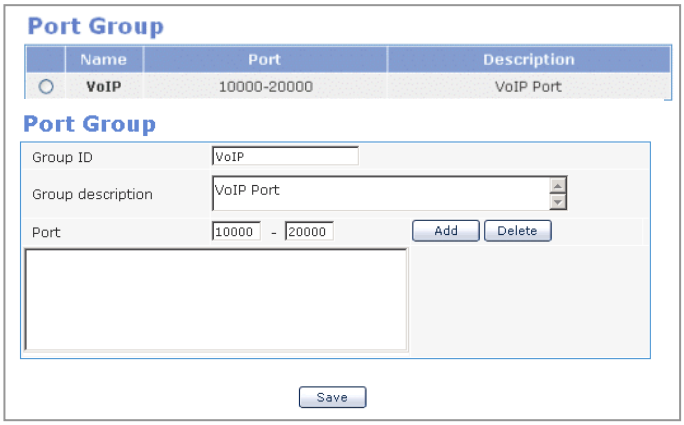

| Меню | Подменю | Описание |
|---|---|---|
| Group (Группа) | Port Group (Группа портов) | Просмотр, настройка, редактирование или удаление группы портов. |
| | IP Group (Группа IP-адресов) | Извлечение, настройка, редактирование или удаление группы IP-адресов. |
| | Filter Group (Группа фильтров) | Просмотр, настройка, редактирование или удаление группы фильтров. |
| | Class Group (Группа классов) | Просмотр, настройка, редактирование или удаление группы классов. |
| Policy (Политика) | - | Настройка класса для порта. |
| Status (Состояние) | - | Отображение класса QoS и фильтрация данных порта в структуре каталога. |
| Management (Управление) | - | Запуск и остановка выполнения QoS и возможность настройки автоматического запуска функции QoS после перезагрузки системы. |

# Group (Группа)

Меню [Group] (Группа) используется для просмотра, настройки, редактирования или удаления групп портов, IP-адресов, фильтров или классов.

## Port Group (Группа портов)

Меню [Port Group] (Группа портов) используется для просмотра, настройки, редактирования или удаления группы портов.

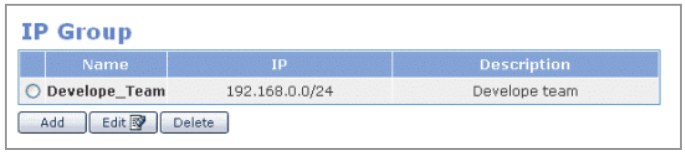



Для отображения окна редактирования группы портов нажмите в приведенном выше окне кнопку [Add] (Добавить). Введите значения для параметров Group ID (Код группы), Group description (Описание группы), укажите номер порта, нажмите кнопку [Add] (Добавить), а затем - кнопку [Save] (Сохранить).

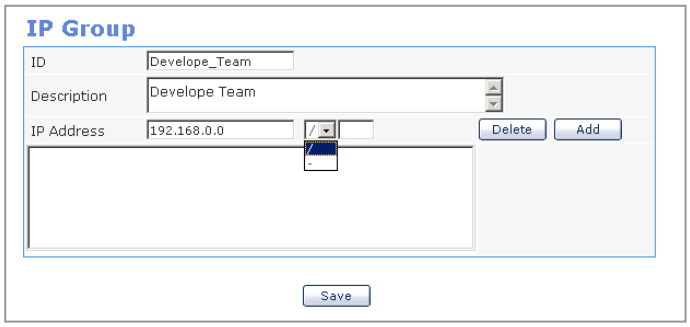
| Элемент | Описание |
|---|---|
| Group ID (Код группы) | Имя группы портов<br>- Имя должно содержать буквы и цифры<br>- Начинаться код группы должен с букв, а не с цифр<br>- Запрещается использовать пробел между символами |
| Group description (Описание группы) | Описание группы портов |
| Port (Порт) | Диапазон портов<br>Для настройки всех портов введите ‘0’. |

# IP Group (Группа IP-адресов)

Меню [IP Group] (Группа IP-адресов) используется для просмотра, настройки, редактирования и удаления группы IP-адресов.



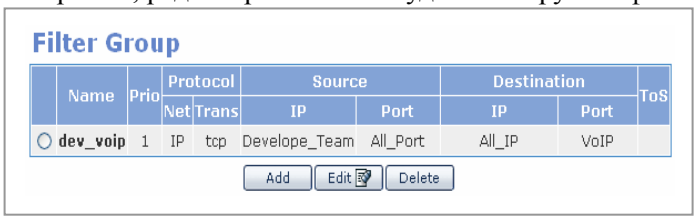

Для отображения окна редактирования группы IP-адресов нажмите в приведенном выше окне кнопку [Add] (Добавить). Введите значения для параметров Group ID (Код группы), Group description (Описание группы), укажите номер порта, нажмите кнопку [Add] (Добавить), а затем - кнопку [Save] (Сохранить).




| Элемент | Описание |
|---|---|
| ID (Код) | Название группы IP-адресов<br>- Имя должно содержать буквы и цифры.<br>- Начинаться код группы должен с букв, а не с цифр.<br>- Запрещается использовать пробел между символами. |
| Group description (Описание группы) | Описание группы IP-адресов |
| IP-адрес | IP address (IP-адрес)<br>/: Используется для указания подсети<br>-: Используется для ввода диапазона IP-адресов<br>Для настройки всех портов введите ‘0.0.0.0/0’. |

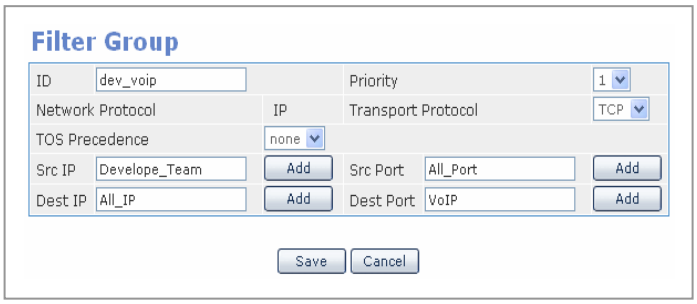
## Filter Group (Группа фильтрации)

Меню [Filter Group] (Группа фильтрации) используется для просмотра, настройки, редактирования или удаления группы фильтрации.




Если в качестве группы фильтрации зарегистрирована группа ‘dev_voip’, как показано на рисунке выше, применяются следующие правила фильтрации: параметры ‘Source’ (Источник) и ‘Destination’ (Назначение) настраиваются в меню [Port Group] (Группа портов) и [IP Group] (Группа IP-адресов). Все пакеты, передающиеся по протоколу TCP с локальными IP-адресами Develop_Team (192.168.0.0/24) и портами подключения VoIP (10000 - 20000), фильтруются с приоритетом ‘1’. Затем фильтр связывается с группой классов, заданной в меню [QoS] → [Group] (Группа) → [Class Group] (Группа классов).

Для отображения окна редактирования группы фильтрации нажмите в приведенном выше окне кнопку [Add] (Добавить). Настройте параметры и нажмите кнопку [Save] (Сохранить). После нажатия кнопки [Add] (Добавить) отображается список групп портов и групп IP-адресов. Выберите IP-адрес и порт из списка.

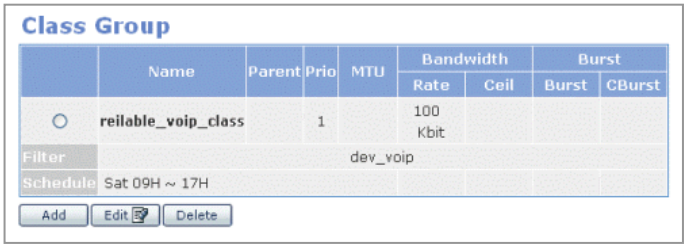



Задание фильтра означает использование правила фильтрации значений в заголовках пакетов. Используются значения, заданные в меню [QoS] → [Group] (Группа) → [Port Group] (Группа портов). Можно также задать фильтрацию для протоколов и полей TOS. Кроме того, для фильтров можно назначать приоритет, используемый для применения правил фильтрации.
Параметры ‘Src IP’ (Исходный IP-адрес), ‘Src Port’ (Исходный порт) и ‘Dest IP’ (IP-адрес назначения), ‘Dest Port’ (Порт назначения) являются

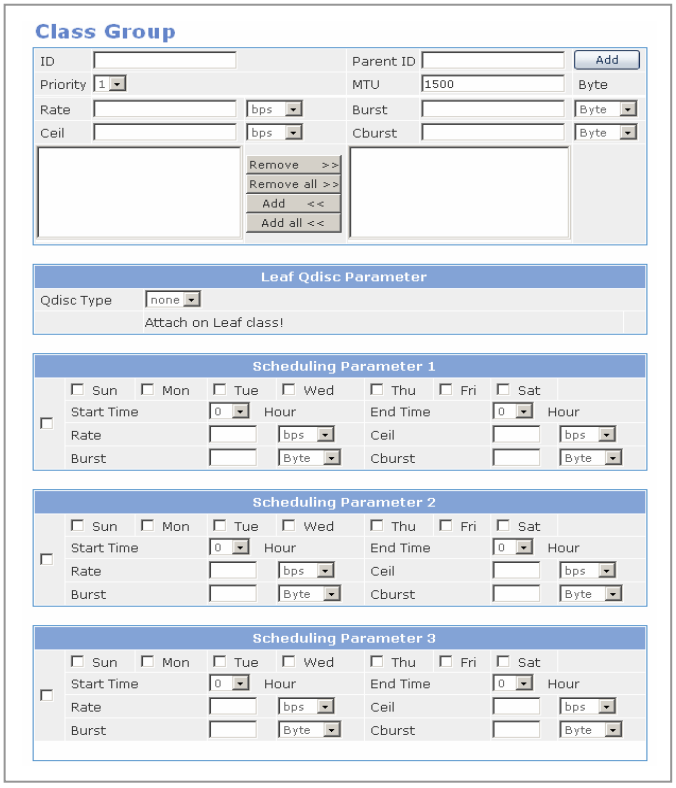
обязательными и требуют ввода соответствующих значений. Если значения для этих параметров не введены, отобразится сообщение об ошибке.

## Class Group (Группа классов)

Меню [Class Group] (Группа классов) используется для просмотра, настройки, редактирования или удаления группы классов. Класс содержит информацию об используемом правиле фильтрации и пропускной способности, которую необходимо назначить для фильтруемого трафика.



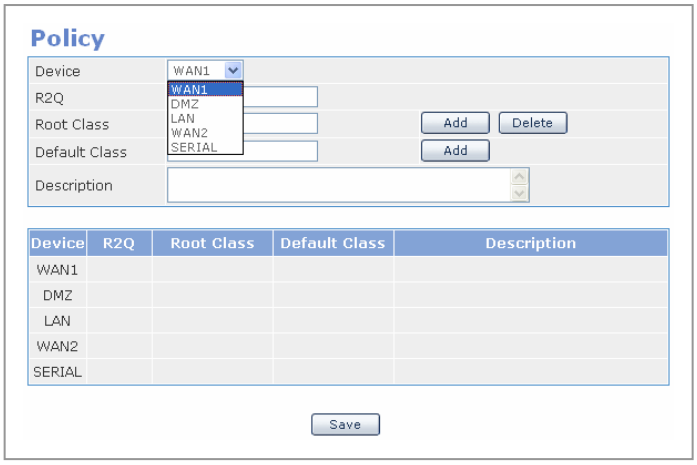

Для отображения окна редактирования группы классов в окне <Class Group> (Группа классов) нажмите кнопку [Add] (Добавить). Настройте параметры и нажмите кнопку [Save] (Сохранить).



| Элемент | Описание |
|---|---|
| Parent ID (Код родительского класса) | QoS обладает иерархической структурой, поэтому классы делятся на корневые (высшего уровня) и ответвления (нижнего уровня) ,а также на родительские и дочерние. Если конечный класс является дочерним классом другого, настройте родительский класс с помощью параметра Parent ID (Код родительского класса). Не вводите значение для параметра Parent ID (Код родительского класса), если конечный класс является корневым (класс высшего уровня, имеющий физическое соединение) или классом по умолчанию (класс, включающий в себя пропускную способность для трафика, не принадлежащего фильтру). |
| Priority (Приоритет) | Если оставшаяся пропускная способность разделена между несколькими классами или все классы стремятся занять избыточную пропускную способность, настройте приоритеты так, чтобы класс с высшим приоритетом занимал полосу пропускания первым. |
| MTU | Параметр MTU (Максимальный блок данных) используется для задания максимального количества пакетов, которые можно передать одновременно. Рекомендуется устанавливать значение, не превышающее максимального размера пакета в сети Ethernet (1504 байт). Если значение для параметра не указано, используется значение по умолчанию ‘1500 Byte’ (1500 байт). |
| Rate (Скорость) | Основное значение пропускной способности, требующейся для настройки класса для назначенной пропускной способности. |
| Ceil (Макс. значение) | Максимальное значение назначенной пропускной способности. |
| Burst (Пакетная запись) | Объем данных, который может быть отправлен классом. |
| Cburst (Одноврем. пакетная запись) | Максимальный объем данных, который может быть передан одновременно. |
| Filter List (Список фильтров) | Задание правил фильтрации для класса. |
| Leaf Qdisc Parameter (Qdisc параметр ответвления) | Задание требуемого значения Qdisc для Qdisc параметра ответвления при настройке класса нижнего уровня. |
| Scheduling Parameter (Параметр расписания) 1/2/3 | Изменение пропускной способности класса в зависимости от дня и часа.<br>Можно задать до трех параметров расписания. |

# Policy (Политика)

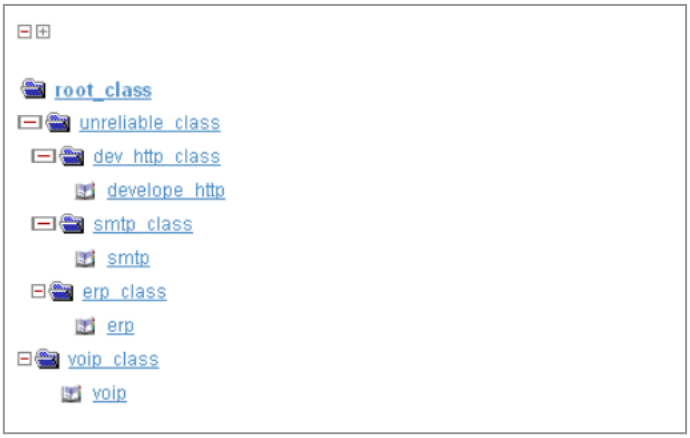
Меню [Policy] (Политика) используется в целях настройки класса для порта. Введите значения для следующих параметров и нажмите кнопку [Save] (Сохранить) для выбора класса порта.




| Элемент | Описание |
|---|---|
| Port (Порт) | Выбор порта (WAN1, DMZ, LAN, WAN2, SERIAL (Последовательный)) |
| R2Q | R2Q используется в качестве переменной для подсчета количества дефицитного циклического обслуживания (DRR).(Bps/r2q) |
| Root Class (Корневой класс) | Класса, подключенный к порту. Нажмите кнопку [Add] (Добавить) и выберите группу классов из списка. |
| Default Class (Класс по умолчанию) | Этот класс определяет пропускную способность для входящего трафика, не применимую для всех правил фильтрации. Нажмите кнопку [Add] (Добавить) и выберите группу классов из списка. |
| Описание | Описание информации по каждому устройству. |

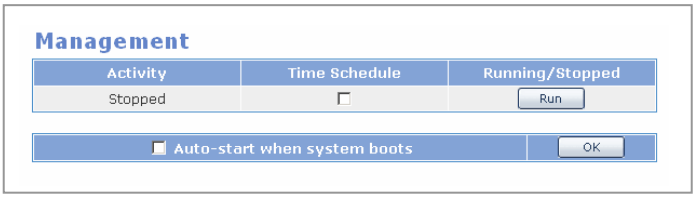
## Status (Состояние)

Меню [Status] (Состояние) используется для отображения класса и фильтров, назначенных для каждого порта в структуре каталога.



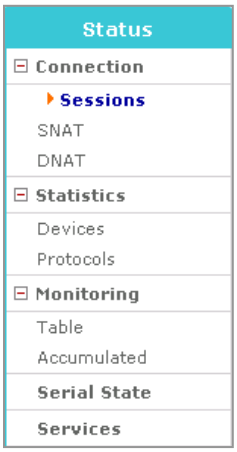

## Management (Управление)

Меню [Management] используется для запуска и остановки службы QoS. Выполнение функции ‘Scheduling Parameter’ (Параметр расписания), заданного в меню [QoS] → [Group] (Группа)→ [Class Group] (Группа классов) также можно запустить или остановить. При выборе параметра автозапуска служба QoS будет автоматически запускаться после перезагрузки системы.



# Status (Состояние)

Чтобы отобразить подменю Status (Состояние) в левой верхней части окна, выберите [Status] (Состояние).



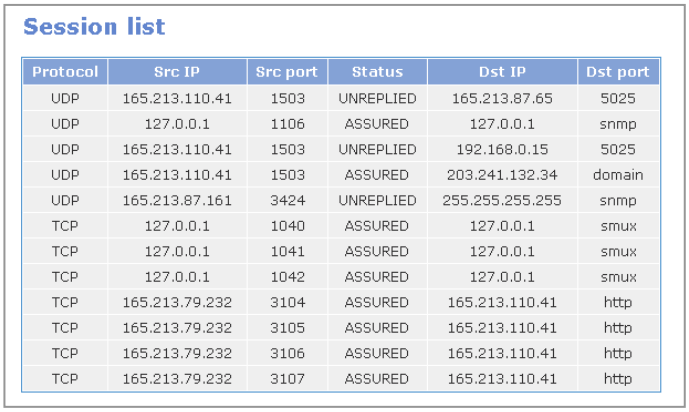

| Меню | Подменю | Описание |
|---|---|---|
| Connection (Соединение) | Sessions (Сеансы) | Отображение IP-адресов и портов, подключенных к серверу Data Server. |
| | SNAT | Отображение состояния соединения SNAT. |
| | DNAT | Отображение состояния соединения DNAT. |
| Statistics (Статистика) | Devices (Устройства) | Отображение сетевой статистики сервером Data Server для каждого устройства, а также для Tx и Rx. |
| | Protocols (Протоколы) | Отображение сетевой статистики сервером Data Server для каждого протокола. |
| Monitoring (Контроль) | Table (Таблица) | Отображение сетевой статистики сервера Data Server в реальном времени в виде таблицы. |
| | Accumulated (Накопленные значения) | Отображение сервером Data Server статистики в виде значений, накопленных в течение года, месяца, недели или часа. |
| Serial State (Состояние последовательного порта) | - | Отображение текущего состояния линии последовательного порта. |
| Services (Службы) | - | Функции сервера Data Server подразделяются на следующие: Security (Безопасность), Router (Маршрутизатор), Management (Управление). Состояния служб отображаются в виде таблицы. |

# Connection (Подключения)

В меню [Connection] (Подключения) отображается состояние соединения сервера Data Server, SNAT и DNAT.

## Sessions (Сеансы)

В меню [Sessions] (Сеансы) отображается информация об IP-адресах и портах, подключенных к серверу Data Server.



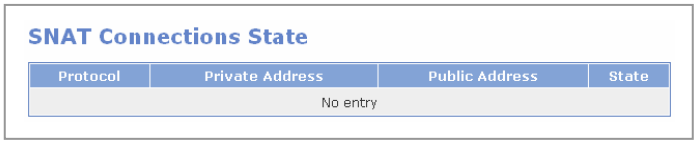
Session list

| Protocol | Src IP | Src port | Status | Dst IP | Dst port |
|---|---|---|---|---|---|
| UDP | 165.213.110.41 | 1503 | UNREPLIED | 165.213.87.65 | 5025 |
| UDP | 127.0.0.1 | 1106 | ASSURED | 127.0.0.1 | snmp |
| UDP | 165.213.110.41 | 1503 | UNREPLIED | 192.168.0.15 | 5025 |
| UDP | 165.213.110.41 | 1503 | ASSURED | 203.241.132.34 | domain |
| UDP | 165.213.87.161 | 3424 | UNREPLIED | 255.255.255.255 | snmp |
| TCP | 127.0.0.1 | 1040 | ASSURED | 127.0.0.1 | smux |
| TCP | 127.0.0.1 | 1041 | ASSURED | 127.0.0.1 | smux |
| TCP | 127.0.0.1 | 1042 | ASSURED | 127.0.0.1 | smux |
| TCP | 165.213.79.232 | 3104 | ASSURED | 165.213.110.41 | http |
| TCP | 165.213.79.232 | 3105 | ASSURED | 165.213.110.41 | http |
| TCP | 165.213.79.232 | 3106 | ASSURED | 165.213.110.41 | http |
| TCP | 165.213.79.232 | 3107 | ASSURED | 165.213.110.41 | http |

| Элемент | Описание |
|---|---|
| Protocol (Протокол) | Тип протокола, используемого для сеанса соединения (UDP, TCP) |
| Src IP (Исходный IP-адрес) | Исходный IP-адрес |
| Src Port (Исходный порт) | Исходный порт |
| Status (Состояние) | - UNREPLIED (Без ответа): На полученных пакетах, требующих ответ, не были найдены ответные пакеты.<br>- ASSURED (Подтвержденные): Получен ответный пакет (‘UNREPLIED’ (Без ответа) изменяется на ‘ASSURED’ (Подтвержденные)) |
| Dst IP (IP-адрес назначения) | IP-адрес назначения |
| Dst Port (Порт назначения) | Порт назначения |

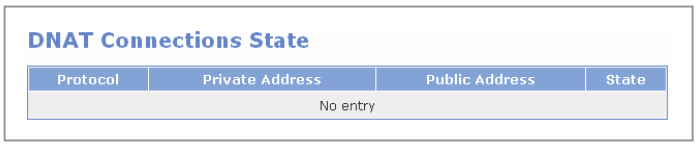
## SNAT

В меню [SNAT] отображается состояние соединения через статический NAT.




## DNAT

В меню [DNAT] отображается состояние соединения через динамический NAT.



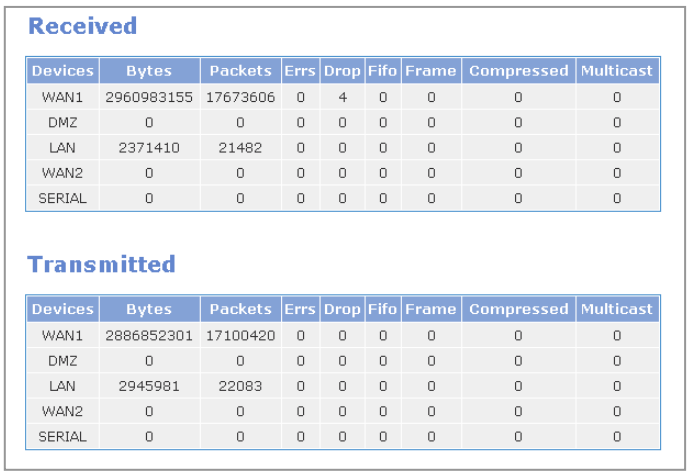

| Элемент | Описание |
|---|---|
| Protocol (Протокол) | Тип протокола (UDP, TCP) |
| Private Address (Личный IP-адрес) | IP-адрес пользователя |
| Public Address (Общий адрес) | IP-адрес подключенного пользователя |
| State (Состояние) | Текущее состояние |

# Statistics (Статистика)

В меню [Statistics] (Статистика) отображается сетевая статистика сервером Data Server для каждого устройства и протокола.

## Devices (Устройства)

Выберите [Statistics] (Статистика)→ [Devices] (Устройства) для отображения сервером Data Server сетевой статистики по полученным и переданным данным для каждого устройства.



**Received**

| Devices | Bytes | Packets | Errs | Drop | Fifo | Frame | Compressed | Multicast |
|---|---|---|---|---|---|---|---|---|
| WAN1 | 2960983155 | 17673606 | 0 | 4 | 0 | 0 | 0 | 0 |
| DMZ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAN | 2371410 | 21482 | 0 | 0 | 0 | 0 | 0 | 0 |
| WAN2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| SERIAL | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

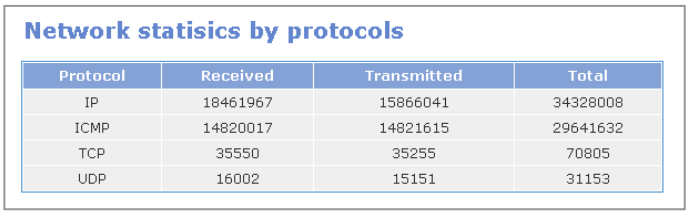
**Transmitted**

| Devices | Bytes | Packets | Errs | Drop | Fifo | Frame | Compressed | Multicast |
|---|---|---|---|---|---|---|---|---|
| WAN1 | 2886852301 | 17100420 | 0 | 0 | 0 | 0 | 0 | 0 |
| DMZ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAN | 2945981 | 22083 | 0 | 0 | 0 | 0 | 0 | 0 |
| WAN2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| SERIAL | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Элемент | Описание |
|---|---|
| Devices (Устройства) | Тип порта |
| Bytes (Байты) | Общее количество принятых и переданных байт |
| Packets (Пакеты) | Общее количество принятых и переданных пакетов |
| Errs (Ошибки) | Количество пакетов с ошибками |
| Drop (Отбрасывание) | Количество отброшенных пакетов |
| Fifo | Очередь FIFO переполнена (переполнение FIFO) |
| Frame (Фрейм) | Неверный тип заголовка Ethernet (Ошибка выравнивания фреймов) |
| Compressed (Сжатые) | Количество сжатых пакетов |
| Multicast (Многоадресные) | Количество многоадресных пакетов |

### Protocols (Протоколы)

Выберите [Statistics] (Статистика) → [Protocols] (Протоколы) для отображения сервером Data Server сетевой статистики для каждого протокола (единица измерения: байт)



**Network statisics by protocols**

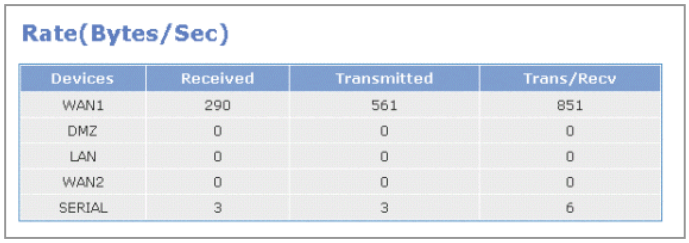
| Protocol | Received | Transmitted | Total |
|---|---|---|---|
| IP | 18461967 | 15866041 | 34328008 |
| ICMP | 14820017 | 14821615 | 29641632 |
| TCP | 35550 | 35255 | 70805 |
| UDP | 16002 | 15151 | 31153 |

## Monitoring (Контроль)

Меню [Monitoring] (Контроль) используется для отображения сетевой статистики сервера Data Server в виде значений, накопленных за определенный промежуток времени.

### Table (Таблица)

Выберите [Monitoring] (Контроль) → [Table] (Таблица) для отображения сервером Data Server статистики в реальном времени. Данные обновляются каждые 5 секунд.

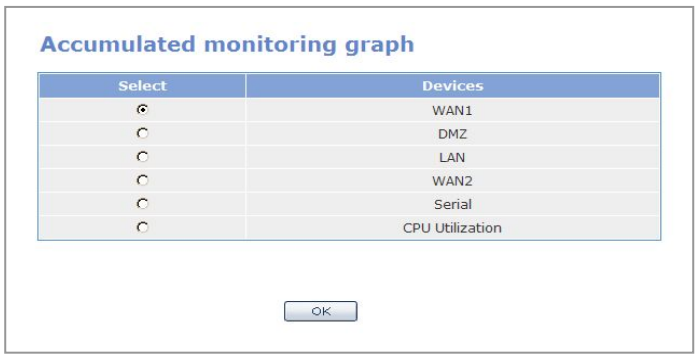


**Rate(Bytes/Sec)**

| Devices | Received | Transmitted | Trans/Recv |
|---|---|---|---|
| WAN1 | 290 | 561 | 851 |
| DMZ | 0 | 0 | 0 |
| LAN | 0 | 0 | 0 |
| WAN2 | 0 | 0 | 0 |
| SERIAL | 3 | 3 | 6 |

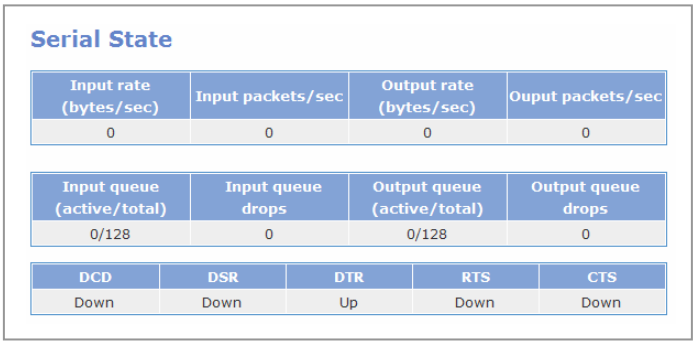
## Accumulated (Накопленные значения)

Выберите [Monitoring] (Контроль) → [Accumulated] (Накопленные значения) для отображения сервером Data Server статистики в виде значений, накопленных в течение года, месяца, недели или часа.




## Serial State (Состояние последовательного порта)

Эта функция используется для отображения нескольких потоков данных и состояния последовательного порта.




| Элемент | Описание |
|---|---|
| Input Rate (Скорость на входе) | Скорость пакетов на входе. |
| Input packets/sec (Пакетов на входе/сек) | Количество пакетов на входе, получаемых в секунду. |
| Output rate (Скорость на выходе) | Скорость пакетов на выходе. |
| Output packets/sec (Пакетов на выходе/сек) | Количество пакетов на выходе, отправляемых в секунду. |

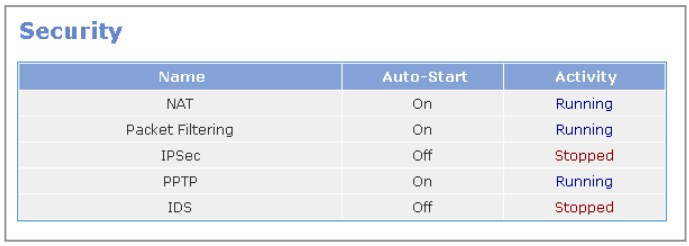
| | |
|---|---|
| Input queue (Очередь на входе) | Количество пакетов в очереди на входе / максимальный размер очереди на входе. |
| Input queue drops (Отброшенные пакеты в очереди на входе) | Количество отброшенных пакетов в очереди на входе или отброшенных в сетевом устройстве, подключенном к последовательному порту. |
| Output queue (Очередь на выходе) | Количество пакетов в очереди на выходе / максимальный размер очереди на выходе. |
| Output queue drops (Отброшенные пакеты в очереди на выходе) | Количество отброшенных пакетов в очереди на выходе. |
| DCD | Обнаружение несущей. Отображение результатов поиска несущей, отправляемых DCE. |
| DSR | Сигнал готовности к работе. Отображение состояния настройки Tx/Rx DCE. |
| DTR | Сигнал готовности терминала. Отображение состояния Tx/Rx канала DTE. |
| RTS | Запрос на отправку. Отображение состояния режима получения DTE Receive Mode. |

# Services (Службы)

В меню [Services] (Службы) в виде таблицы отображаются состояния безопасности, маршрутизатора и служб управления на сервере Data Server.
Если установлен флажок ‘On’ (Вкл) параметра ‘Auto Start’ (Автостарт), служба будет автоматически запускаться при перезагрузке системы. Для параметра ‘Activity’ (Активность) устанавливается значение ‘Running’ (Запущено), если служба предоставлена. В противном случае для него устанавливается значение ‘Stopped’ (Остановлено).

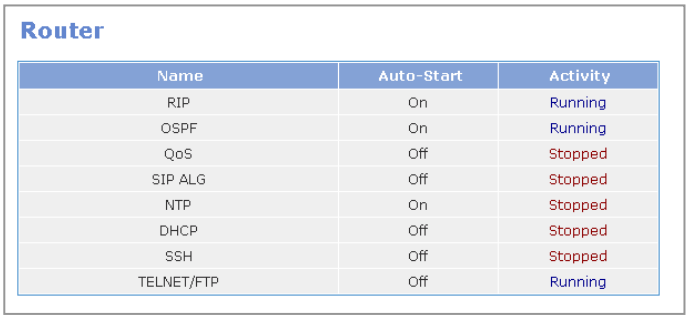
## Безопасность

Этот элемент отображает текущее состояние служб безопасности.



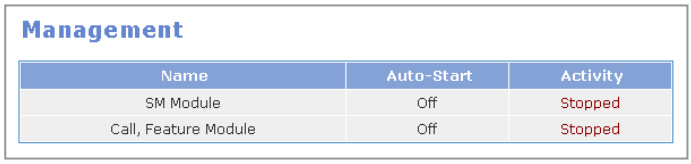
## Маршрутизатор

Этот элемент отображает текущее состояние служб маршрутизатора.




## Управление

Этот элемент отображает текущее состояние служб управления.



# Меню VPN

Чтобы отобразить подменю VPN в верхней левой части окна, выберите [VPN].


| Меню | Подменю | Описание |
|---|---|---|
| IPSec | Config (Настройка) | Включение и выключение протокола IPSec. |
| | Management (Управление) | Разрешение/запрет выполнения IPSec. Включение или выключение запуска IPSec при перезагрузке системы. |
| | Certification (Сертификат) | Создание и удаление сертификата. |
| | Status (Состояние) | Проверка правильности подключения туннеля IPSec. |
| PPTP | Config (Настройка) | Включение и выключение PPTP. |
| | Management (Управление) | Разрешение/запрет выполнения PPTP. Включение или выключение запуска PPTP при перезагрузке системы. |

NOTE

**Настройка клиента VPN Client в Windows XP/2000**

Настройка клиента VPN в MS Windows необходима, если в меню [VPN] на сервере OfficeServ 7200 Data Server включены параметры IPSec и PPTP. Дополнительную информацию о способе настройки см. в ‘ПРИЛОЖЕНИИ A’.

# IPSec

Протокол безопасности IP (IPSec) обеспечивает безопасность уровня IP с помощью протокола Internet Key Exchange (IKE). Служба обеспечения безопасности подразделяется на две службы в зависимости от удаленного оборудования: на службу, обеспечивающую безопасный туннель между локальной и удаленной подсетью и служба, которая обеспечивает безопасность туннеля между локальной подсетью и удаленным хостом. Несмотря на то, что протокол IPSec можно настроить на обеспечение безопасного туннеля между локальным и удаленным хостами, в качестве шлюза используется плата WIM, а не хост. Таким образом, эта служба не используется. Так как при настройке IPSec для обеспечения безопасного туннеля требуются два шлюза, локальный и удаленный, которые имеют общие настройки.

NOTE

**Режим туннеля IPSec**

Сервер OfficeServ 7200 Data Server поддерживает только режим туннеля IPSec и не поддерживает транспортный режим. Если для интерфейса WAN используется последовательный порт, то протокол IPSec не поддерживается. Так как последовательный канал используется в качестве выделенного, использовать протокол IPSec для обеспечения безопасности необязательно.

## Config (Настройка)

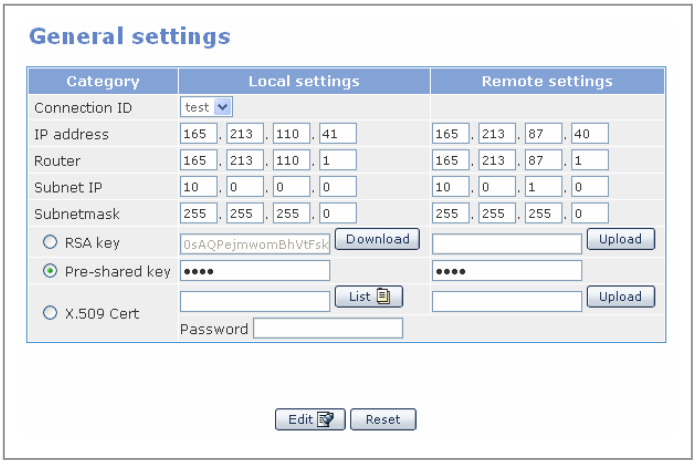
Пользователи могут добавлять, удалять и осуществлять поиск туннелей IPSec в меню [IPSec] → [Config] (Настройка), а также настраивать дополнительные параметры.


Ниже приведено описание кнопок меню:

| Кнопка | Описание |
|---|---|
| Add (Добавить) | Создание туннеля IPSec |
| Delete (Удалить) | Удаление туннеля IPSec |
| Edit (Редактировать) | Изменение данных туннеля IPSec |
| Advanced (Дополнительно) | Настройка дополнительных параметров туннеля IPSec |

## Add (Добавить)

В окне <IPSec Connections> (Соединения IPSec) нажмите кнопку [Add] (Добавить) для отображения окна, изображенного ниже: Введите значение для каждого параметра и нажмите кнопку [Add] (Добавить), чтобы добавить туннель IPSecAdd
Click the [Add] button from the <IPSec Connections> window to display the window below: Enter each item value and click the [Add] button to add an IPSec tunnel.




| Category (Категория) | Описание |
|---|---|
| Connection ID (Идентификатор соединения) | Идентификатор, состоящий из определенных букв (обязателен) |
| IP-адрес | Внешний IP-адрес (обязателен) |
| Router (Маршрутизатор) | IP-адрес маршрутизатора |
| Subnet IP (IP-адрес в подсети) | Внутренний IP-адрес |
| Subnetmask | Internal subnetmask |

| | |
|---|---|
| RSA Key (Ключ RSA)/ Pre-shared Key (Предварительный ключ) /X.509 Cert (сертификат X.509) | Выбор метода проверки подлинности хоста<br>- Ключ RSA: Открытым ключом является ключ RSA в Local settings (Локальные настройки). Нажмите кнопку [Download] (Выгрузить), чтобы сохранить ключ RSA в компьютере и отправить его по каналу наудаленный компьютер. После того, как ключ RSA в Local settings (Удаленные настройки) получит файл по каналу на удаленном компьютере, нажмите кнопку [Upload] (Загрузить) для ввода значения ключа.<br>- Предварительный ключ: Метод проверки подлинности при вводе пароля.<br>- Сертификат X.509: Аутентификация с помощью собственного сертификата и сертификата CA. Local settings (Локальные настройки) напрямую введите имя файла собственного сертификата или нажмите кнопку [List] (Список) и выберите сертификат в списке текущей проверки подлинности. При выборе пункта Certification (Сертификат) автоматически вводится значение Advanced Left ID (Дополнительный левый идентификатор). В Remote settings (Удаленные настройки) нажмите кнопку [Upload] (Загрузить), чтобы получить сторонний сертификат CA. Можно проверить сертификат хоста, зарегистрированного на локальном компьютере и их целостность. |

Если для параметра ‘Router’ (Маршрутизатор) не установлено значение, для него будет использовано значение параметра ‘IP address’ (IP-адрес) в области Local settings (Локальные настройки) и Remote settings (Удаленные настройки).
Если в области Remote settings (Удаленные настройки) для параметров ‘Subnet IP’ (IP-адрес в подсети) и ‘Subnetmask’ (Маска подсети) не установлены значения, будет добавлен безопасный туннель между локальной подсетью и удаленным хостом. Таким образом, клиент IPSec сможет стать частью локальной подсети.

NOTE

**Установка значения для параметра Router (Маршрутизатор)**

Если значение параметра IP address (IP-адрес) (т. е. результат подсетевого маскирования IP-адреса) в области ‘Local settings’(Локальные настройки) совпадает со значением параметра ‘IP Address’ в области ‘Remote settings’ (Удаленные настройки), введите значение параметра ‘IP Address’ в области ‘Remote settings’ в поле параметра ‘Router’ (Маршрутизатор) в области ‘Local settings’, а значение параметра ‘IP Address’ в области ‘Local settings’ в поле параметра ‘IP Address’ в области ‘Remote settings’.

NOTE

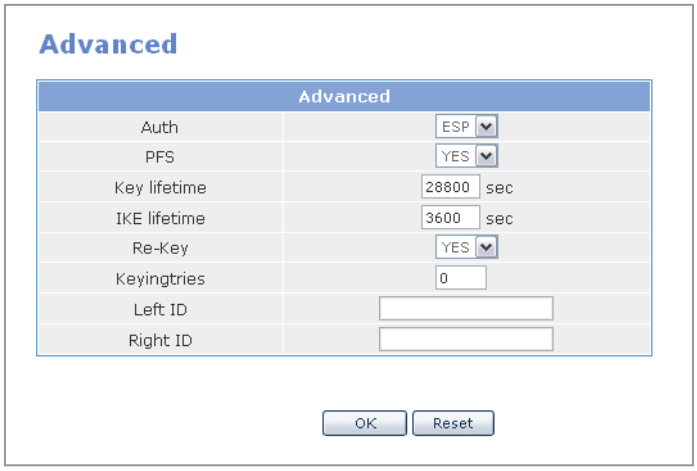
**Установка значения для параметра Connection ID (Идентификатора**

**соединения)**

Идентификатор должен состоять из букв английского алфавита или букв и цифр, а первым символом должна быть буква (идентификатор не может состоять только из цифр).

## Advanced (Дополнительно)

В окне <IPSec Connections> (Соединения IPSec) нажмите кнопку [Advanced] (Дополнительно) для отображения окна, изображенного ниже: Можно настроить дополнительные параметры протокола IPSec. Настройки меню ‘Advanced’ (Дополнительно) доступны, только если взаимная проверка подлинности выполняется с использованием сертификата X.509.



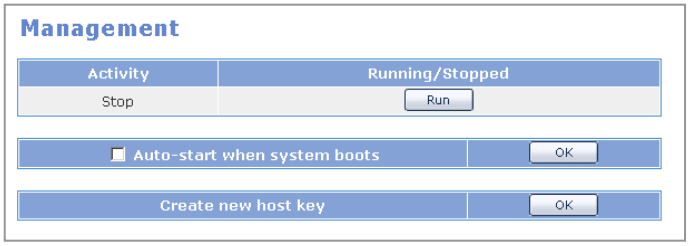

| Элемент | Описание |
|---|---|
| Auth (Проверка подлинности) | Выбор протокола проверки подлинности пакетов.<br>- Заголовок проверки подлинности (Authentication Header - AH): Позволяет выполнять проверку подлинности отправителя данных.<br>- Протокол Encapsulating Security Payload (ESP): Позволяет выполнять проверку подлинности отправителя данных и шифрование данных. |
| PFS | Включение или выключение безопасности при отправке ключа сеанса. |
| Key lifetime (Срок действия ключа) | Срок действия нового ключа, который используется при шифровании пакетов с помощью повторяемого уровня IKE 2. |

| | |
|---|---|
| IKE lifetime (Срок действия IKE) | Время действия IKE<br>По истечении времени действия проверка подлинности хоста (уровень IKE 1) выполняется еще раз. |
| Re-Key | Включение или выключение добавления нового ключа (добавление нового ключа и повторное согласование на уровне IKE 2). |
| Keyingtries | Счетчик попыток обмена ключами при ошибке обмена ключами шифрования на уровне IKE 2. |
| Left ID (Левый идентификатор) | Задание идентификатора если он требуется вместе с IP-адресом. Как правило, IP-адрес используется для проверки подлинности другого хоста на уровне IKE 1. |
| Right ID (Правый идентификатор) | Задание идентификатора если он требуется вместе с IP-адресом. Как правило, IP-адрес используется для проверки подлинности другого хоста на уровне IKE 1. |

Для параметров используются значения по умолчанию. Можно изменять значения параметров PFS или Key lifetime (Срок действия ключа) для совместимости с другими системами. Если параметры ‘Left ID’ (Левый идентификатор) и ‘Right ID’ (Правый идентификатор) не настроены, используется значение IP-адреса.
В X.509 введите предмет сертификата в полях параметров ‘Left ID’ (Левый идентификатор) и ‘Right ID’ (Правый идентификатор) в окне ‘advanced’ (дополнительно).

## Management (Управление)

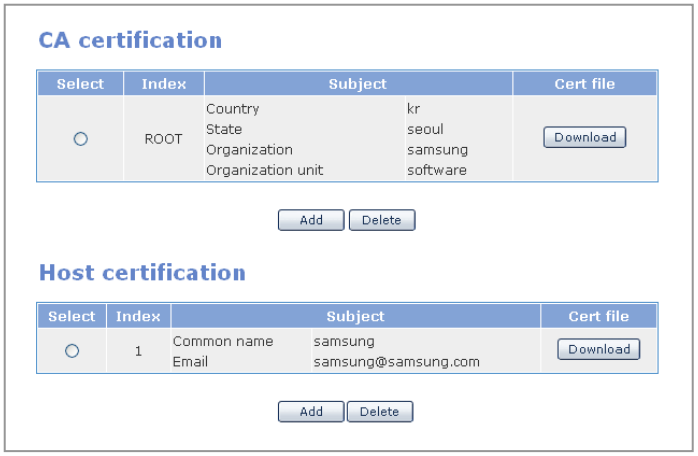
Пользователь может разрешить/запретить выполнение служб IPSec в меню [IPSec] → [Management] (Управление). Установите флажок ‘Auto-start when system boots’ (Автозапуск при загрузке системы) и нажмите кнопку [OK] для автоматического запуска служб IPSec во время перезагрузки системы.




Нажмите кнопку [OK] элемента ‘Create new host key’ (Создать новый ключ хоста), чтобы добавить новый ключ RSA (метод защиты паролем с открытым ключом). Воспользуйтесь этим меню для добавления нового ключа RSA, если используется метод проверки подлинности хоста ключа RSA.

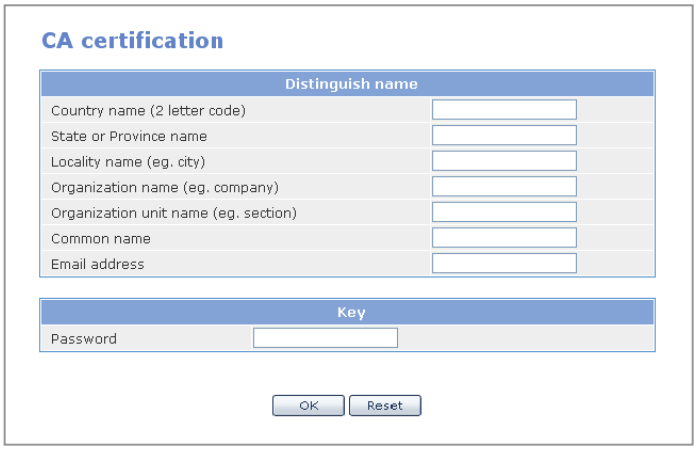
# Certification (Сертификат)

Эта функция позволяет издавать/удалять/загружать сертификаты CA и хоста, а также просматривать список текущих сертификатов.

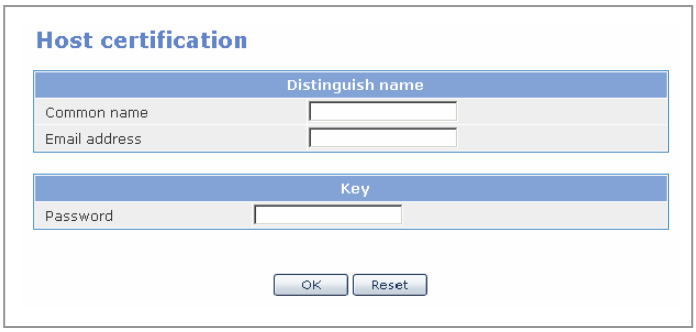



В следующей таблице содержится описание кнопок меню:

| Элемент | Описание |
|---|---|
| (CA) Add (Добавить) | Создание сертификата CA |
| (CA) Delete (Удаление) | Удаление сертификата CA |
| (Host) Add (Добавить) | Создание сертификата хоста |
| (Host) Delete (Удалить) | Удаление сертификата хоста |



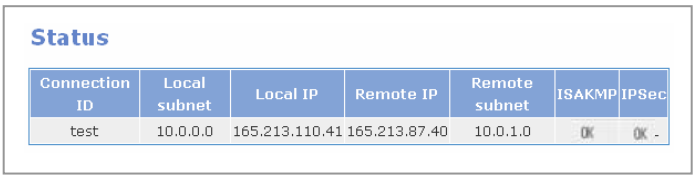
| Элемент | Описание |
|---|---|
| Country name | Название страны (2 буквы, напр. kr, cn) |
| State or Province name | Название штата или провинции |
| Locality name | Название местности |
| Organization name | Название компании |
| Organization unit name | Название отдела организации |
| Common name | Имя пользователя |
| Email address | Адрес электронной почты |
| Password (Пароль) | Пароль для доступа к сертификату |




| Элемент | Описание |
|---|---|
| Common name | Имя пользователя |
| Email address | Адрес электронной почты |
| Password (Пароль) | Пароль для доступа к сертификату |

## Status (Состояние)

Пользователи могут проверить, правильно ли подсоединен туннель назначения IPSec в меню [IPSec] → [Status] (Состояние).

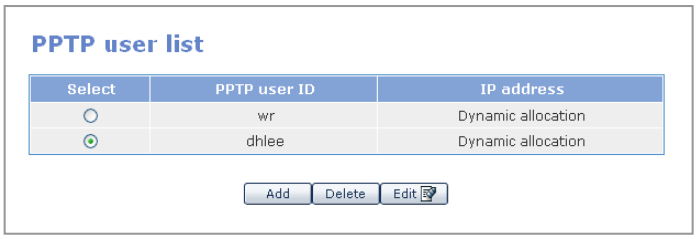


# PPTP

Пользователи могут легко установить безопасный туннель между локальной подсетью и удаленным хостом с помощью протокола Point to Point Tunneling Protocol (PPTP). Так как настройка PPTP достаточно удобна по сравнению с IPSec и программным обеспечением, предоставленным системой Windows, пользователю не составит труда использовать функции VPN.

## Config (Настройка)

Пользователи могут добавлять, редактировать, удалять и искать данные туннеля VPN в меню [PPTP] → [Config] (Настройка), а также настраивать дополнительные параметры.

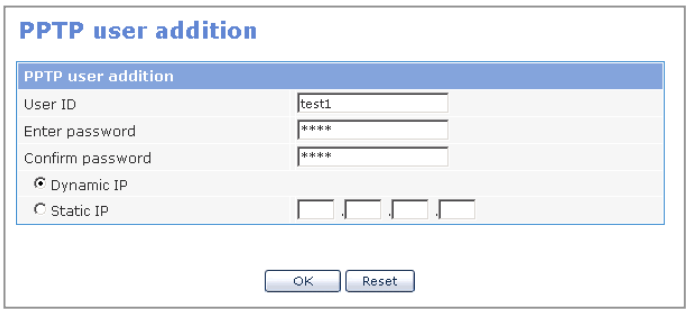



Ниже приведено описание кнопок меню:

| Кнопка | Описание |
|---|---|
| Add (Добавить) | Создание пользователей PPTP |
| Delete (Удалить) | Удаление пользователей PPTP |
| Edit (Редактировать) | Изменение данных пользователя PPTP |

## Add (Добавить)

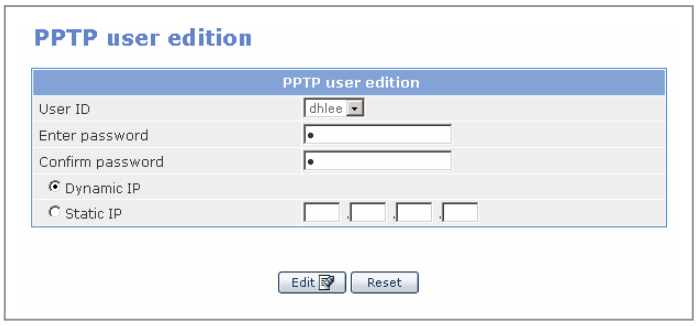
В окне <PPTP user list> (Список пользователей PPTP) нажмите кнопку [Add] (Добавить). Введите значение для каждого параметра и нажмите кнопку [OK], чтобы добавить пользователя PPTP.




| Элемент | Описание |
|---|---|
| User ID (Идентификатор пользователя) | Идентификатор, состоящий из определенных букв |
| Password (Пароль) | Общий пароль |
| Dynamic IP (Динамический IP-адрес) | Ввод динамического IP-адреса удаленного клиента |
| Static IP (Статический IP-адрес) | Ввод статического IP-адреса удаленного клиента (ввод IP-адреса) |

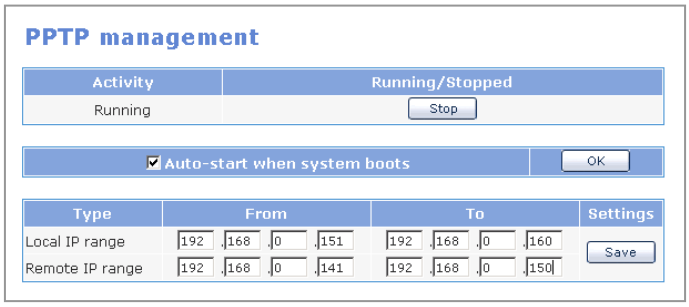
## Edit (Редактировать)

В окне <PPTP user list> (Список пользователей PPTP) нажмите кнопку [Edit] (Редактировать). При этом появляется окно, изображенное ниже. Введите значение для каждого параметра и нажмите кнопку [OK], чтобы отредактировать данные туннеля VPN.



## Management (Управление)

Пользователь может разрешить/запретить выполнение служб PPTP в меню [PPTP] → [Management] (Управление). Установите флажок ‘Auto-start when system boots’ (Автозапуск при загрузке системы) и нажмите кнопку [OK] для автоматического запуска служб PPTP во время перезагрузки системы.




Пользователи могут указать диапазон IP-адресов удаленного клиента, который использует динамический IP-адрес, в поле ‘Local IP range’ (Диапазон локальных IP-адресов), а также задать диапазон IP-адресов в поле ‘Remote IP range’ (Диапазон удаленных IP-адресов) для демона протокола PPP ответственного за удаленного клиента.

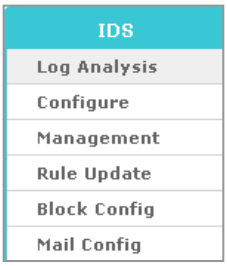
CAUTION

**Задание диапазона IP-адресов**

Количество IP-адресов, заданное для параметров ‘Local IP range’ (Диапазон локальных IP-адресов) и ‘Remote IP range’ (Диапазон удаленных IP-адресов) должно быть одинаковым.
Если, например, количество IP-адресов для параметра ‘Local IP range’ (Диапазон локальных IP-адресов) равно 10, а для параметра ‘Remote IP range’ (Диапазон удаленных IP-адресов) - 20, будут установлены только первые 10.

# Меню IDS

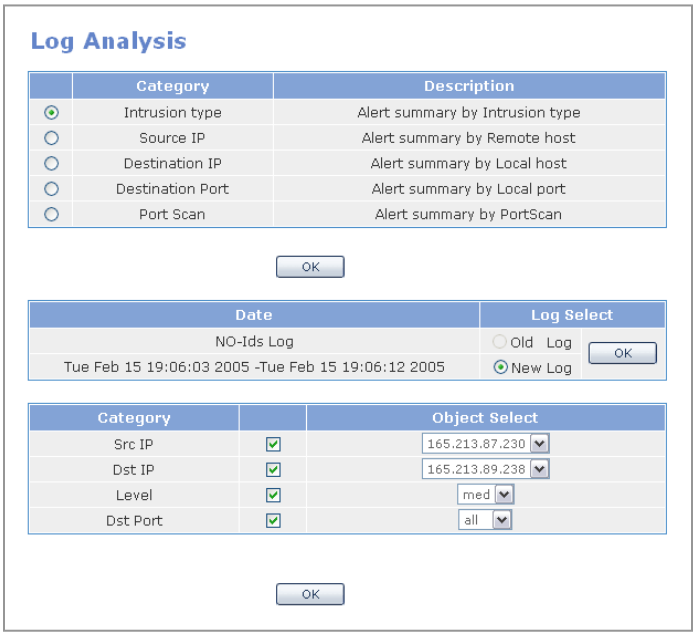
Чтобы отобразить подменю IDS в верхней левой части окна, выберите [IDS].




| Меню | Описание |
|---|---|
| Log Analysis (Анализ записей) | Анализ записей попыток проникновения, обнаруженных с помощью правила системы IDS. |
| Configure (Настроить) | Использование файлов Config (Файл настройки) и Rule (Файл правила) перед запуском IDS. |
| Management (Управление) | Разрешение/запрет выполнения IPSec. Включение или выключение запуска IPSec при перезагрузке системы. |
| Rule Update (Обновление правил) | Обновление путем загрузки новых правил из сети Интернет. |
| Block Config (Настройка блокировки) | Блокировка сетевым экраном исходного IP-адреса, обнаруженного IDS. |
| Mail Config (Настройка почты) | Отправка сообщений IDS при обнаружении IDS. |

# Log Analysis (Анализ записей)

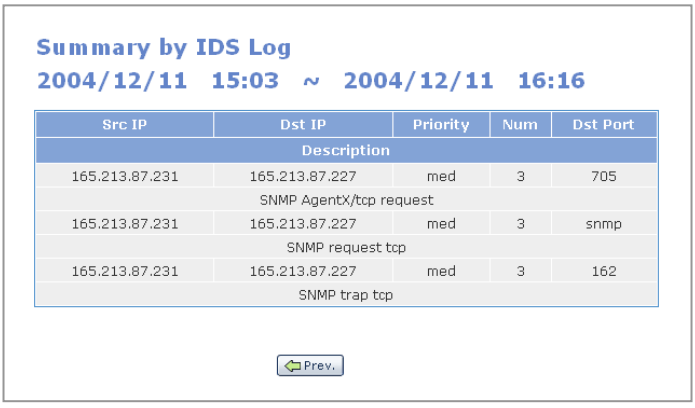
Анализ записей попыток проникновения, обнаруженных с помощью правила системы обнаружения проникновения (IDS) в меню [Log Analysis] (Анализ записей). Выберите Category (Категорию), которую необходимо проанализировать и нажмите кнопку [OK] для отображения результатов заданного анализа записей.




| Category (Категория) | Элемент | Описание |
|---|---|---|
| Category (Категория) | Intrusion type (Тип проникновения) | Анализ записей попыток проникновения, обнаруженных с помощью правил системы IDS разных типов. |
| | Source IP (Исходный IP-адрес) | Анализ записей попыток проникновения, обнаруженных системой IDS, с исходными IP-адресами. |
| | Destination IP (IP-адрес назначения) | Анализ записей попыток проникновения, обнаруженных системой IDS, внешних IP-адресов (WAN1, WAN2, SERIAL) OfficeServ 7200. |

| | | |
|---|---|---|
| | Destination Port (Порт назначения) | Анализ записей в случае совпадения IP-адреса назначения, который содержится в записи, созданной системой IDS, с портом внешнего IP-адреса (WAN1, WAN2, SERIAL). |
| | Port Scan (Сканирование портов) | Анализ записей попыток проникновения, обнаруженных системой IDS, если в них указан тип сканирования портов. |
| Date (Дата) | - | Время создания записи. |
| Log Select (Выбор записи) | Old Log (Старая запись) | Анализ старых записей. |
| | New Log (Новая запись) | Анализ последних записей IDS. |

Выберите пункт ‘Old Log’ (Старая запись) и нажмите кнопку [OK], чтобы выполнить анализ старых записей. При этом в области ‘Object Select’ (Выбор объекта) отобразятся данные, которые содержатся в старых записях.
Выберите пункт ‘New Log’ (Новая запись) и нажмите кнопку [OK], чтобы выполнить анализ последних записей. При этом в области ‘Object Select’ (Выбор объекта) отобразятся данные, которые содержатся в последних записях.
По умолчанию выбран пункт ‘New Log’ (Новая запись). Если запись IDS не существует, отобразится сообщение ‘NO-Ids Log’ (Запись Ids отсутствует).

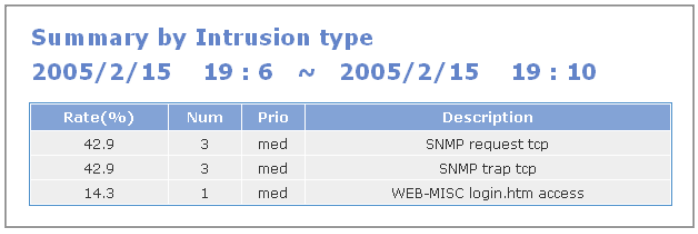



| Элемент | Описание |
|---|---|
| Src IP (Исходный IP-адрес) | Отображение исходного IP-адреса записи обнаруженной попытки проникновения, который является IP-адресом злоумышленника. |

| | |
|---|---|
| Dst IP (IP-адрес назначения) | Отображение IP-адреса назначения записи обнаруженной попытки проникновения, который является IP-адресом атакованного компьютера. |
| Priority (Приоритет) | Уровень риска, зависящий от уровня, который определяется правилами IDS<br>- High (Высокий). Уровень правила - 1 день (высший уровень риска)<br>- Med (Средний). Уровень правила - 2 или 3 дня (средний уровень)<br>- Low (Низкий). Уровень правила - 4 дня (низкий уровень) |
| Num (Количество) | Отображение счетчика атак, типы которых показаны в области ‘Description’ (Описание). |
| Dst Port (Порт назначения) | Отображение IP-адреса назначения. |
| Description (Описание) | Отображение типов атак. |

## Intrusion type (Тип проникновения)

Установите флажок ‘Intrusion type’ (Тип проникновения) в области Category (Категория) в окне <Log Analysis> (Анализ записей) и нажмите кнопку [OK] для отображения окна анализа записей, изображенного ниже: В области Date (Дата) отображается время первого и последнего обнаружения.

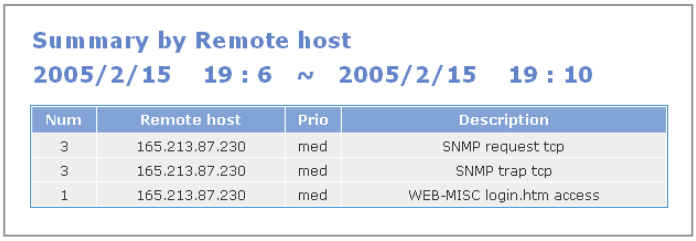



| Элемент | Описание |
|---|---|
| Rate(%) (Процент) | Анализ записей попыток проникновения, обнаруженных системой IDS, определенного типа и отображение результатов в процентном отношении (%). |
| Num (Количество) | Количество записей попыток проникновения, обнаруженных системой IDS, определенного типа |

| | |
|---|---|
| Prio (Приоритет) | Уровень риска, зависящий от уровня, который определяется правилами IDS<br>- High (Высокий). Уровень правила - 1 день (высший уровень риска)<br>- Med (Средний). Уровень правила - 2 или 3 дня (средний уровень)<br>- Low (Низкий). Уровень правила - 4 дня (низкий уровень) |
| Description (Описание) | Типы записей попыток проникновения, обнаруженных системой IDS |

## Source IP

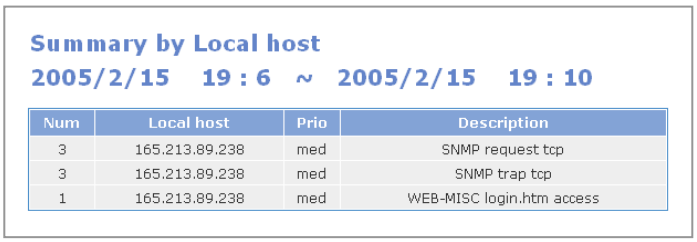
Check ‘Source IP’ from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.




| Элемент | Описание |
|---|---|
| Num (Количество) | Количество записей случаев проникновения, обнаруженных системой IDS, с исходными IP-адресами злоумышленников |
| Remote host (Удаленный хост) | Записи попыток проникновения, обнаруженные системой IDS, с IP-адресами хостов злоумышленников |
| Prio (Приоритет) | Уровень риска, зависящий от уровня, который определяется правилами IDS<br>- High (Высокий). Уровень правила - 1 день (высший уровень риска)<br>- Med (Средний). Уровень правила - 2 или 3 дня (средний уровень)<br>- Low (Низкий). Уровень правила - 4 дня (низкий уровень) |
| Description (Описание) | Типы записей попыток проникновения, обнаруженных системой IDS |

## Destination IP (IP-адрес назначения)

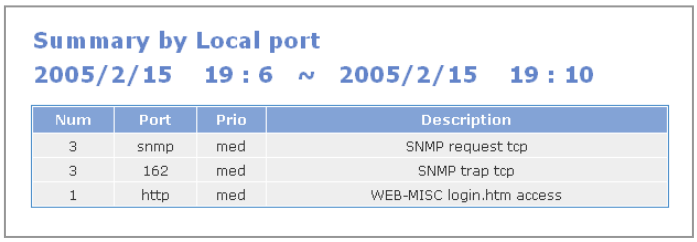
Установите флажок ‘Destination IP’ (IP-адрес назначения) в области Category (Категория) в окне <Log Analysis> (Анализ записей) и нажмите кнопку [OK] для отображения окна анализа записей, изображенного ниже: В области Date (Дата) отображается время первого и последнего обнаружения.




| Элемент | Описание |
|---|---|
| Num (Количество) | Количество записей попыток проникновения, обнаруженных системой IDS, с IP-адресом назначения, на который была произведена атака |
| Local host (Локальный хост) | IP-адрес атакованного хоста, который содержится в записях попыток проникновения, обнаруженных системой IDS |
| Prio (Приоритет) | Уровень риска, зависящий от уровня, который определяется правилами IDS<br>- High (Высокий). Уровень правила - 1 день (высший уровень риска)<br>- Med (Средний). Уровень правила - 2 или 3 дня (средний уровень)<br>- Low (Низкий). Уровень правила - 4 дня (низкий уровень) |
| Description (Описание) | Типы записей попыток проникновения, обнаруженных системой IDS |

## Destination Port (Порт назначения)

Установите флажок ‘Destination Port’ (Порт назначения) в области Category (Категория) в окне <Log Analysis> (Анализ записей) и нажмите кнопку [OK] для отображения окна анализа записей, изображенного ниже: В области Date (Дата) отображается время первого и последнего обнаружения.




| Элемент | Описание |
|---|---|
| Num (Количество) | Количество записей попыток проникновения, обнаруженных системой IDS, которые содержат порт, если IP-адрес назначения, на который была произведена атака, является адресом сети (например, локальной сети или демилитаризованной зоны). |
| Port (Порт) | IP-адрес атакованного хоста, который содержится в записях попыток проникновения, обнаруженных системой IDS |
| Prio (Приоритет) | Уровень риска, зависящий от уровня, который определяется правилами IDS<br>- High (Высокий). Уровень правила - 1 день (высший уровень риска)<br>- Med (Средний). Уровень правила - 2 или 3 дня (средний уровень)<br>- Low (Низкий). Уровень правила - 4 дня (низкий уровень) |
| Description (Описание) | Типы записей попыток проникновения, обнаруженных системой IDS |

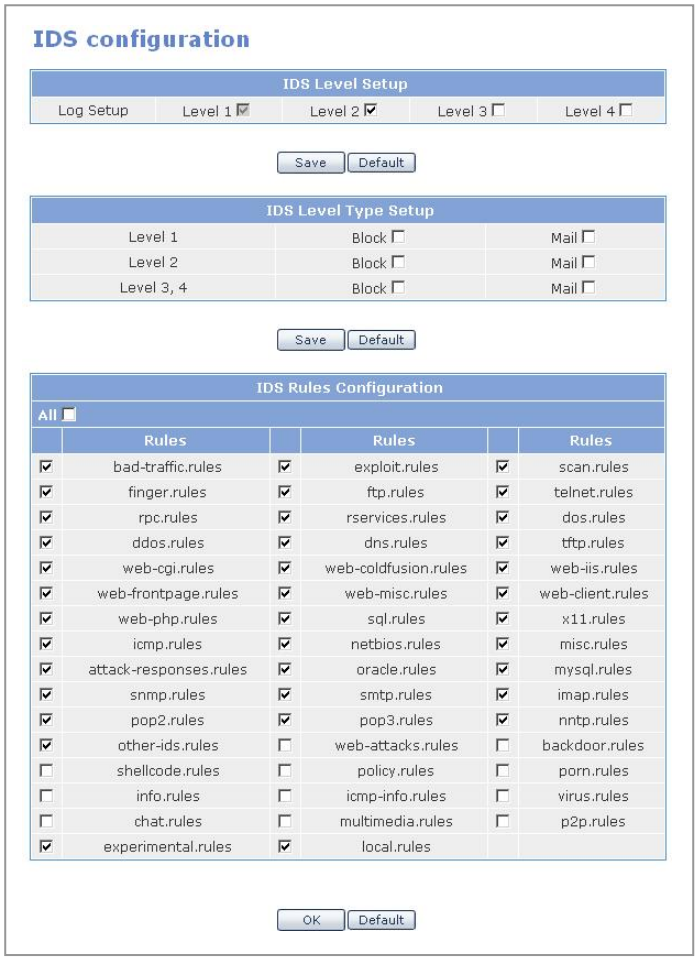
## Port Scan (Сканирование портов)

Установите флажок ‘Port Scan’ (Сканирование портов) в области Category (Категория) в окне <Log Analysis> (Анализ записей) и нажмите кнопку [OK] для отображения окна анализа записей, изображенного ниже: В области Date (Дата) отображается время первого и последнего обнаружения.


| Элемент | Описание |
|---|---|
| ports (порты) | Количество портов TCP и UDP, которые выполнили сканирование портов в записях случаев проникновения, обнаруженных системой IDS. |
| Hosts (Хосты) | Количество сканированных хостами портов в записях случаев проникновения, обнаруженных системой IDS. |
| Remote host (Удаленный хост) | IP-адрес сканированного порта. |

# Configuration (Настройка)

Использование файлов Config (Файл настройки) и Rule (Файл правила) перед запуском IDS в меню [Configuration] (Настройка). После настройки уровня риска в настройке уровня IDS нажмите кнопку [Save] (Сохранить) и выберите правила. Затем нажмите кнопку [OK], чтобы применить правила к файлу настройки IDS и запустить службу IDS.



- IDS Level Setup (Настройка уровня IDS). Существует 4 уровня, которые зависят от уровня риска:

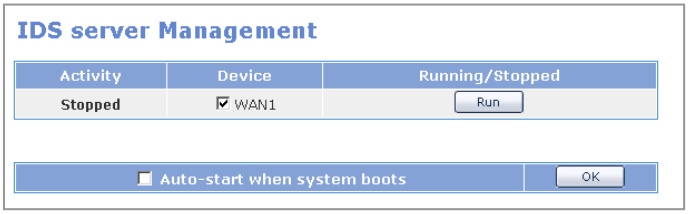
| Настройка уровня | Риск | Описание |
|---|---|---|
| Priority 1 (Приоритет 1) | Высший уровень риска (high) | Правилами IDS определяется только Priority 1 (Приоритет 1) |
| Priority 2 (Приоритет 2) | Средний уровень риска (med) | Правилами IDS определяются Priority 1, 2 (Приоритеты 1, 2). |
| Priority 3 (Приоритет 3) | Средний уровень риска (med) | Правилами IDS определяются Priority 1, 2, 3 (Приоритеты 1, 2, 3). |
| Priority 4 (Приоритет 4) | Низкий уровень риска (low) | Правилами IDS определяются Priority 1, 2, 3, 4 (Приоритеты 1, 2, 3, 4). |

  - Настройка типа уровня IDS. Выберите функцию для каждого уровня и нажмите кнопку [OK].
  - Level 1 (Уровень 1). По умолчанию выполняются функции записи и аварийного оповещения. Можно также включить функцию отключения обнаруженного исходного IP-адреса и отправки электронного письма администратору.
  - Level 2 (Уровень 2). По умолчанию выполняется функция записи. Можно также включить функцию отключения обнаруженного исходного IP-адреса и отправки электронного письма администратору.
  - Level 3, 4 (Уровень 3, 4). По умолчанию выполняется только функция записи. Можно также запретить доступ к IP-адресу обнаруженной начальной точки и включить функцию отправки электронного письма администратору.

- Настройка правил системы IDS. Здесь настраиваются правила, определяющие функцию обнаружения системы IDS. Установите флажок соответствующего правила и нажмите кнопку [Save] (Сохранить), чтобы задать целевой узел или правило для обнаружения. При установке флажка ‘All’ (Все) будут выбраны все правила.

# Management (Управление)

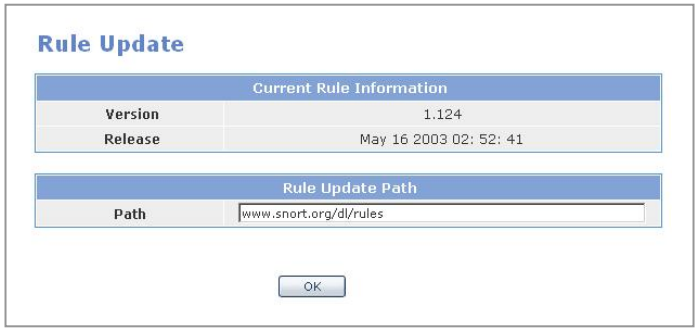
Пользователь может разрешить/запретить работу IDS в меню [Management] (Управление). Установите флажок ‘Auto-start when system boots’ (Автозапуск при загрузке системы) и нажмите кнопку [OK]. При этом служба IDS автоматически запускаться при перезагрузке системы.




| Элемент | Описание |
|---|---|
| Activity (Активность) | - Running (Запущено): IDS работает.<br>- Stopped (Остановлено): работа IDS остановлена. |
| Device (Устройство) | Выбор оборудования для работы с IDS.<br>В качестве оборудования используется только WAN, которая отвечает за настройку сетевого экрана. Также отображается номер оборудования внешней сети, в которой установлен сетевой экран. |
| Running/Stopped (Запущено/Остановлено) | Нажмите кнопку [Run] (Запустить). При этом запустится IDS.<br>Нажмите кнопку [Stop] (Остановить). При этом работа IDS будет остановлена. |
| Auto-start when system boots (Автозапуск при загрузке системы) | При установке флажка и нажатии кнопки [OK] IDS будет автоматически запускаться при перезагрузке системы. Однако при перезагрузке системы сетевой экран запускаться не будет, если система IDS не работает. |

# Rule Update (Обновление правил)

Пользователи могут обновить правила IDS в меню [Rule Update] (Обновление правил). Введите адрес в поле ‘Path’ (Путь) и нажмите кнопку [OK], чтобы загрузить новые правила.




- Current rule information (Информация о текущем правиле). Здесь отображается версия и время создания правила.
- Rule update path (Путь для обновления правил). Введите адрес для загрузки новых правил IDS. При вводе адреса веб-узла опустите ‘http://’, как это показано выше.
  Адрес по умолчанию ‘www.snort.org/dl/rules/(официальный веб-узел IDS<snort>)’.
  Обновление версии выполняется при необходимости: после того, как текущая версия сравнивается с версией обновления (текущая версия - ‘1.124’).

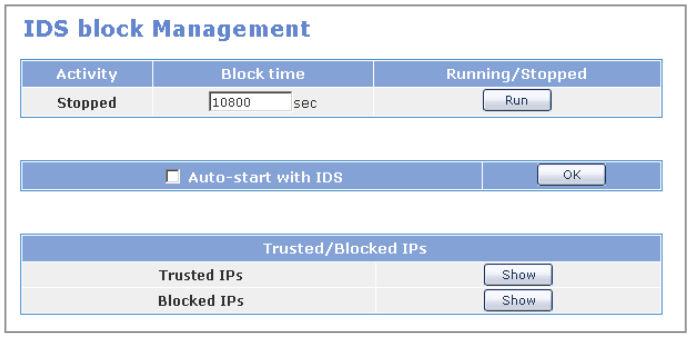
CHECK

**Если не удается обновить правила**

Если адрес сервера доменных имен (DNS) не был введен при установке сетевого экрана, обновление выполнить не удастся. Поэтому проверьте, введен ли адрес DNS, перед обновлением правила.

# Block Config (Настройка блокировки)

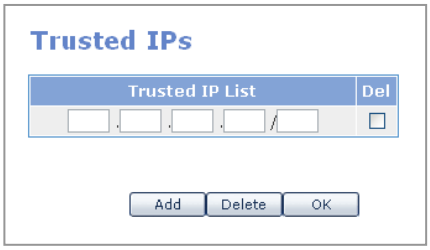
Блокировка исходного IP-адреса, обнаруженного системой IDS, в меню [Block Config] (Настройка блокировки) сетевого экрана. Эта функция выполняется, если система IDS работает.




| Элемент | Описание |
|---|---|
| Activity (Активность) | - Running (Запущено): сервер блокировки IDS работает.<br>- Stopped (Остановлено): сервер блокировки IDS не работает. |
| Block time, sec (Время блокировки, сек.) | Установка времени блокировки исходного IP-адреса, обнаруженного системой IDS.<br>После установки времени и выполнения блокировки сервером IDS исходный IP-адрес блокируется на определенное время, указанное в этом поле, а затем удаляется из Blocked IP List (Списка заблокированных IP-адресов) по истечении времени блокировки.<br>Значение времени блокировки по умолчанию ‘10800’. |
| Running/ Stopped (Запущено/Остановлено) | Нажмите кнопку [Run] (Запустить). Сервер блокировки IDS работает.<br>Нажмите кнопку [Stop] (Остановить). Сервер блокировки IDS не работает. |
| Auto-start when system boots (Автозапуск при загрузке системы) | При установке флажка и нажатии кнопки [OK] IDS будет автоматически запускаться при перезагрузке системы.<br>Однако при перезагрузке системы сетевой экран запускаться не будет, если система IDS не работает. |

### Trusted IPs (Надежные IP-адреса)

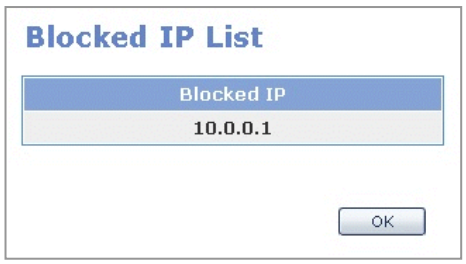
Нажмите кнопку [Show] (Показать) в области ‘Trusted IPs’ (Надежные IP-адреса) окна <IDS block Management> (Управление блокировками IDS) для отображения окна, изображенного ниже: Если исходный IP-адрес, обнаруженный системой IDS, является надежным, введите IP-адрес назначения (или сеть) и нажмите кнопку [Add] (Добавить), чтобы зарегистрировать этот IP-адрес (или сеть).




Так как внутренняя сеть зарегистрирована как надежная, ее регистрация так же, как и регистрация WAN IP необязательна.
Если система IDS неверно выполнила обнаружение, и внешние надежные пользователи не могут получить доступ, следует зарегистрировать соответствующий IP-адрес (или сеть). Таким образом, надежные пользователи смогут получить доступ извне.

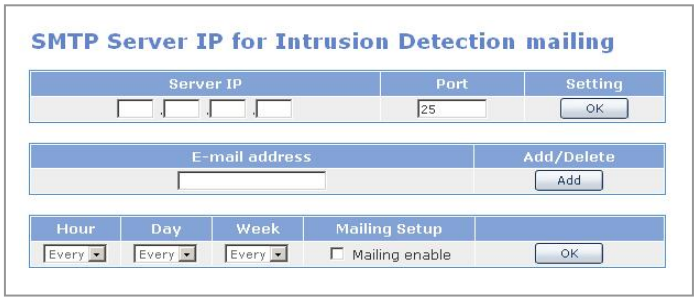
### Blocked IPs (Заблокированные IP-адреса)

Выберите ‘Blocked IPs’ (Заблокированные IP-адреса) в окне <IDS block Management> для отображения окна, изображенного ниже: В этом окне отображаются IP-адреса, заблокированные сервером блокировки IDS или обнаруженные системой IDS.



# Mail Config (Настройка почты)

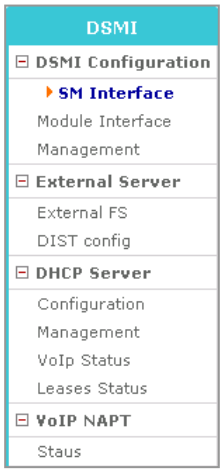
Отправка сигнальных сообщений (записей IDS) администратору в случае обнаружения системой IDS с помощью меню [Mail Config] (Настройка почты).




| Элемент | Описание |
|---|---|
| Server IP (IP-адрес сервера) | IP-адрес почтового сервера<br>Установите почтовый сервер во внутренней сети (например, локальной сети или демилитаризованной зоне) и введите внутренний IP-адрес. |
| Port (Порт) | Простой протокол пересылки почты (SMTP) служебного порта почтового сервера<br>Обычно используется порт номер 25 |
| E-mail address (Адрес электронной почты) | Адрес электронной почты администратора, на который будут отправляться сигнальные сообщения (например, aaa@samsung.com)<br>Нажмите кнопку [Add] (Добавить), чтобы зарегистрировать адрес электронной почты.<br>Нажмите кнопку [Delete] (Удалить), чтобы удалить зарегистрированный адрес электронной почты. |
| Mailing enable/disable (Включить/отключить оповещение письмом) | Установите флажок этого параметра и нажмите кнопку [OK] для включения функции отправки сигнальных сообщений (записей IDS) на зарегистрированный адрес электронной почты. Установите временной промежуток: час, день или неделя. После этого сигнальные сообщения (записи IDS) будут отправляться через определенный промежуток времени. |

# Меню DSMI

Выберите пункт [DSMI], чтобы отобразить подменю DSMI в левой верхней части окна.




| Меню | Подменю | Описание |
|---|---|---|
| DSMI Configuration (Настройка DSMI) | SM Interface (Интерфейс SM) | Настройка функции, отвечающей за обмен сообщениями с системным администратором (System Manager, SM). |
| | Module Interface (Интерфейс модуля) | Настройка среды обмена данными с серверами Call Server и Feature Server. |
| | Management (Управление) | Настройка программы на работу с интерфейсом SM Interface и серверами Call Server и Feature Server. Можно также остановить работу программы или настроить ее на запуск при перезагрузке системы. |
| External Server (Внешний сервер) | External FS (Внешний сервер FS) | Установка или удаление IP-адреса сервера Feature Server, существующего во внешней (общедоступная сеть при использовании NAT), а не в частной сети. |
| | DIST Config (Настройка DIST) | Отправка сообщения, которое было отправлено на порт назначения извне, на терминал назначения внутренней сети. То есть сообщения, полученные определенным портом, отправляются на несколько терминалов. |

**(Продолжение)**

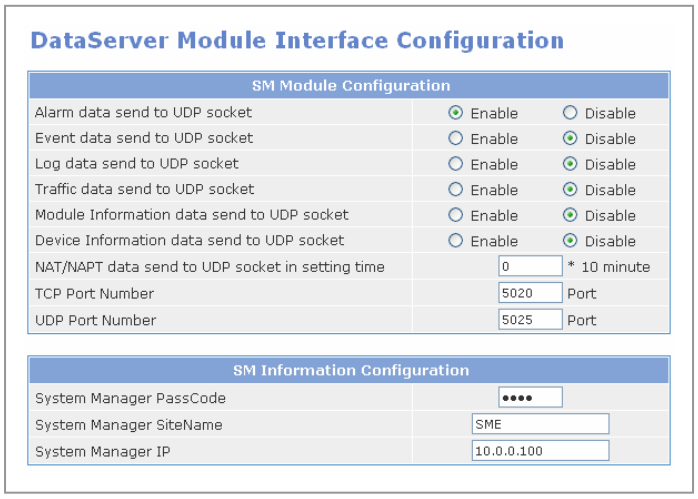
| Меню | Подменю | Описание |
|---|---|---|
| DHCP Server (Сервер DHCP) | Configuration (Настройка) | Настройка внутренней сети на работу с сервером DHCP и пулом IP-адресов для терминала DHCP. Можно настроить пул IP-адресов для Call Server, Feature Server, MGI, IP Phone, SIP Phone и стандартного терминала ввода данных. |
| | Management (Управление) | Разрешение/запрещение работы сервера DHCP. Настройка сервера DHCP на запуск при перезагрузке системы. |
| | VoIP Status (Состояние VoIP) | При работе программы с сервером Call Server или Feature Server выполняется обмен данными IP-терминала системы OfficeServ 7200, полученными с сервера Call Server или Feature Server. |
| | Leases Status (Состояние аренды) | Отображение списка IP-адресов, арендованных клиентами у сервера DHCP. |
| VoIP NAPT | Status (Состояние) | Отображение сведений статического NAPT для службы VoIP OfficeServ 7200. При работе программы с серверами Call Server и Feature Server эти сведения задаются автоматически. Сведения отображаются после завершения настройки. |

# DSMI Configuration (Настройка DSMI)

Настройка среды интерфейса Data Server Module Interface (DSMI) с помощью меню [DSMI Configuration] (Настройка DSMI).

## SM Interface (Интерфейс SM)

Опции, отвечающие за обмен сообщениями системой администрирования (System Manager, SM), можно настроить в меню [SM Interface] (Интерфейс SM). Так как при обмене сообщениями сетевой трафик и система могут быть перегружены из-за чрезмерно большого объема передаваемой информации, пользователю следует контролировать передачу данных и установить необходимый интервал передачи.



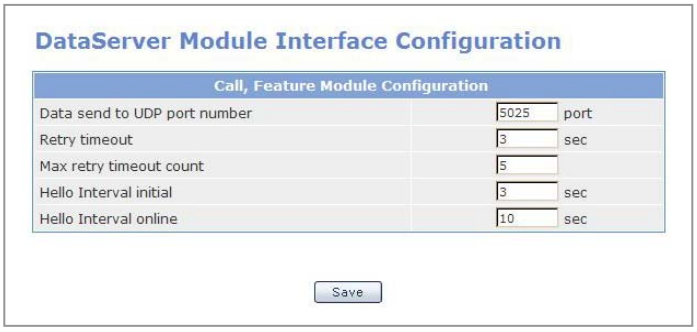

Если данные при обмене сообщениями передаются с помощью протокола UDP, настройте отправку данных, как это изображено выше. Если данные при обмене сообщениями передаются с помощью протокола TCP, пользователю необязательно настраивать отправку данных, так как данные отправляются по требованию системного администратора.
Для порта TCP установлено значение ‘5020’, а для порта UDP - ‘5025’. Эти значения изменять не следует.
В нижнем окне отображается информация телефонного сервера Call Server.

| Category (Категория) | Элемент | Описание |
|---|---|---|
| SM Module (Модуль SM) | Alarm data (Данные аварийной сигнализации) | При установке значения ‘Enable’ (Включено) сигнальное сообщение, которое создается при серьезной ошибке системы или атаке хакера, сразу отправляется системному администратору через порт UDP. |
| | Event data (Данные события) | При установке значения ‘Enable’ (Включено) сгенерированное сообщение о системном событии сразу отправляется системному администратору через порт UDP. |
| | Log data (Данные записи) | Если установлено значение ‘Enable’ (Включено), сообщение сразу отправляется системному администратору через порт UDP при попытке пользователя получить доступ к настройкам системы. |
| | Traffic data (Данные трафика) | При установке значения ‘Enable’ (Включено) данные сетевого трафика, сгенерированные сетевым оборудованием, регулярно отправляются системному администратору через порт UDP (30 минут). |
| | Module Information data (Данные модуля) | При установке значения ‘Enable’ (Включено) данные системного модуля отправляются системному администратору через порт UDP. |
| | Device (Устройство) Information data (Данные устройства) | При установке значения ‘Enable’ (Включено) данные системного сетевого оборудования отправляются системному администратору через порт UDP. |
| | NAT/NAPT data (Данные NAT/NAPT) | Установка интервала времени отправки данных о IP-адресах и соединениях, которые используют службы NAT/NAPT. Например, если ввести ‘5’, данные будет отправляться каждые 50 минут. |
| | TCP Port Number (Номер порта TCP) | Установка значения порта подключения TCP к системе администрирования Значение по умолчанию - 5020. |
| | UDP Port Number (Номер порта UDP) | Установка значения порта подключения UDP к системе администрирования Значение по умолчанию - 5025. |

| | | |
|---|---|---|
| SM Information (Информация о SM) | System Manager Passcode (Пароль системного администратора) | Отображение пароля системного администратора, полученного с телефонного сервера Call Server. Установка пароля нелбходима. |
| | System Manager Sitename (Имя хоста системного администратора) | Отображение имени хоста системного администратора, полученного с телефонного сервера Call Server. Установка имени хоста необходима. |
| | System Manager IP (IP-адрес системного администратора) | Отображение IP-адреса системного администратора, полученного с телефонного сервера Call Server. Установка IP-необходима. |

## Module Interface

Среду для работы с серверами телефонии Call Server или приложений Feature Server можно настроить в меню [Module Interface] (Интерфейс модуля). При перезагрузке системы устанавливаются значения по умолчанию, как показано ниже:

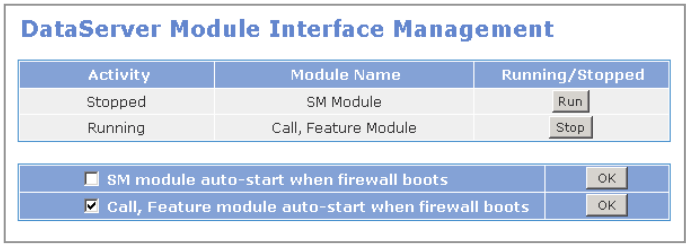



| Элемент | Описание |
|---|---|
| Data send to UDP port number (Отправка данных на номер порта UDP) | Сведения порта UDP для работы программы с сервером Call Server или Feature Server. Значение по умолчанию - ‘5025’. |

| | |
|---|---|
| Retry timeout (Sec) (Тайм-аут повторной попытки, сек.) | DSMI_CF, Call Server, Feature Server и Data Server обмениваются данными с помощью протокола UDP. Если при использовании протокола UDP теряется пакет, то выполняется его повторный запрос. Установка интервала времени между попытками. Например, значение интервала - ‘3’. Означает, что через 3 секунды будет повторно запрошена передача UDP пакета . |
| Max retry timeout count (Макс. количество тайм-аутов повторных попыток) | Счетчик повторных попыток передачи UDP пакетов от служб DSMI_CF и серверами Call Server и Feature Server. Например, если для параметра Retry timeout и Counter (Тайм-аут и счетчик повторной попытки) установлены значения ‘3’ и ‘5', то попытка выполняется пять раз каждые три секунды. Если запрошенный пакет не приходит, повторная передача приостанавливается. |
| Hello Interval initial (Интервал начального приветствия) | Сообщение приветствия - это сообщение, которым периодически обмениваются DSMI_CF, Call Server и Feature Server. Установите интервал времени для отправки сообщений приветствия. |
| Hello Interval online (Интервал интерактивного приветствия) | Программы серверов Call Server и Feature Server отправляют сообщение приветствия с интервалом ‘Hello Interval initial’ (Интервал начального приветствия) для проверки сведений работоспособности другой стороны и отображения рабочего состояния программы после перезагрузки. При получении сообщения приветствия с серверов Call Server и Feature Server во время его оправки оно должно отправляться каждый раз через определенный промежуток времени, указанный для этого параметра. Это значение должно быть больше значения параметра ‘Hello Interval initial’ (Интервал начального приветствия). |

## Management

Службу для обмена данными с SM или серверами Call Server и Feature Server можно запустить или остановить с помощью меню [Management] (Управление). Установите флажок ‘Auto Start’ (Автозапуск). После этого соответствующая программа будет автоматически запускаться при перезагрузке системы.



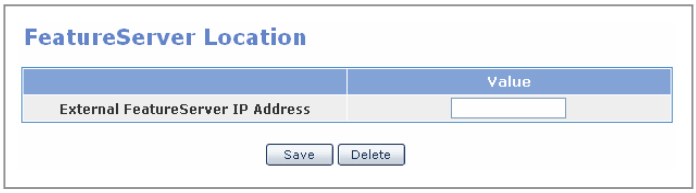

Установите флажок ‘SM module auto-start when firewall system boots’ (Автозапуск модуля SM при загрузке системы сетевого экрана) или ‘Call, Feature module auto-start when firewall system boots’ (Автозапуск модулей Call, Feature при загрузке системы сетевого экрана) и нажмите кнопку [OK]. После этого программа интерфейса SM или Call, Feature будет запускаться автоматически.

# External Server (Внешний сервер)

Если сервер приложений Feature Server находится во внешней общедоступной сети, а система OS7200 во внутренней локальной сети, которая использует NAT, то с помощью меню [External Server] (Внешний сервер) можно указать IP-адрес сервера Feature.

## External FS (Внешний сервер FS)

Установка IP-адреса сервера Feature Server внешней сети в меню [External FS] (Внешний FS).



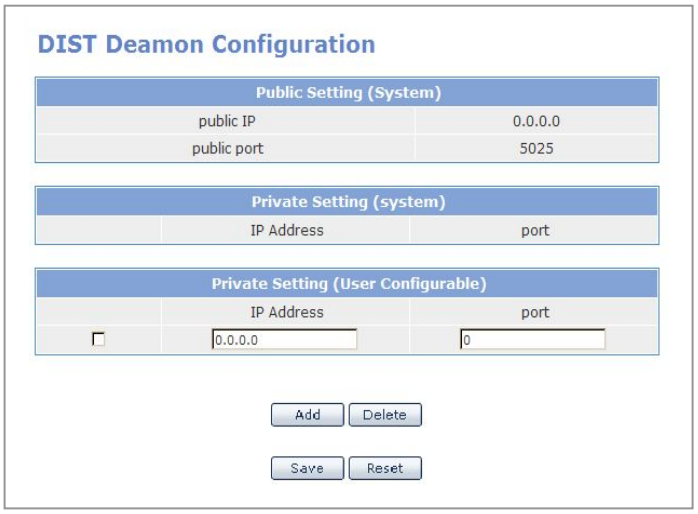

NOTE

**Сервер Feature Server во внутренней сети**

- Если сервер Feature Server находится во внутренней сети, в поле ‘External Feature Server address’ (Адрес внешнего сервера Feature Server) IP-адрес вводить не следует, его следует ввести в поле адреса сервера Feature Server в меню [DSMI] → [DHCP Server] (Сервер DHCP) → [Configuration] (Настройка).
- Если сервер Feature Server указан и в меню [DSMI] → [External Server] (Внешний сервер) → [External FS] (Внешний FS), и в [DSMI] → [DHCP Server] (Сервер DHCP) → [Configuration] (Настройка), пакет UDP будет отправлен на сервер Feature Server, указанный в меню внешнего сервера.

# DIST Config

в меню [DIST Config] (Настройка DIST) настраивются параметры терминала внутренней сети на отправку сообщений, полученных извне по указанному порту,
IP-адреса сервера Feature Server и системного администратора внешней сети, заданные в DSMI, автоматически регистрируются в ‘Private Setting(System)’ (Локальные настройки [система]).
Введите IP-адрес и порт в ‘Private Setting (User Configurable)’ (Локальные настройки [пользовательские]) и по очереди нажмите кнопки [Add] (Добавить) и [Save] (Сохранить) для регистрации дополнительного IP-адреса.

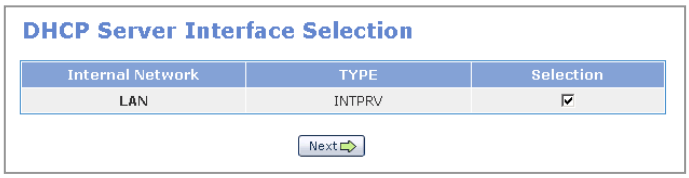


# DHCP Server (Сервер DHCP)

Настройка оборудования для работы с сервером DHCP производится в меню [DHCP Server] (Сервер DHCP) и разрешение или запрещение работы сервера DHCP.

## Configuration (Настройка)

Выберите оборудование внутренней сети для работы с сервером DHCP в меню [Firewall/Network] (Сетевой экран/Сеть) в меню [Configuration] (Настройка).
Войдите в меню [DHCP Server] (Сервер DHCP) → [Configuration] (Настройка) для отображения внутренней сети, для которой установлено значение ‘Internal Private Network’ (Внутренняя частная сеть) или ‘Internal Public Network’ (Внутренняя общедоступная сеть) в меню [Firewall/Network] (Сетевой экран/Сеть) → [Management] (Управление) → [Configuration] (Настройка).



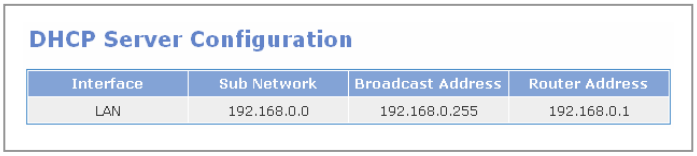

Установите флажок для элемента, который необходимо настроить, и нажмите кнопку [Next] (Далее) для отображения окна <DHCP Server Configuration> (Настройка сервера DHCP) настройки среды.

В окне <DHCP Server Configuration> (Настройка сервера DHCP) отображается значение по умолчанию оборудования, выбранного в окне <DHCP Server Interface Selection> (Выбор интерфейса сервера DHCP). Назначьте для сервера DHCP IP-адреса системы OfficeServ 7200, такие как телефонный сервер Call Server, подсеть которого находится на одном уровне с подсетью выбранного оборудования, сервер Feature Server, IP-телефоны, SIP-телефоны и терминал данных.

Настройте следующие параметры и нажмите кнопку [Save] (Сохранить).

## DHCP Server (Сервер DHCP)

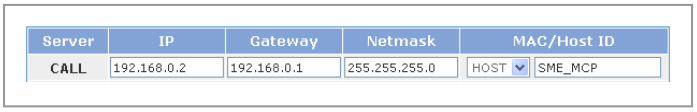
Отображение обычных данных, выделяемых клиенту DHCP. Установка времени аренды.




| Элемент | Описание |
|---|---|
| Sub Network (Подсеть) | Данные подсети<br>Значение устанавливается в меню [Firewall/Network] (Сетевой экран/Сеть) ( [Management] (Управление) ( [Config] (Настройка). Это значение можно изменить в этом меню. |
| Broadcast Address (Широковещательный адрес) | Широковещательный адрес<br>Значение устанавливается в меню [Firewall/Network] (Сетевой экран/Сеть) ( [Management] (Управление) ( [Config] (Настройка). Это значение можно изменить в этом меню. |
| Router Address (Адрес маршрутизатора) | Адрес маршрутизатора<br>Значение устанавливается в меню [Firewall/Network] (Сетевой экран/Сеть) ( [Management] (Управление) ( [Config] (Настройка). Это значение можно изменить в этом меню. |
| Default Lease Time, sec (Время аренды по умолчанию, сек.) | Если клиент DHCP не запрашивает срок действия, то оно будет установлено в соответствии с этим параметром. |
| MAX Lease Time, sec (Макс. время аренды) | Если клиент DHCP запрашивает срок действия, то будет установлено данное максимальное время аренды. |

## Сервер CALL Server

Установка IP-адреса телефонного сервера Call Server. Когда сервер Call Server работает в режиме DHCP, ему назначается IP-адрес. В случае проверки подлинности по имени хоста устанавливается ‘Host ID’ (Идентификатор хоста). По умолчанию ‘SME_MCP’.



| Элемент | Описание |
|---|---|
| IP (IP-адрес) | IP-адрес сервера Call Server |
| Gateway (Шлюз) | Данные шлюза |
| Netmask (Маска сети) | Данные маски сети |
| MAC/Host ID (Идентификатор MAC-адреса/Хоста) | Тип проверки подлинности клиентов<br>- NONE (НЕТ): выполняется запрос IP-адреса DHCP без проверки подлинности.<br>- MAC (MAC-адрес): проверка подлинности по MAC-адресу<br>- HOST (ХОСТ): проверка подлинности по Host ID (значение по умолчанию: SME_MCP) |

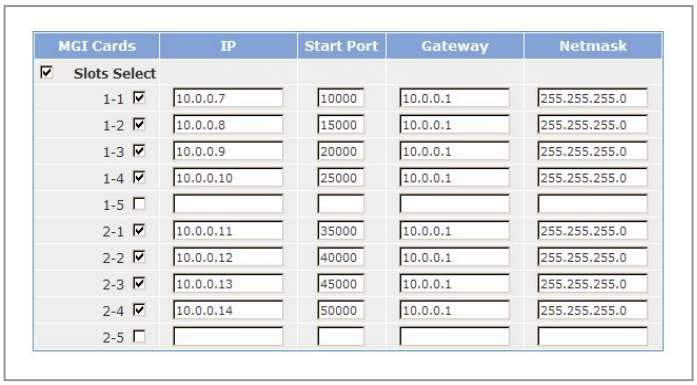
## Сервер Feature Server

Установка IP-адреса сервера Feature Server. Когда сервер Feature Server работает в режиме DHCP, ему назначается IP-адрес. В случае проверки подлинности по имени хоста устанавливается ‘Host ID’ (Идентификатор хоста). По умолчанию ‘SME_FEATURE’.


Если сервер Feature Server не содержит серверы UMS и MAIL, их IP-адреса следует указать. Так как параметры серверов UMS и MAIL неактивны, установите флажок слева и введите соответствующие значения.

## MGI Cards (Карты MGI)

Установка IP-адреса встроенных в систему карт MGI.
После установки флажка ‘Slots Select’ (Выбор слотов) установите флажок слева от параметра и введите соответствующие значения.



Это значение должно быть таким же, как данные сети в меню [Firewall/Network] (Сетевой экран/Сеть) ( [Management] (Управление) ( [Config] (Настройка). Количество карт MGI может достигать 10 штук, а номер, отображаемый слева, означает местоположение слотов. ‘Start Port’ (Начальный порт) означает номер первого из 32 UDP портов, с которым будет работать карта MGI. Если ничего не указано, значение, устанавливается начиная с 10000 и увеличивается для каждого следующего слота на 5000.

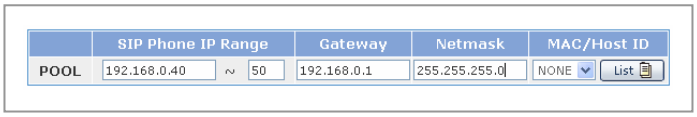
## IP Phone (IP-телефон)

Определение диапазона IP-адресов IP-телефонов в режиме DHCP. Пул IP-адресов DHCP, который определяется в этом меню, настроен на проверку подлинности IP-телефонов серии ITP-5000 и на установку их IP-адресов.


| Элемент | Описание |
|---|---|
| IP Range (Диапазон IP-адресов) | Диапазон IP-адресов IP-телефона (максимальное количество IP-телефонов - 120)<br>Если указан один IP-адрес, введите ‘192.168.0.20~20’. |
| Gateway (Шлюз) | Данные шлюза, указанные в телефонном сервере CALL Server |
| Netmask (Маска сети) | Данные маски сети, указанные в телефонном сервере CALL Server |
| MAC/Host-ID (Идентификатор MAC-адреса/Хоста) | Тип проверки подлинности клиентов<br>- NONE (НЕТ): выполняется запрос IP-адреса DHCP без проверки подлинности.<br>- MAC (MAC-адрес): нажмите кнопку [List] (Список), чтобы ввести MAC-адрес IP-телефона для проверки подлинности.<br>- HOST (ХОСТ): используемый HOST ID для проверки подлинности телефона серии ITP-5000, который указывается внутренне. |

## SIP Phone (SIP-телефон)

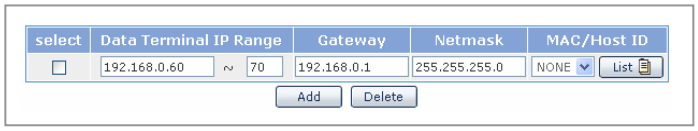
Определение диапазона IP-адресов стандартного SIP-телефона в режиме DHCP.




| Элемент | Описание |
|---|---|
| IP Range (Диапазон IP-адресов) | Диапазон IP-адресов SIP-телефона (максимальное количество IP-телефонов - 120)<br>Если указан один IP-адрес, введите ‘192.168.0.40~40’. |
| Gateway (Шлюз) | Данные шлюза, указанные в телефонном сервере CALL Server |
| Netmask (Маска сети) | Данные маски сети, указанные в телефонном сервере CALL Server |
| MAC/Host-ID (Идентификатор MAC-адреса/Хоста) | Тип проверки подлинности клиентов<br>- NONE (НЕТ): выполняется запрос IP-адреса DHCP без проверки подлинности<br>- MAC (MAC-адрес): нажмите кнопку [List] (Список), чтобы ввести MAC-адрес IP-телефона для проверки подлинности.<br>- HOST (ХОСТ): Так как Host-ID, указываемый внутренне, не используется, нажмите кнопку [List] (Список) для ввода Host-ID. |

### Terminal (Терминал)

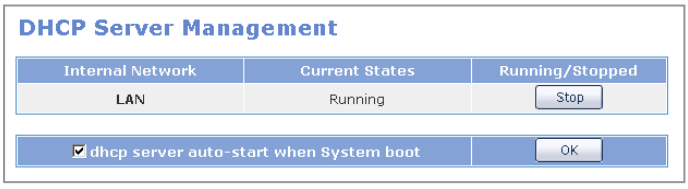
Назначение терминалов для DHCP.




| Элемент | Описание |
|---|---|
| IP Range (Диапазон IP-адресов) | Диапазон IP-адресов терминала данных (максимальное количество IP-телефонов - 120)<br>Если указан один IP-адрес, введите '192.168.0.60~60'. |
| Gateway (Шлюз) | Данные шлюза, указанные в телефонном сервере CALL Server |
| Netmask (Маска сети) | Данные маски сети, указанные в телефонном сервере CALL Server |
| MAC/Host-ID (Идентификатор MAC-адреса/Хоста) | Тип проверки подлинности клиентов<br>- NONE (НЕТ): выполняется запрос IP-адреса DHCP без проверки подлинности.<br>- HOST (ХОСТ): нажмите кнопку [List] (Список) для ввода Host-ID.<br>- MAC (MAC-адрес): нажмите кнопку [List] (Список), чтобы ввести MAC-адрес. |

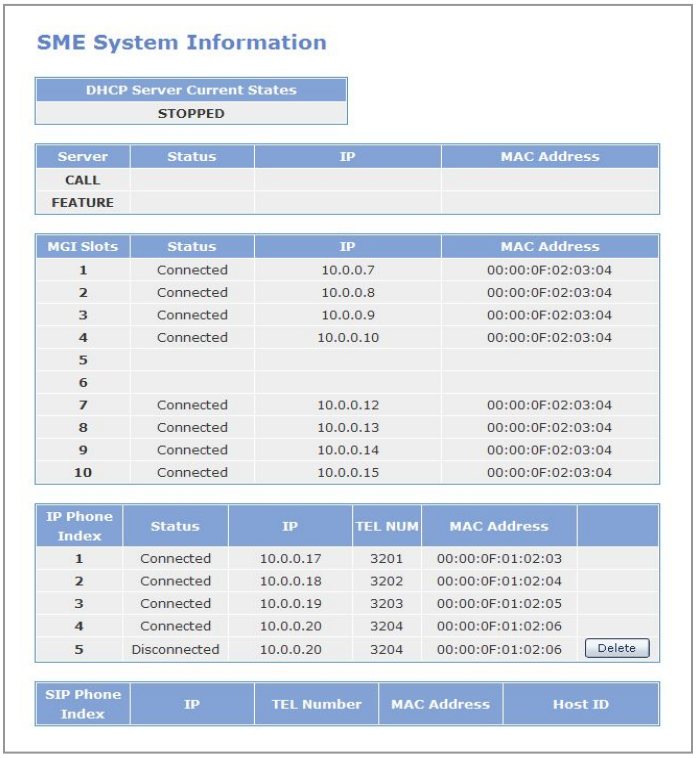
## Management

Select the [DHCP Server] → [Management] menu to allow/inhibit operating the DHCP Server. Check the 'Auto Start' item. Then, the service is provided automatically while the system reboots.



# VoIP Status (Состояние VoIP)

Отображение системных данных OfficeServ 7200, которые удалось получить на данный момент, в меню [DHCP Server] (Сервер DHCP) → [VoIP Status] (Состояние VoIP).
При изменениях в меню [DHCP Server] (Сервер DHCP) → [Configuration] (Настройка) данных сервера DHCP, при работе которого автоматически назначаются IP-адреса для серверов Call Server и Feature Server, эти данные передаются в интерфейс сервера Data Server, и пользователь получает возможность просмотра этих данных в следующем окне.



SME System Information

| DHCP Server Current States |
|---|
| STOPPED |

| Server | Status | IP | MAC Address |
|---|---|---|---|
| CALL | | | |
| FEATURE | | | |

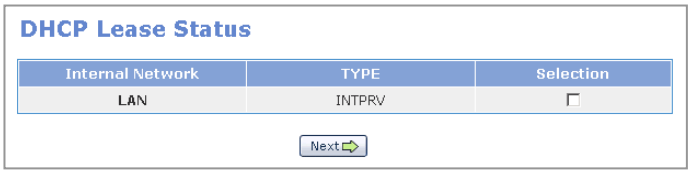
| MGI Slots | Status | IP | MAC Address |
|---|---|---|---|
| 1 | Connected | 10.0.0.7 | 00:00:0F:02:03:04 |
| 2 | Connected | 10.0.0.8 | 00:00:0F:02:03:04 |
| 3 | Connected | 10.0.0.9 | 00:00:0F:02:03:04 |
| 4 | Connected | 10.0.0.10 | 00:00:0F:02:03:04 |
| 5 | | | |
| 6 | | | |
| 7 | Connected | 10.0.0.12 | 00:00:0F:02:03:04 |
| 8 | Connected | 10.0.0.13 | 00:00:0F:02:03:04 |
| 9 | Connected | 10.0.0.14 | 00:00:0F:02:03:04 |
| 10 | Connected | 10.0.0.15 | 00:00:0F:02:03:04 |

| IP Phone Index | Status | IP | TEL NUM | MAC Address | |
|---|---|---|---|---|---|
| 1 | Connected | 10.0.0.17 | 3201 | 00:00:0F:01:02:03 | |
| 2 | Connected | 10.0.0.18 | 3202 | 00:00:0F:01:02:04 | |
| 3 | Connected | 10.0.0.19 | 3203 | 00:00:0F:01:02:05 | |
| 4 | Connected | 10.0.0.20 | 3204 | 00:00:0F:01:02:06 | |
| 5 | Disconnected | 10.0.0.20 | 3204 | 00:00:0F:01:02:06 | Delete |

| SIP Phone Index | IP | TEL Number | MAC Address | Host ID |
|---|---|---|---|---|

## Leases Status (Состояние аренды)

Выберите [DHCP Server] (Сервер DHCP) → [Leases Status] (Состояние аренды). После этого отобразится IP-адрес, выделенный сервером DHCP терминалу данных.

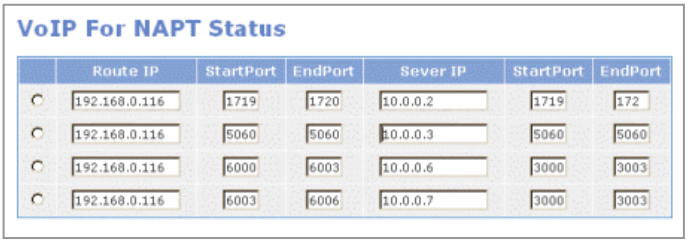



# VoIP NAPT

В меню [VoIP NAPT] отображается NAPT настройки для соединений VoIP

## Status (Состояние)

Connects 32 internet ports and external ports to each MGI card through one to one mapping. Whenever the DHCP Server item is newly set, the program for the connection with the Call Server and with the Feature Server exchanges new information with the Call Server. At this time, the NAPT item is configured on the Data Server for VoIP communication of H.323 phone. The [Status] menu displays the corresponding data.
32 UDP порта каждой платы MGI однозначно увязываются с таким же количеством портов для публичной сети. Каждый раз при настройке элемента DHCP Server (Сервер DHCP) программа, используемая для соединения с сервером телефонии Call Server и приложений Feature Server, обменивается новой информацией с сервером Call Server. В этом примере отражается настройка NAPT на сервере Data Server для соединения H.323 IP-телефона по VoIP с. В меню [Status] (Состояние) отображаются соответствующие данные.



Параметры внутреннего/внешнего IP адреса и порта MGI card (Платы MGI), заданные в меню [DHCP Server] (Сервер DHCP)→ [Configuration] (Настройка) и VoIP NAPT для сервера Call Server и Feature Server, для обработки вызовов, будут переданы DSMI_CF программой серверу телефонии Call Server. В приведенном выше окне эти данные отображаются в виде таблицы VoIP NAPT.

# Меню SIP ALG

Чтобы отобразить подменю SIP ALG в левой верхней части окне, выберите [SIP ALG].


| Меню | Описание |
|---|---|
| Config (Настройка) | Настройка среды SIP |
| Management (Управление) | Разрешение/запрет выполнения SIP ALG. Настройка SIP ALG на запуск при перезагрузке системы. |

NOTE

**SIP ALG (SIP с поддержкой ALG)**

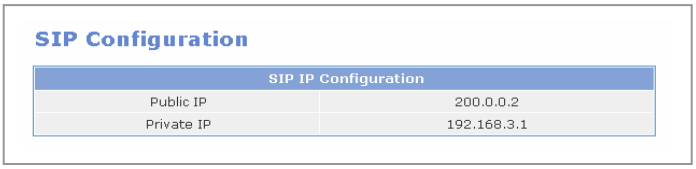
Обычно при защите внутренней сети с помощью сетевого экрана SIP ALG на основе NAT (SIP с поддержкой ALG) защищена от ата, что ограничевает возможность использования различных.ALG решает эту проблему. Таким образом, устройства SIP за сетевым экраном могут обмениваться информацией с внешними устройствами.

# Config (Настройка)

Пользователи могут настраивать среду SIP в меню [Config] (Настройка). Настройте следующие параметры и нажмите кнопку [Save] (Сохранить).

## SIP Configuration (Настройка SIP)

Отображение данных установки сетевого экрана.



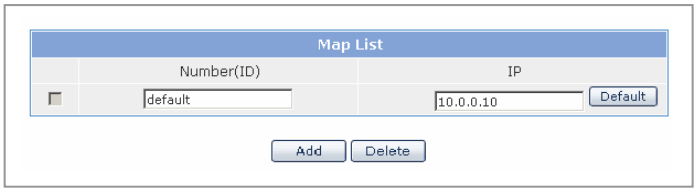

## Private (Личный)

Ввод внутреннего IP-адреса, защищенного сервером Data Server.


Нажмите кнопку [Add], чтобы автоматически добавить область с локальным IP-адресом за сетевым экраном.. Устройство SIP, в добавленной области с локальным IP-адресом, будет обслуживаться функцмей ALG(SIP ALG). Настройте данные маршрутизации устройств SIP напрямую или в разделе Internal IP(LAN, DMZ) Setting в меню [Firewall/Network] → [Management] → [Config] данного руководства.

## Map List (Список привязки)

Ввод данных об устройствах SIP внутри сетевого экрана.

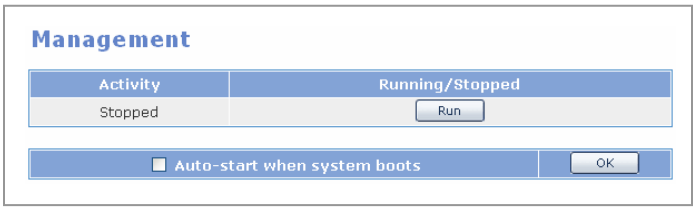



Если IP-адрес или номер телефона не существует в сообщении SIP, отправленном извне сетевого экрана, сообщение SIP преобразуется и

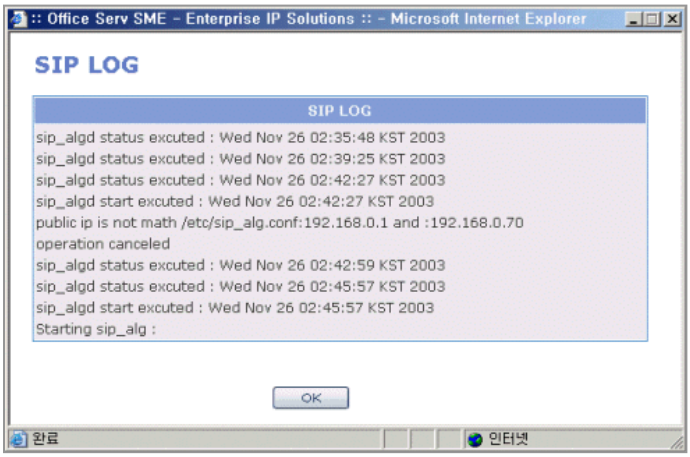
отправляется на IP-терминал, указанный в параметре ‘default’ (по умолчанию). Таким образом очень удобно указать все внутренние телефоны работающие с телефонным сервером, задав IP адрес телефонного сервера Call Server, как ‘default’.

## Management (Управление)

В меню [Management] (Управление) можно разрешить/запретить работу SIP ALG. Установите флажок ‘Auto Start’ (Автозапуск). После этого служба будет автоматически запускаться при перезагрузке системы.



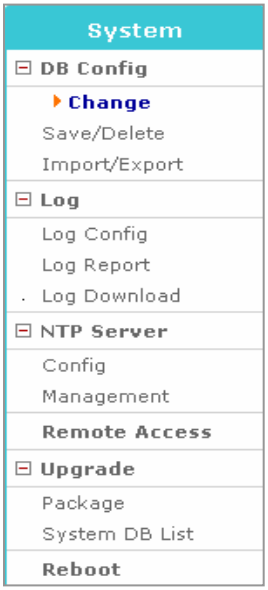

Нажмите кнопку [Run] (Запустить) для запуска SIP ALG:




Окно, изображенное выше, отображается при нормальной работе SIP ALG. При ошибке появляется сообщение ‘operation canceled’ (операция отменена).

# System Menu

Чтобы отобразить подменю SYSTEM в левой верхней части окне, выберите [SYSTEM].




| Меню | Подменю | Описание |
|---|---|---|
| DB Config (Настройка базы данных) | Change (Изменить) | Изменение текущей базы данных на другую или на базу данных по умолчанию. |
| | Save/Delete (Сохранить/Удалить) | Сохранение или удаление базы данных. |
| | Import/Export (Импорт/Экспорт) | Импорт базы данных для резервного копирования в компьютер или экспорт резервной копии базы данных |
| | Switch DB (База данных коммутатора) | Импорт базы данных коммутатора в компьютер или экспорт резервной копии коммутатора из компьютера. |
| Log (Запись) | Log Config (Настройка записи) | Настройка типов записей для сохранения. |
| | Log Search (Поиск записей) | Поиск записей по типу и времени создания. |
| | Log Download (Загрузка записи) | Загрузка всех файлов записей, сохраненных на локальный компьютер. |

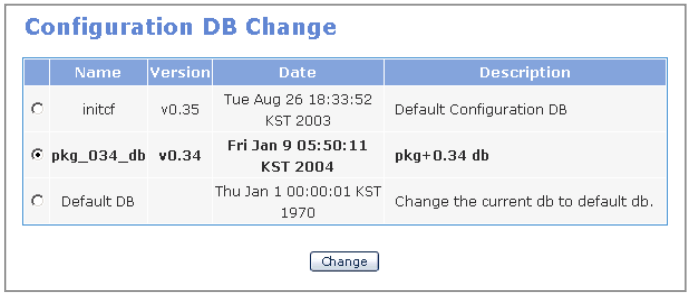
| | | |
|---|---|---|
| NTP Server (Сервер NTP) | Config (Настройка) | Настройка на работу с сервером синхронизации даты и времени. |
| | Management (Управление) | Поиск данных по дате и времени на зарегистрированном сервере и изменение системной даты и времени. |
| Set Date/Time (Настройка даты и времени) | - | Изменение системной даты и времени. |
| Remote Access (Удаленный доступ) | - | Запуск служб Telnet, FTP и SSH для подключения к плате WIM из удаленной области. |
| Upgrade (Обновление) | Package (Пакет) | Обновление пакета DB, Kernel, Ramdisk и Application. |
| | System DB List (Список системных баз данных) | Обновление базы данных до последней версии. |
| Reboot (Перезагрузка) | - | Перезагрузка системы |

# DB Config (Настройка базы данных)

Пользователи могут сохранять и удалять базы данных, а также изменять базу данных на другую в меню [DB Config] (Настройка базы данных).

## Change (Изменить)

Пользователи могут изменять рабочую базу данных на другую или на базу данных по умолчанию с помощью меню [Change] (Изменить). В приведенном ниже рисунке рабочая база данных отображается шрифтом с полужирным начертанием. Выберите базу данных, которую требуется изменить, и нажмите кнопку [Change] (Изменить). После изменения базы данных происходит перезагрузка системы.

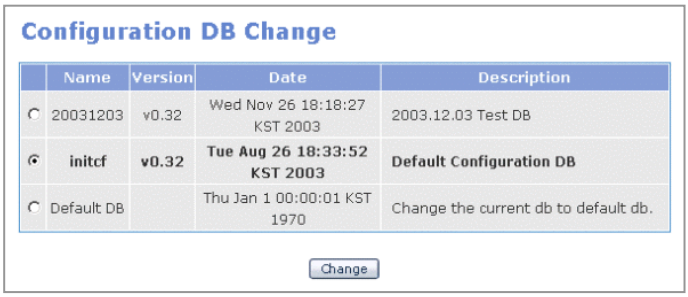



CAUTION

**Изменение базы данных**

Базы данных модулей WIM и LIM встроены в сервер OfficeServ 7200 Data Server. При изменении базы данных происходит перезагрузка системы.

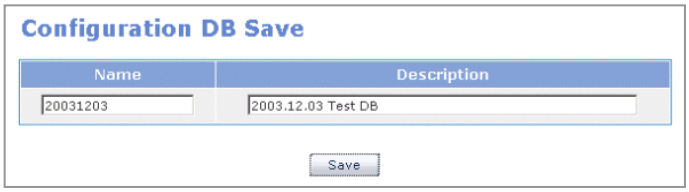
Выберите ‘Default DB’ (База данных по умолчанию) и нажмите кнопку [Change] (Изменить). После этого, выполняется инициализация исходной базы данных, как показано ниже. initcf является исходной базой данных. При выборе значения Default DB (База данных по умолчанию) выполняется инициализация системы. Таким образом, рекомендуется выполнять подключение к диспетчеру Интернет-компонентов через порт LAN (10.0.0.1) внутренней сети.



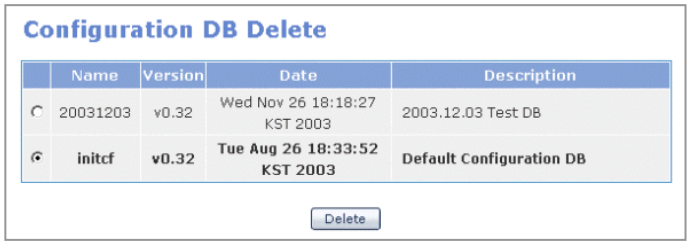
## Save/Delete (Сохранить/Удалить)

Пользователи могут изменять имя рабочей базы данных или удалять базу данных, сохраненную в меню [Save/Delete] (Сохранение/удаление).

Введите имя и описание базы данных, а затем нажмите кнопку [Save] (Сохранить), чтобы сохранить базу данных. После этого сохраненная база данных регистрируется в окне <Configuration DB Delete> (Настройка удаления базы данных).




Выберите базу данных, которую требуется удалить, и нажмите кнопку [Delete] (Удалить). Рабочая база данных отображается шрифтом с полужирным начертанием. Ее удалить невозможно.

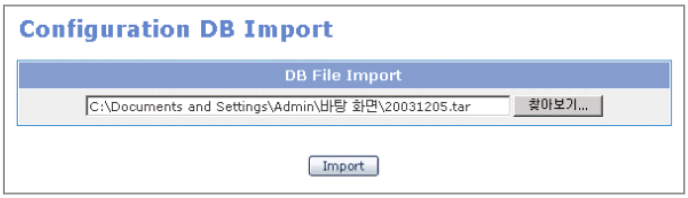


# Import/Export (Импорт/Экспорт)

Через меню [Import/Export] (Импорт/экспорт) пользователи могут импортировать базу данных в ркомпьютер для создания резервной копии в или экспортировать резервную копию из компьютера.

## Import (Импорт)

Для импорта базы данных необходимо, нажав кнопку [Browse] (Обзор), найти файл базы в компьютере, а затем нажать кнопку [Import] (Импорт). После этого база данных регистрируется в окне <Configuration DB Import> (Настройка импорта базы данных).



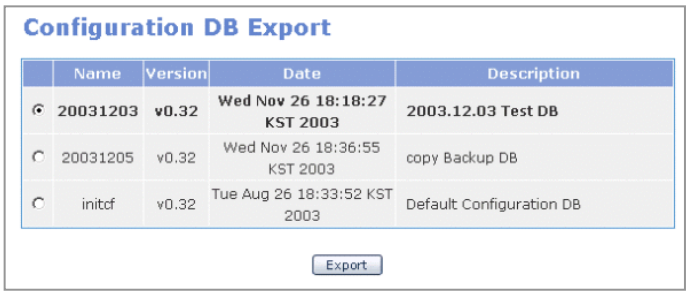

CHECK

**При обнаружении ошибок во время работы функции [Import] (Импорт) проверьте следующие условия.**

- После ввода пути к файлу он не закрывается
- Нажата кнопка [Import] (Импорт) без ввода данных в соответствующие поля.
- Имеется базы данных с одинаковым именем
- Изменено имя файла в существующей базе данных
- имя файла содержит пробелы

## Export

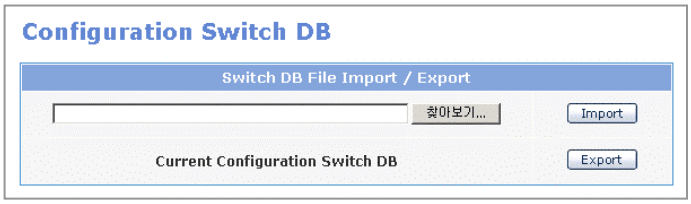
The DB set is displayed with bold letters. Select the target DB and click the [Export] button to save DB to the selected area of a terminal.




Для отправки базы данных в компьютер нажмите кнопку [Save] (Сохранить). После чего распакуйте базу данных с помощью архиватора.

## Switch DB (База данных коммутатора)

Используя меню [Switch DB] (База данных коммутатора) пользователи могут импортировать базу данных коммутатора в компьютер или экспортировать базу данных из компьютера в коммутатор.



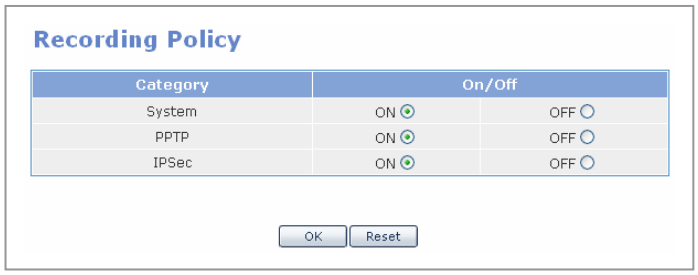

Укажите расположение файла базы данных коммутатора для импорта базы данных из компьютера или, нажав кнопку [Brows…] (Обзор), выберите необходимый файл и нажмите кнопку [Import] (Импорт). Для экспорта базы данных коммутатора в терминал нажмите кнопку [Export] (Экспорт).

# Log (Журнал событий)

В меню[Log] пользователи могут настроить и просмотреть службу регистрации событий системы.

## Log Config (Настройка журнала)

Настройте параметры создания записей в меню [Log Config] (Настройка записи). Для создания записей выберите значение ‘On’ (Вкл), или выберите ‘Off’ (Выкл), если создавать записи необязательно.

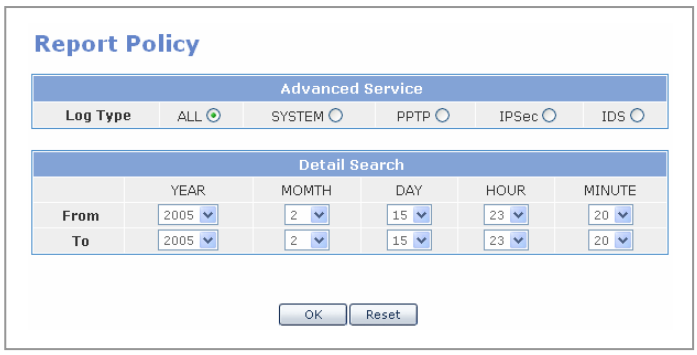



Имеются следующие типы записей.

- Системная запись: запись, относящаяся к системе
- Запись PPTP: записи, связанные с протоколом PPTP VPN
- Запись IPSec: записи, связанные с протоколом IPSec VPN

## Log Report (Отчет о записи)

Для поиска записей по типу и времени создания используется меню [Log Report] (Отчет о записи).

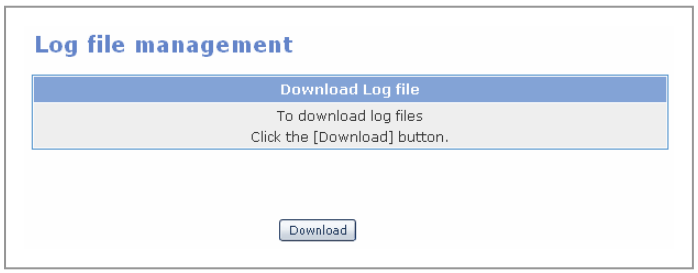


- Log Type (Тип записи): поиск записей по выбранному типу.
  - ALL (Все): поиск всех записей
  - SYSTEM (Системные): поиск всех записей, за исключением PPTP, IPSec и IDS
  - PPTP: поиск записей, связанных с протоколом PPTP VPN
  - IPSec: поиск записей, связанных с протоколом IPSec VPN
  - IDS: поиск записей протокола IDS
- Подробный поиск: поиск записей по времени создания.

Выберите тип и время регистрации записей и нажмите кнопку [OK] для отображения окна, изображенного ниже.

## Log Download (Загрузка журнала)

Пользователи могут выполнять загрузку файлов записей на локальный компьютер в меню [Log Download] (Загрузка журнала).

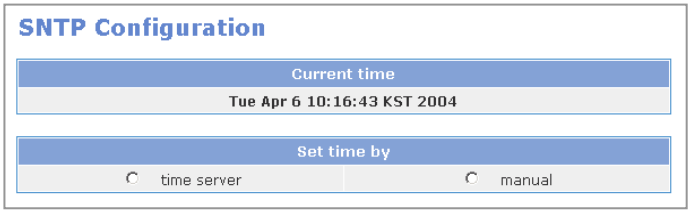



# NTP Server (Сервер NTP)

Пользователи могут настраивать систему на синхронизацию даты и времени от сетевого сервера времени [NTP Server] (Сервер NTP).

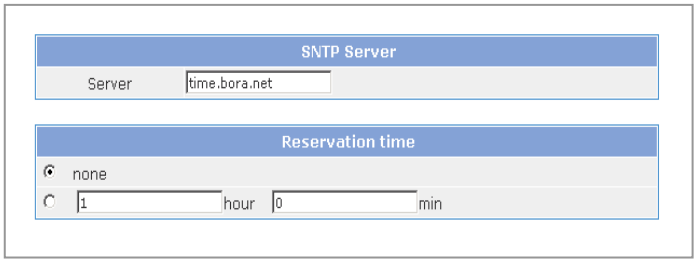
## Config (Настройка)

Для регистрации сервера, с которого будет импортироваться информация о дате и времени, выберите [NTP Server] (Сервер NTP)→ [Config] (Настройка), или введите информацию вручную.



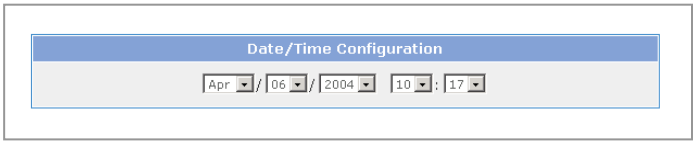
## SNTP server (Сервер SNTP)

Выберите параметр SNTP server (Сервер SNTP). Отобразится окно, изображенное ниже. Зарегистрируйте сервер, с которого будет импортироваться информация о дате и времени, и настройте цикл получения информации. Затем нажмите [OK].




## manual (вручную)

Выберите параметр manual (вручную). Отобразится окно, изображенное ниже. Вручную введите дату и время, а затем нажмите кнопку [OK




NOTE

**Информация о системном времени**

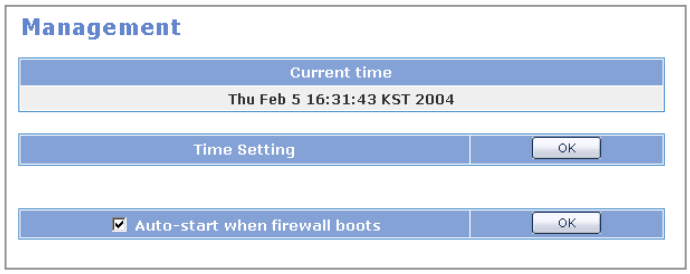
Поскольку в системе сервера Data Server встроенные часы реального времени (RTC) отсутствуют, заданное системное время не сохраняется после перезагрузки системы, а сохраняется каждый час. Поэтому после перезагрузки системы время, установленное ранее, может измениться.

## Time zone (Часовой пояс)


Установите часовой пояс для требуемой области (название города). После ввода значения нажмите кнопку [OK].

## Management (Управление)

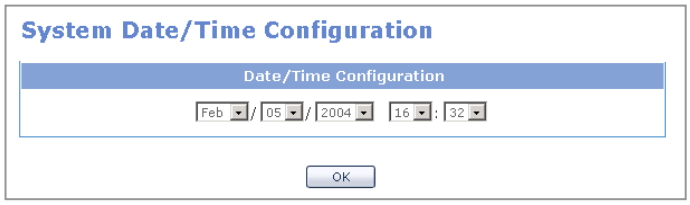
Выберите [NTP Server] (Сервер NTP) → [Management] (Управление) и установите время. Затем установите дату и время, полученные с сервера, заданного в окне <NTP Server Configuration> (Настройка сервера NTP).




Если установлен флажок ‘Auto Start’ (Автостарт), служба будет автоматически запускаться при перезагрузке системы.

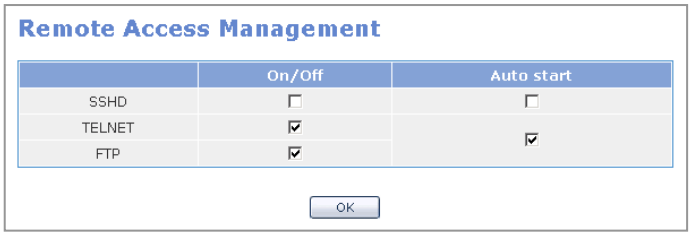
# Set Data/Time

Пользователи могут настраивать системные дату и время с использованием меню [Set Data/Time] (Настройка даты и времени). Если сервер NPT использовать невозможно, пользователь может изменить время вручную. После настройки даты и времени нажмите кнопку [OK].



# Remote Access (Удаленный доступ)

Если в меню [Remote Access] (Удаленный доступ) выполняются службы SSH, Telnet и FTP, пользователи могут получать доступ к плате WIM с удаленного компьютера. Кроме того, если установлен флажок ‘Auto Start’ (Автостарт), служба будет автоматически запускаться при перезагрузке системы.



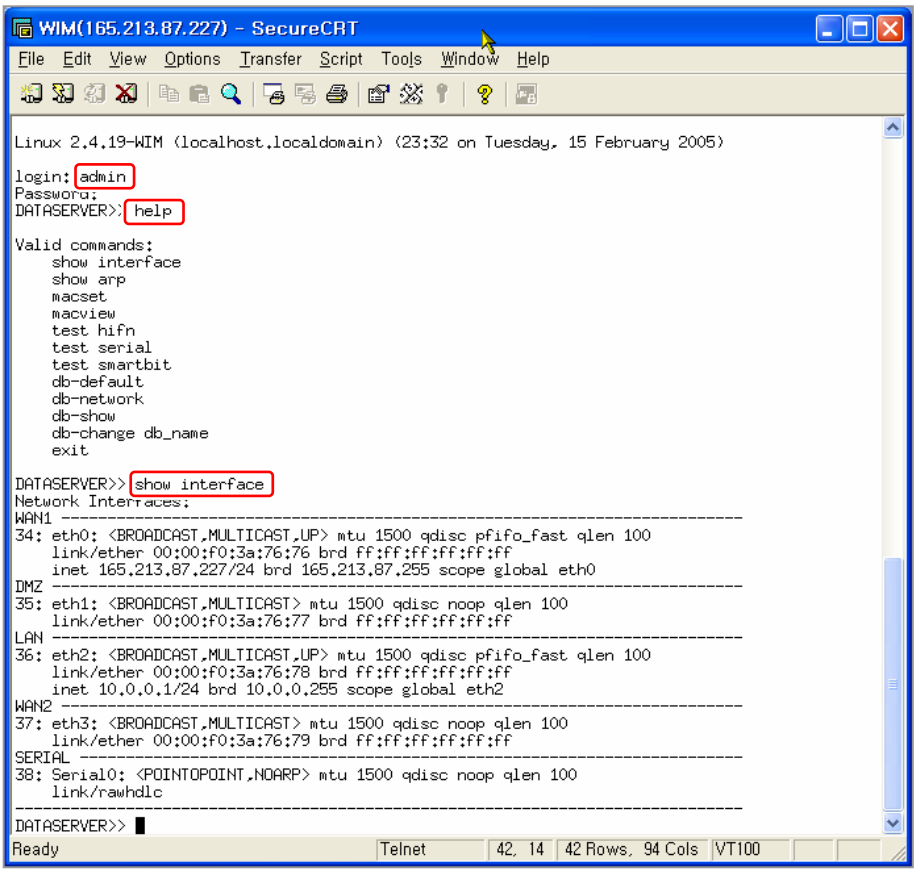

NOTE

**Назначенный активный канал параметра ‘Response Status’ (Состояние ответа)**

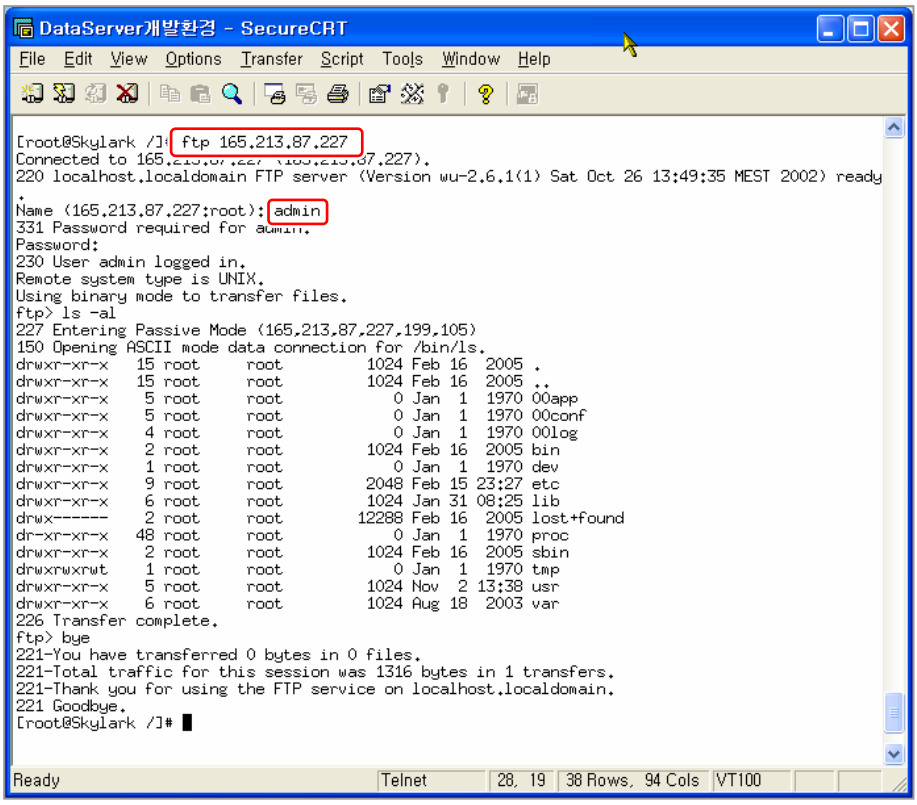
- Доступ к SSH можно получить как из внутренней, так и из внешней сети.
- Если сетевой экран включен, доступ к системе из внешней сети через Telnet/FTP невозможен. Для установки соединения отключите функцию сетевого экрана для порта соответствующей службы. Для этого выберите [Firewall/Network] (Сетевой экран/сеть) → [Remote Accept] (Разрешение удаленного доступа).
- Имя пользователя администратора по умолчанию - ‘admin’, пароль ‘admin’.

Следующие способы используются при установке соединений с службами Telnet, FTP и SSH модуля WAN в локальных и внешних сетях:

## Подключение к Telnet



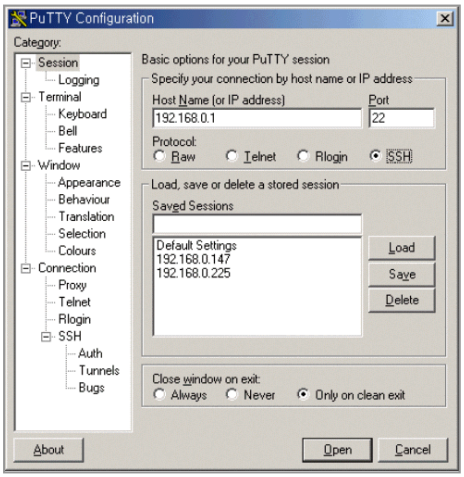
## Подключение к FTP



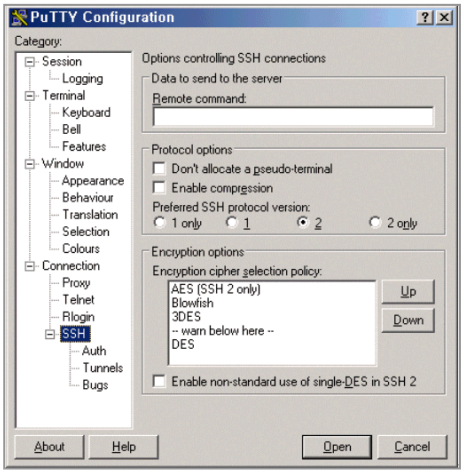
## Подключение к SSH

Программа соединения с SSH использует программу Putty. Для установки программы Putty и соединение SSH выполните следующую процедуру.

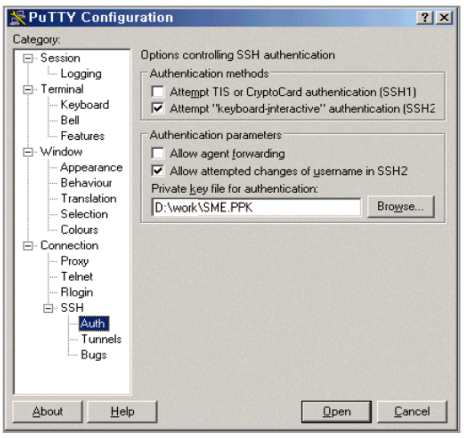
1. Пакет программ Putty можно загрузить в Интернете по следующему адресу:
   ‘http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html’
2. Если выполняется файл ‘putty.exe’, откроется окно, изображенное ниже. В поле Host Name (Имя хоста) введите адрес сетевого экрана, а в качестве протокола выберите ‘SSH’.




3. После этого откроется окно, изображенное ниже. Для параметра Preferred SSH protocol version (Предпочтительная версия протокола SSH) установите значение ‘2’.



*4.* В списке ‘SSH’ выберите элемент ‘Auth’ (Проверка подлинности) для отображения окна, изображенного ниже. Нажмите кнопку [Browse] (Обзор), расположенную рядом с полем ‘Private key file for authentication’ (Файл закрытого ключа для проверки подлинности), для выбора файла закрытого ключа.




CAUTION

**Закрытый ключ**

Закрытый ключ поставляется в комплекте. Закрытый ключ позволяет получать доступ к SSH из внешней сети. Поэтому пользоваться этим ключ должен только надежный администратор.

*5.* Нажмите кнопку [Open] (Открыть) в окне <PuTTY Configuration> (Настройка PuTTY) для установки соединения, как показано ниже. Введите пароль, используемый при шифровании закрытого ключа.

```
Login as: root
Authenticating with public key “rsa-key-20040224”
Passphrase for key “rsa-key-20040224”:
DATASERVER>>
```

# Upgrade (Обновление)

С помощью меню [Upgrade] (Обновление) пользователи могут обновлять Kernel, Ramdisk, Application и пакет базы данных.

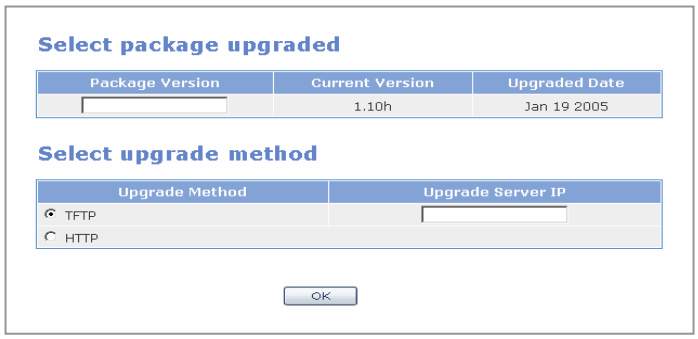
NOTE

**'ds-pkg-vx.xx.tar.gz' File**

Этот файл предназначен для обновления системы и используется в меню [System] (Система) → [Upgrade] (Обновление) → [Package] (Пакет). При этом обновляется база данных системы, хранящаяся в этом файле.

## Пакет

В меню [Upgrade] (Обновление) → [Package] (Пакет) выберите версию пакета и метод обновления. Методы обновления подразделяются по типам на TFTP и HTTP.




NOTE

**Настройка ADSL/VDSL**

Максимальная скорость выгрузки и загрузки зависит от возможности модема ADSL/VDSL.

### Обновление по протоколу TFTP

Пользователи могут обновлять систему OfficeServ 7200 с помощью файла обновления, размещенного на сервере TFTP.
После ввода версии обновляемого пакета в поле 'Package Version' (Версия пакета) и выбора адреса сервера 'TFTP' нажмите кнопку [OK].
Если обновление завершено успешно, перезагрузите систему OfficeServ 7200.
Если сервер обновления не найден или во время обновления обнаружены ошибки, выдается сигнальное сообщение.

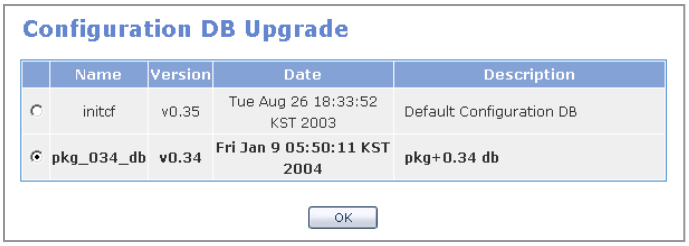
### Upgrade Through HTTP

Пользователи могут обновлять систему OfficeServ 7200 путем загрузки файла обновления с компьютера, на котором расположен файл пакета для обновления.
В поле ‘Package Version’ (Версия пакета) введите версию обновляемого пакета, выберите ‘HTTP’ и нажмите кнопку [OK] для открытия окна, изображенного ниже.


Выберите файл, который необходимо загрузить с компьютера, и нажмите кнопку [OK] для начала обновления. После успешного завершения обновления будет выполнена перезагрузка системы OfficeServ 7200.

## DB File (Файл базы данных)

Обновите базу данных до самой последней версии с помощью меню [Upgrade] (Обновление) → [DB File] (Файл базы данных).




Выберите базу данных, которую необходимо обновить, и нажмите кнопку [OK]. При успешном завершении обновления в области Version (Версия) отобразится последняя версия. Однако если обновление завершится неудачно, отобразится сигнальное сообщение.
.

# Reboot (Перезагрузка)

Пользователи могут перезагрузить систему с помощью меню [Reboot] (Перезагрузка).


При нажатии кнопки [OK] будет завершена работа всех служб и система перезагрузится.
После этого, поскольку веб-экран сервера Data Server не работает до тех пор, пока не будут запущены службы и сеть, закройте веб-экран и повторно подключитесь к системе.

# ПРИЛОЖЕНИЕ A. Настройка VPN в Windows XP/2000

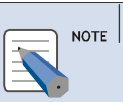
Если в меню [VPN] сервера OfficeServ 7200 Data Server необходимо настроить IPSec и PPTP, необходимо также настроить клиента VPN в MS Windows. В данном разделе описан процесс настройки VPN в Windows XP. Настройки для Windows 2000 аналогичны настройкам Windows XP.

При наличии следующей сетевой среды необходимо выполнить указанные ниже процедуры настройки IPSec и PPTP.

- Внешний IP-адрес OfficeServ: 211.217.127.40
- Внутренний IP-адрес OfficeServ: 192.168.0.1
- Внутренняя IP-адрессация сети: 192.168.0.0
- Внутренняя маска сети: 255.255.255.0
- IP-адрес клиентского компьютера с Windows XP/2000: 211.217.127.73

## Настройка IPSec

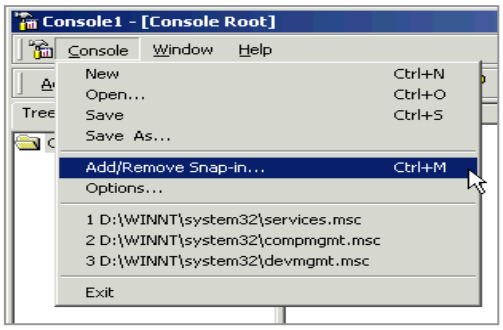
IPSec и различные алгоритмы шифрования/проверки подлинности можно доустановить с установочного компакт-диска с помощью функции обновления Windows в Windows XP/2000. Кроме того, клиент LAN к VPN можно настроить с помощью IPSec.



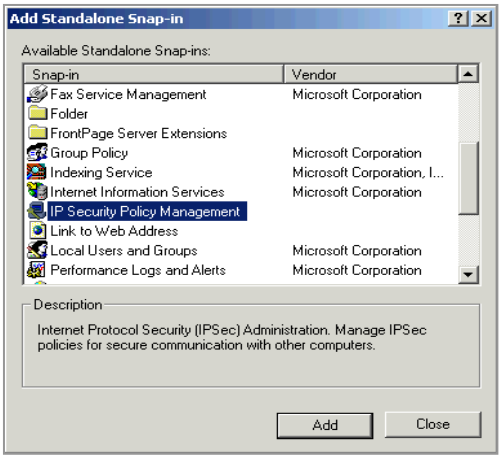

**Настройка IPSec в Windows XP/2000**

- Windows XP: выполните файл ‘IPSeccmd.exe’, расположенный в папке Support/Tools setup на установочном компакт-диске Windows XP.
- Windows 2000: загрузите и установите пакет обновления 2 для Windows 2000 с веб-узла обновления Windows. Можно также выполнить файл ‘IPSecpol.exe’, расположенный в папке Support/Tools setup на установочном компакт-диске Windows 2000.

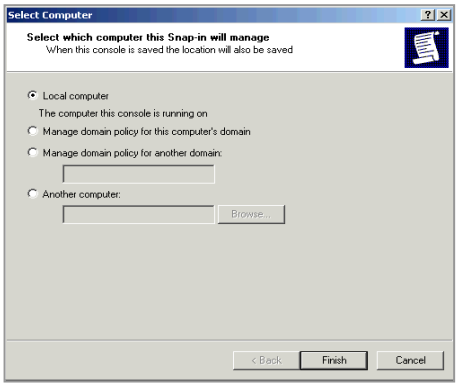
1. В панели задач выберите [Пуск] → [Выполнить] и введите ‘mmc’ для открытия окна, изображенного ниже. В окне консоли выберите [Файл] → [Добавить или удалить оснастку…].



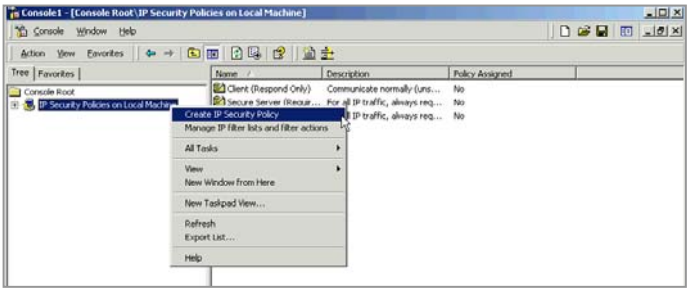

2. В диалоговом окне <Добавить или удалить оснастку…> выберите [Добавить] для отображения следующего окна. В меню "Добавить или удалить оснастку..." выберите "Управление политикой безопасности IP" и нажмите [Добавить].



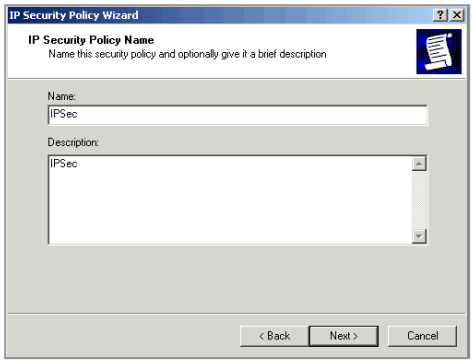
3. В окне, изображенном ниже, выберите "Локальный компьютер(T)" и нажмите кнопку [Готово].



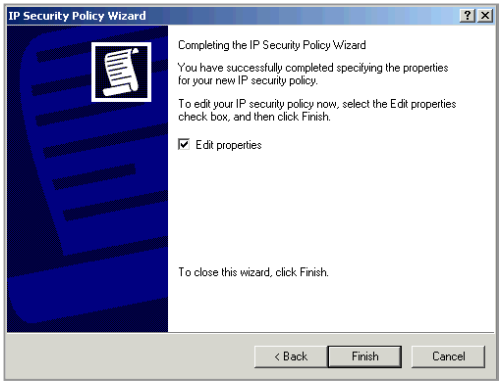

4. Перейдите в окно <Консоль>. После этого в корне консоли будет создан элемент "Политики IP-безопасности на локальном компьютере". Выберите этот элемент, щелкните его правой кнопкой мыши и выберите пункт [Создать политику безопасности IP].



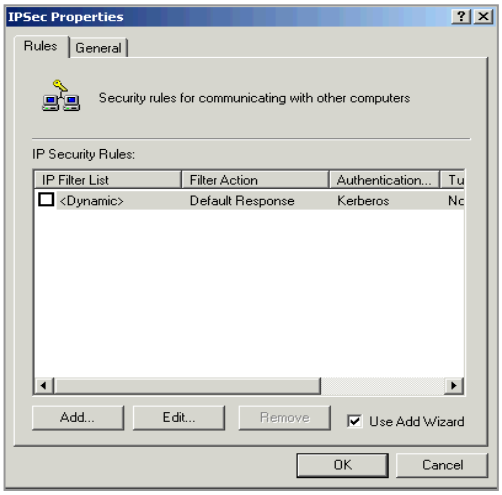

5. В окне <Мастер политики IP-безопасности> нажмите кнопку [Далее], после чего отобразится окно, изображенное ниже. Введите имя и описание, а затем нажмите кнопку [Далее].



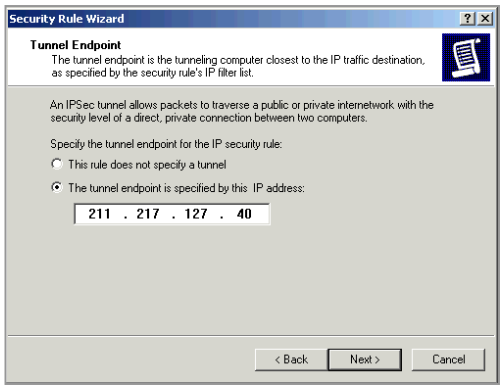
6. Если установлен флажок "Использовать правило по умолчанию(R)", снимите его и нажмите кнопку [Добавить] для отображения окна, изображенного ниже. Выберите параметр "Изменить свойства(P)" и нажмите кнопку [Готово].



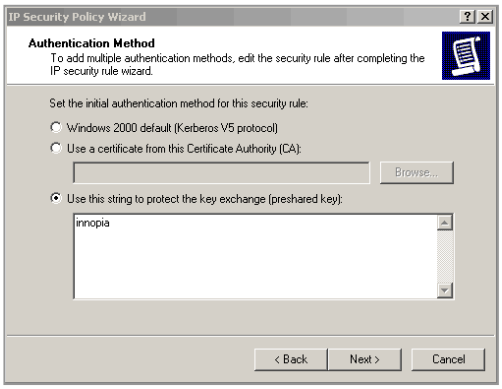

7. При открытии окна <XP_OPSec Registration Information> (Регистрационная информация XP_OPSec) будут отображены созданные элементы. Если установлен флажок соответствующего элемента, снимите его и нажмите кнопку [Добавить].



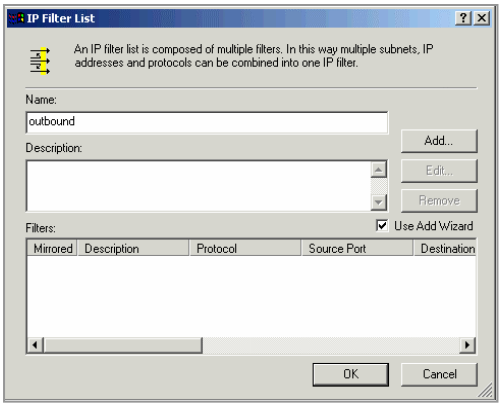
*8.* В окне <Мастер правил безопасности> нажмите кнопку [Добавить], после чего отобразится окно, изображенное ниже. Выберите параметр "Конечная точка туннеля указана данным IP-адресом" и введите внешний IP-адрес сетевого экрана (211.217.127.40). Нажмите кнопку [Далее].



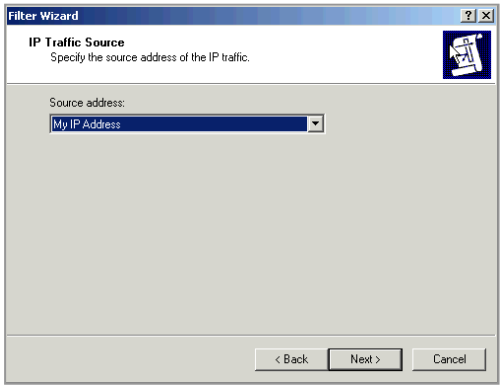

*9.* В окне <Тип сети> выберите локальную сеть (LAN) и нажмите кнопку [Добавить], после чего отобразится окно, изображенное ниже. Выберите параметр "Использовать данную строку для защиты обмена ключами" и введите пароль, зарегистрированный для сетевого экрана. Нажмите кнопку [Далее].



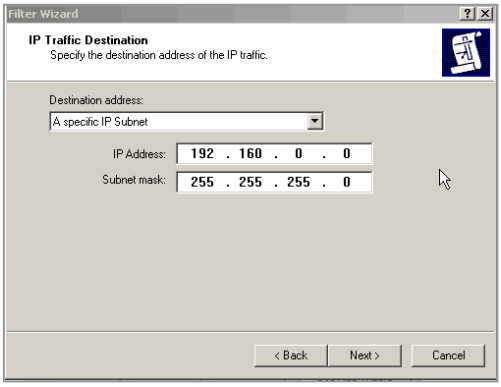
*10.* В окне <Мастер правил безопасности> нажмите кнопку [Добавить], после чего отобразится окно, изображенное ниже. В поле "Имя" введите ‘outbound’ и нажмите кнопку [Добавить].



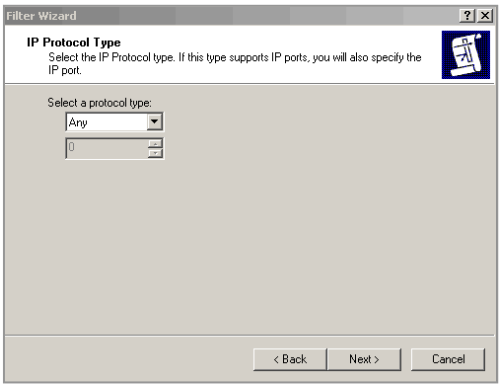

*11.* В окне <Мастер IP-фильтров> нажмите кнопку [Добавить], после чего отобразится окно, изображенное ниже. В поле "Адрес источника" выберите "Мой IP-адрес" и нажмите кнопку [Далее].



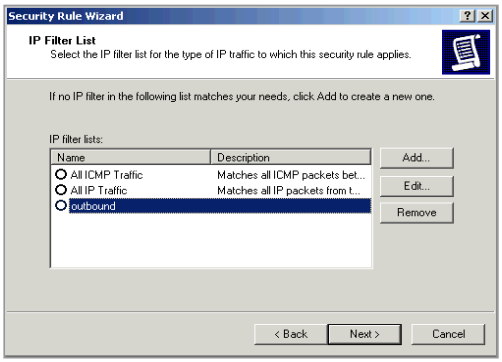
*12.* В качестве адреса назначения укажите "Определенная подсеть IP" и введите внутренний адрес сети (192.168.0.0), а также маску подсети (255.255.255.0). Нажмите кнопку [Далее].




*13.* В поле типа протокола выберите "Все" и нажмите кнопку [Далее]. В окне <Мастер IP-фильтров> установите флажок "Изменить свойства(P)" и нажмите кнопку [Готово].

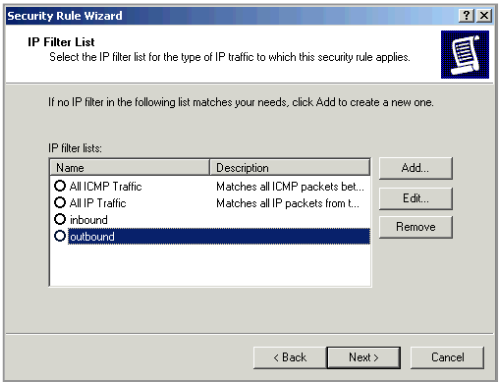


14. Нажмите кнопку [OK]. После этого будет создан элемент outbound. Нажмите кнопку [Добавить] для создания элемента inbound.

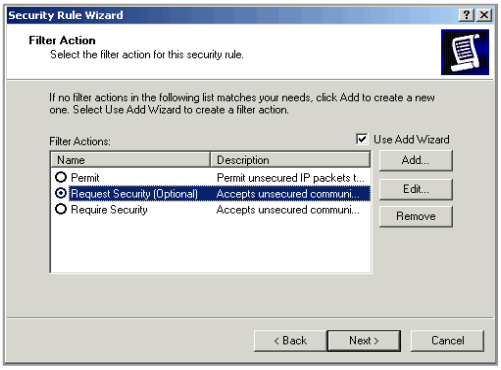



15. В поле "Имя" введите ‘inbound’ и нажмите кнопку [Добавить], как в шаге **10**.
Для этого можно также выполнить действия, указанные в шагах с **11** по **13**.

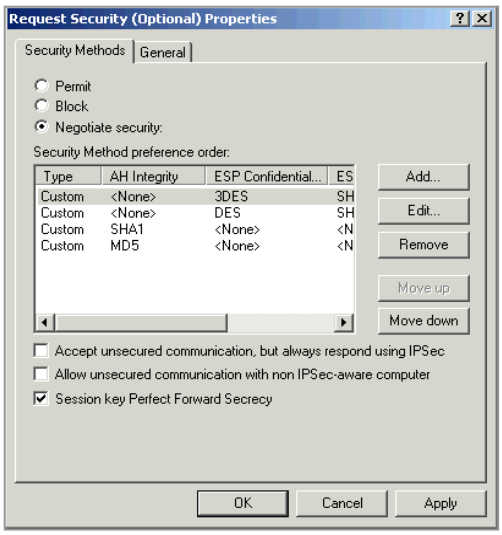
16. Нажмите кнопку [Добавить], после чего отобразится окно, изображенное ниже. Затем выберите элемент ‘outbound’ и нажмите кнопку [Далее].



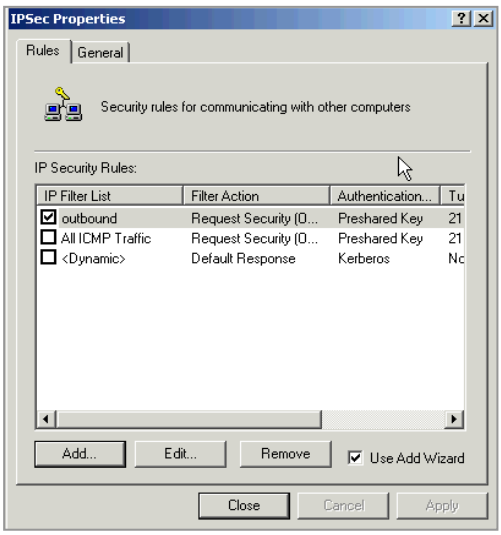
*17.* Выберите элемент "Запрос безопасности [Возможный]" и нажмите кнопку [Изменить].



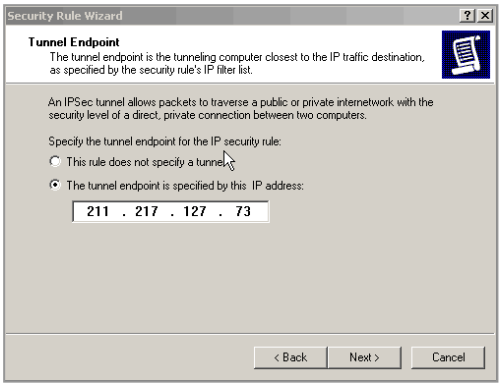

*18.* Выберите параметр "Согласовать безопасность". В области "Методы безопасности в порядке предпочтения" выберите "Целостность AH(Нет), Конфиденциальный ESP(3DES), Целостность ESP(MD5)". Нажмите кнопку [Вверх] для перемещения соответствующего элемента на первый ряд. Установите флажок "Сеансовые циклы безопасной пересылки (PFS)" и нажмите кнопку [OK].



***19.*** Установите флажок "Изменить свойства" и нажмите кнопку [Готово] для отображения окна создания элемента outbound. Нажмите кнопку [Добавить] для создания элемента inbound.



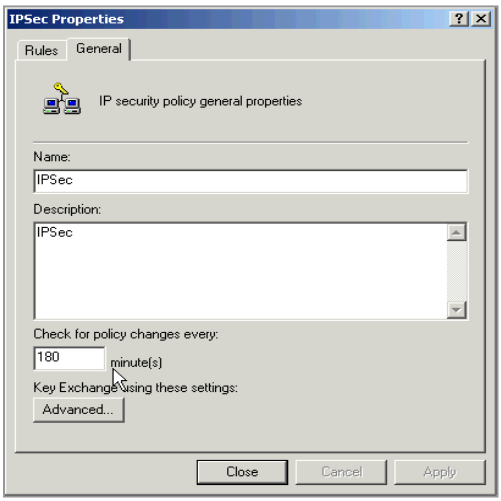

***20.*** В окне <Мастер правил безопасности> нажмите кнопку [Далее], после чего отобразится окно, изображенное ниже. Выберите параметр "Конечная точка туннеля указана данным IP-адресом" и введите IP-адрес клиентского компьютера. Нажмите кнопку [Далее].



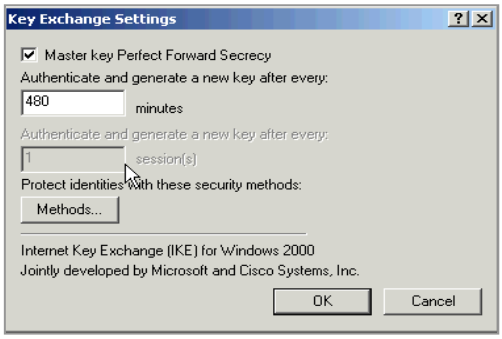

***21.*** В окне <Тип сети> выберите локальную сеть (LAN) и нажмите кнопку [Далее]. Выберите параметр "Использовать данную строку для защиты обмена ключами" и введите пароль, зарегистрированный для сетевого экрана. Нажмите кнопку [Далее]. (См. шаг **9.**)

*22.* В окне шага **16** выберите элемент inbound и нажмите кнопку [Далее]. Выполните действия шагов **17** и **18**.

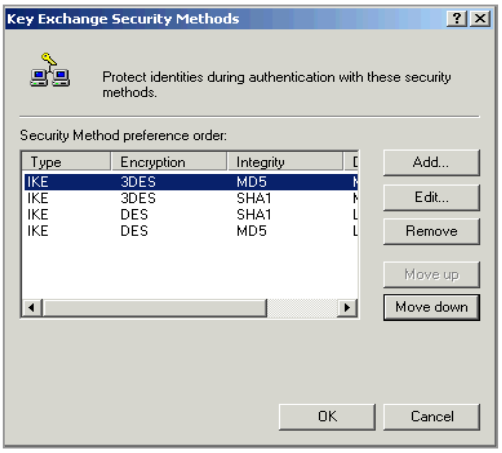
*23.* Установите флажок "Изменить свойства" и нажмите кнопку [Готово] для отображения окна, изображенного ниже. Перейдите на вкладку [Общие] и выберите [Настройка].



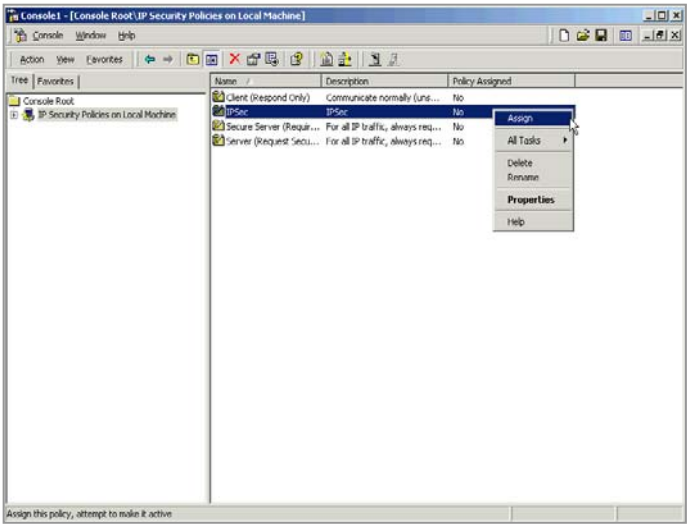

*24.* Установите флажок "Основной ключ безопасной пересылки (PFS)" и нажмите кнопку [Методы…] в окне, изображенном ниже.



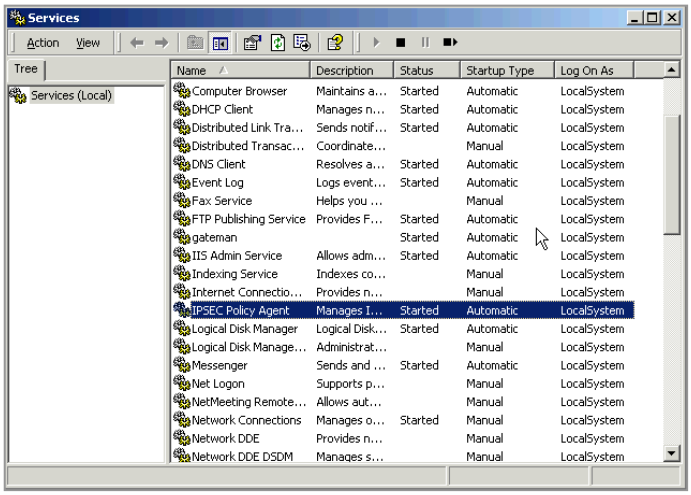
**25.** В приведенном ниже окне выберите "Шифрование (3DES), Целостность (MD5), Диффи-Хелмана (Med)" и нажмите кнопку [Вверх] для перемещения соответствующего элемента на первый ряд. Нажмите кнопку [OK].



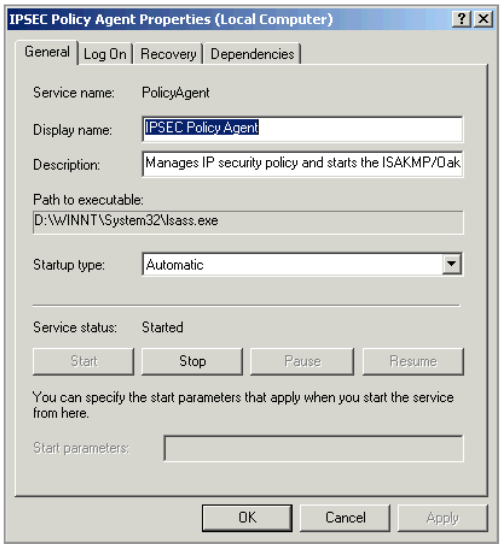

**26.** В окне <Консоль> выберите элемент "Политики IP-безопасности на локальном компьютере". В правом углу окна выберите только что созданный элемент, щелкните его правой кнопкой мыши и выберите пункт [Назначить]. После этого значение параметра назначения политики изменится на "Да".



*27.* В панели задач Window нажмите [Пуск] → [Программы] → [Администрирование] → [Службы] и дважды щелкните элемент "Службы IPSEC".




*28.* В приведенном ниже окне нажмите кнопку [Стоп], затем [Пуск] для перезапуска службы.



*29.* Проверьте состояние соединения для внутреннего IP-адреса сетевого экрана, введя в командной строке команду ping. При получении ответов как в окне, приведенном ниже, IP-адрес подключен правильно.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Negotiating IP Security.
Reply from 192.168.0.1: bytes=32 time=5 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=6 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4 ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 <25% loss>.
Approximate round trip times in milli-seconds:
    Minimum = 4 ms, Maximum = 6 ms, Average = 5 ms
```

# Настройка PPTP

Пользователи могут настраивать VPN с PPTP с помощью установочного компакт-диска, а также с помощью функции обновления Windows в Windows XP/2000.

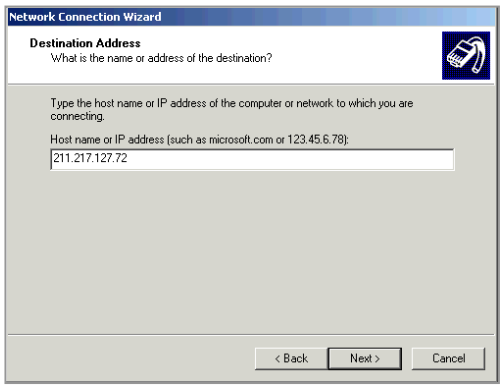
CAUTION

**Настройка PPTP в Windows XP/2000**

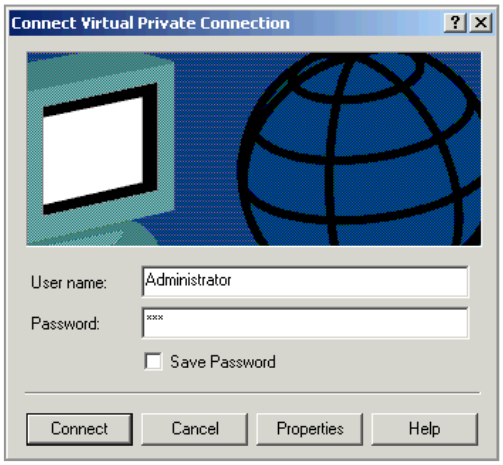
В Windows XP/2000 пользователь может использовать клиент DHCP. При подключении клиента VPN PPTP во время работы клиента DHCP будут обнаружены ошибки. Для предотвращения ошибок отключите клиент DHCP. Для этого выберите [Пуск] → [Программы] → [Администрирование] → [Службы] и выберите установленный клиент PPTP.

*1.* Дважды щелкните значок [Мое сетевое окружение] на рабочем столе Windows и выберите [Свойства]. В правом верхнем углу экрана нажмите [Создать подключение], после чего отобразится окно, изображенное ниже. Нажмите кнопку [Далее].

2. Выберите вариант "Подключить к сети на рабочем месте" и нажмите кнопку [Далее], после чего выберите "Виртуальное частное подключение". Нажмите кнопку [Далее] для отображения окна, изображенного ниже. Введите имя хоста или IP-адрес и нажмите кнопку [Далее]. Введите внешний IP-адрес сетевого экрана и нажмите кнопку [Готово].




3. В панели задач Windows выберите [Пуск] → [Настройки] → [Сетевые подключения] и выберите имя хоста, введенное в окне выше, для отображения окна входа в систему, изображенного ниже. Введите имя пользователя и пароль для проверки правильности подключения VPN в клиенте. Для проверки состояния соединения можно также использовать команду ping (см. **шаг 29** раздела "Настройка IPSec").




После проверки состояния соединения VPN убедитесь, что можно получить доступ к общей папке внутреннего компьютера, подключенного к VPN.

# СПИСОК СОКРАЩЕНИЙ

## A

| | |
|---|---|
| ALG | Application Level Gateway |
| AH | Authentication Header |
| ARP | Address Resolution Protocol |

## C

| | |
|---|---|
| CTI | Computer Telephony Integration |

## D

| | |
|---|---|
| DHCP | Dynamic Host Configuration Protocol |
| DNAT | Destination Network Address Translation |
| DNS | Domain Name Server |
| DRR | Deficit Round Robin |

## E

| | |
|---|---|
| ESP | Encapsulating Security Payload |

## H

| | |
|---|---|
| HDLC | High-level Data Link Control |

# I

| | |
|---|---|
| IDS | Intrusion Detection System |
| IGMP | Internet Group Management Protocol |
| IKE | Internet Key Exchange |
| IPSec | IP Security Protocol |

# L

| | |
|---|---|
| LAN | Local Area Network |

# N

| | |
|---|---|
| NAT | Network Address Translation |
| NMS | Network Management System |

# P

| | |
|---|---|
| PPP | Point-to-Point Protocol |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PPTP | Point to Point Tunneling Protocol |
| PVC | Permanent Virtual Circuit |
| PVID | Port VLAN Identification |

# S

| | |
|---|---|
| STP | Spanning Tree Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SNAT | Source Network Address Translation |
| SNMP | Simple Network Management Protocol |

# V

| | |
|---|---|
| VLAN | Virtual Local Area Network |

## OfficeServ 7200

# Руководство пользователя сервера Data Server



SAMSUNG ELECTRONICS