ZYXEL
Your Networking Ally

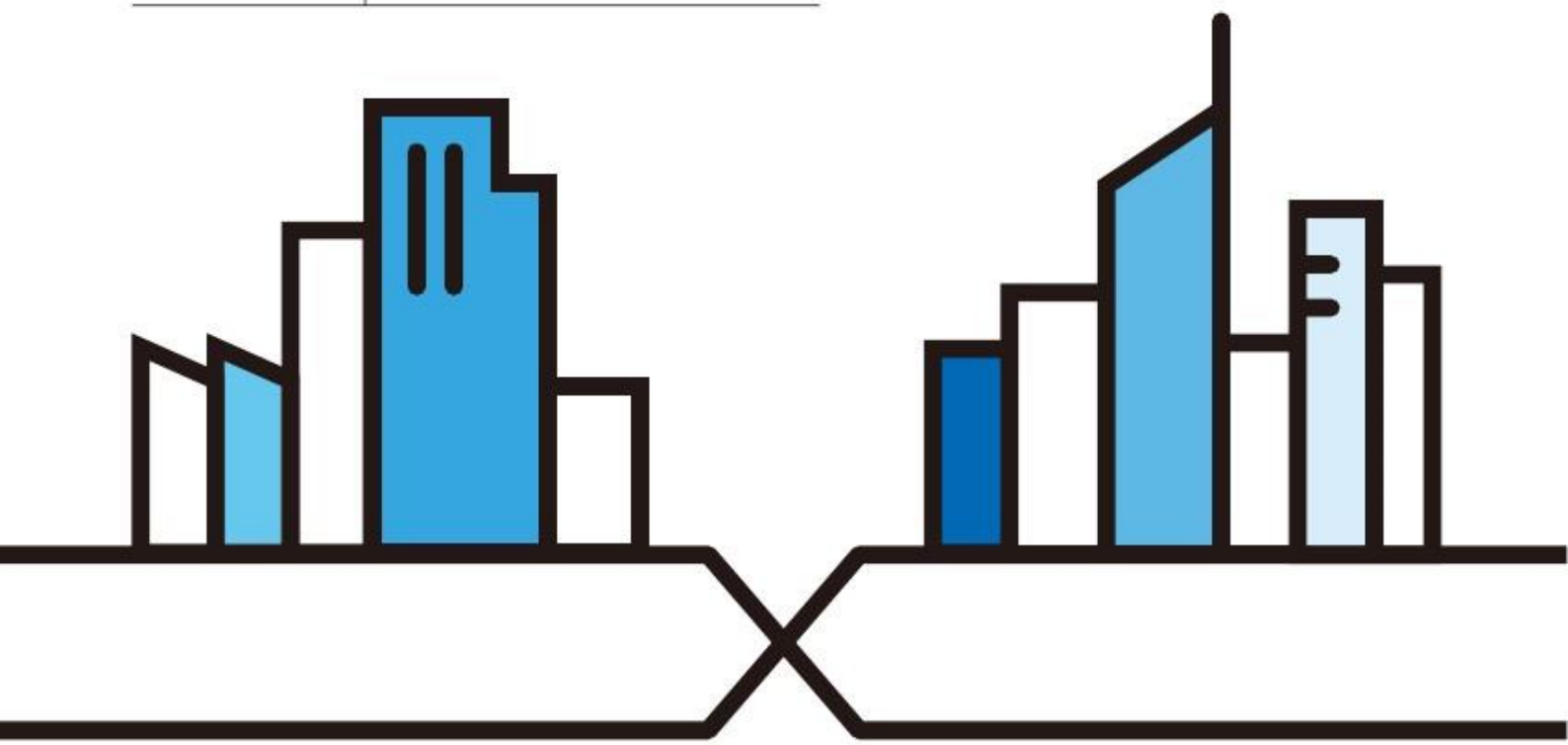
Руководство пользователя

NBG-418N v2

Домашний маршрутизатор Wireless N300

Login по умолчанию	
Web-адрес	http://myrouter (router mode)
LAN IP Address	http://192.168.1.1 (режим маршрутизатора) http://192.168.1.2 (режим non-router)
User Name	admin
Password	1234

Version 1.00 Edition 4, 05/2019



ВАЖНАЯ ИНФОРМАЦИЯ!

ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ПЕРЕД ПЕРВЫМ ИСПОЛЬЗОВАНИЕМ.

СОХРАНИТЕ ЭТО РУКОВОДСТВО – ОНО МОЖЕТ ВАМ ПОНАДОБИТЬСЯ В БУДУЩЕМ!

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. Мы прилагаем максимальные усилия для обеспечения корректности приводимой в этом руководстве информации.

Дополнительная документация

• Краткое руководство по подготовке к эксплуатации Quick Start Guide

В Quick Start Guide объясняется, как подготовить NBG-418N v2 к работе.

• Дополнительная информация

Другую информацию о NBG-418N v2 можно найти на сайте **support.zyxel.com**.

Условные обозначения

Предупреждения и примечания

В этом руководстве предупреждения и примечания обозначаются красным цветом.

Предупреждение сообщает вам об опасности для вашего здоровья и/или вашего устройства.

Примечание: Примечание сообщает вам другую важную информацию, например, что еще нужно сконфигурировать или полезные советы и рекомендации.

Синтаксические обозначения

• В этом руководстве устройство Zyxel обозначается как “NBG-418N v2”.

• **Полужирным шрифтом** обозначаются метки на продукте, названия экранов, названия полей на экране и варианты выбора.

• Правая угловая скобка (>) в имени экрана обозначает щелчок мышью. Например, **Network > WAN > Internet Connection** обозначает, что для перехода к этому экрану сначала нужно щелкнуть **Network** на панели навигации, затем подменю **WAN** и наконец вкладку **Internet Connection**.

Краткое содержание

Содержание

Часть I

Руководство пользователя

Глава 1
Введение

1.1 Обзор

NBG-418N v2 поможет вам расширить вашу проводную сеть без прокладки дополнительных проводов и обеспечит удобный доступ к вашей сети для пользователей мобильных устройств.

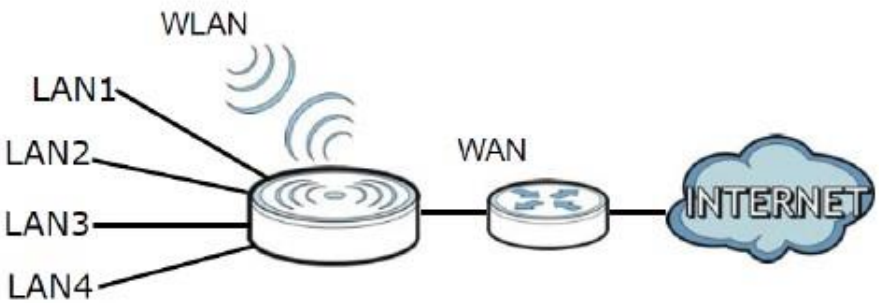
С помощью NBG-418N v2 можно развернуть следующие типы подключений через сеть:

• 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 NBG-418N v2



NBG-418N v2 может обслуживать устройства, совместимые с IEEE 802.11b/g/n, в режиме:

• Маршрутизатора

• Точки доступа

• Универсального повторителя

• Моста

Для управления NBG-418N v2 можно использовать (поддерживаемый) web-браузер. Меню при этом зависят от режима работы устройства.

Режим маршрутизатора

Режим точки доступа или универсального повторителя

Режим моста

См. Главу 4 на стр. 30, где описаны эти режимы.

1.2 Защита NBG-418N v2

Для улучшения безопасности NBG-418N v2 и эффективного управления этим устройством рекомендуется периодически:

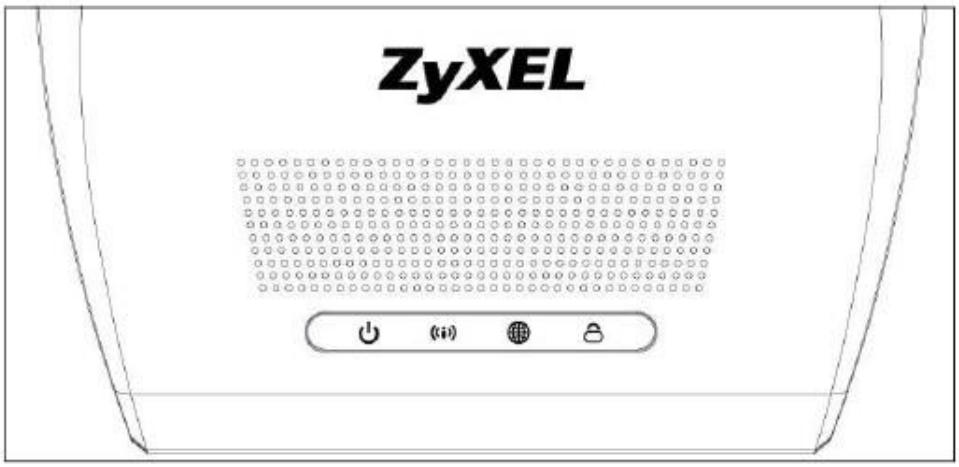
• Менять пароль. Следует использовать пароль, который трудно угадать и который состоит из символов разных типов, например, цифр и букв.

• 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 NBG-418N v2 в заводские настройки по умолчанию. Если у вас есть сделанная ранее резервная копия конфигурационного файла, то не надо заново настраивать всю конфигурацию NBG-418N v2, 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

LED	COLOR	STATUS	**ОПИСАНИЕ**
POWER	Зеленый	Горит	Питание NBG-418N v2 выключено и устройство работает в штатном режиме.
		Не горит	Питание NBG-418N v2 выключено
WAN	Зеленый	Горит	NBG-418N v2 подключен к WAN через порт 10/100MB.
		Мигает	NBG-418N v2 передает/принимает трафик через WAN.
		Не горит	Нет подключения к WAN.
WLAN	Зеленый	Горит	NBG-418N v2 готово к работе в беспроводной сети, но не передает/принимает трафик.
		Мигает	NBG-418N v2 передает/принимает трафик по беспроводной сети. NBG-418N v2 устанавливает соединение WPS с беспроводным клиентом.
		Не горит	Беспроводная сеть не работает.
WPS	Зеленый	Горит	С помощью WPS установлено соединение.
		Мигает	NBG-418N v2 устанавливает соединение WPS с беспроводным клиентом.
		Не горит	WPS не используется или отключена.

1.4 Кнопка WPS/RESET

NBG-418N v2 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 задней панели NBG-418N v2.

1.4.1 Использование кнопки WPS/RESET

1. Убедитесь, что горит светодиод POWER.
2. Нажмите кнопку WPS/RESET и отпустите ее не ранее чем через 3 секунды чтобы включить функцию WPS.
3. Для сброса секунд NBG-418N v2в заводские настройки по умолчанию нажмите кнопку WPS/RESET и отпустите не ранее чем через 10 секунд.

Подробнее о использовании кнопки WPS/RESET см. Раздел 5.3 на стр. 48.

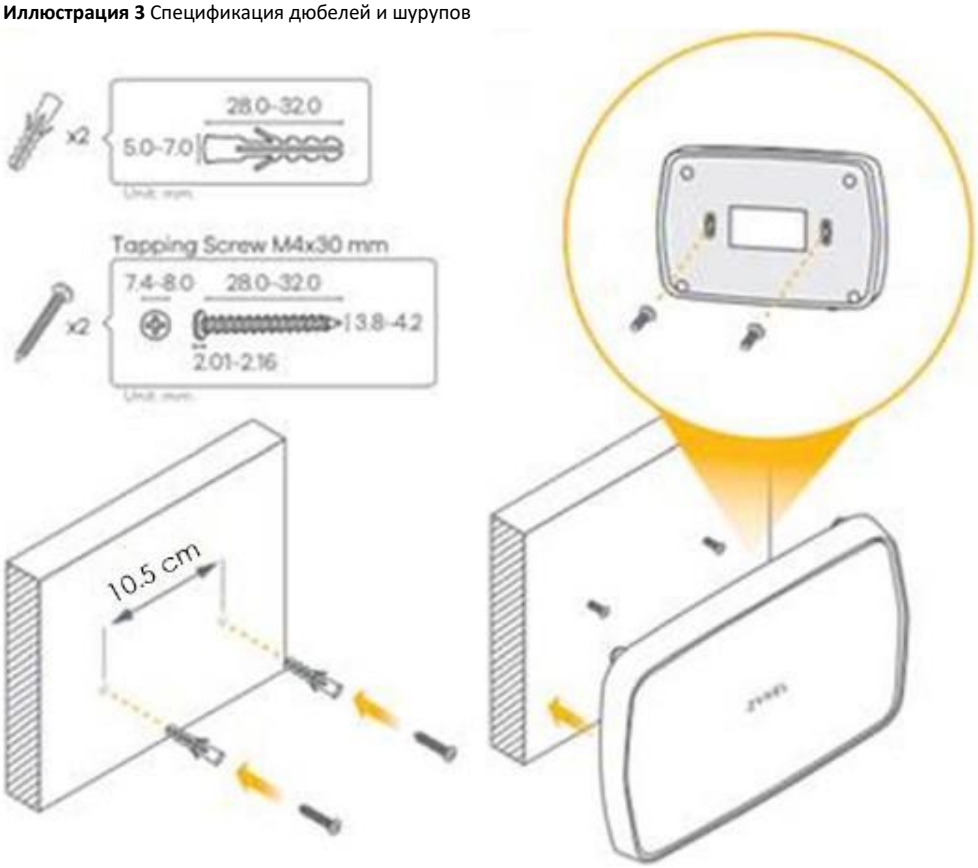
1.5 Монтаж на стене

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 на расстоянии 10,5 см.

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

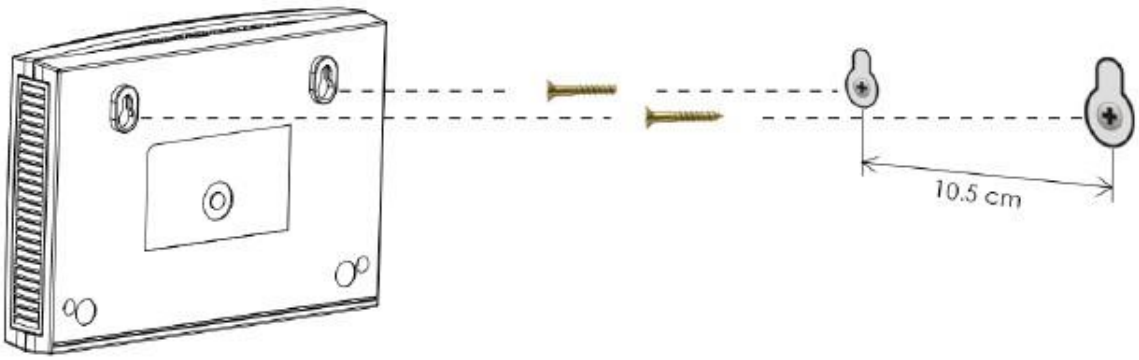
3 Если вы используете дюбели, то просверлите два отверстия для установки дюбелей, затем полностью утопите дюбели в эти отверстия и вверните в них шурупы. Шурупы не следует завинчивать до конца – нужно оставить промежуток примерно 0,5 см между головкой шурупа и стеной.

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

4 Убедитесь, что шурупы зафиксированы и смогут выдержать вес NBG-418N v2 вместе с кабелями.

5 Выровняйте отверстия на задней панели NBG-418N v2 с головками шурупов на стене и наденьте NBG-418N v2 на эти шурупы.

Иллюстрация 4 Пример монтажа на стене



ГЛАВА 2
Web Configurator

2.1 Обзор

В этой главе объясняется, как запустить программу Web Configurator для обслуживания NBG-418N v2, и дается обзор экранов Web Configurator.

Web Configurator – это интерфейс управления на базе HTML для простой и удобной настройки и управления NBG-418N v2 с помощью Интернет-браузера. Для его использования нужен браузер, поддерживающий HTML5, например, Internet Explorer 8.0 или более поздней версии, Mozilla Firefox 3 и более поздней версии либо Safari 2.0 и более поздней версии. Для работы с Web Configurator рекомендуется установить разрешение экрана 1024 x 768.

Для использования Web Configurator нужно разрешить:

• всплывающие окна Web-браузера с вашего устройства (по умолчанию заблокированы в Window 7).

• JavaScript (включен по умолчанию).

• Java permissions (включено по умолчанию).

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

2.2 Доступ к Web Configurator

1 Правильно подключите кабели к NBG-418N v2 и подготовьте ваш компьютер или компьютерную сеть к подключению к NBG-418N v2 (см. «Краткое руководство по подготовке к эксплуатации» Quick Start Guide).

2 Запустите web-браузер.

3 Если NBG-418N v2 работает в режиме маршрутизатора, то в адресной строке браузера введите http://myrouter или http://192.168.212.1. 192.168.212.1 - это адрес IP-адрес LAN в режиме маршрутизатора (это режим работы по умолчанию). (IP-адрес LAN в другом режиме 192.168.1.2).

Ваш компьютер при этом должен быть в одной подсети с NBG-418N v2 для доступа к этому адресу web-сайта. В режиме маршрутизатора NBG-418N v2 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).

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

Иллюстрация 5 Login Screen

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 NBG-418N v2 надо 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 NBG-418N v2.
- Выберите язык Web Configurator. Изменение языка описано в Главе 22 на стр. 132159.

Иллюстрация 8 Выбор типа настройки

2.3 Сброс настроек NBG-418N v2

Если вы забыли свой пароль или IP-адрес или у вас нет доступа к Web Configurator, то нужно с помощью кнопки **WPS/RESET** на задней панели NBG-418N v2 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 **WPS/RESET** не менее чем на 10 секунд для перезапуска/перезагрузки NBG-418N v2 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**.

Иллюстрация 8 Выбор Go to Wizard setup

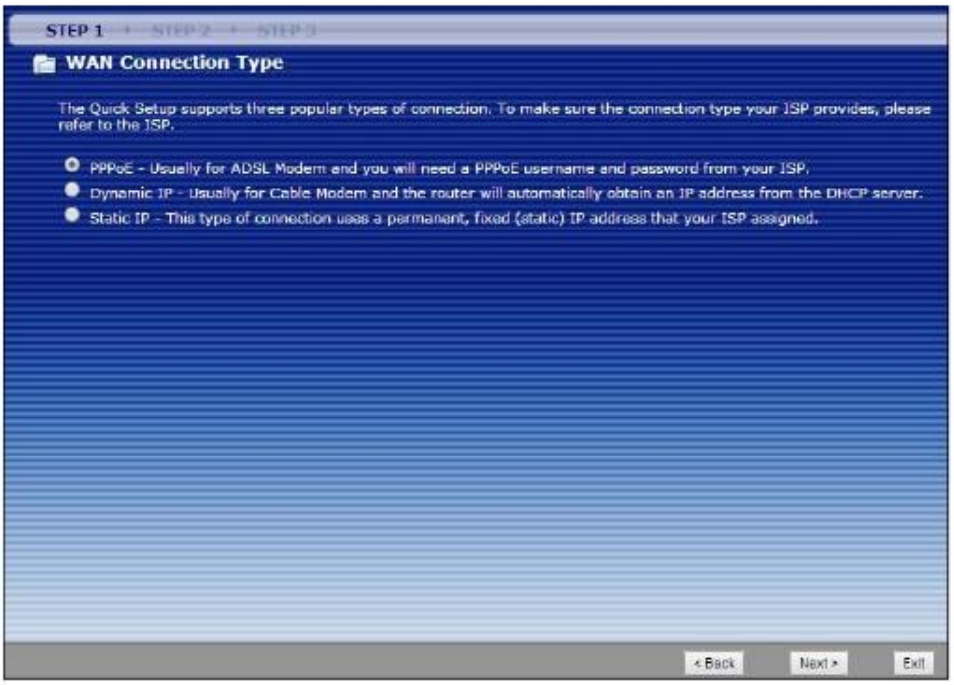
Иллюстрация 9 Экран Welcome to the Connection Wizard

2 Прочитайте информацию на этом экране и щелкните **Next**.

3.2 Визард соединения: ШАГ 1: WAN Connection Type

NBG-418N v2 поддерживает три типа соединения с Интернетом: PPP over Ethernet (PPPoE), Dynamic IP и Static IP. На Шаге 1 Визарда нужно выбрать тип соединения, который поддерживает ваш Интернет-провайдер.

Иллюстрация 10 Шаг визарда 1: WAN Connection Type



В следующей таблице описаны поля этого экрана.

Таблица 3 Шаг визарда 1: WAN Connection Type

ПОЛЕ	ОПИСАНИЕ
PPPoE	Выберите **PPPoE** для настройки соединения по коммутируемым линиям.
Dynamic IP	Выберите **Dynamic IP** если ваш провайдер не назначил вам постоянный IP-адрес.
Static IP	Выберите **Static IP** если ваш провайдер не назначил вам постоянный IP-адрес, который может использовать NBG-418N.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.
Exit	Щелкните **Exit** для выхода из визарда без сохранения изменений.

3.2.1 Соединение PPPoE

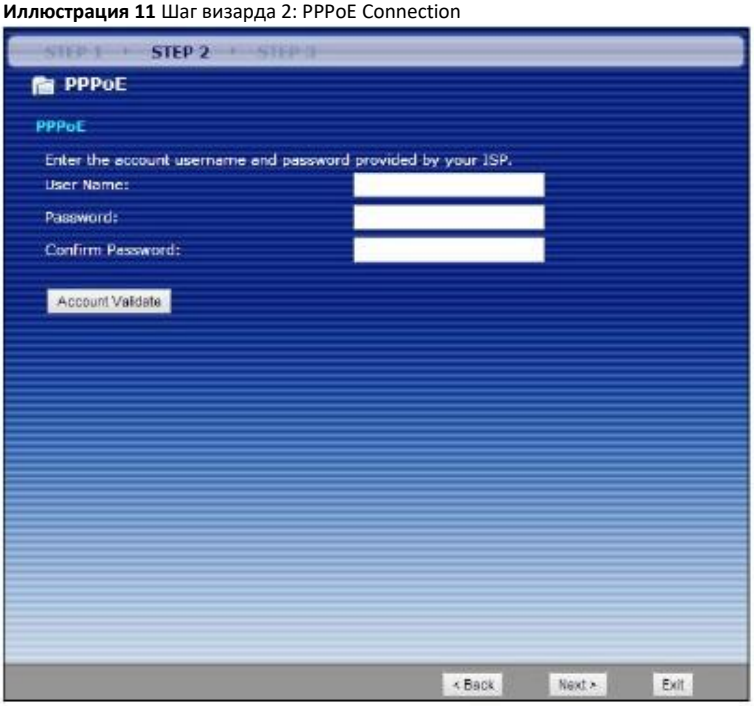
Point-to-Point Protocol over Ethernet (PPPoE) используется для соединения по коммутируемым линиям. PPPoE – это разработанный комитетом IETF (Internet Engineering Task Force) стандарт взаимодействия хоста (персонального компьютера) с широкополосным модемом (например, DSL или кабельным, беспроводным модем и т.п.) для доступа к высокоскоростной сети передачи данных. Сервис-провайдерам PPPoE предоставляет возможность доступ с механизмом аутентификации, совместимым с имеющимися системами контроля доступа (например, RADIUS).

Одно из преимуществ PPPoE – это доступ конечного пользователя к нескольким сетевым сервисом с помощью функции dynamic service selection (динамический выбор сервисов), что позволяет провайдеру легко развертывать новые IP-сервисы для определенных пользователей.

PPPoE упрощает и обслуживание и использование как для подписчика сервисов, так и провайдера/оператора, поскольку не нужно настаивать конфигурацию широкополосного модема, установленного у подписчика.

При использовании PPPoE непосредственно на NBG-418N v2 (а не на отдельных компьютерах) не требуется инсталлировать программу PPPoE на всех ПК локальной сети, и при использовании NAT у всех этих компьютерах будет доступ к Интернету.

Иллюстрация 11 Шаг визарда 2: PPPoE Connection



В следующей таблице описаны поля этого экрана.

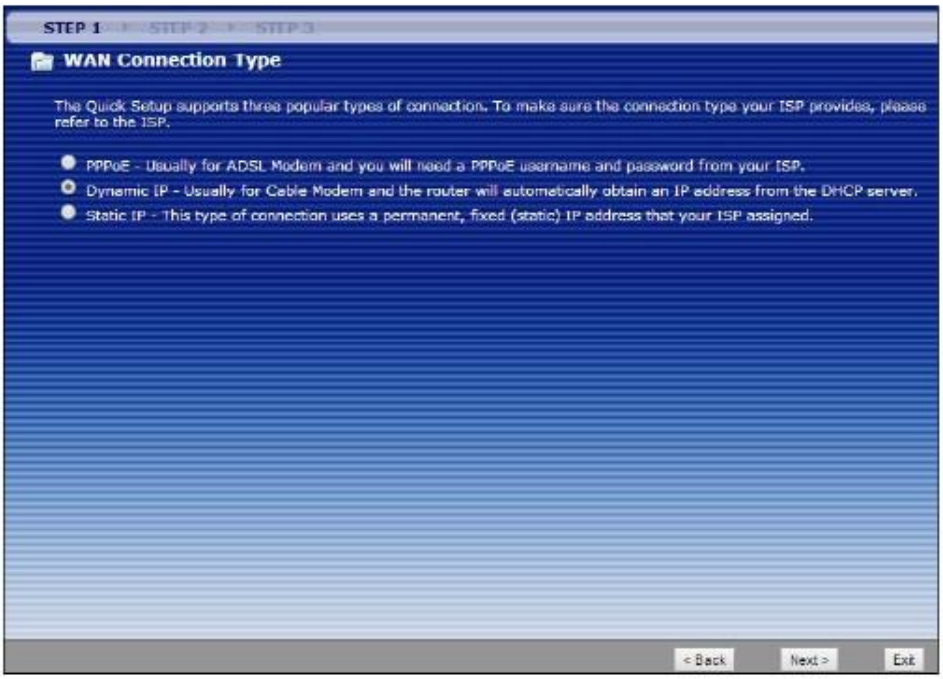
Таблица 4 Шаг визарда 2: PPPoE Connection

ПОЛЕ	ОПИСАНИЕ
PPPoE	
User Name	Введите имя пользователя, которое вам должен сообщить ваш провайдер.
Password	Введите пароль, соответствующий этому **User Name**.
Confirm Password	Введите пароль еще раз для подтверждения.
Account Validate	Щелкните **Account Validate** чтобы установить соединение с Интернетом с использованием инкапсуляции PPPoE.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	**Щелкните Next для продолжения**.
Exit	Щелкните **Exit** для выхода из визарда без сохранения изменений.

3.2.2 Dynamic IP Connection

Используйте Dynamic IP Connection если ваш системный администратор или Интернет-провайдер динамически назначает вам IP-адрес.

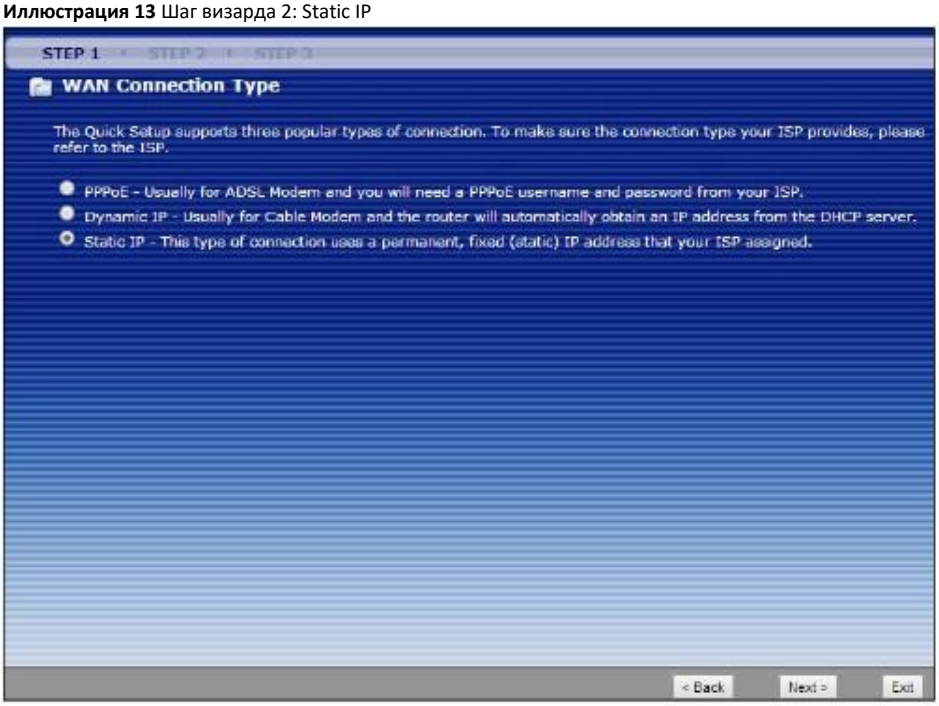
Иллюстрация 12 Шаг визарда 1: Dynamic IP Connection



3.2.3 Static IP Connection

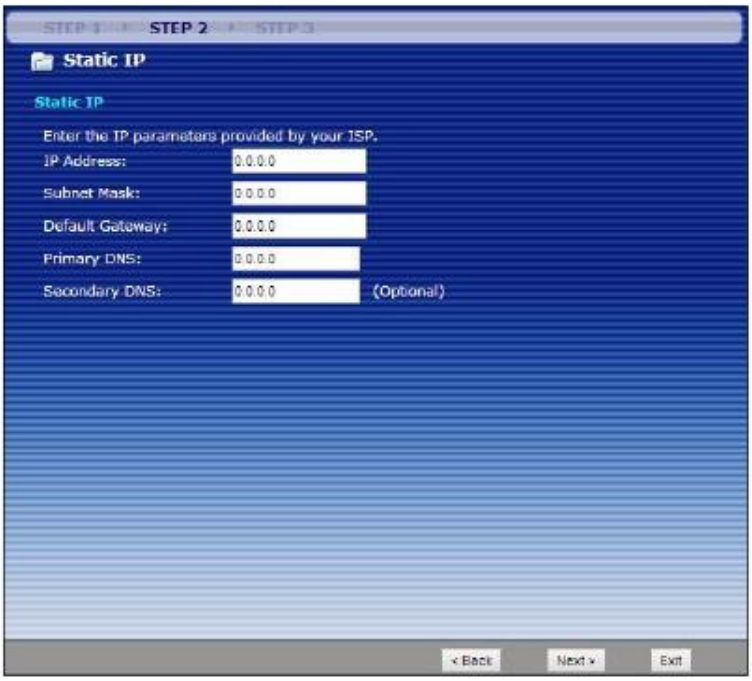
С помощью следующего экрана визарда можно назначить NBG-418N v2постоянный IP-адрес.

Иллюстрация 13 Шаг визарда 2: Static IP



Щелкните **Next** для перехода к следующему экрану

Иллюстрация 14 Шаг визарда 2: Static IP Connection



В следующей таблице описаны поля этого экрана.

Таблица 5 Шаг 2 визарда : Static IP Connection

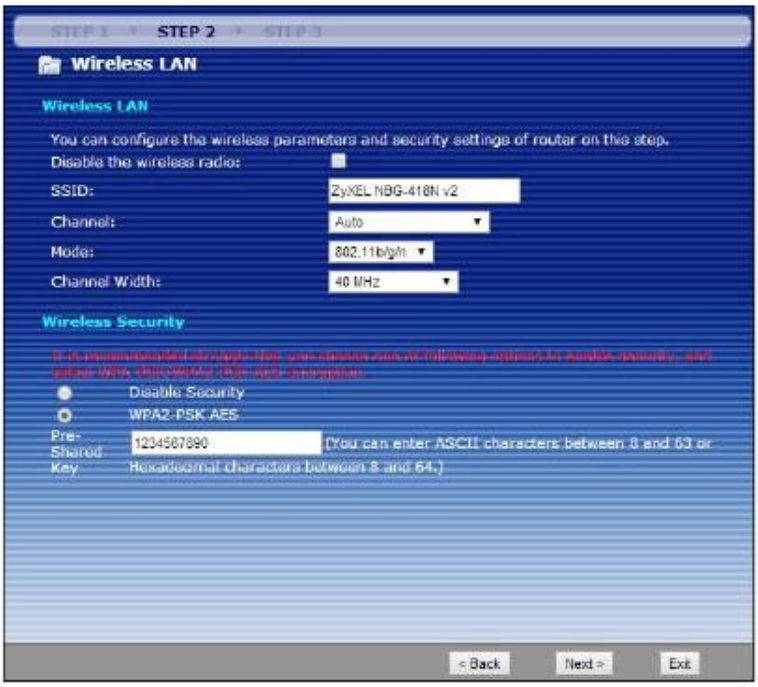
ПОЛЕ	ОПИСАНИЕ
IP Address	Выберите эту опция если ваш провайдер сообщил вам постоянный IP-адрес и/или настройки сервера DNS. Этот IP-адрес должен быть в той же подсети, что и широкополосный модем или маршрутизатор.
Subnet Mask	В это поле нужно ввести маску подсети.
Default Gateway	В это поле нужно ввести IP-шлюза, который вам сообщил ваш провайдер.
Primary 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. NBG-418N v2 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 основного DNS-сервера.
Secondary DNS	Введите в это поле IP-адрес резервного (secondary) DNS-сервера. Это опционное поле.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для продолжения.
Exit	Щелкните **Exit** для выхода из визарда без сохранения изменений.

Щелкните **Next** для настройки на NBG-418N v2параметров WLAN.

3.3 Connection Wizard: ШАГ 2: Wireless LAN

Для настройки беспроводной сети используется следующий экран.

Иллюстрация 15 Шаг 2 визарда: Wireless LAN



В следующей таблице описаны поля этого экрана.

Таблица 6 Шаг 2 визарда : Wireless LAN

ПОЛЕ	ОПИСАНИЕ
Wireless LAN	
Disable the wireless radio	Поставьте галочку в это поле если надо отключить WLAN на NBG-418N v2.
SSID	Введите имя беспроводной сети (до 32 7-битных печатных символов). Если вы изменили SSID беспроводной сети на NBG-418N v2, то надо изменить SSID и у всех беспроводных клиентов, которые используют эту сеть.
Channel	Диапазон радиочастот, используемых беспроводных каналом 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 NBG-418N v2 будет автоматически выбирать канал с наименьшими помехами.
Mode	Выберите из раскрывающегося списка режим IEEE 802.11 WLAN, который будет использовать NBG-418N v2.
Channel Width	Выберите какую ширину беспроводного канала будет использовать ваша беспроводная сеть (20MHz или 40MHz). Если выбрать **Auto**, то NBG-418N v2 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 для увеличения пропускной способности. Беспроводные клиенты при этом также должны использовать 40 MHz.
Wireless Security	
Disable Security	Поставьте галочку в это поле если надо отключить настройки безопасности WLAN.

Таблица 6 Шаг 2 визарда: Wireless LAN (продолжение)

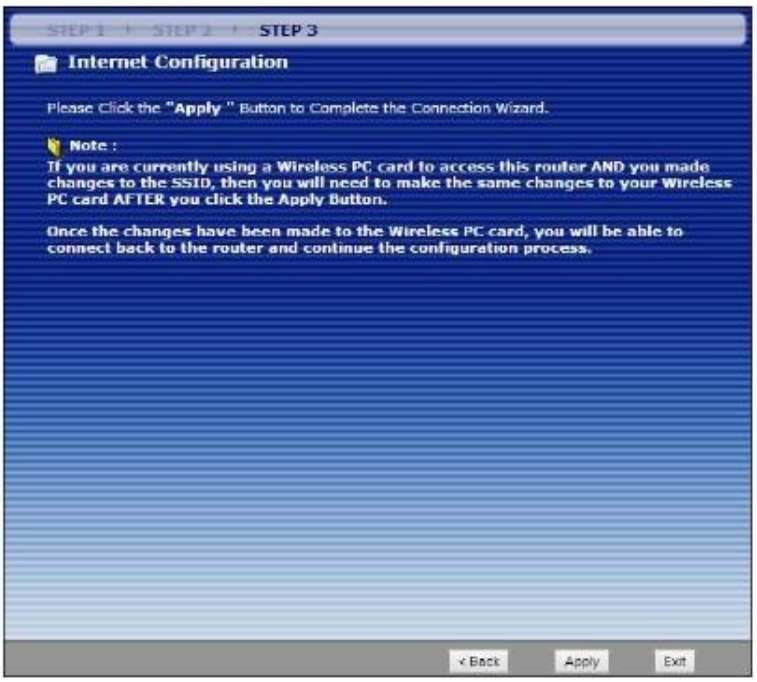
ПОЛЕ	ОПИСАНИЕ
WPA2-PSK AES	Выберите безопасность **WPA2-PSK AES** чтобы сконфигурировать ключ Pre-Shared Key. Эту опцию можно использовать только беспроводной клиент поддерживает WPA2-PSK. Нужно в следующее поле ввести Pre-Shared Key.
Pre-Shared Key	Введите ключ pre-shared key, который может состоять из 8 - 63 символов ASCII или 8 - 64 шестнадцатеричных символа в поле **Pre-Shared Key**.
Back	Щелкните **Back** для возврата к предыдущему экрану.
Next	Щелкните **Next** для перехода к следующему экрану.
Exit	Щелкните **Exit** для выхода из визарда без сохранения изменений.

Примечание: Беспроводные станции и NBG-418N v2 должны использовать одинаковые SSID, channel ID, WPA-PSK (если включено WPA-PSK) или WPA2-PSK (если включено WPA2-PSK).

3.4 Визард соединения: ШАГ 3: Internet Configuration

Щелкните **Apply** для завершения настройки сетевых подключений и доступа к Интернету NBG-418N v2. Экран визарда зависит от выбранного вами типа соединения.

Иллюстрация 16 Шаг визарда 3: Internet Configuration.



3.5 Экран Connection Wizard Complete

Щелкните **Finish** для завершения настройки с помощью визарда.

Иллюстрация 17 Connection Wizard Complete

Теперь ваш NBG-418N v2 может обслуживать вашу сеть; он подключен к Интернету.

ГЛАВА 4
Режимы работы

4.1 Обзор

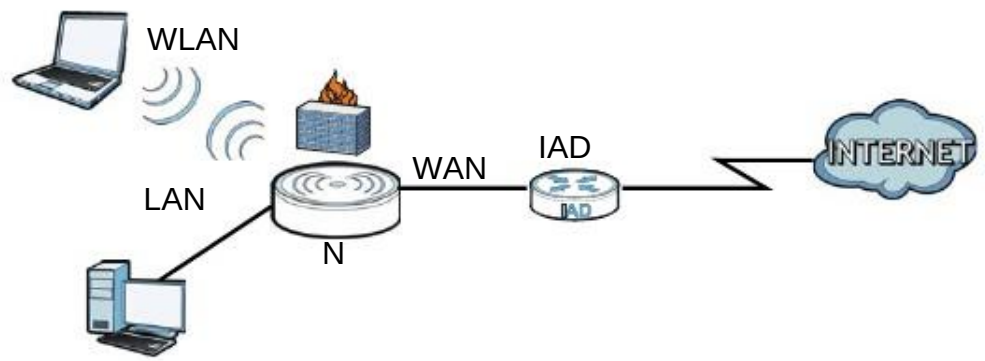
В этом разделе описываются разные режимы использования NBG-418N v2 для обслуживания устройств, поддерживающих IEEE 802.11b/g/n

Примечание: С самого начала правильно выберите режим работы – при изменении режима работы NBG-418N v2 автоматически выполнит перезагрузку.

По умолчанию у NBG-418N v2 в режиме администратора IP-адрес LAN 192.168.212.1. По умолчанию для других режимов работы IP-адрес NBG-418N v2 192.168.1.2.

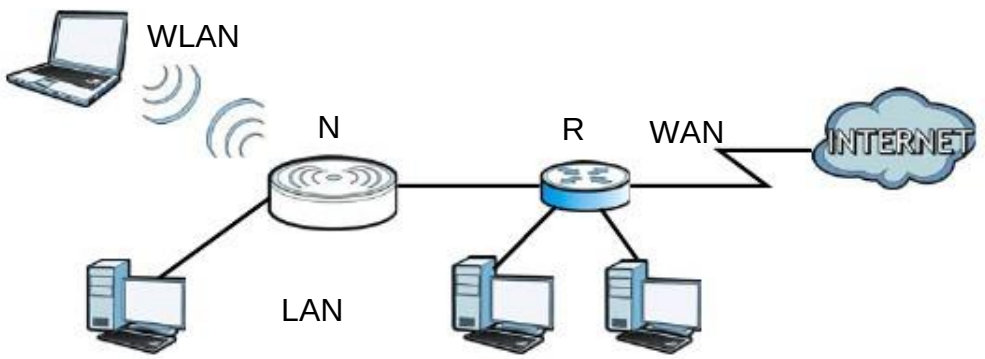
• **Маршрутизатор:** Этот режим позволяет использовать на NBG-418N v2 (N) такие функции маршрутизации, как LAN DHCP, NAT, межсетевой экран и т.п. У NBG-418N v2 отдельные IP-адреса для LAN и WAN. Подключите его порт WAN к такому интегрированному устройству доступа Internet Access Device (IAD), как широкополосный модем.

Иллюстрация 18 Режим маршрутизатора



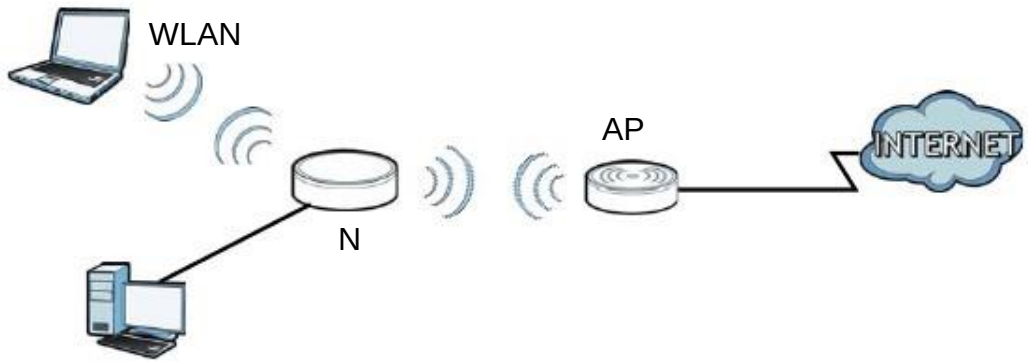
• **Точка доступа:** Этот режим используется если в сети уже есть маршрутизатор (R) и надо развернуть беспроводную сеть и связать мостом проводные и беспроводные соединения NBG-418N v2.

Иллюстрация 19 Режим точки доступа



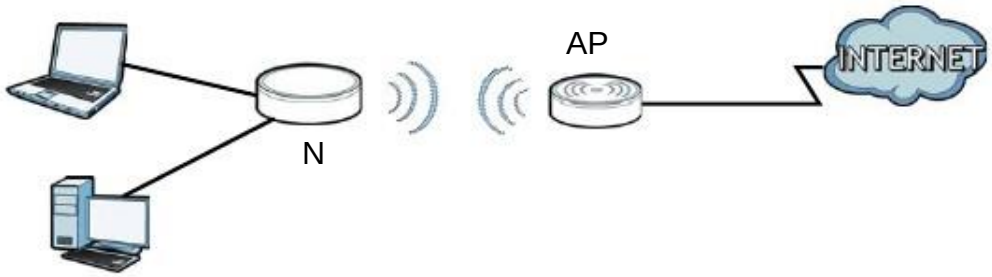
• **Универсальный повторитель**: В этом режиме NBG-418N v2 (N) одновременно работает как точка доступа и беспроводной клиент. Этот режим следует использовать если у вас в сети уже есть беспроводной маршрутизатор или точка доступа и вам нужно, чтобы NBG-418N v2 (N) ретранслировал по беспроводной связи сигналы от беспроводных клиентов точке доступа.

Иллюстрация 20 Универсальный повторитель



• **Мост**: В этом режиме NBG-418N v2 (N) работает только как точка доступа если у вас в сети уже есть беспроводной маршрутизатор или точка доступа, к которой вы хотите подключить по беспроводной связи вашу локальную сеть. В этом режиме для подключения к точке доступа нужно знать ее SSID и настройки безопасности.

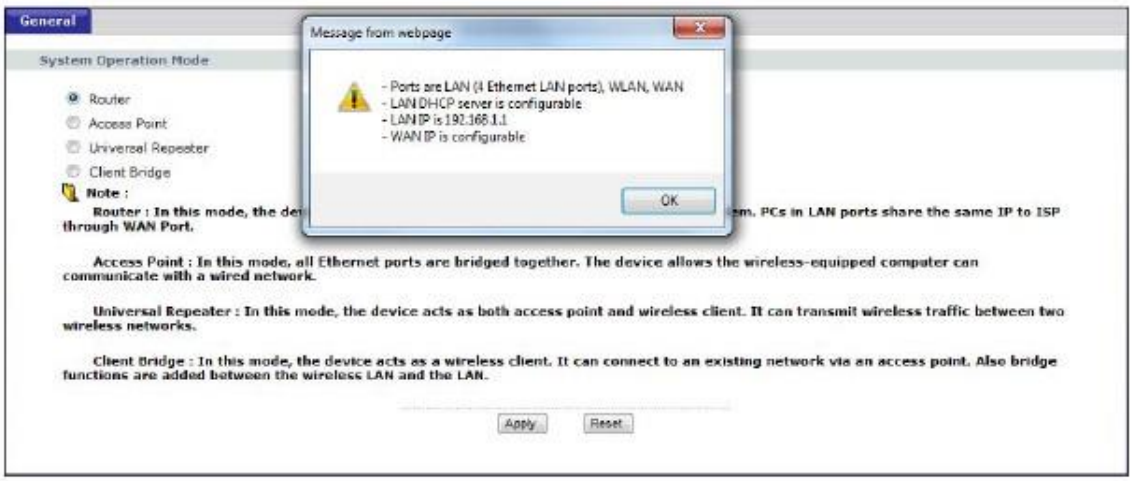
Иллюстрация 21 Мост



4.2 Настройка NBG-418N v2 в режиме маршрутизатора

По умолчанию NBG-418N v2 работает в режиме маршрутизатора. Если NBG-418N v2 работает в другом режиме, то для переключения на режим маршрутизатора нужно выполнить следующую процедуру:

1. Подключите ваш компьютер к порту LAN на NBG-418N v2.
2. По умолчанию IP-адрес NBG-418N v2 192.168.212.1 в режиме маршрутизатора и 192.168.212.2 в режиме точки доступа. В режиме маршрутизатора NBG-418N v2 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 NBG-418N v2.
4. Зайдите в Web Configurator (см. Глава 2 на стр. 18).
5. Перейдите на экран **Maintenance > Sys OP Mode > General** и выберите **Router**.



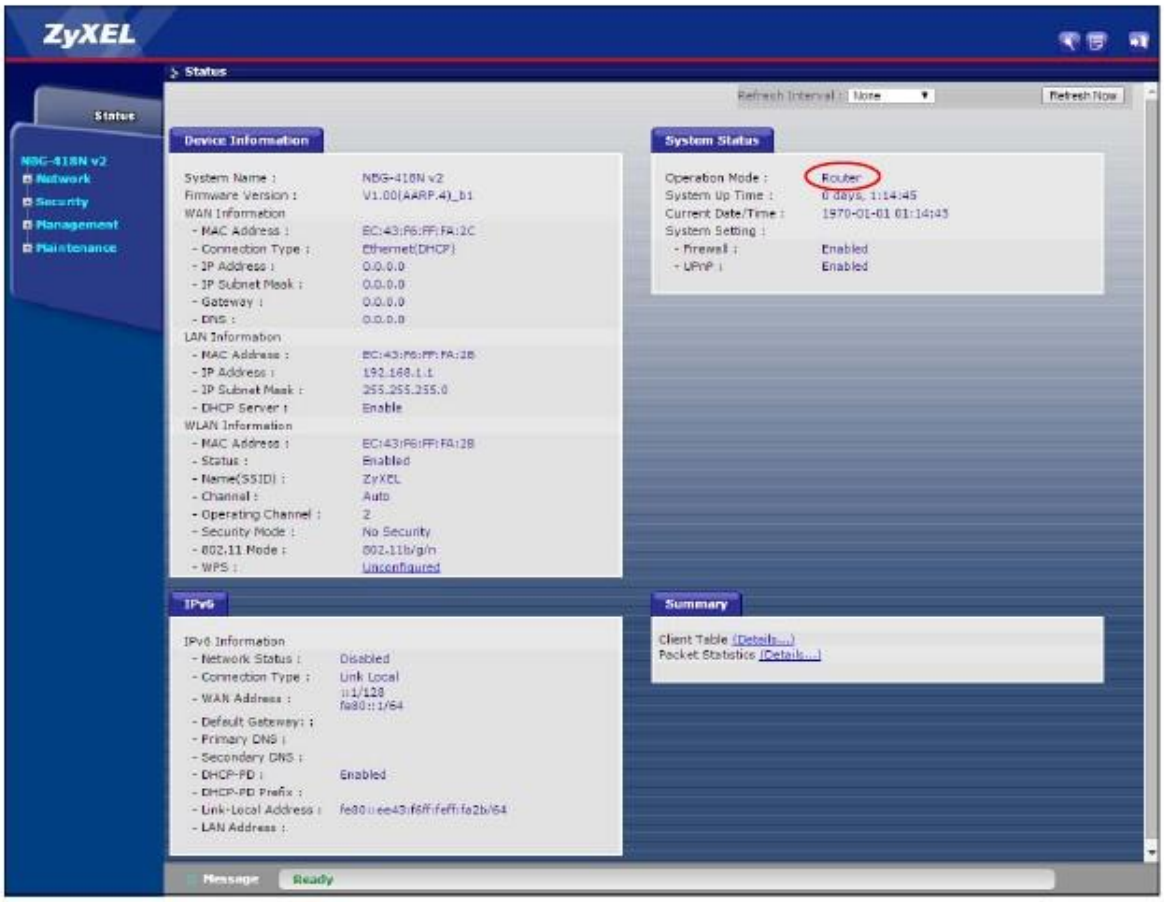
6 Появится всплывающее окно с информацией об этом режиме работы. Щелкните **OK** во всплывающем сообщении Message from webpage и затем **Apply**.

Примечание: Нужно дождаться окончания перезапуска NBG-418N v2 и затем снова зайти на Web Configurator. У NBG-418N v2 IP-адрес изменится на 192.168.212.1.

4.2.1 Status (режим маршрутизатора)

Этот экран отображает состояние NBG-418N v2 в режиме маршрутизатора.

Иллюстрация 22 Экран Status (режим маршрутизатора)



В этой таблице описаны пиктограммы экрана Status.

Таблица 7 Основные пиктограммы экрана Status

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

В следующей таблице описаны поля экрана Status в режиме маршрутизатора.

Таблица 8 Web Configurator - экран 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 NBG-418N v2.
WAN Information	
- MAC Address	MAC-адрес Ethernet-адаптера WAN вашего устройства.
- Connection Type	Текущий тип соединения.

Таблица 8 Web Configurator - экран Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
- 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	
- 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 NBG-418N v2 в беспроводной сети.
- Channel	Номер канала, который был задан вручную либо NBG-418N v2 автоматически сканировал и затем выбрал канал.
- Operating Channel	Номер канала, который NBG-418N v2 сейчас использует для беспроводной сети.
- Security Mode	Тип безопасности беспроводной сети, который использует NBG-418N v2.
- 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**.
IPv6	
Network Status	Состояние сетевого соединения IPv6.
Connection Type	Используемый сейчас тип соединения IPv6.
WAN Address	Текущий WAN IPv6-адрес NBG-418N v2.
Default Gateway	IPV6-адрес шлюза NBG-418N v2.
Primary DNS	IPV6-адрес основного DNS-сервера NBG-418N v2.
Secondary DNS	IPV6-адрес резервного DNS-сервера NBG-418N v2
DHCP-PD	Статус DHCP Prefix Delegation для IPv6.
DHCP-PD Prefix	Префикс Delegated IPv6 DHCP Prefixes.
Link-Local Address	link-local IP-адрес порта LAN в NBG-418N v2. Адрес link-local похож на “private IP address” в IPv4. Можно использовать один адрес same link-local для нескольких интерфейсов устройства.
LAN Address	Адрес LAN для IPv6.
System Status	
Operation Mode	Режим работы: **Router** (маршрутизатор), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост)**.**
System Up Time	Сколько всего времени проработал NBG-418N v2.
Current Date/Time	Дата и время часов NBG-418N v2.
System Setting	
- Firewall	Это поле показывает, включен ли межсетевой экран.

Таблица 8 Web Configurator - экран Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
- UPnP	Это поле показывает, включен ли UPnP.
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 NBG-418N v2.

Иллюстрация 23 Summary: Client Table

В следующей таблице описаны поля этого экрана.

Таблица 9 Summary: Client Table

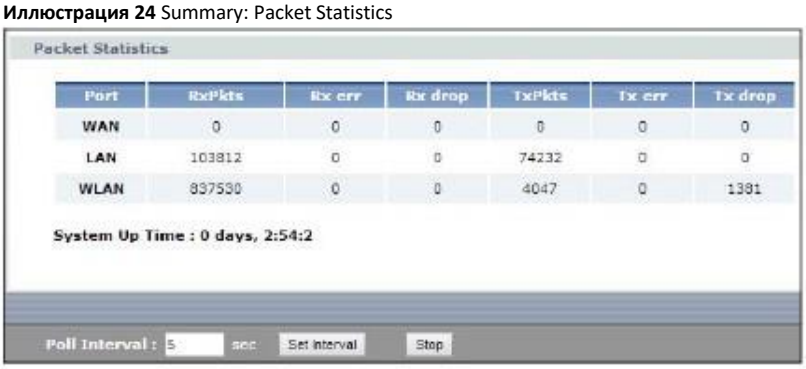
ПОЛЕ	ОПИСАНИЕ
#	Номер компьютера (хоста).
IP Address	IPv4-адрес, соответствующий указанном выше в поле # номеру.
Host Name	Имя компьютера (хоста).
MAC Address	MAC-адрес компьютера, имя которого указано в поле Host Name. У каждого устройства Ethernet есть уникальный адрес MAC (Media Access Control). Этот адрес назначается на заводе и состоит из шести пар шестнадцатеричных цифр, например 00:A0:C5:00:00:02.
Interface	Интерфейс NBG-418N v2, к которому подключен клиент.
IPv6 DHCP Table	
#	Номер по порядку в таблице IPv6 client table.
IPv6 Address	IPv6-адрес компьютера (хоста).
Host Name	Имя компьютера (хоста).
Refresh	Щелкните **Refresh** чтобы обновить этот экран.

4.2.1.2 Summary: Packet Statistics

На экране выводится информация о состоянии портов, статистика по пакетам и время работы после включения или перезагрузки "system up time". Поля этого экрана можно сконфигурировать и обновлять.

Щелкните ссылку **Packet Statistics (Details...)** на экране Status. Здесь выводится состояние портов, статистика по пакетам и время работы системы. В поле **Poll Interval(s)** можно задать периодичность обновления экрана.

Иллюстрация 24 Summary: Packet Statistics



В следующей таблице описаны поля этого экрана.

Таблица 10 Summary: Packet Statistics

ПОЛЕ	ОПИСАНИЕ
Port	Тип порта NBG-418N v2.
RxPkts	Сколько пакетов пришло на этот порт.
Rx err	Сколько пакетов пришло на этот порт с ошибками.
Rx drop	Сколько пакетов, которые пришли на этот порт, было отброшено.
Txpkts	Сколько пакетов было отправлено через этот порт.
Tx err	Сколько пакетов было отправлено через этот порт с ошибками.
Tx drop	Сколько пакетов, которые были отправлены через этот порт, было отброшено.
System Up Time	Общее время работы NBG-418N v2.
Poll Interval(s)	Периодичность обновления статистики на экране.
Set Interval	Щелкните эту кнопку чтобы применить новую периодичность обновления, которую вы задали в поле **Poll Interval(s)**.
Stop	Щелкните **Stop** чтобы остановить обновление статистики.

4.2.2 Панель навигации в режиме маршрутизатора

Меню панели навигации используется для настройки функций NBG-418N v2 в режиме маршрутизатора.

Иллюстрация 25 Меню: режим маршрутизатора

Подменю описаны в следующей таблице.

Таблица 11 Меню: режим маршрутизатора

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Network		
Wireless LAN	General	Экран конфигурирования беспроводной сети.
	MAC Filter	Фильтр MAC-адресов задает блокирование доступа к определенным устройствам или доступа определенных устройств к NBG-418N v2.
	Advanced	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 NBG-418N v2.
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.
	IPv6	Настройка типа соединения IPv6 WAN и адресов LAN/WAN IPv6.
LAN	IP	Настройка IPv4-адреса и маски подсети LAN.
DHCP Server	General	Включение DHCP-сервера NBG-418N v2.
	Advanced	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 NBG-418N v2.
	Port Triggering	Экран для настройки port triggering на NBG-418N v2.
DDNS	General	Экран для настройки Dynamic DNS (сервиса для соответствия фиксированных имен домена и непостоянных IP-адресов).

Таблица 11 Меню: режим маршрутизатора (продолжение)

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Static Route	IP Static Route	Экран для настройки статичных маршрутов IP.
Security		
Firewall	General	Экран для включения/отключения межсетевого экрана.
	Services	Экран для включения/отключения функций ICMP и VPN passthrough.
Content Filter	Filter	Экран для настройки фильтра контента NBG-418N v2.
Management		
Remote MGMT	WWW	Экран для настройки интерфейсов, через которые по IP-адресу можно с помощью HTTP управлять NBG-418N v2.
UPnP	General	Экран для включения UPnP на NBG-418N v2.
Bandwidth MGMT	General	Экран для включения управления полосой пропускания на NBG-418N v2.
	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 NBG-418N v2.
Logs	View Log	Экран для просмотра журналов для выбранных категорий событий.
Tools	Firmware	Экран для загрузки прошивки на NBG-418N v2.
	Configuration	Экран для резервного копирования/восстановления конфигурации и сброса NBG-418N v2 в заводские настройки по умолчанию.
	Restart	Экран для перезагрузки NBG-418N v2 без выключения питания.
Sys OP Mode	General	**Router** (маршрутизатор), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост)**.**
Language	Language	Экран для выбора языка.

4.3 Настройка NBG-418N v2 в режиме точки доступа

1 Подключите ваш компьютер к порту LAN на NBG-418N v2.

2 По умолчанию IP-адрес NBG-418N v2 192.168.212.1 в режиме маршрутизатора и 192.168.212.2 в другом режиме.

3 После настройки IP-адреса компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите IP-адрес NBG-418N v2.

4 Зайдите в Web Configurator (см. Глава 2 на стр. 18).

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

6 Появится всплывающее окно с информацией об этом режиме работы. Щелкните **OK** во всплывающем сообщении Message from webpage и затем **Apply**. Теперь NBG-418N v2 работает в режиме точки доступа (AP Mode) .

Примечание: Нужно дождаться окончания перезапуска NBG-418N v2 и затем снова зайти на Web Configurator.

4.3.1 Экран Status (режим точки доступа AP Mode)

Щелкните **Status**. Этот экран отображает состояние NBG-418N v2 в режиме точки доступа.

Иллюстрация 26 Экран Status (режим точки доступа)

В этой таблице описаны поля экрана Status.

Таблица 12 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 NBG-418N v2.
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	
- MAC Address	This shows the wireless adapter MAC address of your device.
- Status	Состояние беспроводной сети – **On** (включена), **Off** (выключена), **Off by scheduler** (выключена по расписанию).
- Name (SSID)	Имя для идентификации NBG-418N v2 в беспроводной сети.
- Channel	Номер канала, который задан вручную либо NBG-418N v2 автоматически сканировал и выбрал этот канал.
- Operating Channel	Имя для идентификации NBG-418N v2 в беспроводной сети.
- Security Mode	Тип безопасности беспроводной сети, который использует NBG-418N v2.
- 802.11 Mode	Стандарт беспроводной сети IEEE 802.11, который поддерживает NBG-418N v2. Беспроводные клиенты для подключения к NBG-418N v2 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), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост).
System Up Time	Сколько всего времени проработал NBG-418N v2.
Current Date/Time	Дата и время часов NBG-418N v2.
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 NBG-418N v2 в режиме точки доступа.

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

Иллюстрация 27 Меню: режим точки доступа

Подменю описаны в следующей таблице.

Таблица 11 Меню: режим точки доступа

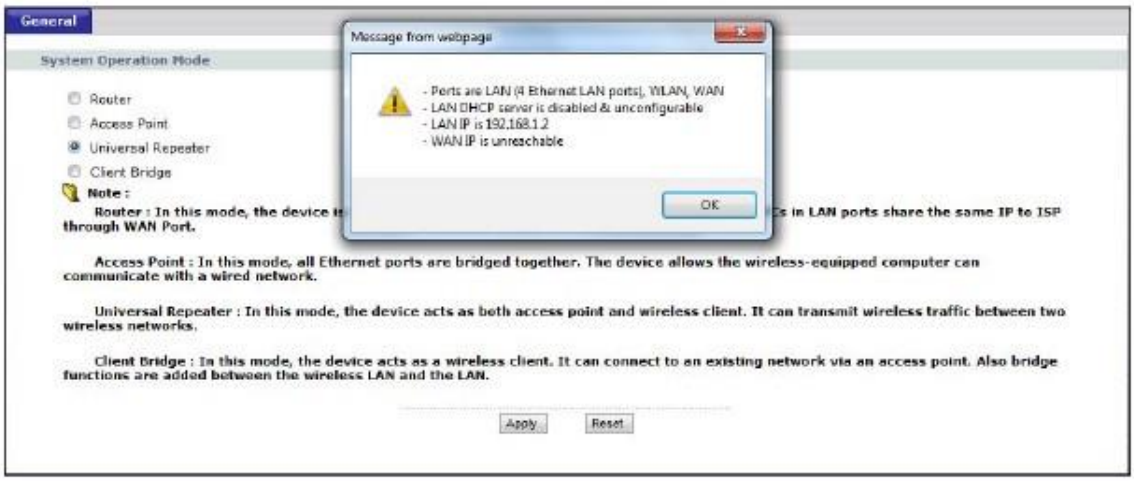
ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Network		
Wireless LAN	General	Экран конфигурирования беспроводной сети.
	MAC Filter	Фильтр MAC-адресов задает блокирование доступа к определенным устройствам или доступа определенных устройств к NBG-418N v2.
	Advanced	Настройка расширенных параметров беспроводной сети.
	WPS	Настройка WPS.
	WPS Station	Добавление беспроводной станции с помощью WPS.
	Scheduling	Расписание включения/отключения беспроводной сети.
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 NBG-418N v2.
Logs	View Log	Экран для просмотра журналов для выбранных категорий событий.
Tools	Firmware	Экран для загрузки прошивки на NBG-418N v2.
	Configuration	Экран для резервного копирования/восстановления конфигурации и сброса NBG-418N v2 в заводские настройки по умолчанию.
	Restart	Экран для перезагрузки NBG-418N v2 без выключения питания.
Sys OP Mode	General	Экран для выбора режима работы устройства (маршрутизатор или точка доступа).
Language	Language	Экран для выбора языка.

4.4 Настройка NBG-418N v2 в режиме универсального повторителя

1. Подключите ваш компьютер к порту LAN на NBG-418N v2.
2. По умолчанию IP-адрес NBG-418N v2 192.168.212.1 в режиме маршрутизатора и 192.168.212.2 в другом режиме.
3. После настройки IP-адреса компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите IP-адрес NBG-418N v2.

4 Зайдите в Web Configurator (см. Глава 2 на стр. 18).

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



6 Появится всплывающее окно с информацией об этом режиме работы. Щелкните **OK** во всплывающем сообщении Message from webpage и затем **Apply**. Теперь NBG-418N v2 работает в режиме универсального повторителя.

Примечание: Нужно дождаться окончания перезапуска NBG-418N v2 и затем снова зайти на Web Configurator.

4.4.1 Status (режим Универсального повторителя)

Щелкните **Status**. Этот экран отображает состояние NBG-418N v2 в режиме Универсального повторителя.

Иллюстрация 28 Экран Status (режим Универсального повторителя)

В этой таблице описаны поля экрана Status.

Таблица 14 Экран Status (режим универсального повторителя)

ПОЛЕ	ОПИСАНИЕ
Device Information	
System Name	Имя системы **System Name**, которые вы ввели на экране Maintenance > System > General.
Firmware Version	Версия прошивки NBG-418N v2.
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	LAN-порт сервера DHCP.
WLAN AP Information	
- 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 NBG-418N v2 в беспроводной сети.
- Channel	Номер канала, который был задан вручную либо NBG-418N v2 автоматически сканировал и затем выбрал канал.
- Operating Channel	Номер канала, который NBG-418N v2 сейчас использует для беспроводной сети.
- Security Mode	Тип безопасности беспроводной сети, который использует NBG-418N v2.
- 802.11 Mode	Стандарт беспроводной сети IEEE 802.11, который поддерживает NBG-418N v2. Беспроводные клиенты для подключения к NBG-418N v2 должны поддерживать тот же стандарт.
- WPS	Состояние WPS (WiFi Protected Setup). Щелкните status чтобы перейти на экран **Network > Wireless LAN > WPS**.
WLAN STA Information	
- SSID	Имя точки доступа, к которой подключен NBG-418N v2.
- Security Mode	Тип безопасности, который используется для подключения NBG-418N v2 к точке доступа.
- Connection Status	Это поле показывает, подключен ли сейчас NBG-418N v2 к этой точке доступа.
System Status	
Operation Mode	Режим работы: **Router** (маршрутизатор), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост)**.**
System Up Time	Сколько всего времени проработал NBG-418N v2.
Current Date/Time	Дата и время часов NBG-418N v2.
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...**
Message	Экран для отображения информации о состоянии NBG-418N v2.

4.4.2 Панель навигации режима универсального повторителя

Меню панели навигации используется для настройки функций NBG-418N v2 в режиме универсального повторителя.

Следующие экран и таблица относятся к функциям, которые настраиваются в режиме универсального повторителя.

Иллюстрация 29 Меню: Режим универсального повторителя

Подменю описаны в следующей таблице.

Таблица 15 Меню: режим универсального повторителя

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Status		Общая информация о NBG-418N v2, состоянии устройства и интерфейсов. На этом экране можно запустить визард и вывести таблицу со сводкой статистики.
Network		
WLAN	AP Select	Экран для выбора точки доступа, к которой нужно подключить NBG-418N v2 (для подключения нужно знать настройки безопасности точки доступа).
	General	Экран конфигурирования беспроводной сети.
	MAC Filter	Фильтр MAC-адресов задает блокирование доступа к определенным устройствам или доступа определенных устройств к NBG-418N v2.
	Advanced	Настройка расширенных параметров беспроводной сети.
	WPS	Настройка WPS.
	WPS Station	Добавление беспроводной станции с помощью WPS.
	Scheduling	Расписание включения/отключения беспроводной сети.
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 NBG-418N v2.
Logs	View Log	Экран для просмотра журналов для выбранных категорий событий.
Tools	Firmware	Экран для загрузки прошивки на NBG-418N v2.
	Configuration	Экран для резервного копирования/восстановления конфигурации и сброса NBG-418N v2 в заводские настройки по умолчанию.
	Restart	Экран для перезагрузки NBG-418N v2 без выключения питания.
Sys OP Mode	General	**Router** (маршрутизатор), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост)**.**
Language	Language	Экран для выбора языка.

4.5 Настройка NBG-418N v2 в режиме моста (Client Bridge)

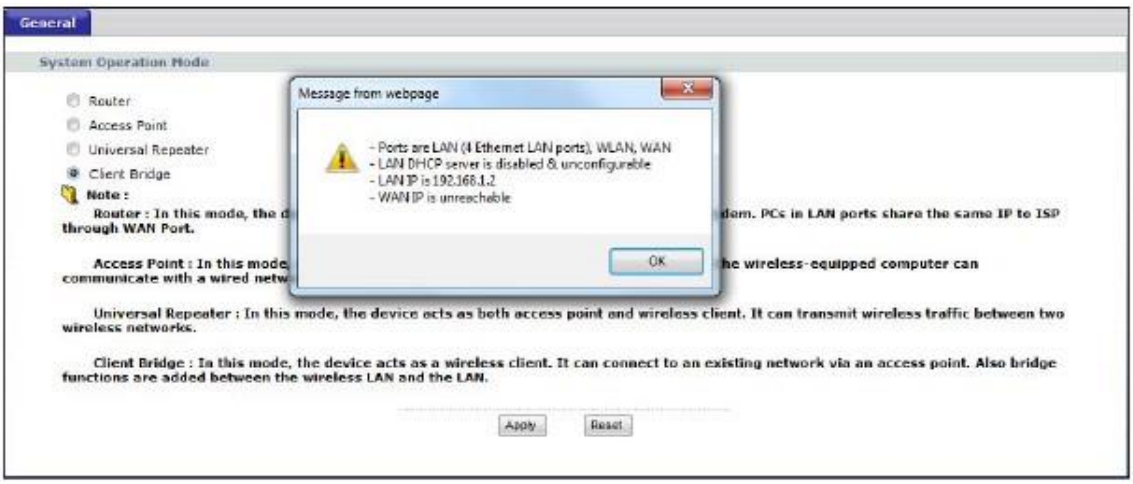
1 Подключите ваш компьютер к порту LAN на NBG-418N v2.

2 По умолчанию IP-адрес NBG-418N v2 192.168.212.1 в режиме маршрутизатора и 192.168.212.2 в другом режиме.

3 После настройки IP-адреса компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите IP-адрес NBG-418N v2.

4 Зайдите в Web Configurator (см. Глава 2 на стр. 18).

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



6 Появится всплывающее окно с информацией об этом режиме работы. Щелкните **OK** во всплывающем сообщении Message from webpage и затем **Apply**. Теперь NBG-418N v2 работает в режиме моста.

Примечание: Нужно дождаться окончания перезапуска NBG-418N v2 и затем снова зайти на Web Configurator.

4.5.1 Status (режим моста)

Щелкните **Status**. Этот экран отображает состояние NBG-418N v2 в режиме моста.

Иллюстрация 30 Экран Status (режим моста)

В этой таблице описаны поля экрана Status.

Таблица 16 Экран Status (режим моста)

ПОЛЕ	ОПИСАНИЕ
Device Information	
System Name	Имя системы **System Name**, которые вы ввели на экране Maintenance > System > General.
Firmware Version	Версия прошивки NBG-418N v2.
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 LAN-порта сервера DHCP.
WLAN STA Information	
- SSID	Имя точки доступа, к которой подключен NBG-418N v2.
- Security Mode	Тип безопасности, который используется для подключения NBG-418N v2 к точке доступа.
- Connection Status	Это поле показывает, подключен ли сейчас NBG-418N v2 к этой точке доступа.
System Status	
Operation Mode	Режим работы: **Router** (маршрутизатор), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост)**.**
System Up Time	Сколько всего времени проработал NBG-418N v2.
Current Date/Time	Дата и время часов NBG-418N v2.
Summary	
Client Table	Экран для вывода информации о клиенте, который сейчас подключен к порту Ethernet LAN NBG-418N v2.
Packet Statistics	Экран для вывода информации о состоянии порта и статистике пакетов.

4.5.2 Панель навигации режима моста

Меню панели навигации используется для настройки функций NBG-418N v2 в режиме моста.

Следующие экран и таблица относятся к функциям, которые настраиваются в режиме моста.

Иллюстрация 31 Меню: Режим моста

Подменю описаны в следующей таблице.

Таблица 17 Меню: режим моста

ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Status		Общая информация о NBG-418N v2, состоянии устройства и интерфейсов. На этом экране можно запустить визард и вывести таблицу со сводкой статистики.
Network		
AP Select	AP Select	Экран для выбора точки доступа, к которой нужно подключить NBG-418N v2 (для подключения нужно знать настройки безопасности точки доступа).
	WLAN Information	На этом экране выводится SSID и режим безопасности точки доступа, к которой подключается NBG-418N v2.
	Advanced	Настройка расширенных параметров беспроводной сети.
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 NBG-418N v2.
Logs	View Log	Экран для просмотра журналов для выбранных категорий событий.
Tools	Firmware	Экран для загрузки прошивки на NBG-418N v2.
	Configuration	Экран для резервного копирования/восстановления конфигурации и сброса NBG-418N v2 в заводские настройки по умолчанию.
	Restart	Экран для перезагрузки NBG-418N v2 без выключения питания.
Sys OP Mode	General	**Router** (маршрутизатор), **Access Point** (точка доступа), **Universal Repeater** (универсальный повторитель) или **Client Bridge** (мост)**.**
Language	Language	Экран для выбора языка.

ГЛАВА 5
Инструкции

5.1 Обзор

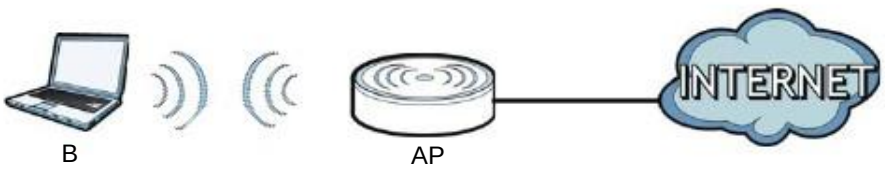
В этой главе собраны инструкции по настройке NBG-418N v2:

- Подключение к Интернету через точку доступа
- Настройка безопасности беспроводной сети, используя WPS на NBG-418N V2 и беспроводном клиенте
- Включение и настройка безопасности беспроводной сети без использования WPS на NBG-418N V2
- Использование нескольких SSID на NBG-418N V2
- Управление полосой пропускания на NBG-418N V2

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 32 Беспроводное соединение с Интернетом через AP



5.3 Настройка безопасности беспроводной сети, используя WPS на NBG-418N v2 и беспроводном клиенте

В этом разделе приведен пример настройки безопасности беспроводной сети, используя WPS. В этом примере NBG-418N v2 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. 49). Это более простой способ.

• **PIN Configuration** - для создания защищенного беспроводного соединения нужно ввести код PIN (Personal Identification Number) беспроводного клиента в интерфейсе NBG-418N v2 (см. Раздел 5.3.2 на стр. 50). Это более безопасный метод, потому что оба устройства могут аутентифицировать друг друга.

5.3.1 Push Button Configuration (PBC)

1. Убедитесь, что NBG-418N v2 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 NBG-418N v2 и нажмите кнопку **Push Button** на экране **Network > Wireless LAN** (2.4G/5G) **> WPS Station**.

Примечание: У NBG-418N v2 кнопка WPS/RESET расположена на задней панели и еще есть программная кнопка WPS в его утилите конфигурирования. Обе кнопки работают одинаково 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.

NBG-418N v2 посылает беспроводному клиенту правильные настройки конфигурации. Это занимает около 2 минут и затем беспроводной клиент может безопасно обмениваться данными с NBG-418N v2.

На следующей иллюстрации показан пример развертывания защищенной беспроводной сети нажатием кнопки и на NBG-418N v2, на беспроводном клиенте (в данном примере NWD210N).

Иллюстрация 33 Пример процесса WPS: вариант с Push Button Configuration

5.3.2 Конфигурирование PIN

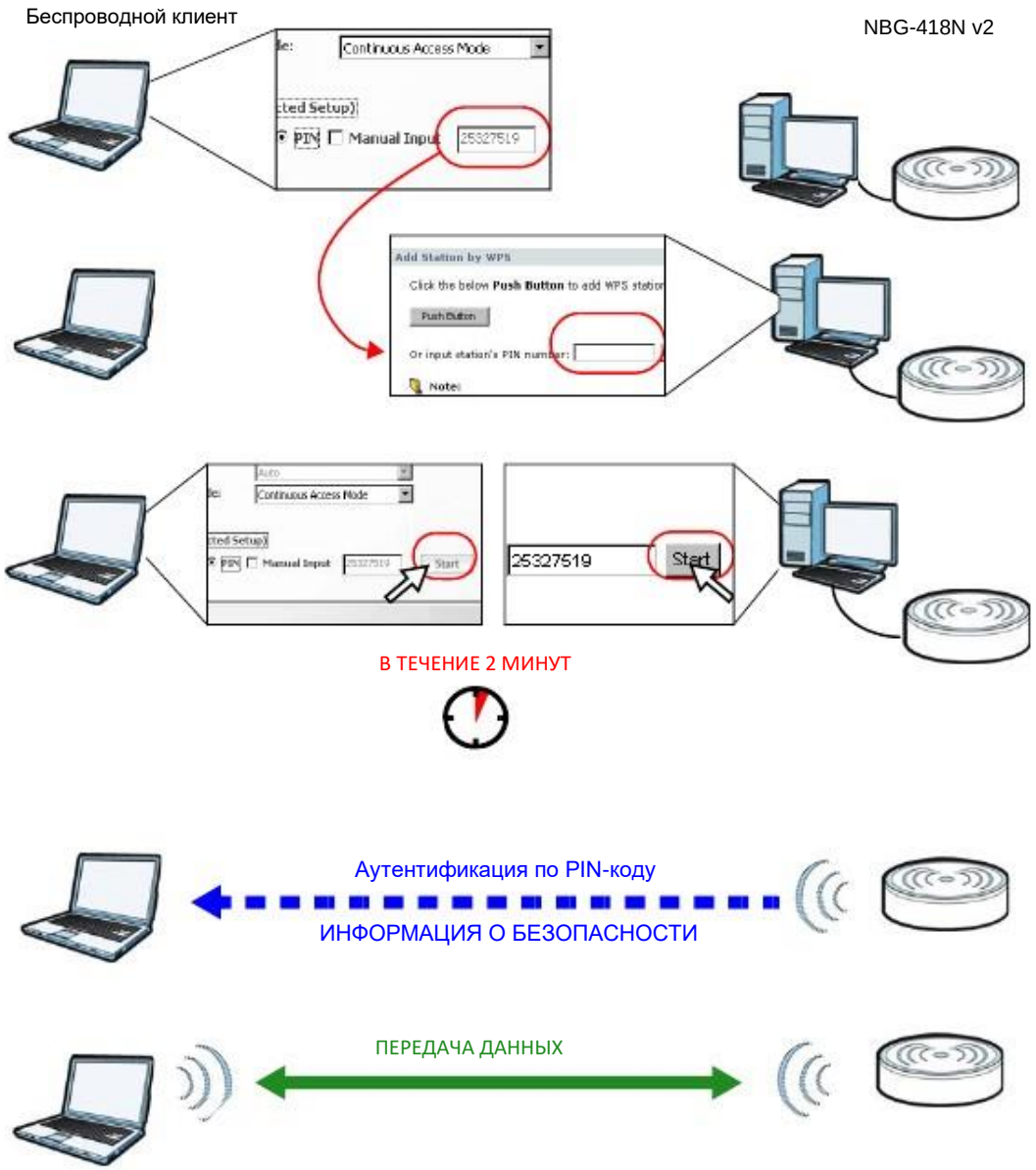
При использовании варианта с конфигурированием PIN нужно использовать интерфейс конфигурирования NBG-418N v2 и утилиту клиента.

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 NBG-418N v2.
3. Щелкните кнопку **Start** (или кнопку рядом с полем PIN) в утилите беспроводного клиента и на экране WPS на NBG-418N v2 в течение 2 минут.

NBG-418N v2 выполняет аутентификацию беспроводного клиента и посылает ему настройки конфигурации. Это занимает около 2 минут и затем беспроводной клиент может безопасно обмениваться данными с NBG-418N v2

На следующей иллюстрации показан пример развертывания защищенной беспроводной сети с помощью PIN и на NBG-418N v2, и на беспроводном клиенте (в данном примере NWD210N).

Иллюстрация 34 Пример процесса WPS: вариант с PIN



5.4 Подключение к беспроводной сети NBG-418N v2 без использования WPS

В этом примере показано, как сконфигурировать безопасность беспроводной сети со следующими параметрами NBG-418N v2.

SSID	SSID_Example3

Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Выполните следующие операции для настройки параметров беспроводной сети на NBG-418N v2.

Сначала нужно подключить оборудование (см. Quick Start Guide) и зайти на Web Configurator через соединение LAN (см. Раздел 2.2 на стр. 18).

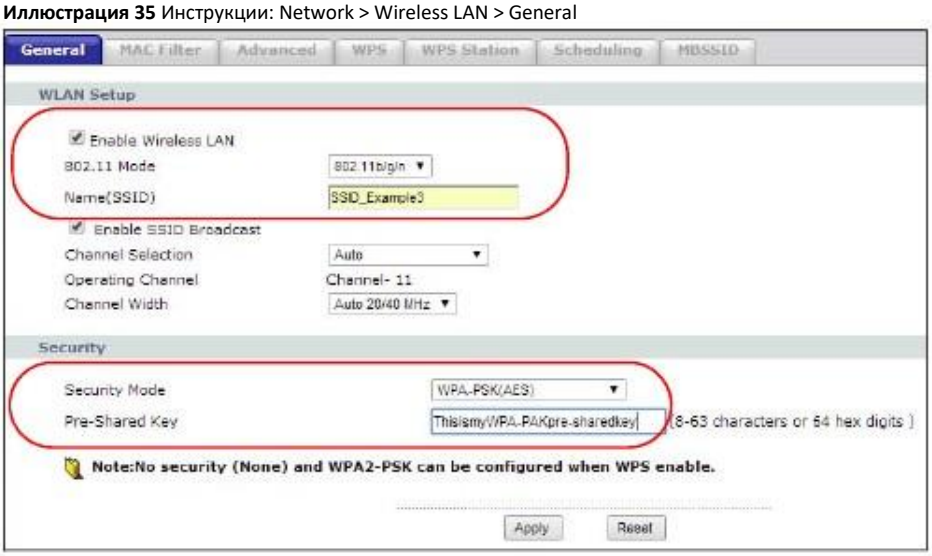
1 Перейдите на экран **Wireless LAN > General** в Web Configurator на NBG-418N v2.

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

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

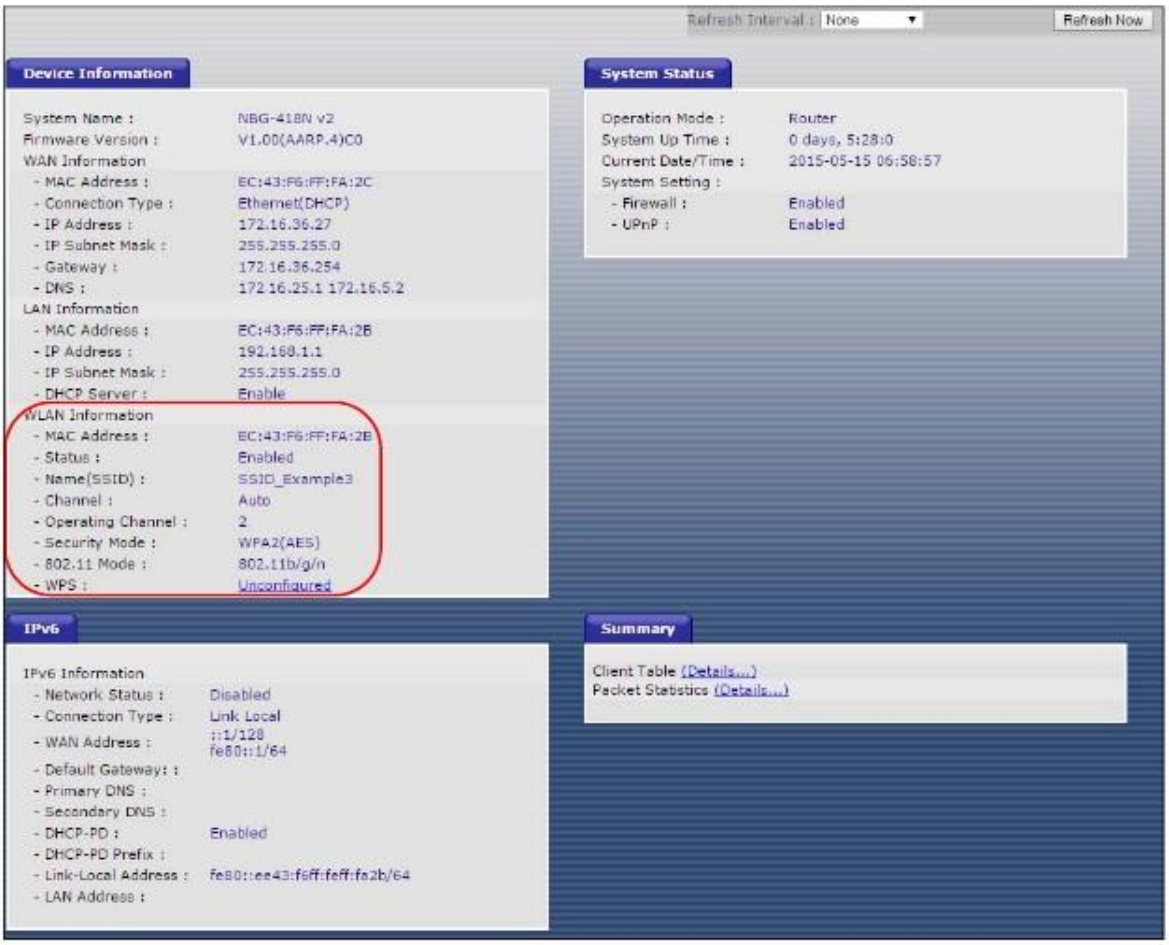
4 Настройте безопасность (Security) на **WPA-PSK/WPA2-PSK** и введите **ThisismyWPA-PSKpre-sharedkey** в поле **Pre-Shared Key**. Щелкните **Apply**.

Иллюстрация 35 Инструкции: Network > Wireless LAN > General



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

Иллюстрация 36 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.

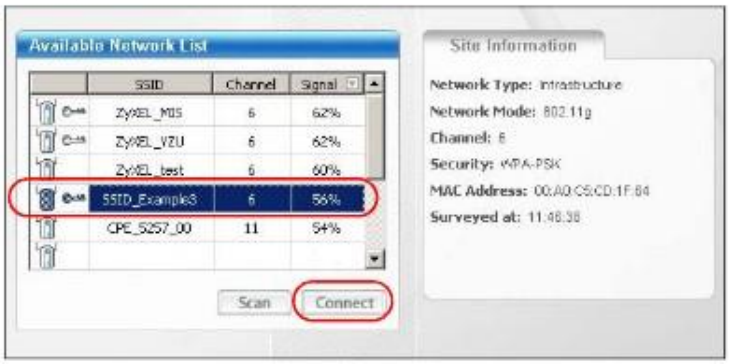
1 NBG-418N v2 поддерживает беспроводные клиенты IEEE 802.11b, IEEE 802.11g и IEEE 802.11n. Убедитесь, что ваш ноутбук или подключенный к нему адаптер WiFi поддерживает хотя бы один из этих стандартов.

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).

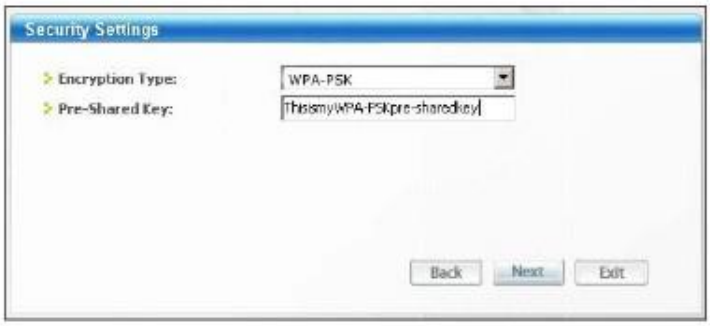
4 Выберите **SSID_Example3** и щелкните **Connect**.

Иллюстрация 37 Подключение беспроводного клиента к беспроводной сети



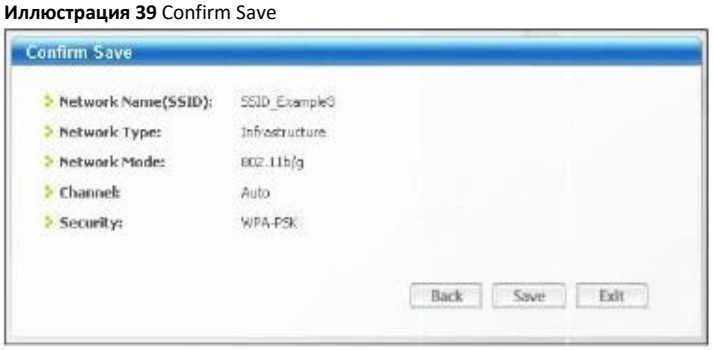
5 Выберите **WPA-PS**K и на следующем экране введите ключ безопасности. Щелкните **Next**.

Иллюстрация 38 Security Settings



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

Иллюстрация 39 Confirm Save



7 Проверьте состояние беспроводного подключения на следующем экране. Если беспроводному клиенту не удается подключиться к NBG-418N v2, то см. Главу Устранение неисправностей этого «Руководства пользователя».

Иллюстрация 40 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.

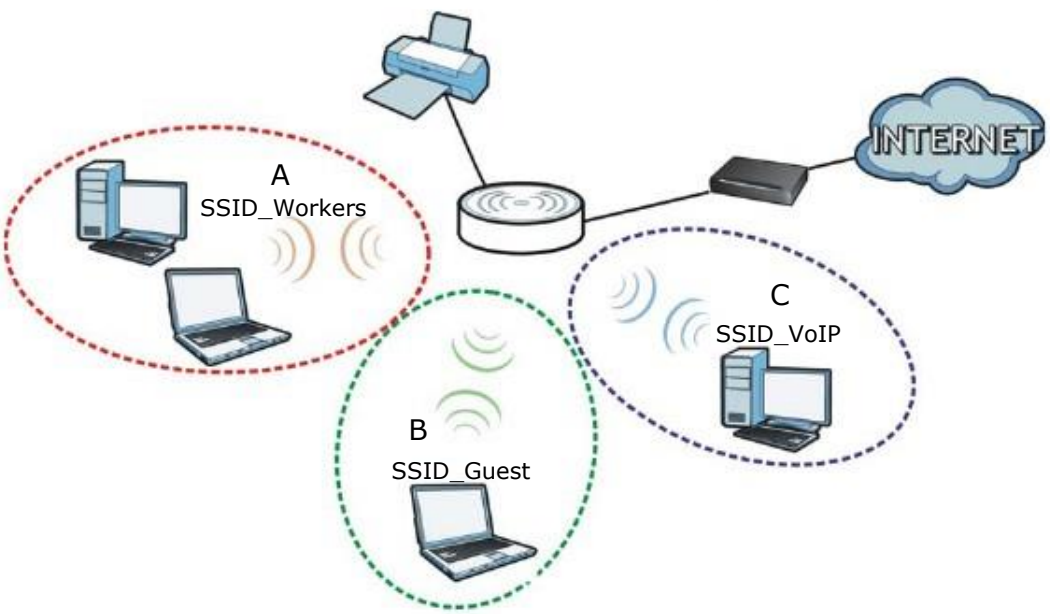
5.5 Использование нескольких SSID на NBG-418N v2

На NBG-418N v2 можно сконфигурировать несколько гостевых SSID (см. Раздел 6.10 на стр. 75).

Благодаря этой функции на базе NBG-418N v2 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 NBG-418N v2 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 NBG-418N v2 (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 NBG-418N v2 работает в режиме маршрутизатора.

В следующем примере показывается, как настроить SSID со следующими параметрами NBG-418N v2, который работает в режиме маршрутизатора.

SSID	ТИП БЕЗОПАСНОСТИ	КЛЮЧ
SSID_Workers	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork

SSID	ТИП БЕЗОПАСНОСТИ	КЛЮЧ
SSID_VoIP	WPA-PSK	VoIPOnly12345678
SSID_Guest	WPA-PSK	keyexample123

1 Подключите ваш компьютер к порту LAN на NBG-418N v2 кабелем Ethernet.

2 По умолчанию IP-адрес NBG-418N v2 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 D на стр. 190 где объясняется как изменить IP-адрес компьютера.

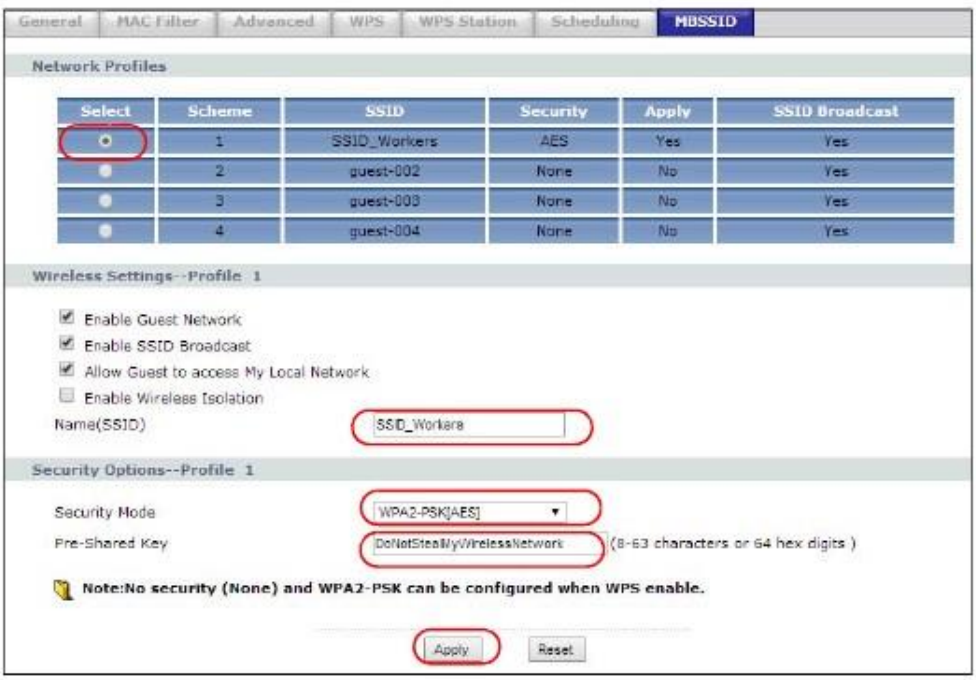
4 После того, как вы правильно настроили IP-адрес вашего компьютера откройте web-браузер (например, Internet Explorer) и в адресной строке введите “192.168.212.1”.

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**.

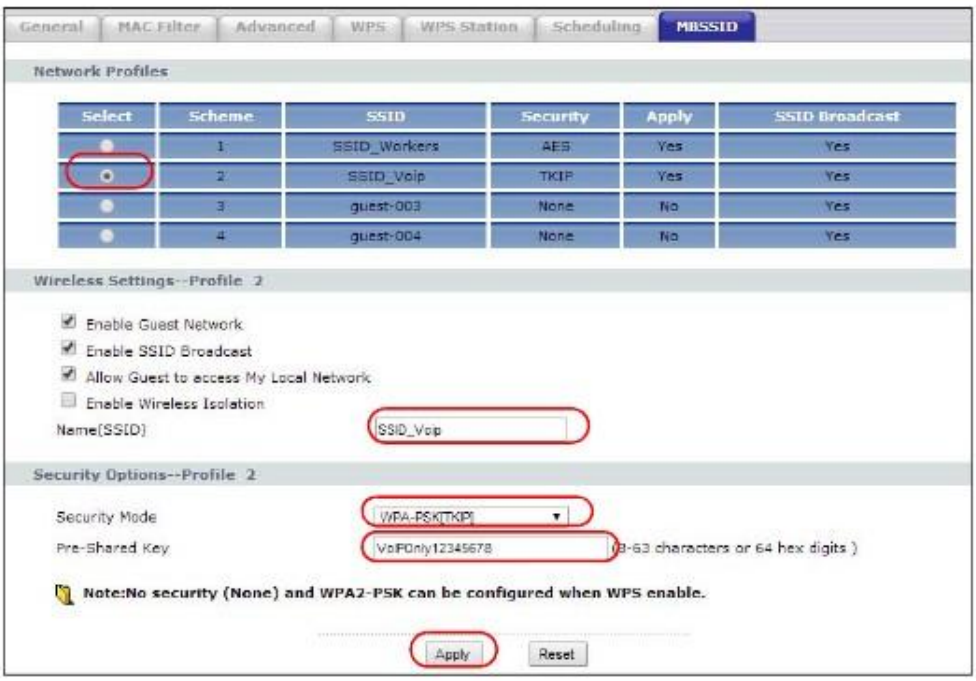
7 Откроется окно, в котором нужно выбрать режим Wizard либо Advance. Щелкните **Go to Advanced Setup** в панели навигации.

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

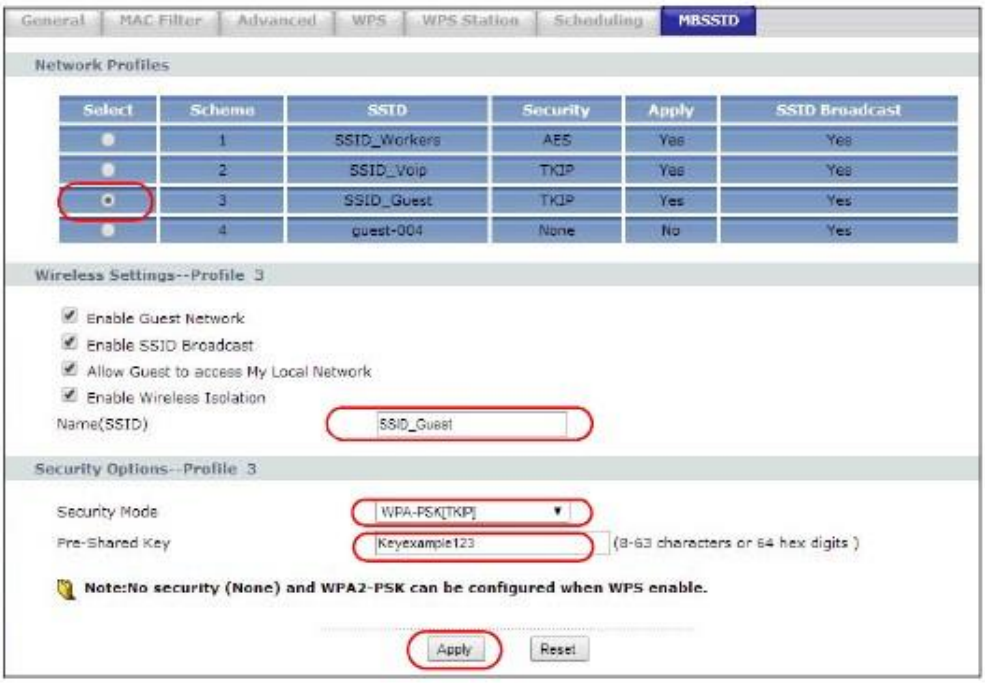


9 Перейдите **Network > Wireless LAN > WLAN Advanced Setup** и поставьте галочку в **Intra-BSS Traffic** чтобы находящиеся в одном беспроводной сети беспроводные клиенты могли обмениваться данными между собой. Щелкните **Apply**.

10 Для создания SSID_VoIP перейдите **Network > Wireless LAN > 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** > **MBSSID**. Выберите **scheme 3** 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

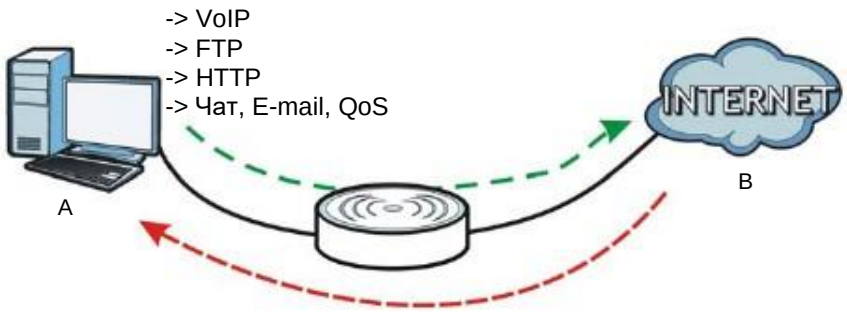
Инструкции по инсталляции Universal Plug and Play на компьютере Windows можно найти в Разделе 16.4 на стр. 129.

5.7 Управление полосой пропускания на NBG-418N v2

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 41 Пример управление полосой пропускания



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

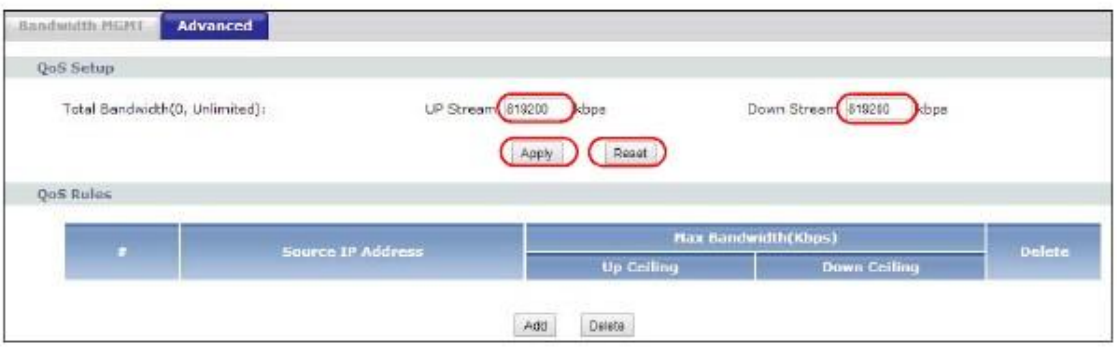
В этом примере Bandwidth Management используется на NBG-418N v2 со следующими параметрами (режим маршрутизатора).

Правило QoS

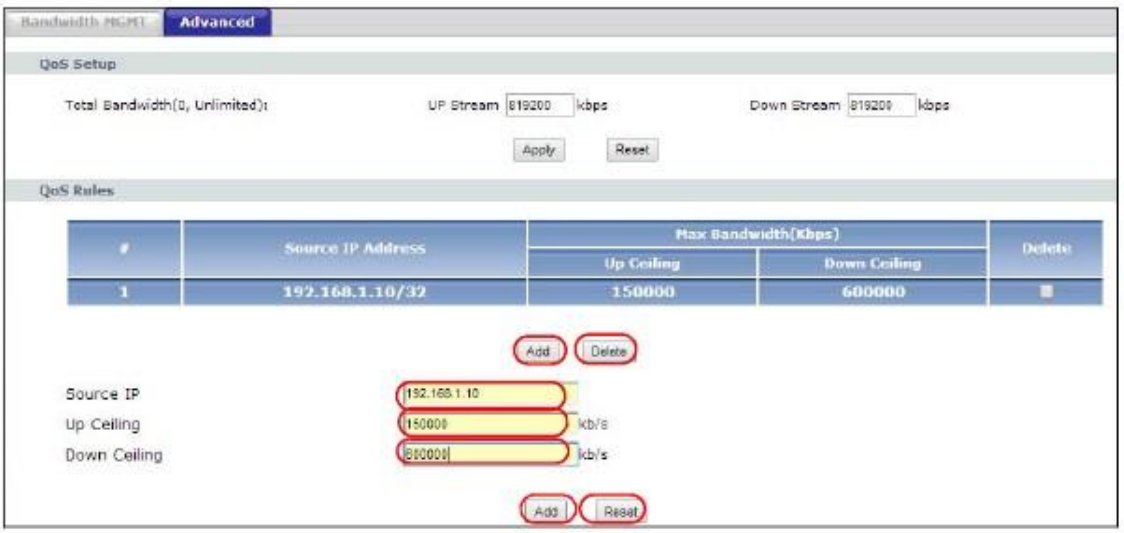
Up Stream	819200 kpbs
Down Stream	819200 kbps
Source IP	192.168.1.10
Up Ceiling	150000 kb/s
Down Ceiling	600000 kb/s

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 (в Source IP Adress этот 32-битный адрес, который назначает ваш провайдер, будет выводиться как 192.168.1.10/32), 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**.

Часть II

Техническая информация

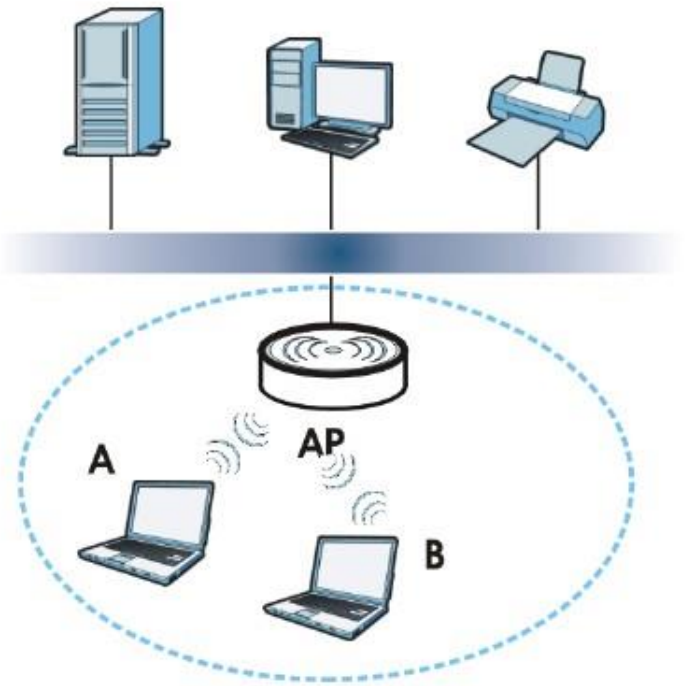
ГЛАВА 6 Беспроводная сеть

6.1 Обзор

В этой главе описана настройка параметров беспроводной сети NBG-418N v2. Подробнее о беспроводных сетях см. приложения.

На следующей иллюстрации показан пример беспроводной сети.

Иллюстрация 42 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. NBG-418N v2 в этом примере работает как точка доступа.

6.2 Экраны, которые описаны в этой главе

Экраны беспроводной сети зависят от режима работы устройства.

Экран беспроводной сети	Router	Access Point	Universal Repeater	Client Bridge
General	✔	✔	✔	
MAC Filter	✔	✔	✔	
Advanced	✔	✔	✔	✔
WPS	✔	✔	✔	
WPS Station	✔	✔	✔	
Scheduling	✔	✔	✔	
MBSSID	✔			
AP Select			✔	✔
WLAN Information				✔

О режимах работы устройства см. Глава 4 на стр. 30.

• Экран **General** для включения беспроводной сети, ввода SSID и выбора режима безопасности беспроводной сети (Раздел 6.4 на стр. 66).

• Экран **MAC Filter** для разрешения или блокировки подключения беспроводных клиентов к NBG-418N v2 на основе их MAC-адреса (Раздел 6.5 на стр. 71).

• Экран **Advanced** для разрешения intra-BSS networking и настройки порогового значения RTS/CTS Threshold (Раздел 6.6 на стр. 71).

• Экран **WPS** для быстрого развертывания беспроводной сети с надежной защитой без настройки вручную параметров безопасности (Раздел 6.7 на стр. 72).

• Экран **WPS Station** для добавления беспроводной станции с помощью WPS (Раздел 6.8 на стр. 73).

• Экран **Scheduling** для настройки расписания включения и отключения беспроводной сети (Раздел 6.9 на стр. 74).

• Экран **MBSSID** для настройки нескольких беспроводных сетей на NBG-418N v2 (Раздел 6.10 на стр. 75).

• Экран **AP Select** для выбора точки доступа, к которой NBG-418N v2 будет подключаться в режиме универсального повторителя. Для подключения вам нужно знать параметры безопасности этой точки доступа (Раздел 6.11 на стр. 76).

• Экран **WLAN Information** для просмотра SSID и информации о безопасности выбранной точки доступа (Раздел 6.12 на стр. 77).

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

Без использования средств безопасности посторонние лица, находящиеся в зоне покрытия беспроводной сети могут не только перехватывать передаваемые по ней данные, но и подключаться к самой сети, и в результате красть информацию и заражать сеть и подключенные к ней компьютеры вирусами и другим вредоносным программным обеспечением. Для защиты от этих рисков разработаны различные системы безопасности, которые гарантируют, что только авторизованные лица могут использовать беспроводную сеть и передавать/принимать по этой сети данные.

Системы безопасности обеспечивают аутентификацию пользователей для того, что доступ к сети получили только те пользователи, у которых есть правильные подтверждения прав доступа (обычно это имя пользователя и пароль либо кодовая фраза), и шифруют передаваемые через беспроводную сеть данные. Ключ для расшифровки данных, без которых их нельзя прочесть, предоставляется только аутентифицированным пользователям.

Существующие сегодня стандарты безопасности отличаются по эффективности. Некоторые используют шифрование, которое легко вскрыть, например, устаревший Wired Equivalent Protocol (WEP). Использование WEP лучше, чем работа без шифрования, но такое шифрование легко взламывается. Другие стандарты надежнее, но их шифрование можно взломать если они используются некорректно. Например, стандарт безопасности WPA-PSK работает надежно если использовать длинные пароли, которые трудно угадать (например, случайная комбинация из 20 букв и цифр), но если для шифрования используется короткий ключ (например, слово из словаря из трех букв), то такую защиту легко взломает хакер.

Ущерб от проникновения в сеть посторонних может оказаться очень большим, поэтому систему безопасности должны использовать не только пользователи, работающие с секретной информацией, но и все пользователи, имеющие доступ к беспроводной сети.

Рекомендуется в качестве ключей безопасности и паролей использовать слова и комбинации цифр, которые вы легко запомните и которые кроме вас мало кому известны, например, если у вашей мамы автомобиль 1970 Dodge Challenger и ее любимый фильм Vanishing Point (который, как вы хорошо помните, снят в 1971 году), то можно в качестве ключ безопасности использовать “70dodchal71vanpoi”.

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 NBG-418N v2 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 он 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 18 Типы шифрования и аутентификации

	БЕЗ АУТЕНТИФИКАЦИИ
Слабее	No Security
↕	Static WEP
	WPA-PSK
Сильнее	WPA2-PSK

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.

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 клиентское устройство A поддерживает **WEP**, а клиентское устройство B - **WEP** и **WPA2-PSK**, то выберите тип безопасности беспроводной сети **WEP**.

Примечание: В беспроводной сети рекомендуется использовать шифрование WPA2-PSK или более сильное. Шифрование IEEE 802.1x и WEP лучше, чем ничего, но при использовании этой защиты неавторизованный пользователь может относительно легко узнать исходную информацию.

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

6.3.5 WiFi Protected Setup (WPS)

NBG-418N v2 поддерживает технологию WiFi Protected Setup (WPS), упрощающую построение защищенной сети WiFi. 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. Каждое соединение WPS работает между двумя устройствами, поддерживающими WPS (об этом должна быть информация в документации к каждому из этих устройств).

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. Когда функция WPS активирована на одном устройстве, то в течение следующих 2 минут она ищет другое устройство с активированным WPS, после чего между устройствами автоматически устанавливается защищенное соединение. О настройке беспроводной сети с использованием WPS см. Раздел 5.3 на стр. 48.

6.4 Экран General

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

Примечание: Если вы настраиваете NBG-418N v2 с устройства, которое подключено к беспроводной сети, и вы изменили у NBG-418N v2 идентификатор SSID, настройки канала или безопасности, то беспроводное соединение с NBG-418N v2 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 NBG-418N v2.

Щелкните **Network > Wireless LAN** чтобы открыть экран **General**.

Иллюстрация 43 Network > Wireless LAN > General (режим маршрутизатора или точки доступа)

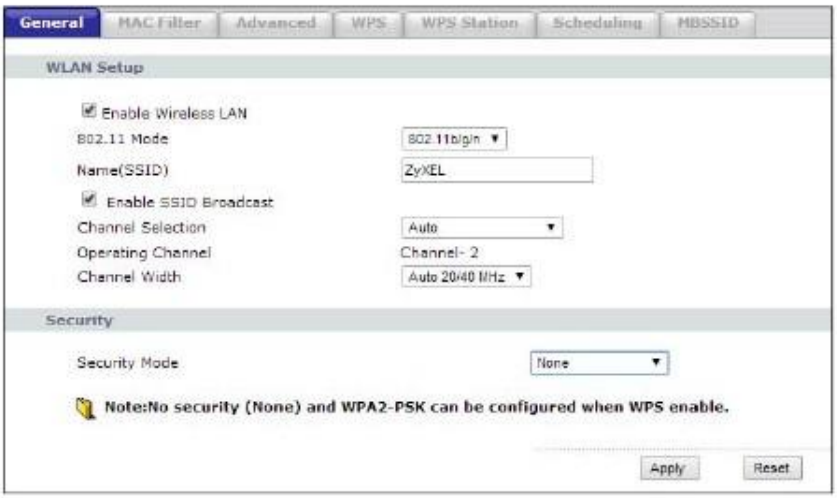


Иллюстрация 44 Network > Wireless LAN > General (режим универсального повторителя)

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

Таблица 19 Network > Wireless LAN > General

ПОЛЕ	ОПИСАНИЕ
WLAN STA Information	Это поле активно только в режиме универсального повторителя. В нем отображаются настройки беспроводной сети и безопасности выбранной точки доступа.
SSID	Имя SSID (Service Set Identity), идентифицирующее беспроводное устройство, к которому вы подсоединяетесь.
Security Mode	Тип безопасности, используемый в беспроводном устройстве, к которому вы подключаетесь.
Operating Channel	Канал, который сейчас использует беспроводное устройство, к которому вы подсоединяетесь.
WLAN AP Information / Wireless Setup	Этот раздел для настройки параметров соединения между NBG-418N v2 и беспроводным клиентом.
Enable Wireless LAN	Поставьте галочку в это поле для активизации беспроводной сети.
802.11 Mode	Выберите режим 802.11 из раскрывающегося списка.

Таблица 19 Network > Wireless LAN > General (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name (SSID)	Имя SSID (Service Set Identity), идентифицирующее набор сервисов Service Set, которые доступны для беспроводной станции. Связанные с точкой доступа (AP) беспроводные станции должны иметь тот же SSID. Введите имя беспроводной сети, которое может состоять 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.
Channel Selection	Выберите рабочую частоту/канал из раскрывающегося списка. Эта опция зависит от частотного диапазона страны, в которой вы находитесь. Подробнее о каналах см. главу Визард соединения. Эта опция доступна только если отключена функция Auto Channel Selection.
Operating Channel	Канал, который сейчас использует NBG-418N v2.
Channel Width	Выбор ширины канала, который будет использовать NBG-418N v2 - **20MHz**, **40MHz** или **Auto 20/40MHz**. 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. Так как не все устройство могут использовать каналы 40MHz, то нужно выбрать **Auto 20/40MHz** чтобы NBG-418N v2 автоматически подстраивал ширину канала.
Security	Настройка параметров соединения NBG-418N v2 с беспроводными клиентами.
Security Mode	Выберите **WEP, WPA-PSK(TKIP), WPA-PSK(AES), WPA2-PSK(TKIP), WPA2-PSK(AES)** или **WPA-PSK/WPA2-PSK AES** чтобы использовать систему безопасности в вашей беспроводной сети. У беспроводных клиентов, которые нужно подключать к сети, должны быть такие же настройки безопасности. После выбора типа безопасности на этом экране появятся дополнительные опции (см. разделы 6.4.2 и 6.4.3). Если выбрать **None**, то любой клиент сможет подключиться к вашей сети без аутентификации.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

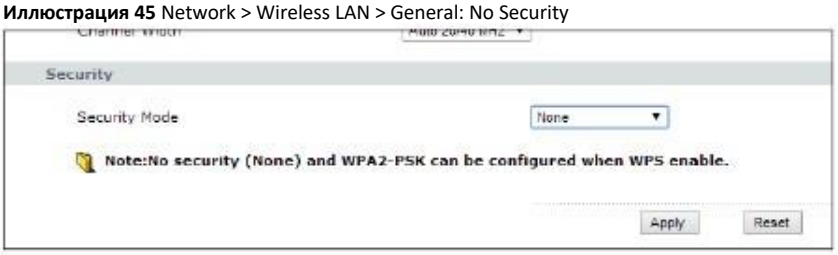
Другие поля этого экрана описаны далее в этой главе.

6.4.1 No Security

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

Примечание: Если на вашем NBG-418N v2 не включена система безопасности, то к вашей сети сможет подключиться любой беспроводной клиент в зоне покрытия NBG-418N v2.

Иллюстрация 45 Network > Wireless LAN > General: No Security



В следующей таблице описаны поля этого экрана.

Таблица 20 Network > Wireless LAN > General: No Security

ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **None** из раскрывающегося списка.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

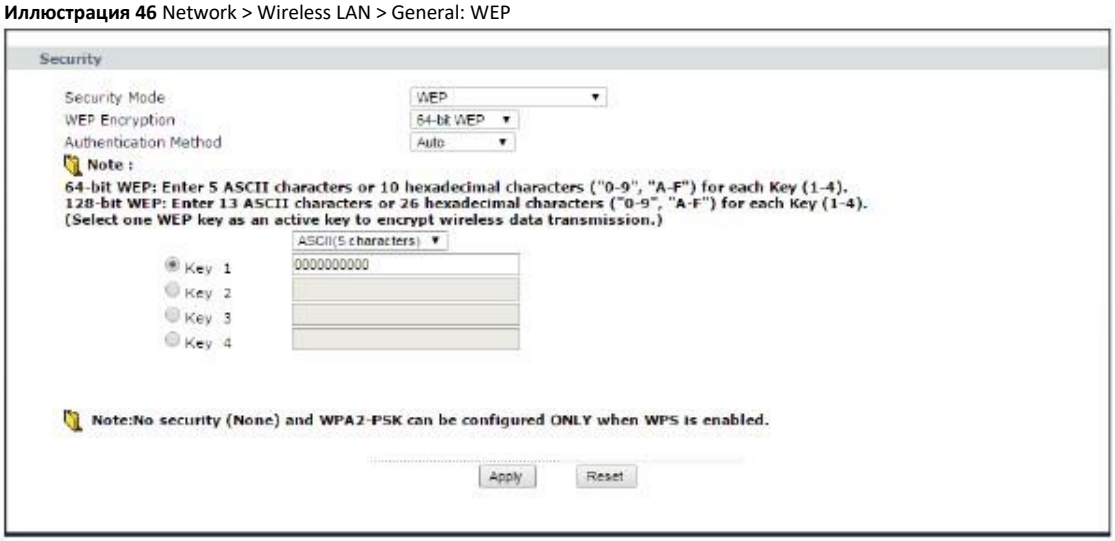
6.4.2 Шифрование WEP

WEP шифрует данные, которые передаются между точкой доступа и беспроводными станциями для защиты соединения от неавторизованного доступа. Эта тип шифрования защищает как трафик как unicast, так и multicast. Точка доступа и беспроводные станции должны иметь один и тот же ключ WEP key.

Для NBG-418N v2 можно настроить до четырех 64-битных или 128-битных ключей WEP, но нельзя одновременно использовать несколько ключей.

Для настройки и включения шифрования WEP щелкните **Network > Wireless LAN** для перехода к экрану General и затем на этом экране в списке **Security Mode** выберите **WEP**.

Иллюстрация 46 Network > Wireless LAN > General: WEP



В следующей таблице описаны поля безопасности беспроводной сети этого экрана.

Таблица 21 Network > Wireless LAN > General: WEP

ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **WEP** из раскрывающегося списка.
WEP Encryption	Выберите **64-bit WEP** или **128-bit WEP** для включения шифрования данных.
Authentication Method	Выберите **Auto** или **Shared Key** из раскрывающегося списка. Это поле определяет, должен ли беспроводной клиента предоставлять ключ WEP чтобы подключиться к точке доступа. В этом поле нужно оставить **Auto** если только вы не хотите использовать принудительную верификацию ключа перед началом сеанса связи между беспроводным клиентом и NBG-418N v2. В этом случае выберите **Shared Key**.
ASCII	Выберите эту опцию чтобы использовать в ключе WEP символы ASCII.
Hex	Выберите эту опцию чтобы использовать в ключе WEP шестнадцатеричные символы.

Таблица 21 Network > Wireless LAN > General: WEP (продолжение)

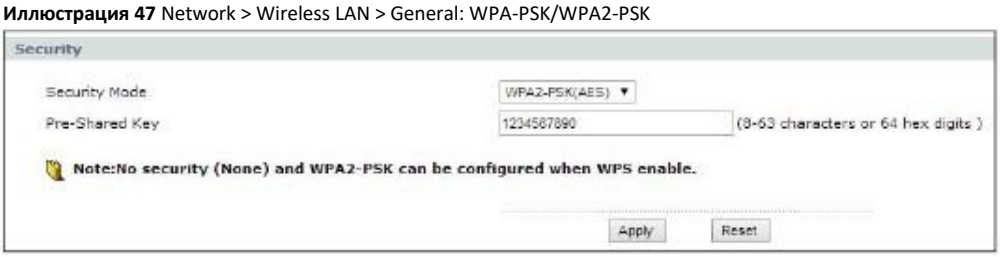
ПОЛЕ	ОПИСАНИЕ
Key 1 to Key 4	Ключи WEP используются для шифрования данных. Для обмена зашифрованными данными на NBG-418N v2и беспроводных станциях должен использоваться одинаковый ключ WEP. Если выбрать **64-bit WEP**, то нужно ввести любые 5 символов ASCII или 10 шестнадцатеричных символов ("0-9", "A-F"). Если выбрать **13-bit WEP**, то нужно ввести любые 13 символов ASCII или 26 шестнадцатеричных символов ("0-9", "A-F"). Нужно сконфигурировать хотя бы один ключ либо несколько ключей, однако одновременно нельзя использовать несколько ключей. Ключ по умолчанию 1.
Apply	Щелкните **Apply** чтобы сохранить изменения на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.4.3 WPA-PSK/WPA2-PSK

Режим безопасности WPA-PSK обеспечивает более надежное шифрование и аутентификацию пользователей, чем WEP. При использовании ключа Pre-Shared Key (PSK), как NBG-418N v2, так и подключающийся клиент используют общий пароль для проверки соединения. Хотя это надежное шифрование, но не такое надежное, как WPA, WPA2 и даже WPA2-PSK. WPA2-PSK – это новый усовершенствованный вариант стандарта шифрования WPA. Он немного улучшает безопасность, хотя из-за использования PSK она не такая высокая, какой могла бы быть.

Щелкните **Network > Wireless LAN** для перехода к экрану General и затем на этом экране в списке **Security Mode** выберите **WPA-PSK** или **WPA2-PSK**.

Иллюстрация 47 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



В следующей таблице описаны поля этого экрана.

Таблица 22 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

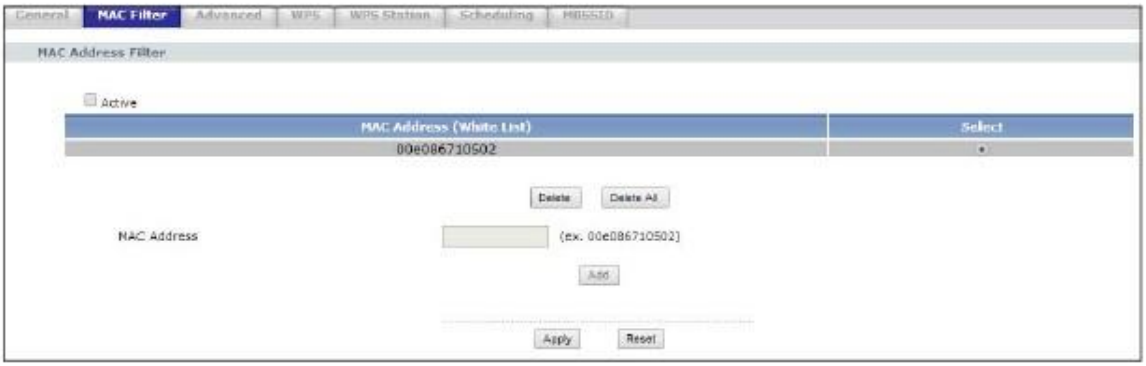
ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **WPA-PSK** или **WPA2-PSK** из раскрывающегося списка. Выберите **WPA-PSK/WPA2-PSK AES** чтобы с NBG-418N v2 могли обмениваться данные беспроводные клиенты как WPA2, так и WPA даже если NBG-418N v2 использует WPA2-PSK.
Pre-Shared Key	**WPA-PSK/WPA2-PSK** использует для аутентификации простой обычный пароль Введите ключ pre-shared key, который может состоять из 8 - 63 символов ASCII (включая пробелы и символы) или 64 шестнадцатеричных символа (“0-9,” “A-F”).
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.5 MAC Filter

Экран **MAC filter** позволяет разрешать доступ к NBG-418N v2 определенным устройствам (**Allow**) либо блокировать их доступ к NBG-418N v2 (**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 NBG-418N v2 щелкните **Network > Wireless LAN > MAC Filter**. Откроется следующий экран.

Иллюстрация 48 Network > Wireless LAN > MAC Filter



В следующей таблице описаны поля этого экрана.

Таблица 23 Network > Wireless LAN > MAC Filter

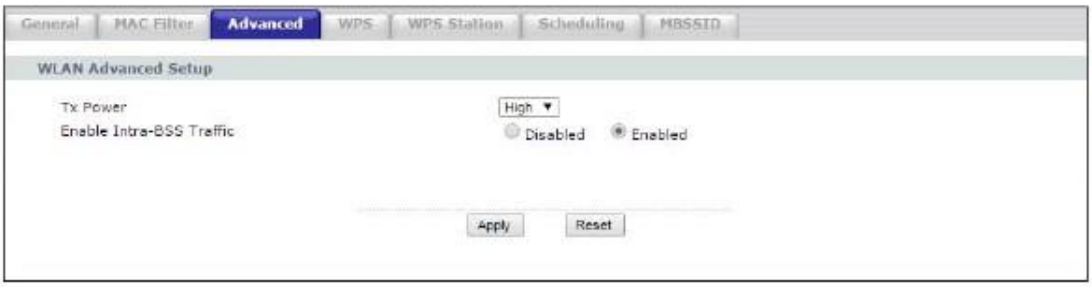
ПОЛЕ	ОПИСАНИЕ
Active	Для включения фильтра MAC-адресов нужно поставить галочку напротив **Active**.
MAC Address (White List)	В этом поле нужно ввести MAC-адреса беспроводных станций, который разрешен доступ к NBG-418N v2. Введите MAC-адрес для внесения в белый и черный список в стандартном формате (шесть пар шестнадцатеричных цифр, например, 12:34:56:78:9a:8c).
Select	Выберите **Select** чтобы выбрать запись в списке MAC-адресов фильтра.
Delete	Щелкните кнопку **Delete** чтобы удалить выбранную запись из списка MAC-адресов фильтра.
Delete All	Щелкните кнопку **Delete All** чтобы удалить все записи из списка MAC-адресов фильтра.
MAC Address	В этом поле нужно ввести MAC-адреса беспроводных станций, который разрешен или запрещен доступ к NBG-418N v2. Введите MAC-адрес для внесения в белый и черный список в стандартном формате (шесть пар шестнадцатеричных цифр, например, 12:34:56:78:9a:8c).
Add	Щелкните **Add** для добавления нового MAC-адреса в правило MAC Filtering rule.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
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 > Advanced**. Откроется следующий экран.

Иллюстрация 49 Network > Wireless LAN > Advanced



В следующей таблице описаны поля этого экрана.

Таблица 24 Network > Wireless LAN > Advanced

ПОЛЕ	ОПИСАНИЕ
Wireless Advanced Setup	
Tx Power	Мощность сигнала на выходе NBG-418N v2. Если рядом с NBG-418N v2 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.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.7 Экран WPS

С помощью WiFi Protected Setup (WPS) можно быстро развернуть защищенную сеть без ручной настройки параметров безопасности. Соединить с помощью WPS оба устройство можно только если оба они поддерживают WPS.

Примечание: NBG-418N v2 применяет настройки безопасности профиля SSID1. Для использования WPS режим безопасности (security mode) в SSID1 должен быть **WPA2-PSK** либо **No Security**.

Примечание: Если функция WPS включена, то UPnP включается автоматически.

Примечание: WPS не работает если выключена беспроводная сеть.

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 > WPS**.

Иллюстрация 50 Network > Wireless LAN > WPS

В следующей таблице описаны поля этого экрана.

Таблица 25 Network > Wireless LAN > 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	
Status	В этом поле стоит **Configured** если NBG-418N v2 подключена к беспроводной сети с помощью WPS либо если выбран **Enable WPS** 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 NBG-418N v2 либо вы щелкнули **Release_Configuration** чтобы удалить все настройки для беспроводной сети и безопасности беспроводной сети.
Release Configuration	Эта кнопка работает только когда в поле WPS status стоит **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG-418N v2.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Refresh	Щелкните **Refresh** чтобы обновить информацию на этом экране.

6.8 Экран WPS Station

Этот экран предназначен для добавления беспроводной станции с помощью WPS. Для перехода к этому экрану щелкните **Network > Wireless LAN> WPS Station**.

Примечание: После нажатия Push Button на этом экран нужно в течение двух 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 двух минут.

Иллюстрация 51 Network > Wireless LAN > WPS Station

В следующей таблице описаны поля этого экрана.

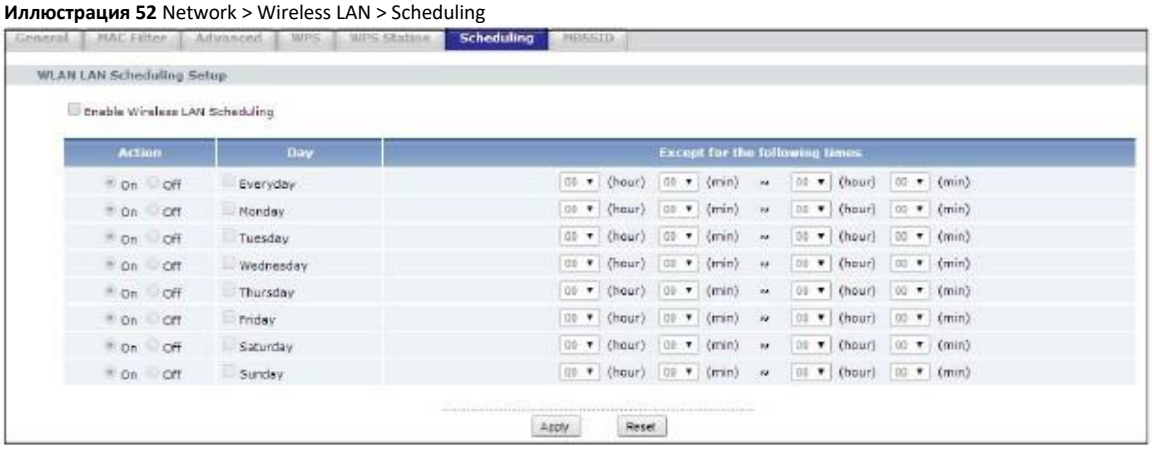
Таблица 26 Network > Wireless LAN > WPS Station

ПОЛЕ	ОПИСАНИЕ
Push Button	Эта кнопка предназначена только для настройки параметров беспроводной сети беспроводной станции с помощью PBC (Push Button Configuration). См. Раздел 5.3.1 на стр. 49. Щелкните эту кнопку чтобы поддерживающий WPS беспроводная станция начала сканирование и синхронизацию параметров безопасности беспроводной сети.
Or input station's PIN number	Используйте эту кнопку если вы настраиваете параметры беспроводной сети на беспроводной станции с помощью метода PIN Configuration. См. Раздел 5.3.2 на стр. 50. Введите PIN-код, который сгенерировала утилита беспроводной станции, затем щелкните **Start** чтобы она подключилась с NBG-418N v2 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 > Scheduling**.

Иллюстрация 52 Network > Wireless LAN > Scheduling



В следующей таблице описаны поля этого экрана.

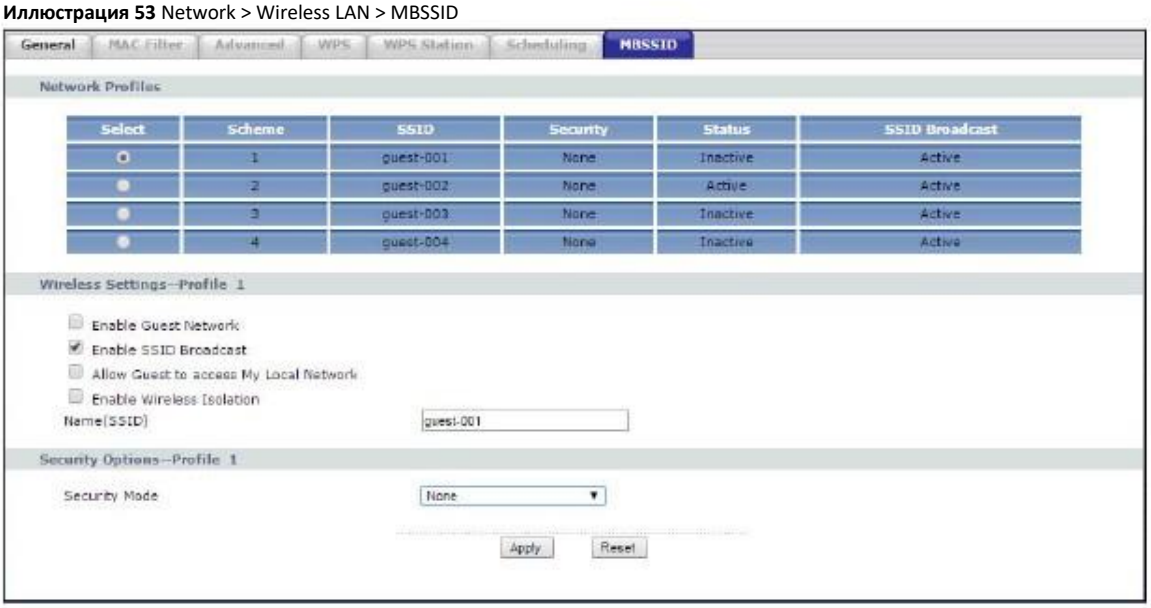
Таблица 27 Network > Wireless LAN > Scheduling

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN Scheduling	Поставьте галочку чтобы включить функцию Wireless LAN scheduling.
Action	Выберите **On** или **Off** чтобы беспроводная сеть включалась или отключалась по расписанию. Это поле работает вместе с полями **Day** и **Except for the following times**.
Day	Выберите **Everyday** (все дни недели) либо определенные дни недели, в которые нужно включать или отключать беспроводную сеть. Это поле работает вместе с полем **Except for the following times**.
	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 вы задали более раннее время включения **On** в WLAN Status, то беспроводная сеть будет выключена в период времени, который задан в двух параметрах Except for the following times. Если вы задали более раннее время включения **Off** в WLAN Status, то беспроводная сеть будет включена в период времени, который задан в двух параметрах Except for the following times.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.10 Экран MBSSID

Этот экран используется для включения на функции Multiple SSID (MBSSID) на NBG-418N v2 и ее настройки. Можно назначить разные типы безопасности разным SSID. Беспроводные клиенты могут подключаться к NBG-418N v2 по разным SSID. Для перехода на следующий экран щелкните **Network > Wireless LAN > MBSSID**.

Иллюстрация 53 Network > Wireless LAN > MBSSID



В следующей таблице описаны поля этого экрана.

Таблица 28 Network > Wireless LAN > MBSSID

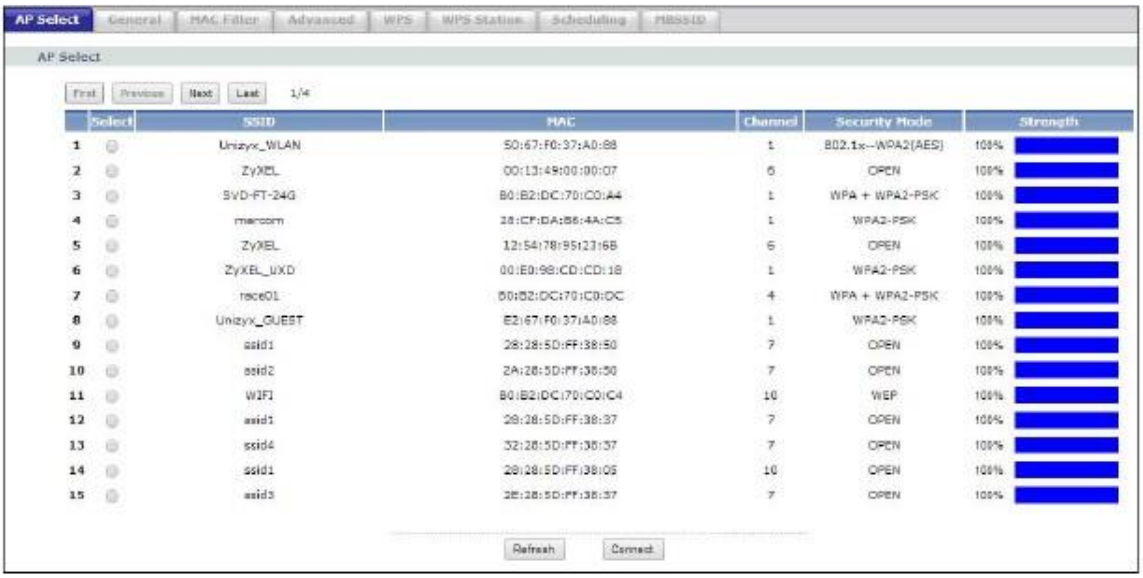
ПОЛЕ	ОПИСАНИЕ
Network Profiles	
Select	Выбор идентификатора Multiple Basic Service Set Identifier (MBSSID) для редактирования.
Scheme	Номер по порядку SSID.
SSID	Имя SSID беспроводного клиента.
Security	Режим безопасности беспроводного клиента. Если безопасность не используется, то в этом поле стоит **None**.
Status	Это поле показывает, можно ли использовать опцию **Enable Guest Network** для SSID.
SSID Broadcast	Это поле показывает, можно ли использовать опцию **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 NBG-418N v2 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 NBG-418N v2.
Name (SSID)	Имя выбранного SSID.
Security Options--Profile1	
Security Mode	Выберите **WEP** или **WPA-PSK(TKIP)**, **WPA2-PSK(AES)** или **WPA-PSK/WPA2-PSK AES** 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 NBG-418N v2. После выбора этой опции на экране будут доступны дополнительные опции. Если выбрать **None**, то любой клиент сможет подключаться к беспроводной сети без шифрования или аутентификации. Подробнее см. Раздел 6.4 на стр. 66.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для загрузки предыдущей конфигурации этого экрана.

6.11 Экран AP Select

На этом экране можно выбрать точку доступа, к которой подключается NBG-418N v2 в режиме универсального повторителя. Для подключения к точке доступа нужно знать ее параметры безопасности.

Для перехода к этому экрану щелкните **Network > Wireless LAN > AP Select**.

Иллюстрация 54 Network > Wireless LAN > AP Select



В следующей таблице описаны поля этого экрана.

Таблица 29 Network > Wireless LAN > AP Select

ПОЛЕ	ОПИСАНИЕ
AP Select	
First	Щелкните кнопку **First** button чтобы перейти на первую страницу таблицы AP select.
Previous	Щелкните кнопку **Previous** чтобы перейти на предыдущую страницу таблицы AP select.
Next	Щелкните кнопку **Next** чтобы перейти на следующую страницу таблицы AP select.
Last	Щелкните кнопку **Last** чтобы перейти на последнюю страницу таблицы AP select.
Select	Выберите беспроводное устройство, к которому вы хотите подключиться.
SSID	Идентификатор SSID (Service Set Identity) беспроводного устройства SSID – это уникальное имя беспроводной сети. У всех устройство одной беспроводной сети должен быть один и тот же идентификатор SSID.
MAC	MAC-адрес беспроводного устройства.
Channel	Номер канала, который использует беспроводное устройство.
Mode	Стандарты беспроводных сетей IEEE 802.11b/g/n, которые поддерживает беспроводное устройство.
Security Mode	Тип безопасности, который использует беспроводное устройство. Если в этом поле стоит **OPEN**, то это означает, что безопасность беспроводной сети не используется и к ней можно подключиться без пароля.
Strength	Мощность сигнала беспроводной сети. Она зависит в основном от мощности передатчика и расстояния от NBG-418N v2 до беспроводного устройства.
Refresh	Щелкните эту кнопку чтобы повторить поиск доступных беспроводных устройств в зоне покрытия и обновить эту таблицу.
Connect	Щелкните эту кнопку чтобы подключить выбранное беспроводное устройство device.

6.12 Экран WLAN Information

Этот экрана используется для просмотра SSID и безопасности выбранных беспроводных сетей когда NBG-418N v2 работает в режиме клиента. Для перехода к этому экрану щелкните **Network > AP Select > WLAN Info**.

Иллюстрация 55 Network > AP Select > WLAN Information

В следующей таблице описаны поля этого экрана.

Таблица 30 Network > AP Select > WLAN Information

ПОЛЕ	ОПИСАНИЕ
SSID	Service Set IDentity точки доступа, к которой подключается NBG-418N v2.
Security Mode	Тип безопасности, используемый точкой доступа, к которой подключается NBG-418N v2.

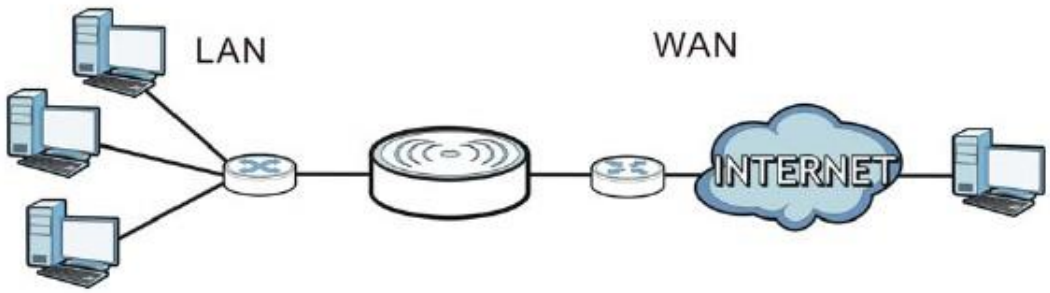
ГЛАВА 7
WAN

7.1 Обзор

В этой главе описываются экраны **WAN**, которые используются для настройки доступа NBG-418N v2 к Интернету.

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 56 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 NBG-418N v2.

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 NBG-418N v2, по которому к нему можно обращаться из внешней сети. NBG-418N v2 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 NBG-418N v2 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.

NBG-418N v2 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 NBG-418N v2), 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 того компьютера в вашей LAN, чей MAC-адрес вы клонируете. После завершения настройки адрес будет скопирован в конфигурационный файл. Рекомендуем клонировать MAC-адрес до подключения порта WAN.

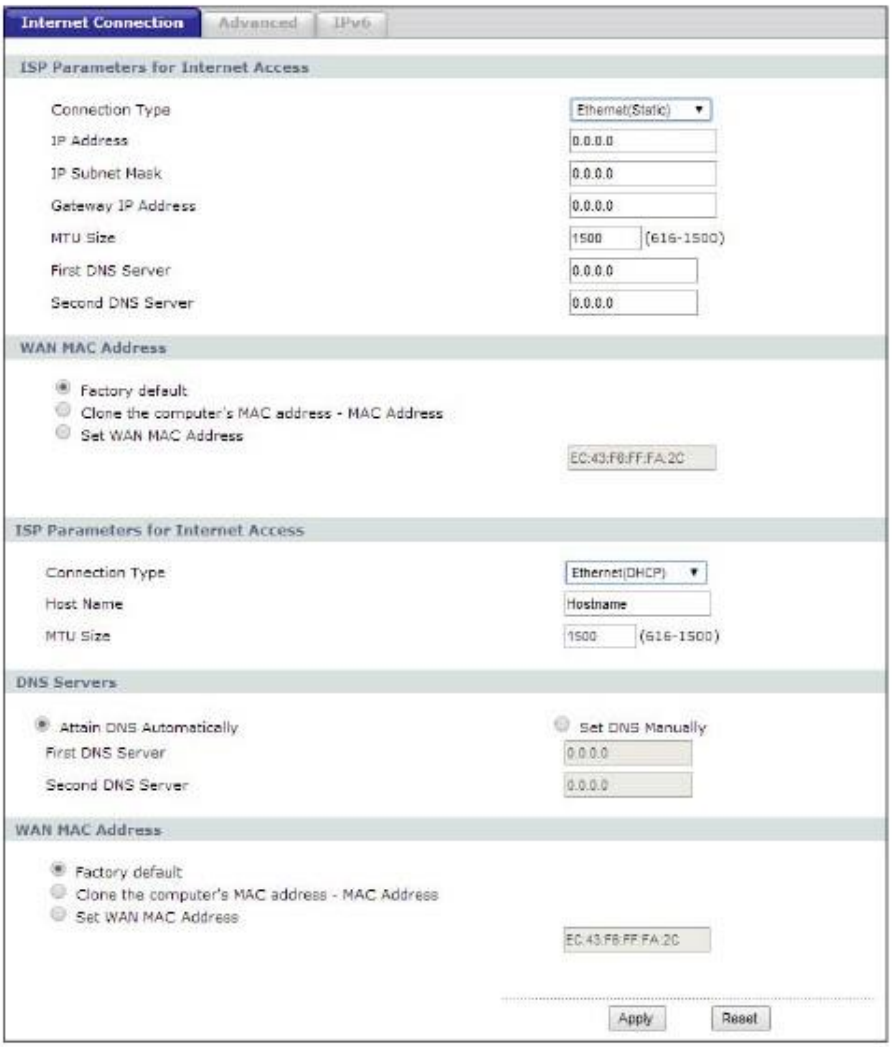
7.3 Экран Internet Connection

С помощью этого экрана можно изменить настройки доступа к Интернету вашего NBG-418N v2. Щелкните **Network > WAN**. Поля экрана зависят от выбранного типа соединения.

7.3.1 Экран Ethernet Encapsulation

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

Иллюстрация 57 Network > WAN > Internet Connection: Ethernet Encapsulation



В следующей таблице описаны поля этого экрана.

Таблица 31 Network > WAN > Internet Connection: Ethernet Encapsulation

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access (Ethernet Static)	
Connection Type	Выберите опцию **Ethernet (Static)** если порт WAN используется как обычный порт Ethernet.
IP Address	Введите в это поле **IP-адрес** WAN.
IP Subnet Mask	Введите в это поле **маску подсети IP**.
Gateway IP Address	Введите в это поле **IP-адрес шлюза** (если ваш провайдер предоставил вам эту информацию.
MTU Size	Максимальный размер пакета MTU (Maximum Transmission Unit), которые могут передаваться через этот интерфейс. Пакеты больше этого размера NBG-418N v2 будет разбивать на несколько пакетов. Допустимые значения - от 576 до 1500, по умолчанию 1500.
First DNS Server Second DNS Server	Введите в это поле IP-адреса первого и второго DNS-сервера.

Таблица 31 Network > WAN > Internet Connection: Ethernet Encapsulation (продолжение)

ПОЛЕ	ОПИСАНИЕ
WAN MAC Address В разделе MAC можно задать MAC-адрес порта WAN. Можно использовать MAC-адрес NBG-418N v2, копируя MAC-адрес компьютера в вашей локальной сети либо вручную ввести 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 того 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.
ISP Parameters for Internet Access (Ethernet DHCP)	
Connection Type	Выберите опцию **Ethernet (DHCP)** если порт WAN используется для обычного соединения Ethernet.
Host Name	Введите имя домена, который соответствует этому соединению Ethernet.
MTU Size	Максимальный размер пакета MTU (Maximum Transmission Unit), которые могут передаваться через этот интерфейс. Пакеты больше этого размера NBG-418N v2 будет разбивать на несколько пакетов. Допустимые значения - от 576 до 1500, по умолчанию 1500.
DNS Services	
Attain DNS Automatically	Щелкните **Reset** для настройки этого экрана с самого начала. Щёлкните кнопку **Attain DNS Automatically** если провайдер динамически назначает вам IP-адрес DNS-сервера (и IP-адрес WAN для NBG-418N v2). В нередактируемом поле справа отображается назначенный провайдером IP-адрес DNS-сервера.
Set DNS Manually	Выберите **Set DNS Manually** если вы знаете IP-адрес DNS-сервера. Нужно ввести IP-адреса первого и второго сервера DNS внизу экрана.
First DNS Server Second DNS Server	Введите IP-адреса первого и второго сервера DNS в эти поля экрана.
WAN MAC Address В разделе MAC можно задать MAC-адрес порта WAN. Можно использовать MAC-адрес NBG-418N v2, копируя MAC-адрес компьютера в вашей локальной сети либо вручную ввести MAC-адрес.	
Factory default	Select this option to use the factory assigned default MAC address.
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 NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.3.2 Экран PPPoE Encapsulation

NBG-418N v2 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).

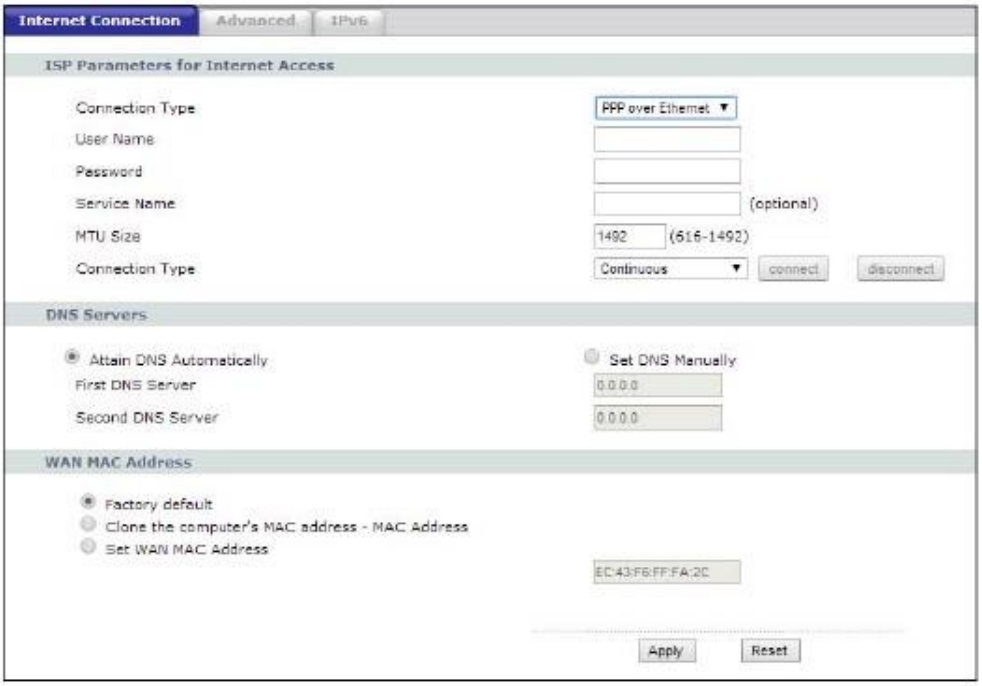
Одним из преимуществ PPPoE является предоставление конечным пользователям доступа к несколькими сетевым сервисам (так называемый dynamic service selection). Благодаря этой функции провайдер может легко создать новые IP-сервисы и предложить их определенным пользователям.

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 NBG-418N v2, 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 58 Network > WAN > Internet Connection: PPPoE Encapsulation



В следующей таблице описаны поля этого экрана.

Таблица 32 Network > WAN > Internet Connection: PPPoE Encapsulation

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	Имя сервиса PPPoE, которое должен сообщить вам провайдер. Это имя нужно PPPoE для доступа к серверу PPPoE.
Idle Timeout	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 NBG-418N v2 может получать и обрабатывать.

Таблица 32 Network > WAN > Internet Connection: PPPoE Encapsulation (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connection Type	Выберите **Continuous** если не надо отключать соединение по таймеру. Выберите **Connection on Demand** если нужно, чтобы маршрутизатор автоматически отключался от сервера PPPoE через определенное время (время отключения в минутах нужно ввести в поле **Idle Timeout**). Выберите **Manual** если нужно устанавливать соединение вручную.
Connect/ Disconnect	Щелкните кнопку **Connect** чтобы установить соединение с заданными выше параметрами либо **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 IP-адрес WAN для NBG-418N v2) 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 NBG-418N v2, копируя MAC-адрес компьютера в вашей локальной сети либо вручную ввести MAC-адрес.	
Factory default	Выберите эту опцию чтобы использовать 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 NBG-418N v2 (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 NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

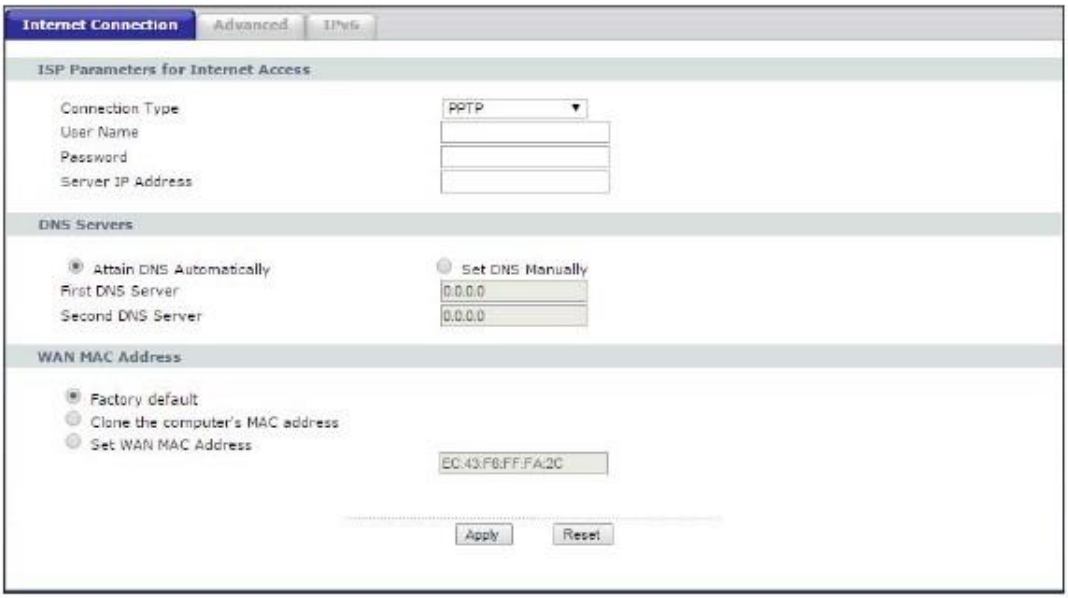
7.3.3 Экран PPTP Encapsulation

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 59 Network > WAN > Internet Connection: PPTP Encapsulation



В следующей таблице описаны поля этого экрана.

Таблица 33 Network > WAN > Internet Connection: PPTP Encapsulation

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.
User Name	Введите имя пользователя, которое вам назначил провайдер.
Password	Пароль пользователя, который указан в поле User Name.
Server IP Address	IP-адрес сервера PPTP server.
DNS Servers	
Attain DNS Automatically/ Set DNS Manually	Щелкните **Attain DNS Automatically** если провайдер динамически назначает вам IP-адрес DNS-сервера (и IP-адрес WAN для NBG-418N v2) 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 NBG-418N v2, копируя MAC-адрес компьютера в вашей локальной сети либо вручную ввести 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 NBG-418N v2 (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

Таблица 33 Network > WAN > Internet Connection: PPTP Encapsulation (продолжение)

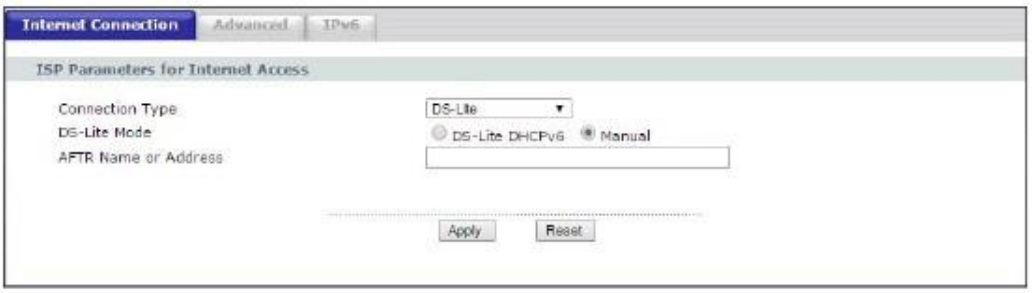
ПОЛЕ	ОПИСАНИЕ
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.3.4 Экран DS-Lite

Функция Dual Stack Lite (DS-Lite) применяется если компьютеры в локальной сети используют IPv4, а сервис-провайдер - IPv6. NBG-418N v2 по туннелю передает пакеты IPv4, инкапсулированные внутри пакетов IPv6, маршрутизатору Address Family Transition Router (AFTR) провайдера для соединения с Интернетом IPv4. Локальная сеть также может использовать сервисы IPV6. NBG-418N v2 использует свой сконфигурированный IPv6 WAN IP для пересылки трафика IPv6 в Интернет IPv6.

Этот экран выводится при выборе **DS-Lite** в опции **Connection Type**.

Иллюстрация 60 Network > WAN > Internet Connection: DS-Lite



В следующей таблице описаны поля этого экрана.

Таблица 34 Network > WAN > Internet Connection: DS-Lite

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access	
Connection Type	Выберите **DS-Lite** чтобы по туннелю передавать пакеты IPv4, инкапсулированные внутри пакетов IPv6, маршрутизатору Address Family Transition Router (AFTR) провайдера для соединения с Интернетом если компьютеры в локальной сети используют IPv4, а Интернет-провайдер - IPv6. Вы можете выбрать тип соединения IPv6 только **Static IPv6, SLAAC/DHCPv6** или **PPP over Ethernet** в экране **Network > WAN > IPv6**.
DS-Lite Mode	Выберите **DS-Lite DHCPv6** чтобы с помощью DHCPv6автоматически получать информацию AFTR. Выберите **Manual** для настройки адреса AFTR вручную.
AFTR Name or Address	Введите имя домена либо IPv6-адрес маршрутизатора Address Family Transition Router (AFTR).
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.4 Экран Advanced Settings

Эта экран используется для настройки конфигурации multicast. Для перехода к нему щелкните **Network > WAN > Advanced**.

Иллюстрация 61 Network > WAN > Advanced

В следующей таблице описаны поля этого экрана.

Таблица 35 Network > WAN > Advanced

ПОЛЕ	ОПИСАНИЕ
Multicast Setup	
Multicast Proxy	Поставьте галочку в **Multicast Proxy** чтобы включить эту функцию в NBG-418N v2. С помощью этой функции proxy маршрутизатор IPv6 может обнаруживать хосты MLD, которые хотят получать пакеты multicast, и определять IP-адреса групп хостов, которые хотят присоединиться к сети multicast.
Multicast Snooping	С помощью функции **Multicast snooping** устройство NBG-418N v2 может проверять проходящие через него пакеты MLD и узнавать о членстве в группе multicast. Ее применение уменьшает трафик multicast.
Auto IP Setup	
Enable Auto-IP-Change mode	Поставьте галочку в **Enable Auto-IP-Change mode** чтобы NBG-418N v2 менял свой IP-адрес LAN на 10.0.0.1 или 192.168.1.1 соответственно когда NBG-418N v2 получает динамический IP-адрес WAN в той же подсети, что и IP-адрес LAN 192.168.1.1 или 10.0.0.1. В этом режиме по-прежнему доступны функции NAT, DHCP-сервера и межсетевого экрана NBG-418N v2.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

7.5 Экран IPv6 Settings

Эта экран используется для настройки конфигурации IPv6. Для перехода к нему щелкните **Network > WAN > IPv6**.

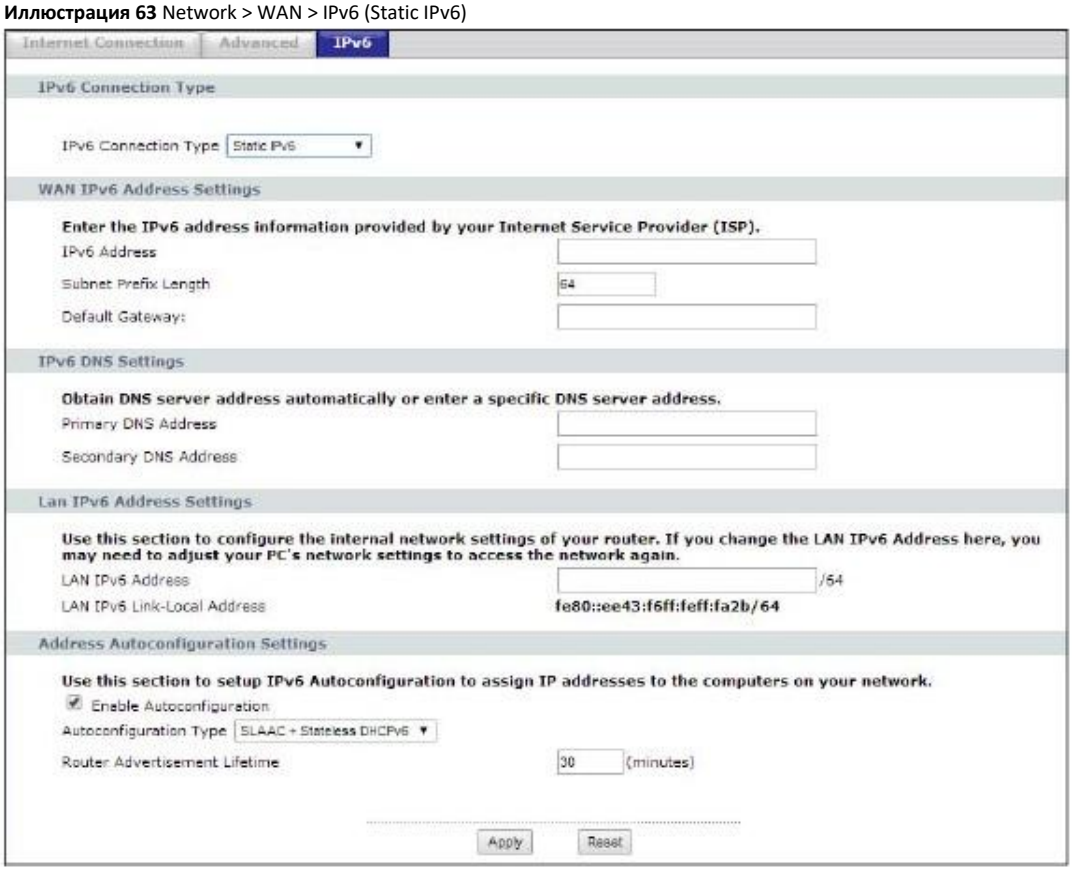
Иллюстрация 62 Network > WAN > IPv6 (Link-local Only)

В следующей таблице описаны поля этого экрана.

Таблица 36 Network > WAN > IPv6 (Link-local Only)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	Выберите **Link-local** чтобы NBG-418N v2 мог обменивать данными с соседними устройства по этому линку. В этом режиме устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Иллюстрация 63 Network > WAN > IPv6 (Static IPv6)



В следующей таблице описаны поля этого экрана.

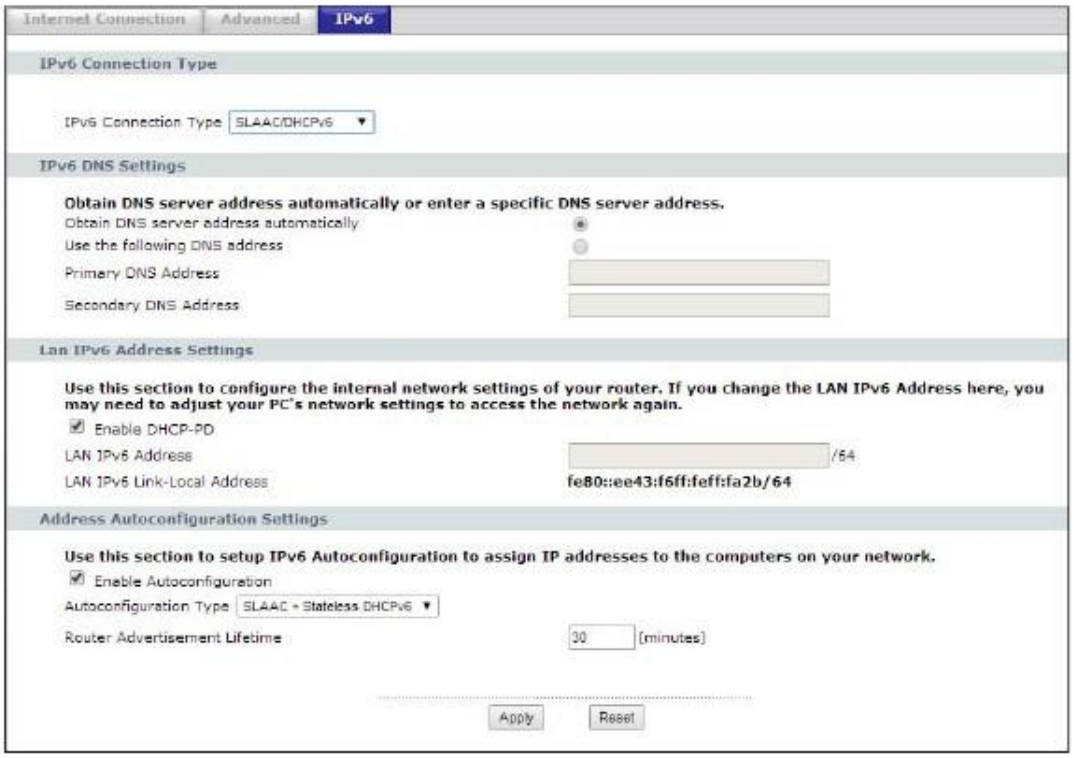
Таблица 37 Network > WAN > IPv6 (Static IPv6)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	Выберите **Static IPv6** если ваш провайдер выделил вам набор фиксированных IPv6-адресов. Вам нужно ввести те данные IPv6 address, Subnet Prefix Length, Default Gateway, Primary и Secondary DNS Server, которые вам предоставил провайдер.
Wan IPv6 Address Settings	
IPv6 Address	В это поле нужно ввести IPv6-адрес на стороне WAN.
Subnet Prefix Length	В это поле нужно ввести длину префикса адреса, которая определяет, сколько битов в IPv6-адресе относятся к адресу сети

Таблица 37 Network > WAN > IPv6 (продолжение)(Static IPv6)

ПОЛЕ	ОПИСАНИЕ
Default Gateway	Введите IP-адрес шлюза next-hop. Шлюз – это маршрутизатор либо коммутатор в той же подсети, что и интерфейс(ы) вашего NBG-418N v2. Шлюз помогает пересылать пакеты конечному получателю.
IPv6 DNS Settings	
Primary DNS Address	Введите IPv6-адрес первого DNS-сервера, который вам назначил провайдер.
Secondary DNS Address	Введите IPv6-адрес второго DNS-сервера, который вам назначил провайдер.
LAN IPv6 Address Settings	
LAN IPv6 Address	Введите в это поле IPv6-адрес порта LAN.
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
Address Auto configuration Settings	
Enable Auto configuration	Щелкните **Enable Auto configuration** если нужно чтобы устройства в локальной сети получали сетевые адреса от сервера DHCPv6.
Auto configuration Type	Выберите **SLAAC + Stateless DHCPv6** чтобы линк автоматически генерировал адрес link-local с помощью stateless auto configuration. Выберите **Stateful (DHCPv6)** если нужно, чтобы у устройств, подключенных к вашей локальной сети, конфигурация TCP/IP была настроена на использование DHCPv6 или они автоматически получали IPv6-адрес.
Router Advertisement Lifetime	Если вы выбрали **SLAAC + Stateless DHCPv6**, то укажите в поле Router Advertisement Lifetime сколько минут устройство может использовать «арендованный» адрес IPv6.
IPv6 Address Range (Start)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Range (End)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле старший адрес из этого диапазона IPv6-адресов.
IPv6 Address Lifetime	Если вы выбрали **Stateful (DHCPv6)**, то в этом поле нужно определить, сколько минут будет действовать IPv6-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Иллюстрация 64 Network > WAN > IPv6 (SLAAC/DHCPv6)



В следующей таблице описаны поля этого экрана.

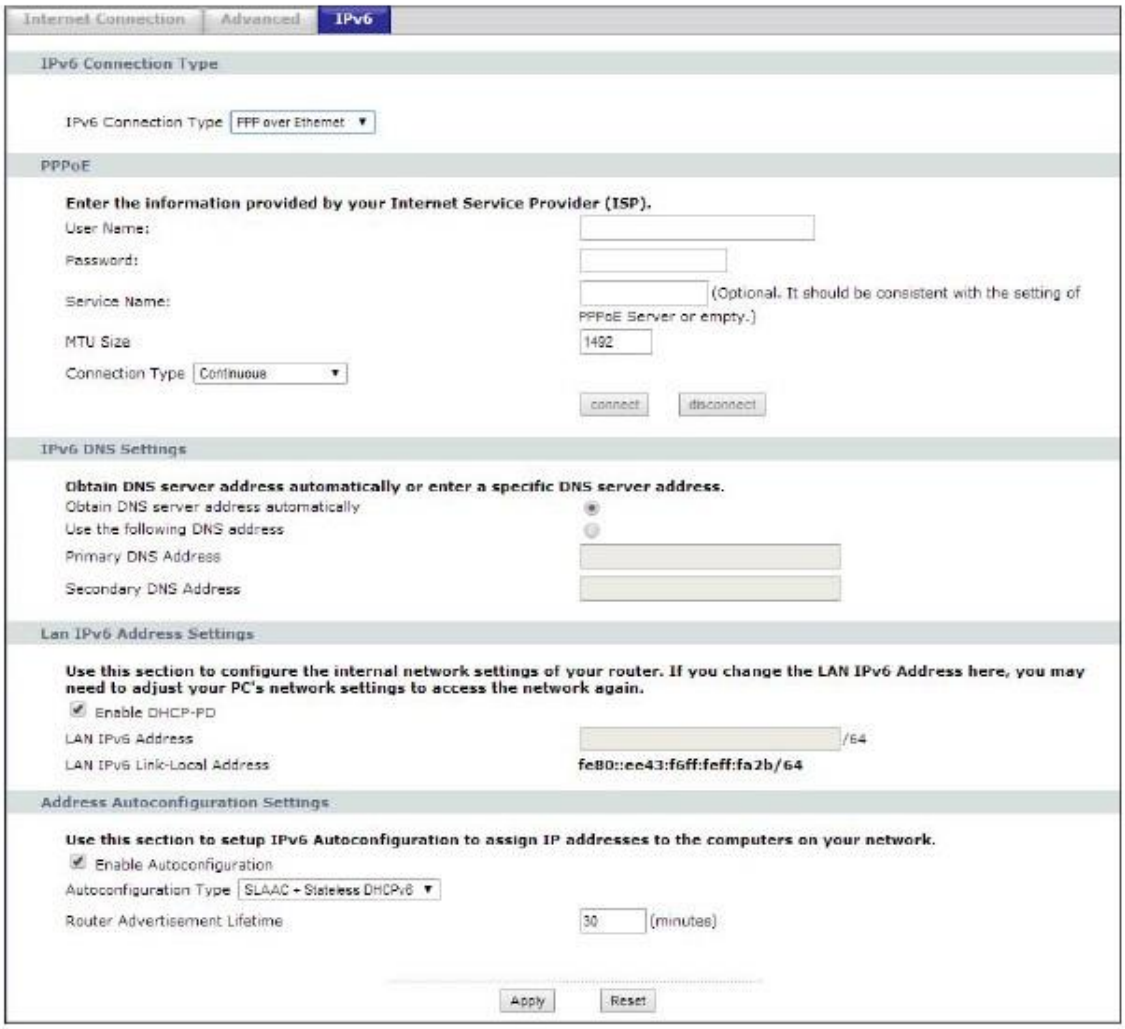
Таблица 38 Network > WAN > IPv6 (SLAAC/DHCPv6)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	Выберите **SLAAC/DHCPv6** если NBG-418N v2 запрашивает IPv6-адрес у сервера провайдера.
IPv6 DNS Settings	
Obtain DNS server address automatically	Щелкните **Obtain DNS server address automatically** чтобы получать адрес сервера DNS от сервера вашего провайдера.
Use the following DNS address	Щелкните **Use the following DNS address** чтобы использовать фиксированный адрес DNS.
Primary and Secondary DNS Address	Введите адрес первого/второго сервера IPv6 DNS, который вам назначил провайдер.
LAN IPv6 Address Settings	
Enable DHCP-PD	Щелкните **Enable DHCP-PD** (DHCP-Prefix delegation) чтобы NBG-418N v2 мог присваивать префиксы клиентам DHCP. Префикс – это часть адреса, которая указывает, что у битов есть постоянное значение или они являются идентификатором сети. Префикс записывается как адрес/длина-префикса.
LAN IPv6 Address	В это поле нужно ввести IPv6-адрес порта LAN если вы отключили IDHCP-PD.
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
Address Auto configuration Settings	
Enable Auto configuration	Щелкните **Enable Auto configuration** чтобы устройства в вашей локальной сети получали сетевые адреса, которыми не управляет DHCPv6-сервер.

Таблица 38 Network > WAN > IPv6 (продолжение)(SLAAC/DHCPv6)

ПОЛЕ	ОПИСАНИЕ
Auto configuration Type	Выберите **SLAAC + Stateless DHCPv6** если нужно, чтобы интерфейс автоматически генерировал адрес link-local с помощью stateless auto configuration. Выберите **Stateful (DHCPv6)** если нужно, чтобы у устройств, подключенных к вашей локальной сети, конфигурация TCP/IP была настроена на использование DHCPv6 или они автоматически получали IPv6-адрес.
Router Advertisement Lifetime	Если вы выбрали **SLAAC + Stateless DHCPv6**, то укажите в поле Router Advertisement Lifetime сколько минут устройство может использовать «арендованный» адрес IPv6.
IPv6 Address Range (Start)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Range (End)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле старший адрес из этого диапазона IPv6-адресов.
IPv6 Address Lifetime	Если вы выбрали **Stateful (DHCPv6)**, то в этом поле нужно определить, сколько минут будет действовать IPv6-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Иллюстрация 65 Network > WAN > IPv6 (PPPoE)



В следующей таблице описаны поля этого экрана.

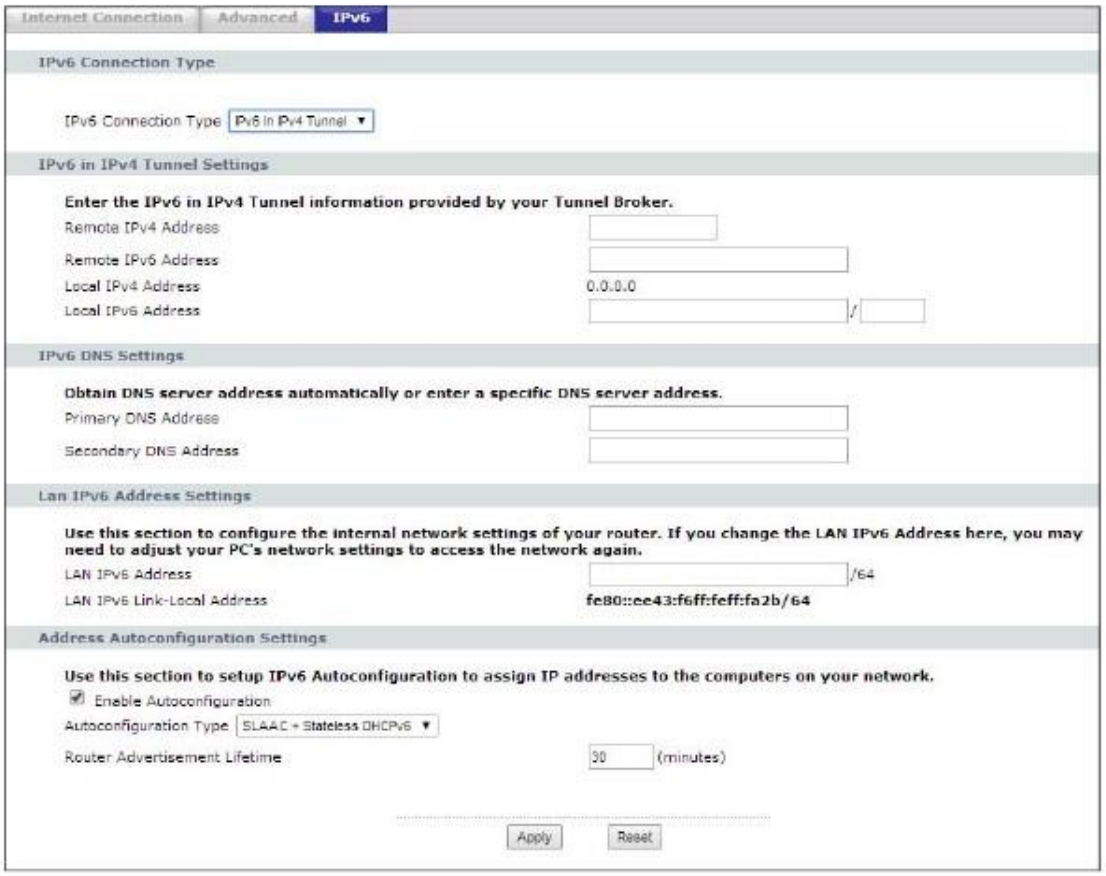
Таблица 39 Network > WAN > IPv6 (PPPoE)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	Выберите **PPPoE** если для подключения к Интернету по IPv6 требуется использовать соединение PPPoE. Обычно для такого подключения к Интернету нужно использовать имя пользователя и пароль, которые вам сообщил провайдер, а также удалить либо отключить клиентскую программу PPPoE на вашем компьютере.
PPPoE	
User Name	Введите имя пользователя (длиной до 31 букв и цифр) для login для доступа к соединению PPPoE.
Password	Введите пароль для этого имени пользователя
Service Name	Введите имя сервиса если это требует ваш Интернет-провайдер.
MTU Size	Введите MTU или максимальный размер фрейма в пакете, который NBG-418N v2 может получать и обрабатывать.

Таблица 39 Network > WAN > IPv6 (продолжение)(PPPoE)

ПОЛЕ	ОПИСАНИЕ
Connection Type	Выберите **Continuous** если не надо отключать соединение по таймеру. Выберите **Connection on Demand** если нужно, чтобы маршрутизатор автоматически отключался от сервера PPPoE через определенное время (время отключения в минутах нужно ввести в поле **Idle Timeout**). Выберите **Manual** если нужно устанавливать соединение вручную.
Connect/ Disconnect	Щелкните кнопку **Connect** чтобы установить соединение с заданными выше параметрами либо **Disconnect** для разрыва соединения.
IPv6 DNS Settings	
Obtain DNS Server address automatically	Щелкните **Obtain DNS server address automatically** чтобы автоматически получать адрес DNS-сервера от провайдера.
Use the following DNS address	Щелкните **Use the following DNS address** чтобы использовать фиксированный адрес DNS.
Primary/Secondary DNS Address	Введите IPv6-адрес первого /второго сервера DNS, который вам назначил провайдер.
LAN IPv6 Address Settings	
Enable DHCP-PD	Щелкните **Enable DHCP-PD** (DHCP-Prefix delegation) чтобы NBG-418N v2 мог присваивать префиксы клиентам DHCP.
LAN IPv6 Address	В это поле нужно ввести IPv6-адрес интерфейса LAN
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
Address Auto configuration Settings	
Enable Auto configuration	Щелкните **Enable Auto configuration** чтобы устройства в вашей локальной сети получали сетевые адреса, которыми не управляет DHCPv6-сервер.
Auto configuration Type	Выберите **SLAAC + Stateless DHCPv6** если нужно, чтобы интерфейс автоматически генерировал адрес link-local с помощью stateless auto configuration. Выберите **Stateful (DHCPv6)** если нужно, чтобы у устройств, подключенных к вашей локальной сети, конфигурация TCP/IP была настроена на использование DHCPv6 или они автоматически получали IPv6-адрес.
Router Advertisement Lifetime	Если вы выбрали **SLAAC + Stateless DHCPv6**, то укажите в поле Router Advertisement Lifetime сколько минут устройство может использовать «арендованный» адрес IPv6.
IPv6 Address Range (Start)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле старший адрес из этого диапазона IPv6-адресов.
IPv6 Address Range (End)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле старший адрес из этого диапазона IPv6-адресов.
IPv6 Address Lifetime	Если вы выбрали **Stateful (DHCPv6)**, то в этом поле нужно определить, сколько минут будет действовать IPv6-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Иллюстрация 66 Network > WAN > IPv6 (IPv6 in IPv4 Tunnel)



В следующей таблице описаны поля этого экрана.

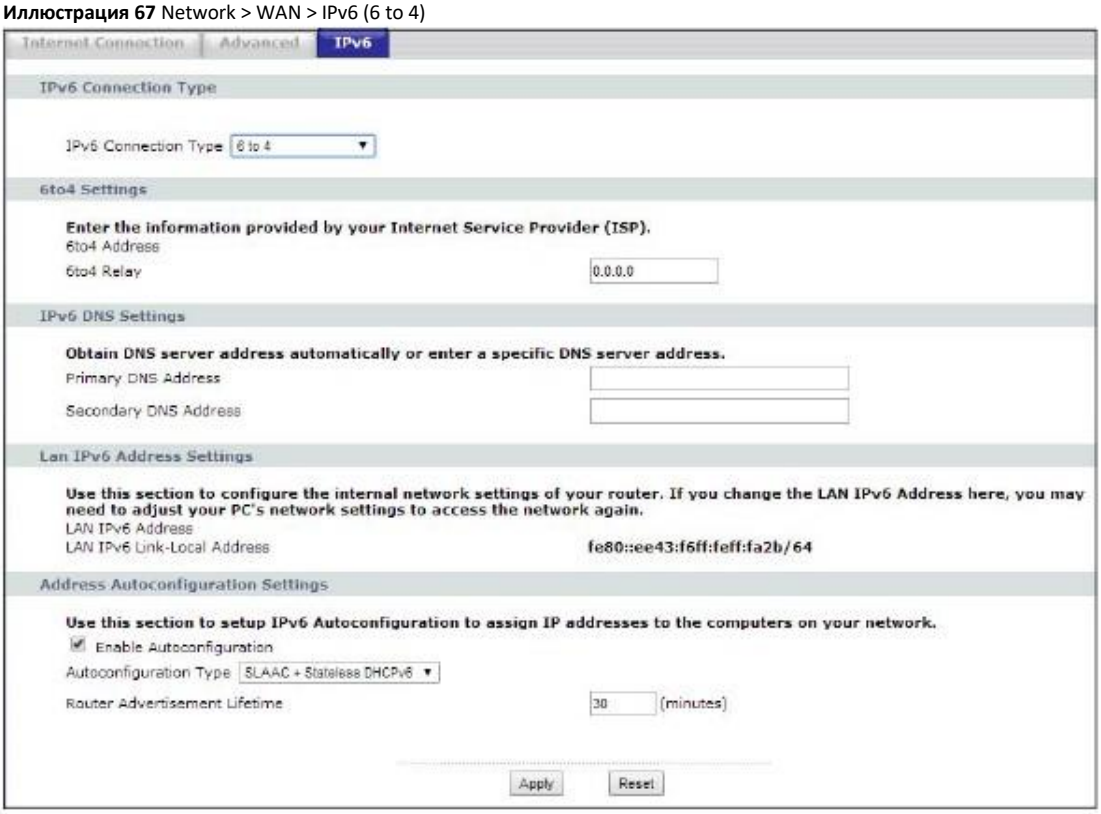
Таблица 40 Network > WAN > IPv6 (IPv6 in IPv4 Tunnel)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	IPv6 в IPv4 Tunnel – это инкапсуляция пакетов IPv6 в пакеты IPv4 для того, чтобы пакеты IPv6 можно было пересылать по инфраструктуре IPv4.
IPv6 in IPv4 Tunnel Settings	
Remote IPv4 Address	Введите IPv4-адрес устройства в удаленной сети.
Remote IPv6 Address	Введите IPv6-адрес устройства в удаленной сети.
Local IPv4 Address	Введите IPv4-адрес устройства в локальной сети.
Local IPv6 Address	Введите IPv6-адрес устройства в локальной сети.
IPv6 DNS Settings	
Primary and Secondary DNS Address	Введите IPv6-адрес первого /второго сервера DNS, который вам назначил провайдер.
Lan IPv6 Address Settings	
LAN IPv6 Address	В это поле нужно ввести IPv6-адрес порта LAN.
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6 (IPv6-capable), могут обмениваться данными между собой на стороне LAN.

Таблица 40 Network > WAN > IPv6 (IPv6 in IPv4 Tunnel)

ПОЛЕ	ОПИСАНИЕ
Address Auto configuration Settings	
Enable Auto configuration	Щелкните **Enable Auto configuration** чтобы устройства в вашей локальной сети получали сетевые адреса, которыми не управляет DHCPv6-сервер.
Auto configuration Type	Выберите **SLAAC + Stateless DHCPv6** если нужно, чтобы интерфейс автоматически генерировал адрес link-local с помощью stateless auto configuration. Выберите **Stateful (DHCPv6)** если нужно, чтобы у устройств, подключенных к вашей локальной сети, конфигурация TCP/IP была настроена на использование DHCPv6 или они автоматически получали IPv6-адрес.
Router Advertisement Lifetime	Если вы выбрали **SLAAC + Stateless DHCPv6**, то укажите в поле Router Advertisement Lifetime сколько минут устройство может использовать «арендованный» адрес IPv6.
IPv6 Address Range (Start)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Range (End)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле старший адрес из этого диапазона IPv6-адресов.
IPv6 Address Lifetime	Если вы выбрали **Stateful (DHCPv6)**, то в этом поле нужно определить, сколько минут будет действовать IPv6-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Иллюстрация 67 Network > WAN > IPv6 (6 to 4)

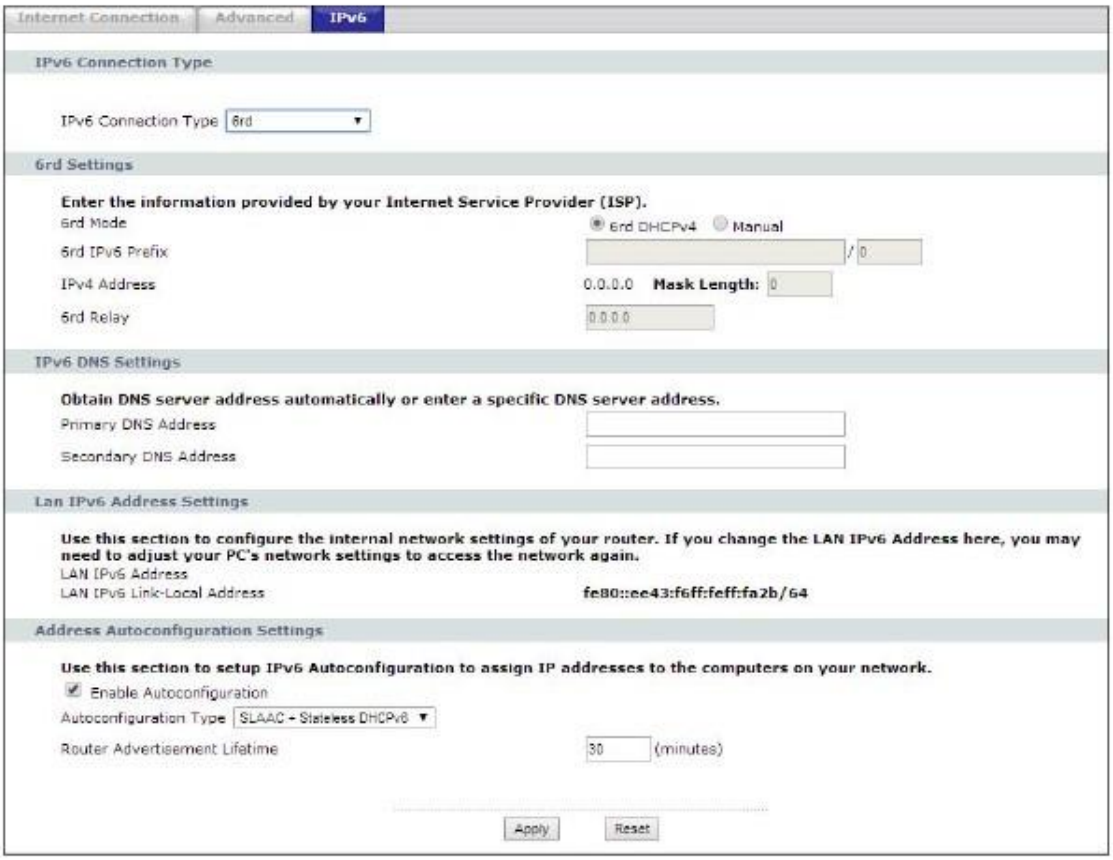


В следующей таблице описаны поля этого экрана.

Таблица 41 Network > WAN > IPv6 (6 to 4)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	**6 to 4** – это технология назначения адресов и автоматического туннелирования для соединения unicast IPv6 между сайтами и хостами IPv6 через Интернет IPv4.
6to4 Settings	
6to4 Address	
6to4 Relay	В это поле нужно ввести IPv6-адрес сервера border relay вашего провайдера.
IPv6 DNS Settings	
Primary/Secondary DNS Address	Введите IPv6-адрес первого /второго сервера DNS, который вам назначил провайдер.
LAN IPv6 Address Settings	
LAN IPv6 Address	Параметр в этом поле нельзя задавать если вы настроили **IPv6 Connection Type** в **6to4, 6rd** или **Link-local only**.
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
Address Auto configuration Settings	
Enable Auto configuration	Щелкните **Enable Auto configuration** чтобы устройства в вашей локальной сети получали сетевые адреса, которыми не управляет DHCPv6-сервер.
Auto configuration Type	Выберите **SLAAC + Stateless DHCPv6** если нужно, чтобы интерфейс автоматически генерировал адрес link-local с помощью stateless auto configuration. Выберите **Stateful (DHCPv6)** если нужно, чтобы у устройств, подключенных к вашей локальной сети, конфигурация TCP/IP была настроена на использование DHCPv6 или они автоматически получали IPv6-адрес.
Router Advertisement Lifetime	Если вы выбрали **SLAAC + Stateless DHCPv6**, то укажите в поле Router Advertisement Lifetime сколько минут устройство может использовать «арендованный» адрес IPv6.
IPv6 Address Range (Start)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Range (End)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Lifetime	Если вы выбрали **Stateful (DHCPv6)**, то в этом поле нужно определить, сколько минут будет действовать IPv6-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Иллюстрация 68 Network > WAN > IPv6 (6rd)



В следующей таблице описаны поля этого экрана.

Таблица 42 Network > WAN > IPv6 (6rd)

ПОЛЕ	ОПИСАНИЕ
IPv6 Connection Type	IPv6 Rapid Deployment (6rd) применяется когда локальная сеть использует IPv6, а сеть Интернет-провайдера - IPv4. Если у NBG-418N v2 IPv4-адрес WAN, то при включенной функции 6rd пакеты IPv6 будут инкапсулироваться в пакеты IPv4 для передачи по сети IPv4 Интернет-провайдера. NBG-418N v2 генерирует глобальный префикс IPv6 из своего IPv4-адреса WAN и по туннелю передает трафик IPv6 маршрутизатору border relay вашего провайдера для соединения с «нативным» Интернетом IPv6. Локальная сеть также использует сервисы IPv4. NBG-418N v2 использует свой сконфигурированный WAN IP для пересылки трафика IPv4 в Интернет IPv4.
6rd Settings	
6rd Mode	Щелкните **6rd DHCPv4** чтобы ваш провайдера автоматически генерировал адрес 6rd DHCPv4. Если выбрать **Manual**, то нужно вручную ввести фиксированный адрес 6rd DHCPv4.
6rd IPv6 Prefix	Введите префикс IPv6 и длину префикса адреса для передачи по туннелю передает трафика IPv6 маршрутизатору border relay вашего провайдера и для соединения с «нативным» Интернетом IPv6.
IPv4 Address	IPv4-адрес WAN для NBG-418N v2. Введите в поле **Mask Length** длину маски подсети IPv4 (от 1 до 32).
6rd Relay	Введите в это поле IPv4-адреса маршрутизатора border relay вашего провайдера.
IPv6 DNS Settings	
Primary/Secondary DNS Address	Введите IPv6-адрес первого /второго сервера DNS, который вам назначил провайдер.
LAN IPv6 Address Settings	

Таблица 42 Network > WAN > IPv6 (6rd)

ПОЛЕ	ОПИСАНИЕ
LAN IPv6 Address	Параметр в этом поле нельзя задавать если вы настроили **IPv6 Connection Type** в **6to4, 6rd** или **Link-local only**.
LAN IPv6 Link-Local Address	IPv6-адрес Link-local на стороне LAN. Он используется маршрутизаторами для связи с соседними устройствами по одному линку. При этом устройства, поддерживающие IPv6-capable, могут обмениваться данными между собой на стороне LAN.
Address Auto configuration Settings	
Enable Auto configuration	Щелкните **Enable Auto configuration** чтобы устройства в вашей локальной сети получали сетевые адреса, которыми не управляет DHCPv6-сервер.
Auto configuration Type	Выберите **SLAAC + Stateless DHCPv6** если нужно, чтобы интерфейс автоматически генерировал адрес link-local с помощью stateless auto configuration. Выберите **Stateful (DHCPv6)** если нужно, чтобы у устройств, подключенных к вашей локальной сети, конфигурация TCP/IP была настроена на использование DHCPv6 или они автоматически получали IPv6-адрес.
Router Advertisement Lifetime	Если вы выбрали **SLAAC + Stateless DHCPv6**, то укажите в поле Router Advertisement Lifetime сколько минут устройство может использовать «арендованный» адрес IPv6.
IPv6 Address Range (Start)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Range (End)	Если вы выбрали **Stateful (DHCPv6)**, то нужно указать диапазон IPv6-адресов, которые сервер DHCPv6 может выделять клиентам. Введите в это поле младший адрес из этого диапазона IPv6-адресов.
IPv6 Address Lifetime	Если вы выбрали **Stateful (DHCPv6)**, то в этом поле нужно определить, сколько минут будет действовать IPv6-адрес.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

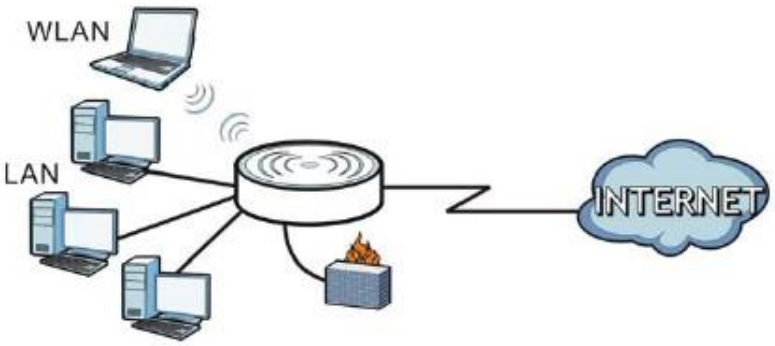
ГЛАВА 8
LAN

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 69 Схема LAN

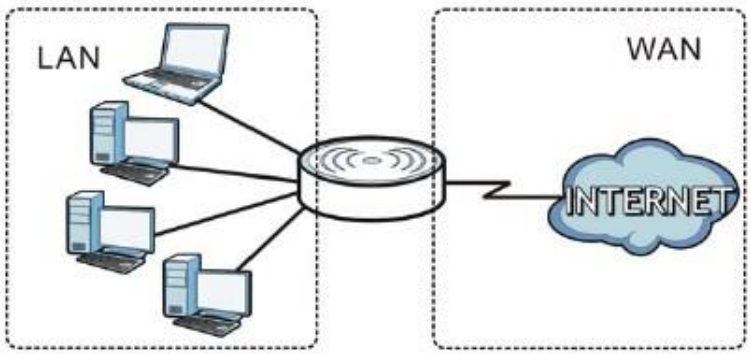


С помощью экранов LAN можно настроить DHCP-сервер LAN и управлять IP-адресами.

8.2 Основные сведения

Фактическое физическое соединение определяет, является ли порт NBG-418N v2 портом LAN или портом WAN. Есть две изолированные друг от друга сети IP - внутренняя LAN и внешняя WAN (см. Иллюстрацию).

Иллюстрация 70 IP-адреса LAN и WAN



Заводские настройки параметров LAN по умолчанию в NBG-418N v2:

• IP-адрес 192.168.1.1 и маска подсети 255.255.255.0 (24 бита)

• Для сервера DHCP выделено 32 IP-адреса клиентов начиная с 192.168.1.33

Эти параметры подходят для большинства сценариев использования устройства. Если ваш провайдер предоставил вам IP-адрес(а) сервера 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 этот 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 три комбинации из трех цифр идентифицируют номер сети, а последняя – отдельные компьютеры в сети.

После того, как вы узнали диапазон доступных вам IP-адресов, выберите один из них для NBG-418N v2, 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 сети. NBG-418N v2 автоматически определит маску подсети на основе введенного вами IP-адреса. Ее можно менять только если этого требует ваш 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.

NBG-418N v2 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

NBG-418N v2 предварительно сконфигурирован с пулом 32-адресов от 192.168.212.33 до 192.168.1.64. В этой конфигурации первые 31 IP-адресов (кроме IP-адреса самого NBG-418N v2) от 192.168.1.2 до 192.168.1.32 зарезервированы для серверов, которые могут быть в вашей сети, например, email, FTP, TFTP, web и т.п.

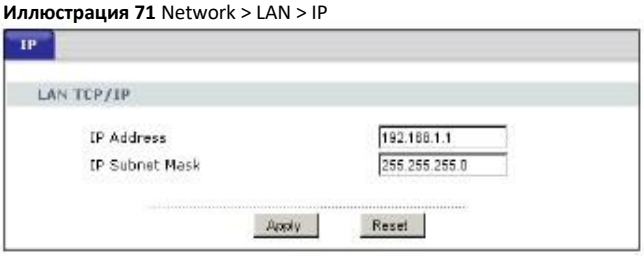
8.2.4 LAN TCP/IP

В NBG-418N v2 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 71 Network > LAN > IP



В следующей таблице описаны поля этого экрана.

Таблица 43 Network > LAN > IP

ПОЛЕ	ОПИСАНИЕ
IP Address	IP-адрес NBG-418N v2 (десятеричные цифры, разделенные точками, заводские настройки по умолчанию 192.168.1.1.
IP Subnet Mask	Маска подсети IP-адреса. NBG-418N v2 автоматически рассчитает маску подсети на основе назначенного вами устройству IP-адреса. Если вы не используете subnetting, то используйте маску подсети, которую рассчитал NBG-418N v2.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
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 NBG-418N v2 как DHCP-сервер LAN либо отключить его. В первом случае NBG-418N v2 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. 102).
- Экран **Static DHCP** для назначения IP-адресов в LAN компьютерам в соответствии с их конкретным MAC-адресом (Раздел 9.5 на стр. 103).
- Экран **Client List**, на котором выводится текущая информация о клиенте DHCP (Раздел 9.6 на стр. 104).

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**.

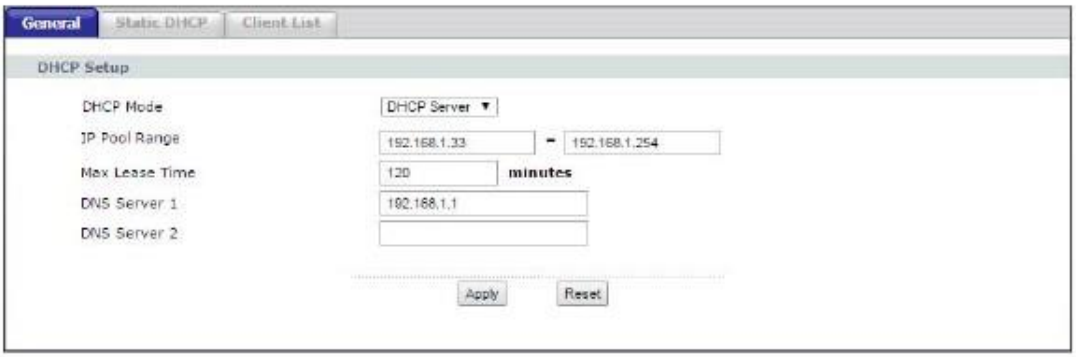
О IP-адресах и маске подсети см. Раздел 8.2.1 на стр. 100.

О серверах DNS см. Раздел 8.2.2 на стр. 100.

9.4 Экран General

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

Иллюстрация 72 Network > DHCP Server > General



В следующей таблице описаны поля этого экрана.

Таблица 44 Network > DHCP Server > General

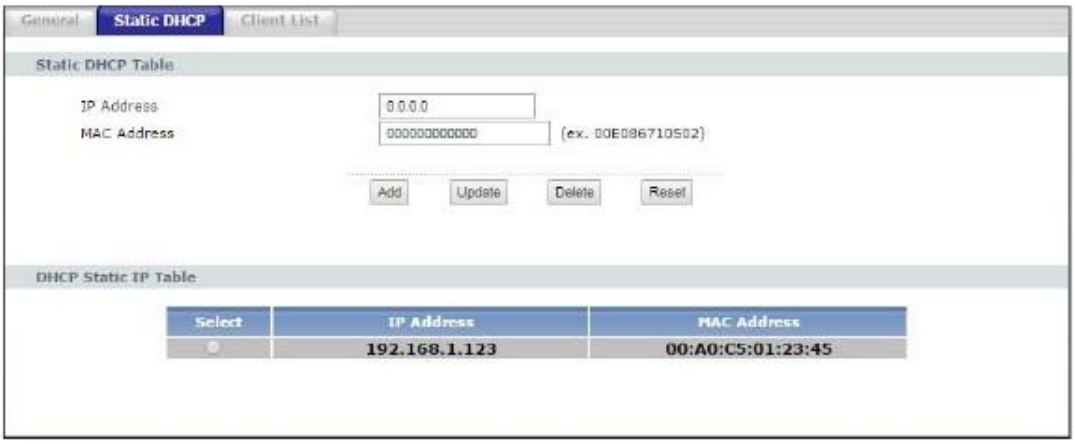
ПОЛЕ	ОПИСАНИЕ
DHCP Mode	В раскрывающемся списке выберите **DHCP server** чтобы NBG-418N v2 работал как сервер DHCP либо, если это необходимо для выполнения инструкций вашего провайдера, выберите **None**. Протокол DHCP (Dynamic Host Configuration Protocol, RFC 2131 и RFC 2132) обеспечивает отдельным 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 Sever1	IP-адрес первого DNS-сервера для сервера DHCP
DNS Sever2	IP-адрес второго DNS-сервера для сервера DHCP
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

9.5 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 NBG-418N v2 посылает клиентам DHCP.

Для изменения настроек static DHCP вашего NBG-418N v2 щелкните **Network > DHCP Server > Static DHCP**. Откроется следующий экран.

Иллюстрация 73 Network > DHCP Server > Static DHCP



В следующей таблице описаны поля этого экрана.

Таблица 45 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.
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	
Select	Щелкните кнопку **Select** чтобы выбрать запись static DHCP.
IP Address	IP-адрес компьютера в вашей LAN
MAC Address	MAC-адрес компьютера в вашей LAN.

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 NBG-418N v2.

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 74 Network > DHCP Server > Client List

В следующей таблице описаны поля этого экрана.

Таблица 46 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 NBG-418N v2.
Refresh	Щелкните **Reset** для перезагрузки DHCP table.

ГЛАВА 10
Network Address Translation

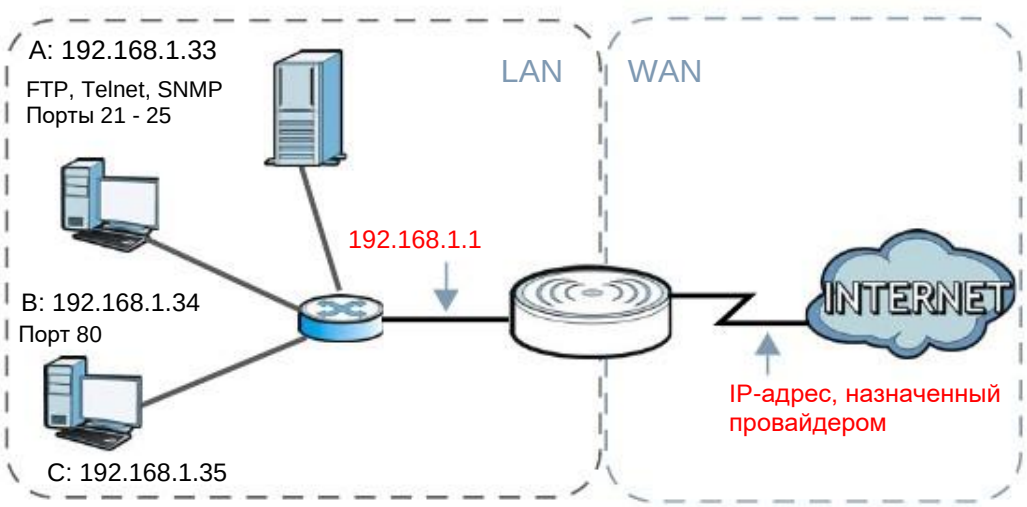
10.1 Обзор

В этой главе объясняется, как настроить NAT на NBG-418N v2.

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. NBG-418N v2 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 75 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 NBG-418N v2.

10.2 Экраны, которые описаны в этой главе

• Экран **General** для включения NAT и настройки сервера по умолчанию server (Раздел 10.3 на стр. 108).

• Экран **Application** для изменения настроек port forwarding на NBG-418N v2 (Раздел 10.4 на стр. 109).

• Экран **Port Triggering** для изменения настроек port trigger на NBG-418N v2 (Раздел 10.5 на стр. 111).

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 NBG-418N v2или внешним, например, компьютеры ваших подписчиков – это внутренние хосты, а web-серверы в Интернете – внешние хосты.

Глобальный/кокальный

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 47 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

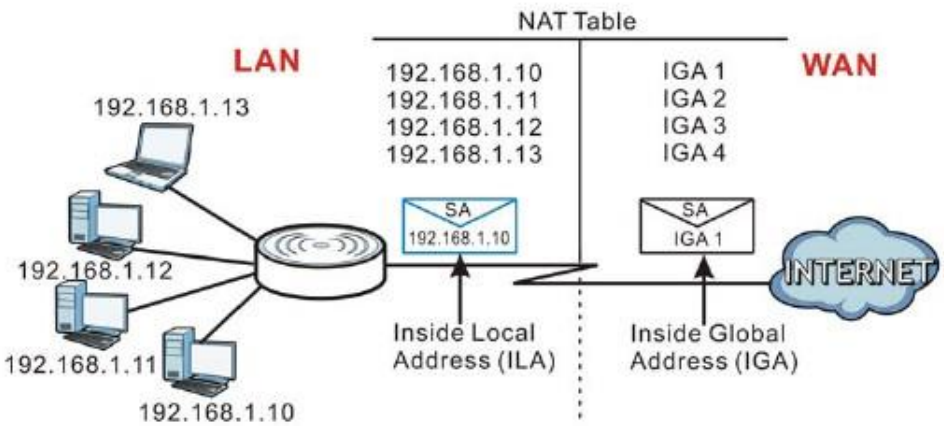
NAT меняет IP-адрес из пакета, который пришел от подписчика (внутренний локальный адрес) на внутренний глобальный адрес и затем пересылает этот пакет в WAN. Когда приходит ответ на этот пакет, то NAT преобразует адрес получателя (внутренний глобальный адрес) обратно в внутренний локальный адрес и затем 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 ILA (Inside Local Address) является адресом источника в LAN, а IGA (Inside Global Address) – адресом источника в WAN. Во входящих пакета ILA – это адрес получателя в LAN, а IGA – это адрес получателя в WAN. 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. 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. NBG-418N v2 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).

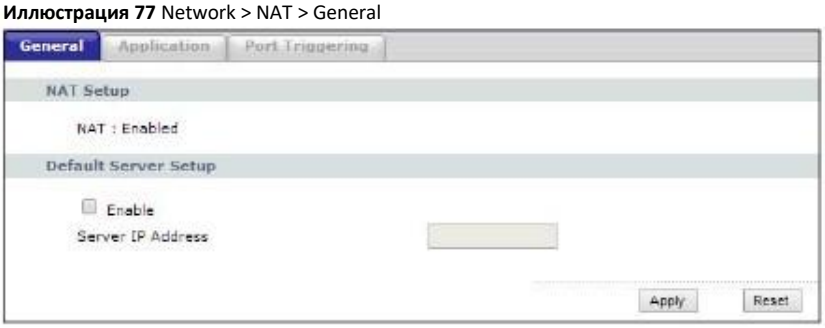
Иллюстрация 76 Как работает NAT



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 77 Network > NAT > General



В следующей таблице описаны поля этого экрана.

Таблица 48 Network > NAT > General

ПОЛЕ	ОПИСАНИЕ
NAT Setup	
Network Address Translation	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). Это показывает, включена ли NAT или нет.
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 NBG-418N v2 будет отбрасывать все пакеты, которые направляются на порты, неуказанные на экране **Application** и не сконфигурированные средствами удаленного управления.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
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.

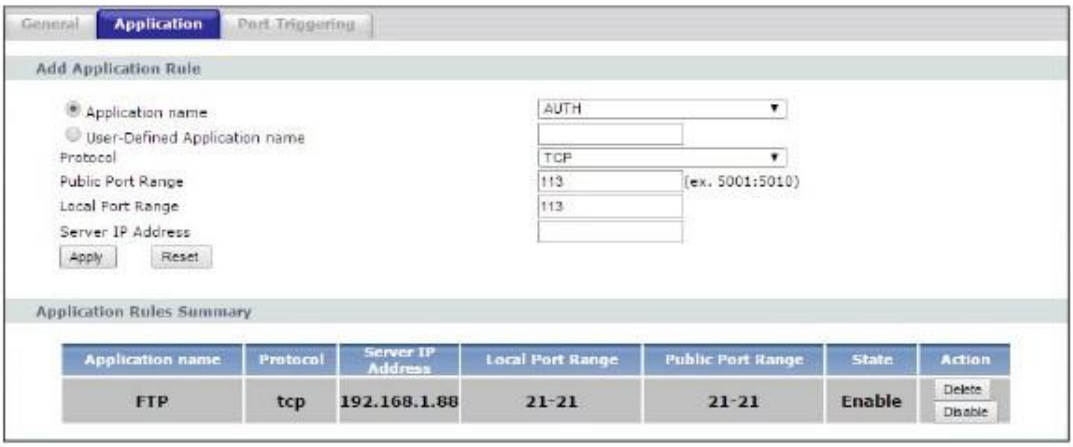
Примечание: Многие Интернет-провайдеры не разрешают домашним пользователям использовать собственный сервер для развертывания сервисов (например, Web или FTP), и в случае нарушения этого запрета могут заблокировать пользователя. Если вы не уверены, что ваш провайдер разрешает домашним пользователям развертывать 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 NBG-418N v2 щелкните **Network > NAT > Application**. Откроется следующий экран.

Примечание: Если на экране NAT > General не назначен IP-адрес для Default Server, то NBG-418N v2 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 G на стр. 237.

Иллюстрация 78 Network > NAT > Application



В следующей таблице описаны поля этого экрана.

Таблица 49 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.
Protocol	Протокол транспортного уровня, поддерживаемый этим сервером.
Server IP Address	Внутренний IP-адрес сервера.
Local Port Range Public Port Range	Номера порта (портов)
State	Это поле показывает, включено ли правило или нет.
Action	Щелкните пиктограмму **Disable** чтобы отключить правило. Щелкните пиктограмму **Delete** чтобы удалить правило.

10.5 Port Triggering

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. NBG-418N v2 записывает IP-адрес компьютера LAN, который послал трафик в WAN с запросом сервиса с определенным номером порта и протоколом («порт-триггер»). Когда WAN-порт NBG-418N v2 получает ответ на запрос, в котором указаны определенный номер порта и протокол (входящий порт), то NBG-418N v2 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 LANn.

Примечание: TCP-порт 7547 зарезервирован для системы.

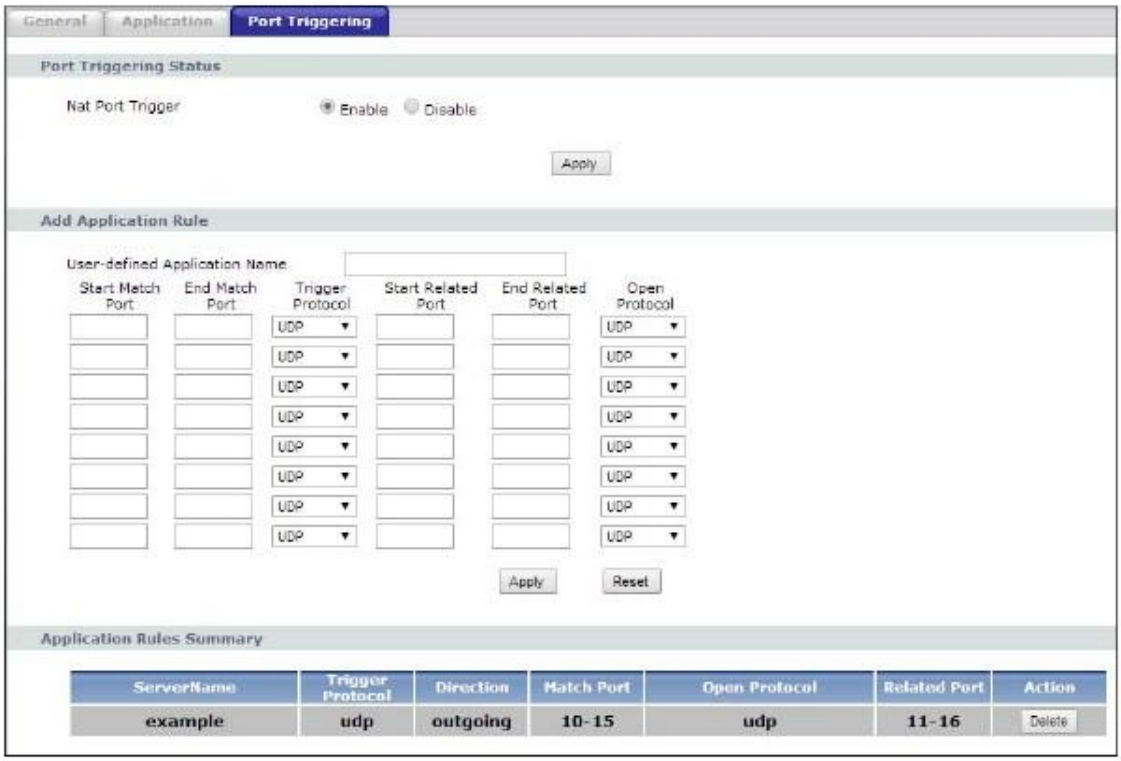
Примечание: в одном правиле может быть максимум 999 портов-триггеров.

Примечание: в одном либо всех правилах может быть максимум 999 открытых портов.

Для изменения настроек портов-триггеров NBG-418N v2 щелкните **Network > NAT > Port Triggering**. Откроется следующий экран.

Примечание: несколько компьютеров в LAN не могут одновременно использовать порт-триггер (диапазон портов).

Иллюстрация 79 Network > NAT > Port Triggering



В следующей таблице описаны поля этого экрана.

Таблица 50 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 NBG-418N v2 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 NBG-418N v2 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 NBG-418N v2 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. NBG-418N v2 будет перенаправлять трафик с этих портов клиентскому компьютеру в LAN, который запросил этот сервис.
End Related Port	Введите номер последнего порта из диапазона портов, которые использует сервер в WAN для определенного сервера. NBG-418N v2 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 NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

Таблица 50 Network > NAT > Port Triggering (продолжение)

ПОЛЕ	ОПИСАНИЕ
Application Rules Summary	
Service Name	Имя правила Application.
Trigger Protocol	Протокол, который запускает на NBG-418N v2 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN.
Direction	Направление, в котором идут пакеты, соответствующие этому правилу.
Match Port	Порты, которые работают как триггеры (они запускают на NBG-418N v2 механизм отслеживания IP-адресов компьютера в LAN, который посылает трафик на сервер в WAN).
Open Protocol	This field displays the protocol a server on the WAN uses when it sends out a particular service.
Related Port	Порт (порты) сервера в WAN, который используется для определенного сервиса. Трафик с этого порта (портов) NBG-418N v2 передает на клиентский компьютер в LAN, который запросил сервис.
Action	Щелкните **Delete** чтобы удалить правило.

10.6 Техническая информация

В этом разделе приводится дополнительная техническая информация о функциях NBG-418N v2, 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.

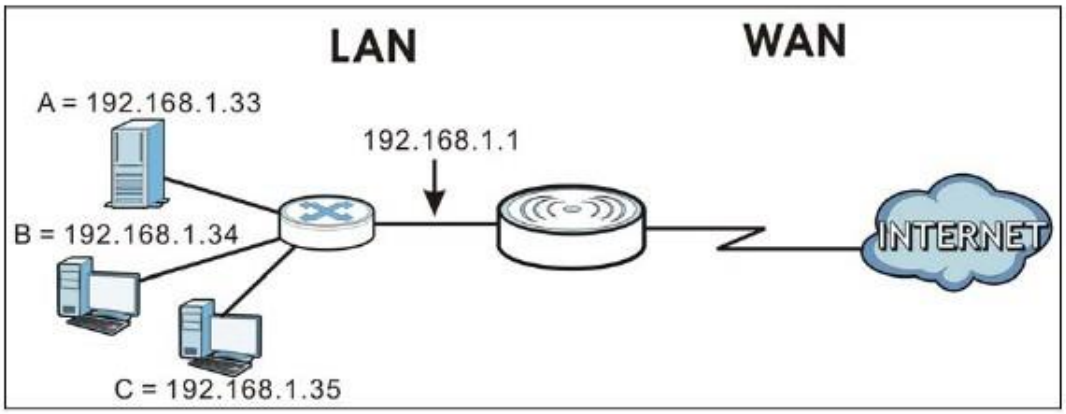
В дополнение к серверам для заданных сервисов NAT поддерживает сервер по умолчанию, на который направляются запросы, в которых не указан адрес сервера. Если сервер по умолчанию не задан, то такие запросы не обрабатываются.

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 80 Пример нескольких серверов, которые находятся за NAT



10.6.3 Trigger Port Forwarding

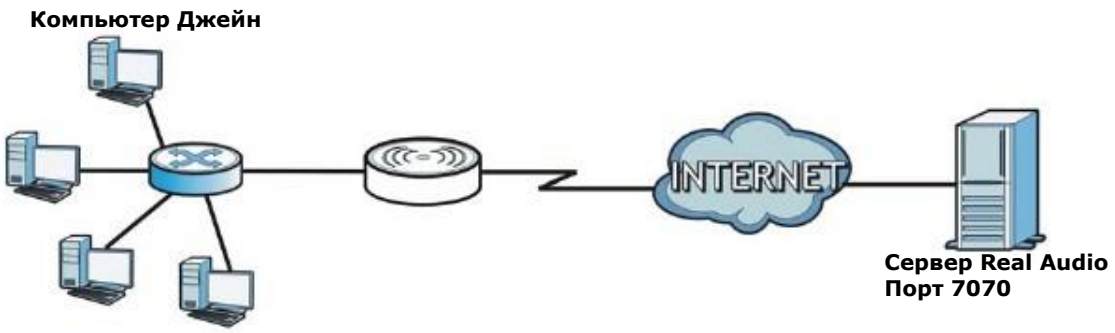
Некоторые сервисы используют выделенный диапазон портов и на стороне клиента, и на стороне сервера. С помощью стандартной функции port forwarding можно настроить в NAT порт на пересылку пакетов сервиса, которые приходят от сервера из WAN, на IP-адреса компьютера на стороне клиента (LAN). Однако port 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. NBG-418N v2 записывает IP-адрес компьютера LAN, который послал трафик в WAN с запросом сервиса с определенным номером порта и протоколом («порт-триггер»). Когда WAN-порт NBG-418N v2 получает ответ на запрос, в котором указаны определенный номер порта и протокол (входящий порт), то NBG-418N v2 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 81 Пример работы Trigger Port Forwarding



1 Джейн запросила файл с сервера Real Audio (порт 7070).

2 Порт 7070 – это «порт-триггер», поэтому NBG-418N v2 запишет IP-адрес компьютера Джейн и свяжет этот адрес с диапазоном «входящих» портов 6970-7170.

3 Сервер Real Audio отвечает на запрос, используя порты в диапазоне 6970-7170.

4 NBG-418N v2 перенаправляет трафик на IP-адрес компьютера Джейн.

5 До разрыва соединения или истечения выделенного времени только Джейн может подключиться к серверу Real Audio. NBG-418N v2 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 NBG-418N v2.

2 Если через порт (диапазон портов) идет непрерывный поток данных приложения, то этот порт (диапазон портов) не сможет использовать другой компьютер в LAN.

ГЛАВА11
Dynamic DNS

11.1 Обзор DNS

DNS

DNS (Domain Name System) обеспечивает соответствие между именем домена и IP-адресом. С помощью сервера DNS можно обращаться к компьютеру по имени его домена.

В дополнение к серверу (серверам) DNS системы каждый интерфейс (сервис) WAN должен иметь собственный список статичных или динамичных серверов DNS. Вы может настроить статичный маршрут DNS чтобы запросы DNS перенаправлялись определенным доменам через определенный интерфейс WAN его серверу (серверам) DNS. NBG-418N v2 использует сервер DNS системы для определения имен доменов, которых нет в таблице маршрутизации DNS. После того, как NBG-418N v2 получит ответ DNS от сервера DNS, он создает новую запись о IP-адресе в таблице маршрутизации.

Dynamic DNS

Dynamic DNS позволяет использовать динамический IP-адрес с одним или несколькими динамическими сервисами DNS, а также предоставлять доступ к вашим серверам FTP и Web, развернутым на вашем компьютере, по постоянному имени домена (например, myhost.dhs.org, где вместо myhost может стоять любое выбранное вами имя choice) вместо доступа по IP-адресу, который меняется при каждом соединении.

Для использования Dynamic DNS нужно иметь зарегистрированную учетную запись dynamic DNS в www.dyndns.org. Этот сервис позволяет пользователям иметь имя домена, хотя они получают динамический IP-адрес от сервис-провайдера или сервера DHCP. Провайдер сервиса Dynamic DNS должен предоставить вам пароль.

Примечание: У NBG-418N v2 должен быть публичный глобальный IP-адрес и у вас должна информация о учетной записи DDNS.

11.1.1 Общие сведения

Метасимвол DYNDNS

Если в имени хоста использовать метасимвол (wildcard), то *.yourhost.dyndns.org будет отображаться в тот же IP-адрес, что и yourhost.dyndns.org. Например, можно использовать для доступа как www.yourhost.dyndns.org, так и имя хоста.

Dynamic DNS нельзя использовать вместе с частным IP-адресом WAN.

11.2 Dynamic DNS

Для задания настроек DDNS вашего NBG-418N v2 щелкните **Network > DDNS**.

Иллюстрация 82 Network > DDNS

В следующей таблице описаны поля этого экрана.

Таблица 51 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	Введите в это поле Имя пользователя, которое вам сообщил провайдер сервиса DDNS.
Password	Введите пароль для имени пользователя DDNS user name.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.
Dynamic DDNS Table	
Select	Поставьте галочку в **Select** чтобы выбрать запись DDNS, для которой нужно изменить параметры.
Dynamic DNS	Это поле показывает, включен ли DDNS (**Enabled**) или выключен (**Disabled**).
Service Provider	Имя провайдера сервиса DDNS.
Host Name	Имя хоста, соответствующее DDNS.
User Name	Имя пользователя, соответствующее DDNS.

ГЛАВА12
Static Route

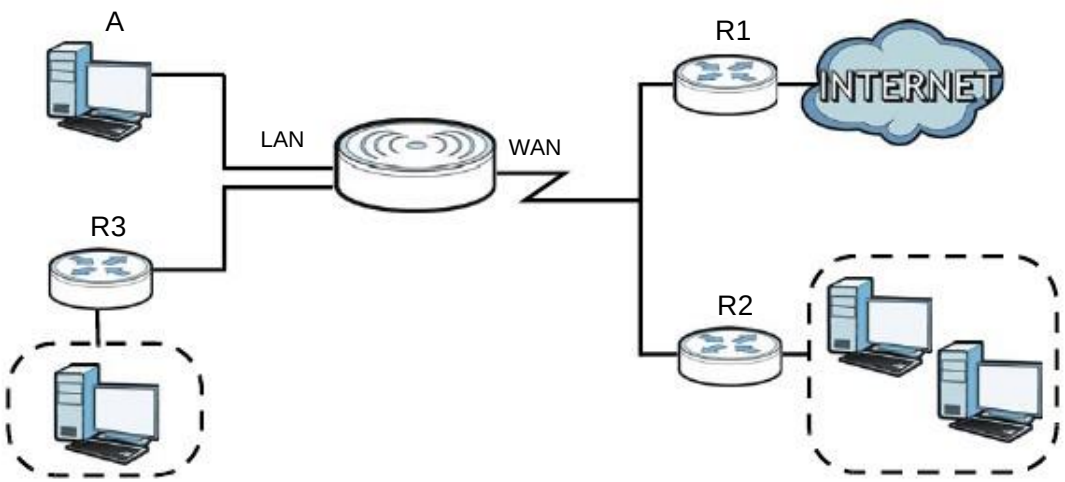
12.1 Обзор

В этой главе объясняется, как сконфигурировать статические маршруты для NBG-418N v2.

Обычно NBG-418N v2 перенаправляет исходящий трафик от компьютеров в LAN в Интернет с помощью шлюза по умолчанию. Если нужно, чтобы NBG-418N v2 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 NBG-418N v2. Основной объем трафика NBG-418N v2 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.

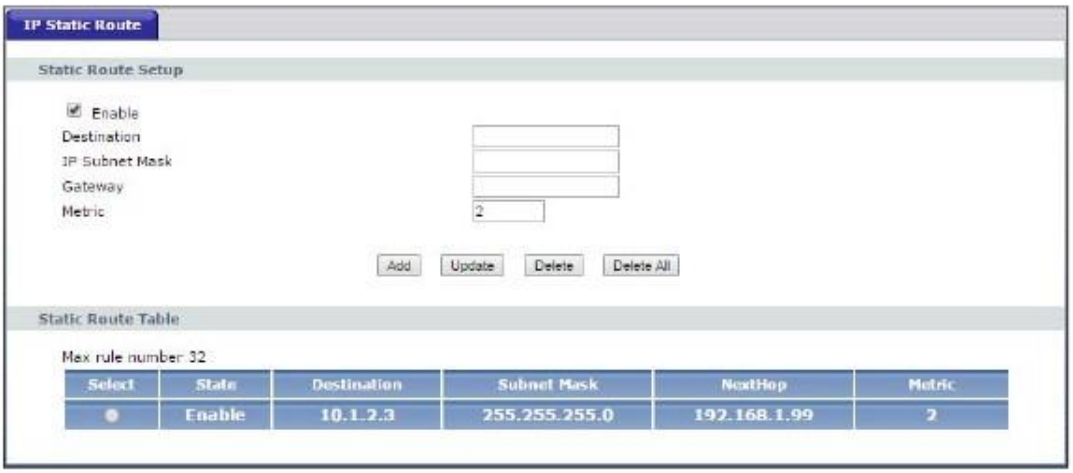
Иллюстрация 83 Пример топологии со статической маршрутизацией



12.2 Экран IP Static Route

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

Иллюстрация 84 Network > Static Route



В следующей таблице описаны поля этого экрана.

Таблица 52 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) NBG-418N v2. 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 NBG-418N v2 до конечного получателя.
Add	Щелкните эту кнопку для создания нового правила.
Update	Щелкните эту кнопку для изменения выбранного правила.
Delete	Щелкните эту кнопку для удаления выбранного правила.
Delete All	Щелкните эту кнопку для удаления всех правил.
#	Номер по порядку отдельного правила статического маршрута.
Select	Щелкните эту кнопку выбора правила для изменения его настроек или его удаления.
State	Это поле показывает, включено ли правило или нет.
Destination	IP-адрес сети конечного получателя. Маршрутизация всегда выполняется на основе адреса сети.
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.
Metric	Число хопов между NBG-418N v2 и конечным получателем.

ГЛАВА13 Межсетевой экран

13.1 Обзор

Эти экраны используются для включения и настройки межсетевого экрана, который защищает NBG-418N v2 и вашу локальную сеть от постороннего и опасного трафика.

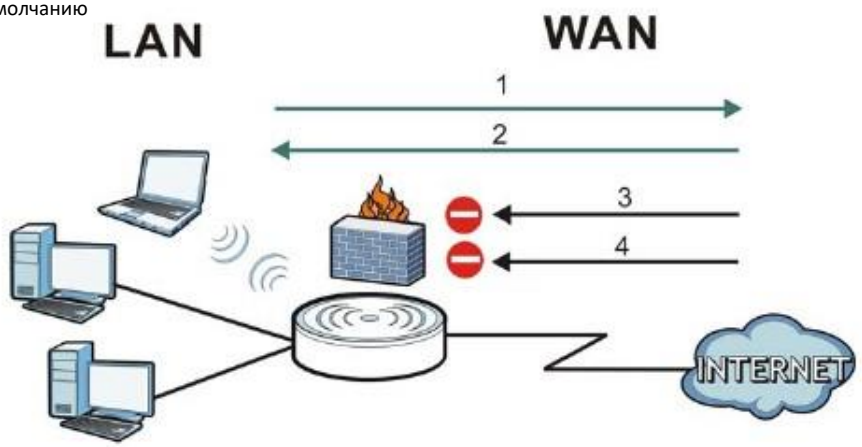
Рекомендуется включать межсетевой экран для защиты компьютеров в LAN от атак хакеров из Интернета и контроля доступа между LAN и WAN. По умолчанию межсетевой экран работает следующим образом:

• 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 85 Работа межсетевого экрана по умолчанию



13.2 Экраны, которые описаны в этой главе

• • Экран **General** для включения/отключения межсетевого экрана NBG-418N v2 (Раздел 13.4 на стр. 121).

• Экран **Services** для включения/отключения функций ICMP и VPN (Раздел 13.5 на стр. 122).

13.3 Основные сведения

Межсетевой экран NBG-418N v2 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 NBG-418N v2

Межсетевой экран NBG-418N v2 – 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**). NBG-418N v2 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.

NBG-418N v2 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 NBG-418N v2 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.

NBG-418N v2 не является конечным устройством VPN, но позволяет трафику проходить между этими конечными точками. NBG-418N v2 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 NBG-418N v2 и настройки журнала сетевого экрана. Для перехода на экран **General** щелкните **Security > Firewall**.

Иллюстрация 86 Security > Firewall > General

В следующей таблице описаны поля этого экрана.

Таблица 53 Security > Firewall > General

ПОЛЕ	ОПИСАНИЕ
Enable Firewall	Это опция включения межсетевого экрана. Когда включен межсетевой экран NBG-418N v2 контролирует доступ и защищает от атак Denial of Service (DoS).
Enable DoS	Опция защиты от атак DoS. NBG-418N v2 будет разрывать сессии которые не установлены полностью (half-open sessions) и превышают пороговое значение.
Apply	Щелкните **Apply** для сохранения изменений.
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 87 Security > Firewall > Services

В следующей таблице описаны поля этого экрана.

Таблица 54 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 **Enable**, то NBG-418N v2 отвечает на все входящие из WAN запросы Ping, а если **Disable** – то не отвечает на Ping из WAN.

Таблица 54 Security > Firewall > Services (продолжение)

ПОЛЕ	ОПИСАНИЕ
VPN Passthrough	Поставьте галочку чтобы включить дополнительные функции pass through: • PPTP эта опция позволяет NBG-418N v2 передавать трафик VPN с помощью протокола PPTP. • IPSEC Passthrough: эта опция позволяет NBG-418N v2 передавать трафик VPN с помощью протокола IPsec. • 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.

ГЛАВА14
Content Filtering

14.1 Обзор

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

При блокировке по ключевым словам NBG-418N v2 отдельно проверяет имя домена или IP-адрес URL и путь к файлу (filepath).

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– это news/pressroom.php.

Поскольку NBG-418N v2 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 NBG-418N v2 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

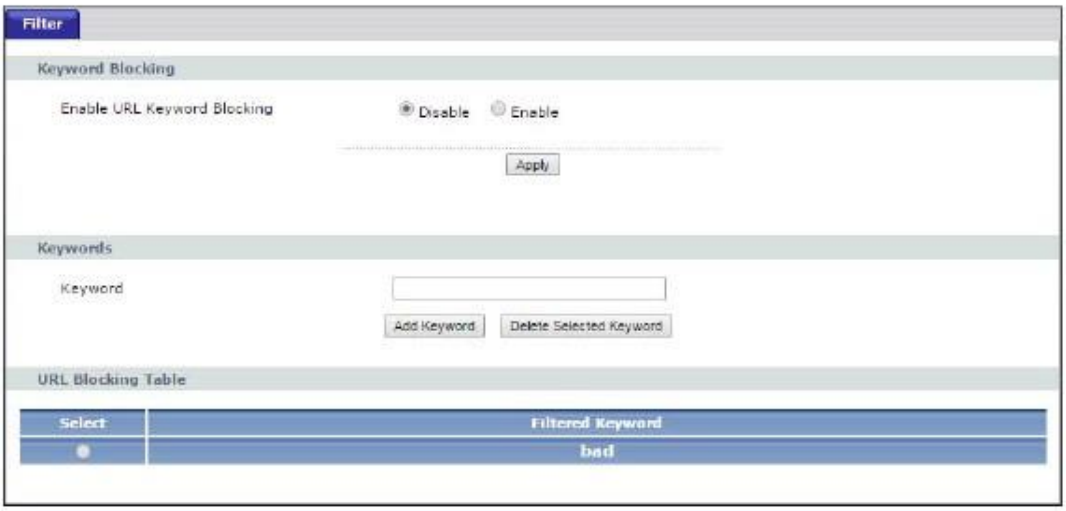
Экран **Filter** позволяет заблокировать доступ пользователей вашей сети к определенным web-сайтам (Раздел 14.3 на стр. 124).

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 88 Security > Content Filter > Filter



В следующей таблице описаны поля этого экрана.

Таблица 55 Security > Content Filter > Filter

ПОЛЕ	ОПИСАНИЕ
Enable URL Keyword Blocking	NBG-418N v2 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.
Add Keyword	Щелкните эту кнопку 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.
Delete Selected Keyword	Щелкните эту кнопку чтобы удалить выбранную запись.
Select	Щелкните чтобы выбрать запись и затем щелкните **Delete Selected Keyword** чтобы удалить ее.
Filtered Keyword	Отображение ключевых слов, которые уже используются для блокировки.

ГЛАВА15
Remote Management (удаленное управление)

15.1 Обзор

В глава посвящена экрану Remote Management.

Примечание: Если вы настраиваете удаленное управление из WAN, то нужно дополнительно настроить правило межсетевого экрана чтобы разрешить доступ к NBG-418N v2 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 NBG-418N v2 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 NBG-418N v2 при конфигурировании из WAN.
- Используйте IP-адрес LAN NBG-418N v2 при конфигурировании из LAN.

15.1.3 Тайм-аут системы

По умолчанию используется тайм-аут системы 5 минут (300 секунд). NBG-418N v2 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 перехода на экран **WWW**.

Иллюстрация 89 Management > Remote MGMT > WWW

В следующей таблице описаны поля этого экрана.

Таблица 56 Management > Remote MGMT > WWW

ПОЛЕ	ОПИСАНИЕ
Enable HTTP from the WAN side	Поставьте галочку в это поле для конфигурирования NBG-418N v2 с помощью HTTP и web-браузера через интерфейст WAN.
Server Port	При необходимости можно менять номер порта сервера **Server port**, но для удаленного управления нужно использовать этот же номер порта.
Secured Client WAN IP Address	**Secured Client** – это проверенный (trusted) компьютер, для которого разрешен доступ к NBG-418N v2 с использованием этого сервиса. Если выбрать **All**, то только у всех компьютеров будет доступ к NBG-418N v2 с использованием этого сервиса. Если выбрать **Selected**, то только у компьютеров с указанным IP-адресом будет доступ к NBG-418N v2 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.

ГЛАВА16
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 7). 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 использования 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 NBG-418N v2 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 90 Management > UPnP > General

В следующей таблице описаны поля этого экрана.

Таблица 57 Management > UPnP > General

ПОЛЕ	ОПИСАНИЕ
Device Name	Описание маршрутизатора NBG-418N v2.
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 NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

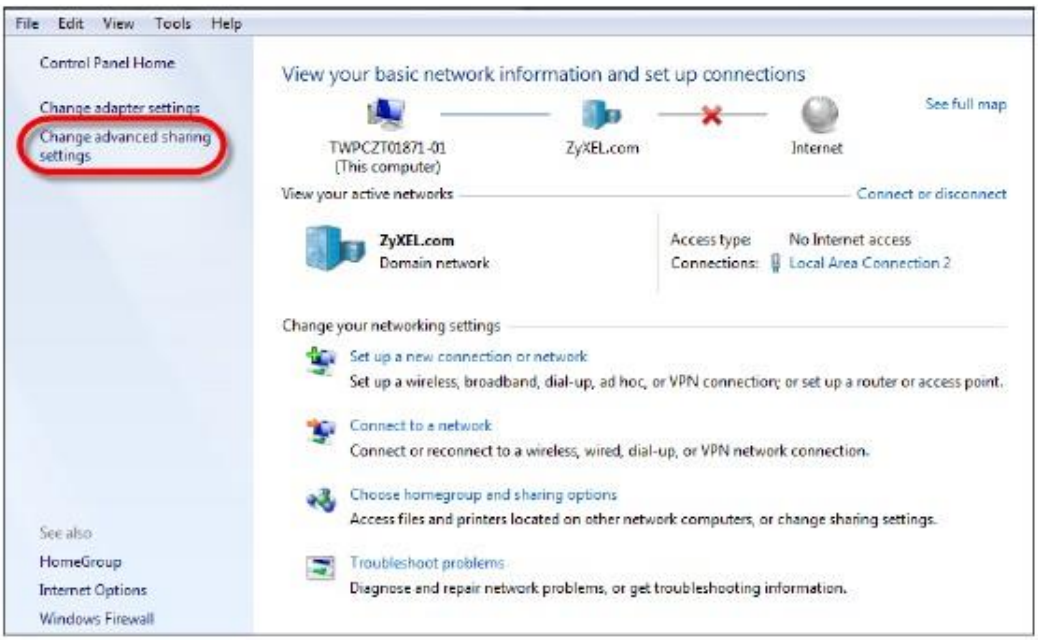
16.4 Пример инсталляции UPnP в Windows 7

В этом примере показано, как можно использовать функцию UPnP в Windows 7. Сервер UPnP инсталлирован в Windows 7. Вам нужно включить UPnP на NBG-418N v2.

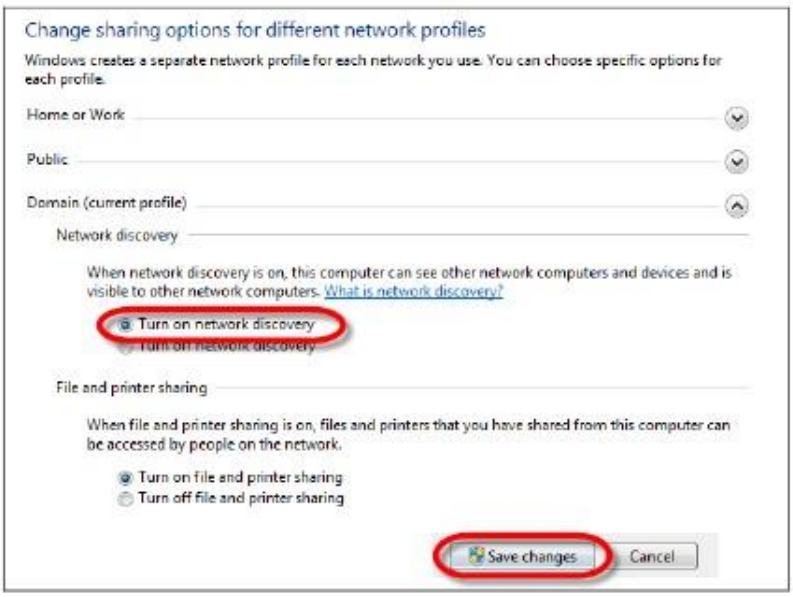
Ваш компьютер должен быть подключен к LAN-порту NBG-418N v2. Включите компьютер и NBG-418N v2.

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 Автоматическое обнаружение в сети устройств, поддерживающих UPnP

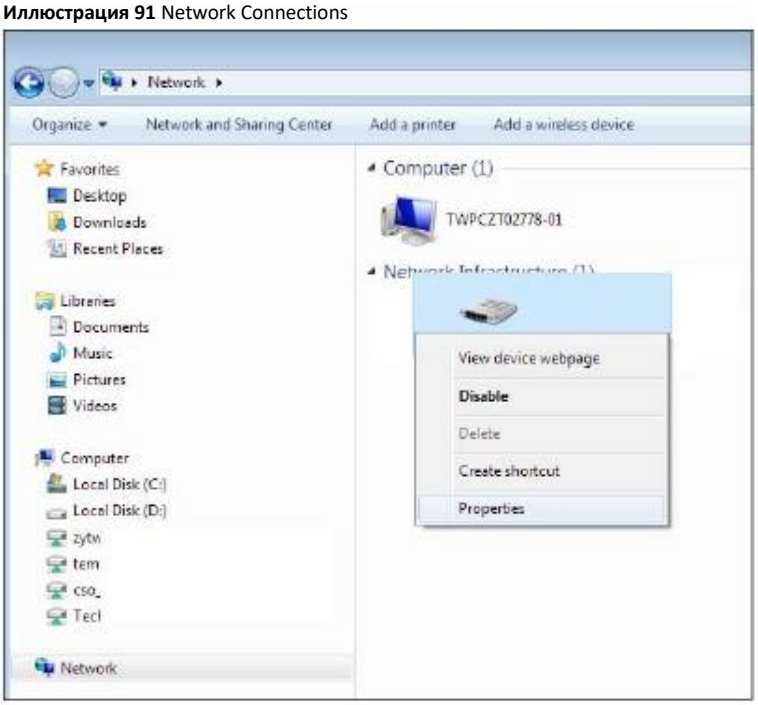
Для выполнения этой процедур нужно включить UPnP на NBG-418N v2 и вашем компьютере.

Компьютер должен быть подключен к порту LAN на NBG-418N v2.

1 Откройте **Windows Explorer** и щелкните **Network**.

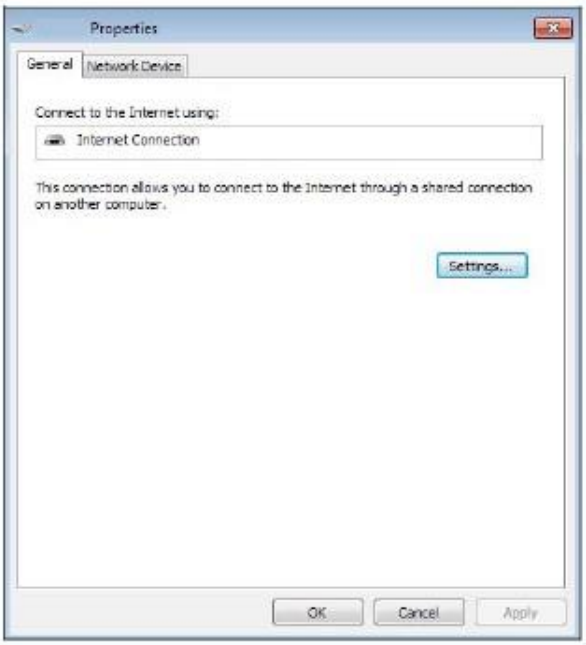
2 Щелкните правой кнопкой пиктограмму NBG-418N v2 и выберите **Properties**.

Иллюстрация 91 Network Connections



3 В окне **Internet Connection Properties** выберите **Settings** чтобы увидеть port mapping.

Иллюстрация 92 Internet Connection Properties



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

Иллюстрация 93 Internet Connection Properties: Advanced Settings

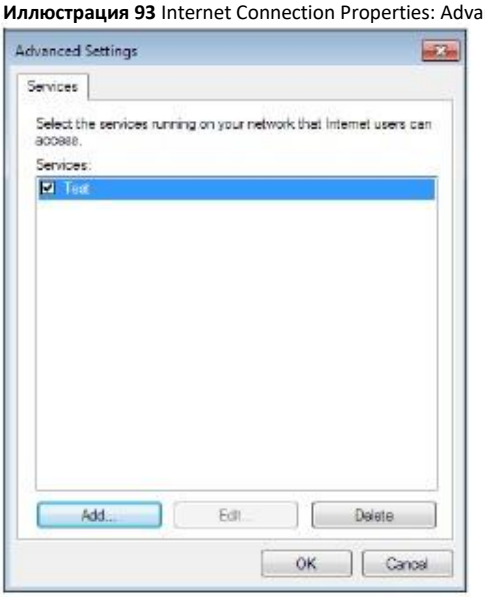
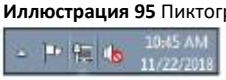


Иллюстрация 94 Internet Connection Properties: Advanced Settings: Add

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

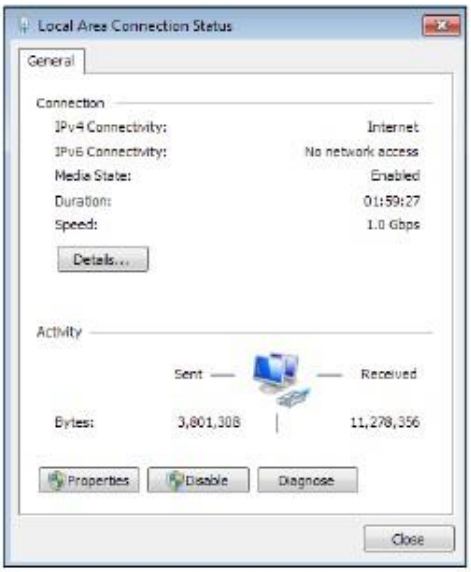
5 Щелкните **OK**. На панели уведомлений должна быть пиктограмма подключения к Интернету.

Иллюстрация 95 Пиктограммы на панели уведомлений



6 Чтобы посмотреть состояния соединения с Интернетом щелкните правой кнопкой пиктограмму параметров сети и щелкните **Open Network and Sharing Center**. Щелкните **Local Area Network**.

Иллюстрация 96 Состояния соединения с Интернетом

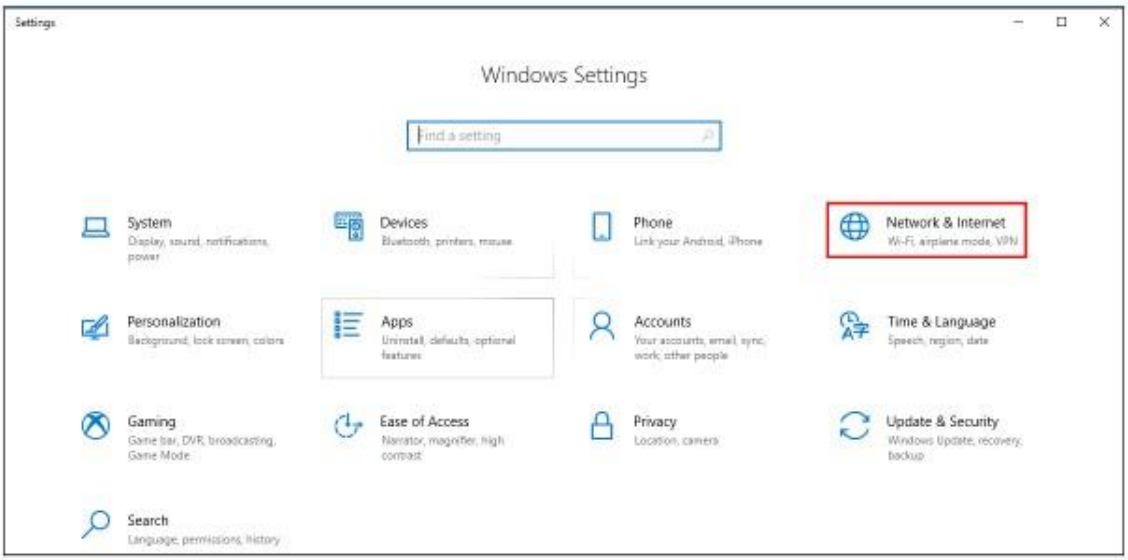


16.5 Пример включения UPnP в Windows 10

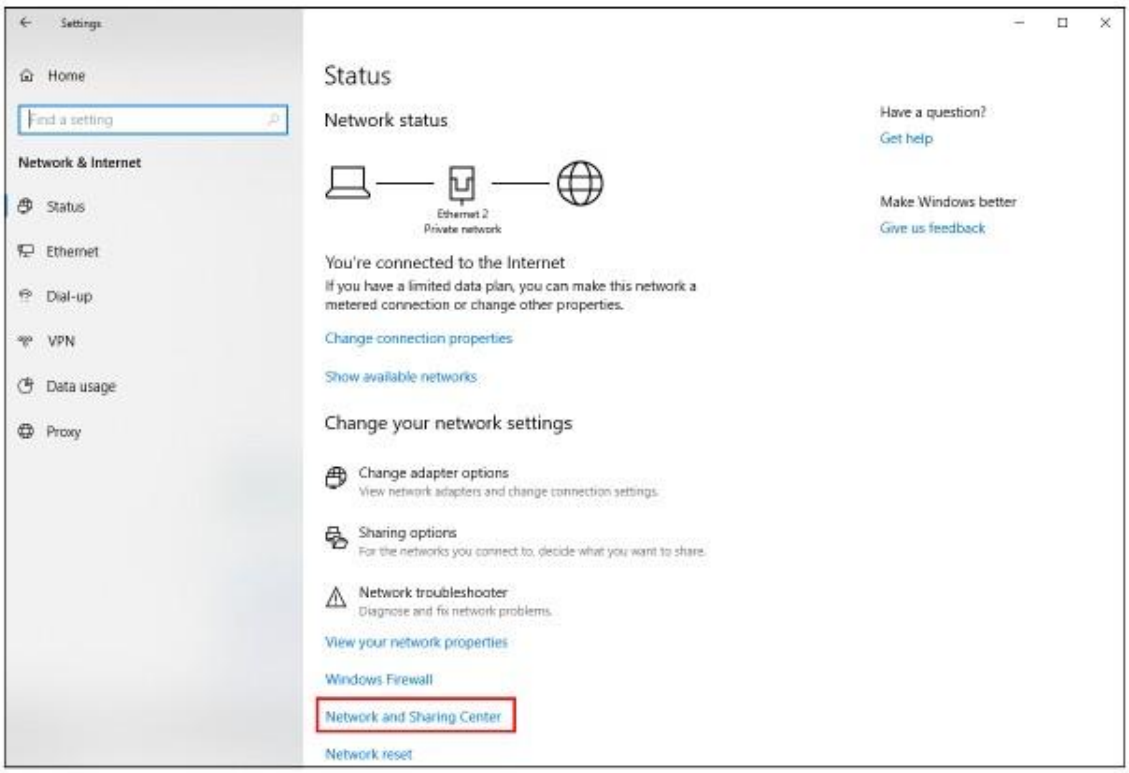
В этом примере показано, как можно использовать функцию UPnP в Windows 10. Сервер UPnP инсталлирован в Windows 10. Для включения UPnP в NBG-418N v2 щелкните **Management > UPnP**.

Ваш компьютер должен быть подключен к LAN-порту NBG-418N v2. Включите компьютер и NBG-418N v2.the NBG-418N v2.

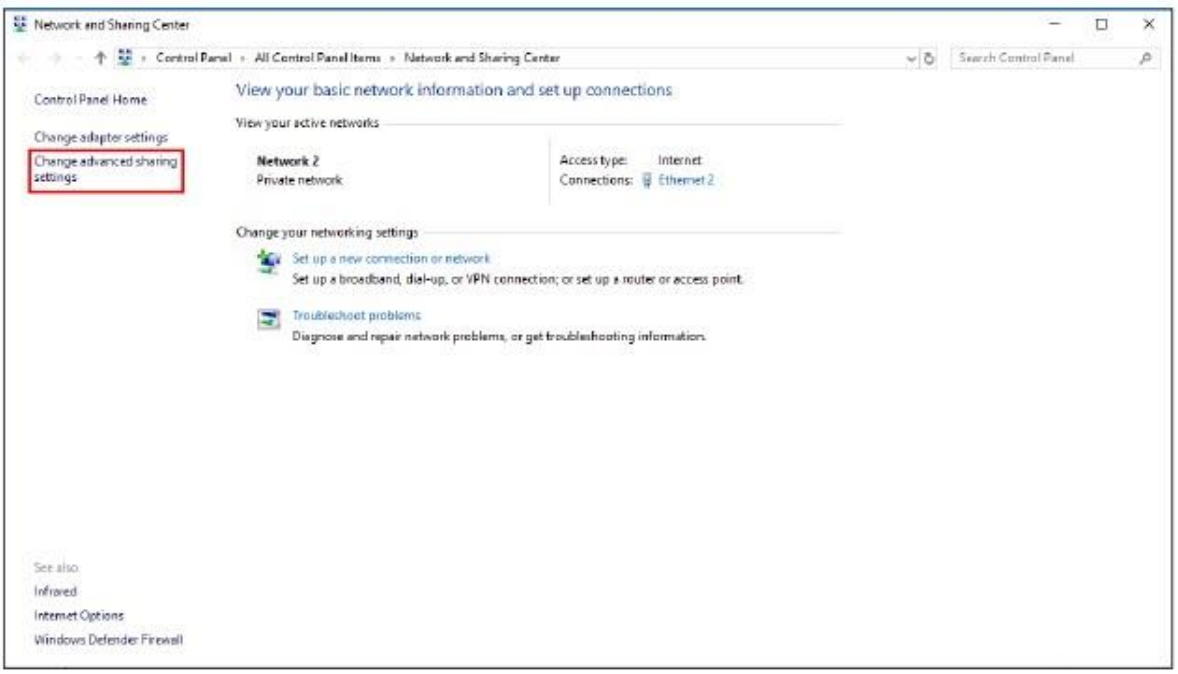
1 Щелкните пиктограмму **Start**, затем, **Settings** и **Network & Internet**.



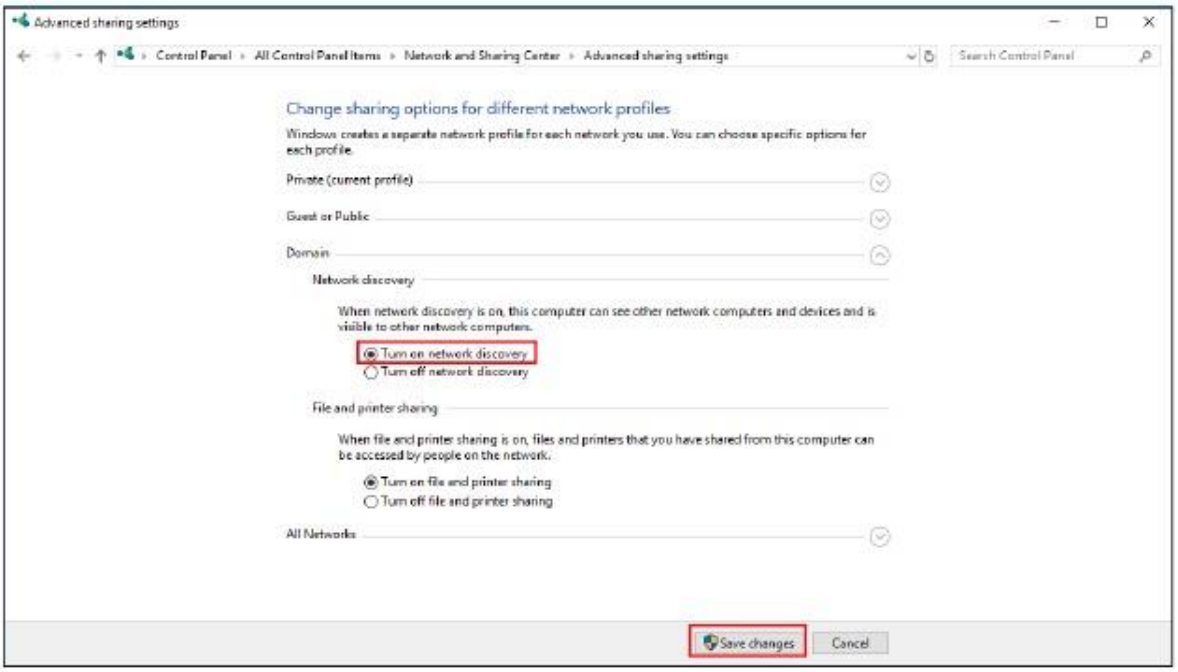
2 Щелкните **Network and Sharing Center**.



3 Щелкните **Change advanced sharing settings**.



4 В разделе **Domain** 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.



16.5.1 Автоматическое обнаружение в сети устройств, поддерживающих UPnP

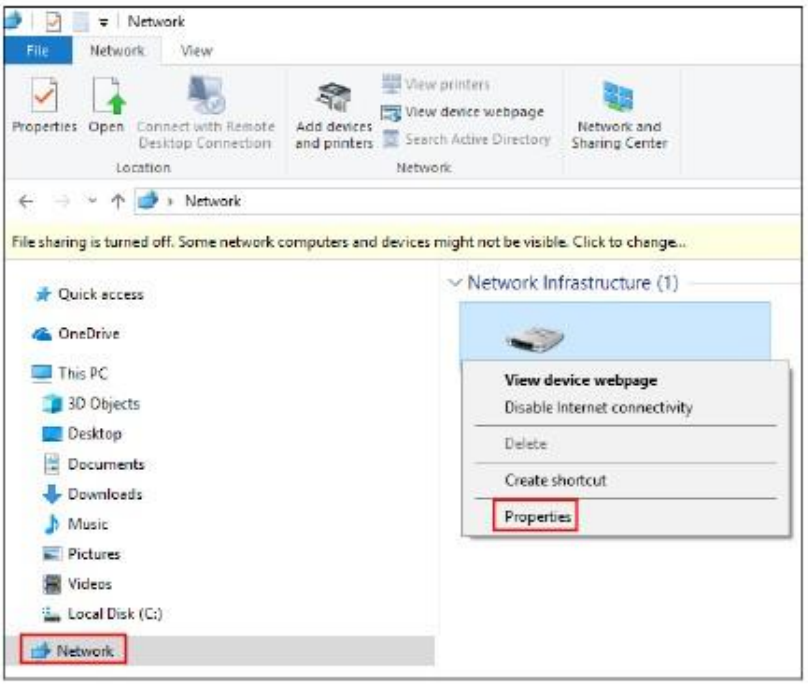
Для выполнения этой процедур нужно включить UPnP на NBG-418N v2 и вашем компьютере.

Компьютер должен быть подключен к порту LAN на NBG-418N v2.

1 Откройте **File Explorer** и щелкните **Network**.

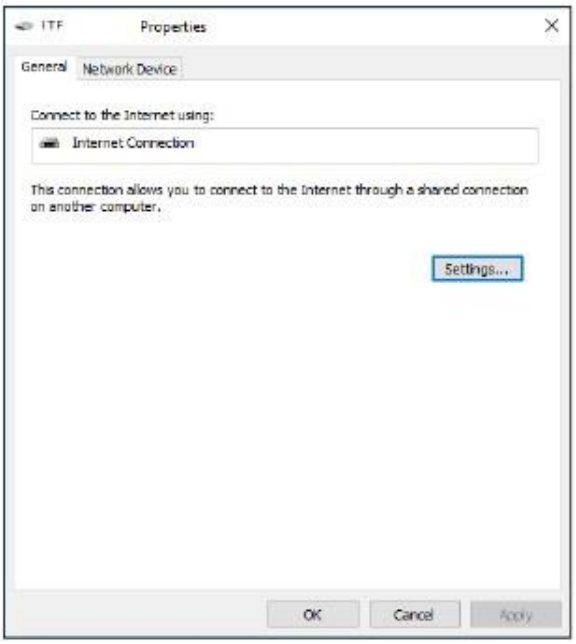
2 Щелкните правой кнопкой пиктограмму NBG-418N v2 и выберите **Properties**.

Иллюстрация 97 Network Connections



3 В окне **Internet Connection Properties** выберите **Settings** чтобы увидеть port mapping.

Иллюстрация 98 Internet Connection Properties



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

Иллюстрация 99 Internet Connection Properties: Advanced Settings

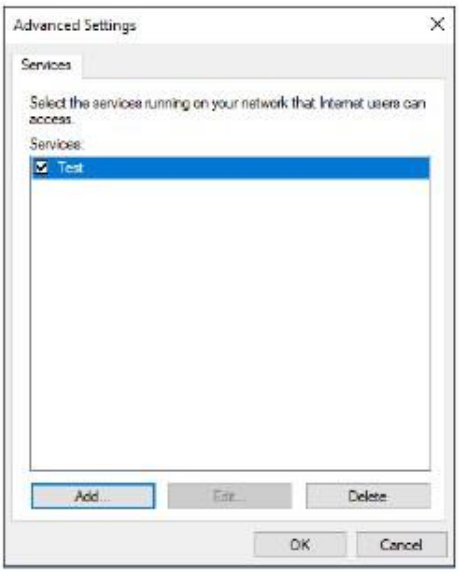
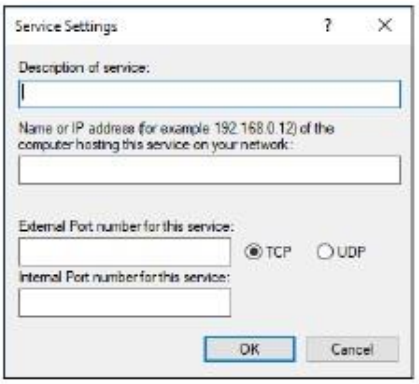


Иллюстрация 100 Internet Connection Properties: Advanced Settings: Add



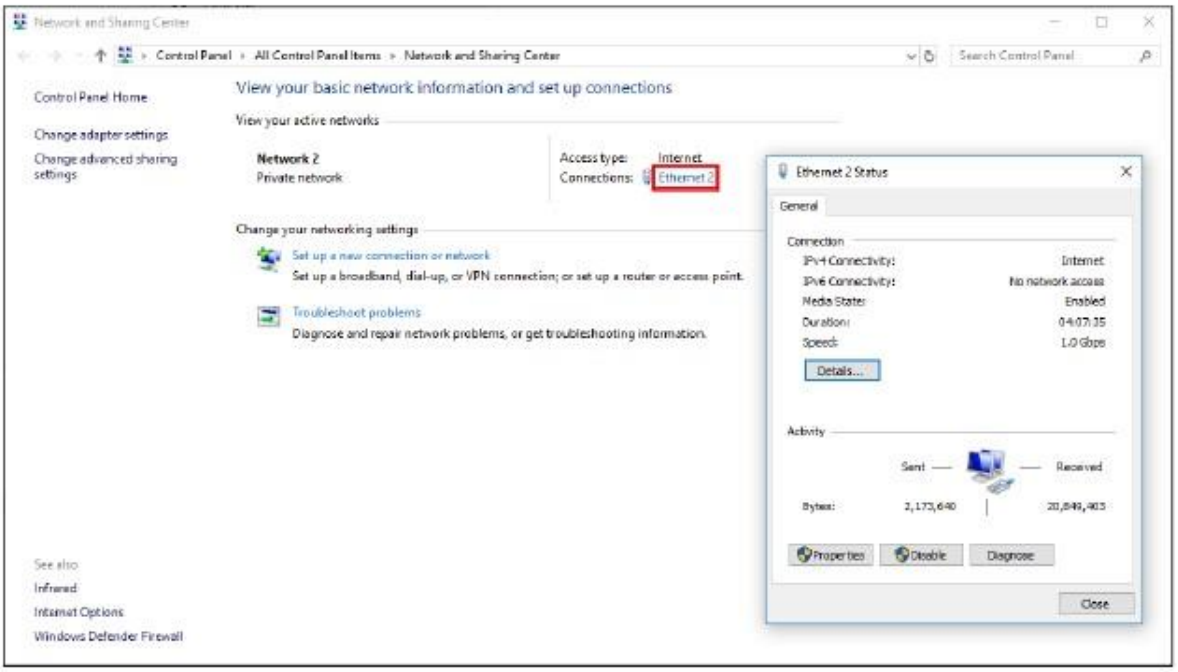
Примечание: При отключении поддерживающих UPnP устройств все port mappings автоматически удаляются.

5 На панели уведомлений должна быть пиктограмма подключения к Интернету

Иллюстрация 101 Пиктограммы на панели уведомлений

6 Чтобы посмотреть состояния соединения с Интернетом щелкните правой кнопкой пиктограмму параметров сети и щелкните **Open Network and Sharing Center**. Щелкните **Connections**.

Иллюстрация 102 Состояния соединения с Интернетом



16.6 Доступ к Web Configurator в Windows 7

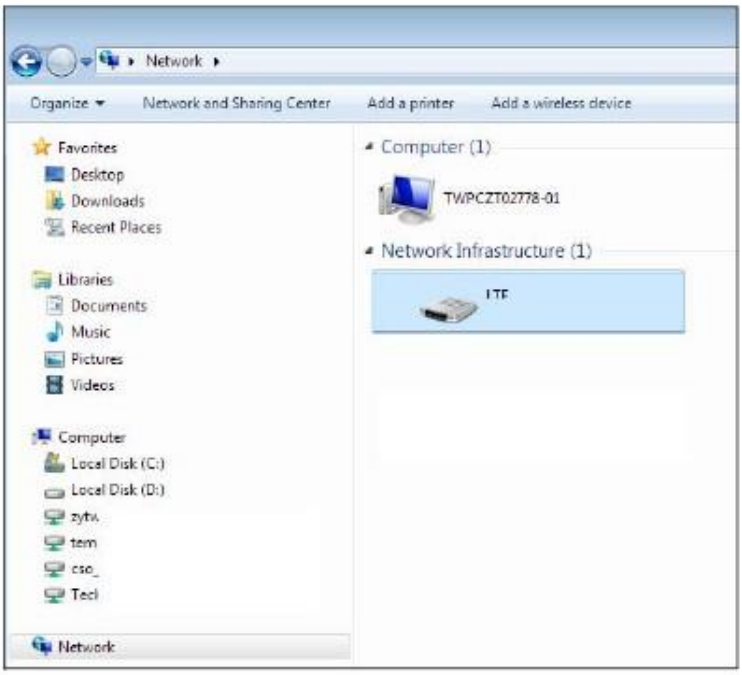
При использовании UPnP можно получить доступ к Web Configurator в NBG-418N v2 даже если вы не знаете IP-адрес NBG-418N v2.

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

1 Откройте Windows Explorer.

2 Щелкните **Network**.

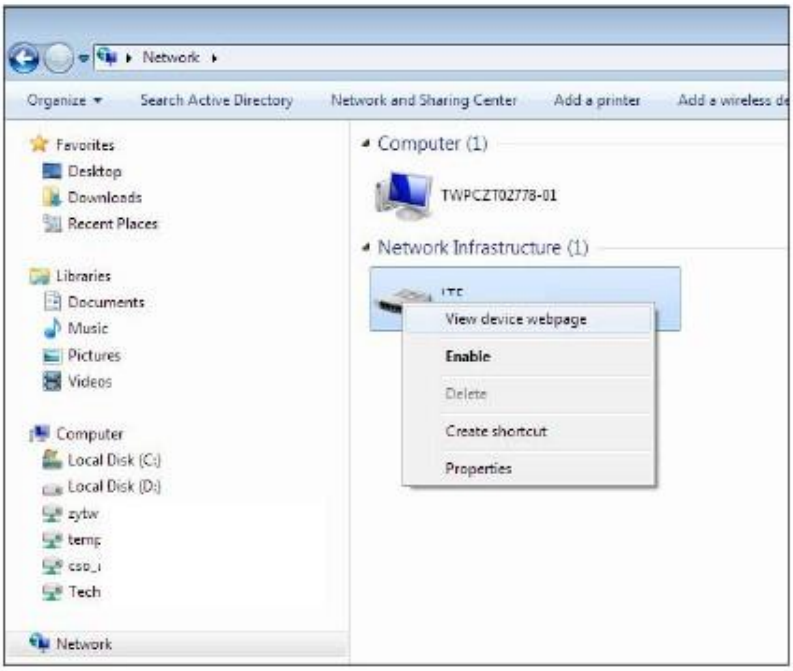
Иллюстрация 103 Network Connections



3 Под **Network Infrastructure** появится пиктограмма с описанием для каждого поддерживающего UPnP устройства.

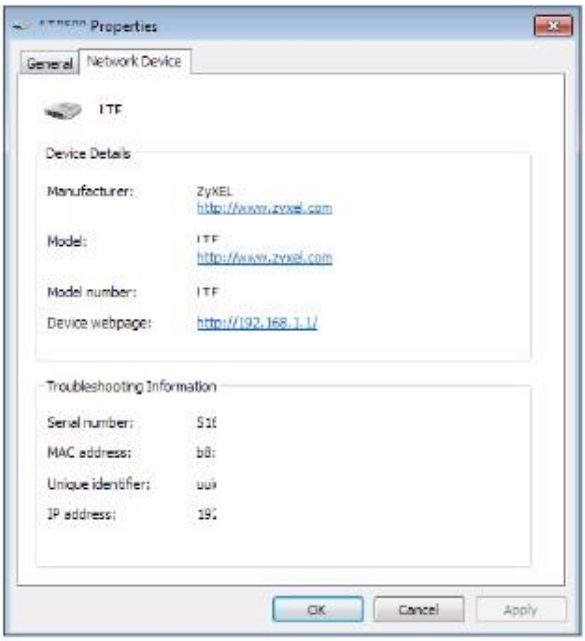
4 Щелкните правой кнопкой пиктограмму вашего NBG-418N v2 и выберите **View device webpage**. Откроется экран входа в Web Configurator.

Иллюстрация 104 Network Connections: My Network Places



5 Щелкните правой кнопкой пиктограмму вашего NBG-418N v2 и выберите **Properties**. Щелкните вкладку Network Device. Откроется окно, в котором выводится основная информация о NBG-418N v2.

Иллюстрация 105 Network Connections: My Network Places: Properties (пример)



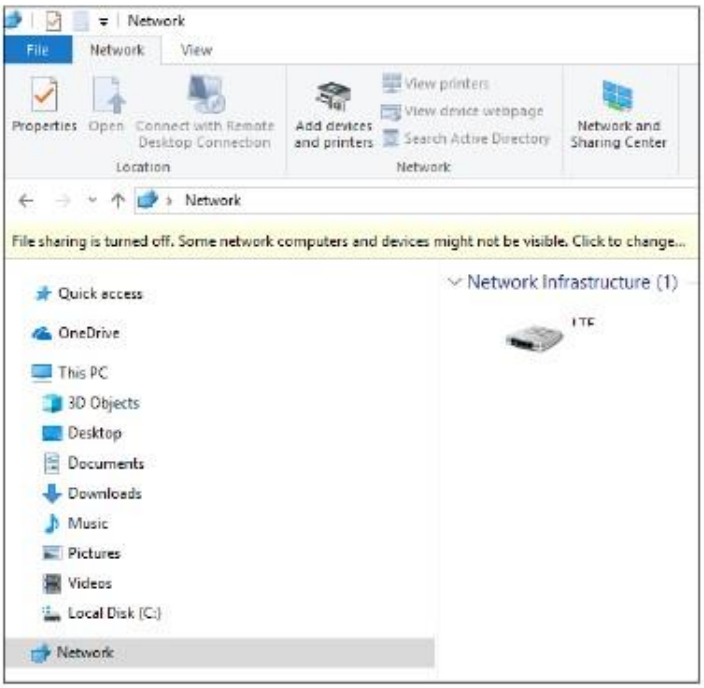
16.7 Доступ к Web Configurator в Windows 10

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

1 Откройте File Explorer.

2 Щелкните Network.

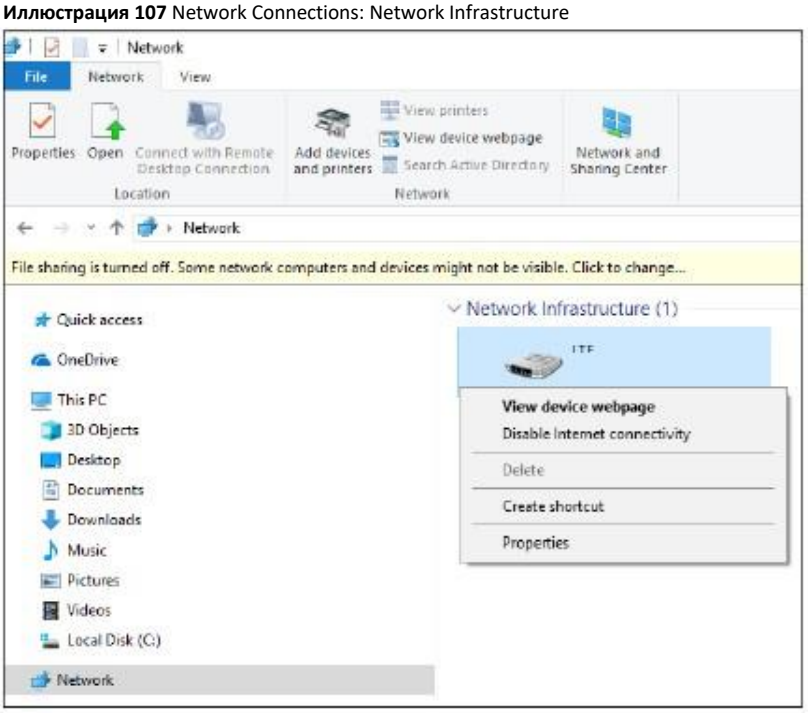
Иллюстрация 106 Network Connections



3 Под **Network Infrastructure** появится пиктограмма с описанием для каждого поддерживающего UPnP устройства.

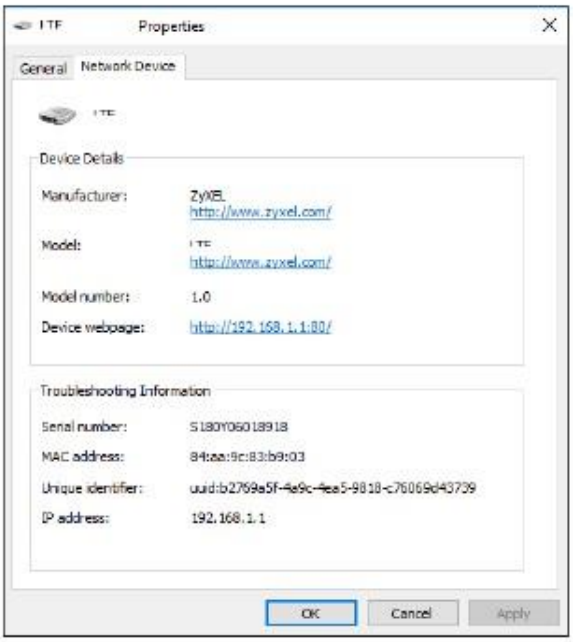
4 Щелкните правой кнопкой пиктограмму вашего NBG-418N v2 и выберите **View device webpage**. Откроется экран входа в Web Configurator

Иллюстрация 107 Network Connections: Network Infrastructure



5 Щелкните правой кнопкой пиктограмму вашего NBG-418N v2 и выберите **Properties**. Щелкните вкладку Network Device. Откроется окно, в котором выводится основная информация о NBG-418N v2.

Иллюстрация 108 Network Connections: Network Infrastructure: Properties (пример)



ГЛАВА17 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 NBG-418N v2.

• Экран **Advanced** для настройки правила QoS (Quality of Service) на NBG-418N v2.

17.3 Основные сведения

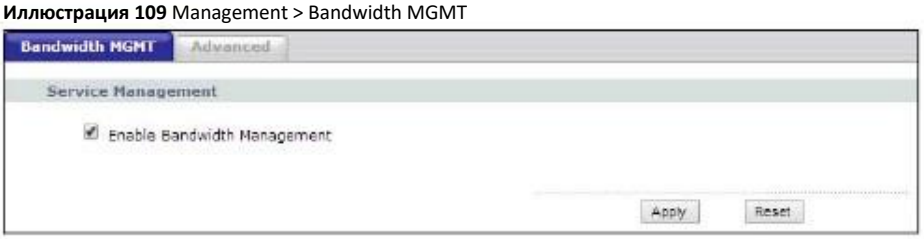
Суммарная полоса пропускания, которая выделяется интерфейсу WAN (от LAN к WAN, от WLAN к WAN) не должна быть больше значения Upstream Bandwidth, которые вы задали на экране Bandwidth Management **Advanced**.

Суммарная полоса пропускания, которая выделяется интерфейсу LAN (от WAN к LAN, от WAN к WLAN) 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 NBG-418N v2. Щелкните **Management > Bandwidth MGMT**. Откроется следующий экран.

Иллюстрация 109 Management > Bandwidth MGMT



В следующей таблице описаны поля этого экрана.

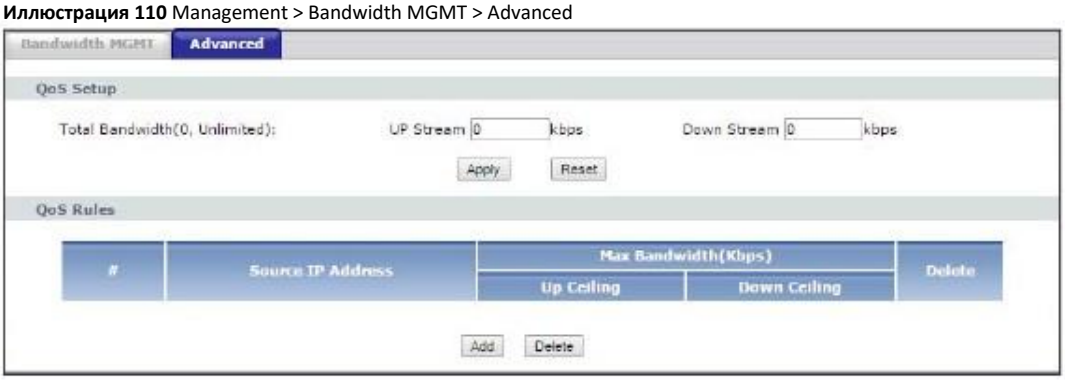
Таблица 58 Management > Bandwidth MGMT > Bandwidth MGMT

ПОЛЕ	ОПИСАНИЕ
Service Management	
Enable Bandwidth Management	Для включения управления полосой пропускания в NBG-418N v2 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 NBG-418N v2. Щелкните **Management > Bandwidth MGMT > Advanced**. Откроется следующий экран.

Иллюстрация 110 Management > Bandwidth MGMT > Advanced



В следующей таблице описаны поля этого экрана.

Таблица 59 Management > Bandwidth MGMT > Advanced

ПОЛЕ	ОПИСАНИЕ
QoS Setup	
Total Bandwidth (0, Unlimited)	Максимальный объем данных (в килобайтах), который NBG-418N v2 может послать и получить через интерфейс-источник.
Up Stream	Введите **Up Stream** или максимальную скорость исходящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG-418N v2.
Down Stream	Введите **Down Stream** или максимальную скорость входящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG-418N v2.
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.
QoS Rules	
#	Номер правила QoS.
Source IP Address	IP-адрес источника данных.
Max Bandwidth (kbps)	
Up Ceiling	Максимальная скорость входящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG-418N v2.

Таблица 59 Management > Bandwidth MGMT > Advanced (продолжение)

ПОЛЕ	ОПИСАНИЕ
Down Ceiling	Максимальная скорость исходящего потока данных (в кбит/сек), которая разрешена для интерфейса-источника NBG-418N v2.
Delete	Поставьте галочку в **Delete** чтобы отметить правило QoS, которое нужно удалить.
Add	Щелкните **Select All** для выбора всех правил.
Delete	Щелкните **Delete** для удаления правила QoS.

ГЛАВА18
System

18.1 Обзор

В этой главе описаны экраны System.

Дополнительная информация об этих экранах дается в главе о визарде настройки.

18.2 Экраны, которые описаны в этой главе

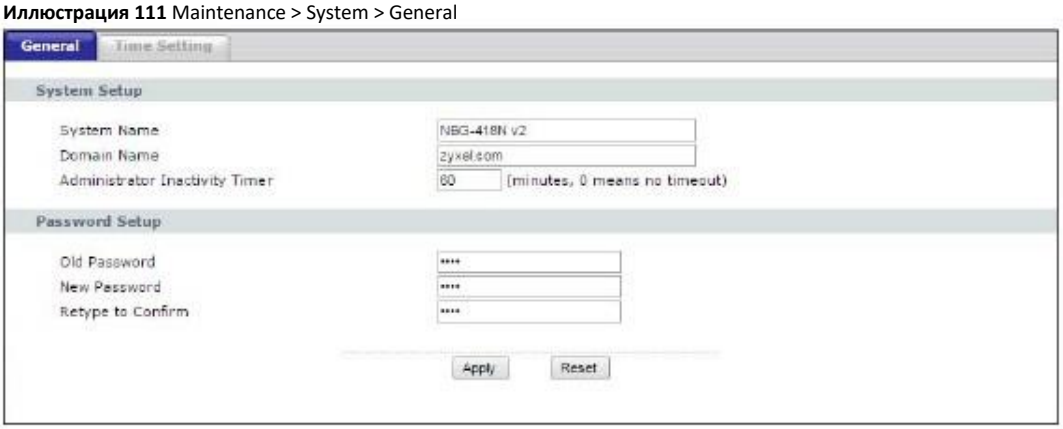
• **General** для ввода имени, по которому можно найти NBG-418N v2 в сети, и пароля (Раздел 18.3 на стр. 146).

• Экран **Time Setting** для изменения времени и даты на часах NBG-418N v2 (Раздел 18.4 на стр. 147).

18.3 Экран General

Этот экран используется для ввода имени, по которому можно найти NBG-418N v2 в сети, и пароля. Щелкните **Maintenance > System**. Откроется следующий экран.

Иллюстрация 111 Maintenance > System > General



В следующей таблице описаны поля этого экрана.

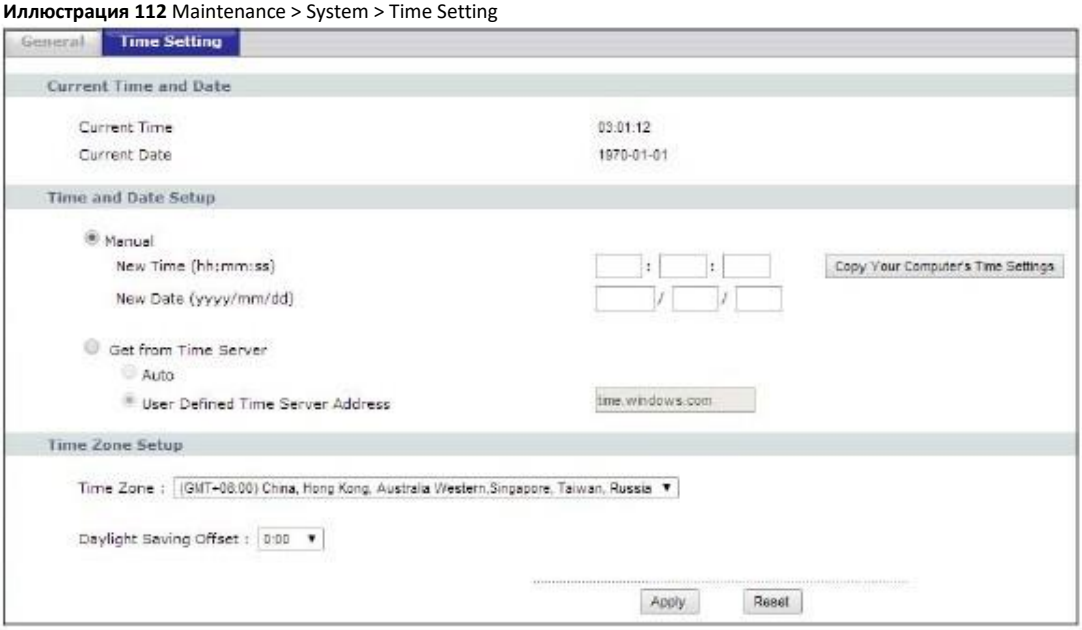
Таблица 60 Maintenance > System > General

ПОЛЕ	ОПИСАНИЕ
System Setup	
System Name	**System Name** – это уникальное имя NBG-418N v2 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 NBG-418N v2 (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 изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

18.4 Экран Time Setting

Если нужно изменить время и дату на часах NBG-418N v2, то щелкните **Maintenance > System > Time Setting**. Откроется следующий экран, на котором можно настроить часы NBG-418N v2 с учетом часового пояса.

Иллюстрация 112 Maintenance > System > Time Setting



В следующей таблице описаны поля этого экрана.

Таблица 61 Maintenance > System > Time Setting

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	Текущее время часов NBG-418N v2. При каждой перезагрузке этой страницы NBG-418N v2 синхронизирует свои часы с сервером точного времени.
Current Date	Текущая дата NBG-418N v2. При каждой перезагрузке этой страницы NBG-418N v2 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. manually. Если вы в **Time and Date Setup** выбрали **Manual**, то в это поле нужно ввести новую дату и щелкнуть **Apply**.
New Date (yyyy/mm/dd)	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 NBG-418N v2 настройки даты и времени вашего компьютера.
Get from Time Server	Если выбрать **Get from time Server**, то NBG-418N v2 будет синхронизировать свои часы с указанным ниже сервером точного времени.
Auto	Если выбрать **Auto**, то NBG-418N v2 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).
Daylight Savings Offset	**Daylight Saving** – 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 NBG-418N v2 будут переводиться на летнее время
Apply	Щелкните **Apply** для сохранения изменений на NBG-418N v2.
Reset	Щелкните **Reset** для настройки этого экрана с самого начала.

ГЛАВА19 Logs (журналы событий)

19.1 Обзор

В этой главе описывается настройка параметров журнала событий NBG-418N v2 и просмотр этого журнала.

В Web Configurator можно просматривать все журналы событий NBG-418N v2.

19.2 Что нужно знать

В этой главе используются следующие термины и концепции:

Алерты и логи

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).

Обзор Syslog

С помощью протокола syslog устройства посылают сообщения о событиях через сеть IP серверам syslog, которые собирают такие сообщения. Поддерживающее syslog устройство может генерировать сообщение syslog и передавать его серверу syslog.

Протокол Syslog описан в стандарте RFC 3164, включая формат пакетов, их содержание и информацию из логов, которая передается в сообщениях syslog. Syslog facility идентифицирует файл на сервере syslog (подробнее см. документацию к вашей программе syslog). В следующей таблице описаны уровни важности сообщений Syslog (Syslog Severity Levels).

Таблица 62 Syslog Severity Levels

КОД	SEVERITY
0	Emergency: Систему нельзя использовать.
1	Alert: Необходимо немедленно предпринять действия.
2	Critical: Критичное состояние системы.
3	Error: Ошибка в системе.
4	Warning: Предупреждение о состоянии системы.
5	Notice: Система работает нормально.

Таблица 62 Syslog Severity Levels

КОД	SEVERITY
6	Informational: Информационное сообщение syslog.
7	Debug: Сообщение для отладки.

Алерты сразу же передаются по email после их возникновения. Логи могут передавать по email после полного заполнения журнала (см. Log Schedule). Если выбрать много категорий алертов и/или логов, то будет пересылаться много писем email.

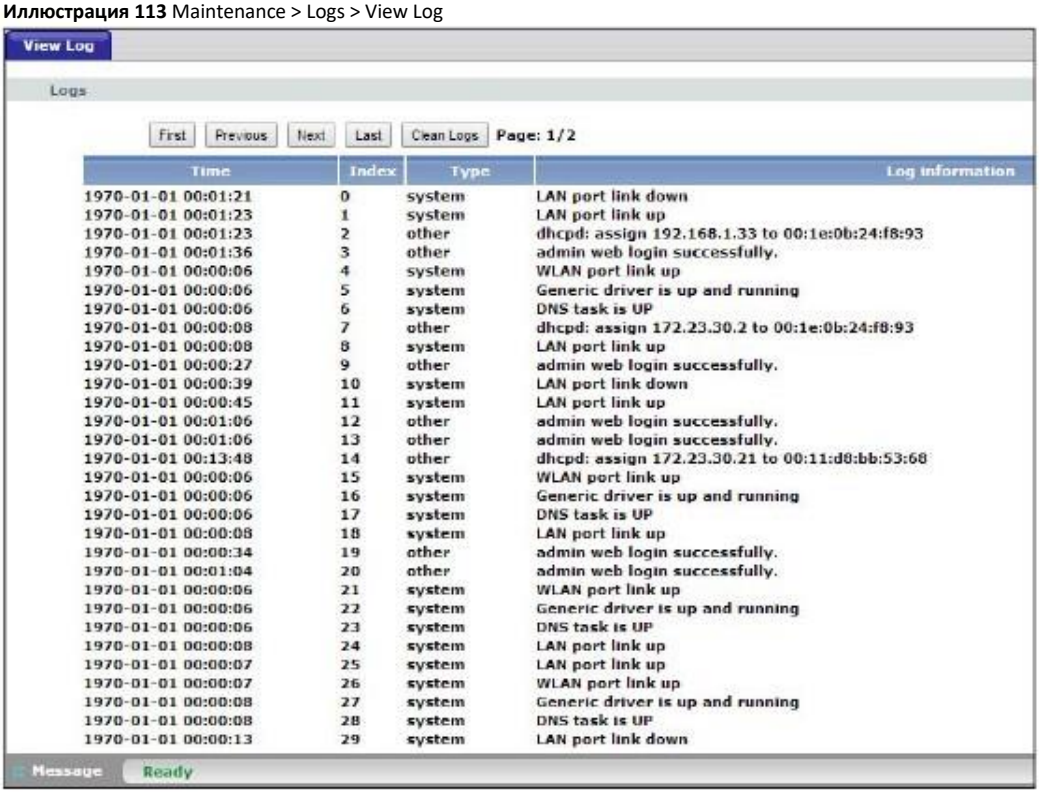
19.3 Экран View Log

На экране **View Log** выводятся внесенные в журнал событий сообщения о NBG-418N v2. 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 113 Maintenance > Logs > View Log



В следующей таблице описаны поля этого экрана.

Таблица 63 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

Таблица 63 Maintenance > Logs > View Log (продолжение)

ПОЛЕ	ОПИСАНИЕ
Next	Щелкните кнопку **Next** чтобы перейти на следующую страницу журнала событий.
Last	Щелкните кнопку **Last** чтобы перейти на последнюю страницу журнала событий.
Clear 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.

ГЛАВА20
Tools (утилиты)

20.1 Обзор

В этой главе объясняется, как загрузить новую прошивку, сделать резервную копию конфигурационных файлов и загрузить их на устройства, перезагрузить NBG-418N v2.

20.2 Экраны, которые описаны в этой главе

• Экран **Firmware** для загрузки прошивки на NBG-418N v2 (Раздел 20.3 на стр. 152).

• Экран **Configuration** для просмотра заводских настроек по умолчанию, конфигурации резервного копирования и восстановления (Раздел 20.4 на стр. 154).

• Экран **Restart** для перезагрузки NBG-418N v2 (Раздел 20.5 на стр. 155).

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 “NBG-418N v2.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 NBG-418N v2.

Иллюстрация 114 Maintenance > Tools > Firmware

В следующей таблице описаны поля этого экрана.

Таблица 64 Maintenance > Tools > Firmware

ПОЛЕ	ОПИСАНИЕ
Choose File	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 NBG-418N v2 автоматически выполнил перезагрузку после завершения загрузки прошивки.
Upload	Щелкните **Upload** чтобы начать загрузку (она занимает до 2 минут).
Check for Latest Firmware Now	Щелкните кнопку **Check for Latest Firmware Now** чтобы NBG-418N v2 нашел новейшую версию прошивки на web-сайте Zyxel.

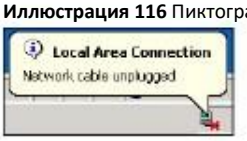
Примечание: Нельзя выключать NBG-418N v2 во время загрузки прошивки!

После того, как на экране появится надпись **Firmware Upload In Process**, нужно подождать несколько минут и снова зайти на NBG-418N v2.

Иллюстрация 115 Предупреждение о загрузке

При автоматической перезагрузке NBG-418N v2 на какое-то время будет разорвано сетевое соединение. В некоторых операционных системах при этом на рабочем столе компьютера появится такая пиктограмма.

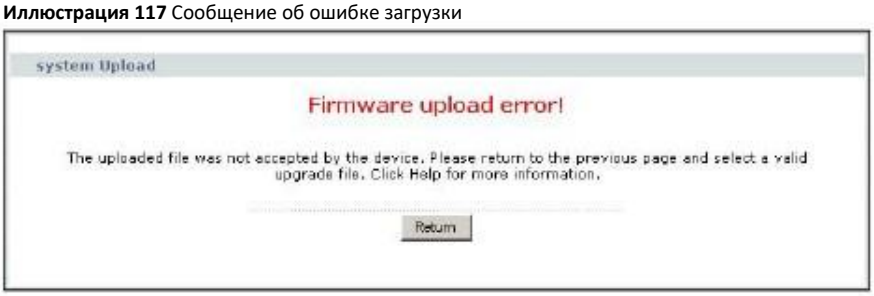
Иллюстрация 116 Пиктограмма о недоступности сети



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**.

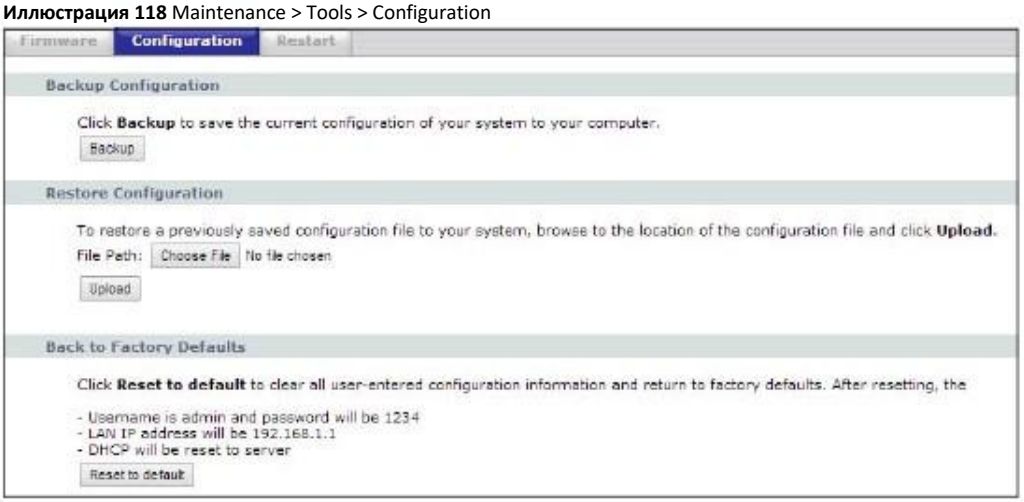
Иллюстрация 117 Сообщение об ошибке загрузки



20.4 Экран Configuration

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

Иллюстрация 118 Maintenance > Tools > Configuration



20.4.1 Backup Configuration (резервное копирование конфигурации)

При резервном копировании вы сохраняете копию текущей конфигурации NBG-418N v2 на вашем компьютере. Перед любым изменением конфигурации NBG-418N v2 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 NBG-418N v2.

20.4.2 Restore Configuration (восстановление конфигурации)

Restore configuration используется для загрузки на NBG-418N v2 новой или ранее сохраненной конфигурации, записанной на вашем компьютере.

Таблица 65 Maintenance Restore Configuration

ПОЛЕ	ОПИСАНИЕ
Choose File	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 NBG-418N v2 во время загрузки конфигурационного файла.

После того, как на экране появится надпись “configuration upload successful”, нужно подождать 1 минуту и снова зайти на NBG-418N v2.

Иллюстрация 119 Успешно выполнено восстановление конфигурации

При автоматической перезагрузке NBG-418N v2 на какое-то время будет разорвано сетевое соединение. В некоторых операционных системах при этом на экране компьютера появится такая пиктограмма.

Иллюстрация 120 Пиктограмма о временной недоступности сети

После загрузки файла конфигурации NBG-418N v2 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 D на стр. 190.

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

Иллюстрация 121 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 NBG-418N v2 по умолчанию.

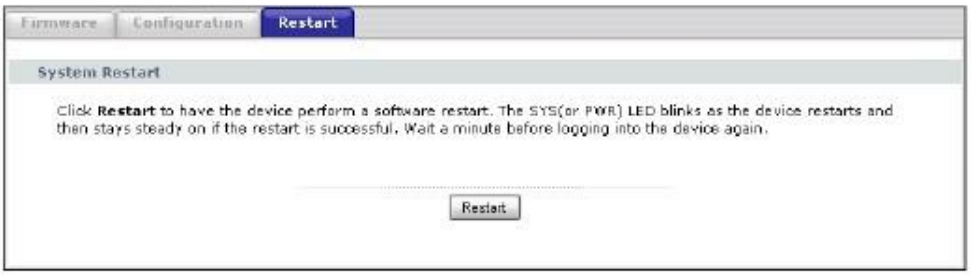
Также для сброса настроек можно нажать кнопку **WPS/RESET** на задней панели NBG-418N v2 (о кнопке **WPS/RESET** см. Раздел 1.4.1 на стр. 15).

20.5 Экран Restart

При использовании Restart перезагрузка NBG-418N v2 выполняет без выключения питания.

Щелкните **Maintenance > Tools > Restart**. Щелкните **Restart** для перезагрузки NBG-418N v2. При перезагрузке конфигурация NBG-418N v2 не меняется.

Иллюстрация 122 Maintenance > Tools > Restart



ГЛАВА21
Sys OP Mode

21.1 Обзор

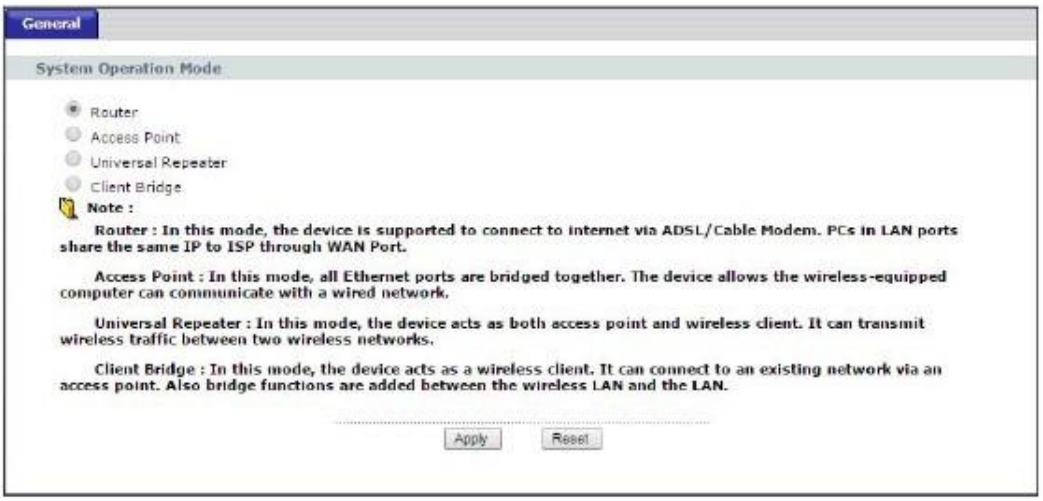
Функция Sys OP Mode (System Operation Mode) позволяет задавать режим работы устройства: маршрутизатор, точка доступа или универсальный повторитель.

См. Глава 4 на стр. 30 о выборе режима работы.

21.2 Экран General

На этом экран выводится информация о вашем подключении к Интернету.

Иллюстрация 123 Maintenance > Sys OP Mode > General



В следующей таблице описаны поля экрана General.

Таблица 66 Maintenance > Sys Op Mode > General

ПОЛЕ	ОПИСАНИЕ
System Operation Mode	
Router	Выберите режим **Router** если вы хотите использовать такие функции маршрутизации NBG-418N v2 (N), как LAN DHCP, NAT, межсетевой экран и т.п. NBG-418N v2 разделяет IP-адреса сетей 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.
Universal Repeater	Выберите режим **Universal Repeater** если в вашей сети уже есть маршрутизатор беспроводной сети или точка доступа и нужно, чтобы NBG-418N v2 ретранслировал по беспроводной сети трафик от этого устройства.

Таблица 66 Maintenance > Sys Op Mode > General (продолжение)

ПОЛЕ	ОПИСАНИЕ
Client Bridge	Выберите режим **Client Bridge** если вашему устройству нужен беспроводной клиент чтобы подключиться к уже имеющейся точке доступа.
Apply	Щелкните **Apply** для сохранения ваших настроек.
Reset	Щелкните **Reset** для возврата к предыдущим настройкам этого экрана.

Если выбрать режим маршрутизатора Router mode, то появится следующее всплывающее сообщение.

Иллюстрация 124 Maintenance > Sys Op Mode > General: Router

• 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 NBG-418N v2 установлен в 192.168.1.1.

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

If you select a non-router mode (Access Point, Universal Repeater or Client Bridge) the following pop-up message window appears.

Иллюстрация 125 Maintenance > Sys Op Mode > General: Non-Router

• В режиме «не-маршрутизатора (non-router) у всех портов Ethernet один и тот же адрес IP.

• 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 NBG-418N v2 установлен в 192.168.1.2.

ГЛАВА22
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 NBG-418N v2.

Иллюстрация 126 Экран Language

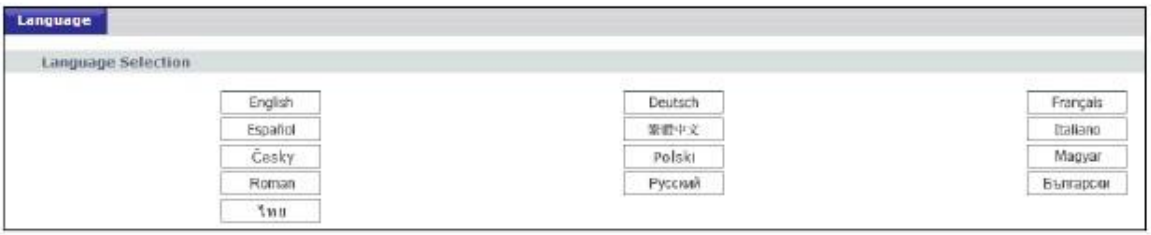


Иллюстрация 127 Пример изменения языка

ГЛАВА 23
Устранение неисправностей

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

23.1 Питание, подключение оборудования и светодиоды

NBG-418N v2 не включается, все светодиоды не горят.

1. Убедитесь, что NBG-418N v2 включен.
2. Убедитесь, что вы используете адаптер питания или силовой кабель, который поставляются вместе с NBG-418N v2.
3. Убедитесь, что адаптер питания подключен к NBG-418N v2 и розетка, в которую вставлена его вилка, не обесточена.
4. Отключите и снова подключите адаптер питания к NBG-418N v2.
5. 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. 14.
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 NBG-418N v2.

5 Если проблему не удалось устранить, то обратитесь в техническую поддержку производителя.

23.2 Доступ к NBG-418N v2 и вход в систему

Я не знаю IP-адрес NBG-418N v2.

1 По умолчанию web-адрес в режиме маршрутизатора http://myrouter.

2 По умолчанию IP-адрес в режиме маршрутизатора 192.168.212.1, а в режиме non-router - 192.168.1.2.

3 Если вы изменили IP-адрес и забыли его, то узнать IP-адрес NBG-418N v2 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 NBG-418N v2 (это зависит от конкретной конфигурации сети). Попробуйте ввести IP-адрес **Default Gateway** в адресную строку браузера.

4 Если это не поможет, то сбросьте NBG-418N v2 в настройки по умолчанию (см. Раздел 23.4 на стр. 163). 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. 163.

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 NBG-418N v2».

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 С на стр. 182.

4 Убедитесь, что ваш компьютер в одной под сети с NBG-418N v2 (если ваш компьютер подключен к NBG-418N v2 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 NBG-418N v2.

5 Сбросьте устройство в заводские настройки по умолчанию и попробуйте зайти на NBG-418N v2 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

• Убедитесь, что не остались открытыми ни одна из предыдущий сессий управления, в которую вы вошли под той же учетной записью пользователя даже если при этом использовались другой интерфейс или браузер.

• 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 NBG-418N v2.

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 NBG-418N v2.

4 Если проблему не удалось решить, то попробуйте сбросить устройство в заводские настройки по умолчанию. См. Раздел 23.4 на стр. 163.

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 подключаться к Интернету через NBG-418N v2.

1 Проверьте соединение оборудования и индикацию светодиодов. См. «Инструкции по подготовке к эксплуатации» (Quick Start Guide) и Раздел 1.3 на стр. 14.

2 Перезагрузите NBG-418N v2.

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

Соединение с Интернетом работает очень медленно или часто прерывается.

1 Возможно, сеть перегружена трафиком. Попробуйте по светодиодам (см. Раздел 1.3 на стр. 14) определить интенсивность трафика, который идет через NBG-418N v2, и закройте часть приложений, использующих Интернет, прежде всего приложения peer-to-peer.

2 Проверьте мощность сигнала. Если он слабый, то переместите NBG-418N v2 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 NBG-418N v2.

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

23.4 Сброс NBG-418N v2 в заводские настройки по умолчанию

Если вы сбросите настройки NBG-418N v2, то все ваши настройки будут потеряны и NBG-418N v2 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 NBG-418N v2 нужно:

1 Убедитесь, что горит светодиод Power.

2 Нажмите кнопку WPS/RESET и отпустите ее не ранее чем через 10 секунд. Будут восстановлены заводские настройки по умолчанию NBG-418N v2.

Если NBG-418N v2 автоматически перезапустится, то дождитесь окончания перезагрузки NBG-418N v2 и зайдите в Web Configurator. Имя пользователя **admin** и пароль **1234**.

Если NBG-418N v2 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 NBG-418N v2 или ping не проходит ни на один компьютер в WLAN.

1 Убедитесь, что на NBG-418N v2 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 NBG-418N v2.

4 Убедитесь, что компьютер находится в зоне покрытия NBG-418N v2.

5 Убедитесь, что компьютер использует те же настройки безопасности беспроводной сети, что и NBG-418N v2.

6 Убедитесь, что межсетевой экран NBG-418N v2 не блокирует трафик между WLAN и LAN.

7 Убедитесь, что не заблокирован удаленный доступ к NBG-418N v2 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 не-маршрутизатора у меня нет доступа к Web Configurator.

При переключении из режима маршрутизатора в режим не-маршрутизатора нужно вручную назначить вашему компьютеру IP-адрес в диапазоне от 192.168.1.3 до 192.168.1.254 (в режиме точки доступа NBG-418N v2 не работает как DHCP-сервер LAN).

Изменение IP-адреса компьютера описано в Приложении D на стр. 190.

Из-за чего плохо работает беспроводная сеть? Как мне решить эту проблему?

Помехи могут возникнуть из-за:

• Препятствий: стен, потолков, мебели и т.п.

• Материалов конструкции здания: металлических дверей, алюминиевых штифтов и т.п.

• Электрических устройств: печей СВЧ, мониторов, электромоторов, беспроводных телефонов и других беспроводных устройств.

Для улучшения скорости и стабильности беспроводного соединения следует:

• Если сигнал слабый, то переставить ваше беспроводное устройство ближе к точке доступа.

• Уменьшить помехи от соседних беспроводных сетей или устройств, например, беспроводных телефонов
.

• Установить точку доступа в зоне прямой видимости беспроводного клиента, например, на стене или потолке.

• Уменьшить число беспроводных клиентов, которые одновременно подключены к точке доступа либо установить дополнительную точку доступа.

• Попробовать закрыть часть интенсивно использующих Интернет программ, прежде всего peer-to-peer.

Что такое Server Set ID (SSID)?

SSID – это уникальное имя беспроводной сети. В одной беспроводной сети у точки доступа и клиентов должен быть одинаковый SSID.

23.6 UPnP

Я использую UPnP и NBG-418N v2 перезагрузился, мой компьютер не видит UPnP и не может обновить My Network Places > Local Network.

1 Проверьте, включен ли UPnP на вашем компьютере (для Windows 7 см. Раздел 16.4 на стр. 129., для Windows 10 - Раздел 16.5 на стр. 133.

2 Убедитесь, что UPnP включен на экране Network Settings > Home Networking > UPnP. См. Раздел 16.3 на стр. 129.

3 Отсоедините кабель Ethernet от порта LAN на NBG-418N v2 или от вашего компьютера.

4 Заново подсоедините кабель Ethernet.

На экране нет пиктограммы Local Area Connection для UPnP.

Перезапустите ваш компьютер.

ПРИЛОЖЕНИЕ A

Поддержка клиентов

Если у вас возникнет какая-то проблема и вы не можете найти ее решение в этой руководстве, то следует обратиться в сервисную службу либо в местное представительство Zyxel в том регионе, где вы приобрели ваше устройство.

См. https://www.zyxel.com/homepage.shtml и https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml.

При обращении в офис от вас потребуется следующая информация.

Требуемая информация

- Модель и серийный номер продукта.
- Информация о гарантии.
- Когда вы купили устройство.
- Общее описание проблемы и как вы пытались ее устранить.

Корпоративная штаб-квартира (всемирная)

Тайвань

- Zyxel Communications Corporation
- https://www.zyxel.com

Азия

Китай

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

Индия

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Казахстан

- Zyxel Kazakhstan
- https://www.zyxel.kz

Корея

- Zyxel Korea Corp.
- http://www.zyxel.kr

Малайзия

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Пакистан

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Филиппины

- Zyxel Philippines
- http://www.zyxel.com.ph

Сингапур

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Тайвань

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Таиланд

- Zyxel Thailand Co., Ltd
- https://www.zyxel.com/th/th/

Вьетнам

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Европа

Беларусь

- Zyxel BY
- https://www.zyxel.by

Бельгия

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

• https://www.zyxel.com/be/fr/

Болгария

• Zyxel България

• https://www.zyxel.com/bg/bg/

Чехия

• Zyxel Communications Czech s.r.o

• https://www.zyxel.com/cz/cs/

Denmark

• Zyxel Communications A/S

• https://www.zyxel.com/dk/da/

Эстония

• Zyxel Estonia

• https://www.zyxel.com/ee/et/

Финляндия

• Zyxel Communications

• https://www.zyxel.com/fi/fi/

Франция

• Zyxel France

• https://www.zyxel.fr

Германия

• Zyxel Deutschland GmbH

• https://www.zyxel.com/de/de/

Венгрия

• Zyxel Hungary & SEE

• https://www.zyxel.com/hu/hu/

Италия

• Zyxel Communications Italy

• https://www.zyxel.com/it/it/

Латвия

• Zyxel Latvia

• https://www.zyxel.com/lv/lv/

Литва

• Zyxel Lithuania

• https://www.zyxel.com/lt/lt/

Нидерланды

• Zyxel Benelux

• https://www.zyxel.com/nl/nl/

Норвегия

• Zyxel Communications

• https://www.zyxel.com/no/no/

Польша

• Zyxel Communications Poland

• https://www.zyxel.com/pl/pl/

Румыния

• Zyxel Romania

• https://www.zyxel.com/ro/ro

Россия

• Zyxel Russia

• https://www.zyxel.com/ru/ru/

Словакия

• Zyxel Communications Czech s.r.o. organizacna zlozka

• https://www.zyxel.com/sk/sk/

Испания

• Zyxel Communications ES Ltd

• https://www.zyxel.com/es/es/

Швеция

• Zyxel Communications

• https://www.zyxel.com/se/sv/

Швейцария

• Studerus AG

• https://www.zyxel.ch/de

• https://www.zyxel.ch/fr

Турция

• Zyxel Turkey A.S.

• https://www.zyxel.com/tr/tr/

Великобритания

• Zyxel Communications UK Ltd.

• https://www.zyxel.com/uk/en/

Украина

• Zyxel Ukraine

• http://www.ua.zyxel.com

Южная Америка

Аргентина

• Zyxel Communications Corporation

• https://www.zyxel.com/co/es/

Бразилия

• Zyxel Communications Brasil Ltda.

• https://www.zyxel.com/br/pt/

Колумбия

• Zyxel Communications Corporation

• https://www.zyxel.com/co/es/

Эквадор

• Zyxel Communications Corporation

• https://www.zyxel.com/co/es/

Южная Америка

• Zyxel Communications Corporation

• https://www.zyxel.com/co/es/

Ближний Восток

Израиль

• Zyxel Communications Corporation

• http://il.zyxel.com/

Ближний Восток

• Zyxel Communications Corporation

• https://www.zyxel.com/me/en/

Северная Америка

США

• Zyxel Communications, Inc. - North America Headquarters

• https://www.zyxel.com/us/en/

Океания

Австралия

• Zyxel Communications Corporation

• https://www.zyxel.com/au/en/

Африка

ЮАР

• Nology (Pty) Ltd.

• https://www.zyxel.com/za/en/

ПРИЛОЖЕНИЕ B

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.

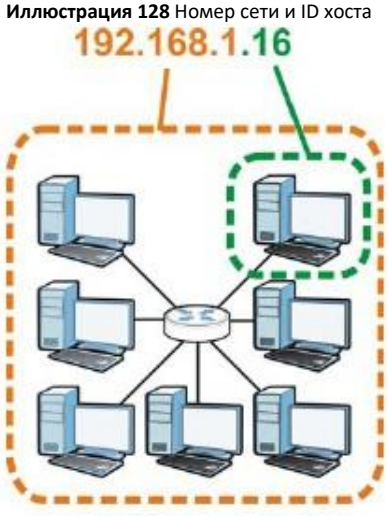
Структура

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 128 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 67 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 68 Маски подсети

	ДВОИЧНЫЕ				**ДЕСЯТИЧНАЯ ЗАПИСЬ**
	1-ЫЙ ОКТЕТ	**2-ЫЙ ОКТЕТ**	**3-ИЙ ОКТЕТ**	**4-ЫЙ 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 69 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 70 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

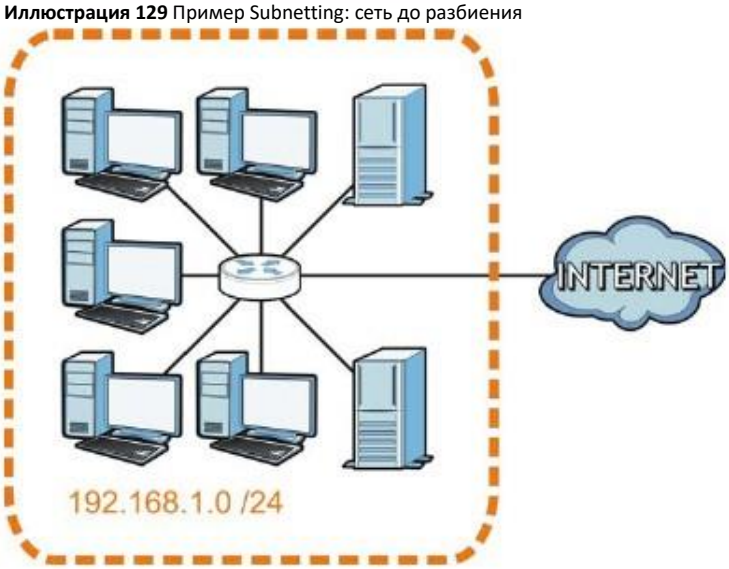
Subnetting (разделение одной сети на несколько)

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 129 Пример Subnetting: сеть до разбиения

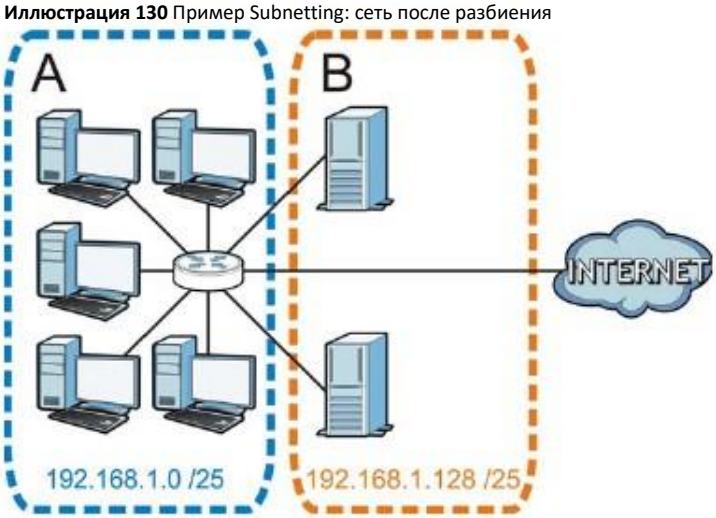


Вы можете «одолжить» один из битов ID хоста чтобы разбить сеть 192.168.1.0 на две подсети. Теперь маска подсети стала 25-битной (255.255.255.128 или /25).

«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 130 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 71 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
IP-адрес (десятичный)	192.168.1.	0
IP Address (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 72 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА В БИТАХ
IP-адрес (десятичный)	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	01000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.0	Начальный ID хоста: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Последний ID хоста: 192.168.1.126	

Таблица 73 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 74 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
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 Host ID: 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 75 Восемь подсетей

ПОДСЕТЬ	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 76 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 77 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
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

Таблица 77 Планирование подсетей в сети (продолжение)

НОМЕР «ОДОЛЖЕННОГО» БИТА ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	ЧИСЛО ХОСТОВ В ПОДСЕТИ
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 NBG-418N v2.

После выбора номера сети выберите IP-адрес для NBG-418N v2, 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. NBG-418N v2 автоматически рассчитает маску подсети на основе введенного вами IP-адреса. Эту маску подсети, которую рассчитал NBG-418N v2, 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 131 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 132 Пример конфликта IP-адресов 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 133 Пример конфликта IP-адресов компьютера и маршрутизатора

ПРИЛОЖЕНИЕ C

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 7) либо разрешите блокировку с исключением для всплывающих окон с IP-адреса вашего устройства

Disable Pop-up Blockers

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

Иллюстрация 134 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 135 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 136 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 137 Pop-up Blocker Settings

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

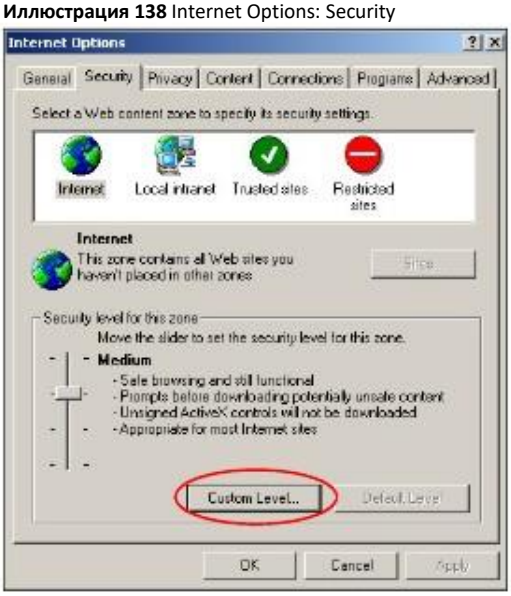
6 Щелкните **Apply** для сохранения настроек.

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 138 Internet Options: Security



2 Щелкните кнопку **Custom Level...**

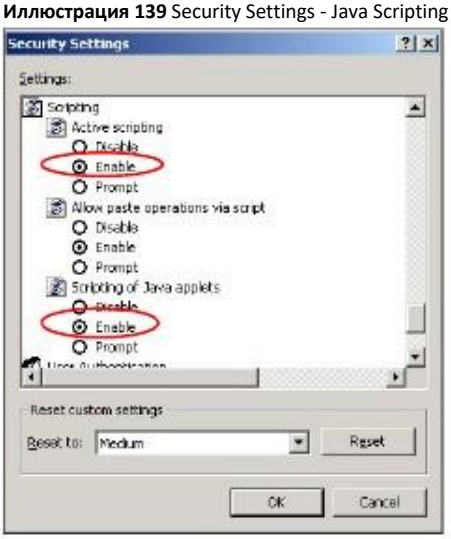
3 Прокрутите список до **Scripting**.

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 139 Security Settings - Java Scripting



Разрешение выполнения Java

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

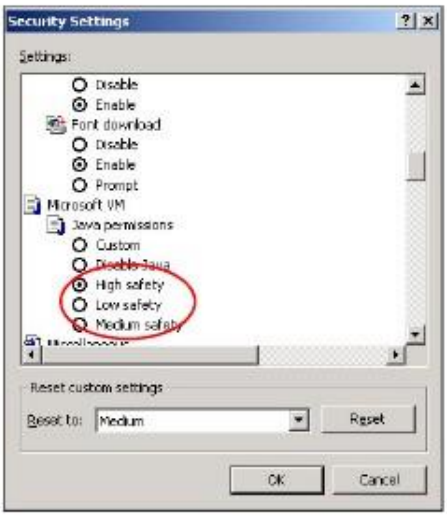
2 Щелкните кнопку **Custom Level...**

3 Прокрутите список до **Microsoft VM**.

4 В **Java permissions** должен быть выбран safety level.

5 Щелкните **OK** чтобы закрыть окно.

Иллюстрация 140 Security Settings - Java



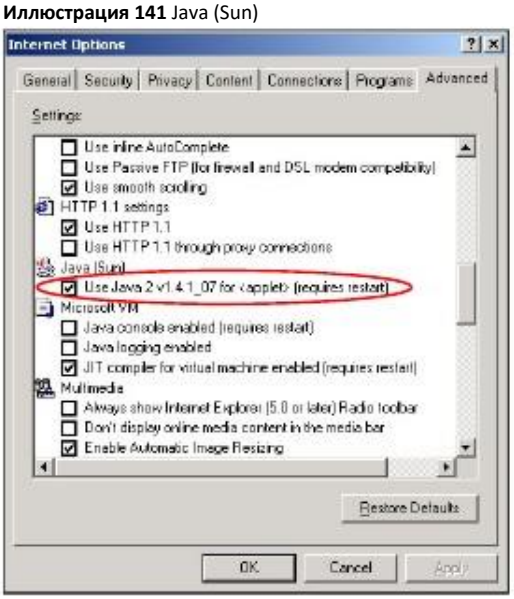
JAVA (Sun)

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 141 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 142 Mozilla Firefox: TOOLS > Options

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

Иллюстрация 143 Mozilla Firefox Content Security

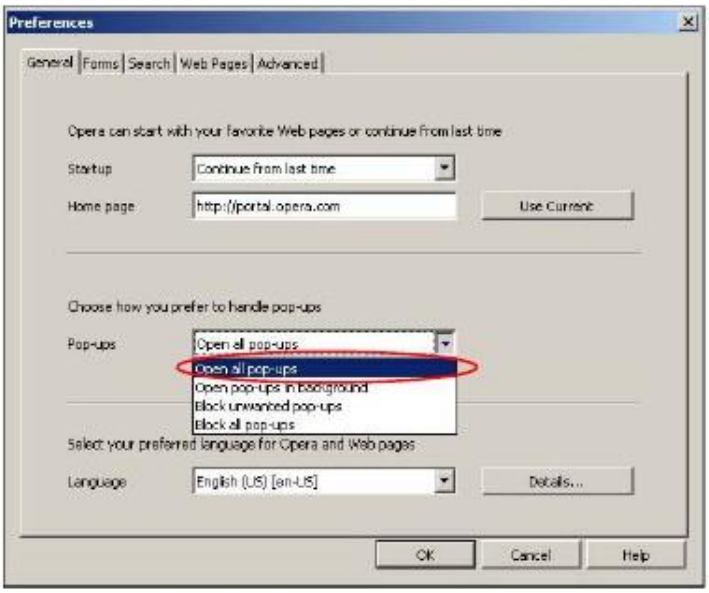
Opera

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**.

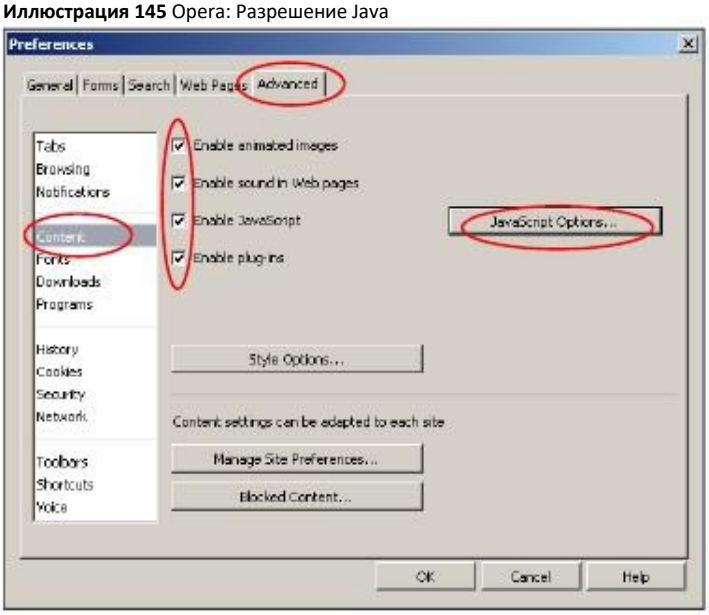
Иллюстрация 144 Opera: Allowing Pop-Ups



Разрешение выполнения кода Java

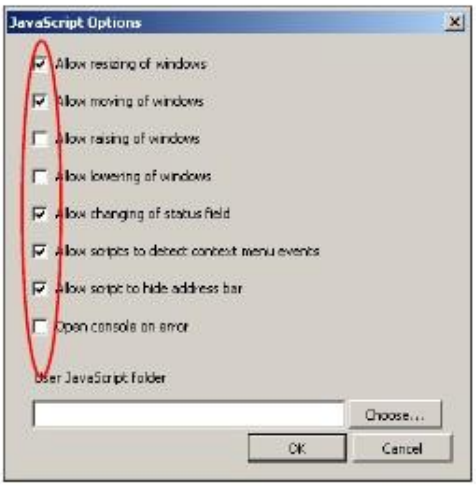
В Opera щелкните **Tools** и затем **Preferences**. Во вкладке **Advanced** выберите в левом меню **Content** и затем поставьте галочки как показано на следующей иллюстрации.

Иллюстрация 145 Opera: Разрешение Java



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

Иллюстрация 146 Opera: JavaScript Options



Выберите нужно опции JavaScript, которые будут разрешены в Opera.

ПРИЛОЖЕНИЕ D

Настройка IP-адреса компьютера

Примечание: Ваша модель NBG-418N v2 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.

If 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 настроить IP-адрес в:

Windows XP/NT/2000

Этот пример с Winsows XP также относится и к Windows 2000 и Windows NT.

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.

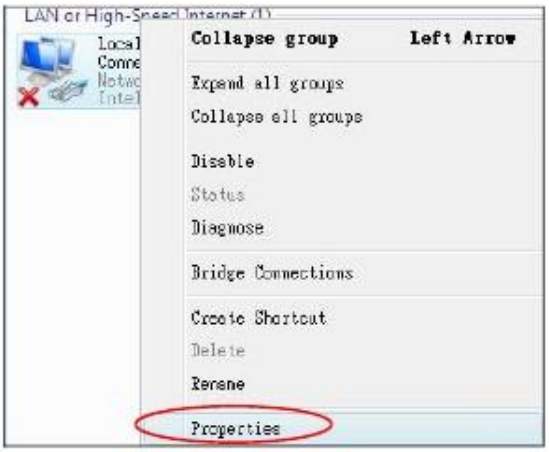
1 Щелкните **Start > Control Panel**.

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

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

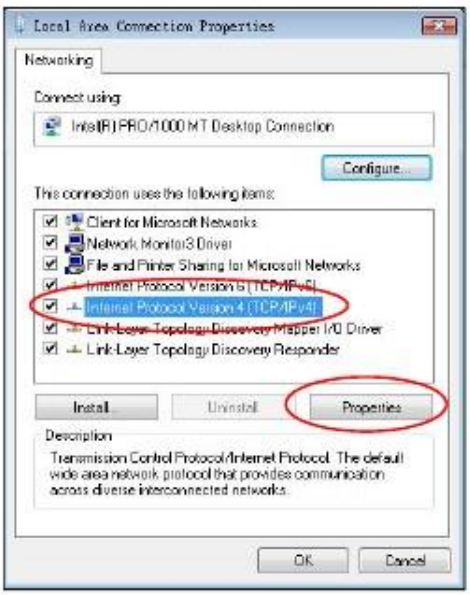
4 Щелкните **Manage network connections**.

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**.

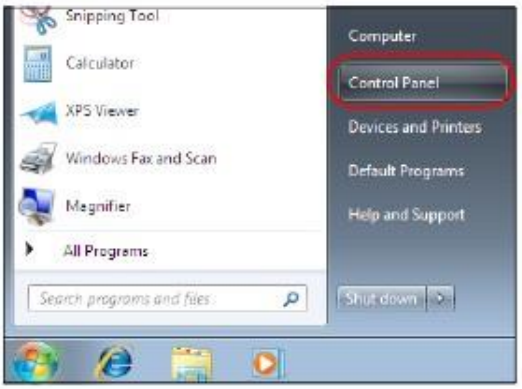
2 В окне **Command Prompt** введите **"ipconfig"** и нажмите **[ENTER]**.

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.

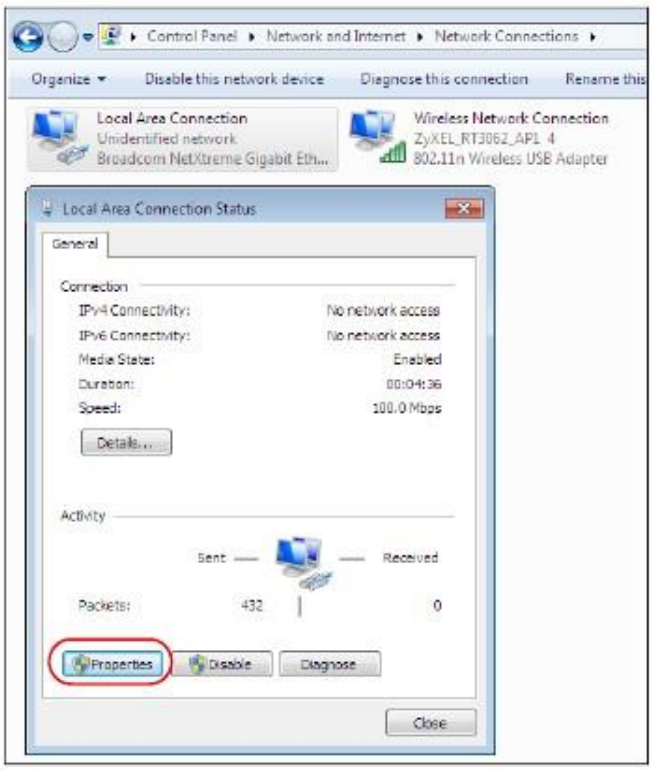
1 Щелкните **Start > Control Panel**.



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

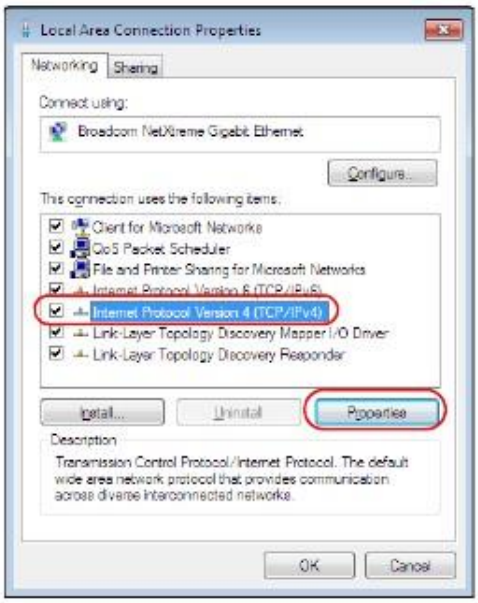
3 Щелкните **Change adapter settings**.

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

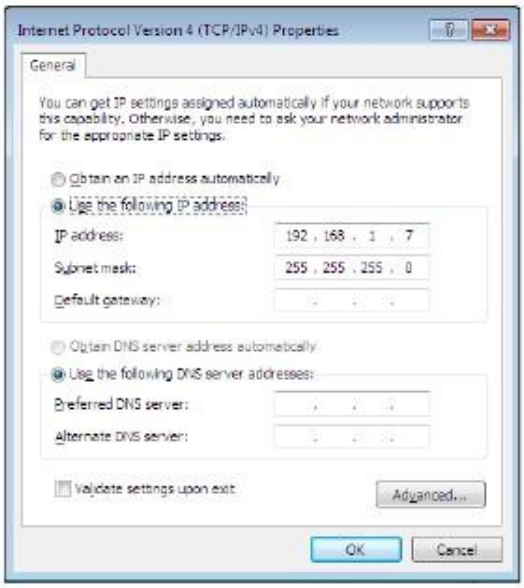


Примечание: Если во время выполнения этой процедуры появится всплывающее окно с просьбой подтвердить продолжение операции, то щелкните **Continue**.

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**.

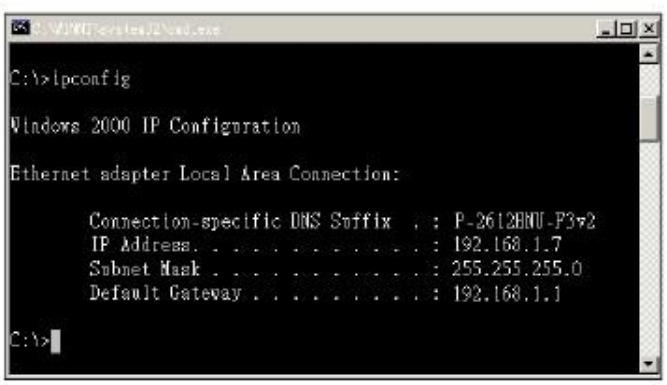
9 Щелкните **OK** чтобы закрыть окно **Local Area Connection Properties**.

Проверка настроек

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

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

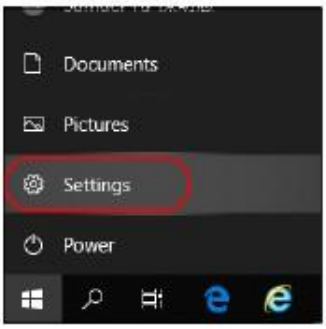
3 На экране будут выведены настройки IP.



Windows 10

На иллюстрациях этого разделе показаны экраны для 10 Pro.

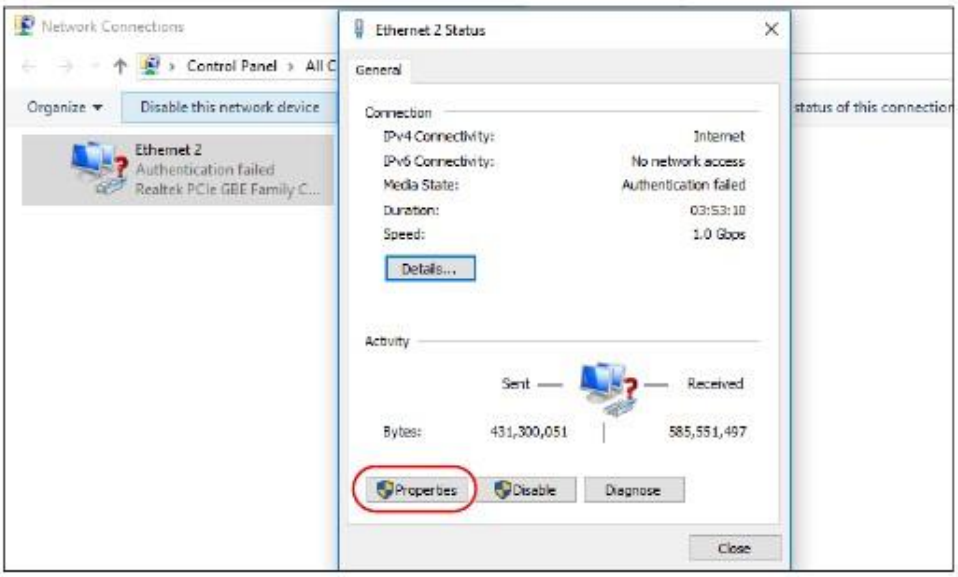
1 Щелкните **Start > Settings**.



2 В окне **Windows Settings** щелкните **Network & Internet**.

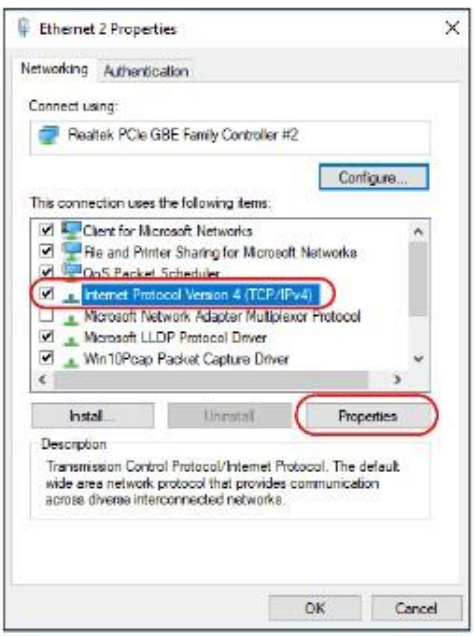
3 Щелкните опцию **Change adapter**. Откроется окно **Network Connections**.

4 Дважды щелкните пиктограмму **Ethernet** и выберите **Properties**.

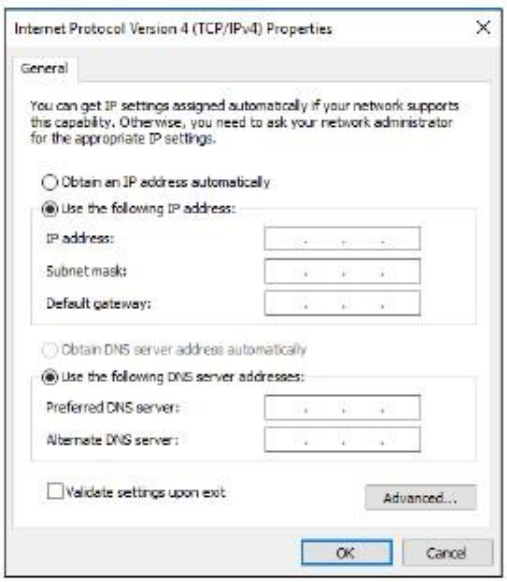


Примечание: Если во время выполнения этой процедуры появится всплывающее окно с просьбой подтвердить продолжение операции, то щелкните **Continue**.

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

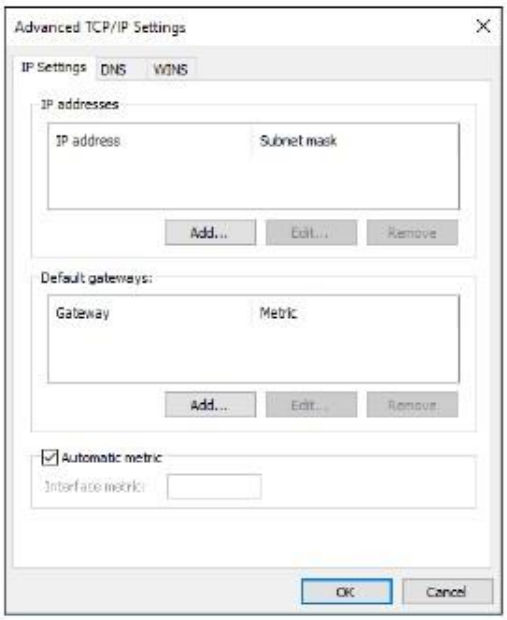


6 Откроется окно **Internet Protocol Version 4 (TCP/IPv4) Properties**.



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 **Advanced TCP/IP Settings**.

9 Щелкните **OK** чтобы закрыть окно **Internet Protocol Version 4 (TCP/IPv4) Properties**.

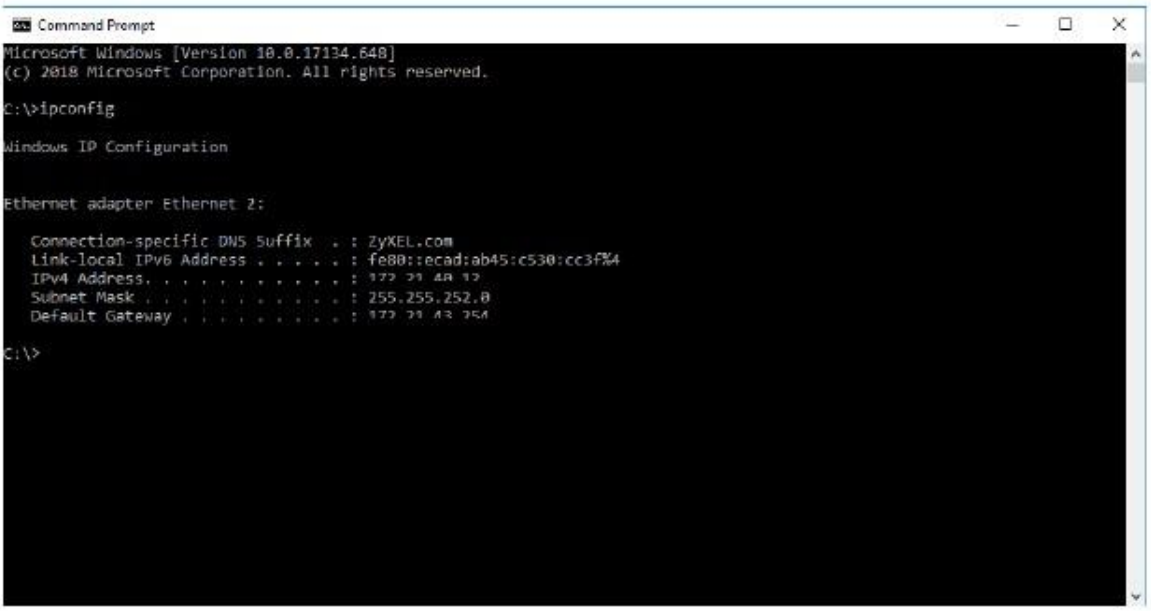
10 Щелкните **OK** чтобы закрыть окно **Ethernet Properties**.

Проверка настроек

1 Щелкните **Start > Windows System > Command Prompt**.

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

3 На экране будут выведены настройки IP.



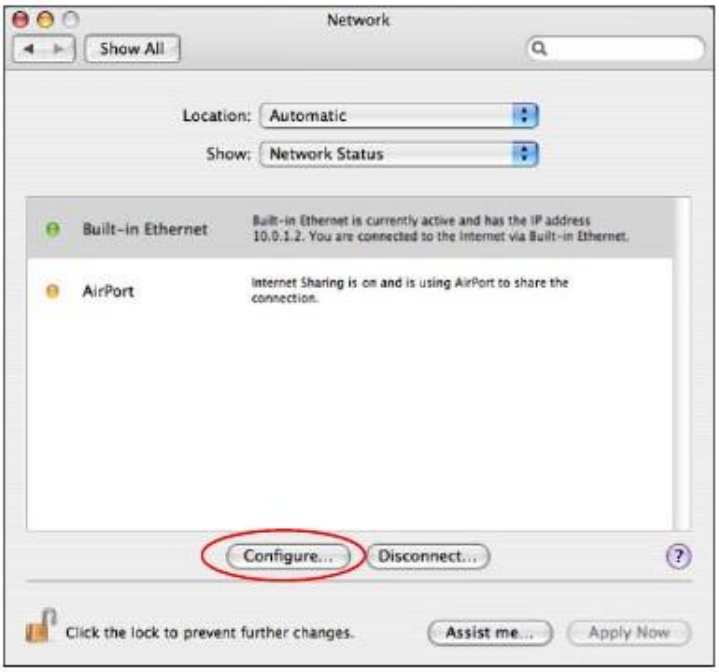
Mac OS X: 10.3 и 10.4

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 147 Mac OS X 10.4: Network Utility

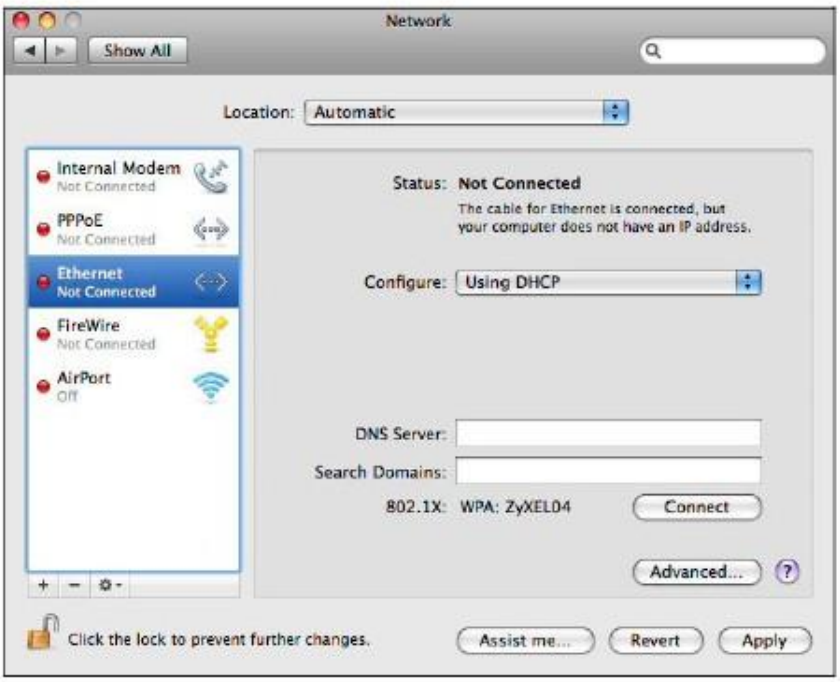
Mac OS X: 10.5 и 10.6

Эти экраны относятся к Mac OS X 10.5 а также к версии 10.6 этой операционной системы.

1 Щелкните **Apple > System Preferences**.

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

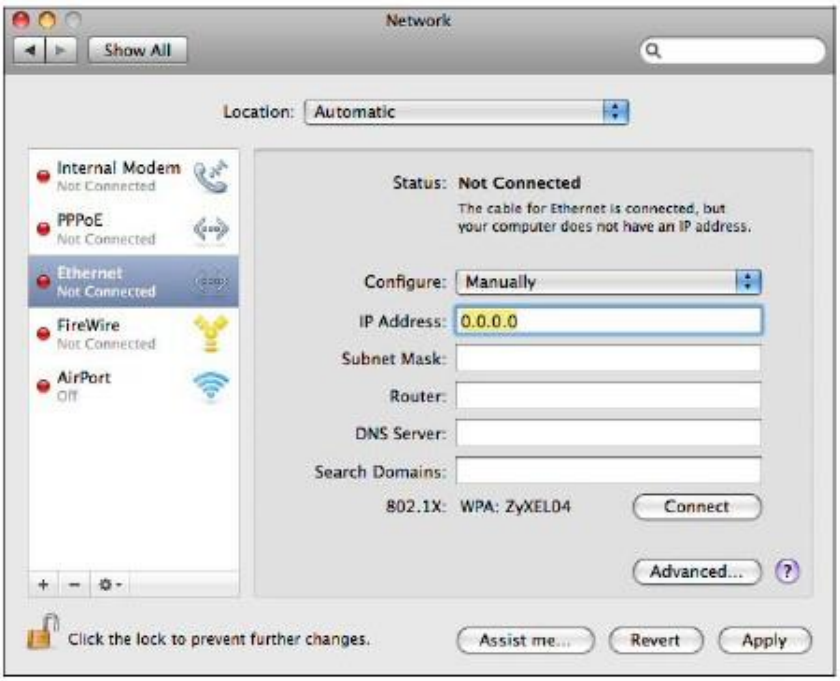
3 Когда откроется панель **Network preferences** выберите **Ethernet** из списка типов сетевых соединений



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 NBG-418N v2.

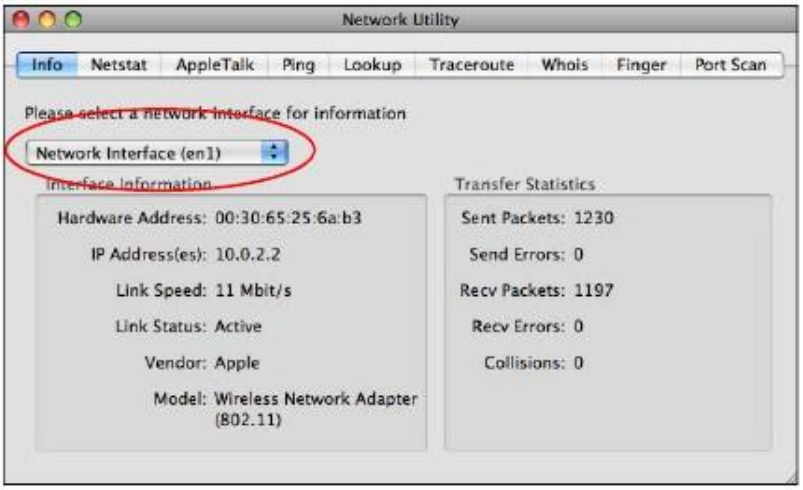


6 Щелкните **Apply** и закройте окно.

Проверка настроек

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

Иллюстрация 148 Mac OS X 10.5: Network Utility



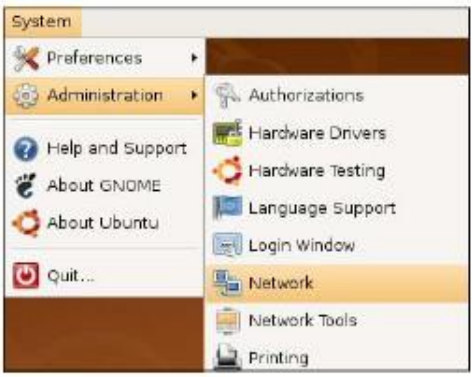
Linux: Ubuntu 8 (GNOME)

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**.

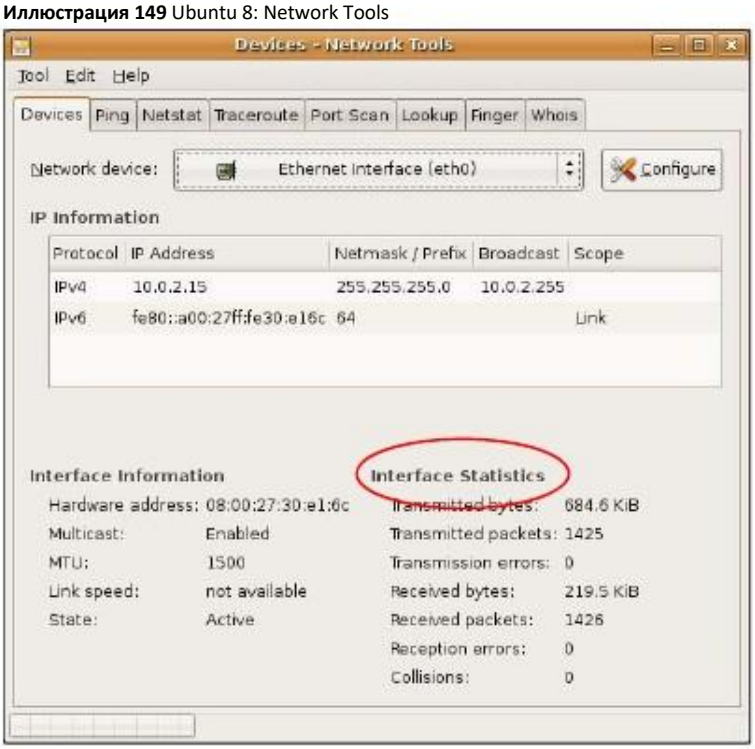
7 Если вы знаете IP-адрес(а) вашего DNS-сервера, то щелкните вкладку **DNS** в окне **Network Settings** и введите информацию о сервере DNS.

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 149 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.

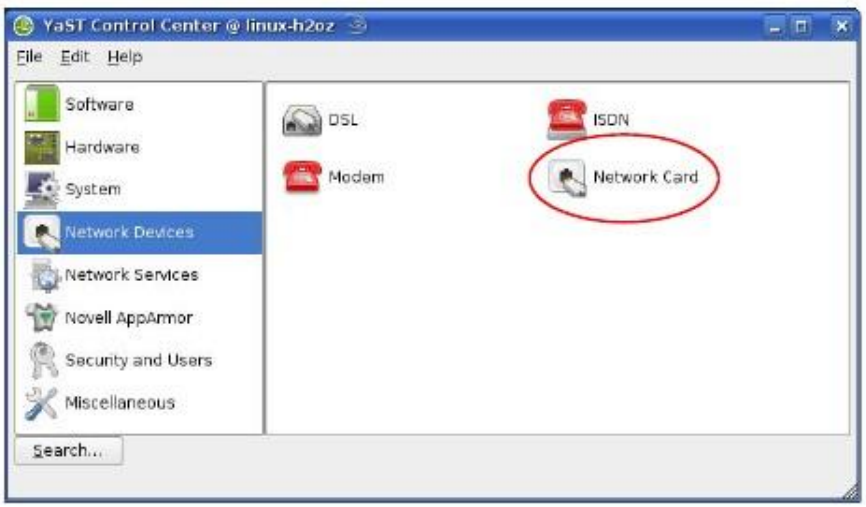
Примечание: Нужно войти в систему как администратор root.

Настройка IP-адреса компьютера в KDE:

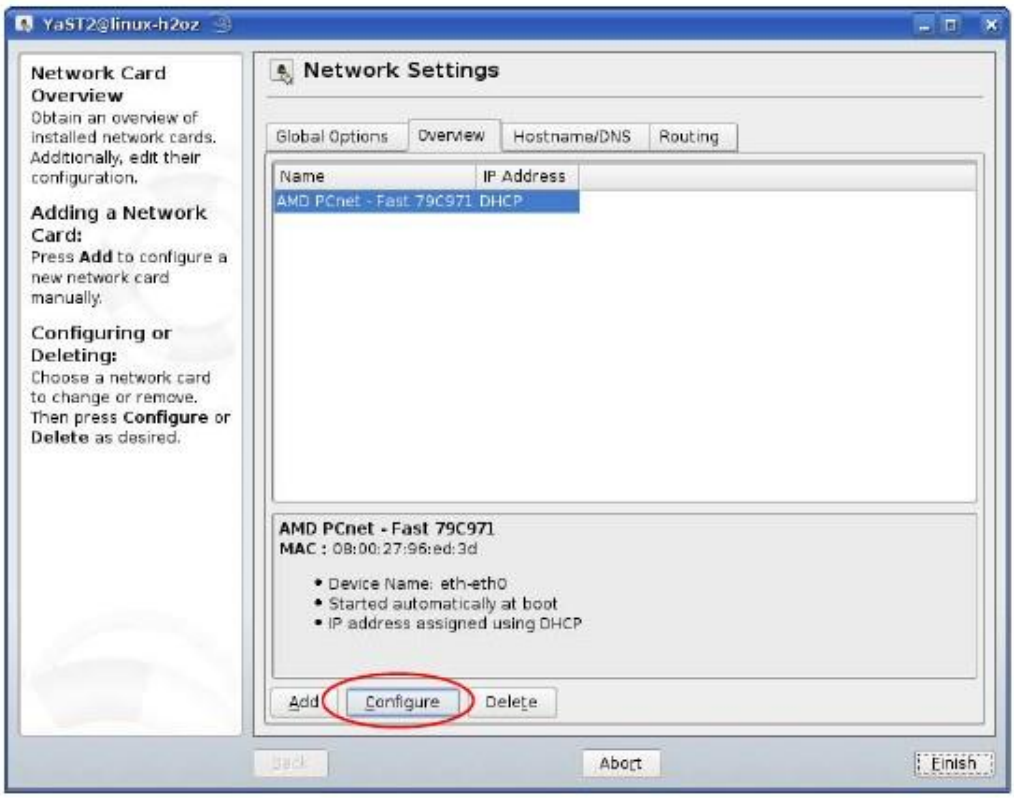
1 Щелкните **K Menu > Computer > Administrator Settings (YaST)**

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**.

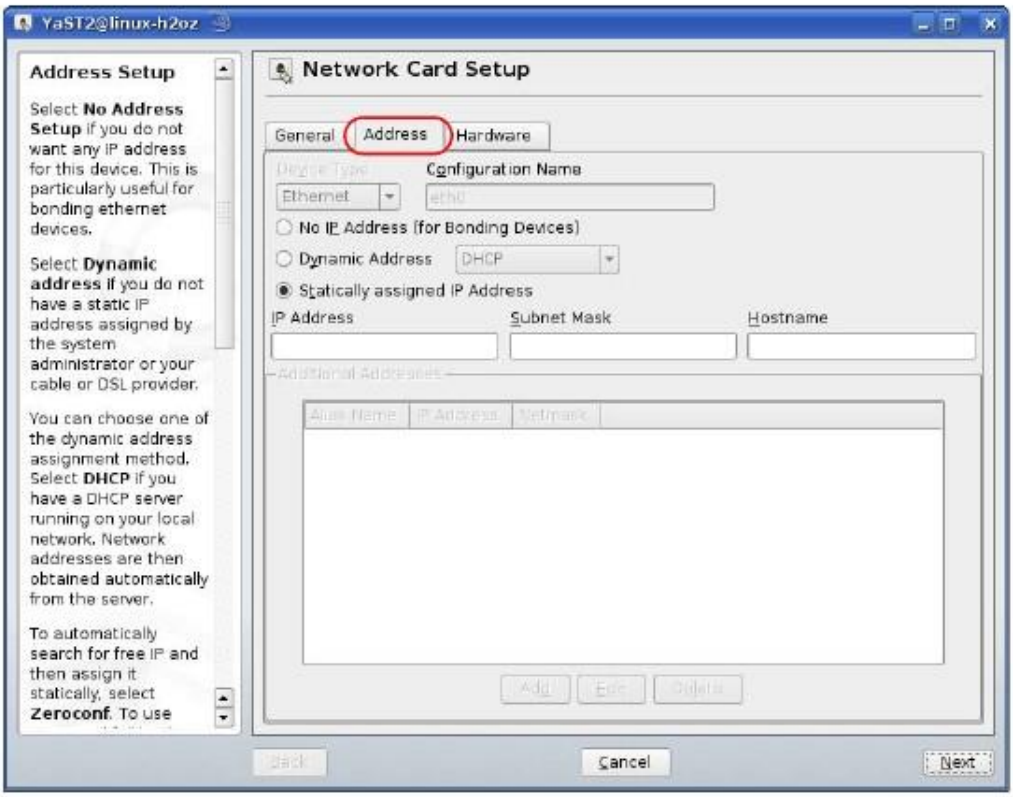


4 Когда откроется окно **Network Settings**, щелкните вкладку **Overview**, выберите из списка имя нужного соединения (**Name**) и щелкните кнопку **Configure**.



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

Иллюстрация 150 openSUSE 10.3: Network Card Setup

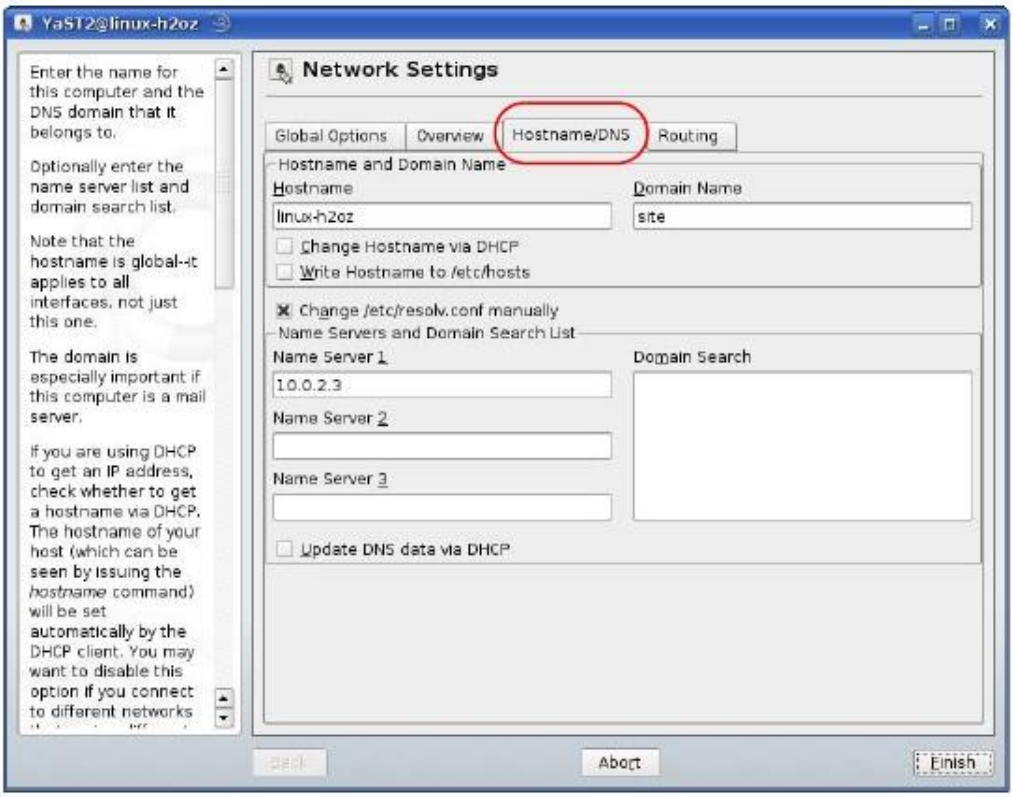


6 Если у вас динамический IP-адрес, то выберите **Dynamic Address (DHCP)**.

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.

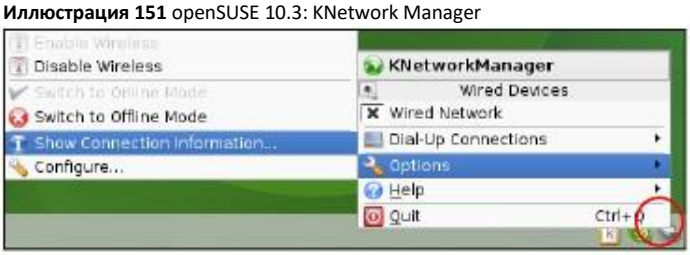


9 Щелкните **Finish** чтобы сохранить настройки и закрыть окно.

Проверка настроек

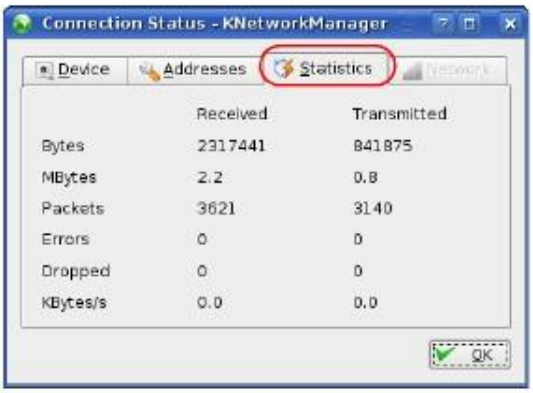
Для проверки настроек TCP/IP щелкните пиктограмму **KNetwork Manager** на панели **Task**. В подменю **Options** выберите **Show Connection Information**.

Иллюстрация 151 openSUSE 10.3: KNetwork Manager



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

Иллюстрация 152 openSUSE: Connection Status - KNetwork Manager



ПРИЛОЖЕНИЕ E

Беспроводная сеть

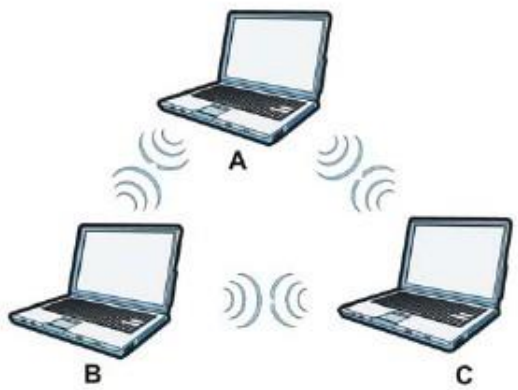
Топологии беспроводной сети

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 153 Соединение Peer-to-Peer Communication в сети Ad-hoc

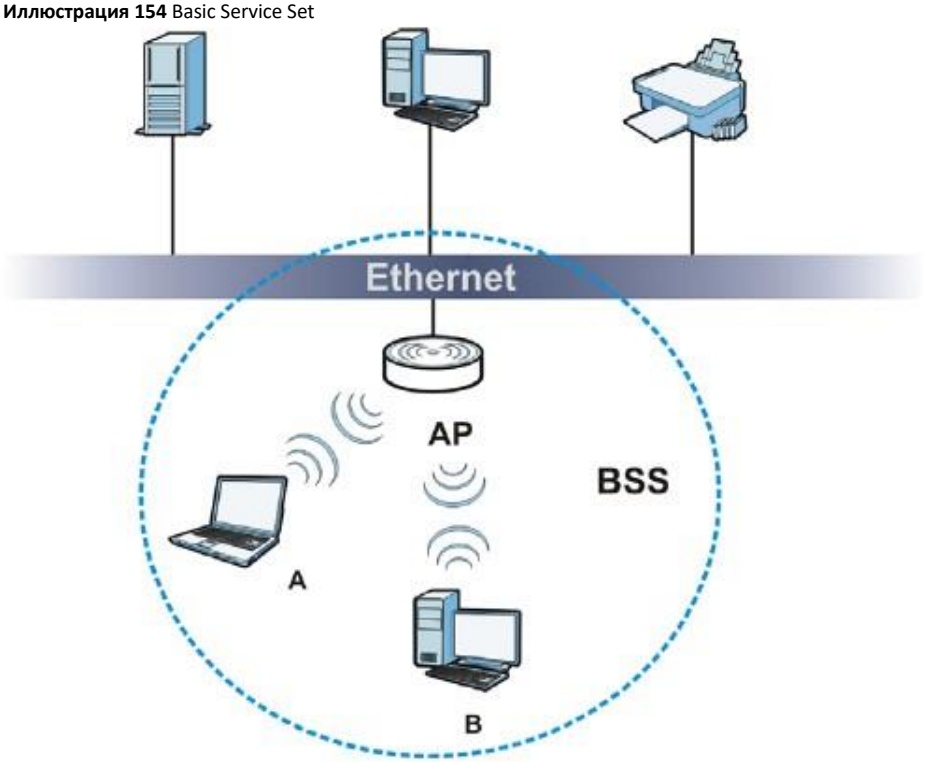


BSS

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 Intra-BSS отключен, то беспроводные клиенты **A** и **B** могут обмениваться данными только с проводной сетью, но не между собой.

Иллюстрация 154 Basic Service Set



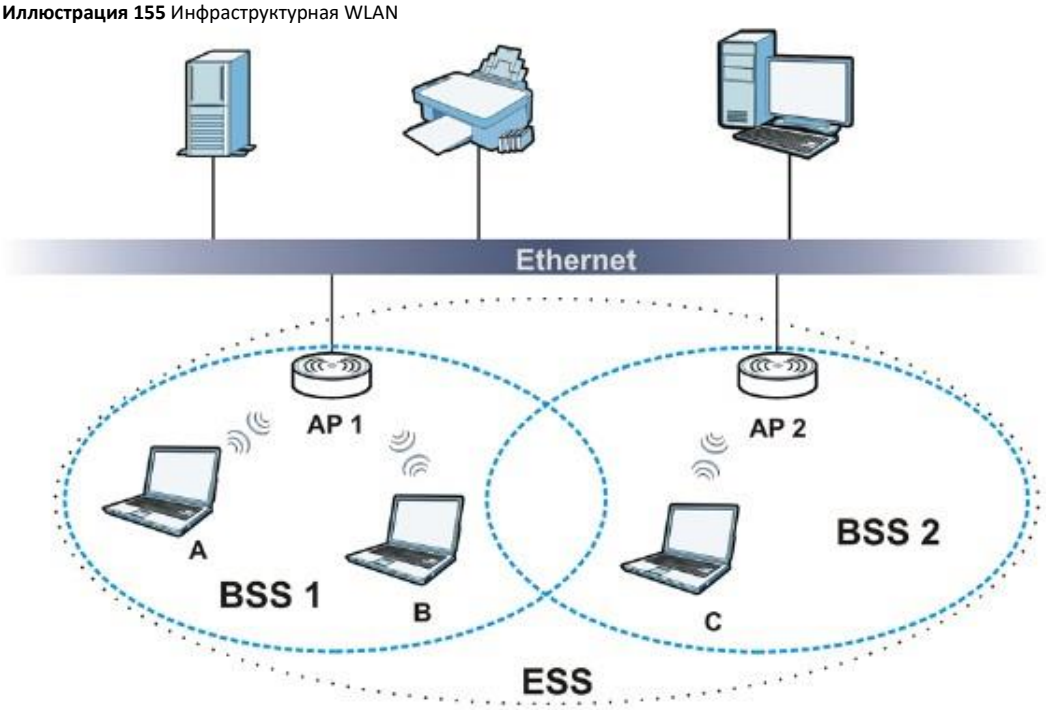
ESS

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 155 Инфраструктурная WLAN



Канал

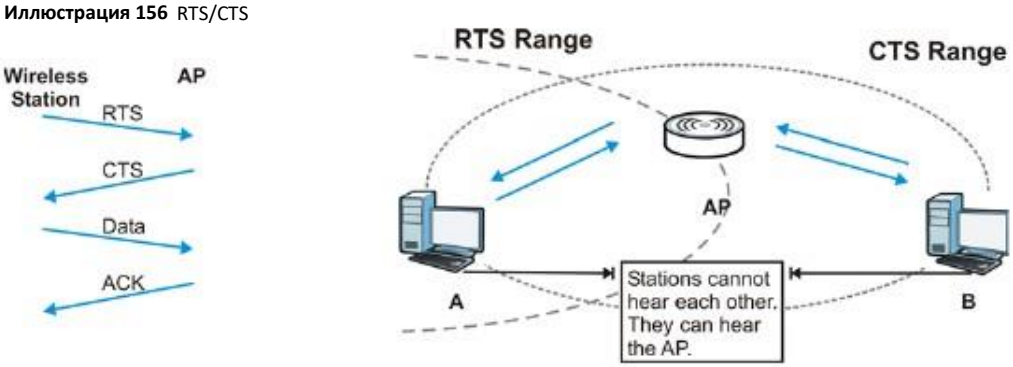
Канал – это частота (частоты) радиосвязи, которые беспроводные клиенты используют для передачи и приема данных. Доступные каналы (частоты) зависят от конкретного географического региона. При выборе из доступных каналов нельзя использовать канал, который уже задействован соседней точкой доступа, иначе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

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 156 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: Хотя RTS Threshold предназначен для улучшения работы сети, он создает дополнительный трафик, из-за которого может упасть производительность 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 NBG-418N v2 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 78 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 NBG-418N v2 поддерживает шифрование данных, аутентификацию клиентов, ограничение доступа к устройству по MAC-адреса и скрытие идентификационных данных NBG-418N v2.

В следующей таблице показана относительная эффективность этих механизмов безопасности, которые поддерживает NBG-418N v2.

Таблица 79 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
Most Secure	

Примечание: На беспроводных клиентах должны использоваться те же настройки безопасности беспроводной сети, что и на NBG-418N v2.

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 - точка доступа ретранслирует сообщения, которыми обмениваются беспроводные клиенты и сетевой сервер RADIUS.

Типы сообщений RADIUS

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

• 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 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 таблице перечислены особенности каждого типа аутентификации.

Таблица 80 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	Легко внедряется	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 распространяет. AES (Advanced Encryption Standard) – это блочный шифр, использующий 256-битный математический алгоритм Rijndael. Оба типа шифрования используют 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.

Wireless Client WPA Supplicants

Wireless client supplicant – это программа, работающая под управлением операционной системы компьютера, и дающая команды беспроводному клиенту по использованию.

Пример использования WPA(2) с RADIUS

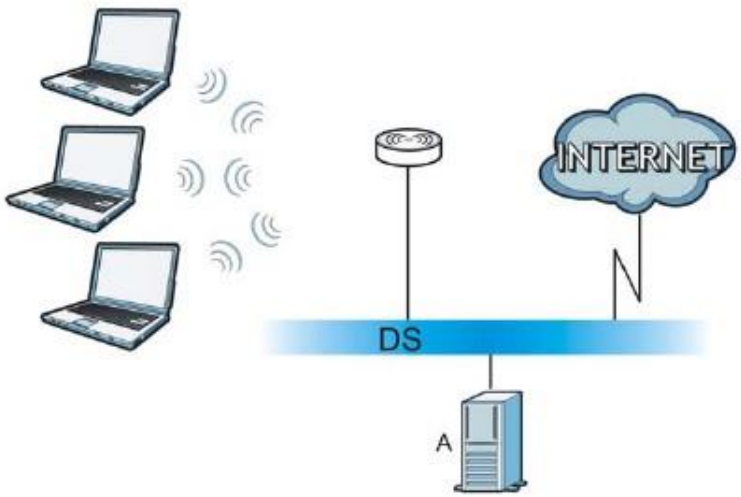
Для настройки WPA(2) нужен IP-адрес сервера RADIUS, номер его порта (по умолчанию 1812) и «общий секретный код» RADIUS. В этом примере применения WPA(2) "A" – это сервер RADIUS, "DS" - distribution system.

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 RADIUS 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 157 Пример применения WPA(2) с RADIUS



Пример использования WPA(2)-PSK

WPA(2)-PSK работает следующим образом:

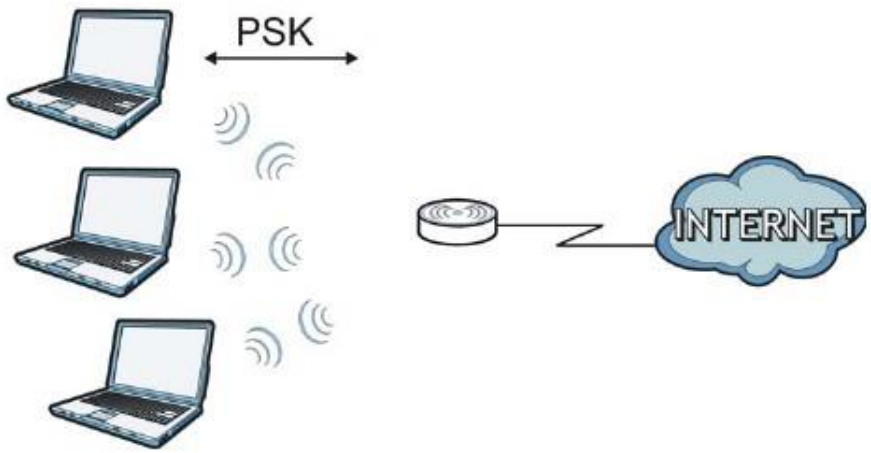
1 Сначала на точке доступа и всех беспроводных клиентах вводится один и тот же пароль. Pre-Shared Key (PSK) состоит из 8 - 63 символов ASCII либо 64 шестнадцатеричных цифр (включая пробелы).

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 158 WPA(2)-PSK Authentication



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 81 Основные типы безопасности беспроводной сети

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	ВВОД КЛЮЧА ВРУЧНУЮ	IEEE 802.1X
Open	None	Нет	Отключен
			Включен без динамического ключа 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 2.4 ГГц или 5 ГГц.

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 F

IPv6

Обзор

IPv6 (Internet Protocol version 6) разработан для расширения адресного пространства и функционала IP. За счет увеличения размера IPv6-адреса до 128 бит (с 32-битных адресов IPv4) максимальное число IP-адресов увеличивается до 3.4 x 10^{38}.

Адресация IPv6

128-битный адрес IPv6 состоит из восьми разделенных двоеточием (:) шестнадцатеричных чисел, например: `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

Адреса IPv6 можно сократить двумя способами:

• Отбросить нули в начале числа, например, `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` можно сократить до `2001:db8:1a2b:15:0:0:1a2f:0`.

• Вместо последовательных блоков нулей использовать двойное двоеточие. Двойное двоеточие можно только один раз использовать в адресе IPv6, например, `2001:0db8:0000:0000:1a2f:0000:0000:0015` можно сократить до `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`,`2001:db8::1a2f:0:0:15` или `2001:db8:0:0:1a2f::15`.

Префикс адреса IPv6 и его длина

Аналогично маске подсети IPv4 в IPv6 адрес сети обозначается с помощью префикса в адресе. Длина префикса IPv6 обозначает, сколько самых важных битов в адресе, начиная с первого левого бита, относятся к адресу сети. Длина префикса обозначается как “/x”, где x is – это число. Например,

```
2001:db8:1a2b:15::1a2f:0/32
```

обозначает, что первые 32 бита (2001:db8) – это префикс подсети.

Адрес Link-local

Адрес link-local - это уникальный идентификатор устройства в локальной сети (LAN). Он аналогичен “частному IP-адресу” IPv4. Один и тот же адрес link-local можно использовать для разных интерфейсов. У unicast-адреса link-local заранее определенный префикс fe80::/10 и записывается этот адрес в следующем формате.:

Таблица 82 Формат unicast-адреса Link-local Unicast

1111 1110 10	0	ID интерфейса
10 битов	54 бита	64 бита

Глобальный адрес

Глобальный адрес - это уникальный идентификатор устройства в Интернете. Он аналогичен публичному IP-адресу в IPv4. Глобальный unicast-адрес начинается с 2 или 3.

Адрес Unspecified

Адрес unspecified (0:0:0:0:0:0:0:0 или ::) используется как адрес отправителя если у устройства нет собственного адреса. Он аналогичен

Адрес Loopback

Адрес loopback (0:0:0:0:0:0:0:1 or ::1) используется чтобы хост мог посылать пакеты себе самого. Он аналогичен “127.0.0.1” в IPv4.

Адрес Multicast

В IPv6 адрес multicast выполняет ту же функцию, что и адрес broadcast в IPv4 (IPv6 не поддерживает Broadcasting). По адресу multicast можно посылать пакеты всем хостам, которые входят в группу a multicast.

Multicast scope определяет размеры группы multicast. У адреса multicast заранее определенный префикс ff00::/8. В следующей таблицы перечислены некоторые предопределенные (predefined) адреса multicast.

Таблица 83 Адреса Predefined Multicast

АДРЕС MULTICAST	ОПИСАНИЕ
FF01:0:0:0:0:0:0:1	Все хосты в локальном узле.
FF01:0:0:0:0:0:0:2	Все маршрутизаторы в локальном узле.
FF02:0:0:0:0:0:0:1	Все хосты на локальном подключенном линке.
FF02:0:0:0:0:0:0:2	Все маршрутизаторы на локальном подключенном линке.
FF05:0:0:0:0:0:0:2	Все маршрутизаторы локального сайта.
FF05:0:0:0:0:0:1:3	Все DHCP-серверы локального сайта.

В следующей таблице перечислены зарезервированные адреса multicast, которые нельзя назначать группе multicast.

Таблица 84 Зарезервированные адреса Multicast

АДРЕС MULTICAST
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0

Таблица 84 Зарезервированные адреса Multicast (продолжение)

АДРЕС MULTICAST
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Маска подсети

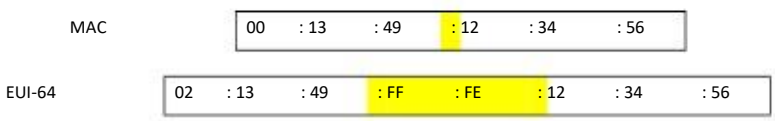
Как адрес IPv6, так и маска подсети IPv6 состоят из 128-битных двоичных цифр, которые разделены на восемь блоков по 16 бит и записываются в виде шестнадцатеричных цифр. В шестнадцатеричном исчислении каждый символ обозначается с помощью четырех битов (1 ~ 10, A ~ F), поэтому каждый 16-битный блок обозначается четырьмя шестнадцатеричными символами, например: FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

ID интерфейса

В IPv6 используется 64-битный идентификатор интерфейса. ID идентифицирует физический интерфейс (например, порт Ethernetport) или виртуальный интерфейс (например, IP-адрес управления в VLAN). У каждого интерфейса свой уникальный ID.

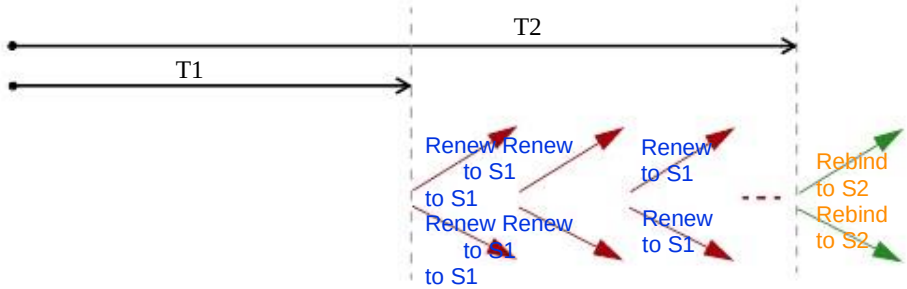
EUI-64

EUI-64 (Extended Unique Identifier) – это разработанный институтом IEEE (Institute of Electrical and Electronics Engineers) формат идентификатора интерфейса, который упрощает внедрение IPv6. Он является расширение 48-битного (6-байтного) MAC-адреса Ethernet (см. ниже). EUI-64 вставляет 16-ричное число fffe между третьим и четвертым байтами MAC-адреса и дополняет 7-й бит первого байта MAC-адреса. См. следующий пример.



Identity Association

Identity Association (IA) – это набор адресов, назначенных клиенту DHCP, с помощью которого сервер и клиент могут управлять набором соответствующих IP-адресов. Каждый IA может быть связан с одним определенным интерфейсом. Клиент DHCP использует IA, назначенный интерфейсу, чтобы получить конфигурацию этого интерфейса с сервера DHCP. Каждый IA состоит из уникального IAID и соответствующей информации IP. Тип IA – это тип адреса в IA. У каждого IA один тип адреса. IA_NA обозначает identity, соответствующую не-временному адресу, а IA_TA – identity, соответствующую временному адресу. У опции IA_NA есть поля T1 и T2, но у опции IA_TA таких полей нет. Сервер DHCPv6 использует T1 и T2 для контроля времени, когда клиент запросил у сервера продления времени жизни любого адреса из IA_NA. После времени T1 клиент посылает серверу (S1) (от которого он получил адреса IA_NA) сообщение Renew. Если ко времени T2 сервер не ответил на это сообщение, то клиент посылается сообщение Rebind любому доступному серверу (S2). Для IA_TA клиент может послать по своему выбору сообщение Renew либо Rebind.



DHCP Relay Agent

Агент DHCP relay agent находится в той же сети, что и клиенты DHCP, и пересылает сообщения между сервером DHCP и клиентами. Если клиент не может по адресу link-local и известному адресу multicast найти в сети сервер DHCP, то он с помощью DHCP relay agent посылает сообщение серверу DHCP, который не подключен к этой сети.

DHCP relay agent может добавить в сообщение Relay-Forward DHCPv6 опции remote identification (remote-ID) и interface-ID. Опция remote-ID содержит определенную пользователем строку, например, имя системы system name. Опция interface-ID сообщает серверу DHCPv6 номер слота, информацию о порте и VLAN ID server. Опция remote-ID option (если она есть) отбрасывается от сообщений the Relay-Reply до того, как relay agent посылает пакеты клиенту. Сервер DHCP копирует опцию interface-ID из сообщения Relay-Forward в сообщение Relay-Reply и снова пересылает его агенту relay agent. interface-ID не меняет даже при перезапуске агента relay agent.

Prefix Delegation (делегирование префиксов)

С помощью делегирования префиксов маршрутизатор IPv6 для своей LAN может использовать префикс IPv6 (адрес сети), который он получил от Интернет-провайдера или маршрутизатора более высокого. NBG-418N v2 использует полученный префикс IPv6 (например, 2001:db2::/48) для генерирования IP-адреса LAN IP. Периодически посылая с помощью multicast сообщения Router Advertisement (RA), NBG-418N v2 передает информацию о префиксе IPv6 хостам в своей LAN. С помощью этого префикса хосты генерируют свои адреса IPv6.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 или ICMP for IPv6) – это спецификация RFC 4443. У ICMPv6 значение предыдущего Next Header равно 58 и оно отличается от значения, которое используется для идентификации ICMP для IPv4. ICMPv6 является частью IPv6. Узлы IPv6 используют ICMPv6 для сообщения о ошибках, которые возникают при обработке пакетов и выполнения других функций диагностики, например "ping".

Neighbor Discovery Protocol (NDP)

Протокол Neighbor Discovery Protocol (NDP) используется для обнаружения других устройств IPv6 и отслеживания доступности соседей в сети. Устройства IPv6 используют следующие типы сообщений ICMPv6:

• Neighbor solicitation: Запрос хоста для определения адреса link-layer address соседа (MAC-адреса) и доступности соседа (reachable). Сосед считается “reachable” если он ответил на сообщение neighbor solicitation от хоста сообщением neighbor advertisement.

• Neighbor advertisement: Ответ узла для «рекламы» своего адреса link-layer address.

• Router solicitation: запрос хоста на поиск маршрутизатора, который может работать как default router и пересылать пакеты.

• Router advertisement: Ответ на a router solicitation или периодический periodical multicast advertisement от маршрутизатора для «рекламы» своего присутствия и других параметров.

IPv6 Cache

Хост IPv6 должен иметь кэш соседа, кэш назначения, список префиксов и список маршрутизаторов по умолчанию. NBG-418N v2 поддерживает и обновляет свой кэш IPv6, постоянно используя информацию из ответа на свои запросы. В IPv6 модуль NBG-418N v2 автоматически настраивает адрес link-local address, а затем посылает сообщение neighbor solicitation message чтобы проверить, не является ли адрес уникальным. Если есть адрес, принадлежность которого нужно выяснить, то NBG-418N v2 также посылает запрос neighbor solicitation message. Если NBG-418N v2 получает в ответ "рекламу" соседа, то он сохраняет адрес link-local address соседа в кэше соседа. Когда NBG-418N v2 использует сообщение link-local address для запроса маршрутизатору и получает в ответ "рекламное" сообщение маршрутизатора, то он добавляет информацию о маршрутизаторе в кэш соседа, список префиксов и кэш назначения. NBG-418N v2 создает запись в кэше списка маршрутизаторов по умолчанию в том случае, когда маршрутизатор можно использовать как маршрутизатор по умолчанию.

Когда NBG-418N v2 нужно послать пакет, то сначала он определяет следующий хоп по кэшу назначения. Если в кэше назначения нет подходящей записи, NBG-418N v2 использует список префиксов, чтобы определить, находится ли адрес назначения на связи (on-link) и доступен ли он напрямую (без пересылки через маршрутизатор). Если с адресом нет связи (unlink), то адрес считается следующим хопом. В противном случае NBG-418N v2 определяет следующий хоп из списка маршрутизаторов по умолчанию или таблицы маршрутизации. После определения IP-адреса следующего хопа NBG-418N v2 просматривает соседний кэш, чтобы получить адрес link-layer address и, когда сосед станет доступен, посылает пакет. Если NBG-418N v2 не может обнаружить запись в кэше соседа или сосед недоступен, то запускает процесс "разрешения" адресов (address resolution). Это помогает уменьшить количество запросов IPv6 и "рекламных" сообщений.

Multicast Listener Discovery

Протокол Multicast Listener Discovery (MLD) (спецификация RFC 2710) разработан на основе версии для IPv4 протокола Internet Group Management Protocol version 2 (IGMPv2). MLD использует тип сообщений ICMPv6 вместо типа сообщений IGMP. MLDv1 эквивалентен IGMPv2, а MLDv2 эквивалентен IGMPv3.

С помощью MLD коммутатор или маршрутизатор IPv6 обнаруживает присутствие тех MLD listener, которые хотят получать пакеты multicast, и IP-адреса групп хостов multicast, которые хотят присоединиться к сети.

MLD snooping и MLD proxy являются аналогами IGMP snooping и IGMP proxy, используемыми в IPv4.

MLD filtering контролирует, к каким группам multicast может присоединиться порт.

Сообщения MLD

Маршрутизатор или коммутатор multicast периодически посылает запросы general queries хостам MLD для обновления таблицы multicast forwarding table. Если хост MLD хочет присоединиться к группе multicast, то он посылает сообщение MLD Report на этот адрес.

Сообщение MLD Done эквивалентно сообщению IGMP Leave. Если хост MLD хочет покинуть группу multicast, то он посылает сообщение Done коммутатору или маршрутизатору. Затем коммутатор или маршрутизатор посылает запрос, относящийся к группе, тому порту, который получил сообщение Done, чтобы определить, должны ли оставаться в группе другие устройства, подключенные к этому порту.

Пример - включение IPv6 в Windows XP/2003/Vista

По умолчанию Windows XP и Windows 2003 поддерживают IPv6. В этом примере команда `ipv6 install`используется в Windows XP/2003 для включения IPv6, а также с помощью команды `ipconfig` выводится автоматически генерируемые IP-адреса.

```
C:\>ipv6 install
Installing..
Succeeded.


C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific   DNS  Suffix   . :
        IP Address. . . . .   . . . . . . . : 10.1.1.46
        Subnet Mask . . . .   . . . . . . . : 255.255.255.0
        IP Address. . . . .   . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . .   . . . . . . . : 10.1.1.254
```

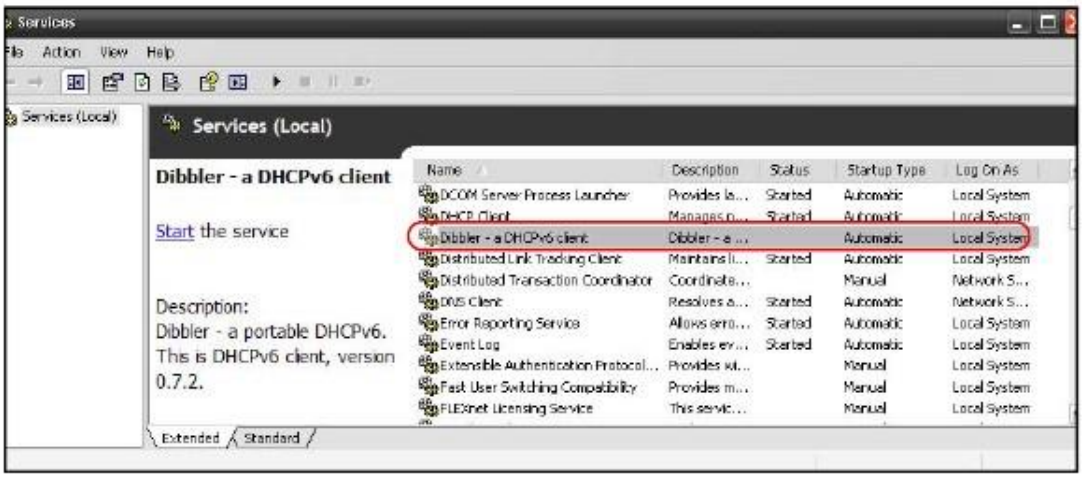
В Windows Vista по умолчанию IPv6 инсталлирован и включен. Для проверки автоматически сконфигурированных адресов IPv6 используйте команду `ipconfig`. Она выведет по крайней мере один адрес IPv6, доступный для интерфейса на вашем компьютере.

Пример - включение DHCPv6 в Windows XP

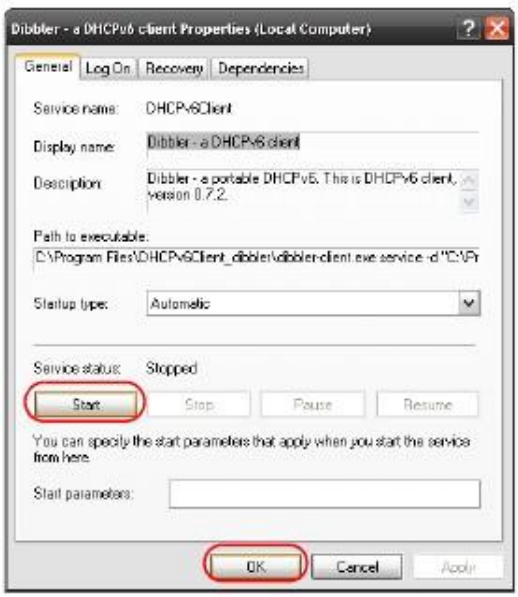
Windows XP не поддерживает DHCPv6. Если в вашей сети IP-адреса назначаются с помощью DHCPv6, то на компьютере Windows XP нужно установить клиентскую программу DHCPv6. (Примечание: этот раздел можно пропустить если вы используете статические IP-адреса или Router Advertisement для назначения адресов IPv6 в вашей сети).

В этом примере в качестве клиента DHCPv6 используется Dibbler. Для включения клиента DHCPv6 на вашем компьютере нужно:

1. Инсталлируйте на компьютере Dibbler и выберите опцию DHCPv6 client.
2. После завершения инсталляции выберите **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
3. Выберите **Start > Control Panel > Administrative Tools > Services**.
4. Дважды щелкните **Dibbler - a DHCPv6 client**.



5 Щелкните **Start** и потом **OK**.



6 Теперь ваш компьютер сможет получать адрес IPv6 от сервера DHCPv6.

Пример - Enabling IPv6 on Windows 7

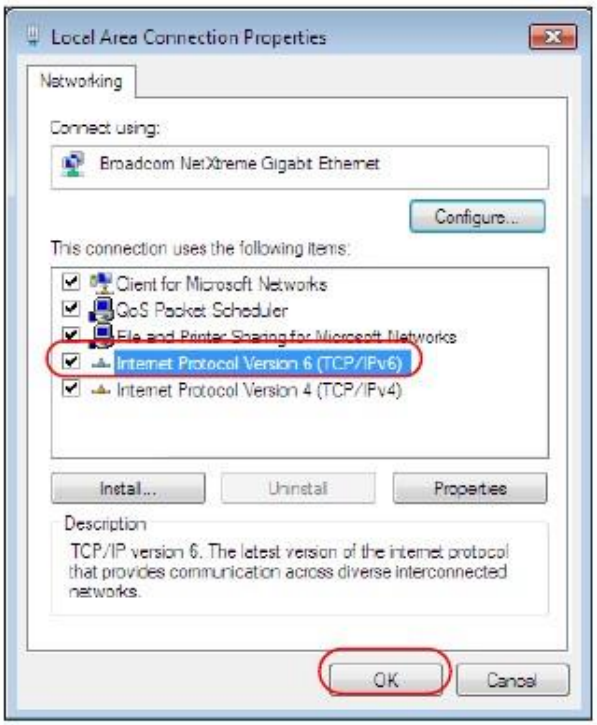
Windows 7 по умолчанию поддерживает IPv6. Также при включении IPv6 на компьютере Windows 7 будет включен и DHCPv6.

Для включения enable IPv6 в Windows 7:

1 Выберите **Control Panel > Network and Sharing Center > Local Area Connection**.

2 Поставьте галочку напротив **Internet Protocol Version 6 (TCP/IPv6)**.

3 Щелкните **OK** для сохранения изменений.



4 Щелкните **Close** чтобы уйти с экрана Local Area Connection Status.

5 Выберите **Start > All Programs > Accessories > Command Prompt**.

6 Командой `ipconfig` проверьте ваш динамический адрес IPv6. В этом примере от сервера DHCP получен глобальный адрес (2001:b021:2d::1000).

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS   Suffix   . :
   IPv6 Address. . . . . .   . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address   . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . .   . . . . . : 172.16.100.61
   Subnet Mask . . . . . .   . . . . . : 255.255.255.0
   Default Gateway . . . .   . . . . . : fe80::213:49ff:feaa:7125%11
                                         172.16.100.254
```

ПРИЛОЖЕНИЕ G

Стандартные сервисы

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**, то это номер протокола IP.

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

Таблица 85 Стандартные сервисы

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	User-Defined	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)	User-Defined	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 85 Стандартные сервисы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
ICMP	User-Defined	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	Еще одна популярная 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	User-Defined	1	Packet INternet Groper – это протокол запросов ICMP echo для проверки доступности 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)	User-Defined	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 the 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 85 Стандартные сервисы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТЫ(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.