ZYXEL
Your Networking Ally

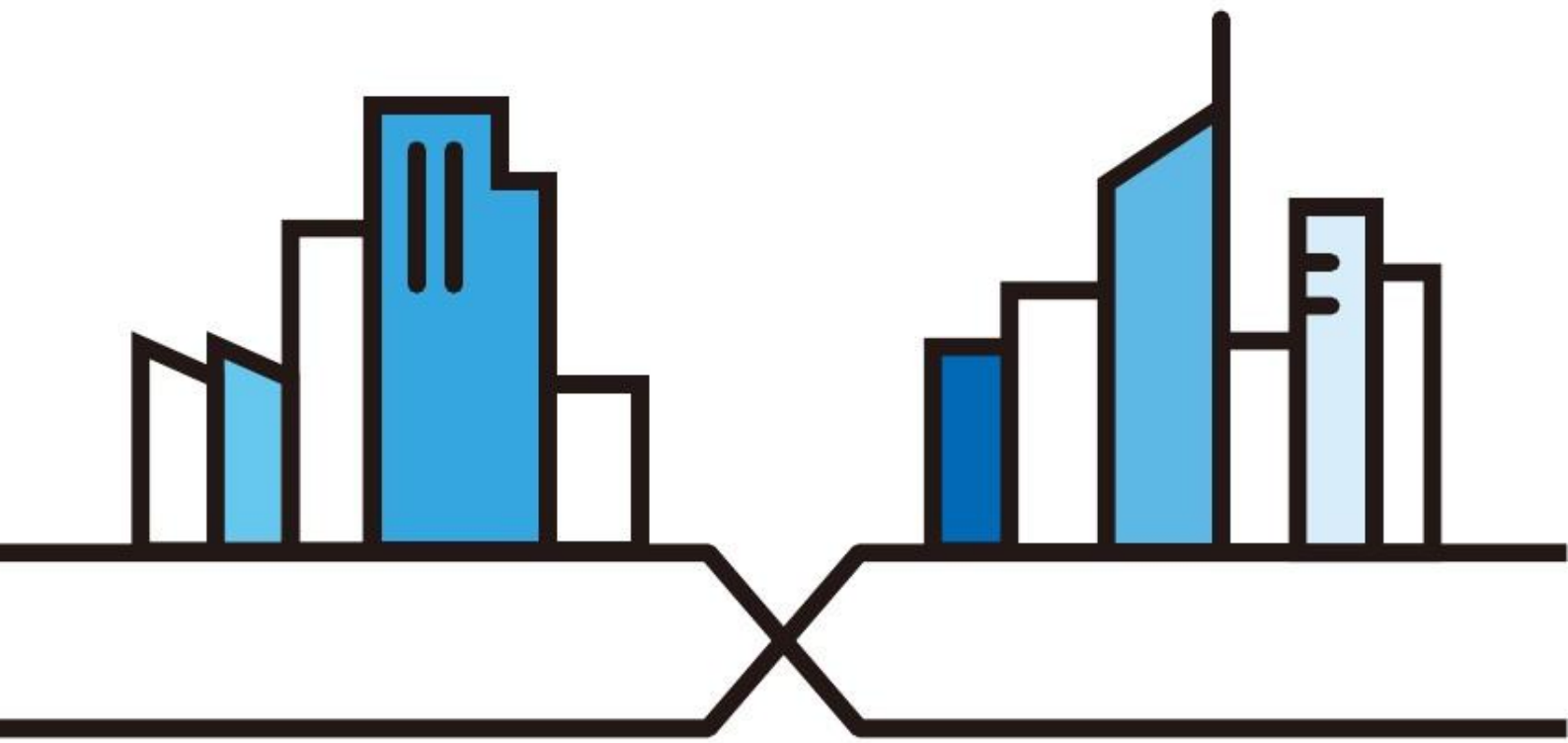
Руководство пользователя

NBG6615

Двухдиапазонный гигабитный беспроводной маршрутизатор AC1200 MU-MIMO

Login по умолчанию	
Login URL	http://192.168.212.1 (режим маршрутизатора) http://192.168.1.2 (режим точки доступа)
User Name	admin
Password	1234

Version 1.0 Edition 2, 08/2019



ВАЖНАЯ ИНФОРМАЦИЯ!

ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ПЕРЕД ПЕРВЫМ ИСПОЛЬЗОВАНИЕМ.

СОХРАНИТЕ ЭТО РУКОВОДСТВО – ОНО МОЖЕТ ВАМ ПОНАДОБИТЬСЯ В БУДУЩЕМ!

Это руководство пользователя для нескольких моделей серии продуктов и некоторые модели могут не поддерживать часть описанных в нем функций прошивки. Скриншоты и изображения для вашего продукта могут несколько отличаться от приведенных в этом руководстве из-за использования в продукте другой версии прошивки или операционной версии компьютера.

Дополнительная документация

• Краткое руководство по подготовке к эксплуатации Quick Start Guide

В Quick Start Guide объясняется, как подключить NBG6615 и запустить программу-визард Web Configurator.

• Дополнительная информация

Другую информацию о NBG6615 можно найти на сайте.

Краткое содержание

Оглавление

Глава I
Руководство пользователя

Глава 1
Введение

1.1 Обзор

NBG6615 поможет вам расширить вашу проводную сеть без прокладки дополнительных проводов и обеспечит удобный доступ к вашей сети для пользователей мобильных устройств.

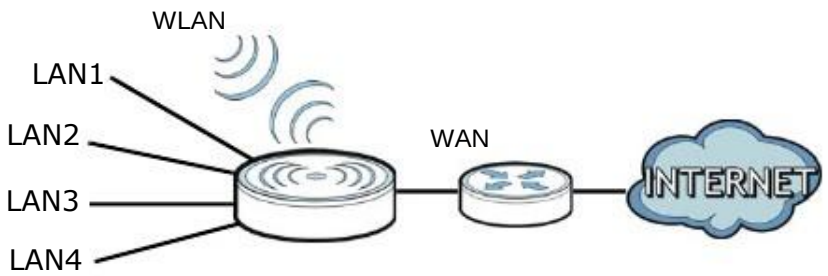
С помощью NBG6615 можно развернуть следующие типы сетевых подключений:

• LAN. Сетевые устройства можно подключить к Ethernet-портам NBG6615 для соединения их между собой и предоставления им доступа к Интернету.

• WLAN. Беспроводные клиенты могут подключиться к NBG6615 для доступа к сетевым ресурсам.

• WAN. Подключение к широкополосному модему/маршрутизатору для доступа к Интернету.

Иллюстрация 1 Сеть NBG6615



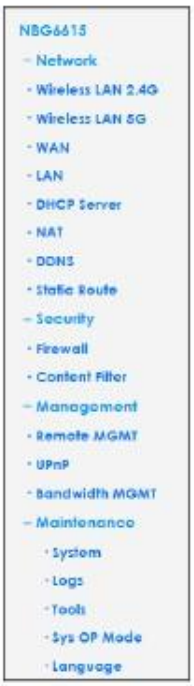
NBG6615 может обслуживать устройства, совместимые с IEEE 802.11b/g/n, в режиме:

• Маршрутизатор

• Точка доступа

Для управления NBG6615можно использовать (поддерживаемый) web-браузер. Меню при этом зависят от режима работы устройства.

Режим маршрутизатора



Режим точки доступа

Подробнее эти режимы описаны в Главе 4 на стр. 28.

1.2 Защита NBG6615

Для улучшения безопасности NBG6615 и эффективного управления этим устройством рекомендуется периодически:

• Менять пароль. Следует использовать пароль, который трудно угадать и который состоит из символов разных типов, например, цифр и букв.

• Записать пароль на бумажке и сохранить ее в надежном месте.

• Выполнять резервное копирование конфигурации (и знать, как ее можно восстановить при необходимости). Восстановление предыдущей версии конфигурации может потребоваться если коммутатор стал работать нестабильно либо не работает. Если вы не помните пароль, то нужно сбросить NBG6615 в заводские настройки по умолчанию. Если у вас есть сделанная ранее резервная копия конфигурационного файла, то не надо заново настраивать всю конфигурацию NBG6615, а достаточно просто восстановить конфигурацию по ее резервной копии.

1.3 Светодиоды

Иллюстрация 2 Передняя панель

В следующей таблице описаны светодиоды и кнопка WPS.

Таблица 1 Светодиоды и кнопка WPS на передней панели

Светодиод	ЦВЕТ	СОСТОЯНИЕ	ИНДИКАЦИЯ
POWER	Белый	Горит	Питание NBG6615 выключено и устройство работает в штатном режиме.
		Не горит	Питание NBG6615 выключено.
		Мигает	Прошивка NBG6615 обновляется, восстанавливается конфигурация или выполняется перезагрузка устройства.
Internet	Белый	Горит	Устройство подключено к Интернету, но трафик не передается.
		Мигает	NBG6615 передает/принимает трафик через WAN.
		Не горит	Устройство не подключено к Интернету.
WLAN_2.4G	Белый	Горит	Беспроводная сеть работает, но в ней сейчас нет трафика.
		Мигает	По беспроводной сети идет трафик.
		Не горит	Беспроводная сеть не работает.
	Желтый	Мигает	NBG6615 устанавливает соединение 2.4G с беспроводным клиентом с помощью WPS.
		Не горит	Процедура WPS сейчас не используется.
		Горит 5 секунд	Соединение установлено с помощью WPS.
WLAN_5G	Белый	Горит	Беспроводная сеть работает, но в ней сейчас нет трафика.
		Мигает	По беспроводной сети идет трафик.
		Не горит	Беспроводная сеть не работает.
	Желтый	Мигает	NBG6615 устанавливает соединение 5G с беспроводным клиентом с помощью WPS.
		Не горит	Процедура WPS сейчас не используется.
		Горит 5 секунд	Соединение установлено с помощью WPS.
Кнопка WPS			Нажатием этой кнопки запускается процесс соединения с помощью WPS.

1.4 Кнопка WPS

NBG6615 поддерживает разработанную альянсом Wi-Fi Alliance промышленную спецификацию Wi-Fi Protected Setup (WPS), которая упрощает создание защищенной беспроводной сети.

С помощью WPS вы сможете быстро построить беспроводную сеть с надежной системой безопасности, которая будет настроена автоматически без вашего участия. Каждое соединение WPS обслуживает передачу данных между двумя устройствами, поддерживающими WPS (информация о поддержке WPS обычно указывается в документации устройства).

На каждом из этих двух устройств нужно нажать кнопку (физическую кнопку на устройстве либо программную в его утилите конфигурирования) либо ввести уникальный идентификатор PIN (Personal Identification Number). После того, как вы включили WPS на одном устройстве надо не позднее чем через 2 минуты включить WPS на другом устройстве чтобы эти устройства нашли друг друга и тогда между ними будет установлено защищенное беспроводное соединение.

Кнопка WPS расположена на передней панели NBG6615.

1.4.1 Использование кнопки WPS

1 Убедитесь, что горит светодиод POWER.

2 Нажмите кнопку WPS и отпустите ее не ранее чем через 3 секунды.

Подобнее о использовании WPS см. Раздел 5.3 на стр. 39.

1.5 Кнопка Reboot/Reset

На задней панели NBG6615 расположена утопленная кнопка reboot/reset. Для перезагрузки нужно отжать эту кнопку скрепкой или аналогичным тонким предметом на 3 – 5 секунд, для сброса NBG6615 в заводские настройки по умолчанию нужно отжать эту кнопку не менее чем на 10 секунд.

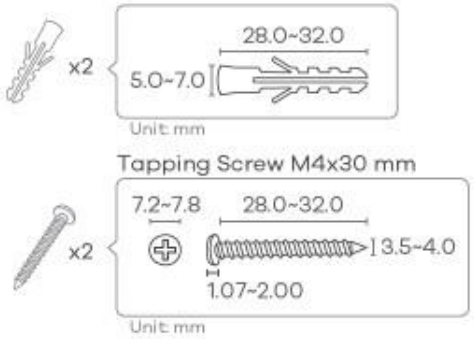
1.6 Монтаж на стене

Если вы устанавливаете устройство на кирпичной или бетонной стене, то вам понадобятся дюбели.

Таблица 2 Информация для монтажа на стене

Расстояние между отверстиями	10.50 см
Шурупы M4	Два
Дюбели (опция)	Два

Иллюстрация 3 Спецификация дюбелей и шурупов



1 Выберите свободное место на стене для монтажа устройства. Стена должна быть достаточно прочной чтобы выдержать вес устройства.

2 Отметьте на стене два места для ввинчивания шурупов, расстояние между которыми должно быть 10,5 см.

Будьте осторожны когда вы сверлите отверстия в стене – убедитесь, что вы не повредите расположенные внутри стены трубы или кабели!

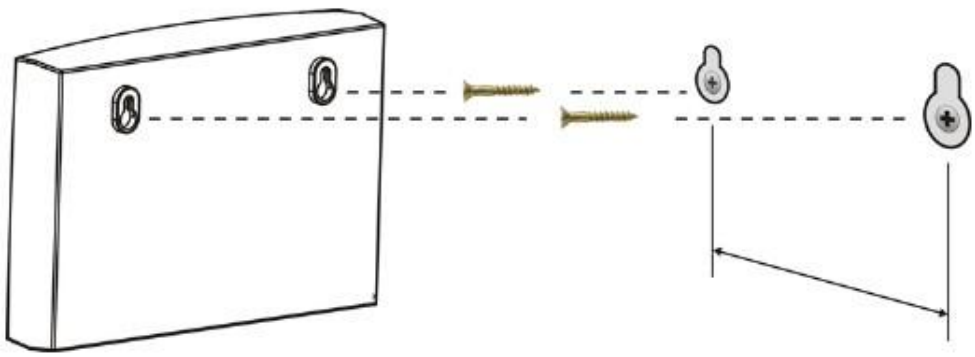
3 Если вы используете дюбели, то просверлите два отверстия для установки дюбелей, затем полностью утопите дюбели в эти отверстия и вверните в них шурупы. Шурупы не следует завинчивать до конца – нужно оставить промежуток примерно 0,5 см между головкой шурупа и стеной.

Если вы не используете дюбели, то отверткой ввинтите шурупы в стену. Шурупы не следует завинчивать до конца – нужно оставить промежуток примерно 0,5 см между головкой шурупа и стеной.

4 Убедитесь, что шурупы зафиксированы выдержать вес NBG6615 вместе с кабелями.

5 Выровняйте отверстия на задней панели NBG6615 с головками шурупов на стене и наденьте NBG6615 на эти шурупы.

Иллюстрация 4 Пример монтажа на стене



Глава 2
Web Configurator

2.1 Обзор

В этой главе объясняется, как для обслуживания работе NBG6615 можно запустить программу Web Configurator, и дается обзор ее экранов.

Web Configurator – это интерфейс управления на базе HTML для простой и удобной настройки и управления NBG6615 с помощью Интернет-браузера. Для его использования нужен браузер, поддерживающий HTML5, например, Internet Explorer 8.0 или более поздней версии, Mozilla Firefox, Google Chrome либо Safari. Для работы с Web Configurator рекомендуется установить разрешение экрана 1366 x 768.

Для использования Web Configurator нужно разрешить:

• всплывающие окна Web-браузера с вашего устройства (по умолчанию заблокированы в Window XP SP2).

• JavaScript (включен по умолчанию).

• Java permissions (включено по умолчанию).

В Главе 23 «Устранение неисправностей» объясняется, как включить эти функции в Internet Explorer.

2.2 Доступ к Web Configurator

1 Правильно подключите кабели к NBG6615 и подготовьте ваш компьютер или компьютерную сеть к подключению к NBG6615 (см. «Краткое руководство по подготовке к эксплуатации» Quick Start Guide).

2 Запустите web-браузер.

3 Если NBG6615 работает в режиме маршрутизатора, то в адресной строке браузера введите "http:// 192.168.212.1". Это адрес IP-адрес LAN в режиме маршрутизатора (это режим работы по умолчанию). (IP-адрес LAN в режиме точки доступа 192.168.1.2).

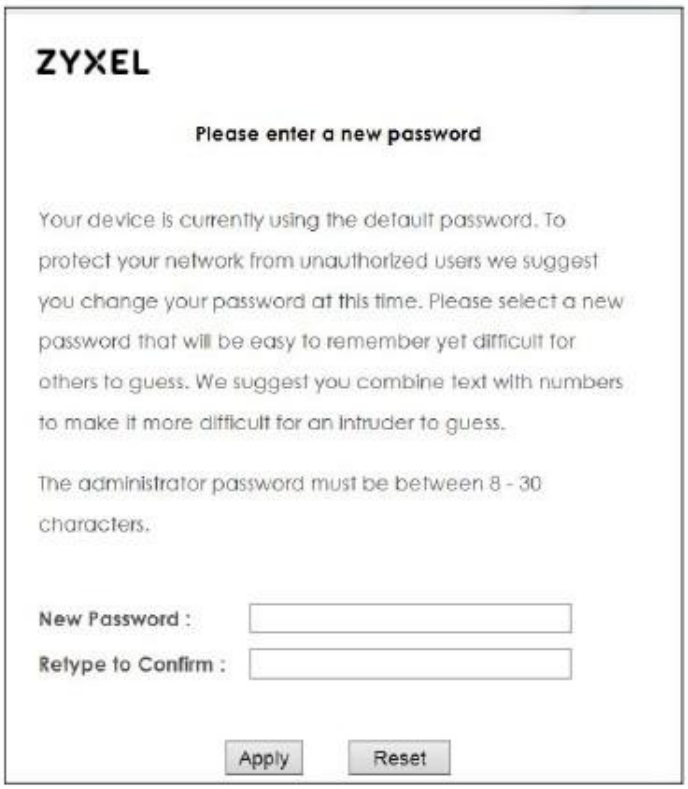
Ваш компьютер при этом должен быть в одной подсети с NBG6615 для доступа к этому адресу web-сайта. В режиме маршрутизатора NBG6615 может назначить вашему компьютеру IP-адрес, поэтому нужно разрешить компьютеру получать IP-адрес автоматически (это настройки компьютера работы по умолчанию) либо назначить ему постоянный IP-адрес в диапазоне от 192.168.212.3 до 192.168.212.254 (см. Приложение C на стр. 157).

4 Введите имя пользователя admin (по умолчанию) и пароль 1234 (по умолчанию) и щелкните **OK**.

Иллюстрация 5 Экран Login

5 Откроется экран для изменения пароля. Настоятельно рекомендуем периодически менять ваш пароль в целях безопасности. Введите новый пароль и щелкните **Apply** для сохранения изменений либо **Ignore** если вы передумали менять пароль

Иллюстрация 6 Экран Change Password



Примечание: Сессия управления автоматически завершается после истечения времени, заданного в поле **Administrator Inactivity Timer** (по умолчанию 5 минут). Если ваша сессия управления закончилась по таймеру, то для управления NBG6615надо снова зайти в Web Configurator.

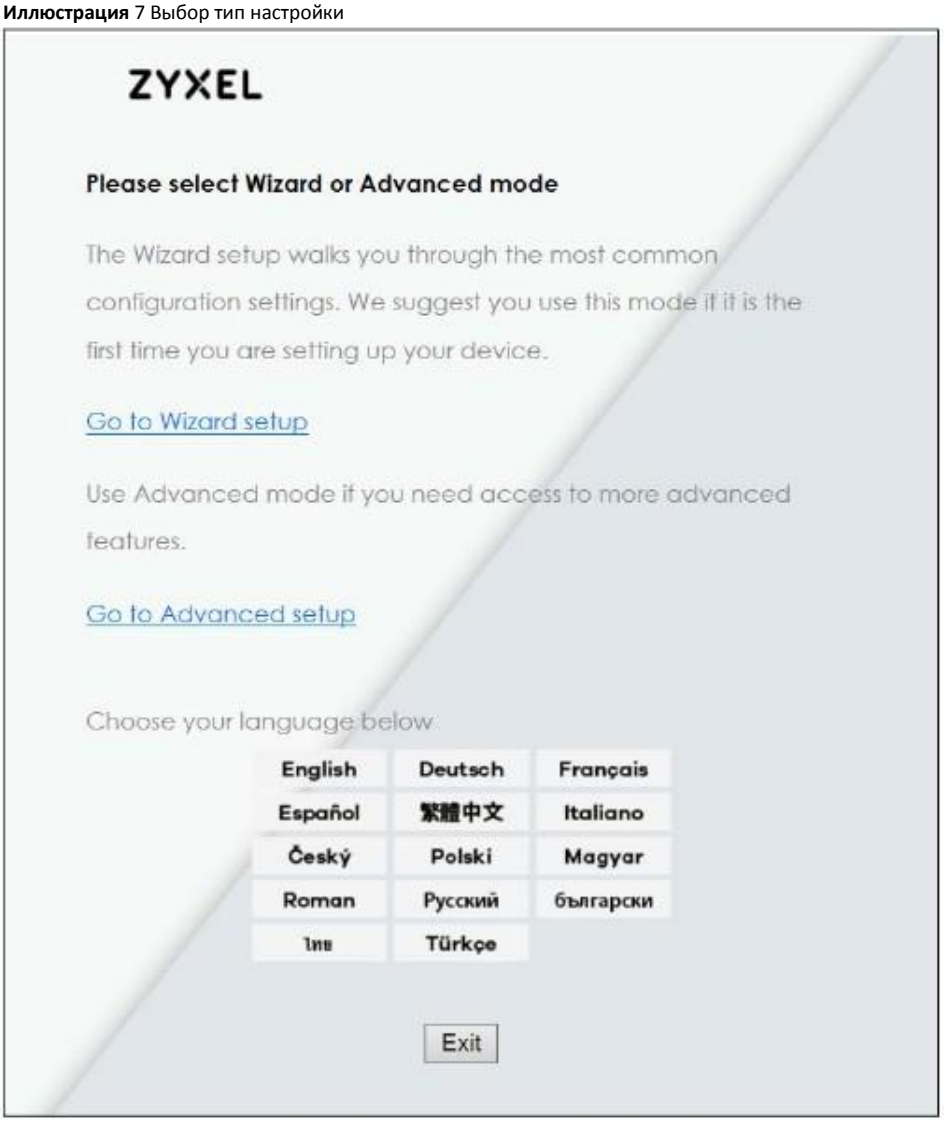
6 Выберите тип настройки.

• Щелкните **Go to Wizard Setup** чтобы настроить основные параметры беспроводной сети и доступа к Интернету с помощью визарда Configuration Wizard.

• Щелкните **Go to Advanced Setup** чтобы посмотреть и сконфигурировать настройки NBG6615.

• Выберите язык Web Configurator. Изменение языка описано в Главе 22 на стр. 132.

Иллюстрация 7 Выбор тип настройки



2.3 Сброс настроек NBG6615

Если вы забыли свой пароль или IP-адрес или у вас нет доступа к Web Configurator, то нужно с помощью кнопки **Reset** на задней панели NBG6615 для загрузки заводских настроек по умолчанию. При этом все ваши настройки будут потеряны, имя пользователя станет **admin** и пароль **1234**, а IP-адрес в режиме маршрутизатора будет “192.168.212.1”.

Убедитесь, что горит светодиод Power и нажмите кнопку **Reset** не менее чем на 10 секунд для перезапуска/перезагрузки NBG6615 с заводскими настройками по умолчанию.

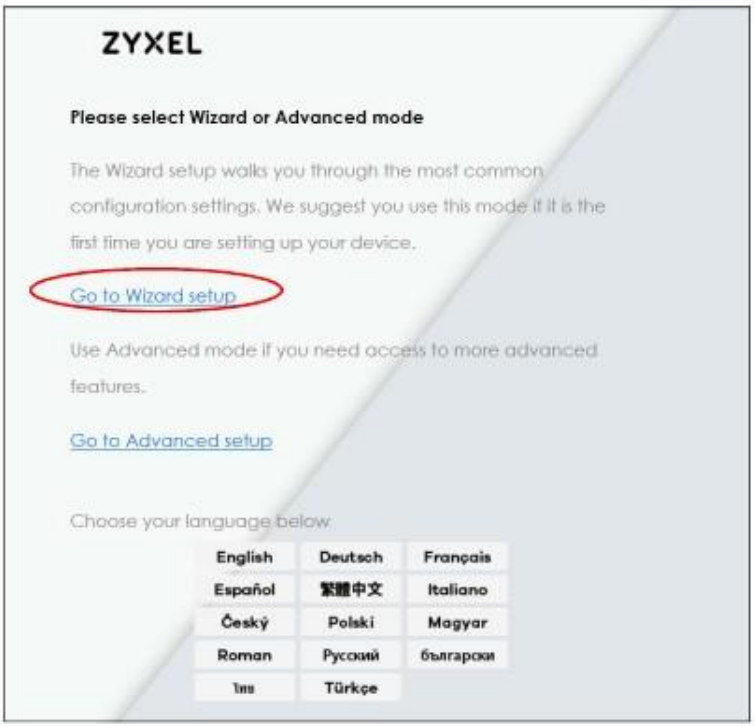
Глава 3
Визард соединения

3.1 Wizard Setup

В этой главе описываются экраны Wizard setup из Web Configurator.

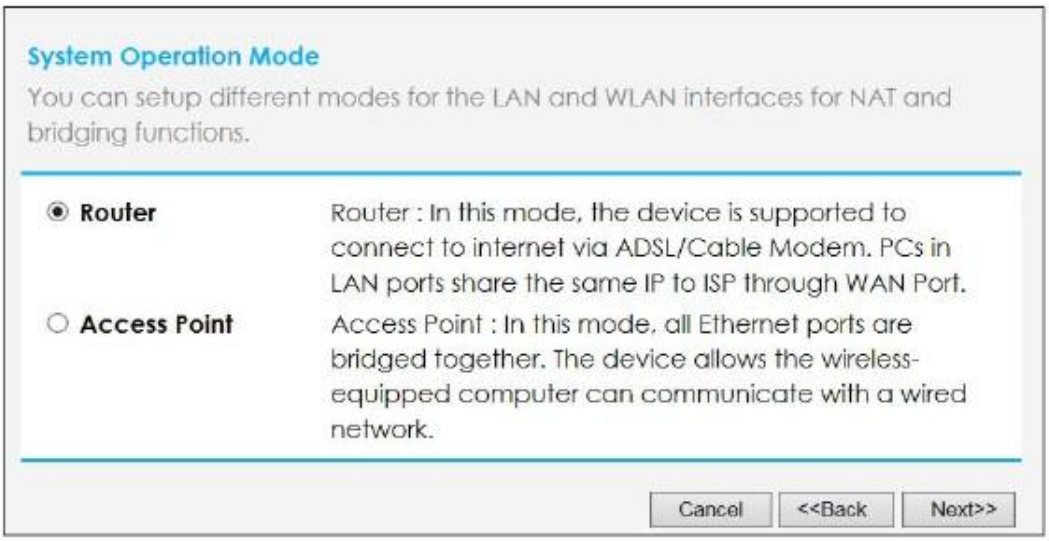
Этот Wizard setup помогает настроить доступ к Интернету (если вы не знаете какую-то информацию, то оставьте соответствующее поле пустым).

1 После запуска Web Configurator щелкните **Go to Wizard setup**.

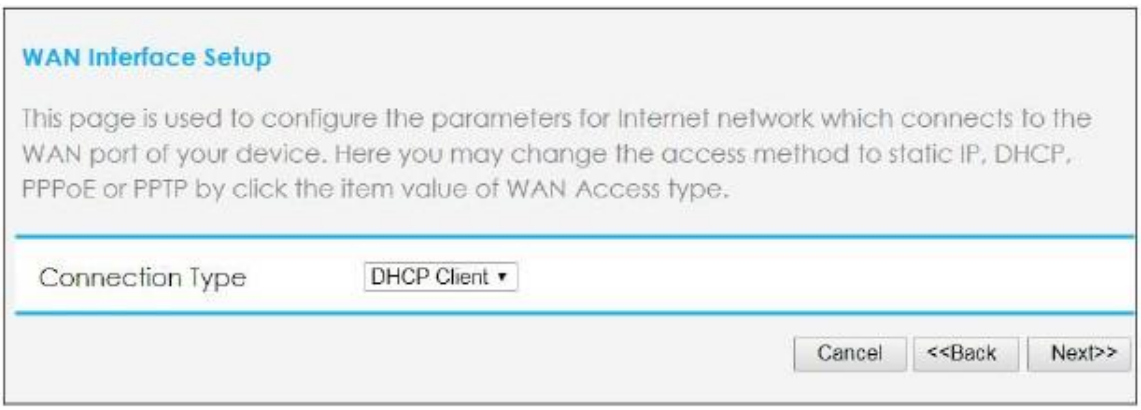


На этом экране можно задать в каком режиме будет использоваться NBG6615 (маршрутизатора или точки доступа). Выберите **Router mode** если нужно чтобы устройство перенаправляло трафик между локальной сетью и другой сетью, например, Интернетом.

Выберите **Access Point** если нужно чтобы устройство работало как мост, по которому передается трафик между клиентами из одной подсети. Щелкните **Next** для сохранения ваших настроек.



2 На экране **WAN Interface Setup** выберите из раскрывающегося списка выберите настройки соединения с Интернетом из четырех вариантов: **Static IP**, **Dynamic Host Configuration Protocol (DHCP Client)**, **PPP over Ethernet (PPPoE)** и **Point to Point Tunneling Protocol (PPTP)**. Уточните у своего провайдера эти настройки. Экран Wizard зависит от выбранного типа соединения.



В следующей таблице описаны поля этого экрана.

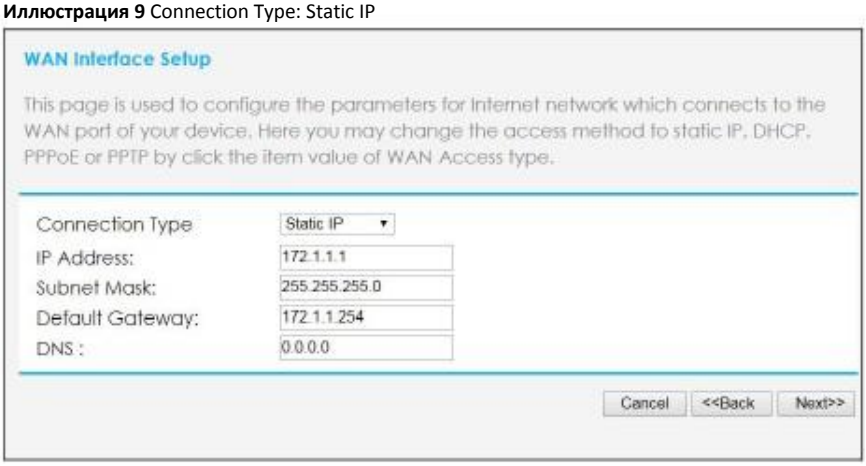
Иллюстрация 8 WAN Interface Setup

ПОЛЕ	ОПИСАНИЕ
Static IP	Выберите **Static IP** если ваш провайдер назначил вам постоянный IP-адрес.
DHCP Client	Выберите **DHCP Client** если ваш провайдер не назначил вам постоянный IP-адрес.
PPPoE	Выберите **PPPoE** для коммутируемого соединения.
PPTP	Выберите **PPTP** для настройки виртуальной частной сети Virtual Private Network (VPN) в незащищенной среде TCP/IP.
Cancel	Щелкните **Cancel** для выхода из визарда без сохранения новых настроек.
Back	Щелкните **Back** для перехода к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.

3.1.1 Static IP Connection

Этот экран визарда используется для назначения NBG6615фиксированного IP-адреса.

Иллюстрация 9 Connection Type: Static IP



В следующей таблице описаны поля этого экрана.

Иллюстрация 10 Connection Type: Static IP

ПОЛЕ	ОПИСАНИЕ
Connection Type	Выберите **Static IP** чтобы у NBG6615 был фиксированный уникальный IP-адрес.
IP Address	Выберите эту опцию если провайдер дал вам IP-адрес и/или настройки DNS-сервера. Фиксированный IP-адрес должен быть в одной сети с вашим широкополосным модемом или маршрутизатором
Subnet Mask	Адрес маски подсети.
Default Gateway	IP-адрес шлюза, который должен сообщить вам ваш провайдер.
DNS	Система Domain Name System (DNS) обеспечивает соответствие между именем домена и IP-адресом. Без использования DNS-сервера вы можете обращаться к компьютеру только по его IP-адресу. NBG6615 использует заданный в этом поле IP-адрес DNS-сервера для определения имен домена для DDNS и сервера точного времени. Введите в это поле IP-адрес DNS-сервера.
Cancel	Щелкните **Cancel** чтобы выйти из Визарда без сохранения изменений.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.

3.1.2 DHCP Client

Если сетевой администратор или провайдер назначает вам IP-адрес динамически, то надо выбрать **DHCP Client**. Обычно этот тип соединения используется с кабельными модемами

Иллюстрация 11 Connection Type: DHCP Client

3.1.3 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) функционирует как коммутируемое соединение. PPPoE – это стандарт IETF (Internet Engineering Task Force), определяющий как хост (ПК) взаимодействует с широкополосным модемом (например, DSL, кабельным или беспроводным) для получения доступа к высокоскоростной сети передачи данных.

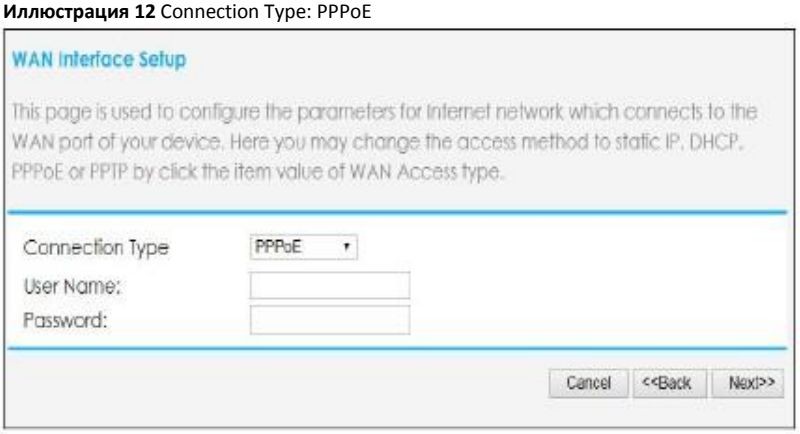
Для сервис-провайдеров PPPoE реализует метод доступа и аутентификации, совместимый с уже имеющейся системой контроля доступа (например, RADIUS).

Одним из преимуществ PPPoE является предоставление конечным пользователям доступа к несколькими сетевым сервисам (так называемый dynamic service selection). Благодаря этой функции провайдер может легко создать новые IP-сервисы и предложить их определенным пользователям.

PPPoE очень удобен и для подписчика сервисов, и для провайдера/оператора, потому что не надо настраивать широкополосный модем, который установлен у подписчика.

Если PPPoE работает непосредственно на NBG6615, а не на компьютерах пользователей, которые подключены к вашей локальной сети, то не нужно устанавливать на этих компьютерах программное обеспечение PPPoE. Кроме того, если включен NAT, то все компьютеры в локальной сети будут иметь доступ к Интернету.

Иллюстрация 12 Connection Type: PPPoE



В следующей таблице описаны поля этого экрана.

Таблица 3 Connection Type: PPPoE

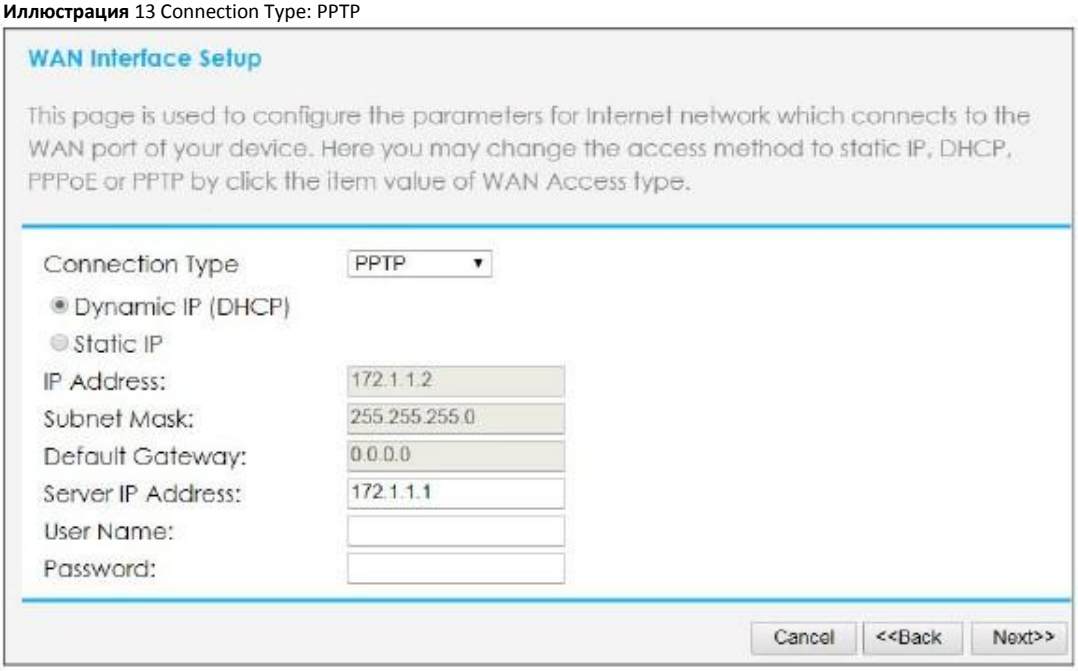
ПОЛЕ	ОПИСАНИЕ
Connection Type	Выберите в раскрывающемся списке PPPoE для коммутируемого соединения.
User Name	Имя пользователя, которое должен сообщить вам ваш провайдер.
Password	Пароль пользователя, который указан в поле User Name.
Confirm Password	Введите пароль еще раз для подтверждения.
Cancel	Щелкните **Cancel** чтобы выйти из визарда без сохранения изменений.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.

3.1.4 PPTP Connection

Point-to-Point Tunneling Protocol (PPTP) – это сетевой протокол для защищенной передачи данных от удаленного клиента на частный сервер с помощью создания виртуальной частной сети Virtual Private Network (VPN) на базе сетей TCP/IP.

PPTP поддерживает создание многопротокольных VPN по требованию на базе Интернета и других публичных сетей.

Иллюстрация 13 Connection Type: PPTP



В следующей таблице описаны поля этого экрана.

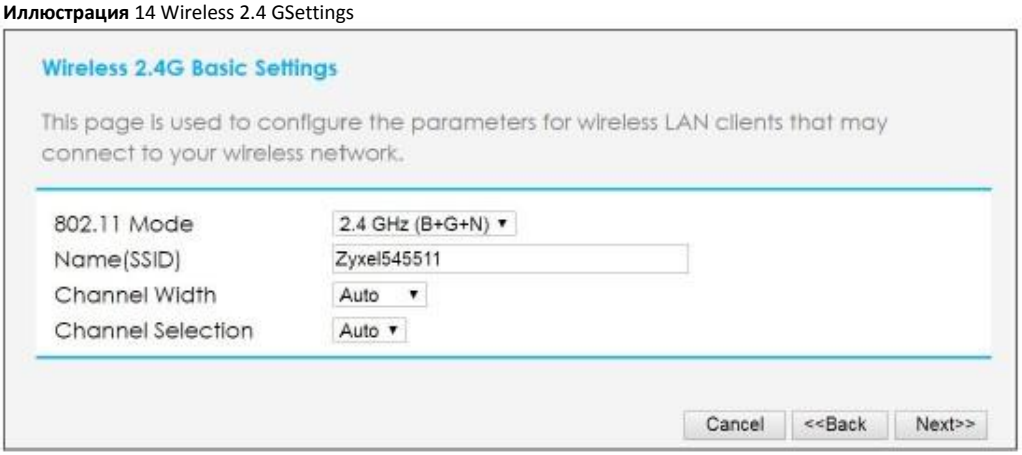
Таблица 4 Connection Type: PPTP

ПОЛЕ	ОПИСАНИЕ
Connection Type	Выберите в раскрывающемся списке PPTP. Выберите **Dynamic IP (DHCP)** если ваш провайдер динамически назначает вам параметры DNS-сервера и IP-адрес WAN для NBG6615. Если у вас есть IP-адрес DNS-сервера, то выберите **Static IP**.
IP Address	Если вы выбрали **Static IP**, то введите постоянный IP-адрес, который вам назначил провайдер.

ПОЛЕ	ОПИСАНИЕ
Subnet Mask	Если вы выбрали **Static IP**, то введите IP-адрес макси подсети, который вам назначил провайдер (если таковой имеется).
Default Gateway	Если вы выбрали **Static IP**, то введите IP-адрес шлюза сервера PPTP.
Server IP Address	Введите IP-адрес сервера PPTP.
User Name	Введите имя пользователя, которое вам назначил провайдер.
Password	Пароль пользователя, который указан в поле User Name.
Cancel	Щелкните **Cancel** чтобы выйти из визарда без сохранения изменений.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.

3 Теперь можно переходить к настройке параметров беспроводной сети. С помощью этого экрана можно задать основные настройки для диапазона беспроводной сети 2.4G.

Иллюстрация 14 Wireless 2.4 GSettings



В следующей таблице описаны поля этого экрана.

Таблица 5 Wireless Settings

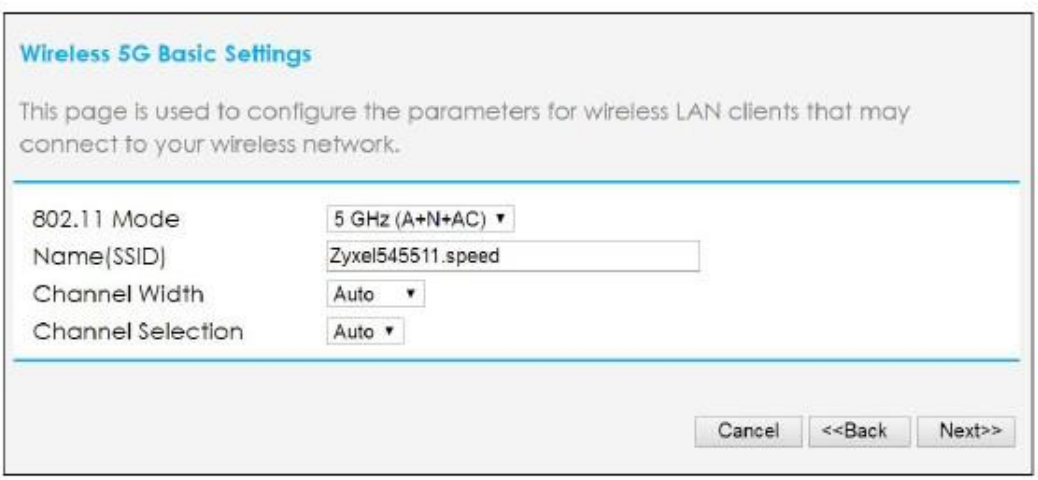
ПОЛЕ	ОПИСАНИЕ
Wireless 2.4G Basic Settings	
802.11 Mode	Выберите из раскрывающегося списка режим IEEE 802.11 WLAN, который будет использовать NBG6615.
Name (SSID)	Введите имя беспроводной сети (до 32 7-битных печатных символов). Если вы изменили SSID беспроводной сети на NBG6615, то надо изменить SSID и на всех беспроводных клиентов, которые используют эту сеть.
Channel Width	Выберите какую ширину беспроводного канала будет использовать NBG6615 (20MHz, 40MHz или 80MHz) (80MHz доступна только для 5G). Если выбрать **Auto**, то NBG6615 автоматически выбирает ширину канала в зависимости от условий работы сети). Выберите **20MHz** если там, где вы развертываете беспроводную сеть, много помех от других беспроводных устройств или беспроводные клиенты не поддерживают функцию channel bonding. Выберите **40MHz** если вы хотите объединить два соседних канала 2.4G для увеличения пропускной способности. Беспроводные клиенты при этом также должны использовать 40 MHz. Выберите **80MHz** (доступно только для 5G) если в беспроводной сети работает только несколько клиентов.

Таблица 5 Wireless Settings

ПОЛЕ	ОПИСАНИЕ
Channel Selection	Диапазон радиочастот, используемых беспроводных каналом by IEEE 802.11b/g/n, называется каналом. Выберите рабочую частоту/канал из раскрывающегося списка в зависимости от частотного диапазона и страны, в которой вы находитесь. Если выбрать **Auto**, то NBG6615 будет автоматически выбирать канал с наименьшими помехами.
Cancel	Щелкните **Cancel** чтобы выйти из визарда без сохранения изменений.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.

4 На следующем этапе нужно выбрать шифрование для защиты данных, которые пересылаются по беспроводной сети. Из раскрывающегося списка можно выбрать **None**, **WPA2-PSK** или **WPA-PSK/WPA2-PSK. WPA2-PSK** это самый надежный протокол шифрования и его рекомендуется использовать всем пользователям. Если у вас устаревшие клиентские устройства не поддерживают **WPA2-PSK**, то выберите **WPA-PSK/WPA2-PSK** чтобы новые устройства могли использовать **WPA2-PSK**, а устаревшие - **WPA-PSK**. После выбора протокола шифрования нужно создать пароль в поле **Pre-shared Key**. Пароль может состоять из 8 - 63 символов ASCII (включая пробелы и символы, регистр букв учитывается) или 64 шестнадцатеричных символа (“0-9,” “A-F”). Щелкните **Next** для сохранения настроек.

5 Повторите шаги 4 и 5 для настройки беспроводной сети 5G.



6 Щелкните **Finished** для завершения работы Wizard setup.

Поздравляем! Вы успешно настроили NBG6615 для обслуживания вашей сети и подключения этого устройства к Интернету.

Глава 4
Режимы работы

4.1 Обзор

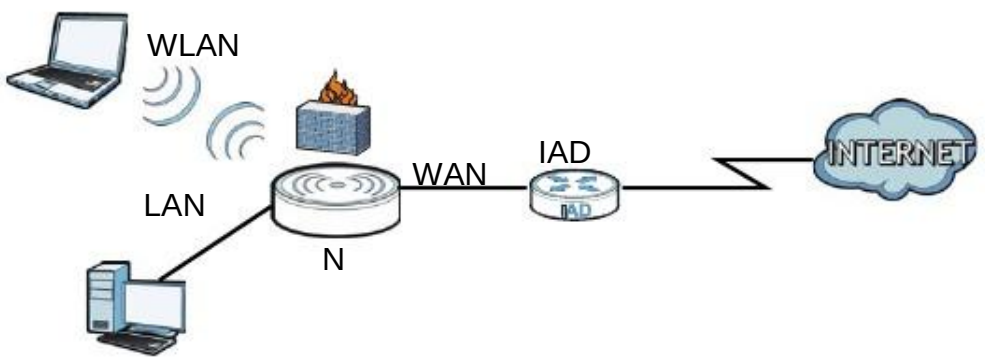
В этом разделе описываются разные режимы использования NBG6615 для обслуживания устройств, поддерживающих IEEE 802.11b/g/n.

Примечание: С самого начала правильно выберите режим работы – при изменении режима работы NBG6615 автоматически выполнит перезагрузку.

По умолчанию у NBG6615 в режиме администратора IP-адрес LAN 192.168.212.1. По умолчанию в режиме работы точки доступа IP-адрес NBG6615 192.168.1.2.

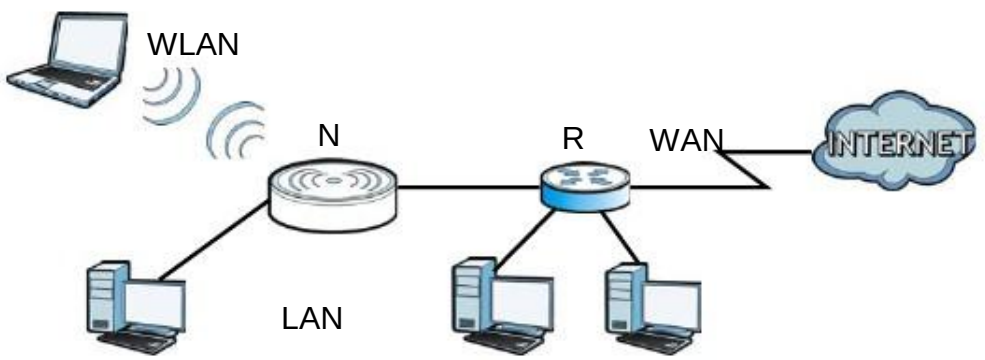
• **Маршрутизатор:** Этот режим позволяет использовать на NBG6615 (N)такие функции маршрутизации, как LAN DHCP, NAT, межсетевой экран и т.п. У NBG6615 отдельные IP-адреса для LAN и WAN. Подключите его порт WAN к такому интегрированному устройству доступа Internet Access Device (IAD), как широкополосный модем.

Иллюстрация 15 Маршрутизатор



• **Точка доступа:** Этот режим используется если в сети уже есть маршрутизатор (R) и надо развернуть беспроводную сеть и связать мостом проводные и беспроводные соединения NBG6615.

Иллюстрация 16 Режим точки доступа



4.2 Настройка NBG6615 в режиме маршрутизатора

По умолчанию NBG6615 работает в режиме маршрутизатора. Если NBG6615 работает в режиме точки доступа, то для переключения на режим маршрутизатора нужно выполнить следующую процедуру:

1 Подключите ваш компьютер к порту LAN на NBG6615.

2 По умолчанию IP-адрес NBG6615 192.168.212.1 в режиме маршрутизатора и 192.168.212.2 в режиме точки доступа. В режиме маршрутизатора NBG6615 может назначить вашему компьютеру IP-адрес, поэтому нужно настроить компьютер на автоматическое получение IP-адреса (это заводская настройка по умолчанию компьютера) либо назначить компьютеру постоянный IP-адрес в диапазон от 192.168.212.3 и до 192.168.212.254.

3 После настройки IP-адреса компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите IP-адрес NBG6615.

4 Зайдите в Web Configurator (см. Глава 2 на стр. 16).

5 Перейдите на экран **Maintenance > Sys OP Mode > General** и выберите **Router**.

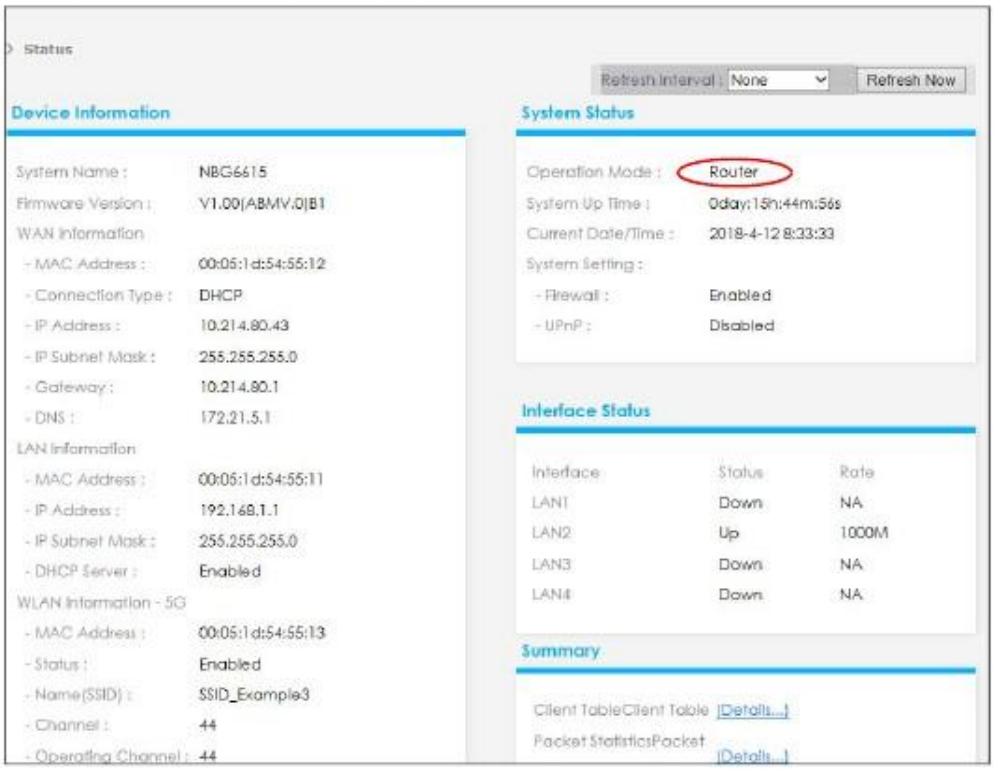
6 Щелкните **Apply**.

Примечание: Нужно дождаться окончания перезапуска NBG6615 и затем снова зайти на Web Configurator. У NBG6615 IP-адрес изменится на 192.168.212.1.

4.2.1 Экран Status (режим маршрутизатора)

Этот экран отображает состояние NBG6615 в режиме маршрутизатора.

Иллюстрация 17 Экран Status (режим маршрутизатора)



В этой таблице описаны пиктограммы экрана Status.

Таблица 6 Основные пиктограаамы экрана Status

ICON	**ОПИСАНИЕ**
	Пиктограмма вызова визарда Setup.
	Пиктограмма просмотра информации о продукте.
	Пиктограмма выхода из Web Configurator.

В следующей таблице описаны поля экрана Status в режиме маршрутизатора.

Таблица 7 Web Configurator экрана Status (режим маршрутизатора)

ПОЛЕ	**ОПИСАНИЕ**
Device Information	
System Name	Имя системы **System Name**, которые вы ввели на экране **Maintenance > System > General**.
Firmware Version	Версия прошивки NBG6615.
WAN Information	
- MAC Address	MAC-адрес Ethernet-адаптера WAN вашего устройства.
- Connection Type	Текущий тип соединения.
- IP Address	IP-адрес порта WAN.
- IP Subnet Mask	Маска подсети порта WAN.
- Gateway	IP-адрес порта WAN шлюза.

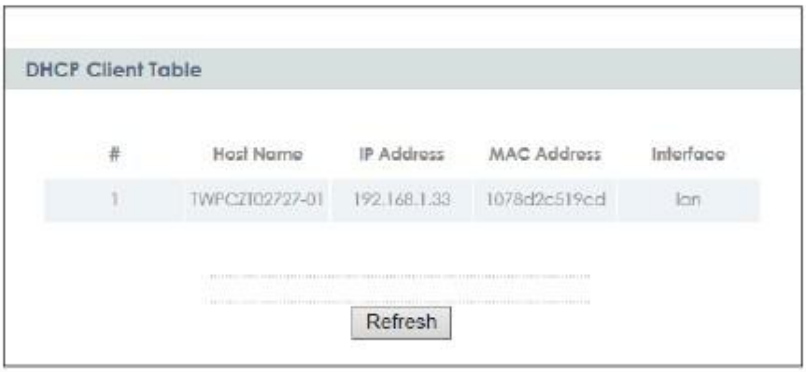
Таблица 7 Web Configurator экрана Status (режим маршрутизатора) (продолжение)

ПОЛЕ	ОПИСАНИЕ
- DNS	IP-адрес сервера DNS.
LAN Information	
- MAC Address	MAC-адрес Ethernet-адаптера LAN вашего устройства.
- IP Address	IP-адрес порта LAN.
- IP Subnet Mask	Маска подсети порта LAN.
- DHCP Server	Состояние сервера DHCP порта LAN.
WLAN Information (5.G/2.4G)	
- MAC Address	MAC-адрес беспроводного адаптера вашего устройства.
- Status	Состояние Wireless LAN: Включена (**On**), выключена (**Off**), выключена по расписанию (**Off by scheduler**).
- Name (SSID)	Имя для идентификации NBG6615 в беспроводной сети.
- Channel	Номер канала, который задается вручную либо NBG6615 автоматически сканирует и выбирает канал.
- Operating Channel	Номер канала, который NBG6615 сейчас использует для беспроводной сети.
- Security Mode	Тип безопасности беспроводной сети, который использует NBG6615.
- 802.11 Mode	Стандарт беспроводных сетей.
- WPS	**Configured** если WPS настроен. **Unconfigured** если WPS не настроен. Для просмотра статуса выберите экран **Network > Wireless LAN > WPS**.
System Status	
Operation Mode	Режим работы: **Router** (маршрутизатор) или **Access Point** (точка доступа).
System Up Time	Сколько всего времени проработал NBG6615.
Current Date/Time	Дата и время часов NBG6615.
System Setting	
- Firewall	Это поле показывает, включен ли межсетевой экран.
- UPnP	Это поле показывает, включен ли UPnP.
Interface	
-Lan 1	Состояние соединения и рабочая скорость первого порта LAN.
-Lan 2	Состояние соединения и рабочая скорость второго порта LAN.
-Lan 3	Состояние соединения и рабочая скорость третьего порта LAN.
-Lan 4	Состояние соединения и рабочая скорость четвертого порта LAN.
Summary	
Client Table	Экран для вывода информации о клиенте. Для перехода к этому экрану щелкните **Details...**.
Packet Statistics	Экран для вывода информации о состоянии порта и статистике пакетов. Для перехода к этому экрану щелкните **Details...**.

4.2.1.1 Summary: Client Table

Щелкните ссылку **Client Table (Details...)** на экране **Status**. В таблице **client table** выводится текущая информация о клиенте, в том числе имя хоста, адреса IP и MAC для всех сетевых клиентов, подключенных к NBG6615.

Иллюстрация 18 Summary: Client Table



В следующей таблице описаны поля этого экрана.

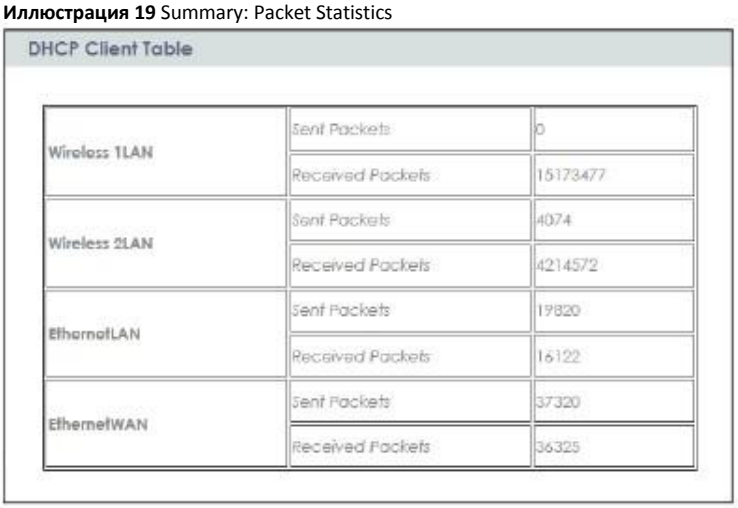
Таблица 8 Summary: Client Table

ПОЛЕ	ОПИСАНИЕ
#	Номер компьютера (хоста).
Host Name	Имя компьютера (хоста).
IP Address	IPv4-адрес, соответствующий указанном выше в поле # номеру.
MAC Address	MAC-адрес компьютера, имя которого указано в поле Host Name. У каждого устройства Ethernet есть уникальный адрес MAC (Media Access Control). Этот адрес назначается на заводе и состоит из шести пар шестнадцатеричных цифр, например 00:A0:C5:00:00:02.
Interface	Интерфейс NBG6615, к которому подключен клиент.

4.2.1.2 Summary: Packet Statistics

Щелкните ссылку **Packet Statistics (Details...)** на экране Status. Здесь выводится статистика для каждого порта по пакетам, которые были отправлены и получены. Для обновления статистики щелкните кнопку **Refresh**.

Иллюстрация 19 Summary: Packet Statistics



4.2.2 Панель навигации в режиме маршрутизатора

Меню панели навигации используется для настройки функций NBG6615 в режиме маршрутизатора.

Иллюстрация 20 Меню: режим маршрутизатора

Подменю описаны в следующей таблице.

Таблица 9 Меню: режим маршрутизатора

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Network		
Wireless LAN (2.4G/ 5G)	General	Экран конфигурирования беспроводной сети.
	MAC Filter	Фильтр MAC-адресов задает блокирование доступа к определенным устройствам или доступа определенных устройств к NBG6615.
	WLAN Advanced Setup	Настройка расширенных параметров беспроводной сети.
	WPS	Настройка WPS.
	WPS Station	Добавление беспроводной станции с помощью WPS.
	Scheduling	Расписание включения/отключения беспроводной сети.
	MBSSID	Настройка нескольких SSID на NBG6615.
WAN	Internet Connection	Настройка параметров Интернет-провайдера, назначение IP-адресов WAN IP, DNS-серверов и MAC-сервера WAN.
	Advanced	Настройка multicast WAN и auto IP.
LAN	IP	Настройка IPv4-адреса и маски подсети LAN.

Таблица 9 Menus: режим маршрутизатора (продолжение)

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
DHCP Server	General	Включение DHCP-сервера NBG6615.
	Static DHCP	Назначение IP-адресов LAN отдельным компьютерам в соответствии с их MAC-адресами и назначение DNS-серверам IP-адресов с помощью DHCP.
	Client List	Текущая информация о клиентах DHCP и назначение IP-адреса в соответствии с MAC-адресом и именем хоста.
NAT	General	Экран для включения NAT.
	Application	Экран для настройки серверов, которые стоят за NBG6615.
	Port Triggering	Экран для настройки port triggering на NBG6615.
DDNS	General	Экран для настройки Dynamic DNS (сервиса для соответствия фиксированных имен домена и непостоянных IP-адресов).
Static Route	IP Static Route	Экран для настройки статичных маршрутов IP static routes.
Security		
Firewall	General	Экран для включения/отключения межсетевого экрана.
	Services	Экран для включения/отключения функций ICMP и VPN passthrough.
	MAC Filter	Экран для составления «белого» и «черного» списка MAC-адресов устройств.
Content Filter	Filter	Экран для настройки фильтра контента NBG6615.
Management		
Remote MGMT	WWW	Экран для настройки интерфейсов, через которые по IP-адресу можно с помощью HTTP управлять NBG6615.
UPnP	UPnP	Экран для включения UPnP на NBG6615.
Bandwidth MGMT	General	Экран для включения управления полосой пропускания на NBG6615.
	Advanced	Экран для задания полосы пропускания для исходящего трафика и редактирования правил управления полосой пропускания.
Maintenance		
System	General	Экран для просмотра настроек администратора (имени системы и домена, пароля, таймера отключения и т.п.).
	Time Setting	Экран для изменения даты и времени NBG6615.
Logs	View Log	Экран для просмотра журналов для выбранных категорий событий.
Tools	Firmware	Экран для загрузки прошивки на NBG6615.
	Configuration	Экран для резервного копирования/восстановления конфигурации и сброса NBG6615 в заводские настройки по умолчанию.
	Restart	Экран для перезагрузки NBG6615 без выключения питания.
Sys OP Mode	General	Экран для выбора режима работы устройства.
Language	Language	Экран для выбора языка.

4.3 Настройка NBG6615 в режиме точки доступа

1 Подключите ваш компьютер к порту LAN на NBG6615.

2 По умолчанию IP-адрес NBG6615 192.168.212.1 в режиме маршрутизатора и 192.168.212.2 в режиме точки доступа.

3 После настройки IP-адреса компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите IP-адрес NBG6615.

4 Зайдите в Web Configurator (см. Глава 2 на стр. 16).

5 Перейдите на экран **Maintenance > Sys OP Mode > General** и выберите **Access Point**.

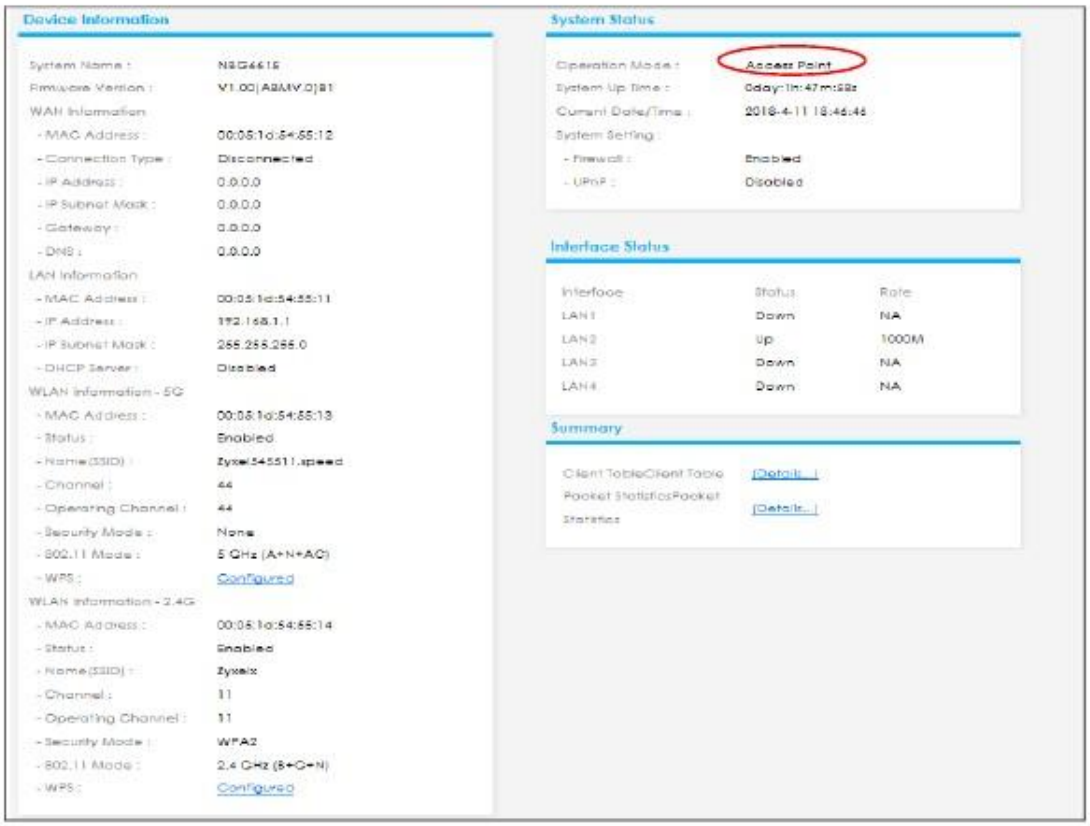
6 Щелкните **Apply**. Теперь NBG6615 работает в режиме точки доступа (AP Mode).

Примечание: Нужно дождаться окончания перезапуска NBG6615 и затем снова зайти на Web Configurator.

4.3.1 Экран Status (режим точки доступа)

Щелкните **Status**. Этот экран отображает состояние NBG6615 в режиме точки доступа.

Иллюстрация 21 Экран Status Screen (режим точки доступа)



В этой таблице описаны поля экрана Status.

Таблица 10 Status Screen (AP Mode)

ПОЛЕ	ОПИСАНИЕ
Device Information	
System Name	Имя системы **System Name**, которые вы ввели на экране Maintenance > System > General.
Firmware Version	Версия прошивки NBG6615.
WAN Information	
-MAC Address	MAC-адрес Ethernet-адаптера WAN вашего устройства.
-Connection Type	Текущий тип соединения.
-IP Address	IP-адрес порта WAN.
-IP Subnet Mask	Маска подсети порта WAN.
-Gateway	IP-адрес порта WAN шлюза.
-DNS	IP-адрес сервера DNS.
LAN Information	
- MAC Address	MAC-адрес Ethernet-адаптера LAN вашего устройства.
- IP Address	IP-адрес порта LAN.
- IP Subnet Mask	Маска подсети порта LAN.
- DHCP Server	Состояние сервера DHCP порта LAN.
WLAN Information (5g/2.4G)	
- MAC Address	MAC-адрес беспроводного адаптера вашего устройства.

Таблица 10 Status Screen (AP Mode) (продолжение)

ПОЛЕ	ОПИСАНИЕ
- Status	Состояние Wireless LAN: Включена (**On**), выключена (**Off**), выключена по расписанию (**Off by scheduler**).
- Name (SSID)	Имя для идентификации NBG6615 в беспроводной сети.
- Channel	Номер канала, который задается вручную либо NBG6615 автоматически сканирует и выбирает канал.
- Operating Channel	Номер канала, который NBG6615 сейчас использует для беспроводной сети.
- Security Mode	Тип безопасности беспроводной сети, который использует NBG6615.
- 802.11 Mode	Стандарт беспроводных сетей IEEE 802.11, который поддерживает NBG6615. Беспроводные клиенты для подключения к NBG6615 должны поддерживать тот же стандарт.
- WPS	Состояние WPS (WiFi Protected Setup). Щелкните status чтобы перейти на экран **Network > Wireless LAN > WPS**.
System Status	
Operation Mode	Режим работы: **Router** (маршрутизатор) или **Access Point** (точка доступа).
System Up Time	Сколько всего времени проработал NBG6615.
Current Date/Time	Дата и время часов NBG6615.
Summary	
Client Table	Экран для вывода информации о клиенте. Для перехода к этому экрану щелкните **Details...**.
Packet Statistics	Экран для вывода информации о состоянии порта и статистике пакетов. Для перехода к этому экрану щелкните **Details...**.

4.3.2 Панель навигации в режиме точки доступа

Меню панели навигации используется для настройки функций NBG6615 в режиме точки доступа.

На следующем экране и в таблице представлены функции, которые можно сконфигурировать в режиме точки доступа.

Иллюстрация 22 Меню: режим точки доступа

Подменю описаны в следующей таблице.

Таблица 11 Меню: режим точки доступа

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Network		
Wireless LAN (2.4G/5G)	General	Экран конфигурирования беспроводной сети.
	MAC Filter	Фильтр MAC-адресов задает блокирование доступа к определенным устройствам или доступа определенных устройств к NBG6615.
	WLAN Advanced Setup	Настройка расширенных параметров беспроводной сети.
	WPS	Настройка WPS.
	WPS Station	Добавление беспроводной станции с помощью WPS.
	Scheduling	Расписание включения/отключения беспроводной сети.
	MBSSID	Настройка нескольких SSID на NBG6615.
LAN	IP	Настройка IP-адреса и маски подсети LAN.
Maintenance		
System	General	Экран для просмотра настроек администратора (имени системы и домена, пароля, таймера отключения и т.п.).
	Time Setting	Экран для изменения даты и времени NBG6615.
Logs	View Log	Экран для просмотра журналов для выбранных категорий событий.
Tools	Firmware	Экран для загрузки прошивки на NBG6615.
	Configuration	Экран для резервного копирования/восстановления конфигурации и сброса NBG6615 в заводские настройки по умолчанию.
	Restart	Экран для перезагрузки NBG6615 без выключения питания.
Sys OP Mode	General	Экран для выбора режима работы устройства (маршрутизатор или точка доступа).
Language	Language	Экран для выбора языка.

Глава 5
Инструкции

5.1 Обзор

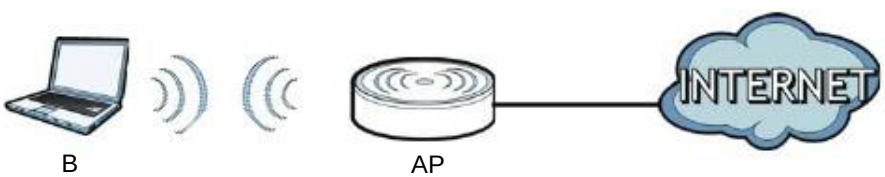
В этой главе собраны инструкции по настройке NBG6615:

- Подключение к Интернету через точку доступа
- Настройка безопасности беспроводной сети, используя WPS на NBG6615 и беспроводном клиенте
- Включение и настройка безопасности беспроводной сети, не используя WPS на NBG6615
- Использование нескольких SSID на NBG6615
- Управление полосой пропускания на NBG6615

5.2 Подключение к Интернету через точку доступа

В этом разделе приведен пример настройки беспроводного соединения точки доступ (**AP**) и беспроводного клиента (ноутбука **B** в этом примере). **B** может подключиться к Интернету по беспроводной сети через **AP**.

Иллюстрация 23 Беспроводное соединение с Интернетом через AP



5.3 Настройка безопасности беспроводной сети, используя WPS на NBG6615 и беспроводном клиенте

В этом разделе приведен пример настройки безопасности беспроводной сети, используя WPS. В этом примере NBG6615 работает как AP, а WiFi-адаптер NWD210N как подключенный к ноутбуку беспроводной клиент.

Примечание: Беспроводной адаптер должен поддерживать WPS (например, а WiFi-адаптер с поддержкой WPS).

Есть два способа создания защищенного беспроводного соединения с помощью WPS:

- **Push Button Configuration (PBC)** – защищенное беспроводное соединения создается одним нажатием кнопки (см. Раздел 5.3.1 на стр. 40). Это более простой способ.

• **PIN Configuration** - для создания защищенного беспроводного соединения нужно ввести код PIN (Personal Identification Number) беспроводного клиента в интерфейсе NBG6615 (см. Раздел 5.3.2 на стр. 41). Это более безопасный метод, потому что оба устройства могут аутентифицировать друг друга.

5.3.1 Push Button Configuration

1 Убедитесь, что NBG6615 включен и ноутбук находится в зоне покрытия этого устройства.

2 Убедитесь, что на ноутбуке инсталлирован драйвер беспроводного клиента (в этом примере NWD210N) и его утилита.

3 В утилите беспроводного клиента найдите настройки WPS. Включите WPS и нажмите кнопку WPS (кнопку **Start** или **WPS**)

4 Зайдите в Web Configurator NBG6615 и нажмите кнопку **Push Button** на экране **Network > Wireless LAN** (2.4G/5G) **> WPS Station**.

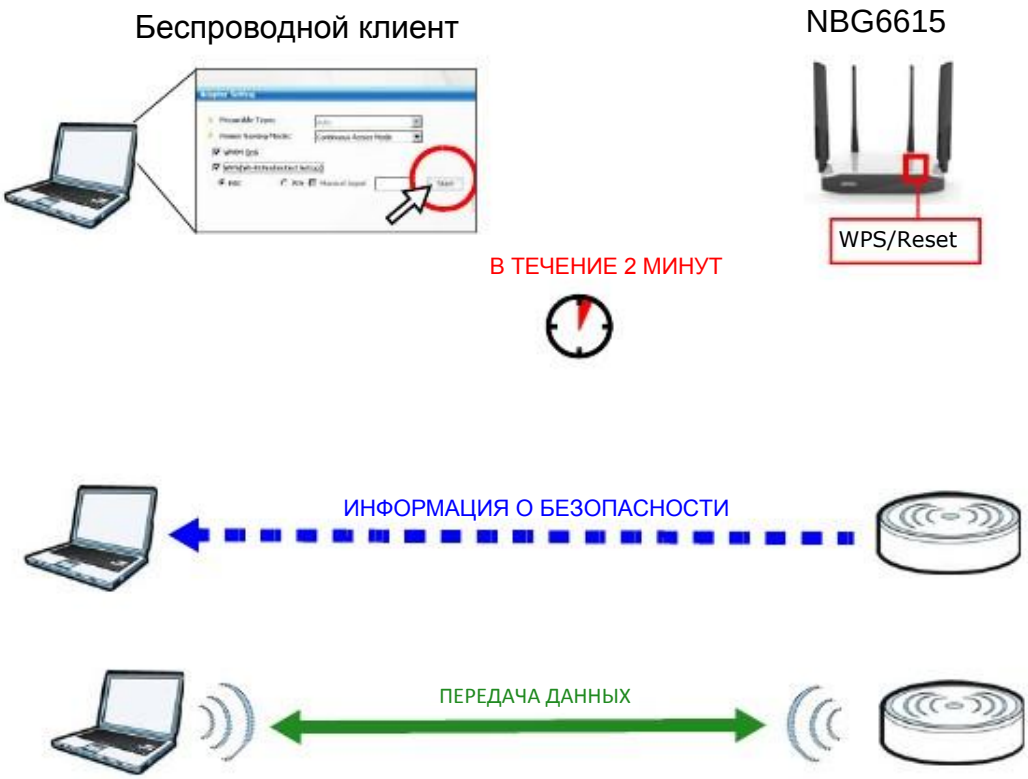
Примечание: У NBG6615 кнопка WPS расположена на верхней панели и еще есть программная кнопка WPS в его утилите конфигурирования. Обе кнопки работают одинаков и можно использовать любую из них.

Примечание: Не имеет значения, какая из кнопок нажата первой. Важно чтобы вторая кнопка была нажата не позднее чем через 2 минуты.

NBG6615 посылает беспроводному клиенту правильные настройки конфигурации. Это занимает около 2 минут и затем беспроводной клиент может безопасно обмениваться данными с NBG6615.

На следующей иллюстрации показан пример развертывания защищенной беспроводной сети нажатием кнопки и на NBG6615, на беспроводном клиенте (в данном примере NWD210N).

Иллюстрация 24 Пример процесса WPS: вариант с Push Button Configuration



5.3.2 Конфигурирование PIN

При использовании варианта с конфигурированием PIN нужно использовать интерфейс конфигурирования NBG6615 и утилиту клиента.

1 Откройте утилиту конфигурирования беспроводного клиента, перейдите в настройки WPS и выберите PIN method чтобы получить код PIN.

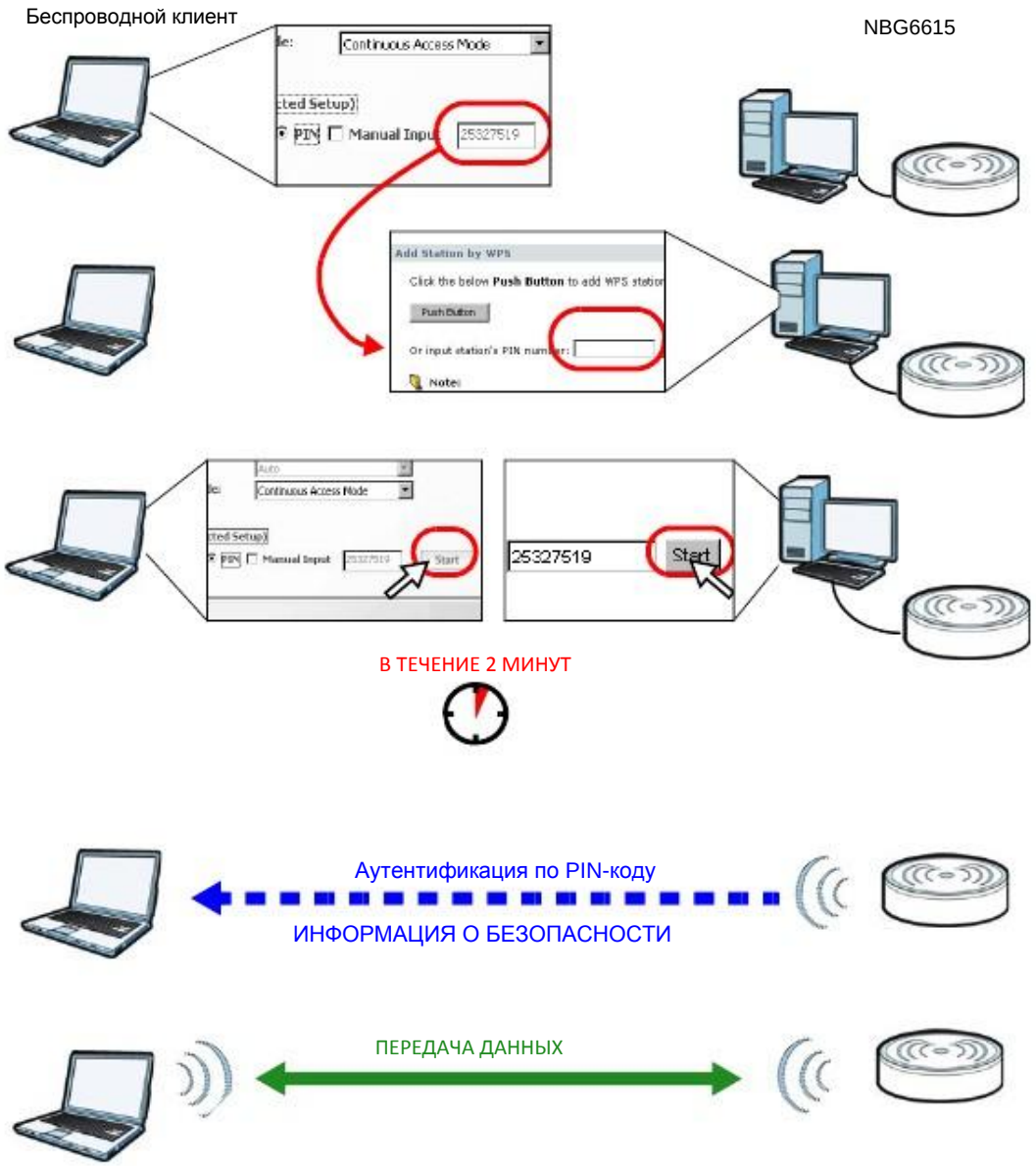
2 Введите код PIN в поле PIN на экране **Network > Wireless LAN (2.4G/5G)> WPS Station** на NBG6615.

3 Щелкните кнопку **Start** (или кнопку рядом с полем PIN) в утилите беспроводного клиента и в экране WPS на NBG6615 в течение 2 минут.

NBG6615 выполняет аутентификацию беспроводного клиента и посылает ему настройки конфигурации. Это занимает около 2 минут и затем беспроводной клиент может безопасно обмениваться данными с NBG6615.

На следующей иллюстрации показан пример развертывания защищенной беспроводной сети с помощью PIN и на NBG6615, и на беспроводном клиенте (в данном примере NWD210N.

Иллюстрация 25 Пример процесса WPS: вариант с PIN



5.4 Подключение к беспроводной сети NBG6615 без использования WPS

В этом примере показано, как сконфигурировать безопасность беспроводной сети со следующими параметрами NBG6615.

SSID	SSID_Example3
Channel	**6**
Security	WPA-PSK/WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Выполните следующие операции для настройки параметров беспроводной сети на NBG6615.

Сначала нужно подключить оборудование (см. Quick Start Guide) и зайти на Web Configurator через соединение LAN (см. Раздел 2.2 на стр. 16).

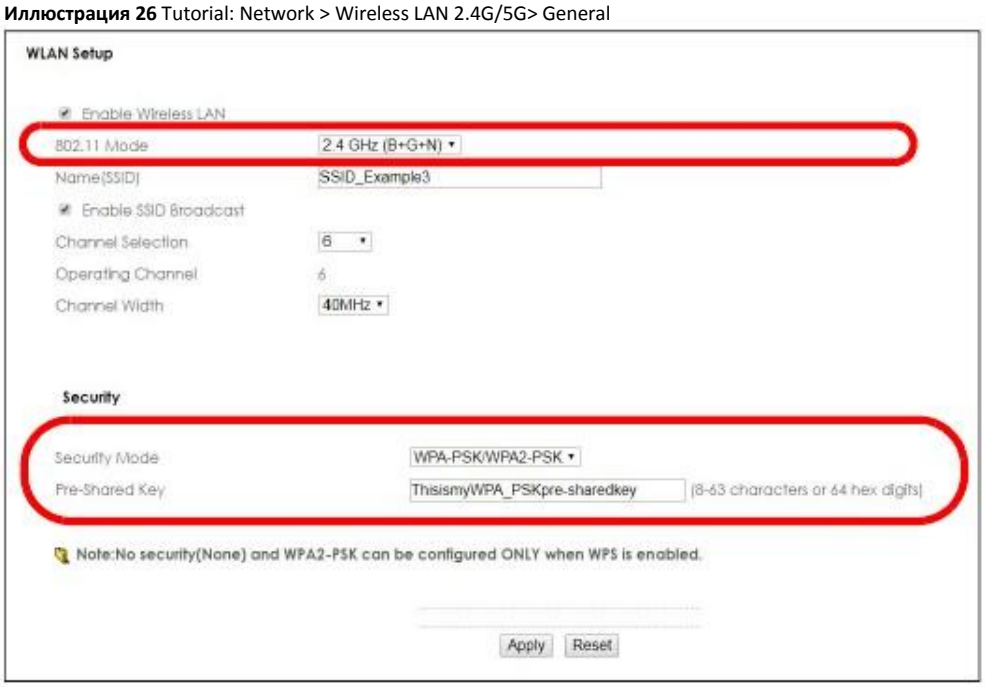
1 Перейдите на экран **Wireless LAN > General** в Web Configurator на NBG6615.

2 Убедитесь, что в поле **Enable Wireless LAN** стоит галочка.

3 Введите **SSID_Example3** как SSID и выберите канал.

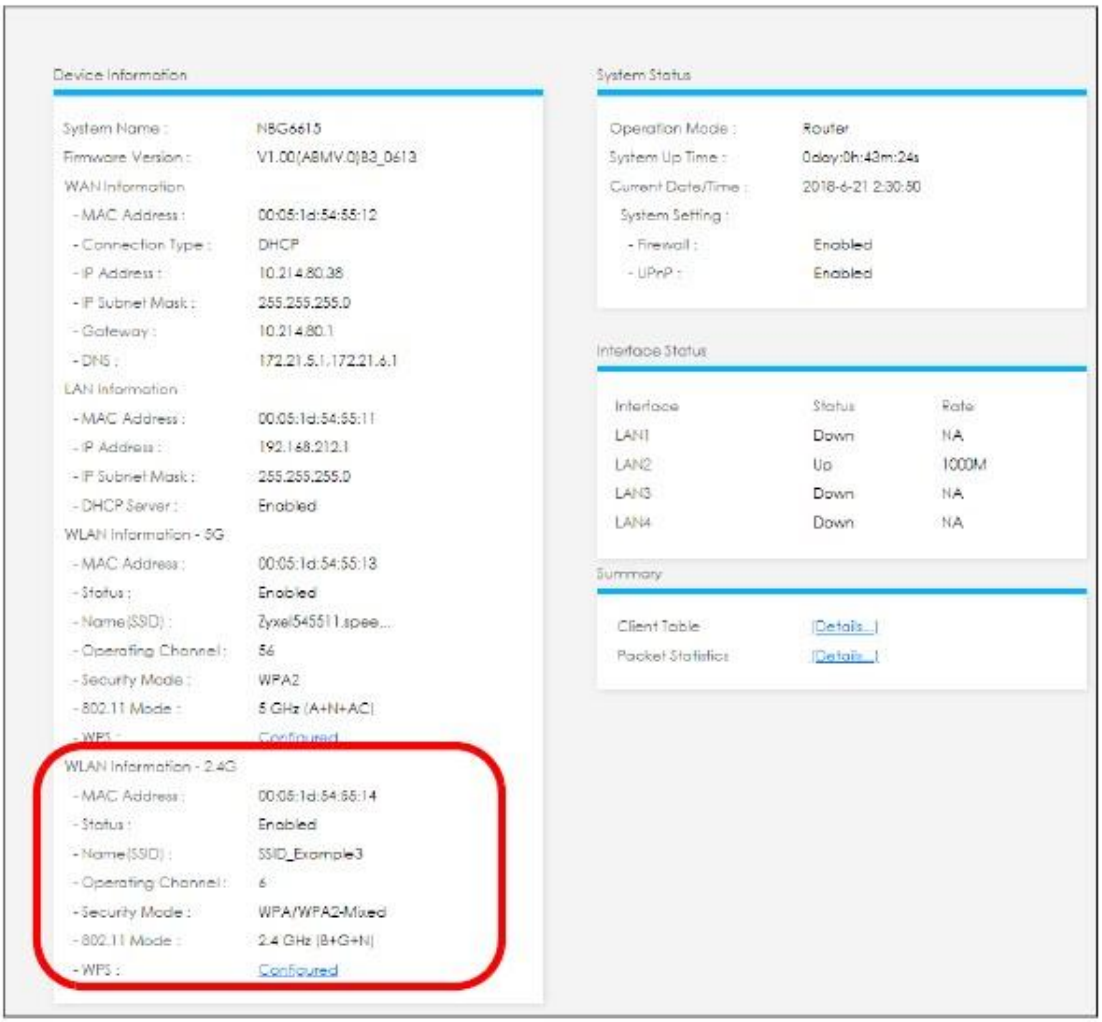
4 Настройте безопасность (Security) на **WPA-PSK/WPA2-PSK** и введите **ThisismyWPA-PSKpre-sharedkey** в поле **Pre-Shared Key**. Щелкните **Apply**.

Иллюстрация 26 Tutorial: Network > Wireless LAN 2.4G/5G> General



5 Откройте экран **Status**. Проверьте настройки беспроводной сети и безопасности в разделе **Device Information** и убедитесь, что в поле **Interface Status** напротив показано, что соединение WLAN работает.

Иллюстрация 27 Tutorial: Status Screen



5.4.1 Настройка конфигурации беспроводного клиента

Примечание: В этом примере показаны экраны утилиты WiFi-адаптера беспроводной сети Zyxel M-302, который установлен на ноутбуке. Для других моделей адаптеров экраны могут отличаться.

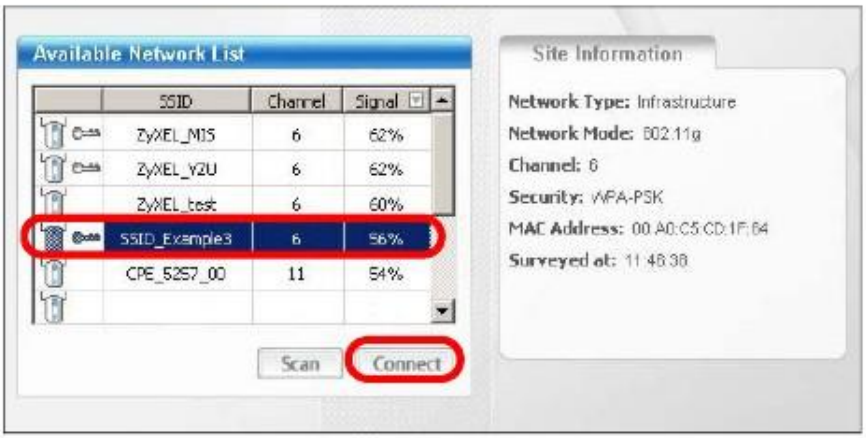
1 NBG6615 поддерживает беспроводные клиенты IEEE 802.11a, IEEE 802.11b, IEEE 802.11g и IEEE 802.11n. Убедитесь, что ваш ноутбук или подключенный к нему адаптер WiFi поддерживает хотя бы один из этих стандартов.

2 Обычно адаптеры WiFi поставляются вместе с программой-утилитой, которую нужно установить на вашем компьютере (см. краткое руководство пользователя, которое входит в комплект поставки адаптера).

3 После инсталляции этой утилиты нужно ее запустить. Если на экране нет пиктограммы это утилиты, то нужно перейти **Start > Programs** найти утилиту в списке программ и щелкнуть по ней. Утилита выводит список обнаруженных адаптером точек доступа (см. пример ниже).

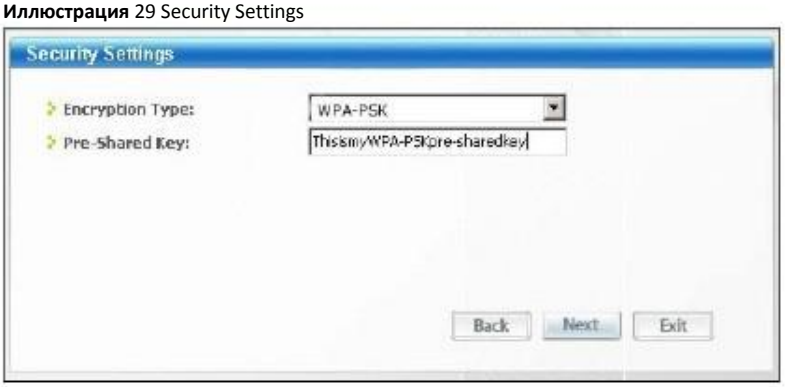
4 Выберите **SSID_Example3** и щелкните **Connect**.

Иллюстрация 28 Подключение беспроводного клиента к беспроводной сети



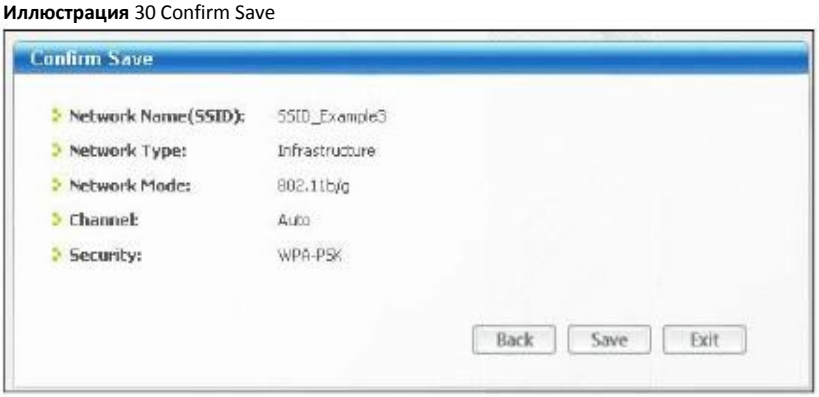
5 Выберите **WPA-PSK** и на следующем экране введите ключ безопасности. Щелкните **Next**.

Иллюстрация 29 Security Settings



6 Откроется окно Confirm Save. Проверьте ваши настройки и щелкните **Save** для продолжения.

Иллюстрация 30 Confirm Save



7 Проверьте состояние беспроводного подключения на следующем экране. Если беспроводному клиенту не удается подключиться к NBG6615, то см. Главу Устранение неисправностей этого «Руководства пользователя».

Иллюстрация 31 Link Status

Если соединение успешно установлено, то откройте браузер и в его адресной строке введите http://www.zyxel.com либо URL другого web-сайта. Если вы сможете подключиться к этому сайту, то это означает, что беспроводное соединение сконфигурировано правильно.

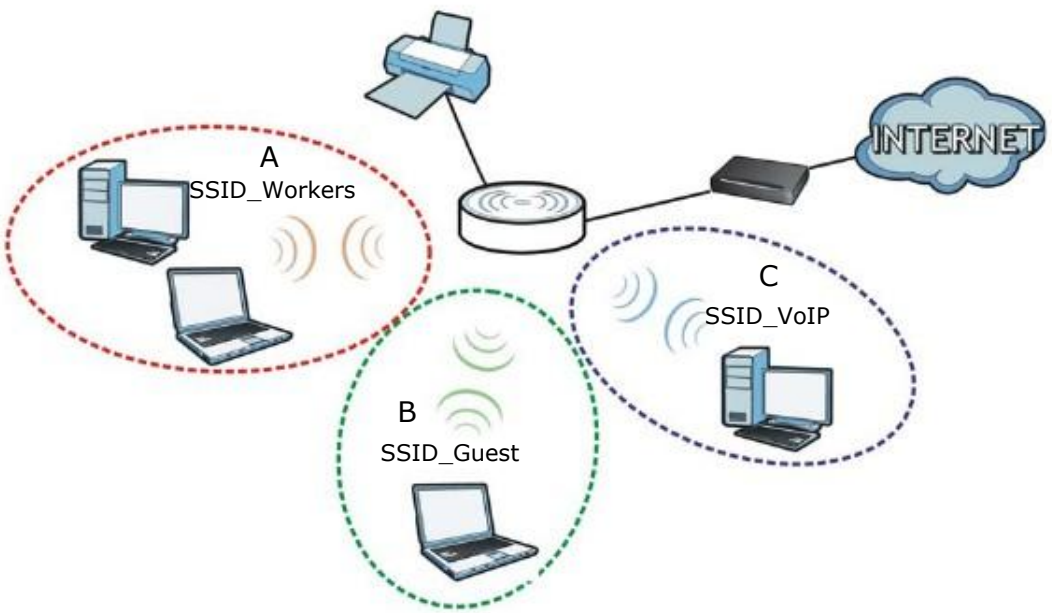
5.5 Использование нескольких SSID на NBG6615

На NBG6615 можно сконфигурировать несколько гостевых SSID (см. Раздел 6.10 на стр. 64).

Благодаря этой функции на базе NBG6615 можно развернуть несколько беспроводных сетей с разными SSID, каждую из которых будет обслуживать отдельная виртуальная точка доступа со своей системой безопасности. Таким образом, каждая SSID в NBG6615 соответствует отдельной точке доступа/беспроводной сети.

Клиенты могут подключиться только к той беспроводной сети, которая соответствует их настройкам безопасности, использующие разные SSID клиенты могут получить доступ к Интернету и к проводной сети, к которой подключено NBG6615 (например, к сетевому принтеру в этой сети).

Например, вы можете развернуть в своем офисе три беспроводные сети **A**, **B** и **C**, и использовать **A** для сотрудников офиса, **B** для посетителей (гостей), а **C** – для установленного в переговорной VoIP-телефона.



5.5.1 Настройка параметров безопасности для нескольких SSID

По умолчанию NBG6615 работает в режиме маршрутизатора.

В следующем примере показывается, как настроить SSID со следующими параметрами NBG6615, который работает в режиме маршрутизатора.

SSID	ТИП БЕЗОПАСНОСТИ	КЛЮЧ
SSID_Workers	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork
SSID_VoIP	WPA-PSK/WPA2-PSK	VoIPOnly12345678
SSID_Guest	WPA-PSK/WPA2-PSK	keyexample123

1 Подключите ваш компьютер к порту LAN на NBG6615 кабелем Ethernet.

2 По умолчанию IP-адрес NBG6615 в режиме маршрутизатора “192.168.1.1” и у вашего компьютера IP-адрес должен быть в диапазоне от “192.168.212.2” и до “192.168.212.254”.

3 На компьютере в Windows выберите **Start > Run** и в диалоговом окне введите “**cmd**”. Чтобы узнать IP-адрес вашего компьютера введите “**ipconfig**”. Если этот IP-адрес вне нужного диапазона, то см. Приложение C на стр. 157 где объясняется как изменить IP-адрес компьютера.

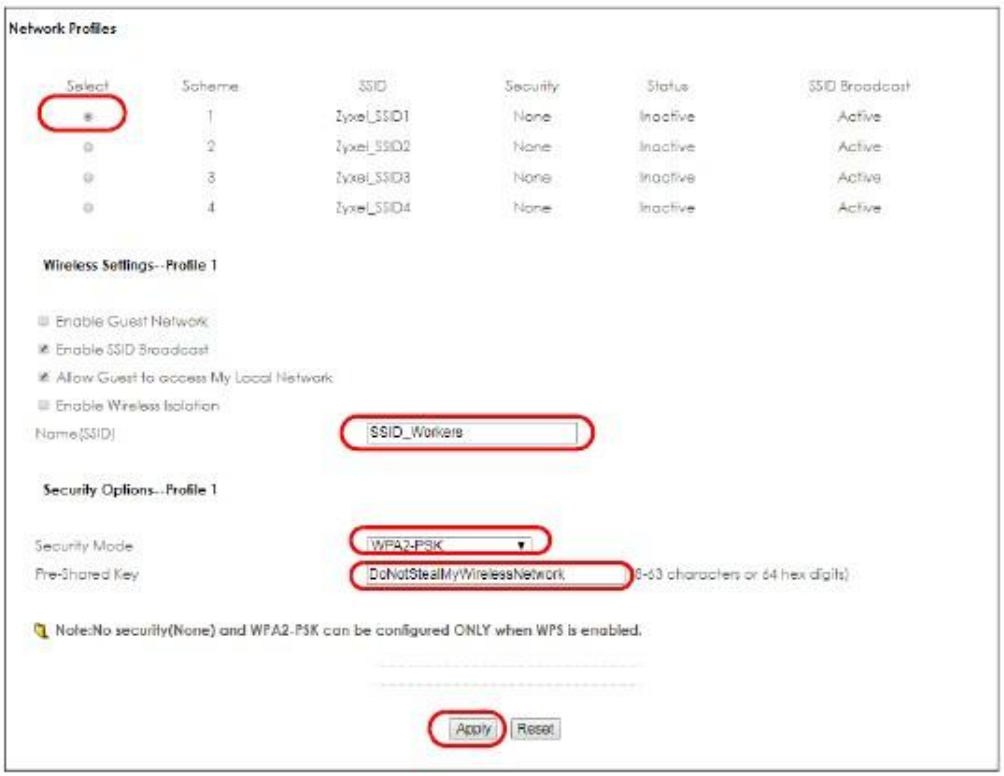
4 После того, как вы правильно настроили IP-адрес вашего компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите “192.168.212.1”.

5 Введите пароль по умолчанию “1234” и щелкните **Login**.

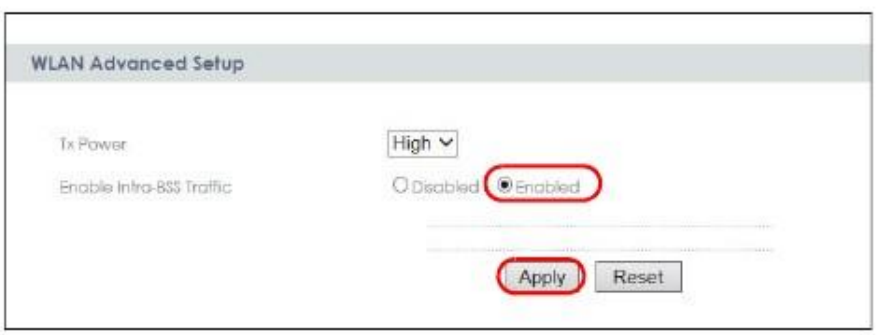
6 Введите новый пароль, затем снова введите его для подтверждения и щелкните **Apply**. Если вы не хотите менять пароль, то щелкните **Ignore**.

7 Откроется окно, в котором нужно выбрать режим Wizard либо Advance. Щелкните **Go to Advanced Setup** в панели навигации.

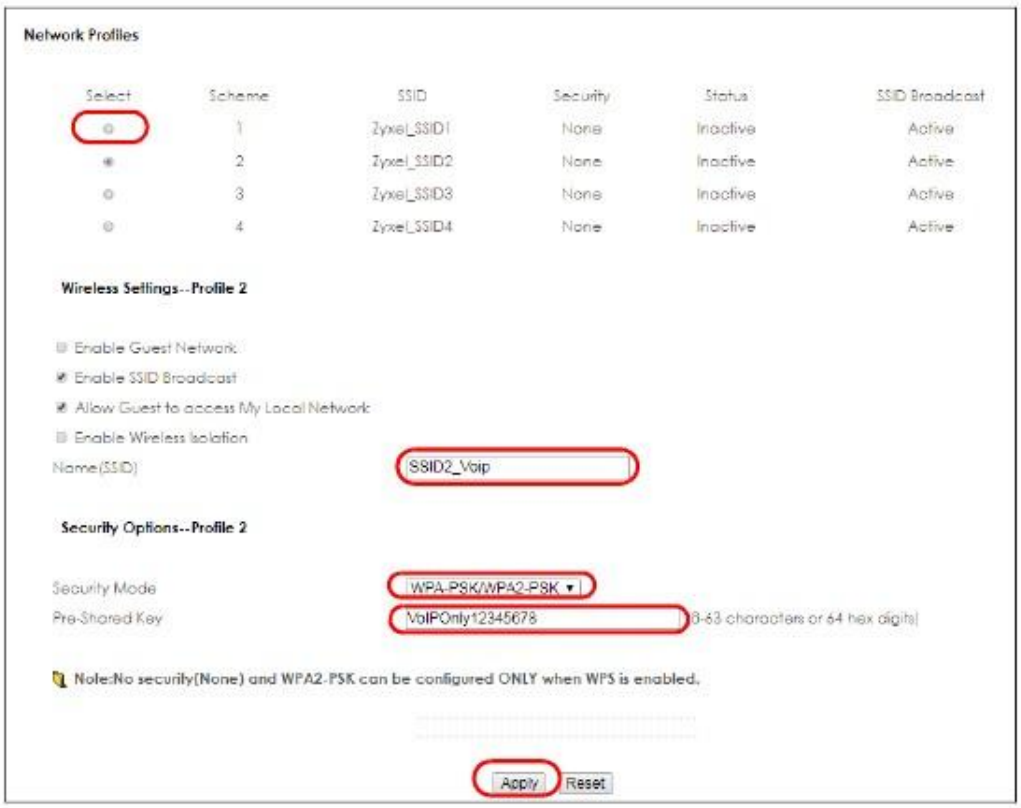
8 Перейдите **Network > Wireless LAN** (2.4G/5G) **> MBSSID**. Введите **SSID_Workers** в поле Name (SSID), выберите **WPA2-PSK** в раскрывающемся списке Security, введите ключ pre-shared key и щелкните **Apply**.



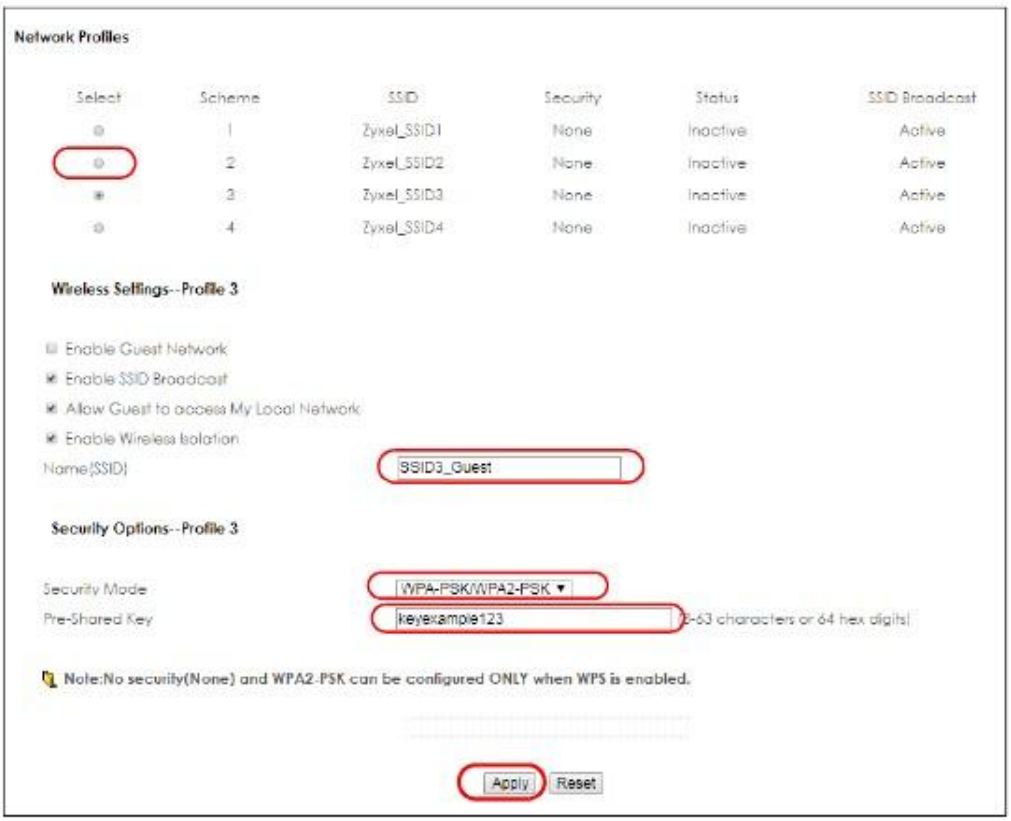
9 Перейдите **Network > Wireless LAN** (2.4G/5G) **> WLAN Advanced Setup** и поставьте галочку в **Intra-BSS Traffic** чтобы находящиеся в одном беспроводной сети беспроводные клиенты могли обмениваться данными между собой. Щелкните **Apply**.



10 Для создания SSID_VoIP перейдите **Network > Wireless LAN** (2.4G/5G)> **MBSSID**. Выберите scheme 2 и введите **SSID_Voip** в поле Name (SSID), выберите **WPA-PSK/WPA2-PSK** в раскрывающемся списке Security, введите ключ **pre-shared key** и щелкните **Apply**.



11 Для создания SSID_ Guest перейдите **Network > Wireless LAN** (2.4G/5G)> **MBSSID**. Выберите scheme 2 и введите **SSID_Guest** в поле Name (SSID), и если вам надо запретить беспроводным клиентам гостевой сети обменивать данными между собой, то щелкните **Enable Wireless Isolation**. Выберите **WPA-PSK/WPA2-PSK** в раскрывающемся списке Security, введите ключ **pre-shared key** и щелкните **Apply**.



5.6 Пример инсталляции UPnP в Windows 7

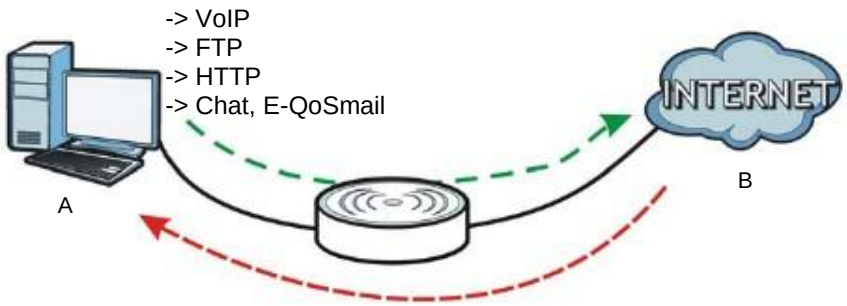
Инструкции по инсталляции Universal Plug and Play на компьютере Windows можно найти в Разделе 16.4 на стр. 110

5.7 Управление полосой пропускания на NBG6615

Управление полосой пропускания (Bandwidth Management) позволяет удобно контролировать использование различных сетевых сервисов. Bandwidth Management используется для управления обычными протоколами (например, HTTP и FTP) и назначает приоритеты трафику для улучшения работы приложений, чувствительных к задержкам, например, связанных с передачей голоса и видео.

На следующей иллюстрации исходящий трафик идет от устройства LAN (**A**) к устройству WAN (**B**). Управление полосой пропускания применяется до того, как пакет попал в WAN. Входящий трафик идет в обратном направлении от устройства WAN (**B)** к устройству LAN (**A**). Управление полосой пропускания применяется до того, как пакет попал в LAN.

Иллюстрация 32 Пример управление полосой пропускания



Можно выделять определенную часть полосы пропускания (бюджет полосы пропускания) определенным приложениям (например, VoIP, Web, FTP и E-mail).

В этом примере Bandwidth Management используется на NBG6615 со следующими параметрами (режим маршрутизатора).

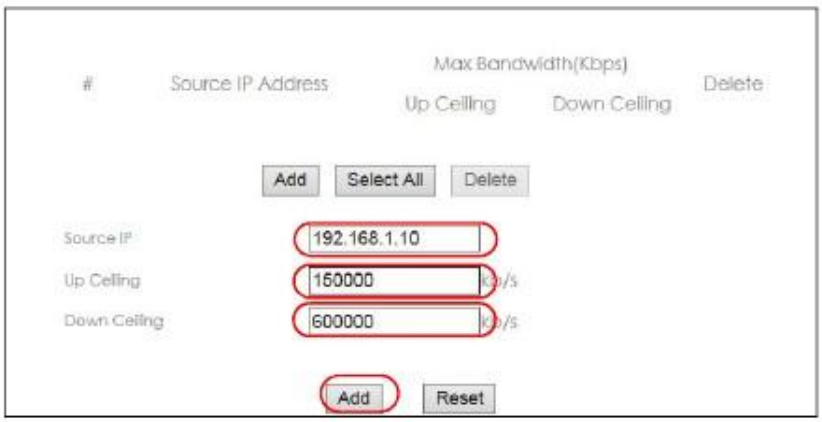
Правило QoS

UP Stream	819200 kpbs
Down Stream	819200 kbps
Source IP	192.168.1.10
Up Ceiling	150000 kb/s
Down Ceiling	600000 kb/s

1 Перейдите в **Management > Bandwidth MGMT > General** и поставьте галочку напротив Enable Bandwidth Management.

2 Перейдите в **Management > Bandwidth MGMT > Advanced** и введите **819200** в поля Total Up Stream и Down Stream Bandwidth в разделе QoS Setup section. Рекомендуется задавать эти значения равными реальной скорости исходящего потока данных. Щелкните **Apply** либо **Reset** чтобы очистить эти поля.

3 Щелкните **Add** в разделе QoS Rules, после чего будет выведено несколько полей. Введите **192.168.1.10** в поле Source IP, затем введите 150000 в поле Up Ceiling и **600000** в поле Down Ceiling и щелкните **Add**. Значения Up/Down Ceiling не могут превышать значение в поле Total Bandwidth. Вы успешно назначили минимальную и максимальную полосу пропускания для определенного IP-адреса.



4 Для удаления правила QoS Rules поставьте галочку напротив правила и щелкните кнопку **Delete**. Для сброса значения полей **Source IP**, **Up/Down Ceiling** щелкните кнопку **Reset**.

Глава II

Техническая информация

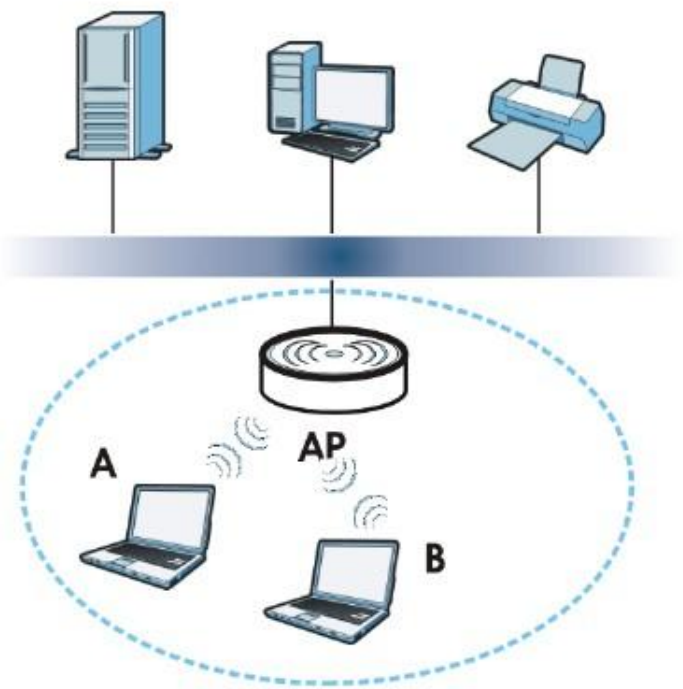
Глава 6 Беспроводная сеть

6.1 Обзор

В этой главе описана настройка параметров беспроводной сети NBG6615. Подробнее о беспроводных сетях см. приложения.

следующей иллюстрации показан пример беспроводной сети.

Иллюстрация 33 Пример беспроводной сети



Беспроводная сеть обведена синей пунктирной линией. Устройства **A** и **B** – это беспроводные клиенты, которые используют точку доступа (AP) для связи с другими устройствами (например, с принтером) и Интернетом. NBG6615 в этом примере работает как точка доступа

6.2 Экраны, которые описаны в этой главе

Режимы работы устройства описаны в Глава 4 на стр. 28.

• Экран **General** для включения беспроводной сети, ввода SSID и выбора режима безопасности беспроводной сети (Раздел 6.4 на стр. 57).

• Экран **MAC Filter** для разрешения или блокировки подключения беспроводных клиентов к NBG6615 на основе их MAC-адреса (Раздел 6.5 на стр. 59).

• Экран **Advanced** для разрешения intra-BSS networking и настройки порогового значения RTS/CTS Threshold (Раздел 6.6 на стр. стр. 60).

• Экран **WPS** для быстрого развертывания беспроводной сети с надежной защитой без настройки вручную параметров безопасности (Раздел 6.7 на стр. 61).

• Экран **WPS Station** для добавления беспроводной станции с помощью WPS (Раздел 6.8 на стр. 63).

• Экран **Scheduling** для настройки расписания включения и отключения беспроводной сети (Раздел 6.9 на стр. 63).

• Экран **MBSSID** для настройки нескольких беспроводных сетей на NBG6615 (Раздел 6.10 на стр. 64).

6.3 Основные сведения

При использовании беспроводной сети необходимо соблюдать следующие основные требования:

• У всех клиентов одной беспроводной сети должен быть одинаковый SSID.

SSID (Service Set IDentifier) – это имя беспроводной сети.

• Если зоны покрытия двух беспроводных сетей перекрываются, то эти сети должны использовать разные каналы.

Также, как и радиостанции и телевизионные каналы, каждая беспроводная сеть использует определенный канал (частоту) для обмена данными.

• Каждое устройство одной беспроводной сети должно использовать систему безопасности, совместимую с точкой доступа этой беспроводной сети.

Система безопасности блокирует использование беспроводной сети неавторизованными устройствами, а также защищает от неавторизованного доступа пересылаемую по беспроводной сети информацию.

6.3.1 Обзор безопасности беспроводной сети

В следующих разделах описаны разные типы системы безопасности беспроводной сети, которые вы можете применять для защиты своей сети.

6.3.2 MBSSID

Обычно для настройки разных Basic Service Set (BSS) нужно использовать несколько точек доступа, однако это ведет к дополнительным затратам на оборудование и увеличивает риск, что каналы будут мешать друг другу. Применяемая в NBG6615 функция MBSSID (Multiple Basic Service Set IDentifier) позволяет с помощью одной точки доступа развернуть одновременно несколько BSS и назначать разным SSID разные типы безопасности. Беспроводные устройства смогут подключиться к одной и той же точке доступа, пользуясь разными BSSID.

6.3.2.1 Примечание о Multiple BSSs

• Одновременно одна точка доступа может обслуживать максимум восемь BSS.

• Для разных BSS нужно использовать разные ключи. Если у двух беспроводных устройств разные BSSID (они подключены к разными BSS), но одинаковые ключи, то они могут перехватывать обмен данными друг друга, хотя и не могут обмениваться данными между собой).

• MBSSID рекомендуется использовать вместе с протоколом безопасности 802.1x.

6.3.3 Фильтр MAC-адресов

У каждого устройства беспроводной сети есть уникальный идентификационный номер – MAC-адрес[1], который обычно состоит из 12 шестнадцатеричных цифр[2], например, 00A0C5000002 или 00:A0:C5:00:00:02. MAC-адрес устройств обычно указывается в их руководстве пользователя или другой документации.

С помощью фильтра MAC-адресов можно разрешить одним устройствами использовать беспроводную сеть, а другим - запретить. Если устройству разрешено использовать беспроводную сеть, оно должно знать SSID сети, канал и используемый в ней стандарт безопасности для доступа к сети. Если клиенту запрещен доступ к беспроводной сети, то оно не сможет подключиться к ней даже если у него правильно настроены параметры сети.

Этот тип безопасности не защищает информацию, пересылаемую по беспроводной сети. Кроме того, есть способы, с помощью которых неавторизованные устройства могут получить MAC-адрес авторизованного устройства и использовать его для доступа к беспроводной сети.

6.3.4 Шифрование

Для защиты информации, пересылаемой по беспроводной сети, можно использовать шифрование. При использовании шифрования для расшифровки пересылаемой информации требуется секретный код.

Таблица 12 Типы шифрования и аутентификации

	БЕЗ АУТЕНТИФИКАЦИИ
Слабее	No Security
↕	
	WPA-PSK/WPA2-PSK
Сильнее	WPA2-PSK

Если пользователи не проходят процедуру регистрации login для входа в беспроводную сеть, то можно выбрать **no encryption, WPA2-PSK** или **WPA-PSK/WPA2-PSK**.

Рекомендуется использовать самое сильный тип шифрования из тех, которые поддерживает беспроводное устройство, например, если у вас устаревшие клиентские устройства не поддерживают **WPA2-PSK**, то выберите **WPA-PSK/WPA2-PSK** чтобы новые устройства могли использовать **WPA2-PSK**, а устаревшие - **WPA-PSK**.

Чем длиннее ключ шифрования, тем надежнее защита информации. Все устройства одной беспроводной сети должны иметь один и тот же ключ шифрования.

6.3.5 WPS

WiFi Protected Setup (WPS) является промышленным стандартом и разработан альянсом WiFi Alliance. С помощью WPS вы сможете без задания настроек безопасности вручную быстро развернуть сеть WiFi с надежной системой безопасности. В зависимости от конкретного устройства можно нажать кнопку (на самом устройстве либо в утилите конфигурирования) либо ввести PIN-код (уникальный идентификатор устройства Personal Identification Number) на обоих устройствах, после чего между ними будет установлено защищенное беспроводное соединение. Настройка защищенной беспроводной сети с помощью WPS описана в Разделе 5.3 на стр. 39.

1. Некоторые беспроводные устройства (например, сканеры) могут обнаружить беспроводную сеть, но не могут ее использовать. У таких устройств может отсутствовать MAC-адрес.
2. Шестнадцатеричные цифры - это 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E и F.

6.4 Экран General

Этот экран используется для включения беспроводной сети, настройки SSID и выбора режима безопасности.

Примечание: Если вы настраиваете NBG6615 с устройства, которое подключено к беспроводной сети, и вы изменили у NBG6615 идентификатор SSID, настройки канала или безопасности, то беспроводное соединение с NBG6615 будет разорвано сразу после того, как вы нажмете **Apply** для подтверждения изменений. Для повторного соединения измените настройки беспроводного соединения вашего устройства в соответствии с новыми настройками NBG6615.

Щелкните **Network > Wireless LAN** (2.4G/5G) чтобы открыть экран **General**.

Иллюстрация 34 Network > Wireless LAN (2.4G/5G) > General (режим маршрутизатора или точки доступа)

В следующей таблице описаны поля основных настроек беспроводной сети этого экрана.

Таблица 13 Network > Wireless LAN > General

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN	Поставьте галочку чтобы включить беспроводную сеть.
802.11 Mode	Выберите режим 802.11 из раскрывающегося списка.
Name (SSID)	Введите имя SSID (Service Set Identity), идентифицирующее набор сервисов Service Set, которые доступны для беспроводного клиента. Имя беспроводной сети состоит из максимум 32 семибитных символов ASCII.
Enable SSID Broadcast	Поставьте галочку напротив **Enable SSID Broadcast** чтобы SSID передавался в заголовке исходящих пакетов. В результате SSID вашей беспроводной сети можно будет определить сканированием с помощью утилит для обследования беспроводной среды.

Таблица 13 Network > Wireless LAN > General (продолжение)

ПОЛЕ	ОПИСАНИЕ
Channel Selection	Выберите рабочую частоту/канал из раскрывающегося списка. Эта опция зависит от частотного диапазона страны, в которой вы находитесь. Если выбрать **Auto**, то NBG6615 автоматически выберет канал, где меньше всего помех.
Operating Channel	Канал, который сейчас использует NBG6615.
Channel Width	Выбор ширины канала, который будет использовать NBG6615 - 20MHz, 40MHz или (доступно для 5GHz) 80MHz. Стандартный канал шириной 20MHz обеспечивают скорость передачи данных до 150Mbps, а канал шириной 40MHz использует два стандартных канала и обеспечивают скорость передачи данных до 300Mbps. Если выбрать **Auto**, то NBG6615 будет автоматически подстраивать ширину каналу с учетом условий работы сети. Выберите **20MHz** если там, где вы развертываете сеть с беспроводными клиентами 2.4G, много других беспроводных клиентов. Выберите **40MHz** если ваши беспроводные клиенты 2.4G поддерживают channel bonding. Выберите **80MHz** если ваши беспроводные клиенты 5G поддерживают channel bonding.
Security Mode	Тип безопасности, используемый в беспроводном устройстве, к которому вы подключаетесь.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

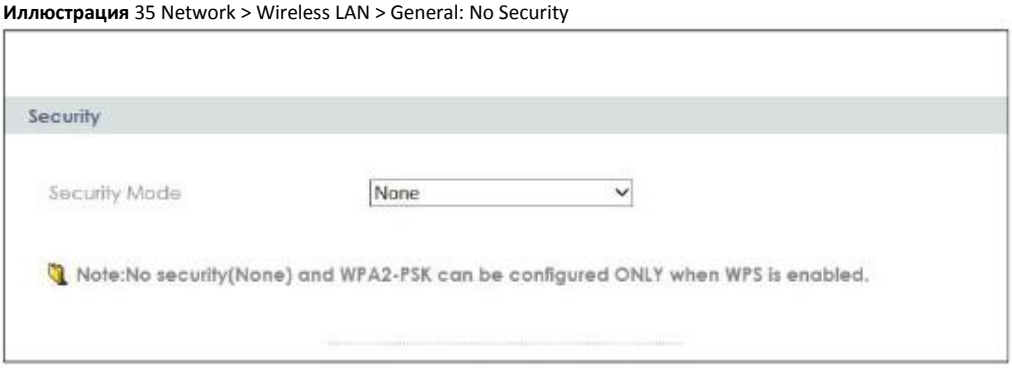
Другие поля этого экрана описаны далее в этой главе.

6.4.1 No Security

Если выбрать **No Security**, то беспроводные клиенты смогут обмениваться данными с точкой доступа без использования шифрования.

Примечание: Если на вашем NBG6615 не включена система безопасности, то к вашей сети сможет подключиться любой беспроводной клиент в зоне покрытия NBG6615.

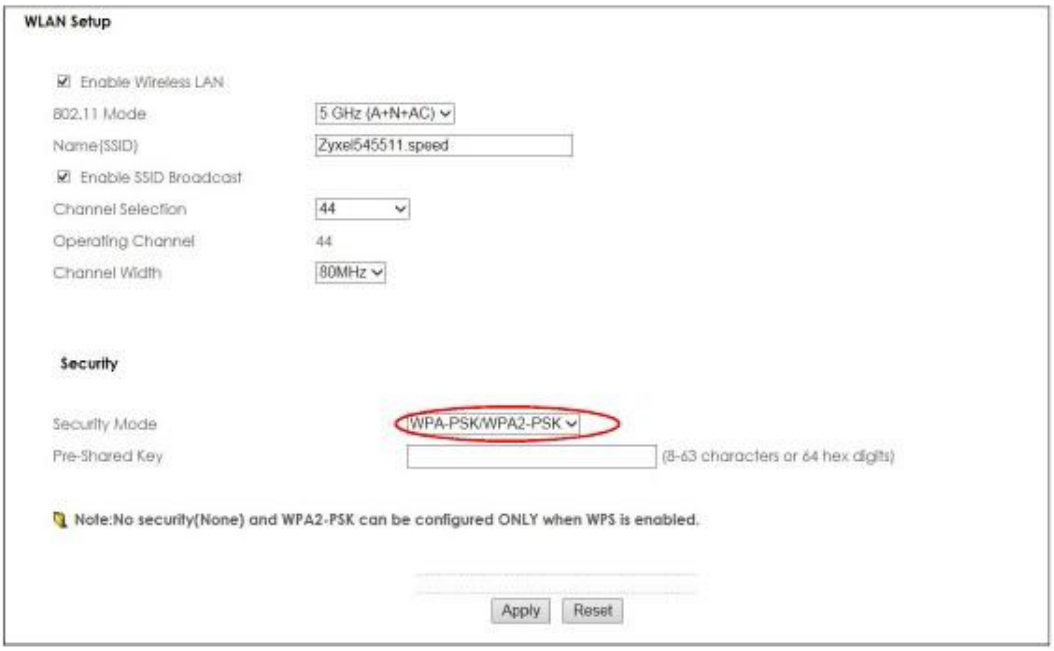
Иллюстрация 35 Network > Wireless LAN > General: No Security



6.4.2 WPA2-PSK или WPA-PSK/WPA2-PSK

Щелкните **Network > Wireless LAN** (2.4G/5G) для перехода на экран General. Из списка Security Mode выберите **WPA2-PSK** или **WPA-PSK/WPA2-PSK**.

Иллюстрация 36 Network > Wireless LAN > General: WPA2-PSK or WPA-PSK/WPA2-PSK



В следующей таблице описаны поля этого экрана.

Таблица 14 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **WPA-PSK** или **WPA-PSK/WPA2-PSK** из раскрывающегося списка. Выберите **WPA-PSK/WPA2-PSK** чтобы с NBG6615 могли обмениваться данные беспроводные клиенты как WPA2, так и WPA даже если NBG6615 использует WPA2-PSK.
Pre-Shared Key	**WPA2-PSK** и **WPA-PSK/WPA2-PSK** используют для аутентификации простой обычный пароль. Введите ключ pre-shared key, который может состоять из 8 - 63 символов ASCII (включая пробелы и символы, регистр букв учитывается) или 64 шестнадцатеричных символа (“0-9,” “A-F”).
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.5 MAC Filter

Экран **MAC filter** позволяет разрешать доступ к NBG6615 определенным устройствам (**Allow**) либо блокировать их доступ к NBG6615 (**Deny**). У каждого устройства Ethernet есть уникальный адрес MAC (Media Access Control), который назначается на заводе и состоит из шести шестнадцатеричных цифр, например, 00:A0:C5:00:00:02. MAC-адрес устройства необходим для конфигурирования этого экрана.

Для изменения настроек фильтра MAC-адресов вашего NBG6615 щелкните **Network > Wireless LAN** (2.4G/5G) **> MAC Filter**. Откроется следующий экран.

Иллюстрация 37 Network > Wireless LAN (2.4G/5G)> MAC Filter

В следующей таблице описаны поля этого экрана.

Таблица 15 Network > Wireless LAN > MAC Filter

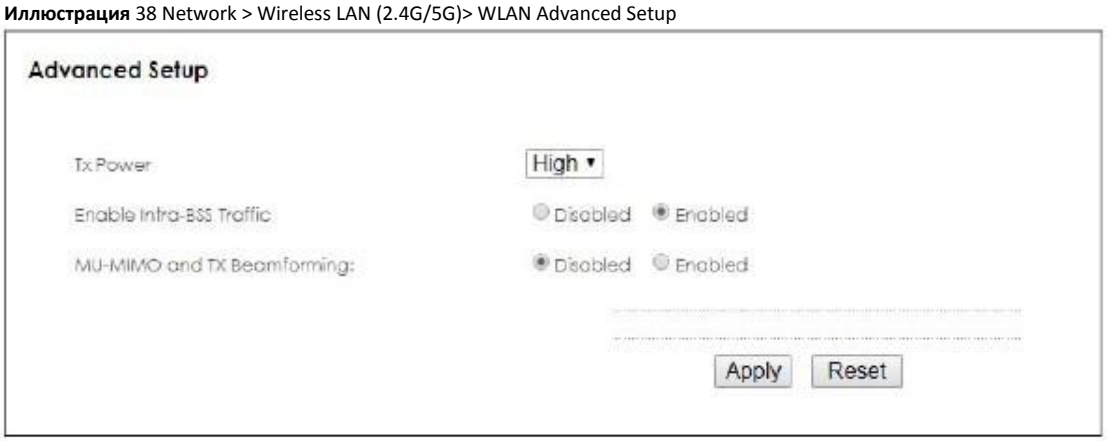
ПОЛЕ	ОПИСАНИЕ
Wireless Active Control Mode	В раскрывающемся списке выберите **Allow Listed** чтобы включить режим whitelist, при котором доступ к беспроводной сети разрешен только для MAC-адресов из белого списка. Если выбрать **Deny Listed** , то будет использоваться режим blacklist, при котором к беспроводной сети не могут получить доступ MAC-адреса из черного списка. Если выбрить **Disable**, то фильтр MAC-адресов будет отключен.
MAC Address	Введите MAC-адрес для внесения в белый и черный список в стандартном формате (6 пар шестнадцатеричных цифр, например, 12:34:56:78:9a:8c). Двоеточия вводить не надо.
Comment	В это поле можно добавить комментарии к MAC-адресам из белого и черного списка.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.6 Экран Wireless LAN Advanced

Этот экран предназначен для разрешения intra-BSS networking и настройки порогового значения RTS/CTS.

Щелкните **Network > Wireless LAN** (2.4G/5G)**> WLAN Advanced Setup**. Откроется следующий экран.

Иллюстрация 38 Network > Wireless LAN (2.4G/5G)> WLAN Advanced Setup



В следующей таблице описаны поля этого экрана.

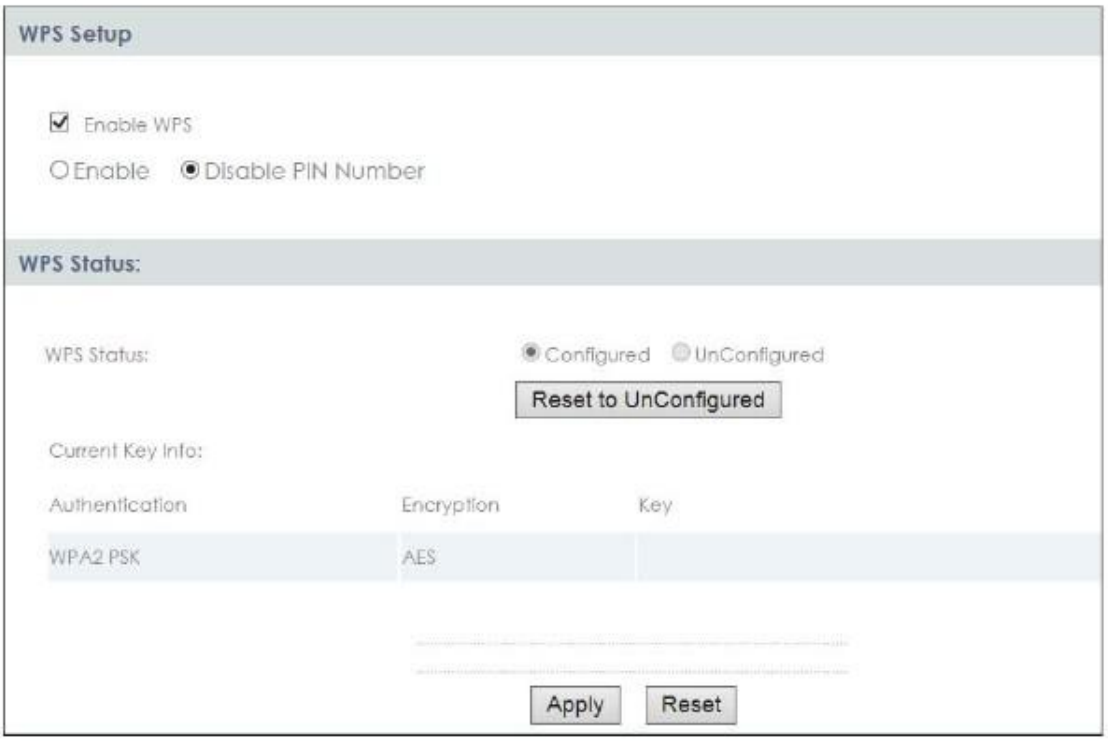
Таблица 16 Network > Wireless LAN (2.4G/5G)> WLAN Advanced Setup

ПОЛЕ	ОПИСАНИЕ
Tx Power	Мощность сигнала на выходе NBG6615. Если рядом с NBG6615 работают другие точки доступа, то нужно уменьшить этот параметр для сокращения помех от других точек доступа.
Enable Intra-BSS Traffic	Basic Service Set (BSS) существует если весь обмен данными между беспроводными клиентами или между ними и проводной сетью идет через одну точку доступа (AP). Трафик Intra-BSS – это трафик между беспроводными клиентами в BSS. Если Intra-BSS включен, то беспроводные клиенты могут обмениваться данными между собой через точку доступа и у них есть доступ к проводной сети, а если отключен, то у них есть доступ к проводной сети, но они не могут обмениваться данными между собой через точку доступа.
MU-MIMO and TX Beamforming	Выберите **Enabled** чтобы включить Multi User-MIMO и Transmit Beamforming для улучшения работы в сети WiFi поддерживающих MU MIMO беспроводных устройств. При использовании Multi User-MIMO несколько беспроводных клиентов могут одновременно обмениваться данными с NBG6615, при этом полоса пропускания распределяется равномерно между всеми беспроводными клиентами, поддерживающими MIMO, и они получают стабильный сигнал WiFI. При использовании Transmit Beamforming сигнал NBG6615 фокусируется на беспроводных клиентах для улучшения покрытия и устранения мертвых зон беспроводной сети.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.7 Экран WPS

С помощью этого экрана можно включить/отключить WPS, просмотреть или генерировать новый код PIN и проверить текущее состояния WPS. Для перехода на этот экран щелкните **Network > Wireless LAN** 2.5G/5G**> WPS**.

Иллюстрация 39 Network > Wireless LAN (2.4G/5G)> WPS



В следующей таблице описаны поля этого экрана.

Таблица 17 Network > Wireless LAN (2.4G/5G)> WPS

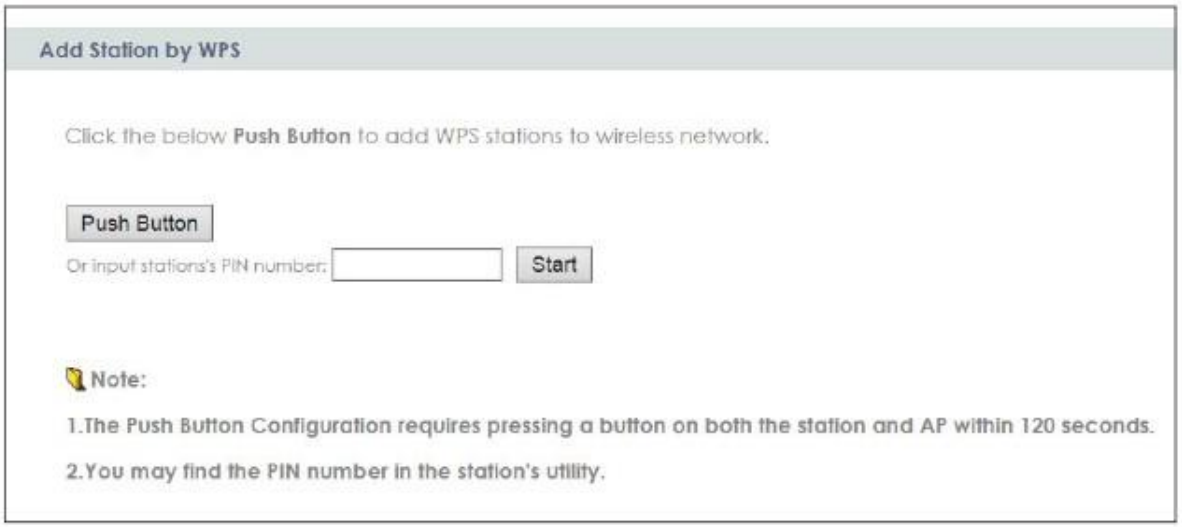
ПОЛЕ	ОПИСАНИЕ
WPS Setup	
Enable WPS	Поставьте галочку напротив **Enable WPS** чтобы включить функцию WPS.
PIN Number	Текущий PIN-код. Щелкните **Generate** чтобы сгенерировать новый PIN-код.
WPS Status	
WPS Status	В этом поле стоит **Configured** если NBG6615 подключена к беспроводной сети с помощью WPS либо если выбран **WPS Enable** и изменены настройки для беспроводной сети или безопасности беспроводной сети. Также на экране будут показаны текущие настройки для беспроводной сети или безопасности беспроводной сети. В этом поле стоит **Unconfigured** если функция WPS отключена и не было никаких изменений настроек беспроводной сети или безопасности беспроводной сети на NBG6615 либо вы щелкнули **Reset to Unconfigured** чтобы удалить все настройки для беспроводной сети и безопасности беспроводной сети.
Reset to Unconfigured	Эта кнопка работает только когда в поле WPS status стоит **Configured**. Щелкните эту кнопку чтобы удалить все настройки NBG6615 для беспроводной сети и безопасности беспроводной сети при соединении с помощью WPS.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Refresh	Щелкните **Refresh** чтобы обновить информацию на этом экране.

6.8 Экран WPS Station Screen

Этот экран предназначен для добавления беспроводной станции с помощью WPS. Для перехода к этому экрану щелкните **Network > Wireless LAN** (2.4G/5G)**> WPS Station**.

Примечание: После нажатия Push Button на этом экран нужно в течение 2 минут нажать аналогичную кнопку в утилите беспроводной станции. Для добавления второй беспроводной станции снова нажмите эти кнопки на обоих устройствах и беспроводной станции после окончанию первых 2 минут.

Иллюстрация 40 Network > Wireless LAN (2.4G/5G)> WPS Station



В следующей таблице описаны поля этого экрана.

Таблица 18 Network > Wireless LAN (2.4G/5G) > WPS Station

ПОЛЕ	ОПИСАНИЕ
Push Button	Эта кнопка предназначена только для настройки параметров беспроводной сети беспроводного клиента с помощью PBC (Push Button Configuration). См. Раздел 5.3.1 на стр. 40. Щелкните эту кнопку чтобы поддерживающий WPS беспроводной клиент начал сканирование и синхронизацию параметров безопасности беспроводной сети.
Or input station's PIN number	Используйте эту кнопку если вы настраивает параметры беспроводной сети на беспроводном клиенте с помощью метода PIN Configuration. См. Раздел 5.3.2 на стр. 41. Введите PIN-код, который выдала утилита беспроводного клиента, затем щелкните **Start** чтобы он подключился с NBG6615 и оба устройства синхронизировал настройки безопасности беспроводной сети.

6.9 Экран Scheduling

Этот экран предназначен для составления расписания включения и выключения беспроводной сети. По умолчанию функция включения и выключения беспроводной сети по расписанию Wireless LAN Scheduling отключена. В расписании можно задавать, в какие дни и в какое время будет включаться/выключаться беспроводная сеть. Для перехода к этому экрану щелкните **Network > Wireless LAN** (2.4G/5G) **> Scheduling**.

Иллюстрация 41 Network > Wireless LAN (2.4G/5G)> Scheduling

В следующей таблице описаны поля этого экрана.

Таблица 19 Network > Wireless LAN (2.4G/5G)> Scheduling

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN Scheduling	Поставьте галочку чтобы включить функцию Wireless LAN scheduling.
Enable	Поставьте галочку чтобы включить Wireless LAN для определенного дня и времени, которые указаны в поле Day и From/To.
Day	Если выбрать **Everyday**, то беспроводная сеть будет работать все дни недели и нельзя выбрать день недели в поле Day. Время суток, когда будет работать беспроводная сеть, назначается в поле From/To.
From/To	Время включения беспроводной сети (час и минута) назначается в первой группе раскрывающихся списков **hour** и **min**, а время выключения беспроводной сети– во второй группе раскрывающихся списков **hour** и **min**. Если время включения и выключения беспроводной сети совпадают, то сеть работает весь день.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.10 Экран MBSSID

Этот экран используется для включения на функции Multiple SSID (MBSSID) на NBG6615 и ее настройки. Можно назначить разные типы безопасности разным SSID. Беспроводные клиенты могут подключаться к NBG6615 по разным SSID. Для перехода на следующий экран щелкните **Click Network > Wireless LAN > MBSSID**.

Иллюстрация 42 Network > Wireless LAN (2.5G/5G)> MBSSID

В следующей таблице описаны поля этого экрана.

Таблица 20 Network > Wireless LAN (2.4G/5G)> MBSSID

ПОЛЕ	ОПИСАНИЕ
Network Profiles	
Select	Выбор идентификатора Multiple Basic Service Set Identifier (MBSSID) для редактирования.
Scheme	Номер по порядку SSID.
SSID	Имя SSID беспроводного клиента.
Security	Режим безопасности беспроводного клиента. Если нет безопасности, то **None**.
Status	Это поле показывает, можно ли использовать выбор **Enable Guest Network**.
SSID Broadcast	Это поле показывает, можно ли использовать выбор **Enable SSID Broadcast** для SSID.
Wireless Settings--Profile 1	
Enable Guest Network	Поставьте галочку в **Enable Guest Network** чтобы включить этот SSID.
Enable SSID Broadcast	Поставьте галочку в **Enable SSID Broadcast** чтобы включить трансляцию SSID Broadcast на разные беспроводные клиенты.
Allow Guest to access My Local Network	Поставьте галочку в **Allow Guest to access my Local Network** чтобы у клиентов был доступ через NBG6615 к локальным сетевым ресурсам.
Enable Wireless Isolation	Поставьте галочку в **Enable Wireless Isolation** чтобы заблокировать для беспроводных клиентов, подключенных к этому SSID, обмен данными между собой через NBG6615.
Name (SSID)	Имя выбранного SSID.
Security Options--Profile1	

Таблица 20 Network > Wireless LAN (2.4G/5G)> MBSSID

ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **WPA2-PSK или WPA-PSK/WPA2-PSK** чтобы обеспечить безопасность вашей беспроводной сети. В этом случае к беспроводной сети смогут подключиться только те беспроводные клиенты, у которых такие настройки безопасности, как у NBG6615. После выбора этой опции на экране будут доступны дополнительные опции. Если выбрать **No Security**, то любой клиент сможет подключаться к беспроводной сети без аутентификации. Подробнее см. Раздел 6.4 на стр. 57.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

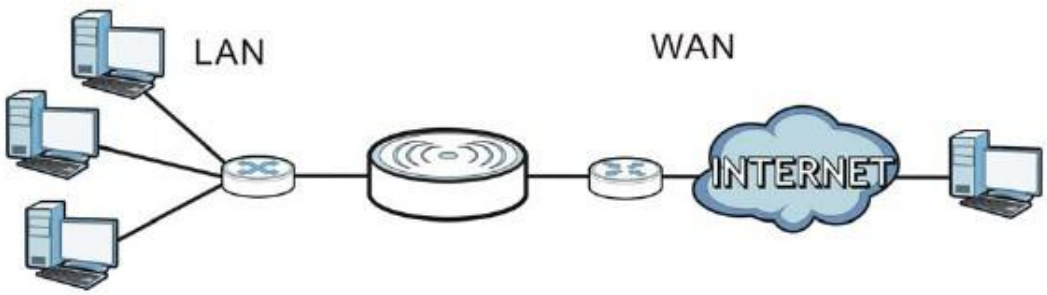
Глава 7
WAN

7.1 Обзор

В этой главе описываются экраны **WAN**, которые используются для настройки доступа NBG6615 к Интернету.

А Соединение WAN (Wide Area Network) – это соединение вашей локальной сети LAN (Local Area Network) с другой сетью или Интернетом, с помощью которого компьютеры вашей LAN могут обмениваться данными с компьютерами, которые находятся в другом месте.

Иллюстрация 43 LAN и WAN



В главе о визарде соединения описаны поля экранов WAN.

7.2 Какие экраны описаны в этой главе

В этой главе объясняется, как настроить экраны для соединения WAN и включить/отключить некоторые дополнительные функции NBG6615.

7.2.1 Конфигурирование соединения с Интернетом

Метод инкапсуляции

При инкапсуляции данные из пакета верхнего уровня вкладываются (инкапсулируются) в пакет нижнего уровня. Для настройки соединения WAN с Интернетом нужно использовать тот же метод инкапсуляции, который использует ваш Интернет-провайдер. Если он применяет коммутируемое подключение к Интернету с помощью PPPoE (PPP over Ethernet) или PPTP (Point-to-Point Tunneling Protocol), то он должен предоставить вам имя пользователя и пароль для аутентификации пользователя.

IP-адрес WAN

адрес WAN – это IP-адрес вашего NBG6615, по которому к нему можно обращаться из внешней сети. NBG6615 использует этот адрес при обмене данными с компьютерами из других сетей. IP-адрес WAN может быть статичным (фиксированным) либо динамичным, и тогда при каждом подключении NBG6615 Интернет-провайдер присваивает ему новый IP-адрес WAN.

Если Интернет-провайдер назначает статичный IP-адрес WAN, то он должен сообщить вам и маску подсети и IP-адрес(а) DNS-сервера (и IP-адрес шлюза если использует метод инкапсуляции Ethernet (ENET ENCAP)).

Получение адреса DNS-сервера

Система Domain Name System (DNS) обеспечивает соответствие между именем домена и IP-адресом, например, имени домена www.zyxel.com соответствует IP-адрес 204.217.0.2. Без использования DNS-сервера вы можете обращаться к компьютеру только по его IP-адресу.

NBG6615 может получить адрес DNS-сервера двумя способами:

1 Вы можете узнать адрес DNS-сервера у вашего Интернет-провайдера и вручную ввести этот адрес в поле DNS Server.

2 Если ваш Интернет-провайдер динамически назначает IP-адрес DNS-серверу вместе с IP-адресом WAN вашего NBG6615), то в поле DNS server нужно задать получение адреса DNS-сервер от Интернет-провайдера.

MAC-адрес WAN

На экране MAC address можно настроить MAC-адрес порта WAN, используя настройки по умолчанию либо клонируя MAC-адрес компьютера в вашей LAN. Выберите **Factory Default** что использовать заводской MAC-адрес по умолчанию.

Если вы не хотите использовать адрес по умолчанию, то выберите **Clone the computer's MAC address - IP Address** и введите IP-адрес компьютера в вашей LAN, чей MAC-адрес вы клонирует. После завершения настройки адрес будет скопирован в конфигурационный файл. Рекомендуем клонировать MAC-адрес до подключения порта WAN.

7.3 Экраны Internet Connection

С помощью этого экрана можно изменить настройки доступа к Интернету вашего NBG6615. Щелкните **Network > WAN**. Поля экрана зависят от выбранного типа соединения.

7.3.1 Экран Static IP

Этот экран выводится при выборе Static IP.

Иллюстрация 44 Network > WAN > Internet Connection: Static IP

В следующей таблице описаны поля этого экрана.

Таблица 21 Network > WAN > Internet Connection: Static IP

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access (Static IP)	
Connection Type	Выберите **Static IP** если порт WAN – это стандартный порт Ethernet.
IP Address	В это поле нужно ввести IP-адрес WAN.
Subnet Mask	В это поле нужно ввести маску подсети.
Default Gateway	IP-адрес шлюза, который вам должен сообщить ваш Интернет-провайдер.
MTU Size	Размер пакета MTU (Maximum Transmission Unit), которые могут передаваться через этот интерфейс. Пакеты больше этого размера NBG6615 будет разбивать на несколько пакетов. Допустимые значения - от 576 до 1500, по умолчанию 1500.
First DNS Server Second DNS Server	Введите IP-адреса первого и второго сервера DNS.
WAN MAC Address В разделе MAC можно задать MAC-адрес порта WAN. Можно использовать MAC-адрес NBG6615, копируя MAC-адрес компьютера в вашей локальной сети либо вручную введя MAC-адрес.	
Factory default	Выберите эту опцию чтобы интерфейс WAN использовал заводской MAC-адрес по умолчанию.

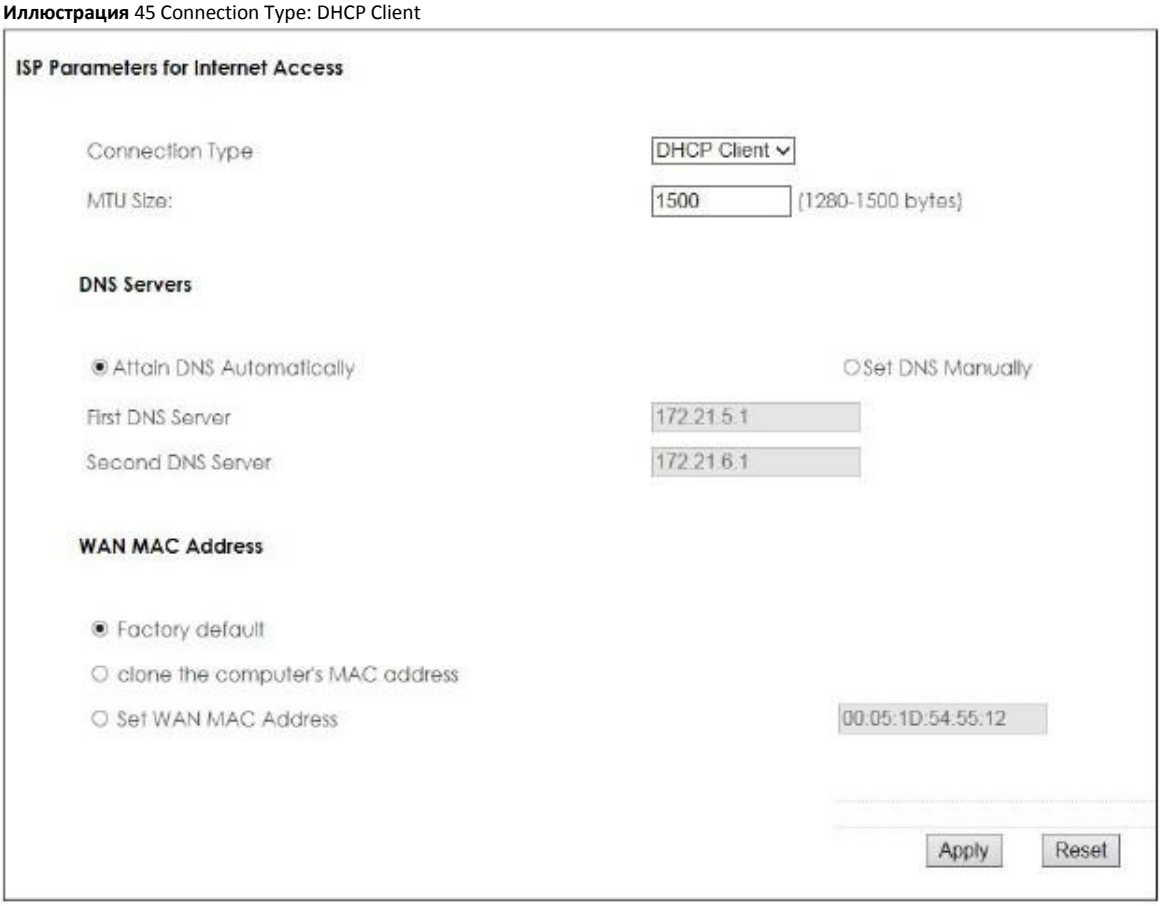
Таблица 21 Network > WAN > Internet Connection: Static IP

ПОЛЕ	ОПИСАНИЕ
Clone the computer's MAC address - MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал другой MAC-адрес, который является копией (клоном) MAC-адреса компьютера, с которого вы настраиваете устройство (он отображается на экране). После успешного завершения настройки адрес копируется в файл ROM и не меняется до тех пор, пока вы не отредактируете настройки или загрузите другой файл ROM.
Set WAN MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал заданный вручную MAC-адрес. Введите в это поле этот MAC-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.3.2 Экран DHCP Client

Выберите **DHCP Client** если Интернет-провайдер или системный администратор динамически назначает вам IP-адрес.

Иллюстрация 45 Connection Type: DHCP Client



В следующей таблице описаны поля этого экрана.

Таблица 22 Connection Type: DHCP Client

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access	
Connection Type	Выберите **DHCP Client** если провайдер динамически назначает вам IP-адрес при соединении.
MTU Size	Размер пакета MTU (Maximum Transmission Unit), которые могут передаваться через этот интерфейс. Пакеты больше этого размера NBG6615 будет разбивать на несколько пакетов. Допустимые значения - от 576 до 1500, по умолчанию 1500.
DNS Servers	
Attain DNS Automatically	Щелкните кнопку **Attain DNS Automatically** если провайдер динамически назначает вам IP-адрес DNS-сервера и NBG6615.
Set DNS Manually	Выберите **Set DNS Manually** если у вас есть IP-адрес сервера DNS. Нужно ввести IP-адрес первого и второго сервера DNS ниже.
First DNS Server Second DNS Server	Если вы выбрали Set DNS Manually, то введите в эти поля IP-адрес первого и второго сервера DNS.
WAN MAC Address В разделе MAC можно задать MAC-адрес порта WAN. Можно использовать MAC-адрес NBG6615, копируя MAC-адрес компьютера в вашей локальной сети либо вручную введя MAC-адрес.	
Factory default	Выберите эту опцию чтобы интерфейс WAN использовал заводской MAC-адрес по умолчанию.
Clone the computer's MAC address - MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал другой MAC-адрес, который является копией (клоном) MAC-адреса компьютера, с которого вы настраиваете устройство (он отображается на экране). После успешного завершения настройки адрес копируется в файл ROM и не меняется до тех пор, пока вы не отредактируете настройки или загрузите другой файл ROM.
Set WAN MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал заданный вручную MAC-адрес. Введите в это поле этот MAC-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.3.3 Экран PPPoE Connection

NBG6615 поддерживает разработанный IETF стандарт RFC 2516 протокола PPPoE (Point-to-Point Protocol over Ethernet), который определяет взаимодействие компьютера с широкополосным модемом (DSL, кабельным, беспроводным и т.п.). Опцию PPP over Ethernet можно использовать для коммутируемого соединения по PPPoE.

Для сервис-провайдеров PPPoE реализует метод доступа и аутентификации, совместимый с уже имеющейся системой контроля доступа (например, RADIUS).

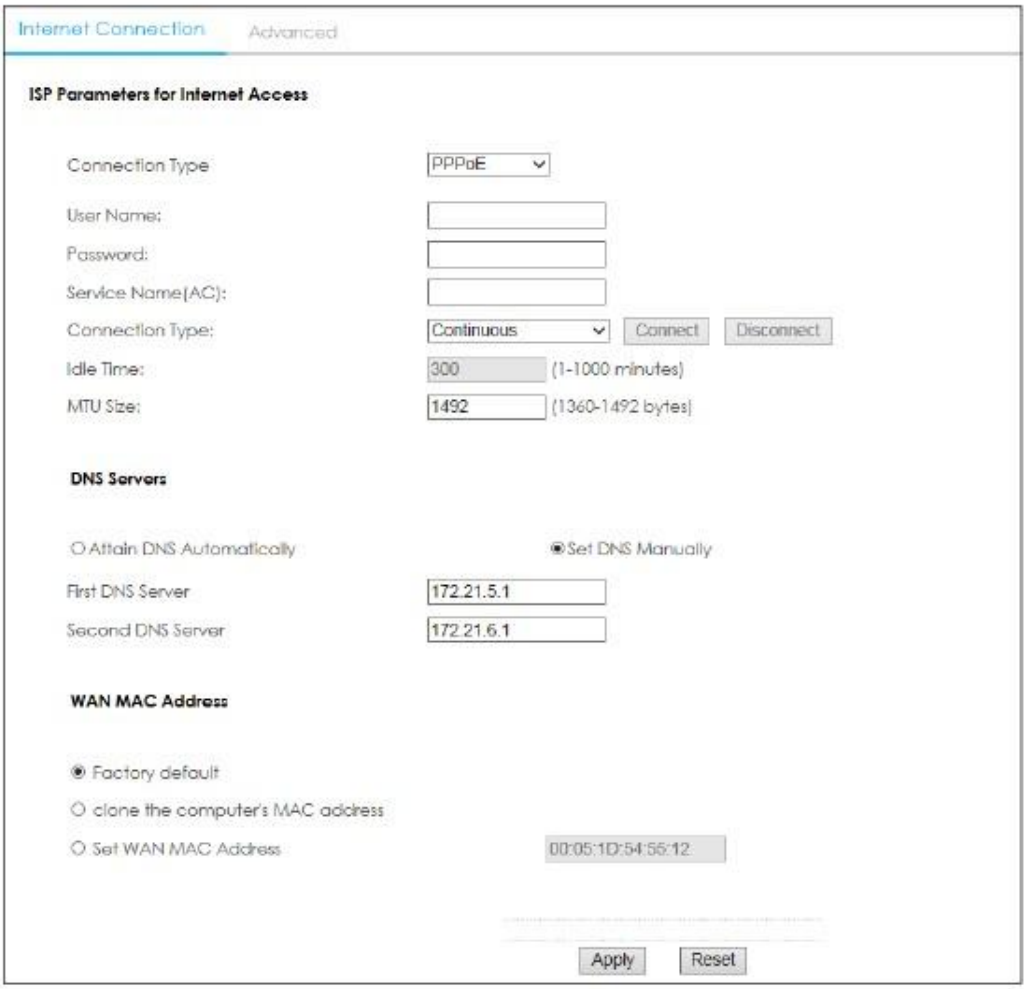
Одним из преимуществ PPPoE является предоставление конечным пользователям доступа к несколькими сетевым сервисам (так называемый dynamic service selection). Благодаря этой функции провайдер может легко создать новые IP-сервисы и предложить их определенным пользователям.

PPPoE очень удобен и для подписчика сервисов, и для провайдера/оператора, потому что не надо настраивать широкополосный модем, который установлен у подписчика.

Если PPPoE работает непосредственно на NBG6615, а не на компьютерах пользователей, которые подключены к вашей локальной сети, то не нужно устанавливать на этих компьютерах программное обеспечение PPPoE. Кроме того, если включен NAT, то все компьютеры в локальной сети будут иметь доступ к Интернету.

Этот экран выводится если выбрать **PPPoE encapsulation**.

Иллюстрация 46 Network > WAN > Internet Connection: PPPoE



В следующей таблице описаны поля этого экрана.

Таблица 23 Network > WAN > Internet Connection: PPPoE

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access	
Connection Type	Выберите **PPP over Ethernet** если вы подключаетесь к Интернету по коммутируемому соединению.
User Name	Имя пользователя, которое должен сообщить вам ваш Интернет-провайдер.
Password	Пароль для этого пользователя.
Service Name (AC)	Имя сервиса PPPoE, которое должен сообщить вам провайдер. Это имя нужно PPPoE для доступа к серверу PPPoE.
Connection Type	Выберите **Continuous** если не нужно, чтобы соединение отключалось по тайм-ауту. Выберите **Connect on Demand** если нужно, чтобы маршрутизатор отключался от сервера PPPoE по тайм-ауту бездействия. В этом случае нужно ввести число минут в поле Idle Timeout. Выберите **Manual** если вы хотите вручную установить соединение.

Таблица 23 Network > WAN > Internet Connection: PPPoE (продолжение)

ПОЛЕ	ОПИСАНИЕ
Idle Time	Это поле активно если выбрать **Connect on Demand**. В это поле нужно ввести число минут, по истечению которого маршрутизатор автоматически отключается от сервера PPPoE по таймеру бездействия.
MTU Size	Введите Maximum Transmission Unit (MTU) или максимальный размер пакета, который NBG6615 может получать и обрабатывать.
Connect/ Disconnect	Щелкните кнопку **Connect** для соединения с заданными выше параметрами либо кнопку **Disconnect** для разрыва соединения.
DNS Servers	
Attain DNS Automatically/Set DNS Manually	Щелкните **Attain DNS Automatically** если провайдер динамически назначает вам IP-адрес DNS-сервера и NBG6615 либо **Set DNS Manually** если у вас есть IP-адрес сервера DNS.
First DNS Server Second DNS Server	В этом поле вводятся IP-адреса первого и второго сервера DNS.
WAN MAC Address В разделе MAC можно задать MAC-адрес порта WAN. Можно использовать MAC-адрес NBG6615, копируя MAC-адрес компьютера в вашей локальной сети либо вручную введя MAC-адрес.	
Factory default	Выберите эту опцию чтобы интерфейс WAN использовал заводской MAC-адрес по умолчанию.
Clone the computer's MAC address - MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал другой MAC-адрес, который является копией (клоном) MAC-адреса компьютера, с которого вы настраиваете NBG6615 (он отображается на экране). После успешного завершения настройки адрес копируется в файл ROM и не меняется до тех пор, пока вы не отредактируете настройки или загрузите другой файл ROM.
Set WAN MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал заданный вручную MAC-адрес. Введите в это поле этот MAC-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.3.4 Экран PPTP Connection

Point-to-Point Tunneling Protocol (PPTP) – это сетевой протокол для защищенной передачи данных от удаленного клиента на частный сервер с помощью создания виртуальной частной сети Virtual Private Network (VPN) на базе сетей TCP/IP.

PPTP поддерживает создание многопротокольных VPN по требованию на базе Интернета и других публичных сетей.

Этот экран выводится при выборе PPTP encapsulation.

Иллюстрация 47 Network > WAN > Internet Connection: PPTP

В следующей таблице описаны поля этого экрана.

Таблица 24 Network > WAN > Internet Connection: PPTP

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access	
Connection Type	Для настройки клиента PPTP нужно заполнить поля User Name и Password для PPP connection и ввести параметры PPTP для PPTP connection. Выберите в этом поле **Dynamic IP (DHCP)** или **Static IP**.
IP Address	Если вы выбрали **Static IP**, то введите постоянный IP-адрес, который вам назначил системный администратор или провайдер.
Subnet Mask	Если вы выбрали **Static IP**, то введите маску подсети, которую вам сообщил системный администратор или провайдер.
Default Gateway	If Если вы выбрали **Static IP**, то введите IP-адрес шлюза, который вам назначил системный администратор или провайдер. В этом поле можно выбрать **Attain the Server by Domain Name** либо **Attain the Server by Ip Address**.
Domain Name	Если вы выбрали **Attain the Server by Domain Name**, то в это поле надо ввести адрес домена, который вам сообщил системный администратор или провайдер.
Server IP Address	Введите IP-адрес сервера PPTP.

Таблица 24 Network > WAN > Internet Connection: PPTP (продолжение)

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя, которое вам назначил провайдер.
Password	Пароль пользователя, который указан в поле User Name.
Connection Type	Выберите **Continuous** если не нужно, чтобы соединение отключалось по тайм-ауту. Выберите **Connect on Demand** если нужно, чтобы маршрутизатор отключался от сервера PPPoE по тайм-ауту бездействия. В этом случае нужно ввести число минут в поле Idle Timeout. Выберите **Manual** если вы хотите вручную установить соединение.
Idle Time	Это поле активно если выбрать **Connect on Demand**. В это поле нужно ввести число минут, по истечению которого маршрутизатор автоматически отключается от сервера PPPoE по таймеру бездействия.
MTU Size	Введите Maximum Transmission Unit (MTU) или максимальный размер пакета, который NBG6615 может получать и обрабатывать.
DNS Servers	
Attain DNS Automatically/ Set DNS Manually	Щелкните **Attain DNS Automatically** если провайдер динамически назначает вам IP-адрес DNS-сервера и NBG6615 либо **Set DNS Manually** если у вас есть IP-адрес сервера DNS.
First DNS Server Second DNS Server	В этом поле вводятся IP-адреса первого и второго сервера DNS.
WAN MAC Address В разделе MAC можно задать MAC-адрес порта WAN. Можно использовать MAC-адрес NBG6615, копируя MAC-адрес компьютера в вашей локальной сети либо вручную введя MAC-адрес.	
Factory default	Выберите эту опцию чтобы интерфейс WAN использовал заводской MAC-адрес по умолчанию.
Clone the computer's MAC address - MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал другой MAC-адрес, который является копией (клоном) MAC-адреса компьютера, с которого вы настраиваете NBG6615 (он отображается на экране). После успешного завершения настройки адрес копируется в файл ROM и не меняется до тех пор, пока вы не отредактируете настройки или загрузите другой файл ROM.
Set WAN MAC Address	Выберите эту опцию чтобы интерфейс WAN использовал заданный вручную MAC-адрес. Введите в это поле этот MAC-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.4 Экран Advanced

Этот экран используется для настройки конфигурации multicast. Для перехода на этот экран щелкните **Network > WAN > Advanced**.

Иллюстрация 48 Network > WAN > Advanced

В следующей таблице описаны поля этого экрана.

Таблица 25 Network > WAN > Advanced

ПОЛЕ	ОПИСАНИЕ
Multicast Setup	
Multicast Proxy & Snooping	Для включения обоих функций NBG6615 выберите **Multicast Proxy & Snooping**. С помощью функции Multicast proxy маршрутизатор IPv6 может обнаруживать хосты MLD, которые хотят получать пакеты multicast, и определять IP-адреса групп хостов, которые хотят присоединиться к сети multicast. С помощью функции Multicast snooping устройство NBG6615 может проверять проходящие через него пакеты MLD и узнавать о членстве в группе multicast. Ее применение уменьшает трафик multicast.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

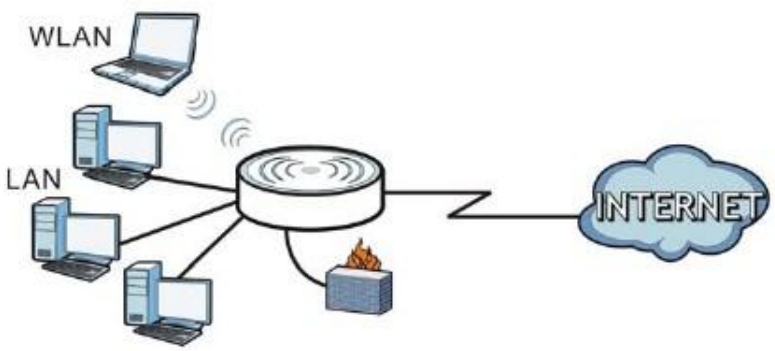
Глава 8
LAN

8.1 Обзор

В этой главе описана настройка параметров конфигурации LAN.

Локальная сеть Local Area Network (LAN) – это общая среда обмена данными ограниченного масштаба (например, внутри одного здания или на одном этаже), к которой подключены разные устройства. Экраны LAN используются для настройки DHCP-сервера LAN, управления IP-адресами и разделения физической сети на несколько логических.

Иллюстрация 49 LAN Setup

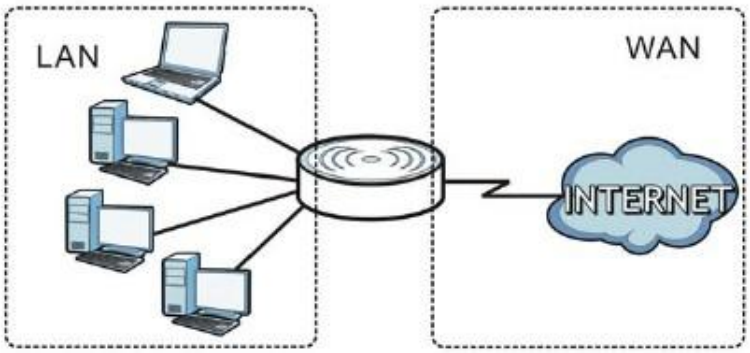


С помощью экранов LAN можно настроить DHCP-сервер LAN и управлять IP-адресами.

8.2 Основные сведения

Фактическое физическое соединение определяет, является ли порт NBG6615 портом LAN или портом WAN. Есть две изолированные друг от друга сети IP - внутренняя LAN и внешняя WAN (см. Иллюстрацию).

Иллюстрация 50 IP-адреса LAN и WAN



Заводские настройки параметров LAN по умолчанию в NBG6615:

• IP-адрес 192.168.212.1 и маска подсети 255.255.255.0 (24 бита)

• Для сервера DHCP выделено 128 IP-адресов клиентов начиная с 192.168.212.33.

Эти параметры подходят для большинства сценариев использования устройства. Если ваш провайдер дал вам IP-адрес(а) сервер DNS, то настройте LAN в соответствии с инструкциями Web Configurator.

8.2.1 IP-адрес и маска подсети

Также как у домов, стоящих на одной улице, в адресе указано одно и то же имя, так и у компьютеров в одной LAN один и тот же IP-адрес сети.

IP-адрес сети можно узнать разными способами. Если ваш провайдер или системный администратор выделил вам блок IP-адресов, то IP-адреса и маску сети надо использовать в соответствии с его инструкциями.

Если провайдер не выделил вам определенный IP-адрес, то скорей всего у вас одна учетная запись пользователя и провайдер назначает вам IP-адрес динамически когда вы подключаетесь к нему. Комитет Internet Assigned Number Authority (IANA) выделил блок адресов для частного использования. Вы можете использовать только эти адреса (если только провайдер не предоставил в виде исключения другие адреса). Например, если IP-адрес – это номер сети, то в ней может быть до 254 адресов отдельных устройств от 192.168.1.1 и до 192.168.1.254 (адреса 0 и 255 зарезервированы). Первые цифры идентифицируют номер сети, а последние три – отдельные компьютеры в сети.

После того, как вы узнали диапазон доступных вам IP-адресов, выберите один из них для NBG6615, например, 192.168.212.1 (но надо убедиться, что этот IP-адрес не использует другое устройство в вашей сети).

Маска подсети определяет часть IP-адреса, которая относится к сети. NBG6615 автоматически определит маску подсети на основе введенного вами IP-адреса. Ее не надо менять (если только об этом вас попросит провайдер).

8.2.2 Назначение адреса DNS-сервера

Система Domain Name System (DNS) обеспечивает соответствие между именем домена и IP-адресом, например, имени домена www.zyxel.com соответствует IP-адрес 204.217.0.2. Без использования DNS-сервера вы можете обращаться к компьютеру только по его IP-адресу

NBG6615 может получить адрес DNS-сервера двумя способами:

1 Вы можете узнать адрес DNS-сервера у вашего Интернет-провайдера и вручную ввести этот адрес в поле DNS Server в Визарде и/или на экране WAN > Internet Connection.

2 Если провайдер не предоставил вам данные сервере DNS, то оставьте значение 0.0.0.0 в полях в Визарде и/или на экране WAN > Internet Connection и тогда провайдер будет динамически назначать вам IP-адрес DNS-сервера.

8.2.3 Настройка пула IP-адресов

NBG6615 предварительно сконфигурирован с пулом 18-адресов от 192.168.212.33 до 192.168.212.160. В этой конфигурации 31 первых IP-адресов (кроме 192.168.212.0, который использует сам NBG6615) от 192.168.212.2 до 192.168.212.32 используются для серверов, например, email, FTP, TFTP, web и т.п.

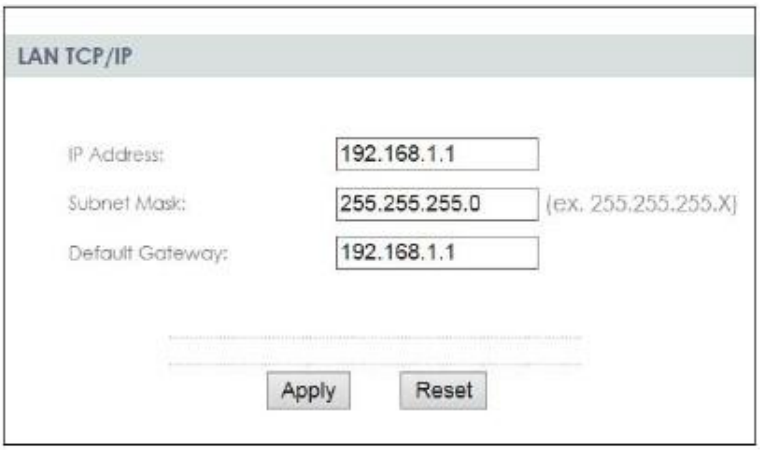
8.2.4 LAN TCP/IP

В NBG6615 использует сервер DHCP, который динамически назначает IP-адреса и серверы DNS системам, который поддерживают функцию клиента DHCP.

8.3 Экран LAN IP

С помощью этого экрана можно настраивать основные параметры локальной сети. Щелкните **Network > LAN**.

Иллюстрация 51 Network > LAN > IP



В следующей таблице описаны поля этого экрана.

Таблица 26 Network > LAN > IP

ПОЛЕ	ОПИСАНИЕ
IP Address	IP-адрес NBG6615 (десятеричные цифры, разделенные точками, заводские настройки по умолчанию 192.168.212).

Таблица 26 Network > LAN > IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subnet Mask	Маска подсети IP-адреса. NBG6615 автоматически рассчитает маску подсети на основе назначенного вами устройству IP-адреса. Если вы не используете subnetting, то используете маску подсети, которую рассчитал NBG6615.
Default Gateway	IP-адрес маршрутизатора LAN. NBG6615 автоматически обновляет значение этого поля на основе введенного вами IP-адреса.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Глава 9
DHCP-сервер

9.1 Обзор

Протокол DHCP (Dynamic Host Configuration Protocol, RFC 2131 и RFC 2132) обеспечивает отдельным клиентам (компьютерам) получение с сервера конфигурации TCP/IP при загрузке. Вы можете настроить NBG6615 как DHCP-сервер LAN либо отключить его. В первом случае NBG6615 назначает конфигурации TCP/IP клиентам, а во втором в локальной сети должен быть другой DHCP сервер либо нужно вручную конфигурировать каждый компьютер.

9.2 Экраны, которые описаны в этой главе

- Экран **General** для включения сервера DHCP (Раздел 9.4 на стр. 81).
- Экран **Static DHCP** для назначения IP-адресов в LAN компьютерам в соответствии с их конкретным MAC-адресом (Раздел 9.5 на стр. 82).
- Экран **Client List**, на котором выводится текущая информация о клиенте DHCP (Раздел 9.6 на стр. 83).

9.3 Основные сведения

У каждого устройства Ethernet есть уникальный адрес MAC (Media Access Control). Этот адрес назначается на заводе и состоит из шести пар шестнадцатеричных цифр, например 00:A0:C5:00:00:02. MAC-адрес сетевого устройства нужно знать для добавления его в список **DHCP Server > Client List**.

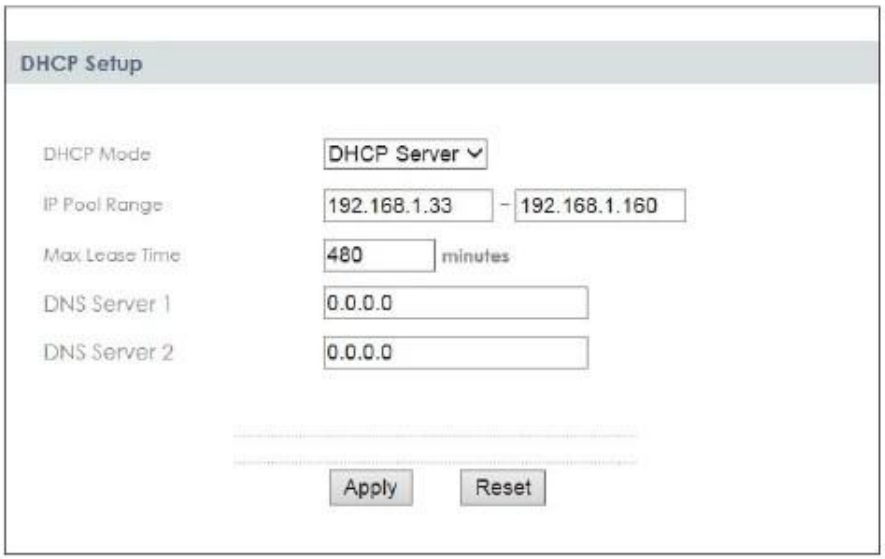
О IP-адресах и маске подсети см. Раздел 8.2.1 на стр. 78.

О серверах DNS см. Раздел 8.2.2 на стр. 78.

9.4 Экран General

С помощью этого экрана можно включить сервер DHCP. Щелкните **Network > DHCP Server**. Откроется следующий экран.

Иллюстрация 52 Network > DHCP Server > General



В следующей таблице описаны поля этого экрана.

Таблица 27 Network > DHCP Server > General

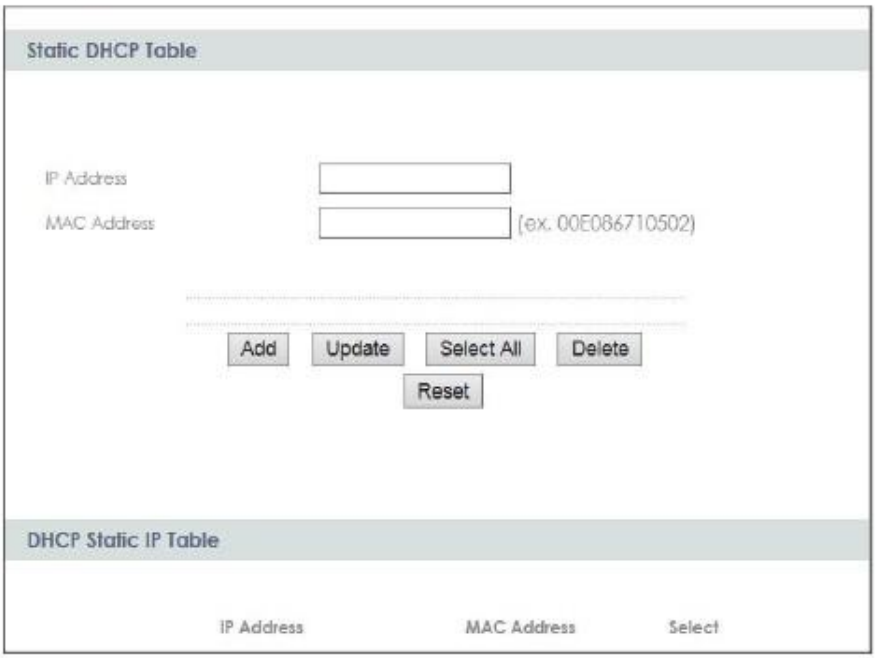
ПОЛЕ	ОПИСАНИЕ
DHCP Mode	В раскрывающемся списке выберите **DHCP server** чтобы NBG6615 работал как сервер DHCP либо, если это необходимо для выполнения инструкций вашего провайдера, выберите **None**. Протокол DHCP (Dynamic Host Configuration Protocol, RFC 2131 и RFC 2132) обеспечивает отдельным клиентам (компьютерам) получение с сервера конфигурации TCP/IP при загрузке. Если вы выбрали **None**, то в локальной сети должен быть другой DHCP-сервер либо нужно вручную конфигурировать каждый компьютер. Если вы выбрали **DHCP server**, то надо заполнить следующие четыре поля.
IP Pool Range	Первый и последний IP-адрес из пула, выделенного для LAN.
Max Lease Time	Это поле определяет длительность тайм-аута, по истечении которого неиспользуемый IP-адрес в LAN отключается. По умолчанию тайм-аут 120 минут, максимум 525600 минут.
DNS Server1	IP-адрес первого DNS-сервера для сервера DHCP.
DNS Server2	IP-адрес второго DNS-сервера для сервера DHCP.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

9.5 Экран Static DHCP

Экран Static DHCP для назначения IP-адресов в LAN определенным компьютерам в соответствии с их MAC-адресами, а также настройки информации сервера DNS, которую NBG6615 посылает клиентам DHCP.

Для изменения настроек static DHCP вашего NBG6615 щелкните **Network > DHCP Server > Static DHCP**. Откроется следующий экран.

Иллюстрация 53 Network > DHCP Server > Static DHCP



В следующей таблице описаны поля этого экрана.

Таблица 28 Network > DHCP Server > Static DHCP

ПОЛЕ	ОПИСАНИЕ
Static DHCP Table	
IP Address	Введите IP-адрес компьютера в вашей LAN.
MAC Address	Введите MAC-адрес компьютера в вашей LAN.
Add	Щелкните кнопку **Add** чтобы добавить новую запись static DHCP.
Update	Щелкните кнопку **Update** чтобы изменить параметры выбранной записи.
Select All	Щелкните кнопку **Select All** чтобы выбрать все записи static DHCP в таблице DHCP Static IP Table.
Delete	Щелкните кнопку **Delete** чтобы уделить выбранную запись static DHCP в таблице DHCP Static IP Table.
Reset	Щелкните кнопку **Reset** чтобы очистить поля IP Address и MAC address.
DHCP Static IP Table	
IP Address	IP-адрес компьютера в вашей LAN.
MAC Address	MAC-адрес компьютера в вашей LAN.
Select	Щелкните кнопку **Select** чтобы выбрать запись static DHCP.

9.6 Экран Client List

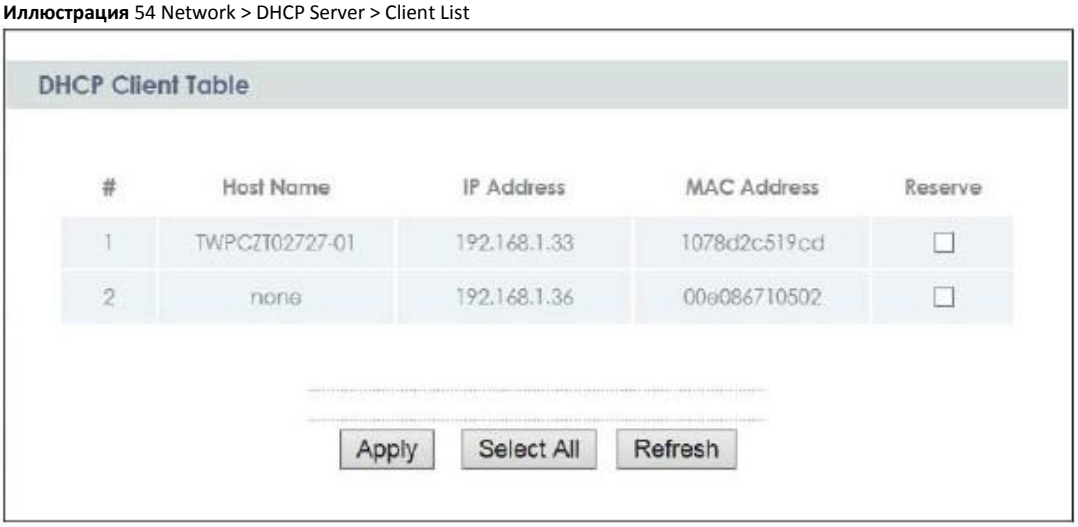
В таблице DHCP выводится текущая информация клиента DHCP (в том числе IP Address, Host Name и MAC Address) для сетевых клиентов, которые использую DHCP-серверы NBG6615.

На этом экране можно назначать IP-адресам MAC-адреса (и имена хостов). Щелкните **Network > DHCP Server > Client List**.

Примечание: Также можно вывести нередактируемый список клиентов, если щелкнуть ссылку **DHCP Table (Details...)** на экране **Status**.

Откроется следующий экран.

Иллюстрация 54 Network > DHCP Server > Client List



В следующей таблице описаны поля этого экрана.

Table 29 Network > DHCP Server > Client List

ПОЛЕ	ОПИСАНИЕ
#	Номер компьютера (хоста).
Host Name	Имя компьютера (хоста).
IP Address	IP-адрес компьютера, подключенного к порту LAN.
MAC Address	MAC-адрес компьютера, имя которого указано в поле **Host Name**. У каждого устройства Ethernet есть уникальный адрес MAC (Media Access Control). Этот адрес назначается на заводе и состоит из шести пар шестнадцатеричных цифр, например, 00:A0:C5:00:00:02.
Reserve	Это поле нужно отметить если вы хотите зарезервировать этот IP-адрес за конкретным MAC-адресом.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Refresh	Щелкните **Reset** для настройки этого экрана с самого начала.

Глава 10
Network Address Translation

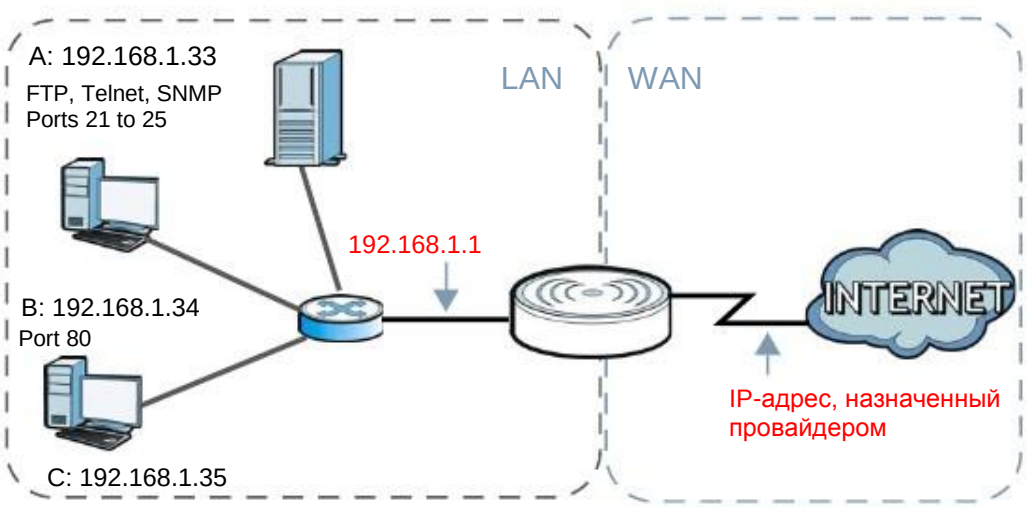
10.1 Обзор

В этой главе объясняется, как настроить NAT на NBG6615.

NAT (Network Address Translation - NAT, RFC 1631) обеспечивает преобразование IP-адреса хоста в пакете. Например, IP-адрес отправителя, используемый в одной сети, в исходящем пакете, преобразуется в IP-адрес другой сети.

У каждого пакета есть адрес отправителя и получателя. В исходящих пакетах NAT преобразует частный (локальный) IP-адрес в уникальный глобальный, который нужен для обмена данными с хостами из других сетей, и далее отправляет пакеты в Интернет. NBG6615 отслеживает исходные адреса вместе с номерами портов и во входящих пакетов с ответами на запросы подставляет эти адреса и номера портов чтобы пакет дошел до отправителя запроса (см. иллюстрацию).

Иллюстрация 55 Пример NAT



Подробнее о преобразовании IP-адресов см. RFC 1631, The IP Network Address Translator (NAT).

Примечание: При настройке NAT нужно создать правило для межсетевого экрана чтобы трафик из WAN пересылался через NBG6615.

10.2 Экраны, которые описаны в этой главе

• Экран **General** для включения NAT и настройки сервера по умолчанию server (Раздел 10.3 на стр. 87).

• Экран **Application** для изменения настроек port forwarding на NBG6615 (Раздел 10.4 на стр. 88).

• Экран **Port Triggering** для изменения настроек port trigger на NBG6615 (Раздел 10.5 на стр. 90).

10.2.1 Основные сведения

В этом разделе объясняются термины и концепции, используемые в этой главе.

Внутренний/Внешний

Это обозначает, является хост внутренним по отношению к NBG6615или внешним, например, компьютеры ваших подписчиков – это внутренние хосты, а web-серверы в Интернете – внешние хосты.

Глобальный/Локальный

IP-адрес хоста в заголовке пакета когда он проходит через маршрутизатор, например, локальный адрес означает IP-адрес хоста когда пакет находится в локальной сети, а глобальный адрес - IP-адрес хоста когда тот же пакет передается по WAN.

Примечание: внутренний/внешний относится к расположению хоста, а глобальный/локальный – к IP-адресу хоста, который записан в заголовке пакета.

Внутренний локальный адрес (ILA) – это IP-адрес внутреннего хоста в заголовке пакета когда пакет все еще в локальной сети, а внутренний глобальный адрес inside global address (IGA) – это IP-адрес того же внутреннего хоста в заголовке пакета когда пакет передается по WAN.

Таблица 30 Определения NAT

ТЕРМИН	ОПИСАНИЕ
Inside	Хост в LAN.
Outside	Хост в WAN.
Local	Адрес пакета (отправителя или получателя), который передается по LAN.
Global	Адрес пакета (отправителя или получателя), который передается по WAN.

Примечание: NAT никогда не меняет локальные или глобальные IP-адреса внешних хостов.

Как NAT преобразует адреса

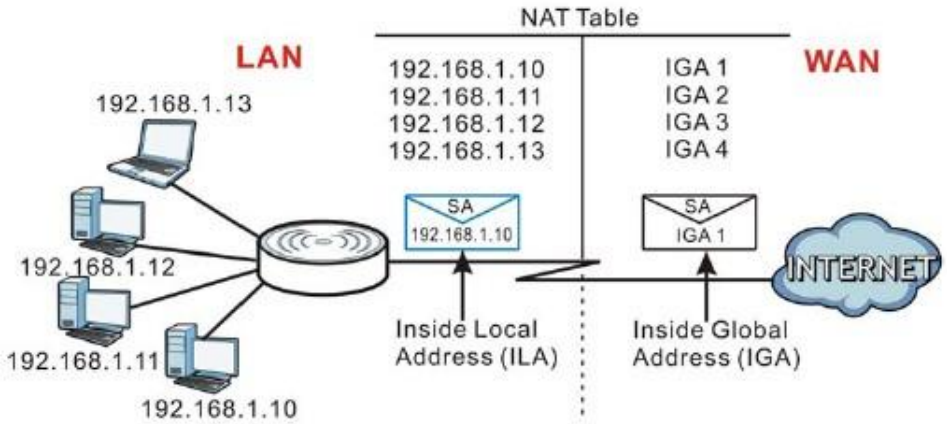
NAT меняет IP-адрес из пакета, который пришел от подписчика (внутренний локальный адрес) на внутренний глобальный адрес и затем пересылает этот пакет в WAN. Когда приходит ответ на этот пакет, то NAT преобразует адрес получателя (внутренний глобальный адрес) обратно в внутренний локальный адрес и затем пересылает этот ответный пакет внутреннему хосту, который отправил запрос. При этом NAT никогда не меняет локальные или глобальные IP-адреса внешних хостов

Глобальные IP-адреса внутренних хостов могут быть статичными или их динамически назначает провайдер. Кроме того, в локальной сети можно размещать специализированные серверы, например, web и telnet, и открывать доступ к ним извне. Если у вас нет таких серверов, то NAT обеспечивает защиту с помощью межсетевого экрана и блокирует все входящие запросы чтобы хакеры не могли узнать параметры вашей сети. Подробнее о преобразовании IP-адресов см. документ RFC 1631, The IP Network Address Translator (NAT).

Как работает NAT

У каждого пакета есть адрес отправителя и получателя. В исходящих пакетах NAT преобразует частный (локальный) IP-адрес в уникальный глобальный, который нужен для обмена данными с хостами из других сетей, и далее отправляет пакеты в Интернет. NBG6615 отслеживает исходные адреса вместе с номерами портов и во входящих пакетов с ответами на запросы подставляет эти адреса и номера портов чтобы пакет дошел до отправителя запроса (см. иллюстрацию).

Иллюстрация 56 Как работает NAT



10.3 Экран General NAT

С помощью этого экрана можно включать NAT и настраивать сервер по умолчанию. Для перехода к экрану **General** щелкните **Network > NAT**.

Иллюстрация 57 Network > NAT > General

В следующей таблице описаны поля этого экрана.

Таблица 31 Network > NAT > General

ПОЛЕ	ОПИСАНИЕ
NAT Setup	
NAT	Network Address Translation (NAT) обеспечивает преобразование IP-адресов одной сети (например, частных IP-адресов из локальной сети) в другие IP-адреса, доступные для компьютеров из другой сети (например, публичные IP-адреса Интернета). Для включения NAT выберите **Enable**, для отключения NAT - **Disable**.
Default Server Setup	
Enable	Для включения сервера по умолчанию выберите **Enable**.
Server IP Address	В дополнение к серверам для заданных сервисов NAT поддерживает сервер по умолчанию, который получает пакеты от портов, не указанных на экране **Application**. Если вы не указали IP-адрес сервера по умолчанию, то NBG6615 будет отбрасывать все пакеты, которые направляются на порты, неуказанные на экране **Application** и не заданные средствами удаленного управления
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

10.4 Экран Application

Экран Application используется для перенаправления входящих запросов сервисов к серверу (серверам) в локальной сети. На этом экране можно указать один порт или диапазон портов, на которые пересылаются запросы, и локальный IP-адрес нужного сервера. Номер порта соответствует конкретному сервису, например, сервису web соответствует порт 80, а сервису FTP - порт 21. В некоторых случаях, например, если неизвестен номер порта для сервиса или когда на сервере работает несколько сервисов (например, FTP и web), нужно задать диапазон номеров портов.

В дополнение к серверам для заданных сервисов NAT поддерживает сервер по умолчанию, на который направляются запросы, в которых не указан адрес сервера. Если сервер по умолчанию не задан, то такие запросы не обрабатываются.

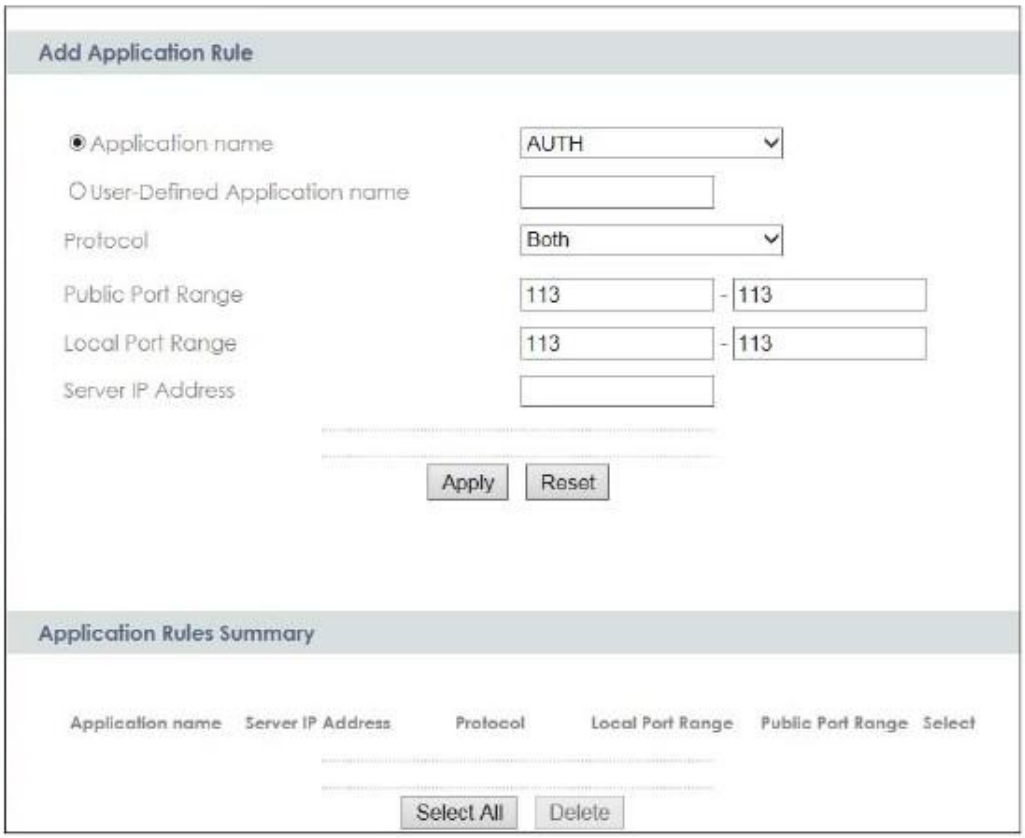
Примечание: Многие Интернет-провайдеры не разрешают домашним пользователям использовать собственный сервер для развертывания сервисов (например, Web или FTP), и в случае нарушения этого запрета могут заблокировать пользователя. Если вы не уверены, что ваш провайдер разрешает домашним пользователям развертывать такие сервисы, то обратитесь за справкой в его офис.

Функция Port Forwarding используется для перенаправления запросов сервисов на серверы в вашей локальной сети. Для изменения настроек Port Forwarding, используемых NBG6615 щелкните **Network > NAT > Application**. Откроется следующий экран.

Примечание: Если на экране NAT > General не назначен IP-адрес для Default Server, то NBG6615 отбрасывает все пакеты, которые идут на порты, которые не указаны на этом экране или не заданы средства удаленного управления.

Стандартные номера портов для сервисов указаны в Приложении E на стр. 197.

Иллюстрация 58 Network > NAT > Application



В следующей таблице описаны поля этого экрана.

Таблица 32 Network > NAT > Application

ПОЛЕ	ОПИСАНИЕ
Add Application Rule	
Application Name	Выберите опцию заранее сконфигурированного сервиса из раскрывающегося списка. Номер порта (номера портов) и протокол для этого сервиса выводятся ниже.
User-Defined Application Name	Введите в этом поле имя правила длиной до 31 печатных символа, либо выберите заранее сконфигурированный сервис из раскрывающегося списка в поле Application Name.
Protocol	Выберите протокол транспортного уровня для этого сервиса. Можно выбрать TCP или UDP.
Public Port Range Local Port Range	Введите номер порта (номера портов), на которые направляются пакеты. Для задания диапазона портов введите разделенным двоеточием (:) номера первого и последнего порта, например, 10:20.
Server IP Address	Введите внутренний IP-адрес сервера, который будет получать пакеты от порта (портов), указанный в поле **Port**.
Apply	Щелкните **Apply** для сохранения изменений в таблице Application Rules Summary.
Reset	Щелкните **Reset** чтобы сбросить изменения и сохранить старые значения в полях **Service Name** и **Port**.
Application Rules Summary	
Application Name	Имя правила.
Server IP Address	Внутренний IP-адрес сервера.
Protocol	Протокол транспортного уровня, поддерживаемый этим сервером.

Таблица 32 Network > NAT > Application (продолжение)

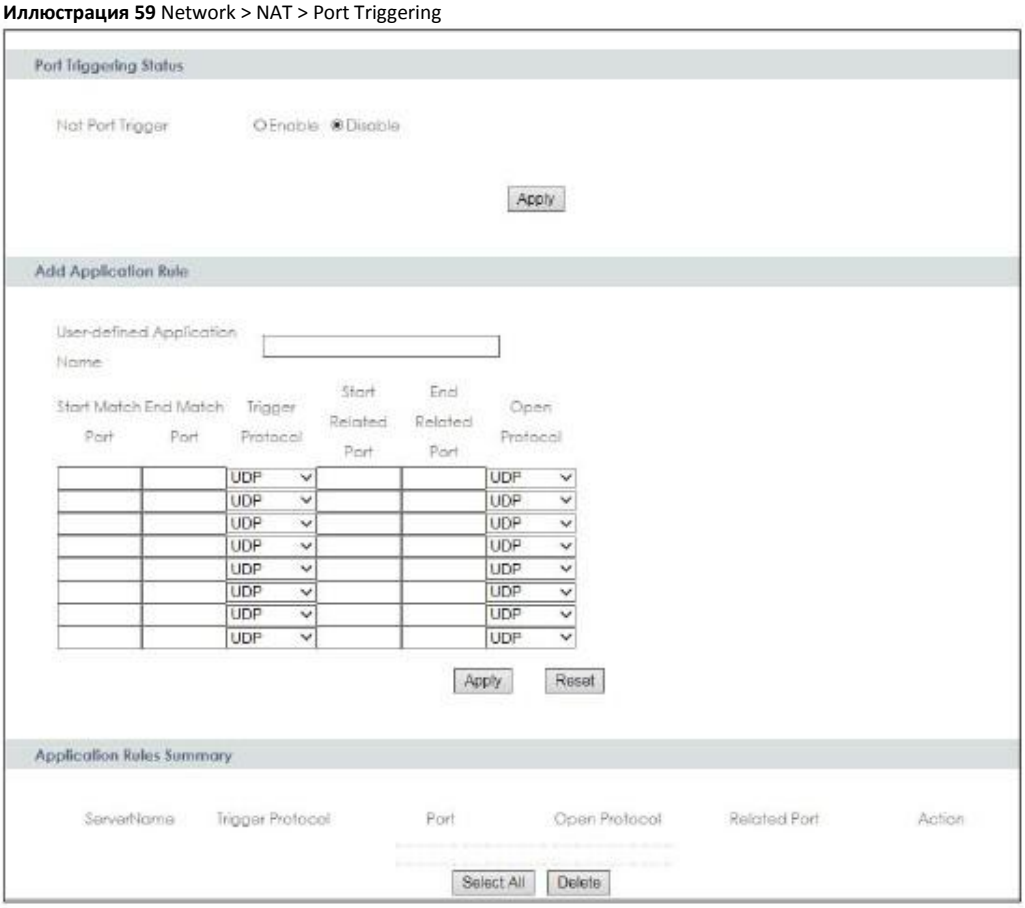
ПОЛЕ	ОПИСАНИЕ
Local Port Range Public Port Range	Номера порта (портов)
Select	Щелкните для выбора записи.
Select All	Щелкните для выбора всех записей.
Delete	Щелкните для удаления выбранной записи (записей).

10.5 Экран Port Triggering

Для изменения настроек port trigger в NBG6615 щелкните **Network > NAT > Port Triggering**. Откроется следующий экран.

Примечание: Несколько компьютеров LAN не могут одновременно использовать диапазон портов port triggering.

Иллюстрация 59 Network > NAT > Port Triggering



В следующей таблице описаны поля этого экрана.

Таблица 33 Network > NAT > Port Triggering

ПОЛЕ	ОПИСАНИЕ
Port Triggering Status	
Nat Port Trigger	Щелкните **Enable** чтобы включить NAT Port Trigger или **Disable** для его отключения.
Apply	Щелкните **Apply** чтобы применить выбранный выше NAT Port Trigger.
Add Application Rule	
User-defined Application Name	Введите уникальное имя длиной до 15 символов с пробелами.
Start Match Port	Введите номер первого порта из диапазона портов, которые работают как триггеры (они запускают на NBG6615 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN).
End Match Port	Введите номер последнего порта из диапазона портов, которые работают как триггеры (они запускают на NBG6615 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN).
Trigger Protocol	Укажите протокол (UDP, TCP или UDP/TCP), который запускает на NBG6615 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN.
Start Related Port	Введите номер первого порта из диапазона портов, которые использует сервер в WAN для определенного сервера. NBG6615 будет перенаправлять трафик с этих портов клиентскому компьютеру в LAN, который запросил этот сервис.
End Related Port	Введите номер первого порта из диапазона портов, которые использует сервер в WAN для определенного сервера. NBG6615 будет перенаправлять трафик с этих портов клиентскому компьютеру в LAN, который запросил этот сервис.
Open Protocol	Укажите протокол (UDP, TCP или UDP/TCP), который использует сервер в WAN для определенного сервиса.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала
Application Rules Summary	
Server Name	Имя правила Application.
Trigger Protocol	Протокол, который запускает на NBG6615 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN.
Port	Порты, которые работают как триггеры (они запускают на NBG6615 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN).
Open Protocol	Протокол, которые сервер в WAN использует для определенного сервиса.
Related Port	Порт сервера в WAN, который используется для определенного сервиса.
Action	Щелкните **Delete** для удаления правила.

10.6 Техническая информация

В этом разделе приводится дополнительная техническая информация о функциях NBG6615, описанных в этой главе.

10.6.1 NAT Port Forwarding: сервисы и номера портов

Функция port forwarding формирует список внутренних серверов (которые находятся за NAT в LAN), например, web или FTP, которые можно открыть для доступа извне даже если из-за использования NAT ваша локальная сеть извне видна как один компьютер.

Экран Application используется для перенаправления входящих запросов сервисов к серверу (серверам) в локальной сети. На этом экране можно указать один порт или диапазон портов, на которые пересылаются запросы, и локальный IP-адрес нужного сервера. Номер порта соответствует конкретному сервису, например, сервису web соответствует порт 80, а сервису FTP - порт 21. В некоторых случаях, например, если неизвестен номер порта для сервиса или когда на сервере работает несколько сервисов (например, FTP и web), нужно задать диапазон номеров портов.

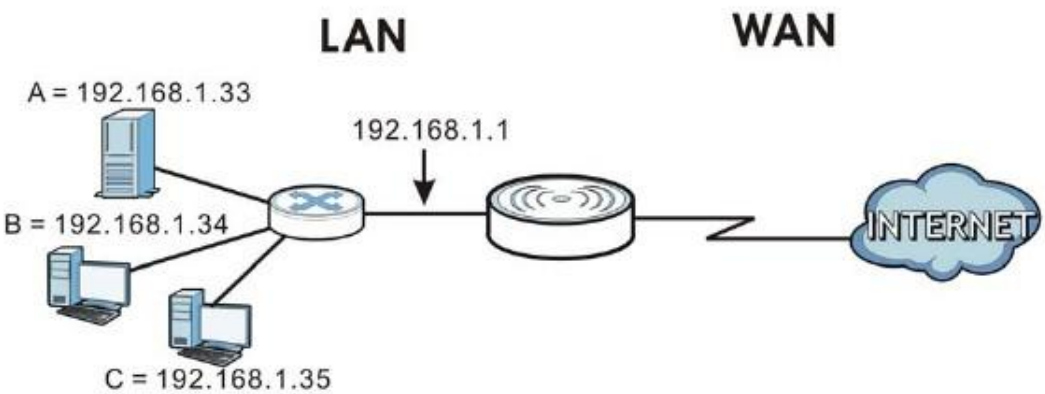
В дополнение к серверам для заданных сервисов NAT поддерживает сервер по умолчанию, на который направляются запросы, в которых не указан адрес сервера. Если сервер по умолчанию не задан, то такие запросы не обрабатываются.

Примечание: Многие Интернет-провайдеры не разрешают домашним пользователям использовать собственный сервер для развертывания сервисов (например, Web или FTP), и в случае нарушения этого запрета могут заблокировать пользователя. Если вы не уверены, что ваш провайдер разрешает домашним пользователям развертывать такие сервисы, то обратитесь за справкой в его офис.

10.6.2 Пример NAT Port Forwarding

В этом примере порты 21-25 выделены серверу, на котором работают сервисы FTP, Telnet и SMTP (**A**), порт 80 – другому серверу (**B**), и IP-адрес 192.168.1.35 выделен третьему серверу (**C**). Сам пользователя назначает IP-адреса LAN, а провайдер IP-адреса WAN. Из интернет сеть NAT видна как один хост.

Иллюстрация 60 Пример нескольких серверов, которые находятся за NAT



10.6.3 Trigger Port Forwarding

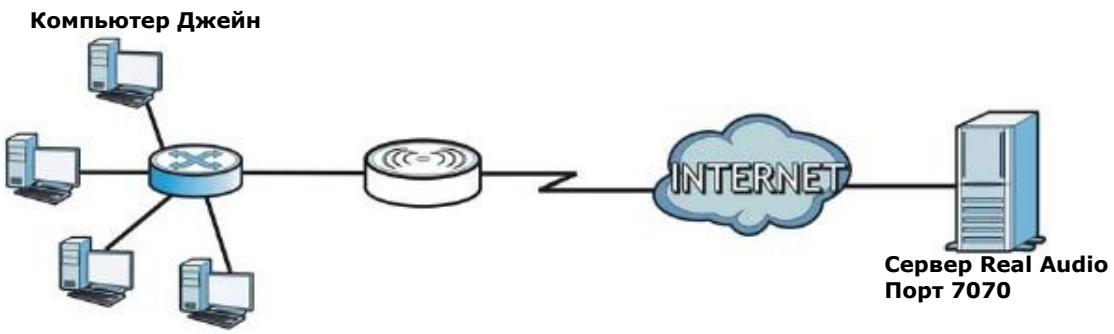
Некоторые сервисы используют выделенный диапазон портов и на стороне клиента, и на стороне сервера. С помощью стандартной функции port forwarding можно настроить в NAT порт на пересылку пакетов сервиса, которые приходят от сервера из WAN, на IP-адреса компьютера на стороне клиента (LAN). Однако port forwarding может пересылать пакеты только на один IP-адрес LAN. Чтобы пакеты этого сервиса приходили на другой компьютер LAN нужно вручную задать IP-адрес этого компьютера для порта с port forwarding вместо IP-адреса первого компьютера.

Эту проблему решает механизм trigger port forwarding, которые позволяет динамически менять IP-адреса компьютеров, использующих сервисов. NBG6615 записывает IP-адрес компьютера LAN, который послал трафик в WAN с запросом сервиса с определенным номером порта и протоколом («порт-триггер»). Когда WAN-порт NBG6615 получает ответ на запрос, в котором указаны определенный номер порта и протокол (входящий порт), то NBG6615 перенаправляет трафик на IP-адрес LAN компьютера, который запросил сервис. После того, как соединение компьютера с этим сервисом будет разорвано, другой компьютер точно также может использовать этот сервис. Trigger port forwarding избавляет от необходимости каждый раз заново настраивать IP-адрес когда нужно предоставить сервис другому компьютеру в LAN.

10.6.4 Пример Trigger Port Forwarding

Ниже приведен пример trigger port forwarding.

Иллюстрация 61 Пример работы Trigger Port Forwarding



1. Джейн запросила файл с сервера Real Audio (порт 7070).
2. Порт 7070 – это «порт-триггер», поэтому NBG6615 запишет IP-адрес компьютера Джейн и свяжет этот адрес с диапазоном «входящих» портов 6970-7170.
3. Сервер Real Audio отвечает на запрос, используя порт в диапазоне 6970-7170.
4. NBG6615 перенаправляет трафик на IP-адрес компьютера Джейн.
5. До разрыва соединения или истечения выделенного времени только Джейн может подключиться к серверу Real Audio. NBG6615 отключается по тайм-ауту через 3 минуты при использовании UDP (User Datagram Protocol) или через 2 часа при использовании TCP/IP (Transfer Control Protocol/Internet Protocol).

10.6.5 Два важных замечания о портах-триггерах

1. Триггер срабатывает только когда пакет идет из внутренний сети извне через NBG6615.
2. Если через порт (диапазон портов) идет непрерывный поток данных приложения, то его не сможет использовать другой порт-триггер в LAN.

Глава 11
Dynamic DNS

11.1 Обзор

Сервис Dynamic Domain Name Service (DDNS) позволяет использовать фиксированное имя домена вместе с динамичным IP-адресом. Пользователи могут подключиться к NBG6615 или серверу вашей сети по постоянному имени домена и не вводить заново IP-адрес, который меняется при каждом подключении.

Примечание: У NBG6615 должен быть публичный глобальный IP-адрес и у вас должна информация о учетной записи DDNS.

11.2 Экран Dynamic DNS

Для изменения настроек DDNS вашего NBG6615 щелкните **Network > DDNS**.

Иллюстрация 62 Network > DDNS

В следующей таблице описаны поля этого экрана.

Таблица 34 Network > DDNS

ПОЛЕ	ОПИСАНИЕ
Enable Dynamic DNS	Поставьте галочку в **Enable Dynamic DNS** чтобы включить DDNS.
Service Provider	Выберите из раскрывающегося списка имя вашего провайдера сервиса DDNS.
Host Name	Имя хоста – это имя домена, который сервис DDNS будет преобразовывать в ваши динамические глобальные IP-адреса. Введите в это поле полное имя хоста, например, ‘yourhost.mydomain.net’. Можно задать имена двух хостов, разделенные запятой (",").
User Name	Имя пользователя сервиса DDNS.

Таблица 34 Network > DDNS

ПОЛЕ	ОПИСАНИЕ
Password	Пароль для пользователя DDNS, указанного в user name.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Глава 12
Static Route

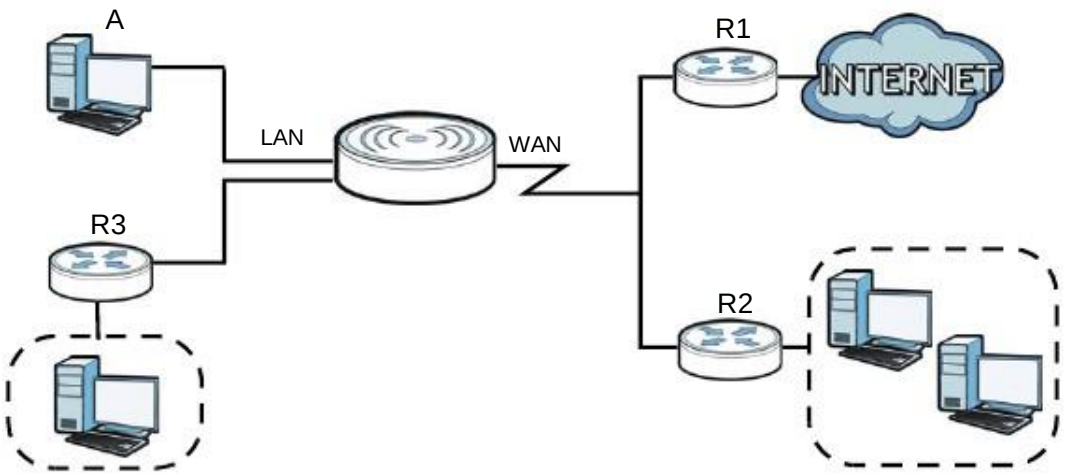
12.1 Обзор

В этой главе объясняется, как сконфигурировать статические маршруты для NBG6615.

Обычно NBG6615 перенаправляет исходящий трафик от компьютеров в LAN в Интернет с помощью шлюза по умолчанию. Если нужно, чтобы NBG6615 мог послать данные на устройства, которые недоступны через шлюз по умолчанию, то используются статические маршруты.

На следующей иллюстрации показан пример, в котором компьютер (**A**) подключен к LAN-интерфейсу NBG6615. Основной объем трафика NBG6615 от **A** идет в Интернет через шлюз по умолчанию (**R1**). Чтобы можно было подсоединиться к сервисам провайдера, которые находятся за маршрутизатором **R2** нужно создать один статический маршрут. Еще один статический маршрут нужен для связи с отдельной сетью, которая находится за маршрутизатором **R3**, подключенным к LAN.

Иллюстрация 63 Пример топологии со статической маршрутизацией



12.2 Экран IP Static Route

Для перехода к экрану Static Route щелкните **Network > Static Route**.

Иллюстрация 64 Network > Static Route

В следующей таблице описаны поля этого экрана.

Таблица 35 Network > Static Route

ПОЛЕ	ОПИСАНИЕ
Enable	Поставьте галочку в это поле чтобы включить правило.
Destination	Введите сетевой IP-адрес конечного получателя. Маршрутизация всегда выполняется на основе сетевого адреса. Если нужно задать маршрутизацию на один хост, то введите маску подсети 255.255.255.255 в поле **subnet mask** чтобы сетевой адрес были идентичен ID хоста.
IP Subnet Mask	Введите маску подсети IP.
Gateway	Введите IP-адрес шлюза next-hop. Шлюз – это маршрутизатор или коммутатор в том же сегменте интерфейса (интерфейсов) NBG6615. Он помогает пересылать пакеты конечному получателю.
Metric	Metric означает «стоимость передачи». Маршрутизатор выбирает оптимальный маршрут для передачи пакетов исходя из этой стоимости. Чем меньше хопов, тем «дешевле» маршрут. Введите число хопов передачи данных (маршрутизаторов), которые нужно пройти от NBG6615 до конечного получателя.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Update	Щелкните эту кнопку для изменения выбранного правила.
Select All	Щелкните эту кнопку для выбора всех правил в Static Route Table.
Delete	Щелкните эту кнопку для удаления выбранных правил из Static Route Table.
Static Route Table	
Destination	IP-адрес конечного получателя. Маршрутизация всегда выполняется на основе сетевого адреса.
Subnet Mask	IP-адрес маски подсети конечного получателя.
NextHop	IP-адрес шлюза. Шлюз – это маршрутизатор или коммутатор в том же сегменте, что и порт LAN или WAN устройства. Он помогает пересылать пакеты конечному получателю.

Таблица 35 Network > Static Route

ПОЛЕ	ОПИСАНИЕ
Metric	Число хопов между NBG6615 и получателем.
Select	Щелкните эту кнопку для выбора правила.

Глава 13 Межсетевой экран

13.1 Обзор

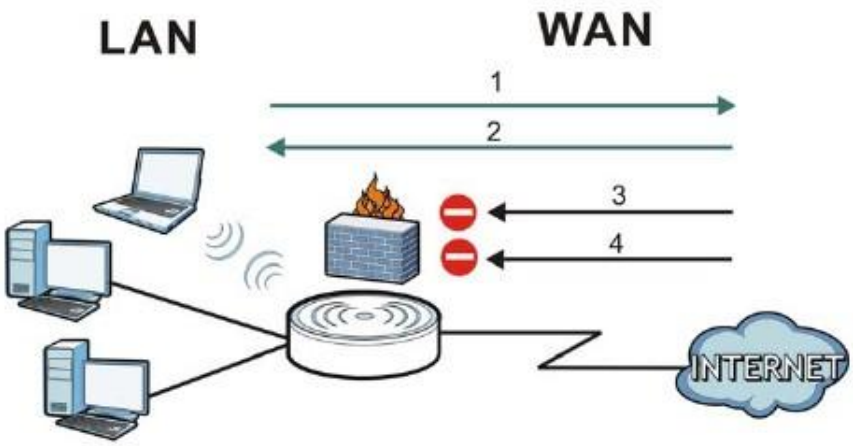
Эти экраны используются для включения и настройки межсетевого экрана, который защищает NBG6615 и вашу локальную сеть от постороннего и опасного трафика.

Рекомендуется включать межсетевой экран для защиты компьютеров в LAN от атак хакеров из Интернета и контроля доступа между LAN и WAN. По умолчанию межсетевой экран работает следующим образом:

- разрешает трафику, который идет от компьютеров в вашей LAN, передаваться по всей сети.
- блокирует доступ в вашу LAN трафика из других сетей.

На следующей иллюстрации показан пример работы межсетевого экран по умолчанию. Пользователь **A** может запустить сессию IM (Instant Messaging) с LAN, при которой трафик он него идет в WAN (**1**). Трафик из WAN, относящийся к этой сессии, межсетевой экран пропускает в LAN (**2**), а остальной трафик из WAN блокируется (**3** и **4**).

Иллюстрация 65 Работа межсетевого экрана по умолчанию



13.2 Экраны, которые описаны в этой главе

- Экран **General** для включения/отключения межсетевого экрана NBG6615 (Раздел 13.4 на стр. 100).
- Экран **Services** для включения/отключения функций ICMP и VPN (Раздел 13.5 на стр. 101).

13.3 Основные сведения

Межсетевой экран NBG6615 физически разделяет LAN и WAN и работает как шлюз безопасности, через который идет весь обмен данными между этими двумя сетями.

13.3.1 Межсетевой экран NBG6615

Межсетевой экран NBG6615 – это межсетевой экран stateful inspection, который во включенном состоянии защищает от атак Denial of Service (для включения щелкните вкладку **General** под **Firewall** и затем поставьте галочку в **Enable Firewall**). NBG6615 используется для безопасного подключения частной локальной сети Local Area Network (LAN) к Интернету и предотвращения кражи данных, их уничтожения или изменения, а также ведения журнала, в который заносятся события, связанные с безопасностью сети.

NBG6615 устанавливается между LAN и широкополосным модемом, через который локальная сеть подключена к Интернету. Он работает как шлюз безопасности, через который идет весь обмен данными между Интернетом и LAN.

У NBG6615 есть один порт Ethernet WAN и четыре порта Ethernet LAN, используемые для разделения локальной сети на два сегмента. Порт WAN (Wide Area Network) подключается к широкополосному кабельному или DSL-модему, который подключен к Интернету.

К портам LAN (Local Area Network) подсоединяется локальная сеть компьютеров, которым нужно обеспечить защиту от угроз Интернета. У этих компьютеров есть доступ к таким сервисам Интернета, как e-mail, FTP и World Wide Web, но извне к ним доступ по умолчанию возможен только если удаленный хост получил разрешение на использование конкретного сервиса.

13.3.2 Функции VPN Pass Through

Virtual Private Network (VPN) – это решение для безопасного соединения двух сетей через Интернет, например, домашней и офисной сети. для его использования требуется специальное оборудование на обоих концах соединения.

NBG6615 не является конечным устройством VPN, но позволяет трафику проходить между этими конечными точками. NBG6615 обеспечивает прохождение через это устройство следующих типов трафик VPN:

- IP security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP)

13.4 Экран General межсетевого экрана

Этот экран используется для включения/отключения межсетевого экрана NBG6615 и настройки журнала сетевого экрана. Для перехода на экран **General** щелкните **Security > Firewall**.

Иллюстрация 66 Security > Firewall > General

В следующей таблице описаны поля этого экрана.

Таблица 36 Security > Firewall > General

ПОЛЕ	ОПИСАНИЕ
Enable Firewall	Это опция включения межсетевого экрана. Когда включен межсетевой экран NBG6615 контролирует доступ и защищает от атак Denial of Service (DoS).
Enable DoS Defense	Опция защиты от атак DoS. NBG6615 будет разрывать сессии которые не установлены полностью (half-open sessions) и превышают пороговое значение.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

13.5 Экран Services

Этот экран используется для включения/отключения функций ICMP и VPN passthrough.

Щелкните **Security > Firewall > Services**. Откроется следующий экран.

Иллюстрация 67 Security > Firewall > Services

В следующей таблице описаны поля этого экрана.

Таблица 37 Security > Firewall > Services

ПОЛЕ	ОПИСАНИЕ
ICMP	Internet Control Message Protocol (ICMP) - это протокол управления сообщениями между хост-сервером и шлюзом в Интернете, а также для генерации отчетов об ошибках. ICMP использует датаграммы Internet Protocol (IP), но сообщения обрабатывает программное обеспечение TCP/IP и их может прочесть пользователь приложений.
Respond to Ping on WAN	Если в этом поле стоит галочка, то NBG6615 отвечает на все входящие из WAN запросы Ping.
VPN Passthrough	Поставьте галочку чтобы включить дополнительные функции pass through: • IPSEC Passthrough: эта опция позволяет NBG6615 передавать трафик VPN с помощью протокола IPsec. • PPTP Passthrough: эта опция позволяет NBG6615 передавать трафик VPN с помощью протокола PPTP. • L2TP Passthrough: эта опция позволяет компьютерам в LAN устанавливать соединения L2TP VPN с серверами в Интернете.
Apply	Щелкните **Apply** для сохранения изменений.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

13.6 Экран MAC Filter

Этот экран используется для включения/отключения фильтра MAC-адресов, который разрешает определенным MAC-адресам посылать трафик через межсетевой экран

Щелкните **Security > Firewall > MAC Filter Screen**. Откроется следующий экран.

Иллюстрация 68 Security > Firewall > Services

В следующей таблице описаны поля этого экрана.

Таблица 38 Security > Firewall > MAC Filter

ПОЛЕ	ОПИСАНИЕ
Enable MAC Filtering	Выберите **Enable** чтобы включить фильтр MAC-адресов.
MAC Address	Введите MAC-адрес для внесения в белый список межсетевого экрана в стандартном формате (6 пар шестнадцатеричных цифр, например, 12:34:56:78:9a:8c). Двоеточия вводить не надо.
Comment	В это поле можно добавить комментарии к MAC-адресам из белого и черного списка.
Apply	Щелкните **Apply** для сохранения изменений.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.
Current Filter Table	
MAC Address	Список разрешенных MAC-адресов.
Application name	В это поле можно добавить идентифицирующую информацию и комментарии к MAC-адресам из белого списка.
Select	Щелкните это поле для выбора записи, которую нужно изменить.

Глава 14
Content Filter

14.1 Обзор

Фильтр контента (Content filter) блокирует определенные URL-адреса.

При блокировке по ключевым словам NBG661 отдельно проверяет имя домена или IP-адрес URL и путь к файлу.

Имя домена или IP-адрес URL – это первые символы в URL после знака “/”, например, в URL-адресе www.zyxel.com.tw/news/pressroom.php имя домена - это www.zyxel.com.tw, а путь к файлу - news/pressroom.php.

Поскольку NBG6615 проверяет имя домена или IP-адрес URL по отдельности, он не может найти комбинацию слов на границе этих двух объектов, например, в URL-адресе www.zyxel.com.tw/news/pressroom.php NBG6615 найдет “tw” в имени домена (www.zyxel.com.tw) и “news” в имени пути (news/pressroom.php), но не сможет найти “tw/news.”

14.2 Экраны, которые описаны в этой главе

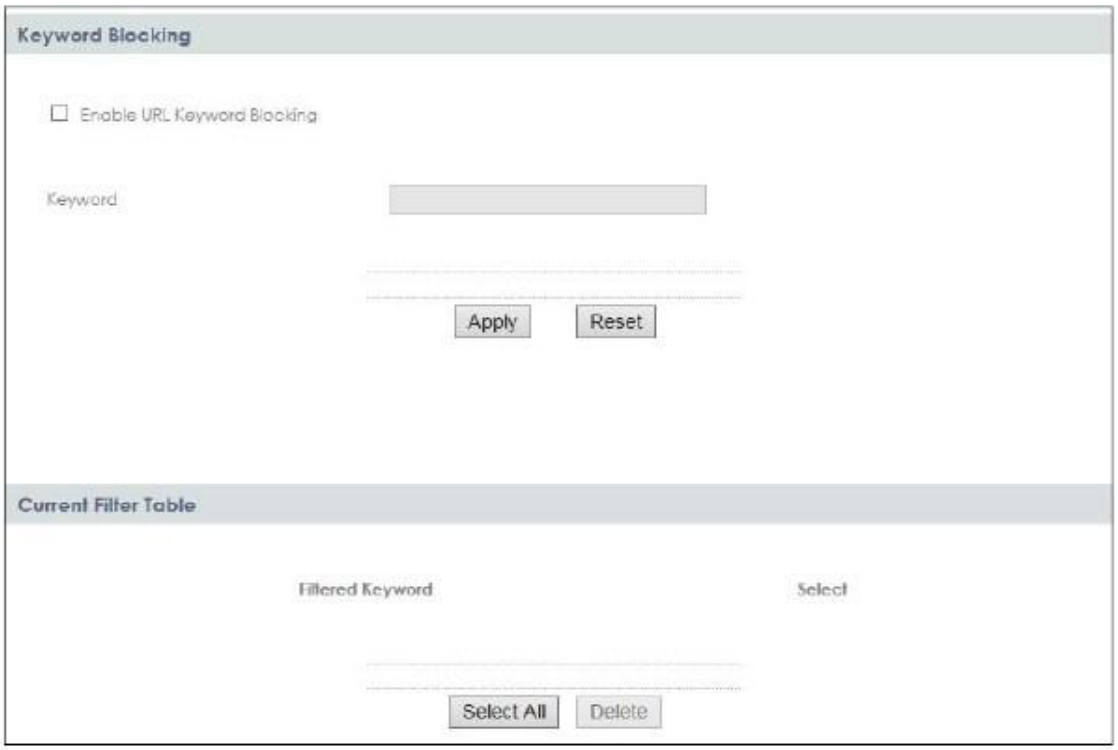
Экран **Filter** позволяет заблокировать доступ пользователей вашей сети к определенным web-сайтам (Раздел 14.3 на стр. 104).

14.3 Экран Filter

Экран **Filter** используется для включения блокировки по ключевым словам и добавления ключевых слов для блокировки.

Щелкните **Security > Content Filter**. Откроется следующий экран.

Иллюстрация 69 Security > Content Filter > Filter



В следующей таблице описаны поля этого экрана.

Таблица 39 Security > Content Filter > Filter

ПОЛЕ	ОПИСАНИЕ
Enable URL Keyword Blocking	NBG6615 может блокировать определенные Web-сайты, у которых в URL есть ключевые слова в имени домена или IP-адресе, например, если задать блокировку по ключевому слову "bad", то будет заблокирован доступ ко всем сайтам, у которых в имени домена или IP-адресе есть это слово, например, URL http://www.website.com/bad.html. Выберите **Enable** чтобы включить эту функции либо **Disable** чтобы отключить ее.
Keyword	Введите в это поле ключевое слово. Можно использовать до 64 любых символов. Метасимволы нельзя использовать. Также можно ввести в это поле IP-адрес из цифр.
Apply	Щелкните эту клавишу после ввода ключевого слова для его внесения в таблицу Content Filter. Когда пользователь попытается получить доступ к web-странице с этим ключевым словом, то Content Filter выдаст сообщение, что доступ к этому сайту заблокирован.
Reset	Щелкните эту кнопку чтобы заново сконфигурировать этот экран.
Current Filter Table	
Filtered Keyword	Отображение ключевых слов, которые уже используются для блокировки.
Select	Щелкните чтобы выбрать запись и затем щелкните **Delete Selected Keyword** чтобы удалить ее.
Select All	Щелкните выбрать все записи.
Delete	Щелкните чтобы удалить выбранные записи.

Глава 15
Remote Management (удаленное управление)

15.1 Обзор

Эта глава посвящена экрану **Remote Management**.

Примечание: Если вы настраиваете удаленное управление из WAN, то нужно дополнительно настроить правило межсетевого экрана чтобы разрешить доступ к NBG6615 из WAN (см. Главу, посвященную межсетевому экрану).

15.1.1 Ограничения удаленного управления

Удаленное правление из WAN не сможет работать если:

1. Этот сервис отключен на экране **Remote Management**.
2. IP-адрес в поле **Secured Client WAN IP Address** отличается от IP-адреса клиента. В этом случает NBG6615 автоматически прекратит сессию.
3. Уже выполняется другая сессия удаленного управления с таким же или большим приоритетом (одновременно нельзя запускать несколько сессий удаленного управления).
4. Доступ заблокирован правилом межсетевого экрана.

15.1.2 Удаленное управление и NAT

Если NAT включен:

- Используйте IP-адрес WAN NBG6615 при конфигурировании из WAN.
- Используйте IP-адрес LAN NBG6615 при конфигурировании из LAN.

15.1.3 Тайм-аут системы

По умолчанию используется тайм-аут системы 5 минут (300 секунд). NBG6615 автоматически прервет сессию управления если никаких действий не производится в течение тайм-аута. Прерывания сессии управления не происходит когда выполняется опрос с помощью экрана статистики. Продолжительность тайм-аута можно изменить на экране **System**.

15.2 Экран WWW

Для изменения настроек World Wide Web вашего, щелкните **Management > Remote MGMT** для отображения экран **WWW**.

Иллюстрация 70 Management > Remote MGMT > WWW

В следующей таблице описаны поля этого экрана.

Таблица 40 Management > Remote MGMT > WWW

ПОЛЕ	ОПИСАНИЕ
Enable HTTP from the WAN side	Если в этом поле стоит галочка, то NBG6615 можно сконфигурировать из WAN по HTTP с помощью web-браузера
Server Port	При необходимости можно менять номер **Server port** для сервиса, но при этом этот же номер порта нужно использовать чтобы с помощью этого сервиса можно было выполнять удаленное управление.
Secured Client WAN IP Address	**Secured Client** – это проверенный (trusted) компьютер, для которого разрешен доступ к NBG6615 с использованием этого сервиса. Если выбрать **All**, то только у компьютеров с указанным IP-адресом будет доступ к NBG6615 с использованием этого сервиса. Примечание: Это относится только к IP-адресам WAN.
Apply	Щелкните **Apply** для сохранения настроек и выхода из этого экрана.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Глава 16
Universal Plug-and-Play (UPnP)

16.1 Обзор

В этой главе описывается конфигурирование функции UPnP в Web Configurator.

Universal Plug and Play (UPnP) – это открытый стандарт распределенных сетей, обеспечивающий с помощью TCP/IP простое сетевое соединение между устройствами peer-to-peer. Устройства UPnP могут динамически подключаться к сети, получать IP-адрес, использовать свой функционал и узнавать о других устройства, подключенных к сети, а когда такое устройство больше не используется, то оно автоматически корректно отключается от сети.

16.2 Что нужно знать

Как узнать, что я использую UPnP?

Оборудование UPnP отмечается пиктограммой в папке Network Connections (Windows XP). Каждое совместимое с UPnP устройство вашей сети отмечается отдельной пиктограммой. Для того, чтобы посмотреть информацию и свойства устройства UPnP, нужно щелкнуть по его пиктограмме.

NAT Traversal

UPnP NAT traversal автоматизирует процесс разрешения приложениям работать через NAT. Сетевые устройства UPnP могут автоматически сконфигурировать сетевые адреса, объявить о своем присутствии в сети другим устройствам UPnP и включить автоматический обмен простыми описаниями продуктов и сервисов. NAT traversal обеспечивает:

- Dynamic port mapping (динамическое отображение портов)
- Определение публичных IP-адресов
- Выделение времени лизинга для mappings

Примером приложения, поддерживающего NAT traversal и UPnP, является Windows Messenger.

Подробнее механизм NAT описан в главе «NAT».

Предупреждение о рисках при использовании UPnP

Приложения NAT traversal автоматически внедряют собственные сервисы и открывают порты межсетевого экрана, что может создать угрозу безопасности сети. В некоторых сетях пользователи с помощью могут получить информацию о сети и ее конфигурации и менять ее параметры.

Когда устройство UPnP подключается к сети, то оно объявляет о своем присутствии с помощью сообщения multicast. Из соображений безопасности в NBG6615 сообщения multicast разрешены только для LAN.

Все поддерживающие устройства UPnP могут свободно обмениваться данным без дополнительного конфигурирования. Если вам не нужна эта функциональность, то отключите UPnP.

16.3 Экран UPnP

Этот экран используется для включения UPnP. Для перехода к нему щелкните **Management > UPnP**.

Иллюстрация 71 Management > UPnP > General

В следующей таблице описаны поля этого экрана.

Таблица 41 Management > UPnP > General

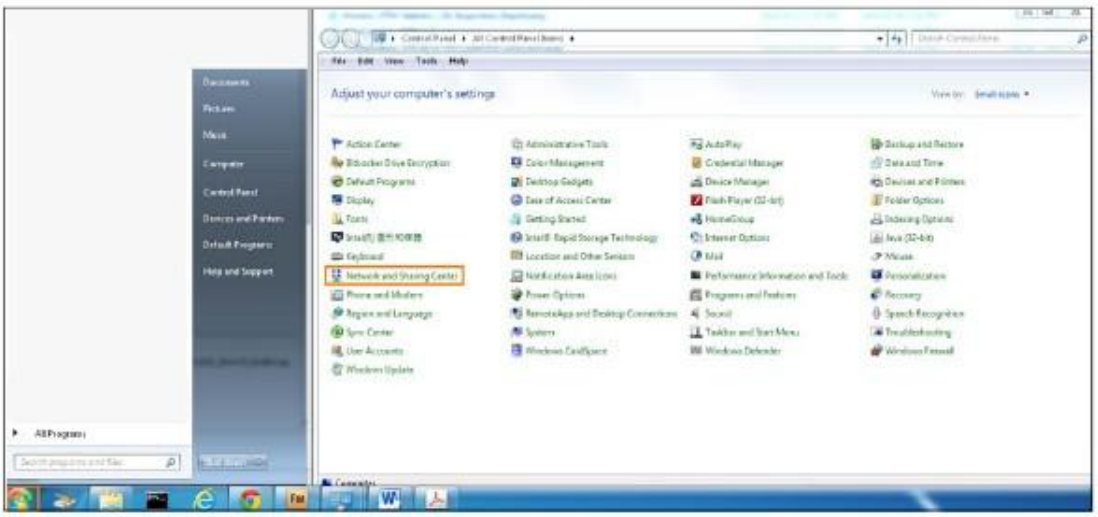
ПОЛЕ	ОПИСАНИЕ
Host Name	Описание маршрутизатора NBG6615.
Enable the Universal Plug and Play (UPnP) Feature	Чтобы включить UPnP поставьте галочку в **Enable the UPnP Features**. При этом нужно учитывать, что любой пользователь может с помощью приложения UPnP попасть на login-экран Web Configurator без указания IP-адреса (однако для доступа к Web Configurator ему нужно ввести пароль).
Apply	Щелкните **Apply** для сохранения настроек на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

16.4 Пример инсталляции UPnP в Windows 7

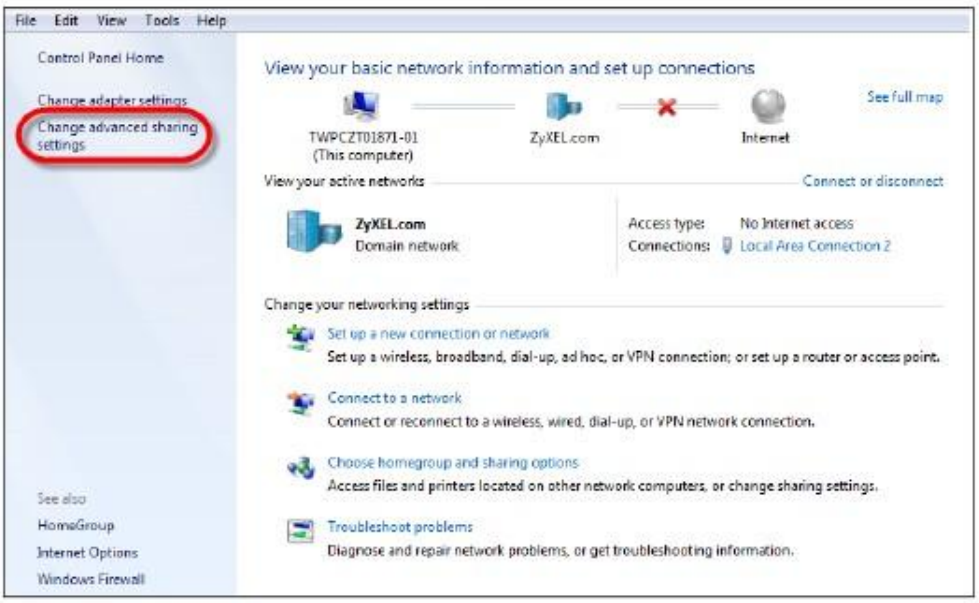
В этом примере показано, как можно использовать функцию UPnP в Windows 7. Сервер UpnP инсталлирован в Windows 7. Вам нужно включить UpnP на NBG6615.

Ваш компьютер должен быть подключен к LAN-порту NBG6615. Включите компьютер и NBG6615.

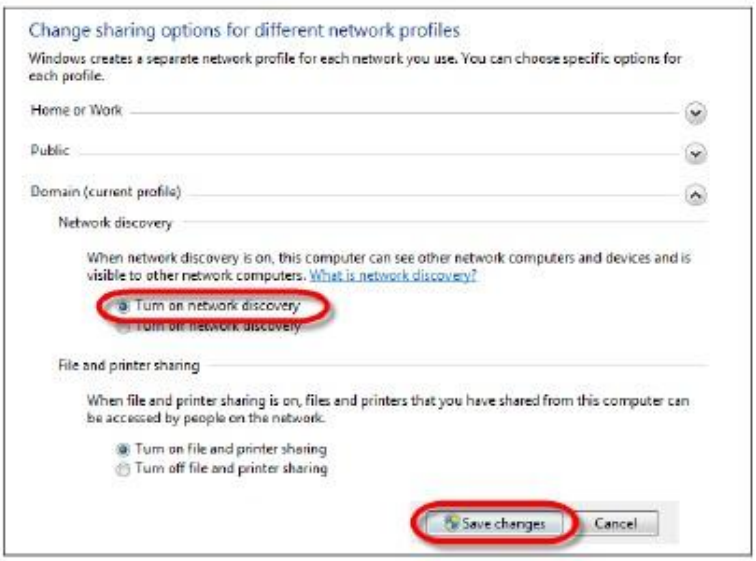
1 Щелкните пиктограмму **Start**, затем **Control Panel** и **Network and Sharing Center**.



2 Щелкните **Change advanced sharing settings**.



3 В разделе **Network Discovery** включите **Turn on network discovery** и щелкните **Save Changes**. С помощью Network discovery ваш компьютер сможет находить в сети другие компьютеры и устройства, и они в свою очередь также смогут находить ваши компьютер. Эта функция очень удобна для совместного использования файлами и принтерами.



16.4.1 Пример использования UPnP в Windows XP

В этом разделе объясняется, как можно использовать функцию UPnP в XP. Для этого нужно инсталлировать UPnP в Windows XP и включить UPnP на NBG6615.

Убедитесь, что компьютер подключен к LAN-порту NBG6615. Включите ваш компьютер и NBG6615.

16.4.1.1 Автоматическое обнаружение в сети устройств, поддерживающих UPnP

1 Щелкните пиктограмму **Start** и and **Control Panel**. Дважды щелкните **Network Connections**. Под **Internet Gateway** появится пиктограмма.

2 Щелкните правой кнопкой пиктограмму и выберите **Properties**.

Иллюстрация 72 Network Connections

3 В окне **Internet Connection Properties** выберите **Settings** чтобы увидеть port mapping, которые были автоматически созданы.

Иллюстрация 73 Internet Connection Properties

4 Можно изменить или удалить port mappings либо, щелкнув **Add to manually** добавить port mappings.

Иллюстрация 74 Internet Connection Properties: Advanced Settings

Иллюстрация 75 Internet Connection Properties: Advanced Settings: Add

Примечание: При отключении поддерживающих UPnP устройств все port mappings автоматически удаляются.

5 Выберите опцию **Show icon in notification area when connected** и щелкните **OK**. В панели уведомлений появится пиктограмма.

Иллюстрация 76 Пиктограмма в панели уведомлений

6 Дважды щелкните по пиктограмме чтобы вывести текущий статус соединения с Интернетом.

Иллюстрация 77 Internet Connection Status

16.4.2 Удобный доступ к Web Configurator

При использовании UPnP можно получить доступ к Web Configurator в NBG6615 даже если вы не знаете IP-адрес NBG6615.

Ниже описана процедура, которую нужно выполнить чтобы получить доступ к Web Configurator.

1 Щелкните пиктограмму **Start** и затем **Control Panel**.

2 Дважды щелкните **Network Connections**.

3 Выберите **My Network Places** под **Other Places**.

Иллюстрация 78 Network Connections

4 Под **Local Network** появится пиктограмма с описанием для каждого поддерживающего UPnP устройства.

5 Щелкните правой кнопкой пиктограмму вашего NBG6615 и выберите **Invoke**. Откроется экран **Login** из Web Configurator.

Иллюстрация 79 Network Connections: My Network Places

6 Щелкните правой кнопкой пиктограмму вашего NBG6615 и выберите **Properties**. Откроется окно свойств Properties, в котором выводится основная информация о NBG6615.

Иллюстрация 80 Пример Network Connections: My Network Places: Properties

Глава 17
Bandwidth MGMT (управление полосой пропускания)

17.1 Обзор

Управление полосой пропускания (Bandwidth Management) позволяет удобно контролировать использование различных сетевых сервисов. Bandwidth Management используется для управления обычными протоколами (например, HTTP и FTP) и назначает приоритеты трафику для улучшения работы приложений, чувствительных к задержкам, например, связанных с передачей голоса и видео.

17.2 Экраны, которые описаны в этой главе

•Экран **Bandwidth MGMT** для включения этой функции NBG6615.

• Экран **Advanced** для настройки правила QoS (Quality of Service) на NBG6615.

17.3 Основные сведения

Суммарная полоса пропускания, которая выделяется интерфейсу WAN (от LAN к WAN, от WLAN к WAN) не должна быть больше значения Upstream Bandwidth, которые вы задали на экране Bandwidth Management **Advanced**.

Суммарная полоса пропускания, которая выделяется интерфейсу WAN (от LAN к WAN, от WLAN к WAN) не должна быть больше значения Downstream Bandwidth, которые вы задали на экране Bandwidth Management **Advanced**.

17.4 Экран Bandwidth MGMT

Этот экран используется для включения функции Bandwidth Management в NBG6615. Щелкните **Management > Bandwidth MGMT**. Откроется следующий экран.

Иллюстрация 81 Management > Bandwidth MGMT

В следующей таблице описаны поля этого экрана.

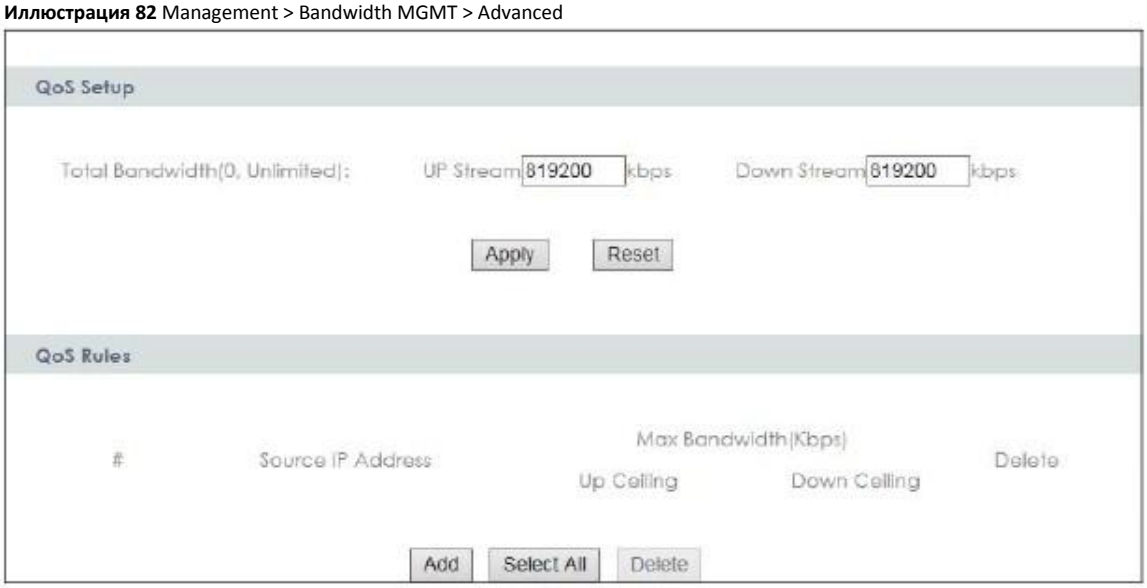
Таблица 42 Management > Bandwidth MGMT > Bandwidth MGMT

ПОЛЕ	ОПИСАНИЕ
Service Management	
Enable Bandwidth Management	Для включения управления полосой пропускания в NBG6615 поставьте галочку в **Enable Bandwidth Management**.
Apply	Щелкните **Apply** для сохранения изменений этого экрана.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

17.5 Экран Advanced

Этот экран используется для настройки правил QoS для NBG6615. Щелкните **Management > Bandwidth MGMT > Advanced**. Откроется следующий экран.

Иллюстрация 82 Management > Bandwidth MGMT > Advanced



В следующей таблице описаны поля этого экрана.

Таблица 43 Management > Bandwidth MGMT > Advanced

ПОЛЕ	ОПИСАНИЕ
QoS Setup	
Total Bandwidth (0, Unlimited)	Максимальный объем данных (в килобайтах), который NBG6615 может послать и получить через интерфейс.
Up Stream	Введите **Up Stream** или максимальную скорость исходящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG6615.
Down Stream	Введите **Down Stream** или максимальную скорость входящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG6615.
Apply	Щелкните **Apply** для сохранения изменений на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.
QoS Rules	

Таблица 43 Management > Bandwidth MGMT > Advanced (продолжение)

ПОЛЕ	ОПИСАНИЕ
#	Номер правила QoS.
Source IP Address	IP-адрес источника данных.
Max Bandwidth (kpbs)	
Up Ceiling	Максимальная скорость входящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG6615.
Down Ceiling	Максимальная скорость исходящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG6615.
Delete	Поставьте галочку в **Delete** чтобы отметить правило QoS, которое нужно удалить.
Add	Щелкните кнопку **Add** чтобы добавить правило QoS.
Select All	Щелкните **Select All** для выбора всех правил.
Delete	Щелкните **Delete** для удаления правила QoS.

Глава 18
System

18.1 Обзор

В этой главе описаны экраны System.

18.2 Экраны, которые описаны в этой главе

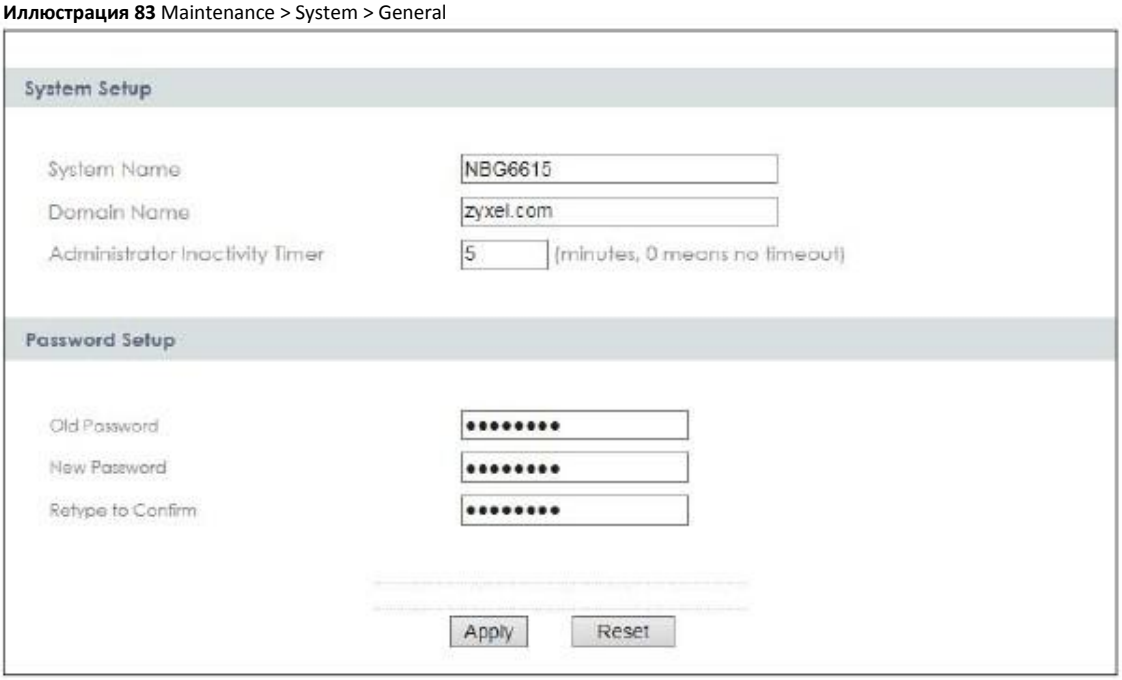
Экран **General** для ввода имени, по которому можно найти NBG6615 в сети, и пароля (Раздел 18.3 на стр. 120).

• Экран **Time Setting** для изменения времени и даты на часах NBG6615 (Раздел 18.4 на стр. 121).

18.3 Экран General

Этот экран используется для ввода имени, по которому можно найти NBG6615 в сети, и пароля. Щелкните **Maintenance > System**. Откроется следующий экран.

Иллюстрация 83 Maintenance > System > General



В следующей таблице описаны поля этого экрана.

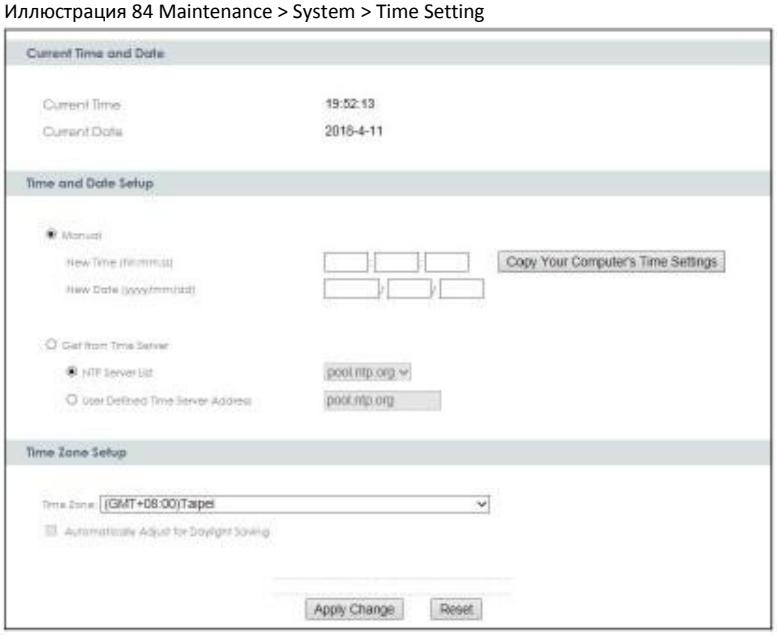
Таблица 44 Maintenance > System > General

ПОЛЕ	ОПИСАНИЕ
System Setup	
System Name	**System Name** – это уникальное имя NBG6615 в сети Ethernet. В это поле рекомендуется ввести имя вашего компьютера (в главе, где описан визард, объясняется, как узнать имя компьютера). Имя может состоять из 30 букв и цифр без пробелов (тире “-” и символ подчеркивания "_" можно использовать).
Domain Name	Введите в это поле имя домена **Domain name** (если вы его знаете). Это имя будут использовать все клиенты DHCP когда включен сервер DHCP.
Administrator Inactivity Timer	Значение этого поля определяет тайм-аут (в минутах) отключения сессии управления по бездействию. Значение по умолчанию – 5 минут. После истечения тайм-аута нужно снова подключиться и ввести пароль. Длительные тайм-ауты создают риски безопасности. Если в этом поле стоит "0", то сессия управления не отключается по бездействию, что создает большие риски безопасности, поэтому не рекомендуем использовать нулевое значение.
Password Setup	Эти поля для изменения пароля NBG6615 (рекомендуем периодически менять пароль).
Old Password	Введите в это поле существующий пароль или пароль по умолчанию.
New Password	Введите в это поле новый пароль системой длиной до 30 символов. При вводе пароля на экране вместо символов отображаются звездочки (*).
Retype to Confirm	Введите еще раз новый пароль в это поле.
Apply	Щелкните **Apply** для сохранения настроек на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

18.4 Экран Time Setting

Если нужно изменить время и дату на часах NBG6615, то щелкните **Maintenance > System > Time Setting**. Откроется следующий экран, на котором можно настроить часы NBG6615 с учетом часового пояса.

Иллюстрация 84 Maintenance > System > Time Setting



В следующей таблице описаны поля этого экрана.

Таблица 45 Maintenance > System > Time Setting

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	Текущее время часов NBG6615. При каждой перезагрузке этой страницы NBG6615 синхронизирует свои часы с сервером точного времени.
Current Date	Текущая дата NBG6615. При каждой перезагрузке этой страницы NBG6615 синхронизирует дату с сервером точного времени.
Time and Date Setup	
Manual	Выберите **Manual** чтобы вручную ввести время и дату. Если вы одновременно вводите новые время и дату, значения Time Zone и Daylight Saving, то время и дата имеют больший приоритет и на эти значения не влияет Time Zone и Daylight Saving.
New Time (hh:mm:ss)	В этом поле выводится текущее время, полученное от сервера точного времени или введенное вручную. Если вы в **Time and Date Setup** выбрали **Manual**, то в это поле нужно ввести новое время и щелкнуть **Apply**.
New Date (yyyy/mm/dd)	В этом поле выводится текущая дата, полученная от сервера точного времени или введенная вручную. Если вы в **Time and Date Setup** выбрали **Manual**, то в это поле нужно ввести новую дату и щелкнуть **Apply**.
Copy Your Computer's Time Settings	Щелкните кнопку **Copy Your Computer's Time Settings** чтобы скопировать на NBG6615 настройки даты и времени вашего компьютера.
Get from Time Server	Если выбрать **Get from time Server**, то NBG6615 будет синхронизировать свои часы с указанным ниже сервером точного времени.
Auto	Если выбрать **Auto**, то NBG6615 будет автоматически находить сервер точного времени и синхронизировать с ним часы после того, как вы щелкните **Apply**.
User Defined Time Server Address	Выберите **User Defined Time Server Address** и введите IP-адрес или URL (до 20 символов ASCII) сервера точного времени. Если вы не знаете этот адрес сервера точного времени, то уточните его у сервис-провайдера или системного администратора.
Time Zone Setup	
Time Zone	Выберите ваш часовой пояс **Time zone**. В этом поле указывается разница по времени вашего часового пояса и времени по Гринвичу Greenwich Mean Time (GMT).
Automatically Adjust for Daylight Saving	**Daylight** – это летнее время, когда в некоторых странах для экономии электроэнергии в середине года часы переводятся на час вперед. Если поставить в это поле галочку, то часы NBG6615 будут переводиться на летнее время.
Apply	Щелкните **Apply** для сохранения настроек на NBG6615.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Глава 19
Logs (журналы событий)

19.1 Обзор

В этой главе описывается настройка параметров журнала событий NBG6615 и просмотр этого журнала.

В Web Configurator можно просматривать все журналы событий NBG6615.

19.2 Что нужно знать

В логи (журнал событий, log) заносятся предупреждения (алерты) о ошибках, кибератаках (попытках захватить контроль) и попытках обращения к заблокированным web-сайтами или web-сайтам с ограниченным функционалом, например, cookies и active X. В такие категории сообщений, как **System Errors** вносятся и логи, и алерты, которые выводятся разным цветом на экране **View Log** (алерты красные, а логи – черные).

Алерты сразу же передаются по e-mail. Логи могут также могут передаваться по e-mail сразу после заполнения (см. **Log Schedule**). Однако если задать много категорий алертов и логов (особенно **Access Control**), то вы будете получать очень много электронных писем.

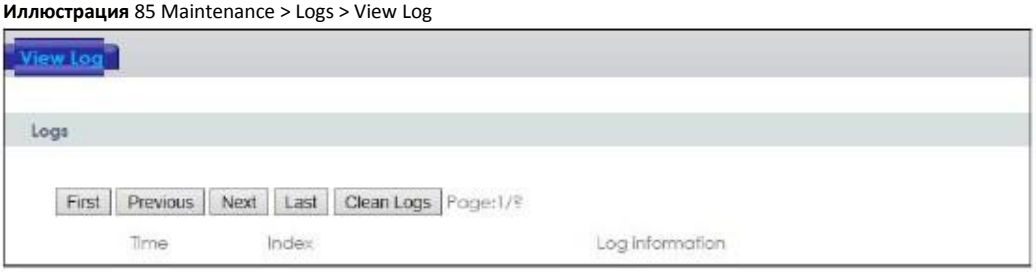
19.3 Экран View Log

На экране **View Log** выводятся внесенные в журнал событий сообщения о NBG6615. Можно выбрать категории сообщений system maintenance (обслуживание системы), system errors (системные ошибки), access control (контроль доступа), allowed web sites либо blocked (разрешенные либо заблокированные web-сайты), заблокированные web-функции, например, ActiveX controls, Java и cookies), attacks (атаки), например, DoS, и IPSec.

Если запись в журнале выделена красным цветом, то она относится к системной ошибке. Когда журнал полностью заполнен, то при поступлении новых записей старые удаляются. Для сортировки записей щелкните заголовок столбца (треугольник обозначает порядок сортировки).

Для перехода к экрану **View Log** щелкните **Maintenance > Logs**.

Иллюстрация 85 Maintenance > Logs > View Log



В следующей таблице описаны поля этого экрана.

Таблица 46 Maintenance > Logs > View Log

ПОЛЕ	ОПИСАНИЕ
First	Щелкните кнопку **First** чтобы перейти на первую страницу журнала событий.
Previous	Щелкните кнопку **Previous** чтобы перейти на предыдущую страницу журнала событий.
Next	Щелкните кнопку **Next** чтобы перейти на следующую страницу журнала событий.
Last	Щелкните кнопку **Last** чтобы перейти на последнюю страницу журнала событий.
Clean Logs	Щелкните кнопку **Clear Logs** чтобы удалить все записи в журнале.
Time	Время создания записи в логе.
Index	Номер записи лога.
Type	Тип записи лога.
Log information	Причина записи лога.

Глава 20
Tools (утилиты)

20.1 Обзор

В этой главе объясняется, как загрузить новую прошивку, сделать резервную копию конфигурационных файлов и загрузить их на устройства, перезагрузить NBG6615.

20.2 Экраны, которые описаны в этой главе

• Экран **Firmware** для загрузки прошивки на NBG6615 (Раздел 20.3 на стр. 125).

• Экран **Configuration** для просмотра заводских настроек по умолчанию, конфигурации резервного копирования и восстановления (Раздел 20.4 на стр. 127).

• Экран **Restart** для перезагрузки NBG6615 (Раздел 20.5 на стр. 128).

20.3 Экран Firmware Upload

Прошивка размещена на сайте www.zyxel.com в файле с расширением “*.bin”, имя которого обычно должно совпадает с названием модели, например “NBG6615.bin”. Загрузка выполняется с помощью HTTP (Hypertext Transfer Protocol) и занимает до 2 минут. После ее завершение происходит перезагрузка устройства.

Щелкните **Maintenance > Tools**. Следуйте инструкциям на экране для загрузки прошивки на NBG6615.

Иллюстрация 86 Maintenance > Tools > Firmware

В следующей таблице описаны поля этого экрана.

Таблица 47 Maintenance > Tools > Firmware

ПОЛЕ	ОПИСАНИЕ
Browse	Щелкните кнопку **Choose File** для найти файл .bin для загрузки. Если это файл с расширением (.zip), то его нужно разархивировать перед загрузкой.
Automatically reset default after firmware upgraded	Поставьте галочку в **Automatically reset default after firmware upgraded** чтобы NBG6615 автоматически выполнил перезагрузку после завершения загрузки прошивки.
Upload	Щелкните **Upload** чтобы начать загрузку (она занимает до 2 минут).

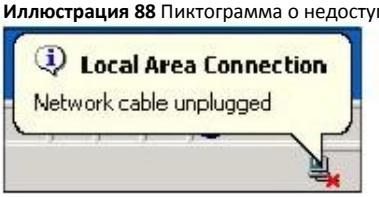
Примечание: Нельзя выключать NBG6615 во время загрузки прошивки!

После того, как на экране появится надпись **Firmware Upload In Process**, нужно подождать несколько минут и снова зайти на NBG6615.

Иллюстрация 87 Предупреждение о загрузке

При автоматической перезагрузке NBG6615 на какое-то время будет разорвано сетевое соединение. В некоторых операционных системах при этом на экране компьютера появится такая пиктограмма.

Иллюстрация 88 Пиктограмма о недоступности сети



Через 2 минуты нужно снова зайти и проверить версию прошивки на экране **Status**.

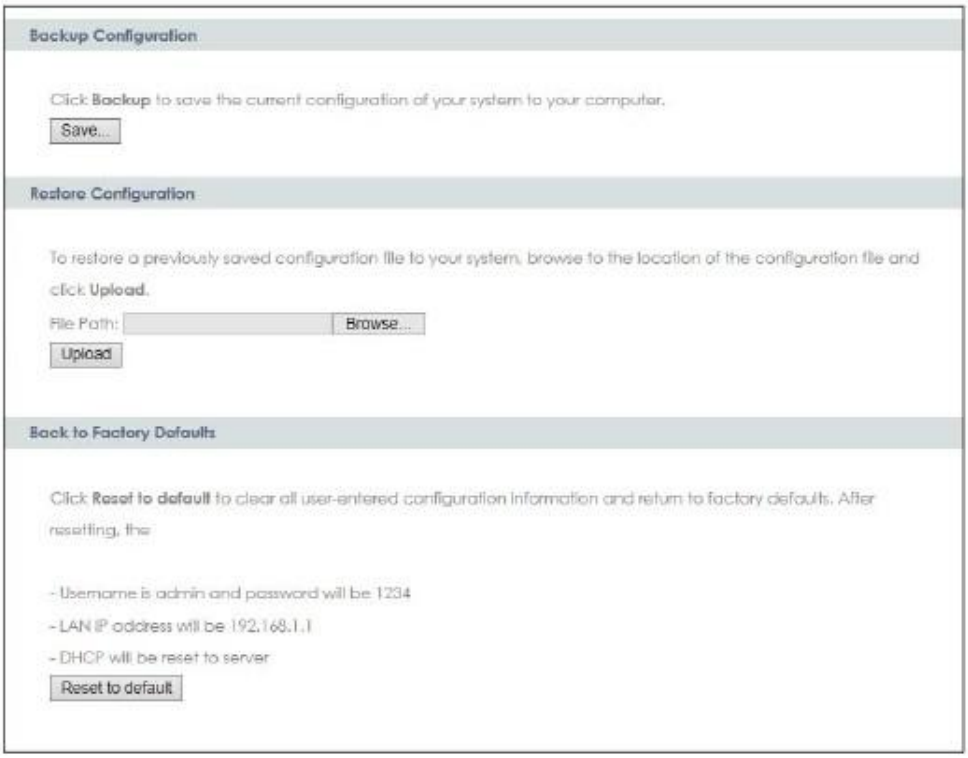
Если загрузка завершится ошибкой, то на экране будет выведено следующее окно. Щелкните **Return** чтобы вернуться на экран **Firmware**.

Иллюстрация 89 Сообщение об ошибке загрузки

20.4 Экран Configuration

Щелкните **Maintenance > Tools > Configuration**. На экран будет выведена информация о заводских настройках по умолчанию, резервном копировании конфигурации и восстановлении.

Иллюстрация 90 Maintenance > Tools > Configuration



20.4.1 Backup Configuration (резервное копирование конфигурации)

При резервном копировании вы сохраняете копию текущей конфигурации NBG6615 на вашем компьютере. Перед любым изменением конфигурации NBG6615 рекомендуется делать ее резервную копию. С ее помощью можно будет восстановить предыдущую конфигурацию если новая конфигурация окажется неправильной.

Щелкните **Backup** чтобы сохранить на вашем компьютере текущую конфигурацию NBG6615.

20.4.2 Restore Configuration (восстановление конфигурации)

Restore configuration используется для загрузки на NBG6615 новой или ранее сохраненной конфигурации, записанной на вашем компьютере.

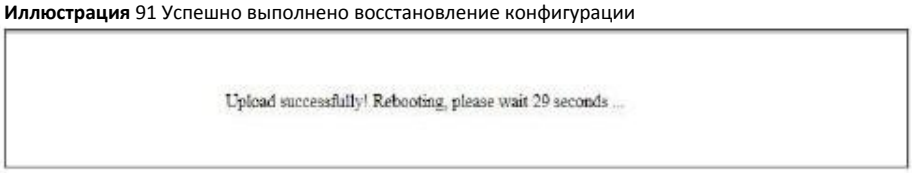
Таблица 48 Maintenance Restore Configuration

ПОЛЕ	ОПИСАНИЕ
Browse	Щелкните **Browse** чтобы найти файл с резервной копией предыдущей конфигурации, который вы сохранили на своем компьютере с помощью кнопки **Backup**.
Upload	Щелкните **Upload** чтобы начать загрузку.

Примечание: Нельзя выключать NBG6615 во время загрузки конфигурационного файла.

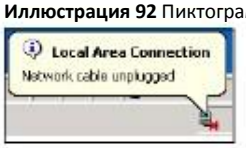
После того, как на экране появится надпись “configuration upload successful”, нужно подождать 30 секунд и снова зайти на NBG6615.

Иллюстрация 91 Успешно выполнено восстановление конфигурации



При автоматической перезагрузке NBG6615 на какое-то время будет разорвано сетевое соединение. В некоторых операционных системах при этом на экране компьютера появится такая пиктограмма.

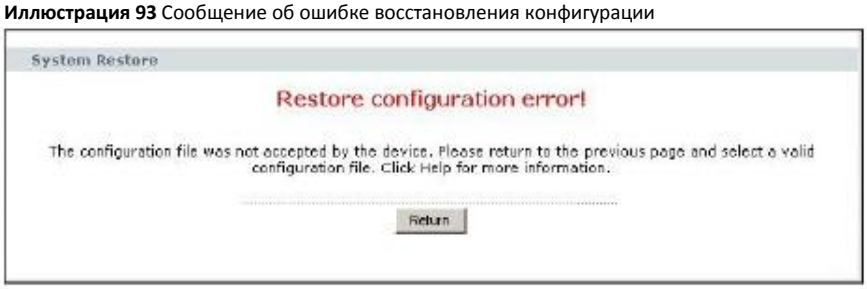
Иллюстрация 92 Пиктограмма о недоступности сети



После загрузки файла конфигурации NBG6615 по умолчанию может потребоваться изменить IP-адрес вашего компьютера чтобы он был в одной сети с IP-адресом по умолчанию (192.168.1.1 в режиме маршрутизатора). О настройке IP-адреса компьютера см. Приложение C на стр. 157.

Если загрузка завершится ошибкой, то на экране будет выведено следующее окно. Щелкните **Return** чтобы вернуться на экран **Configuration**.

Иллюстрация 93 Сообщение об ошибке восстановления конфигурации



20.4.3 Back to Factory Defaults (Восстановление заводских настроек по умолчанию)

При нажатии кнопки **Reset to default** в этом разделе будут сброшены все выполненные пользователем настройки конфигурации и будут восстановлены заводские настройки NBG6615 по умолчанию.

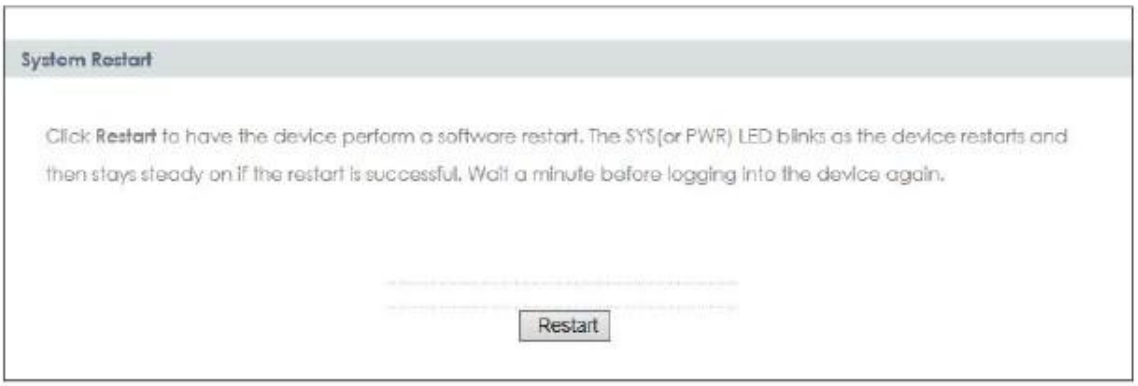
Также для сброса настроек можно нажать кнопку **Reset** на задней панели NBG6615 (о кнопке **Reset** см. Раздел 1.4.1 на стр. 14).

20.5 Экран Restart

При использовании Restart перезагрузка NBG6615 выполняет без выключения питания.

Щелкните **Maintenance > Tools > Restart**. Щелкните **Restart** для перезагрузки NBG6615. При перезагрузке конфигурация NBG6615 не меняется.

Иллюстрация 94 Maintenance > Tools > Restart



Глава 21
Sys OP Mode

21.1 Обзор

Функция Sys OP Mode (System Operation Mode) позволяет задавать режим работы устройства: маршрутизатор или точка доступа.

О выборе режима работы см. Глава 4 на стр. 28.

21.2 Экран General

На этом экран выводится информация о вашем подключении к Интернету.

Иллюстрация 95 Maintenance > Sys OP Mode > General

В следующей таблице описаны поля экрана General.

Таблица 49 Maintenance > Sys Op Mode > General

ПОЛЕ	ОПИСАНИЕ
System Operation Mode	
Router	Выберите режим **Router** если вы хотите использовать такие функции маршрутизации NBG6615 (N), как LAN DHCP, NAT, межсетевой экран и т.п. NBG6615 разделяет IP-адреса LAN и WAN.
Access Point	Выберите режим **Access Point** если в вашей сети уже есть маршрутизатор (R) и вам нужен мост между проводной и беспроводной сетью.
Apply	Щелкните **Apply** для сохранения ваших настроек.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Режим маршрутизатора:

• В этом режиме есть Ethernet-порты LAN и WAN. У этих портов разные IP-адреса.

• DHCP-сервер на вашем устройстве включен и выделяет IP-адресам другим устройствам локальной сети.

• IP-адрес LAN для NBG6615 установлен в 192.168.212.1.

• Вы можете настроить IP-адрес порта WAN (о настройках этого порта можно узнать у вашего провайдера или системного администратора.

Режим точки доступа:

• В этом режиме у всех Ethernet-портов один и тот же IP-адрес.

• Все порты на задней панели устройства – это порты LAN, в том числе и порт с надписью «WAN». Нет порта WAN.

• DHCP-сервер на вашем устройстве выключен. Этот режим можно использовать если вашей сети есть устройство, выполняющее функции DHCP-сервера (например, маршрутизатор), которое выделяет IP-адресам другим устройствам локальной сети либо вам нужно вручную назначать эти адреса.

• IP-адрес LAN для NBG6615 установлен в 192.168.1.2.

Глава 22
Language (язык)

22.1 Экран Language

На этом экране можно изменить язык, который используется в пользовательском интерфейсе Web Configurator.

Выберите нужный язык. Язык пользовательского интерфейса Web Configurator изменится без перезагрузки NBG6615.

Иллюстрация 96 Экран Language

Иллюстрация 97 Пример изменения языка

Глава III

Устранение неисправностей и приложения

Глава 23
Устранение неисправностей

В этой главе собраны рекомендации по устранению типичных проблем, возникающих при использовании устройства. Проблемы разделены на пять категорий:

23.1 Питание, подключение оборудования и светодиоды

NBG6615 не включается, все светодиоды не горят.

1. Убедитесь, что вы используете адаптер питания, который поставляются вместе с NBG6615.
2. Убедитесь, что адаптер питания подключен к NBG6615 и розетка, в которую вставлена его вилка, не обесточена.
3. Отключите и снова подключите адаптер питания к NBG6615.
4. Если проблему не удалось устранить, то обратитесь в техническую поддержку производителя.

Непонятная индикация одного из светодиодов.

1. Проверьте индикацию по таблице в Разделе 1.3 на стр. 13.
2. Проверьте подключения оборудования. См. «Инструкции по подготовке к эксплуатации» (Quick Start Guide).
3. Проверьте, не поврежден ли кабель. Если кабель нужно заменить, то обратитесь к производителю оборудования.
4. Отключите и снова подключите адаптер питания к NBG6615.
5. Если проблему не удалось устранить, то обратитесь в техническую поддержку производителя.

23.2 Доступ к NBG6615 и вход в систему

Я не знаю IP-адрес NBG6615.

1 По умолчанию IP-адрес в режиме маршрутизатора 192.168.212.1, а в режиме точки доступа - 192.168.1.2.

2 Если вы изменили IP-адрес и забыли его, то узнать IP-адрес NBG6615 в режиме маршрутизатора можно если посмотреть адрес шлюза по умолчанию (default gateway) вашего компьютера. Для этого в Windows нужно щелкнуть **Start > Run**, ввести **cmd** и затем **ipconfig**. IP-адрес в **Default Gateway** может совпадать с IP-адресом NBG6615 (это зависит от конкретной конфигурации сети). Попробуйте ввести IP-адрес **Default Gateway** в адресную строку браузера.

3 Сбросьте NBG6615 в настройки по умолчанию (см. Раздел 23.4 на стр. 137). Все ваши настройки при этом будут потеряны.

Я не помню имя пользователя и пароль.

1 По умолчанию имя пользователя **admin** и пароль **1234**.

2 Если вам не удается войти в систему с этим именем пользователя и паролем, то нужно сбросить устройство в заводские настройки по умолчанию. См. Раздел 23.4 на стр. 137.

Не могу открыть экран Login в Web Configurator.

1 Убедитесь, что вы используете правильный IP-адрес.

- По умолчанию IP-адрес в режиме маршрутизатора 192.168.212.
- Если вы изменили IP-адрес, то используйте новый IP-адрес.
- Если вы изменили IP-адрес и не помните его, то см. рекомендации «Я не знаю IP-адрес NBG6615».

2 Проверьте соединение оборудования и индикацию светодиодов. См. «Инструкции по подготовке к эксплуатации» (Quick Start Guide).

3 Убедитесь, что ваш браузер не блокирует всплывающие окна и у него включена поддержка JavaScript и Java. См. Приложение B на стр. 148.

4 Убедитесь, что ваш компьютер в одной под сети с NBG6615 (если ваш компьютер подключен к NBG6615 через маршрутизатор, то этот шаг выполнять не надо).

- Если в вашей сети есть DHCP-сервер, то убедитесь, что ваш компьютер использует динамический IP-адрес.
- Если в вашей сети нет DHCP-сервера, то убедитесь, что IP-адрес вашего компьютера в одной подсети с NBG6615.

5 Сбросьте устройство в заводские настройки по умолчанию и попробуйте зайти на NBG6615 по IP-адресу по умолчанию.

6 Если проблему не удалось устранить, то обратитесь к администратору сети или в техническую поддержку производителя, либо воспользуйтесь дополнительными рекомендациями.

Дополнительные рекомендации

• Если ваш компьютер подключен к порту WAN или к беспроводной сети, то попробуйте зайти в Web Configurator через компьютер, который подключен к порту LAN/ETHERNET.

Я открыл экран Login, но не могу зайти на NBG6615.

1 Убедитесь, что вы правильно ввели пароль. По умолчанию имя пользователя **admin** и пароль **1234**. В пароле учитывается регистр букв, поэтому проверьте, выключен ли [Caps Lock].

2 Возможно, вы некорректно вышли из предыдущей сессии. Попробуйте снова зайти через 5 минут.

3 Отключите и снова подключите адаптер питания к NBG6615.

4 Если проблему не удалось решить, то попробуйте сбросить устройство в заводские настройки по умолчанию. См. Раздел 23.4 на стр. 137.

23.3 Доступ к Интернету

У меня нет доступа к Интернету.

1 Проверьте соединение оборудования и индикацию светодиодов. См. «Инструкции по подготовке к эксплуатации» (Quick Start Guide).

2 Убедитесь, что вы правильно ввели в визарде данные своей учетной записи пользователя сервис-провайдера. При вводе учитывается регистр букв, поэтому убедитесь, что у вас выключен [Caps Lock].

3 Если вы подключаетесь к Интернету по беспроводной сети, то убедитесь, что настройки вашего беспроводного клиента совпадают с настройками точки доступа.

4 Отключите все кабели устройства и выполните указания из «Инструкций по подготовке к эксплуатации» (Quick Start Guide).

5 Перейдите **Maintenance > Sys OP Mode > General**. Проверьте настройки **System Operation Mode**.

6 Если проблему не удалось устранить, то обратитесь к вашему провайдеру.

У меня больше нет доступа к Интернету, хотя раньше я мог подключать к Интернету через NBG6615.

1 Проверьте соединение оборудования и индикацию светодиодов. См. «Инструкции по подготовке к эксплуатации» (Quick Start Guide) и Раздел 1.3 на стр. 13.

2 Перезагрузите NBG6615.

3 Если проблему не удалось устранить, то обратитесь к вашему провайдеру.

Соединение с Интернетом очень медленно или часто прерывается.

1 Возможно, сеть перегружена трафиком. Попробуйте по светодиодам (см. Раздел 1.3 на стр. 13) определить интенсивность трафика, который идет через NBG6615, и закройте часть приложений, использующих Интернет, прежде всего приложения peer-to-peer.

2 Проверьте мощность сигнала. Если он слабый, то переместите NBG6615 ближе к точке доступа и посмотрите, нет ли поблизости устройств, которые создают помехи беспроводной сети (например, печи СВЧ или точки доступа другой беспроводной сети).

3 Перезагрузите NBG6615.

4 Если проблему не удалось устранить, то обратитесь к администратору сети или в техническую поддержку производителя.

23.4 Сброс NBG6615 в заводские настройки по умолчанию

Если вы сбросите настройки NBG6615, то все ваши настройки будут потеряны и NBG6615 перезагрузится с настройками по умолчанию (имя пользователя **admin** и пароль **1234**). Вам надо будет заново ввести свои настройки.

При нажатии кнопки WPS/RESET все ваши настройки будут потеряны.

Для сброса NBG6615 нужно:

1 Убедитесь, что горит светодиод Power.

2 Нажмите кнопку WPS и отпустите ее не ранее чем через 10 секунд. Будут восстановлены заводские настройки по умолчанию NBG6615.

Если NBG6615 автоматически перезапустится, то дождитесь окончания перезагрузки NBG6615 и зайдите в Web Configurator. Имя пользователя **admin** и пароль **1234**.

Если NBG6615 не перезапустится автоматически, то попробуйте отсоединить и снова подсоединить адаптер питания и затем зайдите в Web Configurator. Имя пользователя **admin** и пароль **1234**.

23.5 Проблемы беспроводной сети

У меня нет доступа к NBG6615 или ping не проходит ни на один компьютер в WLAN.

1 Убедитесь, что на NBG6615 включена беспроводная сеть.

2 Убедитесь, что на компьютере включен адаптер беспроводной сети.

3 Убедитесь, что на адаптер беспроводной сети компьютера соответствует стандарту IEEE 802.11 и поддерживает ту же версию этого стандарта, что и NBG6615.

4 Убедитесь, что компьютер находится в зоне покрытия NBG6615.

5 Убедитесь, что компьютер использует те же настройки безопасности беспроводной сети, что и NBG6615.

6 Убедитесь, что межсетевой экран NBG6615 не блокирует трафик между WLAN и LAN.

7 Убедитесь, что не заблокирован удаленный доступ к NBG6615 через интерфейс WLAN. Проверьте настройки удаленного управления.

- Подробнее о беспроводной сети см. Главу 6 Беспроводная сеть.

После того, как я переключился из режима маршрутизатора в режим точки доступа у меня нет доступа к Web Configurator.

При переключении из режима маршрутизатора в режим точки доступа нужно вручную назначить вашему компьютеру IP-адрес в диапазоне от 192.168.1.3 до 192.168.1.254 (в режиме точки доступа NBG6615 не работает как DHCP-сервер LAN.

Изменение IP-адреса компьютера описано в Приложении C на стр. 157.

Приложение A

IP-адреса и подсеть

Это приложение описывает механизм использования IP-адресов и маски подсети.

IP-адрес идентифицирует конкретное устройство в сети. Для обмена данными по сети у всех сетевых устройств (компьютеров, серверов, маршрутизаторов, принтеров и т.п.) должен быть свой IP-адрес. Эти сетевые устройства являются хостами (host) сети.

Маска подсети определяет максимальное число хостов в сети. Также с помощью маски подсети одну сеть можно разбить на несколько подсетей.

Введение в IP-адреса

IP-адрес состоит из номера сети и номера (ID) хоста. Также как у домов, стоящих на одной улице, в адресе указано одно и то же имя, так и у компьютеров в одной сети один и тот же IP-адрес сети, а ID хоста можно считать аналогом номера дома. Маршрутизаторы на основе номера сети определяют, в какую сеть надо переслать пакеты, а ID хоста определяет, какой хост в сети должен получить эти пакеты.

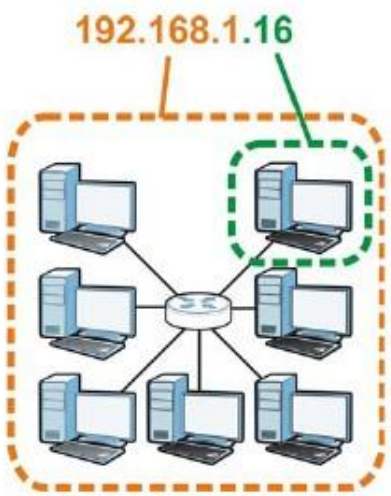
Структура

IP-адрес состоит из четырех комбинаций трех цифр, разделенных точками (например, 192.168.1.1). Эти комбинации цифр называются октетами (octet). В двоичном исчислении октет состоит из восьми цифр (например, 11000000, что соответствует десятеричном числу 192).

Значение октета можно быть от 00000000 до 11111111 в двоичном исчислении, что соответствует от 0 до 255 десятеричном исчислении.

На следующей иллюстрации показан пример IP-адреса, в котором первым три октета (192.168.1) – это номер сети, а четвертый октет – номер хоста.

Иллюстрация 98 Номер сети и ID хоста



От маски подсети зависит, какая часть IP-адреса относится к номеру сети, а какая к ID хоста.

Маски подсети

Маска подсети определяет, какие биты IP-адреса относятся к номеру сети, а какая к ID хоста («подсеть» означает часть сети).

Маска подсети состоит из 32 бит. Если в маске подсети стоит “1”, то соответствующий бит в IP-адреса является частью номера сети, а если “0”, то соответствующий бит в IP-адреса является частью ID хоста.

В следующем примере маска подсети идентифицирует номер сети (выделено полужирным шрифтом) и ID-хоста IP-адреса (192.168.1.2 в десятичной записи).

Таблица 50 Пример IP-адреса, который состоит из номера сети и ID хоста

	ПЕРВЫЙ ОКТЕТ (192)	**ВТОРОЙ ОКТЕТ (168)**	**ТРЕТИЙ ОКТЕТ (1)**	**ЧЕТВЕРТЫЙ ОКТЕТ (2)**
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Subnet Mask (двоичная)	**11111111**	**11111111**	**11111111**	00000000
Номер сети	**11000000**	**10101000**	**00000001**	
ID хоста				00000010

Маска подсети всегда должна состоять из последовательности единиц начиная с левого бита маски, за которой идет последовательность нулей, и ее общая длина должны быть 32 бита.

На маску подсети можно ссылаться по размеру той ее части, в которой записан номер сети (биты с единицами), например, «8-битная маска» обозначает что в первых 8 битах маски записана единица, а в остальных 24 битах - нули.

Маска подсети, как и IP-адрес, обозначается разделенными точками десятичными цифрами. В следующем примере показано, как двоичной и десятичном формате обозначается 8-, 16-, 24- и 29 битная маска подсети.

Таблица 51 Маски подсети

	ДВОИЧНЫЕ				DECIMAL
	ПЕРВЫЙ ОКТЕТ	**ВТОРОЙ ОКТЕТ**	**ТРЕТИЙ ОКТЕТ**	**ЧЕТВЕРТЫЙ ОКТЕТ**	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Длина номера сети определяет максимально возможное число хостов в сети. Чем больше битов относятся к адресу сети, тем меньше битов остается для ID хостов.

IP-адрес, к котором ID хоста состоит из одних нулей, является IP-адресом сети (например, 192.168.1.0 при использовании 24-битной маски подсети). IP-адрес, к котором ID хоста состоит из одних единиц, является широковещательным адресом (broadcast address) сети (например, 192.168.1.255 при использовании 24-битной маски подсети).

Эти два адреса нельзя использовать для отдельных хостов, поэтому максимально возможное число хостов в сети рассчитывается по следующей таблице:

Таблица 52 Максимально возможное число хостов

МАСКА ПОДСЕТИ		**ДЛИНА ID ХОСТА**		МАКСИМАЛЬНОЕ ЧИСЛО ХОСТОВ
8 битов	255.0.0.0	24 бита	$2^{24} – 2$	16777214
16 битов	255.255.0.0	16 битов	$2^{16} – 2$	65534
24 бита	255.255.255.0	8 битов	$2^{8} – 2$	254
29 битов	255.255.255.248	3 бита	$2^{3} – 2$	6

Обозначение

Так маска всегда – это последовательность единиц, за которой идет последовательность нулей, то вместо выписания всех ее 32 битов можно просто указать число единиц в маске. Обычно маска это обозначается IP-адресом, за которым стоит символ “/” и затем число единиц в маске.

Например, 192.1.1.0 /25 – это обозначение IP-адреса 192.1.1.0 с маской подсети 255.255.255.128.

В следующей таблице приведены некоторые возможные обозначения маски подсети.

Таблица 53 Варианты обозначения маски подсети

МАСКА ПОДСЕТИ	**ДРУГОЕ ОБОЗНАЧЕНИЕ**	**ПОСЛЕДНИЙ ОКТЕТ (ДВОИЧНЫЙ)**	**ПОСЛЕДНИЙ ОКТЕТ (ДЕСЯТИЧНЫЙ)**
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

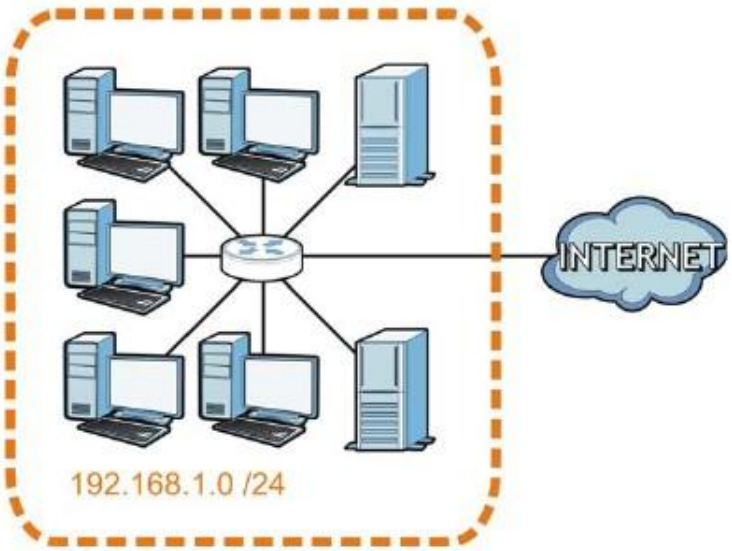
Subnetting (разделение одной сети на несколько)

С помощью механизма subnetting можно разбить одну сеть на несколько подсетей. В следующем примере администратор сети разбивает сеть на две подсети чтобы для обеспечения безопасности изолировать группу серверов от остальной сети компании.

В этом примере сети компании 192.168.1.0. Первые три октета адреса (192.168.1) – это номер сети, а последний ID хоста, поэтому в сети может быть от 2 до 254 (2^{8}) хостов.

На следующей иллюстрации показана сеть компании до применения subnetting.

Иллюстрация 99 Пример Subnetting: сеть до разбиения

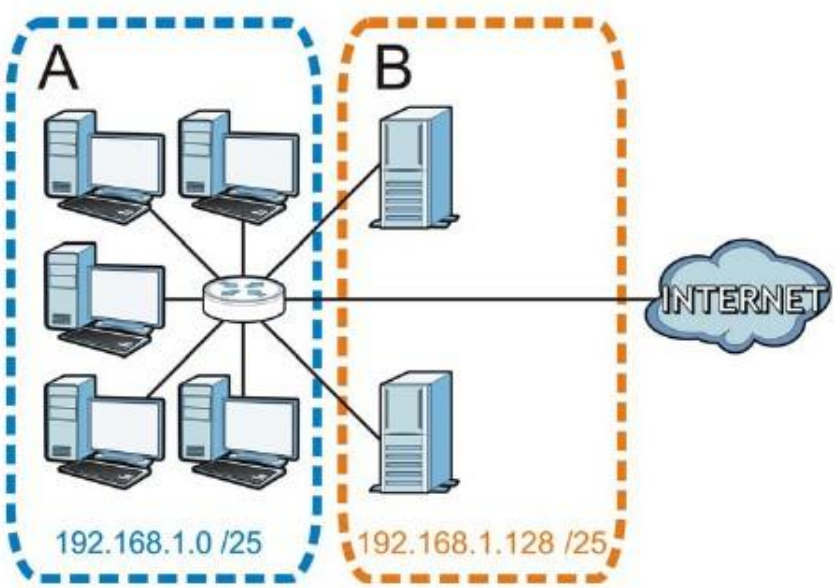


Вы можете «одолжить» один из битов ID хоста чтобы разбить сеть 192.168.1.0 на две подсети. Теперь маска подсети стала 25-битной (255.255.255.128 или /25).

«Одолженный» бит ID хоста может содержать 0 либо 1, что позволяет получить два подсети: 192.168.1.0 /25 и 192.168.1.128 /25.

На следующей иллюстрации показана сеть компании после применения subnetting. Теперь она состоит из подсетей **A** и **B**.

Иллюстрация 100 Пример Subnetting: сеть после разбиения



В 25-битной подсети ID хоста состоит из 7 битов, поэтому в каждой подсети может быть от 2 до 126 ($2^7 – 2$) хостов (ID хоста, который состоит из одних нулей, - это адрес самой подсети, а из одних единиц – это широковещательный адрес).

192.168.1.0 с маской 255.255.255.128 – это сама подсеть A, а 192.168.1.127 с маской 255.255.255.128 – это ее широковещательный адрес, поэтому начальный IP-адрес, который можно назначить хосту в подсети A – это 192.168.1.1, а конечный - 192.168.1.126.

Аналогичным образом в подсети B доступен диапазон ID хостов от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В предыдущем примере с помощью 25-битной маски подсети 24-битные адреса были разбиты на две подсети, а чтобы разбить их на четыре подсети, нужно «одолжить» два бита ID хоста, что даст четыре возможные комбинации (00, 01, 10 и 11). Маска подсети в этом примере 26-битная (11111111.11111111.11111111.11000000) или 255.255.255.192.

Каждая маска содержит 6 битов ID хоста, поэтому в каждой подсети может быть 2^6 - 2 или 62 хоста (ID хоста, который состоит из одних нулей), - это адрес самой подсети, а из одних единиц – это широковещательный адрес).

Таблица 54 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
IP-адрес (десятичный)	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	00000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.0	Начальный ID хоста: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Последний ID хоста:192.168.1.62	

Таблица 55 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
IP-адрес	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	01000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.64	Начальный ID хоста: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Последний ID хоста:192.168.1.126	

Таблица 56 Подсеть 3

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
IP-адрес	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	10000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.128	Начальный ID хоста: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Последний ID хоста:192.168.1.190	

Таблица 57 Подсеть 4

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
IP-адрес	192.168.1.	192
IP-адрес (двоичный)	11000000.10101000.00000001.	11000000

Таблица 57 Subnet 4 (продолжение)

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.192	Начальный ID хоста: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Последний ID хоста:192.168.1.254	

Пример: восемь подсетей

В этом примере с помощью 27-битной маски создаются восемь подсетей (000, 001, 010, 011, 100, 101, 110 и 111).

В следующей таблице приводятся значения последнего октета IP-адреса каждой подсети.

Таблица 58 Восемь подсетей

SUBNET	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Планирование подсети

В этой таблице показано, как можно спланировать распределение адресов в сети с 24-битным номером.

Таблица 59 Планирование подсетей в сети с 24-битным номером

НОМЕР «ОДОЛЖЕННОГО» БИТА ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	ЧИСЛО ХОСТОВ В ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

В этой таблице показано, как можно спланировать распределение адресов в сети с 16-битным номером.

Таблица 60 16 Планирование подсетей в сети с 16-битным номером

НОМЕР «ОДОЛЖЕННОГО» БИТА ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	ЧИСЛО ХОСТОВ В ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382

Таблица 60 Планирование подсетей в сети с 16-битным номером (продолжение)

НОМЕР «ОДОЛЖЕННОГО» БИТА ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	ЧИСЛО ХОСТОВ В ПОДСЕТИ
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Конфигурирование IP-адресов

Получение номера сети зависит от конкретной ситуации. Если провайдер или администратор сети выделяет вам блок зарегистрированных IP-адресов, то выполните следующие инструкции для выбора IP-адресов и маски подсети.

Если провайдер не выделяет вам конкретный номер IP сети, то скорее всего у вас учетная запись на одного пользователя и провайдер динамически назначает вам IP-адрес при каждом вашем подключении. В этом случае рекомендуется выбрать номер сети в диапазоне от 192.168.0.0 до 192.168.255.0. Комитет Internet Assigned Number Authority (IANA) резервирует этот блок адресов специально для частного использования; не используйте никакие другие адреса (за исключением случаев, когда это требует ваш провайдер). Также нужно включить Network Address Translation (NAT) на NBG6615.

После выбора номера сети выберите IP-адрес для NBG6615, который легко запомнить (например, 192.168.1.1), но надо убедиться, что этот IP-адрес не использует другое устройство в вашей сети.

Маска подсети определяет часть IP-адреса, которая относится к номеру сети. NBG6615 автоматически рассчитает маску подсети на основе введенного вами IP-адреса. Эту маску подсети, которую рассчитал NBG6615, нельзя менять (за исключением случаев, когда это требует ваш провайдер).

Частные IP-адреса

Каждый компьютер в Интернете должен иметь свой уникальный номер. Если ваша сеть изолирована от Интернета (например, соединяет только два филиала), то хостам можно назначать IP-адреса без ограничений, однако комитет Internet Assigned Numbers Authority (IANA) зарезервировал следующие три блока IP-адресов для частных сетей:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

Вы можете получить свой IP-адрес от IANA, вашего провайдера либо он может быть назначен из частной сети. Если у вас небольшая организация и вы подключены к Интернету через провайдера, то он может предоставить вам Интернет-адреса для вашей сети, а если вы являетесь подразделением крупной организации, то нужно узнать у вашего системного администратора, какие IP-адреса можно использовать.

В любом нельзя произвольно назначать IP-адреса, обязательно следуйте приведенным выше указаниям. Подробнее о назначении адресов см. документ «RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space».

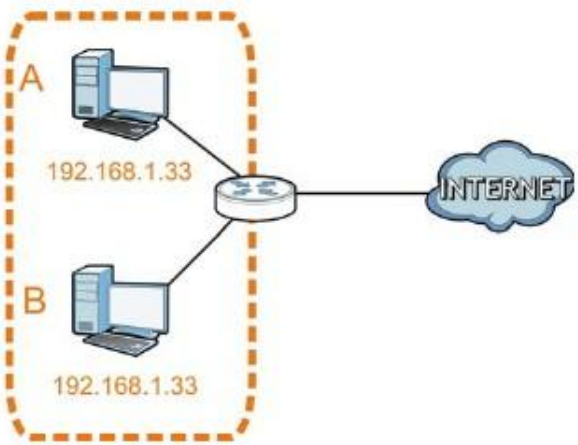
Конфликты IP-адресов

У каждого устройства в сети должен быть уникальный IP-адрес. Если у двух устройств в одной сети один и тот же IP-адрес, но у них будут проблемы доступа к Интернету и другим сетевым ресурсам, а также они сами могут быть недоступны в сети.

Пример конфликта IP-адресов компьютеров

Два устройства не могут использовать один и тот же IP-адрес. В следующем примере у компьютера A статический (фиксированный) IP-адрес, который совпадает с IP-адресом, который компьютер B получил от DHCP-сервера и в результате у обоих компьютеров нет доступа к Интернету. Для устранения проблемы нужно назначить компьютеру A другой статический адрес либо настроить этот компьютер на автоматическое получение IP-адреса.

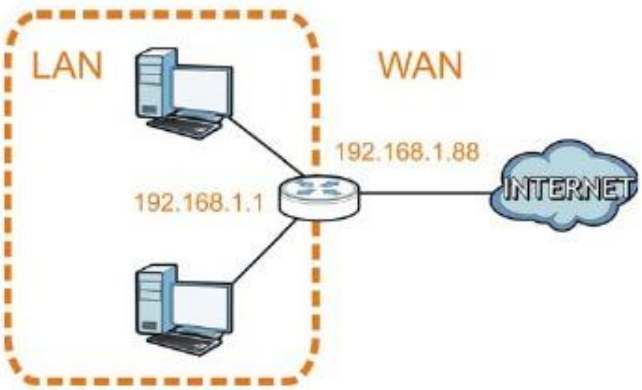
Иллюстрация 101 Пример конфликта IP-адресов компьютеров



Пример конфликта IP-адресов маршрутизатора

Маршрутизатор соединяет между собой разные сети, поэтому у него интерфейсы используют разные номера сетей. Например, если маршрутизатор подключает LAN к Интернету (WAN), то у него должны быть адреса LAN и WAN из разных подсетей. Компьютеры из LAN не могут получить доступ к Интернету, потому что маршрутизатор не может перенаправлять трафик между сетями.

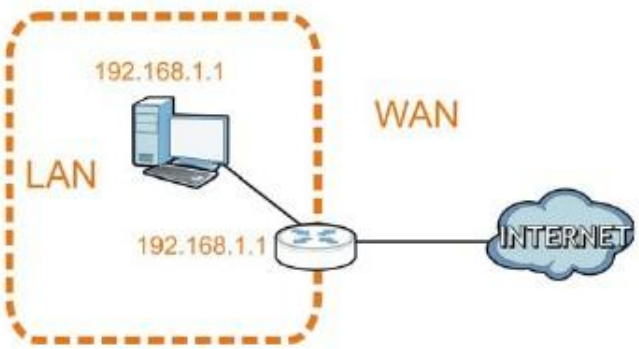
Иллюстрация 102 Пример конфликта IP-адресов компьютера и маршрутизатора



Пример конфликта IP-адресов компьютера и маршрутизатора

Два устройства не могут использовать один и тот же IP-адрес. В следующем примере у компьютера и LAN-порта маршрутизатора один и тот же IP-адрес 192.168.1.1 и поэтому у компьютера нет доступа к Интернету. Для решения проблемы нужно изменить IP-адрес у компьютера или порта LAN маршрутизатора.

Иллюстрация 103 Пример конфликта IP-адресов компьютера и маршрутизатора



Приложение B

Всплывающие окна Windows, запуск JavaScripts и Java

Для использования Web Configurator нужно разрешить:

- Всплывающие окна Web-браузера на вашем устройстве.
- JavaScripts (включен по умолчанию).
- Разрешение на выполнение кода Java (включено по умолчанию).

Примечание: Ниже показаны экраны для Internet Explorer версий 6, 7 и 8. Экраны для других версий Internet Explorer могут немного отличаться.

Блокировка всплывающих окон Internet Explorer

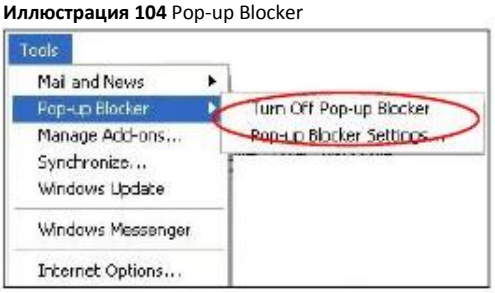
Для подключения к устройству обычно нужно отключить блокировку всплывающих окон.

Отключите эту блокировку (по умолчанию она включена в Windows XP SP (Service Pack) 2) либо разрешите блокировку с исключением для всплывающих окон с IP-адреса вашего устройства.

Отключение блокировки всплывающих окон

1 В Internet Explorer выберите **Tools**, **Pop-up Blocker** и затем **Turn Off Pop-up Blocker**.

Иллюстрация 104 Pop-up Blocker



Проверить, отключена ли блокировка, можно в разделе Pop-up Blocker под вкладкой Privacy.

1 В Internet Explorer выберите **Tools**, **Internet Options**, **Privacy**.

2 Сбросьте галочку в **Block pop-ups** в разделе **Pop-up Blocker** это экрана. Все включенные вами блокировки всплывающих окон из Интернета будут отключены.

Иллюстрация 105 Internet Options: Privacy

3 Щелкните **Apply** для сохранения настроек.

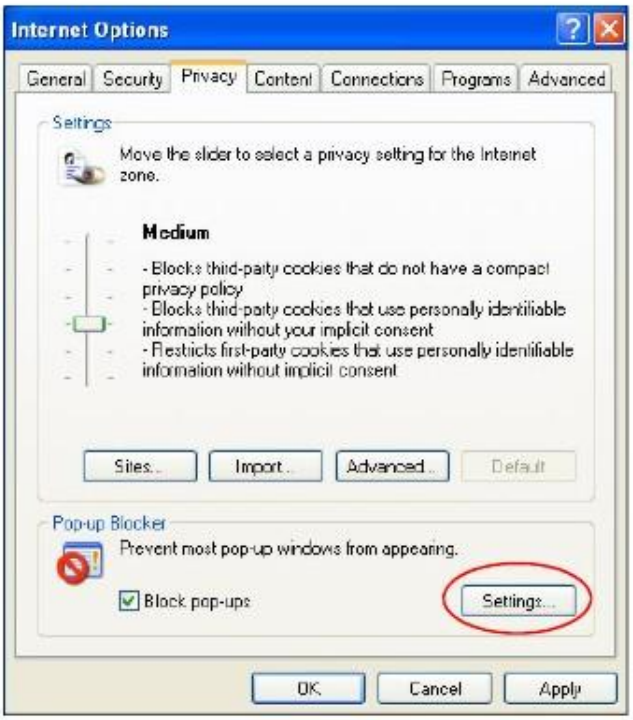
Включение блокировки всплывающих окон с исключениями

Вместо этого можно включить блокировку всплывающих окон с исключениями:

1 В Internet Explorer выберите **Tools**, **Internet Options** и затем вкладку **Privacy**.

2 Выберите **Settings...** чтобы открыть экран **Pop-up Blocker Settings**.

Иллюстрация 106 Internet Options: Privacy



3 Введите IP-адрес вашего устройства (адрес web-страницы, для которой нужно отключить блокировку всплывающих окон) с префиксом “http://”, например, http://192.168.167.1.

4 Щелкните **Add** чтобы добавить этот IP-адрес в список **Allowed sites**.

Иллюстрация 107 Pop-up Blocker Settings

5 Щелкните **Close** для возврата на экран **Privacy**.

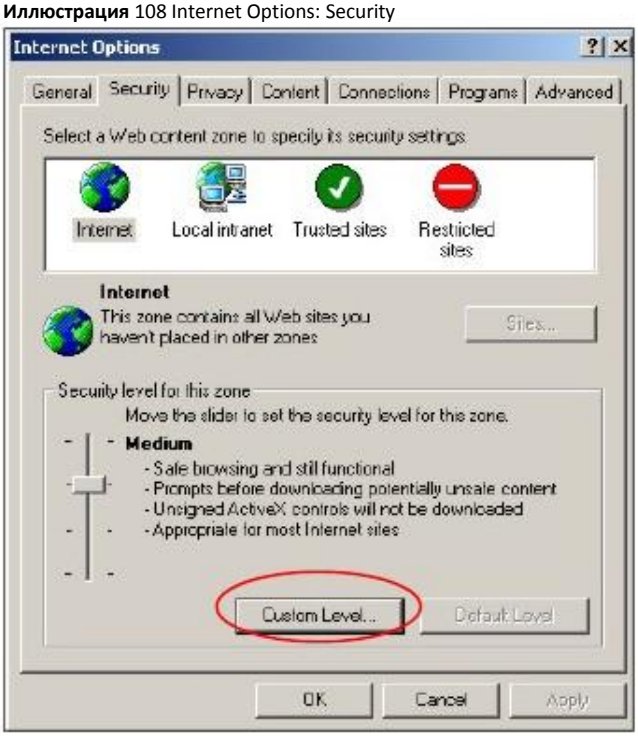
6 Щелкните **Apply** для сохранения настроек.

JavaScripts

Если страницы Web Configurator не отображаются правильно в Internet Explorer, то проверьте, не заблокирован ли JavaScripts.

1 В Internet Explorer выберите **Tools**, **Internet Options** и затем вкладку **Security**.

Иллюстрация 108 Internet Options: Security



2 Щелкните кнопку **Custom Level...**.

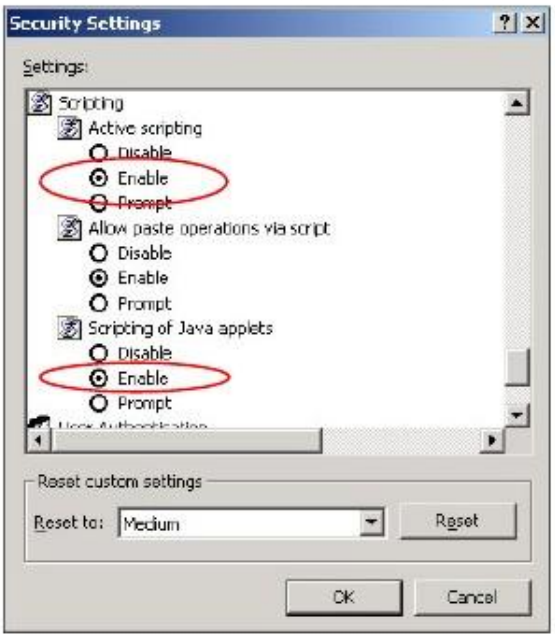
3 Прокрутите список до **Scripting**.

4 В **Active scripting** должен быть выбран пункт **Enable** (по умолчанию).

5 В **Scripting of Java applets** должен быть выбран пункт **Enable** (по умолчанию).

6 Щелкните **OK** чтобы закрыть окно.

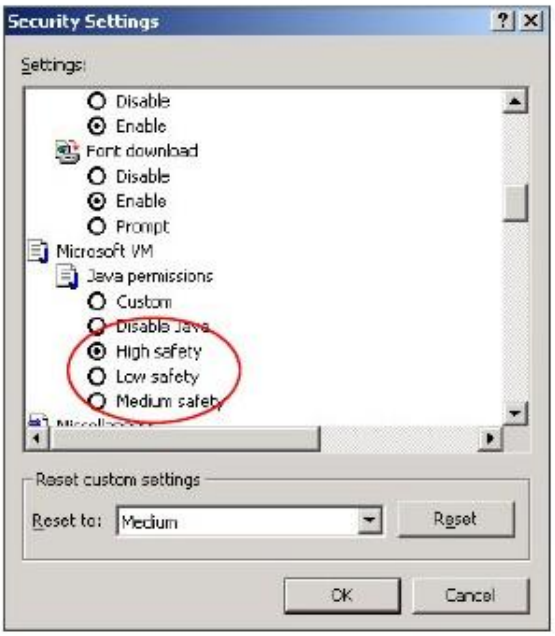
Иллюстрация 109 Security Settings - Java Scripting



Разрешение выполнения Java

1. В Internet Explorer выберите **Tools**, **Internet Options** и затем вкладку **Security**.
2. Щелкните кнопку **Custom Level...**.
3. Прокрутите список до **Microsoft VM**.
4. В **Java permissions** должен быть выбран safety level.
5. Щелкните **OK** чтобы закрыть окно.

Иллюстрация 110 Security Settings - Java



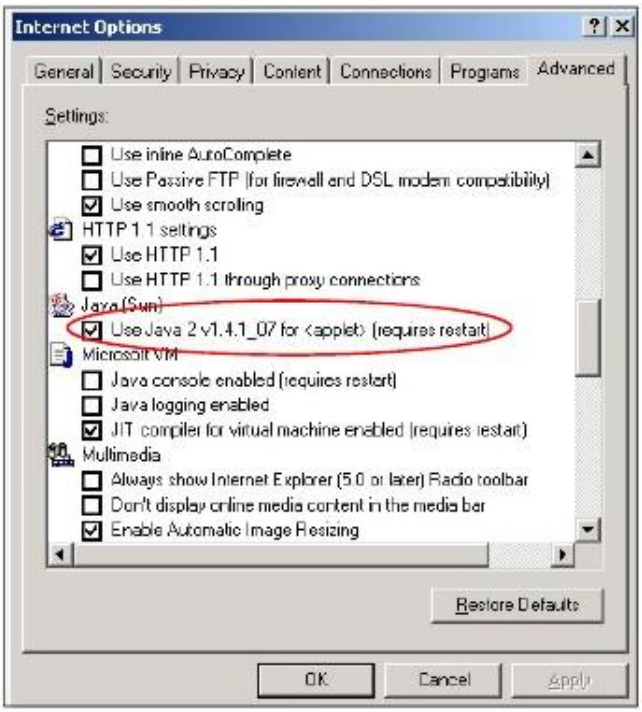
JAVA (Sun)

1 В Internet Explorer выберите **Tools**, **Internet Options** и затем вкладку **Advanced**.

2 Убедитесь, что в **Java (Sun)** выбран **Use Java 2 for <applet>**.

3 Щелкните **OK** чтобы закрыть окно.

Иллюстрация 111 Java (Sun)



Mozilla Firefox

Здесь показаны экраны Mozilla Firefox 2.0 (экраны для других версий этого браузера могут немного отличаться). Эту же процедуру можно использовать и для Mozilla Firefox 3.0.

На одном экране можно включить Java, Javascripts и всплывающие окна. Щелкните **Tools** и затем **Options** на открывшемся экране.

Иллюстрация 112 Mozilla Firefox: tools > Options

Щелкните **Content** чтобы вывести следующий экран. Поставьте галочки как показано на следующей иллюстрации.

Иллюстрация 113 Mozilla Firefox Content Security

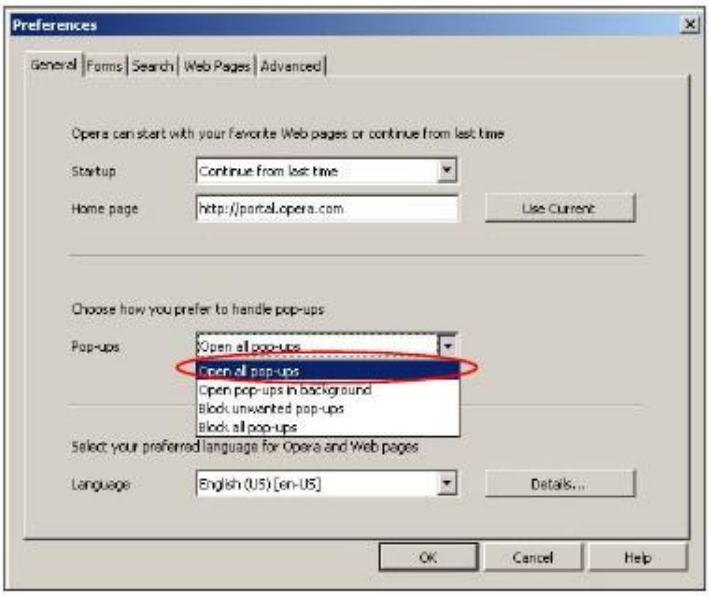
Opera

Здесь показаны экраны Opera 10 (экраны для других версий этого браузера могут немного отличаться).

Разрешение всплывающих окон

В Opera выберите **Tools** и затем **Preferences**. В закладке **General** выберите **Choose how you prefer to handle pop-ups** и выберите **Open all pop-ups**.

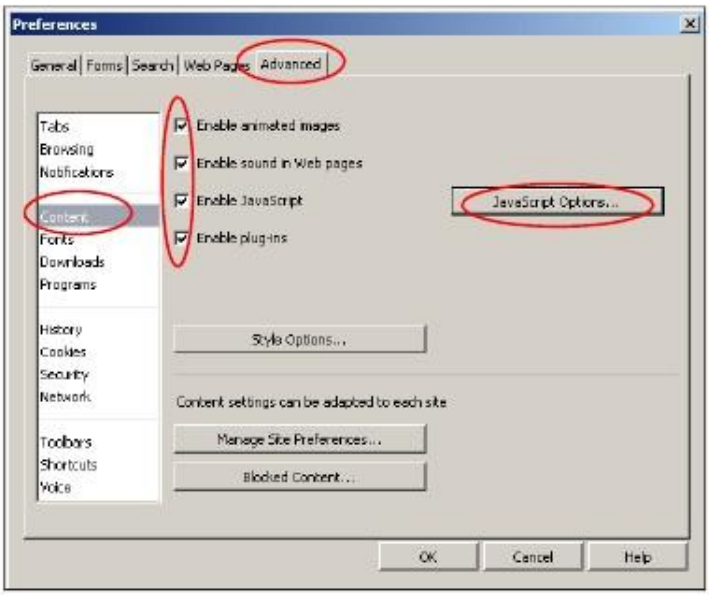
Иллюстрация 114 Opera: Allowing Pop-Ups



Разрешение выполнения кода Java

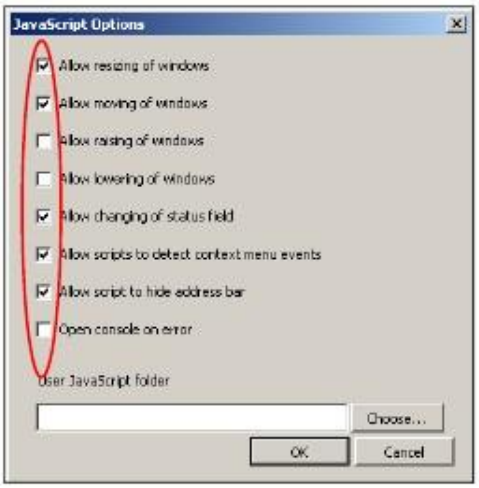
В Opera щелкните **Tools** и затем **Preferences**. Во вкладке **Advanced** выберите в левом меню **Content** и затем поставьте галочки как показано на следующей иллюстрации.

Иллюстрация 115 Opera: Разрешение Java



Для настройки выполнения JavaScript в браузере Opera щелкните **JavaScript Options**.

Иллюстрация 116 Opera: JavaScript Options



Выберите нужно опции JavaScript, которые будут разрешены в Opera.

Приложение C

Настройка IP-адреса компьютера

Примечание: Ваша модель NBG6615 может не поддерживать некоторые операционные системы, настройка для которых описана в этом Приложении (см. спецификацию продукта).

В этом приложении объясняется, как правильно настроить параметры IP на компьютере для работы в сети. Операционные системы Windows Vista/XP/2000, Mac OS 9/OS X и все версии UNIX/LINUX полностью поддерживают протокол TCP/IP.

Если вы вручную настраивает параметры IP, а не используете динамические параметры IP, то убедитесь, что вы назначаете компьютерам IP-адреса, относящиеся к одной подсети.

В этом приложении объясняется, как правильно параметры IP-адрес для операционных систем:

Windows XP

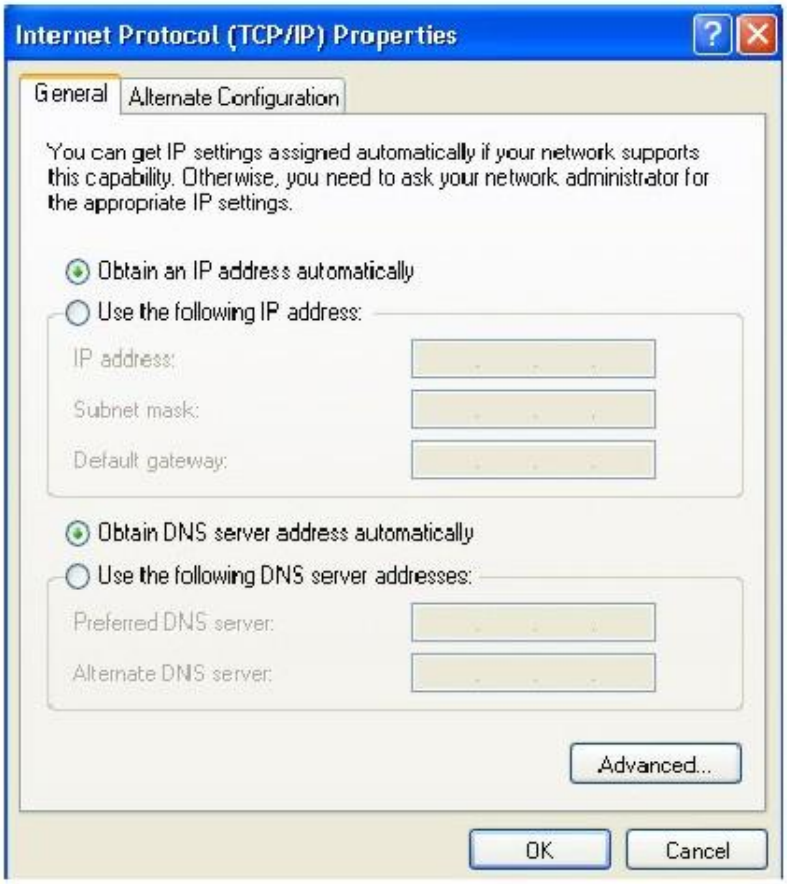
1 Щелкните **Start > Control Panel**.

2 В **Control Panel**, щелкните пиктограмму **Network Connections**.

3 Щелкните правой кнопкой **Local Area Connection** и затем выберите **Properties**.

4 Во вкладке **General** выберите **Internet Protocol (TCP/IP)** и затем щелкните **Properties**.

5 Откроется окно **Internet Protocol TCP/IP Properties**.



6 Если ваш администратор сети или провайдер назначает динамический IP-адрес, то выберите **Obtain an IP address automatically**.

Если ваш администратор сети или провайдер назначил вам статический IP-адрес, то выберите **Use the following IP Address** и введите данные в поля **IP address**, **Subnet mask** и **Default gateway**. Также надо ввести информацию в поля а **Preferred DNS server** и **Alternate DNS server** если ваш администратор сети или провайдер предоставил вам эту информацию.

7 Щелкните **OK** чтобы закрыть окно **Internet Protocol (TCP/IP) Properties**.

8 Щелкните **OK** чтобы закрыть окно **Local Area Connection Properties**.

Проверка настроек

1 Щелкните **Start > All Programs > Accessories > Command Prompt**.

2 В окне **Command Prompt** введите **"ipconfig"** и нажмите **[ENTER]**.

Также можно посмотреть IP-адрес и состояния соединения если перейти в **Start > Control Panel > Network Connections**, щелкнуть правой кнопкой **Network Connection**, щелкнуть Status и затем вкладку **Support**.

Windows Vista

На иллюстрациях этого разделе показаны экраны для Windows Vista Professional.

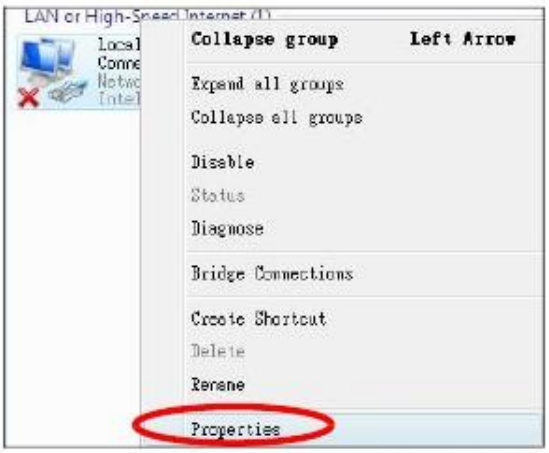
1 Щелкните **Start > Control Panel**.

2 На **Control Panel** щелкните пиктограмму **Network and Internet**.

3 Щелкните пиктограмму **Network and Sharing Center**.

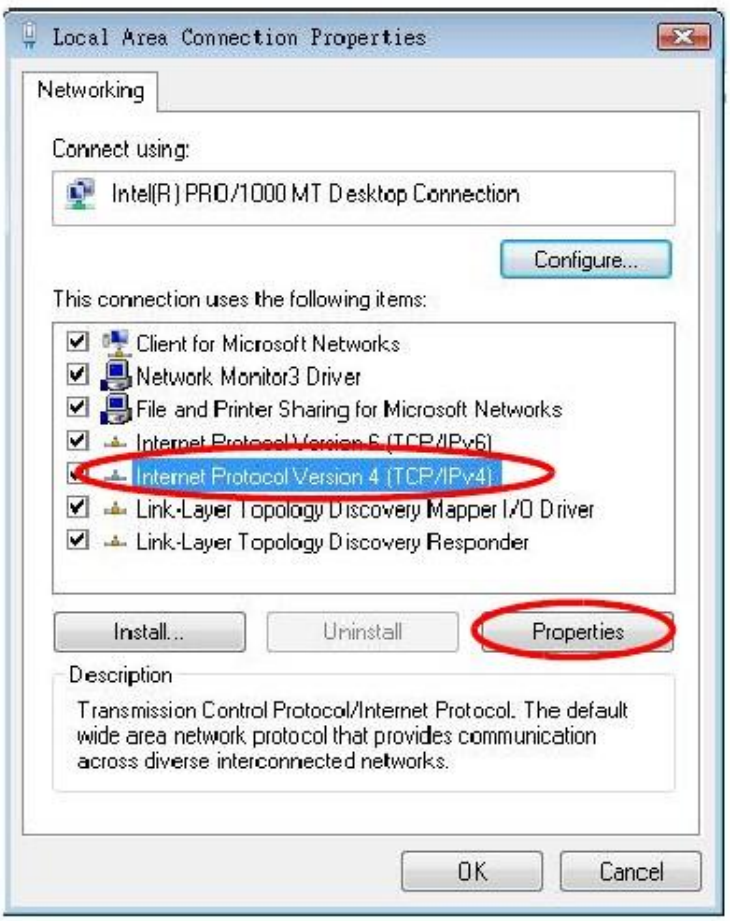
4 Щелкните **Manage network connections**.

5 Щелкните правой кнопкой **Local Area Connection** и выберите **Properties**.

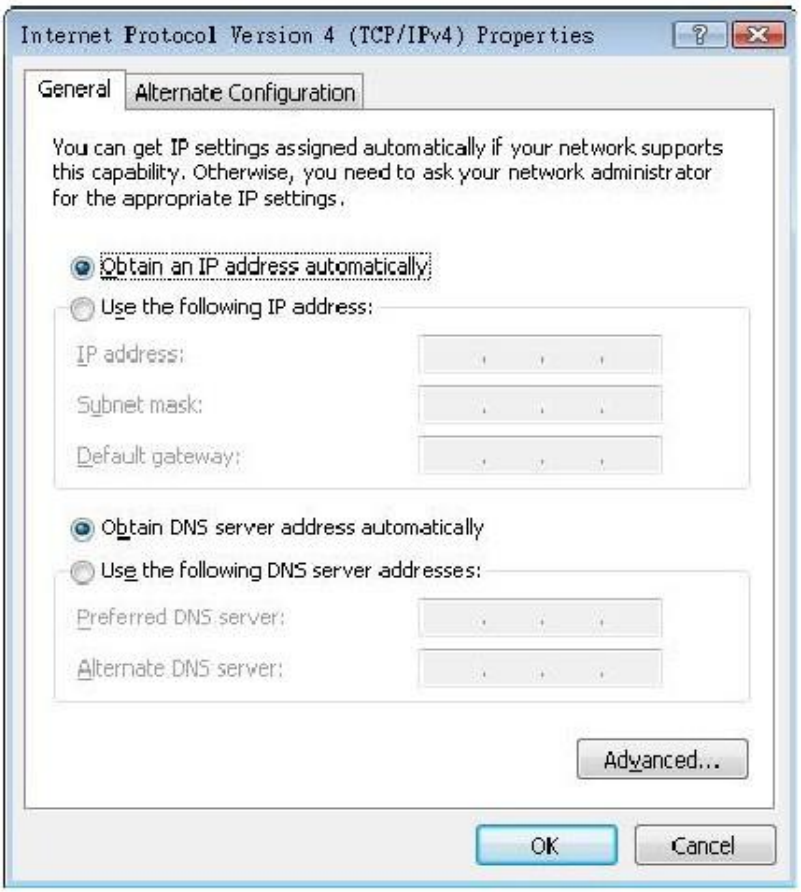


Примечание: Если во время выполнения этой процедуры появится всплывающее окно с просьбой подтвердить продолжение операции, то щелкните **Continue**.

6 Выберите **Internet Protocol Version 4 (TCP/IPv4)** и затем **Properties**.



7 Откроется окно **Internet Protocol Version 4 (TCP/IPv4) Properties**.



8 Если ваш администратор сети или провайдер назначает динамический IP-адрес, то выберите **Obtain an IP address automatically**.

Если ваш администратор сети или провайдер назначил вам статический IP-адрес, то выберите **Use the following IP Address** и введите данные в поля **IP address**, **Subnet mask** и **Default gateway**. Также надо ввести информацию в поля а **Preferred DNS server** и **Alternate DNS server** если ваш администратор сети или провайдер предоставил вам эту информацию.

9 Щелкните **OK** чтобы закрыть окно **Internet Protocol (TCP/IP) Properties**.

10 Щелкните **OK** чтобы закрыть окно **Local Area Connection Properties**.

Проверка настроек

1 Щелкните **Start > All Programs > Accessories > Command Prompt**.

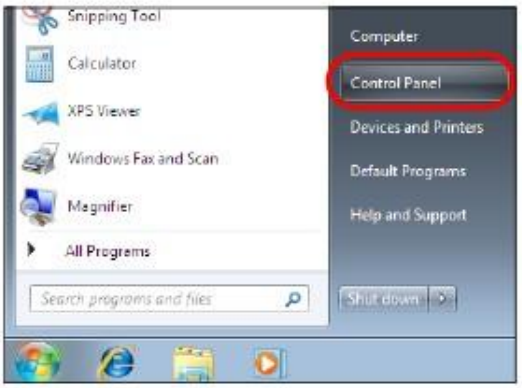
2 В окне **Command Prompt** введите **"ipconfig"** и нажмите **[ENTER]**.

Также можно посмотреть IP-адрес и состояния соединения если перейти в **Start > Control Panel > Network Connections**, щелкнуть правой кнопкой **Network Connection**, щелкнуть Status и затем вкладку **Support**.

Windows 7

На иллюстрациях этого разделе показаны экраны для Windows 7 Enterprise.

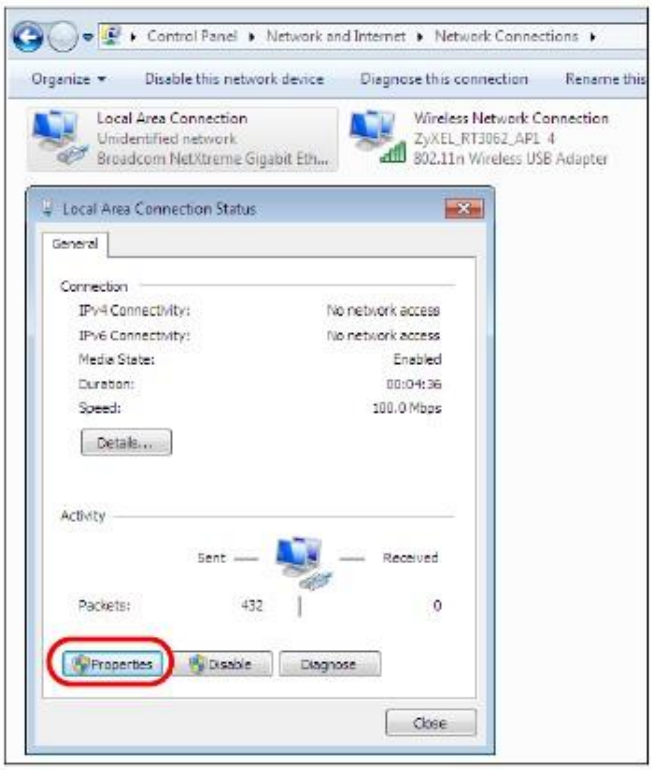
1 Щелкните **Start > Control Panel**.



2 На **Control Panel** щелкните **View network status and tasks** в **Network and Internet**.

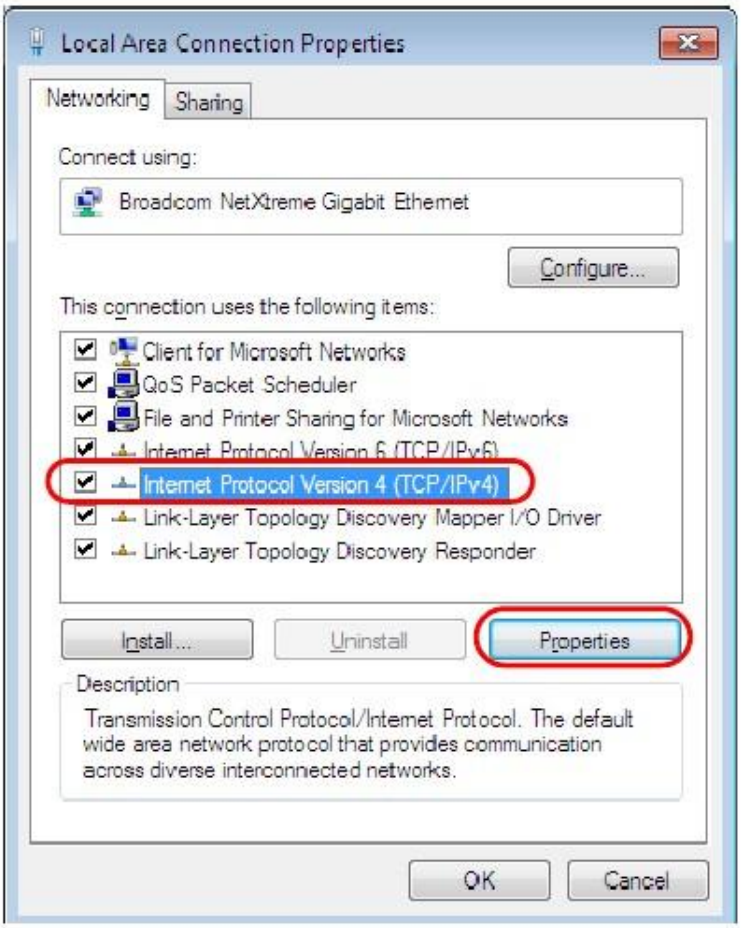
3 Щелкните **Change adapter settings**.

4 Дважды щелкните **Local Area Connection** и выберите **Properties**.

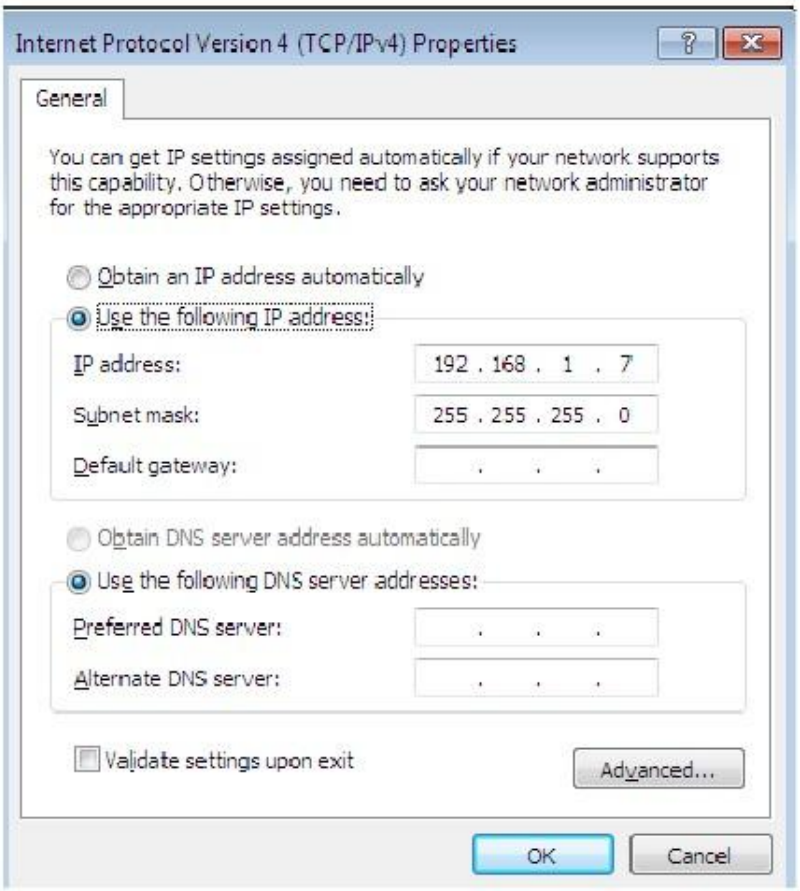


Примечание: Если во время выполнения этой процедуры появится всплывающее окно с просьбой подтвердить продолжение операции, то щелкните **Continue**.

5 Выберите **Internet Protocol Version 4 (TCP/IPv4)** и затем **Properties**.



6 Откроется окно **Internet Protocol Version 4 (TCP/IPv4) Properties**.



7 Если ваш администратор сети или провайдер назначает динамический IP-адрес, то выберите **Obtain an IP address automatically**.

Если ваш администратор сети или провайдер назначил вам статический IP-адрес, то выберите **Use the following IP Address** и введите данные в поля **IP address**, **Subnet mask** и **Default gateway**. Также надо ввести информацию в поля а **Preferred DNS server** и **Alternate DNS server** если ваш администратор сети или провайдер предоставил вам эту информацию. Щелкните **Advanced** если вам нужно задать дополнительные настройки IP, DNS и WINS.

8 Щелкните **OK** чтобы закрыть окно **Internet Protocol (TCP/IP) Properties**.

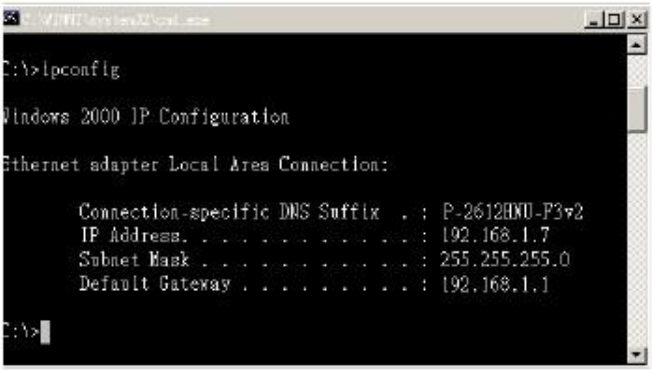
9 Щелкните **OK** чтобы закрыть окно **Local Area Connection Properties**.

Проверка настроек

1 Щелкните **Start > All Programs > Accessories > Command Prompt**.

2 В окне **Command Prompt** введите **"ipconfig"** и нажмите **[ENTER]**.

3 На экране будут выведены настройки IP.



Mac OS X: 10.3 и 10.4

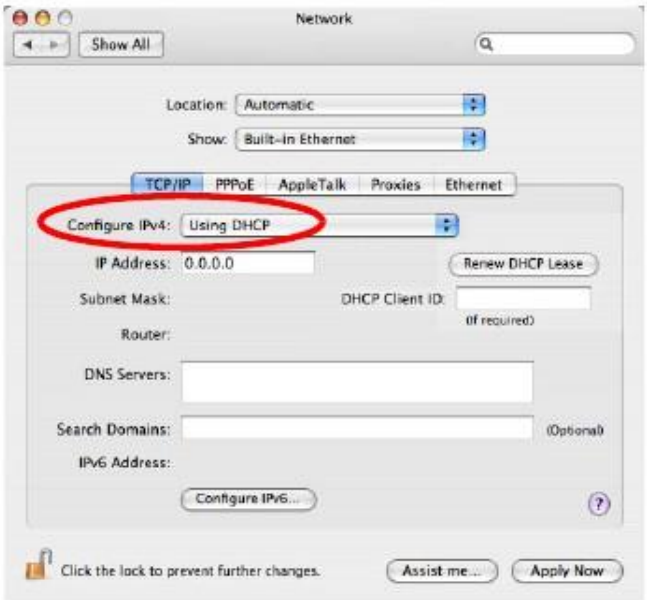
Эти экраны относятся к Mac OS X 10.4, а также к версии 10.3 этой операционной системы.

1 Щелкните **Apple > System Preferences**.

2 В окне **System Preferences** щелкните пиктограмму **Network**.

3 Когда откроется панель **Network preferences** выберите **Built-in Ethernet** из списка типов сетевых соединений и щелкните **Configure**.

4 Для динамического назначения адресов выберите **Using DHCP** из списка **Configure IPv4 list** во вкладке **TCP/IP**.



5 Для статического назначения адресов нужно:

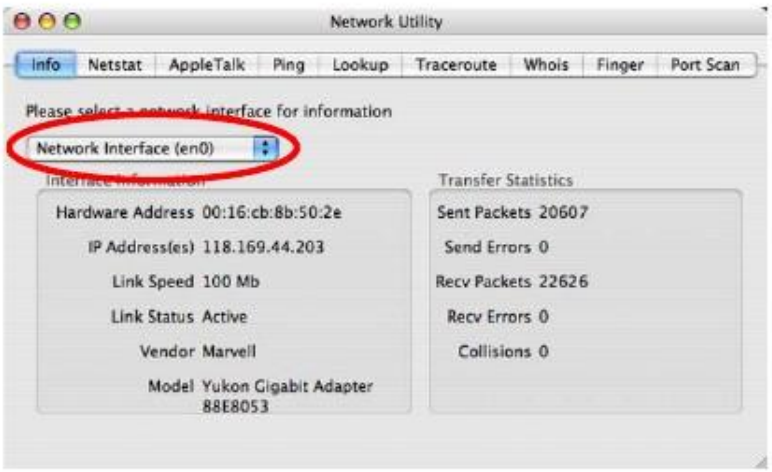
- Из списка **Configure IPv4** выбрать **Manually.**
- В поле **IP Address** ввести ваш IP-адрес**.**
- В поле **Subnet Mask** ввести маску подсети**.**
- В поле **Router** ввести IP-адрес вашего устройства**.**

6 Щелкните **Apply Now** и закройте окно.

Проверка настроек

Для проверки настроек TCP/IP щелкните **Applications > Utilities > Network Utilities** и затем во вкладке **Info** выберите нужный **Network Interface**.

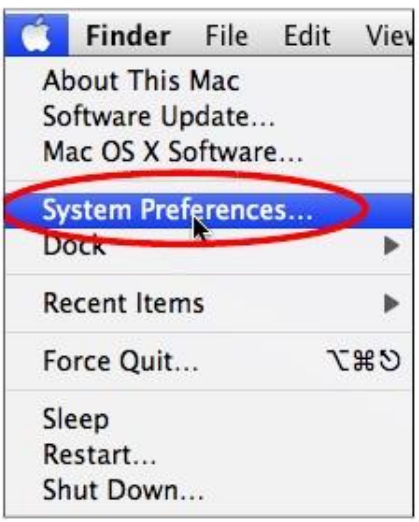
Иллюстрация 117 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 и 10.6

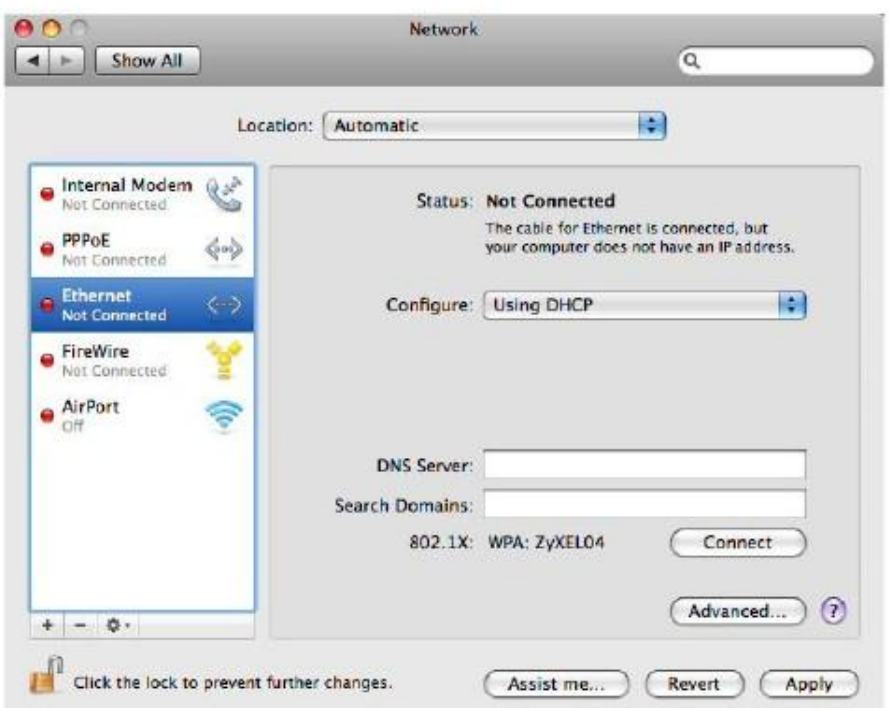
Эти экраны относятся к Mac OS X 10.45 а также к версии 10.6 этой операционной системы.

1 Щелкните **Apple > System Preferences**.



2 В окне **System Preferences** щелкните пиктограмму **Network**.

3 Когда откроется панель **Network preferences** выберите **Ethernet** из списка типов сетевых соединений.

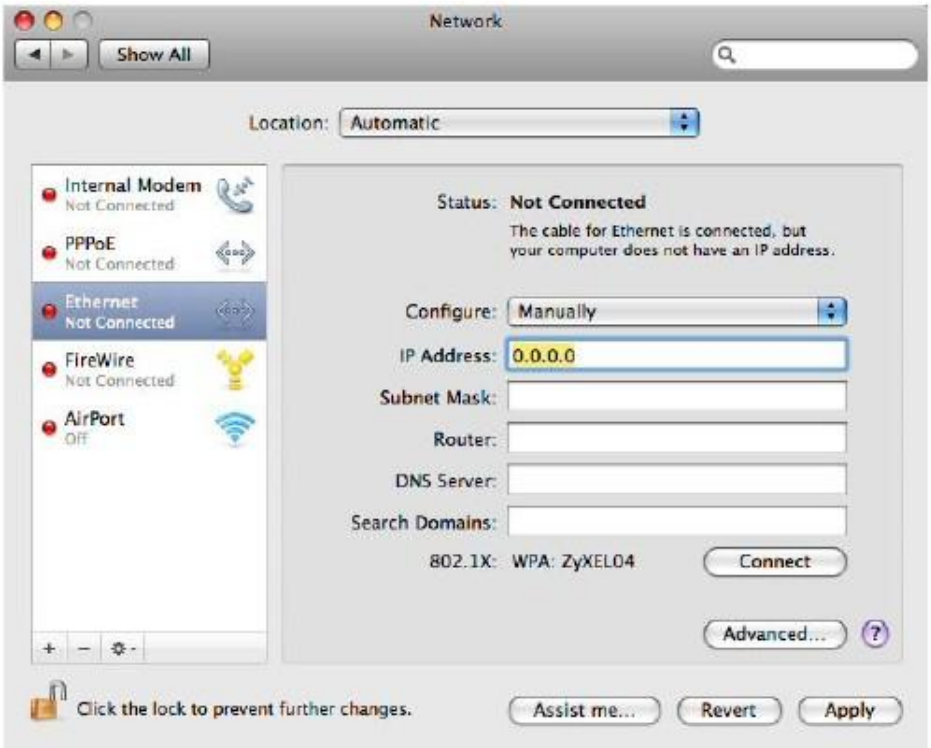


4 Для динамического назначения адресов выберите **Using DHCP** из списка **Configure**.

5 Для статического назначения адресов нужно:

- Из списка **Configure** выбрать **Manually**.
- В поле **IP Address** ввести ваш IP-адрес.

- В поле **Subnet Mask** ввести маску подсети.
- В поле **Router** ввести IP-адрес вашего NBG6615.

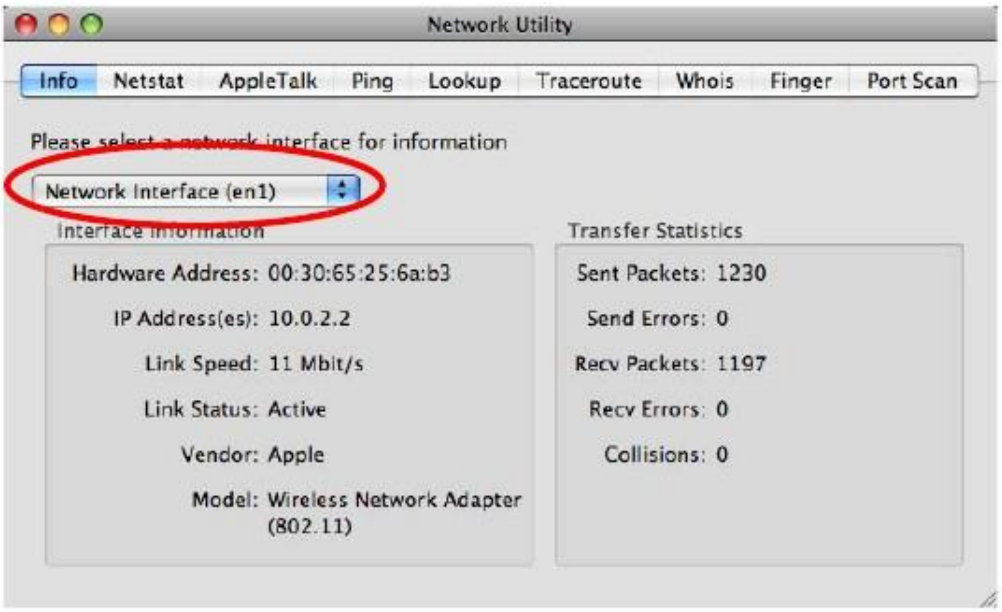


6 Щелкните **Apply** и закройте окно.

Проверка настроек

Для проверки настроек TCP/IP щелкните **Applications > Utilities > Network Utilities** и затем во вкладке **Info** выберите нужный **Network Interface**.

Иллюстрация 118 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

В этом разделе объясняется, как настроить TCP/IP в GNU Object Model Environment (GNOME), используя дистрибутив Ubuntu 8 Linux. Процедура настройки, экраны и расположение файлов могут отличаться от описания в зависимости от вашего дистрибутива, его релиза и конкретной конфигурации компьютера. Следующие экраны относятся к инсталляции по умолчанию Ubuntu 8.

Примечание: Нужно войти в систему как администратор root.

Настройка IP-адреса компьютера в GNOME:

1 Щелкните **System > Administration > Network**.

2 Когда откроется окно **Network Settings** нужно щелкнуть **Unlock** чтобы открыть окно **Authenticate**. (По умолчанию кнопка **Unlock** отключена). Менять конфигурацию может только пользователь с правами администратора.

3 В окне **Authenticate** введите имя пользователя и пароль администратора и затем щелкните кнопку **Authenticate**.

4 Выберите соединения, которые нужно настроить, в окне **Network Settings** и затем щелкните **Properties**.

5 Откроется диалоговое окно **Properties**.

- Если у вас динамический IP-адрес, то в списке **Configuration** выберите **Automatic Configuration (DHCP)**.
- Если у вас статический IP-адрес, то в списке **Configuration** выберите **Static IP address** и заполните поля **IP address, Subnet mask** и **Gateway address**.

6 Щелкните **OK** для сохранения изменений и закрытия диалогового окна **Properties** и возврата на экран **Network Settings**.

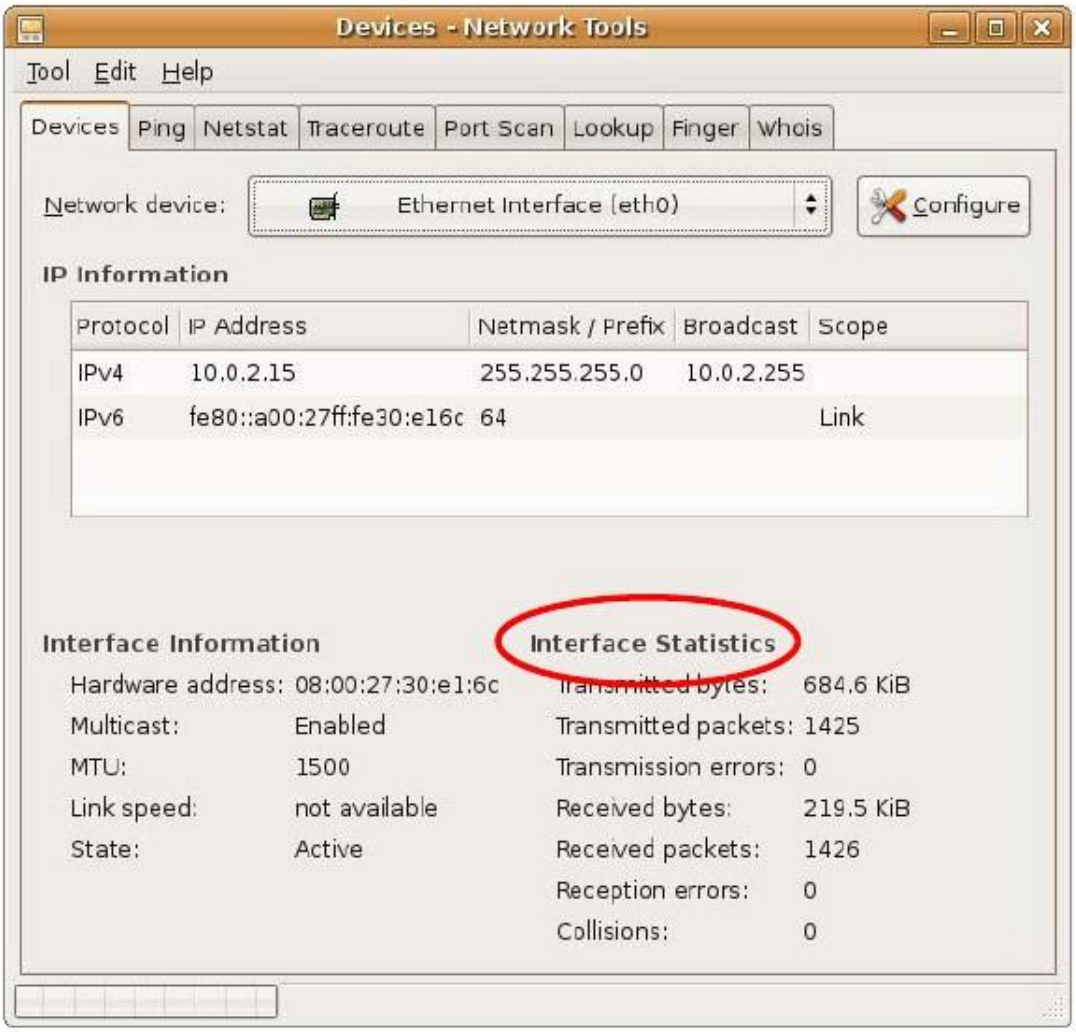
7 Если вы знаете IP-адрес(а) вашего DNS-сервера, то щелкните вкладку **DNS** в окне **Network Settings** и введите информацию о сервере DNS.

8 Щелкните кнопку **Close** чтобы применить новые настройки.

Проверка настроек

Для проверки настроек TCP/IP щелкните **System > Administration > Network Tools** и выберите нужное сетевое устройство **Network device** во вкладке **Devices**. Если это соединение работает, то в колонке **Interface Statistics** будет выведена его статистика.

Иллюстрация 119 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

В этом разделе объясняется, как настроить TCP/IP в K Desktop Environment (KDE), используя дистрибутив openSUSE 10.3 8 Linux. Процедура настройки, экраны и расположение файлов могут отличаться от описания в зависимости от вашего дистрибутива, его релиза и конкретной конфигурации компьютера. Следующие экраны относятся к инсталляции по умолчанию openSUSE 10.3.

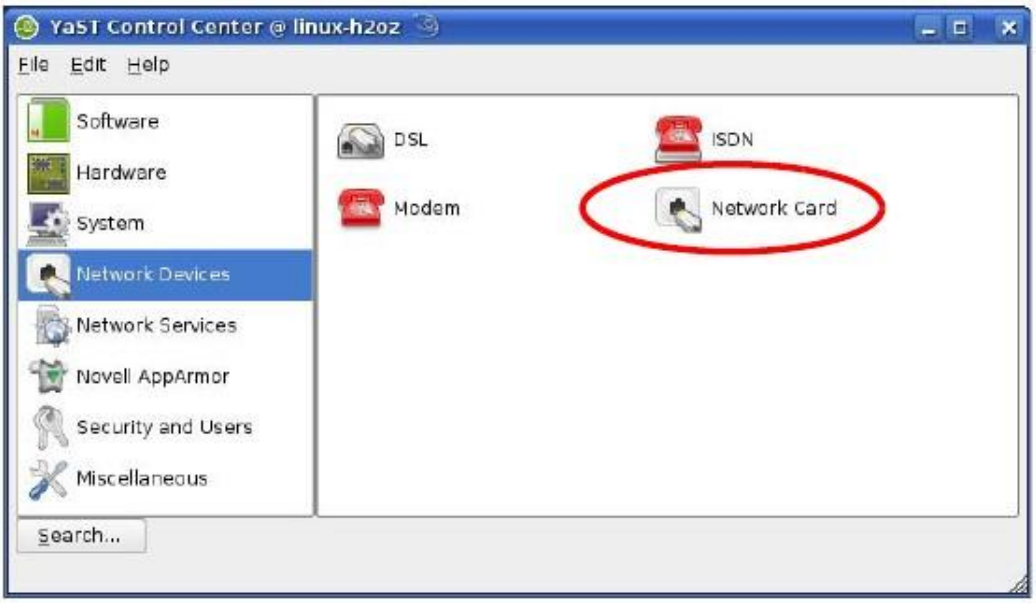
Примечание: Нужно войти в систему как администратор root.

Настройка IP-адреса компьютера в KDE:

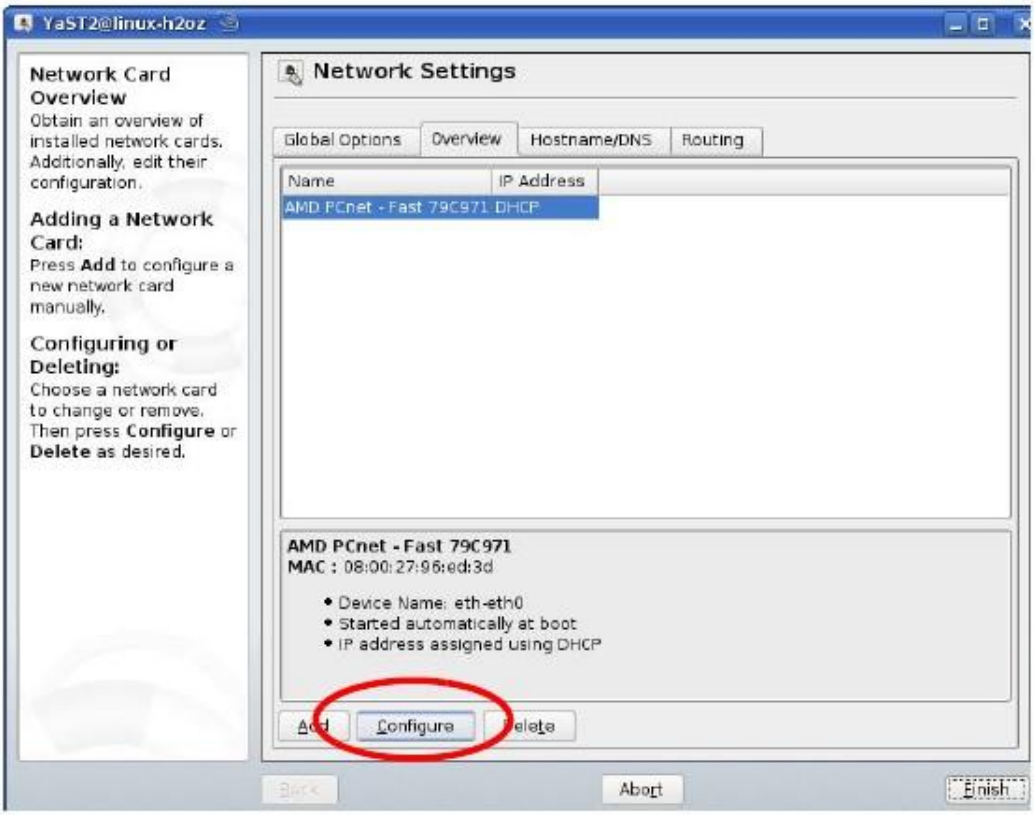
1 Щелкните **K Menu > Computer > Administrator Settings (YaST)**.

2 Когда откроется диалоговое окно **Run as Root - KDE su** нужно ввести пароль администратора и щелкнуть **OK**.

3 Когда откроется окно **YaST Control Center**, выберите **Network Devices** и щелкните пиктограмму **Network Card**.

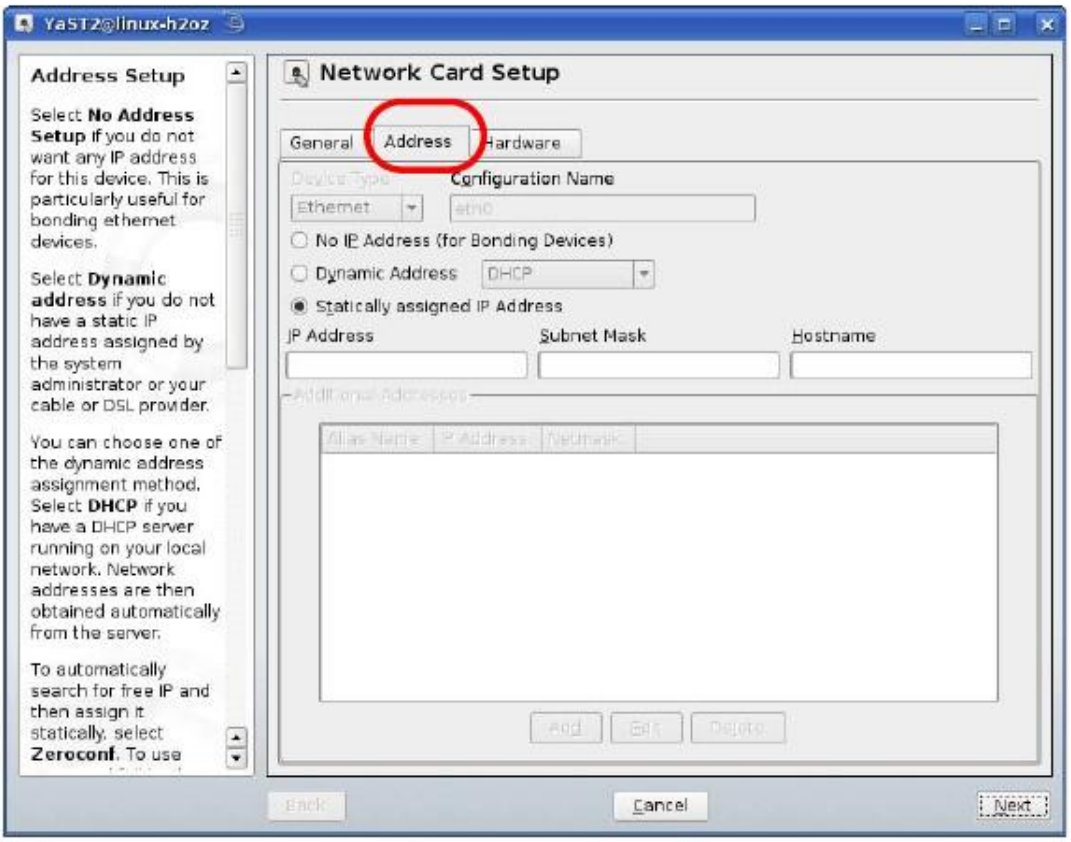


4 Когда откроется окно **Network Settings**, щелкните вкладку **Overview**, выберите из списка имя нужного соединения (**Name**) и щелкните кнопку **Configure**.



5 Когда откроется окно **Network Card Setup** щелкните вкладку **Address**.

Иллюстрация 120 openSUSE 10.3: Network Card Setup

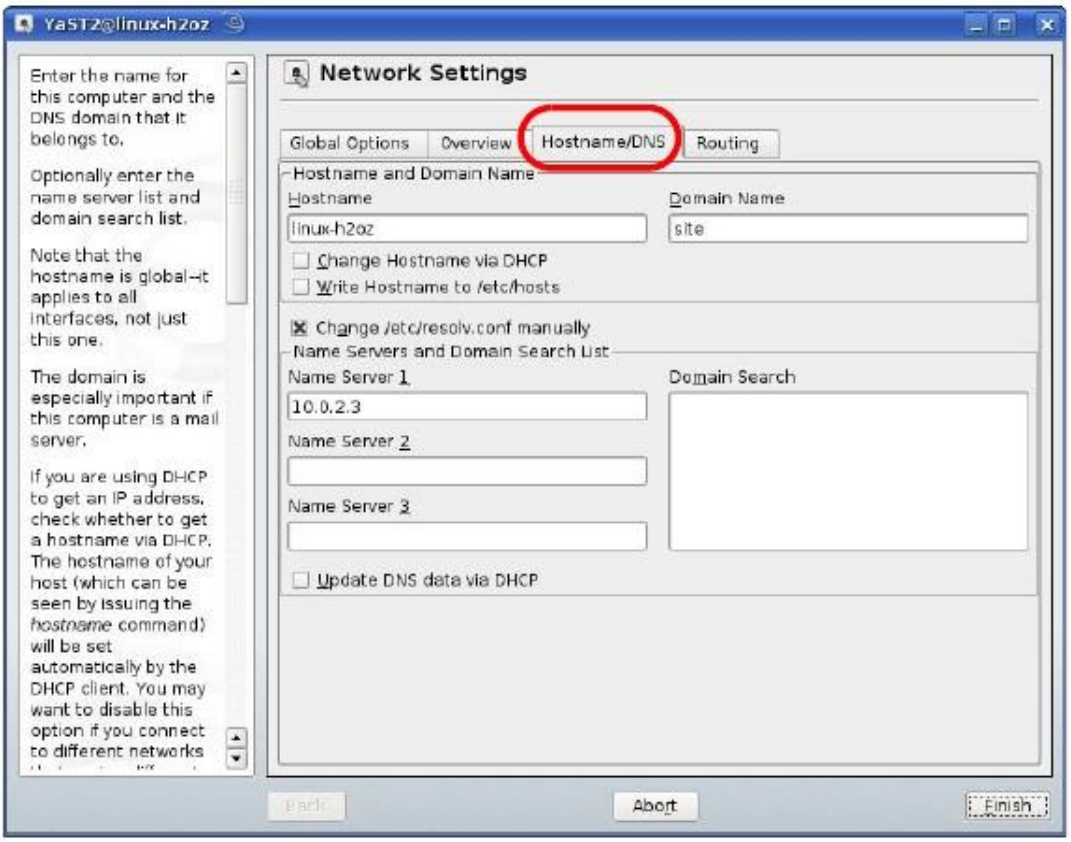


6 Если у вас динамический IP-адрес, то выберите **Dynamic Address (DHCP)**.

Если у вас статический IP-адрес, то выберите **Statically assigned IP Address address** и заполните поля **IP address, Subnet mask** и **Hostname**.

7 Щелкните **Next** для сохранения изменений и закрытия окна **Network Card Setup**.

8 Если вы знаете IP-адрес(а) вашего DNS-сервера, то щелкните вкладку **DNS** в окне **Network Settings** и введите информацию о сервере DNS в соответствующие поля.



9 Щелкните **Finish** чтобы сохранить настройки и закрыть окно.

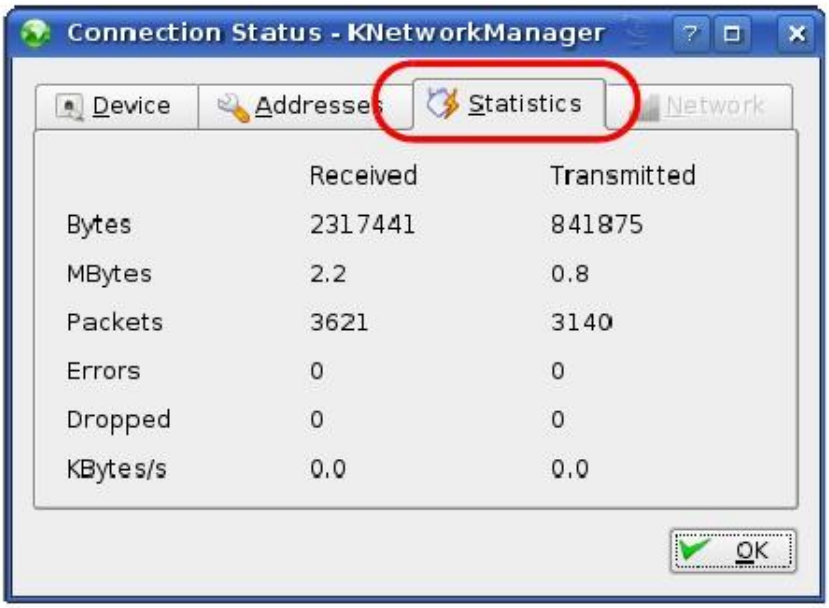
Проверка настроек

Для проверки настроек TCP/IP щелкните пиктограмму **KNetwork Manager** на панели **Task**. В подменю **Options** выберите **Show Connection Information**.

Иллюстрация 121 openSUSE 10.3: KNetwork Manager

Когда откроется окно **Connection Status - KNetwork Manager** щелкните вкладку **Statistics** чтобы убедиться, что соединение работает.

Иллюстрация 122 openSUSE: Connection Status - KNetwork Manager



Приложение D
Беспроводная сеть

Топологии беспроводной сети

В этом разделе описаны возможные топологии беспроводной сети.

Конфигурация беспроводной сети ad-hoc

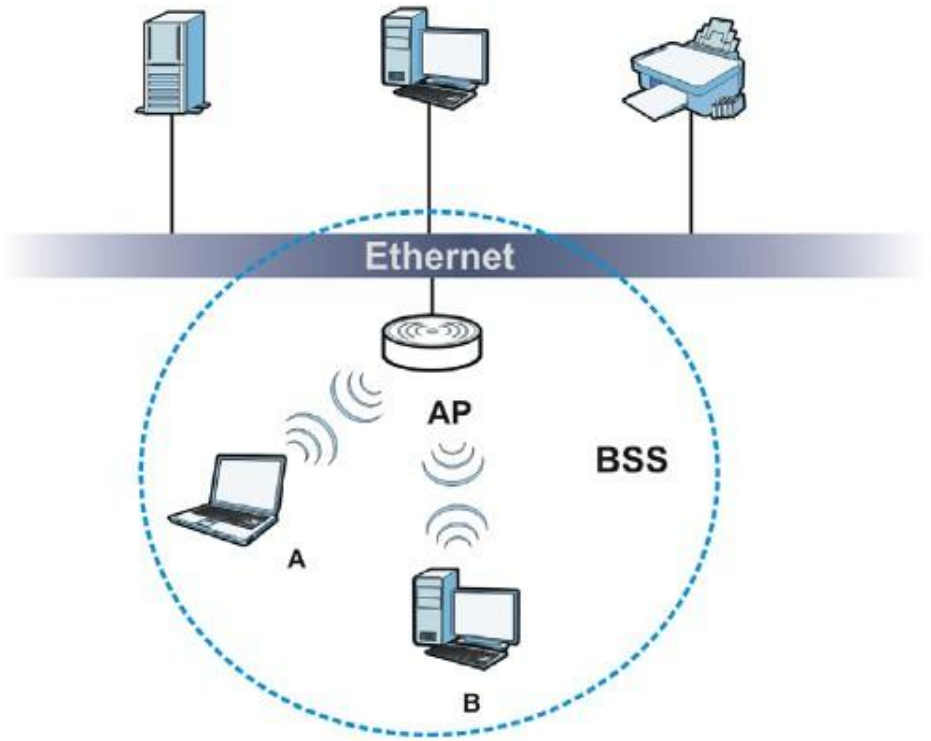
Самая простая конфигурация беспроводной сети – это сеть, состоящая из компьютеров с адаптерами беспроводной сети (A, B, C). Каждый раз, когда два и более беспроводных адаптера оказываются в зоне покрытия друг друга, между ними возникает независимая сеть, обычно называемая сеть ad-hoc или Independent Basic Service Set (IBSS). На следующем примере показан пример беспроводной сети ad-hoc, которая состоит только из ноутбуков, оборудованных беспроводными адаптерами.

Иллюстрация 123 Соединение Peer-to-Peer Communication в сети Ad-hoc

BSS

Basic Service Set (BSS) – это беспроводная сеть, в которой весь обмен данными между беспроводными клиентами или беспроводными клиентами и проводной сетью идет через одну точку доступа Access Point (AP). Если включен Intra-BSS, то беспроводные клиенты **A** и **B** могут обмениваться данными между собой и с проводной сетью. Если отключен, то беспроводные клиенты **A** и **B** могут обмениваться данными только с проводной сетью, но не между собой.

Иллюстрация 124 Basic Service Set



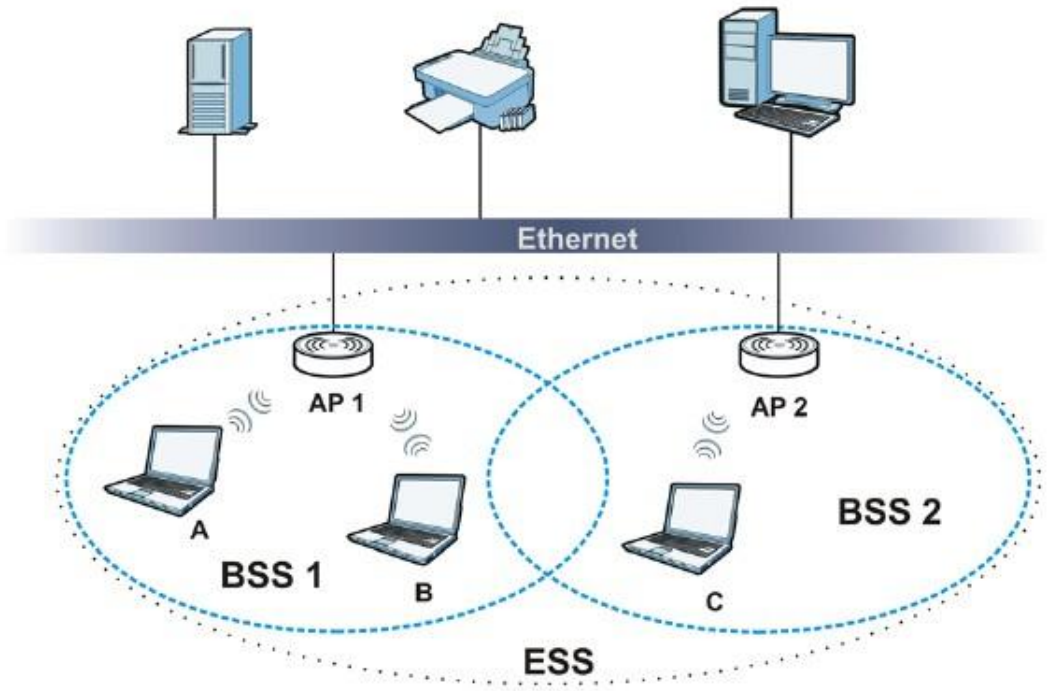
ESS

Extended Service Set (ESS) – это несколько перекрывающихся BSS, у каждого из которых есть своя точка доступа и все эти точки соединены по проводной сети. Проводное соединение между AP называется Distribution System (DS).

Этот топологии беспроводной локальной сети (wireless LAN) называется инфраструктурная WLAN. Точка доступа не только обеспечивает обмен данными с проводной сетью, но и регулирует беспроводной трафик в прилегающей зоне.

ESSID (ESS IDentification) уникально идентифицирует каждый ESS. Все относящиеся к одной ESS точки доступа и подключенные к ним беспроводные клиенты должны иметь один и тот же ESSID, иначе связь между ними не будет работать.

Иллюстрация 125 Инфраструктурная WLAN



Канал

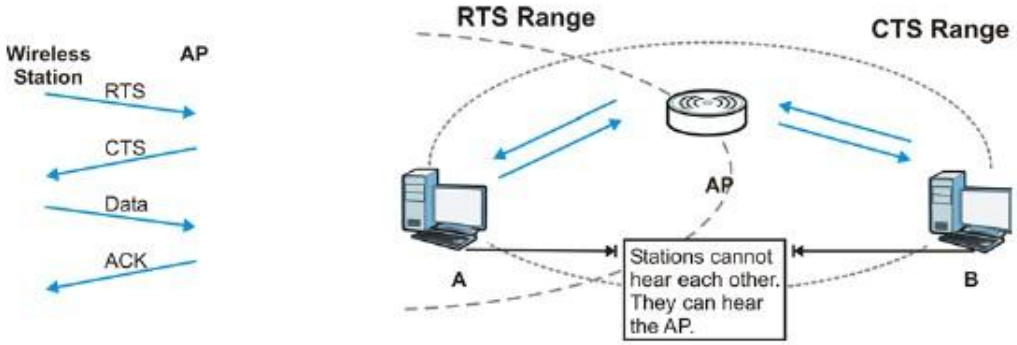
Канал – это частота (частоты) радиосвязи, которые беспроводные клиенты используют для передачи и приема данных. Доступные каналы (частоты) зависят от конкретного географического региона. При выборе из доступных каналов нельзя использовать канал, который уже задействован соседней точкой доступа, иначе возникнет наложение сигналов от двух точек доступа и в результате производительность беспроводной сети упадет

Тем не менее соседние каналы частично перекрываются, поэтому рекомендуется, чтобы между каналами, используемыми соседними точками доступа, было не менее пяти каналов. Например, если в вашем регионе доступно 11 каналов и соседняя точка доступа использует канал 1, то нужно выбрать канал в диапазон от 6 до 11

RTS/CTS

Невидимый узел (hidden node) образуется если две станции находятся в зоне покрытия одной точки доступа, но за пределами покрытия друг друга. На следующей иллюстрации показан пример скрытого узла, где станции (STA) «не слышат» друг друга и поэтому могут определить, какой канал сейчас используется другой станцией, поэтому они скрыты друг от друга.

Иллюстрация 126 RTS/CTS



Когда станция **A** посылает данные точке доступа, то она может не знать, что тот же канал использует станция **B**. Если эти две станции передают данные одновременно, то точка доступ не сможет принять оба потока данных (возникнет коллизия) и в результате часть данных будет потеряна.

RTS/CTS предотвращает коллизии, возникающие из-за соседних хостов. RTS/CTS определяет наибольший размер пакета данных, при пересылке которого не выполняется процедура «рукопожатия» (handshake) (Request To Send) RTS/CTS (Clear to Send).

Если размер пакета превышает значение RTS/CTS (в диапазоне от 0 до 2432 байт), то станция, которая пытается передать этот пакет, сначала должна послать точке доступа сообщение RTS (Request To Send) с запросом на разрешение передачи пакета. При получении этого сообщения точка доступа посылает все другим станциям в зоне своего покрытия сообщение CTS (Clear to Send) чтобы она временно прекратили передачу пакета, а той станции, которое послало сообщение RTS, подтверждение, что сейчас можно передавать пакет

Если размер пакета меньше значения **RTS/CTS**, то он пересылается сразу точке доступа без процедуры RTS (Request To Send)/CTS (Clear to Send) handshake.

RTS/CTS следует использовать только если в вашей сети могут быть невидимые узлы и цена повторной пересылки больших пакетов больше, чем стоимость накладных расходов при выполнении RTS (Request To Send)/CTS (Clear to Send) handshake.

Если значение **RTS/CTS** больше порогового значения Fragmentation Threshold value (см. далее), то процедура RTS (Request To Send)/CTS (Clear to Send) handshake никогда не выполняется, поскольку пакеты с данными разбиваются на несколько небольших, длина которых не может превышать значения **RTS/CTS**.

Примечание: Использование RTS Threshold создает дополнительный трафик, из-за которого может упасть производительность сети, хотя этот механизм предназначен для улучшения работы сети.

Fragmentation Threshold

Fragmentation Threshold – это максимальный размер пакета данных (от 256 до 2432 байтов), который точка доступа не будет разбивать на пакеты меньшей длины.

Большой **Fragmentation Threshold** рекомендуется использовать в сетях, где нет помех, а маленький Fragmentation Threshold для сетей с интенсивным трафиком или работающих в условиях сильных помех.

Если **Fragmentation Threshold** меньше значения **RTS/CTS** (см. выше), то процедура RTS (Request To Send)/CTS (Clear to Send) handshake никогда не выполняется, поскольку пакеты с данными разбиваются на несколько небольших, длина которых не может превышать значения **RTS/CTS**.

Preamble Type (тип преамбулы)

Преамбула – это специальное поле в пакете, по которому получатель этого пакета определяет, что дальше идут данные. Преамбула может быть длинной и короткой

Если преамбула короткая, то производительность увеличивается, потому что сами данные занимают больше битов пакета. Все беспроводные адаптеры, поддерживающие стандарт IEEE 802.11, поддерживают длинную преамбулу, но не все поддерживают короткую преамбулу

Длинную преамбулу следует использовать если вы не знаете, какую преамбулу используют другие беспроводные устройства в сети, а если сеть сильно перегружена трафиком, то длинная преамбула обеспечивает более надежную передачи данных.

Короткую преамбулу следует использовать если ее поддерживают все устройства в сети и вам нужно улучшить эффективность передачи данных.

Используйте динамические настройки чтобы использовать короткую преамбулу когда все устройства беспроводной сети поддерживают ее, а если нет, то NBG6615 использует длинную преамбулу.

Примечание: Связь между беспроводными устройствами не будет работать если у них разная длина преамбулы.

Беспроводные сети IEEE 802.11g

IEEE 802.11g is полностью совместим со стандартом IEEE 802.11b, поэтому адаптер IEEE 802.11b и точка доступа IEEE 802.11g могут обмениваться данными на скорость 11 Mbps или меньше в зависимости от расстояния между ними. IEEE 802.11g поддерживает несколько скоростей передачи, при которых используются разные механизмы модуляции:

Таблица 61 IEEE 802.11g

СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (MBPS)	МОДУЛЯЦИЯ
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Обзор безопасности беспроводных сетей

Безопасность беспроводных сетей необходимо для защиты обмена данными по беспроводной сети между беспроводными клиентами, точками доступа и проводной сетью.

Для обеспечения безопасности беспроводной сети NBG6615 поддерживает шифрование данных, аутентификацию клиентов, ограничение доступа к устройству по MAC-адреса и скрытие идентификационных данных NBG6615.

В следующей таблице показана относительная эффективность этих механизмов безопасности, которые поддерживает NBG6615.

Таблица 62 Уровни безопасность беспроводной сети

УРОВЕНЬ БЕЗОПАСНОСТИ	ТИП БЕЗОПАСНОСТИ
Самый ненадежный	Уникальный SSID (по умолчанию)
	Уникальный SSID с включенным Hide SSID
	Фильтр MAC-адресов
	Шифрование WEP
	IEEE802.1x EAP с аутентификацией с помощью сервера
	Wi-Fi Protected Access (WPA)
	WPA2
Самый надежный	

Примечание: На беспроводных клиентах должен использоваться те же настройки безопасности беспроводной сети, что и на NBG6615.

IEEE 802.1x

Стандарт IEEE 802.1x реализовал расширенные возможности аутентификации и дополнительные управления учетными записями и контроля. Некоторые преимущества IEEE 802.1x:

• Аутентификация пользователей с поддержкой роуминга.

• Поддержка RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) для централизованного управления учетными записями пользователей с помощью сетевого сервера RADIUS.

• Поддержка EAP (Extensible Authentication Protocol, RFC 2486) обеспечивает применение дополнительных механизмом аутентификации без изменений в настройках точки доступа или беспроводного клиента.

RADIUS

RADIUS использует модель клиент-сервера для аутентификации, авторизации и управления учетными записями. Точка доступа является клиентом RADIUS, которую обслуживает сервер RADIUS. Сервер RADIUS выполняет следующие функции:

• Аутентификация

Идентификация пользователей.

• Авторизация

Определение, к каким сетевым серверам может получить пользователь после подключения к сети и аутентификации.

• Управление учетными записями

Отслеживание операций пользователя в сети.

RADIUS использует простой механизм обмена пакетами, в котором через точку доступа идет обмен пакета между беспроводными клиентами и сетевым сервером RADIUS.

Типы сообщений RADIUS

Для аутентификации пользователей между сервером RADIUS и точкой доступа идет обмен сообщениями RADIUS следующих типов:

• Access-Request

  Запрос аутентификации, который посылает точка доступа.

• Access-Reject

  Отказ в доступе, который посылает сервер RADIUS.

• Access-Accept

  Разрешение доступа, которое посылает сервер RADIUS

• Access-Challenge

  Запрос дополнительной информации, требуемой для разрешения доступа, который посылает сервер RADIUS. Точка доступа посылает соответствующий ответ от пользователя и затем еще одно сообщение Access-Request.

Для учета пользователей между сервером RADIUS и точкой доступа идет обмен сообщениями RADIUS следующих типов:

• Accounting-Request

  Запрос учета пользователя, который посылает точка доступа.

• Accounting-Response

  Ответ от сервера RADIUS, где он сообщает что начал/прекратил учет пользователя.

Для обеспечения безопасности точка доступа и сервер RADIUS используют один и тот же секретный ключ shared key (пароль). Этот ключ не пересылается по сети. Кроме того, обмен информацией о пароле тоже шифруется для защиты от неавторизованного доступа.

Типы аутентификации EAP

В этом разделе описаны популярные типы аутентификации EAP-MD5, EAP-TLS, EAP-TTLS, PEAP и LEAP. Ваше беспроводное устройство может поддерживать только часть из этих типов аутентификации.

EAP (Extensible Authentication Protocol) – это протокол аутентификации, который работает выше транспортного механизма IEEE 802.1x, обеспечивая поддержку нескольких типов аутентификации пользователей. Точка доступа с помощью EAP взаимодействует с with EAP-совместимым сервером RADIUS и обеспечивает аутентификацию беспроводной станции с помощью RADIUS.

Используемый тип аутентификации зависит от сервера RADIUS и промежуточной точки (точек) доступа, которая поддерживает IEEE 802.1x.

Для аутентификации EAP-TLS требуется проводное соединение к сети для того, чтобы получить сертификат(ы) от центра выдачи сертификатов Certificate Authority (CA). Этот сертификат используется для аутентификации пользователя и CA выдает сертификаты и гарантирует правильность идентификационных данных его владельца.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 – это самый простой метод односторонней аутентификации. Сервер аутентификации посылает challenge беспроводному клиенту. Клиент подтверждает, что он знает пароль, зашифровывая этот challenge и посылаю его обратно зашифрованным. Пароль не пересылается открытым текстом.

Однако у MD5 есть несколько недостатков. Серверу аутентификации нужно получить незашифрованный пароль, поэтому этот пароль надо где-то хранить, что создает риск неавторизованного доступа к файлу, в котором записан пароль. Кроме того, из-за отсутствия двусторонней аутентификации злоумышленники могут подменить сервер аутентификации. Наконец, аутентификация MD5 не поддерживает аутентификации с динамическими ключами сессий, поэтому нужно сконфигурировать ключи шифрования WEP для шифрования данных.

EAP-TLS (Transport Layer Security)

При использовании EAP-TLS цифровые сертификаты должны быть и у сервера, и у клиента для взаимной аутентификации. Сервер предъявляет свой сертификат клиенту. После проверки идентификатора сервера клиент посылает серверу другой сертификат. Обмен сертификатами происходит по открытому каналу до создания защищенного туннеля, что делает идентификатор пользователя потенциальной жертвой пассивной атаки. Цифровой сертификат – это электронное удостоверение личности отправителя, однако для внедрения EAP-TLS нужен Certificate Authority (CA) для обработки сертификатов, что требует дополнительных затрат на управление.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS – это расширение аутентификации EAP-TLS, которое для установления защищенного соединения использует аутентификацию только на стороне сервера. Потом по этому защищенному соединению посылается имя пользователя и пароль для аутентификации клиента, поэтому идентификационные данные клиента защищены. Для аутентификации клиента EAP-TTLS поддерживает методы EAP и устаревшие методы PAP, CHAP, MS-CHAP и MS-CHAP v2.

PEAP (Protected EAP)

Как и в EAP-TTLS, для установления защищенного соединения используется аутентификацию на стороне сервера, а потом по этому защищенному соединению посылается имя пользователя и пароль для аутентификации клиента, поэтому идентификационные данные клиента защищены. Однако PEAP для аутентификации клиента поддерживает только методы EAP (EAP-MD5, EAP-MSCHAPv2 и EAP-GTC (EAP-Generic Token Card)). EAP-GTC используется только компанией Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) – это реализация компанией Cisco стандарта IEEE 802.1x.

Dynamic WEP Key Exchange

Точка доступа использует уникальный ключ, который сгенерировал сервер RADIUS. Срок действия ключа заканчивается когда беспроводное соединение разрывается по тайм-ауту, происходит разъединение или требуется повторная аутентификация. При каждой повторной аутентификации генерируется новый ключ WEP.

Если эта функция включена, то необязательно конфигурировать ключ шифрования по умолчанию на экране wireless security configuration. Вы можете конфигурировать и сохранять ключи, но они будут использоваться если включен dynamic WEP.

Примечание: EAP-MD5 нельзя использовать вместе с Dynamic WEP Key Exchange

Для улучшения надежности защиты в аутентификации на базе сертификатов (EAP-TLS, EAP-TTLS и PEAP) используются динамические ключи шифрования данных. Обычно это применяется в корпоративных сетях, а для общедоступных сетей имеет смысл использовать аутентификацию на базе имени пользователя и пароля. В следующей таблицы перечислены особенности каждого типа аутентификации.

Таблица 63 Сравнение типов аутентификации EAP

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Взаимная аутентификация	Нет	Да	Да	Да	Да
Сертификат – клиент	Нет	Да	Опция	Опция	Нет
Сертификат – сервер	Нет	Да	Да	Да	Нет
Динамический обмен ключами	Нет	Да	Да	Да	Да
Credential Integrity	Отсутствует	Сильная	Сильная	Сильная	Средняя
Трудность внедрения	Easy	Большая	Средняя	Средняя	Средняя
Защита идентификационных данных клиента	Нет	Нет	Да	Да	Нет

WPA и WPA2

Wi-Fi Protected Access (WPA) является частью стандарта IEEE 802.11i. WPA2 (IEEE 802.11i) – это стандарт безопасности беспроводных сетей, в котором используются более надежные, чем в WPA шифрование, аутентификация и управление ключами.

Основное преимущество WPA (WPA2) по сравнению с WEP – это улучшенное шифрование данных и аутентификация пользователей.

Если и точка доступа, и беспроводные клиенты поддерживают WPA2 и есть внешний сервер RADIUS, то лучше использовать WPA2, который обеспечивает более надежное шифрование, а если нет внешнего сервера RADIUS, то WPA2-PSK (WPA2-Pre-Shared Key), который требует только ввода одного и того же пароля на всех точках доступа, шлюзе и клиентах беспроводной сети. Для доступа к беспроводной сети клиентам нужно только ввести правильный пароль.

Если точка доступа или беспроводные клиенты не поддерживают WPA2, то используйте WPA либо WPA-PSK в зависимости от наличия внешнего сервера RADIUS.

Выберите WEP только когда точка доступа и/или беспроводные клиенты не поддерживают WPA или WPA2. WEP менее надежный, чем WPA или WPA2.

Шифрование

WPA для более надежного шифрования использует Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) и IEEE 802.1x. WPA2 использует TKIP для обеспечения совместимость, но у него более надежное шифрование, чем у TKIP с Advanced Encryption Standard (AES) в режиме Counter с Cipher block chaining Message authentication code Protocol (CCMP).

TKIP использует 128-битные ключи, которые сервер аутентификации динамически генерирует и распространяетr. AES (Advanced Encryption Standard) – это блочный шифр, использующий 256-битный математический алгоритм Rijndael. Оба типа шифрования использует функцию per-packet key mixing function, проверку Message Integrity Check (MIC) под названием Michael, расширенный initialization vector (IV) с правилами последовательностей и механизм re-keying.

WPA и WPA2 периодически выполняют изменение и ротацию ключей шифрования, поэтому один ключ шифрования никогда не используется дважды.

Сервер RADIUS распространяет ключ Pairwise Master Key (PMK) и затем применяет иерархическую систему управления ключами, динамически генерируя с помощью PMK уникальные ключи для шифрования пакетов данных, которые передаются между точкой доступа и беспроводными клиентами. Этот процесс выполняется автоматически в фоновом режиме.

Message Integrity Check (MIC) предотвращает перехват пакетов данных, их изменение и повторную пересылку. При использовании проверки MIC отправитель и получатель с помощью строго математического алгоритма рассчитывают значение MIC. Если значения MIC отправителя и получателя не совпадают, то пакет отбрасывается.

Генерация уникального кода шифрования для каждого пакета и использование Integrity Checking Mechanism (MIC) с TKIP и AES обеспечивает более надежную защиту от неавторизованного доступа для пересылки данных по сети Wi-Fi, чем WEP.

Единственная разница в механизмах шифрования WPA(2) и WPA(2)-PSK – это использование в WPA(2)-PSK простого обычного пароля вместо credentials конкретного пользователя, из-за чего есть риск, что злоумышленники могут узнать этот пароль с помощью перебора возможных комбинаций. Тем не менее WPA(2)-PSK надежнее, чем WEP, поскольку использует один постоянный пароль из букв и цифр для генерации PMK, на основе которого генерируются уникальные временные ключи шифрования, поэтому беспроводные устройства в сети используют разные ключи шифрования (в отличие от WEP).

Аутентификация пользователей

WPA и WPA2 используют IEEE 802.1x and Extensible Authentication Protocol (EAP) для аутентификации беспроводных клиентов по базе данных внешнего сервера RADIUS. WPA2 уменьшает число сообщений обмена ключами с шести до четырех (CCMP 4-way handshake) и в результате сокращает время, необходимое для подключения сети. Также при аутентификации WPA2 в отличие от WPA используются key caching и pre-authentication. Это опционные функции, которые поддерживают не все беспроводные клиенты.

С помощью Key caching беспроводной клиент может сохранить PMK, полученный в результате успешной аутентификации клиента точкой доступа, и затем повторно использовать этот PMK при следующей аутентификации на той же точке доступа.

Pre-authentication обеспечивает быстрый роуминг. С ее помощью беспроводной клиент, который уже подключен к точке доступа, может выполнить аутентификацию IEEE 802.1x на другой точке доступа перед соединением с ней.

Пример использования WPA(2) с RADIUS

Для настройки WPA(2) нужен IP-адрес сервера RADIUS, номер его порта (по умолчанию 1812) и «общий секретный код» RADIUS. В этом примере применения WPA(2) "A" – это сервер RADIUS, "DS" - distribution system.

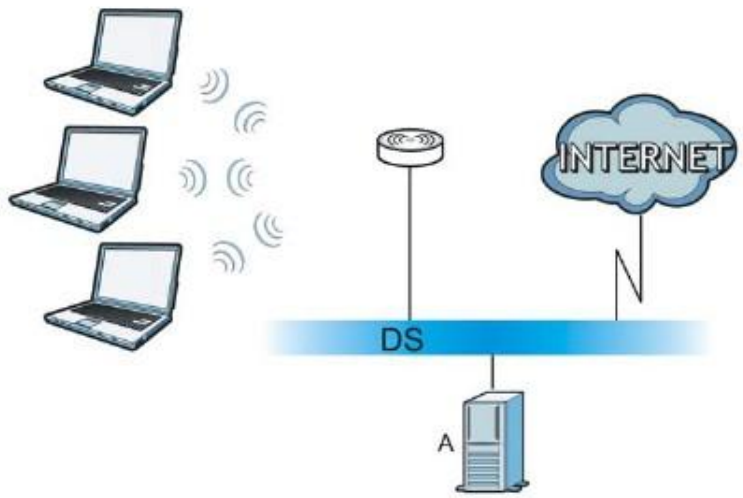
1 Точка доступа передает запрос на аутентификацию от беспроводного клиента серверу RADIUS.

2 Сервер RADIUS проверяет идентификационные данные пользователя по своей базе данных и в зависимости от результатов проверки разрешает или запрещает доступ клиента к сети.

3 В результате аутентификации сервера RADIUS и клиента генерируется 256-битный ключ Pairwise Master Key (PMK).

4 Сервер RADIUS пересылает PMK точке доступа, которая настраивает иерархическую систему управления, динамически генерируя уникальный код шифрования на базе PMK для обмена пакетами данных с беспроводными клиентами.

Иллюстрация 127 Пример применения WPA(2) с RADIUS



Пример использования WPA(2)-PSK

WPA(2)-PSK работает следующим образом:

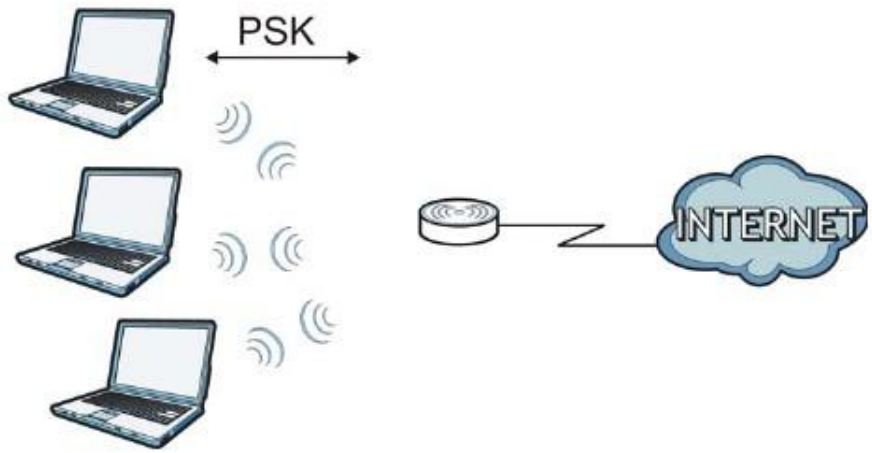
1 Сначала на точке доступа и всех беспроводных клиентах вводится один и тот же пароль. Pre-Shared Key (PSK) состоит из 8 - 63 символов ASCII либо 64 шестнадцатеричных цифр (включая пробелы).

2 Точка доступа проверяет пароль каждого беспроводного клиента. Если пароль правильный, то она разрешает клиенту подключиться к сети.

3 Точка доступа и беспроводные клиенты генерируют общий ключ PMK (Pairwise Master Key). Сам ключ по сети не пересылается, но рассчитывается по PSK и SSID.

4 Точка доступа и беспроводные клиенты создают временные ключи шифрования, используя шифрование TKIP или AES, PMK и «рукопожатие» для обмена информацией, а затем используют эти ключи для шифрования пересылаемых по сети данных.

Иллюстрация 128 Аутентификация WPA(2)-PSK



Сводка основных типов безопасности

По этой таблице можно определить, какие параметры безопасности нужно настроить для каждого метода аутентификации или протокола управления ключами. Работа фильтра MAC-адресов на зависит от настоек этих функций сетевой безопасности

Таблица 64 Основные типы безопасности беспроводной сети

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	ВВОД КЛЮЧА ВРУЧНУЮ	IEEE 802.1X
Open	Отсутствует	Нет	Отключен
			Включен с динамическим ключом WEP
Open	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен без динамического ключа WEP
		Да	Отключен
Shared	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен без динамического ключа WEP
		Да	Отключен
WPA	TKIP/AES	Нет	Включен
WPA-PSK	TKIP/AES	Да	Отключен
WPA2	TKIP/AES	Нет	Включен
WPA2-PSK	TKIP/AES	Да	Отключен

Антенна

Антенна передает радиочастотный сигнал. Передатчик беспроводного устройства с помощью антенны распространяет радиочастотный сигнал. Также антенна принимает радиочастотный сигнал. Зона действия и покрытие беспроводной сети сильно зависит от правильной направленности антенны.

Характеристики антенны

Частота

Антенна использует для беспроводной связи радиочастоты 2.4GHz или 5GHz.

Диаграмма направленности

Диаграмма направленности – это графическое представление границы зоны покрытия антенны.

Усиление антенны

Усиление антенны, которое измеряется в децибелах (dB), означает усиление сигнала в зоне покрытия радиочастотного луча. Чем больше усиление антенны, тем больше покрытие и лучше беспроводная связь.

В помещениях увеличение усиления антенны на 1 dB дает рост покрытия примерно на 2.5%, а на открытом воздухе если нет препятствий распространению сигнала – на 5% (на практике увеличение покрытия зависит от условий работы сети).

Часто усиление антенны обозначается в dBi. Этот показатель рассчитывается как усиление антенны по сравнению с изотропной антенной (изотропная антенна – это идеальная антенна, равномерно распространяющая сигнал по всем направлениям). По показателю dBi можно оценить реальное усиление антенны.

Типы антенн для WLAN

Для беспроводных сетей используются два типа антенн:

• Всенаправленная (omni-directional) антенна распространяет сигнал по всем направлениям в горизонтальной плоскости. Зона покрытия такой антенны имеет форму тора (бублика), поэтому всенаправленная антенна хорошо подходит для помещений. При использовании нескольких точек доступа возникают зоны перекрытия с границами в форме дуги.

• Направленная (directional) антенна фокусирует сигнал в луч подобно лучу фонарика. Угол этого луча определяет ширину покрытия. Обычно угол луча лежит в диапазоне от 20 градусов (узко направленный) до 120 градусов (менее направленный). Направленные антенны хорошо подходят для коридоров и развертывания беспроводной сети point-to-point вне помещений.

Установка антенны

Антенну следует устанавливать как можно выше в том месте, где нет препятствий для распространения сигнала. При развертывании сети point-to–point обе антенны должны быть установлены на одинаковой высоте в непосредственной зоне видимости друг друга.

Если всенаправленная антенна устанавливается на столе или другой горизонтальной поверхности, то ее надо направить вверх, а если на стене или потолке – внизу. Если беспроводную сеть обслуживает только одна точка доступа, то ее всенаправленная антенна должна быть максимально близко к центру зоны покрытия.

Направленную антенну нужно установить так, чтобы она была направлена туда, где нужно обеспечить покрытие беспроводной сети.

Приложение E

Стандартные сервисы

В этой таблице перечислены стандартные сервисы вместе с их протоколами и номерами портов. Полный список номеров портов, тиов/номеров кода и сервисов ICMP размещен на web-сайт IANA (Internet Assigned Number Authority).

• **Имя**: Имя сервиса.

• **Протокол**: Протокол IP, который использует сервис. Если это **TCP/UDP**, то сервис использует тот же номер порта, что и TCP и UDP, а если Выбирает пользователь (USER-DEFINED), то **Порт(ы)** – это номер протокола, а не номер порта.

• **Порт(ы)**: Это значение зависит от **Протокола** (о номерах портов см. RFC 1700).

- Если **Протокол** – это **TCP**, **UDP** или **TCP/UDP**, то номер порта IP.
- Если **Протокол выбирает пользователь (User Defined)**, то это номер протокола IP.

• **Описание:** Краткое описание использования этого сервиса.

Таблица 65 Стандартные сервисы

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Выбирает пользователь	51	Этот сервис использует протокол туннелирования IPSEC AH (Authentication Header).
AIM/New-ICQ	TCP	5190	Мессенджер AOL.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	Клиент DHCP.
BOOTP_SERVER	UDP	67	Сервер DHCP.
CU-SEEME	TCP UDP	7648 24032	Решение для видеоконференций от White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, сервис преобразования имен web (например, www.zyxel.com) в IP-адреса.
ESP (IPSEC_TUNNEL)	Выбирает пользователь	50	Этот сервис используется протоколом туннелирования IPSEC ESP (Encapsulation Security Protocol).
FINGER	TCP	79	Finger – это команда UNIX, позволяющая определить, вошел ли пользователь в систему.
FTP	TCP TCP	20 21	File Transfer Program – программа для быстрой передачи файлов, включая файлы большого размера.
H.323	TCP	1720	NetMeeting использует этот протокол.
HTTP	TCP	80	Hyper Text Transfer Protocol – протокол клиент/сервер для world wide web.
HTTPS	TCP	443	HTTPS – защищенные сессии http, часто используемые в e-commerce.

Таблица 65 Стандартные сервисы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
ICMP	Выбирает пользователь	1	Internet Control Message Protocol обычно используется для диагностики и маршрутизации.
ICQ	UDP	4000	Популярная программа для чата.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol используется когда нужно послать пакеты определенной группе хостов.
IKE	UDP	500	Алгоритм Internet Key Exchange для распространения ключей и управления ими.
IRC	TCP/UDP	6667	Программа для чата
MSN Messenger	TCP	1863	Протокол, который использует Microsoft Networks Messenger.
NEW-ICQ	TCP	5190	Программа для чата.
NEWS	TCP	144	Программа для новостных групп.
NFS	UDP	2049	Network File System - NFS распределенный клиент/серверный файловый сервис для совместного использования файлов в сетях.
NNTP	TCP	119	Network News Transport Protocol – протокол доставки новостей для сервиса USENET newsgroup.
PING	Выбирает пользователь	1	Packet INternet Groper – это протокол для запроса ICMP echo чтобы проверить доступность удаленного хоста.
POP3	TCP	110	С помощью Post Office Protocol version 3 клиентский компьютер скачивает электронную почту с сервера POP3 по временному соединению (TCP/IP или другому).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol для безопасной передачи данных по общедоступным сетям. Это канал управления.
PPTP_TUNNEL (GRE)	Выбирает пользователь	47	PPTP (Point-to-Point Tunneling Protocol) для безопасной передачи данных через общедоступные сети.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	Сервис потоковой передачи аудио через web.
REXEC	TCP	514	Удаленный Execution Daemon.
RLOGIN	TCP	513	Удаленный Login.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Real Time Streaming (media control) Protocol (RTSP) – это протокол удаленного управления мультимедиа в Интернете.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol – это протокол Интернета для обмена сообщениями. С его помощью электронные письма пересылаются между серверами e-mail.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	«Ловушки» для SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language – это язык для доступа к различным базам данных.
SSH	TCP/UDP	22	Программа Secure Shell Remote Login.

Таблица 65 Стандартные сервисы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog посылает логи системы на сервер UNIX.
TACACS	UDP	49	Login Host Protocol используется для (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet – это программа эмуляции удаленного терминала, широко используемая в Интернете и в UNIX. Она работает поверх сетей и позволяет пользователю удаленного зайти на хост-систему.
TFTP	UDP	69	Trivial File Transfer Protocol это протокол передачи файлов через Интернет, похожий на FTP, но использующий UDP (User Datagram Protocol) вместо TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Решение для видеоконференций.